Red Hat build of Keycloak 22.0

Release Notes

Last Updated: 2024-06-03

Legal Notice

Abstract

This guide consists of release notes for Red Hat build of Keycloak.

Table of Contents

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. RED HAT BUILD OF KEYCLOAK 22.0

1.1. OVERVIEW

Red Hat is proud to introduce a new era of identity and access management named Red Hat build of Keycloak. The release of Red Hat build of Keycloak 22.0 replaces any plans for releasing Red Hat Single Sign-On 8.0 or a higher release.

Red Hat build of Keycloak is based on the Keycloak project, which enables you to secure your web applications by providing Web SSO capabilities based on popular standards such as OpenID Connect, OAuth 2.0, and SAML 2.0. The Red Hat build of Keycloak server acts as an OpenID Connect or SAML-based identity provider (IdP), allowing your enterprise user directory or third-party IdP to secure your applications by using standards-based security tokens.

While preserving the power and functionality of Red Hat Single Sign-on, Red Hat build of Keycloak is faster, more flexible, and efficient. Red Hat build of Keycloak is an application built with Quarkus, which provides developers with flexibility and modularity. Quarkus provides a framework that is optimized for a container-first approach and provides many features for developing cloud-native applications.

1.2. UPDATES FOR 22.0.11

This release contains several fixed issues including a fix for CVE-2024-4540. This fix is for a security issue affecting some OIDC confidential clients using PAR (Pushed authorization request). In case you use OIDC confidential clients together with PAR and you use client authentication based on **client_id** and **client_secret** sent as parameters in the HTTP request body (method **client_secret_post** specified in the OIDC specification), it is highly encouraged to rotate the client secrets of your clients after upgrading to this version.

1.3. UPDATES FOR 22.0.10

The release includes several fixed issues. For details, see Fixed Issues.

1.4. UPDATES FOR 22.0.9

This release includes support for installation on Windows systems. For Windows installations, you use the **kc.bat** command instead of the **kc.sh** command.

This release also include Fixed Issues and Known Issues.

1.5. UPDATES FOR 22.0.8

This release includes a fix for CVE-2023-6927.

The release also includes Fixed Issues and Known Issues.

1.6. UPDATES FOR 22.0.7

The release includes several fixed issues. For details, see Fixed Issues.

1.7. NEW FEATURES AND ENHANCEMENTS

The following release notes apply to Red Hat build of Keycloak 22.0.

1.7.1. New distribution based on Red Hat build of Quarkus

Red Hat build of Keycloak 22.0 uses a streamlined distribution model based on Red Hat build of Quarkus instead of Red Hat JBoss Enterprise Application Platform. The new distribution simplifies configuration and operation, resulting in these changes compared to Red Hat Single Sign-On.

- Simpler configuration procedures with interactive command-line help. Instead of editing opaque and complex XML files, you choose from multiple configuration sources, such as a file, the CLI, environment variables, or an encrypted KeyStore.
- Faster startup time and low memory footprint. The server distribution is smaller, the container image contains fewer dependencies and Red Hat build of Keycloak performs multiple optimizations, which lead to better runtime performance.
- JDBC drivers for PostgreSQL, MariaDB, SQL Server, and MySQL included in the distribution.
- Faster feature updates and fixes to issues. The Red Hat build of Keycloak lifecycle is closely aligned with Keycloak, which means that the codebase is closer to upstream and upgrades with innovations can be delivered faster.
- Support for built-in metrics.
- Greater security for the Container Image by making the following changes:
  - The image is based on UBI9 rather than UBI8.
  - Uses of -minimal are replaced by-micro.

1.7.2. New Operator

Red Hat build of Keycloak 22 introduces a brand new OpenShift Operator with reimagined Custom Resources (CRs) to make full use of the new Red Hat build of Quarkus based distribution in modern cloud-native environments. The resulting changes extend the Operator's capabilities and remove some of the most prominent limitations compared to Red Hat Single Sign-On Operator.

