



Keycloak app 19.0.2

Release 19.0.2

Univention GmbH

Mar 23, 2023

CONTENTS

1	Installation	3
2	Update	7
3	Configuration	9
4	Architecture	21
5	Requirements and limitations	23
6	Use cases	25
7	Troubleshooting	27
8	Changelog	29
9	Bibliography	31
	Bibliography	33
	Index	35

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:

1. *Installation* (page 3)
2. *Configuration* (page 9)
3. *Architecture* (page 21)
4. *Requirements and limitations* (page 23)
5. *Use cases* (page 25)
6. *Troubleshooting* (page 27)

This documentation doesn't cover the following topics:

- Usage of Keycloak itself, see the *Keycloak 19.0.0 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_\(OIDC\)](https://en.wikipedia.org/wiki/OpenID#OpenID_Connect_(OIDC))

⁶ <https://www.univention.com/feedback/?keycloak-app=generic>

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 system role *Primary Directory Node* or *Backup Directory 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 18).
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 18).

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

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

1.3 Initial Keycloak configuration

The first installation of the **Keycloak** app in the UCS domain creates an initial configuration.

To not overwrite custom settings, subsequent installations of the **Keycloak** app on additional UCS systems in the domain don't create the initial configuration.

Factory reset of the configuration

For a *factory reset* of the configuration, delete the realm *UCS* in the *Keycloak Admin Console*.

Warning: Beware, your installation loses all custom configuration settings, custom services providers and other changes to the realm *UCS*.

After you deleted the realm *UCS*, create the initial configuration with the following command:

```
$ univention-keycloak init
```

1.4 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 18).

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

1.5 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-ss0-ng.$(hostname -d)/keycloak/realms/ucs/.well-known/openid-configuration"
```

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

```
$ wget "https://ucs-ss0-ng.$(hostname -d)/keycloak/realms/ucs/protocol/saml/descriptor"
```


You can update the **Keycloak** app like any other app with Univention App Center or the command line tool **univention-app**.

This chapter covers additional points to consider before and during the update process.

2.1 Configuration migration during Keycloak app updates

Some updates of the **Keycloak** app require a migration of the domain wide Keycloak configuration, because every Keycloak service in the UCS domain uses the same, shared configuration.

By default, the **Keycloak** app migrates the configuration during the app update process. Some changes may conflict with older versions of the **Keycloak** app. Therefore, make sure that all **Keycloak** app instances on all UCS systems in the domain have the same version.

Tip: You can deactivate the automatic configuration migration during the app update process. Set the value of the UCR variable `keycloak/auto-migration` to `false`.

You can manually migrate the configuration of the **Keycloak** app on all UCS system, **after** you updated the app on all UCS systems to the same version. Use the following command:

```
$ univention-keycloak upgrade-config
```

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 18). 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* ▶ *Keycloak* ▶ *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. *Reinitialize* means the App Center throws away the running Keycloak Docker container and creates a fresh Keycloak Docker container with the just changed settings.

3.1 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 UCS* (page 23).

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-ss0-ng.$domainname/realms/ucs/protocol/saml/descriptor`, for example `https://ucs-ss0-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-ss0-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-ss0-ng.  
$domainname/realms/ucs is unknown
```

3.2 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].

New in version 19.0.1-ucs1: **univention-keycloak** added. For more information about the usage, see the `--help` option.

As an alternative the app **Keycloak** offers a command line tool. For usage, see the following example:

```
$ univention-keycloak oidc/op/cert get \  
--as-pem \  
--output "$SOMEFILENAME"  
$ univention-keycloak oidc/rp create \  
--app-url="https://$(hostname -f)/${MYAPP_URL}/" "${MYAPP_CLIENT_ID}"
```

The option group `oidc/rp` offers additional options like `--client-secret`.

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

3.3 Keycloak as SAML Identity Provider

New in version 19.0.1-ucs1: **univention-keycloak** added. For more information about the usage, see the `--help` option.

The **Keycloak** app can serve as an *SAML IDP*.

