Univention Corporate Client

Manual for administrators

Version 1.0-0
Stand: 18 of February 2013

Table of Contents

www.univention.de

Chapter 1. Introduction

Univention Corporate Client (UCC) is a flexible and economic alternative for the operation and administration of PCs, notebooks and thin clients in companies and institutions. The software contains a Linux-based desktop environment optimised for business use. In addition, UCC serves as a platform for access to remote desktop solutions and virtualized desktops as well as browser or terminal server-based applications.

Univention Corporate Client is the successor to Univention Corporate Desktop (UCD) and UCS Thin Client Services (UCS TCS). Notes on upgrading from UCD and TCS can be found in the Univention Wiki under http://wiki.univention.de/index.php?title=Upgrade-TCS-UCD-to-UCC.

UCC systems are rolled out via an image-based procedure: All the user data - and as such also the user settings - are typically saved on a separate partition. If a new version of the image is installed, the complete operating system installation is overwritten.

UCC clients need to be joined into a UCS domain. The clients are entirely managed through settings from the LDAP. As a result, a UCC system is directly configured after an upgrade or an installation. Features configured from the LDAP include network configuration, hardware settings like dual monitor setups and software selections.

Kubuntu is used as the basis for the images (Version 12.04 in UCC 1.0). Univention provides two preconfigured: a minimal image for thin clients and a larger image for native desktop installations. These two images are maintained and tested by Univention. It is also possible to create modified or completely new images with a minimum of effort using the included image toolkit (see Section 8.1). In contrast to the existing integration of Ubuntu clients in UCS, UCC clients work out of the box and require no further modification.

UCC systems include the most important UCS base components and integrate into the UCS user management: all the users in a UCS domain can log on to UCC clients using their domain password. The integration packages are installed via the Univention App Center (UCC requires UCS 3.1).

UCC support both a local desktop based on KDE Plasma and working on terminal servers (RDP, Citrix XenApp and remotely used KDE desktops). Access to web-based services can also be configured. A UCC desktop system be used both in the company network and in mobile use (all user and group information is cached locally for that).

A UCC system is usually installed over a network using PXE, but can also be setup from local media (DVD ROM or USB stick). The rollout can be performed fully automatic without user interaction (see Section 3.5).

The CompactFlash storage media typically integrated in thin clients are only designed for a limited number of write operations. Thin clients in UCC are thus started with an OverlayFS file system so that all write accesses on the storage media of a booted system are only performed in the system memory and not written to the hard drive. All the write changes are thus lost once the thin client is switched off. This does not pose any problems for access to terminal services, as all the user activities are performed on the respective terminal servers. The system log of UCC clients is performed remotely.

Chapter 2. Installation

Univention Corporate Client integrates into the management system of Univention Corporate Server. UCS 3.1 is a prerequisite for the installation of UCC.

The UCS integration packages are installed via the Univention App Center. General information on the Univention App Center can be found in the UCS manual [ucs-manual].

Figure 2.1. Installing UCC in the Univention App Center
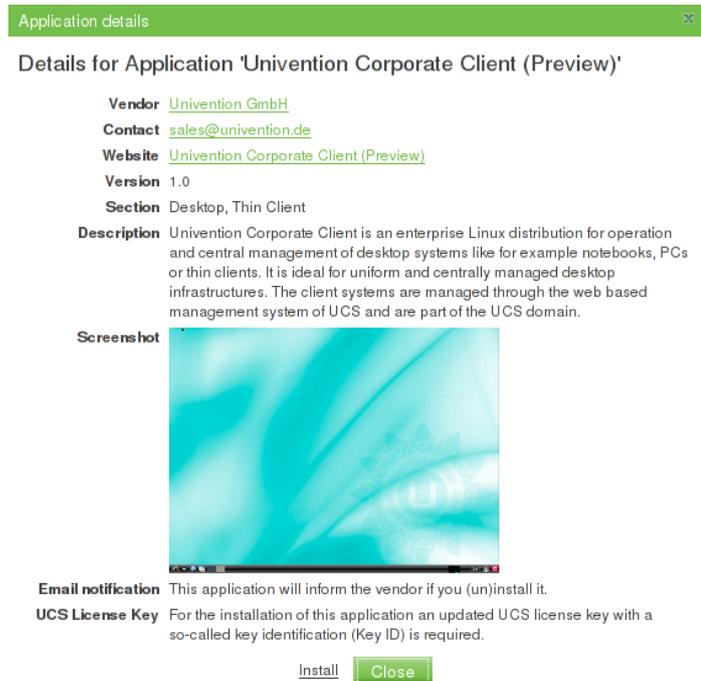
A UCC environment is made up of three components:

• The integration in the UCS management system (UMC modules and LDAP schema extensions). These must be installed on the master domain controller and all backup domain controller systems.

• A UCS server which distributes the images for the installation of UCC systems via PXE. The images used for the installation of UCC systems are loaded from the Univention mirror using an image download tool and then distributed locally to the clients. Custom installation images are also created on UCS servers. UCC servers can be installed in all UCS server roles (master domain controller, backup domain controller, slave domain controller and member server). It is possible to employ more than one UCC server in an environment.

• The UCC clients. They are installed via the images.

2.1. Installation in a single-server environment

All available errata updates should be installed on the master domain controller.

In the Univention App Center, select the *Univention Corporate Client* application and click on **Install**.

The thin client image is downloaded during the installation; the download may take some time depending on the speed of the Internet connection.

Once the component is installed, click on **Restart**.

It is recommended to restart the system before the rollout of UCC clients.

2.2. Installation in a distributed environment

When UCC is installed in an environment with more than one server, the installation is performed in two stages:

All available errata updates should be installed on both the master domain controller and the additional server.

1. Installation of the UMC modules and LDAP schema expansions:

Log on to the master domain controller as the *root* user and run the following command. If backup domain controller systems are in use, the command must also be run on all of these systems. After installation the Univention Management Console server needs to be restarted:

```
univention-add-app ucc_20130218 ucc-management-integration
/etc/init.d/univention-management-console-server restart
```

2. Installation of the UCC server(s)

UCC servers can be installed in all UCS server roles. The UMC module **Univention App Center** must be opened on all the systems on which you wish to install a UCC server.

In the Univention App Center, select the *Univention Corporate Client* application and click on **Install**. The thin client image is downloaded during the installation; the download may take some time depending on the speed of the Internet connection.

Once the component is installed, click on **Restart**.

Finally the join scripts need to be executed on the UCC server:

```
univention-run-join-scripts
```

It is recommended to restart the system before the rollout of UCC clients.

2.3. Management of UCC images

2.3.1. Downloading UCC images

The UCC images are not delivered in the Debian package format; the Debian package format is not best suited to files in the gigabyte range.

Instead, UCC images are downloaded with the ucc-image-download tool. The individual files of the image are referenced via a spec file containing the file names and SHA256 hashes. The hash values are checked

as part of the download procedure in order to detect erroneous transmissions. The proxy settings of a UCS system are taken into account.

The images are available at http://ucc-images.software-univention.de/download/ucc-images/. A local UCC mirror can also be used, see Section 2.3.3.

Univention provides two metapackages, the installation of which initiates the downloading of the images. The packages can be installed with `univention-install` or via the software management module of the Univention Management Console.

- *ucc-thinclient-image* installs the latest thin client image

- *ucc-desktop-image* installs the latest desktop image

The installation of the images is initiated at the end of the installation. The downloaded images are not removed when removing the metapackages. If desired, they should be removed manually in the directory `/var/lib/univention-client-boot`.

Alternatively, the download can also be performed manually by running `ucc-image-download`. The parameter *-s* is used to provide the name of the spec file on the mirror, e.g.:

```
ucc-image-download -s ucc-1.0-thinclient-image.img.spec
```

Interrupted downloads are restarted as standard. You can use the option *--reload* to force the download to restart completely.

