

# Univention Developer Reference



**Manual for developers**

Alle Rechte vorbehalten./ All rights reserved.

The mentioned brand names and registered trademarks are owned by the respective legal owners in each case.

Linux® is a registered trademark of Linus Torvalds.

## Table of Contents

Foreword .....	9
1. Packaging software .....	11
1.1. Introduction .....	11
1.2. Preparations .....	11
1.3. Example: Re-building an UCS package .....	11
1.4. Example: Creating a new UCS package .....	12
1.5. Setup repository .....	17
1.6. Building packages through the openSUSE Build Service .....	18
2. Univention Config Registry .....	19
2.1. Using UCR .....	19
2.1.1. Using UCR from shell .....	19
2.1.2. Using UCR from Python .....	21
2.2. Configuration files .....	22
2.2.1. <code>debian/package.univention-config-registry</code> .....	22
2.2.1.1. File .....	23
2.2.1.2. Multifile .....	24
2.2.1.3. Script .....	25
2.2.1.4. Module .....	25
2.2.2. <code>debian/package.univention-config-registry-variables</code> .....	26
2.2.3. <code>debian/package.univention-config-registry-categories</code> .....	27
2.2.4. <code>debian/package.univention-service</code> .....	28
2.3. UCR Template files <code>conffiles/path/to/file</code> .....	29
2.4. Build integration .....	30
2.5. Examples .....	30
2.5.1. Minimal File example .....	30
2.5.2. Multifile example .....	32
2.5.3. Services .....	33
2.6. Python 3 Migration .....	36
3. Domain Join .....	37
3.1. Join scripts .....	37
3.2. Join status .....	37
3.3. Running join scripts .....	38
3.4. Writing join scripts .....	38
3.4.1. Basic join script example .....	38
3.4.2. Join script exit codes .....	40
3.4.3. Join script libraries .....	41
3.4.3.1. <i>univention-join</i> .....	41
3.4.3.2. <i>shell-univention-lib</i> .....	42
3.5. Writing unjoin scripts .....	46
4. Lightweight Directory Access Protocol (LDAP) in UCS .....	49
4.1. General .....	49
4.2. Packaging LDAP Schema Extensions .....	49
4.3. Packaging LDAP ACL Extensions .....	50
4.4. LDAP secrets .....	52
4.4.1. Password change .....	52
5. Univention Directory Listener .....	55
5.1. Structure of Listener Modules .....	55
5.2. Listener Tasks and Examples .....	59
5.2.1. Basic Example .....	59
5.2.2. Rename and Move .....	59
5.2.3. Full Example with Packaging .....	60
5.2.4. A Little Bit more Object Oriented .....	64

5.3. Technical Details .....	67
5.3.1. User-ID and Credentials .....	67
5.3.2. Internal Cache .....	67
5.3.2.1. univention-directory-listener-ctrl .....	68
5.3.2.2. univention-directory-listener-dump .....	68
5.3.2.3. univention-directory-listener-verify .....	68
5.3.2.4. get_notifier_id.py .....	69
5.3.3. Internal working .....	69
5.3.4. Python 3 Migration .....	71
6. Univention Directory Manager (UDM) .....	73
6.1. Introduction .....	73
6.2. Packaging Extended Attributes .....	74
6.2.1. Selection lists .....	79
6.2.1.1. Static selections .....	79
6.2.1.2. Dynamic selections .....	79
6.2.2. Known issues .....	81
6.2.3. Extended Options .....	81
6.2.4. Extended Attribute Hooks .....	82
6.3. UDM Modules .....	84
6.4. UDM Syntax .....	84
6.4.1. UDM Syntax Override .....	85
6.4.2. UDM LDAP search .....	86
6.5. Packaging UDM Hooks .....	90
6.6. Packaging UDM Extension Modules .....	91
6.7. Packaging UDM Syntax Extension .....	92
6.8. UDM REST API .....	94
6.8.1. Authentication .....	94
6.8.2. API overview .....	94
6.8.3. API usage examples .....	95
6.8.3.1. Create a user via a POST request .....	95
6.8.3.2. Search for users via a GET request .....	97
6.8.3.3. Modify a user via a PUT request .....	99
6.8.3.4. Delete a user via a DELETE request .....	100
6.9. UCS 5.0: Python 3 Migration of modules and extensions .....	100
6.9.1. Compatibility with UCS 4.4 .....	100
6.9.2. Default option .....	101
6.9.3. Mapping functions .....	101
6.9.4. Mapping Encoding .....	102
6.9.5. object.open() / object._post_unmap() .....	103
6.9.6. object.has_key() .....	103
6.9.7. identify() .....	103
6.9.8. _ldap_modlist() .....	104
6.9.9. lookup() .....	104
6.9.10. Syntax classes .....	104
6.9.11. Hooks .....	104
7. Univention Management Console (UMC) .....	105
7.1. Architecture .....	105
7.2. Asynchronous Framework .....	106
7.3. Protocol UMCP 2.0 .....	107
7.3.1. Data flow .....	107
7.3.2. Authentication .....	107
7.3.3. Message format .....	107
7.3.3.1. Message header .....	107
7.3.3.2. Message body .....	108

7.3.4. Examples .....	108
7.4. Protocol HTTP for UMC .....	109
7.4.1. Examples .....	109
7.5. UMC files .....	110
7.5.1. <code>debian/package.umc-modules</code> .....	110
7.5.2. UMC Module Declaration File .....	111
7.6. Local System Module .....	111
7.6.1. Python API .....	111
7.6.2. UMC module API (Python and JavaScript) .....	111
7.6.2.1. XML definition .....	112
7.6.2.2. Python module .....	113
7.6.2.3. UMC store API .....	115
7.6.3. Packaging .....	116
7.7. Domain LDAP Module .....	119
7.8. Disabling a Module .....	119
8. Web services .....	121
8.1. Extending the overview page .....	121
9. App Center .....	123
10. Integration of external repositories .....	125
10.1. Integration of repository components via Univention Management Console .....	125
10.2. Integration of repository components via Univention Configuration Registry .....	126
11. Translating UCS .....	127
11.1. Univention Management Console translations .....	127
11.1.1. Install needed tools .....	127
11.1.2. Obtain a current checkout of the UCS GIT repository .....	127
11.1.3. Create a new translation package .....	127
11.1.4. Edit translation files .....	128
11.1.5. Update the translation package .....	128
11.1.6. Build the translation package .....	129
12. Univention Updater .....	131
12.1. Separate repositories .....	131
12.2. Updater scripts .....	131
12.2.1. Digital signature .....	132
12.3. Release update walkthrough .....	132
13. <i>Single Sign-On</i> : Integrating a service provider into UCS .....	133
13.1. Register new service provider via <code>udm</code> .....	133
13.2. Get information required by the service provider .....	133
13.3. Add direct login link to the <i>UCS Portal</i> page .....	134
14. Miscellaneous .....	135
14.1. Databases .....	135
14.1.1. PostgreSQL .....	135
14.1.2. MySQL .....	135
14.2. UCS lint .....	135
14.3. Function Libraries .....	137
14.3.1. <i>shell-univention-lib</i> .....	137
14.3.2. <i>python-univention-lib</i> .....	138
14.4. Login Access Control .....	139
14.5. Network Packet Filter .....	139
14.5.1. Filter rules by Univention Configuration Registry .....	139
14.5.2. Local filter rules via <code>iptables</code> commands .....	140
14.5.3. Testing Univention Firewall settings .....	140
14.6. Active Directory Connection custom mappings .....	141
A. Bug reporting .....	143
B. Debian packaging .....	145

B.1. Prerequisites and preparation .....	145
B.2. dh_make .....	145
B.3. Debian control files .....	146
B.3.1. debian/control .....	149
B.3.2. debian/copyright .....	152
B.3.3. debian/changelog .....	153
B.3.4. debian/rules .....	153
B.3.5. debian/preinst, debian/prerm, debian/postinst, debian/postrm .....	155
B.4. Building .....	156
B.5. Further reading .....	156
Bibliography .....	157
Index .....	159

## List of Examples

2.1. Use of <code>ucr set</code> .....	19
2.2. Use of <code>ucr get</code> .....	20
2.3. Use of <code>is_ucr_true</code> .....	20
2.4. Use of <code>ucr unset</code> .....	20
2.5. Use of <code>ucr shell</code> .....	20
2.6. Reading a Univention Configuration Registry variable in Python .....	21
2.7. Reading boolean Univention Configuration Registry variables in Python .....	21
2.8. Changing Univention Configuration Registry variables in Python .....	21
2.9. Setting and unsetting Univention Configuration Registry variables in Python .....	22
3.1. Service registration in join script .....	43
3.2. Service unregistration in unjoin script .....	43
3.3. Check for unused service in unjoin script .....	44
3.4. Extension registration in join script .....	45
3.5. Schema unregistration in unjoin script .....	46
4.1. Schema registration in join script .....	50
4.2. LDAP ACL registration in join script .....	52
4.3. Server password change example .....	53
6.1. Extended Attribute for custom LDAP schema .....	77
6.2. Dynamic selection list for Extended Attributes .....	80
6.3. Extended Option .....	82
7.1. Authentication request .....	109
7.2. Search for users .....	109
7.3. Authentication request .....	109
7.4. search for users .....	109
7.5. UMC module category examples .....	113
14.1. Local firewall rule .....	140
14.2. Using <code>nmap</code> for firewall port testing .....	141





# Foreword

This developer guide provides information to extend Univention Corporate Server. It is targeted at third party vendors who intend to provide applications for the Univention App Center and for power users who wish to deploy locally built or modified software.

Feedback is very welcome! Please either file a bug (see Appendix A) or send an e-mail to <feedback@univention.de>.



# Chapter 1. Packaging software

1.1. Introduction .....	11
1.2. Preparations .....	11
1.3. Example: Re-building an UCS package .....	11
1.4. Example: Creating a new UCS package .....	12
1.5. Setup repository .....	17
1.6. Building packages through the openSUSE Build Service .....	18

This chapter describes how software for UCS is packaged. For more details on packaging software in the Debian format, see Appendix B

## 1.1. Introduction

Feedback

UCS is based on the Debian distribution, which is using the deb format to package software. The program `dpkg` is used for handling a set of packages. On installation packages are unpacked and configured, while on un-installation packages are de-configured and the files belonging to the packages are removed from the system. On top of that the apt-tools provide a software repository, which allows software to be downloaded from central file servers. Package files provide an index of all packages contained in the repository, which is used to resolve dependencies between packages: while `dpkg` works on a set of packages given on the command line, `apt-get` builds that set of packages and their dependencies before invoking `dpkg` on this set. `apt-get` is a command line tool, which is fully described in its manual page `apt-get(8)`. A more modern version with a text based user interface is `aptitude`, while `synaptic` provides a graphical frontend.

On UCS systems the administrator is not supposed to use these tools directly. Instead all software maintenance can be done through the UMC, which maps the requests to invocations of the commands given above.

## 1.2. Preparations

Feedback

This chapter describes some simple examples using existing packages as examples. For downloading and building them, some packages must be installed on the system used as a development system. `git` is used to checkout the source files belonging to the packages. `build-essential` must be installed for building the package. `devscripts` provides some useful tools for maintaining packages.

This can be achieved by running the following command:

```
sudo apt-get install git build-essential devscripts
```

## 1.3. Example: Re-building an UCS package

Feedback

Source code: `doc/developer-reference/packaging/testdeb/`

### Procedure 1.1. Checking out and building a UCS package

1. (Optional) Create the top level working directory

```
mkdir work
cd work/
```

2. Either fetch the latest source code from the GIT version control system or download the source code of the currently packaged version.

<https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/packaging/testdeb/>

### Example: Creating a new UCS package

- Checkout example package from GIT version control system

```
git clone https://github.com/univention/univention-corporate-server.git
cd univention-corporate-server/base/univention-ssh
```

- Fetch the source code from the Univention Repository server

- a. Enable unmaintained and source repository once

```
sudo ucr set repository/online/unmaintained=yes \
           repository/online/sources=yes
sudo apt-get update
```

- b. Fetch source code

```
apt-get source univention-ssh
cd univention-ssh-*/
```

3. (Optional) Increment the version number of package to define a newer package

```
debchange --local work 'Private package rebuild'
```

4. Install the required build dependencies

```
sudo apt-get build-dep .
```


5. Build the binary package

```
dpkg-buildpackage -uc -us -b -rfakeroot
```

6. Locally install the new binary package

```
sudo dpkg -i ../univention-ssh-*_*.deb
```

## 1.4. Example: Creating a new UCS package

Feedback 

The following example provides a walk-through for packaging a Python script called `testdeb.py`. It creates a file `testdeb-DATE-time` in the `/tmp/` directory.

A directory needs to be created for each source package, which hosts all other files and sub-directories.

```
mkdir testdeb-0.1
cd testdeb-0.1
```

The file `testdeb.py`, which is the program to be installed, will be put into that directory.

```
#!/usr/bin/env python
"""
Example for creating UCS packages.
"""
import time

now = time.localtime()
filename = '/tmp/testdeb-%s' % time.strftime('%y%m%d%H%M', now)
tmpfile = open(filename, 'a')
tmpfile.close()
```

In addition to the files to be installed some meta-data needs to be created in the `debian/` sub-directory. This directory contains several files, which are needed to build a Debian package. The files and their format will be described in the following sections.

To create an initial `debian/` directory with all template files, invoke the `dh_make(8)` command provided by the package *dh-make*:

```
dh_make --native --single --email user@example.com
```

Here several options are given to create the files for a source package, which contains all files in one archive and only creates one binary package at the end of the build process. More details are given in Section B.2.

The program will output the following information:

```
Maintainer name : John Doe
Email-Address   : user@example.com
Date           : Thu, 28 Feb 2013 08:11:30 +0100
Package Name    : testdeb
Version        : 0.1
License        : blank
Type of Package : Single
Hit <enter> to confirm:
```

The package name *testdeb* and version “0.1” were determined from the name of the directory `testdeb-0.1`, the maintainer name and address were gathered from the UNIX account information.

After pressing the **enter** key some warning message will be shown:

```
Currently there is no top level Makefile. This may require additional
tuning. Done. Please edit the files in the debian/ subdirectory now.
You should also check that the testdeb Makefiles install into $DESTDIR
and not in / .
```

Since this example is created from scratch, the missing `Makefile` is normal and this warning can be ignored. Instead of writing a `Makefile` to install the single executable, `dh_install` will be used later to install the file.

Since the command completed successfully, several files were created in the `debian/` directory. Most of them are template files, which are unused in this example. To improve understandability they are deleted:

```
rm debian/*.ex debian/*.EX
rm debian/README* debian/doc
```

The remaining files are required and control the build process of all binary packages. Most of them don't need to be modified for this example, but others must be completed using an editor.

`debian/control`

The file contains general information about the source and binary packages. It needs to be modified to include a description and contain the right build dependencies:

```
Source: testdeb
Section: univention
Priority: optional
Maintainer: John Doe <user@example.com>
Build-Depends: debhelper (>= 7)
Standards-Version: 3.7.2

Package: testdeb
Architecture: all
```

### Example: Creating a new UCS package

```
Depends: ${misc:Depends}
Description: An example package for the developer guide
  This purpose of this package is to describe the structure of a
  Debian
  packages. It also documents
  .
  * the structure of a Debian/Univention package
  * installation process.
  * content of packages
  * format and function of control files
  .
  For more information about UCS, refer to:
  https://www.univention.de/
```

debian/rules

This file has a Makefile syntax and controls the package build process. Because there is no special handling needed in this example, the default file can be used unmodified.

```
#!/usr/bin/make -f

%:
dh $@
```

Note that tabulators must be used for indentation in this file.

debian/testdeb.install

To compensate the missing Makefile, `dh_install(1)` is used to install the executable. `dh_install` is indirectly called by `dh` from the `debian/rules` file. To install the program into `/usr/bin/`, the file needs to be created manually containing the following single line:

```
testdeb.py usr/bin/
```

Note that the path is not absolute but relative.

debian/testdeb.postinst

Since for this example the program should be invoked automatically during package installation, this file needs to be created. In addition to just invoking the program shipped with the package itself, it also shows how Univention Configuration Registry variables can be set (see Section 2.1.1):

```
#!/bin/sh
set -e

case "$1" in
configure)
  # invoke sample program
  testdeb.py
  # Set UCR variable if previously unset
  ucr set repository/online/server?https://updates.software-
univention.de/
  # Force UCR variable on upgrade from previous package only
  if dpkg --compare-versions "$2" lt-nl 0.1-2
  then
    ucr set timeserver1=time.fu-berlin.de
  fi
;;
```

```
abort-upgrade|abort-remove|abort-deconfigure)
;;
*)
echo "postinst called with unknown argument \"${1}\"" >&2
exit 1
;;
esac

#DEBHELPER#

exit 0
```

debian/changelog

The file is used to keep track of changes done to the packaging. For this example the file should look like this:

```
testdeb (0.1-1) unstable; urgency=low

* Initial Release.

-- John Doe <user@example.com>   Mon, 21 Mar 2013 13:46:39 +0100
```

debian/copyright

This file is used to collect copyright related information. It is critical for Debian only, which need this information to guarantee that the package is freely redistributable. For this example the file remains unchanged.

The copyright and changelog file are installed to the `/usr/share/doc/testdeb/` directory on the target system.

debian/compat,  
debian/source/format

These files control some internal aspects of the package build process. They can be ignored for the moment and are further described in Section B.3.

Now the package is ready and can be built by invoking the following command:

```
dpkg-buildpackage -us -uc
```

The command should then produce the following output:

```
dpkg-buildpackage: source package testdeb
dpkg-buildpackage: source version 0.1-1
dpkg-buildpackage: source changed by John Doe <user@example.com>
dpkg-buildpackage: host architecture amd64
dpkg-source --before-build testdeb
fakeroot debian/rules clean
dh clean
dh_testdir
dh_auto_clean
dh_clean
dpkg-source -b testdeb
dpkg-source: Information: Quellformat »3.0 (native)« wird verwendet
dpkg-source: Information: testdeb wird in testdeb_0.1-1.tar.gz gebaut
dpkg-source: Information: testdeb wird in testdeb_0.1-1.dsc gebaut
```

*Example: Creating a new UCS package*

```
debian/rules build
dh build
    dh_testdir
    dh_auto_configure
    dh_auto_build
    dh_auto_test
fakeroot debian/rules binary
dh binary
    dh_testroot
    dh_prep
    dh_installdirs
    dh_auto_install
    dh_install
    dh_installdocs
    dh_installchangelogs
    dh_installexamples
    dh_installman
    dh_installdocs
    dh_installcron
    dh_installdebconf
    dh_installemacsen
    dh_installifupdown
    dh_installinfo
    dh_installinit
    dh_installmenu
    dh_installmime
    dh_installmodules
    dh_installogcheck
    dh_installogrotate
    dh_installpam
    dh_installppp
    dh_installudev
    dh_installwm
    dh_installxfonts
    dh_installogsettings
    dh_bugfiles
    dh_ucf
    dh_lintian
    dh_gconf
    dh_icons
    dh_perl
    dh_usrlocal
    dh_link
    dh_compress
    dh_fixperms
    dh_installdeb
    dh_gencontrol
    dh_md5sums
    dh_builddeb
dpkg-deb: building package `testdeb' in `../testdeb_0.1-1_all.deb'.
dpkg-genchanges -b >../testdeb_0.1-1_amd64.changes
dpkg-genchanges: binary-only upload - not including any source code
dpkg-source --after-build testdeb
```




```
dpkg-buildpackage: full upload; Debian-native package (full source is included)
```

The binary package file `testdeb_0.1-1_all.deb` is stored in the parent directory. When it is installed manually using `dpkg -i ../testdeb_0.1-2_all.deb` as root, the Python script is installed as `/usr/bin/testdeb.py`. It is automatically invoked by the `postint` script, so a file named `/tmp/testdeb-date-time` has been created, too.

Congratulations! You've successfully built your first own Debian package.

## 1.5. Setup repository

 Feedback 

Until now the binary package is only available locally, thus for installation it needs to be copied manually to each host and must be installed manually using `dpkg -i`. If the package required additional dependencies, the installation process will abort, since packages are not downloaded by `dpkg`, but by `apt`. To support automatic installation and dependency resolution, the package must be put into an `apt` repository, which needs to be made available through `http` or some other mechanism.

For this example the repository is created below `/var/www/repository/`, which is exported by default on all UCS systems, where `apache2` is installed. Below that directory several other sub-directories and files must be created to be compatible with the UCS Updater. The following example commands create a repository for UCS version 4.3 with the component name `testcomp`:

```
WWW_BASE="/var/www/repository/4.3/maintained/component"
TESTCOMP="testcomp/all"
install -m755 -d "$WWW_BASE/$TESTCOMP"
install -m644 -t "$WWW_BASE/$TESTCOMP" *.deb
( cd "$WWW_BASE" &&
  rm -f "$TESTCOMP/Packages" * &&
  apt-ftparchive packages "$TESTCOMP" > "Packages" &&
  gzip -9 < "Packages" > "$TESTCOMP/Packages.gz" &&
  mv "Packages" "$TESTCOMP/Packages" )
```

This repository can be included on any UCS system by appending the following line to `/etc/apt/sources.list`, assuming the FQDN of the host providing the repository is named `repository.server`:

```
deb http://repository.server/repository/4.3/maintained/component
testcomp/all/
```

### Note

It is important that the directory, from where the `apt-ftparchive` command is invoked, matches the first string given in the `sources.list` file after the `deb` prefix. The URL together with the suffix `testcomp/all/` not only specifies the location of the `Packages` file, but is also used as the base URL for all packages listed in the `Packages` file.

Instead of editing the `sources.list` file directly, the repository can also be included as a component, which can be configured by setting several UCR variables. As UCR variables can also be configured through UDM policies, this simplifies the task of installing packages from such a repository on many hosts. For the repository above the following variables need to be set:

```
ucr set \
  repository/online/component/testcomp=yes \
  repository/online/component/testcomp/server=repository.server \
  repository/online/component/testcomp/prefix=repository
```

## 1.6. Building packages through the openSUSE Build Service


The openSUSE Build Service (OBS) is a framework to generate packages for a wide range of distributions. Additional information can be found at <https://build.opensuse.org/>. If OBS is already used to build packages for other distributions, it can also be used for Univention Corporate Server builds. The build target for UCS 4.3 is called *Univention UCS 4.3*. Note that OBS doesn't handle the integration steps described in later chapters (e.g. the use of Univention Configuration Registry templates).

# Chapter 2. Univention Config Registry

2.1. Using UCR .....	19
2.1.1. Using UCR from shell .....	19
2.1.2. Using UCR from Python .....	21
2.2. Configuration files .....	22
2.2.1. <code>debian/package.univention-config-registry</code> .....	22
2.2.1.1. File .....	23
2.2.1.2. Multifile .....	24
2.2.1.3. Script .....	25
2.2.1.4. Module .....	25
2.2.2. <code>debian/package.univention-config-registry-variables</code> .....	26
2.2.3. <code>debian/package.univention-config-registry-categories</code> .....	27
2.2.4. <code>debian/package.univention-service</code> .....	28
2.3. UCR Template files <code>conffiles/path/to/file</code> .....	29
2.4. Build integration .....	30
2.5. Examples .....	30
2.5.1. Minimal File example .....	30
2.5.2. Multifile example .....	32
2.5.3. Services .....	33
2.6. Python 3 Migration .....	36


The Univention Config Registry (UCR) is a local mechanism, which is used on all UCS system roles to consistently configure all services and applications. It consists of a database, where the currently configured values are stored, and a mechanism to trigger certain actions, when values are changed. This is mostly used to create configuration files from templates by filling in the configured values. In addition to using simple place holders its also possible to use Python code for more advanced templates or to call external programs when values are changed. UCR values can also be configured through an UDM policy in Univention directory service (LDAP), which allows values to be set consistently for multiple hosts of a domain.

## 2.1. Using UCR

Feedback 

Univention Configuration Registry provides two interfaces, which allows easy access from shell scripts and Python programs.

### 2.1.1. Using UCR from shell

Feedback 

`univention-config-registry` (and its alias `ucr`) can be invoked directly from shell. The most commonly used functions are:

```
ucr set [ key=value ] [ key?value ]...
```

Set Univention Configuration Registry variable `key` to the given `value`. Using `=` forces an assignment, while `?` only sets the value if the variable is unset.

#### Example 2.1. Use of `ucr set`

```
ucr set print/papersize?a4 \
variable/name=value
```

```
ucr get key
```

Return the current value of the Univention Configuration Registry variable `key`.

**Example 2.2. Use of `ucr get`**

```
case "$(ucr get system/role)" in
  domaincontroller_*)
    echo "Running on a UCS Domain Controller"
    ;;
esac
```

For variables containing boolean values the shell-library-function `is_ucr_true key` from `/usr/share/univention-lib/ucr.sh` should be used. It returns 0 (success) for the values "1", "yes", "on", "true", "enable", "enabled", 1 for the negated values "0", "no", "off", "false", "disable", "disabled". For all other values it returns a value of 2 to indicate inappropriate usage.

**Example 2.3. Use of `is_ucr_true`**

```
. /usr/share/univention-lib/ucr.sh
if is_ucr_true repository/online/unmaintained
then
  echo "Unmaintained is enabled"
fi
```

```
ucr unset key ...
```

Unset the Univention Configuration Registry variable key.

**Example 2.4. Use of `ucr unset`**

```
ucr unset print/papersize variable/namme
```

```
ucr shell [ key ...]
```

Export some or all Univention Configuration Registry variables in a shell compatible manner as environment variables. All shell-incompatible characters in variable names are substituted by underscores (\_).

**Example 2.5. Use of `ucr shell`**

```
eval "$(ucr shell)"
case "$server_role" in
  domaincontroller_*)
    echo "Running on a UCS Domain Controller serving $ldap_base"
    ;;
esac
```

It is often easier to export all variables once and then reference the values through shell variables.


**Warning**

Be careful with shell quoting, since several Univention Configuration Registry variables contain shell meta characters. Use `eval "$(ucr shell)"`.

**Note**

`ucr` is installed as `/usr/sbin/ucr`, which is not on the search path `$PATH` of normal users. Changing variables requires root access to `/etc/univention/base.conf`, but reading works for normal users too, if `/usr/sbin/ucr` is invoked directly.

## 2.1.2. Using UCR from Python

Feedback 

UCR also provides a Python binding, which can be used from any Python program. An instance of `univention.config_registry.ConfigRegistry` needs to be created first. After loading the current database state with `load()` the values can be accessed by using the instance like a Python dictionary:

### Example 2.6. Reading a Univention Configuration Registry variable in Python

```
from univention.config_registry import ConfigRegistry
ucr = ConfigRegistry()
ucr.load()
print ucr['variable/name']
print ucr.get('variable/name', '<not set>')
```

For variables containing boolean values the methods `is_true()` and `is_false()` should be used. The former returns `True` for the values "1", "yes", "on", "true", "enable", "enabled", while the later one returns `True` for the negated values "0", "no", "off", "false", "disable", "disabled". Both methods accept an optional argument `default`, which is returned as-is when the variable is not set.

### Example 2.7. Reading boolean Univention Configuration Registry variables in Python

```
if ucr.is_true('repository/online/unmaintained'):
    print "unmaintained is explicitly enabled"
if ucr.is_true('repository/online/unmaintained', True):
    print "unmaintained is enabled"
if ucr.is_false('repository/online/unmaintained'):
    print "unmaintained is explicitly disabled"
if ucr.is_false('repository/online/unmaintained', True):
    print "unmaintained is disabled"
```

Modifying variables requires a different approach. The function `ucr_update()` should be used to set and unset variables.

### Example 2.8. Changing Univention Configuration Registry variables in Python

```
from univention.config_registry.frontend import ucr_update
ucr_update(ucr, {
    'foo': 'bar',
    'baz': '42',
    'bar': None,
})
```

The function `ucr_update()` requires an instance of `ConfigRegistry` as its first argument. The method is guaranteed to be atomic and internally uses file locking to prevent race conditions.


The second argument must be a Python dictionary mapping UCR variable names to their new value. The value must be either a string or `None`, which is used to unset the variable.

As an alternative the old functions `handler_set()` and `handler_unset()` can still be used to set and unset variables. Both functions expect an array of strings with the same syntax as used with the command line tool `ucr`. As the functions `handler_set()` and `handler_unset()` don't automatically update any instance of `ConfigRegistry`, the method `load()` has to be called manually afterwards to reflect the updated values.

### Example 2.9. Setting and unsetting Univention Configuration Registry variables in Python

```
from univention.config_registry import handler_set, handler_unset
handler_set(['foo=bar', 'baz?42'])
handler_unset(['foo', 'bar'])
```

## 2.2. Configuration files

Feedback 

Packages can use the UCR functionality to create customized configuration files themselves. UCR *diverts* files shipped by Debian packages and replaces them by generated files. If variables are changed, the affected files are *committed*, which regenerated their content. This diversion is persistent and even outlives updates, so they are not overwritten by configuration files of new packages.

For this, packages need to ship additional files:

`conffiles/path/to/file`

This template file is used to create the target file. There exist two variants: A *single file template* consists of only a single file, from which the target file is created, while a *multi file template* can consist of multiple file fragments, which are concatenated to form the target file. See Section 2.3 below for more information.

`debian/package.univention-config-registry`

This mandatory information file describes the each template file. It specifies the type of the template and lists the UCR variable names, which shall trigger the regeneration of the target file. See Section 2.2.1 below for more information.

`debian/package.univention-config-registry-variables`

This optional file can add descriptions to UCR variables, which should describe the use of the variable, its default and allowed values. See Section 2.2.2 below for more information.

`debian/package.univention-config-registry-categories`


This optional file can add additional categories to group UCR variables. See Section 2.2.3 below for more information.

`debian/package.univention-service`

This optional file is used to define long running services. See Section 2.2.4 below for more information.

In addition to these files code needs to be inserted into the package maintainer scripts (see Section B.3.5), which registers and unregisters these files. This is done by calling `univention-install-config-registry` from `debian/rules` during the package build binary phase. The command is part of the ***univention-config-dev*** package, which needs to be added as a Build-Depends build dependency of the source package in `debian/control`.

### 2.2.1. `debian/package.univention-config-registry`

Feedback 


This file describes all template files in the package. The file is processed and copied by `univention-install-config-registry` into `/etc/univention/templates/info/` when the package is built.

It can consist of multiple sections, where sections are separated by one blank line. Each section consists of multiple key-value-pairs separated by a colon followed by one blank. A typical entry has the following structure:

```
Type: <type>
[Multifile|File]: <filename>
[Subfile: <fragment-filename>]
Variables: <variable1>
...
```

Type specifies the type of the template, which the following sections describe in more detail.

### 2.2.1.1. File

Feedback 

A single file template is specified as type `file`. It defines a template, where the target file is created from only a single source file. A typical entry has the following structure:

```
Type: file
File: <filename>
Variables: <variable1>
User: <owner>
Group: <group>
Mode: <file-mode>
Preinst: <module>
Postinst: <module>
...
```

The following keys can be used:

**File (required)**

Specifies both the target and source file name, which are identical. The source file containing the template must be put below the `conf/files/` directory. The file can contain any textual content and is processed as described in Section 2.3.

The template file is installed to `/etc/univention/templates/files/`.

**Variables (optional)**

This key can be given multiple times and specifies the name of UCR variables, which trigger the file commit process. This is normally only required for templates using `@!@` Python code regions. Variables used in `@%@` sections do not need to be listed explicitly, since `ucr` extracts them automatically.

The variable name is actually a Python regular expression, which can be used to match, for example, all variable names starting with a common prefix.

**User (optional),**

**Group (optional),**

**Mode (optional)**

These specify the symbolic name of the user, group and octal file permissions for the created target file. If no values are explicitly provided, then `root:root` is used by default and the file mode is inherited from the source template.

