Simplified Usage Guide

Version 1.1

BitIdentify SDL

Preface/Terminology

Virtualization is a technology that enables you to split one computer into multiple separate, distinct, and secure environments with different software/hardware properties. Each distinct environment is called a Virtual Machine, in our system, these Virtual Machines are *Open and Secure Machines*.

The Host is what runs our Virtual Machines (Open/Secure), it's a an in-house built Linux Operating System customized for security and virtualization.

The Guests are the Virtual Machines Open and Secure, in most cases these are running Windows 10 Operating System.

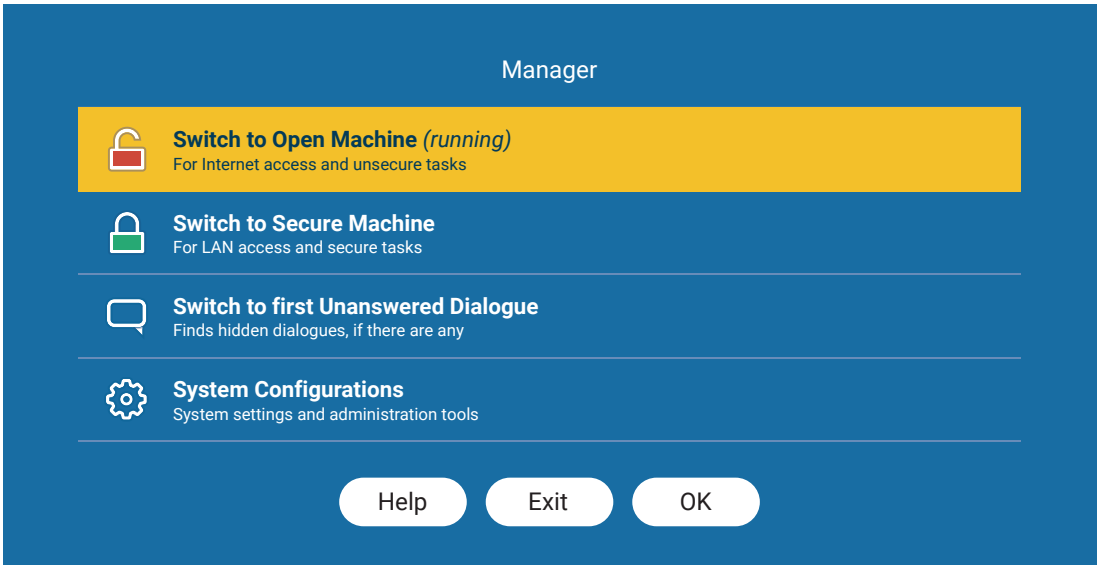
Guest 1: Open Machine
This is the internet-connected Virtual Machine used for web-browsing, email, and other internet-related tasks. This machine works like a normal PC.

Guest 2: Secure Machine
This Virtual Machine is not internet-connected and fully isolated from malware, viruses, and hackers. It's a secure work environment in which the user can work on classified information safe in the knowledge it cannot leave the machine.

Simple and common tasks

In this section we will go trough all the common tasks you might do on a daily basis.

Using the menus



The Manager-menu

The menus throughout the InproaHST SDL-system use simple list-based navigation, options are listed top to bottom. The user navigates the menus as follows:

Using the mouse:

Click on the preferred option to highlight it then click the **OK** button.

Using keyboard:

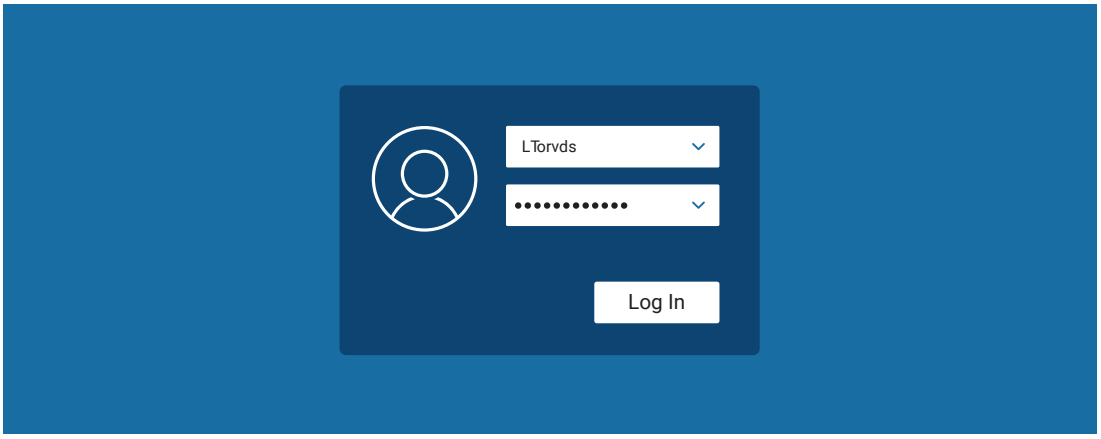
Using the up and down arrow keys, select the preferred option and hit the **Enter** key to select it (same as the **OK** button).

Cancel - It cancels the menu and returns you to the previous screen.

Help - Contains more detailed explanations on the different options.