The full list of available parameters can be queried with the *-h* option.

The root password of the installed system is initially specified in the image. To avoid there being an identical root password on all UCC systems operated with the official Univention images, the root password is "personalised" during the image download: the root password of the UCC server is set as the root password on the images. You can also use the *--set-root-pw-interactive* option of the `ucc-image-download` command to set a different root password.

For existing images, the root password can be set subsequently with the command `ucc-image-root-password`, e.g.

```
ucc-image-root-password -i ucc-1.0-rev2-desktop-image.img -p
```

2.3.2. Deleting UCC images

Feedback 💬

The `ucc-image-remove -l` command can be used to output an overview of the available images. An image can be deleted using the parameter *-r* and specifying a spec file, e.g.:

```
ucc-image-remove -r ucc-1.0-desktop-image.img.spec
```

2.3.3. Operating a local UCC image mirror

Feedback 💬

If you are operating a number of UCC servers or an infrastructure completely disconnected from the Internet, you can also operate a local UCC mirror. In this case, the images need to be stored on an HTTP server. Then the Univention Configuration Registry variable `ucc/image/download/url` on the UCC servers needs to be set to the download path.

2.4. Official UCC images

Feedback 💬

Univention provides two preconfigured UCC images: a minimal image for thin clients and a larger image for native desktop installations. These two images are maintained and tested by Univention.

UCC systems operated with these images must have at least 512 MB of system memory available.

The thin client image offers a minimal desktop and support for terminal sessions on Windows and UCC terminal servers. In addition, a local LXDE desktop environment is also available. Thin clients which are to be operated with this image must be equipped with at least 2 GB of local disk space (e.g., CompactFlash or SSD).

The desktop client image offers a KDE Plasma desktop and support for terminal sessions on Windows and UCC terminal servers (support for Citrix XenApp can be subsequently installed).

Software packages can also be installed or removed to complement the range of functions of the standard UCC images. Software updates can also be initiated through a policy (see Section 4.3)

www.univention.de

Chapter 3. Management, rollout and updates of UCC systems

UCC systems are rolled out via an image-based procedure. The recommended rollout procedure is creating the UCC systems in the Univention Management Console in advance. When the image is installed, the image installation tool then checks whether there is already a computer account available for the client and uses it. If the computer name is not stored in advance, the name can be specified interactively during the installation.

3.1. Administration of UCC systems in the Univention Management Console

Feedback 💬

UCC systems are registered and administrated with the system role *Univention Corporate Client* in the computer management module of the Univention Management Console.

In the command line frontend Univention Directory Manager, clients are managed with the *computers/ucc* module.

The following settings must be configured for every UCC client as a minimum:

• The *name* of the client (composed of lowercase and uppercase letters, numbers, hyphens and underscores).

• The *MAC address* of the client in the notation XX:XX:XX:XX:XX:XX

• The *IP address* of the client

Figure 3.1. Management of a UCC system in the UMC

A forward and reverse zone for DNS resolution should be assigned under **DNS Forward and Reverse Lookup Zone**. These zones are created automatically in the scope of the installation of the master domain controller. The name and the IP address of the UCC client can thus also be resolved in the UCS DNS service.

The network configuration of UCC clients is managed through DHCP in the default setting. A DHCP service must also be assigned under **DHCP**. These are also created automatically in the scope of the installation of the domain controller master. The UCC client is then registered for the DHCP server and the configured IP address is assigned to the DHCP.

UCS offers you the possibility of centrally managing the IP addresses and DNS/DHCP settings of a network in a network object in the LDAP. This can considerably facilitate the management of UCC clients by selecting the network object in **Network** input field: The next free IP address of the network and the DNS and DHCP settings are then adopted automatically.

Figure 3.2. Management of IP addresses through a network object

During the installation of an UCS system, a network object with the name *default* is saved as standard, which can usually be used in normal cases. If, for example, several sites are to be managed, additional networks can be defined using the **Networks** wizard in the Univention Management Console.

The DHCP configuration is then also performed via the UMC. The network properties of UCC clients can be centrally specified per subnetwork. The settings can be set via the UMC's **DHCP** wizard. The DHCP service of the current domain must be selected. The selection list which opens then shows the subnetwork object, which can be opened with a click. The following properties can be specified under **Policies** amongst others:

• *DNS* allows the assignment of one or more name servers

• *Routing* allows the assignment of a default gateway. This must be set to ensure proper routing!

• *Lease time* allows configuration of a lease time for an IP address

In the default setting, fixed IP addresses are assigned and only to clients registered in the LDAP.

The DHCP administration also offers numerous, extensive configuration options, which are generally, however, not required in UCC client operation. They are described in the DHCP section in the UCS manual [ucs-manual].

3.2. Configuration of the PXE server in a multi-server environment

Feedback

The rollout of UCC systems usually occurs via PXE (see Section 3.3). If UCC is operated in a single server environment the server distributing the IP adresses to the clients is identical to the PXE server providing the UCC images for installation.

If UCC is used in a distributed environment, there may be DHCP servers not serving as PXE servers. In that case the UCS server distributing the UCC images needs to be configured through a **DHCP Boot** policy. Please see the UCS manual for additional information [ucs-manual-pxeboot].

3.3. Rollout of images

The image with which a UCC client is operated is configured in the Univention Management Console in the **Images** tab on UCC computer objects. All the UCC images registered in the UCS management system are available for selection. The registration is effected with join scripts during the installation of the image, see Section 2.3.1.

The Univention Management Console can also be used to edit several objects at once, which permits the assignment of images to several computers at once. This is documented in the UCS manual [ucs-manual-multiedit].

Figure 3.3. Assigning the desktop image to a UCC client
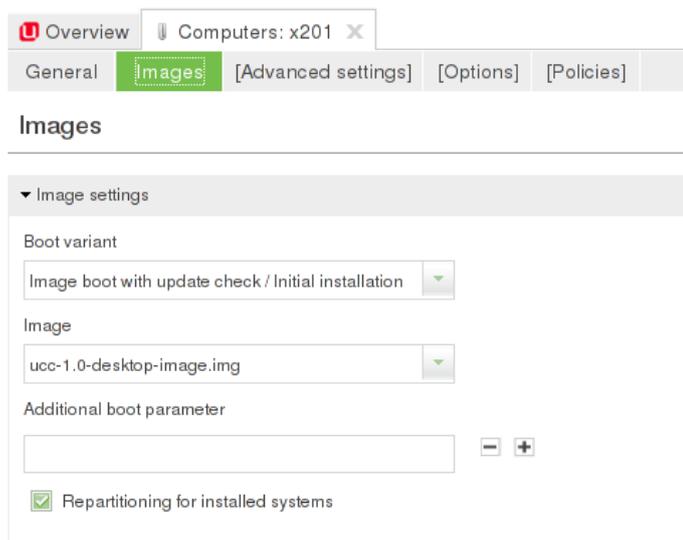
UCC clients can be operated in three different installation modes, which can be assigned via the **Boot variant** field:

- **Live boot** Here the image is started via PXE and mounted via NFS. The client must be configured for PXE boot in the BIOS. Technically, all UCC systems are always treated as having read/write storage media: If an image is mounted from a source which itself only allows readonly access (from a live DVD or as in this case from a NFS share), an OverlayFS file system is employed: All the write changes are cached in the system memory and are lost when the computer is switched off. Thin clients are also always run with an overlayfs for a local installation, further information can be found under Section 3.9.

- **Image boot with update check / Initial installation** This mode is used for two purposes:

  - The initial installation of a UCC client

  - For updates of UCC systems to a new UCC image

  If there are no partitions present, the system is partitioned. After the installation of the image, the system is joined into the UCS domain. If this boot variante is used on an existing UCC installation, is is detected whether the installed image differs from the image to be installed. If that is the case, the system, the UCC system partition is overwritten. In this case, no new partitioning occurs.