**Preinst (optional),**

**Postinst (optional)**

These specify the name of a Python module located in `/etc/univention/templates/modules/`, which is called before and after the target file is re-created. The module must implement the following two functions:

```
def preinst(config_registry, changes):
```

`debian/package.univention-config-registry`


```
pass
def postinst(config_registry, changes):
    pass
```

Each function receives two arguments: The first argument `config_registry` is a reference to an instance of `ConfigRegistry`. The second argument `changes` is a dictionary of 2-tuples, which maps the names of all changed variables to (old-value, new-value).

`univention-install-config-registry` installs the module file to `/etc/univention/templates/modules/`.

If a script `/etc/univention/templates/scripts/full-path-to-file` exists, it will be called after the file is committed. The script is called with the argument `postinst`. It receives the same list of changed variables as documented in Section 2.2.1.3.

### 2.2.1.2. Multifile

Feedback 

A multi file template is specified once as type `multifile`, which describes the target file name. In addition to that multiple sections of type `subfile` are used to describe source file fragments, which are concatenated to form the final target file. A typical multifile has the following structure:

```
Type: multifile
Multifile: <target-filename>
User: <owner>
Group: <group>
Mode: <file-mode>
Preinst: <module>
Postinst: <module>
Variables: <variable1>

Type: subfile
Multifile: <target-filename>
Subfile: <fragment-filename>
Variables: <variable1>
...
```

The following keys can be used:

#### Multifile (required)

This specifies the target file name. It is also used to link the multifile entry to its corresponding subfile entries.

#### Subfile (required)

The source file containing the template fragment must be put below the `conffiles/` directory in the Debian source package. The file can contain any textual content and is processed as described in Section 2.3. The template file is installed to `/etc/univention/templates/files/`.

Common best practice is to start the filename with two digits to allow consistent sorting and to put the file in the directory named like the target filename suffixed by `.d`, that is `conffiles/target-filename.d/00fragment-filename`.

#### Variables (optional)

Variables can be declared in both the `multifile` and `subfile` sections. The variables from all sections trigger the commit of the target file. Until UCS-2.4 only the `multifile` section was used, since UCS-3.0 the `subfile` section should be preferred (if needed).




User (optional),  
Group (optional),  
Mode (optional),  
Preinst (optional),  
Postinst (optional)

Same as above for file.

The same script hook as above for file is also supported.

### 2.2.1.3. Script

Feedback 

A script template allows an external program to be called when specific UCR variables are changed. A typical script entry has the following structure:

```
Type: script
Script: <filename>
Variables: <variable1>
```

The following keys can be used:

Script (required)

Specifies the filename of an executable, which is installed to `/etc/univention/templates/scripts/`.

The script is called with the argument `generate`. It receives the list of changed variables on standard input. For each changed variable a line containing the name of the variable, the old value, and the new value separated by `@%@` is sent.

Variables (required)

Specifies the UCR variable names, which should trigger the script.

### Warning

There is *no* guarantee that `Script` is executed *after* a file has been committed. If this is required for e.g. restarting a service place the script instead at the location mentioned at the end of Section 2.2.1.1 [24].

### Note

The script interface is quiet limited for historical reasons. Consider it deprecated in favor of `Module`.

### 2.2.1.4. Module

Feedback 

A module template allows a Python module to be run when specific UCR variables are changed. A typical module entry has the following structure:

```
Type: module
Module: <filename>
Variables: <variable1>
```

The following keys can be used:

`debian/package.univention-config-reg-  
istry-variables`

Module (required)

Specifies the filename of a Python module, which is installed to `/etc/univention/templates/modules/`.

The module must implement the following function:

```
def handler(config_registry, changes):
    pass
```

The function receives two arguments: The first argument `config_registry` is a reference to an instance of `ConfigRegistry`. The second argument `changes` is a dictionary of 2-tuples, which maps the names of all changed variables to (old-value, new-value).

`univention-install-config-registry` installs the module to `/etc/univention/templates/modules/`.


Variables (required)

Specifies the UCR variable names, which should trigger the module.

## Warning

There is *no* guarantee that Module is executed *after* a file has been committed. If this is required for e.g. restarting a service use `Preinst` or `Postinst` as mentioned in Section 2.2.1.1 [24] instead.

## 2.2.2. `debian/package.univention-config-registry-variables`

Feedback 

For UCR variables a description should be registered. This description is shown in the *Univention Config Registry* module of the UMC as a mouse-over. It can also be queried by running `ucr info variable/name` on the command line.

The description is provided on a per-package basis as a file, which uses the ini-style format. The file is processed and copied by `univention-install-config-registry-info` into `/etc/univention/registry.info/variables/`. The command `univention-install-config-registry-info` is invoked indirectly by `univention-install-config-registry`, which should be called instead from `debian/rules`.

For each variable a section of the following structure is defined:

```
[<variable/name>]
Description[en]=<description>
Description[<language>]=<description>
Type=<type>
ReadOnly=<yes|no>
Categories=<category,...>
```

`[variable/name]` (required)

For each variable description one section needs to be created. The name of the section must match the variable name.

To describe multiple variables with a common prefix and/or suffix, the regular expression `.*` can be used to match any sequence of characters. This is the only supported regular expression!

Description[ *language* ] (required)

A descriptive text for the variable. It should mention the valid and default values. The description can be given in multiple languages, using the two-letter-code following [ISO639].

Type (required)

The syntax type for the value. This is unused in UCS-3.1, but future versions might use this for validating the input. Valid values include `str` for strings, `bool` for boolean values, and `int` for integers.


ReadOnly (optional)

This declares a variable as read-only and prohibits changing the value through UMC. The restriction is not applied when using the command line tool `ucr`. Valid values are `true` for read-only and `false`, which is the default.

Categories (required)

A list of categories, separated by comma. This is used to group related UCR variables. New categories don't need to be declared explicitly, but it is recommended to do so following Section 2.2.3.

## 2.2.3. `debian/package.univention-config-registry-categories`

Feedback 

UCR variables can be grouped into categories, which can help administrators to find related settings. Categories are referenced from `.univention-config-registry-variables` files (see Section 2.2.2). They are created on-the-fly, but can be described further by explicitly defining them in a `.univention-config-registry-categories` file.

The description is provided on a per-package basis as a file, which uses the ini-style format. The file is processed and copied by `univention-install-config-registry-info` into `/etc/univention/registry.info/categories/`. The command `univention-install-config-registry-info` is invoked indirectly by `univention-install-config-registry`, which should be called instead from `debian/rules`.

For each category a section of the following structure is defined:

```
[<category-name>]
name[en]=<name>
name[<language>]=<translated-name>
icon=<file-name>
```

```
[category-name]
```

For each category description one section needs to be created.

name[ *language* ] (required)

A descriptive text for the category. The description can be given in multiple languages, using the two-letter-code following [ISO639].

icon (required)

The file name of an icon in either the Portable Network Graphics (PNG) format or Graphics Interchange Format (GIF). This is unused in UCS-3.1, but future versions might display this icon for variables in this category.

## 2.2.4. debian/package.univention-service

Long running services should be registered with UCR and UMC. This enables administrators to control these daemons using the UMC module *System services*.

The description is provided on a per-package basis as a file, which uses the ini-style format. The file is processed and copied by `univention-install-service-info` into `/etc/univention/service.info/services/`. The command `univention-install-service-info` is invoked indirectly by `univention-install-config-registry`, which should be called instead from `debian/rules`.

For each service a section of the following structure is defined:

```
[<service-name>]
description[<language>]=<description>
start_type=<service-name>/autostart
systemd=<service-name>.service
icon=<service/icon_name>
programs=<executable>
name=<service-name>
init_script=<init.name>
```

```
[service-name],
name=service-name (optional)
```

For each daemon one section needs to be created. The service-name should match the name of the init-script in `/etc/init.d/`. If the name differs, it can be overwritten by the `name=` property.

`description[ language ]` (required)

A descriptive text for the service. The description can be given in multiple languages, using the two-letter-code following [ISO639].

`start_type` (required)

Specifies the name of the UCR variable, which controls if the service should be started automatically. It is recommended to use the shell library `/usr/share/univention-config-registry/init-autostart.lib` to evaluate the setting from the init-script of the service. If the variable is set to `false` or `no`, the service should never be started. If the variable is set to `manually`, the service should not be started automatically, but invoking the init-script directly with `start` should still start the service.

`systemd` (optional)

A comma separated list of **systemd** service names, which are enabled/disabled/masked when `start_type` is used. This defaults to the name of the service plus the suffix `.service`.

`init_script` (optional)

The name of the legacy init script below `/etc/init.d/`. This defaults to the name of the service. This option should not be used any more in favor of `systemd`.


`programs` (required)

A comma separated list of commands, which must be running to qualify the service as running. Each command name is checked against `/proc/*/cmdline`. To check the processes for additional arguments, the command can also consist of additional shell-escaped arguments.

icon (optional)

The file name of an icon in either Portable Network Graphics (PNG) format or Graphics Interchange Format (GIF) format. This is unused in UCS-3.1, but future versions might display the icon for the service.

## 2.3. UCR Template files `conffiles/path/to/file`

Feedback 

For each file, which should be written, one or more template files need be to created below the `conffiles/` directory. For a single-File template (see Section 2.2.1.1), the filename must match the filename given in the `File:` stanza of the *file* entry itself. For a Multifile template (see Section 2.2.1.2), the filename must match the filename given in the `File:` stanza of the *subfile* entries.

Each template file is normally a text file, where certain sections get substituted by computed values during the file commit. Each section starts and ends with a special marker. UCR currently supports the following kinds of markers:

`@@@` variable reference

Sections enclosed in `@@@` are simple references to Univention Configuration Registry variable. The section is replaced inline by the current value of the variable. If the variable is unset, an empty string is used.

ucr scans all files and subfiles on registration. All Univention Configuration Registry variables used in `@@@` are automatically extracted and registered for triggering the template mechanism. They don't need to be explicitly enumerated with `Variables:`-statements in the file `debian/package.univention-config-registry`.

`@!@` Python code

Sections enclosed in `@!@` contain Python code. Everything printed to `STDOUT` by these sections is inserted into the generated file. The Python code can access the `configRegistry`<sup>1</sup> variable, which is an already loaded instance of `ConfigRegistry`. Each section is evaluated separately, so no state is kept between different Python sections.

All Univention Configuration Registry variables used in a `@!@` Python section must be manually matched by a `Variables:` statement in the `debian/package.univention-config-registry` file. Otherwise the file is not updated on changes of the UCR variable.

```
@@@UCRWARNING=%PREFIX@@@,
@@@UCRWARNING_ASCII=%PREFIX@@@
```

This variant of the variable reference inserts a warning text, which looks like this:

```
# Warning: This file is auto-generated and might be overwritten by
#           univention-config-registry.
#           Please edit the following file(s) instead:
# Warnung: Diese Datei wurde automatisch generiert und kann durch
#           univention-config-registry überschrieben werden.
#           Bitte bearbeiten Sie an Stelle dessen die folgende(n)
#           Datei(en):
#
#           /etc/univention/templates/files/etc/hosts.d/00-base
#           /etc/univention/templates/files/etc/hosts.d/20-static
#           /etc/univention/templates/files/etc/hosts.d/90-ipv6defaults
#
```

<sup>1</sup> Historically Univention Configuration Registry was named “Univention Base Config”. For backward compatibility the alias `baseConfig` is still provided. It should not be used anymore and will be removed in a future version of UCS.

It should be inserted once at the top to prevent the user from editing the generated file. For single File templates, it should be on the top of the template file itself. For Multifile templates, it should only be on the top the first subfile.


Everything between the equal sign and the closing @%% defines the *PREFIX*, which is inserted at the beginning of each line of the warning text. For shell scripts, this should be # , but other files use different characters to start a comment. For files, which don't allow comments, the header should be skipped.

## Warning

Several file formats require the file to start with some *magic data*. For example shell scripts must start with a hash-bang (#!) and XML files must start with `<?xml version="1.0" encoding="UTF-8" ?>` (if used). Make sure to put the warning after these headers!

The UCRWARNING\_ASCII variant only emits 7-bit ASCII characters, which can be used for files, which are not 8 bit clean or unicode aware.

## 2.4. Build integration

Feedback 

During package build time `univention-install-config-registry` needs to be called. This should be done by overriding the `dh_auto_install_target` in `debian/rules`:


```
override_dh_auto_install:
    univention-install-config-registry
    dh_auto_install
```

This invocation copies the referenced files to the right location in the binary package staging area `debian/package/etc/univention/`. Internally `univention-install-config-registry-info` and `univention-install-service-info` are invoked, which should not be called explicitly anymore. The calls also insert code into the files `debian/package.preinst.debhelper`, `debian/package.postinst.debhelper` and `debian/package.prerm.debhelper` to register and un-register the templates. Therefore it's important that customized maintainer scripts use the `#DEBHELPER#` marker, so that the generated code gets inserted into the corresponding `preinst`, `postinst` and `prerm` files of the generated binary package.

The invocation also adds ***univention-config*** to `misc:Depends` to ensure that the package is available during package configuration time. Therefore it's important that `${misc:Depends}` is used in the `Depends` line of the package section in the `debian/control` file.


```
Package: ...
Depends: ..., ${misc:Depends}, ...
```

## 2.5. Examples

Feedback 

This sections contains several simple examples for the use of Univention Configuration Registry. The complete source of these examples is available separately. The download location is given in each example below. Since almost all Univention Corporate Server packages use UCR, their source code provides additional examples.

### 2.5.1. Minimal File example

Feedback 

This example provides a template for `/etc/papersize`, which is used to configure the default paper size. A Univention Configuration Registry variable `print/papersize` is registered, which can be used to configure the papersize.

Source code: [doc/developer-reference/ucr/papersize/](https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/ucr/papersize/)<sup>1</sup>

conf/files/etc/papersize

The template file only contains one line. Please note that this file does not start with the “UCR-WARNING”, since the file must only contain the paper size and no comments.

```
@%@print/papersize@%@
```

debian/papersize.univention-config-registry

The file defines the templates and is processed by `univention-install-config-registry` during the package build and afterwards by `univention-config-registry` during normal usage.

```
Type: file
File: etc/papersize
```

debian/papersize.univention-config-registry-variables

The file describes the newly defined Univention Configuration Registry variable.

```
[print/papersize]
Description[en]=specify preferred paper size [a4]
Description[de]=Legt die bevorzugte Papiergröße fest [a4]
Type=str
Categories=service-cups
```

debian/papersize.postinst

Sets the Univention Configuration Registry variable to a default value after package installation.

```
#!/bin/sh

#DEBHELPER#

ucr set print/papersize?a4

exit 0
```

debian/rules

Invoke `univention-install-config-registry` during package build to install the files to the appropriate location. It also creates the required commands for the maintainer scripts (see Section B.3.5) to register and unregister the templates during package installation and removal.

```
#!/usr/bin/make -f

override_dh_auto_install:
    dh_auto_install
    univention-install-config-registry

%:
    dh $@
```

Note that tabulators must be used for indentation in this Makefile-type file.

<sup>1</sup> <https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/ucr/papersize/>

## Multifile example


debian/control

The automatically generated dependency on **univention-config** is inserted by `univention-install-config-registry` via `debian/papersize.substvars`.

```
Source: papersize
Section: univention
Priority: optional
Maintainer: Univention GmbH <packages@univention.de>
Build-Depends: debhelper (>= 7),
               univention-config-dev,
Standards-Version: 3.7.2

Package: papersize
Architecture: all
Depends: ${misc:Depends}
Description: An example package to configure the papersize
 This purpose of this package is to show how Univention Config
 Registry is used.
.
For more information about UCS, refer to:
https://www.univention.de/
```

## 2.5.2. Multifile example

Feedback 

This example provides templates for `/etc/hosts.allow` and `/etc/hosts.deny`, which is used to control access to system services. See `hosts_access(5)` for more details.

Source code: [doc/developer-reference/ucr/hosts/](#)<sup>1</sup>

```
conffiles/etc/hosts.allow.d/00header,
conffiles/etc/hosts.deny.d/00header
```

The first file fragment of the file. It starts with `@@@UCRWARNING=# @@@`, which is replaced by the warning text and a list of all subfiles.

```
@@@UCRWARNING=# @@@
# /etc/hosts.allow: list of hosts that are allowed to access the
  system.
#                               See the manual pages hosts_access(5) and
  hosts_options(5).
```

```
conffiles/etc/hosts.allow.d/50dynamic,
conffiles/etc/hosts.deny.d/50dynamic
```

A second file fragment, which uses Python code to insert access control entries configured through the Univention Configuration Registry variables `hosts/allow/` and `hosts/deny/`.

```
@!@
for key, value in sorted(configRegistry.items()):
    if key.startswith('hosts/allow/'):
        print value
@!@
```

<sup>1</sup> <https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/ucr/hosts/>



debian/hosts.univention-config-registry

The file defines the templates and is processed by univention-install-config-registry.

```
Type: multifile
Multifile: etc/hosts.allow

Type: subfile
Multifile: etc/hosts.allow
Subfile: etc/hosts.allow.d/00header

Type: subfile
Multifile: etc/hosts.allow
Subfile: etc/hosts.allow.d/50dynamic
Variables: ^hosts/allow/. *

Type: multifile
Multifile: etc/hosts.deny

Type: subfile
Multifile: etc/hosts.deny
Subfile: etc/hosts.deny.d/00header

Type: subfile
Multifile: etc/hosts.deny
Subfile: etc/hosts.deny.d/50dynamic
Variables: ^hosts/deny/. *
```

debian/hosts.univention-config-registry-variables

The file describes the newly defined Univention Configuration Registry variables.

```
[hosts/allow/. *]
Description[en]=An permissive access control entry for system
  services, e.g. "ALL: LOCAL"
Description[de]=Eine erlaubende Zugriffsregel für Systemdienste, z.B.
  "ALL: LOCAL".
Type=str
Categories=service-net

[hosts/deny/. *]
Description[en]=An denying access control entry for system services,
  e.g. "ALL: ALL".
Description[de]=Eine verbotende Zugriffsregel für Systemdienste,
  z.B. "ALL: ALL".
Type=str
Categories=service-net
```

### 2.5.3. Services

Feedback 

This example provides a template to control the atd service through an Univention Configuration Registry variable atd/autostart.

Source code: [doc/developer-reference/ucr/service/](https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/ucr/service/)<sup>1</sup>

<sup>1</sup> <https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/ucr/service/>

conffiles/etc/init.d/atd

The template replaces the original file with a version, which checks the Univention Configuration Registry variable `atd/autostart` before starting the `at` daemon. Please note that the “UCRWARNING” is put after the hash-bash line.

```
#!/bin/sh
@@@UCRWARNING=# @@@
### BEGIN INIT INFO
# Provides:          atd
# Required-Start:    $syslog $time $remote_fs
# Required-Stop:     $syslog $time $remote_fs
# Default-Start:     2 3 4 5
# Default-Stop:      0 1 6
# Short-Description: Deferred execution scheduler
# Description:       Debian init script for the atd deferred
#                    executions
#                    scheduler
### END INIT INFO
# pidfile: /var/run/atd.pid
#
# Author: Ryan Murray <rmurray@debian.org>
#

PATH=/bin:/usr/bin:/sbin:/usr/sbin
DAEMON=/usr/sbin/atd
PIDFILE=/var/run/atd.pid

test -x $DAEMON || exit 0

. /lib/lsb/init-functions

case "$1" in
    start)
        # check ucr autostart setting
        IAL="/usr/share/univention-config-registry/init-autostart.lib"
        if [ -f "$IAL" ]; then
            . "$IAL"
            check_autostart atd atd/autostart
        fi
        log_daemon_msg "Starting deferred execution scheduler" "atd"
        start_daemon -p $PIDFILE $DAEMON
        log_end_msg $?
        ;;
    stop)
        log_daemon_msg "Stopping deferred execution scheduler" "atd"
        killproc -p $PIDFILE $DAEMON
        log_end_msg $?
        ;;
    force-reload|restart)
        $0 stop
        $0 start
        ;;
    status)
        status_of_proc -p $PIDFILE $DAEMON atd && exit 0 || exit $?

```

```
    ;;
*)
    echo "Usage: $0 {start|stop|restart|force-reload|status}"
    exit 1
    ;;
esac

exit 0
```

Note the inclusion of `init-autostart.lib` and use of `check_autostart`.

`debian/service.univention-config-registry`

The file defines the templates.

```
Type: file
File: etc/init.d/atd
Mode: 755
Variables: atd/autostart
```

Note the additional `Mode` statement to mark the file as executable.

`debian/service.univention-config-registry-variables`

The file adds a description for the Univention Configuration Registry variable `atd/autostart`.

```
[atd/autostart]
Description[en]=Automatically start the AT daemon on system startup
[yes]
Description[de]=Automatischer Start des AT-Dienstes beim Systemstart
[yes]
Type=bool
Categories=service-at
```

`debian/service.postinst`

Set the Univention Configuration Registry variable to automatically start the `atd` on new installations.

```
#!/bin/sh

#DEBHELPER#

ucr set atd/autostart=yes

exit 0
```

`debian/control`


***univention-base-files*** must be added manually as an additional dependency, since it is used from within the shell code.

```
Source: service
Section: univention
Priority: optional
Maintainer: Univention GmbH <packages@univention.de>
Build-Depends: debhelper (>= 7),
    univention-config-dev,
```

```
Standards-Version: 3.7.2

Package: service
Architecture: all
Depends: ${misc:Depends},
        univention-base-files,
Description: An example package to configure services
 This purpose of this package is to show how Univention Config
 Registry is used.
.
For more information about UCS, refer to:
https://www.univention.de/
```

## 2.6. Python 3 Migration

Feedback 

In UCS 5.0 all UCR templates and UCR modules must be Python 2 and Python 3 compatible. This must also be the case for UCS 4.4 and newer, because during the upgrade to UCS 5.0 UCR templates can be evaluated with either Python version.

Most templates simply use the Python 2 print statement:

```
print configRegistry.get('my/variable')
```

Parenthesis have to be added:

```
print(configRegistry.get('my/variable'))
```

Please note that it is not possible yet to use Python 3 only syntax (as in Python 2 print is a statement), such as:

```
print(configRegistry.get('my/variable'), file=sys.stderr)
```

It is also not possible to use

```
from __future__ import print_function
```

as Univention Configuration Registry executes Python code before the template is imported.

The deprecated variable `baseConfig` has been removed in UCS 5.0 but `configRegistry` remains for using.

The API of `ConfigRegistry` works with `str`. For Python 2 this equals bytes, while for Python 3 this is a unicode string.

The test case `/usr/share/ucs-test/03_ucr/37check-ucr-templates-py3-migration-status.py` from the package **ucs-test-ucr** can be used to check if the UCR template output works with both Python versions and is idempotent.

UCR modules and scripts have no API changes. They simply need to be migrated to be Python 3 compatible.


## Chapter 3. Domain Join

3.1. Join scripts .....	37
3.2. Join status .....	37
3.3. Running join scripts .....	38
3.4. Writing join scripts .....	38
3.4.1. Basic join script example .....	38
3.4.2. Join script exit codes .....	40
3.4.3. Join script libraries .....	41
3.4.3.1. <i>univention-join</i> .....	41
3.4.3.2. <i>shell-univention-lib</i> .....	42
3.5. Writing unjoin scripts .....	46

An UCS system is normally joined into a domain. This establishes a trust relation between the different hosts, which enables users to access services provided by any host of the domain.


Joining a system into a domain requires write permission to create and modify entries in the Univention directory service (LDAP). Local `root` permission on the joining host is not sufficient to get write access to the domain wide LDAP service. Instead valid LDAP credentials must be entered interactively by the administrator doing the join.

### 3.1. Join scripts

Feedback 

Packages requiring write access to the Univention directory service can provide so called *join scripts*. They are installed into `/usr/lib/univention-install/`. The name of each join script is normally derived from the name of the binary package containing it. It is prefixed with a two-digit number, which is used to order the scripts lexicographically. The filename either ends in `.inst` or `.uinst`, which distinguishes between join script and unjoin script (see Section 3.5). The file must have the executable permission bits set.

### 3.2. Join status

Feedback 

For each join script a version number is tracked. This is used to skip re-executing join scripts, which already have been executed. This is mostly a performance optimization, but is also used to find join scripts which need to be run.

The text file `/var/univention-join/status` is used to keep track of the state of all join scripts. For each successful run of a join script a line is appended to that file. That record consists of three space separated entries:

```
$script_name v$version successful
```

1. The first entry contains the name of the join script without the two-digit prefix and without the `.inst` suffix, usually corresponding to the package name.
2. The second entry contains a version number prefixed by a `v`. It is used to keep track of the latest version of the join script, which has been run successfully. This is used to identify, which join scripts need to be executed and which can be skipped, because they were already executed in the past.
3. The third column contains the word *successful*.

If a new version of the join script is invoked, it just appends a new record with a higher version number at the end of the file.

### 3.3. Running join scripts

There exist three commands related to running join scripts:

`univention-join`

When `univention-join` is invoked, a machine account is created. The *distinguished name* (dn) of that entry is stored locally in the Univention Configuration Registry variable `ldap/hostdn`. A random password is generated, which is stored in the file `/etc/machine.secret`.

After that the file `/var/univention-join/status` is cleared and all join scripts located in `/usr/lib/univention-install/` are executed in lexicographical order.

`univention-run-join-scripts`

This command is similar to `univention-join`, but skips the first step of creating a machine account. Only those join scripts are executed, whose current version is not yet registered in `/var/univention-join/status`.

`univention-check-join-status`

This command only checks for join scripts in `/usr/lib/univention-install/`, whose version is not yet registered in `/var/univention-join/status`.

When packages are installed, it depends on the server role, if join scripts are invoked automatically from the `postinst` Debian maintainer script or not. This only happens on master and backup domain controller system roles, where the local `root` user has access to the file containing the LDAP credentials. On all other system roles the join scripts need to be run manually by invoking `univention-run-join-scripts` or doing so through UMC.

### 3.4. Writing join scripts

Similar to the Debian maintainer scripts (see Section B.3.5) they should be idem-potent: They should transform the system from any state into the state required by the package, that is:

- They should create newly introduced objects in the Univention directory service
- They should not fail if the object already exists
- They should be careful about modifying objects, which might have been modified by the administrator in the past

Join scripts may be called from multiple system roles and different versions. Therefore it is important that these scripts *do not destroy or remove data still used by other systems!*

#### 3.4.1. Basic join script example

This example provides a template for writing join scripts. The package is called *join-template* and just contains a join and an unjoin script. They demonstrate some commonly used functions.

Source code: `doc/developer-reference/join/join-template/`

`50join-template.inst`

The join script in UCS packages is typically located in the package root directory. It has the following base structure:

---

<https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/join/join-template/>

```
#!/bin/sh

## joinscript api: bindpwdfile

VERSION=1
. /usr/share/univention-join/joinscripthelper.lib
joinscript_init

SERVICE="MyService"

eval "$(ucr shell)"

. /usr/share/univention-lib/ldap.sh
ucs_addServiceToLocalhost "$SERVICE" "$@"

udm "computers/$server_role" modify "$@" \
  --dn "$ldap_hostdn" \
  --set reinstall=0 || die

# create container for extended attributes to be placed in
udm container/cn create "$@" \
  --ignore_exists \
  --position "cn=custom attributes,cn=univention,$ldap_base" \
  --set name="myservice" || die

# some extended attributes would be added here

joinscript_save_current_version
exit 0
```

Please note the essential argument "\$@" when udm is invoked, which passes on the required LDAP credentials described in Section 4.4. Since UCS 4.3-0 erratum 85 credentials can also be passed via a file to prevent the password from being visible from the process tree. To enable this API one of the following comments must be placed inside the join script:

```
## joinscript api: bindpwdfile
```

This instructs univention-join and univention-run-join-script to pass the credential password via a file. The name of the file is passed via the parameter `--bindpwdfile path`. The old parameter `--bindpwd secret` will not be supplied in this case.

```
## joinscript api: nocredentials
```

This instructs univention-join and univention-run-join-script to not pass the credentials via the `--bind*` parameters at all. Instead the script may retrieve the credentials from the two files named `/var/run/univention-join/binddn` and `/var/run/univention-join/bindpwd`. They exist only while univention-join or univention-run-join-script are running.

```
debian/join-template.install
```

The scripts need to be installed into `/usr/lib/univention-install/`, which is achieved by the following lines:

```
50join-template.inst usr/lib/univention-install/
```

<https://errata.software-univention.de/#/?erratum=4.3x85>

```
50join-template-uninstall.uinst usr/lib/univention-uninstall/
```

Note that this package also installs an unjoin script.

```
debian/join-template.postinst
```

The join script should be invoked automatically on master and backup domain controller systems. On all other system roles an administrator must run the join script manually through `univention-run-join-scripts`.

```
#!/bin/sh

#DEBHELPER#

if [ "$1" = "configure" ]
then
    uinst=/usr/lib/univention-install/50join-template-uninstall.uinst
    [ -e "$uinst" ] && rm "$uinst"
fi

. /usr/share/univention-lib/base.sh
call_joinscript 50join-template.inst

exit 0
```

```
debian/control
```


The package uses two shell libraries, which are described in more detail in Section 3.4.3. Both packages providing them must be added as additional runtime dependencies.

The unjoin functions were added to UCS 3.1-0 only as erratum update 81<sup>1</sup>. Because of this the minimum versions must be specified explicitly.

```
Source: join-template
Section: univention
Priority: optional
Maintainer: Univention GmbH <packages@univention.de>
Build-Depends: debhelper (>= 7)
Standards-Version: 3.7.2

Package: join-template
Architecture: all
Depends: univention-join (>= 5.0.20-1),
        shell-univention-lib (>= 2.0.17-1),
        ${misc:Depends}
Description: An example package for join scripts
 This purpose of this package is to show how
 Univention Join scripts are used.
.
 For more information about UCS, refer to:
 https://www.univention.de/
```

### 3.4.2. Join script exit codes

Feedback 

Join scripts must return the following exit codes:

<sup>1</sup> <https://errata.software-univention.de/ucs/3.1/80.html>



0

The join script was successful and completed all tasks to join the software package on the system into the domain. All required entries in the Univention directory service were created or do already exist as expected.

The script will be marked as successfully run. As a consequence the join script will not be called again in this version.

1

The script did not complete and some task to fully join the system into the domain are still pending. Some entries could not be created in LDAP or exist in a state, which is incompatible with this version of the package.


The script needs to be run again after fixing the problem, either manually or automatically.

2

Some internal functions were called incorrectly. For example the credentials were wrong.


The script needs to be run again.

### 3.4.3. Join script libraries

Feedback 

There exist two shell libraries, which provide functions which help in writing join scripts:

#### 3.4.3.1. *univention-join*

Feedback 

The package contains the shell library `/usr/share/univention-join/join-scripthelper.lib`. It provides functions related to updating the join status file.

```
joinscript_init
```

This function parses the status file and exits the shell script, if a record is found with a version greater or equal to value of the environment variable `VERSION`. The name of the join script is derived from `$0`.

```
joinscript_save_current_version
```

This function appends a new record to the end of the status file using the version number stored in the environment variable `VERSION`.

```
joinscript_check_any_version_executed
```

This function returns success (0), if any previous version of the join scripts was successfully executed. Otherwise it returns a failure (1).

```
joinscript_check_specific_version_executed version
```

This function returns success (0), if the specified version `version` of the join scripts was successfully executed. Otherwise it returns a failure (1).

```
joinscript_check_version_in_range_executed min max
```

This function returns success (0), if any successfully run version of the join script falls within the range `min..max`, inclusively. Otherwise it returns a failure (1).

```
joinscript_extern_init join-script
```

The check commands mentioned above can also be used in other shell programs, which are not join scripts. There the name of the join script to be checked must be explicitly given. Instead of calling `joinscript_init`, this function requires an additional argument specifying the name of the `join-script`.

```
joinscript_remove_script_from_status_file name
```

Removes the given join script from the join script status file `/var/univention-join/status`. The name should be the basename of the joinscript without the prefixed digits and the suffix `.inst`. So if the joinscript `/var/lib/univention-install/50join-template.inst` shall be removed, one has to execute `joinscript_remove_script_from_status_file join-template`. Primarily used in unjoin scripts.

```
die
```

A convenience function to exit the join script with an error code. Used to guarantee that LDAP modifications were successful: `some_udm_create_call || die`

These functions use the following environment variables:

#### VERSION

This variable must be set before `joinscript_init` is invoked. It specifies the version number of the join script and is used twice:

1. It defines the current version of the join script.
2. If that version is already recorded in the status file, the join script qualifies as having been run successfully and the re-execution is prevented. Otherwise the join status is incomplete and the script needs to be invoked again.

