univention
be open.

Keycloak app 18.0.2

Release 18.0.2

Univention GmbH

Jul 18, 2022

CONTENTS

Welcome to the documentation about the Univention **Keycloak** app. The app installs Keycloak[1], an open source software product for single sign-on with identity and access management. Furthermore, the app adds authentication to applications and secure services.

This documentation is for system administrators who operate the **Keycloak** app from Univention App Center connected to the LDAP directory in Univention Corporate Server (UCS). It covers the following topics:

This documentation doesn't cover the following topics:

- Usage of Keycloak itself, see the *Keycloak 18.0.0 Documentation* [1].
- Usage of UCS (Univention Corporate Server), see *UCS 5.0 Manual* [2].

To understand this documentation, you need to know the following concepts and tasks:

- Use and navigate in a remote shell on Debian GNU/Linux derivative Linux distributions like UCS. For more information, see Shell and Basic Commands[2] from *The Debian Administrator's Handbook*, Hertzog and Mas [3].
- Manage an app through Univention App Center[3] in *UCS 5.0 Manual* [2].
- Know the concepts of SAML (Security Assertion Markup Language[4]) and OIDC (OpenID Connect[5]) and the differences between the two standards.

Your feedback is welcome and highly appreciated. If you have comments, suggestions, or criticism, please send your feedback[6] for document improvement.

[1] https://www.keycloak.org/
[2] https://www.debian.org/doc/manuals/debian-handbook/short-remedial-course.en.html#sect.shell-and-basic-commands
[3] https://docs.software-univention.de/manual/5.0/en/software/further-software.html#computers-softwareselection
[4] https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
[5] https://en.wikipedia.org/wiki/OpenID#OpenID_Connect_(OIDC)
[6] https://www.univention.com/feedback/?keycloak-app=generic

CHAPTER

ONE

INSTALLATION

You can install the **Keycloak** app like any other app with Univention App Center. The App Center only allows to install Keycloak on a UCS system with the system role *Primary Director Node*. For more information, see Primary Directory Node[7] in *UCS 5.0 Manual* [2].

UCS offers two different ways for app installation:

- With the web browser in the UCS management system
- With the command-line

For general information about Univention App Center and how to use it for software installation, see Univention App Center[8] in *UCS 5.0 Manual* [2].

1.1 Installation with the web browser

To install Keycloak from the UCS management system, use the following steps:

1. Use a web browser and sign in to the UCS management system.
2. Open the *App Center*.
3. Select or search for *Keycloak* and open the app with a click.
4. To install Keycloak, click *Install*.
5. Leave the *App settings* in their defaults or adjust them to your preferences. For a reference, see *Settings* (page 8).
6. To start the installation, click *Start Installation*.

Note: To install apps, the user account you choose for login to the UCS management system must have domain administration rights, for example the username `Administrator`. User accounts with domain administration rights belong to the user group `Domain Admins`.

For more information, see Delegated administration for UMC modules[9] in *UCS 5.0 Manual* [2].

[7] https://docs.software-univention.de/manual/5.0/en/domain-ldap/system-roles.html#domain-ldap-primary-directory-node
[8] https://docs.software-univention.de/manual/5.0/en/software/app-center.html#software-appcenter
[9] https://docs.software-univention.de/manual/5.0/en/central-management-umc/delegated-administration.html#delegated-administration

1.2 Installation with command-line

To install the **Keycloak** app from the command-line, use the following steps:

1. Sign in to a terminal or remote shell with a username with administration rights, for example `root`.
2. Choose between default and custom settings and run the appropriate installation command.

   For installation with default settings, run:

```
$ univention-app install keycloak
```

   To pass customized settings to the app during installation, run the following command:

```
$ univention-app install --set $SETTING_KEY=$SETTING_VALUE keycloak
```

> **Caution:** Some settings don't allow changes after installation. To overwrite their default values, set them before the installation. For a reference, see *Settings* (page 8).