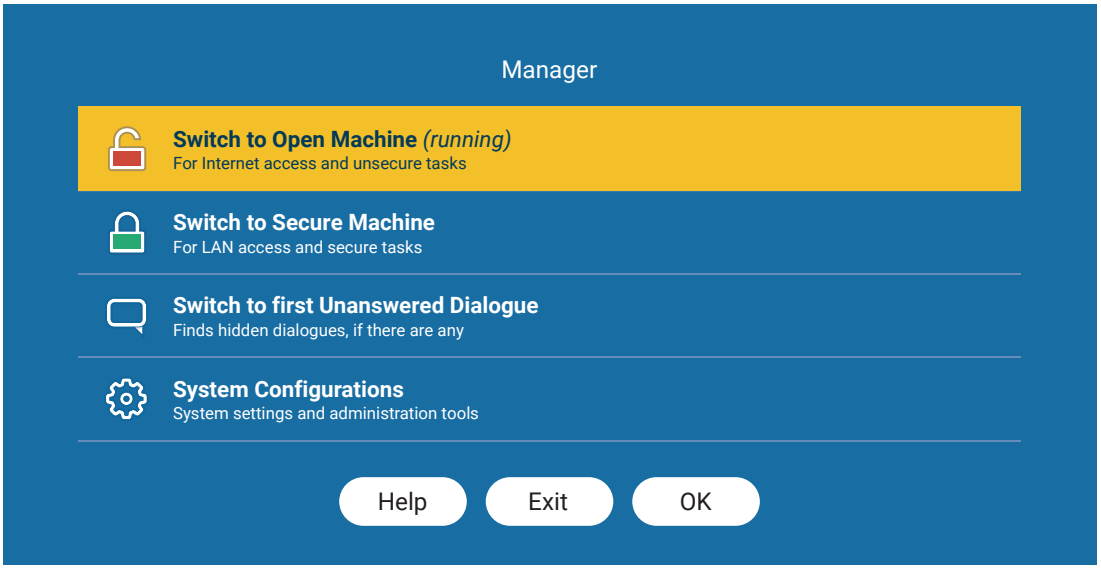
Starting the system

1. Press the power button on your computer.



The Login-window

2. Wait for the system to load and a login-window to appear.
Input username and password, press **Log In**.

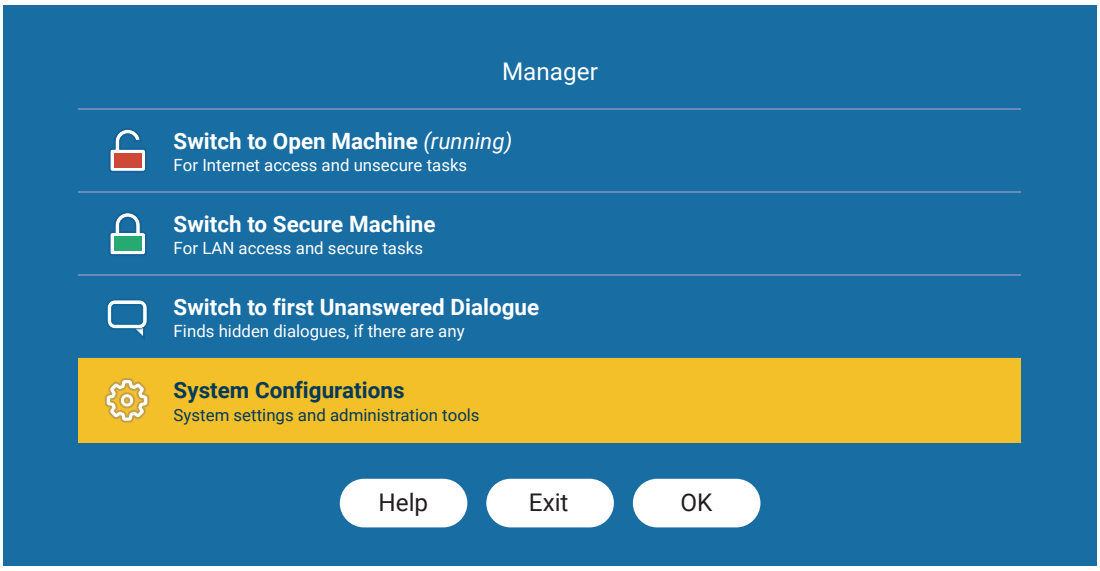


The Manager-menu

3. The Manager-menu will appear and here you can choose to either start the **Open Machine** or **Secure Machine**.

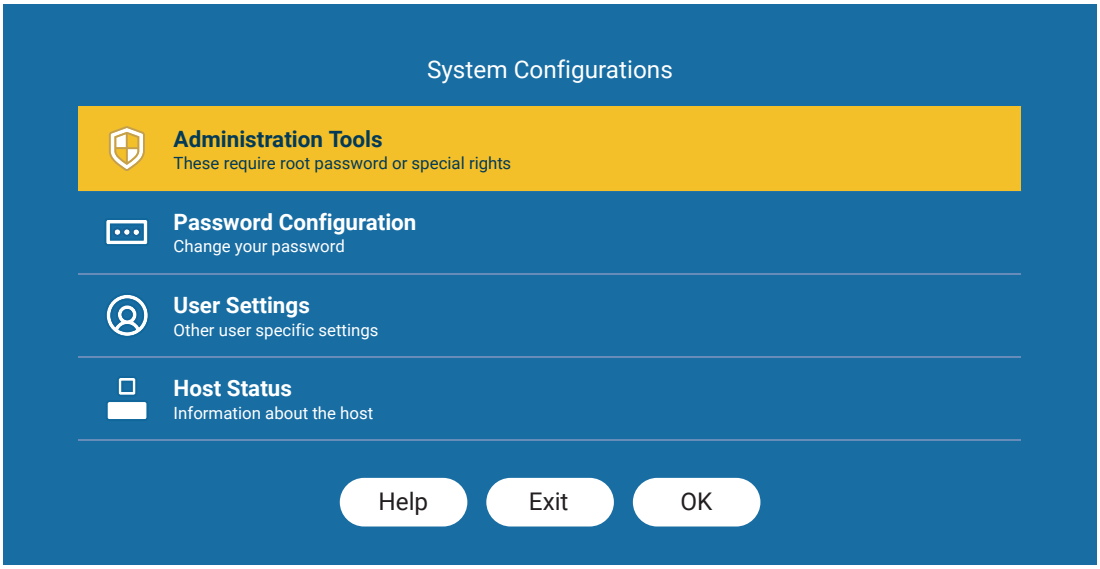
Adding WiFi network

1. Press **(<Ctrl> + <Alt>) <Ctrl> + <Alt> + M** to load the Manager-menu.



The Manager-menu

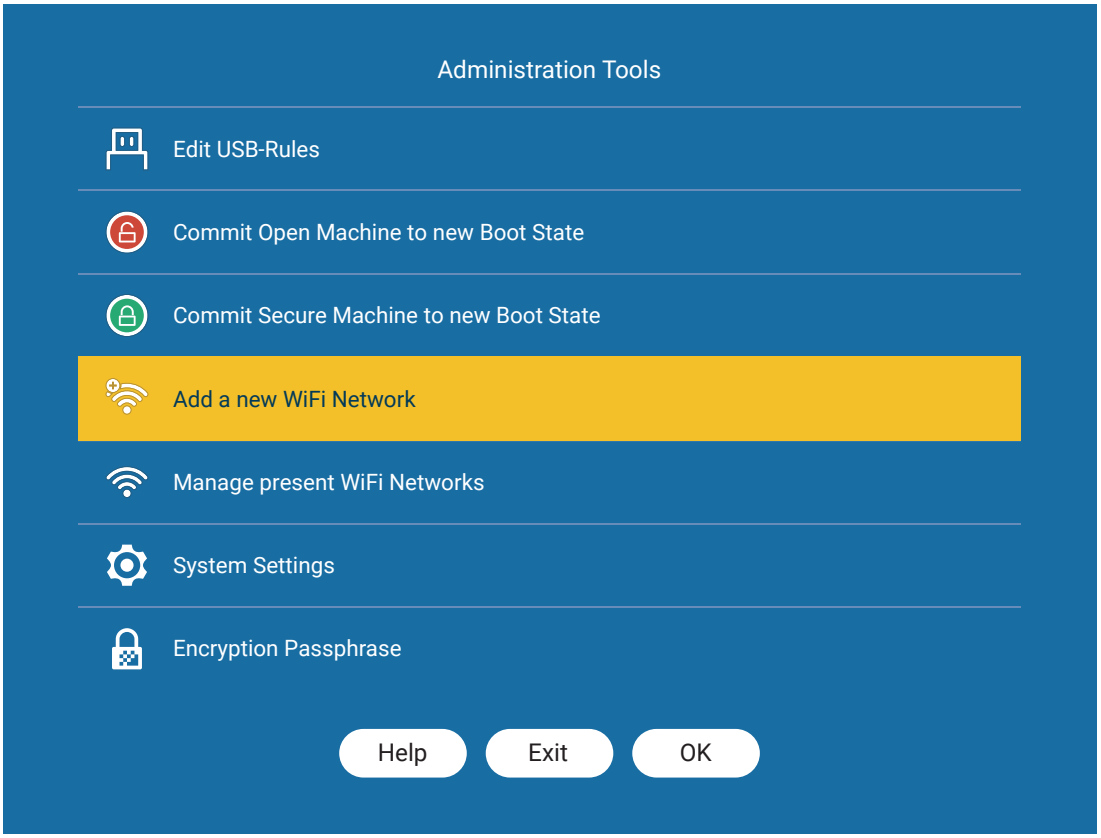
2. Select **System Configurations**.



The System Configurations-menu

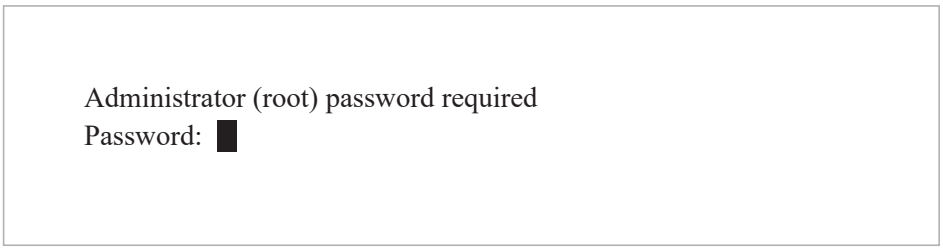
3. The System Configurations-menu will appear, select **Administration Tools.**

Continues on the next page...



The Administrations Tools-menu

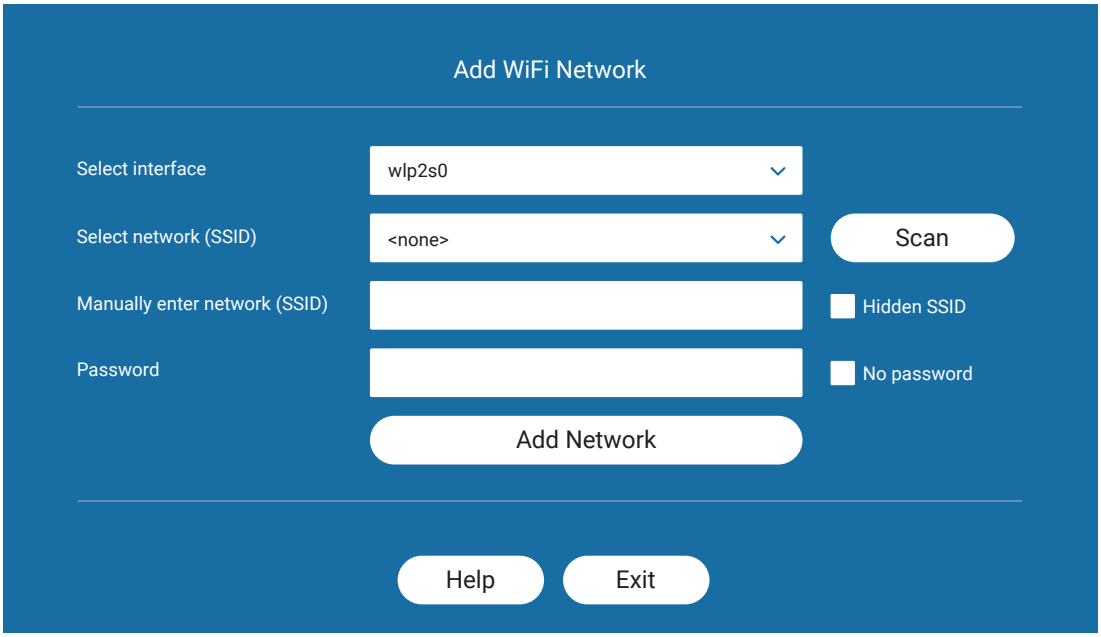
4. The Administration Tools menu will appear, select **Add a new WiFi Network.**



The Root-password dialog

5. Before you can configure your WiFi the system needs the **Root-password** (a special password used for administrative tasks).

Continues on the next page...



6. The **Add WiFi Network** menu will appear, press **Scan** to refresh the list of available WiFi networks. Select your WiFi network from the list.
7. Input the password for the WiFi network.
8. Press **Add Network** to add this network to your list of preferred networks.
9. Press **Exit** to return to the previous menu.