The version number should be incremented for a new version of the package, when the join script needs to perform additional modifications in LDAP compared to any previous packaged version.

The version number must be a positive integer. The variable assignment in the join script must be on its own line. It may optionally quote the version number with single quotes (') or double quotes ("). The following assignment are valid:

```
VERSION=1
VERSION='2'
VERSION="3"
```

#### JS\_LAST\_EXECUTED\_VERSION

This variable is initialized by `joinscript_init` with the latest version found in the join status file. If no version of the join script was ever executed and thus no record exists, the variable is set to 0. The join script can use this information to decide what to do on an upgrade.

### 3.4.3.2. shell-univention-lib

Feedback 

The package contains the shell library `/usr/share/univention-lib/base.sh`. Since package version `>= 2.0.17-1` it provides the following functions:

```
call_joinscript [--binddn bind-dn [--bindpwd bind-password] | [--bindpwdfile
filename]] [XXjoin-script.inst]
```

This calls the join script called `XXjoin-script.inst` from the directory `/usr/lib/univention-install/`. The optional LDAP credentials `bind-dn` and `bind-password` respective filename are passed on as-is.

```
call_joinscript_on_dcmaster [--binddn bind-dn {[--bindpwd bind-password] |
[--bindpwdfile filename]]} [XXjoin-script.inst]
```

Similar to `call_joinscript`, but also checks the system role and only executes the script on the master domain controller.

```
remove_joinscript_status [name]
```

Removes the given join script name from the join script status file `/var/univention-join/status`. Note that this command does the same as `joinscript_remove_script_from_status_file` provided by **univention-join** (see Section 3.4.3.1).

```
call_unjoinscript [--binddn bind-dn {[--bindpwd bind-password] | [--bindpwdfile
filename]]} [XXunjoin-script.uinst]
```

Calls the given unjoin script `unjoin-script` on master and backup domain controller systems. The file name must be relative to the directory `/usr/lib/univention-install/`. The optional LDAP credentials `bind-dn` and `bind-password` respective filename are passed on as-is. Afterwards the unjoin script is automatically deleted.

```
delete_unjoinscript [XXunjoin-script.uinst]
```

Deletes the given unjoin script `XXunjoin-script.uinst` if it does not belong to any package. The file name must be relative to the directory `/usr/lib/univention-install/`.

```
stop_udm_cli_server
```

When `univention-directory-manager` is used the first time a server is started automatically that caches some information about the available modules. When changing some of this information (e.g. when adding or removing extended attributes) the server should be stopped manually.

The package also contains the shell library `/usr/share/univention-lib/ldap.sh`. It provides convenience functions to query the Univention directory service and modify objects. For (un)join scripts the following functions might be important:

```
ucs_addServiceToLocalhost servicename [--binddn bind-dn {[--bindpwd bind-
password] | [--bindpwdfile filename]]}
```

Registers the additional service `servicename` in the LDAP object representing the local host. The optional LDAP credentials `bind-dn` and `bind-password` respective filename are passed on as-is.

### Example 3.1. Service registration in join script

```
ucs_addServiceToLocalhost "MyService" "$@"
```

```
ucs_removeServiceFromLocalhost servicename [--binddn bind-dn {[--bindpwd
bind-password] | [--bindpwdfile filename]]}
```

Removes the service `servicename` from the LDAP object representing the local host, effectively reverting an `ucs_addServiceToLocalhost` call. The optional LDAP credentials `bind-dn` and `bind-password` respective filename are passed on as-is.

### Example 3.2. Service unregistration in unjoin script

```
ucs_removeServiceFromLocalhost "MyService" "$@"
```

```
ucs_isServiceUnused servicename [--binddn bind-dn {[--bindpwd bind-pass-  
word] | [--bindpwdfile filename]}]
```

Returns 0 if no LDAP host object exists where the service `servicename` is registered with.

### Example 3.3. Check for unused service in unjoin script

```
if ucs_isServiceUnused "MyService" "$@"  
then  
    uninstall_my_service  
fi
```

```
ucs_registerLDAPExtension [--binddn bind-dn { --bindpwd bind-password | --  
bindpwdfile filename }]  
{ { --schema filename | --acl filename | --udm_syntax filename | --udm_hook file-  
name ...}  
| --udm_module filename [--messagecatalog filename...] [--umcregistration filename]  
[--icon filename...] }  
[--packagename packagename] [--packageversion packageversion] [--ucsversionstart  
ucsversion] [--ucsversionend ucsversion]
```

The shell function `ucs_registerLDAPExtension` from the Univention shell function library (see Section 14.3) can be used to register several extension in LDAP. This shell function offers several modes:

```
--schema filename.schema
```

Register one or more LDAP schema extension (see Section 4.2)

```
--acl filename.acl
```

Register one or more LDAP access control list (see Section 4.3)

```
--udm_syntax filename.py
```

Register one or more UDM syntax extension (see Section 6.4)

```
--udm_hook filename.py
```

Register one or more UDM hook (see Section 6.2.4)

```
--udm_module filename.py
```

Register a single UDM module (see Section 6.3)

The modes can be combined. If more than one mode is used in one call of the function, the modes are always processed in the order as listed above. Each of these options expects a filename as an required argument.

The following options can be given multiple times, but only after the option `--udm_module`:

```
--messagecatalog prefix/language.mo
```

The option can be used to supply message translation files in GNU message catalog format. The language must be a valid language tag, i.e. must correspond to a subdirectory of `/usr/share/locale/`.

```
--umcmessagecatalog prefix/language-module_id-application_name.mo
```

Similar to the option above this option can be used to supply message translation files in GNU message catalog format, but for the UMC. The filename takes the form `language-moduleid.mo`,

e.g. `de-udm.mo`, where *language* must be a valid language tag, i.e. must correspond to a subdirectory of `/usr/share/locale/`. The *moduleid* is specified in the UMC registration file (see Section 7.5.2). The MO files are then placed under `/usr/share/univention-management-console/i18n/` in a subdirectory with the corresponding language short code.

`--umcregistration filename.xml`

The option can be used to supply an UMC registration file (see Section 7.5.2) to make the UDM module accessible via Univention Management Console (UMC).

`--icon filename`

The option can be used to supply icon files (png or jpeg, in 16×16 or 50×50, or svgz).

Called from a joinscript, the function automatically determines some required parameters, like the app identifier plus Debian package name and version, required for the creation of the corresponding object. After creation of the object the function waits up to 3 minutes for the master domain controller to signal availability of the new extension and reports success or failure. For UDM extensions it additionally checks that the corresponding file has been made available in the local filesystem. Failure conditions may occur e.g. in case the new LDAP schema extension collides with the schema currently active. The master domain controller only activates a new LDAP schema or ACL extension if the configuration check succeeded.

## Note

The corresponding UDM modules are documented in Chapter 4 and Chapter 6.

Before calling the shell function the shell variable `UNIVENTION_APP_IDENTIFIER` should be set to the versioned app identifier (and exported to the environment of subprocesses). The shell function will then register the specified app identifier with the extension object to indicate that the extension object is required as long as this app is installed anywhere in the UCS domain.

The options `--packagename` and `--packageversion` should usually not be used, as these parameters are determined automatically. To prevent accidental downgrades the function `ucs_registerLDAPExtension` (as well as the corresponding UDM module) only execute modifications of an existing object if the Debian package version is not older than the previous one.

`ucs_registerLDAPExtension` supports two additional options to specify a valid range of UCS versions, where an extension should be activated. The options are `--ucsversionstart` and `--ucsversionend`. The version check is only performed whenever the extension object is modified. By calling this function from a joinscript, it will automatically update the Debian package version number stored in the object, triggering a re-evaluation of the specified UCS version range. The extension is activated up to and excluding the UCS version specified by `--ucsversionend`. This validity range is not applied to LDAP schema extensions, since they must not be undefined as long as there are objects in the LDAP directory which make use of it.

### Example 3.4. Extension registration in join script

```
export UNIVENTION_APP_IDENTIFIER="appID-appVersion" ## example
. /usr/share/univention-lib/ldap.sh

ucs_registerLDAPExtension "$@" \
  --schema /path/to/appschemaextension.schema \
  --acl /path/to/appaclextension.acl \
  --udm_syntax /path/to/appudmsyntax.py
```

```
ucs_registerLDAPExtension "$@" \
--udm_module /path/to/appudmmodule.py \
--messagecatalog /path/to/de.mo \
--messagecatalog /path/to/eo.mo \
--umregistration /path/to/module-object.xml \
--icon /path/to/moduleicon16x16.png \
--icon /path/to/moduleicon50x50.png


ucs_unregisterLDAPExtension [--binddn bind-dn { --bindpwd bind-password |
--bindpwdfile filename }]
{ --schema objectname | --acl objectname | --udm_syntax objectname | --udm_hook
objectname | --udm_module objectname ...}
```

There is a corresponding `ucs_unregisterLDAPExtension` function, which can be used to unregister extension objects. This only works if no App is registered any longer for the object. It must not be called unless it has been verified that no object in LDAP still requires this schema extension. For this reason it should generally not be called in unjoin scripts.

### Example 3.5. Schema unregistration in unjoin script

```
. /usr/share/univention-lib/ldap.sh
ucs_unregisterLDAPExtension "$@" --schema appschemaextension
```

## 3.5. Writing unjoin scripts

Feedback 

On package removal packages should clean up the data in Univention directory service. Removing data from LDAP also requires appropriate credentials, while removing a package only requires local `root` privileges. Therefore UCS provides support for so-called *unjoin scripts*. In most cases it reverts the changes of a corresponding join script.

### Warning

A domain is a distributed system. Just because one local system no longer wants to store some information in Univention directory service does not mean that the data should be deleted. There might still be other systems in the domain which still require the data.

Therefore “the first system to come” should setup the data, while only “the last system to go” may clean up the data.

Just like join scripts an unjoin script is prefixed with a two-digit number for lexicographical ordering. To reverse the order of the unjoin scripts in comparison to the corresponding join scripts, the number of the unjoin script should be 100 minus the number of the corresponding join script. The suffix of an unjoin script is `-uninstall.uinst` and it should be installed in `/usr/lib/univention-uninstall/`.

On package removal the unjoin script would be deleted as well, while the Univention directory service might still contain data managed by the package. Therefore the script must be copied from there to `/usr/lib/univention-install/` in the `prerm` maintainer script.

Example: The package *univention-fetchmail* provides both a join script `/usr/lib/univention-install/91univention-fetchmail.inst` and the corresponding unjoin script as `/usr/lib/univention-uninstall/09univention-fetchmail-uninstall.uinst`.

As of UCS 3.1 `.inst` and `.uinst` are not distinguishable in the *UMC Join module* by the user. Therefore it is important to use the `-uninstall` suffix to give users a visual hint. Internally join scripts are always executed before unjoin scripts and then ordered lexicographically by their prefix.

To decide if an unjoin script is the last instance and should remove the data from LDAP, a service can be registered for each host where the package is installed.

For example the package *univention-fetchmail* uses `ucs_addServiceFromLocalhost "Fetchmail" "$@"` in the join script to register and `ucs_removeServiceFromLocalhost "Fetchmail" "$@"` in the unjoin script to unregister a service for the host. The data is removed from LDAP when in the unjoin script `ucs_isServiceUnused "Fetchmail" "$@"` returns 0. As a side effect adding the service also allows using this information to find and list those servers currently providing the Fetchmail service.

50join-template-uninstall.uinst

This unjoin script reverts the changes of the join script from Section 3.4.1.

```
#!/bin/sh

## joinscript api: bindpwdfile

# VERSION is needed for some tools to recognize that as a join script
VERSION=1
. /usr/share/univention-join/joinscripthelper.lib
joinscript_init

SERVICE="MyService"

eval "$(ucr shell)"

. /usr/share/univention-lib/ldap.sh
ucs_removeServiceFromLocalhost "$SERVICE" "$@" || die
if ucs_isServiceUnused "$SERVICE" "$@"
then
    # was last server to implement service. now the data
    # may be removed
    univention-directory-manager container/cn remove "$@" --dn \
        "cn=myservice,cn=custom attributes,cn=univention,$ldap_base" || die

    # Terminate UDM server to force module reload
    . /usr/share/univention-lib/base.sh
    stop_udm_cli_server
fi

# do NOT call "joinscript_save_current_version"
# otherwise an entry will be appended to /var/univention-join/status
# instead the join script needs to be removed from the status file
joinscript_remove_script_from_status_file join-template

exit 0
```

debian/join-template.prerm

The unjoin script has to be copied to the join script directory before it gets removed:

```
#!/bin/sh

#DEBHELPER#

if [ "$1" = "remove" ]
```

## Writing unjoin scripts

```
then
  cp /usr/lib/univention-uninstall/50join-template-uninstall.uinst \
    /usr/lib/univention-install/
fi

exit 0
```

debian/join-template.postrm

The unjoin script should be invoked automatically on master and backup domain controller systems after the package is removed. On all other system roles an administrator must run the join script manually through `univention-run-join-scripts`.

```
#!/bin/sh

#DEBHELPER#

if [ "$1" = "remove" ]
then
  . /usr/share/univention-lib/all.sh
  call_unjoinscript 50join-template-uninstall.uinst
fi

exit 0
```

debian/join-template.postinst

In case the package is installed again and the unjoin script still exists, because it was never executed, the unjoin script must be removed:

```
#!/bin/sh

#DEBHELPER#

if [ "$1" = "configure" ]
then
  uinst=/usr/lib/univention-install/50join-template-uninstall.uinst
  [ -e "$uinst" ] && rm "$uinst"
fi

. /usr/share/univention-lib/base.sh
call_joinscript 50join-template.inst


exit 0
```



# Chapter 4. Lightweight Directory Access Protocol (LDAP) in UCS

4.1. General .....	49
4.2. Packaging LDAP Schema Extensions .....	49
4.3. Packaging LDAP ACL Extensions .....	50
4.4. LDAP secrets .....	52
4.4.1. Password change .....	52

## 4.1. General

Feedback 


An LDAP server provides authenticated and controlled access to directory objects over the network. LDAP objects consist of a collection of attributes which conform to so called LDAP schemata. An in depth documentation of LDAP is beyond the scope of this document, other sources cover this topic exhaustively, e.g. <http://www.zytrax.com/books/ldap/> or the man pages (`slapd.conf(5)`, `slapd.access(5)`).

At least it should be noted that OpenLDAP offers two fundamentally different tool sets for direct access or modification of LDAP data: The `slap*` commands (`slapcat`, etc.) are very low level, operating directly on the LDAP backend data and should only be used in rare cases, usually with the LDAP server not running. The `ldap*` commands (`ldapsearch`, etc.) on the other hand are the proper way to perform LDAP operations from the command line and their functionality can equivalently be used from all major programming languages.

On top of the raw LDAP layer, the Univention Directory Manager offers an object model on a higher level, featuring advanced object semantics (see Chapter 6). That is the level that usually appropriate for app developers, which should be considered before venturing down to the level of direct LDAP operations. On the other hand, for the development of new UDM extensions it is important to understand some of the essential concepts of LDAP as used in UCS.

One essential trait of LDAP as used in UCS, is the strict enforcement of LDAP schemata. An LDAP server refuses to start if an unknown LDAP attribute is referenced either in the configuration or in the backend data. This makes it critically important to install schemata on all systems. To simplify this task UCS features a builtin mechanism for automatic schema replication to all UCS hosted LDAP servers in the UCS domain (see Chapter 5). The schema replication mechanism is triggered by installation of a new schema extension package on the UCS master. For redundancy it is strongly recommended to install schema extension packages also on the UCS backup systems. This way, a UCS backup can replace a UCS master in case the master needs to be replaced for some reason. To simplify these tasks even further, UCS offers methods to register new LDAP schemata and associated LDAP ACLs from any UCS system.

## 4.2. Packaging LDAP Schema Extensions

Feedback 

For some purposes, e.g. for app installation, it is convenient to be able to register a new LDAP schema extension from any system in the UCS domain. For this purpose, the schema extension can be stored as a special type of UDM object. The module responsible for this type of objects is called `settings/ldapschema`. As these objects are replicated throughout the UCS domain, the master domain controller and backup domain controller systems listen for modifications of these objects and integrate them into the local LDAP schema directory. As noted above, this simplifies the task of keeping the schema on the backup domain controller systems up to date with that on the master domain controller.

The commands to create the LDAP schema extension objects in UDM may be put into any join script (see Chapter 3). A LDAP schema extension object is created by using the UDM command line interface `univention-directory-manager` or its alias `udm`. LDAP schema extension objects can be stored anywhere

in the LDAP directory, but the recommended location would be `cn=ldapschema,cn=univention`, below the LDAP base. Since the join script creating the attribute may be called on multiple hosts, it is a good idea to add the `--ignore_exists` option, which suppresses the error exit code in case the object already exists in LDAP.

The UDM module `settings/ldapschema` requires several parameters:

`name` (required)

Name of the schema extension.

`data` (required)

The actual schema data in bzip2 and base64 encoded format.

`filename` (required)

The file name the schema should be written to on master domain controller and backup domain controller. The file name must not contain any path elements.

`package` (required)

Name of the Debian package which creates the object.

`packageversion` (required)

Version of the Debian package which creates the object. For object modifications the version number needs to increase unless the package name is modified as well.

`appididentifier` (optional)

The identifier of the app which creates the object. This is important to indicate that the object is required as long as the app is installed anywhere in the UCS domain. Defaults to `string`.

`active` (internal)

A boolean flag used internally by the master domain controller to signal availability of the schema extension (default: `FALSE`).

Since many of these parameters are determined automatically by the `ucs_registerLDAPExtension` shell library function, it is recommended to use the shell library function to create these objects (see Section 3.4.3.2).

### Example 4.1. Schema registration in join script

```
export UNIVENTION_APP_IDENTIFIER="appID-appVersion" ## example
. /usr/share/univention-lib/ldap.sh

ucs_registerLDAPExtension "$@" \
  --schema /path/to/appschemaextension.schema
```

## 4.3. Packaging LDAP ACL Extensions

Feedback 

For some purposes, e.g. for app installation, it is convenient to be able to register a new LDAP ACL extension from any system in the UCS domain. For this purpose, the UCR template for an ACL extension can be stored as a special type of UDM object. The module responsible for this type of objects is called `settings/ldap-acl`. As these objects are replicated throughout the UCS domain, the master domain controller, backup domain controller and slave domain controller systems listen for modifications on these objects and integrate

them into the local LDAP ACL UCR template directory. This simplifies the task of keeping the LDAP ACLs on the backup domain controller systems up to date with those on the master domain controller.

The commands to create the LDAP ACL extension objects in UDM may be put into any join script (see Chapter 3). A LDAP ACL extension object is created by using the UDM command line interface `univention-directory-manager` or its alias `udm`. LDAP ACL extension objects can be stored anywhere in the LDAP directory, but the recommended location would be `cn=ldapacl,cn=univention`, below the LDAP base. Since the join script creating the attribute may be called on multiple hosts, it is a good idea to add the `--ignore_exists` option, which suppresses the error exit code in case the object already exists in LDAP.

The UDM module `settings/ldapacl` requires several parameters:

`name` (required)

Name of the ACL extension.

`data` (required)

The actual ACL UCR template data in bzip2 and base64 encoded format.

`filename` (required)

The file name the ACL UCR template data should be written to on master domain controller, backup domain controller and slave domain controller. The file name must not contain any path elements.

`package` (required)

Name of the Debian package which creates the object.

`packageversion` (required)

Version of the Debian package which creates the object. For object modifications the version number needs to increase unless the package name is modified as well.

`appidentifier` (optional)

The identifier of the app which creates the object. This is important to indicate that the object is required as long as the app is installed anywhere in the UCS domain. Defaults to `string`.

`ucsversionstart` (optional)

Minimal required UCS version. The UCR template for the ACL is only activated by systems with a version higher than or equal to this.

`ucsversionend` (optional)

Maximal required UCS version. The UCR template for the ACL is only activated by systems with a version lower or equal than this. To specify validity for the whole 4.1-x release range a value like 4.1-99 may be used.

`active` (internal)

A boolean flag used internally by the master domain controller to signal availability of the ACL extension on the master domain controller (default: `FALSE`).


Since many of these parameters are determined automatically by the `ucs_registerLDAPExtension` shell library function, it is recommended to use the shell library function to create these objects (see Section 3.4.3.2).

### Example 4.2. LDAP ACL registration in join script

```
export UNIVENTION_APP_IDENTIFIER="appID-appVersion" ## example
. /usr/share/univention-lib/ldap.sh

ucs_registerLDAPExtension "$@" \
    --acl /path/to/appaclextension.acl
```

## 4.4. LDAP secrets

Feedback 

The credentials for different UCS domain accounts are stored in plain-text files on some UCS systems. The files are named `/etc/*.secret`. They are owned by the user `root` and allow read-access for different groups.

`/etc/ldap.secret` for `cn=admin,$ldap_base`


This account has full write access to all LDAP entries. The file is only available on master and backup domain controller systems and is owned by the group `DC Backup Hosts`.

`/etc/machine.secret` for `$ldap_hostdn`

Each host uses its account to get at least read-access to LDAP. Domain controllers in the container `cn=d-c,cn=computers,$ldap_base` get additional rights to access LDAP attributes. The file is available on all joined system roles and is readable only by the local `root` user and group.

During package installation, only the maintainer scripts (see Section B.3.5) on master and backup domain controller can use their `root` permission to directly read `/etc/ldap.secret`. Thus only on those roles the join scripts get automatically executed when the package is installed. On all other system roles, the join scripts need to be executed manually. This can either be done through the *UMC Join module* or through the command line tool `univention-run-join-scripts`. Both methods require appropriate credentials.

### 4.4.1. Password change

Feedback 

To reconfirm the trust relation between UCS systems, computers need to regularly change the password associated with the machine account. This is controlled through the Univention Configuration Registry variable `server/password/change`. For UCS servers this is evaluated by the script `/usr/lib/univention-server/server_password_change`, which is invoked nightly at 01:00 by `cron(8)`. The interval is controlled through a second Univention Configuration Registry variable `server/password/interval`, which defaults to 21 days.

The password is stored in the plain text file `/etc/machine.secret`. Many long running services read these credentials only on startup, which breaks when the password is changed while they are still running. Therefore UCS provides a mechanism to invoke arbitrary commands, when the machine password is changed. This can be used for example to restart specific services.

Hook scripts should be placed in the directory `/usr/lib/univention-server/server_password_change.d/`. The name must consist of only digits, upper and lower ASCII characters, hyphens and underscores. The file must be executable and is called via `run-parts(8)`. It receives one argument, which is used to distinguish three phases:

#### Procedure 4.1. Server password change procedure

1. Each script will be called with the argument `prechange` before the password is changed. If any script terminates with an exit status unequal zero, the change is aborted.

2. A new password is generated locally using `makepasswd(1)`. It is changed in the Univention directory service via UDM and stored in `/etc/machine.secret`. The old password is logged in `/etc/machine.secret.old`.

If anything goes wrong in this step, the change is aborted and the changes need to be rolled back.

3. All hook scripts are called again.
  - If the password change was successful, `postchange` gets passed to the hook scripts. This should complete any change prepared in the `prechange` phase.
  - If the password change failed for any reason, all hook scripts are called with the argument `nochange`. This should undo any action already done in the `prechange` phase.

### Example 4.3. Server password change example

Install this file to `/usr/lib/univention-server/server_password_change.d/`.

```
#!/bin/sh
case "$1" in
prechange)
    # nothing to do before the password is changed
    exit 0
    ;;
nochange)
    # nothing to do after a failed password change
    exit 0
    ;;
postchange)
    # restart daemon after password was changed
    invoke-rc.d my-daemon restart
    ;;
esac
```

`init-scripts` should only be invoked indirectly through `invoke-rc.d(8)`. This is required for `chroot` environments and allows the policy layer to control starting and stopping in certain special situations like during an system upgrade.



# Chapter 5. Univention Directory Listener

5.1. Structure of Listener Modules .....	55
5.2. Listener Tasks and Examples .....	59
5.2.1. Basic Example .....	59
5.2.2. Rename and Move .....	59
5.2.3. Full Example with Packaging .....	60
5.2.4. A Little Bit more Object Oriented .....	64
5.3. Technical Details .....	67
5.3.1. User-ID and Credentials .....	67
5.3.2. Internal Cache .....	67
5.3.2.1. univention-directory-listener-ctrl .....	68
5.3.2.2. univention-directory-listener-dump .....	68
5.3.2.3. univention-directory-listener-verify .....	68
5.3.2.4. get_notifier_id.py .....	69
5.3.3. Internal working .....	69
5.3.4. Python 3 Migration .....	71

Replication of the directory data within a UCS domain is provided by the Univention Directory Listener/Notifier mechanism:


- The Univention Directory Listener service runs on all UCS systems.
- On the master domain controller (and possibly existing backup domain controller systems) the *Univention Directory Notifier* service monitors changes in the LDAP directory and makes the selected changes available to the Univention Directory Listener services on all UCS systems joined into the domain.

The active Univention Directory Listener instances in the domain connect to a Univention Directory Notifier service. If an LDAP change is performed on the master domain controller (all other LDAP servers in the domain are read-only), this is registered by the Univention Directory Notifier and reported to the listener instances.

Each Univention Directory Listener instance hosts a range of Univention Directory Listener modules. These modules are shipped by the installed applications; the print server package includes, for example, listener modules which generate the CUPS configuration.

Univention Directory Listener modules can be used to communicate domain changes to services which are not LDAP-aware. The print server CUPS is an example of this: The printer definitions are not read from the LDAP, but instead from the file `/etc/cups/printers.conf`. Now, if a printer is saved in the printer management of the Univention Management Console, it is stored in the LDAP directory. This change is detected by the Univention Directory Listener module *cups-printers* and an entry gets added to, modified in or deleted from `/etc/cups/printers.conf` based on the modification in the LDAP directory.

## 5.1. Structure of Listener Modules

Feedback 

By default the Listener loads all modules from the directory `/usr/lib/univention-directory-listener/system/`. Other directories can be specified using the option `-m` when starting the `univention-directory-listener` daemon.

Each listener module must declare several string constants. They are required by the Univention Directory Listener to handle each module. They should be defined at the beginning of the module.

```
name = "module_name"
```

```
description = "Module description"
filter = "(objectClass=*)"
attribute = ["objectClass"]
modrdn = "1"
```

`name (str, required)`

This name is used to uniquely identify the module. This should match with the filename containing this listener module without the `.py` suffix. The name is used to keep track of the module state in `/var/lib/univention-directory-listener/handlers/`.

`description (str, required)`

A short description. It is currently unused and displayed nowhere.

`filter (str, required)`

Defines a LDAP filter which is used to match the objects the listener is interested in. This filter is similar to the LDAP search filter as defined in RFC 2254, but more restricted:

- it is case sensitive
- it only supports equal matches

### Note

The name `filter` has the drawback that it shadows the Python built-in function `filter()`, but its use has historical reasons. If that function is required for implementing the listener module, an alias-reference may be defined before overwriting the name or it may be explicitly accessed via the Python `__builtin__` module.

`attributes (List[str], optional)`

A Python list of LDAP attribute names which further narrows down the condition under which the listener module gets called. By default the module is called on all attribute changes of objects matching the filter. If the list is specified, the module is only invoked when at least one of the listed attributes is changed.

`modrdn (str, optional)`

Setting this variable to the string `1` changes the signature of the function `handler()`. It receives an additional 4th argument, which specifies the LDAP operation triggering the change.

`handle_every_delete (bool, optional)`

The Listener uses its cache to keep track of objects, especially their previous values and which modules handles which objects. The Univention Configuration Registry variable `listener/cache/filter` can be used to prevent certain objects from being stored in the cache. But then the Listener no longer knows which module must be called when such an object is deleted. Setting this variable to `True` will make the Listener call the function `handler()` of this module whenever any object is deleted. The function then must use other means to determine itself if the deleted object is of the appropriate type as `old` will be `None`.

`priority (float, optional)`

This variable can be used to explicitly overwrite the default order in which the modules are executed. By default modules are executed in random order. `replication.py` defaults to `0.0` as it must be executed first, all other modules default to `50.0`.

---

<http://tools.ietf.org/html/rfc2254>



In addition to the static strings a module must implement several functions. They are called in different situations of the live-cycle of the module.

```
def initialize(): pass
def handler(dn, new, old[, command='']): pass
def clean(): pass
def prerun(): pass
def postrun(): pass
def setdata(key, value): pass
```

`handler(dn, new, old, command='')` (required)

This function is called for each change matching the `filter` and `attributes` as declared in the header of the module. The distinguished name (`dn`) of the object is supplied as the first argument `dn`.

Depending on the type of modification, `old` and `new` may each independently either be `None` or reference a Python dictionary of lists. Each list represents one of the multi-valued attributes of the object. The Univention Directory Listener uses a local cache to store the values of each object as it has seen most recently. This cache is used to supply the values for `old`, while the values in `new` are those retrieved from that LDAP directory service which is running on the same server as the Univention Directory Notifier (master domain controller or backup domain controller servers in the domain).

If and only if the global `modrdn` setting is enabled, `command` is passed as a fourth argument. It contains a single letter, which indicates the type of modification. This can be used to distinguish an *modrdn* operation from a delete operation followed by a create operation.

`m` (modify)

Signals a modify operation, where an existing object is changed. `old` contains a copy of the previously cached values and `new` contains the new values as retrieved from the LDAP directory service.

`a` (add)

Signals the addition of a new object. `old` is `None` and `new` contains the values of the added object.

`d` (delete)

Signals the removal of a previously existing object. `old` contains a copy of the previously cached values, while `new` is `None`.

`r` (rename: modification of distinguished name via `modrdn`)

Signals a change in the distinguished name, which may be caused by renaming an object or moving the object from one container into another. The module is called with this command instead of the *delete* command, so that modules can recognize this special case and avoid deletion of local data associated with the object. The module will be called again with the *add* command just after the *modrdn* command, where it should process the rename or move operation. Each module is responsible for keeping track of the rename-case by internally storing the previous distinguished name during the *modrdn* phase of this two phased operation.

`n` (new or schema change)

This command can signal two changes:

- If `dn` is `cn=Subschema`, it signals that a schema change occurred.
- All other cases signal the initialization of a new object, which should be handled just like a normal *add* operation.

`initialize()` (optional),  
`clean()` (optional)

The function `initialize()` is called once when the Univention Directory Listener loads the module for the first time. This is recorded persistently in the file `/var/lib/univention-directory-listener/name`, where `name` equals the value from the header.

If for whatever reason the listener module should be reset and re-run for all matching objects, the state can be reset by running the command `univention-directory-listener-ctrl resync name`. In that case the function `initialize()` will be called again.

The function `clean()` is only called when the Univention Directory Listener is initialized for the first time or is forced to “re-initialize from scratch” using the `-g` or `-i` option. The function should purge all previously generated files and return the module into a clean state.

`prerun()` (optional),  
`postrun()` (optional)

For optimization the Univention Directory Listener does not keep open an LDAP connection all time. Instead the connection is opened once at the beginning of a change and closed only if no new change arrives within 15 seconds. The opening is signaled by the invocation of the function `prerun()` and the closing by `postrun()`.

The function `postrun()` is most often used to restart services, as restarting a service takes some time and makes the service unavailable during that time. It's best practice to use the `handler()` only to process the stream of changes, set UCR variables or generate new configuration files. Restarting associated services should be delayed to the `postrun()` function.

## Warning

The function `postrun()` is only called, when no change happens for 15 seconds. This is not on a per-module basis, but globally. In an ever changing system, where the stream of changes never pauses for 15 seconds, the functions may never be called!

