UDC Deployment Appliance

IGEL Universal Desktop Converter Deployment Appliance for virtual environments.

- UDC Deployment Appliance Manual (see page 3)

UDC Deployment Appliance Manual

Overview

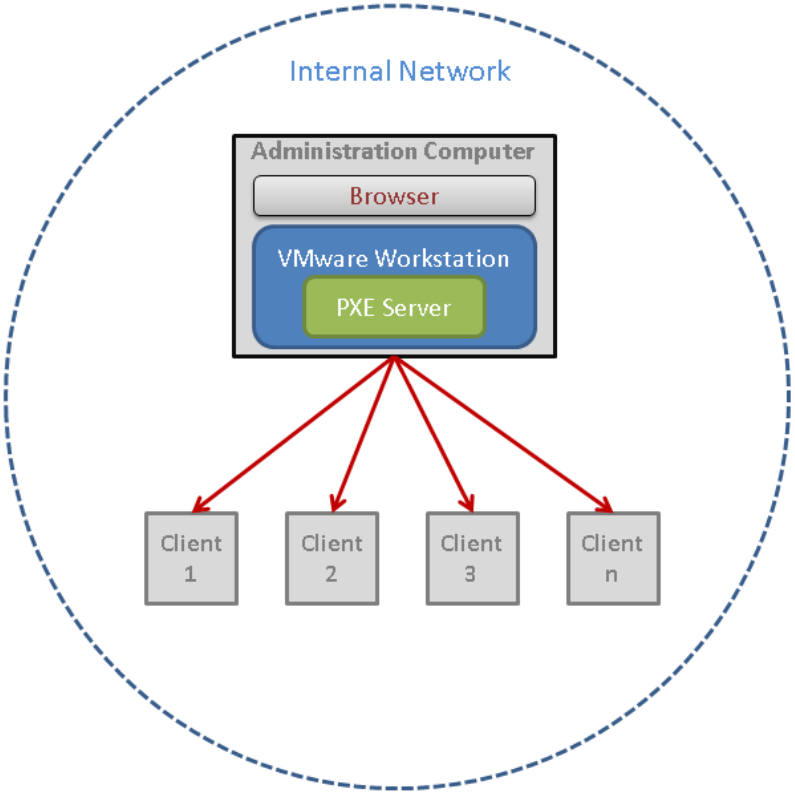
The IGEL UDC Deployment Appliance enables you to migrate your existing PCs or thin client hardware to fully manageable IGEL OS thin clients. The Deployment Appliance is implemented as a virtual machine which runs in a hypervisor, i.e. VMware Workstation, VMware Player, or Oracle VirtualBox.

The deployment procedure is as follows:

The Deployment Appliance is installed and placed in a separate network. All devices that are to be converted are also placed into this network, and network booting is enabled on this devices. When a device boots, the PXE server at the heart of the Deployment Appliance rolls out the UDC2 or UDC3 firmware file to it. Once a device is converted, the Deployment Appliance adds its MAC address to a filter so that the deployment process does not start again in the case of a reboot.

In addition to that, you can add devices to the MAC address filter manually to prevent them from being converted. This is possible with IGEL UDC Deployment Appliance version 4.1 or higher.

The following figure shows an example setup with the Deployment Appliance running in a VMware Workstation:



System Requirements

Ensure that the administration computer meets the following requirements:

- 2 GB RAM
- 30 GB disk storage
- 64-bit compatible

Hypervisor Version

Install one of the following hypervisors in a version that supports OVA files:

- VMware Workstation
  or
- VMware Player
  or
- Oracle VirtualBox

Web Browser

A web browser is needed to download the firmware from the IGEL download site and upload it to the Deployment Appliance.

