OpenXT™ Engine Administrator Guide High-assurance
isolation & security for virtual environments

Table of Contents

Chapter 1. Overview and System Setup

OpenXT provides a local virtualized desktop with enhanced isolation of mutually distrusting virtual machines (VMs). OpenXT supports the customization of isolation policies for a variety of enterprise mobile and desktop use cases. Some OpenXT features:

- Service VM architecture for extensibility and secure isolation of critical services

- Rich APIs for partner extensibility

- Secure Measured Launch using Intel Trusted Execution Technology (TXT)

- Multiple GPU and seamless mouse support, allowing you to run multiple 3D Graphics Support VMs on separate monitors

- Read-only control domain

- Encrypted VM disks.

- SELinux and XSM (Xen Security Modules) policy enforcement

- Network Driver Virtual Machine (NDVM) that provides an isolated networking service for VMs

- VM disk persistence for returning a VM to its original state on each reboot

Centrally mange your OpenXT devices and VMs using OpenXT Synchronizer. See *OpenXT™ Synchronizer Administrator Guide* for more information about OpenXT Synchronizer.

1.1. Hardware Compatibility

OpenXT supports the following systems and devices. Newly-supported devices in this release are listed in bold text:

1.1.1. Laptop Systems

- HP EliteBook 8460p

- HP EliteBook 8440p

- HP EliteBook 2560p

- HP EliteBook 2760p

- **HP EliteBook 2170p**

- **HP EliteBook 2570p**

- **HP EliteBook 8470p**

- **HP EliteBook 8570p**

- **HP EliteBook 9470m**

- Dell Latitude E6420

> **Note**
>
> BIOS A13 on the E6420 is not compatible with Intel TXT and the Measured Launch feature of OpenXT

- Dell Latitude E6410

- Dell Latitude E6220

> **Note**
>
> BIOS A08 on the E6220 is not compatible with Intel TXT and the Measured Launch feature of OpenXT

- **Dell Latitude E6230**[*]

- **Dell Latitude E6330**[*]

- **Dell Latitude E6430**[*]

- **Dell Latitude E6430S**[*]

- **Dell Latitude E6530**[*]

- **Lenovo X230**

- **Lenovo T430**

- **Lenovo T430S**

- **Lenovo T520**

- **Lenovo T530**

- **Lenovo ThinkPad X1 Carbon**

1.1.2. Desktop Systems

- HP 8100 mini-tower

- HP 8200 mini-tower

- **HP Z220**

- **HP 8300 mini-tower**

- **HP 8300**

- Dell 980 mini-tower

- Dell 980 small form factor (SFF)

- Dell 990 mini-tower

- Dell 990 small form factor (SFF)

- **Dell 9010**[*]

---

[*]Warning: Current BIOS versions of Dell systems with 3rd-generation i5 and i7 CPUs (Ivy Bridge) have bugs related to Measured Launch. If you are using one of these systems, you will be warned when setting up Measured Launch. On a system with these problems, the measurement stored by the BIOS in PCR[1] must be excluded from the PCR values used to seal the OpenXT Engine config partition. For a description of PCR[1] and the contents measured within see the OpenXT Architecture Guide. When Dell issues a new BIOS with this issue resolved, the value of PCR[1] can be added back to the measurement list by an administrator using the Procedure: "To restore PCR[1] to the list of PCRs to which the Engine config partition is sealed".

- **Dell 9010 (SFF)**[*]

- **Lenovo M92P (SFF)**

- **Lenovo M92P (Tiny)**

- **Lenovo M91P (SFF)**

SFF systems currently do not support GPU add-on devices.

1.1.3. Discrete Graphics Processors

- ATI Radeon HD 4550 PCI Express

- ATI Radeon HD 5450 PCI Express

- ATI Radeon HD 5500 PCI Express

- ATI Radeon HD 6570 PCI Express

- NVIDIA Quadro 2000

> **Note**
>
> The combination of an HP 8200 using an ATI Radeon HD 6570 is not supported.

1.1.4. Network Interfaces

- PCI Express Network Interface Card (NIC), e.g. Broadcom NetExtreme II 5722

1.1.5. Intel TXT and Intel AMT

For OpenXT use cases which require Intel Trusted Execution Technology (TXT), but not Intel Active Management

Technology (AMT), the following options are available from system manufacturers and are supported by OpenXT:

1. Contact your system manufacturer to purchase a non-vPro SKU variant of a supported desktop and an Intel CPU that supports TXT and VT-d.

2. Purchase and install a third-party PCI Express network interface card in a supported desktop. Use the System BIOS to disable the onboard, integrated Intel NIC. AMT must remain enabled in the system BIOS.

1.2. Device Preparation before OpenXT Installation

Before Installing OpenXT on All Devices:

1. Install the most recent BIOS version available from the system manufacturer. In some cases the most recent BIOS may be incompatible with OpenXT.

2. Enable the following Intel vPro features in the system BIOS:

    a. VT-x

    b. VT-d

    c. TPM

    d. TXT

Before Installing OpenXT on a Dell or HP Desktop With an Nvidia or ATI Video Card:

1. Install the video card in PCI Express slot 4.

2. In the BIOS video configuration menu:

    a. Enable the Intel integrated video adapter.

    b. Specify Intel as the primary video adapter.

Before Installing OpenXT on a Dell 980:

• Disable unused devices in the BIOS to reduce interrupt conflicts:

    a. Set **System Configuration > Serial Port #2** to **Disabled**.

    b. Set **System Configuration > Parallel** to **Disabled**.

    c. Set **Drives > SATA-2** to **Disabled**.

    d. Set **Drives > SATA-3** to **Disabled**.

    e. Set **Drives > External SATA** to **Disabled**.

    f. Set **Miscellaneous Devices > WiFI NIC Slot** to **Disabled**.

    g. Set **Miscellaneous Devices > Optiplex ON Reader** to **Disabled**.

1.3. Setup Instructions

After you have updated and configured your BIOS, use the following procedure to prepare your OpenXT device:

1. Install OpenXT on the target device using the installation media.

2. Create a VM. See Section 2.3: "Creating VMs on OpenXT " for more information.

3. Install an operating system on the VM. See the Procedure: "To Install an Operating System onto a VM" for more information.

4. Install the OpenXT Tools on the VM. See Section 2.3.3: "Installing the OpenXT Tools" for more information.

5. Install any other VMs in the same manner.

6. Perform any optional VM and platform configuration required. See Chapter 3: "*VM Configuration and Lockdown Policy*" and Chapter 4: "*Platform Configuration*" for more information.

1.3.1. Installation Media

You can install OpenXT from optical media or a USB storage device.

To use optical media, burn an image of the ISO file to a blank CD or DVD. From Windows 7 you can right-click on the ISO file and select **Burn Disk Image** and follow the prompts. From a Linux system there are similar methods from the graphical interface, or you can use the **dd** command. See the documentationof your Linux distribution for more information.

To use a USB storage device, you need to make the device bootable as well as image the ISO file.

From a Windows system, you can use the utility *UNetbootin*.

To create a bootable ISO image on a USB storage device on Windows:

Download and install UNetbootin.

If you retrieve the UNetbootin distribution from another location, ensure that it is at least version 549 or newer.

1. Insert your USB storage device in a USB port.

2. Launch UNetbootin and select **DiskImage**.

3. Click on the browse button the right of the **ISO** field and browse to the location of the ISO.

4. With **Type** set to *USB Drive*, use the drop-down menu to select the drive letter of your USB storage device.

5. Click **OK**. You will see a progress bar as the USB device is prepared and the ISO is imaged.

6. Once the process is complete, click **Exit**.

From a Linux system, there are similar methods from the graphical interface, or you can use the **cat** from a command line shell. With the USB storage device in place, enter:

```
cat installer.iso > /dev/sd<x>
```

where *x* is the correct drive ID for your USB storage device.

Warning

Be sure to triple-check the target for the **cat**, to avoid erasing another drive, potentially the one with your Linux OS on it!

1.3.2. Installing or Upgrading

Important

Before upgrading OpenXT, ensure that all VMs on the OpenXT device are shut down.

OpenXT offers two installation modes: quick installation or advanced installation. Use the arrow keys and the **Enter** key to navigate through the installation wizard. Press **Esc** to go back a step.

Note

The display might switch off during the late stages of installation. This is no cause for concern. Simply press any key on the keyboard to wake the display up.

To Perform a Quick Install or Upgrade:

Quick install does not include the option to enable ssh access to the control domain nor to enable Measured Launch. If you choose **Quick install** and later decide to enable ssh access, you can do so by opening a command-line terminal from the OpenXT control domain and entering the command **xec set enable-ssh true**. See Section 1.4.2: "Enabling Measured Launch for the Control Domain After Installation" for further details about enabling Measured Launch on a running installation.

1. Boot from the OpenXT installation media or network in the case of a PXE boot setup.

2. Choose **Quick install**.

3. Choose **OK** and review the software license.

4. Choose **OK**, then **Yes** to accept the terms of the license.

5. Select the keyboard layout of the device and choose **Select**.

6. Choose **Verify** to ensure that the installation media is valid and uncorrupted, or **Skip**.

7. If an existing OpenXT installation is detected, you are presented with the option to **Refresh** or perform a **Fresh Install**. If you select **Refresh**, OpenXT will be upgraded to the newer version of the software and your existing settings and VMs preserved. When the upgrade is complete, you are prompted to reboot.

> **Note**
>
> If you choose to upgrade from a previous version, you will need to update the OpenXT Tools on all VMs.

> **Note**
>
> If you chose to upgrade or refresh an existing system that has been configured for Measured Launch using install media (CDROM etc) you will be required to enter the administrative password during the first boot sequence after the upgrade.

If you choose **Fresh Install**, the installation procedure continues in the next step below.

8. You are warned that the hard drive partition will be overwritten. Select **Continue**.

> **Note**
>
> If the device has OEM partitions on it, the installer detects this and gives you a choice of leaving these partitions intact or removing them and using the entire hard drive.

9. Next you are prompted to provide a password for the system. You will need this password to log in to the control domain and generate status reports or perform other diagnostics. Enter the password and choose **OK**.

10. You are then prompted to confirm your password by entering it again. Enter the password and choose **OK**.

11. The installation commences, and a progress bar is displayed. When the installation has completed, choose **Continue** and then **Reboot** to reboot the machine.

12. When the device has rebooted the UIVM for OpenXT is displayed. If you have performed an upgrade from a previous version of OpenXT, you need to update the OpenXT Tools software installed on the VMs on your OpenXT device. To upgrade the OpenXT Tools, first uninstall the existing OpenXT Tools and then run the OpenXT Tools installer.

> **Note**
>
> If 3D Graphics Support is enabled on your VM, before upgrading the OpenXT Tools, shut down the VM, disable 3D Graphics Support, then boot the VM.

To Perform an Advanced Install or Upgrade:

1. Boot from the OpenXT installation media.

2. Choose **Advanced Install**.

3. Choose **OK** and review the software license.

4. Choose **OK** and **Yes** to accept the terms of the license.

5. Select the keyboard layout of the device and choose **Select**.

6. You are asked if you have any optional Supplemental Packs that you want to install. Choose **Yes** or **No**.

7. Choose **Verify** to ensure that the installation media is valid and uncorrupted, or **Skip** to move to the next installation step.

8. If an existing OpenXT installation is detected, you are presented with the option to **Refresh** or perform a **Fresh Install**. If you select **Refresh**, OpenXT will be upgraded to the newer version of the software and your existing settings and VMs preserved. When the upgrade is complete, you are prompted to reboot.

    > **Note**
    >
    > If you choose to upgrade from a previous version, you will need to update the OpenXT Tools on all VMs.

    If you choose **Fresh Install**, the installation procedure continues in the next step below.

9. You are warned that the hard drive partition will be overwritten. Select **Continue**.

    > **Note**
    >
    > If the device has OEM partitions on it, the installer detects this and gives you a choice of leaving these partitions intact or removing them and using the entire hard drive.

10. Choose **Continue** to begin the installation.

11. Next you are prompted to provide a password for the system. You will need this password to log in to the control domain and generate status reports or perform other diagnostics. Enter the password and choose **OK**.

12. You are then prompted to confirm your password by entering it again. Enter the password and choose **OK**.

13. Select **Yes** to enable remote access to the OpenXT device over SSH. This allows you to connect directly to the OpenXT hypervisor file system to perform diagnostic tasks.

14. Follow through the steps for configuring Measured Launch, if you wish to have this enabled. Enabling Measured Launch is the recommended configuration, though it requires additional configuration in the system BIOS. If you need to make BIOS configuration changes, you will be prompted to do so.

15. When the installation has completed, press **Continue** and then **Reboot** to reboot the machine.

16. When the device has rebooted the UIVM for OpenXT is displayed. If you have performed an upgrade from a previous version of OpenXT, you need to update the OpenXT Tools software installed on the VMs on your OpenXT device. To upgrade the OpenXT Tools, first uninstall the existing OpenXT Tools and then run the OpenXT Tools installer.

    > **Note**
    >
    > If 3D Graphics Support is enabled on your VM, before upgrading the OpenXT Tools, shut down the VM, disable 3D Graphics Support, then boot the VM.

1.4. Measured Launch for the Control Domain

When enabled, OpenXT Measured Launch measures security-critical components in the Engine Control Domain. OpenXT relies on features in the hardware to assist in measuring software components early in the boot process and to provide protection from tampering by other system software. This requires device support for Intel vPro hardware.

> **Warning**
>
> The machine must be vPro-compliant for TXT to work properly (the Intel sticker should mention "vPro"). In addition, the BIOS must be configured properly.

With Measured Launch enabled, any changes to the system or boot options will result in a prompt for the administrator password before the system continues booting. When the prompt is displayed, you can choose for this single boot to be allowed with the modification, or for the changes to be permanently allowed on subsequent boots.

If the changes are not permanently allowed, the administrative password will be required on all subsequent boots until the changes are allowed permanently, or reverted.

> **Warning**
>
> Some BIOS versions of Dell systems with 3rd-generation i5 and i7 CPUs (Ivy Bridge) have bugs related to Measured Launch. If you are using one of these systems, you will be warned when setting up Measured Launch. On a system with these problems, the measurement stored by the BIOS in PCR[1] must be excluded from the PCR values used to seal the OpenXT Engine configuration partition. For a description of PCR[1] and the contents measured within see the *OpenXT Architecture Guide*.
>
> When Dell issues a new BIOS with this issue resolved, the value of PCR[1] can be added back to the measurement list by an administrator using the procedure the Procedure: "To restore PCR[1] to the list of PCRs to which the Engine config partition is sealed".

1.4.1. Enabling Measured Launch for the Control Domain at Installation

It is possible to enable Measured Launch during the setup procedure using the *Advanced installation* option. This method is automated and will walk you through proper configuration. This is the recommended configuration method.

> **Note**
>
> Enabling Measured Launch at installation time will cause two additional reboots during the first boot process. The first boot of a OpenXT system typically requires one reboot after some file system operations are performed. The initial Measured Launch sealing operation must be performed after these file system operations are completed. The system will reboot again after the initial sealing operation. This final reboot will be the first first Measured Launch of the platform.

1.4.2. Enabling Measured Launch for the Control Domain After Installation

OpenXT highly recommends configuring Measured Launch at install time. It is possible, however, to enable Measured Launch after installation using the following steps:

> **Warning**
>
> The following steps *must* be performed *exactly* as described, in the *exact order* given below, before installing OpenXT. If this procedure is not executed successfully, all VMs that are encrypted will *not* be protected.

To Enable Measured Launch:

1. Update the system BIOS to the latest version available from the OEM.

2. Boot the system and enter the BIOS setup.

3. Disable the serial port and the parallel port. We also recommend that you disable any other devices or ports that you do not plan on using.

4. Exit the BIOS setup, saving the changes, reboot, and enter the BIOS setup again.

5. Disable TXT.

6. Exit the BIOS setup, saving the changes, reboot, and enter the BIOS setup again.

7. Clear the TPM (this will also disable it).

8. Exit the BIOS setup, saving the changes, reboot, and enter the BIOS setup again.

9. Enable the TPM.

10. Exit the BIOS setup, saving the changes, and power off the machine (do NOT reboot).

11. Power up the machine, enter the BIOS setup again and enable TXT.

12. Exit the BIOS setup, saving the changes, and again power off the machine (do NOT reboot).

13. Power up the machine, boot to the installation media, and install OpenXT.

14. Once installed, when OpenXT boots, before doing anything else, open a command prompt (**CTRL+SHIFT+T**, and as an SELinux admin (see the Procedure: "Entering the Administrative Role" for how to enter the SELinux admin role), run the following command:

    ```
    tpm-setup
    ```

15. Close the command prompt window.

16. Restart the machine by clicking the **Power** on the upper left corner of the UIVM for OpenXT and selecting **Restart**.

17. On the initial boot after running **tpm-setup**, the control domain filesystem is inspected and the results stored in the TPM. After boot, it is necessary to restart again immediately, by clicking the **Power** on the upper left corner of the UIVM for OpenXT and selecting **Restart**.

➥ **Warning**

After you enable TXT and TPM in the system BIOS, be sure to complete the tpm-setup process as soon as possible.

- If TXT and TPM are BIOS-enabled but the tpm-setup procedure is incomplete, you might experience hardware-specific instability. For example, the device may not sleep properly in this state. Time spent in such a state must be minimized at all costs. No VM or platform operations should be performed in this state.

- To minimize system exposure to remote attackers before the tpm-setup procedure is complete, perform OpenXT platform provisioning and tpm-setup in an isolated network or standalone configuration. The tpm-setup procedure should be completed as soon as possible after OpenXT installation.

1.4.3. Restoring PCR[1] to Measured Launch Configuration

To restore PCR[1] to the list of PCRs to which the Engine config partition is sealed:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Enter the SELinux administrative domain as described in the Procedure: "Entering the Administrative Role"

3. Execute the following command to add PCR[1] to the list of PCRs included in the seal operation:

    ```
    sed -i -e 's&^\(.*\)^&\1 -p 1&' /config/config.pcrs
    ```

4. Mount the file system writable to force the system to reseal itself:

    ```
    rw
    ```

5. Reboot the system after powering off all VMs. PCR[1] will not be restored to the measurement list until the platform is rebooted. On reboot, the administrative password will be required to reseal the platform.