For apps that want to act as a *SAML SP*, you need to add a `client` configuration in Keycloak through the *Keycloak Admin Console* (page 4). For more information about how to create a SAML client configuration, see *Keycloak Server Administration Guide: Creating a SAML client* [5].

As an alternative the app **Keycloak** offers a command line tool. For usage, see the following example:

```
$ univention-keycloak saml/idp/cert get \
--as-pem --output "$SOMEFILENAME"
$ univention-keycloak saml/sp create \
--metadata-url "https://$(hostname -f)/$METADATA-URL-OF-THE-APP"
```

The option group `saml/sp` offers additional options like `--client-signature-required`.

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

3.4 Backup and restore

Administrators can create a backup of the **Keycloak** app data. The data comprises information for example about the realm, clients, groups, and roles. To create a backup, run the *export* action as in the following steps:

```
$ univention-app shell keycloak /opt/keycloak/bin/kc.sh export \
--dir /var/lib/univention-appcenter/apps/keycloak/data/myexport
```

In this example `myexport` is a freely chosen directory name.

To restore the backup into the app **Keycloak**, run the *import* action as in the following step:

```
$ univention-app shell keycloak /opt/keycloak/bin/kc.sh import \
--dir /var/lib/univention-appcenter/apps/keycloak/data/myexport
```

Warning: **Keycloak** defines the scope of exported data and may not contain every configuration option the program offers.

3.5 MariaDB as database

The **Keycloak** app uses PostgreSQL as default database back end. This section explains how to configure the app **Keycloak** to connect and use a MariaDB database back end. The setup requires a configuration through *Settings* (page 18). Administrators can select the database back end either during initial app installation of **Keycloak** or change it later after installation.

The following examples for the database configuration assume that a user account with the appropriate permissions for MariaDB exists. They use the database user account `keycloak` and the password `database-password`.

Note: The database user needs the following minimum privileges to work in a single machine setup. Use the `GRANT` command¹⁰:

¹⁰ <https://mariadb.com/kb/en/grant/>

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, ALTER, REFERENCES, INDEX, DROP
ON `<database>`.* TO `<user>`@`<host>`;
```

To specify a MariaDB database during installation, run

```
$ univention-app install \
--set kc/db/url="jdbc:mariadb://${database_hostname}:3306/keycloak" \
--set kc/db/password="database-password"
```

To specify a MariaDB database after installation in UMC:

1. Sign in to the UCS management system.
2. Go to *App Center* ▶ *Keycloak* ▶ *Manage Installation* ▶ *App Settings*.
3. Search for the variable `Database URI`. Set the value to your MariaDB endpoint, for example `jdbc:mariadb://$database_hostname:3306/keycloak` and click *Apply Changes*.

To specify a MariaDB database after installation on the command line:

```
$ univention-app configure keycloak \
--set kc/db/url "jdbc:mariadb://${database_hostname}:3306/keycloak" \
--set kc/db/password "database-password"
```

And to persist this change also in LDAP, use the following commands:

```
$ univention-install jq
$ new_json=$(univention-ldapsearch -LLL \
'(&(cn=keycloak)(univentionObjectType=settings/data))' \
| sed -n 's/^univentionData: //p' | base64 -d | bzip2 --decompress \
| jq '.uri = "jdbc:mariadb://${database_hostname}:3306/keycloak"')
$ udm settings/data modify \
--dn "cn=keycloak,cn=data,cn=univention,${ucr get ldap/base}" \
--set data=$(echo "$new_json" | bzip2 -c | base64 -w0)
```

3.6 Multiple installations in the domain

Administrators can install the app **Keycloak** on several nodes in a UCS domain to increase availability and provide failover using the default DNS name `ucs-sso-ng. $(hostname -d)`. The default installations in the domain don't require any interaction from the administrator. This will also provide session synchronization between all **Keycloak** installations on the domain.

Note: If the **Keycloak** app is installed on multiple systems in the domain and updates are available, make sure to update the app on all systems so that all instances of the app in the domain are on the same version.

3.7 Two-factor authentication for Keycloak

Warning: The two-factor capability isn't supported. Usage isn't recommended in production environments.

New in version 19.0.1-ucs1:

- Added functionality to enable 2FA (Two-Factor Authentication) to **univention-keycloak**. For more information about the usage, see the `--help` option.

The app **Keycloak** offers a 2FA option. 2FA is an authentication method that grants users access to a service after they sign in with a password and a OTP (one-time password) randomly generated by a third-party OTP password generator like *FreeOTP* or *Google Authenticator*.

2FA increases the protection for user data, because users need to provide two pieces: knowledge (password) and something in the users' possession (the OTP). It also increase the security of the system by avoiding account locking on known accounts because of malicious attacks. For more information, see [Wikipedia: Multi-factor authentication](#)¹¹.

After you activate 2FA for a group of users, Keycloak asks those users for their OTP on each login. To simplify the configuration process, you can use a command-line tool to enable 2FA.

To activate or deactivate 2FA for a user group, follow the instructions in the next sections.

3.7.1 Activate two-factor authentication for domain administrators

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

```
$ univention-keycloak 2fa enable --group-2fa "Domain Admins"
```

2. The next time a user belonging to the `Domain Admins` group tries to sign in, Keycloak forces them to configure the 2FA following the instructions given during the login.

3.7.2 Deactivate two-factor authentication for domain administrators

1. *Sign in to Keycloak Admin Console* (page 4).
2. Navigate to *UCS realm* ▶ *Groups*.
3. Select `Domain Admins` in the list and click *Edit*.
4. Navigate to *Role Mappings* on the tabs.
5. Remove `2FA role` from *Assigned roles*.

3.8 Keycloak ad hoc federation

Warning: Keycloak ad hoc federation isn't supported. Usage isn't recommended in production environments.

New in version 19.0.1-ucs2.

Keycloak SPI (Service Provider Interfaces) extension for ad hoc federation added. Keycloak offers identity brokering to delegate authentication to one or more identity providers for OpenID Connect or SAML 2.0.

See also:

For more information about identity brokering and first login flow, see *Keycloak Server Administration Guide: Identity Broker First Login* [6].

The app **Keycloak** provides *ad hoc federation* to enable identity brokering and add user accounts to UCS as so-called *shadow accounts*. It supports the *design decision about not having user accounts in Keycloak* (page 22).

The app **Keycloak** installs the **univention-authenticator** SPI plugin. The plugin creates the local shadow copy of the user account in the OpenLDAP directory services through the REST API of UDM (Univention Directory Manager). *Ad hoc federation* is useful when administrators want to keep track of all users in UCS.

See also:

For more information on SPI, see *Keycloak Server Development Guide: Authentication SPI* [7].

¹¹ https://en.wikipedia.org/wiki/Multi-factor_authentication

3.8.1 Import external CA certificates

Federation involves other, for example external, server systems and requires trust. Certificates are a way to implement trust. To tell your Keycloak system to trust another system for the ad-hoc federation, you need to import the CA certificate for that system. Keycloak needs the CA certificate to verify the encrypted connection with the other system.

Use the following steps to add the CA certificate of the other system:

```
$ docker cp /path/to/externalCA.pem keycloak:/externalCA.pem
$ univention-app shell keycloak \
keytool -cacerts -import -alias ucsCA -file /externalCA.pem -storepass "changeit" -
↪noprompt
```

Repeat this procedure when any CA certificate expires. In case of any CA related TLS error, restart the container:

```
$ docker restart keycloak
```

3.8.2 Create custom authentication flow

First, you as administrator need to create a custom authentication flow to use *univention-authenticator* SPI:

1. *Sign in to Keycloak Admin Console* (page 4).
2. Navigate to *UCS realm* ▶ *Authentication*.
3. Select *First Broker Login* in the list and click *Copy*.
4. Give a name to the authentication flow and click *OK*.
5. In the *Review Profile (review profile config)* click *Actions* and select *Config*.
6. Select *Off* in the list, click *Save* and navigate back to the authentication flow.
7. Click *Add execution* to get to the *Create Authenticator Execution* page.
8. Select *Univention Authenticator* in the list and click *Save*.
9. On the *Flows* tab in the *Authentication* section, change the *Univention Authenticator* in the displayed table to *Required*.
10. To finish the configuration, click *Actions* in the *Univention Authenticator* and select *Config*.
11. Fill in the following configuration options for the *Univention Authenticator*:
 - Alias** Name of the configuration.
 - UDM REST API endpoint** The API endpoint of UDM where UCS stores the shadow copy of the user.
 - Username** Username of a user account that can write to UDM.
 - Password** Password of the user account that can write to UDM.
12. Click *Save*.

3.8.3 Create an identity provider for Microsoft Active Directory

After you created the *custom authentication flow* (page 14), Keycloak can use ad hoc federation on any configured federated login. In this section, you learn how to set up a federated login using a [Microsoft Active Directory Federation Services](#)¹².

To create an identity provider for Active Directory that uses the ad hoc federation follow the next steps:

1. *Sign in to Keycloak Admin Console* (page 4).
2. Navigate to *UCS realm* ▶ *Identity Providers*.
3. Click *Add provider...* and select *SAML v2.0*.
4. Fill in the fields *Alias* and *Display Name*. You **can't** change the field *Alias* later.
5. Select your authentication flow with the *Univention Authenticator* on the *First Login Flow*.
6. Fill in the field *Service Provider Entity ID* with the *EntityID* from the *Relying Party* on the Active Directory Federation Services.
7. Set the *Single Sign-On Service URL* to the single sign-on URL from the *Relying Party*.
8. In *Principal Type* select *Unspecified* in the fields *NameID Policy Format*, *Attribute [Name]*.
In *Principal Attribute* select *sAMAccountName*.
9. Enable the following properties:
 - *Allow Create*
 - *HTTP-POST Binding Response*
 - *HTTP-POST Binding for AuthnRequest*
 - *Want AuthnRequests Signed*
10. For the field *Signature Algorithm* select *RSA_SHA256*
For the field *SAML Signature Key Name* select *CERT_SUBJECT*.
11. Enable *Validate Signature* and add the certificate to *Validating x509 Certificates*.
12. Click *Save*

3.8.4 Mappers for the identity provider

The identity provider needs the following mapper configuration to work properly with Univention Corporate Server:

1. To create a mapper in the identity provider configuration navigate to *UCS realm* ▶ *Identity Provider* ▶ *Your Identity Provider* ▶ *Mappers*.
2. Click *Create*
3. Configure the mapper for the email address with the following properties:
 - Name** Name of the mapper
 - Sync Mode Override** `import`
 - Type of mapper** `Attribute Importer`
 - Attribute Name** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
 - User Attribute Name** `email`
4. Configure the mapper for the first name with the following properties:
 - Name** Name of the mapper

¹² <https://learn.microsoft.com/en-us/windows-server/identity/active-directory-federation-services>

Sync Mode Override import

Type of mapper Attribute Importer

Attribute Name http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/givenname

User Attribute Name firstName

5. Configure the mapper for the last name with the following properties:

Name Name of the mapper

Sync Mode Override import

Type of mapper Attribute Importer

Attribute Name http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/surname

User Attribute Name lastName

6. Configure the mapper for `univentionObjectIdentifier` with the following properties:

Name Name of the mapper

Sync Mode Override import

Type of mapper Attribute Importer

User attribute objectGuid

User attribute Name univentionObjectIdentifier

7. Configure the mapper for `univentionSourceIAM` with the following properties:

Name Name of the mapper

Sync Mode Override import

Type of mapper Hardcoded attribute

User attribute univentionSourceIAM

User attribute value Identifier of the identity provider.

8. Configure the mapper for `external- $\{\text{ALIAS}\}$ - $\{\text{ATTRIBUTE}.sAMAccountName\}$` with the following properties:

Name Name of the mapper

Sync Mode Override import

Type of mapper Username Template Importer

User attribute external- $\{\text{ALIAS}\}$ - $\{\text{ATTRIBUTE}.sAMAccountName\}$

Target LOCAL

3.8.5 Configure Active Directory Federation services for ad hoc federation