`setdata(key, value)` (optional)

This function is called up to four times by the Univention Directory Listener main process to pass configuration data into the modules. The following keys are supplied in the following order:

`basedn`

The base distinguished name the Univention Directory Listener is using.

`binddn`

The distinguished name the Univention Directory Listener is using to authenticate to the LDAP server (via `simple bind`).

`bindpw`

The password the Univention Directory Listener is using to authenticate to the LDAP server.


`ldapserver`

The hostname of the LDAP server the Univention Directory Listener is currently reading from.

## Note

It's strongly recommended to avoid initiating LDAP modifications from a listener module. This potentially creates a complex modification dynamic, considering that a module may run on several systems in parallel at their own timing.

## 5.2. Listener Tasks and Examples

Feedback 

All changes trigger a call to the function `handle()`. For simplicity and readability it is advisable to delegate the different change types to different sub-functions.

### 5.2.1. Basic Example

Feedback 

The following boilerplate code delegates each change type to a separate function. It does not handle renames and moves explicitly, but only as the removal of the object at the old dn and the following addition at the new dn.

Source code: `doc/developer-reference/listener/simple.py`

```
def handler(dn, new, old):
    if new and not old:
        handler_add(dn, new)
    elif new and old:
        handler_modify(dn, old, new)
    elif not new and old:
        handler_remove(dn, old)
    else:
        pass # ignore

def handler_add(dn, new):
    """Handle addition of object."""
    pass # replace this

def handler_modify(dn, old, new):
    """Handle modification of object."""
    pass # replace this

def handler_remove(dn, old):
    """Handle removal of object."""
    pass # replace this
```

### 5.2.2. Rename and Move

Feedback 

In case rename and move actions should be handled separately, the following code may be used:

Source code: `doc/developer-reference/listener/modrdn.py`

```
modrdn = "1"

_delay = None
```

<https://github.com/univention/univention-corporate-server/blob/4.4-0/doc/developer-reference/listener/simple.py>  
<https://github.com/univention/univention-corporate-server/blob/4.4-0/doc/developer-reference/listener/modrdn.py>

```
def handler(dn, new, old, command):
    global _delay
    if _delay:
        old_dn, old = _delay
        _delay = None
        if "a" == command and old['entryUUID'] == new['entryUUID']:
            handler_move(old_dn, old, dn, new)
            return
        handler_remove(old_dn, old)

    if "n" == command and "cn=Subschema" == dn:
        handler_schema(old, new)
    elif new and not old:
        handler_add(dn, new)
    elif new and old:
        handler_modify(dn, old, new)
    elif not new and old:
        if "r" == command:
            _delay = (dn, old)
        else:
            handler_remove(dn, old)
    else:
        pass # ignore, reserved for future use


def handler_move(old_dn, old, new_dn, dn):
    """Handle rename or move of object."""
    pass # replace this

def handler_schema(old, new):
    """Handle change in LDAP schema."""
    pass # replace this
```

## Warning

Please be aware that tracking the two subsequent calls for `modrdn` in memory might cause duplicates, in case the Univention Directory Listener is terminated while such an operation is performed. If this is critical, the state should be stored persistently into a temporary file.

## 5.2.3. Full Example with Packaging

 Feedback 

The following example shows a listener module, which logs all changes to users into the file `/root/UserList.txt`.

Source code: `doc/developer-reference/listener/printusers/`

```
"""
Example for a listener module, which logs changes to users.
"""
__package__ = "" # workaround for PEP 366
import listener
```

<https://github.com/univention/univention-corporate-server/tree/4.4-0/doc/developer-reference/listener/printusers/>

```
import os
import errno
import univention.debug as ud
from collections import namedtuple

name = 'printusers'
description = 'print all names/users/uidNumbers into a file'
filter = """\
(&
  (|
    (&
      (objectClass=posixAccount)
      (objectClass=shadowAccount)
    )
    (objectClass=univentionMail)
    (objectClass=sambaSamAccount)
    (objectClass=simpleSecurityObject)
    (objectClass=inetOrgPerson)
  )
  (!(objectClass=univentionHost))
  (!(uidNumber=0))
  (!(uid=*))
)""".translate(None, '\t\n\r')
attributes = ['uid', 'uidNumber', 'cn']
_Rec = namedtuple('Rec', ' '.join(attributes))

USER_LIST = '/root/UserList.txt'

def handler(dn, new, old):
    """
    Write all changes into a text file.
    This function is called on each change.
    """
    if new and old:
        _handle_change(dn, new, old)
    elif new and not old:
        _handle_add(dn, new)
    elif old and not new:
        _handle_remove(dn, old)

def _handle_change(dn, new, old):
    """
    Called when an object is modified.
    """
    o_rec = _rec(old)
    n_rec = _rec(new)
    ud.debug(ud.LISTENER, ud.INFO, 'Edited user "%s"' % (o_rec.uid,))
    _writeit(o_rec, u'edited. Is now:')
    _writeit(n_rec, None)

def _handle_add(dn, new):
```

```

"""
Called when an object is newly created.
"""
n_rec = _rec(new)
ud.debug(ud.LISTENER, ud.INFO, 'Added user "%s"' % (n_rec.uid,))
_writeit(n_rec, u'added')

def _handle_remove(dn, old):
    """
    Called when an previously existing object is removed.
    """
    o_rec = _rec(old)
    ud.debug(ud.LISTENER, ud.INFO, 'Removed user "%s"' % (o_rec.uid,))
    _writeit(o_rec, u'removed')

def _rec(data):
    """
    Retrieve symbolic, numeric ID and name from user data.
    """
    return _Rec(*(data.get(attr, (None,))[0] for attr in attributes))

class AsRoot(object):
    """
    Temporarily change effective UID to 'root'.
    """

    def __enter__(self):
        listener.setuid(0)

    def __exit__(self, exc_type, exc_value, traceback):
        listener.unsetuid()

def _writeit(rec, comment):
    """
    Append CommonName, symbolic and numeric User-Identifier, and comment to
    file.
    """
    nuid = u'*****' if rec.uid in ('root', 'spam') else rec.uidNumber
    indent = '\t' if comment is None else ' '
    try:
        with AsRoot():
            with open(USER_LIST, 'a') as out:
                print >> out, u'%sName: "%s"' % (indent, rec.cn)
                print >> out, u'%sUser: "%s"' % (indent, rec.uid)
                print >> out, u'%sUID: "%s"' % (indent, nuid)
                if comment:
                    print >> out, u'%s%s' % (indent, comment,)
    except IOError as ex:
        ud.debug(

```

```

    ud.LISTENER, ud.ERROR,
    'Failed to write "%s": %s' % (USER_LIST, ex))

def initialize():
    """
    Remove the log file.
    This function is called when the module is forcefully reset.
    """
    try:
        with AsRoot():
            os.remove(USER_LIST)
            ud.debug(
                ud.LISTENER, ud.INFO,
                'Successfully deleted "%s"' % (USER_LIST,))
    except OSError as ex:
        if errno.ENOENT == ex.errno:
            ud.debug(
                ud.LISTENER, ud.INFO,
                'File "%s" does not exist, will be created' % (USER_LIST,))
        else:
            ud.debug(
                ud.LISTENER, ud.WARN,
                'Failed to delete file "%s": %s' % (USER_LIST, ex))

```

Some comments on the code:

- Overwriting `__package__` is currently necessary, as the Univention Directory Listener imports the listener module by its own mechanism, which is incompatible with the mechanism normally used by Python itself. Be aware, that this might cause problems when using *pickle*.
- The LDAP filter is specifically chosen to only match user objects, but not computer objects, which have a uid characteristically terminated by a \$-sign.
- The `attribute` filter further restricts the module to only trigger on changes to the numeric and symbolic user identifier and the last name of the user.
- To test this run a command like `tail -f /root/UserList.txt &`. Then create a new user or modify the *lastname* of an existing one to trigger the module.

For packaging the following files are required:

`debian/printusers.install`

The module should be installed into the directory `/usr/lib/univention-directory-listener/system/`.

```
printusers.py usr/lib/univention-directory-listener/system/
```

`debian/printusers.postinst`

The Univention Directory Listener must be restarted after package installation and removal:

```

#!/bin/sh
set -e

case "$1" in
configure)

```

```

invoke-rc.d univention-directory-listener restart
;;
abort-upgrade|abort-remove|abort-deconfigure)
;;
*)
    echo "postinst called with unknown argument \"\$1\"" >&2
    exit 1
;;
esac

#DEBHELPER#

exit 0

```

debian/printusers.postrm

```

#!/bin/sh
set -e


case "$1" in
remove)
    invoke-rc.d univention-directory-listener restart
    ;;
purge|upgrade|failed-upgrade|abort-install|abort-upgrade|disappear)
    ;;
*)
    echo "postrm called with unknown argument \"\$1\"" >&2
    exit 1
;;
esac

#DEBHELPER#

exit 0

```

## 5.2.4. A Little Bit more Object Oriented

Feedback 

For larger modules it might be preferable to use a more object oriented design like the following example, which logs referential integrity violations into a file.

Source code: [doc/developer-reference/listener/obj.py](https://github.com/univention/univention-corporate-server/blob/4.4-0/doc/developer-reference/listener/obj.py)

```

__package__ = "" # workaround for PEP 366
name = "refcheck"
description = "Check referential integrity of uniqueMember relations"
filter = "(uniqueMember=*)"
attribute = ["uniqueMember"]
modrdn = "1"

import os
import ldap
import listener
import univention.debug as ud
from pwd import getpwnam

```

<https://github.com/univention/univention-corporate-server/blob/4.4-0/doc/developer-reference/listener/obj.py>



```
class LocalLdap(object):
    PORT = 7389

    def __init__(self):
        self.data = {}
        self.con = None

    def setdata(self, key, value):
        self.data[key] = value

    def prerun(self):
        try:
            self.con = ldap.open(self.data["ldapservers"], port=self.PORT)
            self.con.simple_bind_s(self.data["binddn"], self.data["bindpw"])
        except ldap.LDAPError as ex:
            ud.debug(ud.LISTENER, ud.ERROR, str(ex))

    def postrun(self):
        try:
            self.con.unbind()
            self.con = None
        except ldap.LDAPError as ex:
            ud.debug(ud.LISTENER, ud.ERROR, str(ex))

class LocalFile(object):
    USER = "listener"
    LOG = "/var/log/univention/refcheck.log"

    def initialize(self):
        try:
            ent = getpwnam(self.USER)
            with AsRoot():
                open(self.LOG, "wb")
                os.chown(self.LOG, ent.pw_uid, -1)
        except OSError as ex:
            ud.debug(ud.LISTENER, ud.ERROR, str(ex))

    def log(self, msg):
        with open(self.LOG, 'ab') as log:
            print >> log, msg

    def clean(self):
        try:
            with AsRoot():
                os.remove(self.LOG)
        except OSError as ex:
            ud.debug(ud.LISTENER, ud.ERROR, str(ex))

class AsRoot(object):
```

```
"""
Temporarily change effective UID to 'root'.
"""

def __enter__(self):
    listener.setuid(0)

def __exit__(self, exc_type, exc_value, traceback):
    listener.unsetuid()

class ReferentialIntegrityCheck(LocalLdap, LocalFile):
    MESSAGES = {
        (False, False): "Still invalid: ",
        (False, True): "Now valid: ",
        (True, False): "Now invalid: ",
        (True, True): "Still valid: ",
    }

    def __init__(self):
        super(ReferentialIntegrityCheck, self).__init__()
        self._delay = None

    def handler(self, dn, new, old, command=''):
        if self._delay:
            old_dn, old = self._delay
            self._delay = None
            if "a" == command and old['entryUUID'] == new['entryUUID']:
                self.handler_move(old_dn, old, dn, new)
                return
            self.handler_remove(old_dn, old)

        if "n" == command and "cn=Subschema" == dn:
            self.handler_schema()
        elif new and not old:
            self.handler_add(dn, new)
        elif new and old:
            self.handler_modify(dn, old, new)
        elif not new and old:
            if "r" == command:
                self._delay = (dn, old)
            else:
                self.handler_remove(dn, old)
        else:
            pass # ignore, reserved for future use

    def handler_add(self, dn, new):
        if not self._validate(new):
            self.log("New invalid object: " + dn)

    def handler_modify(self, dn, old, new):
        valid = (self._validate(old), self._validate(new))
        msg = self.MESSAGES[valid]
        self.log(msg + dn)
```

```
def handler_remove(self, dn, old):
    if not self._validate(old):
        self.log("Removed invalid: " + dn)


def handler_move(self, old_dn, old, new_dn, new):
    valid = (self._validate(old), self._validate(new))
    msg = self.MESSAGES[valid]
    self.log("%s %s -> %s" % (msg, old_dn, new_dn))

def handler_schema(self):
    self.log("Schema change")


def _validate(self, data):
    try:
        for dn in data["uniqueMember"]:
            self.con.search_ext_s(dn, ldap.SCOPE_BASE, attrlist=[], attrsonly=1)
        return True
    except ldap.NO_SUCH_OBJECT:
        return False
    except ldap.LDAPError as ex:
        ud.debug(ud.LISTENER, ud.ERROR, str(ex))
        return False

__instance = ReferentialIntegrityCheck()
initialize = __instance.initialize
handler = __instance.handler
clean = __instance.clean
prerun = __instance.prerun
postrun = __instance.postrun
setdata = __instance.setdata
```

## 5.3. Technical Details


Feedback 

### 5.3.1. User-ID and Credentials

Feedback 

The listener runs with the effective permissions of the user `listener`. If root-privileges are required, `listener.setuid()` can be used to switch the effective UID. When done, `listener.unsetuid()` should be called to drop back to the `listener` UID. It's best practice to code this as `try/finally` clauses in Python.

### 5.3.2. Internal Cache

Feedback 

The directory `/var/lib/univention-directory-listener/` contains several files:

`cache/cache.mdb`, `cache/lock.mdb`

Starting with UCS 4.2 the LMDB cache database contains a copy of all objects and their attributes. It is used to supply the old values supplied through the `old` parameter, when the function `handle()` is called.

The cache is also used to keep track, for which object which module was called. This is required when a new module is added, which is invoked for all already existing objects when the Univention Directory Listener is restarted.

On domain controllers the cache could be replaced by doing a query to the local LDAP server, before the new values are written into it. But member server do not have a local LDAP server, so there the cache is needed. Also note that the cache keeps track of the associated listener modules, which is not available from the LDAP.

`cache.lock`

Starting with UCS 4.2 this file is used to detect if a listener opened the cache database.

`cache.db, cache.db.lock`

Before UCS 4.2 the BDB cache file contained a copy of all objects and their attributes. With the update to UCS 4.2 it gets converted into an LMDB database.

`notifier_id`


This file contains the last *notifier ID* read from the Univention Directory Notifier.

`handlers/`

For each module the directory contains a text file consisting of a single number. The name of the file is derived from the values of the variable `name` as defined in each listener module. The number is to be interpreted as a bit-field of `HANDLER_INITIALIZED=0x1` and `HANDLER_READY=0x2`. If both bits are set, it indicates that the module was successfully initialized by running the function `initialize()`. Otherwise both bits are unset.


The package ***univention-directory-listener*** contains several commands useful for controlling and debugging problems with the Univention Directory Listener. This can be useful for debugging listener cache inconsistencies.

### 5.3.2.1. univention-directory-listener-ctrl

Feedback 

The command `univention-directory-listener-ctrl resync name` can be used to reset and re-initialize a module. It stops any currently running listener process, removes the state file for the specified module and starts the listener process again. This forces the functions `clean()` and `initialize()` to be called one after the other.

### 5.3.2.2. univention-directory-listener-dump

Feedback 

The command `univention-directory-listener-dump` can be used to dump the cache file `/var/lib/univention-directory-listener/cache.db`. The Univention Directory Listener must be stopped first by invoking `service univention-directory-listener stop`. It outputs the cache in format compatible to the LDAP Data Interchange Format (LDIF).

### 5.3.2.3. univention-directory-listener-verify


Feedback 

The command `univention-directory-listener-verify` can be used to compare the content of the cache file `/var/lib/univention-directory-listener/cache.db` to the content of an LDAP server. The Univention Directory Listener must be stopped first by invoking `service univention-directory-listener stop`. LDAP credentials must be supplied at the command line. For example, the following command would use the machine password:

```
univention-directory-listener-verify \
-b "${ucr get ldap/base}" \
-D "${ucr get ldap/hostdn}" \
```


```
-w "$(cat /etc/machine.secret)"
```

### 5.3.2.4. get\_notifier\_id.py

Feedback 

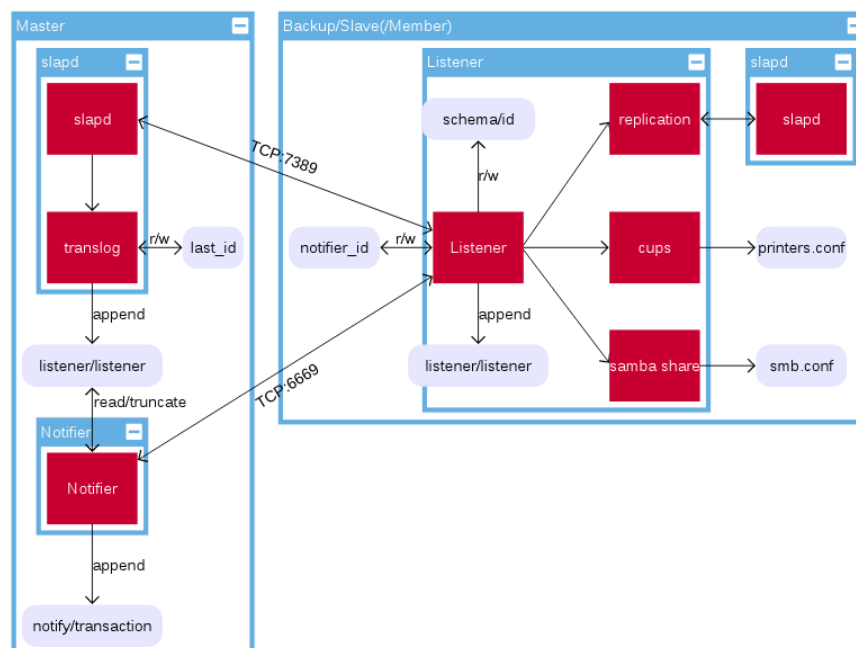
The command `/usr/share/univention-directory-listener/get_notifier_id.py` can be used to get the latest ID from the notifier. This is done by querying the Univention Directory Notifier running on the LDAP server configured through the Univention Configuration Registry variable `ldap/master`. The returned value should be equal to the value currently stored in the file `/var/lib/univention-directory-listener/notifier_id`. Otherwise the Univention Directory Listener might still be processing a transaction or it might indicate a problem with the Univention Directory Listener

### 5.3.3. Internal working

Feedback 

The Listener/Notifier mechanism is used to trigger arbitrary actions when changes occur in the LDAP directory service. In addition to the LDAP server `slapd` it consists of two other services: The Univention Directory Notifier service runs next to the LDAP server and broadcasts change information to interested parties. The Univention Directory Listener service listens for those notifications, downloads the changes and runs listener modules performing arbitrary local actions like storing the data in a local LDAP server for replication or generating configuration files for non-LDAP-aware local services.

**Figure 5.1. Listener/Notifier mechanism**



On startup the listener connects to the notifier and opens a persistent TCP connection to port 6669. The host can be configured through several Univention Configuration Registry variables:

- If `notifier/server` is explicitly set, only that named host is used. In addition the Univention Configuration Registry variable `notifier/server/port` can be used to explicitly configure a different TCP port other than 6669.
- Otherwise on the master domain controller and on all backup domain controllers, only the host named in `ldap/master` is used.

- Otherwise on all other system roles a host is chosen randomly from the combined list of names in `ldap/master` and `ldap/backup`<sup>1</sup>.

The following steps occur on changes:

### Procedure 5.1. Listener/Notifier procedure

1. An LDAP object is modified on the master domain controller. Changes initiated on all other system roles are re-directed to the master.
2. The UCS-specific overlay-module `translog` assigns the next transaction number. It uses the file `/var/lib/univention-ldap/last_id` to keep track of the last transaction number. As a fall-back the transaction number of the last entry from the file `/var/lib/univention-ldap/notify/transaction` is used. The module appends the transaction ID, DN and change type to the file `/var/lib/univention-ldap/listener/listener`<sup>2</sup>.
3. The Univention Directory Notifier watches that file, picks up and removes each line it processed. The transaction is appended to the file `/var/lib/univention-ldap/notify/transaction`<sup>3</sup>, including the DN. For efficient access by transaction ID the index `transaction.index` is updated.
4. All listeners get notified of the new transaction. Before UCS 4.3-3 erratum update 427<sup>4</sup> the information already included the latest transaction ID, DN and the change type. With protocol version 3 only the transaction ID is included.
5. Each listener opens a connection to the LDAP server running on the UCS system which was used to query the Notifier. With protocol version 3 the listener first queries the LDAP server for the missing DN and change type information by retrieving the entry `reqSession=ID,cn=translog`. With that it retrieves the latest state of the object identified through the DN. If access is blocked, for example, by *selective replication*, the change is handled as a delete operation instead.
6. The old state of the object is fetched from the local listener cache located in `/var/lib/univention-directory-listener/cache/`.
7. For each module it is checked, if either the old or new state of the object matches the `filter` and `attributes` specified in the corresponding Python variables. If not, the module is skipped. `replication.py` is always called first to guarantee that the data is available from the local LDAP server for all subsequent modules.
8. If the function `prerun()` of module was not called yet, this is done to signal the start of changes.
9. The function `handler()` specified in the module is called, passing in the DN and the old and new state.
10. The main listener process updates its cache with the new values, including the names of the modules which successfully handled that object. This guarantees that the module is still called, even when the filter criteria would no longer match the object after modification.
11. On a backup domain controller the Univention Directory Listener writes the transaction data to the file `/var/lib/univention-ldap/listener/listener`<sup>5</sup> to allow the Univention Directory Notifier to be cascaded. This is configured internally with the option `-o` of `univention-directory-listener` and is done for load balancing and failover reasons.

<sup>1</sup>This list of backup domain controllers stored in the Univention Configuration Registry variable `ldap/backup` is automatically updated by the listener module `ldap_server.py`.

<sup>2</sup>Referred to as `FILE_NAME_LISTENER`, `TRANSACTION_FILE` in the source code


<sup>3</sup>Referred to as `FILE_NAME_TF` in the source code

<sup>4</sup><http://errata.software-univention.de/ucs/4.3/427.html>

<sup>5</sup>Referred to as `FILE_NAME_LISTENER`, `TRANSACTION_FILE` in the source code

12. The transaction ID is written into the local file `/var/lib/univention-directory-listener/notifier_id`.
13. After 15 seconds of inactivity the function `postrun()` is invoked for all prepared modules. This signals a break in the stream of changes and requests the module to release its resources and/or start pending operations.

### 5.3.4. Python 3 Migration

Feedback 

As of UCS 5.0 the Univention Directory Listener uses Python 3 to execute listener modules.

For a successful migration all functions must be migrated to work with Python 3. There is no change in the module variables (name, description, filter, ...) necessary.

The data structure of the arguments `new` and `old` given to the `handler()` function now explicitly differentiates between byte strings (bytes) and unicode strings (str). The dictionary keys are strings while the LDAP attribute values are list of byte strings:

```
{
  'associatedDomain': [b'example.net'],
  'krb5RealmName': [b'EXAMPLE.NET'],
  'dc': [b'example'],
  'nisDomain': [b'example.net'],
  'objectClass': [
    b'top',
    b'krb5Realm',
    b'univentionPolicyReference',
    b'nisDomainObject',
    b'domainRelatedObject',
    b'domain',
    b'univentionBase',
    b'univentionObject'
  ],
  'univentionObjectType': [b'container/dc'],
}
```

While in UCS 4 `handler()` typically looked like:

```
def handler(dn, new, old):
    if 'myObjectClass' in new.get('objectClass', []):
        value = new['myAttribute'][0]
        ...
```

In UCS 5 it would look like:

```
def handler(dn, new, old): # type: (str, Mapping[str, Sequence[bytes]],
    Mapping[str, Sequence[bytes]]) -> None
    if b'myObjectClass' in new.get('objectClass', []):
        value = new['myAttribute'][0].decode('UTF-8')
        ...
```





# Chapter 6. Univention Directory Manager (UDM)

6.1. Introduction .....	73
6.2. Packaging Extended Attributes .....	74
6.2.1. Selection lists .....	79
6.2.1.1. Static selections .....	79
6.2.1.2. Dynamic selections .....	79
6.2.2. Known issues .....	81
6.2.3. Extended Options .....	81
6.2.4. Extended Attribute Hooks .....	82
6.3. UDM Modules .....	84
6.4. UDM Syntax .....	84
6.4.1. UDM Syntax Override .....	85
6.4.2. UDM LDAP search .....	86
6.5. Packaging UDM Hooks .....	90
6.6. Packaging UDM Extension Modules .....	91
6.7. Packaging UDM Syntax Extension .....	92
6.8. UDM REST API .....	94
6.8.1. Authentication .....	94
6.8.2. API overview .....	94
6.8.3. API usage examples .....	95
6.8.3.1. Create a user via a POST request .....	95
6.8.3.2. Search for users via a GET request .....	97
6.8.3.3. Modify a user via a PUT request .....	99
6.8.3.4. Delete a user via a DELETE request .....	100
6.9. UCS 5.0: Python 3 Migration of modules and extensions .....	100
6.9.1. Compatibility with UCS 4.4 .....	100
6.9.2. Default option .....	101
6.9.3. Mapping functions .....	101
6.9.4. Mapping Encoding .....	102
6.9.5. object.open() / object._post_unmap() .....	103
6.9.6. object.has_key() .....	103
6.9.7. identify() .....	103
6.9.8. _ldap_modlist() .....	104
6.9.9. lookup() .....	104
6.9.10. Syntax classes .....	104
6.9.11. Hooks .....	104

The Univention Directory Manager (UDM) is a wrapper for LDAP objects. Traditionally LDAP stores objects as a collection of attributes, which are defines by so called schemata. Modifying entries is slightly complicated, as there are no high-level operations to add or remove values from multi-valued attributes, or to keep the password used by different authentication schemes such as Windows NTLM-hashes, UNIX MD5 hashes, or Kerberos tickets in sync.

## 6.1. Introduction

Feedback

The command line client `udm` provides different modes of operation.

```
udm [--binddn bind-dn --bindpwd bind-password] [module] [mode] [options]
```

Creating object:

```
udm module create --set property=value...
```

```
eval "$(ucr shell)"
udm container/ou create --position "$ldap_base" --set name="xxx"
```

Multiple `--sets` may be used to set the values of a multivalued property.

The equivalent LDAP command would look like this:

```
eval "$(ucr shell)"
ldapadd -D "cn=admin,$ldap_base" -y /etc/ldap.secret <<__LDIF__
dn: uid=xxx,$ldap_base
objectClass: organizationalRole
cn: xxx
__LDIF__
```

List object:

```
udm module list [ --dn dn | --filter property=value ]
```

```
udm container/ou list --filter name="xxx"
```

```
univention-ldapsearch cn=xxx
```

Modify object:

```
udm module modify [ --dn dn | --filter property=value ] [ --set property=value | --append property=value | --remove property=value ...]
```

```
udm container/ou modify --dn "cn=xxx,$ldap_base" --set name="xxx"
```

For multivalued attributes `--append` and `--remove` can be used to add additional values or remove existing values. `--set` overwrites any previous value, but can also be used multiple times to specify further values. `--set` and `--append` should not be mixed for any property in one invocation.

Delete object:

```
udm module remove [ --dn dn | --filter property=value ]
```

```
udm container/ou delete --dn "cn=xxx,$ldap_base"
```

If `--filter` is used, it must match exactly one object. Otherwise `udm` refuses to delete any object.

## 6.2. Packaging Extended Attributes

Feedback 

Each UDM module provides a set of mappings from LDAP attributes to properties. This set is not complete, because LDAP objects can be extended with additional *auxiliary objectClasses*. *Extended Attributes* can be used to extend modules to show additional properties. These properties can be mapped to any already defined LDAP attribute, but objects can also be extended by adding additional auxiliary object classes, which can provide new attributes.

For packing purpose any additional LDAP schema needs to be registered on the master domain controller, which is replicated from there to all other Domaincontrollers via the Listener/Notifier mechanism (see Chapter 5). This is best done through a separate schema package, which should be installed on the master domain controller and backup domain controller. Since Extended Attributes are declared in LDAP, the commands to create them can be put into any join script (see Chapter 3). To be convenient, the declaration should be

also included with the schema package, since installing it there does not require the Administrator to provide additional LDAP credentials.

An Extended Attribute is created by using the UDM command line interface `univention-directory-manager` or its alias `udm`. The module is called `settings/extended_attribute`. Extended Attributes can be stored anywhere in the LDAP, but the default location would be `cn=custom_attributes,cn=univention`, below the LDAP base. Since the join script creating the attribute may be called on multiple hosts, it is a good idea to add the `--ignore_exists` option, which suppresses the error exit code in case the object already exists in LDAP.

The module `settings/extended_attribute` requires many parameters. They are described in ????

`name` (required)

Name of the attribute.

`CLIName` (required)

An alternative name for the command line version of UDM.

`shortDescription` (required)

Default short description.

`translationShortDescription` (optional, multiple)

Translation of short description.

`longDescription` (required)

Default long description.

`translationLongDescription` (optional, multiple)

Translation of long description.

`objectClass` (required)

The name of an LDAP object class which is added to store this property.

`deleteObjectClass` (optional)

Remove the object class when the property is unset.

`ldapMapping` (required)

The name of the LDAP attribute the property matches to.

`syntax` (optional)

A syntax class, which also controls the visual representation in UDM. Defaults to `string`.

`default` (optional)

The default value is used when a new UDM object is created. It is also used when for an object if the option is enabled, which only then activates the property.

`valueRequired` (optional)

A value must be entered for the property.

`multivalue` (optional)

Controls if only a single value or multiple values can be entered. This must be in sync with the `SINGLE-VALUE` setting of the attribute in the LDAP schema.

`mayChange` (optional)

The property may be modified later.

`notEditable` (optional)

Disable all modification of the property, even when the object is first created. The property is only modified through hooks.

`hook` (optional)

The name of a Python class implementing hook functions. See Section 6.2.4 for more information.

`doNotSearch` (optional)

If this is enabled, the property is not show in the drop-down list of properties when searching for UDM objects.

`tabName` (optional)

The name of the tab in the UMC where the property should be displayed. The name of existing tabs can be copied from UMC session with the `English` locale. A new tab is automatically created for new names. If no name is given, ???

`translationTabName` (optional, multiple)

Translation of tab name.

`tabPosition` (optional)

This setting is only relevant, when a new tab is created by using a `tabName`, for which no tab exists. The integer value defines the position where the newly tab is inserted. By default the newly created tab is appended at the end, but before the *Extended settings* tab.

`overwriteTab` (optional)

If enabled, the tab declared by the UDM module with the name from the `tabName` settings is replaces by a new clean tab with only the properties defined by Extended Attributes.

`tabAdvanced` (optional)

If this setting is enabled, the tab is created inside the *Extended settings* tab instead of being a tab by its own.

`groupName` (optional)

The name of the group inside a tab where the property should be displayed. The name of existing groups can be copied from UMC session with the `English` locale. A new tab is automatically created for new names. If no name is given, the property is placed before the first tab.

`translationGroupName` (optional, multiple)

Translation of group name.

groupPosition (optional)

This setting is only relevant, when a new group is created by using a `groupName`, for which no group exists. The integer value defines the position where the newly group is inserted. By default the newly created group is appended at the end.

overwritePosition (optional)

The name of an existing property this property wants to overwrite.

disableUDMWeb (optional)

Disables showing this property in the UMC.

fullWidth (optional)

The widget for the property should span both columns.

module (required, multiple)

A list of module names where this Extended Attribute should be added to.

options (required, multiple)

A list of options, which enable this Extended Attribute.

version (required)

The version of the Extended Attribute format. The current version is 2.

