univention
be open.

Univention Corporate Client 3.0

Manual for administrators

Version 3.0
Date: 2016-08-16

Univention GmbH
Mary-Somerville-Straße 1
28359 Bremen
Deutschland
feedback@univention.de

univention
be open.

Table of Contents

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.

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

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

Unity is used as the basis for the images (Version 16.04 in UCC 3.0). Univention provides two preconfigured images: a minimal image for thin clients and a larger image for 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 9.1). In contrast to the 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 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 supports both a local desktop based on Ubuntu and working on terminal servers (RDP, Citrix XenApp). Access to web-based services can also be configured using a full-screen Firefox browser session. A UCC desktop system be used both in the company network and in mobile use (all user and group information are cached locally for that).

A UCC system is usually installed over a network using PXE. The rollout can be performed fully automatic without user interaction (see Section 4.4).

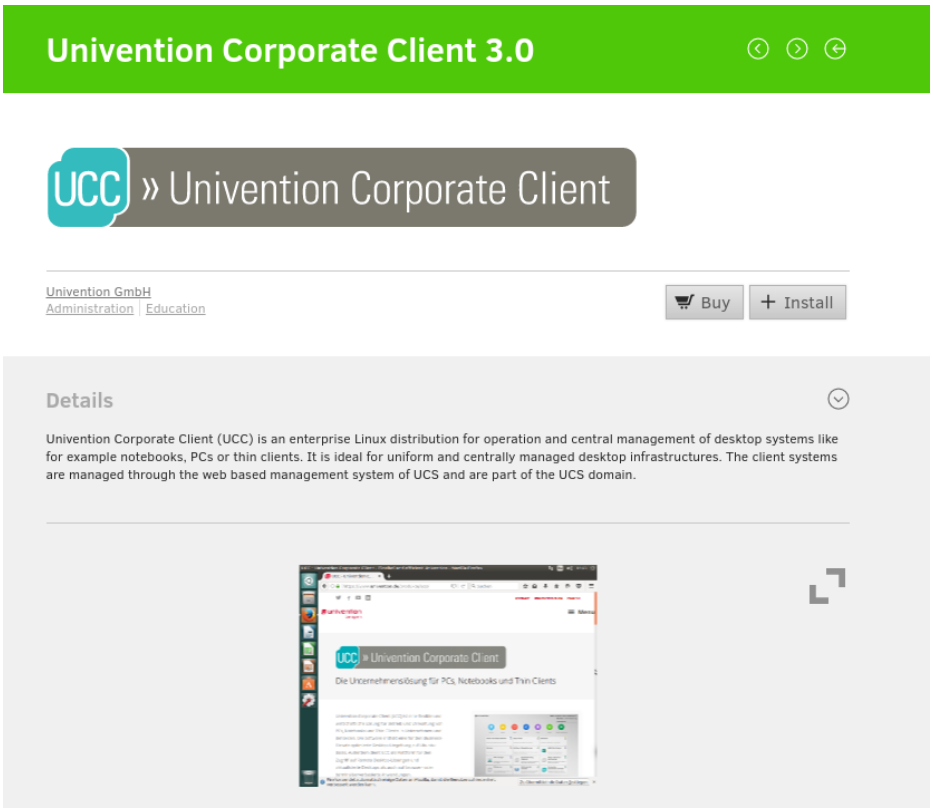
The CompactFlash storage media typically integrated in thin clients are only designed for a limited number of write operations. Thin clients in UCC are thus started with an OverlayFS file system so that all write accesses on the storage media of a booted system are only performed in the system memory 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 4.1 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). They are automatically installed on the master domain controller and all backup domain controller via the Univention App Center.

- 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 Univention Management Console module and then distributed locally to the clients. 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 provided by Univention.

UCC clients use the 32-bit Intel architecture (i386) for thin client images, and amd64 for desktop images.

2.1. Installation

Feedback

The UCC server can be installed on any UCS server role (master domain controller, backup domain controller, slave domain controller or member server). All available errata updates should be installed on that system.

In the Univention App Center, select the *Univention Corporate Client* application and click on **Install**. The integration in the UCS management system (UMC modules and LDAP schema extensions) are automatically installed on the master domain controller and all backup domain controller via the Univention App Center.

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

The join scripts are automatically run on master domain controller and backup domain controller systems during the installation of the UCC app. The **Domain join** UMC module must be run on slave domain controller and member server installations and the **Execute all pending join scripts** option selected for the UCC server to be ready for use.

Following the installation, the initial configuration is performed via a wizard in the Univention Management Console (see Section 3.1) or via manually configured policies. The UCS wizard is recommended for the initial setup for small to medium-sized installations.

UCC can be installed on more than one server, e.g., if UCC clients are to be operated at more than one site. Further information can be found in Section 4.7.

2.2. 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. The images are downloaded via a Univention Management Console module, see Section 2.3.

UCC systems operated with these images must have at least 512 MB of system memory available. Since UCC 3.0 is based on Ubuntu 16.04, all x86 and amd64 desktop hardware which is supported in Ubuntu 16.04 is also supported in Univention Corporate Client. You can either test whether your device is compatible or contact the hardware supplier for compatibility information.

The thin client image offers a minimal desktop and support for accessing terminal sessions on Windows. UCC thin client images integrate the Citrix Receiver for accessing Citrix terminal services. 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 Ubuntu 16.04 desktop and support for terminal sessions to Windows (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 5.3)

2.3. Downloading/removing UCC images

Feedback

The UCC images are not delivered in the Debian package format (the format is not best-suited to files in the gigabyte range). Instead, UCC images can be downloaded via the Univention Management Console module **UCC Images**. A list of all available images is shown when the module is started. Already downloaded images are shown as **installed**; not yet installed images as **available**. Each image is furnished with a version number;

the official UCC images are updated regularly and - if available - shown with an updated version number. The **Download** and **Remove** options can be used to add and remove images.

The images are downloaded from http://ucc-images.software-univention.de/download/ucc-images/. A local UCC mirror can also be used, see Section 2.3.2.

Alternatively, images can also be managed via command line tools: `ucc-image-download` can be used to download images. The individual files of the image are referenced via a specification file containing the file names and SHA-256 hashes. The hash values are checked as part of the download procedure in order to detect erroneous transmissions. The parameter `-s` is used to provide the name of the specification file on the mirror. The full list of available parameters can be queried with the `-h` option. 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 specification file.