To configure the Active Directory Federation Services to properly work with ad hoc federation you need to configure it with the following steps:

1. Sign in as *Administrator* in Active Directory Federation Services.
2. Open *Relying Party Trust* and click *Add Relying Party Trust*.
3. Select *Claim aware* and click *Start*.
4. On the *Select Data Source* page, select *Import data about the relying party published online or on a local network*.

5. In the field *Federation metadata address* insert the metadata URL: `https://ucs-sso-ng.$(ucr get domainname)/auth/realms/ucs/broker/SAML_IDP_name/endpoint/descriptor`.
6. Specify a *Display Name*. Click *Next*.
7. Select your wanted *Access Control Policy*. Click *Next*.
8. Review your final configuration and click *Next*.
9. Click *Close*.
10. Add the claims to the ticket.

objectGUID

1. Click *Add rule* and select *Send LDAP Attributes as Claims*.
2. Add a claim for `objectGUID` to the ticket:

Claim Rule name Name of the Claim

Attribute Store Active Directory

LDAP attribute objectGUID

Outgoing Claim Type objectGUID

sAMAccountName

1. Click *Add rule* and select *Send LDAP Attributes as Claims*.
2. Add a claim for `sAMAccountName` to the ticket:

Claim Rule name Name of the Claim

Attribute Store Active Directory

LDAP attribute SAM-Account-Name

Outgoing Claim Type sAMAccountName

Email address

1. Click *Add rule* and select *Send LDAP Attributes as Claims*.
2. Add a claim for the email address to the ticket:

Claim Rule name Name of the Claim

Attribute Store Active Directory

LDAP attribute E-mail Addresses

Outgoing Claim Type E-mail Address

Given name

1. Click *Add rule* and select *Send LDAP Attributes as Claims*.
2. Add a claim for the given name to the ticket:

Claim Rule name Name of the Claim

Attribute Store Active Directory

LDAP attribute Given-Name

Outgoing Claim Type Given Name

Surname

1. Click *Add rule* and select *Send LDAP Attributes as Claims*.
2. Add a claim for the surname to the ticket:

Claim Rule name Name of the Claim

Attribute Store Active Directory**LDAP attribute** Surname**Outgoing Claim Type** Surname

- Apply and save the rules.

3.9 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 19.0.0 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* [8].

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	<code>-server -Xms1024m -Xmx1024m</code>	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 <code>ucs/web/theme</code> ¹³ .	Installation and app configuration

¹³ <https://docs.software-univention.de/manual/5.0/en/appendix/variables.html#envvar-ucs-web-theme>

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	<code>ucs-sso-ng.\$domainname</code>	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 18).

Possible values: `true` or `false`

Required	Default value	Set
Yes	<code>true</code>	Installation and app configuration

keycloak/federation/remote/identifier

This property stores the name of the UDM property that stores the unique identifier of the remote IAM objects. It is only used for ad hoc federation.

Required	Default value	Set
No	<code>univentionObjectIdentifier</code>	Installation and app configuration

keycloak/federation/source/identifier

This property stores the name of the UDM property that stores the remote source of an IAM objects. It is only used for ad hoc federation.

Required	Default value	Set
No	<code>univentionSourceIAM</code>	Installation and app configuration

keycloak/database/connection

Specifies the IP addresses from which the default PostgreSQL database can receive connections.

Required	Default value	Set
No	None	Installation and app configuration

kc/db/url

Specifies the database JDBC URL (for example `jdbc:postgresql://dbhost/keycloak`) to connect Keycloak. Defaults to `jdbc:postgresql://fqdn:5432/keycloak`.

Required	Default value	Set
No	<code>jdbc:postgresql://fqdn:5432/keycloak</code>	Installation and app configuration

kc/db/username

Specifies the database username. Defaults to `keycloak`.

Required	Default value	Set
No	<code>keycloak</code>	Installation and app configuration

kc/db/kind

Specifies the kind of database. Defaults to postgres.

Required	Default value	Set
No	postgres	Installation and app configuration

kc/db/password

Specifies the password to connect to the database.

Required	Default value	Set
No	None	Installation and app configuration

ucs/self/registration/check_email_verification

Controls if the login is denied for unverified, self registered user accounts. For more information, see [Account verification](#)¹⁴ in the *UCS 5.0 Manual* [2].

Required	Default value	Set
No	False	Installation and app configuration

keycloak/login/messages/en/accountNotVerifiedMsg

English error message for a self-registered user account that isn't verified yet. The error message supports HTML format.

Required	Default value	Set
No	See default value in Listing 3.1 after the table.	Installation and app configuration

Listing 3.1: Default value for `keycloak/login/messages/en/accountNotVerifiedMsg` (page 20)

