Introduction to IMPEX USB Protect

SYSCTL AB

Table of Contents

1 Introduction to Impex

This document is an introduction to Impex, a security control used for managing removable digital media (USB memory sticks, SD cards, removable hard drives, floppy disks, DVD's, etc).

The introduction is both a user guide and a quick overview of the device. In the text we describe a number of uses and practical steps on how to use Impex.

The Impex station is a physical unit with two USB ports on the front to which one attaches removable media that one wants to verify that it is free from malicious code.

Impex has been developed to examine or check all files on a digital media. Normally one uses two removable media with Impex, one that is source media and another that is target media. Files are read from the source media and are then examined. If no malicious code is found, the files are then copied to the target media. Before the files are copied the target media will be formatted and emptied from all content. This is done to avoid having a mix between unchecked files and newly copied, checked, files.

In this introductory text we will give an example on how to copy files between two media. There will also be examples on how to explicitly empty (format) a USB memory, and another to empty it more securely (shred). Another example is to check a USB-drive without actually copying it between two ports.

Since Impex must be easy to use and easy to understand, we have implemented support for more than 15 languages in the Impex interface. In this document we will describe how to change language in the graphical user interface. We will also describe how you can view various settings on an Impex station.

1.1 How Impex works

The Impex station works with multiple antivirus engines and in multiple passes. This will result in that a file will be read multiple times. Exactly how many times a file is read or how many antivirus engines are checking the files will depend on a number of items, including how many AV engines are configured on a specific Impex station and how certain configuration parameters are set in the administration server, ICC.

Since Impex reads files multiple times there can be issues with large digital media, media with many or large files, or with legacy, slow removable media. In the worst case there can be combinations of these which in turn will result in long execution times and long times to perform the checks and controls. One way to try to speed things up is that Impex will try its best to always copy files to a temporary storage on an internal storage device with very good performance. To display that there is progress with the examination, the Impex station will display a progress bar at the bottom of the screen.

1.2 Impex and ICC

One or more Impex stations is connected to a server, called Impex Control Center, ICC. From the ICC one can set parameters in the Impex station. Depending on prior changes that have been done with ICC, the Impex station that you have access to might look different, behave differently and deliver different results.

An Impex station sends information to the ICC. An example of information sent is the scan record and metadata of files and scannings. Another example is audit logs on who is using the station and what actions they are doing.

1.3 Impex and peripherals

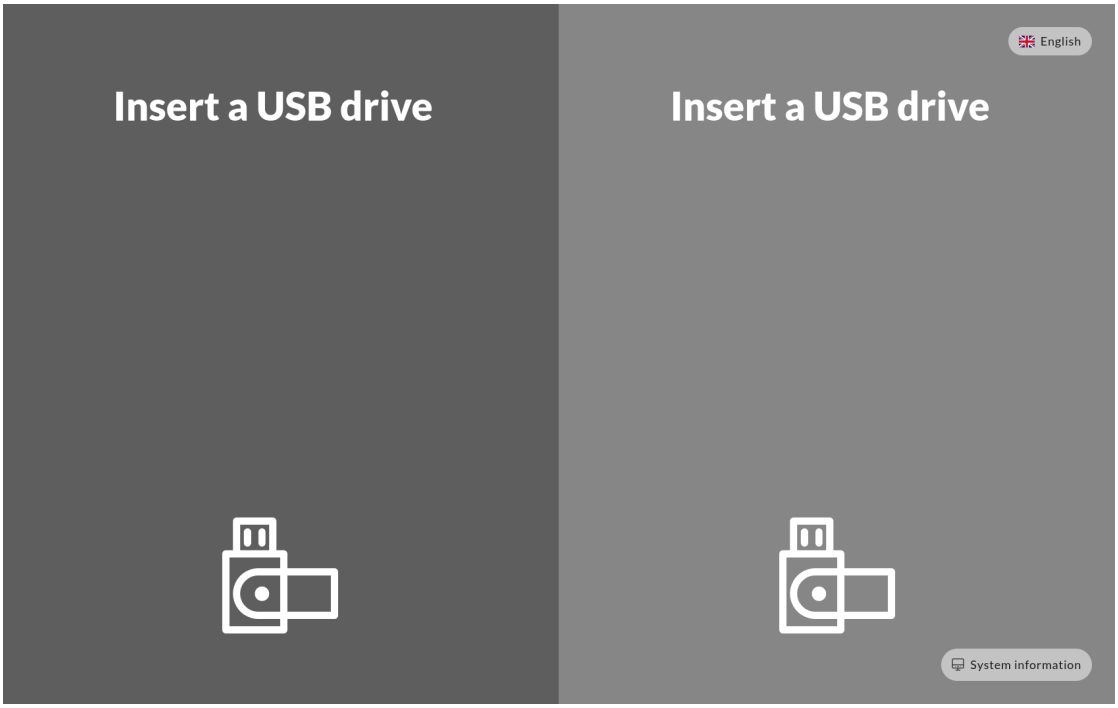
Impex can be equipped with many peripherals or auxiliary additions. One common example is the addition of a receipt printer, that will be used to print physical evidence that a scan has taken place. Other additions and peripherals include wall mounts, various media as well as a DVD reader or a SD card reader.

1.4 Using Impex in your organisation

Many organisations have developed special policy documents, handbooks and routines for how removable media can or is allowed to be used, how they should be examined, how they need to be protected, etc. It is important that you are informed and have competence on what types of media is accepted as permitted media, which can be used as source or target devices, what one should do if Impex is alarming that it has detected malware, and how you should handle digital or physical receipts from Impex.

2 Scan and transfer files from one USB drive to another

This chapter contains a step-by-step guide for scanning mobile media, e.g. a USB drive, to examine if there is malicious content on it, like computer viruses, trojan horses or other malware. If no malware is found, it transfers the content to a second USB drive.



Initial screen

In the following example the source media is attached to the left port. IMPEX will of course support having the source media or the target media attached to any of the ports. This flexibility can be changed from the administration server ICC to make certain media usable only in certain ways.

Before you start, you will see a generic screen welcoming you to insert your media into the Impex station. At this point in time, it is also possible to change the language that is used for all dialogues. Impex is available in most major languages.

1. Insert the source media (usb drive) into the left port

2. Insert the destination media or target drive in the right port

The screen should now display both of the drives, their brand, model name and serial number. Note that if the serial number is longer than 30 characters it will only show the last 30 characters.

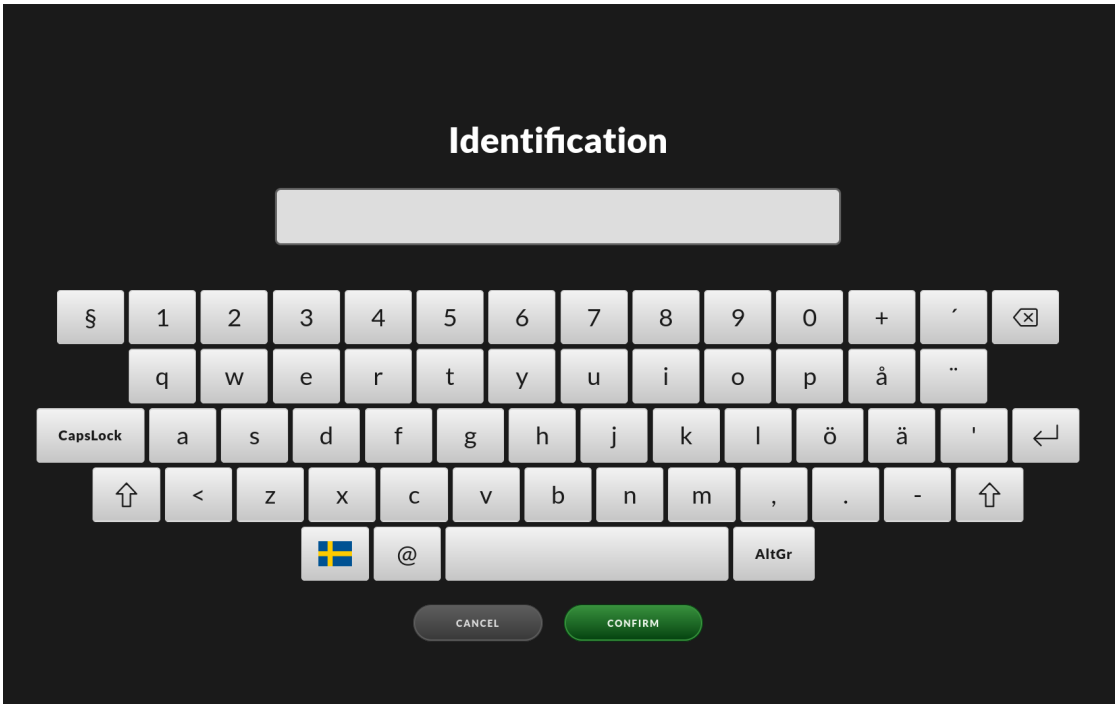
Press the “View Content” button to look at the actual files on the drive.

Two drives connected

3. Press on the left arrow to transfer the files to the right side drive

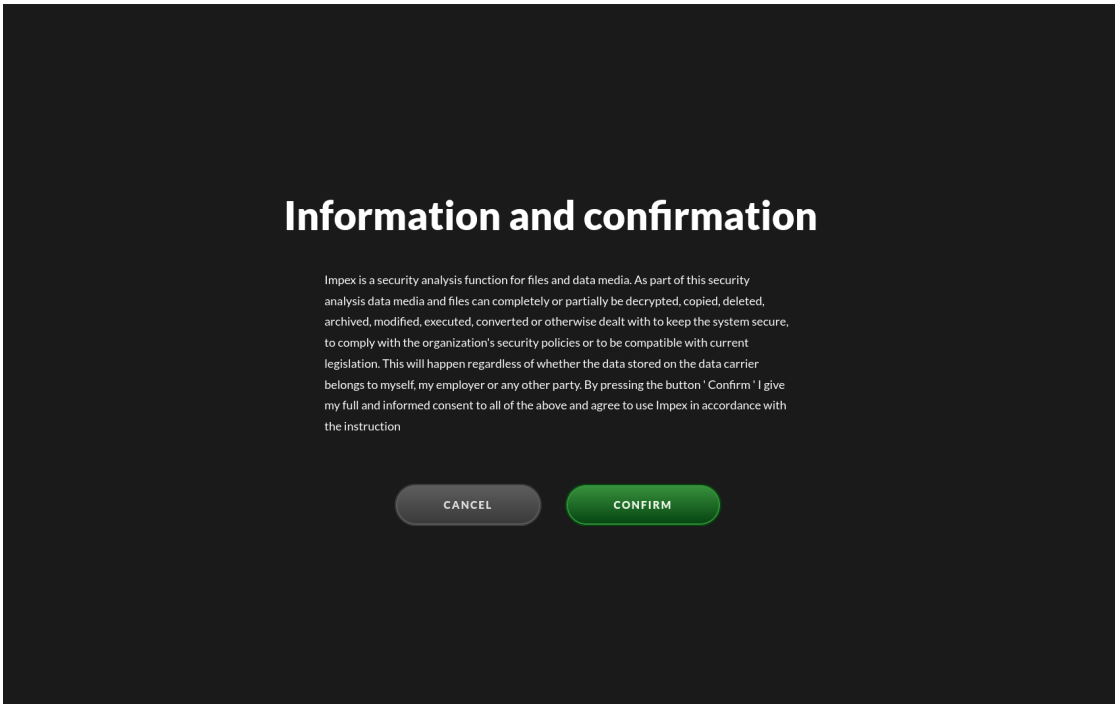
Please note that the right side drive will be erased and cleaned (formatted) to make sure it is empty. If the source drive is a CD or DVD the target drive file system will be **exfat**.

4. Depending on your local security policy you might have to enter your identification using the on-screen keyboard and press a confirm button to continue



The identification screen

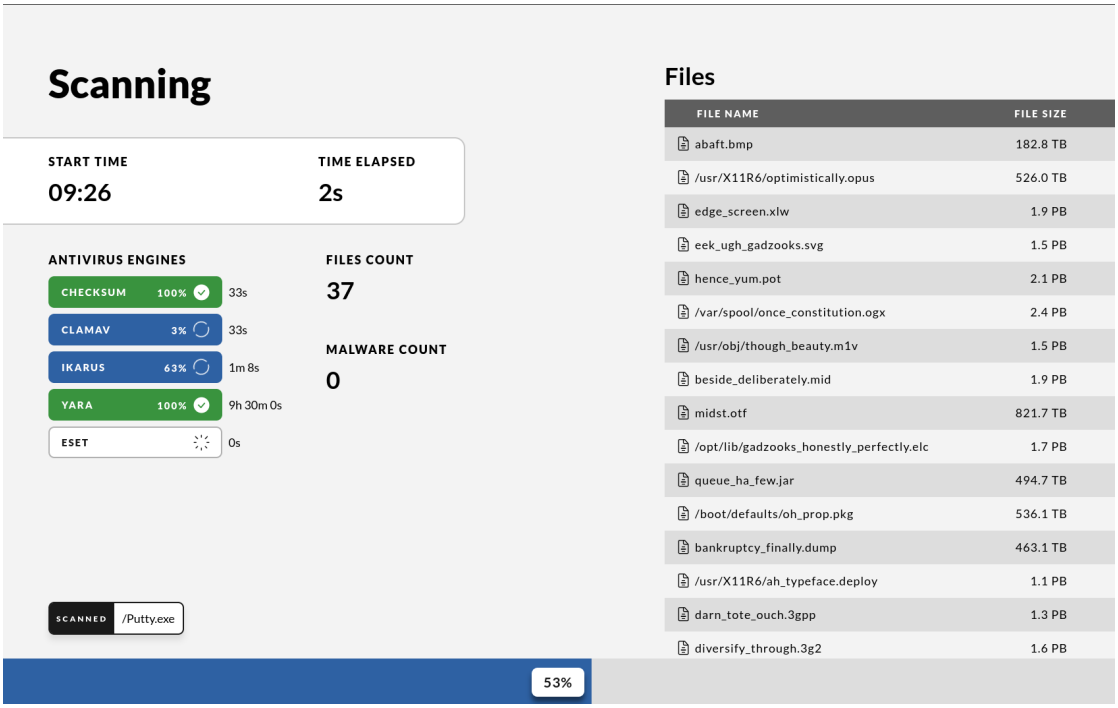
This is a pop-up screen on which you need to fill in your email address. If the Impex has been configured to, there might also be a list of preloaded names to choose from, making it easier, and faster, for users to use the identification screen. This will work as the following - you start to fill in the name, but as soon as your name is determined to be one of the computer's internal list, it will show you the names that start with the characters you have entered. If the name is on the list, you can easily just select it by pressing a finger on the touch screen on the name, and the name will be filled in automatically in the Impex station name form.