2.3.1. Setting the initial root password for UCC images

Feedback

The root password of the installed UCC 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 UCS server is set as the root password on the images. 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-3.0-desktop-image.img -p
```

2.3.2. Operating a local UCC image mirror

Feedback

If you are running 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.

Chapter 3. Management of UCC systems in the Univention Management Console

3.1. Initial setup of a UCC environment

Feedback

A Univention Management Console wizard is provided for the initial configuration of a UCC environment. It guides you through the basic setup of a UCC environment with thin clients and/or desktop clients. Different standard policies are created and configured. The setup wizard is suitable for small to medium-sized environments. The policies can also be manually configured in the Univention Management Console for more complex requirements in which different policies are to be used for different containers of the LDAP directory or multiple DHCP subnets are to be operated. The policies required for each option are listed in the respective chapters.

The setup wizard is started via the Univention Management Console module **UCC Setup**. In the main menu, you can first select whether to set up thin clients and/or desktop systems. UCC images will be downloaded if required.

UCS offers 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 IP addresses: When creating a UCC client the next free IP address of the network is selected automatically. Also, DNS and DHCP settings are configured automatically.

In the UCC wizard it is now possible to select an existing network object in the **Network configuration** dialogue or create a new one. During the installation of a UCS system, a network object with the name *default* is created as standard. It uses the network of the master domain controller. If only a certain IP segment is to be used for the UCC systems, a new network object can be created with the **Specify a new IP segment** dialogue. For example, if the IP addresses 192.168.100.100 to 192.168.100.200 are used for UCC systems, *192.168.100.0* must be entered as the **Network address**, *24* as the **Netmask** and *192.168.100.100* / *192.168.100.200* entered as the **First IP address / Last IP address**.

The network configuration of UCC clients is managed through DHCP in nearly all cases The wizard checks whether a default gateway is assigned via DHCP. If this is not the case, a dialogue window opens in which the gateway can be configured. In the default setting, fixed IP addresses are assigned only to clients registered in the LDAP.

The next menu item allows you to select whether desktops and/or thin clients should be configured. No additional configuration is required for Linux desktop systems. The wizards for setting up the thin client access on terminal services are described in the following sections:

- Thin client access to Windows terminal servers (Section 10.1)
- Thin client access to Citrix terminal servers (Section 10.2)
- Thin client access to a website (Section 7.4)

Once the wizard is finished, the UCC clients now need to be registered in the Univention Management Console. This is described in Section 3.2.

3.2. Managing 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. The UCC setup wizard automatically creates three computer containers for thin clients (`cn=computers, cn=ucc-thinclients`), desktop systems (`cn=computers, cn=ucc-desktops`). These should be selected in the **Container** input field depending on the type of the UCC client.

In the default setting, the dialogue window for creating a UCC system only shows the most important input fields. Clicking on **Advanced** shows all the options. This is only necessary in exceptional cases.

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

- The **Hostname** 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`. It is required for DHCP.
- A **Network** needs to be selected: generally the network configured in the UCC Setup wizard. The **IP address** is suggested automatically and can be adjusted if necessary.

Each UCC client must be registered in the DNS and DHCP. The network object assigns these entries automatically. If a UCC client is created without a network object (which is only needed in exceptional cases), it is important to ensure that the entries for the **Forward zone for DNS entry**, **Reverse zone for DNS entry** and **DHCP service** are configured.

The assigned name server is preconfigured automatically. If it is necessary to adjust the assigned server, the **DHCP DNS** *default-settings* policy must be edited.

Clicking on **Next** configures the assigned UCC image and the boot version. The boot versions are documented in Section 4.1.

UCC clients save their currently installed image in the UCS `LDAP`. This makes it possible to search for UCC clients with outdated images and configure them to update their image on the next boot. In the **Computers** module extended search options, one can search for the object **Type** `Univention Corporate Client`, and the property `image name`. Multiple objects can then be edited simultaneously to update their boot settings.

3.3. Monitoring UCC systems with Nagios

Feedback

Univention Corporate Server integrates Nagios for the monitoring of systems and services. UCC systems can also be integrated in the Nagios monitoring. To this end, the **Nagios support** option must be enabled under **Options** in the Univention Management Console for the systems to be monitored on the computer object. More information on Nagios can be found in the UCS manual [ucs-manual-nagios].

In the default setting, the NRPE service is not installed on UCC systems. That means that only remote Nagios checks can be applied.

Chapter 4. Rollout of UCC systems

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

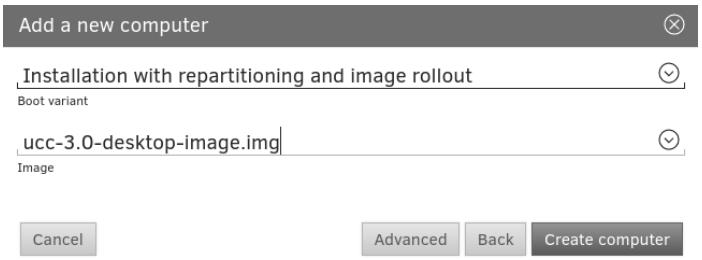
When the image is installed, the image installation tool checks whether there is already a computer account available for the client and uses it. If the computer name is not stored in advance, the name can be specified interactively during the installation. The recommended rollout procedure is creating the UCC systems in the Univention Management Console in advance. See Chapter 3 for more information on managing UCC systems in the Univention Management Console.

4.1. Rollout of images

Feedback

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 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.

Figure 4.1. Assigning the desktop image to a UCC client



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].

On UCC systems, user-specific data such as the home directory 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 image configuration, see Section 9.2. It is also possible to perform completely new partitioning schemes - e.g. an encrypted hard drive - with an adapted partitioning script, see Section 4.2).

UCC clients can be operated in five different modes, which can be assigned via the **Boot variant** field. The client must be configured for PXE boot in the BIOS.

- **Live boot** Here the image is started via PXE and mounted via NFS. 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 read-only access (from a live DVD or as in this case from an 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 4.8.

- **Installation with repartitioning and image rollout**: This mode is used for the initial installation of a UCC client. It is also required whenever a UCC client should be reinstalled completely or switched to a different partition scheme. The partitions of the system are setup as configured in the image configuration. A prompt must be confirmed before the partitioning begins (it can be disabled using the boot option `force_partition`, see below). After the installation of the image, the system is joined into the UCS domain.

  ## Caution

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

- **Image boot with update check** is used to update an existing UCC installation to a new version. It is detected whether the installed image differs from the image to be installed. If that is the case, the UCC image on the system is replaced. In contrast to the partition option above, no new partitioning occurs. All user data on the `/home` partition is retained. This only works if the computer boots via PXE, as changes in the initrd / initrd system architecture may otherwise cause errors.

- **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 a successful installation performed with **Image boot with update check** or **Installation with repartitioning and image rollout**, the system returns to this boot mode automatically.

- **Local boot**: In the boot versions **Image boot without update check** and **Image boot with update check**, the UCC system is started with PXE and the locally installed system started following the update check. If this option is enabled, a special PXE configuration is created for the computer, with which the PXE firmware of the system does not perform a PXE boot, but instead starts the locally installed system directly. This is comparable to a certain extent with if the boot order in the BIOS of the system were changed over to a local disk, but does not require any adaptation of the BIOS.

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

`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).

`force_partition`
: If an image is rolled out and the **Installation with repartitioning and image rollout** option used, a warning message appears reminding you that all the data on the hard drive will be lost if the repartitioning is performed. This warning message needs to be confirmed. If the `force_partition` boot option is assigned, the security prompt is not shown any more.

The **Dedicated image server** select box allows to select a dedicated server for the installation/update of the particular UCC client. During the rollout the dedicated image server is the first choice for downloading the image to the client. In order for clients to download the kernel and initramfs during PXE boot, a PXE boot policy also has to be configured, see Section 4.7.

4.2. Custom partition scripts / Configuring an encrypted disk

Feedback

In the standard setting the partitioning scheme is configured in the image configuration. A different partitioning can be configured using partition scripts. They are stored on the UCS server(s) in the directory `/var/lib/univention-client-boot/partition-scripts/`. The file name below that directory needs to be configured in the **Additional boot options**, see Section 4.1) using the command `partition_script=FILENAME`. The filename is specified relative to the directory, e.g. `partition_script=desktop_encrypted.example`.

An example configuration which configures an encrypted LUKS hard disk for the UCC desktop image is shipped as `desktop_encrypted.example`.

4.3. Domain join of UCC systems

Feedback

Only UCC clients, which are joined into a UCS domain can be configured centrally. Unjoined clients can 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 4.1). 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.

4.4. Configuration of a fully automated rollout

Feedback

In the default setting, a user name and password must be specified when joining the domain. The rollout of UCC systems can also 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 3.2), the following steps are necessary:

- An image must be generated in which the interactive confirmation of he partitioning is disabled. This can be achieved by setting the option `continuation_prompt` to `false` (see Section 9.2). Alternatively the boot option `force_partition` can be used, see Section 4.1).
- 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. Alternatively, the account can be specified with `-u`, the domain with `-d` and the password with `-p`.
- The clients are then rolled out fully automatically without user interaction.

4.5. Roll-outs 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 Blu-ray disks.

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

The client to be installed must be created in the UMC computer management first (see Section 3.2), otherwise it doesn't have an IP address assigned and the domain join would fail.

4.6. Persistently stored system settings

Feedback

System data which must be preserved during a UCC update (e.g., the join status) are stored 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. Ten megabytes of disk space are reserved for storing the Univention Configuration Registry settings and the persistent configuration files.

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

Feedback

The rollout of UCC systems usually occurs via PXE (see Section 4.1). If UCC is operated in a single server environment the server distributing the IP addresses 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].

4.8. OverlayFS on thin clients

Feedback

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

In UCC thin clients 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 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.

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 5.1). This variable allows tools such as `univention-ucc-software-update` to detect whether they are running on a thin client using OverlayFS.

To force a thin client to boot in rw mode without changing the configuration the command `univention-ucc-force-rw-boot` can be used. A reboot of the thin client is required afterwards.

4.9. Rollout of UEFI systems

Feedback

Univention Corporate Client uses a BIOS-based boot by default. Alternatively, for systems which no longer support a BIOS boot, it is possible to generate UCC images with which the rollout and operation can be performed via the *Unified Extensible Firmware Interface* standard.

Not all UEFI-compatible systems also support UEFI booting via PXE. This should be checked in advance and consideration given to updating the UEFI firmware.

An image configuration is delivered with the image build tool for UEFI systems: `/usr/share/doc/ucc-image-toolkit/example/ucc-desktop-efi.cfg.gz`. Information on building an image can be found in Section 9.1.

As standard, the `pxelinux.0` boot loader is used for the rollout of BIOS-based systems and assigned in the Univention Management Console via a **DHCP Boot** policy. A UEFI-compatible boot loader must be assigned via this type of policy for the UEFI rollout. `syslinux.efi32` must be assigned as the **Boot filename** for i386 systems and `syslinux.efi64` for amd64 systems.

If a UEFI-compatible image has been generated and the DHCP boot policy defined, the rollout of a UEFI system is not different from the standard rollout via the BIOS.

4.10. Rollout problems with subsequently enlarged hard disks

Feedback

If a hard disk has been subsequently enlarged - typically if a virtualized disk is used - the rollout may encounter GPT partition data from the previous installation procedure, which no longer correspond to the current size of the disk. Generally speaking, when enlarging the memory of a virtualized system, it is more advisable to add an additional disk.

As a workaround, the system can be started with the `debugshell=y` boot option (see Section 4.1 and the GPT table rewritten with the following command:

```
parted -s PARTITIONDEVICE mklabel GPT
```

4.11. Operating thin clients without persistent access to LDAP servers

Feedback

In the default configuration UCC thin clients require a connection to an LDAP server to start and receive their configuration from LDAP. For special configurations UCC can also be configured to cope with inaccessible LDAP servers. The exact setup may vary a lot depending on the setup so the following items are not a comprehensive list of necessary changes, but rather building blocks to adapt to such a setup:

- The Univention Configuration Registry variable `ucc/ldap/network/timeout` can be used to configure a timeout for connecting to the LDAP server, by default ten seconds.

- By default the policies which apply to a thin client are retrieved from LDAP during system startup. If the package ***univention-ucc-eval-policies-on-join*** is installed into a UCC image, the system policies are retrieved during the join of the thin client and stored in the image (`/var/cache/ucc/client-policy-*`) These files can be treated as fallback values: If the thin client is able to connect to an LDAP server during startup, the current values are fetched from LDAP and overwrite the existing values in `/var/cache/ucc/` temporarily (since the thin client image uses OverlayFS, see Section 4.8). If the thin client cannot connect to an LDAP server the local values are used.

- Instead of only writing the fallback values during the system rollout, it is also possible to cache them on every system start: In that case the package ***univention-ucc-eval-policies-on-boot*** needs to be installed instead of ***univention-ucc-eval-policies-on-join***. It should be noted that this leads to a write access on the thin client storage on every boot! This may lead to problems on thin clients with storage media which is only designed for a limited amount of write accesses (such as CompactFlash).

Chapter 5. Configuration of UCC systems

5.1. Setting of Univention Configuration Registry settings on UCC clients

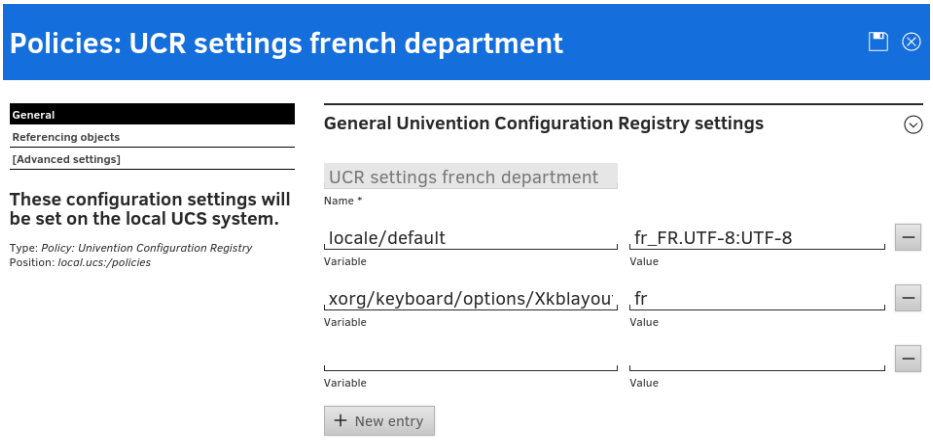
The configuration of UCC system settings is mostly performed using Univention Configuration Registry. Typically, these settings are not saved locally on the UCC client systems, but rather via UCR policies via the LDAP.

The UCC setup wizard (see Section 3.1) creates three Univention Configuration Registry policies automatically, which are linked to the containers for thin clients and desktops: These policies can be edited directly:

- `ucc-common-settings` is linked to the `cn=computers` container, and thus applies for thin clients and desktops.
- `ucc-thinclient-settings` is linked to the `cn=computers,cn=ucc-thinclients` container, and thus only applies for thin clients.
- `ucc-desktop-settings` is linked to the `cn=computers,cn=ucc-desktops` container, and thus only applies for desktops.

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 5.1. 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 4.8).

5.2. Definition of Cron jobs / executing commands at system startup

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].

Cron jobs can also be used to execute commands during system startup using the `@reboot` option. The following Univention Configuration Registry variables (see Section 5.1) configure the execution of `/usr/bin/example` as the user root during the system boot. `COMMAND1` can be replaced with arbitrary identifiers:

```
cron/COMMAND1/command=/usr/bin/example
cron/COMMAND1/time=@reboot
```

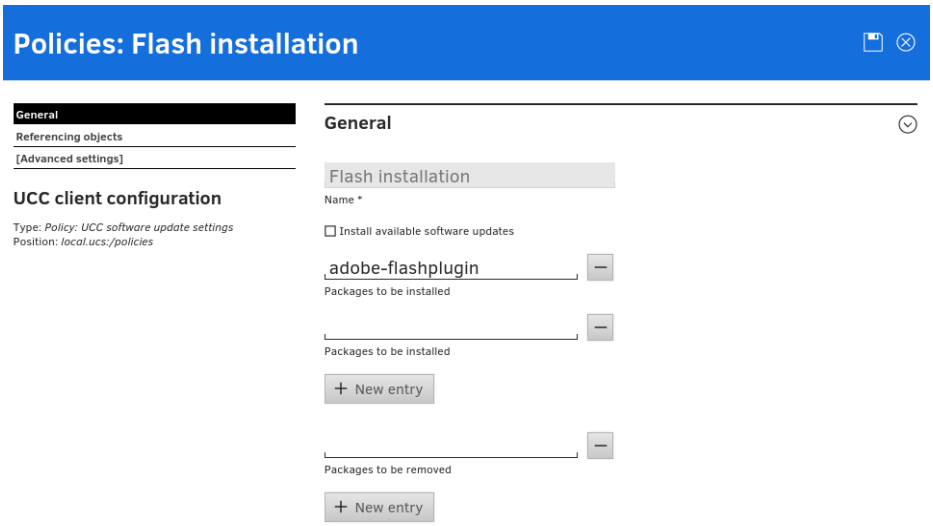
5.3. Software updates / Installing additional software

Feedback

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 update can also be started manually by running the `univention-ucc-software-update --force` command.

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

Figure 5.2. 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.

Caution

Always test UCC software updates on a test system 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?

It is not possible to update the kernel on thin clients; a new image must be rolled out instead.

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

```
apt-get update
apt-get install emacs24
```

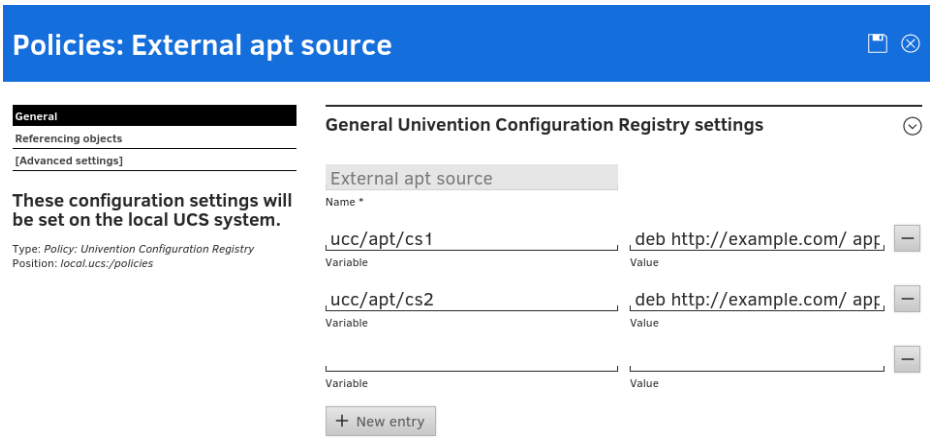
The installation/updates are logged in `/var/log/univention/software-updates.log`.

In the default setting, only the UCC repositories are used as package sources. Univention Configuration Registry policies can be used to add new package sources (see Section 5.1). The variables must be specified in the form `ucc/apt/ID1` = `apt source entry`, e.g.:

```
ucc/apt/cs1=deb http://example.com/ application/all/
```

```
ucc/apt/cs2=deb http://example.com/ application/i386/
```

Figure 5.3. Example UCR policy for configuring an apt source



Thin clients employ an OverlayFS (see Section 4.8). 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.

5.4. Configuration of the keyboard layout / locale

Feedback

In the standard setting, the keyboard layout and the language setting (locale) of the UCS system acting as 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.

5.5. Configuration of the time zone / time server

Feedback

In the standard setting, the time zone of the UCS system acting as 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*. Further information on configuring Univention Configuration Registry variables can be found in Section 5.1.

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. Further information on configuring Univention Configuration Registry variables can be found in Section 5.1.

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

5.6. Print server configuration

Feedback

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. Further information on configuring Univention Configuration Registry variables can be found in Section 5.1.

5.7. Remote logging

Feedback

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 UCS system acting as PXE server.

The log files are stored in the `/var/log/univention/ucc-clients/` directory. A separate log file is maintained for each client. The log files are also rotated with Logrotate, e.g., `syslog-client01.log`, `syslog-client01.log.1`, etc.

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.

5.8. SSH access to UCC clients

Feedback

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

5.9. Boot-splash startup animation

Feedback

A startup animation (boot-splash) is displayed when a UCC client is started. It 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 UCS system acting as PXE server can be set to `no` to deactivate it completely.

5.10. Custom start scripts

Feedback

Clients can sync and execute custom start scripts that are placed on the UCC image server. This is a way to configure individual settings on clients during boot time.

The Univention Configuration Registry variable `ucc/custom_start_scripts/enabled` has to be set to `yes` on UCC clients, e.g. by a Univention Configuration Registry variable policy. for the feature to be enabled. Only if this is configured, the following happens during UCC boot time:

- The content of the directory `/var/lib/univention-client-boot/custom_start_scripts` from the image server is synced to the UCC client directory `/usr/lib/univention-custom-start-scripts`.
- `run-parts` is run on `/usr/lib/univention-custom-start-scripts`. Filenames have to conform to the `run-parts` policy as seen in the manpage, to execute files in the directory.

A simple example script is included and available in `/usr/share/ucc-pxe-boot/custom_start_scripts_example/`. It is a simple script which installs a ***pam_mount*** config file, so that the user's home directory is mounted at `~/NetworkStorage`. The example config file has to be adapted to every UCS domain environment in order to work

Chapter 6. Hardware configuration of UCC systems

6.1. Network configuration

Feedback

The network configuration of UCC clients is generally performed via DHCP. The configuration of MAC and IP addresses, etc., occurs in the UCS management system, see Section 3.2.

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 permanent 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`.

6.2. 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 CD-ROM/DVD-ROM. `VFAT`, `NTFS` and `ext*` file systems are supported.

The mounting of mass storage devices is disabled on desktop systems (as mass storage devices are automatically mounted in the Unity desktop anyway). If you still wish to enable the function in exceptional cases, this can be done by setting the Univention Configuration Registry variable `ucc/mount` to `true`.

The local mount points are made available in Windows 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.

Filesystems directly written to devices (such as `/dev/sda`) are not mounted by default (only the respective partitions like `/dev/sda1`). If the Univention Configuration Registry `ucc/mount/blacklist/disable` is set to `true`, full partitions are mounted as well.

It is also possible to disable devices for the automatic mount. The Univention Configuration Registry variable `ucc/mount/blacklist` (space-separated list) can be used to configure a list of device names which are not mounted (`sda sdb sdc sdd sde` by default).

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 10).

6.3. Sound support

Feedback

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

- In RDP sessions to Windows terminal servers, audio is transported via an RDP channel.
- 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 10.

6.4. Managing drivers/kernel modules

Feedback

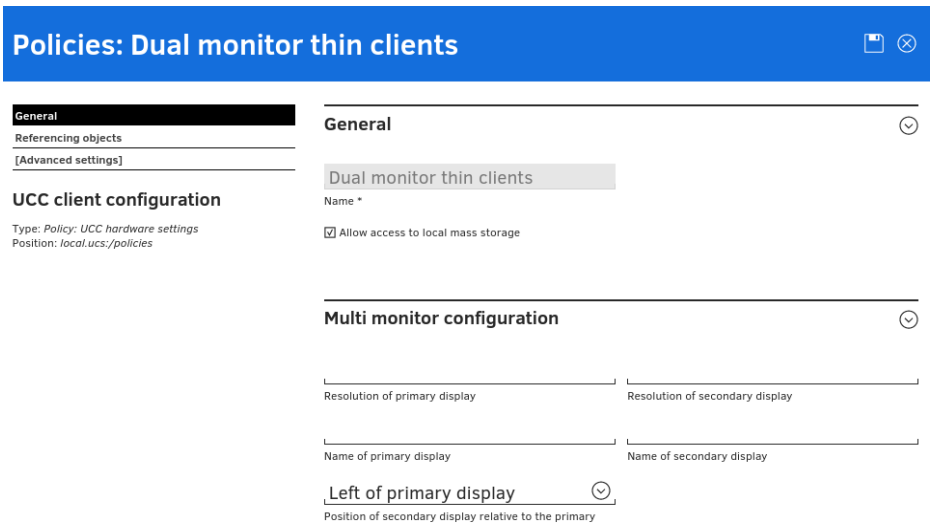
The drivers to be used are detected automatically during system start and loaded via the udev device manager. At this point, the necessary device links are also created under `/dev/`. If drivers are not detected, kernel modules to be loaded can be added via the Univention Configuration Registry variable `kernel/modules`. If more than one kernel module is to be loaded, these must be separated by a semicolon. The Univention Configuration Registry variable `kernel/blacklist` can be used to configure a list of one or more kernel modules for which automatic loading should be prevented. Multiple entries must also be separated by a semicolon.

6.5. Configuration of dual-display setups

Feedback

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

Figure 6.1. Configuring dual monitor display



Dual-display setups can be configured using a **UCC client configuration** computer policy in the UCS management system: This is primarily only relevant for thin clients; on desktop systems, the users can also configure their display settings autonomously via the Unity system settings.

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 7. User logins

7.1. User logins on LightDM

Feedback

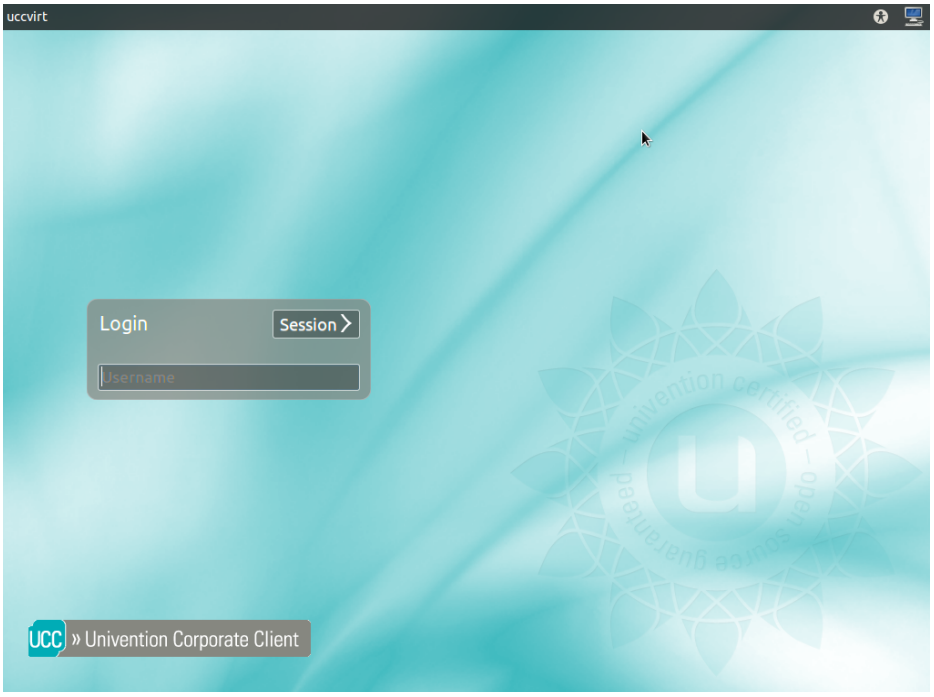
7.1.1. Session selection

Feedback

UCC uses LightDM as its login manager. When the UCC client is started, a login mask is shown. The user can choose between different session types using the **Session** menu.

If the UCC client is not yet joined or in live boots, an automatic login is performed with a temporary guest user. Such an automatic login can also be configured for joined systems, see Section 7.1.3

Figure 7.1. 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 7.2. Session selection at LightDM

The following session scripts are supported:

- Univention Corporate Client based on Ubuntu (Chapter 8)
- Citrix XenApp (Section 10.2)
- Microsoft Windows Terminal Server (Section 10.1)
- Firefox (with direct login to a configured website) (Section 7.4)
- LXDE (Lightweight X11 Desktop Environment) (Chapter 8)

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

Feedback

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. If the UCC environment was configured via the UCC setup wizard (see (Section 3.1), the setting is already preconfigured.

7.1.3. Configuration of an automatic login and session selection

Feedback

Instead of an interactive login, it is also possible to configure an automatic login. 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.

By default a temporary guest user is used for the automatic login. Alternatively, the Univention Configuration Registry variable `lightdm/autologin/user` allows the configuration of the user under which the automatic login should occur.

If an automatic login is configured, 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 7.5.

7.1.4. Session scripts

Feedback

Scripts can be run at different times during session setup and when exiting the session. All executable scripts 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 the greeter is started
- `/etc/lightdm/greeter-setup`: Is run if the greeter starts a session

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

Feedback

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

7.2. Local caching of user and group information

Feedback

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 7.3), 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.

If the Univention Configuration Registry variable `ucc/nss/update/force` is set to `true`, the user and group information is obtained during every login.

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.

7.3. Logins to offline UCC systems / password credentials caching

Feedback

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. When logging on with cached credentials, the message **You have been logged on using cached credentials** is displayed.

Password changes are not immediately visible to PAM modules executed later in the PAM stack; please refer to the release notes for more details.

7.4. Firefox session script

Feedback

The Firefox session script starts a Firefox web browser in a full-screen session. It can be used, for example, to access an intranet page directly from thin clients or to configure a groupware web client.

For setting up the Firefox access to a website, the **UCC Setup** wizard must be opened in the Univention Management Console. The **Configure direct web browser access to a preconfigured web site** option must be selected under **Thin client configuration** in the **Configuration of terminal services** submenu.

The website to be accessed should be entered in the **Automatically connect to this web site** input field. If the wizard is not used, the Univention Configuration Registry variable `firefox/startsite` must be configured.

The Firefox session script can be customized with the Univention Configuration Registry variable `firefox/session/cmd`. This variable can be set to a base64 encoded bash code snippet which is executed just before the Firefox command is called. The bash code can overwrite the Firefox command with