- **Image boot without update check** In this boot mode, the locally installed image is started and no check for a newly available image performed. Following an installation performed with **Image boot with update check / Initial installation**, the system returns to this boot mode automatically.

The **Additional boot parameter** input field can be used to add any parameters to the initial RAM disk, which performs the installation/rollout. Two preconfigured options are:

- *debugshell=y* : If an error occurs during installation of the image, a shell opens in which the problem can be analysed further.

- *verbose=y* : The shell scripts of the initial RAM disk are started with the parameter "-x", with which the current control flow can be better monitored (useful for debugging).

3.4. Partitioning / separation of user and system data

On the systems installed with images, user-specific data such as the home of the users must be stored separately from the system data on another partition. This is the case in the default partition configuration.

The partitioning scheme is specified in the images configuration, see Section 8.2.

The **Repartitioning for installed systems** option on the **Images** tab of a UCC client in the computer management of the Univention Management Console forces repartitioning of a system. A prompt must be confirmed before the partitioning begins.

Caution

Existing user data on a /home partition on a system are also deleted!

The GNU Parted version used in Ubuntu 12.04 has a bug, which means that the *bootable* flag of the protective MBR disappears when you edit a partition. This can cause boot problems with some BIOS implementations. This bug does not occur during partitioning in UCC as the flag is set manually via a script (`set-bootable-flag-on-protective-mbr`). As such, manual partitioning should be avoided or the script be executed after partitioning.

It is also possible to perform completely new partitioning schemes - e.g. an encrypted hard drive - with an adapted partitioning script, see Section 8.3).

3.5. Configuration of a fully automated rollout

The rollout of UCC systems can be completely automated so that user interaction is no longer necessary. Once all the clients to be rolled out have been created in the UCS management system (see Section 3.1), the following steps are necessary:

An image must be generated in which the interactive confirmation of the partitioning is disabled. This can be achieved by setting the option *continuation_prompt* to *false* (see Section 8.2).

Then the credentials of a user need to be stored in the image, which is authorised to join clients in the domain (the user must be a member of the *Domain Admins* and *DC Backup Hosts* groups for this). For security reasons, this user should only be created during the rollout and then removed or disabled after the rollout.

These credentials are now saved in the image with the tool `ucc-image-set-join-information`. The parameter *-i* is used to specify an image and the join account and its password are interactively prompted.

The clients are then rolled out fully automatically without user interaction.

3.6. Domain join of UCC systems

Only UCC clients, which are joined into a UCS domain can be centrally configured. Unjoined clients can still be used for special setups like live systems or demo points.

The domain join is typically performed in the scope of the rollout via PXE (see Section 3.3). The domain join can also be subsequently performed by running `univention-join`. The subsequent domain join cannot be performed via SSH, but should instead be run via a local login or, if virtualization is employed, via VNC. The system must be restarted after the join.

UCS installations, in which the master domain controller was installed in a release older than 2.3 still use MD5 as the hashing algorithm for the SSL certificates. Later releases use SHA1 as the hashing algorithm. UCC clients cannot join a domain still using MD5 hashes. The necessary steps to migrate a UCS domain from MD5 to SHA1 are documented in the Univention Support Database (http://sdb.univention.de/1150).

3.7. Rollouts using an ISO image

Feedback

While the standard rollout mechanism for UCC systems is PXE-based, it is also possible to perform installations using ISO images, which can be written to USB sticks, DVDs or BluRays.

The images are available at http://ucc-images.software-univention.de/download/ucc-images/.

The client to be installed should be created in the UMC computer management first (see Section 3.1).

After the image has been written to disk and the boot medium is started, a boot menu appears. Here, **UCC - Image boot with update check / Initial installation** needs to be selected and the *e* key pressed. Then the boot options need to be modified from *ucc=update* to *ucc=rollout*. If the client already contains a partitioning, which needs to be replaced *repartition=y* needs to be added.

3.7.1. UCC installation as Xen Guest

Feedback

To install an UCC ISO image in a Xen DomU, the DomU must be configured to be fully virtualized (HVM). On an UCS System with a virtual machine manager the operating system option 'Other' has to be used [ucs-manual-uvmm]. Please note that the official UCC desktop image uses a kernel that supports pvops, so I/O performance is that of a paravirtualized guest when pvops is supported by Dom0. On an official thinclient image another kernel with pvops support can be installed, e.g. linux-image-generic-pae. More information about pvops can be found at http://wiki.xen.org/wiki/Paravirtualization_%28PV%29.

3.8. Persistently stored system settings

Feedback

System data which must be preserved during an update (e.g., the join status) are saved separately from the system data and automatically restored after updates. These files and selected Univention Configuration Registry variables are registered in the UCR variables `ucc/persistent/files` and `ucc/persistent/ucr`. Important standard UCC settings are preconfigured automatically and can be expanded for local adaptations.

3.9. OverlayFS on thin clients

Feedback

The CompactFlash storage media typically integrated in thin clients are only designed for a limited number of write operations.

Thin clients are thus started in UCC with an OverlayFS file system so that all write accesses on the storage media of a booted system are only performed in the system memory and not written to the hard drive. All the write changes are thus lost once the thin client is switched off. This does not pose any problems for access to terminal services, as all the user activities are performed on the respective terminal servers. The standard write access is selectively enabled for individual operations such as the installation of new UCC images or subsequent installation of software.

If a thin client uses storage media which allows permanent write access, the Overlayfs can also be disabled by adding *mount=rw* to the **Images -> Additional boot parameter** of the computer object in the computer management module of the Univention Management Console.

www.univention.de

In addition the Univention Configuration Registry variable `ucc/thinclientoverlayfs` must be set to *false* on the affected thin clients using a Univention Configuration Registry policy (see Section 4.1). This variable allows tools such as `univention-ucc-software-update` to detect whether they are running on a thin client using overlayfs.

Chapter 4. Configuration of UCC systems

4.1. Setting of Univention Configuration Registry settings on UCC clients

Feedback

The configuration of UCC system settings is mostly performed using Univention Configuration Registry. Typically, these settings are not saved locally on the UCC client systems, but rather via UCR policies via the LDAP.

Univention Configuration Registry policies can be managed in the Univention Management Console in the **Policies** menu. At least one UCR variable must be configured with the **Variable** and **Value** fields. Additional variables can be added by clicking on the plus sign. The UCR policies are evaluated when the system is started and then once an hour.

Figure 4.1. Configuring UCR values through a policy
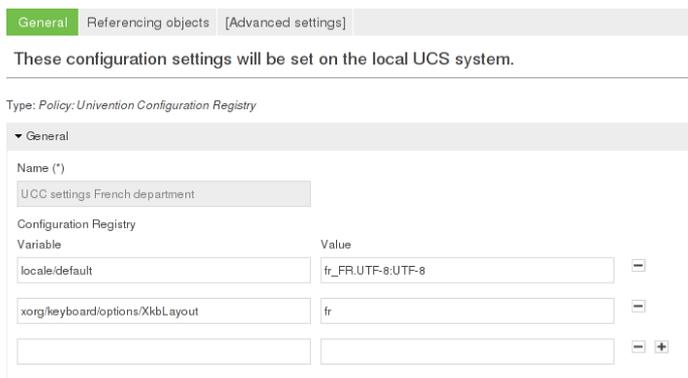
In addition to policies, Univention Configuration Registry variables can also be set via the command line frontend. However, we recommend performing the UCR settings via policies as the locally set variables are lost when image updates are installed or thin clients are switched off (see Section 3.9).

4.2. Definition of Cron jobs

Feedback

Regularly recurring actions can be defined and run on UCC clients via Cron jobs. The configuration is performed as in Univention Corporate Server via Univention Configuration Registry or local configuration files under `/etc/cron.d`. Further information can be found in the UCS manual [ucs-manual-cron].

4.3. Software updates / Installing additional software

Caution

Always test UCC software updates on the target platform before updating all clients. UCC Updates have been tested on official UCC images. If individual images have been created for an environment a number of things should be considered before updating.