1.5. SELinux and XSM Policy in the Control Domain

By default, SELinux and XSM (Xen Security Modules) policy in the control domain is in the enforcing mode. The following sections describe the ways in which you can change this behavior for the current OpenXT session, or

through configuration options that are put into effect on each system boot. This section closes with a brief discussion of the effect SELinux has on the execution of system administration commands.

1.5.1. Possible Modes of Operation for SELinux and XSM

There are 3 possible values for SELinux in the `/etc/selinux/config` file. This file is parsed on system boot and this value determines how SELinux behaves when the policy is loaded into the kernel. These modes are defined by the values:

- `enforcing`, which enables all SELinux functionality.

- `permissive`, which allows operations but creates a log of operations that would be denied if SELinux was set to `enforcing`.

- `disabled`, which disables SELinux in the kernel. Putting the system into this state is highly discouraged.

When XSM policy is present the OpenXT hypervisor has only two modes of operation:

- `enforcing`, which enables all XSM functionality.

- `permissive`, which allows operations but creates a log of operations that would be denied if XSM was set to `enforcing`.

XSM has no equivalent of the SELinux `disabled` mode when a policy is loaded.

1.5.2. Controlling SELinux Policy Enforcement on System Boot

By default, SELinux policy in the control domain is in enforcing mode. This can be seen by consulting the `/etc/selinux/config` file and viewing its contents:

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

Any change to this file requires a system reboot to take effect. Runtime changes to the SELinux enforcement status can be made by following the instructions in Section 1.5.4: "Changing the SELinux Mode for the Current Session".

To change SELinux Policy Enforcement from Enforcing to Permissive:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Enter the SELinux administrative domain as described in the Procedure: "Entering the Administrative Role"

3. Run the following command:

```
sed -i -e "s/SELINUX=enforcing/SELINUX=permissive/" /etc/selinux/config
```

To change SELinux Policy Enforcement from Permissive to Enforcing:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Enter the SELinux administrative domain as described in the Procedure: "Entering the Administrative Role"

3. Run the following command:

```
sed -i -e "s/SELINUX=permissive/SELINUX=enforcing/" /etc/selinux/config
```

1.5.3. Controlling XSM Policy Enforcement on System Boot

The XSM policy is interpreted and enforced by the OpenXT hypervisor. All data relevant to XSM is passed to the hypervisor as command-line options at boot time by the GRUB boot loader. Thus all configuration changes relevant

to XSM must be made through the GRUB configuration file: `/boot/system/grub/grub.cfg`. Any change to this file requires a system reboot to take effect; no changes to XSM enforcement can be made at run time.

To Change XSM Policy Enforcement from Enforcing to Permissive:

1.　In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2.　Enter the SELinux administrative domain as described in the Procedure: "Entering the Administrative Role".

3.　Run the following command:

```
sed -i -e "s/flask_enforcing=1/flask_enforcing=0/" /boot/system/grub/grub.cfg
```

To Change XSM Policy Enforcement from Permissive to Enforcing:

1.　In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2.　Enter the SELinux administrative domain as described in the Procedure: "Entering the Administrative Role".

3.　Run the following command:

```
sed -i -e "s/flask_enforcing=0/flask_enforcing=1/" /boot/system/grub/grub.cfg
```

1.5.4. Changing the SELinux Mode for the Current Session

To view the SELinux mode for the current session:

1.　In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2.　Change to the administrative role as described in the Procedure: "Entering the Administrative Role"

3.　Execute the **getenforce** command.

To change the SELinux mode to permissive:

1.　In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2.　Change to the administrative role as described in the Procedure: "Entering the Administrative Role"

3.　Run the following command:

```
setenforce permissive
```

4.　To verify the command was successful you may execute the procedure described in the Procedure: "To view the SELinux mode for the current session".

To change the SELinux mode to enforcing:

1.　In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2.　It's assumed that if the administrator is putting SELinux into enforcing mode that the current mode is permissive and it will be unnecessary to change to the administrative role.

3.　Run the following command:

```
setenforce enforcing
```

4.　To verify the command was successful you may execute the procedure described in the Procedure: "To view the SELinux mode for the current session".

1.5.5. The Effect of SELinux on Administrative Commands

OpenXT supports many administrative functions while the SELinux policy is enforced. To execute administrative commands while SELinux is enforcing, the administrator must follow this procedure:

Entering the Administrative Role:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Verify your current role by executing the following command:

    ```
    id -Z
    ```

    Your role should be:

    ```
    root:staff_r:staff_t:s0-s0:c0.c1023
    ```

3. Run the following command to enter the administrative domain:

    ```
    newrole -r sysadm_r
    ```

    `sysadm_r` is the identifier for the standard SELinux system administrator role.

4. Verify the role has changed to `sysadm_r` by executing the following command:

    ```
    id -Z
    ```

    Your role should now be:

    ```
    root:sysadm_r:sysadm_t:s0-s0:c0.c1023
    ```

5. Execute the command as you normally would.

If the command fails even while in the administrative role you may put SELinux into its permissive mode using the procedure described in the Procedure: "To change the SELinux mode to permissive" and re-execute the command.

1.5.6. Temporarily Disabling SELinux To Allow File Writing

Before copying files to the control domain filesystem, for example ISOs or VHD files, you need to enter the SELinux administrative role, temporarily disable SELinux enforcement, and set the filesystem to read/write. After copying the desired files, re-enable SELinux and reset the file system to read only.

➡ **Note**

> You can also use the `/tmp` directory, which is by default read/write.

To Temporarily Disable SELinux To Allow File Writing:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Enter the following commands:

    ```
    nr
    setenforce 0
    rw
    ```

3. When you have completed your copy operation, run the following commands to re-enable SELinux and reset the filesystem to read only:

    ```
    setenforce 1
    ro
    ```
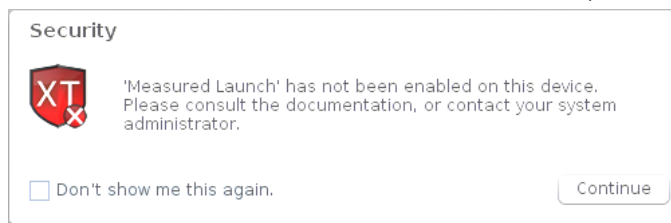
Chapter 2. Using OpenXT

When you start your OpenXT device, the UIVM for OpenXT UI is displayed. This is the user interface that allows you to manage your OpenXT device and the VMs installed on it. Using UIVM for OpenXT you can:

- Create VMs, edit VM properties, and delete VMs.

- Set up networking.

- Control the power saving functions of VMs and the device as a whole.

- Manage OpenXT device settings, including authentication, touchpad sensitivity and speed, and UIVM for OpenXT wallpaper.

- Manage USB devices.

> **Note**
>
> If the Measured Launch feature has not been enabled, a message box appears:
>
> Security
> 'Measured Launch' has not been enabled on this device. Please consult the documentation, or contact your system administrator.
> ☐ Don't show me this again.   Continue
>
> Click **Continue** to clear the message.

> **Note**
>
> If one or more VMs have been set to start automatically on device startup, you can return to UIVM for OpenXT by either:
>
> - Pressing **Ctrl + 0**.
>
> - Clicking **Home** in the switcher bar located in the middle of the top of the VM display.

Figure 2.1: "UIVM for OpenXT With No VMs Installed" shows OpenXT as it appears before any VMs are installed.

13

Figure 2.1. UIVM for OpenXT With No VMs Installed:
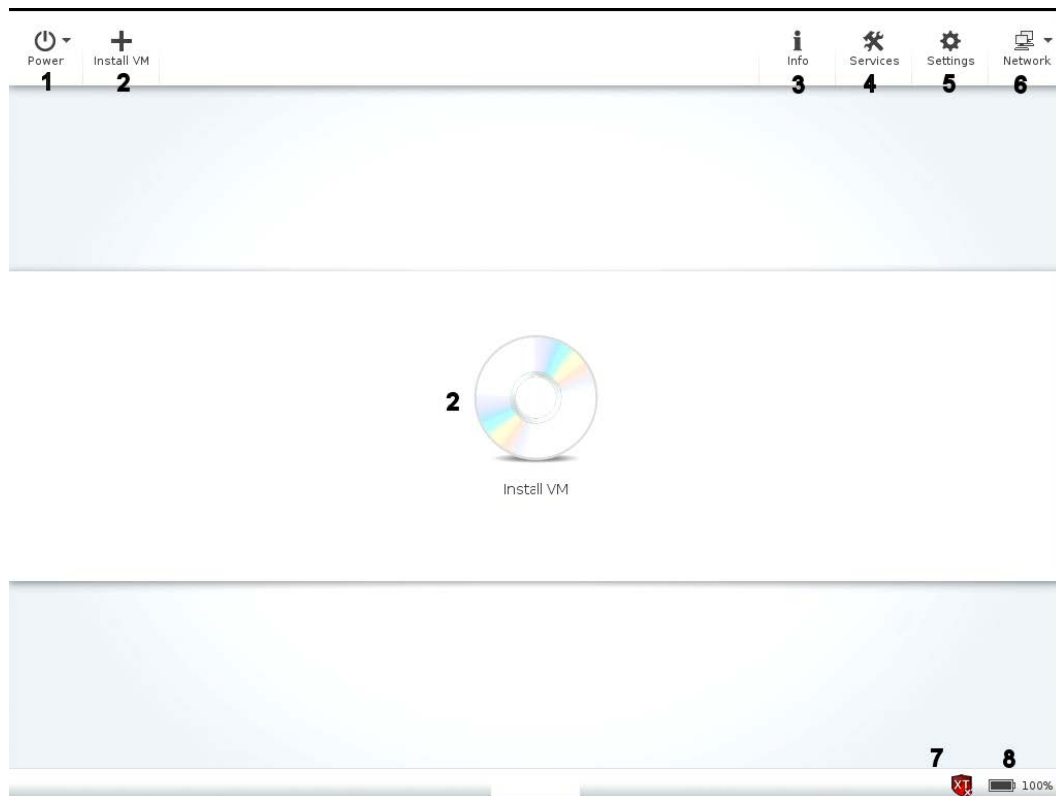
Legend for Figure 2.1: "UIVM for OpenXT With No VMs Installed"

1. **Power** Provides power controls for the device and the VMs running on it, allowing you to shut down, sleep, hibernate and restart OpenXT and all the VMs running on it.

2. **Install VM** Click here to create a new VM. When no VM has yet been installed, there is also a **Install VM** icon in the center of the main window.

3. **Info** Click here to open the **Information** window. In this window you can see information about the software version, the hardware components and the network interfaces present. You can also generate status reports from this window.

4. **Services** Click here to open the **Services** window. In this window you can see a list of the service VMs present on the host. By default, there is a Network service VM present on the system after installation. In this window you can control many of the properties of your OpenXT device.

5. **Settings** Click here to open the **Settings** window. In this window you can control many of the properties of your OpenXT device.

6. **Network** Click here to set up wired and wireless networking for your OpenXT device. You can control which networks each VM has access to by editing the VM properties.

7. An **XT Measured Launch icon** displays the status of the *Measured Launch* security settings.

8. A **Battery Power Gauge** shows how much power is left in the case of a laptop running on battery power.

2.1. OpenXT Services

The **Services** window lists the service VMs that are present on the system. By default, there is a Network service VM present on the system after installation. There are a number of general settings for service VMs that can be changed by clicking the **Edit** button to the right of a service VM in the list.

The properties shown by clicking **Edit** are the same as the properties available in the **VM Details** dialog that allows you to view and modify user VM properties. See Section 2.6: "VM Details" for details.

2.2. OpenXT Settings

There are a number of general settings for the OpenXT device that can be changed from the **Settings** dialog box.
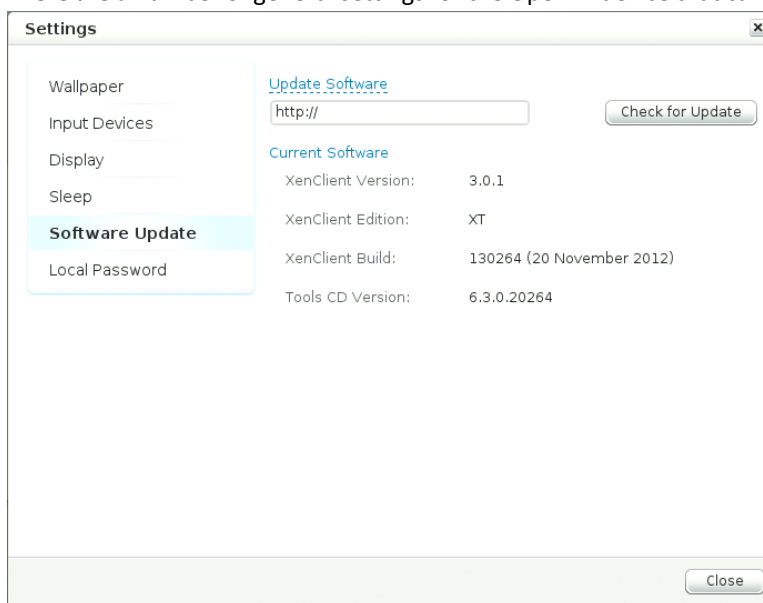
- **Wallpaper** allows you to choose a background image to use as wallpaper for the UIVM for OpenXT.

- **Input Devices** allows you to choose a **Keyboard Layout**, enable or disable **Touchpad Options** (Tap to Click and Scrolling), adjust the **Touchpad Speed**, and choose whether or not there is a **Mouse Pointer Trail**.

- **Display** allows you to adjust the **Screen Brightness**, and to enable **Screen Lock Settings**.

- **Sleep** allows you to define how the OpenXT system and the VMs running on it orchestrate how it will sleep. Under **System sleep**, you can choose what happens to the system given that any running VMs are asleep. The choices are **Do not put the system to sleep** or **Put the entire system to sleep after** _x_ **minutes**, where _x_ is a number of minutes that you specify. Under **When the lid closes**, you can choose to either **Put the entire system to sleep** (VMs and all) or **Do not put anything to sleep**, separately for when the system is on AC power or on battery power.

- **Software Update** allows you to view the current version and build of the OpenXT software and the Tools CD version, and allows you to provide a URL and check there for newer versions of the software.

- **Local Password** allows you to set a password to enable local authentication.

2.3. Creating VMs on OpenXT

You can create VMs on OpenXT by using operating system installation media. The following operating systems are supported:

- *Microsoft Windows*

  - Windows XP SP3 32-bit

  - Windows 7 SP1 32-bit

  - Windows 7 SP1 64-bit

  - Windows 8

- *Linux*

  - Ubuntu 11.04 32-bit

  - Ubuntu 12.04 32-bit

  - Ubuntu 12.10 32-bit

  - Ubuntu 13.04 32-bit

  - Ubuntu 13.10 32-bit

> **Important**
>
> The Ubuntu Unity desktop manager is not supported by OpenXT. Please use an alternative desktop
> manager. For example:
> ```
> apt-get install lubuntu-desktop
> ```

There are three main steps to creating a VM on OpenXT:

- Create the VM, specifying:

  - a name

  - an optional description

  - which template it will use

  - how much virtual memory and how many virtual CPUs it will have

  - how much disk space it will use

  - the type of network it will be on

- Install a supported operating system on the VM.

- Install the OpenXT Tools on the VM.

Once these steps have been completed, you can optionally enable 3D Graphics Support for this VM. Only one running
VM can benefit from 3D Graphics Support technology.

2.3.1. Creating VMs from an Installation Disk
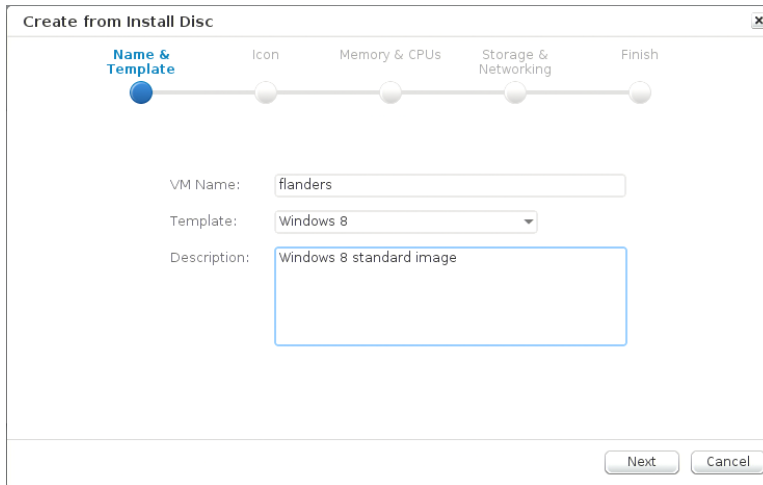
> **Note**
>
> - If you are installing from an external optical drive that was connected to your OpenXT device when
>   OpenXT booted, please unplug the optical drive and plug it in again before continuing.
>
> - Installation using an external optical media device is not supported if your device has an internal optical
>   media drive.
>
> - OpenXT only supports operating systems installed on the primary partition.
>
> - When installing a second VM from an installation disk, shut down the VM you installed first. Otherwise,
>   the first VM continues to own the physical optical media drive, and the second VM will therefore fail to
>   see the drive and will be unable to boot into the installer.