   Example: To define a different administration user in Keycloak, run:

```
$ univention-app install --set keycloak/admin/user="Administrator" keycloak
```

1.3 Sign in to Keycloak Admin Console

After a successful installation, signed in domain administrator users see the tile *Keycloak* on the UCS Portal, that directs them to the *Keycloak Admin Console*.

The URL has the following scheme: `https://ucs-sso-ng.`*`$domainname`*`/admin/`. The *`$domainname`* is your UCS domain name.

Example: https://ucs-sso-ng.example.com/admin/

The username for login is the *name of the initial admin user* defined during installation and saved in the UCR variable *`keycloak/admin/user`* (page 8).

Note: All users in the `Domain Admins`, for example the domain user `Administrator`, can also sign in to the Keycloak Admin Console.

1.4 Fetch metadata for service provider configuration

OIDC (OpenID Connect) and SAML (Security Assertion Markup Language) both offer machine readable information to the services that want to use the authentication services in Keycloak. This information is the metadata discovery documents.

In the Keycloak Admin Console you can find them at *realm settings* ‣ *UCS* ‣ *Endpoints*. At the endpoints you see *OpenID Endpoint Configuration* and *SAML 2.0 Identity Provider Metadata*. To view the metadata discovery documents, click the endpoint entries.

With the following commands you can obtain the URLs to the metadata information. Some services comfortably take the URL and configure the authentication automatically.

To download the metadata information for OIDC, run the following command:

```
$ wget "https://ucs-sso-ng.$(hostname -d)/keycloak/realms/ucs/.well-known/openid-
↪configuration"
```

To download the metadata information for SAML, run the following command:

```
$ wget "https://ucs-sso-ng.$(hostname -d)/keycloak/realms/ucs/protocol/saml/
↪descriptor"
```

CHAPTER

TWO

CONFIGURATION

The **Keycloak** app offers various configuration options. Some settings don't allow changes after installation. Therefore, you must set them carefully **before** installation. You find those settings marked with *Only before installation* in *Settings* (page 8). You can change all other settings at any time after the installation.

To change settings after installation, sign in to the UCS management system with a username with administration rights and go to *App Center* ‣ *Keyloak* ‣ *Manage Installation* ‣ *App Settings*. On the appearing *Configure Keycloak* page, you can change the settings and apply them to the app with a click on *Apply Changes*.

The App Center then *reinitializes* the Docker container for the Keycloak app. *Reinitilize* means the App Center throws away the running Keycloak Docker container and creates a fresh Keycloak Docker container with the just changed settings.

2.1 Use Keycloak for login to UCS Portal

The **Keycloak** app can take over the role of the *SAML IDP* for the UCS Portal. And the portal can use Keycloak for user authentication.

Warning: The LDAP server will not recognize SAML tickets that the *simpleSAMLphp* based identity provider issued after you restart it. Users will experience invalidation of their existing sessions.

For more information about production use, see *Installation on Primary Directory Node* (page 13).

To configure the UCS portal to use Keycloak for authentication, run the following steps on the system where you installed Keycloak:

1. Set the UCR variable `umc/saml/idp-server` to the URL `https://ucs-sso-ng.$domainname/realms/ucs/protocol/saml/descriptor`, for example `https://ucs-sso-ng.example.org/realms/ucs/protocol/saml/descriptor`. This step tells the portal to use Keycloak as IDP.

   Sign in to the UCS management system and then go to *System* ‣ *Univention Configuration Registry* and search for the variable `umc/saml/idp-server` and set the value as described before.

   Open a shell on the UCS system as superuser `root` where you installed Keycloak and run the following command:

   ```
   $ ucr set \
   > umc/saml/idp-server=\
   > "https://ucs-sso-ng.$(hostname -d)/realms/ucs/protocol/saml/descriptor"
   ```

2. Modify the portal to use SAML for login:

   In the UCS management system go to *Domain* ‣ *Portal* ‣ *login-saml*. On the tab *General* in the section *Advanced* activate the *Activated* checkbox.