The confirmation screen

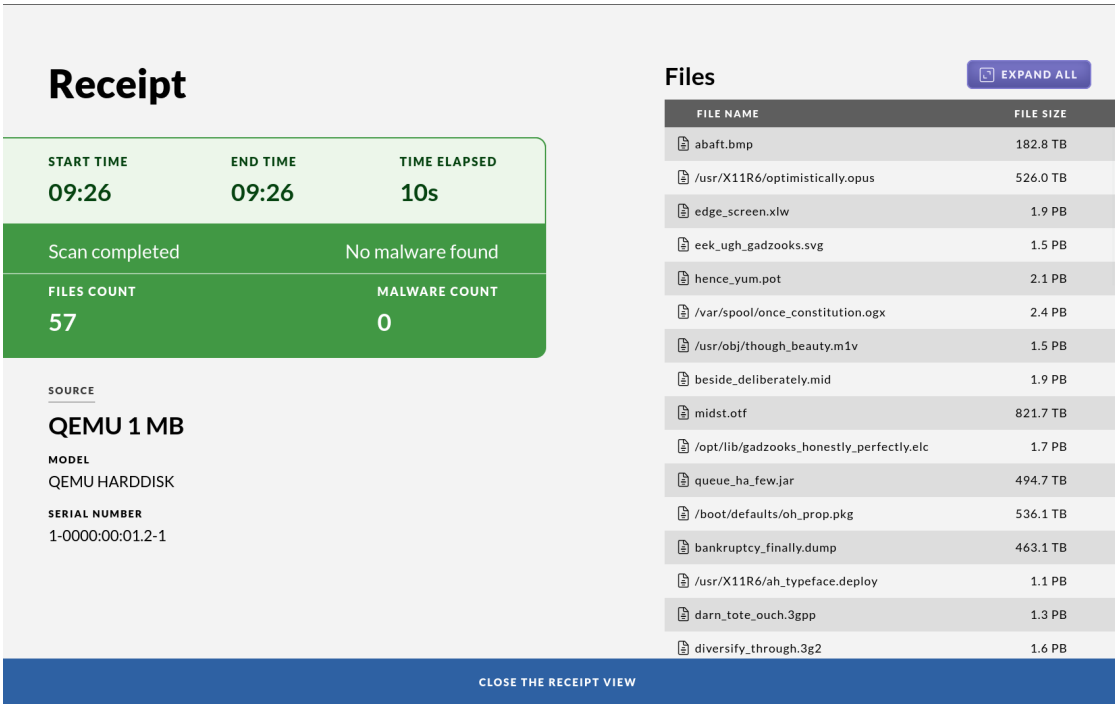
The confirmation screen will display some information describing the process used by, and the action taken by, Impex. It asks you to read and acknowledge this information before proceeding.

The files on your source USB drive will now be analysed for virus, malware and other unwanted software. During this process a progress bar will be shown depicting a rough estimate on how much time is left.



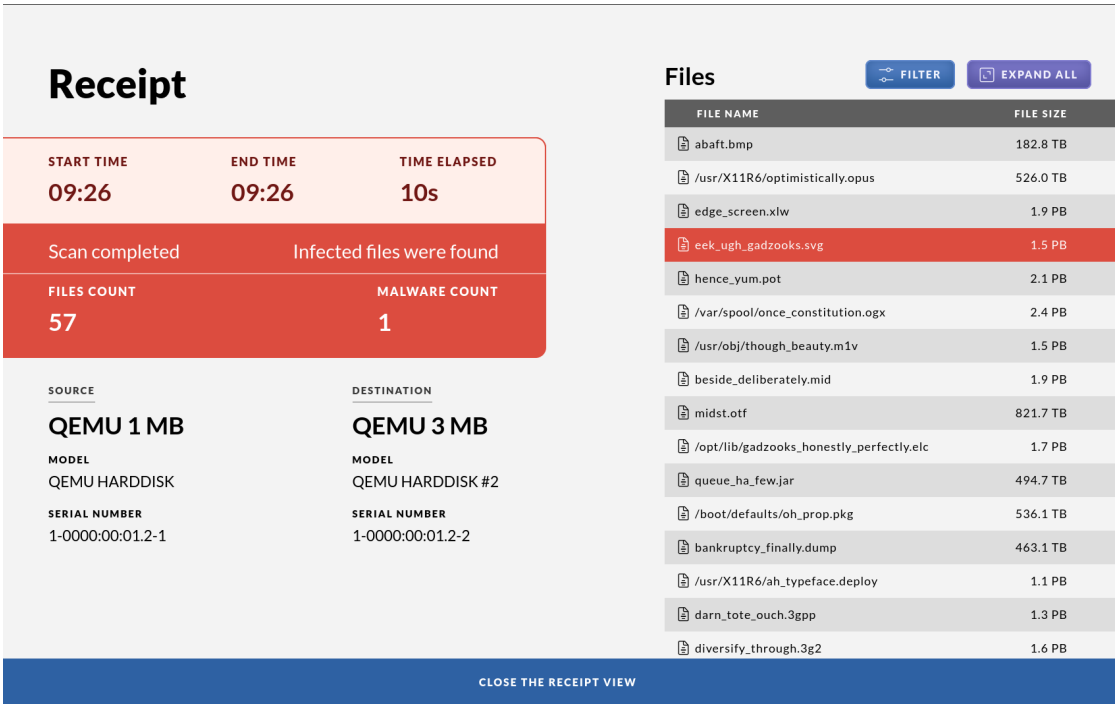
The progress bar

If nothing malicious was detected you will see a green screen together with a receipt which gives an overview of which files were scanned and their unique checksums. If a printer is attached and enabled you will also get a printout of a summary.



The summary screen

In the case that unwanted files were detected the screen will go red and a listing will show which file or files contained malware. Note that in this case no files will be transferred so the target USB drive will still be clean. If a printer is attached and enabled you will also get a printout. To view only the malicious files, press “Filter”. The source drive containing the malicious files will not be modified or cleaned by the system.



Screen when malware was detected

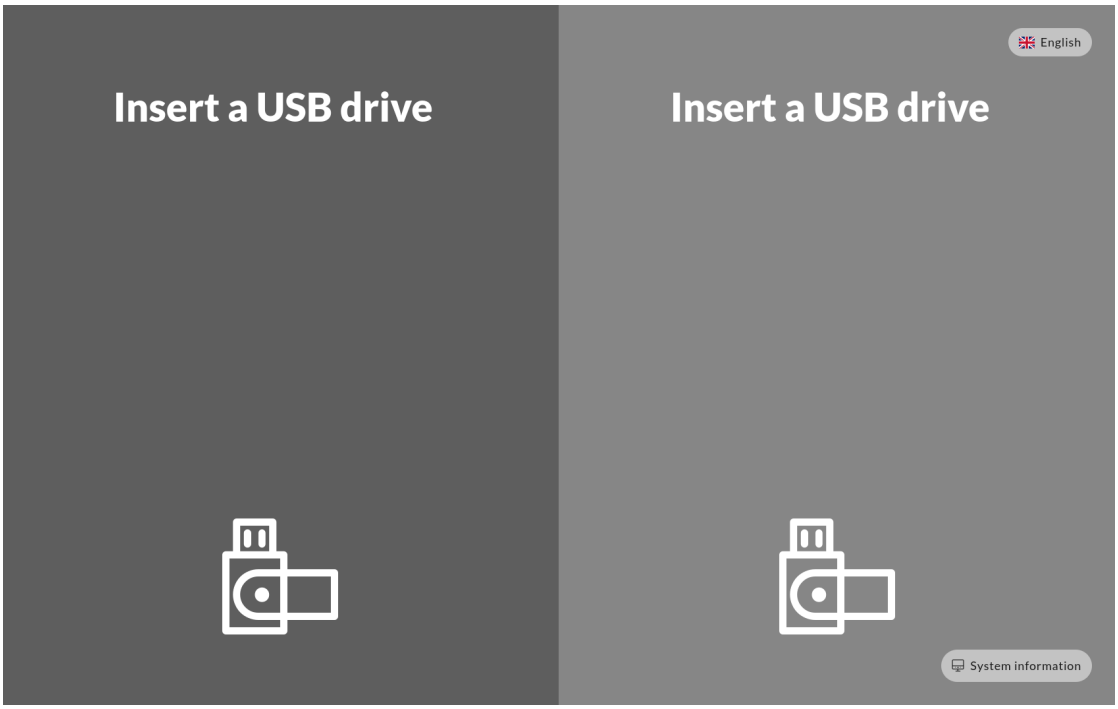
Your local security policy should dictate what to do with the source USB drive in case malware is found.

5. To complete the scanning press “Done” and pull out the USB drives

If at any point you want to abort the procedure, pull the USB drives. It is also worth mentioning that the station does not require you to copy from left to right. The process can also be done in the other direction. That means you can also transfer files from right to left. The files will be analysed and scanned before being copied, no matter in what direction they are copied to. This can in certain situations be more intuitive depending on the physical placement of the IMPEX station.

3 Scan/transfer from a bitlocker USB drive to another device

This chapter contains a step-by-step guide for scanning mobile media, e.g. a USB drive, to examine if there is malicious content on it, like computer viruses, trojan horses or other malware. If no malware is found, it transfers the content to a second USB drive.



Initial screen

In the following example the source media is attached to the left port. IMPEX will of course support having the source media or the target media attached to any of the ports. This flexibility can be changed from the administration server ICC to make certain media usable only in certain ways.

Before you start, you will see a generic screen welcoming you to insert your media into the Impex station. At this point in time, it is also possible to change the language that is used for all dialogues. Impex is available in most major languages.

1. Insert the source media (usb drive) into the left port

2. Insert the destination media or target drive in the right port

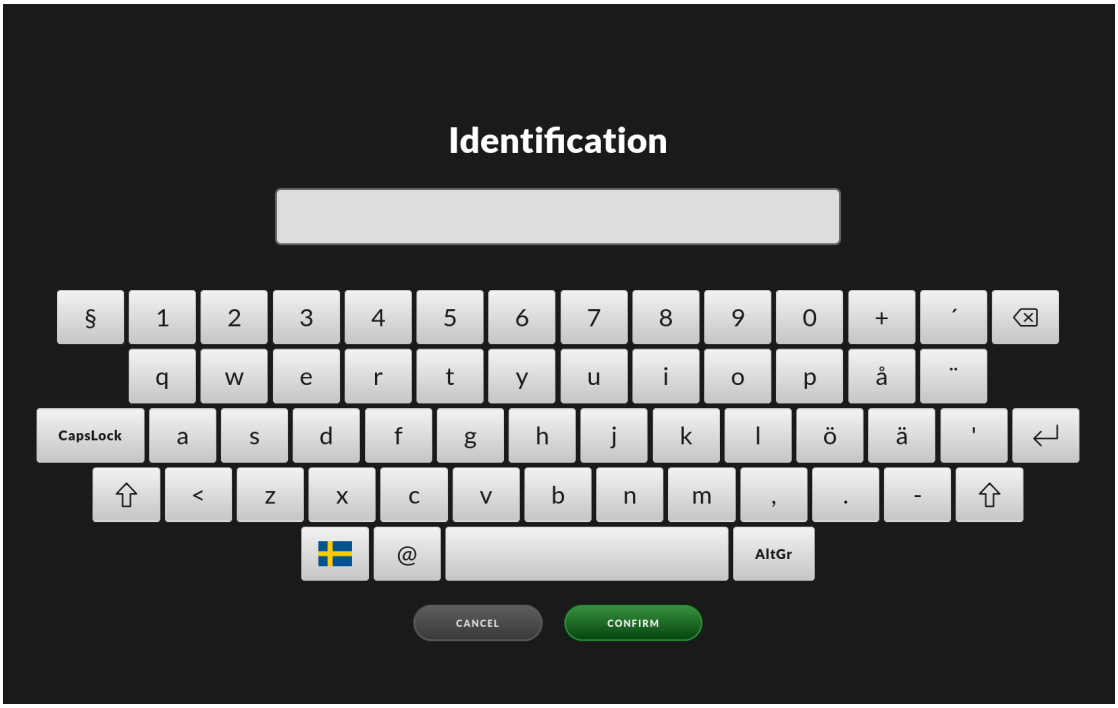
The screen should now display both of the drives, their brand and model name. Press the “View Content” button to look at the actual files on the drive.

Two drives connected

3. Press on the left arrow to transfer the files to the right side drive

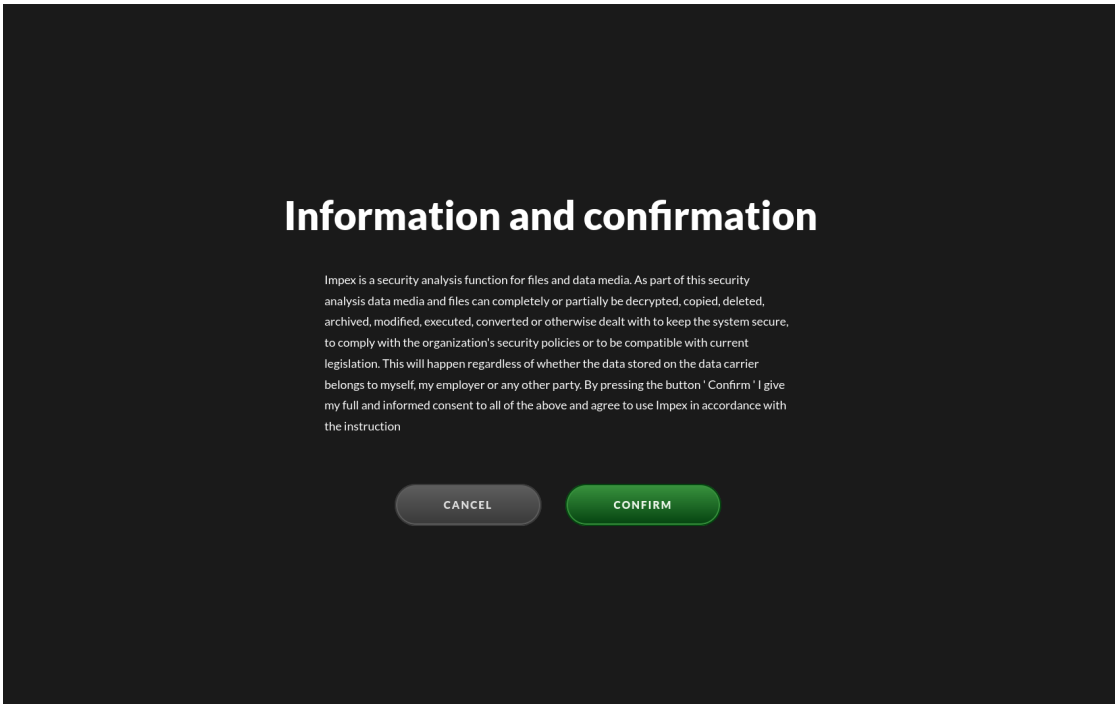
Please note that the right side drive will be erased and cleaned (formatted) to make sure it is empty. If the source drive is a CD or DVD the target drive file system will be **exfat**.