To Create a VM Using an Installation Disc:

1. Click **Add VM** and choose **Install from Disc**. The **Create from Install Disc** wizard opens with the **Name & Template** page displayed.
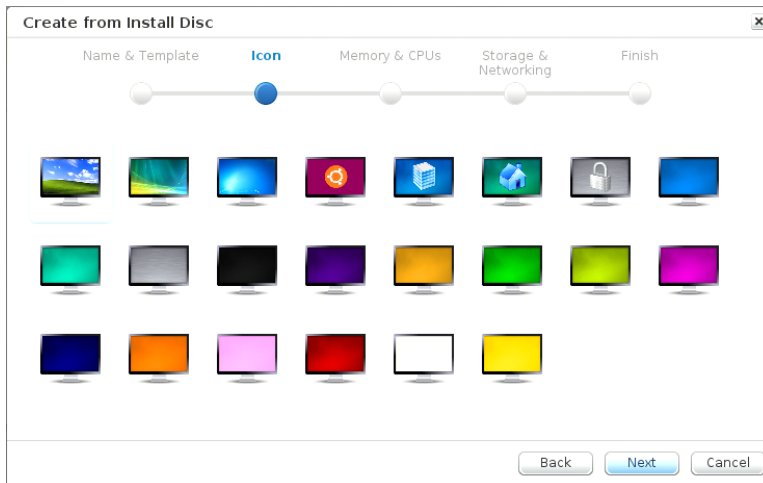

    Enter a **VM Name** and an optional **Description**, if desired. Select the operating system template from the **Template** dropdown list. The choices are:

    • Windows 8

    • Windows (7, XP)

    • Linux (Debian, Ubuntu)

2. Click the **Next** button. The **Icon** page is displayed.

    Select an icon to represent the VM.

3. Click the **Next** button. The **Memory & CPUs** page is displayed.

Specify the amount of **Memory** to assign to the VM. (The total amount of memory and the available free memory on the device are displayed below.)

Choose the number of **vCPUs** (virtual CPUs) to assign to the VM from the dropdown list.

4.   Click the **Next** button. The **Storage & Networking** page is displayed.

Specify the **Virtual Disk Size** to assign to the VM (the default is 80 GB).

Select from the choices available for **Disk Encryption** - *AES-256* (the default), *AES-128*, or *None*.

Select the **Wired Network** mode. The options are:

• *Internal* which only allows for network communication between VMs.

• *Bridged* (the default), which gives the VM full access to the networks that the OpenXT host computer is connected to.

• *Shared* which creates a private network on the OpenXT system and allows outgoing connections using NAT (Network Address Translation). This reuses a single IP address for all VMs on the system. In this case incoming connections to the VM are not possible.

Note

Bridged mode requires that each virtual NIC is appropriately configured. Either the physical network will have to provide DHCP to allow the interface to establish an IP address and associated configuration, or you will need to statically configure the network settings on that interface from within the VM.

Select the **Wireless Network** mode. The options depend on what wireless devices are present on the system. On a laptop with a standard wireless interface and a mobile wireless interface, for example, the choices would be:

• *Shared Wireless*, which gives the VM full access to the wireless network(s) that the OpenXT host device is connected to using a wireless network card.

• *Shared 3G*, which gives the VM access to any 3G networks that the OpenXT host device is connected to.

5. Click the **Next** button. The **Finish** page is displayed.
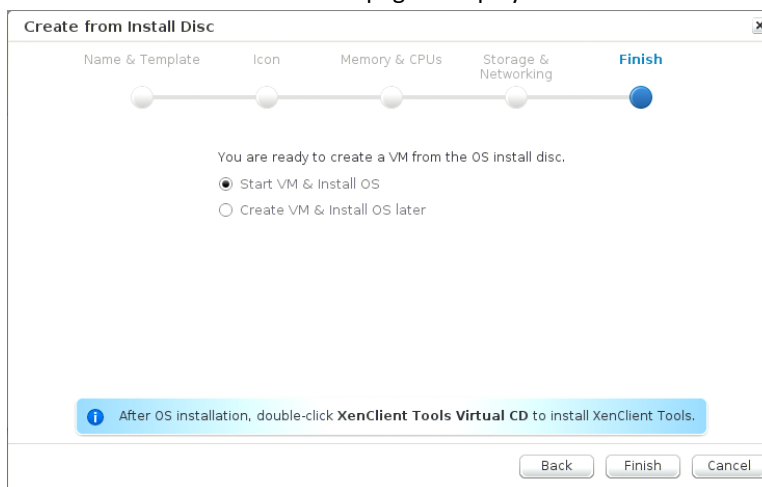
By default, **Start VM & Install OS** is selected. If you would prefer to install the operating system at a later time, select the **Create VM & Install OS later** radio button.

Warning

• If you are using a Windows installation disk that originated from a OEM supplier, do *not* start the VM automatically - be sure to select the **Create VM & Install OS later** radio button. You will first need to enable OEM installation for the VM so that system properties are presented in a manner that allows the OEM installation disk to verify that it is being installed on genuine hardware. See the Procedure: "To Enable VM Installation from OEM Installation Media" for information about how to do this.

• For Ubuntu version 12.10, do *not* start the VM automatically - be sure to select the **Create VM & Install OS later** radio button. There an error in the kernel in this release of Ubuntu that prevents installation of it on a VM unless you follow the Procedure: "To Install Ubuntu 12.10 onto a VM".

6. Click the **Finish** button. The VM will be created according to your specifications.

Note

If you selected disk encryption while creating the VM, a message may appear requesting you to move the mouse to generate entropy to be used in the encryption process.

If you selected **Start VM & Install OS** above, the OpenXT display switches to the VM display and you can perform the installation. If you selected **Create VM & Install OS later** above, the display will return to the UIVM for OpenXT, where you will see an icon representing the new VM.

Now that you have created a new VM, the next step is to install an operating system on it as described in the Procedure: "To Install an Operating System onto a VM".

2.3.2. Installing an Operating System on a VM

To Install an Operating System onto a VM:

1. Insert the installation media into the optical media drive. For a network boot installation, skip to the next step.

2. Start the VM if it is not already started. The new VM takes focus and begins to boot into the operating system installation procedure. For a network boot, press **F12** (or the relevant key) and select the appropriate boot device.

    Note

    For security reasons the optical media drive is only accessible from one VM at a time. If a VM is running that has the optical drive assigned to it, it is necessary to shut down that VM before you can boot into the operating system installation medium.

3. Complete the operating system installation as you would do on a physical machine.

    Note

    OpenXT recommends not enabling automatic Windows updates until you have installed the OpenXT Tools.

4. When installation is complete, install the OpenXT Tools as described in the next section.

    For an Ubuntu VM (with the exception of Ubuntu 12.10), first update the operating system software, and then install the OpenXT Tools as described in the next section.

5. For a Windows VM, run Windows Update.

6. Once the installation is complete and updates have been installed you can press **Ctrl + 0** to return to UIVM for OpenXT

To Enable VM Installation from OEM Installation Media:

If you are installing Windows from an OEM version of the Windows installation media, use this procedure to enable OEM installation:

1. Hover your mouse over the VM icon and click **Details** to open the VM details window.

2. Click the **Advanced** menu item.

3. From the **Allow OEM Windows installs** dropdown list, select **Enabled**.

4. Click **Save**.

5. Restart OpenXT. When OpenXT has restarted, start the VM and continue with the standard VM installation procedure.

To Install Ubuntu 12.10 onto a VM:

1. Follow the normal procedure using the **Create from Install Disk** wizard with the **Linux (Debian, Ubuntu)** template up to the final step, and choose **Create VM & Install OS later** before clicking **Finish**.

2. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

3. Run the following command:

```
xec-vm -n <ubuntu_12.10_VM_name> set xci-cpuid-signature false
```

4. Close the console, and start the VM with the ISO in the optical drive. Follow the prompts to install the operating system.

> **Note**
>
> You will not be able to install the OpenXT Tools until you update the kernel.

5. Update the kernel in the standard manner.

6. Shut down the VM.

7. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

8. Run the following command:

```
xec-vm -n <ubuntu 12.10 VM name> set xci-cpuid-signature true
```

9. Close the console, and start the VM.

10. Install OpenXT Tools in the usual manner as described in the Procedure: "To Install the OpenXT Tools on a Linux VM".

2.3.3. Installing the OpenXT Tools

After VM installation is complete, there is the additional step of installing the OpenXT Tools on it before it can be used. The OpenXT Tools include high performance virtualization-aware drivers, and the OpenXT Switcher Bar to allow switching between the VMs using a mouse. Additionally, because OpenXT uses a network driver service VM, there is no network connectivity available until the OpenXT Tools (which include the network PV driver) have been installed in the VM.

> **Warning**
>
> Running a VM without OpenXT Tools installed is **not** a supported configuration. VMs without the OpenXT Tools yet installed are indicated with a warning icon in UIVM for OpenXT.

> **Warning**
>
> Installation of any software that uses low-level drivers to monitor disk operations before installing the OpenXT Tools (for example, antivirus software) will result in problems when hibernating, rebooting, or shutting down the VM. The installation of the OpenXT Tools is required for a VM to properly run on OpenXT.

> **Note**
>
> If you intend to create a stub domain on this VM to host its ioemu process, note that this must be done before installing the OpenXT Tools. See Section 3.4: "Using Stub Domains".

To Install the OpenXT Tools on a Windows 8 or Windows 7 VM:

1. Select **Computer** from the **Start** menu, or press **Win + E**.

2. Select the optical drive from the displayed storage devices, which is usually mapped as the `E:` drive.

3. Run `setup.exe` from the disk, accept the license agreement, and follow the prompts.

Note

> The OpenXT Tools require Windows .NET 4. If the VM has an earlier version of .NET, the OpenXT
>
> Tools installer will perform this setup first before installing the drivers.

4. Reboot the VM to complete the tools installation.

To Install the OpenXT Tools on a Windows XP VM:

The OpenXT Tools installer requires Microsoft .NET, which is not included in Windows XP. For this reason, on a Windows XP VM, the OpenXT Tools are installed in two stages: basic paravirtualized drivers are installed first, followed by the remaining tools.

➥ **Note**

> This section is only relevant if a stub domain is not enabled on the VM. See Section 3.4: "Using Stub Domains"

1. Connect the OpenXT device to a wired network with Internet access (to allow the .NET download).

2. Use UIVM for OpenXT to install a Windows XP VM from physical vendor media.

3. In the Windows XP VM, select the Tools CD and navigate to the **Packages** directory.

4. Run `xensetup.exe` to install the paravirtualized I/O drivers.

5. Reboot the VM and follow prompts to install PV devices.

6. Confirm network connectivity from VM to off-host IP address.

7. In Windows XP VM, run the Tools CD.

8. Choose **Install OpenXT Tools**; this will automatically download .NET.

9. Reboot the VM.

To Install the OpenXT Tools on a Linux VM:

➥ **Note**

> Do not install the OpenXT Tools on Linux using **dpkg** directly, nor by double-clicking on the package
>
> via the graphical desktop.

1. At a command line shell on the VM, change users to become the superuser:

```
sudo su
```

2. Display the available drives with the command

```
df -k
```

and observe the name of the optical drive with the OpenXT Tools; it will be something like `/media/ XenClient-tools-<version number>`.

3. Change to the `linux` directory on the optical drive with the OpenXT Tools package:

```
cd /media/XenClient-tools-<version number>/linux
```

4. Run the `install.sh` script:

```
./install.sh
```

5. Reboot the VM.

> **Note**
>
> The UIVM for OpenXT will show the tools as installed, but a reboot is required to properly complete the Tools installation.

> **Note**
>
> Ubuntu versions 11.04 and 12.04 exhibit issues with 3D Graphics. For these operating systems, please follow the OpenXT Tools installation above and the following procedure.

To Install a PVM-capable Intel Graphics Driver On a Ubuntu 11.04 or 12.04 VM:

> **Note**
>
> Do not install the OpenXT Tools on Linux using **dpkg** directly, nor by double-clicking on the package via the graphical desktop.
>
> Note that for this procedure:
>
> • an internet connection is required
>
> • the script must be executed as root
>
> • the script will download 100 MB of kernel source files in order to build a new Linux graphics driver

1. At a command line shell on the VM, change users to become the superuser:

```
sudo su
```

2. Display the available drives with the command

```
df -k
```

and observe the name of the optical drive with the OpenXT Tools; it will be something like `/media/XenClient-tools-<version number>`.

3. Change to the `linux` directory on the optical drive with the OpenXT Tools package:

```
cd /media/XenClient-tools-<version number>/linux
```

4. Run the `fix-i915-passthrough.sh` script:

```
./fix-i915-passthrough.sh
```

5. Reboot the VM.

2.4. Configuring Networks for the OpenXT Device

OpenXT device networks can be used by all VMs installed on the OpenXT device. Each individual VM can be configured to allow or disallow access to the configured networks. Use the UIVM for OpenXT Network Manager to configure your OpenXT device networks. See Chapter 2: "*Using OpenXT*" for more information about UIVM for OpenXT.

To Configure a Wired Network Connection for OpenXT:

A wired connection is automatically created if the computer is plugged in to a network. To confirm that a wired connection exists:

1. In UIVM for OpenXT, click the **Network** button. A list of available and already connected network connections is displayed.

2. Ensure that the **Wired Ethernet Connection** entry is not labeled as disconnected and grayed out.

To Configure a Static IP Address for OpenXT:

1. In UIVM for OpenXT, click on the **Network** button and select **Edit Connections...**. The **Network Connections** dialog is displayed. Wired and wireless networks are listed in their own page, selected by the tabs at the top of the dialog.
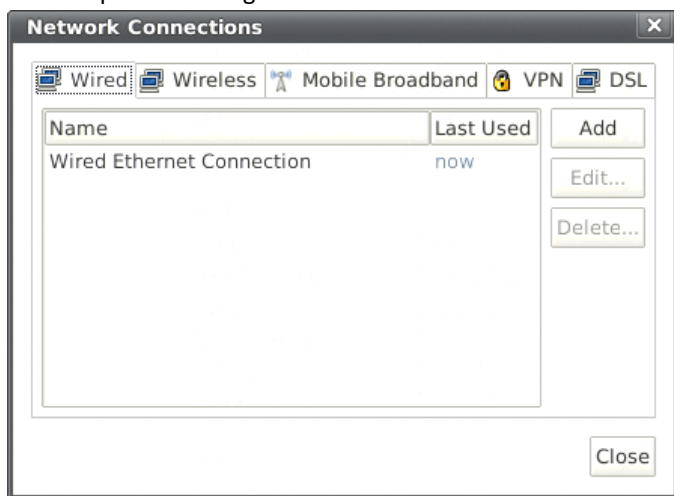
2. Select the network to edit and click the **Edit** button. The **Editing** *<network_name>* dialog is displayed.

3. Click the **IPv4 Settings** tab.

4. Select **Manual** from the **Method** dropdown list.

5. Click the **Add** button to the right of the **Addresses** section.

6. Click in the **Address** field and enter the desired static IP address.

7. Click in the **Netmask** field and enter the desired netmask.

8. Click in the **Gateway** field and enter the desired gateway address.

9. Below the **Addresses** section, click in the **DNS servers** text box and enter the desired DNS server address.

10. Click in the **Search domains** text box and enter the desired DNS server address.

11. Click the **Save...** button.

To Configure a Wireless Network Connection for OpenXT:

1. In UIVM for OpenXT, click the **Network** button.

2. Choose your preferred wireless network from the list and enter your security credentials when prompted.

To Import a Certificate for Use in Wireless Network Authentication:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Switch roles to the sysadm_r role as follows:

```
newrole -r sysadm_r
```

3. Run the following command to determine the IP address of the control domain:

```
ifconfig
```

   The relevant IP address is the one for `eth0`.

4. Create the directory `/config/certs/<ndvm-name>`:

```
mkdir -p /config/certs/<ndvm-name>
```

5. If there is only one NDVM (Network VM), copy the certificates to the `/config/certs/Network` directory using the control domain IP address. For example:

```
scp company.ca.cer root@10.80.249.175:/config/certs/Network
```

   If there are multiple NDVMs and you need to make the certificates available to another NDVM (not the one named *Network*), you need to run the following command:

```
xec-vm -n <ndvm-name> set icbinn-path /config/certs/<ndvm-name>
```

   and then copy the certificates to the `/config/certs/<ndvm-name>` directory using the control domain IP address. For example:

```
scp company.ca.cer root@10.80.249.175:/config/certs/<ndvm-name>
```

   On Windows you could use PSCP, the PuTTY Secure Copy client, or WinSCP to transfer the certificates to the control domain.

6. Close the console.

7. Reboot the OpenXT device.

8. In UIVM for OpenXT, click the **Network** button (or, if you have multiple NDVMs, click the desired NDVM button). From the bottom of the menu, select **Edit Connections** to display the **Network Connections** dialog box.

9. Click on the **Wireless** tab, select the network name, and click **Edit**.

10. In the dialog box that opens, select the **Wireless Security** tab and click on **CA Certificate** to display a browse dialog. Select the certificate and click **Open**, then click **Save** on the edit dialog, and finally click **Close** on the **Network Connections** dialog.

To Change a VM MAC Address:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the command:

```
xec-vm -n <vm_name> -c 0 set mac "<new_mac_address>"
```

2.5. Switching Between VMs

The OpenXT switcher bar is displayed when you click the small black bar at the top center of your VM screen. You can use the switcher bar or one of the other methods listed below to switch between VMs.

Note

   The switcher bar is installed when you install the OpenXT Tools. Note that it might not appear on the first boot after tools installation. If so, reboot the VM once more and the Switcher bar will be displayed.

To switch from UIVM for OpenXT to a VM, you can:

- Press **Ctrl +** *<vm_switcher_key>*, for example, **Ctrl + 1**. This is known as the VM Switcher key. To return to UIVM for OpenXT at any time, press **Ctrl + 0**.

- Click on a VM icon.

- Click the **Switch** button near the top left of a VM's **Details** dialog.

To switch between VMs, you can:

- Use VM Switcher keys.

- Click on a VM icon in the Switcher bar. You can also click **Home** to return to UIVM for OpenXT.

- Press **Windows Key + Alt** to cycle through all running VMs, in a manner similar to the way **Alt + Tab** switches between Windows applications.

> **Note**
>
> The ability to switch between VMs is disabled when a VM with 3D Graphics Support enabled is booting, shutting down, or when logging in to it. This includes when Windows is installing updates before shutting down. See Section 2.10: "3D Graphics Support" for more information about 3D Graphics Support.

2.6. VM Details

UIVM for OpenXT provides a simple, intuitive interface that you use to install VMs, start and stop VMs, and edit their properties.