- Is there enough free space to perform the update?

- How long does the update take on the target platform? Large packages take a considerable amount of time to download. Slow hardware can prolong the update when e.g. the initramfs has to be recreated.

- Does all hardware still work after a kernel update?

Every UCC image comes with a predefined software package selection. A computer policy in the UCS management system can be used to install available software updates and install/uninstall software packages. This check is performed every time the system is started.

The settings are defined with a **UCC software update settings** computer policy in the Univention Management Console:

Figure 4.2. Installing additional software through a software update policy
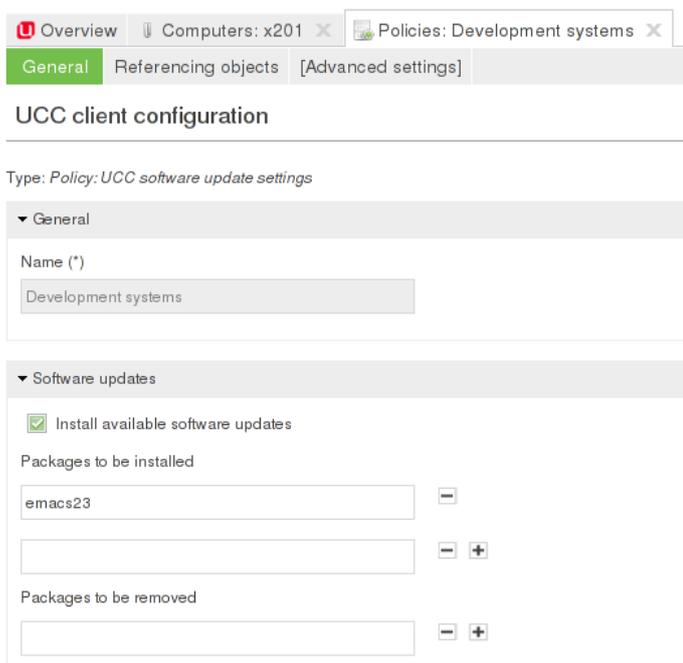
- **Install available software updates** updates all the installed packages for which updates are available.

- **Packages to be installed** is a list of packages which are installed if they have not yet been installed and which are updated if a newer version is available.

- **Packages to be removed** is a list of packages to be removed. This function should be used with care to ensure that no packages which are essential for UCC are removed due to dependencies.

www.univention.de

The installation/updates are logged in `/var/log/univention/software-updates.log`.

Thin clients employ an OverlayFS (see Section 3.9). For this reason, the installation of updates is performed in several stages on thin clients: The client is restarted to change to the writeable mode and then following installation of the updates restarted again to change to the OverlayFS mode.

Additional software packages can be installed on the command line using `apt-get`:

```
apt-get update
apt-get install emacs23
```

4.4. Configuration of the keyboard layout / locale

Feedback

In the standard setting, the keyboard layout and the language setting (locale) of the UCC PXE server is also employed on the UCC clients. If UCC systems are not installed using PXE, the Univention Configuration Registry variables specified below need to be set via a policy:

The Univention Configuration Registry variable `xorg/keyboard/options/XkbLayout` can be used to set another keyboard layout, e.g., *de* for German or *fr* for French.

The Univention Configuration Registry variable `locale/default` can be used to set a different locale, e.g., *de_DE.UTF-8:UTF-8* for German or *fr_FR.UTF-8:UTF-8* for French. Please note that it may be necessary to install additional language packages for some locales. The standard thin client image includes German and English; the standard desktop image includes English, German, French, Dutch and Spanish.

The language and keyboard settings are evaluated every time the system is started.

4.5. Configuration of the CIFS home share

Feedback

The *univention-ucc-cifshome-pam-mount* package allows the automatic mount of a CIFS share with home directory of the the user during login. It must be configured using the following Univention Configuration Registry variables:

- `ucc/mount/cifshome/server`: The name of the server from which the share is mounted.

- `ucc/mount/cifshome/share`: The name of the share to be mounted.

- `ucc/mount/cifshome/options`: This configures a optional list of mount options. The full list of available options can be found in the *mount.cifs* manpage.

4.6. Configuration of the time zone / time server

Feedback

In the standard setting, the time zone of the UCC PXE server is also employed on the UCC clients. If UCC systems are not installed using PXE, the time zone needs to be set via a policy:

The Univention Configuration Registry variable `ucc/timezone` can be used to set a different time zone. The available time zones can be found in the `/usr/share/zoneinfo/` directory, for example *Europe/Berlin*.

Authentication in UCC is performed through Kerberos. For this reason, synchronised time sources are essential. When a UCC client joins a domain, the master domain controller of the domain is set as the time server. The Univention Configuration Registry variable `ucc/timeserver` can be used to configure a different server.

The system time is synchronised via NTP every time the system is started.

4.7. Print server configuration

UCC can use one or several print servers from the UCS domain. The Univention Configuration Registry variable `ucc/cups/server` configures the server(s) to use; multiple servers need to be separated by a blank character.

4.8. Remote logging

In addition to local logging, the system logging (syslog) of UCC clients can also be performed remotely against a central log host based on rsyslog. As standard, the logging is performed against the UCC PXE server.

The Univention Configuration Registry variable `ucc/pxe/append` can be adapted to deactivate the remote logging (syslog=n) or reroute it to another log host (syslogserver=HOSTNAME). These configuration options are only set during the installation or update of an UCC system.

4.9. SSH access to UCC clients

As standard, an SSH login is possible on UCC clients. The login is performed with the local root account or a domain account.

4.10. Bootsplash startup animation

A startup animation (bootsplash) is displayed when a UCC client is started. This can be hidden by pressing the Escape key to diagnose the startup in full details.

The Univention Configuration Registry variable `ucc/pxe/bootsplash` on the UCC PXE server can be set to *no* to deactivate it completely.

www.univention.de

Chapter 5. Hardware configuration of UCC systems

5.1. Network configuration

Feedback ⟲

The network configuration of UCC clients is generally performed via DHCP. The configuration of MAC and IP addresses, etc., is performed in the UCS management system, see Section 3.1.

The network interfaces of a joined UCC client are managed via the Network Manager. Here you can also configure additional connections such as a VPN/Wifi access or a static IP address.

During the PXE live boot of a UCC system, the primary interface (eth0) is not managed by Network Manager.

While offline operation is supported for images running the desktop image, thin clients require a permanenent network connection.

The wireless regulatory domain is set to *00* as standard. With some access points, it can be necessary to configure this to the national code using the command `iw reg set`.

5.2. USB mass storage access on thin clients

Feedback ⟲

The *univention-ucc-remote-mount* package installed as standard allows access to the USB-CD/DVD drives, hard drives and sticks connected to a UCC thin client. If a USB mass storage device is connected to the client, a local mount is performed via a udev rule. The terminal service solutions then provide this directory through the terminal session. The additional component `cdpinger` is used for the integration of USB-CDROM/DVDROMs. VFAT, NTFS and ext* file systems are mounted.

The local mount points are made available in UCC, Windows terminal server and XenApp terminal server sessions if the option **Allow access to local mass storage** is activated in the **UCC client configuration** policy in the UMC computer management.

In the standard setting, data on thin clients are cached for up to a tenth of a second before they are written on the USB medium. The behaviour can be adapted with the Univention Configuration Registry variables `ucc/sysctl/dirtywritebackcentisecs` and `ucc/sysctl/dirtyexpiredcentisecs`.

Setting the Univention Configuration Registry variable `ucc/mount/sync` to *true* allows all changes to be written directly. This generally leads to considerable performance losses.

The access to the mounted USB media is described in the corresponding sections on terminal services (see Chapter 9).

5.3. Sound support

Feedback ⟲

The sound output is activated in UCC clients as standard. Sound is also output in terminal sessions:

• In RDP sessions to Windows terminal servers, audio is transported via an RDP channel.