4. Depending on your local security policy you might have to enter your identification using the on-screen keyboard and press a confirm button to continue



The identification screen

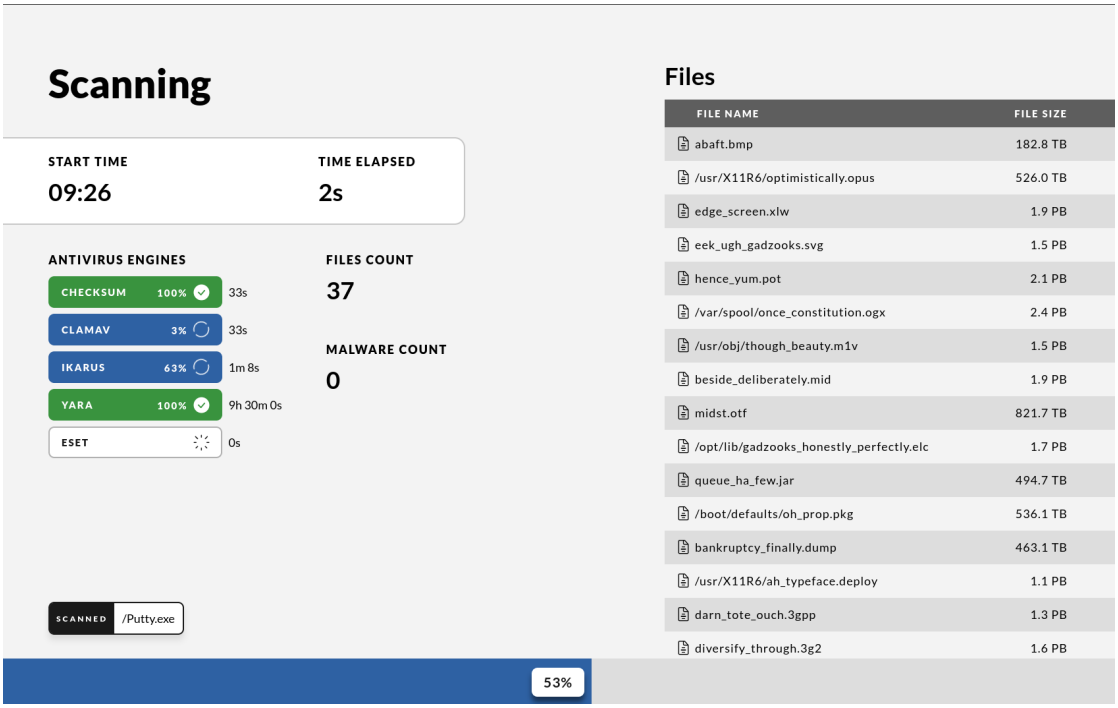
This is a pop-up screen on which you need to fill in your email address. If the Impex has been configured to, there might also be a list of preloaded names to choose from, making it easier, and faster, for users to use the identification screen. This will work as the following - you start to fill in the name, but as soon as your name is determined to be one of the computer's internal list, it will show you the names that start with the characters you have entered. If the name is on the list, you can easily just select it by pressing a finger on the touch screen on the name, and the name will be filled in automatically in the Impex station name form.



The confirmation screen

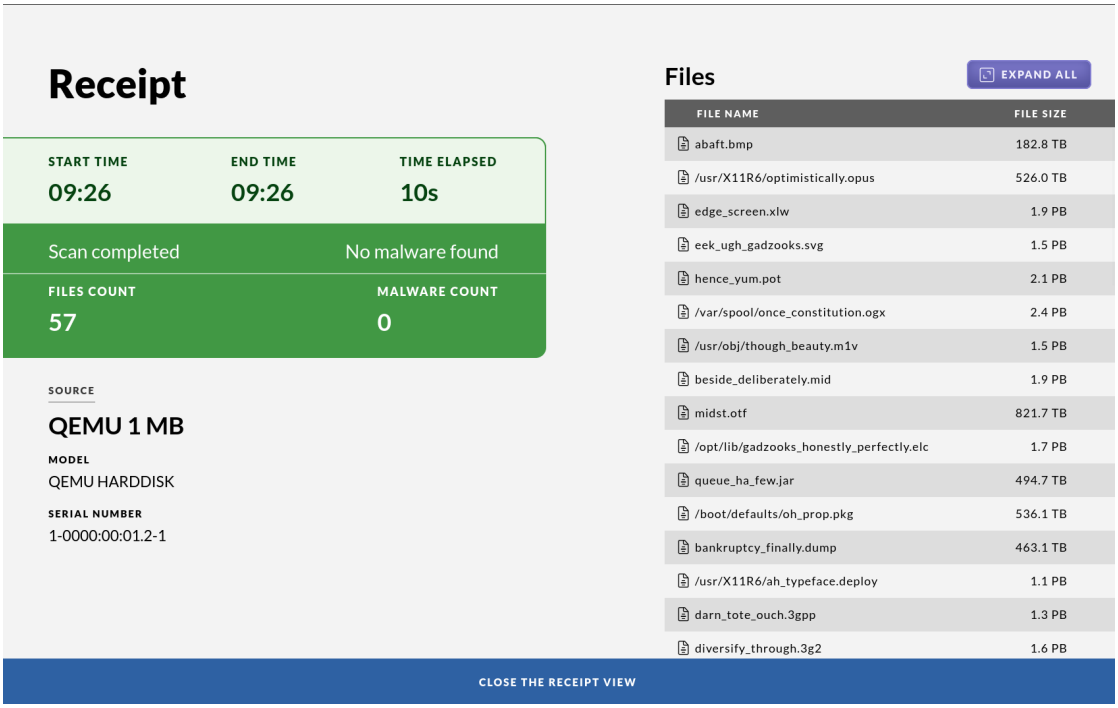
The confirmation screen will display some information describing the process used by, and the action taken by, Impex. It asks you to read and acknowledge this information before proceeding.

The files on your source USB drive will now be analysed for virus, malware and other unwanted software. During this process a progress bar will be shown depicting a rough estimate on how much time is left.



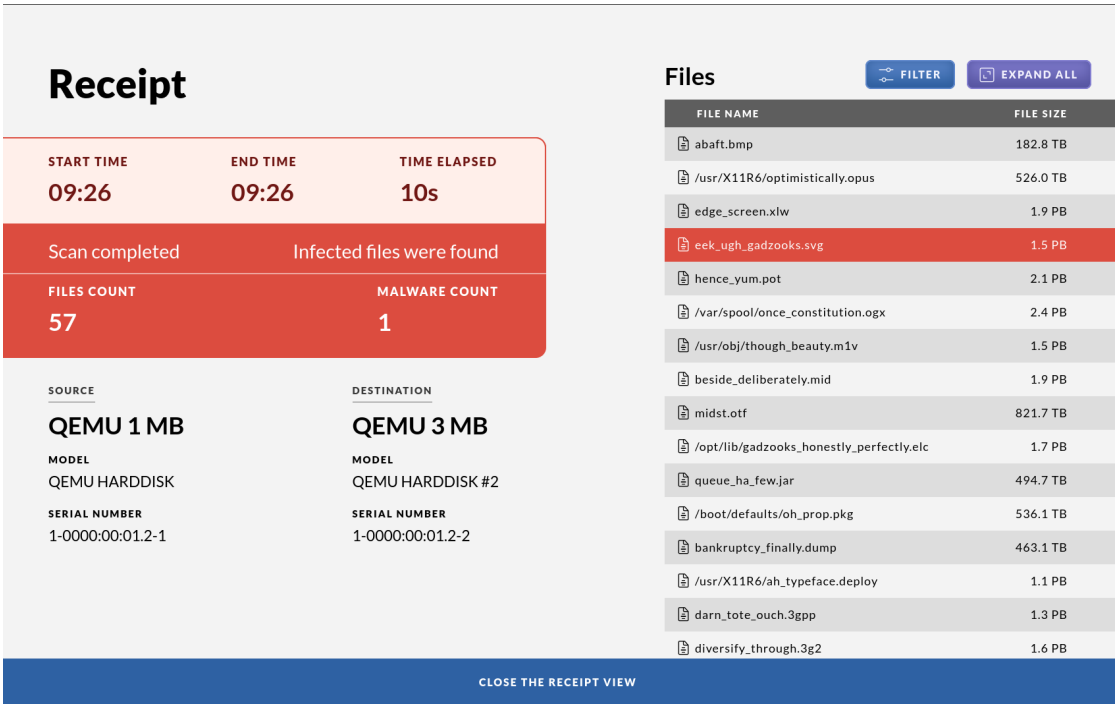
The progress bar

If nothing malicious was detected you will see a green screen together with a receipt which gives an overview of which files were scanned and their unique checksums. If a printer is attached and enabled you will also get a printout of a summary.



The summary screen

In the case that unwanted files were detected the screen will go red and a listing will show which file or files contained malware. Note that in this case no files will be transferred so the target USB drive will still be clean. If a printer is attached and enabled you will also get a printout. To view only the malicious files, press “Filter”. The source drive containing the malicious files will not be modified or cleaned by the system.



Screen when malware was found

Your local security policy should dictate what to do with the source USB drive in case malware is found.

5. To complete the scanning press “Done” and pull out the USB drives

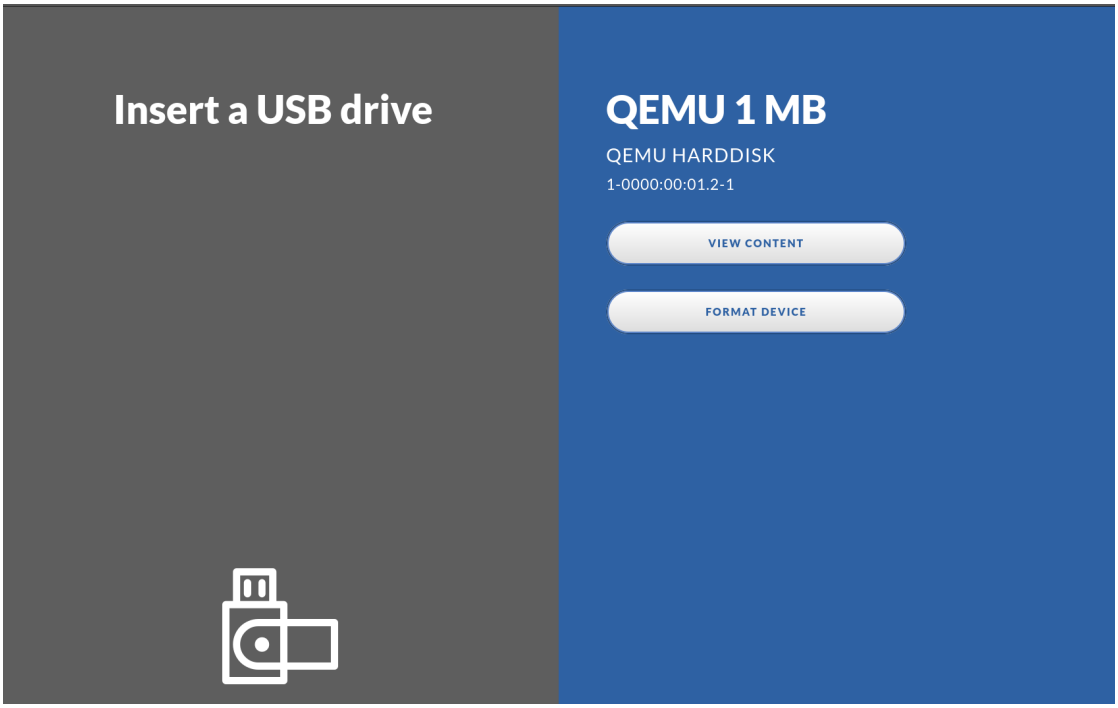
If at any point you want to abort the procedure, pull the USB drives. It is also worth mentioning that the station does not require you to copy from left to right. The process can also be done in the other direction. That means you can also transfer files from right to left. The files will be analysed and scanned before being copied, no matter in what direction they are copied to. This can in certain situations be more intuitive depending on the physical placement of the IMPEX station.

4 Format a USB drive

If the "Allow format only" option has been enabled in the IMPEX Control Center one can also use the IMPEX station for formatting a USB drive. If the option is turned on the "Format device" button appears when just one drive is inserted. It does not matter in which port the drive is inserted.

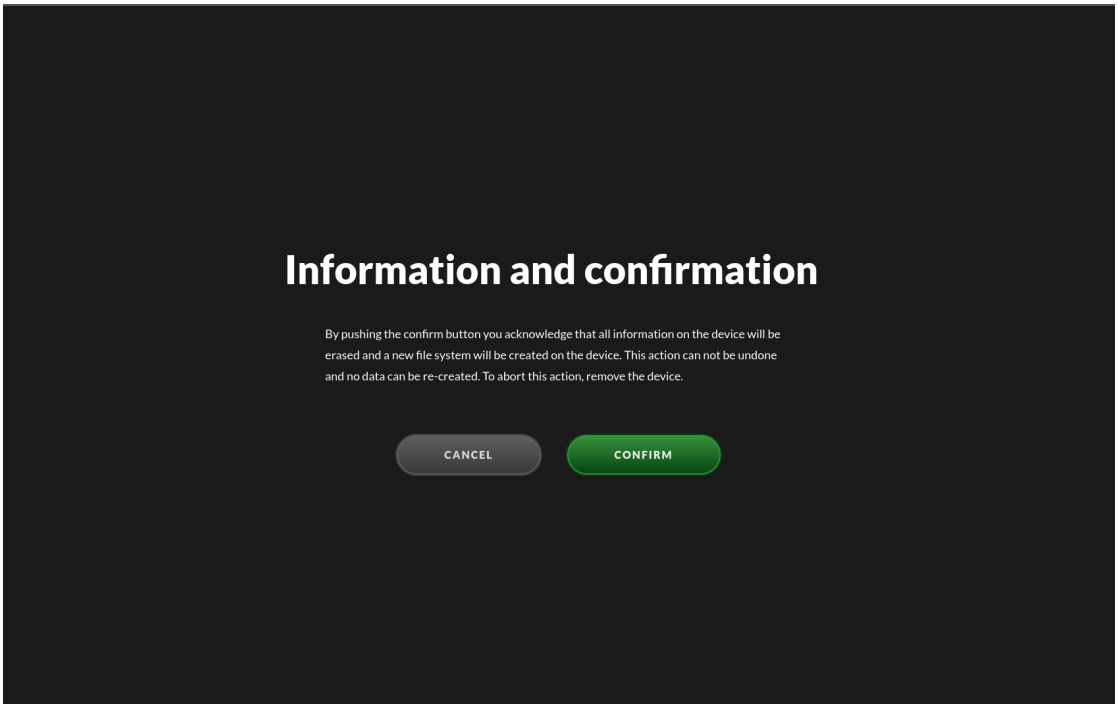
4.1 Format a Bitlocker drive

When formatting a bitlocker drive one can format it in two ways. If the Bitlocker password is entered, the filesystem *inside* the Bitlocker container will be formatted as NTFS. If the Bitlocker password is not entered, by pressing "cancel", the entire drive will be formatted and the Bitlocker container will thus be wiped, turning the drive into a normal USB drive.