   Open a shell on the UCS system as superuser `root` where you installed Keycloak and run the following command:

```
$ udm portals/entry modify \
> --dn "cn=login-saml,cn=entry,cn=portals,cn=univention,$(ucr get ldap/base)" \
> --set activated=TRUE
```

3. To activate the changes, restart the LDAP server `slapd` within a maintenance window.

   In the UCS management system go to *System ‣ System Services*. Search for `slapd` and click to select the service. Then click *Restart*.

   Open a shell on the UCS system as superuser `root` where you installed Keycloak and run the following command:

```
$ service slapd restart
```

Note: If you don't restart the LDAP server, you will see the following message in `/var/log/syslog`:

`slapd[…]: SASL [conn=…] Failure: SAML assertion issuer https://ucs-sso-ng.$domainname/realms/ucs is unknown`

2.2 Keycloak as OpenID Connect provider

The **`Keycloak`** app can serve as an OpenID Connect provider (*OIDC Provider*). The following steps explain how to configure an OIDC relying party (*OIDC RP*) to use Keycloak for authentication:

1. *Sign in to Keycloak Admin Console* (page 4).
2. Navigate to *UCS realm ‣ Clients ‣ Create*.
3. Specify the `client-id` for the client application (*OIDC RP*). Use the same `client-id` in the configuration of the client application.
4. Select `openid-connect` in the *Client Protocol* drop-down list.
5. Enter the *root URL*, the endpoint URL of the client application (*OIDC RP*).
6. Click *Save*.
7. Finally, the administrator can review the URL settings and customize them, if necessary.

For more information, see *Keycloak Server Administration Guide: OIDC clients* [4].

Note: If the administrator chooses `Confidential` as *Access Type* on the client configuration page, Keycloak offers an additional *Credentials* tab with the credentials.

2.3 Settings

The following references show the available settings within the **`Keycloak`** app. Univention recommends to keep the default values.

Keycloak has a lot more possibilities for configuration and customization. For more information, consult *Keycloak 18.0.0 Documentation* [1].

`keycloak/admin/user`
: Defines the name of the first user with administration rights in Keycloak. The file `/etc/keycloak.secret` stores this user's password on the system you installed the app.

Required	Default value	Set
Yes	`admin`	Only before installation

keycloak/log/level
Configures the verbosity of log messages in Keycloak.

Possible values `ALL`, `DEBUG`, `ERROR`, `FATAL`, `INFO`, `OFF`, `TRACE`, `WARN`.

For a detailed description of the log level values, see *Keycloak documentation: Configuring logging* [5].

Required	Default value	Set
Yes	`INFO`	Installation and app configuration

keycloak/java/opts
Defines the options that the Keycloak app appends to the *java* command.

Required	Default value	Set
Yes	`-server -Xms1024m -Xmx1024m`	Installation and app configuration

keycloak/theme
Defines the theme that Keycloak uses for the login interface. A CSS file with the same name must exist in the directory `/usr/share/univention-web/themes/`. The setting value only uses the basename of the file without the extension `css`.

Possible values `dark` and `light`

If you provide custom CSS files with other names, they add to the possible values.

Possible values `true` and `false`.

Required	Default value	Set
No	Same value as UCR variable `ucs/web/theme`[10].	Installation and app configuration

keycloak/server/sso/fqdn
Defines the FQDN to the identity provider in your environment's UCS domain. Defaults to `ucs-sso-ng.*$domainname*`.

Required	Default value	Set
No	None	Installation and app configuration

keycloak/server/sso/autoregistration
If set to `true` (default), the UCS system with the Keycloak app installed registers its IP address at the hostname of the identity provider defined in *keycloak/server/sso/fqdn* (page 9).

Possible values: `true` or `false`

Required	Default value	Set
Yes	`true`	Installation and app configuration

[10] https://docs.software-univention.de/manual/5.0/en/appendix/variables.html#envvar-ucs-web-theme

CHAPTER

THREE

ARCHITECTURE

The **Keycloak** app architecture consists of the following elements:

- The operating environment UCS with the App Center and the Docker engine running Keycloak.
- The Keycloak software.
- The OpenLDAP LDAP directory in UCS as identity store for Keycloak
- A SQL database as data persistence layer with read-write access for Keycloak.