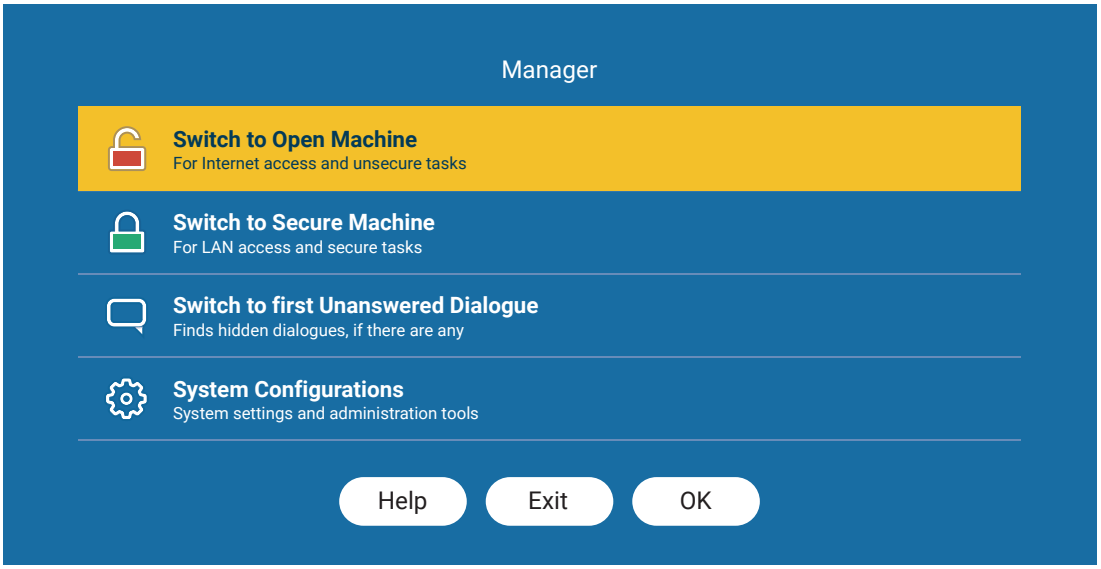
*NOTE 1: If there is more than one network-interface (external USB-WiFi dongle) select the right interface under **Select Interface**. Normally you can skip this step.*

NOTE 2: In this version, we only support WPA2 with a password, which is the normal security-type for WiFi.

Switching Machines

*NOTE: While in either the Open or Secure Machine you need to press <**Ctrl> + <Alt>** one extra time before using any other command. This is because we are using a virtual environment.*

1. While using either the Open or Secure Machine, press (**<Ctrl> + <Alt>**) **<Ctrl> + <Alt> + M** to load the Manager-menu.



The Manager-menu

2. The Manager-menu appears, choose to either switch to the Open or Secure Machine.
3. The system suspends the current Machine, a progress bar appears and the other Machine is loaded.

Switching Machines with shortcuts

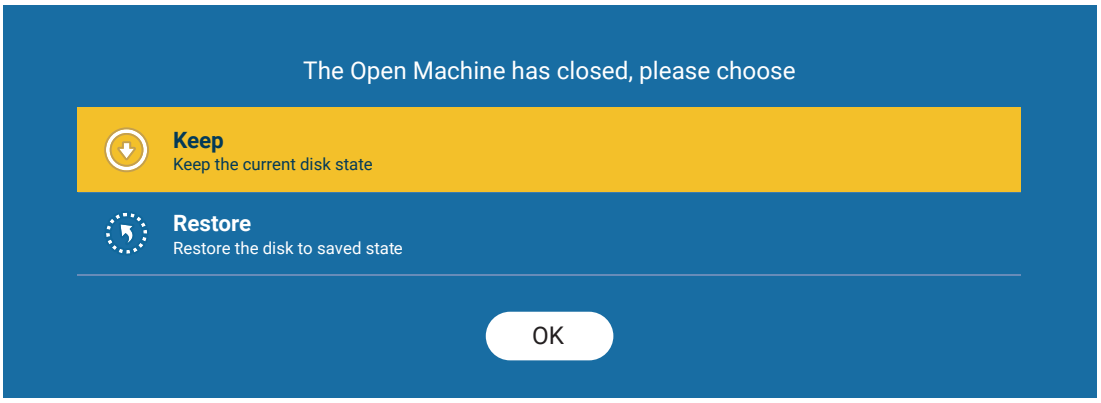
Secure Machine: Press (**<Ctrl> + <Alt>**) **<Ctrl> + <Alt> + S** to switch to the Secure Machine.

Open Machine: Press (**<Ctrl> + <Alt>**) **<Ctrl> + <Alt> + O** to switch to the Open Machine.

Shut down the Open & Secure Machine normally (Keep)

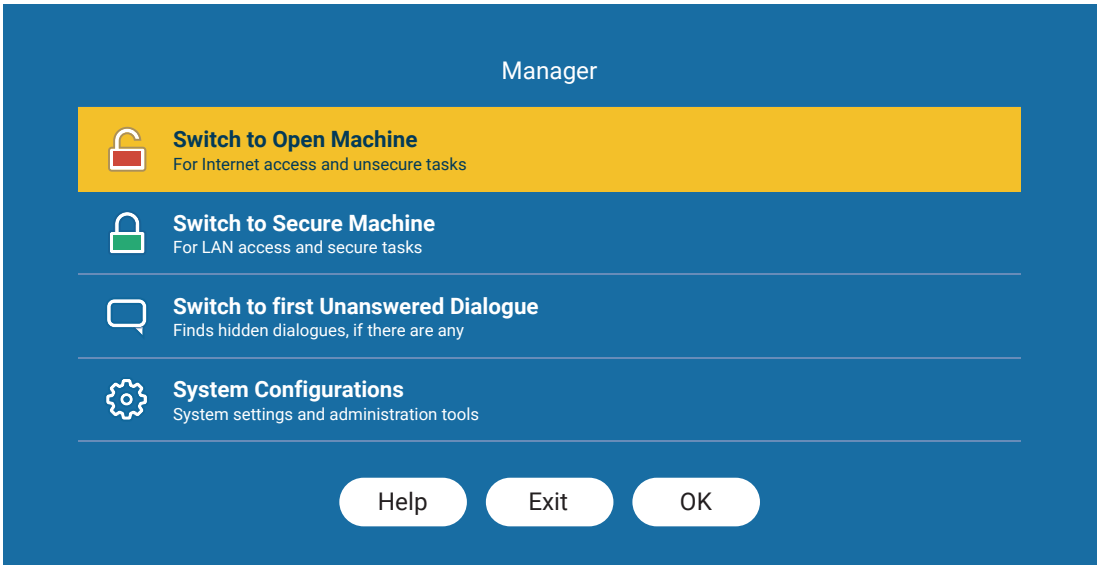
This is the standard way to shut down the system, modifications are kept and the system restarts just like any other Windows computer.

1. While in either Open or Secure Machine, shut down Windows normally by clicking the Windows icon, power icon, and select **Shut down** from the menu.



The Keep/Restore-menu

2. The Keep/Restore-menu is shown, select **Keep** as this is the normal option for a standard shutdown, all changes are kept.



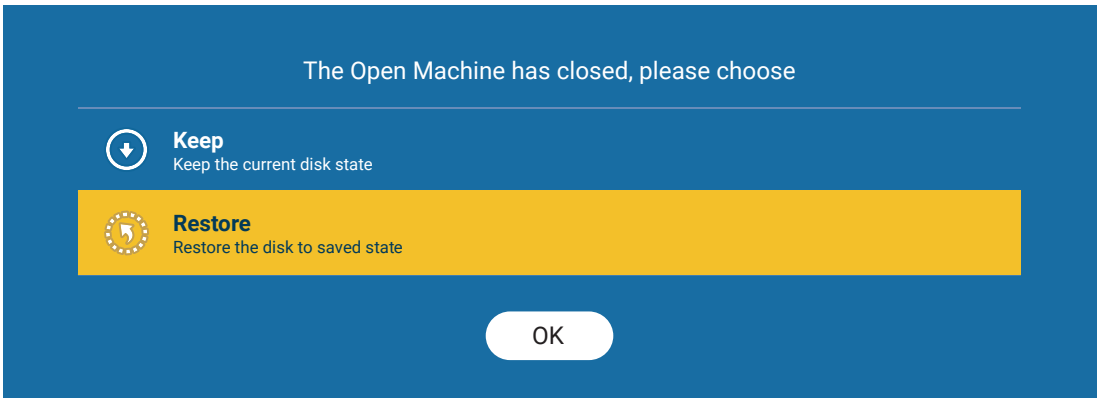
The Manager-menu

3. The process is completed very quickly and then the Manager-menu is shown.
4. To completely shut down the system; press the **Power Button** on your computer.
   *Note: If nothing happens, select **Switch to first Unanswered Dialogue** and press **OK**. Then press the **Power Button** again.*
5. Your system should be completely shut down.