The following figure shows the UIVM for OpenXT interface with three VMs installed on it. Running VMs are labeled **On** and shut down VMs are labeled **Off**. If you hover your mouse pointer over a VM icon, it increases in size and presents you with a power switch icon (either **Shut Down** for a running VM or **Start** for a shut down VM), and a button labeled **Details**.
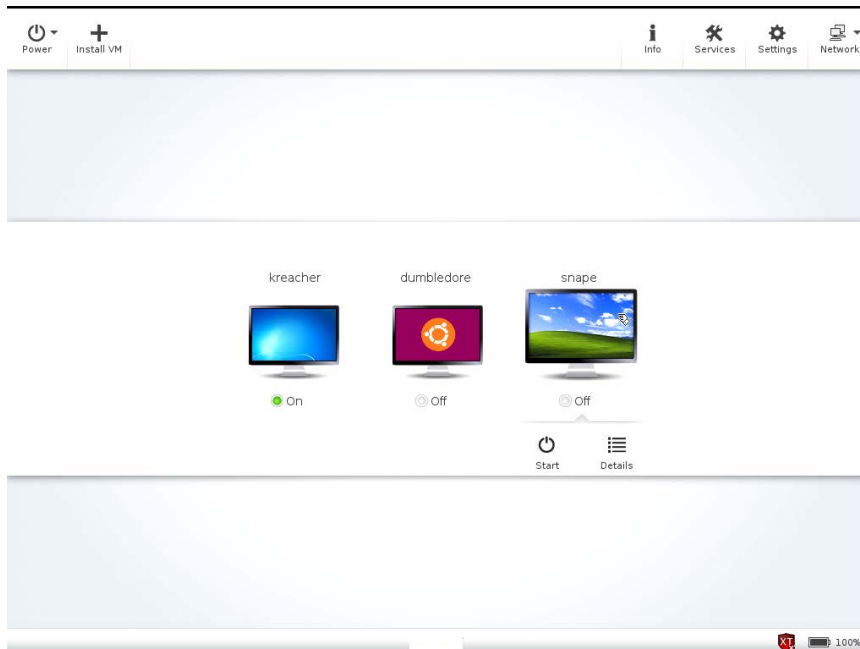
To access VM options, hover your mouse over a VM icon, then click the **Details** button. The **VM Details** window is displayed.
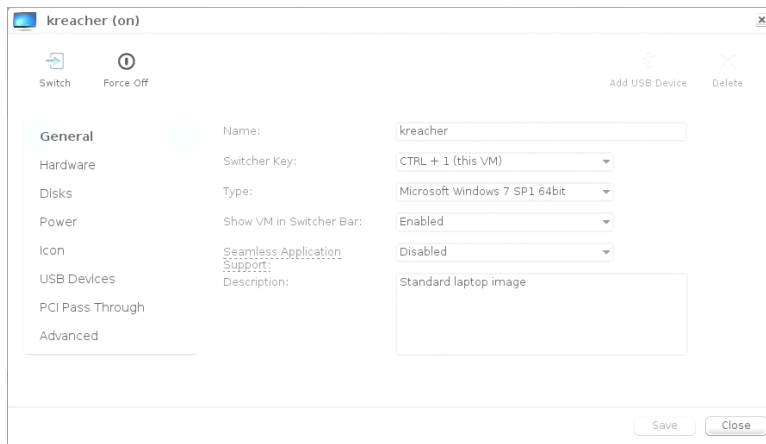
The buttons along the top left of the window depend on whether the VM is currently running or not. If it is, you can **Switch** to the VM's display from the UIVM for OpenXT, or **Shut Down**, **Reboot**, **Sleep** or **Hibernate** the VM.

On the top right are buttons to **Add USB Device** and to **Delete** the VM. The latter is greyed out and unavailable unless the VM is shut down.

On the left side below the power buttons are links that open the various views of the VM's details:

- **General** contains the a text box with VM **Name**; a pull-down list of available key combinations you can select as the **Switcher Key** for this VM; a pull-down list of operating systems you can select as the **Type** for this VM; a control, **Show VM in Switcher Bar**, that enables whether or not this VM will be displayed in the Switcher Bar.

- **Hardware** allows you to view and edit various hardware settings, such as the number of **vCPUs**; the amount of **Memory (MB)**; whether **3D Graphics** is enabled or disabled for this VM; a control to select whether the OpenXT Tools are present in the **Virtual CD** drive; the **Guest Tools Version**; a control to select the **Wireless Network**; a control to set the **Wired Network**; and **Wired MAC Address**.

- **Disks** allows you to view and edit the virtual disks for this VM. For each disk, you can enable or disable Persistence (which controls whether or not changes to the disk data persist across reboots). You can also **Delete** a disk, and you can **Add** a new disk. The latter two are greyed out and unavailable unless the VM is shut down.

- **Power** allows you to enable **Autoboot**, which causes the VM to be started automatically when you start your OpenXT device; **Power Control**, which enables you to specify whether or not the host will hibernate, sleep, or shut down when the VM does; and a control to add or delete boot devices and specify the **Boot Order**.

- **Icon** allows you to select a VM icon to be used to represent it in UIVM for OpenXT.

- **USB Devices** allows you to see the USB devices currently assigned to this VM. You can choose whether each device is always used with this VM via the **Always Use With This VM** checkbox. You can also choose whether or not any free USB devices will be automatically assigned to this VM via the **Auto-assign USB Devices** control.

- **PCI Pass Through** allows you to pass through any of the PCI devices (for example, the USB controllers) to the VM. If any devices are already listed, you can **Stop** passing them through. These are greyed out and unavailable unless the VM is shut down.

> **Note**
>
> If you assign a USB controller to a VM using PCI Pass Through, you need to reboot the system before you can use devices attached to that controller. Likewise if you unassign a PCI devices a reboot is required before it will be available to be assigned elsewhere.

27

Caution

This section is for advanced features that should only be modified if you understand their impact on the system.

- **Advanced** allows you to change advanced VM features. These are grouped into

  - **Isolation Policies**, which includes enabling or disabling the VM's use of a **Stub Domain**, **Wired Network Access**, **Wireless Network Access**, **CD Reading**, **CD Writing**, **Audio Playback**, and **Audio Recording**.

  - **Hardware Compatibility**, which includes enabling or disabling whether or not to **Allow OEM Windows Install**, **Expose Physical Hardware Information**, **Expose Physical OEM Hardware** and **Intel AMT Passthrough**

  - **Virtual Compatibility**, which allows you to enable or disable whether or not to **Emulate Microsoft Hyper-V**, enable or disable if this VM is a **Hardware Virtual Machine**, and allows you to set the values for certain advanced parameters of the system: **Kernel Path**, **Kernel Extraction Path**, **Command Line**, and **Initial Ramdisk**.

Caution

This section is for advanced features that should only be modified if you understand their impact on the system.

2.7. VM Networks

OpenXT device networks can be used by all VMs installed on the OpenXT device. You use the UIVM for OpenXT Network Manager to configure your OpenXT device networks. See Section 2.4: "Configuring Networks for the OpenXT Device" for more information about the networks available to the OpenXT device.

Each individual VM can be configured to allow or disallow access to the configured networks. This is done through each VM's **Details** dialog. Hover your mouse over a VM icon, then click the **Details** button. The **Details** window is displayed. Click **Networks** to display the current networks this VM has access to. You can click the **Remove** button to the right of a network to remove it.

Note

Making changes on the Networks tab is not allowed until the OpenXT Tools have been installed and the VM has been shut down.
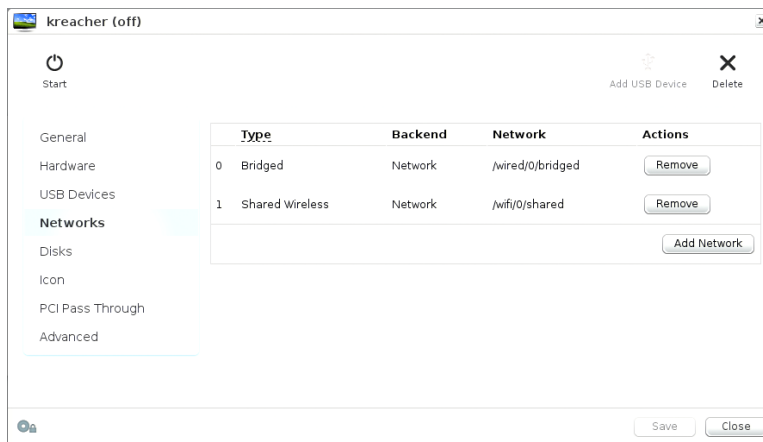
To add another network, click the **Add Network** button. The **Add a Network** dialog opens:
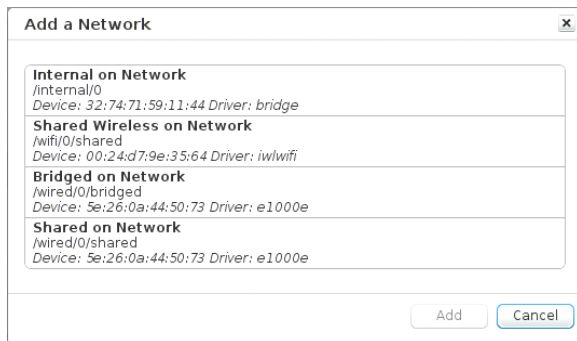
This dialog allows you to see all the networks available to the OpenXT device and allows you to select any of them to add to the VM.

For more information about OpenXT networking see Chapter 5: "*Networking Configuration*".

2.8. VM Power Controls

When a VM is running, UIVM for OpenXT displays a set of power and configuration controls.
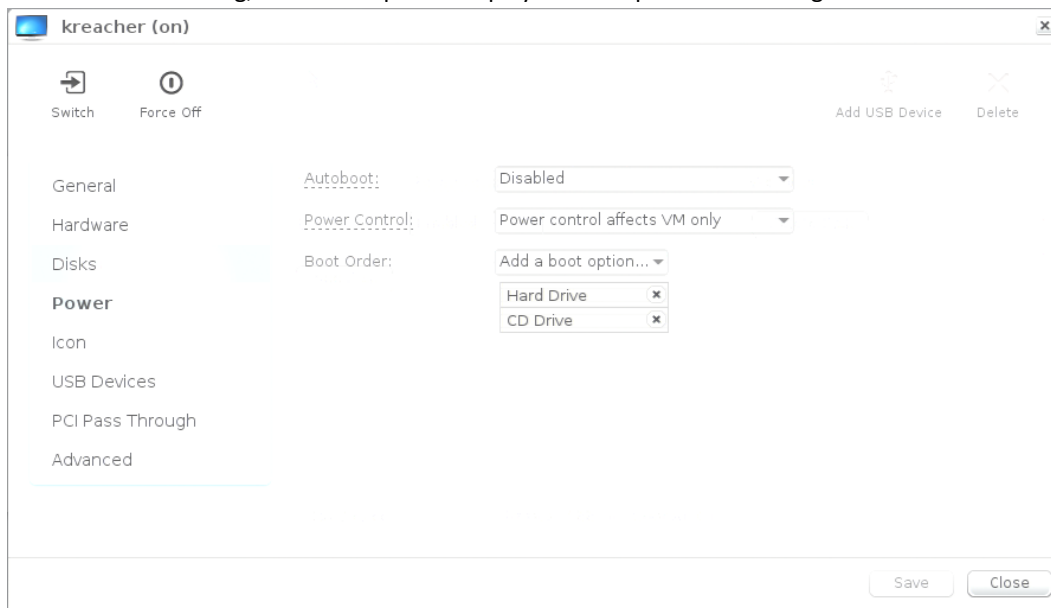
Force Shut Down performs a hard shut down of the VM, similar to disconnecting the power source from a bare metal device. **Shut Down**, **Reboot** and **Hibernate** perform the same function as if they were initiated from within the VM. You can also use any one of the following combinations to achieve the power action effect you desire:

Click a VM icon
　　This will start the VM if it is not already started.

Shift + click a VM icon
　　This will start the VM without switching focus to it.

Shift + click a **Start** icon
　　This will start the VM without switching focus to it.

The **Autoboot** property controls whether this VM is started automatically when the OpenXT device is started. The **Power Down** property controls whether the OpenXT device is shut down automatically when the VM is shut down.

> **Note**
>
> Sleeping a 3D Graphics Support VM is equivalent to sleeping the entire device, except that the other VMs are not put into the sleep state. Attempting to switch away from a sleeping 3D Graphics Support VM results in the 3D Graphics Support VM leaving the sleep state.

2.9. Working With VMs

This section contains procedures for working with VMs.

To Edit VM Properties:

1. Hover your mouse over the VM icon and click **Details** to open the VM details window.
2. Click the relevant tab.
3. Click **Edit** and make your changes.
4. Click **Save**. Most configuration items only take effect on the next boot of the VM.

To Delete a VM:

Use the following procedure to delete a VM.

> **Warning**
>
> There is no way to recover a deleted VM.

1. Shutdown the VM.
2. Hover your mouse over the VM icon and click **Details** to open the VM details window.
3. Click **Delete**, and confirm that you want to delete the VM.

To Assign a USB Device to a VM:

1. Ensure that the VM you want to assign the USB device to is running.
2. Hover your mouse over the VM icon and click **Details** to open the VM details window.
3. Click **Add a Device**. The **Connect a Device** dialog is displayed.
4. Select the USB device in the list.
5. If the USB device you want to re-assign is currently in use by a running VM you will be warned to eject the device first.
6. Click **Connect**.
7. If you want the assignment to persist across reboots, check the **Always use with this VM** checkbox.
8. Click **Save**.

To Change the VM Switcher Key:

1. Hover your mouse over the VM icon and click **Details** to open the VM details window.
2. Click **General**.
3. Click **Edit**.
4. Select the new switcher key from the **Switcher Key** dropdown list. If you select a switcher key that is already in use by another VM, the switcher keys of the two VMs will be swapped.

5. Click **Save**.

2.10. 3D Graphics Support

3D Graphics Support provides support for hi-fidelity 3D applications by providing direct access to the graphics processor of the OpenXT device. Only one running VM can have 3D Graphics Support enabled.

> **Important**
>
> Ensure that your OpenXT device is not connected to a second screen when enabling or disabling 3D
>
> Graphics Support.

To Enable 3D Graphics Support:

1. Hover your mouse over the VM icon and click **Details** to open the VM details window.
2. If you are enabling 3D Graphics Support on a Vista VM, navigate to **Start > Control Panel > Classic View > System > Advanced System Settings > Hardware > Windows Update Driver Settings** and select **Ask me each time I connect a new device before checking for drivers**.
3. Shut down the VM.
4. Click **Hardware**.
5. Click **Edit**.
6. From the **3D Graphics** dropdown list, select **Enabled**.
7. Click **Save**.
8. Restart the VM. A newly enabled 3D Graphics Support VM boots and automatically installs the required graphics drivers. A reboot is required after the drivers have installed. When the 3D Graphics Support VM has booted, an optimum graphics resolution is automatically chosen.

    > **Note**
    >
    > It may be neccessary to manually install graphics drivers for devices with Intel HD 4000 graphics.

> **Note**
>
> If you are using a supported AMD/ATI graphics card on a laptop, please download and install the graphics drivers from the support section of your laptop manufacturer's website, not from the AMD/ATI website.

If you install the drivers on a Vista VM, the graphics drivers will not install automatically. Use the following procedure to install graphics drivers on a Vista VM.

To Install Graphics Drivers on Vista:

1. Navigate to **Start > Control Panel > Classic View > Device Manager**.
2. Right-click on **Standard VGA Graphics Adapter** and select **Update Driver Software...**.
3. Select **Search automatically for updated driver software** and then **Don't search online**. This will cause the correct graphics drivers to be installed. A reboot will be required after the drivers have been installed.

> **Warning**
>
> It has been observed that sometimes the installation of the graphics drivers on Vista can end with a black screen and unresponsive device. Should this occur, wait for all hard drive activity to cease, and manually reboot your OpenXT device.

If you install ATI drivers on a Windows 7 VM, the graphics drivers will cause a blue screen on the VM. Use the following procedure to install ATI graphics drivers on a Windows 7 VM.

To Install ATI Graphics Drivers on Windows 7:

1. Hover your mouse over the VM icon and click **Details** to open the VM details window.

2. Shut down the VM.

3. Click **Hardware**.

4. Click **Edit**.

5. From the **3D Graphics** dropdown list, select **Enabled**.

6. Click **Save**.

7. Restart the VM. The VM boots and automatically installs the graphics drivers.

8. Navigate to **Start > Control Panel > Hardware and Sound** and select **Device Manager** in the **Devices and Printers** section to open the **Device Manager** dialog box.

9. Under Display Adapters, right-click on the ATI display adapter and select **Disable** from the menu.

10. Restart the VM.

11. Install the ATI drivers. This automatically enables the adapter.

12. Repeat the above steps to open the **Device Manager** dialog box and this time disable the OpenXT graphics adapter.

13. Restart the VM.

Chapter 3. VM Configuration and Lockdown Policy

➥ **Note**

Changes to a VM's policy require a reboot of the VM to take effect.

3.1. Configuring a 3D Graphics Support VM With an Nvidia or ATI GPU

To Enable 3D Graphics Support on a VM with Direct Access to the GPU Video Hardware:

1. Install all VM software updates, ensure that the OpenXT Tools are installed, and confirm working network connectivity.

2. Shutdown the VM.

3. Hover your mouse over the VM icon and click **Details** to open the VM details window.

4. Click the **Hardware** tab.

5. From the **3D Graphics Support** dropdown list, select the GPU you want to assign to the VM and click **Save**.

6. Start the VM. Do not use the automated Windows driver install functionality for the newly detected GPU.

7. If the GPU is a ATI GPU, deactivate it before installing the driver:

   a. Open Device Manager.

   b. Under Display Adaptors, identify the ATI device.

   c. Right click on the ATI device and select Disable.

   d. Reboot the VM.

8. Download and install the Windows XP Nvidia Quadro Driver 259.12 or later (Nvidia GPU) or the Catalyst driver 10.9 or later (ATI GPUs).