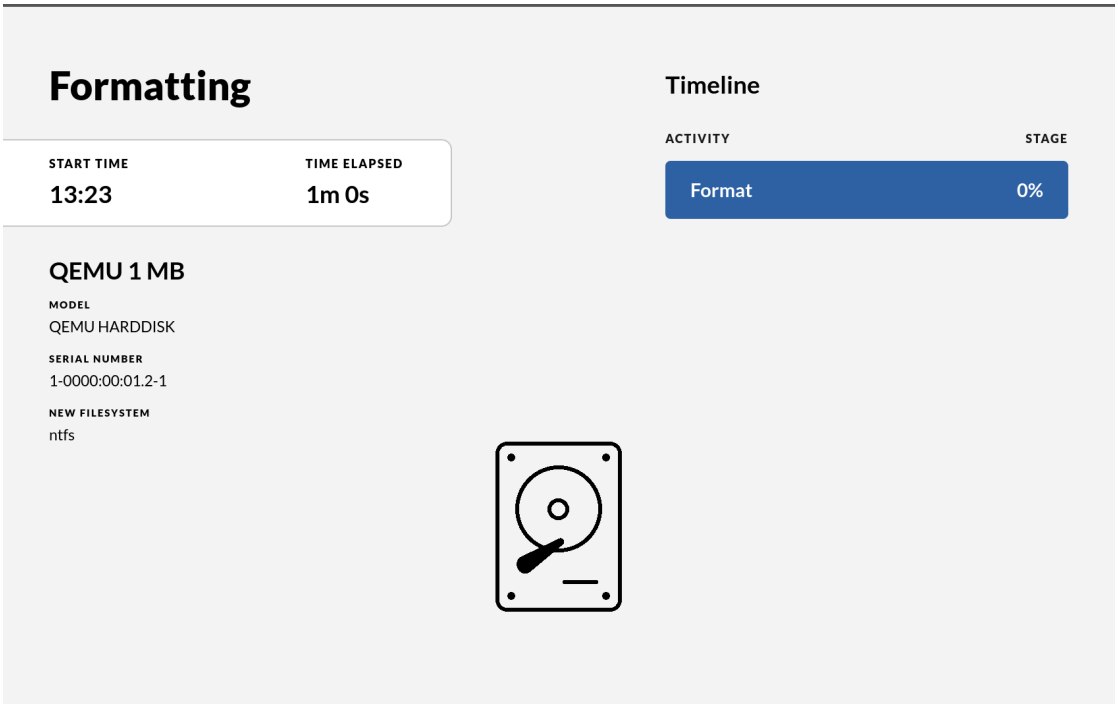
View after inserting a drive in the right side port

1. **Insert a USB Drive**
2. **Press the "Format Device" button**
3. **Read the text and then press "Confirm"**



The confirm screen

This screen will display text describing the actions you are about to take. If you click on “confirm”, the next step will be to format the attached USB drive. If you have changed your mind, or performed this action in error, just remove the attached USB device to interrupt the formatting.

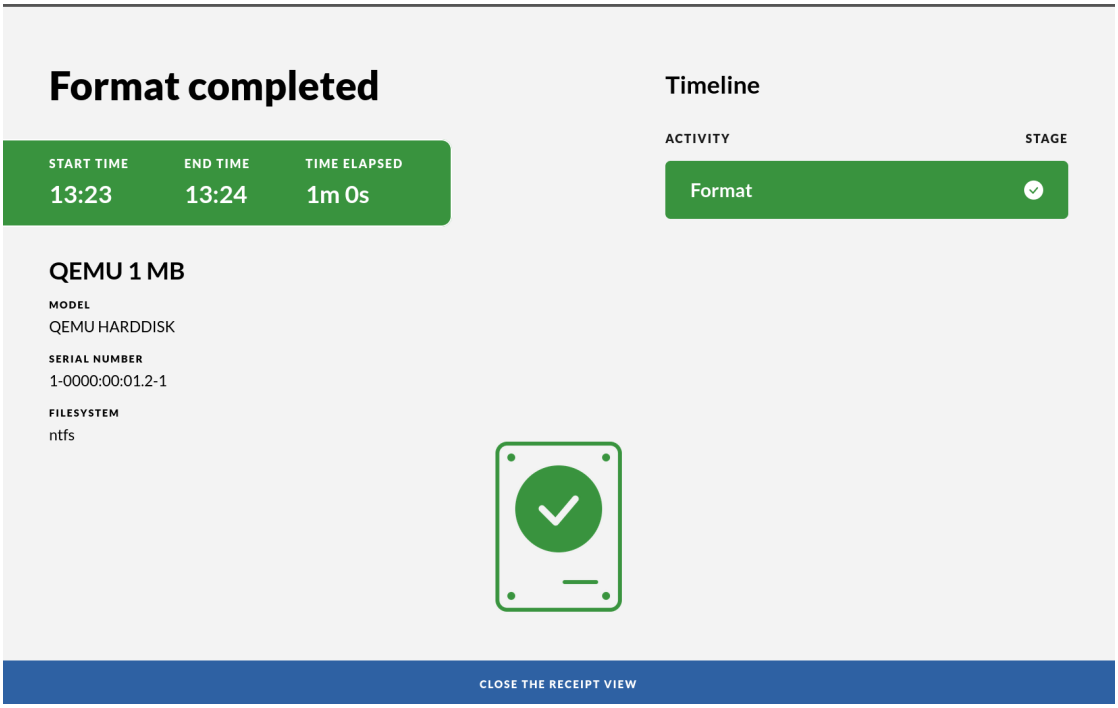


The progress screen

The progress bar is a measure that will display the progress of the actual formatting

After acknowledging that the user understands that the USB drive will be erased and all information on it will be lost the drive will be formatted and a new **FAT32** file system created on it. If the drive is larger than 2TB it will be partitioned with **GPT** and the file system will be **exfat**. The default file system **FAT32** can be changed in the ICC to be always **exfat** or always **NTFS**.

After the process is complete the final view will contain a receipt showing information about the drive.



The receipt screen

The receipt is shown on the screen. The receipt contains important information, including:

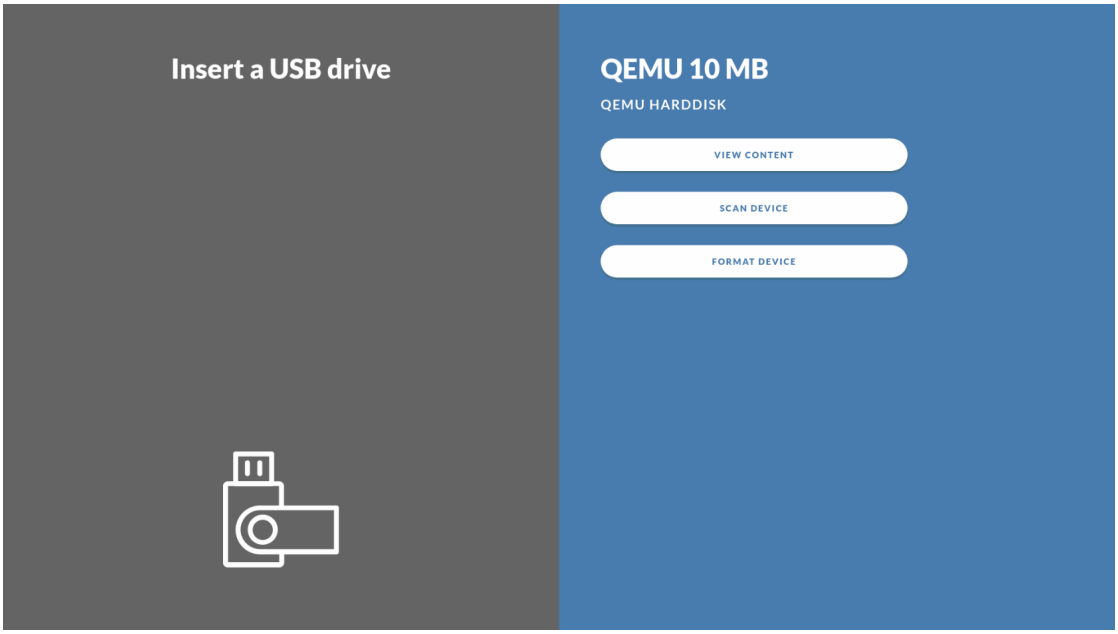
- brand and model of the attached usb devices
- name of the attached usb devices
- file system used when formatting
- serial numbers of the attached devices

4. Press “Done” and remove the USB drive

The USB drive is now formatted and clean, ready for use.

5 Scan one USB drive

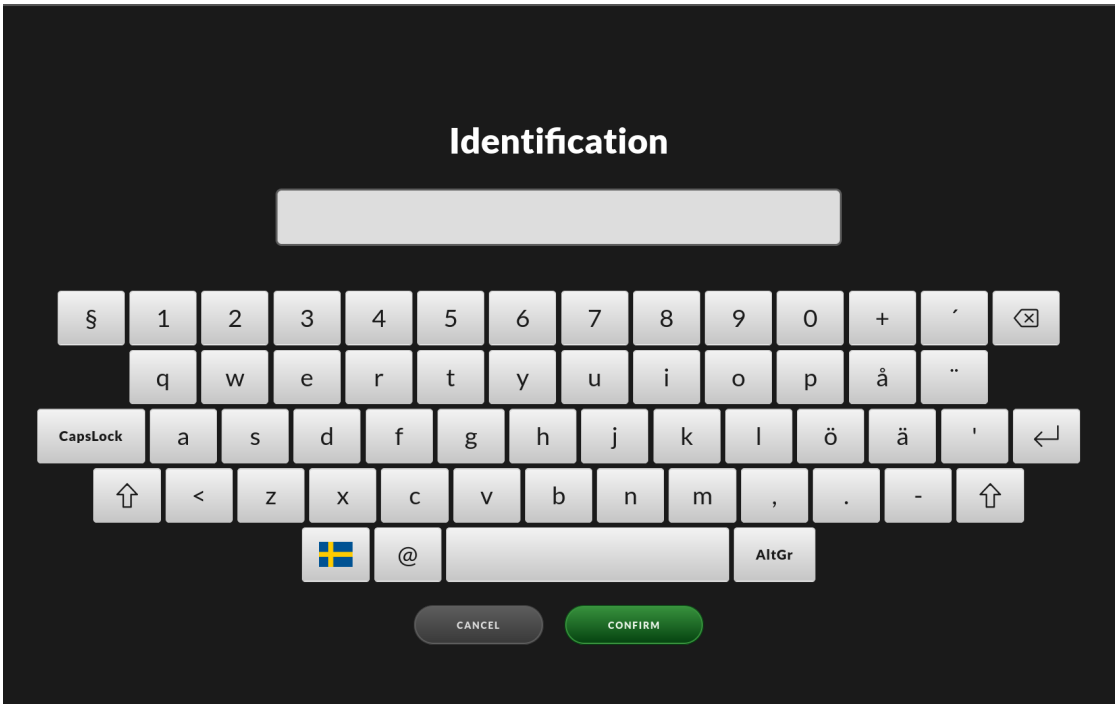
If the “Allow scan only” option has been enabled in the IMPEX Control Center one can also use the IMPEX station for scanning a USB drive without transferring any files. If enabled, a “Scan Device” button appears when only one drive is inserted. It does not matter in which port the drive is inserted.



View after inserting a drive in the right side port

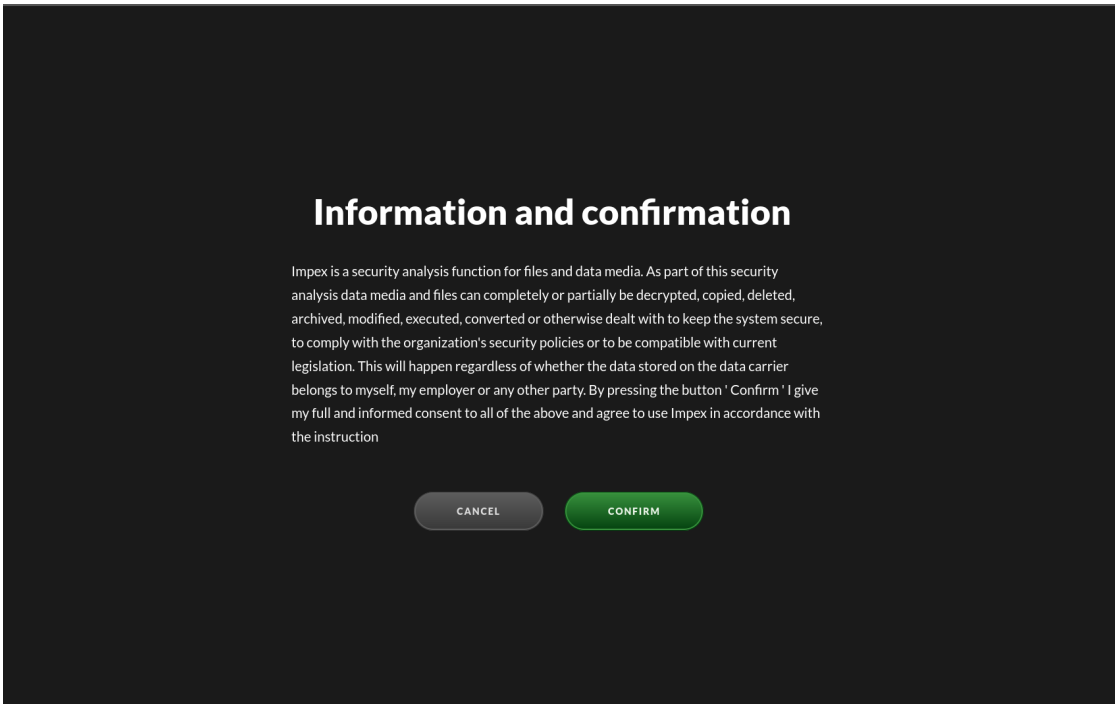
1. **Insert a USB Drive**
2. **Press the “Scan Device” button**

Depending on your local security policy you might have to enter your identification using the on-screen keyboard and press a confirm button to continue.