Deployment Steps

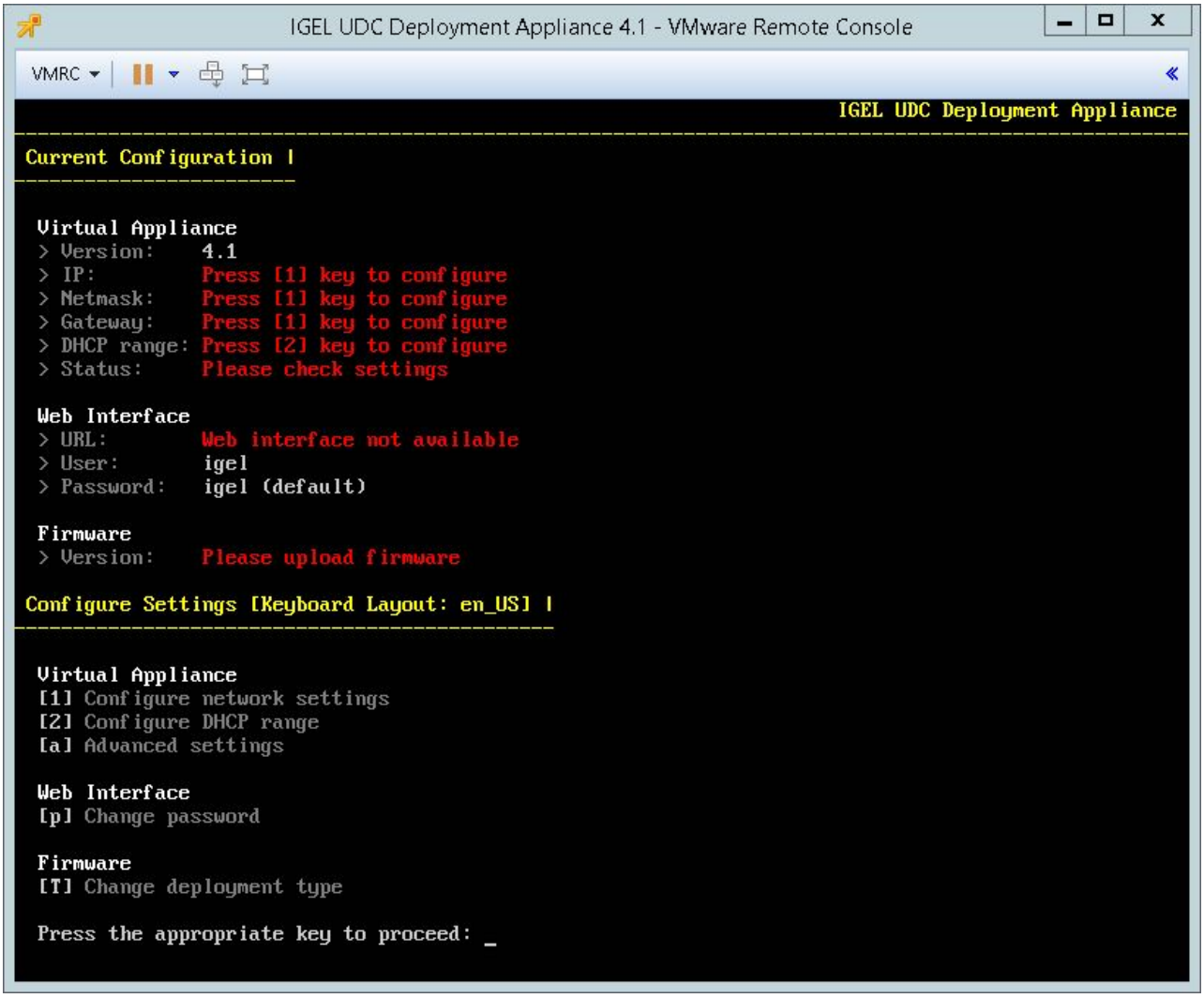
Importing the OVA File

> In the following step-by-step procedure, VMware Workstation is used. For VMware Player or Oracle VirtualBox, please refer to the appropriate documentation.

1. Open the browser on the administration computer and download the `ova` file from the IGEL download server (`http://myigel.biz` > `IGEL_UDC_DEPLOYMENT_APPLIANCE`).
2. Import the `ova` file into VMware Workstation.
3. Click **File > Import OVF Template** in VMware Workstation to start importing a virtual machine.
4. Follow the **Connection Wizard** through the import process.
5. Choose `Virtual Appliance` as **source type**.
6. Choose `(ova) location` as **source file**.
7. Choose `Other Virtual Machine` as **Destination Type**.
8. Enter the **Name** and **Location** for the virtual machine.
9. Choose `Import and Convert` as **Import Option**.
10. Choose `Bridged` as **VMNetwork Configuration**.
11. Start the import process.

Configuring the Deployment Appliance

▶ Start the Deployment Appliance.
The main menu opens.



▶ To configure the Deployment Appliance, use the following keys:

Key	Action
[1]	Configure the network settings
[2]	Configure the DHCP range settings

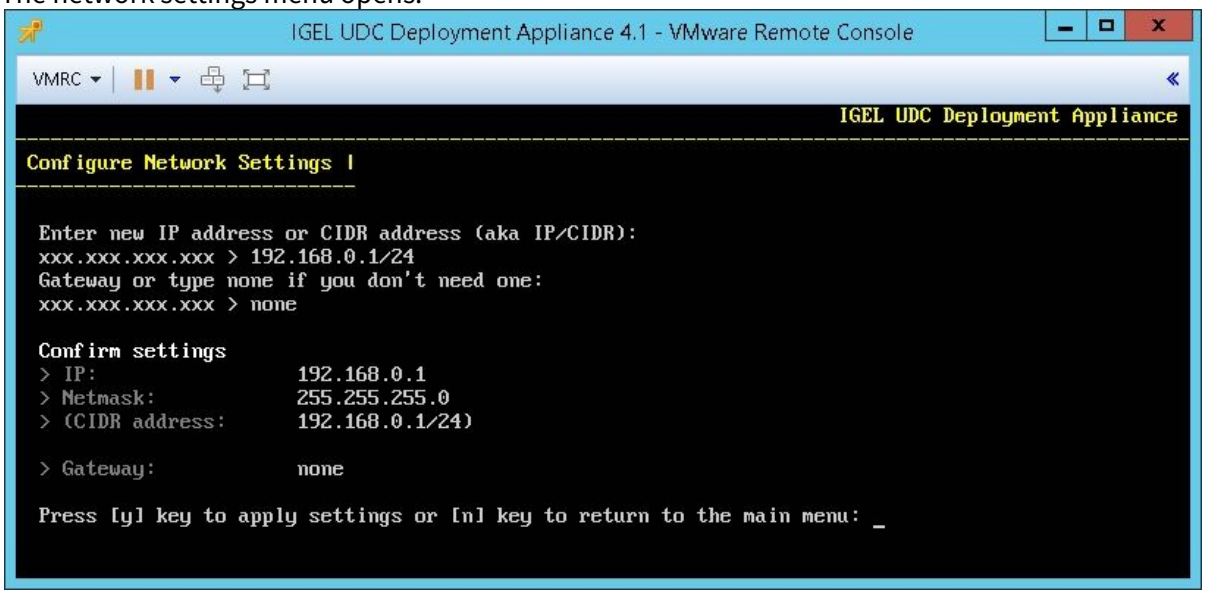
[A]	Configure advanced settings
[P]	Change the web interface password
[Shift + T]	Change the deployment type

_____

- Configuring the Network Settings (see page 8)
- Configuring the DHCP Range (see page 9)
- Using Your Own DHCP Server (see page 10)
- Configuring Advanced Settings (see page 11)
- Changing the Password (see page 22)