This architecture view doesn't go into detail of the Keycloak software itself, because it's beyond the scope of this documentation.

3.1 Overview

Figure 3.1 shows the architecture with the most important elements.

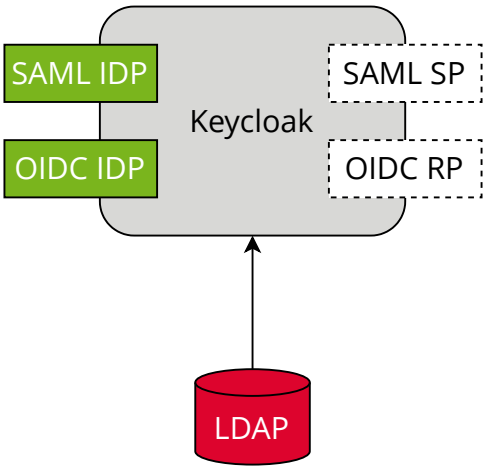

Figure 3.1: Keycloak app architecture
View focuses on the elements Keycloak, SAML and OIDC as its most important interfaces for single sign-on, and the LDAP directory.

The following list describes the elements in more detail.

Keycloak *Keycloak* is the Keycloak software as distributed by the Keycloak project as container image for Docker. The **Keycloak** app uses the software as-is without any changes to the software code.

LDAP *LDAP* is the LDAP directory provided by UCS with the OpenLDAP software. In UCS it is the storage for all identity and infrastructure data of the UCS domain. For more information, see LDAP directory[11] in *UCS 5.0 Manual* [2].

[11] https://docs.software-univention.de/manual/5.0/en/domain-ldap/ldap-directory.html#domain-ldap

SAML IDP *SAML IDP* stands for *SAML Identity Provider* and is the SAML interface in Keycloak that offers user authentication as a service through SAML.

SAML SP *SAML SP* stands for *SAML Service Provider* and is the SAML interface in Keycloak that outsources its user authentication function to an *IDP*.

OIDC Provider *OP* is short for *OpenID Connect Provider*. In Keycloak this OIDC interface offers user authentication as a service.

OIDC RP *OIDC RP* is short for *OpenID Connect Relying Party*. In Keycloak this OIDC interface outsources its user authentication function to an *OP*.

3.2 Design decisions

One goal of the **Keycloak** app is to provide a ready to run Keycloak setup for UCS. To reach that goal, the Univention team made the following decisions.

The **Keycloak** app configures a so-called *user federation* in the realm *UCS* in Keycloak. In general, a user federation synchronizes users from LDAP and Active Directory servers to Keycloak. In the Keycloak app, the user federation **doesn't** synchronize user accounts from LDAP to Keycloak, but delegates authentication decisions to LDAP. A realm manages a set of users, credentials, roles, and groups in Keycloak.

The user federation in the realm *UCS* uses the LDAP DN (Distinguished Name) `uid=sys-idp-user,cn=users,$ldap_base` to bind to the LDAP directory in UCS.

The app registers `ucs-sso-ng.$domainname` to the DNS that serves as host for API entry points of Keycloak and administrative web interface.

CHAPTER

FOUR

REQUIREMENTS AND LIMITATIONS

To ensure a smooth operation of the **Keycloak** app on UCS, administrators need to know the following requirements and limitations:

4.1 User federation and synchronization

The app configures a user federation in the realm *UCS*. **Don't** remove the user federation or Keycloak won't be able to resolve users anymore.

The configured user federation in the realm *UCS* doesn't synchronize the user accounts from the UCS LDAP to Keycloak. For more information, see *Design decisions* (page 12).

4.2 Installation on Primary Directory Node

The App Center installs the **Keycloak** app only on a Primary Directory Node in your UCS environment, see *Installation* (page 3). The app is therefore not suitable for production use in UCS domains that have Backup Directory Nodes.