• In sessions to UCC terminal servers, the remote sound output is redirected via PulseAudio.

• In Citrix XenApp sessions, sound output is transmitted via the Citrix protocol.

Information of the configuration of the sound output in terminal services can be found in Chapter 9.

5.4. Configuration of dual-display setups

UCC uses the Xorg autodetection for the configuration of the graphics adapter. This automatically determines the suitable driver for the graphics card and the appropriate display parameters.

Figure 5.1. Configuring dual monitor display
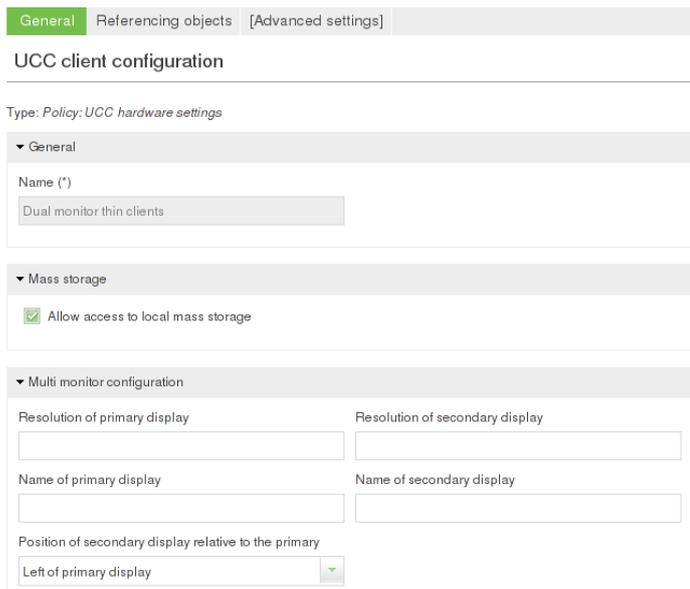
Dual-display setups can be configured using a **UCC client configuration** computer policy in the UCS management system:

To configure a dual-display setup, at least the position of the primary display relative to the secondary display must be specified in the **Position of secondary display relative to the primary** field:

• Left of primary display

• Right of primary display

• Above primary display

• Below primary display

Setting the resolutions via the **Resolution of primary display** and **Resolution of secondary display** fields is optional: If they are not set, they are assigned the recommended value (xrandr --auto). The values for width and height should be separated by an *x*, e.g., *1024x768*.

The Xorg-internal names of the displays are also automatically detected and listed alphabetically. In this way, the order is always fixed. If automatic determination of the display names is used, a message like the one below is written in the syslog:

```
Dec 17 13:12:34 x201 logger: The display settings for x201 were
queried automatically, if you want to set them through a policy
use the display names LVDS1 and VGA1
```

These values can then be specified in the **Name of primary display** and **Name of secondary display** fields.

For special cases such as the configuration of a third display, a local display setup script can be configured. This is done by setting the UCR variable Univention Configuration Registry variable `ucc/displayscript` to a script, which is then run for the Xorg configuration instead of the standard script.

Chapter 6. User logins

6.1. User logins on LightDM

Feedback 💬

6.1.1. Session selection

Feedback 💬

UCC uses LightDM as its login manager. When the UCC client is started, a login mask is shown. If the UCC client is not yet joined, an automatic login is performed with a temporary guest user. The user can choose between different session types. LightDM can optionally also be configured in such a way that a session is started automatically without additional user login, see Section 6.1.3

Figure 6.1. User login at LightDM
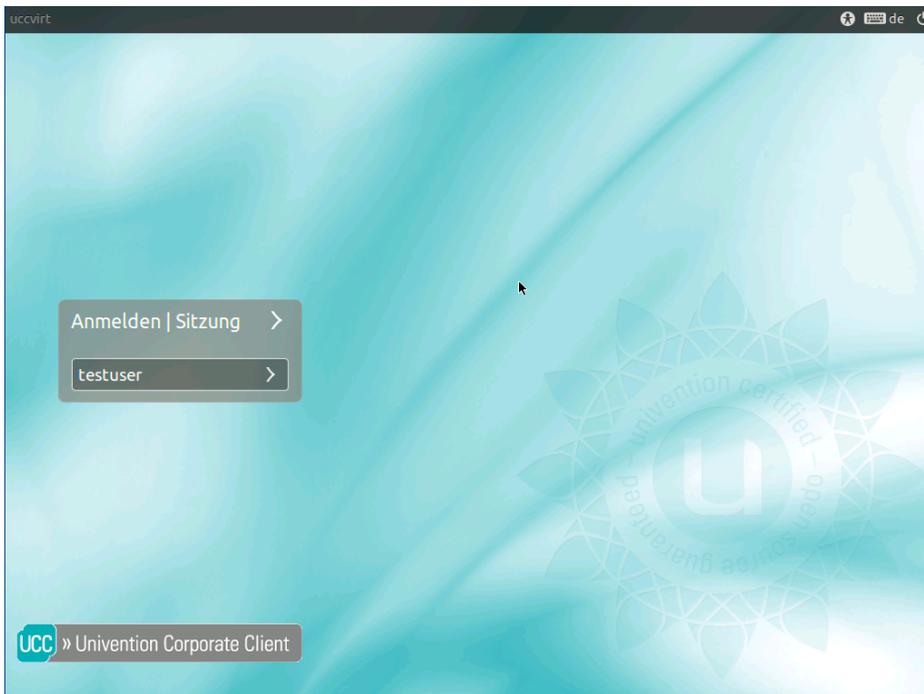
If a password has expired or a user is scheduled for a password change the next time she logs in, the password change is performed in the scope of the login. Password changes are currently not possible when using the RDP session script, this will be fixed in a future release.

It must be noted that although the Univention Management Console permits the creation of users with a space in their user name - as these user names are legitimate in Active Directory domains - it is not possible to logon to UCC clients with these user names.

The last chosen user session is cached per user.

Figure 6.2. Session selection at LightDM

The following session scripts are supported in UCC 1.0:

- Univention Corporate Client based on KDE (on a local system and as a terminal service) (Section 9.1, Chapter 7)

- Citrix XenApp (Section 9.3)

- Microsoft Windows Terminal Server (Section 9.2)

- Firefox (with direct login to a configured website) (Section 6.4)

- LXDE (Lightweight X11 Desktop Environment) (Chapter 7)

6.1.2. Configuration of a default session for a user's first login

To configure the default session that is set for a user's first login on a client, the Univention Configuration Registry variable `lightdm/sessiondefault` must contain the name of one of the session scripts in `/usr/share/xsessions`. For subsequent logins on a client the last chosen session is cached on a per user basis.

6.1.3. Configuration of an automatic login and session selection

Instead of an interactive login, it is also possible to configure an automatic login with the guest user. This is useful for a UCC client which is only used for access to terminal services or to a website (e.g., for kiosk systems).

This is done by setting the Univention Configuration Registry variable `lightdm/autologin` to *yes* and `lightdm/autologin/session` to a session script. The session scripts can be found in the `/usr/share/xsessions` directory, in other words, *firefox* for example.

In the case described above, the LightDM login dialogue is no longer shown. The session can alternatively also be specified in the user management of the Univention Management Console. This is performed in the **Force this session for user logins** input field in the *UCC user session* policy: Independently of the selection of the session script during the LightDM user login, the login is always performed with the predefined session. The sessions available in the policy can be extended, see Section 6.5.

6.1.4. Session scripts

Scripts can be run at different times during session setup and when exiting the session. All the scripts which can be run in the following directories are run alphabetically with root rights:

- `/etc/lightdm/session-setup`: Is run before the session script is executed.

- `/etc/lightdm/session-cleanup`: Is run after the session script is exited.

- `/etc/lightdm/display-setup`: Is run if a greeter session is run.

- `/etc/lightdm/greeter-setup`: Is run if a greeter session is started.