9. Do *not* reboot when prompted by the Nvidia or ATI driver installation.

10. Open Windows XP Device Manager.

11. Select **Display Adapters > OpenXT Xen Display Driver**.

12. Right-click on the device and select **Disable**.

13. Confirm that the device should be disabled.

14. Accept the prompt to restart the device.

15. After the VM restarts, the VM boot screen will be shown on the Intel display, but the desktop (after boot) will be shown on the Nvidia or ATI display.

3.2. Configuring Audio Device Assignment

Use the following procedure to prevent a VM from recording audio.

To Disable Audio Recording from a VM:

1. In UIVM for OpenXT select the **Details** dialog for the desired VM.

2. On the left side, select **Advanced**.

3. On the right side, under **Isolation Policies**, select **Disabled** for **Audio Recording**.

4. Click **Save**, and close the dialog.

5. If the VM is running, reboot it for the change to take effect.

➥ **Note**

> By default, there is no detection of HDMI and DP audio devices if they are present, and therefore no audio output from them.
>
> HDMI audio output will work only if the HDA audio controller PCI device controlling the HDMI connector is passed through to the VM. In case of an Nvidia/AMD adapter, there is always a different HDA device controlling the HDMI sound output on the card.
>
> A good way of using the HDMI connector would be to pass trough the Nvidia/AMD HDA PCI device to the VM. In this case we could have, for example, shared sound across all VMs provided by the standard Intel integrated HDA adapter (native speakers, headphones, mic.) and a fully passed-through HDA Nvidia/AMD adapter (HDMI connector on the discrete card) to one single VM. The HDA Nvidia/AMD adapter can be passed through to a different VM without needing to reboot the host platform.

Use the following procedure to enable VT-d passthrough of the host audio device to a single VM. This functionality can only be used for a single VM. After you enable this for one VM, you need to disable audio playback for the remaining VMs.

To Enable Audio Device Assignment to One VM:

1. Shut down the desired VM.

2. In UIVM for OpenXT open the **Details** dialog for the desired VM.

3. On the left side, select **PCI Pass Through**.

4. Select the Audio Controller from the list of devices, then click **Pass Through**.

5. Click **Save**, and close the dialog.

6. Start the VM.

7. Open Device Manager and ensure that there is no problem reported with the audio device.

3.3. Configuring Optical Disk Policies

To Disable Writing to an Optical Disk for a VM:

1. In UIVM for OpenXT select the **Details** dialog for the desired VM.

2. On the left side, select **Advanced**.

3. On the right side, under **Isolation Policies**, select **Disabled** for **CD Reading**.

4. Click **Save**, and close the dialog.

5. If the VM is running, reboot it for the change to take effect.

To Disable Write Access to an Optical Disk for a VM:

1. In UIVM for OpenXT select the **Details** dialog for the desired VM.

2. On the left side, select **Advanced**.

3. On the right side, under **Isolation Policies**, select **Disabled** for **CD Writing**.

4. Click **Save**, and close the dialog.

5.   If the VM is running, reboot it for the change to take effect.

> **Note**
>
> These settings only affect the internal CD/DVD drive. USB drives are not affected.

3.4. Using Stub Domains

A VM can be set up to use a stub domain to host its `ioemu` process. This has the advantage of the `ioemu` process being behind the single Xen scheduler without also being behind the Linux scheduler in the control domain, and also provides an additional level of security for the control domain.

> **Note**
>
> Ensure that stub domains are enabled before installing the OpenXT Tools inside the VM. Stub domains are enabled by default.

To Enable a Stub Domain for a VM:

1.   In UIVM for OpenXT select the **Details** dialog for the desired VM.

2.   On the left side, select **Advanced**.

3.   On the right side, under **Isolation Policies**, select **Enabled** for **Stub Domain**.

4.   Click **Save**, and close the dialog.

5.   If the VM is running, reboot it for the change to take effect.

> **Note**
>
> If you want to add disks to a stub domain, only device nodes `sd[a-h]` and `hd[a-h]` with the maximum number of partitions are supported.

3.5. Enabling USB Controller Assignment to One VM

To Assign a USB Controller to a Single VM:

1.   Shut down the desired VM.

2.   In UIVM for OpenXT select the **Details** dialog for the desired VM.

3.   On the left side, select **PCI Pass Through**.

4.   On the right side, click on **Pass Through PCI Device**. A dialog box appears.

5.   Select the desired USB Controller from the list of devices, then click **Pass Through**.

6.   Click **Save**, and close the dialog.

7.   Start the VM.

8.   Open Device Manager and ensure that there is no problem reported with the Universal Serial Bus controllers.

9.   Press **Ctrl+0** to switch back to UIVM for OpenXT.

10. Plug a USB device into one of the USB ports assigned to the VM.

11. Select the **Details** dialog for the VM. On the left side, select **USB Devices**. Check that the device is listed.

12. Switch back to the VM. The USB device should be present.

On some models of supported hardware, USB devices may share the same USB bus. In this case all USB devices on the specified bus will be passed through to the VM.

3.6. Networking Policy Settings

To Prevent Use of Wired Networking Inside a Specific VM:

1. In UIVM for OpenXT select the **Details** dialog for the desired VM.

2. On the left side, select **Advanced**.

3. On the right side, under **Isolation Policies**, select **Disabled** for **Wired Network Access**.

4. Click **Save**, and close the dialog.

5. If the VM is running, reboot it for the change to take effect.

To Prevent Use of Wireless Networking Inside a Specific VM:

1. In UIVM for OpenXT select the **Details** dialog for the desired VM.

2. On the left side, select **Advanced**.

3. On the right side, under **Isolation Policies**, select **Disabled** for **Wireless Network Access**.

4. Click **Save**, and close the dialog.

5. If the VM is running, reboot it for the change to take effect.

3.7. VM Property Editing Policy Settings

To Allow or Disallow Editing of VM Properties:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. To disable the ability to modify VM settings, run the command:

```
xec-vm -n <vm_name> set policy-modify-vm-settings false
```

or, to enable it:

```
xec-vm -n <vm_name> -i com.citrix.xenclient.xenmgr.vm.unrestricted set policy-modify-vm-settings \
true
```

3. Reboot the VM.

To Disable Advanced and PCI Pass Through Settings for VMs:

This procedure allows you to prevent modification of the **Advanced** and **PCI Pass Through** settings from the VM **Details** for a specific VM. You can also set this for *any* VMs on this OpenXT host; see the Procedure: "To Hide Advanced and PCI Pass Through Settings for All VMs" for details.

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. To hide **Advanced** and **PCI Pass Through** tabs on the VM **Details** dialog, run the command:

```
xec-vm -n <vm_name> set policy_modify_vm_advanced false
```

or, to enable it:

```
xec-vm -n <vm_name> -i com.citrix.xenclient.xenmgr.vm.unrestricted set policy_modify_vm_advanced \
true
```

3. Reboot the VM.

To Prevent Use of the Print Screen Key Inside a Specific VM:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the command:

```
xec-vm -n <vm_name> set policy-print-screen false
```

3. Reboot the VM.

Chapter 4. Platform Configuration

4.1. Enabling Control Domain Network Access

In OpenXT the Network Driver Virtual Machine (NDVM) provides network connectivity to other VMs. By default the control domain does not have network access.

To Enable Control Domain Network Access:

> **Note**
>
> The IP address of the wired connection as displayed in the **Connection Information** box in UIVM for OpenXT is not the IP address of the hypervisor control domain. Instead, it displays the IP address of the Network Driver Domain service VM (NDVM). If you have enabled ssh, open a terminal from the UIVM for OpenXT, log in, and run the command **ifconfig** to obtain the IP address of `eth0`. Use this IP address to ssh to the control domain.

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the following commands:

    ```
    xec set enable-ssh true
    reboot
    ```

To Disable Control Domain Network Access:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the following commands:

    ```
    xec set enable-ssh false
    reboot
    ```

4.2. VM Disk Persistence

This setting determines whether or not changes to the data on a disk remain after the VM is rebooted.

> **Note**
>
> Please ensure that you have installed the OpenXT Tools in the VM and performed all VM configuration before disabling persistence for disks.

To Disable VM Disk Persistence:

1. In UIVM for OpenXT select the **Details** dialog for the desired VM.

2. On the left side, select **Disks**.

3. On the right side, under **Persistence**, select **Disabled**.

4. Click **Save**, and close the dialog.

5. If the VM is running, reboot it for the change to take effect.

> **Note**
>
> Some Windows registry keys, specifically those related to Active Directory (AD), are maintained and not reset.

To Enable Disk Persistence:

1. In UIVM for OpenXT select the **Details** dialog for the desired VM.

2. On the left side, select **Disks**.

3. On the right side, under **Persistence**, select **Disabled**.

4. Click **Save**, and close the dialog.

5. If the VM is running, reboot it for the change to take effect.

4.2.1. Setting Read-only Mode for a Disk on the Tapdisk Level

Although VMs can opt to use read-only filesystems just using their own logic, extra security can be achieved if read-only mode is toggled on the tapdisk level, so that it is actually guarded by the Control Domain.

To turn on read-only mode for a disk:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the command:

```
xec-vm -n <vm_name> --disk <disk-num> set mode r
```

To turn on read/write mode for a disk:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the command:

```
xec-vm -n <vm_name> --disk <disk-num> set mode w
```

4.3. Enabling Mouse Switching Between VMs Pinned to Displays

If you have multiple graphics processors, OpenXT supports running two separate VMs side by side, each on its own monitor. The mouse cursor can be dragged seamlessly from one VM to the other.

The settings to control this appear on the **Settings** dialog on the **Display** page if the system has two graphics processors.
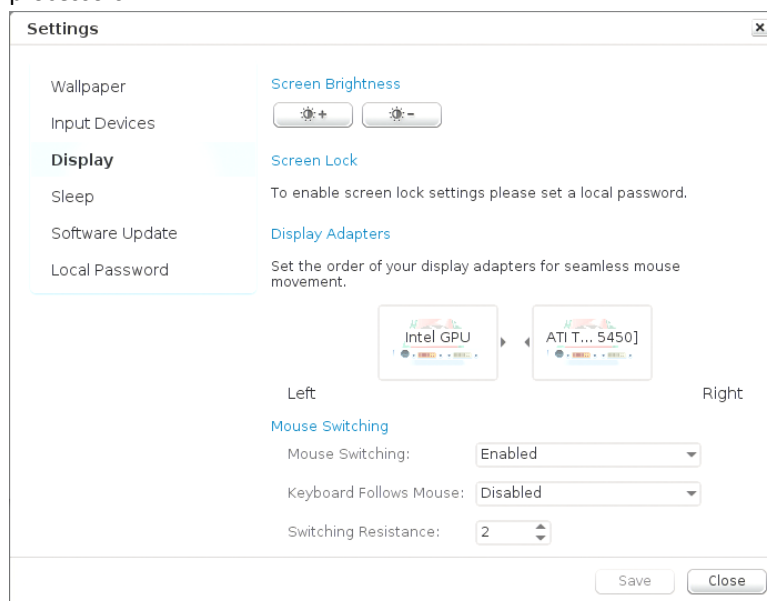
To control mouse switching between multiple VMs:

1. In UIVM for OpenXT, click **Settings** to open the dialog box, then select **Display** .

2. If necessary, under *Display Adapters*, click one of the small arrows between the monitor icons to change their order relative to which adapter is connected to which monitor (left or right).

3. Under *Mouse Switching*, **Mouse Switching** is enabled, **Keyboard Follows Mouse** is disabled, and **Switching Resistance** is set to 2 by default. Use the pull-downs to change any of these settings as desired.

4. Click **Save**, then **Close**.

4.4. Platform Lockdown Policy Settings

This section lists policy settings that be used to modify the appearance and behavior of UIVM for OpenXT on a OpenXT device.

Command	Allows / Disallows	Example
vm-creation-allowed	VM Installation	xec set vm-creation-allowed false
connect-remote-desktop-allowed	XenDesktop connection buttons	xec set connect-remote-desktop-allowed true
vm-deletion-allowed	VM deletion	xec set vm-deletion-allowed false
ota-upgrades-allowed	over-the-air upgrades	xec set ota-upgrades-allowed false
modify-settings	modifying platform settings	xec set modify-settings false
modify-services	modifying services	xec set modify-services false
modify-advanced-vm-settings	modifying advanced VM settings	xec set modify-advanced-vm-settings false

To Hide Advanced and PCI Pass Through Settings for All VMs:

This procedure allows you to prevent modification of the **Advanced** and **PCI Pass Through** settings from the VM **Details** tab for *any* VM on the host. You can also set this for individual VMs; see the Procedure: "To Disable Advanced and PCI Pass Through Settings for VMs" for details.

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. To hide the **Advanced** and **PCI Pass Through** sections from the VM **Details** tab for any VM on the host, run the command:

```
xec policy-modify-vm-advanced false
```

or, to show these sections:

```
xec policy-modify-vm-advanced true
```

3. Reboot the VM.

Chapter 5. Networking Configuration

OpenXT networking services are provided via a Network service VM called *Network*. You can view and modify this service VM via the **Services** button in UIVM for OpenXT.

5.1. Configuring Shared Networks

172.16.x.0/24 is the range of IP addresses used by OpenXT for shared networks (wired, wifi, or internal networks). Any VMs on these networks will be assigned an IP from this range. If this range clashes with your deployed network setup or if for any other reason you want to use a different address range instead of the default one, this can be modified by running the following command:

```
xec -s com.citrix.xenclient.networkdaemon -o <network-object> set nat-prefix <subnet>
```

For example if you run:

```
xec -s com.citrix.xenclient.networkdaemon -o /wired/0/shared set nat-prefix 192.168.2.0
```

shared networks will use the 192.168.2.0/24 subnet and the DHCP range will begin at 192.168.2.10.

5.2. Adding Internal Networks

By default an NDVM has a single internal network. This provides maximum isolation between internal networks. OpenXT recommends this configuration for maximum security. Use the following procedure to create more internal networks per NDVM if desired.

To add an additional internal network to an NDVM:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Assume the necessary roles and run the command:

   ```
   xec -s com.citrix.xenclient.networkdaemon create-network internal <network-id> "uuid=<ndvm-uuid>"
   ```

   The parameters are:

   network-id
   > The number identifying the internal network. The network created will be assigned the identifier `/internal/<network-id>`. This number can not be already assigned to other internal network.

   ndvm-uuid
   > UUID of the NDVM where the internal network will be created.

3. Reboot to apply the changes.

5.3. NDVM Firewall Configuration

NDVM firewalling is enabled for OpenXT. However, the filtering is supported only on bridged networks. When a VM is on a bridged network, the following commands can be used to edit the firewall rules. The default behaviour is to accept all traffic to and from the VM. Any traffic that needs to be dropped needs to be added as a rule.

To list the firewall rules, run the command:

```
xec-vm -n <vm-name> list-net-firewall-rules
```

To add a firewall rule:

```
xec-vm -n <vm-name> add-net-firewall-rule <id> <direction> <remote-ip> <iptables-options>
```

where:

- *id* is the number indicating the order in which the rules should be run

- *direction* - specifies in or out (filter for the VM's incoming/outgoing traffic)

- *remote-ip* - is the IP address of the source or destination subnet when processing the in or out filter

- *extra* - conatins any additional iptables flags

To delete a rule, run the command:

```
xec-vm -n <vm-name> delete-net-firewall-rule <id>
```

For example, to drop all the traffic from a VM named *win7*, you could run the following:

```
xec-vm -n win7 add-net-firewall-rule 1 "in" "0.0.0.0/0" ""
xec-vm -n win7 add-net-firewall-rule 2 "out" "0.0.0.0/0" ""
```

5.4. Setting Up and Configuring Multiple NDVMs

By default the NDVM called *Network* has all the network PCI devices assigned to it. You might want to be able to run additional VMs, each connected to a different isolated network. This can be enabled by running one Network Driver Domain VM (NDVM) per network.

Once a new NDVM has been added, it will appear in UIVM for OpenXT as an icon in the menu bar along the top, labeled with the NDVM's name, to the right of the default *Network* icon.

To create multiple NDVMs:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Any changes to the default NDVM's PCI rules will be reset on every system reboot. Therefore, before anything else, you need to make the NDVM settings persistent. To do so, run the following command:

    ```
    db-write /xenmgr/overwrite-ndvm-settings false
    ```

3. To create a new NDVM, run the following command:

    ```
    create-ndvm <ndvm_name>
    ```

    The NDVM that gets created will initially have no PCI devices assigned to it.

4. The network devices are assigned to VMs using PCI rules. To list the PCI rules of an NDVM, use the command:

    ```
    xec-vm -n <ndvm_name> list-pt-rules
    ```

5. Modify the NDVM pass through rules as follows:

    a. List the PCI pass through rules set on the default NDVM:

    ```
    xec-vm -n Network list-pt-rules
    ```

    This command lists the PCI rules that determines the type of PCI devices passed through to the NDVM. For example:

    ```
    {
      "id"   = 0
      "rule" = match class=0x0200
    }
    {
      "id"   = 1
      "rule" = match class=0x0280
    }
    ```

    b. List all the PCI devices passed through to the default Network VM with the command:

```
xec-vm -n Network list-pt-pci-devices
```

This returns a list of all the PCI devices that are assigned to the Network VM. For example, running this command on the default Network VM will output something like the following:

```
{
  "addr"      = 0000:00:19.0
  "class"     = 0x200
  "device-id" = 0x1502
  "name"      = Intel Corporation 82579LM Gigabit Network Connection
  "vendor-id" = 0x8086
}
{
  "addr"      = 0000:03:00.0
  "class"     = 0x280
  "device-id" = 0x85
  "name"      = Intel Corporation Centrino Advanced-N 6205
  "vendor-id" = 0x8086
}
```

c.   Next we want to create more specific rules for passing through PCI devices. To do this, first remove the class-based rule for wired networks from the default Network VM named *Network*:

```
xec-vm -n Network delete-pt-rule "0x200" "" ""
```

and then remove the class-based rule for wireless networks:

```
xec-vm -n Network delete-pt-rule "0x280" "" ""
```

> **Note**
>
> You can add a specific device to the list with the command **xec-vm -n *<ndvm_name>* add-pt-rule "*<class>*" "" ""**.

d.   To specifically assign one of these devices, create a pass through rule using the PCI BDF (Domain:Bus:Device.Function) format, specifying the listed *addr* value of the PCI device from the **list-pt-pci-devices** command above as follows:

```
xec-vm -n <ndvm_name> add-pt-rule-bdf <addr_value>
```

> **Note**
>
> By default, the Network VM has all network devices assigned to it using PCI *class* rules. The class-based rules are sufficient for most machines that have just one device of each class (for example, most laptops). But for machines that have more than one device of a specific class, PCI BDF (Domain:Bus:Device.Function) rules are used to assign and remove them.