Use the **Keycloak** app only in a UCS environment without Backup Directory Nodes, because otherwise:

- Users may encounter sign in problems at the UCS management system on other UCS systems.
- Other apps may not be able to authenticate users through SAML without manual interaction.

The installation might not break anything in production. But, experiments with reconfiguration of, for example, UMC and other services so that they use Keycloak, may have undesired results. In particular, when you change the UCR variable `umc/saml/idp-server` to point to your Keycloak installation. The LDAP server will not recognize SAML tickets that the *simpleSAMLphp* based identity provider issued after you restart it. Users will experience invalidation of their existing sessions.

4.3 No user activation for SAML

In the *Users* UMC module, the user account's *SAML settings* at *Account ▸ SAML settings* don't require anymore that administrators activate identity providers for user accounts. Therefore, any user account can use SAML for single sign-on. The behavior is the same as for the OIDC capability before through the **Kopano Connect** app.

4.4 Password restriction

Keycloak offers a password policies feature, see *Keycloak Server Administration Guide: Password policies* [6]. Because of the user federation with UCS, see *Design decisions* (page 12), Keycloak **doesn't** manage the users credentials.

UCS takes care of password policy definition and enforcement. For more information, see LDAP directory[12] in *UCS 5.0 Manual* [2].

[12] https://docs.software-univention.de/manual/5.0/en/domain-ldap/ldap-directory.html#domain-ldap

CHAPTER

FIVE

TROUBLESHOOTING

When you encounter problems with the operation of the **Keycloak** app, this chapter providers information where you can look closer into and to get an impression about what is going wrong.

5.1 Log files

The **Keycloak** app produces different logging information in different places.

/var/log/univention/appcenter.log Contains log information around activities in the App Center.

The App Center writes Keycloak relevant information to this file, when you run app lifecycle tasks like install, update and uninstall or when you change the app settings.

/var/log/univention/join.log Contains log information from join processes. When the App Center installs Keycloak, the app also joins the domain.

Keycloak Docker container The app uses the vanilla Keycloak Docker image[13]. The App Center runs the container. You can view log information from the Keycloak Docker container with the following command:

```
$ univention-app logs keycloak
```

Keycloak Admin Console Offers to view event logs in *Events* in the *Manage* section. Administrators can see *Login Events* and *Admin Events*. For more information, see *Keycloak Server Administration Guide: Configuring auditing to track events* [7].

5.2 Debugging

To increase the log level for more log information for the **Keycloak** app, see *keycloak/log/level* (page 9).

This log level only affects the log information that Keycloak itself generates and writes to the Docker logs. The App Center sets the Docker container's KEYCLOAK_LOGLEVEL environment variable to the value of *keycloak/log/level* (page 9).

[13] https://quay.io/repository/keycloak/keycloak

CHAPTER

SIX

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] *Keycloak 18.0.0 Documentation*. URL: https://www.keycloak.org/archive/documentation-18.0.html.

[2] *UCS 5.0 Manual*. Univention GmbH, 2021. URL: https://docs.software-univention.de/manual/5.0/en/.

[3] Raphaël Hertzog and Roland Mas. *The Debian Administrator's Handbook*, chapter Shell and Basic Commands. Freexian SARL, First edition, 2020. URL: https://www.debian.org/doc/manuals/debian-handbook/short-remedial-course.en.html#sect.shell-and-basic-commands.

[4] *Keycloak Server Administration Guide: OIDC clients*. URL: https://www.keycloak.org/docs/18.0/server_admin/#_oidc_clients.

[5] *Keycloak documentation: Configuring logging*. URL: https://www.keycloak.org/server/logging#_root_log_level.

[6] *Keycloak Server Administration Guide: Password policies*. URL: https://www.keycloak.org/docs/18.0/server_admin/#_password-policies.

[7] *Keycloak Server Administration Guide: Configuring auditing to track events*. URL: https://www.keycloak.org/docs/18.0/server_admin/index.html#configuring-auditing-to-track-events.

INDEX