6.1.5. Configuration of environment variables and execution of scripts during user login

A **UCC desktop settings** user policy can be used to configure environment variables in the user session. All the variables set with the **Variable** and **Value** options are then set in the user session scripts.

The settings set via the **Desktop logon scripts** and **Desktop logout scripts** settings are run before and after the user login with the rights of the accessing user.

The scripts must be specified as absolute file names and must not contain any spaces. Also, the scripts must be executable.

6.2. Local caching of user and group information

UCC systems store user and group information in local files integrated via an NSS module. In combination with caching of the login credentials (see Section 6.3), this allows operation of UCC clients without a connection to an LDAP server of the UCS domain.

The user and group information is extracted via a listener module (`ucc-nss-passwd.py`) on the UCS-based UCC servers into a `passwd` and a `group` file.

These files are read from UCC systems via an NSS module (libnss-extrausers). The user and group data are downloaded in two ways:

- The current files are downloaded when the UCC client is started.

- If the user is not yet present on the UCC system, the download is also initiated during login via the PAM stack.

As standard, all of the users in the domain are always copied to the client. For special cases - such as notebooks, on which only a few users should be present - the Univention Configuration Registry variable `ucc/nss/update/hostspecific` should be set to *true*. In this case, the download script for the user data on the UCS server searches for the `/var/cache/ucc/HOSTNAME.passwd` and `/var/cache/ucc/HOSTNAME.group` files in which system-specific user data can be stored.

6.3. Logins to offline UCC systems / password credentials caching

Kerberos authentication is performed on UCC systems with a network connection.

In addition, successful login attempts are cached via the PAM module pam_ccreds, i.e., if a user has successfully logged in once with an active network connection, she can also continue to log in with this password when working offline.

6.4. Firefox session script

The Firefox session script starts a Firefox web browser in a fullscreen session. If the Univention Configuration Registry variable `firefox/startsite` is set to an URL, the website is automatically opened.

6.5. Registration of sessions in the Univention Management Console

Sessions are registered in the Univention Management Console. New sessions can be created by selecting the UMC module **LDAP directory** and adding a **UCC session script** object below *cn=univention,cn=UCC,dc=Session*.

Chapter 7. Univention Corporate Client desktop environment

7.1. Introduction

Univention Corporate Client offers a desktop environment based on the KDE Plasma desktop in version 4.8. It offers a compilation of software components suitable for typical business applications.

Figure 7.1. Univention Corporate Client desktop
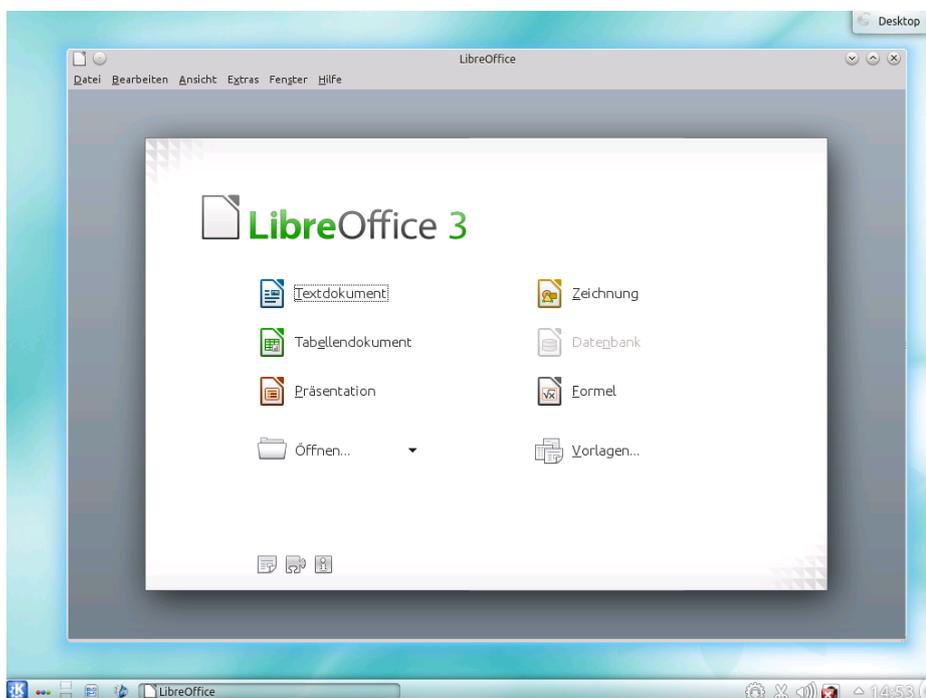
Extensive documentation and manuals for all the KDE components can be found at http://docs.kde.org/.

LibreOffice is the core application of the Univention Corporate Client and offers the full scope of functions of a modern Office suite. In addition to standardised, open formats such as the OpenDocument format, OpenOffice.org can also be used to open and edit documents created in other office applications such as Microsoft Office. To ensure uncomplicated distribution, documents can also be easily exported in PDF format.

Extensive documentation on Libreoffice can be found at http://www.libreoffice.org/get-help/documentation/.

Mozilla Firefox is also supplied for accessing websites. The Adobe Flash plugin is integrated for the playback of Flash animations.

Thin clients only offer a slimmed down desktop environment based on LXDE. LXDE is only provided for simple administrative environments.

7.2. Configuration of proxy settings for the desktop

The proxy settings in Firefox and KDE can be centrally configured via Univention Configuration Registry variables provide by the package *univention-ucc-proxy-settings* (see Section 4.1). `ucc/proxy/http` configures a specific proxy, e.g. *http://192.168.0.100:3128*. Alternatively the URL to a PAC (proxy auto-config) file can be provided with the variable `ucc/proxy/autoconfig/url`.

Proxy settings configured with the variables above are immutable for the user. In Firefox the respective dialogues are greyed out. In the system settings of KDE changes can be made in the dialogues, but they are discarded when clicking **Apply**.

Chapter 8. Generation of adapted UCC images

8.1. Image toolkit

Feedback

Beside the official UCC images provided by Univention it is also possible to build local images. These images are generated via a toolkit run on a UCS server installed on a UCS domain controller. The image generation requires a considerable amount of space; we recommend ensuring that there are at least 100 GB of free disk space available on the system.

On systems on which an image is integrated, two conditions currently need to be fulfilled as otherwise disruptions might occur in the image build:

- Bind must be installed. This is the case as standard on UCS domain controllers.

- A DNS forwarder must be configured with the Univention Configuration Registry variable `dns/forwarder1`.

Image generation is performed with the `ucc-image` tool in the *ucc-image-toolkit* package. The images are defined via a configuration file. In addition to the image, the image toolkit also creates an initial ram disk (initrd) and a kernel. An ISO image can also optionally be created. In addition, a spec file is generated, which is used when downloading a UCC image (see Section 2.3.1).

The configurations of the two official UCC images are also provided in this package and can be used as templates for your own configurations:

- `/usr/share/doc/ucc-image-toolkit/example/ucc-desktop.cfg`

- `/usr/share/doc/ucc-image-toolkit/example/ucc-thinclient.cfg`

The images are created with the `ucc-image` command as the *root* user.

The parameter *-c* must be used to specify a configuration file. If the parameter *--compress* is set, the image is compressed with xz. The option *-t* can be used to specify a target directory. After image generation the images need to be copied to the directory `/var/lib/univention-client-boot/` on the UCC servers. The join script needs to be copied to `/usr/lib/univention-install`. After that, `univention-run-join-script` needs to be executed.

The image generation is logged in `/var/log/univention/ucc-image-toolkit.log`. The option *-l* can also be used to specify a different log file.

8.2. Overview of image parameters

Feedback

The following parameters can be used. The configuration files can be commented with a hash (#):

- *arch*: The system architecture, i386 or amd64. The official UCC images are provided as i386. When building an image for amd64 *linux-image-generic* needs to be used as the kernel package.