> **Note**
>
> You can remove a specific device from the list with the command **xec-vm -n *<ndvm_name>* delete-pt-rule-bdf *<addr_value>***.

e.   To verify the changes you made, run the following command to list the rules:

```
xec-vm -n <ndvm_name> list-pt-rules
```

6.   Reboot the OpenXT device.

> **Note**
>
> The control domain always uses the */wired/0/bridged* network when there is a wired connection. This can be overwritten by running the command:
>
> ```
> db-write /networkdaemon/dom0/network <network-id>
> ```

Reboot the system for the control domain to start using the new network.

To Change a Network Name:

To change the network label, set the `label` property of the network object. This is the label used in the

Networks tab of a VM in UIVM for OpenXT.

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.
2. Run the following command:

```
xec -s com.citrix.xenclient.networkdaemon -o <network-object> set label <network-label>
```

For example:

```
xec -s com.citrix.xenclient.networkdaemon -o /wired/0/bridged set label <lab_network>
```

> **Note**
>
> Bridged and shared networks using the same physical interface (only possible with wired networks) use the same label. So in the above example `/wired/0/bridged` and `wired/0/shared/` will be identified by the label **lab_network**.

5.5. Transparent Bridging

By default, when a OpenXT device is connected to a wired network, the Network VM requests an IP address on the network. If a VM is configured to use shared networking, the NDVM uses this IP address as the source address when performing NAT (Network Address Translation) on outgoing connections from the VM.

If no VMs are configured to use shared networking, the NDVM can instead be set up as a transparent bridge. In this mode, the NDVM does not request an IP address on the wired network, but still provides VMs that use bridged networking with full access to the wired network.

When multiple NDVMs are in use, this mode can be configured separately for each Network VM.

> **Note**
>
> When transparent bridging is enabled, UIVM for OpenXT will display the network icon for the Network VM as disconnected, and the options to configure the network interfaces will be disabled.

To enable transparent bridging for a Network VM:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.
2. Enter the command:

```
newrole -r sysadm_r
```

and provide the password.

3. Enter the command:

```
xec-vm -n <ndvm_name> set-domstore-key transparent-bridging true
```

4. Reboot the OpenXT device.

To disable transparent bridging for a Network VM:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Enter the command:

```
newrole -r sysadm_r
```

and provide the password.

3. Enter the command:

```
xec-vm -n <ndvm_name> set-domstore-key transparent-bridging false
```

4. Reboot the OpenXT device.

5.6. V4V Firewall Configuration

V4V firewall rules are specified as part of a VM's configuration. This is accomplished using the **add-v4v-firewall-rule** command from the command line console on the OpenXT device:

```
xec-vm -n <vm_name> add-v4v-firewall-rule <rule>
```

Firewall rules are instantiated when the VM is started and removed when it is shut down.

OpenXT recommends to not use the Linux **viptables** command directly except for debugging purposes.

5.7. Support for 802.1x Authentication in VMs (experimental)

Normal packet flow with 802.1x packets disappear in the Network Driver Domain VM (NDVM). This is due to the default behavior of the Linux bridging code, which drops packets from the MAC group which contain 802.1x.

OpenXT includes a simple Linux kernel patch that allows for selective control of this behavior on a per-bridge basis.

➥ **Note**

> Currently this capability is experimental only.

This capability is disabled by default. You can verify this for a bridge by reading the state of the `break_8021d` file as follows:

```
cat /sys/devices/virtual/net/brbridged/bridge/break_8021d
```

The output of the command will be `0` if 802.1x guest authentication is disabled, `1` if it is enabled.

➥ **Note**

> As always, you must be in the `sysadm_r role` to effect these sorts of changes. You must also be in the NDVM, as that's where the bridge for wired network traffic resides. Therefore, since your ssh session will begin in the control domain, you'll need to be in the `sysadm_r` role in both the control domain and the NDVM before you can change the relevant settings.

To enable 802.1x authentication in a user VM:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the command:

```
newrole -r sysadm_r
```

and provide the password.

3. SSH to the NDVM:

```
sshv4v network
```

4. Again, enter the command:

```
newrole -r sysadm_r
```

and provide the password.

5. Enable 802.1x authentication with the following command:

```
echo 1 > /sys/devices/virtual/net/brbridged/brige/break_8021d
```

To disable 802.1x authentication in a user VM:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Enter the command:

```
newrole -r sysadm_r
```

and provide the password.

3. SSH to the NDVM:

```
sshv4v network
```

4. Again, enter the command:

```
newrole -r sysadm_r
```

and provide the password.

5. Run the follow command to disable 802.1x authentication:

```
echo 0 > /sys/devices/virtual/net/brbridged/brige/break_8021d
```

Chapter 6. Other Administrative Tasks

6.1. Password Handling

To change the root user password for OpenXT, open a command prompt (**Ctrl+Shift+t**), and run the following commands:

```
echo -n "<OLD_PASSWORD>" > /tmp/oldpass
echo -n "<NEW_PASSWORD>" > /tmp/newpass
sec-change-root-credentials /tmp/newpass /tmp/oldpass
```

Changes made to the configuration partition cause the system to prompt for the passphrase set in the TPM setup process. Run the following command to change this passphrase if required:

```
openssl rsa -des3 -in /boot/system/install/data/recovery-private-key.conf \
-passin stdin -out /boot/system/install/data/recovery-private-key.conf \
-passout stdin
```

Enter the old passphrase and press **Enter**. Then enter the new passphrase and press **Enter**. The following output is written to the console:

```
writing RSA key
```

Chapter 7. Troubleshooting

7.1. General Troubleshooting

If you experience a technical issue with OpenXT, please immediately generate a system status report to capture essential information from the system that will enable diagnosis. The status report can be supplied to a technical support representative. You may also want to visit the OpenXT Forums here[*] for solutions.

To Open a Control Domain Console:

- In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window. Alternately press **Ctrl + Shift + H** to open a larger control domain terminal window.

    > **Note**
    >
    > Use **Alt + Tab** to bring the console back into focus should it end up behind UIVM for OpenXT.

To Generate a OpenXT Status Report:

> **Important**
>
> VMs must be running for the status report to be able to gather important VM-specific diagnostic information.

1. SELinux must be temporarily disabled in the control domain to generate a status report. To disable it:

    a. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

    b. Enter the commands

    ```
    nr
    setenforce 0
    ```

2. In UIVM for OpenXT, click **Info > Status Report**, then click the **Create Status Report** button. Alternately, press **Ctrl + Alt + R**. The **Create Status Report** wizard is displayed.

3. Select what information you would like to include in the status report. Screenshots and diagnostic information about the VMs running on the OpenXT device can be extremely helpful with the diagnosis of technical issues, but you may prefer not to divulge this information. If you do not want to include screenshots of VMs in the status report, uncheck the **Include screenshots of the VMs in this report checkbox**. If you do not want any other diagnostic information about your VMs to be included, uncheck the **Include other diagnostic information from the VMs in this report** checkbox.

4. Click the **Next** button.

5. Enter a short (8 words or less if possible) summary of the problem you have encountered in the **Summary** text box.

6. Enter a more detailed description of the problem in the **Description** text area.

7. Click the **Next** button.

8. Enter the steps that you think are required to reproduce the problem in the **Steps to Reproduce** text area.

9.

10. Click the **Next** button.

---

[*]

11. Click the **Next** button again to start generating the report. The report is saved as a `.tar.gz` file on the control domain file system in the `/storage/status-report` directory. The file is named after the summary of the issue.

    Because the status report might contain sensitive information, no direct download link is provided. It is instead required to log in to a control domain console as the `root` user in order to access the status report. Contact your system administrator if you do not access to the `root` user password to arrange for the status report to be retrieved. To retrieve the status report, either use **SCP**, **WinSCP**, or an equivalent tool.

12. Re-enable SELinux as follows:

    a. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

    b. Enter the commands:

    ```
    nr
    setenforce 1
    ```

7.1.1. Recovering From a Full Disk

1. Reboot the OpenXT host.

2. While the OpenXT boot screen is displayed, press **Esc**.

3. Select **OpenXT Technical Support option: console access**.

4. When a console is available, you will be prompted to enter the administrative password, which is the password you created when you installed OpenXT.

5. Delete the file `/storage/xc-reserved`:

    ```
    rm /storage/xc-reserved
    ```

    This will free up sufficient disk space to allow you to boot into OpenXT and back up your VMs.

7.1.2. Moving a Hard Disk from One OpenXT System to Another

When you move a hard disk from one OpenXT system to another, you need to "bless" the disk. This is a security feature to keep the data secure in case of theft.

1. After putting the drive in the OpenXT device, start it up.

2. While the OpenXT boot screen is displayed, press **Esc**.

3. Select **OpenXT Technical Support option: console access**.

4. When a console is available, you will be prompted to enter the administrative password, which is the password you created when you installed OpenXT.

5. You will then be asked, "Would you like to reseal the device with the current configuration?" Answer yes, then you can reboot the device and use your VMs.

7.1.3. Optical Drive Assignment When UIVM for OpenXT Is In Focus

When UIVM for OpenXT is in focus, and a CD/DVD is inserted in the optical drive, it is assigned to the VM that gets focus first upon switching. The optical drive is then not available from other VMs unless you release it from the VM it was assigned to.

7.1.4. To Turn On ATAPI Logging to Debug CD/DVD Issues

1. Open a console from UIVM for OpenXT.

2. Run the command:

```
touch /etc/debugcdrom
```

3. Logs will be written to `/var/log/cdrom-<VM_slot_number>.log` until the `/etc/debugcdrom` file is removed.

7.1.5. To Boot Into a Control Domain Console

1. Reboot the OpenXT host.

2. While the OpenXT boot screen is displayed, press and hold **Shift**.

3. Boot into the **console access** option.

4. When a console is available, log in as `root`.

7.1.6. To Refresh UIVM for OpenXT

• In UIVM for OpenXT, press **Ctrl + Q**.

7.1.7. To Change the Control Domain Root Password

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Create a text file containing your old password.

3. Create a text file containing your new password.

4. Run the following command:

```
sec-change-root-credentials <new_password_file_path> \
<old_password_file_path>
```

Both files will be securely deleted when you run the **sec-change-root-credentials** command.

7.1.8. To Troubleshoot Ubuntu Driver Issues

Ubuntu in OpenXT uses paravirtualized drivers to increase performance by eliminating CPU cycles previously used to emulate devices. Should you experience problems, you can try reverting to the emulated drivers using this procedure:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the command:

```
xec-vm -n <vm_name> set viridian true
```

3. Reboot your Ubuntu VM.

7.1.9. WiFi Connections and Ubuntu VMs

In Ubuntu VMs, WiFi connections appear as wired connections. The connection shows a NAT'd IP address in the VM because host WiFi is always shared (that is, NAT'd), rather than bridged, due to the nature of WiFi networks.

7.1.10. Masking SSEs in the VM CPUID

Some PXE servers require that some Streaming SIMD Extensions (SSEs) are masked in the CPUID of a VM. To do this:

1. In UIVM for OpenXT, press **Ctrl + Shift + T** to open a control domain terminal window.

2. Run the following command to disable SSE, SSE 4.2, SSE 4.1, SSE 3 and SSE2:

```
xec-vm -n <vm_name> set cpuid \
1:ecx=xxxxxxxxxxx00xxxxxxxxx0xxxxxxxx0,edx=xxxxx00xxxxxxxxxxxxxxxxxxxxxxxxxx
```

In this command, `0` causes the corresponding bit to be unset and `x` sets the corresponding bit to a safe default.

To reset the CPUID back to default at a later stage, run the command:

```
xec-vm -n <vm_name> set cpuid ""
```

7.1.11. To Return to UIVM for OpenXT from an Unresponsive VM (Force Switching)

Use this procedure to return to UIVM for OpenXT if a VM with 3D Graphics Support enabled becomes unresponsive to attempts to switch away from it.

> **Warning**
>
> Forcing a switch should only be attempted as a last resort. Particularly, forcing a switch while a 3D Graphics Support VM is booting or shutting down can lead to the VM graphics becoming corrupt. OpenXT highly recommends immediately shutting down any VM you have force switched away from and restarting it.

1. Press and hold **Ctrl + 0** for 15 seconds.

2. If UIVM for OpenXT is still not displayed, press **Ctrl + 0** once again to switch to UIVM for OpenXT.

7.1.12. To Determine the IP Address of a OpenXT Device

1. In UIVM for OpenXT click on the Network Manager icon at the top-right of the screen, and select **Connection Information** from the popup menu.

2. The details of all active network connections are displayed, including the IP address.

> **Note**
>
> The IP address of the wired connection as displayed in the **Connection Information** box in UIVM is not the IP address of the hypervisor control domain. Instead, it displays the IP address of the Network Driver Domain service VM (NDVM). If you have enabled ssh, open a terminal from the UIVM, log in, and run the command **ifconfig** to obtain the IP address of `eth0`. Use this IP address to ssh to the control domain.

7.1.13. To Clear the Trusted Platform Module (TPM) firmware

Refer to the BIOS section of your PC manual for instructions on clearing the TPM.

7.2. Installation Troubleshooting

This section describes some troubleshooting tips to use during OpenXT installation.

While running the OpenXT installer you can switch what you see using the following key strokes:

Alt + F1
   Switch back to the installer.

Alt + F2
   Show the installation log file.

Alt + F3, **Alt + F5** or **Alt + F6**.

Show a login prompt to a console window. Log in as `root`.

> **Note**
>
> To use this functionality external SSH access must be enabled. To enable SSH, run the following command in a terminal window in UIVM for OpenXT: **xec -x enable-ssh true**.

Alt + F4

Show the system log file.

Alt + F7

Enter the interactive status-report generation tool.

7.2.1. To Generate an Installation Status Report

1. During installation, press **Alt + F7** and select **Continue**.

2. Enter a description of the issues you are experiencing with the installation and select **OK**. The system will start to generate a status report.

3. When report generation is complete, the status report filename is displayed. Select **Web Server**.

4. The URL of a web server is displayed. Point your web browser to the address displayed to download the installation status report.

7.2.2. To Troubleshoot PXE Installation Issues

*   OpenXT uses a customized `pxelinux.0` file, which can be found on the installer CD at `/isolinux/pxelinux.0`. This file must be copied to your PXE server.

How OpenXT Allocates Resources to VMs

Given that multiple VMs are using the same hardware, OpenXT must manage this interaction. This appendix describes how OpenXT handles shared hardware resources.

1. CPU

OpenXT provides virtual CPUs (vCPUs) to the VMs running on it. OpenXT automatically shares the computing load over the physical CPUs present on the OpenXT device.

In general, VMs running more intense workloads (for example, anything multi-threaded or running in separate processes) should be be assigned more vCPUs.

While it is possible to allocate more vCPUs to a VM than the number of physical CPUs on the OpenXT hosting them, there is no advantage gained from doing so.

2. RAM

You can allocate available RAM to individual VMs. When a VM is started the specified RAM is hard-allocated to it. On shutting down the VM, the memory is freed and made available for other VMs to use. A certain amount of RAM is required for OpenXT operation, so not all installed device RAM is available to be allocated to VMs.

3. GPU

The physical GPU can optionally be directly allocated to a single VM. This is part of the 3D Graphics Support experience, providing excellent graphics performance to your favored VM.

4. Network and Internet Connections

OpenXT networking is handled on two levels: host-wide connectivity, and the connectivity of each individual VM. A wired or wireless connection is configured using Network Manager in UIVM for OpenXT for the OpenXT host. Each VM can then be configured individually to control the level of access to the network or networks that the host is connected to. All network traffic is routed through a single network interface at any given time. By default Network Manager sets up wired networking so that an address will be obtained by DHCP, if possible.

5. USB Devices

USB devices are handled differently according to their type. Human Interface Devices (HID) (for example, the mouse and keyboard) are directly connected to the OpenXT platform and exposed in a secure manner to the VM that is currently in active use. Other USB devices, for example external disk drives and CD drives, would potentially suffer from contention issues if more than one VM attempts to write to them simultaneously. Because of this, OpenXT attaches such devices to the VM that is being used when they are plugged in to the computer. You can also use UIVM for OpenXT to assign a plugged-in USB device to a different VM.

➡ **Important**

- OpenXT recommends that you take care to eject USB devices as the operating system expects before assigning them to another VM. Not doing this causes OpenXT to force-eject the USB device, which can lead to loss of data.

- OpenXT highly recommends not updating the firmware or software of any device attached to a OpenXT device over USB. Such updates have been known to fail and may render the device unusable.

Note

- Plugging a non-HID USB device into your OpenXT computer while switched to UIVM for OpenXT causes the USB device to be mounted in the hypervisor control domain by default. You can then assign the device to a VM using UIVM for OpenXT.

5.1. External Optical Media Drives

To enable the use of external USB optical media drives to install VMs using installation disks, external USB optical media devices behave differently from other USB devices. See the following table for information about how they behave. Examples of this type of device include:

- USB CD drive

- USB DVD drive

The following table describes how this type of USB device interacts with OpenXT.