```
cmd=("/usr/bin/myfirefox")
cmd+=(--my-options $USER)
```

or supplement the default command.

```
cmd+=(--my-new-option-for-the-default-firefox-command ABC)
```

7.5. Registration of sessions in the Univention Management Console

Feedback

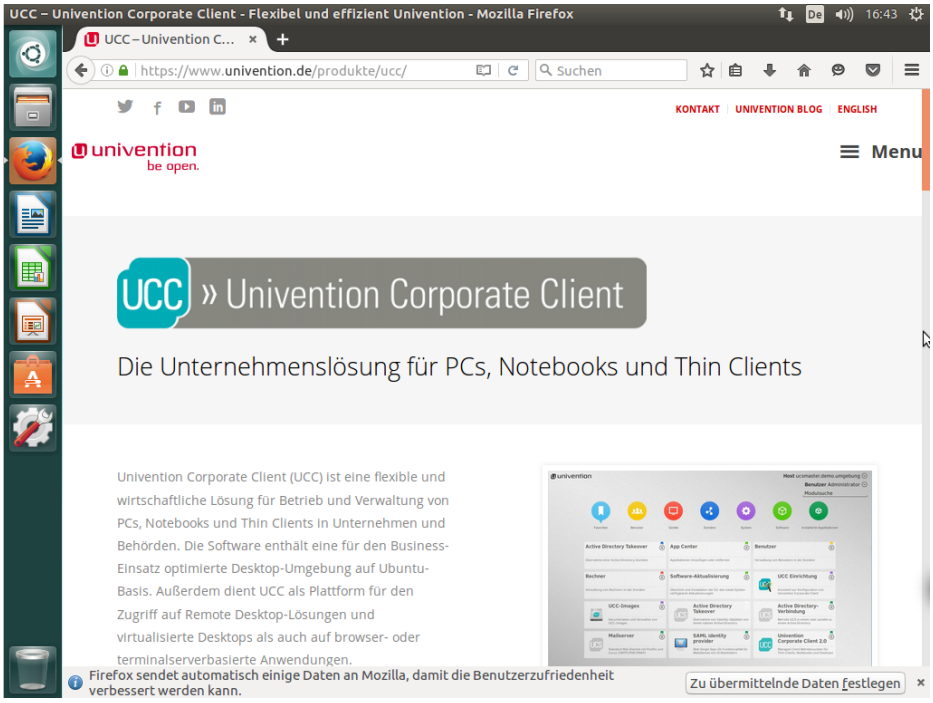
Sessions are registered in the Univention Management Console. New sessions can be created by selecting the UMC module **LDAP directory** and adding a **UCC session script** object below `cn=univention,cn=UCC,dc=Session`.

Chapter 8. Univention Corporate Client desktop environment

8.1. Introduction

Univention Corporate Client offers a desktop environment based on the Unity desktop. It offers a compilation of software components suitable for typical business applications.

Figure 8.1. Univention Corporate Client desktop



Extensive documentation and manuals for Unity can be found at https://help.ubuntu.com/lts/ubuntu-help/index.html.

LibreOffice is a 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 it 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.

8.2. Configuration of proxy settings for the desktop

Feedback

The proxy settings in Firefox and Unity can be centrally configured via Univention Configuration Registry variables provide by the package ***univention-ucc-proxy-settings*** (see Section 5.1). `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 Unity changes can be made in the dialogues, but they are discarded when clicking **Apply**.

Chapter 9. Generation of adapted UCC images

9.1. Image toolkit

Feedback

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

Image generation is performed with the `ucc-image` tool in the ***ucc-image-toolkit*** package. The images are defined via a configuration file (see Section 9.2). 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 specification file is generated, which is used when downloading a UCC image (see Section 2.3).

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

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. If no target directory has been specified, a temporary directory is created under `/tmp/`.

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.

9.2. Overview of image parameters

Feedback

The following configuration settings can be used to build a custom UCC image. We recommend using one of the standard configuration files as a template. The configuration file is then processed by the image toolkit, see Section 9.1). The configuration files can be commented with a hash (#):

General section

- *arch*: The system architecture, i386 or amd64. The official UCC images are provided as i386 for thin clients, and amd64 for desktops.

- *version*: The Ubuntu code name on which the image is based. It must be taken into account that the Univention modifications are only built and tested for a specific release, in the case of UCC 3.0 for Ubuntu 16.04 (xenial).
- *hostname*: The standard host name of an unjoined UCC client. The name is set to the name configured in the LDAP during 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 downloaded from the Univention server, it is adapted during the download, see Section 2.3. 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.

Software section

- *mirror*: Configures the mirror from which the Ubuntu packages are downloaded. We advise against using a standard Ubuntu mirror; some packages are built with patches in UCC. When a non Univention mirror is used, it is not possible to guarantee that these packages will be updated when Ubuntu packages are updated.
- *updates*, *security*, *backports*: Here, `true`/`false` can be used to specify whether, in addition to the standard release, updated bug fix packages (updates), security updates or back-ports should also be integrated into the image.
- *universe*, *multiverse*: These options (true/false) integrate additional archive suites from Ubuntu, see [ubuntu-repositories] for details.
- *sources_list*: Additional apt sources can be integrated here. Additional sources can also be added for an installed client via Univention Configuration Registry(see Section 5.3). This parameter is required for integrating apt sources as early as during the image generation.
- *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. Multiple packages need to be separated by newlines. The following packages are required on each UCC system as a minimum:
  - ***linux-image-generic***: The Linux kernel
  - ***univention-ucc-bootstrap***: A range of dummy init scripts which are run during generation of the image
  - ***univention-ucc-grub***: The integration packages for the boot loader Grub
  - ***univention-corporate-client***: This package integrates the central UCC services
- *packages_hold*: A list separated by newlines of one or more packages which are not to be updated. To this end, the packages are set to the *hold* installation status in the dpkg database.

Configuration section

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

Image section

- *version*: 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 inside the image file; 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 placed in the initrd.
- *kernel, initrd*: The Linux kernel of a UCC system is stored 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 generated which can be booted from USB or a DVD drive, see Section 4.5.
- *include_image_on_iso*: If set to true and if `iso` is specified, the UCC image is integrated into the ISO image.
- *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. This can be avoided with the `force_partition` boot option, see Section 4.1.
- *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.

9.3. Modification of existing images

UCC images can be edited without the need for a complete rebuild, e.g. to pre-install 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-3.0-desktop-image.img \
> /var/lib/univention-client-boot/ucc-3.0-desktop-image.img.md5
```