Configuring the Network Settings

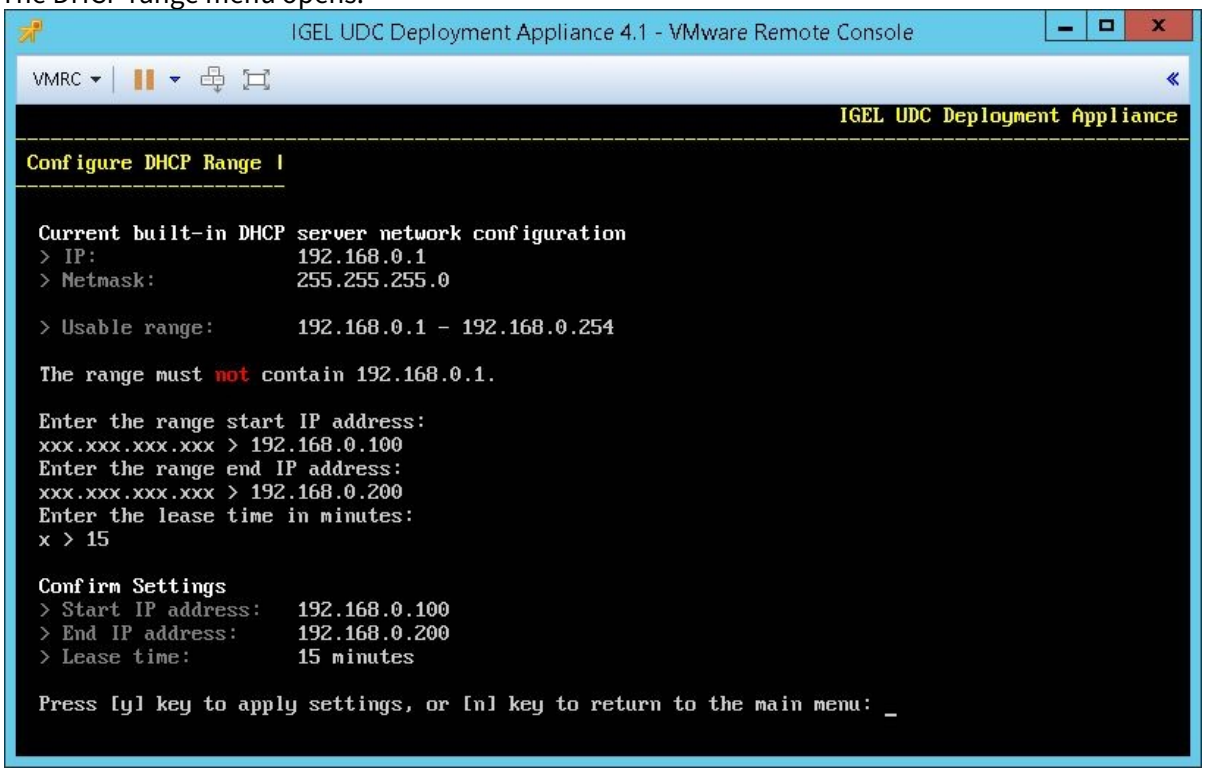
1. In the main menu, press [1] to configure the network settings.
   The network settings menu opens.



2. Enter the following parameters:
   - **IP address or CIDR address**: The IGEL Deployment Appliance will use this address for firmware delivery. Also, the web interface can be reached via this IP address.
   - **Netmask**: Netmask for the IGEL Deployment Appliance.
   - **Gateway**: Default gateway for the IGEL Deployment Appliance.
3. Press [Y] to confirm the settings.

Configuring the DHCP Range

1. In the main menu, press [2] to configure the DHCP range for the built-in DHCP server.
   The DHCP range menu opens.



2. Enter the following parameters:
   - **Start IP address**: Lowest IP address of the DHCP range.
   - **End IP address**: Highest IP address of the DHCP range.
   - **Lease time**: Timespan during which an IP address is reserved for a device.
3. Press [Y] to confirm the settings.
   The DHCP server will restart and assign IP addresses to all devices in the network.

> ⓘ It is possible to exclude a device from being configured by the built-in DHCP server. For further information, see Adding a MAC Address to the Filter (see page 20).

> ⓘ It is possible to use your own DHCP server instead of the built-in DHCP server of the Deployment Appliance, see Using Your Own DHCP Server (see page 10).