Action	Behavior
Plug in and turn on your OpenXT device	Device is not assigned to anything
Plug in when UIVM for OpenXT is on the screen	Device is assigned to the control domain, and can be used to install VMs **Warning** Because OpenXT mounts the external media drive as if it were internal hardware, unplugging the device while a VM that is using it is running can cause unpredictable VM behavior. OpenXT recommends avoiding this.
Plug in when a VM is on the screen	Device is assigned to the VM on screen
Plug in when previously assigned to a VM, without the **Always** checkbox checked in UIVM for OpenXT	Device is assigned as per one of the previous 2 actions
Plug in when previously assigned to a VM, with the **Always** checkbox checked in UIVM for OpenXT	The device is assigned to the VM it was previously assigned to if it is running, or when it is booted

5.2. USB Keyboards and Pointing Devices

When such a device is plugged in it can be used to control any virtual machine. For examples, keystrokes from a USB keyboard are directed to whichever VM is currently being displayed. A pointing device (for example, a mouse or trackpad) can alternately be assigned to a particular VM if desired, for example, to take advantage of pointing device functionality that is not passed through by OpenXT. Doing this might take a short while to take effect if the VM that the device is assigned to does not yet have the required drivers to use the device. If you do assign a pointing device to a particular VM it will be made available to other VMs when the VM it is assigned to is shut down.
USB 3.0 pointing devices (mouse and keyboard) have been tested and found to work with OpenXT. In addition to this most USB storage devices should work when attached to a USB 3.0 port. There is limited support for other devices. In particular, isochronous devices such as USB webcams are known not to work.

Note

- If you assign a pointing device to a particular VM, it will not be available for use in UIVM for OpenXT or any other VMs.
- USB devices are released from a VM when the VM enters the sleep state.

5.3. Other USB Devices

The following table describes how this type of USB device interacts with OpenXT.

Action	Behavior
Plug in and turn on your OpenXT device or plug in when UIVM for OpenXT is on the screen	Device can be assigned to a VM
Plug in when a VM is on the screen	Device is assigned to the VM on screen
Plug in when previously assigned to a VM, without the **Always** checkbox checked in UIVM for OpenXT	Device is assigned as per one of the previous 2 actions
Plug in when previously assigned to a VM, with the **Always** checkbox checked in UIVM for OpenXT	The device is assigned to the VM it was previously assigned to if it is running, or when it is booted

5.4. Composite USB Devices

Composite USB devices expose interfaces to more than one USB device function. An example of this sort of composite device is a USB webcam with an integrated microphone.

5.5. Internal USB Devices

Some built-in hardware devices present themselves to OpenXT as USB devices. Examples of this type of USB device include built-in bluetooth receivers and fingerprint readers. As this type of USB device is rarely unplugged (which in most cases would require physically altering the device), the following behavior occurs:

Action	Behavior
On OpenXT boot, when previously assigned to a VM, without the **Always** checkbox checked in UIVM for OpenXT	Device is unassigned
On OpenXT boot, when previously assigned to a VM, with the **Always** checkbox checked in UIVM for OpenXT	The device is assigned to the VM it was previously assigned to if it is running, or when it is booted

6. Optical Media Sharing

Optical media drives are not shared between VMs. When a disk is inserted, it is accessible from the VM that is in focus at the time. Other VMs are not able to access the disk contents and appear to have an empty optical media drive. To use the disk with a different VM, eject it, switch to the intended VM, and insert the disk.

When UIVM for OpenXT is in focus, and a disk is inserted into the optical drive, it gets assigned to the VM that gets focus first on switching. The optical drive is then not available from other VMs until the time it is released from the VM it was assigned to.

7. Hard Drive Disk Sharing

OpenXT uses a thin-provisioning strategy for VM virtual disks. This means that disk space is only taken up when the virtual disk is written to. It is therefore possible to assign more virtual disk space to VMs than is physically available, and equally possible to fill the entire hard drive should you take this approach. Please exercise caution not to end up in a position where a VM attempts to write to a full disk, as this can cause catastrophic OpenXT failure.

To recover from the situation where you have filled the OpenXT disk, follow Section 7.1.1: "Recovering From a Full Disk".

8. Manufacturer-Specific Device Features

Supported OpenXT devices often come with manufacturer-specific features, such as fingerprint readers, screen brightness control buttons, sound volume control buttons and so on. Some of these devices require software from the manufacturer to be installed in order to get them working correctly. Additionally, most of these features have not been designed for use with multiple VMs running on a device. For example, a sound volume level control button could conceivably increase the volume of all running VMs, or instead just increase the volume of the VM currently in focus, or alternately manipulate the sound volume of all running VMs to be the same as the new value for VM currently in focus. Conversely, when a user manipulates the volume of a VM from within the VM, the question arises whether this should affect the volume of the device as a whole and all the VMs currently running. As this example shows, even simple buttons to increase and decrease volume behave in very complicated fashion when multiple VMs are involved. Many manufacturer-specific devices are simply not designed to function on more than one VM.
OpenXT provides the following features and guidance for using manufacturer-specific features:

- If a 3D Graphics Support VM is running, features are likely to work best when used when the 3D Graphics Support VM is in focus.

- For best results when running an 3D Graphics Support VM, pass through the manufacturer's hardware and hardware information to the 3D Graphics Support VM.

- Some features will only work if passed through directly to a single VM. To do this, in the **Advanced** tab of the VM's **Details** window, set **Expose Physical OEM Hardware** to **Enabled**. This will cause the feature to only work with that VM.

- Some features require software to be installed which can only be installed if the manufacturer's hardware and hardware information if passed through directly to a single VM. To do this, in the **Advanced** tab of the VM's **Details** window, set **Expose Physical OEM Hardware** to **Enabled** and **Expose Physical Hardware Information** to **Enabled**. This will cause the feature to only work with that VM.

9. External Monitors and Docking Stations

OpenXT supports attaching external monitors to mirror the laptop display. When hotplugging a monitor when a 3D Graphics Support VM is running, always switch to the 3D Graphics Support VM first before attaching the monitor. The same applies when docking a OpenXT device to a docking station. This ensures that optimal native resolutions are chosen for all screens.

Installing OpenXT Over a Network Using PXE

This appendix describes how to set up PXE boot and enable the installation of OpenXT over a network.

OpenXT uses a customized `pxelinux.0` file, which can be found on the installer CD at `/isolinux/pxelinux.0`. This file must be copied to your PXE server.

The first step is to copy the `packages.main` directory from the OpenXT installer CD to a location on an FTP or HTTP server. The location URL of the parent directory of the `packages.main` directory is specified in the answerfile created in the next step.

The second step is to create an answerfile and put it in the same directory as the `packages.main` folder. The answerfile specifies the answers to questions asked by the UIVM for OpenXT installer, and the location of the required packages.

➡️ **Note**

> Please ensure that your networking configuration is set up to enable PXE boot. For example, if you are using DHCP please ensure that your DHCP server is configured to provide the route to your TFTP server.

The following is an example answerfile:

```
<interactive>false</interactive>
<mode>fresh</mode>
<source type="url">http://192.168.1.1/xenclient_packages_dir</source>
<primary-disk>sda</primary-disk>
<network-interface mode="dhcp"></network-interface>
<password>3oUQYK4w4dCB.</password>
<enable-ssh>true</enable-ssh>
<license-key></license-key>
```

Next, copy the contents of the `isolinux` directory into the PXE directory on your TFTP server, for example, `/tftpboot/pxe`. Then edit the file `isolinux.cfg`, which is an example config file used by the PXELINUX program (http://www.syslinux.org/wiki/index.php/PXELINUX). You can use this as a working example to build a config appropriate for your network. For simple configurations you should only need to edit the file to specify the location of your answerfile. For example, if you placed your answerfile on a web server, you could provide the HTTP URL as follows:

```
answerfile=http://mywebserver.com/answers.ans
```

Save the edited the `isolinux.cfg` file to the default config location for PXELINUX, which is `pxelinux.cfg/default` relative to the root of the PXE directory on your TFTP server, for example, `/tftpboot/pxe/pxelinux.cfg/default`.

➡️ **Note**

> The manner in which `PXELINUX` selects which `pxelinux.cfg` to use when a machine boots on the network is determined by a number of factors. The provided file simply places the configuration in the default location where it will be used by all machines served by DHCP on the network when they network boot.

The following table describes the allowable syntax of a OpenXT answerfile.

➡️ **Warning**

> The answerfile uses a pseudo-XML syntax and is not parsed by an XML parser. With the exceptions of the `preinstall`, `postinstall` and `quick-option` tags which may span multiple lines, all tags should be on one line only with no extraneous whitespace.

The backslash (\) characters used in examples to indicate the continuation of a line must be removed in the actual configuration file.

Tag name	Description	Required?

interactive	Determines whether the installer will interact with the user or not. If `false` the answerfile must contain all mandatory tags or the installation will fail. If `true` the user will be prompted to provide information where answerfile entries do not exist.
	
	```<interactive>true</interactive>```
	
	```<interactive>false</interactive>```
		no

quick-option	Used as a parent for other answerfile tags. If this tag is in the answerfile, the user will be prompted to choose whether they want to perform a quick install or an advanced install. If the user selects to do a quick install, the answerfile tags that are children of this tag, that is, between `<quick-option>` and `</quick-option>`, are used, as well as all the other tags in the answerfile. If the user chooses the advanced install, this tag is ignored and the options specified elsewhere in the answerfile are used.
	
	```<quick-option>```
	```# other answerfile tags go here```
	```# for quick install```
	```</quick-option>```
		no

eula	Set the `accept` parameter of the `eula` element to `yes` to automatically accept the OpenXT end-user license agreement (EULA). Set the parameter to `defer` to cause the user to be prompted to accept the EULA when first booting the OpenXT device. ```<eula accept="defer">```	no

Tag name	Description	Required?
source	The installation package source. The URL option can specify either `http` or `ftp`. The `local` option is for optical media installs. The `verify="true"` attribute determines whether or not the media should be verified before performing the installation. If you specify the `type="harddisk"` attribute, the installer `initrd` must be repacked to include a copy of the `packages.main` repository at the root of the filesystem. A copy of this repository can be found on the installation ISO. This option enables PXE-only network installation in situations where network installation using the other options is not feasible. If you specify the `type="bootmedia"` attribute, the installer will attempt to install from a bootable partition. To prepare a bootable partition, boot from the OpenXT installation media, then press **Alt + F3** to open a console window. In the console, log in as `root` and run the `prepare-hd-install` script to copy the installer and the repository from the CD-ROM to the partition. Specify the `oem="true"` attribute if you want the installer to treat the prepared partition as an OEM partition when partitioning the disk. ``` <source type="url"> \ http://127.0.0.1/foo/bar</source> <source type="bootmedia"></source> <source type="local" verify="true"> \ </source> <source type="harddisk" oem="true"> \ </source> ```	no
mode	Required for automated installation. Indicates whether to perform a destructive `fresh` installation in which all data on the primary drive will be destroyed, or to `upgrade` an existing installation. ``` <mode>fresh</mode> <mode>upgrade</mode> ```	yes
primary-disk	Required for automated installation if more than one disk is detected on the machine. Specify the UNIX disk name. ``` <primary-disk>sda</primary-disk> ```	sometimes

Tag name	Description	Required?

partition-mode	Determines what changes are made to the partition layout of the primary disk when performing a fresh installation.
	
	The `overwrite` option will overwrite an existing installation. All other partitions on the disk will be preserved. This option is only available if there is an existing installation on the disk.
	
	The `use-free-space` option will install into the available free space on the disk. All existing partitions on the disk will be preserved. This option is only available if free space exists on the disk, a new primary partition can be created and there is no existing installation on the disk.
	
	The `erase-non-oem` option will preserve any OEM partitions, erasing all other partitions on the disk and installing into the available space. (At present only Dell Utility Partitions are detected as OEM partitions.)
	
	The `erase-entire-disk` option will erase all partitions on the disk and install into the free space. All existing partitions will be erased.
	
	If no option is specified for an automated installation, the installer will attempt to use the following options in order:
	
	1. overwrite
	2. use-free-space
	3. erase-non-oem
	4. erase-entire-disk
	
	<pre><partition-mode>overwrite \
	</partition-mode>
	<partition-mode>use-free-space \
	</partition-mode>
	<partition-mode>erase-non-oem \
	</partition-mode>
	<partition-mode>erase-entire-disk \
	</partition-mode>
	<partition-mode></partition-mode></pre>
		yes

install-mbr	Determines whether a new master boot record is installed on the target disk. The `auto` option will install a new master boot record unless an OEM master boot record is found on the target disk. Only Dell master boot records are detected. Defaults to `auto` if no option is specified.
	
	<pre><install-mbr>true</install-mbr>
	<install-mbr>false</install-mbr>
	<install-mbr>auto</install-mbr>
	<install-mbr><install-mbr></pre>
		no

Tag name	Description	Required?
network-interface	Specifies the network device for use by the installer. Required for automated installs performed over the network. ``` <network-interface mode="dhcp"> \ </network-interface> <network-interface mode="static" \ address="10.0.0.1" \ netmask="255.255.255.0" \ gateway="10.0.0.2" dns="10.0.0.3"> \ </network-interface> ```	sometimes
language	Used to set the user interface language. The following languages are supported: • en-us (English) • fr-fr (French) • de-de (German) • ja-jp (Japanese) • zh-cn (Simplified Chinese) • es-es (Spanish) *Example:* ``` <language>fr-fr</language> ``` Specify the `defer` option to cause the user to be prompted to set the language on first boot. ``` <language defer="true"></language> ``` If the language element is not included in the answer file, the language defaults to en-us (US English).	no

Tag name	Description	Required?

keyboard	Used to set the keyboard layout. The following keyboard layouts are supported:
	
	• cn (China)
	• fr (France)
	• de (Germany)
	• it (Italy)
	• jp (Japan)
	• es (Spain)
	• ch (Switzerland)
	• gb (United Kingdom)
	• us (United States)
	
	Example:
	
	`<keyboard>us</keyboard>`
	
	Specify the `defer` option to cause the user to be prompted to set the keyboard layout on first boot.
	
	`<keyboard defer="true"></keyboard>`
	
	If the keyboard element is not included in the answer file, the keyboard layout defaults to us (United States).
		no

password	Used to set the system password. The value is assumed to be an encrypted password.
	
	The following command can be used to generate an encrypted password:
	
	`$ openssl passwd -1`
	
	Setting an empty password permits access without entering a password.
	
	Specify the `defer` option to cause the user to be prompted to set the password on first boot.
	
	`<password></password>`
	`<password>3oUQYK4w4dCB.</password>`
	`<password defer="true"></password>`
		no

Tag name	Description	Required?

recovery-public-key	Specifies a public/private key pair that enables the user to recover a forgotten password for an encrypted virtual disk.
	
	``
	<recovery-public-key> \
	-----BEGIN PUBLIC KEY-----
	.
	.
	-----END PUBLIC KEY----- \
	</recovery-public-key>
	
	<recovery-private-key> \
	-----BEGIN RSA PRIVATE KEY-----
	.
	.
	-----END RSA PRIVATE KEY----- \
	</recovery-private-key>
	``
	
	The following commands can be used to generate a public/private key pair with a passphrase:
	
	``
	$ openssl genrsa -des3 -out private_key 2048
	$ openssl rsa -pubout -in private_key -out public_key
	``
		no

enable-ssh	Used to enable or disable the control domain **ssh** server, which allows external ssh access for diagnostic purposes. ``` <enable-ssh>true</enable-ssh> <enable-ssh>false</enable-ssh> ```	no

Tag name	Description	Required?

vhds	Installs a precreated virtual hard disk on to the system.
	
	Each `vhd` block specifies a virtual hard disk to be installed. (At present only one virtual hard disk can be specified.) A new UUID (universally unique identifier) will be assigned to the virtual hard disk on installation.
	
	The `label` option specifies a unique label for the virtual hard disk which can be referenced in the `vms` element. This label is only used during the installation process.
	
	The `vhd-source` tag specifies the source of the virtual hard disk image. Valid prefixes include:
	
	• `http://`
	
	• `ftp://`
	
	• `file://`
	
	• `dev://`
	
	Note that the image will be retrieved after partitioning the target disk, so if the `dev://` prefix is used, it must not refer to a partition which is erased during the installation process.
	
	If the `vhd-source` tag is specified multiple times, it is assumed that the image has been split into fragments (for example, to work around a file size limit on the source filesystem) which must be concatenated to recover the original image.
	
	The `compress` option indicates that the image has been compressed. Valid values are `gzip` and `bzip2`. If the image has also been split, it is assumed that the image was split after compression.
	
	<pre>\<vhds>
	  \<vhd label="vhd1" compress="gzip">
	    \<vhd-sources>
	      \<vhd-source> \\
	  dev://sda1/my.vhd.part1 \\
	  \</vhd-source>
	      \<vhd-source> \\
	  dev://sda1/my.vhd.part2 \\
	  \</vhd-source>
	    \</vhd-sources>
	  \</vhd>
	\</vhds></pre>
		no

Tag name	Description	Required?
vms	Installs a precreated virtual machine on to the system.	no
	Each `vm` element specifies a virtual machine to be installed. (At present only one virtual machine can be specified.) A new UUID is assigned to the virtual machine on installation.	
	The `vm-source` tag specifies the source of the configuration file for the virtual machine. Valid prefixes include:	
	• `http://` • `ftp://` • `file://` • `dev://`	
	⟼ **Warning**	
	The file is retrieved after partitioning the target disk, so if the `dev://` prefix is used, it must not refer to a partition which is erased during the installation process.	
	The configuration file will automatically be updated to reflect the virtual machine's new UUID.	
	The optional `vm-vhds` block allows the configuration file to be updated to reflect the new UUIDs of any virtual hard disks used by the virtual machine. Each `vm-vhd` tag specifies the index of the disk as listed within the configuration file and the label of the disk as specified in the `vhd` block.	

	<pre><vms>
	  <vm>
	    <vm-source>http://my.url/my-vm.db \
	 </vm-source>
	    <vm-vhds>
	      <vm-vhd index="0" label="vhd1"> \
	      </vm-vhd>
	    <vm-vhds>
	  </vm>
	</vms></pre>	

skipready	If this tag is present, the **Are you ready to install?** screen is not displayed. `<skipready></skipready>`	no
preinstall	Used to supply a script to be executed prior to installation.	no
	⟼ **Warning**	
	Including answerfile tags in the pre-install script can cause the answerfile parser to produce unpredictable results.	