The identification screen

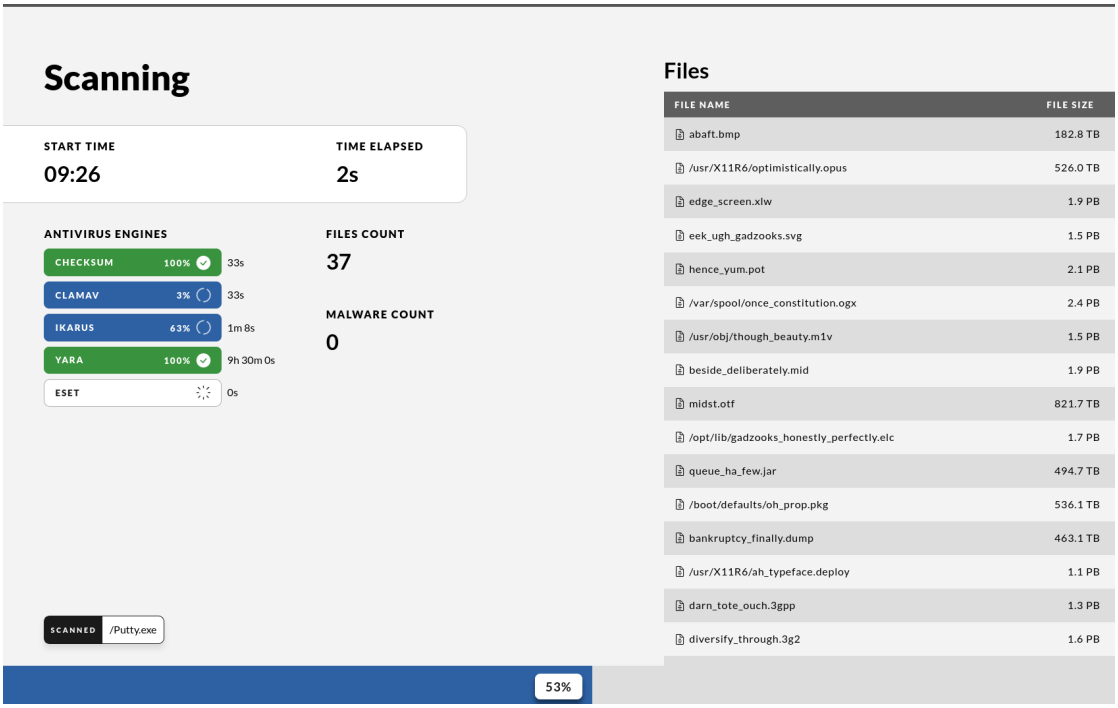
This is a pop-up screen on which you need to fill in your email address. If the Impex has been configured to, there might also be a list of preloaded names to choose from. making it easier, and faster, for users to use the identification screen.



The confirm screen

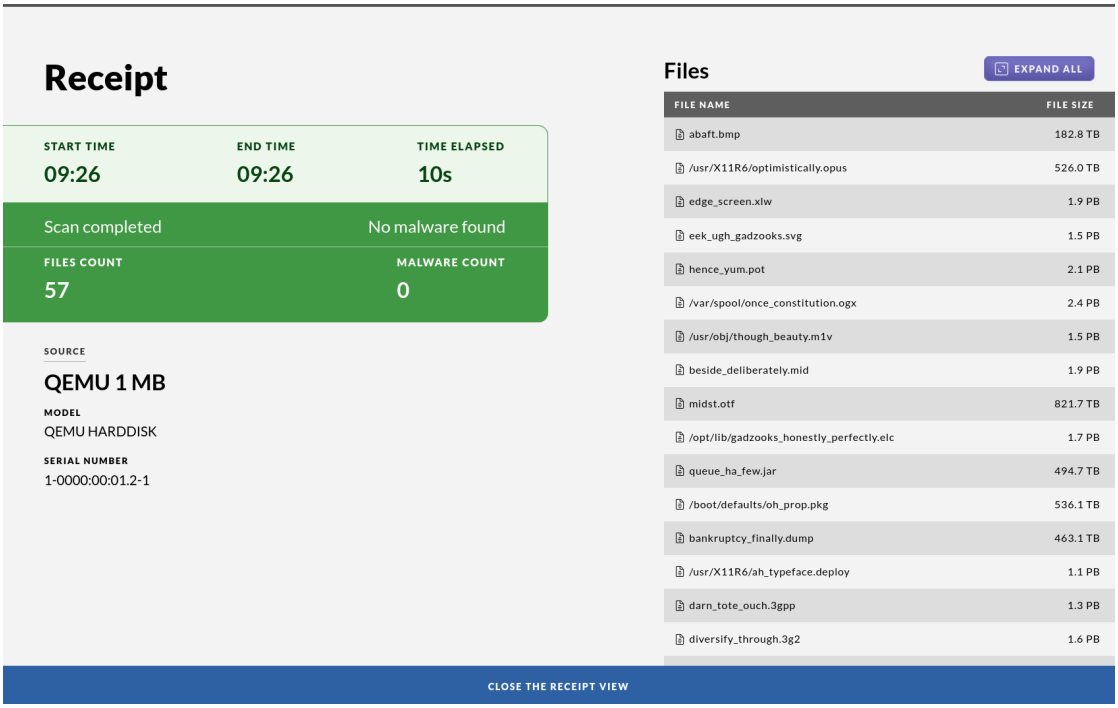
The confirmation screen will display some information describing the process used by, and the action taken by, Impex. It asks you to read and acknowledge this information before proceeding.

The files on the USB drive will now be analysed for virus, malware and other unwanted software. During this process a progress bar will be shown depicting a rough estimate on how much time is left.



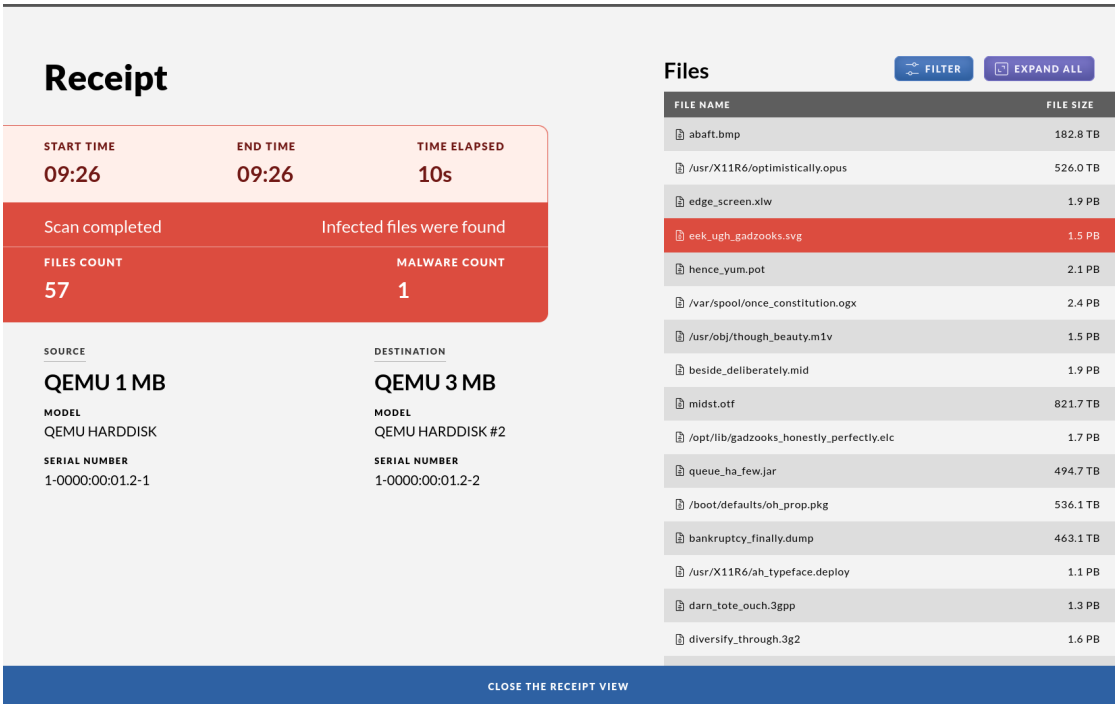
The progress bar

If nothing malicious was detected you will see a green screen together with a receipt which gives an overview of which files were scanned and their unique checksums. If a printer is attached and enabled you will also get a printout of this summary.



The summary screen

In the case that unwanted files were detected the screen will go red and a listing will show which file or files contained malware. If a printer is attached and enabled you will also get a printout. To only view the malicious files, press “Filter”. The drive containing the malicious files will not be modified or cleaned by the system.



Screen when malware was detected

Your local security policy should dictate what to do with the USB drive in case malware is found.

4. To complete the procedure press “Done” or pull out the USB drive

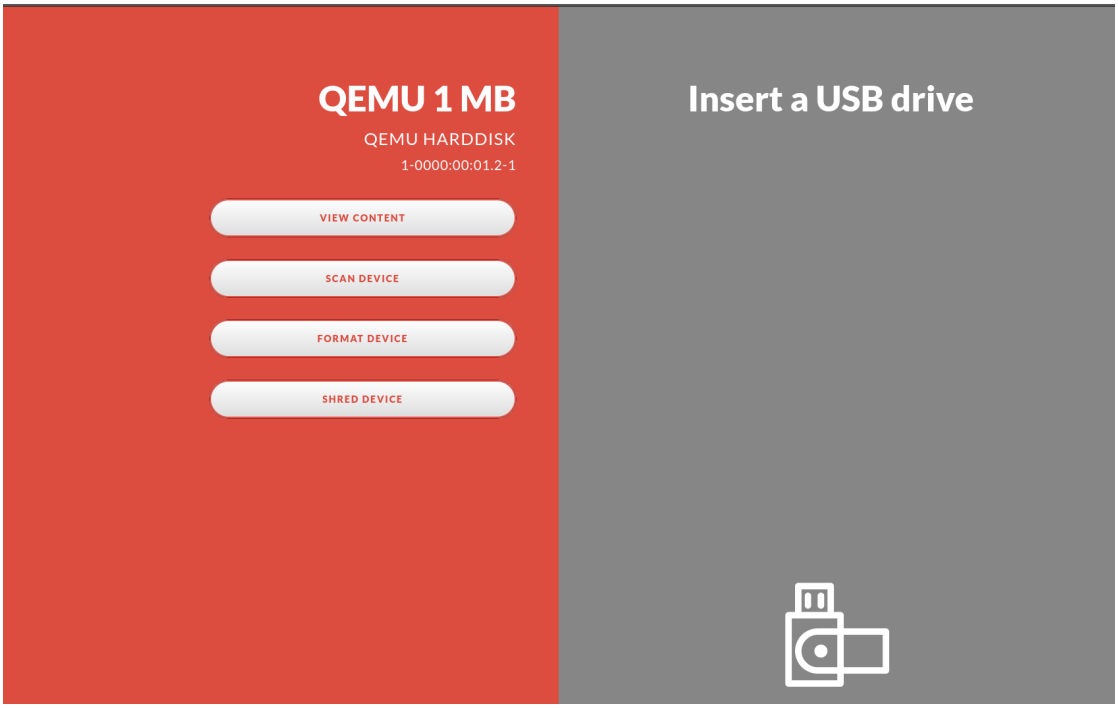
Either press “Done” or remove the USB-device to close the receipt-view. If the USB-device is removed while the receipt-view is active, “Done” will be replaced by a ten second countdown, and when the countdown reaches zero the view will be closed.

To abort the countdown simply press it and it will be replaced by “Done” and the receipt-view will remain active until “Done” is pressed.

If at any point you want to abort the procedure before this, pull the USB drive.

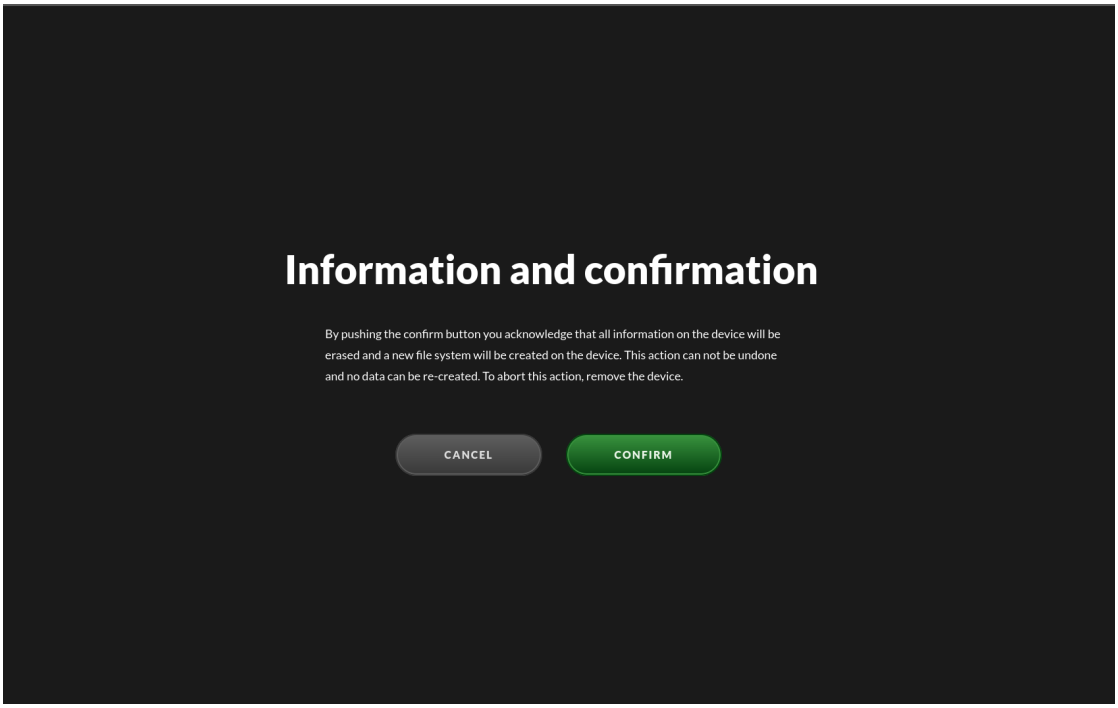
6 Shred a USB drive

If the “Allow shred only” option has been enabled in the IMPEX Control Center one can also use the IMPEX station for shredding a USB drive. If the option is turned on the “Shred device” button appears when just one drive is inserted. It does not matter in which port the drive is inserted.