## Tip

Create the Extended Attribute first through UMC-UDM. Modify it until you're satisfied. Only then dump it using `udm settings/extended_attribute list` and convert the output to an equivalent shell script creating it.

### Example 6.1. Extended Attribute for custom LDAP schema

This example provides a simple LDAP schema called `extended-attribute.schema`, which declares one object class `univentionExamplesUdmOC` and one attribute `univentionExamplesUdmAttribute`.

```
#objectIdentifier univention 1.3.6.1.4.1.10176
#objectIdentifier univentionCustomers univention:99999
#objectIdentifier univentionExamples univentionCustomers:0
objectIdentifier univentionExamples 1.3.6.1.4.1.10176:99999:0
objectIdentifier univentionExmaplesUdm univentionExamples:1
objectIdentifier univentionExmaplesUdmAttributeType
  univentionExmaplesUdm:1
objectIdentifier univentionExmaplesUdmObjectClass
  univentionExmaplesUdm:2

attributetype ( univentionExmaplesUdmAttributeType:1
  NAME 'univentionExamplesUdmAttribute'
  DESC 'An example attribute for UDM'
  EQUALITY caseIgnoreMatch
  SUBSTR caseIgnoreSubstringsMatch
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15{42}
```

```

SINGLE-VALUE
)

objectClass ( univentionExmaplesUdmObjectClass:1
  NAME 'univentionExamplesUdmOC'
  DESC 'An example object class for UDM'
  SUP top
  AUXILIARY
  MUST ( univentionExamplesUdmAttribute )
)

```

w The schema is shipped as `/usr/share/extended-attribute/extended-attribute.schema` and installed by calling `ucs_registerLDAPExtension` from the join-script `50extended-attribute.inst`.

```

#!/bin/sh

#DEBHELPER#

. /usr/share/univention-lib/base.sh

call_joinscript 50extended-attribute.inst

exit 0

```

This script calls the join-script `50extended-attribute.inst`, which also creates an Extended Attribute by using the `udm` command line interface:

```

#!/bin/bash

## joinscript api: bindpwdfile

VERSION=1
. /usr/share/univention-join/joinscripthelper.lib
. /usr/share/univention-lib/ldap.sh
joinscript_init

# register LDAP schema for new extended attribute
ucs_registerLDAPExtension "$@" \
  --schema /usr/share/extended-attribute/extended-attribute.schema

# Register new service entry for this host
eval "$(ucr shell)"
udm settings/extended_attribute create "$@" --ignore_exists \
  --position "cn=custom attributes,cn=univention,$ldap_base" \
  --set name="My Attribute" \
  --set CLIName="myAttribute" \
  --set shortDescription="Example attribute" \
  --set translationShortDescription="'de_DE' 'Beispielattribut'" \
  --set longDescription="An example attribute" \
  --set translationLongDescription="'de_DE' 'Ein Beispielattribut'" \
  --set tabAdvanced=1 \
  --set tabName="Examples" \
  --set translationTabName="'de_DE' 'Beispiele'" \
  --set tabPosition=1 \

```


```
--set module="groups/group" \
--set module="computers/memberserver" \
--set syntax=string \
--set default="Lorem ipsum" \
--set multivalue=0 \
--set valueRequired=0 \
--set mayChange=1 \
--set doNotSearch=1 \
--set objectClass=univentionExamplesUdmOC \
--set ldapMapping=univentionExamplesUdmAttribute \
--set deleteObjectClass=0
# --set overwritePosition=
# --set overwriteTab=
# --set hook=
# --set options=

# Terminate UDM server to force module reload
. /usr/share/univention-lib/base.sh
stop_udm_cli_server

joinscript_save_current_version
exit 0
```


This example is deliberately missing an unjoin-script (see Section 3.5) to keep this example simple. It should check if the Extended Attribute is no longer used in the domain and then remove it.

## 6.2.1. Selection lists

 Feedback 

Sometimes an Extended Attribute should show a list of options to choose from. This list can either be static or dynamic. After defining such a new syntax it can be used by referencing its name in the `syntax` property of an Extended Attribute.

### 6.2.1.1. Static selections

 Feedback 


The static list of available selections is defined once and can not be modified interactively through UMC. Such a list is best implemented though a custom syntax class. As the implementation must be available on all system roles, the new syntax is best registered in LDAP. This can be done by using `ucs_registerLDAPExtension` which is described in Section 3.4.3.2.

As an alternative the file can be put into the directory `/usr/lib/python2.7/dist-packages/univention/admin/syntax.d/`.

The following example is comparable to the default example in file `/usr/lib/python2.7/dist-packages/univention/admin/syntax.d/example.py`:

```
class StaticSelection(select):
    choices = [
        ('value1', 'Description for selection 1'),
        ('value2', 'Description for selection 2'),
        ('value3', 'Description for selection 3'),
    ]
```

### 6.2.1.2. Dynamic selections

 Feedback 

A dynamic list is implemented as an LDAP search, which is described in Section 6.4.2. For performance reason it is recommended to implement a class derived from `UDM_Attribute` or `UDM_Objects` instead of using

LDAP\_Search. The file `/usr/lib/python2.7/dist-packages/univention/admin/syntax.py` contains several examples.

### Example 6.2. Dynamic selection list for Extended Attributes

The idea is to create a container with sub-entries for each selection. This following listing declares a new syntax class for selecting a profession level.

```
class DynamicSelection(UDM_Objects):
    udm_modules = ('container/cn',)
    udm_filter = '(&(objectClass=organizationalRole)
(ou:dn:=DynamicSelection))'
    simple = True # only one value is selected
    empty_value = True # allow selecting nothing
    key = '%(name)s' # this is stored
    label = '%(description)s' # this is displayed
    regex = None # no validation in frontend
    error_message = 'Invalid value'
```

The Python code should be put into a file named `DynamicSelection.py`. The following code registers this new syntax in LDAP and adds some values. It also creates an Extended Attribute for user objects using this syntax.

```
syntax='DynamicSelection'
base="cn=univention,$(ucr get ldap/base)"

udm container/ou create --position "$base" \
    --set name="$syntax" --set description='UCS profession level'
dn="ou=$syntax,$base"

udm container/cn create --position "$dn" \
    --set name="value1" --set description='UCS Guru (> 5)'
udm container/cn create --position "$dn" \
    --set name="value2" --set description='UCS Regular (1..5)'
udm container/cn create --position "$dn" \
    --set name="value3" --set description='UCS Beginner (< 1)'

udm container/cn create --ignore_exists --position "$base" \
    --set name='udm_syntax'
dn="cn=udm_syntax,$base"
udm settings/udm_syntax create --position "$dn" \
    --set name="$syntax" --set filename="DynamicSelection.py" \
    --set data="$(bzip2 <DynamicSelection.py | base64)" \
    --set package="$syntax" --set packageversion="1"

udm settings/extended_attribute create --position "cn=custom attributes,
$base" \
    --set name='Profession' \
    --set module='users/user' \
    --set tabName='General' \
    --set translationTabName='"de_DE" "Allgemein"' \
    --set groupName='Personal information' \
    --set translationGroupName='"de_DE" "Persönliche Informationen"' \
    --set shortDescription='UCS profession level' \
    --set translationShortDescription='"de_DE" "UCS Erfahrung"' \
```



```
--set longDescription='Select a level of UCS experience' \
--set translationLongDescription='"de_DE" "Wählen Sie den Level der
Erfahrung mit UCS"' \
--set objectClass='univentionFreeAttributes' \
--set ldapMapping='univentionFreeAttribute1' \
--set syntax="$syntax" --set mayChange=1 --set valueRequired=0
```

## 6.2.2. Known issues

Feedback

- The `tabName` and `groupName` values must exactly match the values already used in the modules. If they do not match, a new tab or group is added. This also applies to the translation: They must match the already translated strings and must be repeated for every Extended Attribute again and again. The untranslated strings are best extracted directly from the Python source code of the modules in `/usr/lib/python2.7/dist-packages/univention/admin/handlers/**/*.py`. For the translated strings run `msgunfmt /usr/share/locale/language-code/LC_MESSAGES/univention-admin*.mo`.
- The `overwritePosition` values must exactly match the name of an already defined property. Otherwise UDM will crash.
- Extended Attributes may be removed, when matching data is still stored in LDAP. The schema on the other hand must only be removed when all matching data is removed. Otherwise the server `slapd` will fail to start.
- Removing `objectClasses` from LDAP objects must be done manually. Currently UDM does not provide any functionality to remove unneeded object classes or methods to force-remove an object class including all attributes, for which the object class is required.

## 6.2.3. Extended Options

Feedback

UDM properties can be enabled and disabled via *options*. For example all properties of a user related to Samba can be switched on or off to reduce the settings shown to an administrator. If many Extended Attributes are added to a UDM module, it might proof necessary to also create new options. Options are per UDM module.

Similar to Extended Attributes an Extended Option is created by using the UDM command line interface `univention-directory-manager` or its alias `udm`. The module is called `settings/extended_options`. Extended Options can be stored anywhere in the LDAP, but the default location would be `cn=custom_attributes,cn=univention`, below the LDAP base. Since the join script creating the option may be called on multiple hosts, it is a good idea to add the `--ignore_exists` option, which suppresses the error exit code in case the object already exists in LDAP.

The module `settings/extended_options` has the following properties:

`name` (required)

Name of the option.

`shortDescription` (required)

Default short description.

`translationShortDescription` (optional, multiple)

Translation of short description.

`longDescription` (required)

Default long description.

translationLongDescription (optional, multiple)

Translation of long description.

default (optional)

Enable the option by default.

editable (optional)

Option may be repeatedly turned on and off.

module (required, multiple)

A list of module names where this Extended Option should be added to.

objectClass (optional, multiple)

A list of LDAP object classes, which when found, enable this option.

### Example 6.3. Extended Option

```
eval "$(ucr shell)"
udm settings/extended_options create "$@" --ignore_exists \
--position "cn=custom attributes,cn=univention,$ldap_base" \
--set name="My Option" \
--set shortDescription="Example option" \
--set translationShortDescription="'de_DE' 'Beispieloption'" \
--set longDescription="An example option" \
--set translationLongDescription="'de_DE' 'Eine Beispieloption'" \
--set default=0 \
--set editable=0 \
--set module="users/user" \
--set objectClass=univentionExamplesUdmOC
```

## 6.2.4. Extended Attribute Hooks

Feedback 

Hooks provide a mechanism to pre- and post-process the values of Extended Attributes. Normally UDM properties are stored as-is in LDAP attributes. Hooks can modify the LDAP operations when an object is created, modified, deleted or retrieved. They are implemented in Python and the file must be placed in the directory `/usr/lib/python2.7/dist-packages/univention/admin/hooks.d/`. The file name must end with `.py`.

The module ***univention.admin.hook*** provides the class `simpleHook`, which implements all required hook functions. By default they don't modify any request but do log all calls. This class should be used as a base class for inheritance.

```
hook_open(self,
          obj);
```

This method is called by the default open handler just before the current state of all properties is saved.

```
hook_ldap_pre_create(self,
                    obj);
```

This method is called before a UDM object is created. It is called after the module validated all properties but before the *add-list* is created.

```
list hook_ldap_addlist(self,
                        obj,
                        al= []);
```

This method is called before a UDM object is created. It gets passed a list of two-tuples (`ldap-attribute-name`, `list-of-values`) which will be used to create the LDAP object. The method must return the (modified) list. Notice that `hook_ldap_modlist` will also be called next.

```
hook_ldap_post_create(self,
                      obj);
```

This method is called after the object was created in LDAP.

```
hook_ldap_pre_modify(self,
                     obj);
```

This method is called before a UDM object is modified. It is called after the module validated all properties but before the *modification-list* is created.

```
list hook_ldap_modlist(self,
                       obj,
                       ml= []);
```

This method is called before a UDM object is created or modified. It gets passed a list of tuples, which are either two-tuples (`ldap-attribute-name`, `list-of-new-values`) or three-tuples (`ldap-attribute-name`, `list-of-old-values`, `list-of-new-values`). It will be used to create or modify the LDAP object. The method must return the (modified) list.

```
hook_ldap_post_modify(self,
                      obj);
```

This method is called after the object was modified in LDAP.

```
hook_ldap_pre_remove(self,
                     obj);
```

This method is called before a UDM object is removed.

```
hook_ldap_post_remove(self,
                      obj);
```

This method is called after the object was removed from LDAP.

The following example implements a hook, which removes the object-class `univentionFreeAttributes` if the property `isSampleUser` is no longer set.

```
from univention.admin.hook import simpleHook

class RemoveObjClassUnused(simpleHook):
    type = 'RemoveObjClassUnused'


    def hook_ldap_post_modify(self, obj):
        """Remove unused objectClass."""
        ext_attr_name = 'isSampleUser'
        class_name = 'univentionFreeAttributes'
```

```
if obj.ldapinfo.get(ext_attr_name) in ('1',) and \
    obj.info.get(ext_attr_name) in ('0', None):
    if class_name in obj.ldapattr.get('objectClass', []):
        obj.ldap.modify(obj.dn,
            [('objectClass', class_name, '')])
```

After installing the file the hook can be activated by setting the hook property of an Extended Attribute to RemoveObjClassUnused:


```
udm settings/extended_attribute modify \
--dn ... \
--set hook=RemoveObjClassUnused
```

## 6.3. UDM Modules

Feedback 

The development of Univention Directory Manager modules is currently only documented in Univention Wiki (currently only available in German): [https://wiki.univention.de/index.php?title=Entwicklung\\_und\\_Integration\\_eigener\\_Module\\_in\\_Univention\\_Directory\\_Manager](https://wiki.univention.de/index.php?title=Entwicklung_und_Integration_eigener_Module_in_Univention_Directory_Manager)

## 6.4. UDM Syntax

Feedback 

Every UDM property has a syntax, which is used to check the value for correctness. Univention Corporate Server already provides several syntax types, which are defined in the Python file `/usr/lib/python2.7/dist-packages/univention/admin/syntax.py`. The following list of syntaxes is not complete, for a complete overview the file should be consulted directly.

```
string,
string64,
OneThirdString,
HalfString,
TwoThirdsString,
FourThirdsString,
OneAndAHalfString,
FiveThirdsString,
TextArea
```

Different string classes, which are mapped in Univention Management Console to text input widgets with different widths and heights.

```
string_numbers_letters_dots,
string_numbers_letters_dots_spaces,
IA5string,
...
```

Different string classes with restrictions on the allowed character set.

```
Upload,
Base64Upload,
jpegPhoto
```

Binary data.

```
integer
```

Positive integers.

```
boolean,  
booleanNone,  
TrueFalse,  
TrueFalseUpper,  
TrueFalseUp
```

Different boolean types which map to yes and no or true and false.

```
hostName,  
DNS_Name,  
windowsHostName,  
ipv4Address,  
ipAddress,  
hostOrIP,  
v4netmask,  
netmask,  
IPv4_AddressRange,  
IP_AddressRange,  
...
```

Different classes for host names or addresses.

```
unixTime,  
TimeString,  
iso8601Date,  
date
```

Date and time.

```
GroupDN,  
UserDN,  
UserID,  
HostDN,  
DomainController,  
Windows_Server,  
UCS_Server,  
...
```


Dynamic classes, which do an LDAP search to provide a list of selectable values like users, groups and hosts

```
LDAP_Search,  
UDM_Objects,  
UDM_Attribute
```

These syntaxes do an LDAP search and display the result as a list. They are further described in Section 6.4.2.

Additional syntax classes can be added by placing a Python file in `/usr/lib/python2.7/dist-packages/univention/admin/syntax.d/`. They're automatically imported by UDM.

### 6.4.1. UDM Syntax Override


Feedback 

Sometimes the predefined syntax is inappropriate in some scenarios. This can be because of performance problems with LDAP searches or the need for more restrictive or lenient value checking. The latter case might require a change to the LDAP schema, since `slapd` also checks the provided values for correctness.

The syntax of UDM properties can be overwritten by using Univention Configuration Registry variables. For each module and each property the variable `directory/manager/web/modules/module/properties/property/syntax` can be set to the name of a syntax class. For example `directory/manager/web/modules/users/user/properties/username/syntax=uid` would restrict the name of users to not contain umlauts.

Since UCR variables only affect the local system, the variables must be set on all systems where UDM is used. This can be either done through a Univention Configuration Registry policy (see ????) or by setting the variable in the `.postinst` script of some package, which is installed on all hosts.

## 6.4.2. UDM LDAP search

Feedback 

It is often required to present a list of entries to the user, from which she can select one or — in case of a multi-valued property — more entries. Several syntax classes derived from `select` provide a fixed list of choices. If the set of values is known and fixed, it's best to derive an own class from `select` and provide the Python file in `/usr/lib/python2.7/dist-packages/univention/admin/syntax.d/`.

If on the other hand the list is dynamic and is stored in LDAP, UDM provides three methods to retrieve the values.

`UDM_Attribute`

This class does a UDM search. For each object found all values of a multi-valued property are returned.

For a derived class the following class variables can be used to customize the search:

`udm_module`

The name of the UDM module, which does the LDAP search and retrieves the properties.

`udm_filter`

An LDAP search filter which is used by the UDM module to filter the search. The special value `dn` skips the search and directly returns the property of the UDM object specified by `depends`.

`attribute`

The name of a multi-valued UDM property which stores the values to be returned.

`is_complex`,  
`key_index`,  
`label_index`

Some UDM properties consist of multiple parts, so called *complex* properties. These variables are used to define, which part is displayed as the label and which part is used to reference the entry.

`label_format`

A Python format string, which is used to format the UDM properties to a label string presented to the user. `%(property-name)s` should be used to reference properties. The special property name `$attribute$` is replaced by the value of variable `attribute` declared above.

`regex`

This defines an optional regular expression, which is used in the frontend to check the value for validity.

**static\_values**

A list of two-tuples (`value`, `display-string`), which are added as additional selection options.

**empty\_value**

If set to `True`, the empty value is inserted before all other static and dynamic entries.

**depends**

This variable may contain the name of another property, which this property depends on. This can be used to link two properties. For example, one property can be used to select a server, while the second dependent property then only lists the services provided by that selected host. For the dependent syntax `attribute` must be set to `dn`.

**error\_message**

This error message is shown when the user enters a value which is not in the set of allowed values.

The following example syntax would provide a list of all users with their telephone numbers:

```
class DelegateTelephoneNumber(UDM_Attribute):
    udm_module = 'users/user'
    attribute = 'phone'
    label_format = '%(displayName)s: %($attribute$s)s'
```

**UDM\_Objects**

This class performs a UDM search returning each object found.

For a derived class the following class variables can be used to customize the search:

**udm\_modules**

A List of one or more UDM modules, which do the LDAP search and retrieve the properties.

**key**

A Python format string generating the key value used to identify the selected object. The default is `dn`, which uses the distinguished name of the object.

**label**

A Python format string generating the display label to represent the selected object. The default is `None`, which uses the UDM specific `description`. `dn` can be used to use the distinguished name.

**regex**

This defines an optional regular expression, which is used in the frontend to check the value for validity. By default only valid distinguished names are accepted.

**simple**

By default a widget for selecting multiple entries is used. Setting this variable to `True` changes the widget to a combo-box widget, which only allows to select a single value. This should be in-sync with the `multivalue` property of UDM properties.

use\_objects

By default UDM opens each LDAP object through a UDM module implemented in Python. This can be a performance problem if many entries are returned. Setting this to `False` disables the Python code and directly uses the attributes returned by the LDAP search. Several properties can then no longer be used as key or label, as those are not explicitly stored in LDAP but are only calculated by the UDM module. For example, to get the fully qualified domain name of a host `%(name)s`. `%(domain)s` must be used instead of the calculated property `%(fqdn)s`.

udm\_filter,  
static\_values,  
empty\_value,  
depends,  
error\_message

Same as above with `UDM_Attribute`.

The following example syntax would provide a list of all servers providing a required service:

```
class MyServers(UDM_Objects):
    udm_modules = (
        'computers/domaincontroller_master',
        'computers/domaincontroller_backup',
        'computers/domaincontroller_slave',
        'computers/memberserver',
    )
    label = '%(fqdn)s'
    udm_filter = 'service=MyService'
```

LDAP\_Search

This is the old implementation, which should only be used, if `UDM_Attribute` and `UDM_Objects` are not sufficient. In addition to ease of use it has the drawback that Univention Management Console can not do as much caching, which can lead to severe performance problems.

LDAP search syntaxes can be declared in two equivalent ways:

*Python API*

By implementing a Python class derived from `LDAP_Search` and providing that implementation in `/usr/lib/python2.7/dist-packages/univention/admin/syntax.d/`.

*UDM API*

By creating a UDM object in LDAP using the module `settings/syntax`.

The Python API uses the following variables:

syntax\_name

This variable stores the common name of the LDAP object, which is used to define the syntax. It is only used internally and should never be needed when creating syntaxes programmatically.

filter

An LDAP filter to find the LDAP objects providing the list of choices.



**attribute**

A list of UDM module property definitions like "shares/share: dn". They are used as the human readable label for each element of the choices.

**value**

The UDM module attribute that will be stored to identify the selected element. The value is specified like shares/share: dn

**viewonly**

If set to True the values can not be changed.

**addEmptyValue**

If set to True the empty value is add to the list of choices.

**appendEmptyValue**

Same as addEmptyValue but added at the end. Used to automatically choose an existing entry in the frontend.

```
class MyServers(LDAP_Search):
    def __init__(self):
        LDAP_Search.__init__(self,
            filter=( '(&(univentionService=MyService) '
                '(univentionServerRole=member))' ),
            attribute=(
                'computers/memberserver: fqdn',
            ),
            value='computers/memberserver: dn'
        )
        self.name = 'LDAP_Search' # required workaround
```

The UDM API uses the following properties:

**name (required)**

The name for the syntax.

**description (optional)**

Some descriptive text.

**filter (required)**

An LDAP filter, which is used to find the objects.

**base (optional)**

The LDAP base, where the search starts.

**attribute (optional, multivalued),****ldapattribute (optional, multivalued)**

The name of UDM properties, which are display as a label to the user. Alternatively LDAP attribute names may be used directly.

value (optional),  
ldapvalue (optional)

The name of the UDM property, which is used to reference the object. Alternatively an LDAP attribute name may be used directly.

viewonly (optional)


If set to 1 the values can not be changed.

addEmptyValue (optional)

If set to 1 the empty value is add to the list of choices.

```
eval "$(ucr shell)"
udm settings/syntax create "$@" --ignore_exists \
--position "cn=custom attributes,cn=univention,$ldap_base" \
--set name=MyServers \
--set filter='(&(univentionService=MyService)
(univentionServerRole=member))' \
--set attribute='computers/memberserver: fqdn' \
--set value='computers/memberserver: dn'
```

## 6.5. Packaging UDM Hooks

Feedback 

For some purposes, e.g. for app installation, it is convenient to be able to deploy a new UDM hook in the UCS domain from any system in the domain. For this purpose, a UDM hook can be stored as a special type of UDM object. The module responsible for this type of objects is called `settings/udm_hook`. As these objects are replicated throughout the UCS domain, the UCS servers listen for modifications on these objects and integrate them into the local UDM.

The commands to create the UDM hook objects in UDM may be put into any join script (see Chapter 3). Like every UDM object a UDM hook object can be created by using the UDM command line interface `univention-directory-manager` or its alias `udm`. UDM hook objects can be stored anywhere in the LDAP directory, but the recommended location would be `cn=udm_hook,cn=univention`, below the LDAP base. Since the join script creating the attribute may be called on multiple hosts, it is a good idea to add the `--ignore_exists` option, which suppresses the error exit code in case the object already exists in LDAP.

The module `settings/udm_hook` requires several parameters. Since many of these are determined automatically by the `ucs_registerLDAPExtension` shell library function, it is recommended to use the shell library function to create these objects (see Section 3.4.3.2).

name (required)

Name of the UDM hook.

data (required)

The actual UDM hook data in bzip2 and base64 encoded format.

filename (required)

The file name the UDM hook data should be written to by the listening servers. The file name must not contain any path elements.

`package` (required)

Name of the Debian package which creates the object.

`packageversion` (required)

Version of the Debian package which creates the object. For object modifications the version number needs to increase unless the package name is modified as well.

`appidentifier` (optional)

The identifier of the app which creates the object. This is important to indicate that the object is required as long as the app is installed anywhere in the UCS domain. Defaults to `string`.

`ucsversionstart` (optional)

Minimal required UCS version. The UDM hook is only activated by systems with a version higher than or equal to this.


`ucsversionend` (optional)

Maximal required UCS version. The UDM hook is only activated by systems with a version lower than or equal to this. To specify validity for the whole 4.1-x release range a value like 4.1-99 may be used.

`active` (internal)

A boolean flag used internally by the master domain controller to signal availability of the new UDM hook on the master domain controller (default: `FALSE`).

## 6.6. Packaging UDM Extension Modules

Feedback 

For some purposes, e.g. for app installation, it is convenient to be able to deploy a new UDM module in the UCS domain from any system in the domain. For this purpose, a UDM module can be stored as a special type of UDM object. The module responsible for this type of objects is called `settings/udm_module`. As these objects are replicated throughout the UCS domain, the UCS servers listen for modifications on these objects and integrate them into the local UDM.

The commands to create the UDM module objects in UDM may be put into any join script (see Chapter 3). Like every UDM object a UDM module object can be created by using the UDM command line interface `univention-directory-manager` or its alias `udm`. UDM module objects can be stored anywhere in the LDAP directory, but the recommended location would be `cn=udm_module,cn=univention`, below the LDAP base. Since the join script creating the attribute may be called on multiple hosts, it is a good idea to add the `--ignore_exists` option, which suppresses the error exit code in case the object already exists in LDAP.

The module `settings/udm_module` requires several parameters. Since many of these are determined automatically by the `ucs_registerLDAPExtension` shell library function, it is recommended to use the shell library function to create these objects (see Section 3.4.3.2).

`name` (required)

Name of the UDM module, e.g. `newapp/someobject`.

`data` (required)

The actual UDM module data in `bzip2` and `base64` encoded format.

`filename` (required)

The file name the UDM module data should be written to by the listening servers. The file name may contain path elements and should conform to the name of the UDM module (e.g. `newapp/someobject.py`).

`messagecatalog` (optional)

Multivalued property to supply message translation files (syntax: `<language tag> <base64 encoded GNU message catalog>`).

`umcregistration` (optional)

XML definition required to make the UDM module available though the Univention Management Console (base64 encoded XML)

`icon` (optional)

Multivalued property to supply icons for the Univention Management Console (base64 encoded png, jpeg or svgz).

`package` (required)

Name of the Debian package which creates the object.

`packageversion` (required)

Version of the Debian package which creates the object. For object modifications the version number needs to increase unless the package name is modified as well.

`appidentifier` (optional)

The identifier of the app which creates the object. This is important to indicate that the object is required as long as the app is installed anywhere in the UCS domain. Defaults to `string`.

`ucsversionstart` (optional)

Minimal required UCS version. The UDM module is only activated by systems with a version higher than or equal to this.


`ucsversionend` (optional)

Maximal required UCS version. The UDM module is only activated by systems with a version lower than or equal to this. To specify validity for the whole 4.1-x release range a value like 4.1-99 may be used.

`active` (internal)

A boolean flag used internally by the master domain controller to signal availability of the new UDM module on the master domain controller (default: `FALSE`).

## 6.7. Packaging UDM Syntax Extension

Feedback 

For some purposes, e.g. for app installation, it is convenient to be able to deploy a new UDM syntax in the UCS domain from any system in the domain. For this purpose, a UDM syntax can be stored as a special type of UDM object. The module responsible for this type of objects is called `settings/udm_syntax`. As

these objects are replicated throughout the UCS domain, the UCS servers listen for modifications on these objects and integrate them into the local UDM.

The commands to create the UDM syntax objects in UDM may be put into any join script (see Chapter 3). Like every UDM object a UDM syntax object can be created by using the UDM command line interface `univention-directory-manager` or its alias `udm`. UDM syntax objects can be stored anywhere in the LDAP directory, but the recommended location would be `cn=udm_syntax,cn=univention`, below the LDAP base. Since the join script creating the attribute may be called on multiple hosts, it is a good idea to add the `--ignore_exists` option, which suppresses the error exit code in case the object already exists in LDAP.

The module `settings/udm_syntax` requires several parameters. Since many of these are determined automatically by the `ucs_registerLDAPExtension` shell library function, it is recommended to use the shell library function to create these objects (see Section 3.4.3.2).

`name` (required)

Name of the UDM syntax.

`data` (required)

The actual UDM syntax data in `bzip2` and `base64` encoded format.

`filename` (required)

The file name the UDM syntax data should be written to by the listening servers. The file name must not contain any path elements.

`package` (required)

Name of the Debian package which creates the object.

`packageversion` (required)

Version of the Debian package which creates the object. For object modifications the version number needs to increase unless the package name is modified as well.

`appidentifier` (optional)

The identifier of the app which creates the object. This is important to indicate that the object is required as long as the app is installed anywhere in the UCS domain. Defaults to `string`.

`ucsversionstart` (optional)

Minimal required UCS version. The UDM syntax is only activated by systems with a version higher than or equal to this.


`ucsversionend` (optional)

Maximal required UCS version. The UDM syntax is only activated by systems with a version lower than or equal to this. To specify validity for the whole 4.1-x release range a value like 4.1-99 may be used.

`active` (internal)

A boolean flag used internally by the master domain controller to signal availability of the new UDM syntax on the master domain controller (default: `FALSE`).


## 6.8. UDM REST API

Feedback 

UCS provides a REST API which can be used to inspect, modify, create and delete UDM objects via HTTP requests.

The API is accessible from `https://<SERVERNAME-OR-IP>/univention/udm/`.

### 6.8.1. Authentication

Feedback 

To be able to use the API you have to authenticate with a user account which is a member of an authorized group. The group authorization is managed via the `directory/manager/rest/authorized-groups/<group-name>` UCR variables. The API comes predefined with the UCR variables `directory/manager/rest/authorized-groups/domain-admins`, `directory/manager/rest/authorized-groups/dc-backup` and `directory/manager/rest/authorized-groups/dc-slaves` which authorizes the groups Domain Admins, DC Backup Hosts and DC Slave Hosts respectively.

To authorize additional groups you just have to create a new UCR variable. If you haven't already, create the group you want to authorize:

```
udm groups/group create --position="cn=groups,$(ucr get ldap/base)" --
set name="UDM API Users"
```

Now set the UCR variable to allow the group members to use the API.

```
ucr set directory/manager/rest/authorized-groups/udm-api-users="cn=UDM
API Users,cn=groups,$(ucr get ldap/base)"
```

#### Note

The authorization of a group only allows the group members to access the API in the first place. After that, which actions the user can perform with the API is regulated via ACLs. For example a normal Domain Users user can't create or delete objects.

After you add or modify a `directory/manager/rest/authorized-groups/<group-name>` UCR variable you have to restart the API service for the changes to take effect.

```
service univention-directory-manager-rest restart
```

### 6.8.2. API overview

Feedback 

You can interact with the API by sending HTTP requests to resources and by using different HTTP methods you can achieve different results.


**Table 6.1. HTTP methods**

Verb	Description
GET	Retrieve a resource
POST	Create a resource
PUT	Replace or move a resource
PATCH	Modify or move a resource
DELETE	Delete a resource

For an in depth overview over which resources are available, which HTTP methods are allowed on them and which query parameters are available for a given HTTP method visit <https://<SERVERNAME-OR-IP>/univention/udm/schema/> with a browser.

By visiting <https://<SERVERNAME-OR-IP>/univention/udm/> with a browser you can navigate and use the API interactively.

## 6.8.3. API usage examples


Feedback 

In the following section you will learn how to create, modify, search and delete a user via the API.

While you try out these examples you will often see the `"_links"` and `"_embedded"` properties in the responses. These properties are defined by *HAL*, the Hypertext Application Language, which is used in the API. These properties contain links which can be used to traverse the API. For example the `"_links"` property of the response to a paginated query could contain the `"next"` property which points to the next page.

For more information on *HAL* please refer to the Internet Draft for *HAL*<sup>1</sup>.