- Full Red Hat build of Keycloak server configuration support through Keycloak CR
- Close alignment of configuration UX with bare metal installations to simplify Operator adoption
- Support for all databases that the Red Hat build of Keycloak server supports
- Realm Import CR supports capturing full Realm representation in comparison to a few selected fields in Red Hat Single Sign-On Operator's Realm CR

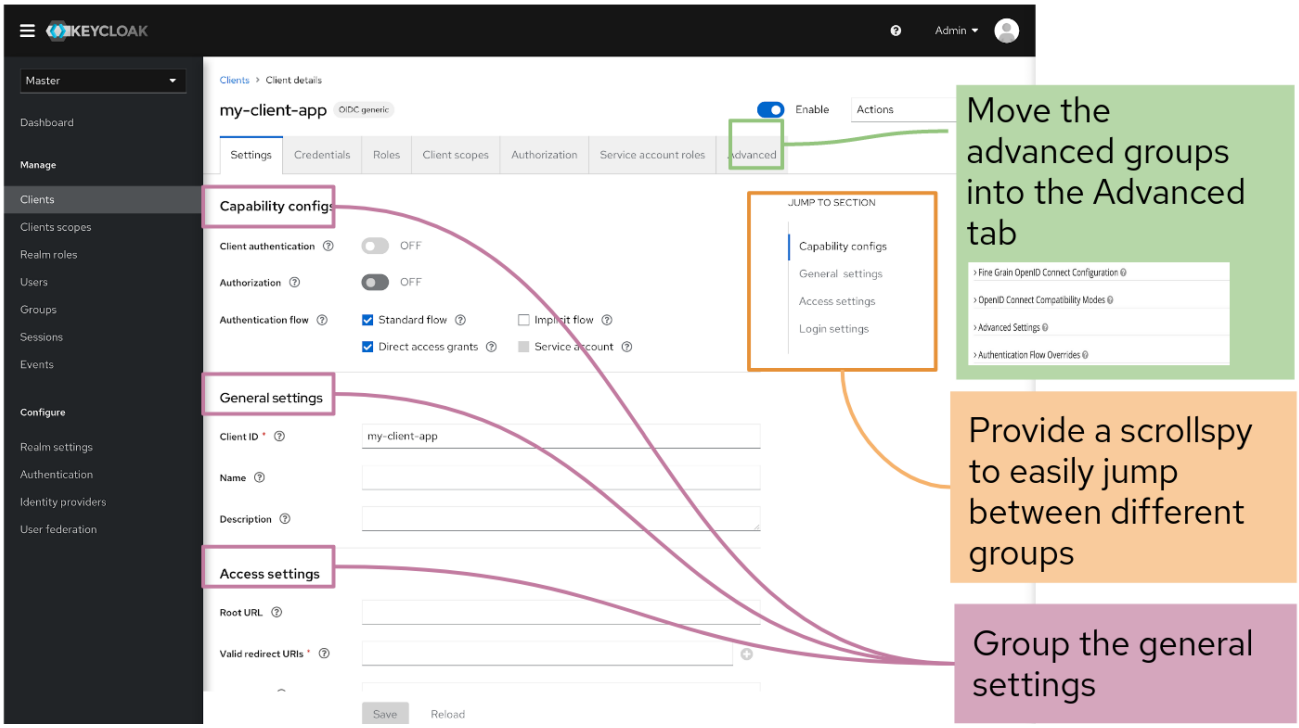
1.7.3. Admin Console v2

The Admin Console v2 is redesigned to be easier to use and more accessible. The v2 console provides the same capabilities, such as creating client applications, managing users, and monitoring sessions, but now these actions are much easier to perform.

1.7.3.1. Reorganized pages

The Admin Console v1 had many pages filled with long lists of controls. You could easily miss the advanced features at the bottom. In the v2 console, that type of page is revised to group the general controls together and the advanced functionality has moved to its own tab.