Shut down with restore (Restore)

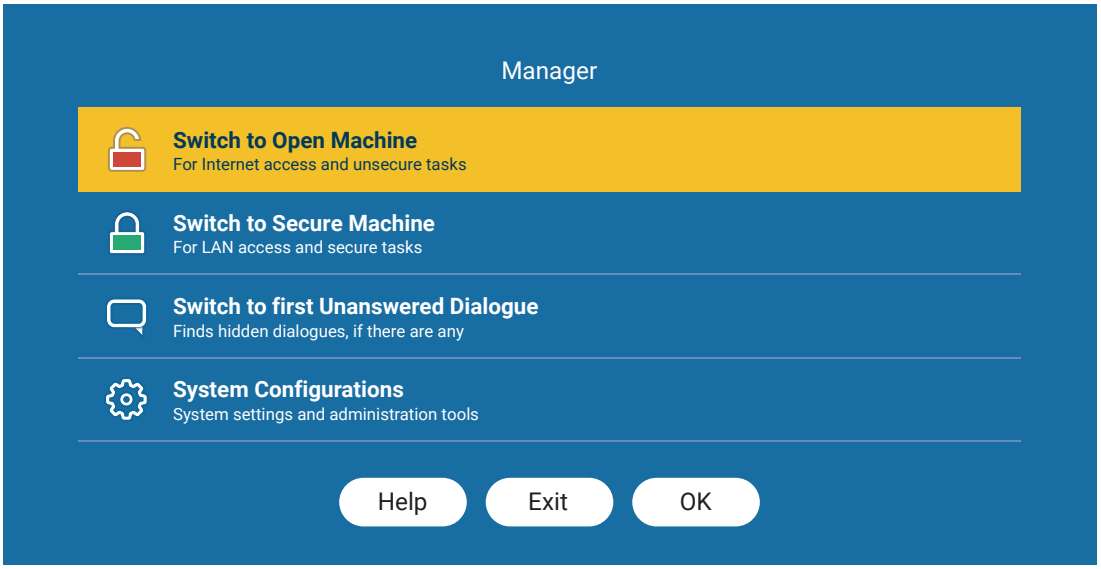
If the guest got infected with a virus or malware (or is unsure if he might be infected) a Restore is recommended, all system files are reset to their original uninfected state. NOTE: This restores the PC to the last time it was committed, all changes made (installed programs) after the latest committ will be lost.

1. While in either Open or Secure Machine, shut down or restart Windows normally by clicking the Windows icon, power icon and select from the menu.



The Keep/Restore-menu

2. The Keep/Restore-menu is shown, select **Restore** and the system reverts back to a working state.



The Manager-menu

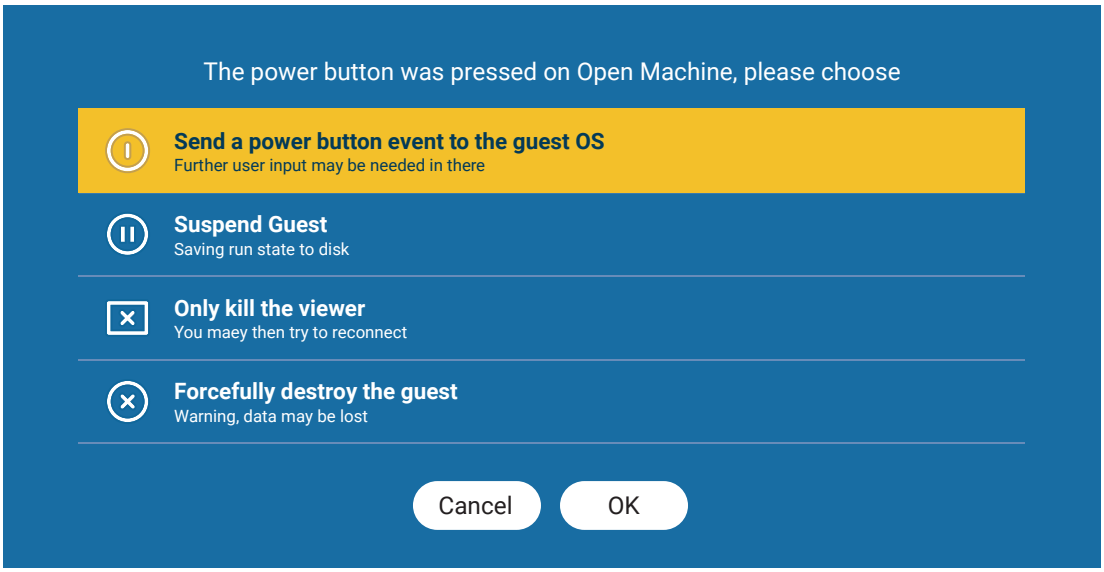
3. The process is compleated very quickly and then the Manager-menu is shown.
4. To completely shut down the system; press the **Power Button** on your computer.
5. Your system should be completely shut down.

Power Button options

Since the system runs multiple OS'es there is more than one option on what the physical Power Button does on your computer. When pressed you will get a menu outlining your options.

1. Press the physical **Power Button** on your PC

   The Power Button-menu is shown, please choose:



The Power Button-menu

2. **Send a power button event to the Guest OS**
   This option works like a normal PC, it will shut down your Guest OS (Windows in most cases).

Suspend Guest

This option will save your Open/Secure Machine's current state and suspend it.

Only kill viewer

This option kills the viewer (the viewer is the applications that control this, and all, menus).

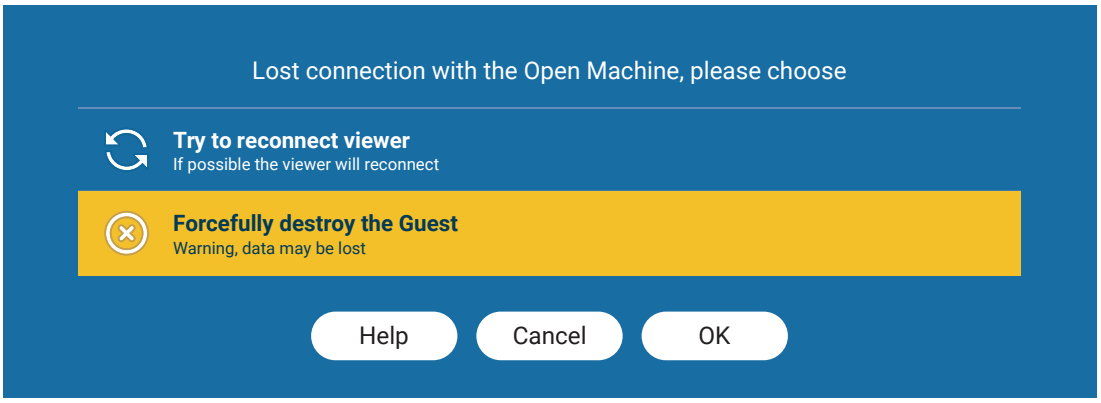
Forcefully destroy the guest

This option cut's the power to the running Guest Machine, just like pulling the plug on your PC.

WARNING: This option might result in lost or corrupted data on your running Guest (Open/Secure).

Lost connection

If the Host (Linux core) loses connection with the Guests (Open/Secure), the Lost connection-menu is shown. This menu is also shown if the user selects ***Only kill viewer*** *under* ***Power Button Options****.*



The Lost Connection-menu

Try to reconnect the viewer

If the user pressed **Only kill the viewer** in the **Power Button Options** this option restarts the viewer.

Forcefully destroy the Guest

This option cut's the power to the running Guest Machine, just like pulling the plug on your PC.

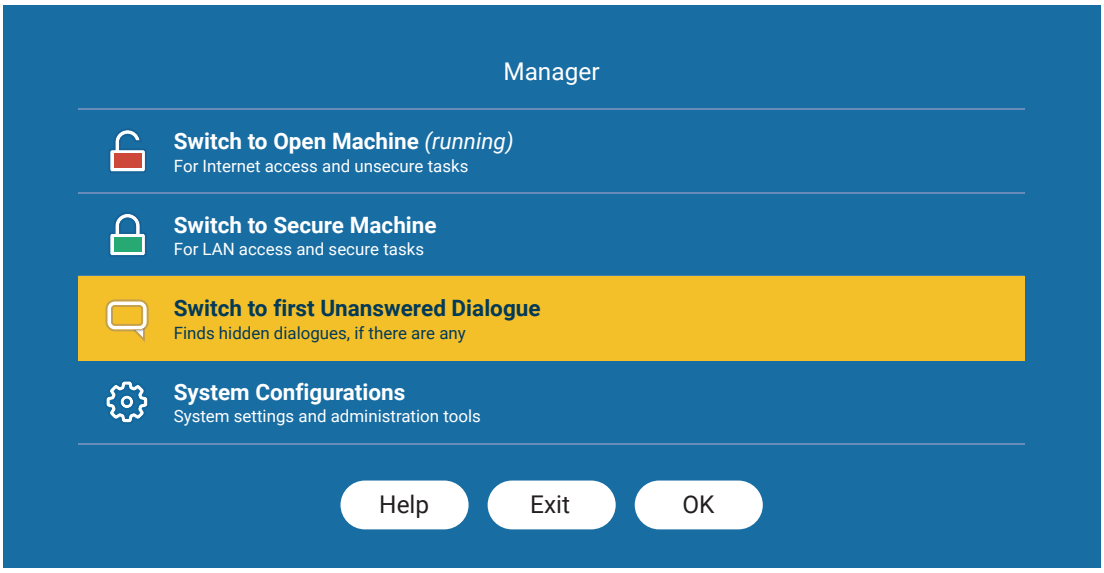
WARNING: This option might result in lost or corrupted data on your running Guest (Open/Secure).