### 6.8.3.1. Create a user via a POST request

Feedback 

To create a new user your first want to get a template that describes a valid user and has all attributes filled out with default values.

You can get the template for an UDM module with:

```
curl -X GET -H "Accept: application/json" \
  https://api-user:password@<SERVERNAME-OR-IP>/univention/udm/<module>/
add
```

So for the users/user module you get the template with:

```
curl -X GET -H "Accept: application/json" \
  https://api-user:password@<SERVERNAME-OR-IP>/univention/udm/users/
user/add
```

To work with the template you can save it into a file and to make it more readable you can use something like python's `json.tool`.

```
curl -X GET -H "Accept: application/json" \
  https://api-user:password@<SERVERNAME-OR-IP>/univention/udm/users/
user/add \
  | python -m json.tool > user_template.json
```

The JSON file contains meta information (keys that start with underscore '\_') that are not necessary to create a user. These can be filtered out to make it easier to work with the template file. The following example produces such a condensed template:

```
curl -X GET -H "Accept: application/json" \
  https://api-user:password@<SERVERNAME-OR-IP>/univention/udm/users/
user/add \
  | python -c 'import sys, json; \
    template = json.load(sys.stdin); \
    template = {key:value for key, value in template.items() if not \
    key.startswith("_")}; \
    json.dump(template, sys.stdout, indent=4)' > user_template.json
```

<sup>1</sup> <https://tools.ietf.org/html/draft-kelly-json-hal-08>

The content of `user_template.json` should look something like this.

```
{
  "position": "cn=users,dc=mydomain,dc=intranet",
  "objectType": "users/user",
  "options": {
    "pki": false
  },
  "policies": {
    "policies/pwhistory": [],
    "policies/umc": [],
    "policies/desktop": []
  },
  "properties": {
    "mobileTelephoneNumber": [],
    "certificateSubjectOrganisationalUnit": null,
    "groups": [],
    "sambahome": null,
    "departmentNumber": [],
    "certificateSerial": null,
    "certificateSubjectCommonName": null,
    "primaryGroup": "cn=Domain
Users,cn=groups,dc=mydomain,dc=intranet",
    "uidNumber": null,
    "disabled": false,
    "unlock": false,
    "street": null,
    "postcode": null,
    "scriptpath": null,
    "sambaPrivileges": [],
    "description": null,
    "certificateIssuerCommonName": null,
    "mailForwardCopyToSelf": false,
    "employeeType": null,
    "homedrive": null,
    "overridePWLength": null,
    "title": null,
    "mailAlternativeAddress": [],
    "userCertificate": null,
    "organisation": null,
    "homeSharePath": "",
    "certificateIssuerOrganisationalUnit": null,
    "e-mail": [],
    "userexpiry": null,
    "pwdChangeNextLogin": null,
    "mailHomeServer": null,
    "unixhome": "/home/",
    "gecos": "",
    "sambaUserWorkstations": [],
    "preferredLanguage": null,
    "certificateIssuerState": null,
    "pagerTelephoneNumber": [],
    "username": null,
    "umcProperty": [],
    "certificateIssuerCountry": null,
```



```

    "homeTelephoneNumber": [],
    "shell": "/bin/bash",
    "homePostalAddress": [],
    "firstname": null,
    "certificateIssuerOrganisation": null,
    "lastname": null,
    "city": null,
    "certificateSubjectMail": null,
    "mailForwardAddress": [],
    "phone": [],
    "gidNumber": null,
    "birthday": null,
    "employeeNumber": null,
    "objectFlag": [],
    "sambaLogonHours": null,
    "certificateSubjectLocation": null,
    "displayName": "",
    "password": null,
    "lockedTime": null,
    "sambaRID": null,
    "secretary": [],
    "certificateSubjectOrganisation": null,
    "overridePWHistory": null,
    "mailPrimaryAddress": null,
    "country": null,
    "roomNumber": [],
    "certificateSubjectCountry": null,
    "locked": false,
    "certificateDateNotBefore": null,
    "passwordexpiry": null,
    "certificateVersion": null,
    "homeShare": null,
    "certificateIssuerMail": null,
    "unlockTime": null,
    "serviceprovider": [],
    "profilepath": null,
    "certificateIssuerLocation": null,
    "jpegPhoto": null,
    "certificateDateNotAfter": null,
    "certificateSubjectState": null
  }
}

```


Now you can modify the attributes the new user should have and send the modified template, via a POST request, to create a new user.

```

curl -X POST -H "Accept: application/json" -H "Content-Type:
  application/json" \
  https://api-user:password@<SERVERNAME-OR-IP>/univention/udm/users/
  user/ --data @user_template.json

```

### 6.8.3.2. Search for users via a GET request

 Feedback 

In this example we search for a users/user object where the "firstname" property starts with "Ale" and the "lastname" property ends with "er".

```
curl -X GET -H "Accept: application/json" \
  "http://api-user:password@<SERVERNAME-OR-IP>/univention/udm/users/
  user/?query\[firstname\]=Al%2A&query\[lastname\]=%2Aer"
```

The response should look something like this (some fields where omitted for clarity):


```
{
  "_embedded": {
    "udm:object": [
      {
        "dn": "uid=alexpower,cn=users,dc=mydomain,dc=intranet",
        "id": "alexpower",
        "objectType": "users/user",
        "options": {
          "pki": false
        },
        "policies": {
          "policies/desktop": [],
          "policies/pwhistory": [],
          "policies/umc": []
        },
        "position": "cn=users,dc=mydomain,dc=intranet",
        "properties": {
          "birthday": null,
          "city": null,
          "country": null,
          "departmentNumber": [],
          "description": null,
          "disabled": false,
          "displayName": "Alex Power",
          "e-mail": [],
          "employeeNumber": null,
          "employeeType": null,
          "firstname": "Alex",
          "gecos": "Alex Power",
          "gidNumber": 5001,
          "groups": [
            "cn=Domain
            Users,cn=groups,dc=mydomain,dc=intranet"
          ],
          "homePostalAddress": [],
          "homeShare": null,
          "homeSharePath": "alexpower",
          "homeTelephoneNumber": [],
          "homedrive": null,
          "jpegPhoto": null,
          "lastname": "Power",
          "locked": false,
          "lockedTime": "0",
          "mailAlternativeAddress": [],
          "mailForwardAddress": [],
          "mailForwardCopyToSelf": "0",
          "mailHomeServer": null,
          "mailPrimaryAddress": null,
          "mobileTelephoneNumber": [],
```

```

    "objectFlag": [],
    "organisation": null,
    "overridePWHistory": null,
    "overridePWLength": null,
    "pagerTelephoneNumber": [],
    "password": null,
    "passwordexpiry": null,
    "phone": [],
    "postcode": null,
    "preferredLanguage": null,
    "primaryGroup": "cn=Domain
Users,cn=groups,dc=mydomain,dc=intranet",
    "profilepath": null,
    "pwdChangeNextLogin": null,
    "roomNumber": [],
    "sambaLogonHours": null,
    "sambaPrivileges": [],
    "sambaRID": 5018,
    "sambaUserWorkstations": [],
    "sambahome": null,
    "scriptpath": null,
    "secretary": [],
    "serviceprovider": [],
    "shell": "/bin/bash",
    "street": null,
    "title": null,
    "uidNumber": 2009,
    "umcProperty": {},
    "unixhome": "/home/alexpowers",
    "unlock": false,
    "unlockTime": "",
    "userexpiry": null,
    "username": "alexpowers"
  },
  "uri": "http://10.200.28.110/univention/udm/users/user/
uid%3Dalexpowers%2Ccn%3Dusers%2Cdc%3Dmydomain%2Cdc%3Dintranet"
}
]
},
"results": 1
}

```

### 6.8.3.3. Modify a user via a PUT request

 Feedback 

To modify a user you first get the current state of the user. To prevent modification conflicts you also have to get the entity tag (*Etag*) of the user resource. The *Etag* can be found in the response headers; it is used to identify a specific version of a resource.

```

curl -X GET -H "Accept: application/json" --dump-header user.headers \
  https://api-user:univention@<SERVERNAME-OR-IP>/univention/udm/users/
user/<dn> \
  | python -m json.tool > user.json

```

## Note

<dn> should be URL encoded.

Now you can edit the user in the `user.json` file to your liking. After you are done, send the changed `user.json` via a PUT request to modify the user. To avoid modification conflicts it is required to send the value of the *Etag* header, which you saved earlier in the `user.headers` file, as the value for the "If-Match" header.


```
curl -X PUT -H "Accept: application/json" -H "Content-Type: application/json" -H 'If-Match: "<Etag>"' \
  "https://api-user:password@<SERVERNAME-OR-IP>/univention/udm/users/user/<dn>" --data @user.json
```

## Note

<dn> should be URL encoded.

The quotes around the *Etag* are required.

### 6.8.3.4. Delete a user via a DELETE request

Feedback 


To delete a user you just have to send a DELETE request to `/univention/udm/users/user/<dn>`

```
curl -X DELETE http://api-user:password@<SERVERNAME-OR-IP>/univention/udm/users/user/<dn>
```

## Note


<dn> should be URL encoded.

## 6.9. UCS 5.0: Python 3 Migration of modules and extensions

Feedback 

UCS 5.0 switched from Python 2 to Python 3. This also affects Univention Directory Manager. Starting with UCS 5.0 the modules and extensions like syntax classes and hooks must be compatible with both Python versions to ensure easier transition. Python 2 will be removed completely with UCS 5.1. This chapter describes important aspects of the migration as well as changes to the API.

### 6.9.1. Compatibility with UCS 4.4

Feedback 

Most changes proposed in this chapter are compatible with UCS 4.4. One exception is the registration of the mapping encoding. The changes suggested here should already be included in the UDM modules for UCS 4.4 to make the update easier. The changes suggested here should already be included for UCS 4.4. Otherwise the update to UCS 5.0 may be problematic. Apps that still install UDM modules under UCS 4.4, while the Primary Node may already be UCS 5, must also contain the customizations in the UDM modules or register 2 different variants, otherwise the app will not be displayed on the Primary Node in Univention Management Console / Univention Directory Manager, for example.

For the registration of UDM extensions the parameters to specify the compatible starting and end UCS version are now mandatory. While a Join script looked like:

```
. /usr/share/univention-lib/ldap.sh
```

```
ucs_registerLDAPExtension "$@" \
--udm_module /usr/lib/python3/dist-packages/univention/admin/handlers/
foo/bar.py
```

it may now specify the compatible UCS versions:

```
. /usr/share/univention-lib/ldap.sh

ucs_registerLDAPExtension "$@" \
--ucsversionstart "4.4-0" --ucsversionend "5.99-0" \
--udm_module /usr/lib/python3/dist-packages/univention/admin/handlers/
foo/bar.py
```


or registers two separate versions compatible for each UCS version:

```
. /usr/share/univention-lib/ldap.sh

ucs_registerLDAPExtension "$@" \
--ucsversionstart "4.4-0" --ucsversionend "4.99-0" \
--udm_module /usr/lib/python2.7/dist-packages/univention/admin/
handlers/foo/bar.py

ucs_registerLDAPExtension "$@" \
--ucsversionstart "5.0-0" --ucsversionend "5.99-0" \
--udm_module /usr/lib/python3/dist-packages/univention/admin/handlers/
foo/bar.py
```

## 6.9.2. Default option


Feedback 

If not already present the module should define a default Univention Directory Manager option:

```
options = {
    'default': univention.admin.option(
        short_description=short_description,
        default=True,
        objectClasses=['top', 'objectClassName'],
    )
}
class object(...):
    ...
```

This enables generic functionality like automatic creation of search filters, automatic identification of objects and obsoletes the need to create the add-list manually.

## 6.9.3. Mapping functions

Feedback 

The unmap functions must decode the given list of byte strings (bytes) into unicode strings (str). The map functions must encode the result of the unmap functions (e.g. unicode strings str) into a list of byte strings (bytes). Both functions have a new optional parameter *encoding*, which is a tuple consisting of the encoding (defaulting to UTF-8) and the error handling in case de/encoding fails (defaulting to strict).

Old UCS 4 code most often looked like:

```
def map_function(value):
    return [value]
```

```
def unmap_function(value):
    return value[0]

mapping.register('property', 'attribute', map_function, unmap_function)
```


In UCS 5.0 the code has to look like:

```
def map_function(value, encoding=None): # type: (Union[Text,
    Sequence[Text]], Optional[Tuple[str, str]]) -> List[bytes]
    return [value.encode(*encoding)]

def unmap_function(value, encoding=None): # type: (Sequence[bytes],
    Optional[Tuple[str, str]]) -> Text
    return value[0].decode(*encoding)

mapping.register('property', 'attribute', map_function, unmap_function)
```

## 6.9.4. Mapping Encoding

Feedback 

### Warning

Specifying the mapping encoding is incompatible with UCS 4.4.

The registration of the mapping of LDAP attributes to Univention Directory Manager properties now has to specify the correct encoding explicitly. The default encoding used is UTF-8. As most LDAP data is stored in UTF-8 the encoding parameter can be left out for most properties.

The encoding can simply be specified in the registration of a mapping:

```
mapping.register('property', 'attribute', map_function, unmap_function,
    encoding='ASCII')
```

The encoding depends on the LDAP syntax of the corresponding LDAP attribute. Syntaxes storing binary data should either be specified as ISO8859-1 or preferably should be decoded to an ASCII representation of base64 via `univention.admin.mapping.mapBase64` and `univention.admin.mapping.unmapBase64`. The attributes of the following syntaxes e.g. should be set to ASCII as they consist of ASCII only characters or a subset of ASCII (e.g. numbers).


- IA5 String (1.3.6.1.4.1.1466.115.121.1.26)
- Integer (1.3.6.1.4.1.1466.115.121.1.27)
- Printable String (1.3.6.1.4.1.1466.115.121.1.44)
- Boolean (1.3.6.1.4.1.1466.115.121.1.7)
- Numeric String (1.3.6.1.4.1.1466.115.121.1.36)
- Generalized Time (1.3.6.1.4.1.1466.115.121.1.24)
- Telephone Number (1.3.6.1.4.1.1466.115.121.1.50)
- UUID (1.3.6.1.1.16.1)

- Authentication Password (1.3.6.1.4.1.4203.1.1.2)

To find out the syntax of an LDAP attribute programmatically e.g. for the attribute `gecos`:


```
python -c '
from univention.uldap import getMachineConnection
from ldap.schema import AttributeType
conn = getMachineConnection()
schema = conn.get_schema()
attr = schema.get_obj(AttributeType, "gecos")
print(attr.syntax)'
```

### 6.9.5. `object.open()` / `object._post_unmap()`

Feedback 


LDAP attributes contained in `self.oldattr` are usually transformed into property values (in `self.info`) by the mapping functions. In some cases this cannot be done automatically. Instead this is done manually in the methods `open()` or `_post_unmap()`. These functions must consider transforming byte strings (bytes in `self.oldattr`) into unicode strings (str in `self.info`).

### 6.9.6. `object.has_key()`

Feedback 

The method `has_key()` has been renamed into `has_property()`. The method `has_property()` is already present in UCS 4.4.

### 6.9.7. `identify()`

Feedback 

The `identify()` function must now consider that the given attribute values are byte strings. The code prior looked like:

```
def identify(dn, attr, canonical=False):
    return 'objectClassName' in attr.get('objectClass', [])
```

In UCS 5.0 the code have to look like:

```
class object(...):
    ...
    @classmethod
    def identify(cls, dn, attr, canonical=False):
        return b'objectClassName' in attr.get('objectClass', [])

identify = object.identify
```


In most cases the `identify()` function only checks for the existence of a specific LDAP `objectClass`. The generic implementation can be used instead, which requires the default UDM option to be set:

```
options = {
    'default': univention.admin.option(
        short_description=short_description,
        default=True,
        objectClasses=['top', 'objectClassName'],
    )
}
class object(...):
    ...
```

`_ldap_modlist()`

```
identify = object.identify
```

### 6.9.8. `_ldap_modlist()`

Feedback 

The methods `_ldap_modlist()` and `_ldap_addlist()` now must insert byte strings into the `add/modlist`. The code prior looked like:

```
class object(...):
    ...
    def _ldap_addlist(al):
        al = super(object, self)._ldap_addlist(al)
        al.append(('objectClass', ['top', 'objectClassName']))
        return al

    def _ldap_modlist(ml):
        ml = super(object, self)._ldap_modlist(ml)
        value = ...
        new = [value]
        ml.append(('attribute', self.oldattr.get('attribute', []), new))
        return ml
```

In UCS 5.0 the code have to look like:

```
class object(...):
    ...
    def _ldap_addlist(al):
        al = super(object, self)._ldap_addlist(al)
        al.append(('objectClass', [b'top', b'objectClassName']))
        return al

    def _ldap_modlist(ml):
        ml = super(object, self)._ldap_modlist(ml)
        value = ...
        new = [value.encode('UTF-8')]
        ml.append(('attribute', self.oldattr.get('attribute', []), new))
        return ml
```


The `_ldap_addlist()` is mostly not needed and should be replaced by specifying a default option (see above).

### 6.9.9. `lookup()`

Feedback 


The `lookup()` should be replaced by specifying a default option as described above. The class method `rewrite_filter()` can be used to add additional filter rules.

### 6.9.10. Syntax classes

Feedback 

Syntax classes now must ensure to return unicode strings.

### 6.9.11. Hooks

Feedback 

For hooks the same rules as in `_ldap_modlist()` apply.




# Chapter 7. Univention Management Console (UMC)

7.1. Architecture .....	105
7.2. Asynchronous Framework .....	106
7.3. Protocol UMCP 2.0 .....	107
7.3.1. Data flow .....	107
7.3.2. Authentication .....	107
7.3.3. Message format .....	107
7.3.3.1. Message header .....	107
7.3.3.2. Message body .....	108
7.3.4. Examples .....	108
7.4. Protocol HTTP for UMC .....	109
7.4.1. Examples .....	109
7.5. UMC files .....	110
7.5.1. <code>debian/package.umc-modules</code> .....	110
7.5.2. UMC Module Declaration File .....	111
7.6. Local System Module .....	111
7.6.1. Python API .....	111
7.6.2. UMC module API (Python and JavaScript) .....	111
7.6.2.1. XML definition .....	112
7.6.2.2. Python module .....	113
7.6.2.3. UMC store API .....	115
7.6.3. Packaging .....	116
7.7. Domain LDAP Module .....	119
7.8. Disabling a Module .....	119

The Univention Management Console (UMC) is a service that runs on all UCS systems by default. This service provides access to several system information and implements modules for management tasks. What modules are available on a UCS system depends on the system role and the installed components. Each domain user can log on to the service via a web interface. Depending on the access policies for the user the visible modules for management tasks will differ.

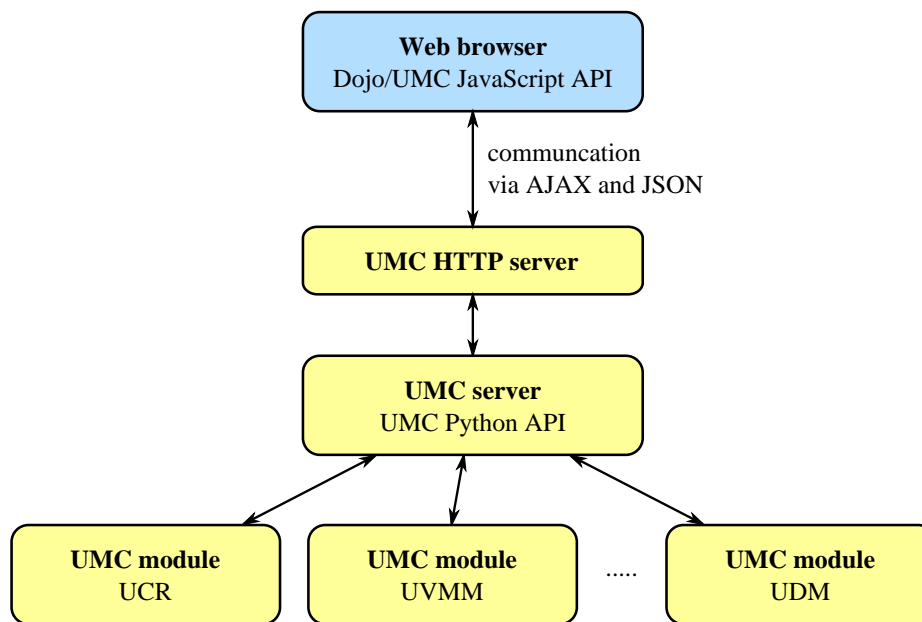
In the following the technical details of the architecture and the Python and JavaScript API for modules are described.

## 7.1. Architecture

 Feedback 


The Univention Management Console service consists of four components. The communication between these components is encrypted using SSL. The architecture and the communication channels is shown in Figure 7.1.

**Figure 7.1. UMC architecture and communication channels**



- The *UMC server* is the core component. It provides access to the modules and manages the connection and verifies that only authorized users gets access. The protocol used to communicate is the *Univention Management Console Protocol* (UMCP) in version 2.0.
- The *UMC HTTP server* is a small web server that provides HTTP access to the UMC server. It is used by the web frontend.
- The *UMC module* processes are forked by the UMC server to provide a specific area of management tasks within a session.

## 7.2. Asynchronous Framework

Feedback 

All server-side components of the UMC service are based on the asynchronous framework Python Notifier, that provides techniques for handling quasi parallel tasks based on events. The framework follows three basic concepts:

### Non-blocking sockets

For servers that should handling several communication channels at a time have to use so called non-blocking sockets. This is an option that needs to be set for each socket, that should be management by the server. This is necessary to avoid blocking on read or write operations on the sockets.

### Timer


To perform tasks after a defined amount of time the framework provides an API to manage timer (one shot or periodically).

### Signals

To inform components within a process of a specific a events the framework provide the possibility to define signals. Components being interested in events may place a registration.


Further details, examples and a complete API documentation for Python Notifier can be found at the website of Python Notifier<sup>1</sup>.

## 7.3. Protocol UMCP 2.0

Feedback 

This protocol is used by the UMC server for external clients and between the UMC server and its UMC module processes.

### 7.3.1. Data flow

Feedback 

The protocol is based on a server/client model. The client sends requests to the server that will be answered with a response message by the server.

With a status code in the response message the client can determine the type of result of its request:

- An error occurred during the processing of the request. The status code contains details of the error.
- The command was processed successfully. A status message may contain details about the performed task.


### 7.3.2. Authentication

Feedback 

Before a client may send request messages to the server that contain commands to execute, the client has to authenticate. After a successful authentication the UMC server determines the permissions for the user defined by policies in the LDAP directory. If the LDAP server is not reachable a local cache is checked for previously discovered permissions. If none of these sources is available the user is prohibited to use any command.

The authentication process within the UMC server uses the PAM service `univention-management-console`. By default, this service uses a cache for credentials if the LDAP server is not available to provide the possibility to access the UMC server also in case of problems with the LDAP server.

### 7.3.3. Message format

Feedback 

The messages, request and response, have the same format that consists of a single header line, one empty line and the body.

The header line contains control information that allows the UMC server to verify the correctness of the message without reading the rest of the message.

#### 7.3.3.1. Message header

Feedback 

The header defines the message type, a unique identifier, the length of the message body in bytes, the command and the mime type of the body.

```
(REQUEST|RESPONSE)/<id>/<length of body>[/<mime-type>]:
<command>[ <arguments>]
```

By the first keyword the message type is defined. Supported message types are REQUEST and RESPONSE. Any other type will be ignored.

Separated by a / the message id follows, that must be unique within a communication channel. By default it consists of a timestamp and a counter.

The next field is a number, defining the length of the body in bytes, starting to count after the empty line.

<sup>1</sup> <https://github.com/crunchy-github/python-notifier>

## Examples

Since UMCP 2.0 there is as another field specifying the mime type of the body. If not given then the guessed value for the mime type is `application/json`. If the body can not be decoded using a JSON parser the message is invalid.

The last two fields define the UMCP command that should be executed by the server. The following commands are supported:

### AUTH

This commands sends an authentication request. It must be the first command send by the client. All commands send before a successful authentication are rejected.

### GET

This command is used to retrieve information from the UMC server, e.g. a list of all UMC modules available in this session.


### SET

This command is used to define settings for the session, e.g. the language.

### COMMAND

This command is used to pass requests to UMC modules. Each module defines a set of commands, that it implements. The UMC module command is defined by the first argument in the UMCP header, e.g. a request like `REQUEST/123423423-01/42/application/json: COMMAND ucr/query` passes on the module command `ucr/query` to a UMC module.

## 7.3.3.2. Message body

Feedback 

The message body may contain one object of any type, e.g. an image, an OpenOffice document or a JSON object. The JSON object is the default type and is the only supported mime type for request messages. It contains a dictionary that has a few predefined keys (for both message types):

### options

Contains the arguments for the command.

### status

Defines the status code in response messages. The codes are similar to the HTTP status codes , e.g. 200 defines a successful execution of the command.


### message

May contain a human readable description of the status code. This may contain details to explain the user the situation.

### flavor

An optional field. If given in a request message the module may act differently than without the flavor.

## 7.3.4. Examples

Feedback 

This section contains a few example messages of UMCP 2.0.

### Example 7.1. Authentication request

```
REQUEST/130928961341733-1/147/application/json: AUTH
{"username": "root", "password": "univention"}
```

### Example 7.2. Search for users


Request:

```
REQUEST/130928961341726-0/125/application/json: COMMAND udm/query
{"flavor": "users/user",
 "options": {"objectProperty": "name",
             "objectPropertyValue": "test1*1",
             "objectType": "users/user"}}
```

Response:


```
RESPONSE/130928961341726-0/1639/application/json: COMMAND udm/query
{"status": 200,
 "message": null,
 "options": {"objectProperty": "name",
             "objectPropertyValue": "test1*1",
             "objectType": "users/user"},
 "result": [{"ldap-dn": "uid=test11,cn=users,dc=univention,dc=qa",
             "path": "univention.qa:/users",
             "name": "test11",
             "objectType": "users/user"},
 ...
             {"ldap-dn": "uid=test191,cn=users,dc=univention,dc=qa",
             "path": "univention.qa:/users",
             "name": "test191",
             "objectType": "users/user"}]}
```

## 7.4. Protocol HTTP for UMC

Feedback 

With the new generation of UMC there is also an HTTP server available that can be used to access the UMC server. The web server is implemented as a frontend to the UMC server and translates HTTP POST requests to UMCP commands.

### 7.4.1. Examples

Feedback 

#### Example 7.3. Authentication request

```
POST http://192.0.2.31/univention/auth HTTP/1.1
{"options": {"username": "root", "password": "univention"}}
```

#### Example 7.4. search for users

Request

```
POST http://192.0.2.31/univention/command/udm/query HTTP/1.1
```

```
{ "options": { "container": "all",
               "objectType": "users/user",
               "objectProperty": "username",
               "objectPropertyValue": "test1*1" },
  "flavor": "users/user" }
```

Response


```
{ "status": 200,
  "message": null,
  "options": { "objectProperty": "username",
               "container": "all",
               "objectPropertyValue": "test1*1",
               "objectType": "users/user" },
  "result": [ { "ldap-dn": "uid=test11,cn=users,dc=univention,dc=qa",
                "path": "univention.qa:/users",
                "name": "test11",
                "objectType": "users/user" },
              ...
              { "ldap-dn": "uid=test191,cn=users,dc=univention,dc=qa",
                "path": "univention.qa:/users",
                "name": "test191",
                "objectType": "users/user" } ] }
```

## 7.5. UMC files

Feedback 

Files for building a UMC module.

### 7.5.1. `debian/package.umc-modules`

Feedback 

`dh-umc-module-build` builds translation files. `dh-umc-module-install` installs files. Configured through `debian/package.umc-modules`.

```
Module: module-name
Python: umc
Definition: umc/module-name.xml
Javascript: umc
Icons: umc/icons
```

Module

Internal (?) name of the module.

Python

Directory containing the Python code relative to top-level directory.

Definition

Path to an XML file, which describes the module. See Section 7.5.2 for more information.


Javascript

Directory containing the Java-Script code relative to top-level directory.

Icons (deprecated)

Directory containing the Icons relative to top-level directory. Must provide icons in sizes 16×16 (umc/icons/16x16/udm-module.png) and 50×50 (umc/icons/50x50/udm-module.png) pixels.

## 7.5.2. UMC Module Declaration File

Feedback 


umc/module.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<!--DOCTYPE umc SYSTEM "management/univention-management-console/doc/
module.dtd"-->
<umc version="2.0">
  <module id="udm" icon="udm-MODULE" version="1.0"
translationId="MODULE">
    <name>...</name>
    <description>...</description>
    <flavor>...</flavor>
    <categories>
      <category name="domain"/>
    </categories>
    <command>...</command>
  </module>
</umc>
```

umc/categories/category.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<umc version="2.0">
  <categories>
    <category id="category" priority="..." icon="....svg" color="#xxxxxxx"/>
  </categories>
</umc>
```


## 7.6. Local System Module

Feedback 

The UMC server provides management services that are provided by so called UMC modules. These modules are implemented in Python (backend) and in JavaScript (web frontend). The following page provides information about developing and packaging of UMC modules. It is important to know the details of Section 7.1.


The package **univention-management-console-dev** provides the command `umc-create-module`, which can be used to create a template for a custom UMC module.

### 7.6.1. Python API

Feedback 

The Python API for the UMCP is defined in the python module `univention.management.console.protocol`.

### 7.6.2. UMC module API (Python and JavaScript)


Feedback 

A UMC module consists of three components

- A XML document containing the definition.

- The Python module defining the command functions.
- The JavaScript frontend providing the web frontend.

### 7.6.2.1. XML definition

Feedback 

The UMC server knows three types of resources that define the functionality it can provide:

UMC modules

provide commands that can be executed if the required permission is given.

Syntax types


can be used to verify the correctness of command attributes defined by the UMCP client in the request message or return values provided by the UMC modules.

Categories

help to define a structure and to sort the UMC modules by its type of functionality.

All these resources are defined in XML files. The details are described in the following sections

#### 7.6.2.1.1. Module definition

Feedback 

The UMC server does not load the Python modules to get the details about the modules name, description and functionality. Therefore each UMC module must provide an XML file containing this kind of information. The following example defines a module with the id udm:

```
<?xml version="1.0" encoding="UTF-8"?>
<umc version="2.0">
  <module id="udm" icon="udm/module" version="1.0">
    <name>Univention Directory Manager</name>
    <description>Manages all UDM modules</description>
    <flavor icon="udm-users" id="users/user">
      <name>Users</name>
      <description>Managing users</description>
    </flavor>
    <categories>
      <category name="domain"/>
    </categories>
    <command name="udm/query" function="query"/>
    <command name="udm/containers" function="containers"/>
  </module>
</umc>
```

The element `module` defines the basic details of a UMC module.

`id`

This identifier must be unique among the modules of an UMC server. Other files may extend the definition of a module by adding more flavors or categories.

`icon`

The value of this attribute defines an identifier for the icon that should be used for the module. Details for installing icons can be found in the Section 7.6.3.



The child elements `name` and `description` define the English human readable name and description of the module. For other translations the build tools will create translation files. Details can be found in the Section 7.6.3.

This example defines a so called *flavor*. A flavor defines a new name, description and icon for the same UMC module. This can be used to show several virtual modules in the overview of the web frontend. Additionally the flavor is passed to the UMC server with each request i.e. the UMC module has the possibility to act differently for a specific flavor.

As the next element `categories` is defined in the example. The child elements `category` set the categories within the overview where the module should be shown. Each module can be part of multiple categories. The attribute `name` is the internal identify of a category.

At the end of the definition file a list of commands is specified. The UMC server only passes commands to a UMC module that are defined. A command definition has two attributes:


`name`

is the name of the command that is passed to the UMC module. Within the UMCP message it is the first argument after the UMCP COMMAND.

`function`

defines the method to be invoked within the python module when the command is called.

#### 7.6.2.1.2. Category definition


Feedback 

The predefined set of categories can be extended by each module.