```
'Your account is not verified.<br>You must <a id="loginSelfServiceLink" href=
↪ "https://{hostname}.{domainname}/univention/selfservice/#/selfservice/
↪ verifyaccount" target="_blank">verify your account</a> before you can login.
↪ <br/>'
```

keycloak/login/messages/de/accountNotVerifiedMsg

German error message for a self-registered user account that isn't verified yet. The error message supports HTML format.

Required	Default value	Set
No	See default value in Listing 3.2 after the table.	Installation and app configuration

Listing 3.2: Default value for `keycloak/login/messages/de/accountNotVerifiedMsg` (page 20)

```
'Konto nicht verifiziert.<br>Sie m\u00FCssen Ihr <a id="loginSelfServiceLink"
↪ href="https://{hostname}.{domainname}/univention/selfservice/#/selfservice/
↪ verifyaccount" target="_blank">Konto verifizieren</a>, bevor Sie sich
↪ einloggen k\u00F6nnen.<br/>'
```

¹⁴ <https://docs.software-univention.de/manual/5.0/en/user-management/user-self-service.html#user-management-password-changes-by-users-selfregistration-account>

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.

4.1 Overview

Figure 4.1 shows the architecture with the most important elements.

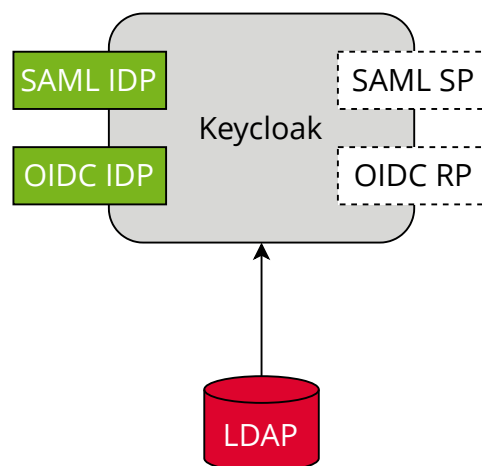


Figure 4.1: Keycloak app architecture

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 unmodified Keycloak binary image and additionally includes files to for example support synchronization of data between instances deployed on the same domain.

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](#)¹⁵ in *UCS 5.0 Manual* [2].

¹⁵ <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*.

4.2 Design decisions

One goal of the **Keycloak** app is to provide a ready to run Keycloak setup for UCS. To reach that goal, the Univenton 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-ss0-ng.$domainname` to the DNS that serves as host for API entry points of Keycloak and administrative web interface.

REQUIREMENTS AND LIMITATIONS

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

5.1 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 22).

5.2 Installation on UCS

The App Center installs the app **Keycloak** on a UCS 5.0-x Primary Directory Node or Backup Directory Node in your UCS environment, see *Installation* (page 3). The app is suitable for production use in UCS domains. Administrators need to keep in mind, other apps may be unable to authenticate users through SAML without manual reconfiguration.

Administrators need to take care with experiments that involve the reconfiguration, for example, of UMC, and other services to use Keycloak. The experiments may have undesired results. In particular, when you change the UCR variable `umc/saml/idp-server` to point to your Keycloak installation and restart the LDAP server, the LDAP server doesn't accept SAML tickets any longer that the *simpleSAMLphp* based identity provider issued. So users find their existing sessions invalidated.

5.3 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.

5.4 Password restriction

Keycloak offers a password policies feature, see *Keycloak Server Administration Guide: Password policies* [9]. Because of the user federation with UCS, see *Design decisions* (page 22), Keycloak **doesn't** manage the users credentials.

UCS takes care of password policy definition and enforcement. For more information, see *LDAP directory*¹⁶ in *UCS 5.0 Manual* [2].

5.5 Application clients