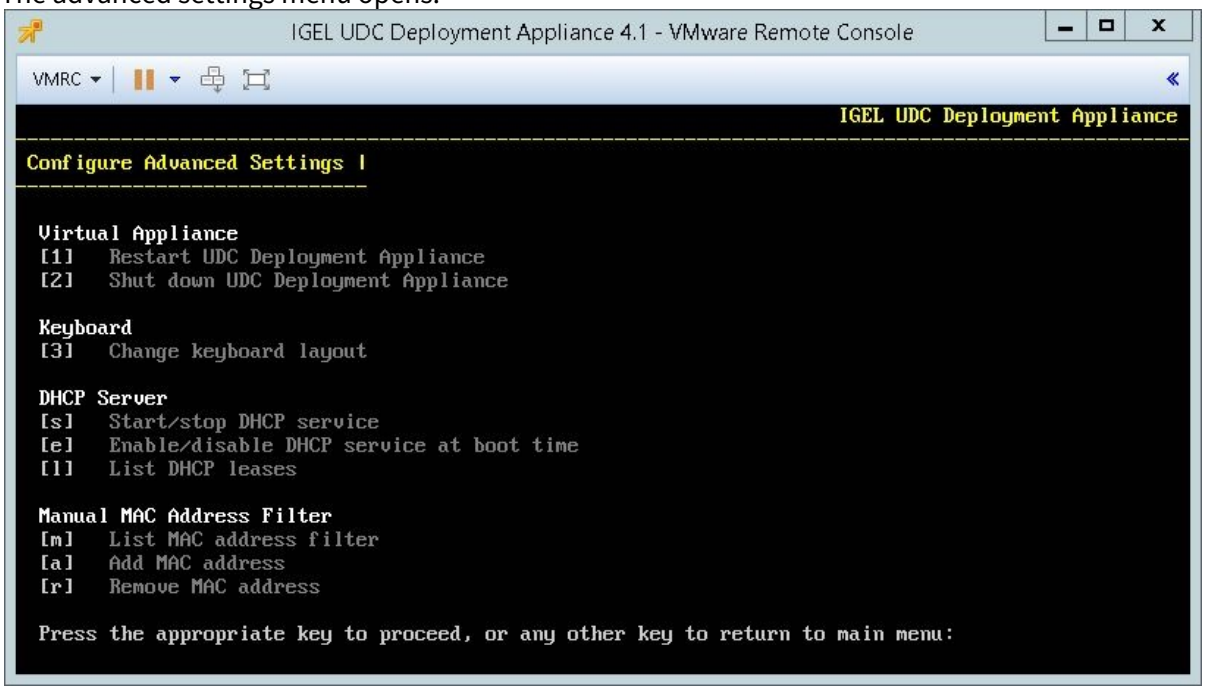
Using Your Own DHCP Server

When you use your own DHCP server instead of the built-in DHCP server, the MAC address filter will not be effective. The MAC address filter is required if some devices in the network are not to be converted.

1. Ensure that the DHCP server built into the Deployment Appliance is stopped or disabled; see Starting/Stopping the DHCP Service (see page 16) or Enabling/Disabling the DHCP Service (see page 17).
2. Connect to your DHCP server.
3. Create a **DHCP option 67**.
4. Enter `pxelinux.0` as the boot file name.
5. Create a **DHCP option 66**.
6. Enter the IP of the Deployment Appliance (in our example: `192.168.0.10`).

Configuring Advanced Settings

1. In the main menu, press [A] to open the advanced settings menu.
   The advanced settings menu opens.



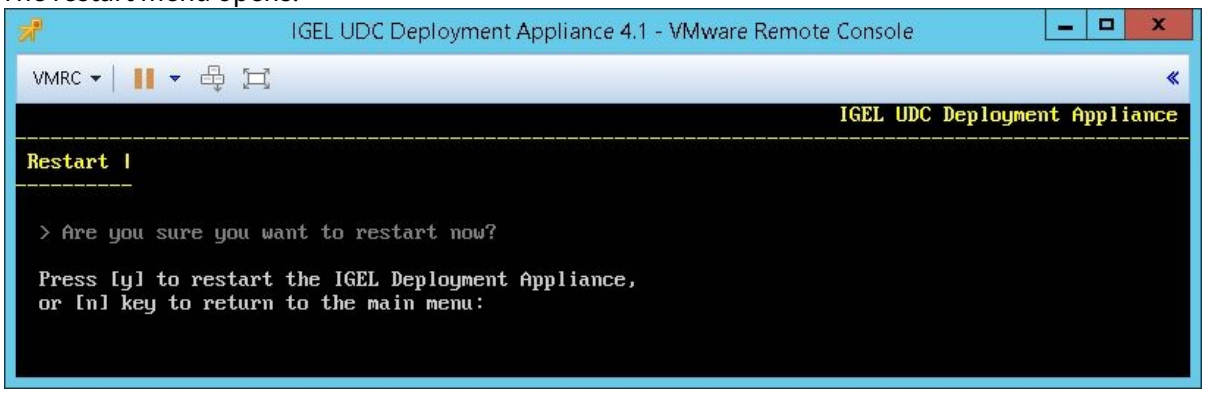
2. To change settings or start/stop services, use the following keys:

Key	Action
[1]	Restart the Deployment Appliance; see Restarting the Deployment Appliance (see page 13).
[2]	Shut down the Deployment Appliance; see Shutting Down the Deployment Appliance (see page 14).
[3]	Change the keyboard layout; see Changing the Keyboard Layout (see page 15).
[S]	Start or stop the DHCP service; see Starting/Stopping the DHCP Service (see page 16).
[E]	Enable or disable the DHCP service at boot time; see Enabling/Disabling the DHCP Service (see page 17).
[L]	List the current DHCP leases; see Listing the DHCP Leases (see page 18).
[M]	List the MAC addresses that are to be filtered out by the MAC address filter; see Listing the MAC Address Filter (see page 19).
[A]	Add MAC address to the MAC address filter; see Adding a MAC Address to the Filter (see page 20).

[R]	Remove MAC address from the MAC address filter; see Removing a MAC Address from the Filter (see page 21).

Restarting the Deployment Appliance

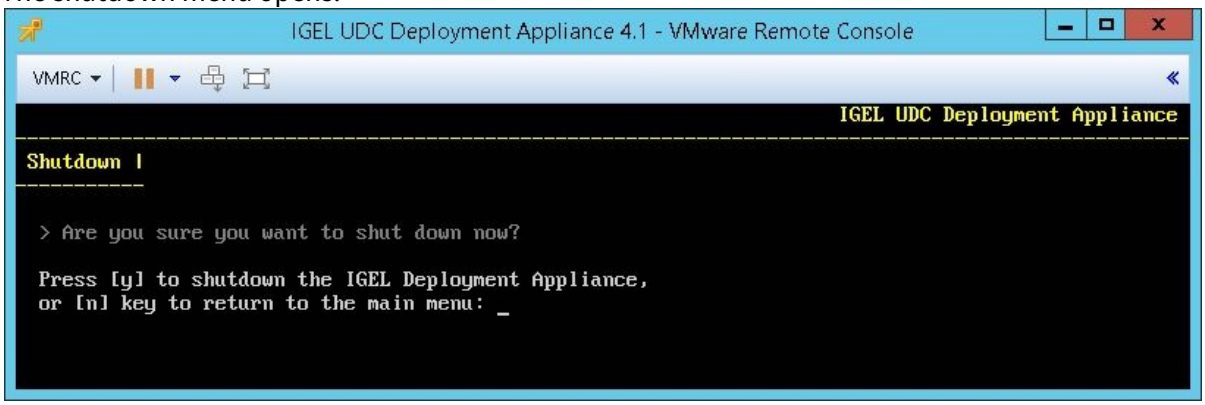
1. In the advanced settings menu, press [1] to open the restart menu.
   The restart menu opens.