#### Example 7.5. UMC module category examples

```
<?xml version="1.0" encoding="UTF-8"?>
<umc version="2.0">
  <categories>
    <category id="favorites">
      <name>Favorites</name>
    </category>
    <category id="system">
      <name>System</name>
    </category>
    <category id="wizards">
      <name>Wizards</name>
    </category>
    <category id="monitor">
      <name>Surveillance</name>
    </category>
  </categories>
</umc>
```

#### 7.6.2.2. Python module

Feedback 

The Python API for UMC modules primary consists of one base class that must be implemented. As an addition to python API provides some helper:

- exception classes
- translation support

- logging functions
- UCR access

In the definition file for the UMC module specifies functions for the commands provided by the module. These functions must be implemented as methods of the class `Instance` that inherits from `univention.management.console.base.Base`.

The following Python code example matches the definition in the previous section:

```
from univention.management.console import Translation
from univention.management.console.base import Base, UMC_Error
from univention.management.console.log import MODULE
from univention.management.console.config import ucr
from univention.management.console.modules.sanitizers import
    IntegerSanitizer
from univention.management.console.modules.decorators import sanitize

_ = Translation('univention-management-console-modules-udm').translate

class Instance(Base):

    def init(self):
        """Initialize the module with some values"""
        super(Instance, self).init()
        self.data = [int(x) for x in ucr.get('some/examle/ucr/variable',
            '1,2,3').split(',')]

    def query(self, request):
        """get all values of self.data"""
        self.finished(request.id, self.data)

    @sanitize(item=IntegerSanitizer(required=True))
    def get(self, request):
        """get a specific item of self.data"""
        try:
            item = self.data[request.options['item']]
        except IndexError:
            MODULE.error('A invalid item was accessed.')
            raise UMC_Error(_('The item %d does not exists.') %
                (request.options['item'],), status=400)
        self.finished(request.id, self.data[item])

    @sanitize(IntegerSanitizer(required=True))
    def put(self, request):
        """replace all data with the list provided in request.options"""
        self.data = request.options
        self.finished(request.id, None)
```

Each command methods has one parameter that contains the UMCP request. Such an object has the following properties:

`id`

the unique identifier of the request.

`options`

contains the arguments for the command. For most commands it is a dictionary.

`flavor`

the name of the flavor that was used to invoke the command. This might be `None`.

The method `init()` in the example is invoked when the module process starts. It could e.g. be used to initialize a database connection. The other methods in the example will serve specific request. To respond to a request the function `finished` must be invoked. To validate the request body the decorator `@sanitize` might be used with various sanitizers defined in `univention.management.console.modules.sanitizers`. For a way to send an error message back to the client the `UMC_Error` can be raised with the error message as argument and an optional HTTP status code. The base class for modules provides some properties and methods that could be useful when writing UMC modules:

`username`

The username of the owner of this session.

`user_dn`

The DN of the user or `None` if the user is only a local user.

`password`

The password of the user.


`init()`

Is invoked after the module process has been initialized. At that moment, the settings, like locale and username and password are available.

`destroy()`

Is invoked before the module process shuts down.

### 7.6.2.3. UMC store API

Feedback 

In order to encapsulate and ease the access to module data from the JavaScript side, a *store* object offers a unified way to query and modify module data. The UMC JavaScript API comes with an object store implementation of the Dojo store API<sup>2</sup>. This allows the JavaScript code to easily access/modify module data and to observe changes on the data in order to react immediately. The following methods are supported:

`get(id)`

Returns a dictionary of all properties for the object with the specified identifier.

`put(dictionary, options)`

modifies an object with the corresponding properties and an optional dictionary of options.

`add(dictionary, options)`

Adds a new object with the corresponding properties and an optional dictionary of options.

<sup>2</sup> <http://dojotoolkit.org/reference-guide/dojo/store.html>

```
remove(id)
```

Removes the object with the specified identifier.

```
query(dictionary)
```

Queries a list of objects (returned as list of dictionaries) corresponding to the given query which is represented as dictionary. Note that not all object properties need to be returned in order to save bandwidth.

The UMC object store class in JavaScript will be able to communicate directly with the Python module if the following methods are implemented:

```
module/get
```

Expects as input a list of unique IDs (as strings) and returns a list of dictionaries as result. Each dictionary entry holds all object properties.

```
module/put
```

Expects as input a list of dictionaries where each entry has the properties *object* and *options*. The property *object* holds all object properties to be set (i.e., this may also be a subset of all possible properties) as a dictionary. The second property *options* is an optional dictionary that holds additional options as a dictionary.

```
module/add
```

Expects similar input values as *module/put*.

```
module/remove
```

Expects as input a list of dictionaries where each entry has the properties *object* (containing the object's unique ID (as string)) and *options*. The options property can be necessary as a removal might be executed in different ways (recursively, shallow removal etc.).


```
module/query
```

Expects as input a dictionary with entries that specify the query parameters and returns a list of dictionaries. Each entry may hold only a subset of all possible object properties.

Further references:

- Dojo object store reference guide<sup>3</sup>
- Object store tutorial<sup>4</sup>
- HTML5 IndexedDB object store API<sup>5</sup>

### 7.6.3. Packaging

Feedback 

A UMC module consists of several files that must be installed at a specific location. As this mechanism is always the same there are debhelper tools making package creation for UMC modules very easy.

The following example is based on the package for the UMC module UCR.

<sup>3</sup> <http://dojotoolkit.org/reference-guide/dojo/store.html>

<sup>4</sup> <http://www.sitepen.com/blog/2011/02/15/dojo-object-stores/>

<sup>5</sup> <http://www.w3.org/TR/IndexedDB/#object-store>

A UMC module may be part of a source package with multiple binary packages. The examples uses a own source package for the module.

As a first step create a source package with the following directories and files:

- `univention-management-console-module-ucr/`
- `univention-management-console-module-ucr/debian/`
- `univention-management-console-module-ucr/debian/univention-management-console-module-ucr.umc-modules`
- `univention-management-console-module-ucr/debian/rules`
- `univention-management-console-module-ucr/debian/changelog`
- `univention-management-console-module-ucr/debian/control`
- `univention-management-console-module-ucr/debian/copyright`
- `univention-management-console-module-ucr/debian/compat`

All these files are standard Debian packaging files except `univention-management-console-module-ucr.umc-modules`. This file contains information about the locations of the UMC module source files:

```
Module: ucr
Python: umc/python
Definition: umc/ucr.xml
Syntax: umc/syntax/ucr.xml
Javascript: umc/js
Icons: umc/icons
```

The keys in this file of the following meaning:

Module

The internal name of the module

Python

A directory that contains the python package for the UMC module

Definition

The filename of the XML file with the module definition

Javascript

A directory containing the JavaScript source code

Icons

A directory containing the icons required by the modules web frontend

Syntax (optional)

The filename of the XML file with the syntax definitions

Category (optional)

The filename of the XML file with the category definitions

The directory structure for such a UMC module file would look like this:

- `univention-management-console-module-ucr/umc/`

```

◦ univention-management-console-module-ucr/umc/syntax/
◦ univention-management-console-module-ucr/umc/syntax/ucr.xml
◦ univention-management-console-module-ucr/umc/js/
◦ univention-management-console-module-ucr/umc/js/ucr.js
◦ univention-management-console-module-ucr/umc/js/de.po
◦ univention-management-console-module-ucr/umc/de.po
◦ univention-management-console-module-ucr/umc/icons/
◦ univention-management-console-module-ucr/umc/icons/16x16/
◦ univention-management-console-module-ucr/umc/icons/16x16/ucr.png
◦ univention-management-console-module-ucr/umc/icons/24x24/
◦ univention-management-console-module-ucr/umc/icons/24x24/ucr.png
◦ univention-management-console-module-ucr/umc/icons/64x64/
◦ univention-management-console-module-ucr/umc/icons/64x64/ucr.png
◦ univention-management-console-module-ucr/umc/icons/32x32/
◦ univention-management-console-module-ucr/umc/icons/32x32/ucr.png
◦ univention-management-console-module-ucr/umc/ucr.xml
◦ univention-management-console-module-ucr/umc/python/
◦ univention-management-console-module-ucr/umc/python/ucr/
◦ univention-management-console-module-ucr/umc/python/ucr/de.po
◦ univention-management-console-module-ucr/umc/python/ucr/__init__.py

```

If such a package has been created a few things need to be adjusted

debian/compat

```
7
```

debian/rules

```

%:
dh $@

override_dh_auto_build:
dh-umc-module-build
dh_auto_build

override_dh_auto_install:
dh-umc-module-install
dh_auto_install

```

debian/control

```


Source: univention-management-console-module-ucr
Section: univention
Priority: optional
Maintainer: Univention GmbH <packages@univention.de>
Build-Depends: debhelper (>= 7.0.50~),
    dh-python,
    univention-management-console-dev,
    python-all
Standards-Version: 3.5.2

Package: univention-management-console-module-ucr
Architecture: all
Depends: univention-management-console-server
Description: UMC module for UCR

```

This package contains the UMC module for Univention Configuration Registry

## 7.7. Domain LDAP Module


 Feedback 

Done through *flavor*.

```
<?xml version="1.0" encoding="UTF-8"?>
<umc version="2.0">
  <module id="udm" icon="udm-MODULE" version="1.0"
    translationId="MODULE">
    <flavor priority="25" icon="udm-MODULE-SUBMODULE" id="MODULE/
SUBMODULE">
      <name>MODULE name</name>
      <description>MODULE description</description>
    </flavor>
    <categories>
      <category name="domain"/>
    </categories>
  </module>
</umc>
```

Must use `/umc/module/category/@name="domain"`! Must use `/umc/module/@translationId` to specify alternative translation file, which must be installed as `/usr/share/univention-management-console/i18n/language/module.mo`.

## 7.8. Disabling a Module

 Feedback 

To disabling a module use the following XML file as a template:

```
<?xml version="1.0" encoding="UTF-8"?>
<umc version="2.0">
  <module id="udm" icon="udm/module" version="1.0"
    translationId="MODULE">
    <name/>
    <description/>
    <flavor id="MODULE/SUBMODULE" deactivated="yes" />
  </module>
</umc>
```






# Chapter 8. Web services

8.1. Extending the overview page ..... 121

## 8.1. Extending the overview page

 Feedback 

When a user opens `http://localhost/` or `http://hostname/` in a browser, she is redirected to the *UCS overview* page.

Depending on the preferred language negotiated by the web browser the user is either redirected to the German or English version. The overview page is split between **Installed web services** and **Administration** entries.

The start page can be extended using Univention Configuration Registry variables. `PACKAGE` refers to a unique identifier, typically the name of the package shipping the extensions to the overview page. The configurable options are explained below:

- `ucs/web/overview/entries/admin/PACKAGE/OPTION` variables extend the administrative section.
- `ucs/web/overview/entries/service/PACKAGE/OPTION` variables extend the web services section.

To configure an extension of the overview page the following options must/can be set using the pattern `ucs/web/overview/entries/admin/PACKAGE/OPTION=VALUE` (and likewise for services).

- `link` defines a link to a URL representing the service (usually a web interface).
- `label` specifies a title for an overview entry. The title can also be translated; e.g. `label/de` can be used for a title in German.
- `description` configures a longer description of an overview entry. The description can also be translated; e.g. `description/de` can be used for a description in German. Should not exceed 60 characters, because of space limitations of the rendered box.
- Optionally an icon can be displayed. Using `icon` either a filename or a URI can be provided. When specifying a filename, the name must be relative to the directory `/var/www`, i.e. with a leading `/`. All file formats typically displayed by browsers can be used (e.g. PNG/JPG). All icons must be scaled to 50x50 pixels.
- The display order can be specified using `priority`. Depending on the values the entries are displayed in *lexicographical* order (i.e.  $100 < 50$ ).

The following example configures the link to the Nagios web interface:

```
ucs/web/overview/entries/admin/nagios/description/de: Netzwerk-, Host-
und Serviceüberwachung
ucs/web/overview/entries/admin/nagios/description: Network, host and
service monitoring system
ucs/web/overview/entries/admin/nagios/icon: /icon/50x50/nagios.png
ucs/web/overview/entries/admin/nagios/label/de: Univention Nagios
ucs/web/overview/entries/admin/nagios/label: Univention Nagios
ucs/web/overview/entries/admin/nagios/link: /nagios/
ucs/web/overview/entries/admin/nagios/priority: 50
```



## Chapter 9. App Center

The Univention App Center provides a platform for software vendors and an easy-to-use entry point for Univention Corporate Server users to extend their environment with business software.

The documentation how to develop Apps for Univention App Center can be found in the App Center Developer Guide<sup>1</sup>

---

<sup>1</sup> [https://wiki.univention.de/index.php?title=Category:App\\_Center\\_Developer\\_Guide](https://wiki.univention.de/index.php?title=Category:App_Center_Developer_Guide)



# Chapter 10. Integration of external repositories

10.1. Integration of repository components via Univention Management Console .....	125
10.2. Integration of repository components via Univention Configuration Registry .....	126

Sometimes it might be necessary to add external repositories, e.g. when testing an application which is developed for the UCS@school. Such components can be registered via Univention Management Console or in Univention Configuration Registry.

Components can be versioned. This ensures that only components are installed that are compatible with a UCS version.

empty or unset

All versions of the same major number will be used. If for example UCS-4.4 is installed, all repositories of the component with version numbers 4.0, 4.1, 4.2, 4.3 and 4.4 will be used if available.


current

*current* Using the keyword *current* will likewise include all versions of the same major version. Additionally it will block all minor and major upgrades of the installed UCS system until the respective component is also available for the new release. Patch level and errata updates are not affected. If for example UCS-3.1 is currently installed and UCS-3.2 or UCS-4.0 is already available, the release updated will be postponed until the component is also available for version 3.2 and 4.0 respectively.

*major.minor*

By specifying an explicit version number only the specified version of the component will be used. Release updates of the system will not be hindered by such components. Multiple versions can be given using commas as delimiters, for example *3.2,4.0*.

## 10.1. Integration of repository components via Univention Management Console

Feedback 

A list of the integrated repository components is in the UMC module **Repository Settings**. Applications which have been added via the Univention App Center are still listed here, but should be managed via the **App Center** module.

A further component can be set up with **Add**. The **Component name** identifies the component on the repository server. A free text can be entered under **Description**, for example, for describing the functions of the component in more detail.

The host name of the download server is to be entered in the input field **Repository server**, and, if necessary, an additional file path in **Repository prefix**.

A **Username** and **Password** can be configured for repository servers which require authentication.

A software component is only available once **Enable this component** has been activated.

A differentiation is also made for components between *maintained* and *unmaintained* components.

## 10.2. Integration of repository components via Univention Configuration Registry

The following Univention Configuration Registry variables can be used to register a repository component. It is also possible to activate further functions here which cannot be configured via the UMC module. *NAME* stands for the component's name:

`repository/online/component/NAME/server`

The repository server on which the components are available. If this variable is not set, the server from the Univention Configuration Registry variable `repository/online/server` uses.

`repository/online/component/NAME`

This variable must be set to *enabled* if the components are to be mounted.

`repository/online/component/NAME/localmirror`

This variable can be used to configure whether the component is mirrored locally. In combination with the Univention Configuration Registry variable `repository/online/component/NAME/server`, a configuration can be set up so that the component is mirrored, but not activated, or that it is activated, but not mirrored.

`repository/online/component/NAME/description`

A descriptive name for the repository.

`repository/online/component/NAME/prefix`

Defines the URL prefix which is used on the repository server. This variable is usually not set.

`repository/online/component/NAME/username`

If the repository server requires authentication, the user name can be entered in this variable.

`repository/online/component/NAME/password`

If the repository server requires authentication, the password can be entered in this variable.

`repository/online/component/NAME/version`

This variable controls the versions to include, see Chapter 10 for details.


`repository/online/component/NAME/defaultpackages`

A list of package names separated by blanks. The UMC module *Repository Settings* offers the installation of this component if at least one of the packages is not installed. Specifying the package list eases the subsequent installation of components.

# Chapter 11. Translating UCS

11.1. Univention Management Console translations .....	127
11.1.1. Install needed tools .....	127
11.1.2. Obtain a current checkout of the UCS GIT repository .....	127
11.1.3. Create a new translation package .....	127
11.1.4. Edit translation files .....	128
11.1.5. Update the translation package .....	128
11.1.6. Build the translation package .....	129


## 11.1. Univention Management Console translations

 Feedback 

By default UCS includes English and German localizations. Univention provides a set of tools that facilitates the process of creating translations for Univention Management Console.

This section describes all steps necessary to create a working translation package for UCS. We recommend having a running UCS installation where the tools can be set up in an easy manner. Further more a current GIT checkout of the UCS source code is required.


### 11.1.1. Install needed tools

 Feedback 

The package **univention-ucs-translation-template** contains all tools required to setup and update a translation package. It requires some additional Debian tools to build the package. Run the following command on your UCS to install all needed packages.

```
sudo univention-install univention-ucs-translation-template dpkg-dev git
```


### 11.1.2. Obtain a current checkout of the UCS GIT repository

 Feedback 

The GIT repository is later processed to get initial files for a new translation(often referred to as PO file or Portable Objects).

```
mkdir ~/translation
cd ~/translation
git clone \
  --single-branch --depth 1 --shallow-submodules \
  https://github.com/univention/univention-corporate-server
```

### 11.1.3. Create a new translation package

 Feedback 

To create a new translation package for, e.g., French in the current working directory, the following command must be executed:

```
cd ~/translation
univention-ucs-translation-build-package \
  --source ~/translation/univention-corporate-server \
  --languagecode fr \
  --locale fr_FR.UTF-8:UTF-8 \
  --language-name French
```

This creates a new directory `~/translation/univention-l10n-fr/` which contains a Debian source package of the same name. It includes all source and target files for the translation.

## 11.1.4. Edit translation files

The translation source files (.po files) are located below the directory `~/translation/univention-110n-fr/fr`. Each file should be edited to create the translation.

These files are generated by the package **gettext**. The manual can be found at <https://www.gnu.org/software/gettext/manual/gettext.html>. Translation files created by **gettext** consist of a header and various entries of the form

```
#: umc/app.js:637
#, python-format
msgid "The %s will expire in %d days and should be renewed!"
msgstr ""
```

The first line provides a hint, where the text is used. The second line is optional and contains flags, which indicate the type and state of the translation. The string `fuzzy` indicates an entry, which was copied by **gettext** from a previous version and needs to be updated.

The line starting with `msgid` contains the original text. The translation has to be placed on the line containing `msgstr`. Long texts can be split over multiple lines, where each line must start and end with a double-quote. The following example from the German translation shows a text spanning two lines, with the placeholder present in the original and translated text.

```
#: umc/js/appcenter/AppCenterPage.js:1067
#, python-format
msgid ""
"If everything else went correct and this is just a temporary network "
"problem, you should execute %s as root on that backup system."
msgstr ""
"Wenn keine weiteren Fehler auftraten und dies nur ein temporäres "
"Netzwerkproblem ist, sollten Sie %s als root auf dem Backup System "
"ausführen."
```

Some lines contain parameters, in this example `%s` and `%d`. They are indicated by a flag like `c-format` or `python-format`, which must not be removed. The placeholders have to be carried over to the translated string unmodified and in the same order. Some other files contain placeholders of the form `%{text}s`, which are more flexible and can be reordered.

After a file has been translated completely, the line containing `fuzzy` at the beginning of the entry should be removed to avoid warnings. If a translation string consists of multiple lines the translated string should roughly contain as many lines as the original string.

## 11.1.5. Update the translation package

First update your GIT checkout:

```
cd ~/translation/univention-corporate-server
git pull --rebase
```


If changes affecting translations are made in the GIT repository, existing translation packages need to be updated to reflect those changes. Given a path to an updated GIT checkout, `univention-ucs-translation-merge` can update a previously created translation source package. The following example will update the translation package **univention-110n-fr**:

```
univention-ucs-translation-merge \
    ~/translation/univention-corporate-server \
```



```
~/translation/univention-l10n-fr
```

### 11.1.6. Build the translation package

Feedback 

Before using the new translation, the Debian package has to be built and installed. This can be done with the following commands:

```
cd ~/translation/univention-l10n-fr
sudo apt-get build-dep .
dpkg-buildpackage -uc -us -b -rfakeroot
sudo dpkg -i ../univention-l10n-fr_*.deb
```

After logging out of the Univention Management Console the new language should now be selectable in the Univention Management Console login window. Untranslated strings will be still shown in their original language, i.e. in English.




# Chapter 12. Univention Updater

12.1. Separate repositories .....	131
12.2. Updater scripts .....	131
12.2.1. Digital signature .....	132
12.3. Release update walkthrough .....	132

The Univention Updater is used for updating the software. It is based on the Debian APT tools. On top of that the updater provides some UCS specific additions.

## 12.1. Separate repositories

Feedback 


UCS releases are provided either via DVD images or via online repositories. For each major, minor and patch-level release there is a separate online repository. They are automatically added to the files in `/etc/apt/sources.list.d/` depending on the Univention Configuration Registry variables `version/version` and `version/patchlevel`, which are managed by the updater.

Separate repositories are used to prevent automatic updates of software packages. This is done to encouraged users to thoroughly test a new release before their systems are updated. The only exception from this rule are the *errata* updates, which are put into a single repository, which is updated incrementally.

Therefore the updater will include the repositories of a new release in a file called `/etc/apt/sources.list.d/00_ucs_temporary_errata_components_update.list` and then do the updates. Only at the end of a successful update are the Univention Configuration Registry variables updated.

Additional components can be added as separate repositories using Univention Configuration Registry variables `repository/online/component/...`, which are described in *????* manual. Setting the variable `.../version=current` can be used to mark a component as required, which blocks an upgrade until the component is available for the new release.

## 12.2. Updater scripts

Feedback 

In addition to the regular Debian Maintainer Scripts (see Section B.3.5) the UCS updater supports additional scripts, which are called before and after each release update. Each UCS release and each component can include its own set of scripts.

```
preup.sh
```

These scripts is called before the update is started. If any of the scripts aborts with an exit value unequal zero, the update is canceled and never started. The scripts receives the version number of the next release as an command line argument.

For components their `preup.sh` scripts is called twice: Once before the main release `preup.sh` script is called and once more after the main script was called. This is indicated by the additional command line argument `pre` respectively `post`, which is *inserted before* the version string.


```
postup.sh
```

These scripts is called after the update successfully completed. If any of the scripts aborts with an exit value unequal zero, the update is canceled and does not finish successfully. The scripts receives the same arguments as described above.

The scripts are located in the `all/` component of each release and component. For UCS-4.4 this would be `4.4/maintained/4.4-0/all/preup.sh` and `4.4/maintained/components/some-com-`

`ponent/all/preup.sh` for the `preup.sh` script. The same applies to the `postup.sh` script. The full process is shown in Procedure 12.1.

## 12.2.1. Digital signature


Feedback 

From UCS 3.2 on the scripts must be digitally signed by an PGP (Pretty Good Privacy) key stored in the keyring of `apt-key(8)`. The detached signature must be placed in a separate file next to each updater scripts with the additional file name extension `.gpg`, that is `preup.sh.gpg` and `postup.sh.gpg`. These extra files are downloaded as well and any error in doing so and in the validation process aborts the updater immediately.

The signatures must be updated after each change to the underlying scripts. This can be automated or be done manually with a command like the following: `gpg -a -u key-id --passphrase-file keyphrase-file -o script.sh.gpg -b script.sh`

Signatures can be checked manually using the following command: `apt-key verify script.sh.gpg script.sh`

## 12.3. Release update walkthrough

Feedback 

For an release update the following steps are performed. It assumes a single component is enabled. If multiple components are enabled, the order in which their scripts are called is unspecified. It shows which scripts are called in which order with which arguments.

### Procedure 12.1. Update process steps


1. Create temporary source list file `00_ucs_temporary_errata__components_update.list`
2. Download the `preup.sh` and `postup.sh` files for the next release and all components into a temporary directory and validate their PGP signatures
3. Execute `component-preup.sh pre $version`
4. Execute `release-preup.sh $version`
5. Execute `component-preup.sh post $version`
6. Download the new `Packages` and `Release` files. Their PGP signatures validated by APT internally.
7. Perform the update
8. Set the release related Univention Configuration Registry variables to the new version
9. Execute `component-postup.sh pre $version`
10. Execute `release-postup.sh $version`
11. Execute `component-postup.sh post $version`

# Chapter 13. Single Sign-On: Integrating a service provider into UCS

13.1. Register new service provider via udm .....	133
13.2. Get information required by the service provider .....	133
13.3. Add direct login link to the UCS Portal page .....	134

UCS provides *Single Sign-On* functionality with a SAML 2.0 compatible identity provider based on *simple-samlphp*. The identity provider is by default installed on the DC Master and all DC Backup servers. A DNS Record for all systems providing *Single Sign-On* services is registered for failover, usually `ucs-sso.domainname`. Clients are required to be able to resolve the *Single Sign-On* DNS name.


## 13.1. Register new service provider via udm

Feedback 

New service providers can be registered by using the Univention Directory Manager module `saml/serviceprovider`. To create a new service provider entry in a *joinscript*, see the following example:

```
eval "$(ucr shell)"
udm saml/serviceprovider create "$@" \
  --ignore_exists \
  --position "cn=saml-serviceprovider,cn=univention,$ldap_base" \
  --set isActivated=TRUE \
  --set Identifier="MyServiceProviderIdentifier" \
  --set NameIDFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" \
  --set simplesamlAttributes="false" \
  --set AssertionConsumerService="https://$hostname.$domainname/sso-login-page" \
  --set simplesamlNameIDAttribute="uid" \
  --set privacyPolicyURL="https://example.com/policy.html" \
  --set serviceProviderOrganizationName="My Service Name" \
  --set serviceproviderdescription="A long description shown to the user on the Single Sign-On page." || die
```

## 13.2. Get information required by the service provider

Feedback 

The service provider usually requires at least a public certificate or XML metadata about the identity provider. The certificate can e.g. be downloaded with the following call:

```
eval "$(ucr shell)"
wget --ca-certificate /etc/univention/ssl/ucsCA/CAcert.pem \
  https://"${ucs_server_sso_fqdn:-ucs-sso.$domainname}"/simplesamlphp/saml2/idp/certificate \
  -O /etc/idp.cert
```

The XML metadata is available e.g. from

```
eval "$(ucr shell)"
wget --ca-certificate /etc/univention/ssl/ucsCA/CAcert.pem \
  https://"${ucs_server_sso_fqdn:-ucs-sso.$domainname}"/simplesamlphp/saml2/idp/metadata.php \
  -O /etc/idp.metadata
```

Add direct login link to the UCS Portal page

The *Single Sign-On* Login page to be configured in the service provider is `https://ucs-sso.domain-name/simplesamlphp/saml2/idp/SSOService.php`

### 13.3. Add direct login link to the *UCS Portal* page

Feedback 

To provide users with a convenient link to an identity provider initiated login, the following ucr command may be used


```
fqdn="ucs-sso.domainname"
myspi="MyServiceProviderIdentifier"
ucr set ucs/web/overview/entries/service/SP/description="External
Service Login" \
ucs/web/overview/entries/service/SP/label="External Service SSO" \
ucs/web/overview/entries/service/SP/link="https://$fqdn/simplesamlphp/
saml2/idp/SSOService.php?spentityid=$myspi" \
ucs/web/overview/entries/service/SP/description/de="Externer Dienst
Login" \
ucs/web/overview/entries/service/SP/label/de="Externer Dienst SSO" \
ucs/web/overview/entries/service/SP/priority=50
```

Where `MyServiceProviderIdentifier` is the identifier used when creating the UDM service provider object.

# Chapter 14. Miscellaneous


14.1. Databases .....	135
14.1.1. PostgreSQL .....	135
14.1.2. MySQL .....	135
14.2. UCS lint .....	135
14.3. Function Libraries .....	137
14.3.1. <i>shell-univention-lib</i> .....	137
14.3.2. <i>python-univention-lib</i> .....	138
14.4. Login Access Control .....	139
14.5. Network Packet Filter .....	139
14.5.1. Filter rules by Univention Configuration Registry .....	139
14.5.2. Local filter rules via iptables commands .....	140
14.5.3. Testing Univention Firewall settings .....	140
14.6. Active Directory Connection custom mappings .....	141

## 14.1. Databases

Feedback 


UCS ships with two major database management systems, which are used for UCS internal purposes, but can also be used for custom additions.

### 14.1.1. PostgreSQL

Feedback 


UCS uses PostgreSQL by default for its package tracking database, which collects the state and versions of packages installed on all systems of the domain.

### 14.1.2. MySQL

Feedback 

By default the MySQL root password is set to \_\_\_\_\_. Debian provides the *dbconfig* package, which can be used to create and modify additional databases from maintainer scripts.

## 14.2. UCS lint

Feedback 

Use *ucslint* to find packaging mistakes. Called best from *debian/rules*, needs build dependency on *ucslint*.

```
override_dh_auto_test:
    dh_auto_test
    ucslint
```

For each issue, *ucslint* prints one line, which line contains several fields separated by ::

```
severity:module-id-test-id[:filename[:line-number[:column-
number]]]:message
```

For some issues extra context data is printed on the following lines, which are indented with space characters. All other lines start with a letter specifying the severity:

E

Error: Missing data, conflicting information, real bugs.

W

Warning: Possible bug, but might be okay in some situations.

## I

Informational: found some issue, which needs further investigation.

## S

Style: There might be some better less error prone way.

The severities are ordered by importance. By default `ucslint` only aborts on errors, but this can be overwritten using the `--exitcode-categories` argument followed by a subset of the characters `EWIS`.

After the severity an identifier follows, which uniquely identifies the module and the test. The module is given as four digits, which is followed by a dash and the number of the test in that module. Currently the following modules exist:

## 0001-CheckJoinScript

Checks join file issues

## 0002-CopyPasteErrors

Checks for copy&paste error from example files

## 0004-CheckUCR

Checks UCR info files

## 0006-CheckPostinst

Checks Debian maintainer scripts

## 0007-Changelog

Checks `debian/changelog` file for conformance with Univention rules

## 0008-Translations

Checks translation files for completeness and errors

## 0009-Python

Checks Python files for common errors

## 0010-Copyright

Checks for Univention copyright

## 0011-Control

Checks `debian/control` file for errors

## 0013-bashism

Checks files using `/bin/sh` for BASH constructs

## 0014-Depends

Checks files for missing runtime dependencies on UCS packages



0015-FuzzyNames

Checks for mis-spellings of *Univention*

0016-Deprecated

Checks files for usage of deprecated functions


0017-Shell

Checks shell scripts for quoting errors

The module and test number may be optionally followed by a file name, line number in that file, and column number in that line, where the issue was found. After that a message is printed, which describes the issue in more detail.


Since `ucslint` is very Univention centric, many of its tests return false positives for software packages by other parties. Therefore many tests need to be disabled. For that a file `debian/ucslint.overrides` can be created with list of modules and test, which should be ignored. Without specifying the optional filename, line number and column number, the test is globally disabled for all files.

## 14.3. Function Libraries

Feedback 

The source package *univention-lib* provides two binary packages *shell-univention-lib* and *python-univention-lib*, which contain common library functions usable in shell or Python programs.

### 14.3.1. *shell-univention-lib*

Feedback 

This package provides several libraries in `/usr/share/univention-lib/`, which can be used in shell scripts.

```
/usr/share/univention-lib/admember.sh
```

This file contains some helpers to test for and to manage hosts in AD member mode.

```
/usr/share/univention-lib/base.sh
```

This file contains some helpers to create log files, handle unjoin scripts (see Section 3.5) or query the network configuration.

```
/usr/share/univention-lib/ldap.sh
```

This file contains some helpers to query data from LDAP, register and unregister service entries, LDAP schema and LDAP ACL extensions.

```
/usr/share/univention-lib/samba.sh
```

This file contains a helper to check if Samba4 is used.

```
/usr/share/univention-lib/ucr.sh
```

This file contains some helpers to handle boolean Univention Configuration Registry variables and handle UCR files on package removal.


```
/usr/share/univention-lib/umc.sh
```

This file contains some helpers to handle UMC (see Chapter 7) related tasks.

```
/usr/share/univention-lib/all.sh
```

This is a convenient library, which just includes all libraries mentioned above.