Keycloak offers the possibility to create SAML or OIDC clients using the command line tool **univention-keycloak**. Administrators can adjust the generic client configuration, if they need a specific configuration. In this case you can use the *Keycloak Admin Console* (page 4).

¹⁶ <https://docs.software-univention.de/manual/5.0/en/domain-ldap/ldap-directory.html#domain-ldap>

USE CASES

This section describes some uses cases for the app **Keycloak** to give a deeper insight of the app's capability.

6.1 Expired password and change password on next sign-in

In some situations, administrators create a user account with a temporary password that requires the account owner to change their password during their first sign-in. The procedure can be company policy or just considered a good practice. Also, if for any other reason like a lost or compromised user password, the account owner can contact the administrator and request a password change.

See also:

User management module - Account tab¹⁷ For user account expire and set password upon first login, refer to *UCS 5.0 Manual* [2].

To enable these capabilities with **Keycloak**, the app offers the following extensions. The extensions *only* provide the capabilities in the *UCS* realm with the **Keycloak** app installed.

Univention LDAP mapper In *Keycloak Admin Console* (page 4) follow *UCS realm* ▶ *User Federation* ▶ *ldap-provider* ▶ *Mappers*

The LDAP mapper reads necessary attributes from the LDAP directory and triggers a password update when needed.

Univention update password In *Keycloak Admin Console* (page 4) follow *UCS realm* ▶ *Authentication* ▶ *Required Actions*

Univention update password provides dialogs and forms in the Keycloak login flow.

¹⁷ <https://docs.software-univention.de/manual/5.0/en/user-management/umc.html#users-management-table-account>

TROUBLESHOOTING

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

7.1 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](#)¹⁸. 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* [10].

7.2 Debugging

To increase the log level for more log information for the **Keycloak** app, see [keycloak/log/level](#) (page 18).

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 18).

¹⁸ <https://quay.io/repository/keycloak/keycloak>

CHANGELOG

This changelog documents all notable changes to the Keycloak app. [Keep a Changelog](#)¹⁹ is the format and this project adheres to [Semantic Versioning](#)²⁰.

8.1 19.0.2-ucs2

Released: 23. March 2023

- This release of Keycloak app includes extensions for
 1. Univention LDAP mapper
 2. Univention Password reset
 3. Univention Self service
- **Keycloak** now checks the password expiry during the login and presents a password change dialog if the password is expired.
- The app now offers a setting to deny the login for unverified, self registered user accounts. For more information, see *use cases* (page 25).

8.2 19.0.1-ucs3

Released: 14. October 2022

- This release of Keycloak includes an extended version of the command line program **univention-keycloak**. Use it to directly create Keycloak *Client* configurations for *SAML Service Providers* and *OpenID Connect Relying Parties*.

8.3 19.0.1-ucs2

Released: 9. September 2022

- This release of **Keycloak** includes an SPI extension for so called ad-hoc federation. See the documentation for details.
- Administrators can install the app **Keycloak** on UCS 5.0-x UCS Primary Directory Nodes. For more information, see *Installation on UCS* (page 23).

¹⁹ <https://keepachangelog.com/en/1.0.0/>

²⁰ <https://semver.org/spec/v2.0.0.html>