Chapter 10. Terminal services with UCC

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

- 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 7.1.1)
- Automatic session selection where login is performed with a guest user. In this case, no login dialogue is shown (see Section 7.1.3).

10.1. Windows terminal services (RDP)

Feedback

UCC supports login to Windows 2003/2008/2012-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 which uses the NeutrinoRDP client (a fork of the FreeRDP code base). The password entered by the user during login to LightDM is cached by a PAM module and automatically provided to NeutrinoRDP, 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.

10.1.1. Installation

Feedback

The session script for RDP (***univention-ucc-session-rdp***) is installed on desktop systems and thin clients in the default setting.

10.1.1.1. Installation using the setup wizard

Feedback

For setting up the RDP access to RDP terminal servers, the **UCC Setup** wizard must be opened in the Univention Management Console. The **Configure access to a Windows terminal server** option must be selected under **Thin client configuration** in the **Configuration of terminal services** submenu.

The host name of the RDP terminal server must be entered in the **Host name of terminal server** input field. If a Windows terminal server is used, the domain name must be entered in the **Domain name** input field.

If sound is to be transmitted to the accessing client from the terminal session, the **Enable sound** option must be enabled. The sound output in the RDP session is transmitted via an RDP session channel.

USB storage devices (USB sticks or CD/DVD drives), which can be inserted in the thin client, can be passed through to the RDP session. This is done by enabling the **Enable USB storage passthrough** option. Further details on the mounting of devices can be found in Section 6.2. The transmission is performed via a session channel of the RDP protocol.

10.1.1.2. Installation without the UMC wizard

Feedback

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`.

Mass storage devices mounted on the thin client (see Section 6.2) is available in the RDP session if the Univention Configuration Registry variable `rdp/redirectdisk` is set to `true`.

Sound output is enabled by default. It can be disabled by setting the Univention Configuration Registry variable `rdp/disable-sound` to `true`.

10.1.1.3. Advanced configuration

Feedback

10.1.1.3.1. Network level authentication / certificate approval

Feedback

The RDP client uses the "Network Level Authentication" (NLA) authentication method as standard. This can be disabled by setting the Univention Configuration Registry variable `rdp/checknla` to `false`.

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/tlsencryption` to `false`.

10.1.1.3.2. Further configuration options for the RDP session

Feedback

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`.

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

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

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

The RDP session script can be customized with the Univention Configuration Registry variable `rdp/session/cmd`. This variable can be set to a base64 encoded bash code snippet which is executed just before the RDP command is called. The bash code can overwrite the RDP command with

```
cmd=("/usr/bin/myrdpclient")
cmd+=(--my-options $USER)
```

or supplement the default command.

```
cmd+=(--my-new-option-for-the-default-rdp-command ABC)
```

10.2. Citrix XenApp and XenDesktop terminal services

Feedback

UCC supports access to Citrix XenApp and XenDesktop terminal servers. Citrix Receiver is included in UCC thin client images to connect to Citrix servers. This documentation refers to Citrix Receiver 13.3.

Citrix 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.

Access to a Citrix terminal service is performed via the *XenApp* session script. This opens a full-screen Firefox session with the login web interface of the Citrix installation. If the browser is closed, a menu opens in which you are offered the possibility to log in to Citrix again, shutdown the thin client or select another session.

10.2.1. Installation

Feedback

10.2.1.1. Installation using the setup wizard

Feedback

For setting up access to a Citrix terminal service, the **UCC Setup** wizard must be opened in the Univention Management Console. The **Configure access to a Citrix terminal server** option must be selected under **Thin client configuration** in the **Configuration of terminal services** submenu.

The **URL for Citrix farm login** option is used to configure the URL of the Citrix web interface. The session script then opens the web interface directly in Firefox during login.

Citrix Receiver version 13.4 is included in the UCC Thin Client image. Other Citrix Receiver versions may be included manually in a Thin Client image. It must be downloaded for the 32 bit Intel architecture as a DEB file using the download link provided and saved in a local directory. Support is only provided for the included Citrix Receiver. To include a different version, choose the option **Use custom receiver**

The UCC thin client image in which you wish to install the Citrix Receiver must now be selected in the **Please select the image(..)** field. After clicking on **Upload** and selecting the DEB file of the Citrix Receiver, it will be automatically integrated in the UCC image.