First unanswered dialog

Dialog windows can stack up in the background if not handled directly, this option switches to the first unanswered dialog.

Visual representation of dialogs stacking behind the main window

1. While using either the Open or Secure Machine, press **(<Ctrl> + <Alt>) <Ctrl> + <Alt> + M** to load the Manager-menu.



The Manager-menu

2. Select **First Unanswered Dialog** and you are switched to the first Unanswered Dialog.

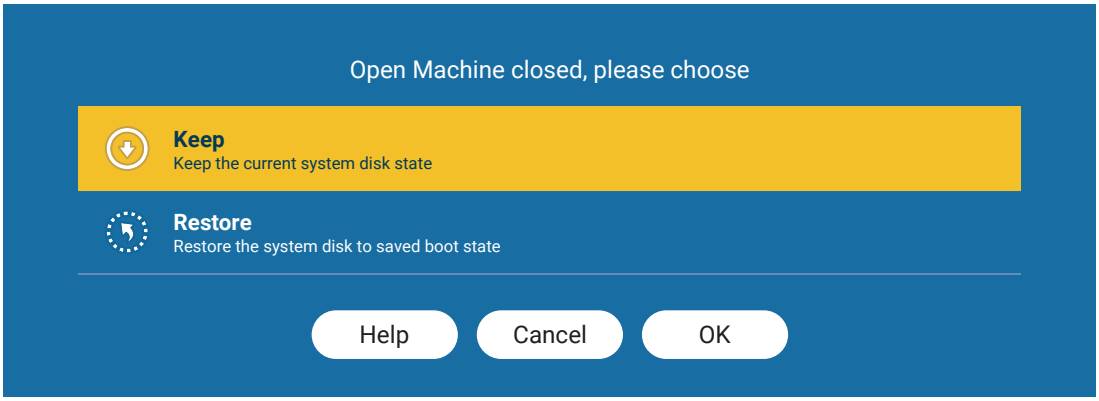
Advanced tasks

This section deals with more advanced tasks and should not be atempted by novice users, before going further please consult your administrator.

Download & install a program on both the Open & Secure Machines

NOTE 1: Preferably start with a recently restored Open Machine, follow the previous guide before this one: ***Shut down with restore (Restore)***

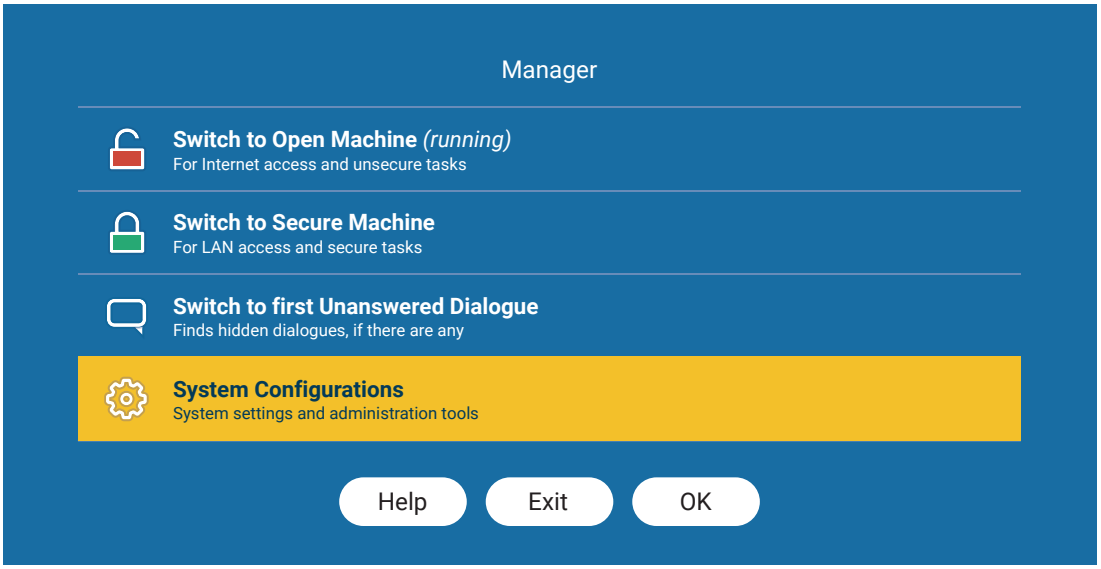
1. While in the Open Machine: Start a web browser and download the program you wish to install.
2. Install the program as you would on a standard PC.
3. Shut down Windows normally.



The Keep/Restore-menu

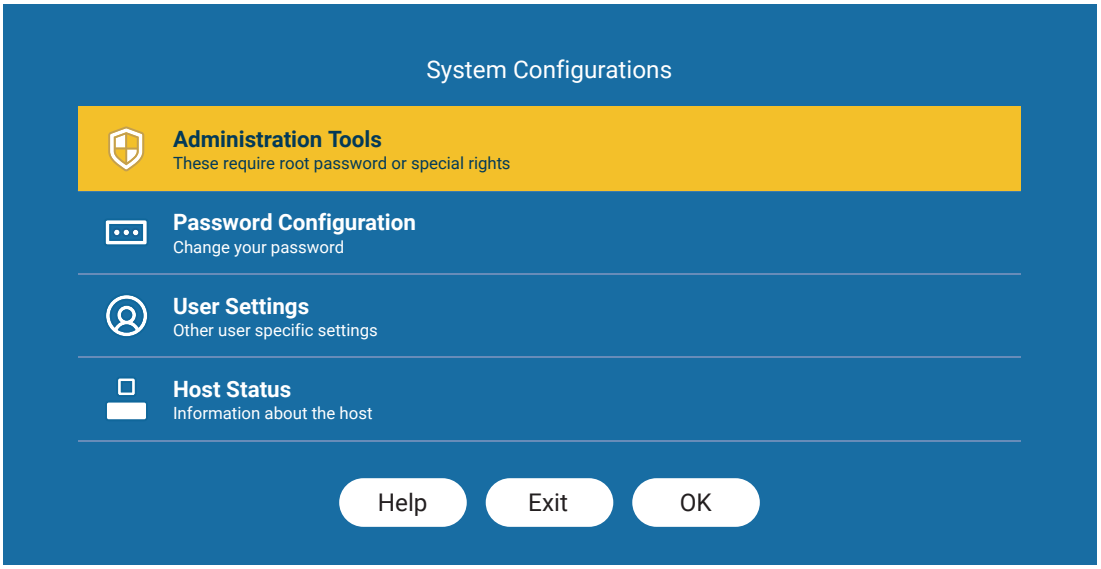
4. The Keep/Restore-menu appears, choose to **Keep.**

   NOTE 2: Make sure the Secure Machine is shut down and not suspended before the next step, if unsure switch to the Secure Machine and shut down Windows normally.