8.4 19.0.1-ucs1

Released: 7. September 2022

- The app now offers **univention-keycloak**, a command line program to configure *SAML SP* and *OIDC Provider* clients in Keycloak directly.
univention-keycloak simplifies the integration of client apps with Keycloak and the downloads of signing certificates for example as PEM file (see option groups `saml/idp/cert` or `oidc/op/cert`).
- **univention-keycloak** supports the setup of a 2FA authentication flow for the members of a specific LDAP group. The second factor is a time-based one-time password (TOTP) in this case.
- The app updates to *Keycloak* version 19.0.1 of the upstream Docker image from <https://quay.io/repository/keycloak/keycloak>.
- Administrators can install the app **Keycloak** on UCS 5.0-x UCS Primary Directory Nodes. For more information, see *Installation on UCS* (page 23).

8.5 18.0.0-ucs1

Released: 28. June 2022

- Initial release of the app.
- Administrators can install the Keycloak app on UCS 5.0-x Primary Directory Nodes.
- The app uses the upstream Docker image from <https://quay.io/repository/keycloak/keycloak>.

CHAPTER

NINE

BIBLIOGRAPHY

BIBLIOGRAPHY

- [1] *Keycloak 19.0.0 Documentation*. URL: <https://www.keycloak.org/archive/documentation-19.0.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/19.0.3/server_admin/#_oidc_clients.
- [5] *Keycloak Server Administration Guide: Creating a SAML client*. URL: https://www.keycloak.org/docs/19.0.3/server_admin/#_client-saml-configuration.
- [6] *Keycloak Server Administration Guide: Identity Broker First Login*. URL: https://www.keycloak.org/docs/19.0.3/server_admin/#_identity_broker_first_login.
- [7] *Keycloak Server Development Guide: Authentication SPI*. URL: https://www.keycloak.org/docs/19.0.3/server_development/#_auth_spi.
- [8] *Keycloak documentation: Configuring logging*. URL: https://www.keycloak.org/server/logging#_configuring_the_root_log_level.
- [9] *Keycloak Server Administration Guide: Password policies*. URL: https://www.keycloak.org/docs/19.0.3/server_admin/#_password-policies.
- [10] *Keycloak Server Administration Guide: Configuring auditing to track events*. URL: https://www.keycloak.org/docs/19.0.3/server_admin/index.html#configuring-auditing-to-track-events.

D

Database URI, [12](#)

E

environment variable

- Database URI, [12](#)
- kc/db/kind, [19](#)
- kc/db/password, [20](#)
- kc/db/url, [19](#)
- kc/db/username, [19](#)
- keycloak/admin/user, [5, 18](#)
- keycloak/auto-migration, [7](#)
- keycloak/database/connection, [19](#)
- keycloak/federation/remote/identifier, [19](#)
- keycloak/federation/source/identifier, [19](#)
- keycloak/java/opts, [18](#)
- keycloak/log/level, [18, 27](#)
- keycloak/login/messages/de/accountNotVerifiedMsg, [20](#)
- keycloak/login/messages/en/accountNotVerifiedMsg, [20](#)
- keycloak/server/sso/autoregistration, [19](#)
- keycloak/server/sso/fqdn, [18, 19](#)
- keycloak/theme, [18](#)
- ucs/self/registration/check_email_verification, [20](#)
- umc/saml/idp-server, [9, 23](#)
- uv-manual:ucs/web/theme, [18](#)

K

- Keycloak, [21](#)
- keycloak/admin/user, [5](#)
- keycloak/auto-migration, [7](#)
- keycloak/log/level, [27](#)
- keycloak/login/messages/de/accountNotVerifiedMsg, [20](#)
- keycloak/login/messages/en/accountNotVerifiedMsg, [20](#)
- keycloak/server/sso/fqdn, [19](#)

L

LDAP, [21](#)

O

- OIDC Provider, [22](#)
- OIDC RP, [22](#)

S

- SAML IDP, [22](#)
- SAML SP, [22](#)

U

- umc/saml/idp-server, [9, 23](#)
- uv-manual:ucs/web/theme, [18](#)