2. Press [Y].
   The virtual machine containing the Deployment Appliance is restarted.

Shutting Down the Deployment Appliance

1. In the advanced settings menu, press [2] to open the shutdown menu.
   The shutdown menu opens.



2. Press [Y].
   The virtual machine containing the Deployment Appliance is shut down.

Changing the Keyboard Layout

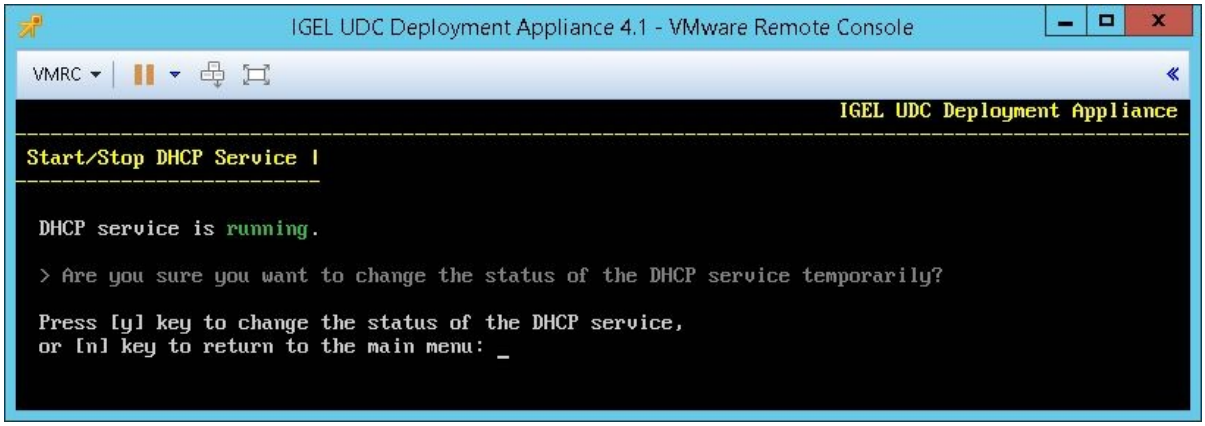
1. In the advanced settings menu, press [3] to open the keyboard layout menu.
   The keyboard layout menu opens.

2. Press the appropriate key to choose a system locale:
   - [1]: `en_US.UTF-8` (US English; default)
   - [2]: `en_GB.UTF-8` [ ](GB English)
   - [3]: `de_DE.UTF-8` (German)
   - [4]: `fr_FR.UTF-8` (French)

   The keyboard layout is changed, together with the system locale.

Starting/Stopping the DHCP Service

1. In the advanced settings menu, press [S] to open the DHCP start/stop menu.
   The current status of the DHCP service is shown in the menu.

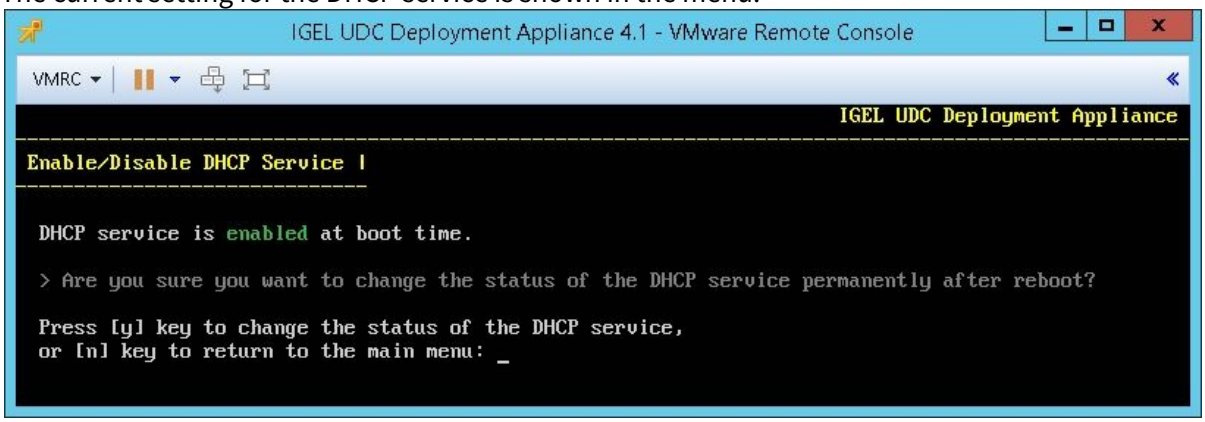


2. Press [Y] to start or stop the DHCP service of the Deployment Appliance.
   If the DHCP service has been running before, it will stop now.
   If the DHCP service has not been running before, it will start now.

Enabling/Disabling the DHCP Service

Disabling the DHCP service of the Deployment Service makes sense if you prefer using you own DHCP server; see Using Your Own DHCP Server (see page 10).

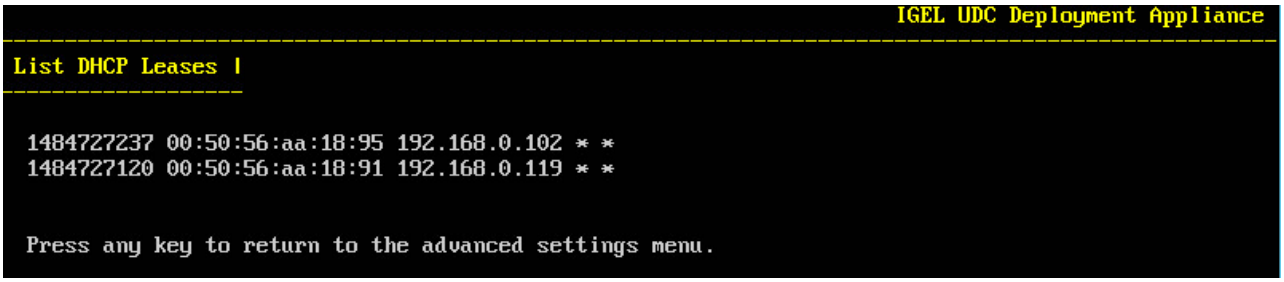
1. In the advanced settings menu, press [E] to open the DHCP enable/disable menu.
   The current setting for the DHCP service is shown in the menu.