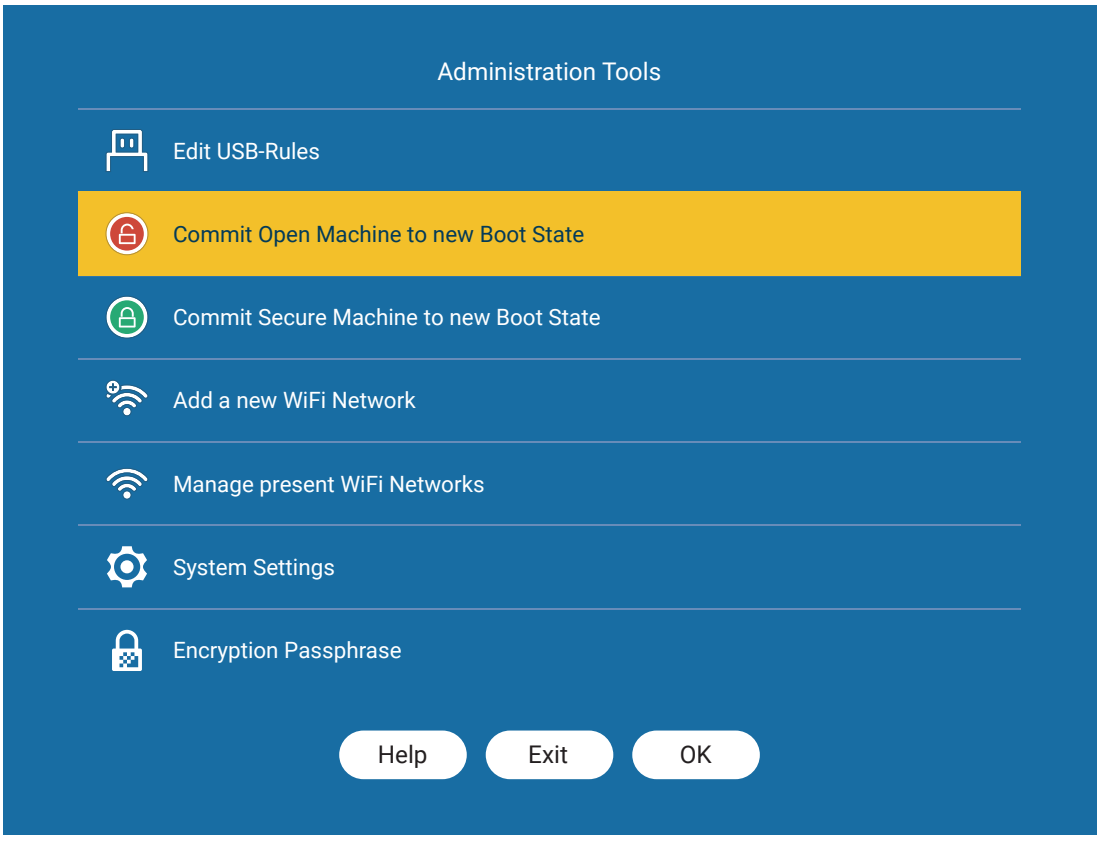
The Manager-menu

5. The Manager-menu appears, choose **System Configurations**.



The System Configurations-menu

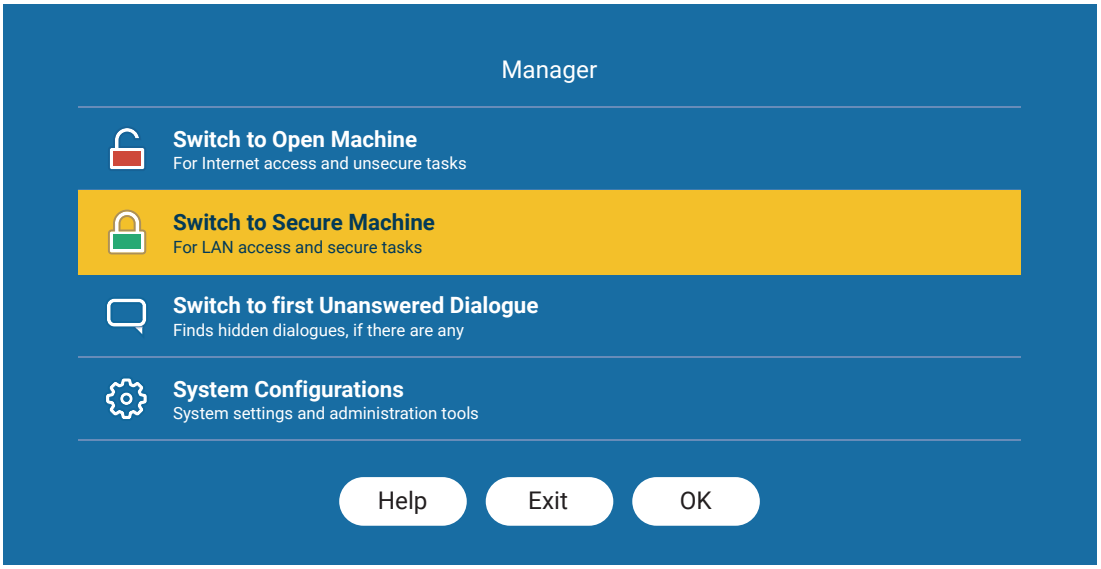
6. Choose **Administration Tools**.



The Administration Tools-menu

7. Choose **Commit Open Machine to new Boot State.**

continues on the next page...



The Manager-menu

8. The commit is done and the Manager-menu is shown once more, choose **Secure Machine.**
9. The Secure Machine is started and the program is installed and ready to use on both Machines.

NOTE ABOUT COMMIT AND WALLPAPERS: When doing a commit the Windows SDL Open/Secure wallpaper might be changed. It's important that you change it back since it's the only way to visually identify what Machine you are in (ie: red for Open Machine and Green for Secure Machine).

Option 1 (Reload the theme-pack)
Open the **Share** folder and then the **SDL** folder, doubble click on **SDL Open.deskthemepack** or **SDL Secure.deskthemepack** depending on what side you are currently using.

Option 2 (Only update the wallpaper)
Right-click on your desktop and choose **Personalize** and then click on the SDL Wallpaper in the list.

If unsure what Machine you are using please check what shared disk you are connected to, if you are on the Secure Machine your drive says "Secure" and vice versa for Open. You can also check if you have an internet connection by opening a browser if you can connect to the Internet you are on the Open Machine.

Install OS updates on both Open & Secure Machine

NOTE 1: Preferably start with a recently restored Open Machine, follow the previous guide before this one: ***Shut down with restore (Restore)***

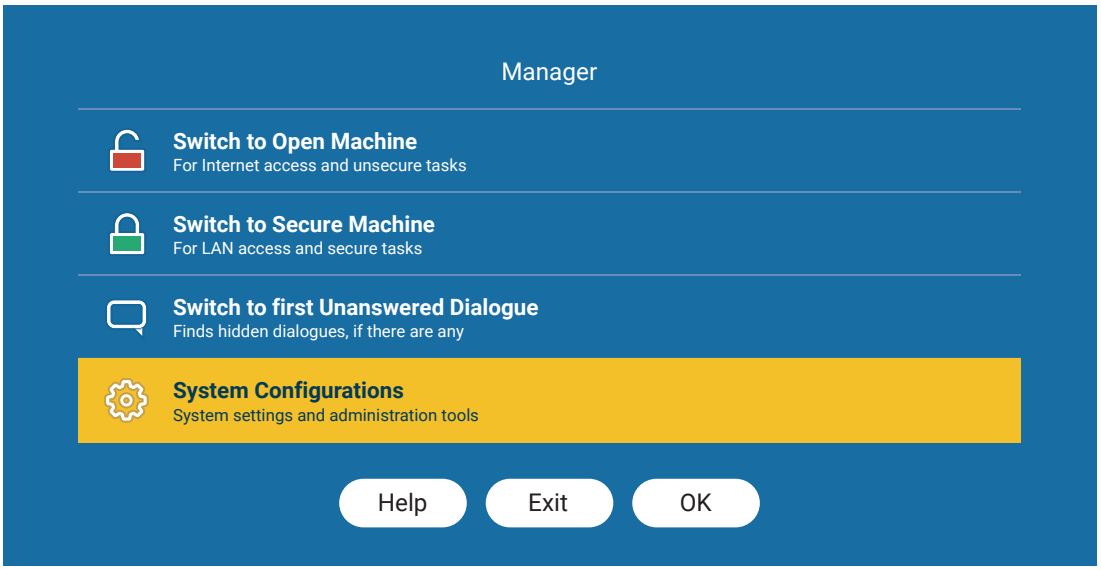
The process for installing OS updats is the same as previous chapter; ***Download & install a program on both the Open & Secure Machines****, with some expections. Some OS updates require multiple reboots before they are fully installed, it's very important that the OS update is fully installed before committing the system.*

1. While in the Open Machine: Run your operating systems update manager (In Windows this would be Windows Update), let it download and install the update.
2. Restart you PC when the update manager tells you to, wait for it to reboot and log back into your OS.
3. Run the update manager again (Windows Update), this is to make sure everything is downloaded, reboot a second time. Some large OS updates require you to reboot multiple times before it's finishes installing.
4. When you have logged back into your OS after reboot, follow the previous guide ***Download & install a program on both the Open & Secure Machines*** from step #3.

NOTE: If the Secure Machine fails to boot after upgrading Windows, commit the Open Machine a second time.

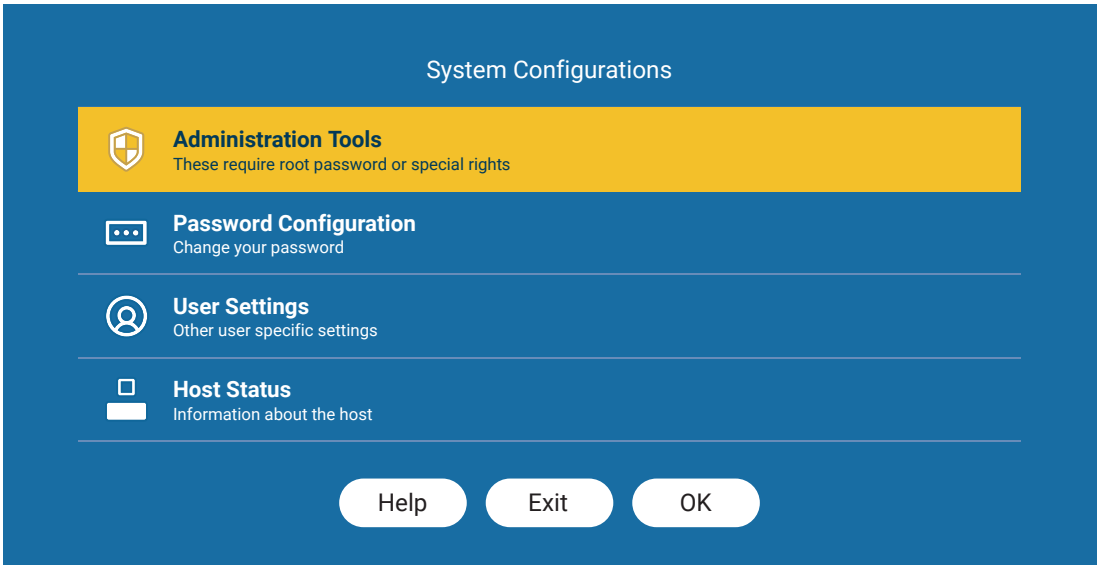
Adding USB-device using the USB-rules editor