- *version*: The Ubuntu code name on which the image is based. It must be taken into account that the Univention modifications are always only compiled and tested for a specific release, in the case of UCC 1.0 for Ubuntu 12.04 (precise).

- *hostname*: The standard host name of an unjoined UCC client. The name is set to the name configured in the LDAP in the scope of the domain join.

- *domainname*: The standard domain name of an unjoined UCC client. The domain is set in the scope of the domain join.

- *root_password*: The SHA-512 hash of the standard root password. If the official image is loaded from the Univention server, it is adapted during the download, see Section 2.3.1. To generate an individual hash, the *whois* package must be installed. The command `mkpasswd -H sha-512 PASSWORD` can be used to generate the hash value.

- *mirror*: Configures the mirror from which the Ubuntu packages are downloaded.

- *updates, security, backports*: Here, true/false can be used to specify whether, in addition to the standard release, updated bugfix packages (updates), security updates or backports should also be integrated into the image.

- *universe, multiverse*: These options (true/false) integrate additional archive suites from Ubuntu, see [ubuntu-repositories] for details.

- *ucc*: Installs some basic packages required during image generation.

- *sources_list*: Additional apt sources can be integrated here.

- *packages_no_recommends, packages*: In the Debian package format, packages can declare recommendations for packages which should be additionally installed during installation of a package. In these options, packages can be specified which should be installed with or without their recommended packages.

- *ucr_variables*: Here one can define Univention Configuration Registry variables which are then set directly in the installed image.

- *version*: Here one can specify a version for the image which, among other things, is also displayed in the image selection in the Univention Management Console.

- *size*: The size of the image in megabytes.

- *filesystem*: The file system used; it is recommended to retain ext4 here.

- *name*: The name of the image.

- *initramfs_modules*: You can specify a list of kernel modules here which should be loaded in the initrd.

- *kernel, initrd*: The Linux kernel of a UCC system is saved separately from the image. The file names are defined here.

- *iso*: If a name of a file is defined here, a bootable ISO image is also generated with which can be booted from USB or a DVD drive.

- *device*: Specifies which device should be partitioned, e.g., hda or sda. *auto* establishes the first available disk.

- *continuation_prompt* If this option is set to true, a prompt appears to verify whether partitioning should be performed.

- *continuation_message_top, continuation_message, continuation_dialog, continuation_dialog_yes, continuation_dialog_no, continuation_dialog_error*: Different dialogue texts during partitioning which can be adapted or compiled.

- *remove_partitions*: Here you can specify a list of partitions which should be removed during partitioning. Alternatively, *auto* removes all partitions.

- *partition_start*: A whole number value in megabytes, which specifies where the partitioning should start.

- *partition<NUMBER>_name*: The name of the partition.

- *partition<NUMBER>_size*: The size of the image. Here you can either specify a numerical value in megabytes, a percentage or *expand*. expand then uses the remaining available space on the disk.

- *partition<NUMBER>_fs*: The file system to be used, e.g., ext4.

- *partition<NUMBER>_mountpoint*: The directory under which the file system should be mounted.

- *partition<NUMBER>_image_mount*: Uses true/false to specify whether the file system should be mounted in the image as standard.

- *partition<NUMBER>_copy_files*: Specifies whether the partition should be copied during an image update. Usually only required for the boot partition.

8.3. Configuring an encrypted disk

Feedback

A script can be mounted for further partitioning steps such as setting up an encrypted hard drive.

The *ucc-image-toolkit* package contains the file `/usr/share/doc/ucc-image-toolkit/example/custom_partition.example`, which can be used to set up an encrypted hard disk partition, for example. The necessary steps for the integration of the script in the initrd can be found at the beginning of the script.

8.4. Modification of existing images

Feedback

UCC images can be edited without the need for a complete rebuild, e.g.to preinstall an additional package or to perform various configuration modifications. The following steps need to be executed as root:

```
mkdir /mnt/img
mount -o loop /var/lib/univention-client-boot/IMAGENAME.img  /mnt/img/
chroot /mnt/img
( perform arbitrary changes.. )
sync
exit
umount /mnt/img
```

After modifying the UCC image the MD5 checksums need to be recalculated. The MD5 sums determine whether a rolled-out image has been modified:

```
md5sum /var/lib/univention-client-boot/ucc-1.0-rev3-desktop-image.img \
> /var/lib/univention-client-boot/ucc-1.0-rev2-desktop-image.img.md5
```

Chapter 9. Terminal services with UCC

In addition to the operation of stationary UCC clients, UCC also supports access to terminal services. Login is supported to:

• UCC terminal servers

• Windows terminal services via the RDP protocol

• Citrix XenApp

There are three possibilities for configuring access to a terminal service:

• An interactive selection of the session by the user during login to LightDM (see Section 6.1.1)

• A user login to LightDM where a session is forcibly specified by the administrator

• Automatic session selection where login is performed with a guest user. In this case, no login dialogue is shown.

9.1. UCC terminal services

Feedback 💬

9.1.1. Installation

Feedback 💬

The UCC standard desktop is based on KDE Plasma and can also be provided for thin clients as a terminal server.

As a terminal server, a UCC system is setup with the standard desktop image. Then the *univention-ucc-application-server* package is installed and `univention-run-join-scripts` must be run. UCC terminal servers are registered as a service in the UCS management system.

The access to UCC terminal servers is performed with the session script *UCC-remote*. All applications are run on the UCC terminal server and only the graphic output transmitted to the thin client.

It should be noted that UCC terminal services are based on X11 forwarding, which are rather bandwidth-intensive compared to an optimised remote access protocol like RDP or Citrix ICA. For Linux-based desktop deployments it should be evaluated whether local installations might be more suitable for the intended scenario:

www.univention.de

- In comparison to a standard Linux desktop installation UCC offers very quick and easy client rollout.

- Thin client hardware based on the x86 architecture are niche hardware and often more expensive than a standard desktop PC. Many of the traditional benefits of thin clients (e.g. fanless operation) can also be found in current desktop PC hardware. In addition a setup of standard PCs avoids the need for terminal servers.

- In almost every environment some systems need to be mobile systems / notebooks. A rollout of stationary clients instead of thin clients ensure that a homogenous environment is used.

9.1.2. Assignment of users to terminal servers

Feedback

The UCC terminal server to be used can be assigned via a *UCC user session* user policy. One or several servers can be specified in the **UCC terminal server** input field. If more than one server is configured, the server with the lowest system load is selected during login.

9.1.3. Configuration of graphic transmission

Feedback

The screen content output can be transmitted in two different ways, which must be compared and selected depending on the application scenario and the available thin client hardware:

- Transmission of the data via SSH-tunnelled X forwarding

- Transmission of the data via pure X forwarding

The transmission via SSH offers the advantage of an encrypted transmission and the optional compression of the data considerably reduces the bandwidth requirement. However, data encryption can cause bottlenecks in cases such as streaming videos, which require large bandwidths. The SSH-tunnelled access is also not suitable for use with very old thin client hardware.

The standard setting is transmission via SSH-tunnelled X forwarding; it is possible to switch back to pure X forwarding for older hardware. To enable X forwarding, the Univention Configuration Registry variable `lightdm/xserver/allowtcp` must be set to *true* on UCC clients and LightDM restarted.

The encryption algorithms used by SSH can be adapted via the Univention Configuration Registry variable `ucc/session/remote/ssh/cipher`. SSH compression can be disabled with the Univention Configuration Registry variable `ucc/session/remote/ssh/compression`.

As standard, UCC uses a KDE profile optimised for remote operation on terminal servers, in which some graphic-intensive effects are disabled. The use of this profile can be disabled per UCC terminal server by setting the Univention Configuration Registry variable `ucc/session/remote/profile` to false.