2. Press [Y] to enable or disable the DHCP server of the Deployment Appliance.
   If the DHCP has been enabled before, it will be disabled after the next reboot.
   If the DHCP has been disabled before, it will be enabled after the next reboot.

Listing the DHCP Leases

▶ In the advanced settings menu, press [L] to open the DHCP leases menu.
The current DHCP leases are shown in a table.



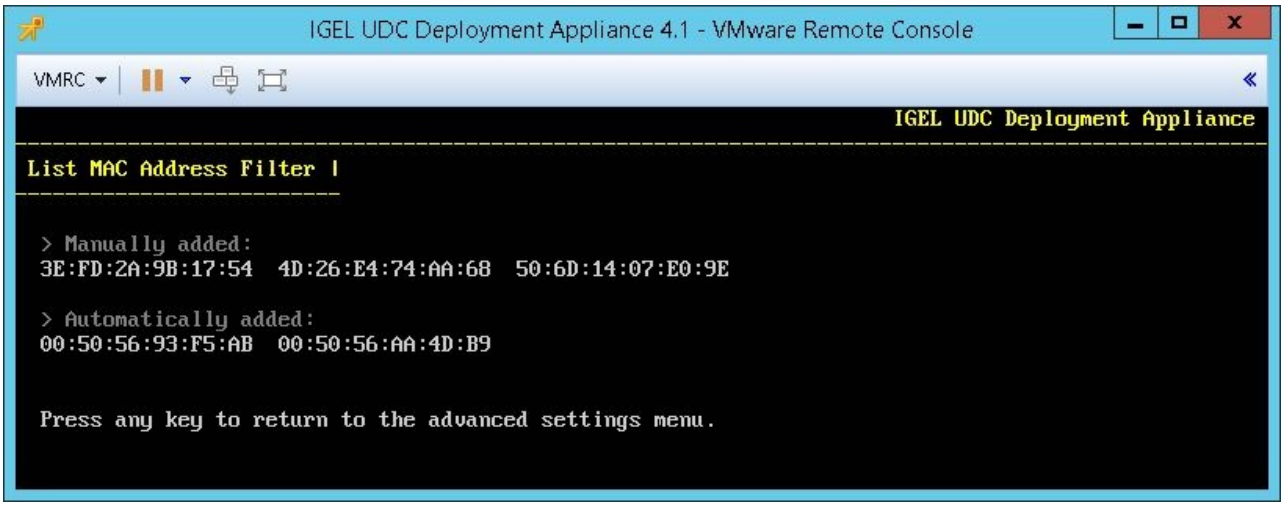
Example:

Point in time when the lease ends (epoch time)	MAC address of the device	IP address assigned to the device	Computer name (if known)	Client ID (if known)
`1484727237`	00:50:56:aa:18:95	192.168.0.102	`device1`	`igel1`

Listing the MAC Address Filter

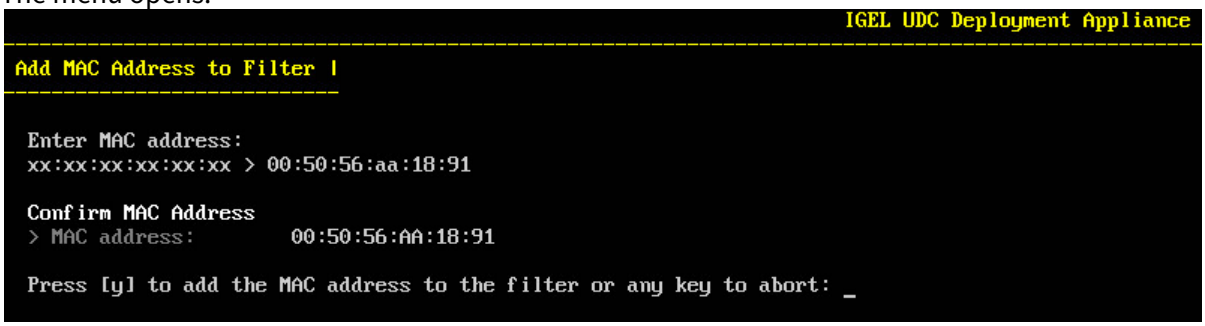
▶ In the advanced settings menu, press [M] to open the MAC address filter list.

The address filter list shows the MAC addresses of those devices which will not receive an IP address from the DHCP service, and will not be converted with the UDC3/UDC2 firmware.



Adding a MAC Address to the Filter

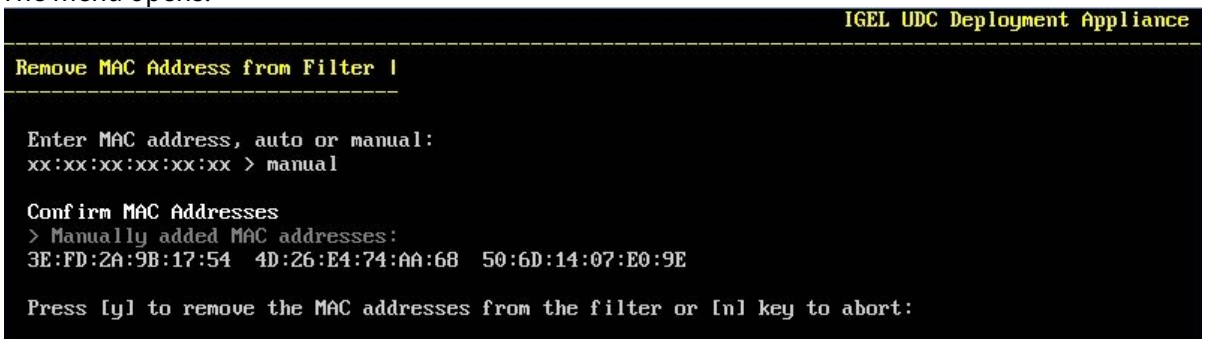
1. In the advanced settings menu, press [A] to open the menu for adding a MAC address to be filtered out.
   The menu opens.