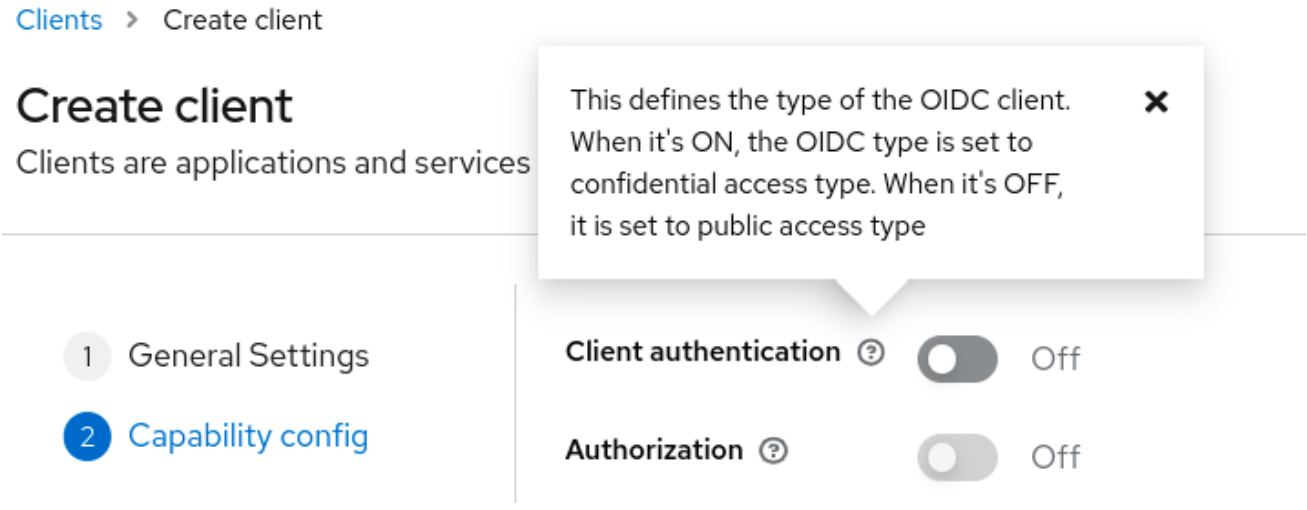
Controls are organized into advanced and general groups



1.7.3.2. Tooltips are easier to use

In the v1 console, when you hover over a field, the tooltips block fields you need to set. In the v2 console, you click a question mark (?) to display tooltips. Even expert users find they cannot recall the meaning of every control, so the tooltips are important.

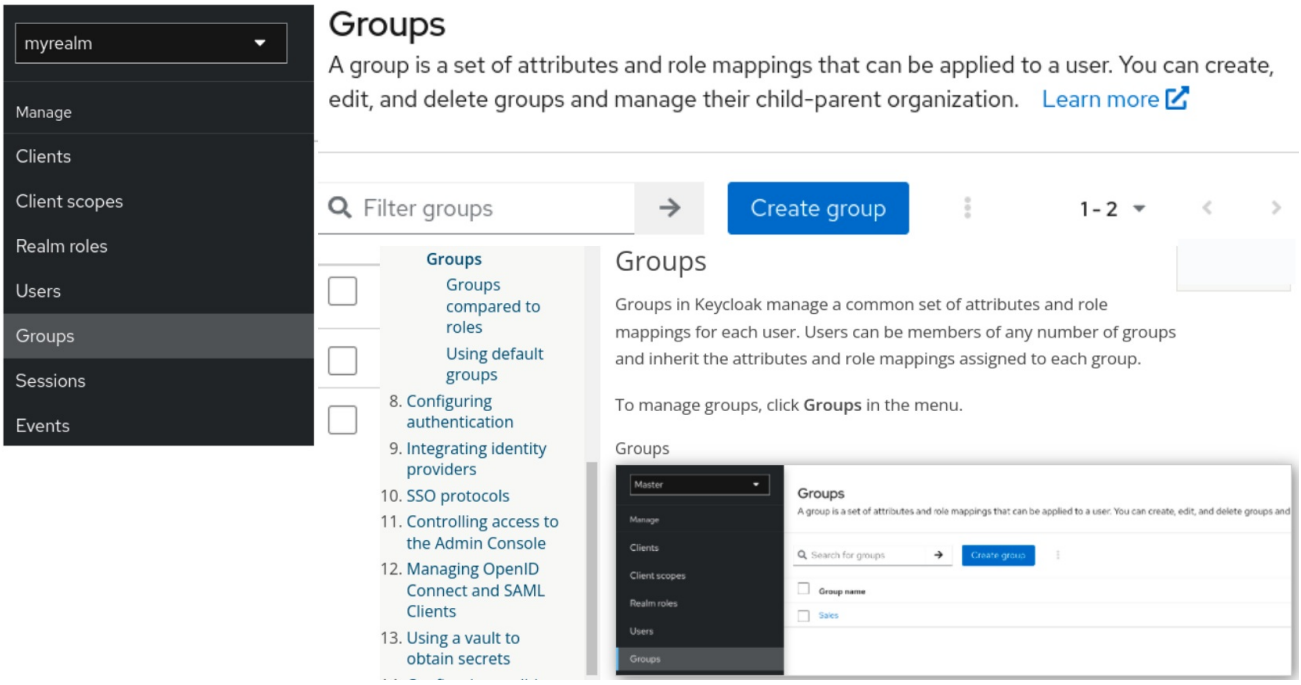
Improved tooltips do not hide field names



1.7.3.3. Quick access to related documentation

If you need more help, you can click **Learn More** to see the related documentation topic. You do not need to hunt for the right guide and then search that guide for the right topic. Just click **Learn More**.