1. Press **(<Ctrl> + <Alt>) <Ctrl> + <Alt> + M** to load the Manager-menu



The Manager-menu

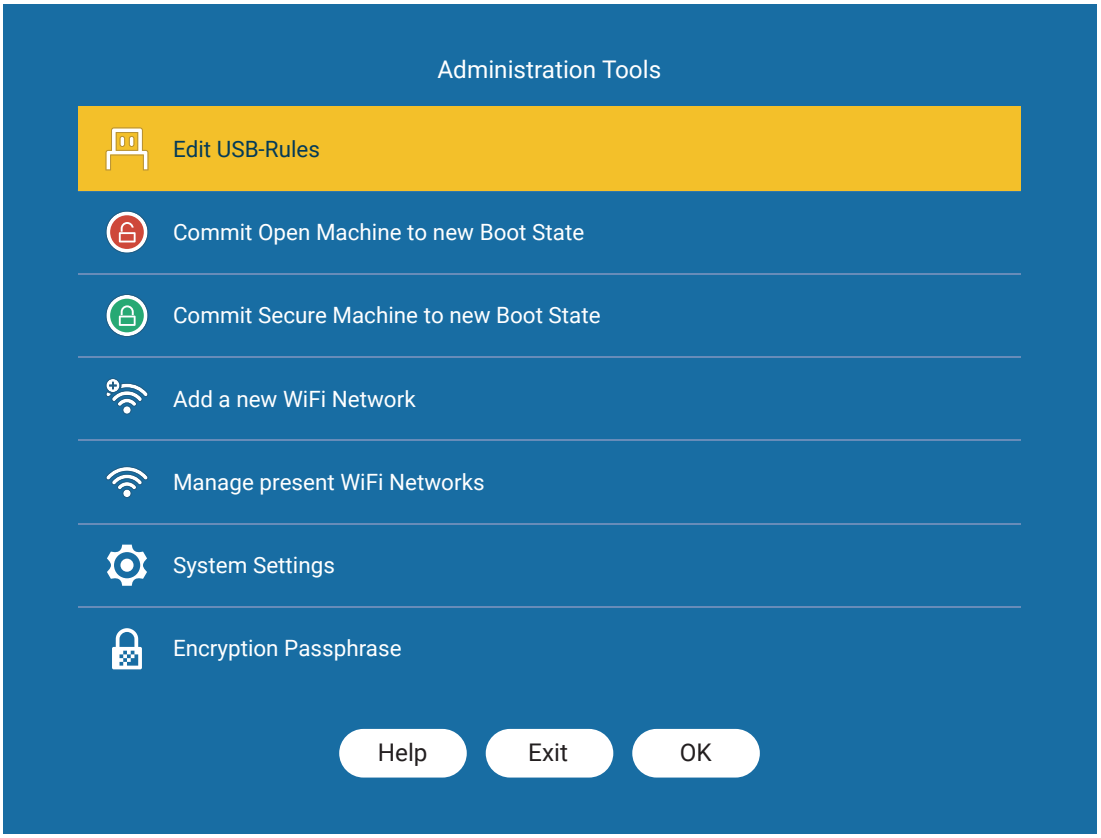
2. Select **System Configurations**.



The Administration Tools-menu

3. Select **Administration Tools** and input the root-password in the terminal that pops up, press enter.

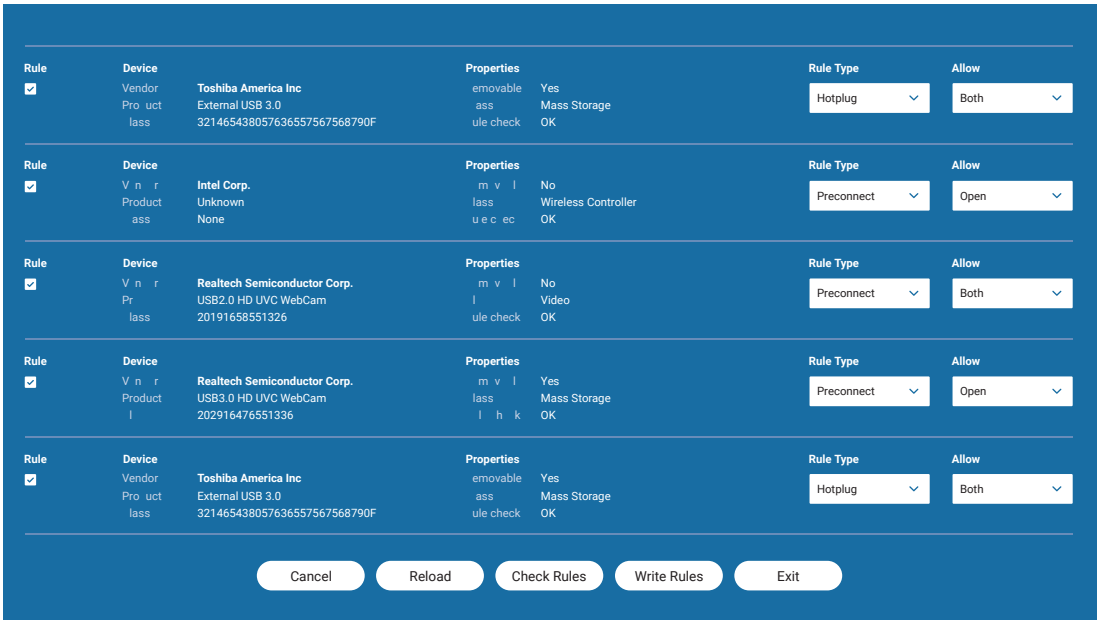
continues on the next page...



The Administration Tools-menu

4. In the Administration Tools-menu select **Edit USB-Rules**.

continues on the next page...



The USB-rules editor

5. The USB-Rules Editor is loaded, insert the USB-device you want to use in the system.
6. Press **Reload** to make the new USB-device visible in the list.
7. The new USB-device should be identifiable with the **Vendor** and **Product** description.
8. On the droplist **Rule Type** to the right of the device:

   Hotplug = The USB-device has to be plugged in every time you load a new Machine. This is recommended for USB-sticks and USB-hard drives.

   Preconnect = The USB-device may always be connected, this is recommended for devices like printers, webcams, and other fixed equipment.
9. On the droplist **Allow** to the right of the device:

   Open = Only allow the device on the Open Machine.

   Secure = Only allow the deivce on the Secure Machine.

   Both = Allow the device on both the Open and Secure Machine (with this option only **Hotplug** is possible, for security reasons).
10. Press **Check Rules** at the bottom and the system checks if all features are allowed.
11. If rules are ok press **Write Rules** and the rules are saved.
12. Press **Exit** to go back to the Manager-menu.

Adding Network Devices

In the InproaHST SDL system, automatic network discovery is blocked for security reasons. This means Windows (or other OS'es) will not find for example network printers on the network automatically. Printers and other network devices must be added with IP. In this example, we will be adding a printer in a Windows-environment.

Adding Printer with Windows default drivers

Adding a printer with Windows default drivers is easy but gives you limited functionality, but usually works for normal printing.

1. Make sure the network device you are adding has been given a dedicated IP address on your router.
2. Navigate to **Settings** and then **Printers & scanners**.
3. Press the button Add a printer or scanner and wait until the link **The printer that I want isn't listed** appears and click it.
4. Select **Add a printer using TCP/IP address or hostname**.
5. Type your printer's IP address into the field **Hostname or IP address** and press next.
6. Wait for it to finish and use the recommended settings, press next.
7. If you like you can rename the printer here, press next.
8. Select if you want to share the printer or not, press next.
9. Your printer should now work, press **Print a test page** to test it.

Adding Printer with vendor-specific drivers

To get all features working on a printer, such as a scanner, vendor-specific drivers are needed. The process varies from vendor to vendor but most installers have an option to find the printer with IP-address. Either it's done during the install process or after the installation is finished.

Frequently Asked Question (FAQ)

Q: No keyboard shortcut seems to work at all.

A: You're at the initial login screen. The shortcuts don't (and shouldn't) work until you have successfully logged in.

A: Make sure you don't move the mouse between the presses, then the focus gets back to the guest OS.

Q: Sometimes when I press the power button nothing happens.

A: This happens when the system is still processing some earlier power button event. Make sure you have answered all power button dialogues and that any action ordered has finished.

Q: I run Windows as guest OS, and when I commit on one side, I get the wrong wallpaper on the other side.

Q: I run Windows as guest OS, and when I do a restore on the side where I did not do the latest commit, I get the wrong wallpaper.

A: This is due to Windows insisting on keeping cached versions of the wallpaper on the system disk, even if the actual wallpaper image is stored elsewhere.

For now, in these specific situations, enter settings and reselect the wallpaper that was supposedly already set. Alternatively, make a habit to remove these caches before committing, but this is easy to forget.