2. Enter the MAC address of the device you want to exclude from UDC deployment.
3. Press [Y] to confirm.
   The device will not receive an IP address from the DHCP service, and will not be converted with the UDC3/UDC2 firmware.

Removing a MAC Address from the Filter

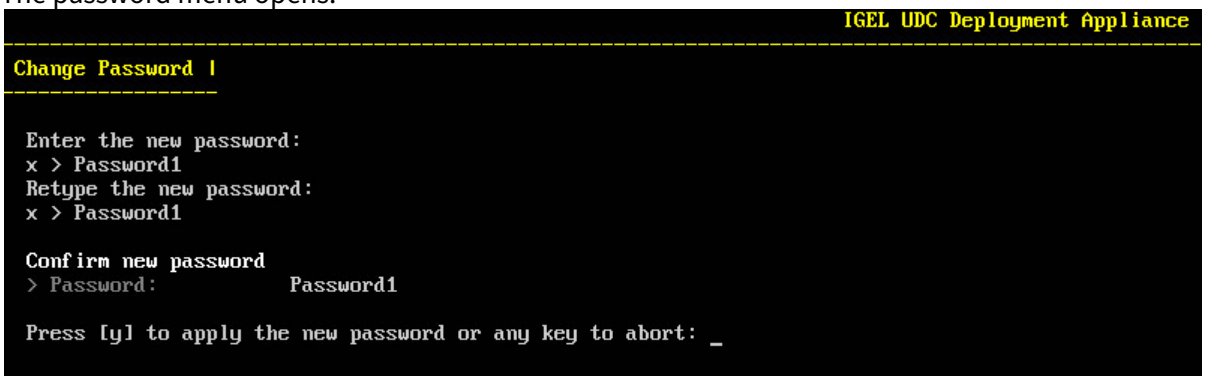
1. In the advanced settings menu, press [A] to open the menu for removing a MAC address from the filter.
   The menu opens.



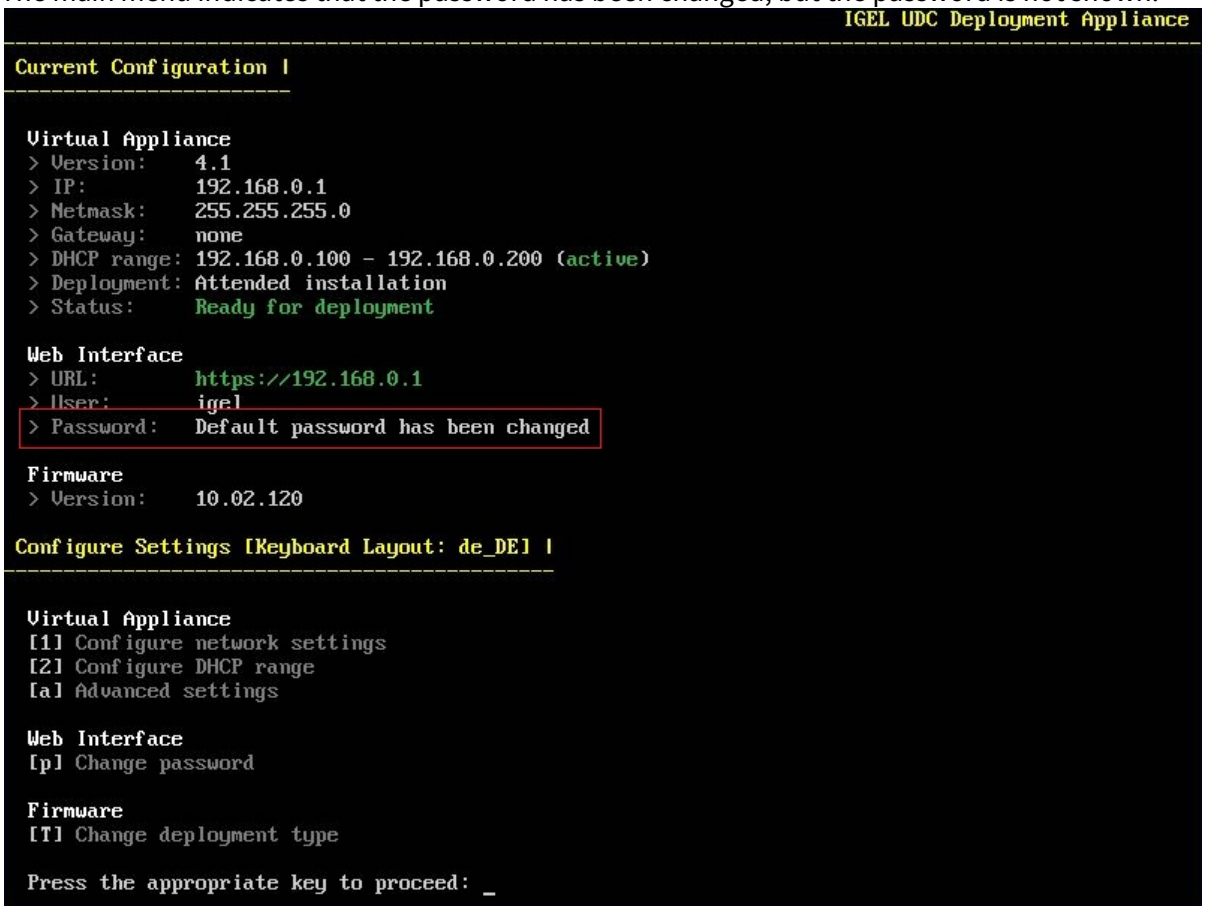
2. Enter **auto**, **manual** or the **MAC address** of the device you want to remove from the filter.
   All members of the selected group or the MAC address will be deleted from the MAC address filter.
3. Press [Y] to confirm.
   The device will receive an IP address from the DHCP service, and can be converted with the UDC3/ UDC2 firmware.