Learn More buttons display related documentation



1.7.3.4. Accessibility enhancements

The v2 console has major accessibility improvements to provide a better user experience for users with visual impairments and users who use screen readers. For example:

- For users with low vision or color vision deficiencies, text elements now meet the WCAG 2 AA contrast ratio thresholds, providing clear contrast to background colors.
- For users who rely on screen readers, form elements include labels and all input fields have accessible names. Also, images now have alternative text.
- For interactive controls, each focusable element now has an active and unique ID, eliminating confusion and aiding navigation.

The new design features many improvements in flow and organization while retaining all functionality. However, one change exists for bearer-only clients, which are clients that use no OAuth flows. This access type is no longer a choice when you create a client, but the bearer-only switch still exists on the server side. See the Server Administration Guide for more details.

1.7.4. FIPS version 140-2 support

Support for deploying Red Hat build of Keycloak 22.0 into a FIPS 140-2 enabled environment is available. For the details, see FIPS 140-2.

1.7.5. OpenJDK 17 support

Red Hat build of Keycloak supports OpenJDK 17 for both the server and adapters.

- The Red Hat build of Keycloak server is supported only on OpenJDK 17.
- Adapters are supported only on OpenJDK 11 and 17.

1.7.6. Adapter support

The following Java Client Adapters are no longer released starting with Red Hat build of Keycloak 22:

- JBoss EAP 6
- JBoss EAP 7
- Spring Boot
- JBoss Fuse 6
- JBoss Fuse 7

In contrast to the initial release of OpenID Connect, this protocol is now widely supported across the Java Ecosystem and much better interoperability and support is achieved by using the capabilities available from the technology stack, such as your application server or framework.

These capabilities have now reached their end-of-life and are available only from Red Hat Single Sign-On 7.6. Therefore, before the end of the long-term support, consider alternative capabilities for your applications.

Whenever you find issues integrating Red Hat build of Keycloak with Red Hat Single Sign-On Client Adapters, you now have compatibility mode settings from the Client Settings in the administration console cases. Therefore, you can disable some aspects of the Red Hat build of Keycloak server to preserve compatibility with older client adapters. More details are available in the tool tips of individual settings.

For more details, see the Migration Guide.

1.7.7. Other improvements

Red Hat build of Keycloak 22.0 includes the following additional improvements over Red Hat Single Sign-On 7.6.

1.7.7.1. SAML backchannel logout

Red Hat build of Keycloak 22.0 includes SAML SOAP Backchannel single-logout, which provides a real backchannel logout capability to a SAML client registered in Red Hat build of Keycloak. This feature adds the capability to receive logout requests sent by SAML clients over SOAP binding.

1.7.7.2. OIDC logout

Red Hat Single Sign-On 7.6 included support for OIDC logout. Red Hat build of Keycloak 22.0 contains these improvements to OIDC logout:

- Support for the **client_id** parameter, which is based on the OIDC RP-Initiated Logout 1.0 specification. This capability is useful to detect what client should be used for Post Logout Redirect URI verification in case that **id_token_hint** parameter cannot be used. The logout confirmation screen still needs to be displayed to the user when only the **client_id** parameter is used without the **id_token_hint** parameter so clients are encouraged to use the **id_token_hint** parameter if they do not want the logout confirmation screen to be displayed to the user.

- The **Valid Post Logout Redirect URIs** configuration option is added to the OIDC client and is aligned with the OIDC specification. You can use a different set of redirect URIs for redirection after login and logout. The value **+** used for **Valid Post Logout Redirect URIs** means that the logout uses the same set of redirect URIs as specified by the option of **Valid Redirect URIs**. This change also matches the default behavior when migrating from a previous version due to backwards compatibility.

For more details, see OIDC logout in the Server Administration Guide.

1.7.7.3. Search groups by attribute

You can now search groups by attribute by using the Admin REST API in a similar way to a client search by attributes.

1.7.7.4. Support for count users based on custom attributes

The User API now supports querying the number of users based on custom attributes. The /{realm}/users/count endpoint contains a new **q** parameter. It expects the following format:

```
q=<name>:<value> <attribute-name>:<value>
```

1.7.7.5. View group membership in the Account Console

You can now allow users to view their group memberships in the Account Console. A user must have the **account, view-groups** option for the groups to show up in that console.