The integration package *libreoffice-kde* (installed as standard) provides improved integration of LibreOffice in the KDE desktop environment. However, these integration packages also result in a considerably increased graphic throughput when browsing the menus. To reduce the data quantities transmitted in terminal service operation, *libreoffice-kde* can be uninstalled on UCC terminal services.

9.1.4. Session timeouts

Feedback

The terminal server and the client send keep alive messages regularly (by default every 100 seconds). If the client has not been reached after the third attempt (i.e., 300 seconds = five minutes), the server terminates the connection (and vice versa: the client also terminates the connection if the server cannot be reached). The value for the test on the server can be set using the Univention Configuration Registry variable `sshd/clientAliveInterval` and on the client using the Univention Configuration Registry variable `ucc/session/remote/session/timeout`.

9.1.5. Sound output

Sound output in the terminal server session is transmitted via the sound server PulseAudio. The sound transmission can be disabled by setting the Univention Configuration Registry variable `ucc/session/remote/disable-sound` to *yes* on the UCC client.

9.1.6. Access to USB mass storage devices on the thin client

A USB mass storage device attached on the thin client (see Section 5.2) is integrated via a KDE autostart script during login. This generates a KDE file bookmark, which creates a connection to the mount directory on the thin client via the FISH protocol. This bookmark is displayed as a separate drive in the file manager Dolphin, for example. In applications which do not use the KDE dialogues (e.g., Firefox), the files firstly need to be saved in another directory and then copied to the USB stick in Dolphin.

The authentication of the access is performed with Kerberos; there is no need to enter a password manually. During the first access to the client, the SSH host key must be confirmed.

9.2. RDP terminal services

UCC supports login to Windows 2003-based and Windows 2008R2-based Windows terminal servers via the RDP protocol. The Windows terminal servers can be joined in the UCS domain or alternatively the access can be performed against an external domain.

The login is performed via the *RDP* session script installed as standard, which uses `freerdp` for the access. The password entered by the user during login to LightDM is cached by a PAM module and automatically provided to Freerdp, i.e., it is not necessary to enter it again when logging in to the terminal server.

The RDP client Remmina is provided as a client with which an RDP connection can be configured and started on the desktop.

9.2.1. Assignment of the terminal server and the Windows domain

The terminal server and the Windows domain of the terminal server can be specified per user via a *UCC user session* user policy. Alternatively, the server and the domain can also be specified per client by setting the Univention Configuration Registry variables `rdp/domainname` and `rdp/server`.

`rdp/user` can be used to specify a different user name from the current one during login.

9.2.2. Access to USB mass storage devices on the thin client

A mass storage device mounted on the thin client (see Section 5.2) is mounted in the session if the Univention Configuration Registry variable `rdp/redirectdisk` is set to *true*. The transmission is performed via a session channel of the RDP protocol.

9.2.3. Networklevel authentication / certificate approval

The RDP client does not use the "Network Level Authentication" (NLA) authentication method as standard. If NLA is enabled on the terminal server, this can be enabled by setting the Univention Configuration Registry variable `rdp/checknla` to *true*.

Verification of the login certificate is also disabled as standard. It can be enabled by setting the Univention Configuration Registry variable `rdp/ignorecertificate` to *true*.

In special cases, it may be necessary to disable the TLS encryption of the RDP connection entirely. This is done by setting the Univention Configuration Registry variable `rdp/checktls` to *false*.

9.2.4. Sound output in the RDP session

As standard, the sound output in the RDP session is transmitted via an RDP session channel. The sound output can be disabled by setting the Univention Configuration Registry variable `rdp/disable-sound` to *true*.

9.2.5. Further options for the RDP session

The Univention Configuration Registry variable `rdp/keyboard` can be used to configure a different keyboard layout for the RDP session from that of the current client. The layout is specified in the same format as the Univention Configuration Registry variable `xorg/keyboard/options/XkbLayout`.

The Univention Configuration Registry variable `rdp/additionaloptions` can be used to provide any additional options to freerdp (e.g., to enable additional plugins).

`rdp/geometry` can be used to specify the screen resolution.

`rdp/clienthostname` allows you to specify a different host name from the current computer name in the RDP session.

9.3. Citrix XenApp terminal services

UCC supports access to Citrix XenApp terminal servers. This documentation refers to Citrix XenApp 6.5 Enterprise on Windows Server 2008R2, which uses a Windows 2008R2 domain controller and the Citrix Receiver 12.1.

Citrix XenApp supports two login methods:

• Access to the XenApp terminal server is configured by an ICA session file in which the connection parameters are configured.

• The access is performed via a Citrix Farm web interface the user logs in to. During the login, an ICA file tailored to the user is generated, which is started via a browser plugin in the Citrix Receiver client.

UCC only integrates the browser-based login method.

9.3.1. Installation

To set up the session script *XenApp* on a client, the *univention-ucc-session-xenapp* package must be installed (see Section 4.3). It also installs some packages required by the Citrix Receiver. Then the Univention Configuration Registry variable `citrix/webinterface` must be set to the URL of the Citrix Farm web interface. The session script then opens the web interface directly in Firefox during login.

The Citrix Receiver cannot be supplied with UCC and must be downloaded from the Citrix website as a DEB package and installed on the client. [1] Version 12.1 is needed as the minimum version. Citrix Receiver 13 is not yet supported in UCS 1.0.

The following steps describe how to install the Citrix Receiver package into an existing UCC image. Due to a bug in the Citrix Receiver package these steps need to be performed on a 32 bit system! During the installation of `icaclient` and `ctxusb` the EULA needs to be confirmed.

```
mkdir /mnt/img
mount -o loop /var/lib/univention-client-boot/IMAGENAME.img /mnt/img/
cp ~/icaclient-12.1.0_i386.deb ~/ctxusb-2.2.0_i386.deb /mnt/img
```

---

[1]http://www.citrix.com/downloads/citrix-receiver/receivers-by-platform/receiver-for-linux-121.html

```
chroot /mnt/img
dpkg -i icaclient-12.1.0_i386.deb
dpkg -i ctxusb-2.2.0_i386.deb
sync
exit
umount /mnt/img
```

The Citrix Receiver uses /dev/random as a randomness source as standard. /dev/random blocks access if insufficient entropy is available from hardware sources. This is the case on many thin clients. If the Univention Configuration Registry variable citrix/linkdevrandom is set to *true*, /dev/random is converted to a symbolic link to /dev/urandom which prevents these delays.

If the Citrix web interfaces performs authentication against an Active Directory domain separate from UCS, it is possible to configure a login-less access to the web interface by setting the Univention Configuration Registry variable lightdm/autologin/session to *XenApp* and the Univention Configuration Registry variable lightdm/autologin to *yes*.

9.3.2. Sound transmission / Access to USB storage devices on the thin client

Feedback 🗩

Configuration parameters such as full screen display or the sound transmission are configured in the Citrix Farm settings. They are then saved in the ICA file generated for the user during login and implemented by the Citrix Receiver.

An USB storage device on a thin client (see Section 5.2) is available under Drive Z: in the Citrix session.

9.3.3. Accelerating the playback of Flash videos

Feedback 🗩

The Citrix client offers the possibility of optimising the playback of Flash videos: instead of streaming the video on the server and transmitting every image, the video is transmitted to the client and played locally in the terminal session. This requires the installation of the Flash plugin on the UCC client (included in the default settings).

Bibliography

[ucs-manual] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-3.1.html.

[ucs-manual-multiedit] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/handbuch-3.1.html#central%3Auser-interface%3Aedit.

[ucs-manual-cron] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-3.1.html#computers%3AExecuting_recurring_actions_with_Cron.

[ucs-manual-pxeboot] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual.html#ip-config:Configuration_of_boot_server/PXE_settings.

[ubuntu-repositories] Ubuntu Community Wiki. 2013. *Repositories Ubuntu*. https://help.ubuntu.com/community/Repositories/Ubuntu.

[ucs-manual-uvmm] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-3.1.html#uvmm:chapter.