	<pre><preinstall>#!/bin/bash
	touch /tmp/i.was.here
	</preinstall></pre>	

Tag name	Description	Required?
postinstall	A post install script, executed at the end of a successful installation. ``` <postinstall>#!/bin/ash -e mkdir -p /mnt/storage mount /dev/xenclient/storage /mnt/storage mkdir -p /mnt/storage/hello-from-postinstall cd /mnt/storage/hello-from-postinstall ls -l .. >postinstall-sample cd / umount /mnt/storage </postinstall> ```	no
measure-launch	Configure OpenXT Measured Launch. The default is to not configure Measured Launch during anything other than an advanced interactive install. Providing the value `true` in this tag will cause installer to configure Measured Launch by default. If this value is set to `false` during an interactive install the user will not be given the option to configure Measured Launch.	no

Licenses

1. Intel Graphics and Sound Drivers

1.1. INTEL SOFTWARE LICENSE AGREEMENT (OEM / IHV / ISV Distribution & Single User)

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING. Do not use or load this software and any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

Please Also Note:

• If you are an Original Equipment Manufacturer (OEM), Independent Hardware Vendor (IHV), or Independent Software Vendor (ISV), this complete LICENSE AGREEMENT applies;

• If you are an End-User, then only Exhibit A, the INTEL SOFTWARE LICENSE AGREEMENT, applies.

For OEMs, IHVs, and ISVs:

LICENSE. This Software is licensed for use only in conjunction with Intel component products. Use of the Software in conjunction with non-Intel component products is not licensed hereunder. Subject to the terms of this Agreement, Intel grants to You a nonexclusive, nontransferable, worldwide, fully paid-up license under Intel's copyrights to:

a. use, modify and copy Software internally for Your own development and maintenance purposes; and

b. modify, copy and distribute Software, including derivative works of the Software, to Your end-users, but only under a license agreement with terms at least as restrictive as those contained in Intel's Final, Single User License Agreement, attached as Exhibit A; and

c. modify, copy and distribute the end-user documentation which may accompany the Software, but only in association with the Software.

If You are not the final manufacturer or vendor of a computer system or software program incorporating the Software, then You may transfer a copy of the Software, including derivative works of the Software (and related end-user documentation) to Your recipient for use in accordance with the terms of this Agreement, provided such recipient agrees to be fully bound by the terms hereof. You shall not otherwise assign, sublicense, lease, or in any other way transfer or disclose Software to any third party. You shall not reverse- compile, disassemble or otherwise reverse-engineer the Software.

Except as expressly stated in this Agreement, no license or right is granted to You directly or by implication, inducement, estoppel or otherwise. Intel shall have the right to inspect or have an independent auditor inspect Your relevant records to verify Your compliance with the terms and conditions of this Agreement.

CONFIDENTIALITY. If You wish to have a third party consultant or subcontractor ("Contractor") perform work on Your behalf which involves access to or use of Software, You shall obtain a written confidentiality agreement from the Contractor which contains terms and obligations with respect to access to or use of Software no less restrictive than those set forth in this Agreement and excluding any distribution rights, and use for any other purpose. Otherwise, You shall not disclose the terms or existence of this Agreement or use Intel's name in any publications, advertisements, or other announcements without Intel's prior written consent. You do not have any rights to use any Intel trademarks or logos.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel may make changes to the

Software, or to items referenced therein, at any time and without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY. If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES. EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

LIMITATION OF LIABILITY. IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

TERMINATION OF THIS AGREEMENT. Intel may terminate this Agreement at any time if you violate its terms. Upon termination, you will immediately destroy the Software or return all copies of the Software to Intel.

APPLICABLE LAWS. Claims arising under this Agreement shall be governed by the laws of California, excluding its principles of conflict of laws and the United Nations Convention on Contracts for the Sale of Goods. You may not export the Software in violation of applicable export laws and regulations. Intel is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Intel.

GOVERNMENT RESTRICTED RIGHTS. The Software is provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or their successors. Use of the Software by the Government constitutes acknowledgment of Intel's proprietary rights therein. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052.

EXHIBIT A

INTEL SOFTWARE LICENSE AGREEMENT (Final, Single User)

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING. Do not use or load this software and any associated materials (collectively, the 'Software' until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

LICENSE. You may copy the Software onto a single computer for your personal, noncommercial use, and you may make one back-up copy of the Software, subject to these conditions:

1. This Software is licensed for use only in conjunction with Intel component products. Use of the Software in conjunction with non-Intel component products is not licensed hereunder.

2. You may not copy, modify, rent, sell, distribute or transfer any part of the Software except as provided in this Agreement, and you agree to prevent unauthorized copying of the Software.

3. You may not reverse engineer, decompile, or disassemble the Software.

4. You may not sublicense or permit simultaneous use of the Software by more than one user.

5. The Software may contain the software or other property of third party suppliers, some of which may be identified in, and licensed in accordance with, any enclosed `license.txt` file or other text or file.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. Intel may make changes to the Software, or to items referenced therein, at any time without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

LIMITED MEDIA WARRANTY. If the Software has been delivered by Intel on physical media, Intel warrants the media to be free from material physical defects for a period of ninety (90) days after delivery by Intel. If such a defect is found, return the media to Intel for replacement or alternate delivery of the Software as Intel may select.

EXCLUSION OF OTHER WARRANTIES. EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Intel does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

LIMITATION OF LIABILITY. IN NO EVENT SHALL INTEL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION, OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

TERMINATION OF THIS AGREEMENT. Intel may terminate this Agreement at any time if you violate its terms. Upon termination, you will immediately destroy the Software or return all copies of the Software to Intel.

APPLICABLE LAWS. Claims arising under this Agreement shall be governed by the laws of California, excluding its principles of conflict of laws and the United Nations Convention on Contracts for the Sale of Goods. You may not export the Software in violation of applicable export laws and regulations. Intel is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Intel.

GOVERNMENT RESTRICTED RIGHTS. The Software is provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the Government is subject to restrictions as set forth in FAR52.227-14 and DFAR252.227-7013 et seq. or their successors. Use of the Software by the Government constitutes acknowledgment of Intel's proprietary rights therein. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052.

SLA/OEM/IHV/RBK/ April 23, 2004

1.2. DISCLAIMER

Intel is making no claims of usability, efficacy or warranty. The INTEL SOFTWARE LICENSE AGREEMENT contained herein completely defines the license and use of this software.

Information in this document is provided in connection with Intel products. Except as expressly stated in the INTEL SOFTWARE LICENSE AGREEMENT contained herein, no license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products, including liability or warranties relating to fitness for a particular purpose, merchantability or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, lifesaving, or life-sustaining applications.

Intel Corporation disclaims all warranties and liabilities for the use of this document, the software and the information contained herein, and assumes no responsibility for any errors which may appear in this document or the software, nor does Intel make a commitment to update the information or software contained herein. Intel reserves the right to make changes to this document or software at any time, without notice.

Other names and brands may be claimed as the property of others.

Copyright (c) Intel Corporation, 2010

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of 3Dlabs Inc. Ltd. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (C) 2002-2009 3Dlabs Inc. Ltd.

All rights reserved

2. Intel Wireless Drivers

Copyright (c) 2006-2009, Intel Corporation. All rights reserved.

Redistribution. Redistribution and use in binary form, without modification, are permitted provided that the following conditions are met:

• Redistributions must reproduce the above copyright notice and the following disclaimer in the documentation and/ or other materials provided with the distribution.

• Neither the name of Intel Corporation nor the names of its suppliers may be used to endorse or promote products derived from this software without specific prior written permission.

• No reverse engineering, decompilation, or disassembly of this software is permitted.

Limited patent license. Intel Corporation grants a world-wide, royalty-free, non-exclusive license under patents it now or hereafter owns or controls to make, have made, use, import, offer to sell and sell ("Utilize") this software, but solely to the extent that any such patent is necessary to Utilize the software alone, or in combination with an operating system licensed under an approved Open Source license as listed by the Open Source Initiative at http:// opensource.org/licenses. The patent license shall not apply to any other combinations which include this software. No hardware per se is licensed hereunder.

DISCLAIMER. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY

OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

3. 3rd Party Copyrights

Software covered by the following third party copyrights may be included with this product and will also be subject to the software license agreement: Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1991, 1999 Free Software Foundation, Inc, Copyright (C) 2000--2006 Kevin Atkinson, Copyright (C) 2002, 2003, 2004, 2006 Kevin Atkinson, Copyright (C) 1991 Free Software Foundation, Inc, Copyright (C) 1991, 1999 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (c) Lennart Kolmodin, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1991, 1999 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 19yy <name of author>, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1996-2006 Julian R Seward., Copyright (C) 1996-2007 Julian R Seward., Copyright (C) 1991, 1999 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1998-2009 Texas Instruments. All rights reserved, Copyright (C) 2000-2005 by David Brownell, Copyright (C) 2000-2005 by David Brownell <dbrownell@users.sourceforge.net>, Copyright (C) 2001 Intersil Americas Inc, Copyright (C) 2002 David S. Miller, Copyright (C) 2002 David S. Miller (davem@redhat.com), Copyright (C) 2002 NetChip Technology, Inc. (http, Copyright (C) 2003 Conexant Americas Inc. All Rights Reserved, Copyright (C) 2003 David Brownell, Copyright (C) 2003-2005 David Hollis <dhollis@davehollis.com>, Copyright (C) 2003-2005 Pontus Fuchs, Giridhar Pemmasani, Copyright (C) 2003-2005 by David Brownell, Copyright (C) 2003-2006, Marvell International Ltd, Copyright (C) 2004 - 2006 rt2x00 SourceForge Project, Copyright (C) 2004 - 2009 Felix Fietkau <nbd@openwrt.org>, Copyright (C) 2004 - 2009 Gertjan van Wingerde <gwingerde@gmail.com>, Copyright (C) 2004 - 2009 Ivo van Doorn <IvDoorn@gmail.com>, Copyright (C) 2004 Florian Schirmer (jolt@tuxbox.org), Copyright (C) 2004 Pekka Pietikainen (pp@ee.oulu.fi), Copyright (C) 2004, 2005, 2006 Nokia Corporation, Copyright (C) 2004, Intel Corporation <jketreno@linux.intel.com>, Copyright (C) 2004-2005 Intel Corporation <jketreno@linux.intel.com>, Copyright (C) 2005 Andreas Jaggi <andreas.jaggi@waterwave.ch>, Copyright (C) 2005 Danny van Dyk <kugelfang@gentoo.org>, Copyright (C) 2005 Martin Langer <martin-langer@gmx.de>, Copyright (C) 2005 Nokia Corporation (taken from islsm_pda.h), Copyright (C) 2005 Stefano Brivio <st3@riseup.net>, Copyright (C) 2005 Stefano Brivio <stefano.brivio@polimi.it>, Copyright (C) 2005 Texas Instruments Incorporated, Copyright (C) 2005 by David Brownell, Copyright (C) 2005, 2006 Michael Buesch <mb@bu3sch.de>, Copyright (C) 2005-2006 Michael Buesch <mb@bu3sch.de>, Copyright (C) 2005-2007 Derek Smithies <derek@indranet.co.nz>, Copyright (C) 2005-2007 Michael Buesch <mb@bu3sch.de>, Copyright (C) 2005-2007 Ulrich Kunitz <kune@deine-taler.de>, Copyright (C) 2005-2008 Michael Buesch <mb@bu3sch.de>, Copyright (C) 2006 - 2007 Ivo van Doorn, Copyright (C) 2006 Broadcom Corporation, Copyright (C) 2006 Felix Fietkau (nbd@openwrt.org), Copyright (C) 2006 by Ole Andre Vadla Ravnas (ActiveSync), Copyright (C) 2006, Red Hat, Inc. /, Copyright (C) 2006-2007 Daniel Drake <dsd@gentoo.org>, Copyright (C) 2006-2007 Michael Wu <flamingice@sourmilk.net>, Copyright (C) 2007 Conexant Systems, Inc, Copyright (C) 2007 Dmitry Torokhov, Copyright (C) 2007 Ivo van Doorn, Copyright (C) 2007 Larry Finger <Larry.Finger@lwfinger.net>, Copyright (C) 2007 Michael Buesch <mb@bu3sch.de>, Copyright (C) 2007 by Bjorge Dijkstra <bjd@jooz.net>, Copyright (C) 2007, Red Hat, Inc, Copyright (C) 2007, Red Hat, Inc. /, Copyright (C) 2007-2008 Luis R. Rodriguez <mcgrof@winlab.rutgers.edu>, Copyright (C) 2008 Christian Lamparter <chunkeey@web.de>, Copyright (C) 2008 Felix Fietkau <nbd@openwrt.org>, Copyright (C) 2008 Google Inc, Copyright (C) 2008 Nokia Corporation, Copyright (C) 2008 Nokia Corporation and/or its subsidiary(-ies), Copyright (C) 2008, cozybit Inc, Copyright (C) 2008-2009 Marvell Semiconductor Inc, Copyright (C) 2008-2009 Nokia Corporation, Copyright (C) 2008-2009 by Jussi Kivilinna <jussi.kivilinna@mbnet.fi>, Copyright (C) 2009 Alban Browaeys prahal@yahoo.com>, Copyright (C) 2009 Albert Herranz, Copyright (C) 2009 Axel Kollhofer <rain_maker@root-forum.org>, Copyright (C) 2009 Bart Zolnierkiewicz <bzolnier@gmail.com>, Copyright (C) 2009 Bartlomiej Zolnierkiewicz, Copyright (C) 2009 Bartlomiej Zolnierkiewicz <bzolnier@gmail.com>, Copyright (C) 2009 Bob Copeland (me@bobcopeland.com), Copyright (C) 2009 Felix Fietkau <nbd@openwrt.org>, Copyright (C) 2009 Gertjan van Wingerde <gwingerde@gmail.com>, Copyright (C) 2009 Intel Corporation <ilw@linux.intel.com>, Copyright (C) 2009 Intel Corporation. All rights reserved, Copyright (C) 2009 Ivo van Doorn <IvDoorn@gmail.com>, Copyright (C) 2009 Luis Correia <luis.f.correia@gmail.com>, Copyright (C) 2009 M&N Solutions GmbH, 61191 Rosbach, Germany, Copyright (C) 2009 Mark Asselstine <asselsm@gmail.com>, Copyright (C) 2009 Mattias Nissler <mattias.nissler@gmx.de>, Copyright (C) 2009 Michael Buesch <mb@bu3sch.de>, Copyright (C) 2009 Nokia

1989, 1991 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (C) 1989, 1991 Free Software Foundation, Inc, Copyright (c) 1994 by Silicon Graphics Computer Systems, Inc, Copyright (C) 1991-2000 Silicon Graphics, Inc. All Rights Reserved, Copyright (C) 1994-2003 The XFree86 Project, Inc. All Rights Reserved, Copyright (C) 1996-1999 SciTech Software, Inc, Copyright (C) 1999 Egbert Eich, Copyright (C) 1999,2000 by Eric Sunshine <sunshine@sunshineco.com>, Copyright (C) 2000 Jakub Jelinek (jakub@redhat.com), Copyright (C) 2000 Keith Packard, Copyright (C) 2001-2004 Harold L Hunt II All Rights Reserved, Copyright (C) 2001-2005 by Thomas Winischhofer, Vienna, Austria, Copyright (C) 2003 Anders Carlsson, Copyright (C) 2005 Bogdan D. bogdand@users.sourceforge.net, Copyright (C) 2008 Bart Trojanowski, Symbio Technologies, LLC, Copyright (C) Colin Harrison 2005-2008, Copyright (C) David Mosberger-Tang, Copyright (c) 1987 by the Regents of the University of California, Copyright (c) 1987, 1989-1990, 1992-1995 X Consortium, Copyright (c) 1989, 1990, 1993, 1994, Copyright (c) 1991, 1996-1997 Digital Equipment Corporation, Maynard, Massachusetts, Copyright (c) 1994, 1995 Hewlett-Packard Company, Copyright (c) 1994-2003 by The XFree86 Project, Inc, Copyright (c) 1995 X Consortium, Copyright (c) 1997 Matthieu Herrb, Copyright (c) 1997 Metro Link Incorporated, Copyright (c) 1998 Todd C. Miller <Todd.Miller@courtesan.com>, Copyright (c) 2000 by Conectiva S.A. (http, Copyright (c) 2000, 2001 Nokia Home Communications, Copyright (c) 2001 Andreas Monitzer, Copyright (c) 2001, Andy Ritger aritger@nvidia.com, Copyright (c) 2001-2004 Greg Parker, Copyright (c) 2001-2004 Torrey T. Lyons, Copyright (c) 2002 Apple Computer, Inc, Copyright (c) 2002, 2008, 2009 Apple Computer, Inc, Copyright (c) 2002-2003 Apple Computer, Inc, Copyright (c) 2002-2009 Apple Inc, Copyright (c) 2003 Torrey T. Lyons, Copyright (c) 2003 by the XFree86 Project, Inc, Copyright (c) 2003-2004 Torrey T. Lyons, Copyright (c) 2004, X.Org Foundation, Copyright (c) 2004-2005 Alexander Gottwald, Copyright (c) 2005 Alexander Gottwald, Copyright (c) 2007 Jeremy Huddleston, Copyright (C) 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, Copyright (C) 1992, 1993, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, Copyright (C) 1994 X Consortium, Copyright (c) 1984, 1985 by X Consortium, Copyright (c) 1987, 1988 X Consortium, Copyright (c) 2001 by Juliusz Chroboczek, Copyright (C) 1989, 1991 Free Software Foundation, Inc

This contains work of the U.S. Government that is not subject to copyright protection in the United States. Foreign copyrights may apply.

4. BSD License Variants

4.1. 4-clause License (original "BSD License")

Copyright (c) <year>, <copyright holder>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the <organization>.

- Neither the name of the <organization> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY <COPYRIGHT HOLDER> ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL <COPYRIGHT HOLDER> BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

4.2. 3-clause License ("New BSD License")

4.3. 2-clause License ("Simplified BSD License" or "FreeBSD License")

Index

Symbols

A

C

D

E

F

I

M

N

O

P

S

T

U