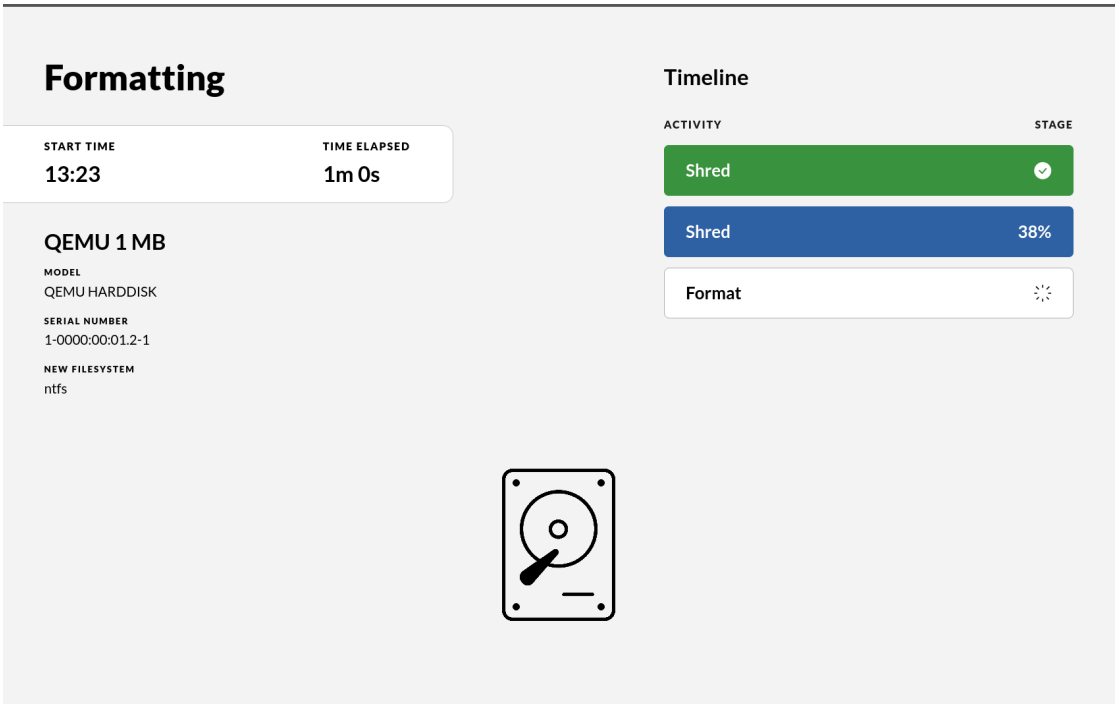
View after inserting a drive in the left side port

1. **Insert a USB Drive**
2. **Press the “Shred Device” button**
3. **Read the text and then press “Confirm”**



The confirm screen

This screen will display text describing the actions you are about to take. If you click on “confirm”, the next step will be to shred and format the attached USB drive. If you have changed your mind, or performed this action in error, just remove the attached USB device to interrupt the shredding and formatting.



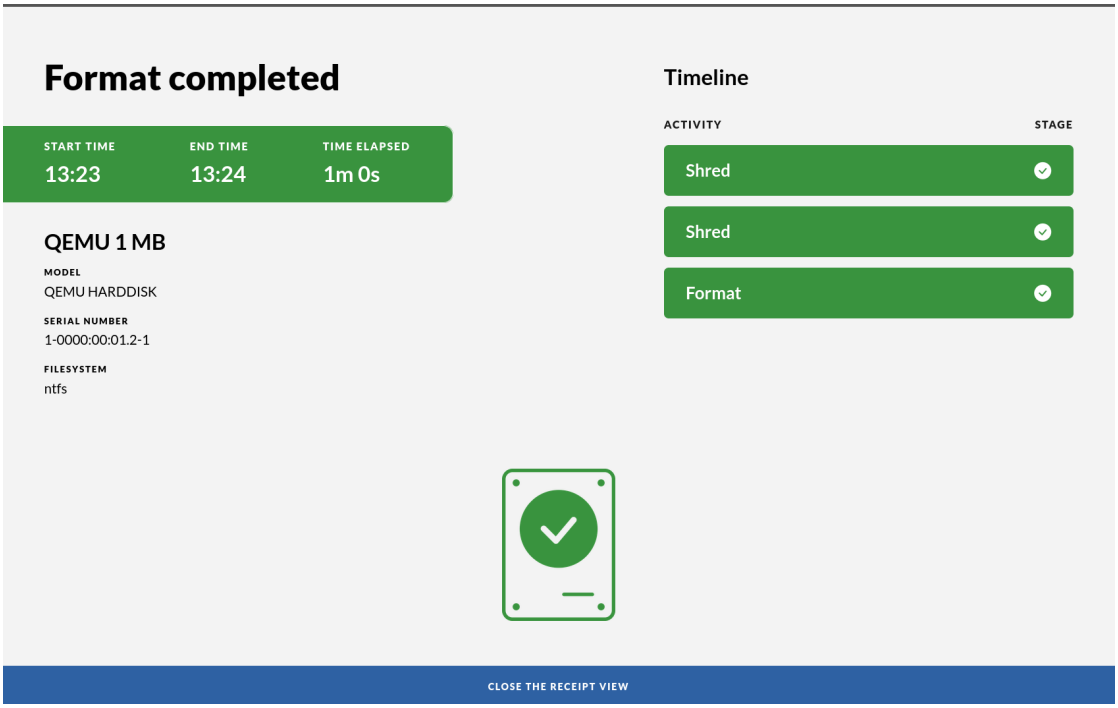
The progress screen

The progress bar is a measure that will display the progress of the actual shredding.

After acknowledging that the user understands that the USB drive will be shredded and all information on it will be lost the drive will be formatted and a new **FAT32** file system created on it. If the drive is larger than 2TB it will be partitioned with **GPT** and the file system will be **exfat**. The default file system **FAT32** can be changed in the ICC to be always **exfat** or always **NTFS**.

After the process is complete the final view will contain a receipt showing information about the drive. It will also contain information on how many passes of shredding occurred. The system automatically shreds in three passes if the drive is detected to be a magnetic spin disk. If it is a flash drive, only one pass is done to preserve write cycles on the hardware. Since there is no problem with magnetic residues on a flash drive, one pass is considered enough.

Note that some drive enclosures, perhaps with some RAID or SSD disk cache functionality do not report a rotation rate even if they contain magnetic spin disks. In this case IMPEX will only do one write cycle and it is up to the end user to redo the shred action as many times as policy demands.



The receipt screen

The receipt is shown on the screen. The receipt will contain important information, including:

- brand and model of the attached usb devices
- name of the attached usb devices
- file system used when formatting
- serial numbers of the attached devices
- how many shredding passes was performed

4. Press "Done" and remove the USB drive

The USB drive is now formatted and clean, ready for use.

5. Shredding disclaimer on SSDs

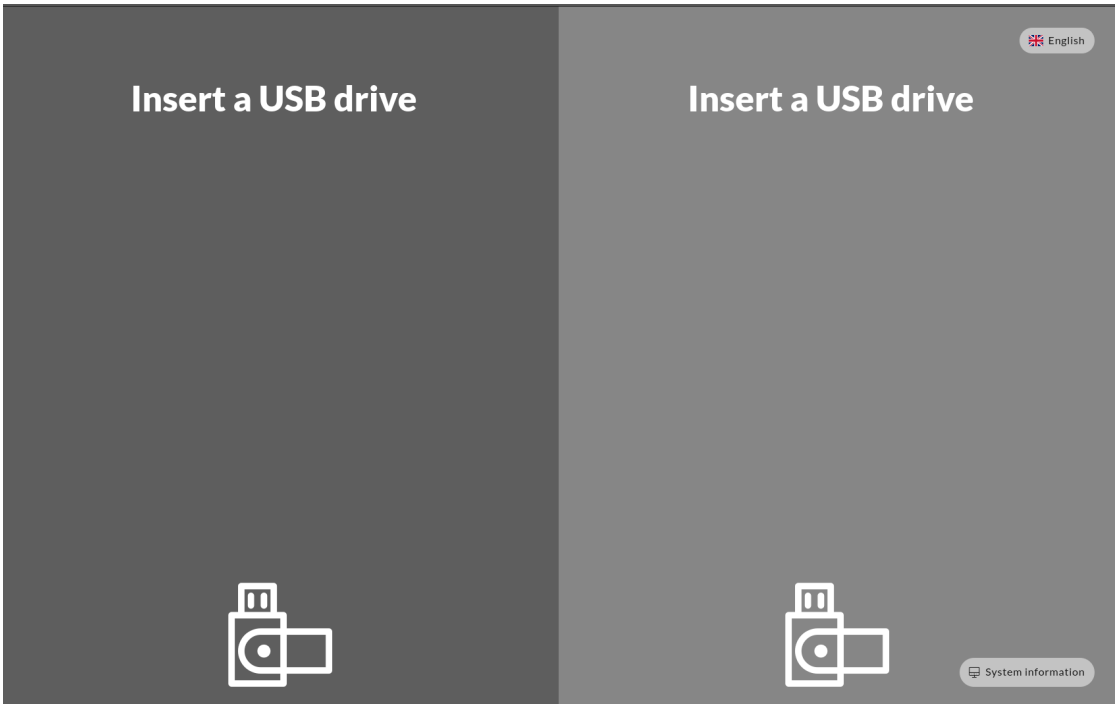
Due to how flash drives work, there is no guarantee that each sector gets shredded. The firmware in the drive might direct writes to different sectors even though the same block is written to. This is called wear leveling and is a method to increase a SSDs life span.

6. Bitlocker exception

Bitlocker drives cannot be shredded at the moment because IMPEX cannot re-create the bitlocker container. If a device has a bitlocker container on it, the shred-button will not be shown. We recommend changing the bitlocker password to something very long which is practically the same as shredding it. This might change in an upcoming version.

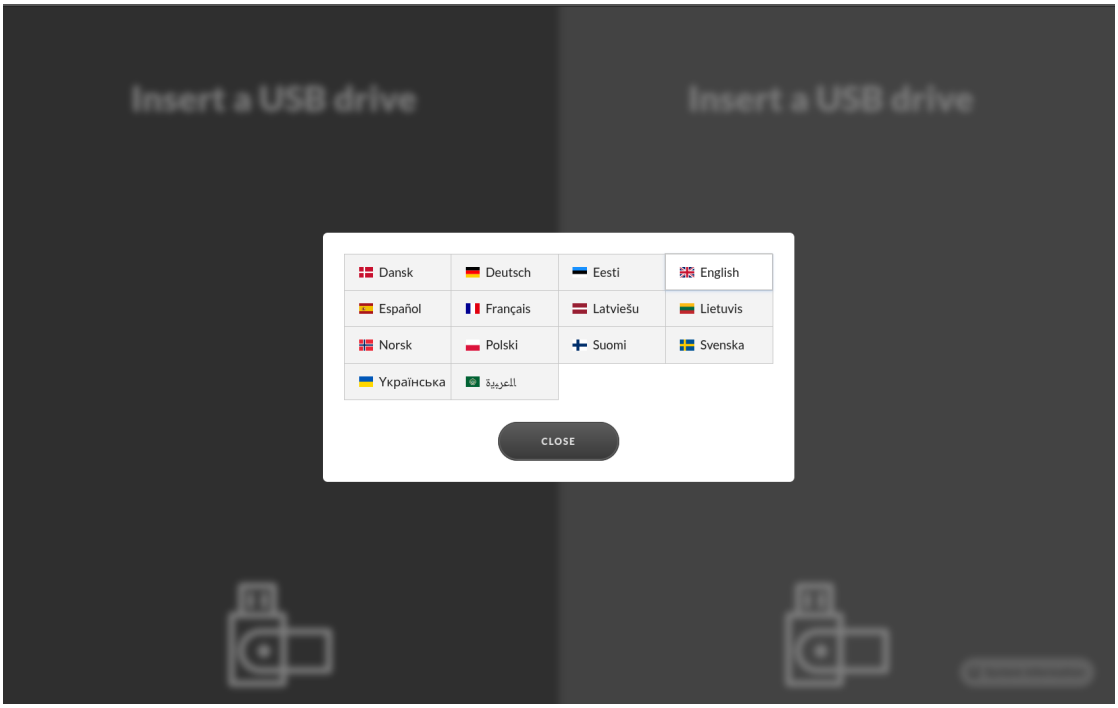
7 Change language

The IMPEX station interface has support for several languages. To switch languages press on the Flag symbol up in the right corner and choose your desired language in the popup.



Flag symbol screen

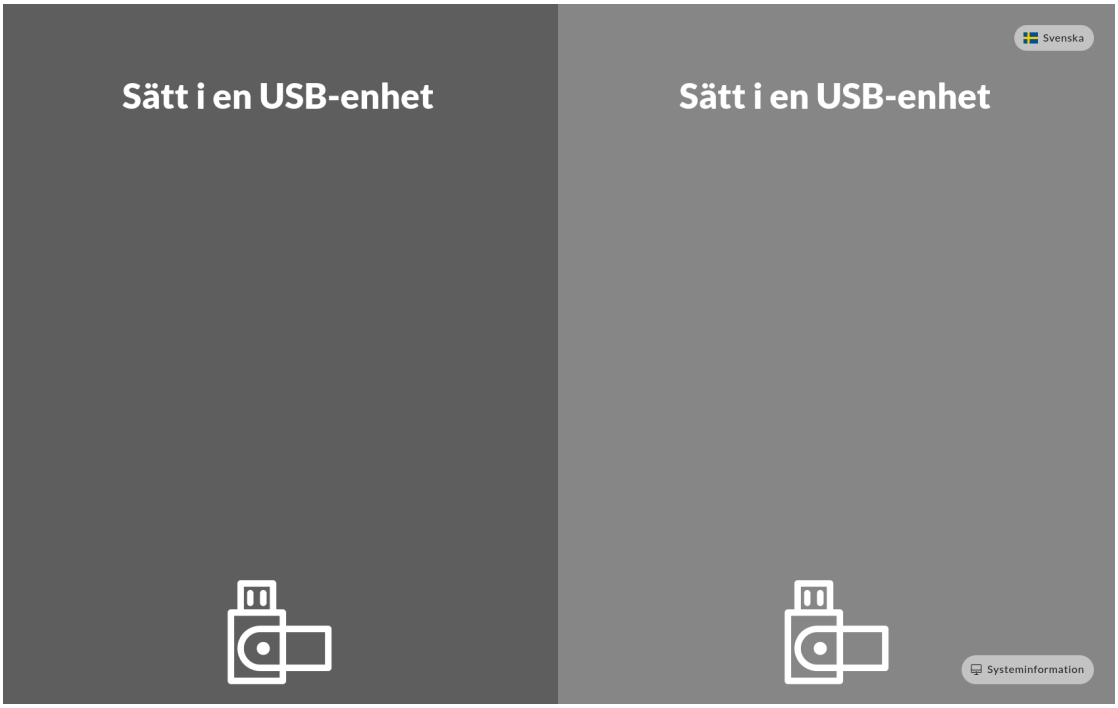
This is the screen with a language symbol in the top right corner. By clicking on the touch screen, you will be able to change language settings in the Impex station.