### 14.3.2. *python-univention-lib*

Feedback 

This package provides several Python libraries located in the module *univention.lib*.

#### *univention.lib.admember*

This module contains functions to test for and to manage hosts in AD member mode.

#### *univention.lib.atjobs*

This module contains functions to handle at-jobs.

#### *univention.lib.error*

This module provides the function `formatTraceback`, which returns the full stack trace for an exception.

#### *univention.lib.fstab*

This module provides some functions for handling the file `/etc/fstab`.

```
python -m univention.lib.getMailFromMailOrUid { uid | email }
```

This program returns the distinguished name of the user, which either matches the user identifier or email address given to the command as an argument.

#### *univention.lib.i18n*

This module provides some classes to handle texts and their translations.

#### *univention.lib.ldap\_extension*

This module provides some helper functions internally used to register LDAP extension as described in Section 3.4.3.2.

#### *univention.lib.listenerSharePath*

This module provides some helper functions internally used by the Directory Listener module handling file shares.

#### *univention.lib.locking*

This module provides some functions to implement mutual exclusion using file objects as locking objects.

#### *univention.lib.misc*

This module provides miscellaneous functions to query the set of configured LDAP servers, localized domain user names, and other functions.

#### *univention.lib.package\_manager*

This module provides some wrappers for `dpkg` and `APT`, which add functions for progress reporting.

#### *univention.lib.s4*

This module provides some well known SIDs and RIDs.

### *univention.lib.shell*

This module provides two functions for escaping shell command line arguments and creating at jobs.

### *univention.lib.ucrLogrotate*

This module provides some helper functions internally used for parsing the Univention Configuration Registry variables related to logrotate(8).

### *univention.lib.ucs*

This module provides the class `UCS_Version` to more easily handle UCS version strings.

### *univention.lib.umc*

This module provides the class `Client` to handle connections to remote UMC servers.


### *univention.lib.umc\_module*

This module provides some functions for handling icons.

### *univention.lib.urllib2\_ssl*


This module provides a pack-port of *urllib2* from Python-3.3, which implements proper certificate checking.

## 14.4. Login Access Control

 Feedback 


Access control to services can be configured for individual services by setting certain Univention Configuration Registry variables. Setting `auth/SERVICE/restrict` to `true` enables access control for that service. This will include the file `/etc/security/access-SERVICE.conf`, which contains the list of allowed users and groups permitted to login to the service. Users and groups can be added to that file by setting `auth/SERVICE/user/USER` and `auth/SERVICE/group/GROUP` to `true` respectively.

## 14.5. Network Packet Filter

 Feedback 

Firewall rules are setup by *univention-firewall* and can be configured through Univention Configuration Registry or by providing additional UCR templates.

### 14.5.1. Filter rules by Univention Configuration Registry

 Feedback 

Besides predefined service definitions, Univention Firewall also allows the implementation of package filter rules via Univention Configuration Registry. These rules are included in `/etc/security/packetfilter.d/` via a Univention Configuration Registry module.

Filter rules can be provided via packages or can be configured locally by the administrator. Local rules have a higher priority and overwrite rules provided by packages.

All Univention Configuration Registry settings for filter rules are entered in the following format:

Local filter rule

```
security/packetfilter/protocol/port(s)/address=policy
```

Package filter rule

```
security/packetfilter/package/package/protocol/port(s)/address=policy
```

## Local filter rules via iptables commands

The following values need to be filled in:

*package* (only for packaged rules)

The name of the package providing the rule.

*protocol*

Can be either `tcp` for server services using the *Transmission Control Protocol* or `udp` for services using the stateless *User Datagram Protocol*.

*port*,

*min-port:max-port*

Ports can be defined either as a single number between 1 and 65535 or as a range separated by a colon:

*min-port:max-port*

*address*

This can be either `ipv4` for all IPv4 addresses, `ipv6` for all IPv6 addresses, `all` for both IPv4 and IPv6 addresses, or any explicitly specified IPv4 or IPv6 address.

*policy*

If a rule is registered as `DROP`, then packets to this port will be silently discarded; `REJECT` can be used to send back an ICMP message `port unreachable` instead. Using `ACCEPT` explicitly allows such packets. (IPTables rules are executed until one rule applies; thus, if a package is accepted by a rule which is discarded by a later rule, then the rule for discarding the package does not become valid).

Filter rules can optionally be described by setting additional Univention Configuration Registry variables. For each rule and language, an additional variable suffixed by “/ *language*” can be used to add a descriptive text.

Some examples:

### Example 14.1. Local firewall rule

```
security/packetfilter/tcp/2000/all=DROP
security/packetfilter/tcp/2000/all/en=Drop all packets to TCP port 2000
security/packetfilter/udp/500:600/all=ACCEPT
security/packetfilter/udp/500:600/all/en=Accept UDP port 500 to 600
```

All package rules can be globally disabled by setting the Univention Configuration Registry variable `security/packetfilter/use_packages` to `false`.


## 14.5.2. Local filter rules via iptables commands

Feedback 

Besides the existing possibilities for settings via Univention Configuration Registry, there is also the possibility of integrating user-defined enhanced configurations in `/etc/security/packetfilter.d/`, e.g. for realizing a firewall or *Network Address Translation*. The enhancements should be realized in the form of shell scripts which execute the corresponding `iptables` for IPv4 and `ip6table` for IPv6 calls. For packages this is best done through using a Univention Configuration Registry template as described in Section 2.2.1.1.

Full documentation for IPTables can be found at <http://www.netfilter.org/>.

## 14.5.3. Testing Univention Firewall settings

Feedback 

Package filter settings should always be thoroughly tested. The network scanner `nmap`, which is integrated in Univention Corporate Server as a standard feature, can be used for testing the status of individual ports.


Since Nmap requires elevated privileges in the network stack, it should be started as `root` user. A TCP port can be tested with the following command: `nmap HOSTNAME -p PORT(S)`

A UDP port can be tested with the following command: `nmap HOSTNAME -sU -p PORT(S)`

### Example 14.2. Using `nmap` for firewall port testing

```
nmap 192.0.2.100 -p 400
nmap 192.0.2.110 -sU -p 400-500
```

## 14.6. Active Directory Connection custom mappings

Feedback 

For general overview about the *Active Directory Connection* app, see *Active Directory Connection*<sup>1</sup>.

It is also possible to modify and append custom mappings. For that to work a file has to be created named `/etc/univention/connector/ad/localmapping.py`. Within that file the following function should be implemented:

```
def mapping_hook(ad_mapping):
    return ad_mapping
```

The contents of the `ad_mapping` variable can be modified to influence the mapping.

---

<sup>1</sup> <https://docs.software-univention.de/manual-4.4.html#ad-connector:general>



# Appendix A. Bug reporting

UCS is neither error free nor feature complete. Issues are tracked using Bugzilla at <https://forge.univention.org/bugzilla/>.

Create an account.

Search for existing entries before opening new reports.

Include the version info: `ucr search --brief ^version/`.

Provide enough information to help us reproduce the bug.

Search <https://help.univention.com/c/knowledge-base/supported/>

Search <https://wiki.univention.de/>

Search <https://help.univention.com/> and ask for help. In addition to our support team many of our partners are also present there. Your questions might also help other users while you may profit from issues already solved for other users.





# Appendix B. Debian packaging

This chapter describes how software for Univention Corporate Server is packaged in the Debian format. It allows proper dependency handling and guarantees proper tracking of file ownership. Customers can package their own internal software or use the package mechanism to distribute configuration files consistently to different machines.

Software is packaged as a *source package*, from which one or more *binary packages* can be created. This is useful to create different packages from the same source package. For example the Samba source package creates multiple binary packages: one containing the file server, one containing the client commands to access the server, and several other packages containing documentation, libraries, and common files shared between those packages. The directory should be named *package\_name-version*.

## B.1. Prerequisites and preparation

Feedback 

Some packages are required for creating and building packages.

### *build-essential*

This meta package depends on several other packages like compilers and tools to extract and build source packages. Packages must not declare an explicit dependency on this and its dependent packages.

### *devscripts*


This package contains additional scripts to modify source package files like for example `debian/changelog`.

### *dh-make*

This program helps to create an initial `debian/` directory, which can be used as a starting point for packaging new software.

These packages must be installed on the development system. For this the *unmaintained* repository must be enabled. After this the missing packages can be installed on the command line using `univention-install` or through UMC, which is described in the [ucs-handbuch].

## B.2. `dh_make`

Feedback 

`dh_make` is a tool, which helps creating the initial `debian/` directory. It is interactive by default and asks several questions about the package to be created.

```
Type of package: single binary, indep binary, multiple binary, library,
kernel module, kernel patch?
[s/i/m/l/k/n]
```

**s**, single binary

A single architecture specific binary package is created from the source package. This is for software which needs to be compiled individually for different CPU architectures like `i386` and `amd64`.

**i**, indep binary

A single architecture-independent binary package is created from the source package. This is for software which runs unmodified on all CPU architectures.

**m**, multiple binary

Multiple binary package are created from the source package, which can be both architecture independent and dependent.

**l**, library

Two or more binary packages are created for a compiled library package. The runtime package consists of the shared object file, which is required for running programs using that library. The development package contains the header files and other files, which are only needed when compiling and linking programs on a development system.

**k**, kernel module

A single kernel-dependent binary package is created from the source package. Kernel modules need to be compiled for each kernel flavor. *dkms* should probably be used instead. This type of packages is not described in this manual.

**n**, kernel patch

A single kernel-independent package is created from the source package, which contains a patch to be applied against an unpacked Linux kernel source tree. *dkms* should probably be used instead. This type of packages is not described in this manual.

In Debian a package normally consists of an upstream software archive, which is provided by a third party like the Samba team. This collection is extended by a Debian specific second TAR archive or a patch file, which adds the `debian/` directory and might also modify upstream files for better integration into a Debian system.

When a source package is built, `dpkg-source(1)` separates the files belonging to the packaging process from files belonging to the upstream package. For this to work, `dpkg-source` needs the original source either provided as a TAR archive or a separate directory containing the unpacked source. If neither of these is found and `--native` is not given, `dh_make` prints the following warning:

```
Could not find my-package_1.0.orig.tar.gz
Either specify an alternate file to use with -f,
or add --createorig to create one.
```

The warning from `dh_make` states that no pristine upstream archive was found, which prohibits the creation of the Debian specific patch, since the Debian packaging tools have no way to separate upstream files from files specific to Debian packaging. The option `--createorig` can be passed to `dh_make` to create a `.orig.tar.gz` archive before creating the `debian/` directory, if such separation is required.

## B.3. Debian control files

Feedback 

The control files in the `debian/` directory control the package creation process. The following sections provide a short description of these files. A more detailed description is available in the [Debian FAQ].

Several files will have the `.ex` suffix, which mark them as examples. To activate these files, they must be renamed by stripping this suffix. Otherwise the files should be deleted to not clutter up the directory by unused files. In case a file was deleted and needs to be restored, the original templates can be found in the `/usr/share/debhelper/dh_make/debian/` directory.

The `debian/` directory contains some global configuration files, which can be put into two categories: The files `changelog`, `control`, `copyright`, `rules` are required and control the build process of all binary packages. Most other files are optional and only affect a single binary package. Their filename is prefixed with the name of the binary package,<sup>1</sup>

<sup>1</sup> If only a single binary package is build from the source package, this prefix can be skipped, but it is good practice to always use the prefix.

The following files are required:

`changelog`

Changes related to packaging, not the upstream package. See Section B.3.3 below for more information.

`compat`

The Debhelper tools support different compatibility levels. For UCS-3.x the file must contain a single line with the value 7. See `debhelper(7)` for more details.

`control`

Contains control information about the source and all its binary packages. This mostly includes package name and dependency information. See Section B.3.1 below for more information.

`copyright`

This file contains the copyright and license information for all files contained in the package. See Section B.3.2 below for more information.

`rules`

This is a Makefile style file, which controls the package build process. See Section B.3.4 below for more information.

`source/format`

This file configures how `dpkg-source(1)` separates the files belonging to the packaging process from files belonging to the upstream package. Historically the Debian source format 1.0 shipped packages as a TAR file containing the upstream source plus one patch file, which contained all files of the `debian/` sub-directory in addition to all changes to upstream files.

The new format 3.0 (`quilt`) replaces the patch file with a second TAR archive containing the `debian/` directory. Changes to upstream files are no longer applied as one giant patch, but split into logical changes and applied using a built-in `quilt(1)`.

For simple packages, where there is no distinction between upstream and the packaging entity, the 3.0 (`native`) format can be used instead, where all files including the `debian/` directory are contained in a single TAR file.

The following files are optional and should be deleted if unused, which helps other developers to concentrate on only the files relevant to the packaging process:

`README.Debian`

Notes regarding package specific changes and differences to default options, for example compiler options. Will be installed into `/usr/share/doc/package_name/README.Debian`.

`package.cron.d`

Cron tab entries to be installed. See `dh_installcron(1)` for more details.

`package.dirs`

List of extra directories to be created. See `dh_installdirs(1)` for more details.<sup>2</sup>

---

<sup>2</sup> May other `dh_` tools automatically create directories themselves, so in most cases this file is unneeded.

`package.install`

List of files and directories to be copied into the package. This is normally used to partition all files to be installed into separate packages, but can also be used to install arbitrary files into packages. See `dh_install(1)` for more details.

`package.docs`

List of documentation files to be installed in `/usr/share/doc/package/`. See `dh_installdocs(1)` for more details.

`package.emacsen-install`,  
`package.emacsen-remove`,  
`package.emacsen-startup`

Emacs specific files to be installed below `/usr/share/emacs-common/package/`. See `dh_installemacsen(1)` for more details.

`package.doc-base*`

Control files to install and register extended HTML and PDF documentation. See `dh_installdocs(1)` for more details.

`package.init.d`,  
`package.default`

Start-/stop script to manage a system daemon or service. See `dh_installinit(1)` for more details.

`package.manpage.1`,  
`package.manpage.sgml`

Manual page for programs, library functions or file formats, either directly in troff or SGML. See `dh_installman(1)` for more details.

`package.menu`

Control file to register programs with the Debian menu system. See `dh_installmenu(1)` for more details.

`watch`

Control file to specify the download location of this upstream package. This can be used to check for new software versions. See `uscan(1)` for more details.

`package.preinst`,  
`package.postinst`,  
`package.prerm`,  
`package.postrm`

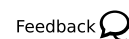
Scripts to be executed before and after package installation and removal. See Section B.3.5 below for more information.

`package.maintscript`

Control file to simplify the handling of *conffiles*. See `dpkg-maintscript-helper(1)` and `dh_installdeb(1)` for more information.

Other debhelper programs use additional files, which are described in the respective manual pages.

## B.3.1. debian/control



The control file contains information about the packages and their dependencies, which is needed by dpkg. The initial control file created by dh\_make looks like this:

```
Source: testdeb
Section: unknown
Priority: optional
Maintainer: John Doe <user@example.com>
Build-Depends: debhelper (>= 5.0.0)
Standards-Version: 3.7.2

Package: testdeb
Architecture: any
Depends: ${shlibs:Depends}, ${misc:Depends}
Description: <insert up to 60 chars description>
<insert long description, indented with spaces>
```

The first block beginning with Source describes the source package:

### Source

The name of the source package. Must be consistent with the directory name of the package and the information in the changelog file.

### Section<sup>3</sup>

A category name, which is used to group packages. There are many predefined categories like libs, editors, mail, but any other string can be used to define a custom group.

### Priority<sup>4</sup>

Defines the priority of the package. This information is only used by some tools to create installation DVD. More important packages are put on earlier CD, while less important packages are put on later CD.

#### essential

Packages are installed by default and dpkg prevents the user from easily removing it.

#### required

Packages which are necessary for the proper functioning of the system. The package is part of the base installation.

#### important

Important programs, including those which one would expect to find on any Unix-like system. The package is part of the base installation.

#### standard

These packages provide a reasonably small but not too limited character-mode system.

#### optional

Package is not installed by default. This level is recommended for most packages.

<sup>3</sup> <http://www.debian.org/doc/debian-policy/ch-archive.html#s-subsections>

<sup>4</sup> <http://www.debian.org/doc/debian-policy/ch-archive.html#s-priorities>

extra

This contains all packages that conflict with some other packages.

Maintainer

The name and email address of a person or group responsible for the packaging.

Build-Depends,  
Build-Depends-Indep

A list of packages which are required for building the package.

Standards-version

Specifies the Debian Packaging Standards version, which this package is conforming to. This is not used by UCS, but required by Debian.

All further blocks beginning with `Package` describes a binary package. For each binary package one block is required.

Package

The name of the binary package. The name must only consist of lower case letters, digits and dashes. If only a single binary package is build from a source package, the name is usually the same as the source package name.

Architecture

Basically there are two types of packages: Architecture dependent packages must be build for each architecture like `i386` and `amd64`, since binaries created on one architecture do not run on other architectures. A list of architectures can be explicitly given, or `any` can be used, which is then automatically replaced by the architecture of the system where the package is built.

Architecture independent packages only need to be built once, but can be installed on all architectures. Examples are documentation, scripts and graphics files. They are declared using `all` in the architecture field.

Description

The first line should contain a short description of up to 60 characters, which should describe the purpose of the package sufficiently. A longer description can be given after that, where each line is indented by a single space. An empty line can be inserted by putting a single dot after the leading space.

Most packages are not self-contained but need other packages for proper function. Debian supports different kinds of dependencies.

Depends

A essential dependency on some other packages, which must be already installed and configured before this package is configured.

Recommends

A strong dependency on some other packages, which should normally be co-installed with this package, but can be removed. This is useful for additional software like plug-ins, which extends the functionality of this package, but is not strictly required.

### Suggests

A soft dependency on some other packages, which are not installed by default. This is useful for additional software like large add-on packages and documentation, which extends the functionality of this package, but is not strictly required.

### Pre-Depends

A strong dependency on some other package, which must be fully operational even before this package is unpacked. This kind of dependency should be used very sparsely. It's mostly only required for software called from the `.preinst` script.

### Conflicts

A negative dependency, which prevents the package to be installed while the other package is already installed. This should be used for packages, which contain the same files or use the same resources, for example TCP port numbers.

### Provides

This package declares, that it provides the functionality of some other package and can be considered as a replacement for that package.

### Replaces

A declaration, that this package overwrites the files contained in some other package. This deactivates the check normally done by `dpkg` to prevent packages from overwriting files belonging to some other package.

### Breaks

A negative dependency, which requests the other package to be upgraded before this package can be installed. This is a lesser form of `Conflicts`. `Breaks` is almost always used with a version specification in the form `Breaks: package (< version)`: This forces *package* to be upgraded to a version greater than *version* before this package is installed.

In addition to literal package names, debhelper supports a substitution mechanism: Several helper scripts are capable of automatically detecting dependencies, which are stored in variables.

`${shlibs:Depends}`

`dh_shlibdeps` automatically determines the shared library used by the programs and libraries of the package and stores the package names providing them in this variable.

`${python:Depends}`

`dh_python` detects similar dependencies for Python modules.

`${misc:Depends}`

Several Debhelper commands automatically add additional dependencies, which are stored in this variable.

In addition to specifying a single package as a dependency, multiple packages can be separated by using the pipe symbol (`|`). At least one of those packages must be installed to satisfy the dependency. If none of them is installed, the first package is chosen as the default.

A package name can be followed by a version constraint enclosed in parenthesis. The following operators are valid:

&lt;&lt;

is less than

&lt;=

is less than or equal to

=

is equal to

&gt;=

is greater than or equal to


&gt;&gt;

is greater than

An Example:

```
Depends: libexample1 (>= ${binary:Version}),
        exim4 | mail-transport-agent,
        ${shlibs:Depends}, ${misc:Depends}
Conflicts: libgg0, libggil
Recommends: libncurses5 (> 5.3)
Suggests: libgii0-target-x (= 1:0.8.5-2)
Replaces: vim-python (< 6.0), vim-tcl (<= 6.0)
Provides: www-browser, news-reader
```

### B.3.2. debian/copyright

Feedback 

The copyright file contains copyright and license information. For a downloaded source package it should include the download location and names of upstream authors.

```
This package was debianized by John Doe <max@example.com> on
Mon, 21 Mar 2009 13:46:39 +0100.
```

```
It was downloaded from <fill in ftp site>
```

```
Copyright:
```

```
Upstream Author(s): <put author(s) name and email here>
```

```
License:
```

```
<Must follow here>
```

The file does not require any specific format. Debian now recommends to use a machine-readable format, but this is not required for UCS. The format is described in <http://dep.debian.net/deps/dep5/> at looks like this:

```
Format: http://www.debian.org/doc/packaging-manuals/copyright-
format/1.0/
Upstream-Name: Univention GmbH
Upstream-Contact: <package@univention.de>
Source: https://docs.software-univention.de/

Files: *
```



Copyright: 2013-2022 Univention GmbH  
License: AGPL

### B.3.3. debian/changelog

Feedback 

The changelog file documents the changes applied to this Debian package. The initial file created by `dh_make` only contains a single entry and looks like this:

```
testdeb (0.1-1) unstable; urgency=low

* Initial Release.

-- John Doe <user@example.com> Mon, 21 Mar 2013 13:46:39 +0100
```

For each new package release a new entry must be prepended before all previous entries. The version number needs to be incremented and a descriptive text should be added to describe the change.

The command `debchange` from the *devscripts* package can be used for editing the changelog file. For example the following command adds a new version:

```
dch -i
```

After that the changelog file should look like this:

```
testdeb (0.1-2) unstable; urgency=low

* Add more details.

-- John Doe <user@example.com> Mon, 21 Mar 2013 17:55:47 +0100

testdeb (0.1-1) unstable; urgency=low


* Initial Release.

-- John Doe <user@example.com> Mon, 21 Mar 2013 13:46:39 +0100
```

The date and time stamp must follow the format described in RFC 2822<sup>4</sup>. `debchange` automatically inserts and updates the current date. Alternatively `date -R` can be used on the command line to create the correct format.

For UCS it is best practice to mention the bug ID of the UCS bug tracker (see Appendix A) to reference additional details of the bug fixed. Other parties are encouraged to devise similar comments, e.g. URLs to other bug tracking systems.

### B.3.4. debian/rules

Feedback 

The file `rules` describes the commands needed to build the package. It must use the Make syntax `[make]`. It consists of several rules, which have the following structure:

```
target: dependencies
command
...
```

Each rule starts with the target name, which can be a file name or symbolic name. Debian requires the following targets:

<sup>4</sup> <http://tools.ietf.org/html/rfc2822>

clean

This rule must remove all temporary files created during package build and must return the state of all files back to the same state as when the package is freshly extracted.

build,  
build-arch,  
build-indep

These rules should configure the package and build either all, all architecture dependent or all architecture independent files. These rules are called without root permissions.

binary,  
binary-arch,  
binary-indep

These rules should install the package into a temporary staging area. By default this is the directory `debian/tmp/` below the source package root directory. From there files are distributed to individual packages, which are created as the result of these rules. These rules are called with root permissions.

Each command line must be indented with one tabulator character. Each command is executed in a separate shell, but long command lines can be split over consecutive lines by terminating each line with a backslash (`\`).

Each rule describes a dependency between the target and its dependencies. `make` considers a target to be out-of-date, when a file with that name `target` does not exist or when the file is older than one of the files it depends on. In that case `make` invokes the given commands to re-create the target.

In addition to file names also any other word can be used for target names and in dependencies. This is most often used to define “phony” targets, which can be given on the command line invocation to trigger some tasks. The above mentioned `clean`, `build` and `binary` targets are examples for that kind of targets.

`dh_make` only creates a template for the rules file. The initial content looks like this:

```
#!/usr/bin/make -f
# -*- makefile -*-
# Sample debian/rules that uses debhelper.
# This file was originally written by Joey Hess and Craig Small.
# As a special exception, when this file is copied by dh-make into a
# dh-make output file, you may use that output file without restriction.
# This special exception was added by Craig Small in version 0.37 of dh-
# make.

# Uncomment this to turn on verbose mode.
#export DH_VERBOSE=1

%:
dh $@
```

Since UCS-3.0 the `debian/rules` file is greatly simplified by using the `dh` sequencer. It is a wrapper around all the different debhelper tools, which are automatically called in the right order.

## Tip

To exactly see which commands are executed when `dpkg-buildpackage` builds a package, invoke `dh target --no-act` by hand, for example `dh binary --no-act` lists all commands to configure, build, install and create the package.

In most cases it's sufficient to just provide additional configuration files for the individual debhelper commands as described in Section B.3. If this is not sufficient, any debhelper command can be individually overridden by adding an *override* target to the rules file. For example the following snippet disables the automatic detection of the build system used to build the package and passes additional options:

```
override_dh_auto_configure:
./setup --prefix=/usr --with-option-foo
```

Without that explicit override `dh_auto_configure` would be called, which normally automatically detects several build systems like `cmake`, `setup.py`, `autoconf` and others. For these `dh` also passes the right options to configure the default prefix `/usr` and use the right compiler flags.

After configuration the package is built and installed to the temporary staging area in `debian/tmp/`. From there `dh_install` partitions individual files and directories to binary packages. This is controlled through the `debian/package.install` files.

This file can also be used for simple packages, where no build system is used. If a path given in the `debian/package.install` file is not found below `debian/tmp/`, the path is interpreted as relative to the source package root directory. This mechanism is sufficient to install simple files, but fails when files must be renamed or file permissions must be modified.

### B.3.5. `debian/preinst`, `debian/prerm`, `debian/postinst`, `debian/postrm` Feedback

In addition to distributing only files packages can also be used to run arbitrary commands on installation, upgrades or removal. This is handled by the four “Maintainer scripts”, which are called before and after files are unpacked or removed:

`debian/package.preinst`

called before files are unpacked.

`debian/package.postinst`

called after files are unpacked. Mostly used to (re-)start services after package installation or upgrades.

`debian/package.prerm`

called before files are removed. Mostly used to stop services before a package is removed or upgraded.

`debian/package.postrm`

called after files have been removed.

The scripts themselves must be shell scripts, which should contain a `#DEBHELPER#` marker, where the shell script fragments created by the `dh_` programs are inserted. Each script is invoked with several parameters, from which the script can determine, if the package is freshly installed, upgraded from a previous version, or removed. The exact arguments are described in the template files generated by `dh_make`.


The maintainer scripts can be called multiple times, especially when errors occur. Because of that the scripts should be idempotent, that is they should be written to “achieve a consistent state” instead of blindly doing the same sequence of commands again and again. A bad example would be to append some lines to a file on each invocation. The right approach would be to add a check, if that line was already added and only do it otherwise.

#### Warning

It is important that these scripts handle error conditions properly: Maintainer scripts should terminate with `exit 0` on success and `exit 1` on fail, if things go catastrophically wrong.

On the other hand an exit code unequal to zero usually aborts any package installation, upgrade or removal process. This prevents any automatic package maintenance and usually requires manual intervention of a human administrator. Therefore it is essential that maintainer scripts handle error conditions properly and are able to recover an inconsistent state.

## B.4. Building

Feedback 

Before the first build is started, remove all unused files from the `debian/` directory. This simplifies maintenance of the package and helps other maintainers to concentrate on only the relevant differences from standard packages.


The build process is started by invoking the following command:

```
dpkg-buildpackage -us -uc
```

The options `-us` and `-uc` disable the PGP signing process of the source and changes files. This is only needed for Debian packages, where all files must be cryptographically signed to be uploaded to the Debian infrastructure.

Additionally the option `-b` can be added to restrict the build process to only build the binary packages. Otherwise a source package will also be created.

## B.5. Further reading

Feedback 

- [Debian FAQ]
- [Debian Guide]
- [Debian Policy]
- [Debian Reference]

# Bibliography

[ucs-handbuch] Univention GmbH. 2022. *Univention Corporate Server - Manual for users and administrators*. <https://docs.software-univention.de/manual/5.0/en/>.

[make] Free Software Foundation. 2010. *The GNU Make manual*<sup>1</sup>.

[ISO639] International Organization for Standardization. 2002. *ISO 639-1: Alpha-2 code*<sup>2</sup>.

[Debian FAQ] Debian. 2012. *The Debian GNU/Linux FAQ - Basics of the Debian package management system*<sup>3</sup>.

[Debian Guide] Debian. 2013. *Debian New Maintainers' Guide*<sup>4</sup>.

[Debian Policy] Debian. 2012. *Debian Policy Manual*<sup>5</sup>.

[Debian Reference] Debian. 2012. *Debian Developer's Reference*<sup>6</sup>.

---

<sup>1</sup> <https://www.gnu.org/software/make/manual/>

<sup>2</sup> <http://www.loc.gov/standards/iso639-2/>

<sup>3</sup> [http://www.debian.org/doc/manuals/debian-faq/ch-pkg\\_basics](http://www.debian.org/doc/manuals/debian-faq/ch-pkg_basics)

<sup>4</sup> <http://www.debian.org/doc/devel-manuals#maint-guide>

<sup>5</sup> <http://www.debian.org/doc/debian-policy/>

<sup>6</sup> <http://www.debian.org/doc/manuals/developers-reference/>



# Index

## A

Apache (see Web Services)  
App center, 123

## B

Bug (see Bugzilla)  
Bugzilla, 143

## C

Config Registry, 19  
  Categories, 27  
  Configuration files, 22  
  Descriptions, 26  
  Examples, 30  
    Multifile, 32  
    Services, 33  
    Single File, 30  
  Repository, 17  
  Services, 28  
  Template  
    Module, 25  
    Multi file, 24  
    Script, 25  
    Single file, 23  
    Template file, 29  
Custom Attributes (see Extended Attributes)

## D

Database, 135  
  MySQL, 135  
  PostgreSQL, 135  
Directory Listener, 55  
  Cache, 67  
  Credentials, 67  
  Debug, 67  
  Example module, 59  
  modrdrn, 59  
  Notifier ID, 69  
  Verify, 68  
Directory Manager, 73  
  Custom Modules, 84  
  Extended Attributes (see Extended Attributes)  
  Hook extension, 44  
  Hooks  
    Packaging, 90  
  LDAP search, 86  
  Module extension, 44  
  Syntax extension, 44  
  Syntax override, 85  
Domain join, 37

Domain credentials, 52  
  Machine credential change, 52  
Join script (see Join script)  
Join status, 37  
Running, 38

## E

Example  
  Config Registry, 30  
Extended Attributes, 74  
  Hooks, 82  
  Options, 81  
  Selection list, 79

## J

Join (see Domain join)  
Join script  
  Exit codes, 40  
  Helpers (see Library)  
  Library, 41  
  Return codes (see Exit codes)  
  Writing, 38

## L

LDAP  
  Access control list extension, 44  
  Schema extension, 44  
Listener (see Directory Listener)  
Localisation (see Translation)

## M

Management Console, 105  
  Files, 110  
  Module  
    Disable, 119  
    LDAP, 119  
    System, 111  
  umc-modules, 110  
  XML, 111

## P

Package  
  binary-, 145  
  source-, 145  
Packaging, 11  
  Build dependencies, 145  
  Checking for errors, 135  
  Debian, 145  
  Library functions, 137  
  Modifying existing package, 11  
  New package, 12  
  Package repository, 17  
postup (see Updater)

preup (see Updater)  
Python 3  
    Migration, 71, 100

## **R**

Registry (see Config Registry)  
Repository (see Packaging)

## **S**

Server password change (see Domain join)  
Single Sign-On  
    SAML, 133  
SSO (see Single Sign-On)

## **T**

Translation, 127

## **U**

UCR (see Config Registry)  
UDM (see Directory Manager)  
UMC (see Management Console)  
Univention Directory Listener (see Directory Listener)  
Univention Directory Manager (see Directory Manager)  
Univention Management Console (see Management Console)  
Update (see Updater)  
Updater  
    Repositories, 131  
    Scripts, 131  
    System update, 131  
Upgrade (see Updater)

## **W**

Web Services, 121