1.7.7.6. Essential claim configuration in OpenID Connect identity providers

OpenID Connect identity providers support a new configuration to specify that the ID tokens issued by the identity provider must have a specific claim. Otherwise, the user can not authenticate through this broker.

The option is disabled by default; when it is enabled, you can specify the name of the JWT token claim to filter and the value to match (supports regular expression format).

1.7.7.7. Support for JWE encrypted ID Tokens and UserInfo responses in OpenID Connect identity providers

The OpenID Connect identity providers now support Json Web Encryption (JWE) for the ID Token and the UserInfo response. The providers use the realm keys defined for the selected encryption algorithm to perform the decryption.

1.7.7.8. Hardcoded group mapper

The new hardcorded group mapper allows adding a specific group to users brokered from an Identity Provider.

1.7.7.9. User session note mapper

The new user session note mapper allows mapping a claim to the user session notes.

1.7.7.10. Improvements in LDAP and Kerberos integration

Red Hat build of Keycloak supports multiple LDAP providers in a realm, which support Kerberos integration with the same Kerberos realm. When an LDAP provider is unable to find the user who was authenticated through Kerberos/SPNEGO, Red Hat build of Keycloak tries to fall back to the next LDAP provider. Red Hat build of Keycloak has also better support for the case when a single LDAP provider supports multiple Kerberos realms, which are in trust with each other.

1.8. TECHNOLOGY PREVIEW AND DEVELOPER PREVIEW FEATURES

Red Hat build of Keycloak includes several technology preview and developer preview features. You are strongly cautioned against using these features in a production environment. They are disabled by default and may be changed or removed at a future release. For more detail on Technology and Developer Preview features, see Developer and Technology Previews.

Red Hat build of Keycloak includes several technology preview and developer preview features. You are strongly cautioned against using these features in a production environment. They are disabled by default and may be changed or removed at a future release. For more detail on Technology and Developer Preview features, see Developer and Technology Previews.

The following Technology Preview features exist. They are described in the Server Administration Guide.

- Client secret rotation, which increases security by alleviating problems such as secret leakage
- Recovery codes, an alternate method of two-factor authentication
- User profile configuration, which uses a declarative style and supports progressive profiling
- Scripts, the option to use JavaScript to write custom authenticators
- Update email flow, which supports users when changing email addresses

The following Developer Preview features exist. Developer Preview features are not documented.

- Token exchange, a process of using a set of credentials or token to obtain a completely different token; this feature was previously a technology preview feature.
- Fine-grained admin permissions, which assign restricted access policies for managing a realm; this feature was previously a technology preview feature.
- Map Storage, an alternative way to store realm information in other databases and stores.

1.9. REMOVED AND DEPRECATED FEATURES

These features were removed:

- JBoss EAP 6 and 7 OpenID Connect adapters
- Spring Boot OpenID Connect adapter
- Java Servlet Filter OpenID Connect adapter
- JBoss EAP 6 and 7 SAML adapters
- Account Console v1
- Admin Console v1
- Technology preview for replacing OpenShift 3 internal IdP with Red Hat build of Keycloak
- Client and User CRs for the Operator (temporarily removed).
- Legacy cross-site replication (formerly a Technology Preview feature)

- Deprecated methods that apply to data providers, user session provider. See the corresponding replacements, which are documented in Javadoc.

This feature is deprecated:

- Loading the Red Hat build of Keycloak JavaScript adapter directly from the Red Hat build of Keycloak server.

1.10. FIXED ISSUES

Each release includes fixed issues:

- Red Hat build of Keycloak 22.0.11 Fixed Issues .
- Red Hat build of Keycloak 22.0.10 Fixed Issues .
- Red Hat build of Keycloak 22.0.9 Fixed Issues .
- Red Hat build of Keycloak 22.0.8 Fixed Issues .
- Red Hat build of Keycloak 22.0.7 Fixed Issues .

1.11. KNOWN ISSUES

The 22.0.11 version includes the following known issue:

- RHBK-721 - Instructions for adding custom attributes to the Account Console do not work

1.12. SUPPORTED CONFIGURATIONS

For the supported configurations for Red Hat build of Keycloak 22.0, see Supported configurations.

1.13. COMPONENT DETAILS

For the list of supported component versions for Red Hat build of Keycloak 22.0, see Component details.