Changing the Password

1. In the main menu, press [P] to change the password for the web interface.
   The password menu opens.



2. Enter the new password.
3. Press [Y] to confirm the new password.
   The main menu indicates that the password has been changed, but the password is not shown.



Getting the Firmware Files

The UDC firmware is provided by https://www.igel.com. The download path depends on the exact version to be used.

- To download the firmware for UDC3, go to https://www.igel.com/software-downloads/software-downloads-former-universal-desktop-and-legacy-versions/ **> OS 10 & V5 > Universal Desktop Converter 3 (OS 10) (STICK).**
- To download the firmware for UDC2, go to https://www.igel.com/software-downloads/software-downloads-former-universal-desktop-and-legacy-versions/ **> OS 10 & V5 > Universal Desktop Converter 2 (V5) (STICK).**

Uploading the Firmware to the PXE Server

1. Open the web interface in a web browser. The URL is `https://`. For defining the IP address, see Configuring the Network Settings (see page 8).

   > If the browser presents a certificate warning, you can ignore it. The CA (certificate authority) is unknown to the administration computer because the certificate is self-signed.

2. Enter the password for the web interface. The default password is `igel`; it should be changed as soon as possible.
   The web interface opens.
3. Click the button next to **Select firmware** and select the appropriate file (`UDC2Stick_[version].zip` and iso files) on the administration computer.

   > For UDC3, the firmware name is `UD2Stick_10[minor version].zip` (IGEL OS 10.02.100 or older) or `UDC3_10[minor version].zip` (IGEL OS 10.02.120 or newer).

4. Click **Upload**.
   The upload process starts.

When the upload is finished, the Deployment Appliance starts to prepare the firmware.

When the preparation is finished, the **System Information** is updated as followed:

The Deployment Appliance is ready for firmware deployment.

▶ Continue with choosing the appropriate deployment type, see Choosing the Deployment Type (see page 28).

UDC3_10[MINOR_VERSION].zip.

Choosing the Deployment Type

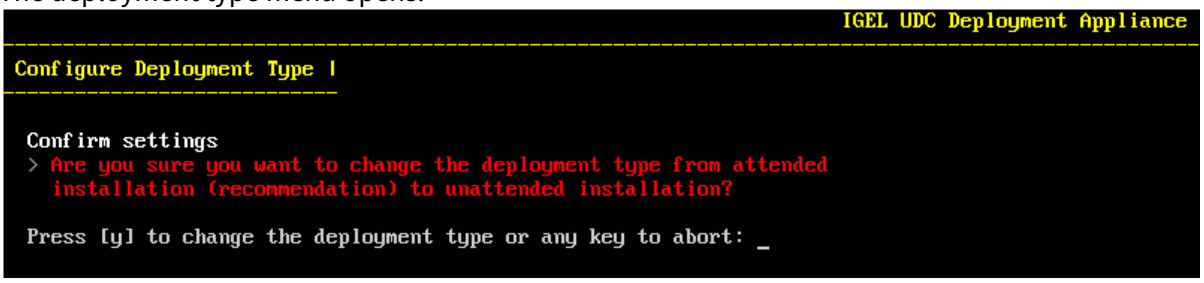
Before you reboot each device, you can choose whether the conversion should be started manually or automatically:

> Make sure that your network only contains devices which are to be converted by UDC3 or UDC2, and which have no valuable data. All data on the local storage will be lost!

- Attended installation (default): The device presents a dialog. When the dialog is confirmed, the UDC3 or UDC2 firmware is installed on the device.
- Unattended installation: The device presents a dialog with a timeout. When the dialog is confirmed or the timeout is reached, the firmware is written to the device.

To change the deployment type:

1. In the main menu, press [Shift] + [T].
   The deployment type menu opens.



2. Press [Y] to confirm the settings.
   If the installation type has been attended installation before, it will be changed to unattended installation.
   If the installation type has been unattended installation before, it will be changed to attended installation.

Installing the UDC

A mechanism ensures that the UDC firmware is deployed only once to each client. After successful installation the target device sends back to the appliance that the OS is installed. The appliance inserts the MAC address of the client into the MAC address filter (see page 19), which can be found under automatically added (see page 19). Afterwards the client does not become a DHCP address from the build-in DHCP server. The client boots into the rolled out firmware regularly without network. You can then remove (see page 21) it yourself from the MAC address filter. The appliance would deploy the firmware again to this device after a reboot.

1. Ensure that the BIOS of your target devices is set to network installation. Other system requirements are listed in the official data sheets for UDC3 or UDC2 at http://www.igel.com.
2. Boot the target devices with the IGEL UDC3 / IGEL UDC2 image.
   If you have chosen attended deployment, the firmware will be installed when the dialog on the devices is confirmed.
   If you have chosen unattended deployment, the firmware will be installed after a 10-second timeout.

For security reasons, the UDC3/UDC2 is not installed alongside the target system's legacy operating system, nor can it be installed in a dual-boot configuration. Nevertheless, in situations where it is absolutely necessary to preserve the target system's operating system, it is possible to install the UDC3/UDC2 onto a live bootable USB memory stick.

In the next step, you need to import licenses; see Licensing the UDC (see page 30).

Licensing the UDC

Licenses can be imported

- during installation of the UDC2 manually (UDC2 only) or
- through the **License Management** features of the *IGEL Universal Management Suite*.

The UDC3/UDC2 license is not transferrable between PCs. However, IGEL recognizes when computer equipment does fail, and therefore offers a license replacement program. Within one year of purchase, IGEL will provide a replacement license when an end-user organization reports the MAC addresses of both the failed device and its replacement.