The Flag symbol menu

When you have clicked on the flag symbol, a menu will appear. This menu will display the different languages that you can select to set the Impex station user interface language.

This is what the interface looks like after changing the language setting to Swedish.

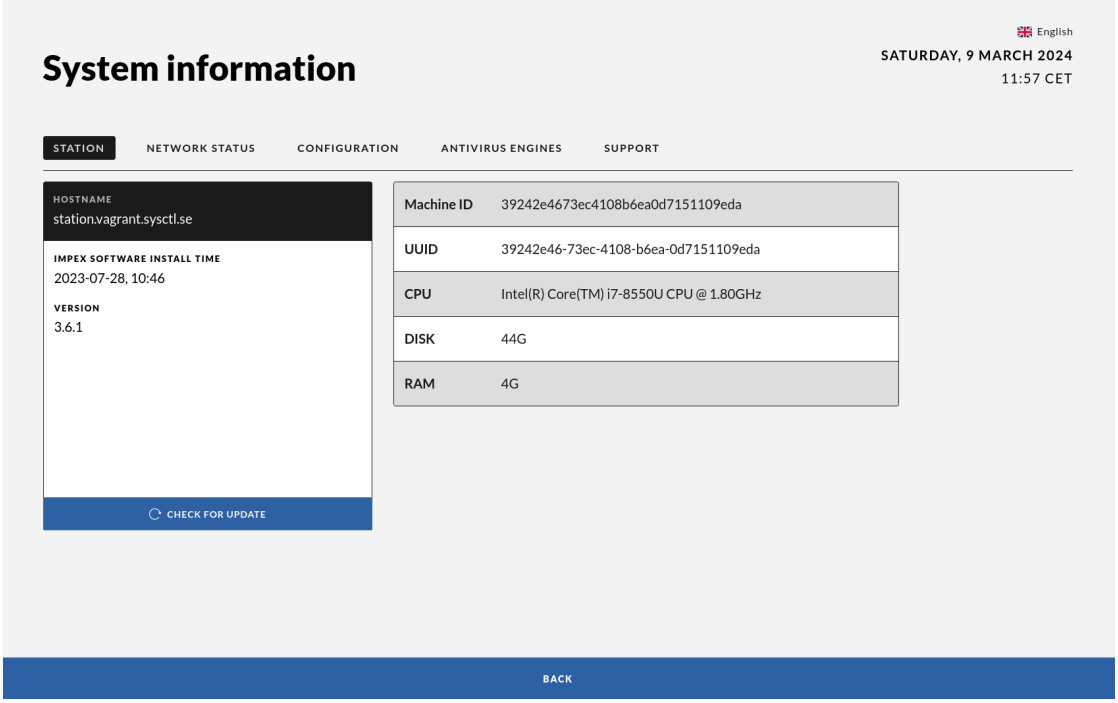


Interface after changing to Swedish

8 System Information Page

The System Information page contains information about the configuration and health of the IMPEX station.

On the initial screen down in the right corner is the link to the information page. This link will be green in case the Anti Virus signatures and Operating System are up to date and red in case they are out of date.



The System Information Page

The information page has four sections. The “STATION” section contains information about the version of the IMPEX software, the local station’s identification and its hostname. It also contains the last time AV and OS updates were fetched.

The “CONFIGURATION” and “ANTIVIRUS ENGINES” sections show settings set in the Impex Control Center for this station. These settings can only be changed on the server side.

The “NETWORK STATUS” section shows the network address configuration and which IMPEX Control Center the station is connected to.

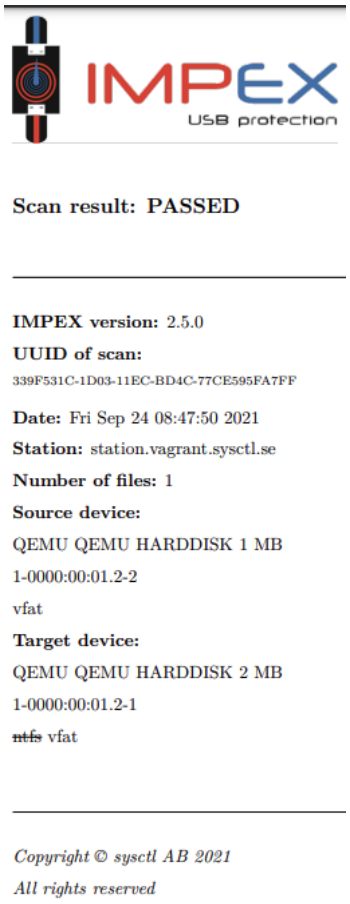
This page is primarily meant for the technical staff on site but might be useful for others as well.

9 Examples of printed receipt

Pictures of the physical receipt to demonstrate the content of receipts when malware is found or when a normal run, without any malware is reported.

9.1 Receipt without any found malware

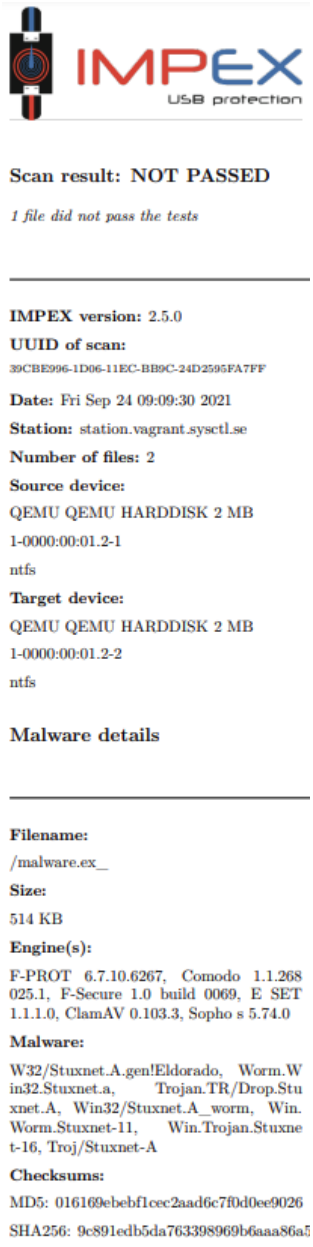
This example is of a receipt that is printed when Impex did not find any malware.



Receipt with info on scan when no malware was found

9.2 Receipt from when Impex have found malware

This example is of a receipt that is printed when Impex has found malware. Note that the various names given to the malware are written as well as which AV engines were active on the station when the scan was performed.



IMPEX
USB protection

Scan result: NOT PASSED

1 file did not pass the tests

IMPEX version: 2.5.0

UUID of scan:

39CBE996-1D06-11EC-BB9C-24D2595FA7FF

Date: Fri Sep 24 09:09:30 2021

Station: station.vagrant.sysctl.se

Number of files: 2

Source device:

QEMU QEMU HARDDISK 2 MB

1-0000:00:01.2-1

ntfs

Target device:

QEMU QEMU HARDDISK 2 MB

1-0000:00:01.2-2

ntfs

Malware details

Filename:

/malware.ex_

Size:

514 KB

Engine(s):

F-PROT 6.7.10.6267, Comodo 1.1.268 025.1, F-Secure 1.0 build 0069, E SET 1.1.1.0, ClamAV 0.103.3, Sopho s 5.74.0

Malware:

W32/Stuxnet.A.gen!Eldorado, Worm.W in32.Stuxnet.a, Trojan.TR/Drop.Stu xnet.A, Win32/Stuxnet.A_worm, Win. Worm.Stuxnet-11, Win.Trojan.Stuxne t-16, Troj/Stuxnet-A

Checksums:

MD5: 016169ebebf1cec2aad6c7f0d0ee9026

SHA256: 9c891edb5da763398969b6aaa86a5

Receipt with info on scan where malware was found

10 Scan and transfer files from one USB drive to another (only text instruction)

This step-by-step guide is for scanning a USB drive for virus and malware and if none are found, transfer them to a second USB drive.

1. Insert the source drive into the left port

2. Insert the destination or target drive in the right port

The screen should now display both of the drives, their brand and model name. Press the "View Content" button to look at the actual files on the drive.

3. Press on the left arrow to transfer the files to the right side drive

Please note that the right side drive will be erased and cleaned (formatted) to make sure it is empty. If the source drive is a CD or DVD the target drive file system will be **exfat**.

4. Depending on your local security policy you might have to enter your identification using the on-screen keyboard and press a confirm button to continue

The files on your source USB drive will now be analysed for virus, malware and other unwanted software. During this process a progress bar will be shown depicting a rough estimate on how much time is left.

If nothing malicious was detected you will see a green screen together with a receipt which gives an overview of which files were scanned and their unique checksums. If a printer is attached and enabled you will also get a printout of this summary.

In the case that unwanted files were detected the screen will go red and a listing will show which file or files contained malware. Note that in this case no files will be transferred so the target USB drive will still be clean. If a printer is attached and enabled you will also get a printout. To view only the malicious files, press "Filter". The source drive containing the malicious files will not be modified or cleaned by the system.

Your local security policy should dictate what to do with the source USB drive in case malware is found.

5. To complete the scanning press "Done" and pull out the USB drives

If at any point you want to abort the procedure, pull the USB drives. It is also worth mentioning that the station does not require you to copy from left to right. The process can also be done in the other direction. That means you can also transfer files from right to left. The files will be analysed and scanned before being copied, no matter in what direction they are copied to. This can in certain situations be more intuitive depending on the physical placement of the IMPEX station.

11 Administration

11.1 Updates and patching

Impex updates itself automatically without any need to perform anything on the station. There are two types of updates that are installed.

- Signature files
- System updates

11.1.1 Signature files

Signature files are downloaded regularly and installed several times a day for different engines. This does not affect any scans.

11.1.2 System Updates

Every night, the station checks for new system updates and, when available, installs them.

When an update of the system is in progress, it is not possible to start a scan, formatting or shred.

If a scan is in progress or if it is less than three hours since a scan, formatting or shred is completed, the check for updates will wait until the following night.

11.2 Weekly reboots

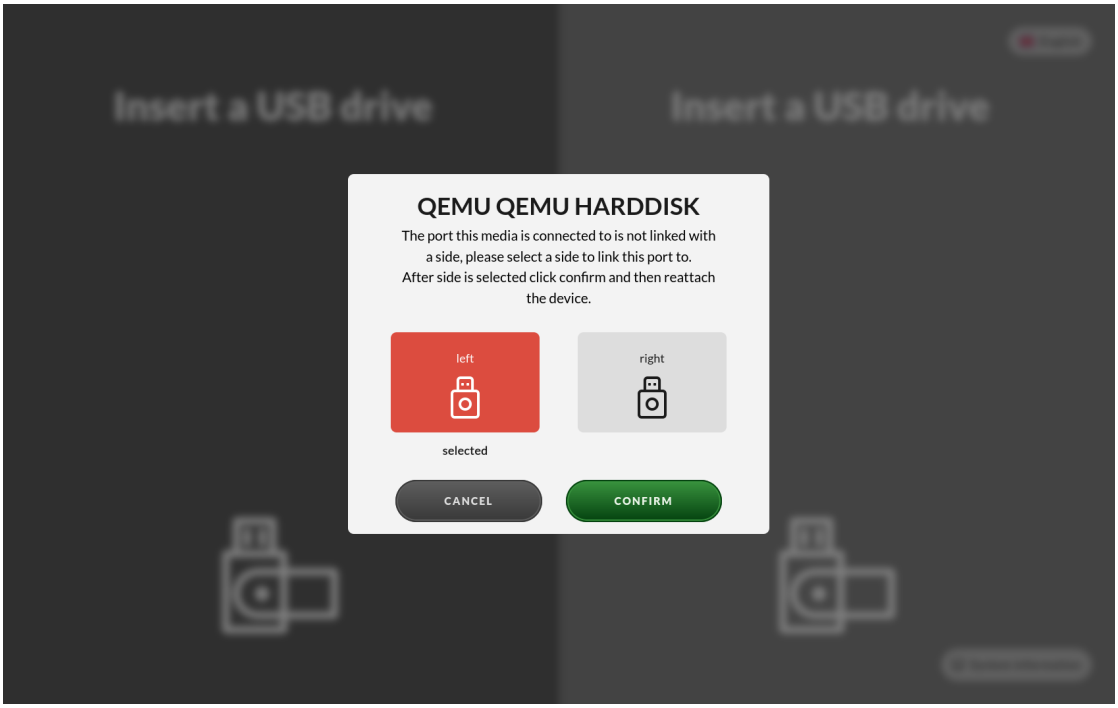
The station will restart once a week on Sundays 06:01 in the morning with 10 minutes of random delay.

If the result from the receipt view is required after a scan and it has disappeared due to the station having restarted and no person has been on site, it is possible to use Impex receipt printer or check the result on the server to which the station is connected.

11.3 Configure USB sides

Impex stations use two sides that are visualized on screen. These sides are then mapped to a USB port and named left and right, there can be multiple USB ports mapped to the same side but only one of those ports mapped to a side can be used at the same time.

In a situation where the USB port is not mapped, usually when the station is new or the sides mapping has been reset from the ICC, a dialog will show on the screen asking for what side the attached device should be mapped to. It is not the actual device that gets mapped to a side, it is the USB port the device is attached to that gets mapped to the selected side.