Q: I run Windows as guest OS, and whenever I start one of the sides, the system complains about not being able to reconnect all network devices (specifically either "open" or "secure").

A: Since Windows keeps the information about which network devices to connect to on the system disk, we end up having to specify both the shared disk networks on both sides, one of which _should_ fail to connect. This is somewhat annoying, but the alternative would be to set it up manually whenever you want to use it.

Q: When I (try to) connect to a certain ISP or to a certain local network, there are network problems.

A: The InproaHST system uses a few private networks for internal communication between the host and the virtual machines. If the private address you get from the ISP or the local network conflicts with these, there will be problems. While the internal networks have been given addresses that are rarely used, there can be no guarantee that this won't happen. In the unlikely event that it does, the conflicting network(s) will have to be moved. As yet, this has to be done manually.

Q: I have used the USB Rules Editor to allow a new USB device, but it still doesn't get connected to the guest.

A: There are a few things involved in getting a USB device to work on the guest.

1) Write and save the rule.

2) Get the rule to actually be used. To do this you need to restart the virtual machine viewer since it doesn't reload new rules on the fly.
Conceptually, the easiest way to do this is to just restart the guest.
The least intrusive way is to only restart the viewer itself.

3) Get the device to be recognized as a valid one. The check for this is done when it is connected, so you normally have to remove and reinsert it after the above steps. (If it is a fixed device, reboot...)

4) Make sure you haven't run out of USB redirection channels. If you have, any further devices connected will be silently ignored even if perfectly valid.

Q: When switching back and forth between the guests, USB devices get disconnected.

A: This is a normal consequence of how USB communication is handled. If the device has a hotplug only rule, you will need to remove and reinsert it if you want to continue using it.

Q: When switching back and forth between the guests, their clocks lag behind.

A: This is due to their clocks not running when they're suspended. Depending on how the guest OS handles clock adjustments, this may or may not sort itself out in reasonable time even if a time server is used. (It is quite common to allow large jumps only at start-up.)

Key commands

Generally: If you are in one of the virtual machines, you first have to release the focus from it with a separate **<Ctrl> + <Alt>** before the actual key command.

By “separate” is implied that you have to release the keys before doing the key command, so that you end up doing two separate presses. If you aren’t in a virtual machine, you don’t have to do this, but it also does no harm, so you may do it anyway if it feels simpler to do it the same way all the time.

NOTE: The key commands don’t work if caps lock or num lock is active, easy to miss...

<ctrl> + <alt> + n = go to the next window

<ctrl> + <alt> + tab = go to the next window

<ctrl> + <alt> + o = go to the Open Machine (starting it if needed)

<ctrl> + <alt> + s = go to the Secure Machine (starting it if needed)

<ctrl> + <alt> + m = go to the manager (with GUI interface for some of this)

<ctrl> + <alt> + d = go to the first dialog waiting for response

<ctrl> + <alt> + x = start a new xterm (a terminal for the host)

<alt> + <ctrl> + t = xterm (root)

<alt> + <ctrl> + h = host status

<alt> + <ctrl> + p = prepare license

<alt> + <ctrl> + l = license check

<alt> + <ctrl> + a = airplane mode (if available)

Note that **<Ctrl> + <Alt> + O/S** will prioritize going to any unanswered dialog for the machine in question rather than the machine window itself.

The power button is handled in a context dependant way. When pressed while inside a virtual machine, you will be asked what to do with the machine. If pressed outside of any virtual machine, it will check for reasons why a shut-down would not be advisable, and if any is found, inform you about it. If no such reason is found, it will do a system-friendly shutdown of the system.

3’d party tools

In order to work efficently in a the SDL system, some 3’d party tools might be necessary. We will cover the process of saving webpages for offline viewing in the Secure machine, and how to communicate in the Secure LAN-network.

Saving online webpage for offline viewing on Secure Machine

In order to view webpages on the Secure Machine, you first have to download them with your browser. The easiest way to do this is via a browser plugin.

Saving a webpage as HTML

This is the most comprehensive way to save a webpage for offline viewing, but it takes a bit longer than saving as PDF.

1. Add the plugin SingleFile for your broswer:

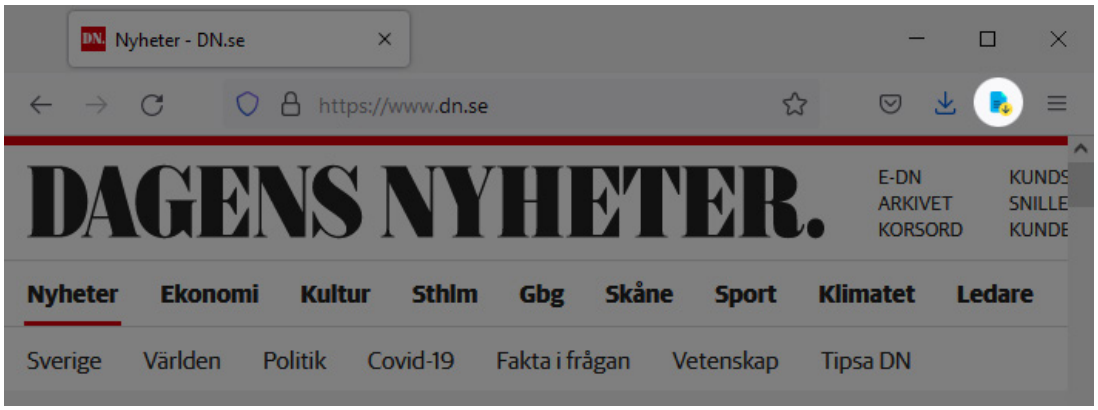
   Firefox: https://addons.mozilla.org/en-US/firefox/addon/single-file/

   Chrome: https://chrome.google.com/webstore/detail/singlefile/mpiodijhokgodhhofbcjdecpffjipkle?hl=en

   Edge: https://microsoftedge.microsoft.com/addons/detail/singlefile/efnbkdcfmcmnhlkaijjjmhjjgladedno

Usage

2. Go to the webpage you want to save.



3. Press the small blue document icon in the top right corner of your browser.
   - A small window will appear in the bottom left corner of your browser, when it dissapears it's done.
4. Your saved webpage is now downloaded to your **Downloads** folder.
5. Move the saved webpage from the **Downloads** folder to the **Share** folder.
6. Start the Secure Machine and open your saved webpage from the **Share** folder.

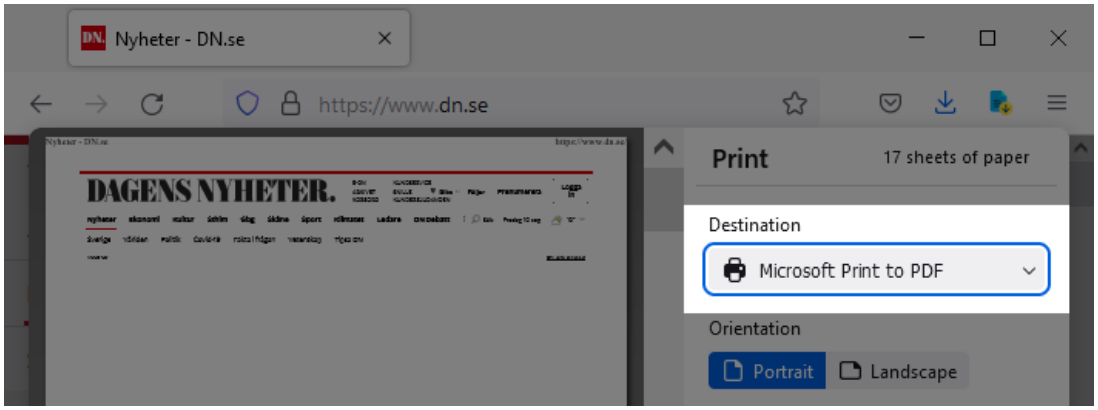
Continues on the next page...

Saving a webpage as PDF

This is the fastest way to save a webpage for offline viewing.

Usage

2. Go to the webpage you want to save.
3. Choose **Print** from the menu (or press **Ctrl + P**).



4. In the print dialogue window, choose **Microsoft Print to PDF**.
5. Press **Print** and save your PDF on the Share-drive.
   When the print dialogue dissaperars the saving is done.

Messaging coworkers in the same LAN-network

For easy and secure communications within the LAN-network, a LAN-messaging application can be used, we will list a few different options and the ports that need to be opened on the host to make them work.

1. **Lan-Messager**

   Simple, open source and free.

   Requirements:
   Open ports TCP 50000, UDP 50000 on host.

   Download: http://lanmsngr.sourceforge.net/

2. **Pidgin**

   More advanced features, supports many protocols.

   Requirements:
   Bonjour print services: https://support.apple.com/kb/DL999
   Open ports TCP 5222, 5269, TLS 5223 on host.

   Download: https://www.pidgin.im/install/

3. **Softros LAN-Messager**

   Easy-to-use paid service with support.

   Requirements:
   Open ports TCP/UDP 19771, 19880 on host.

   Download: https://messenger.softros.com/downloads/

4. **Mattermost**

   More advanced commiunication suite that supports group chats, file sharing and all other modern features one would expect.

   Requirements: Runs as a self-hosted server.

   Download: https://mattermost.com/pricing-self-managed/