In the default setting, each user of the Citrix terminal server must confirm the end user license agreement (EULA) the first time he/she accesses the terminal server. If the **Confirm the End User License Agreement of Citrix Receiver** option is enabled, the license is confirmed automatically.

As the authentication during the Citrix login occurs on the web interface and if Citrix is the only terminal service, it is not necessary for the user to log on to the thin client again. If the **Automatic thin client login** option is enabled, the login to LightDM occurs automatically.

10.2.1.2. Installation without the UMC wizard

Feedback

This section provides a brief description of the setting up Citrix Receiver for complex scenarios in which the UCC setup wizard should not be used. For general information on Citrix and UCC, please see Section 10.2.1.1

The Citrix Receiver for 32 bit systems must be downloaded as a DEB file from http://www.citrix.de/downloads/citrix-receiver/linux/receiver-for-linux-132.html.

The `ucc-image-add-citrix-receiver` tool can be used to install the Citrix Receiver in a UCC thin client image. The parameter `-i` specifies the UCC image and `-d` the DEB file with the Citrix Receiver. The ***univention-ucc-session-xenapp*** meta package is installed automatically.

If the EULA is to be confirmed automatically, the Univention Configuration Registry variable `citrix/acceptеula` must be set to `true` by means of a policy. The web interface for the Citrix login must be configured via the `citrix/webinterface` variable.

To configure a login-less access to the web interface the Univention Configuration Registry variable `lightdm/autologin/session` must be set to `XenApp` and the Univention Configuration Registry variable `lightdm/autologin` to `yes`.

10.2.1.3. Advanced configuration

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.

In the default setting, the Citrix Receiver accesses the thin client's sound card(s) via the ALSA interface. For special cases - e.g., systems with multiple sound cards - the Univention Configuration Registry variable `citrix/pulseaudio` can be set to `true`. The result of this is that the PulseAudio sound daemon is started in the XenApp session script (this e.g. ensures the assignment of a primary sound card).

Citrix Receiver can be configured via the `wfclient.ini` file on the UCC thin client. To disable the default settings, the UCR variable `ucc/xenapp/wfclientdefaults` has to be set to `false`. To set additional options in the ini file, a UCR variable in the form `ucc/xenapp/wfclient/identifier=value` has to be set. The value will then be written to the `wfclient.ini` file.

The package ***univention-ucc-firefox-config*** is installed on UCC thin clients by default. To set defaults for Firefox, a UCR variable in the form `ucc/firefox/defaults/identifier=value` can be set. The value will then be written to the file `/usr/lib/firefox/defaults/pref/ucc-prefs.js`

The Citrix session supports USB redirection (if configured on the server). Special rules to enable/disable USB redirection for devices can be configured with the UCR variable `ucc/xenapp/ctxusb/rules` on the UCC thin client.

For customization purposes the XenApp session script supports hooks. These hooks are basically bash scripts which have to be placed in the correct hook directory. The session script executes these hooks via `run-parts` at different stages of the script. The following hook directories are supported:

- /usr/share/univention-ucc-session-xenapp/hooks/top.d - start of the session script
- /usr/share/univention-ucc-session-xenapp/hooks/pre-firefox.d - before starting firefox
- /usr/share/univention-ucc-session-xenapp/hooks/post-firefox.d - after firefox finished
- /usr/share/univention-ucc-session-xenapp/hooks/bottom.d - end of the session script

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

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 6.2) is available under Drive Z: in the Citrix session.

10.2.3. Accelerating the playback of Flash videos

Feedback

The Citrix Receiver 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 (the package is called ***adobe-flashplugin***).

To suppress the pop-up question to optimize flash playback, a UCR policy should e.g. set `ucc/xenapp/wf-client/flashsetting` to `HDXFlashUseFlashRemoting=Always`.

In the default setting the Flash version on the client and the Flash version on the Citrix server need to be identical. Releases of Adobe Flash later than 11.2 are no longer available for Linux. The version check can be disabled on the Citrix server. For this a registry key needs to be added on the Citrix server in the location **HKEY_LOCAL_MACHINE -> Software -> Wow6432Node -> Citrix -> HdxMediaStreamForFlash -> Server -> PseudoServer**. The new key must be created as a `dword`, named *FlashPlayerVersionComparisonMask* and set to `0`.

To verify the local Flash playback, you can play a Flash video on the Citrix server and query the process list on the UCC client using `ps aux`. If the Flash redirection is working correctly, you should see a process named `FlashContainer.bin`.

10.2.4. Windows Media HDX playback

Feedback

To enable Citrix Windows Media HDX playback on the client the following packages are installed on the UCC client by default: ***gstreamer0.10-plugins-ugly***, ***gstreamer0.10-plugins-good***, ***gstreamer0.10-plugins-bad***, ***gstreamer0.10-alsa***, ***gstreamer0.10-fluendo-mp3***, ***gstreamer0.10-ffmpeg*** and ***gstreamer0.10-x***.

10.2.5. XenApp client printers

Feedback

XenApp Printing allows to map local printers to the Citrix session. This requires a local printer queue on the UCC client. By installing the package ***univention-ucc-usb-raw-printer*** a raw printer queue is created for every USB printer connected to the client.

XenApp Printing also allows to map remote printers to the Citrix session. By the installation of the package ***univention-ucc-printerconfig*** the UCC client can be configured as print client (cups). The print server can be configured with the Univention Configuration Registry variable `ucc/cups/server`. All the remote printers, known to the UCC client, are automatically mapped to the XenApp session (if printer redirection is configured onthe XenApp server).

10.2.6. Possible graphical glitches with Citrix Receiver

Feedback

Some thin-clients show graphical glitches when using Citrix terminal services. In this case a Citrix policy to enable legacy graphics mode has to be configured. More information about the different graphic modes can be found at http://blogs.citrix.com/2014/10/22/whats-new-with-hdx-display-in-xendesktop-xenapp-7-x/.

Chapter 11. List of tested thin client hardware

The list of supported thin client hardware can be downloaded from http://download.univention.de/doc/Hardware_compatibility_list.pdf.

Bibliography

[ucs-manual] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-4.0.html.

[ucs-manual-multiedit] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-4.0.html#central%3Auser-interface%3Aedit.

[ucs-manual-cron] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-4.0.html#computers%3AExecuting_recurring_actions_with_Cron.

[ucs-manual-nagios] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-4.0.html#nagios::general.

[ucs-manual-pxeboot] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-4.0.html#ip-config:Configuration_of_boot_server_PXE_settings.

[ubuntu-repositories] Ubuntu Community Wiki. 2014. *Repositories Ubuntu*. https://help.ubuntu.com/community/Repositories/Ubuntu.