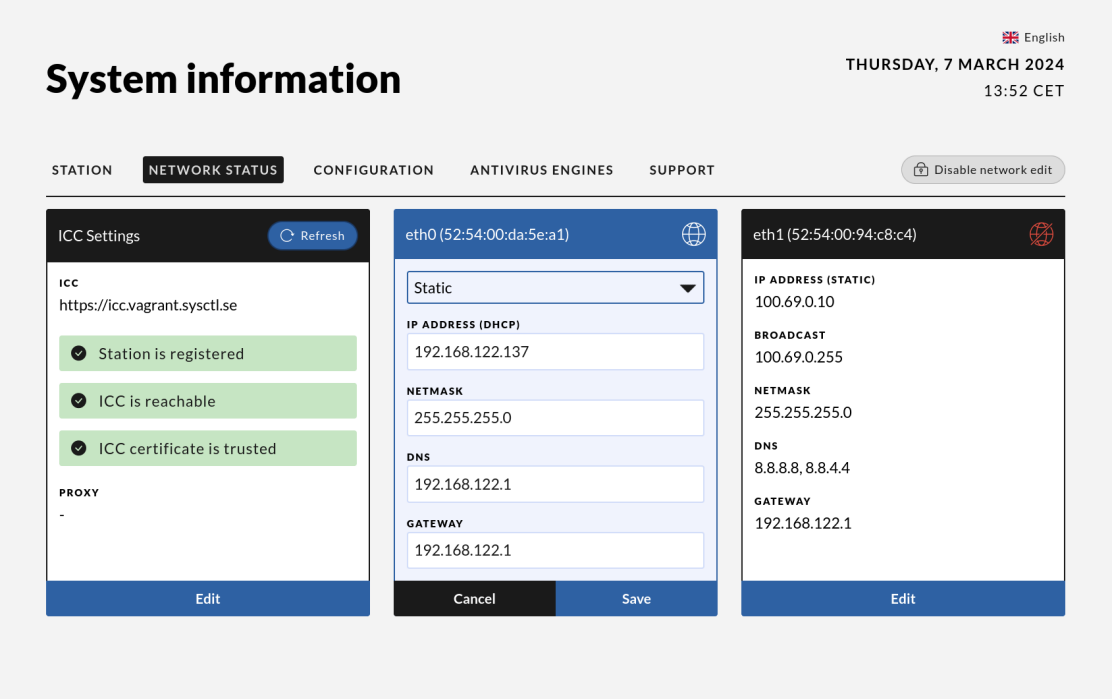


Map USB port to a side

View of a device selected as the left side after it was attached to an unmapped port.

11.4 Configure network settings

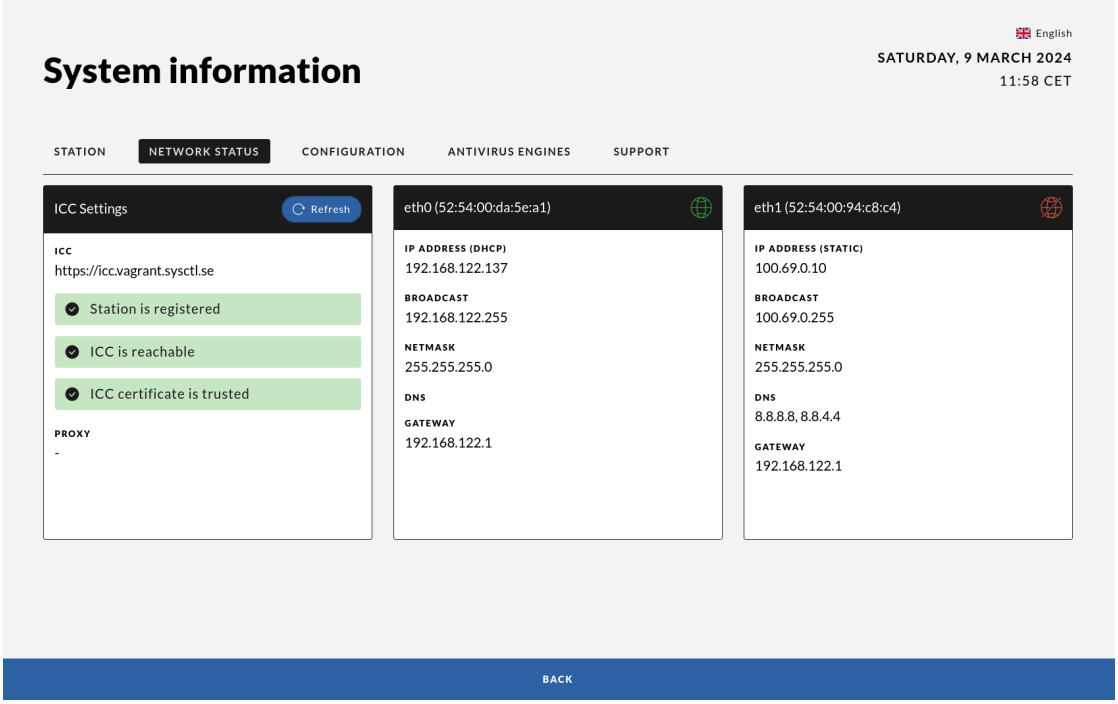
A working network connection is required for a station to be able to get updates, configurations and send scan/transfer reports to the ICC. To configure network settings on a station that has never been connected to a ICC press “System Information” on the screen and then “Network Status”. Click edit on the device to configure and choose between Auto or Manual, Auto will not require any more configuration while Manual will need IP-address, netmask, an optional DNS and a gateway.



Configure network interface

11.5 Change a station's network settings

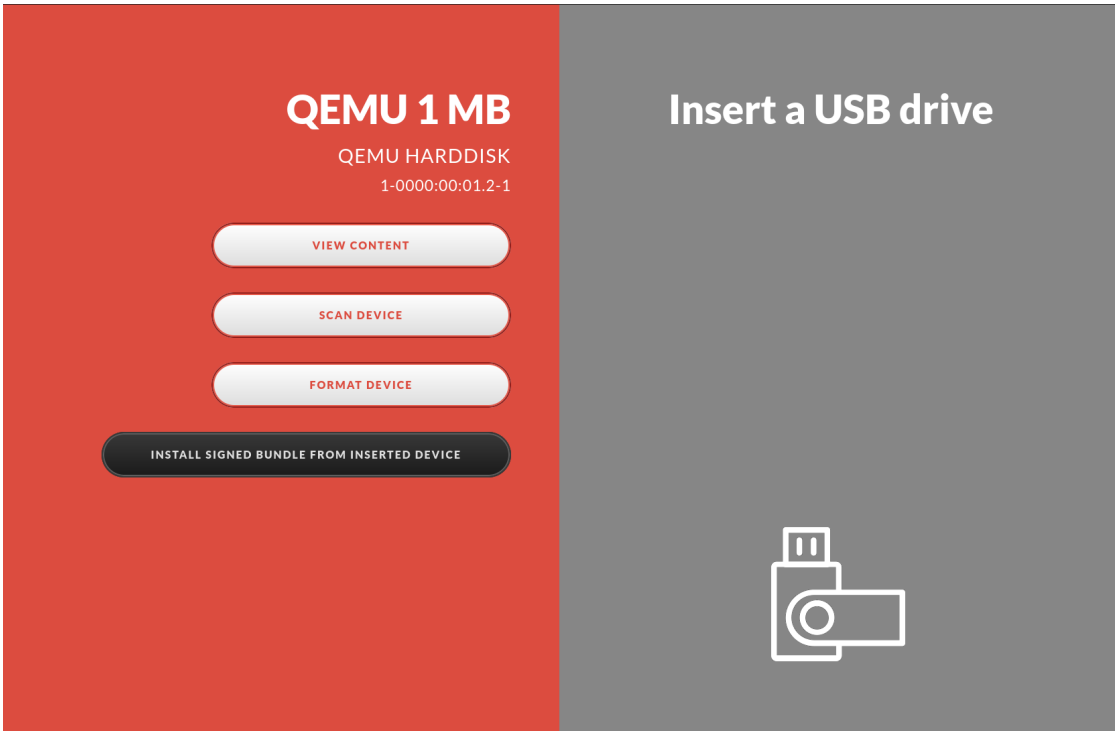
Due to network, location or policy changes it might at some point be desirable to change a station's network settings, for example adding a proxy or changing the station IP.



Network status

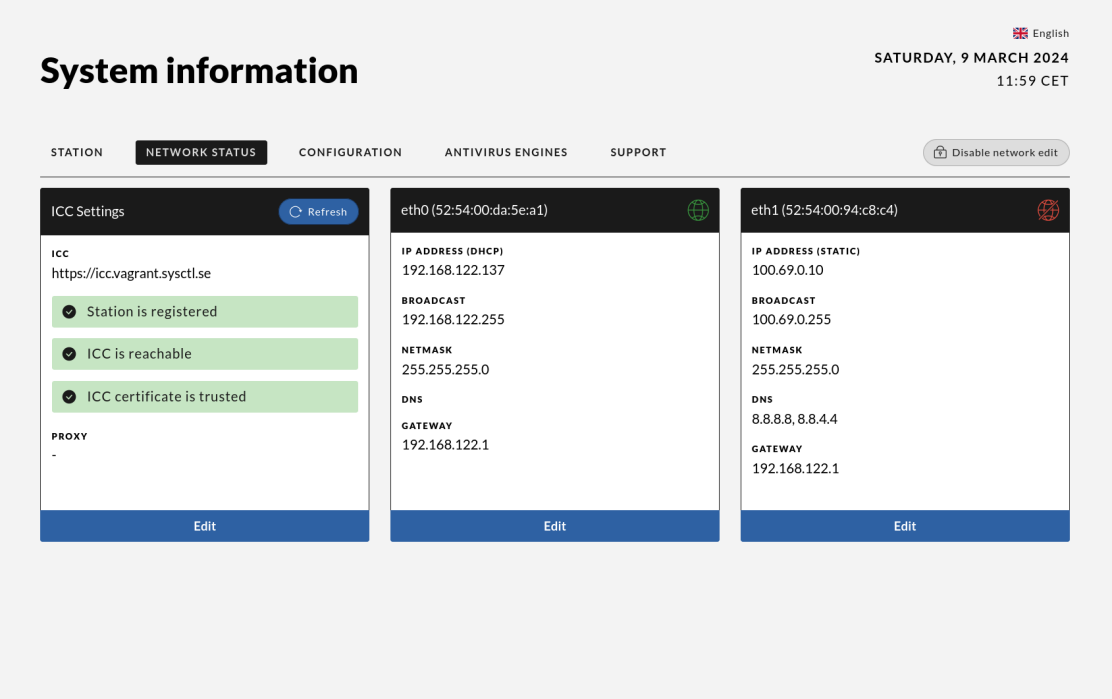
To be able to change the network settings one first needs to download the “station network edit”-signify bundle from the ICC. Unzip the bundle and put the two files (run.sh and SHA256.sig) on a USB-device and insert it into the station.

After the USB-device is inserted press the “Install signed bundle from inserted device” and then press the link to the network status view, this will add an edit-option to ICC-settings and interfaces.



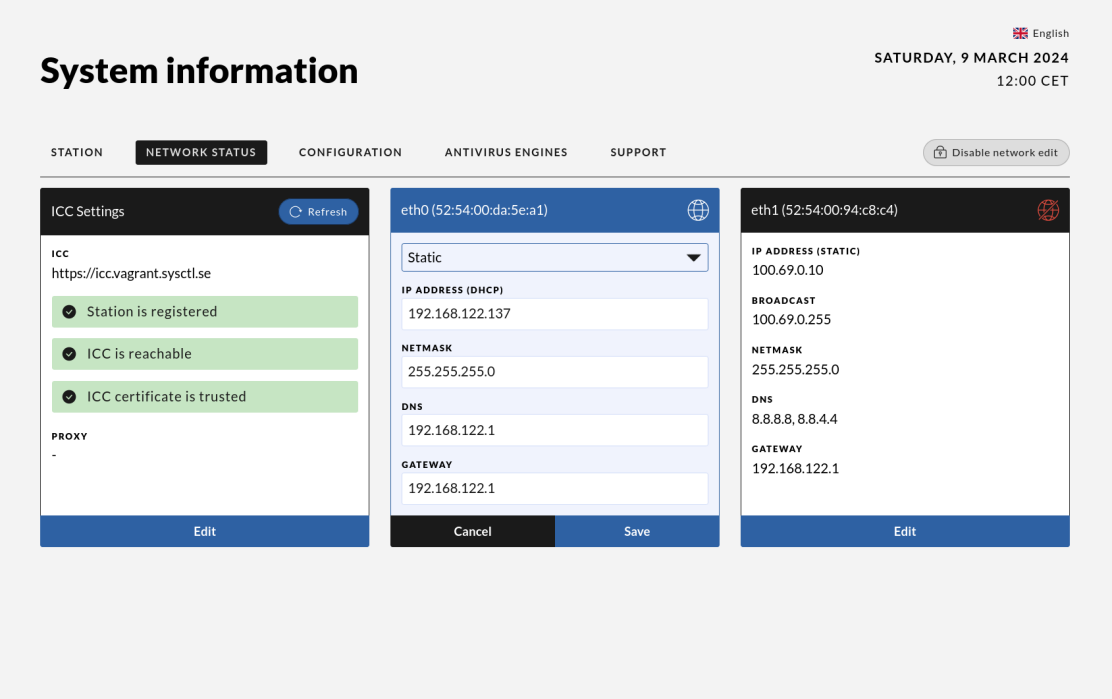
Execute signed bundle

Note that the signify-bundle only works on stations that are connected to the ICC where the bundle is downloaded from.



View after signify-bundle

Press edit on the correct network device to edit it and then save to apply the new changes.



Editing network-settings

When everything is set to the desired new settings and saved, just remove the device and edit-mode will be disabled.

This USB drive is valid for one week and only works on the stations connected to the ICC when the bundle was generated on it. The bundle gets re-generated every Monday morning.

11.6 Connect to ICC

Click edit on ICC settings and set the ICC server. This is the minimal field required to register a station to an ICC server. There is also a possibility to map the ICC IP to a hostname and to connect through a proxy.

12 Advanced administration

12.1 Console access

In certain cases an administrator needs to use the console access to change settings on a station. Console access will only give root privileges to the station, no personal accounts exist.

This access should only be used after recommendation from sysctl.

Most administrative actions can be performed via the ICC server but in some rare cases console access might be needed. With console access the following can be done:

- Change the credentials for the wireless network
- Set new root password
- Troubleshoot the network
- Requirements
  - To gain access to the console a keyboard is needed.
  - Keyboards must be allowed in the station.
  - Keyboard access is by default not possible.

To enable it one must change a setting in the configuration card for this station in the ICC server GUI.

12.1.1 Single boot the station to set a new password

The keyboard has an english keylayout in the grub menu.

1. Attach a keyboard to the station
2. Reboot the station by pressing the power button once and wait until the station is turned off.
3. Press the power button again to start it up.
4. Hit the *ESC*-key during the boot to enable GRUB
5. Type the username *root* and the grub password(can be extracted from the ICC server)
6. Type *normal* and press enter and then press *ESC* once
7. Press "e" to edit boot parameters
8. For the row starting with the name linux, add "rw init=/bin/bash" at the end
9. Type *CTRL+X* to boot in to single user mode
10. Type *passwd* to set a new password
11. Type the command *touch /.autorelabel* to ensure correct SELinux labels
12. Type the command *exec /sbin/init* to restart the station

12.1.2 Manually disable UDEV rules

1. Single boot the station and set a new password
2. Before step 12:
3. Change *"udev_rule": true* to *false* by editing the following file

   /opt/sysctl/impex/impexd/config.json

- Reboot the station described in step 12