Introduktion till IMPEX USB Protect

SYSCTL AB

Innehållsförteckning

1 Introduktion till Impex

Detta dokument är en introduktion till Impex, en säkerhetsfunktion som används för att kontrollera flyttbara digitala lagringsmedier (USB-minnen, SD-kort, löstagbara hårddiskar, disketter, DVD-skivor, CD-R-skivor, mm). Texten är både en användarhandledning och en enkel översikt över utrustningen. I texten ges ett antal korta beskrivningar över vanliga handgrepp och användningsfall med Impex.

Impex-stationen är en fysisk enhet med två USB-portar på framsidan till vilka man ansluter det flyttbara media som man vill kontrollera så det är fritt från skadlig kod.

Impex är utvecklat för att kontrollera alla filer på ett media. Normalt sett så arbetar man med två stycken lagringsmedia, ett som är källmedia och ett som är mottagarmedia. Filer läses från källmediet och kontrolleras. Ifall ingen skadlig kod är hittad så kopieras filerna över till mottagarmediat. Innan filerna kopieras så kommer dock mottagarmediat att tömmas på allt innehåll, det vill säga formateras. Detta görs så att det inte blir sammanblandning mellan gamla filer och nyöverförda filer.

Den främsta anledningen till att Impex använder sig av två olika media är att det finns olika typer av IT-attacker som kan ske på filnivå medans andra kan ske genom att själva lagringsmediat är manipulerat och på så sätt blivit skadligt för den dator till vilket den ansluter. Impex har som uppgift att bara föra över filer, så att en Impex-användare kan få över filerna till ett lagringsmedia som det går att lita på istället för ett okänt källmedia.

I denna introduktionstext kommer vi att ge exempel på hur man kopierar filer mellan två media. Det kommer också visas hur man kan använda Impex till att tömma (formatera) ett USB-minne, att tömma minnet på ett säkrare sätt (shred) och att kontrollera minnet utan att kopiera mellan två portar.

Eftersom Impex måste vara lättanvänd och lättförståbar så finns det språkstöd för över 15 olika språk. I dokumentet kommer det att beskrivas hur man byter språk i det grafiska gränssnittet. Vi beskriver också hur man kontrollerar olika inställningar och parametrar i Impex-stationen.

1.1 Impex arbetssätt

Impex-stationen arbetar med flera antivirus-motorer och i flera pass. Detta innebär att filerna läses flera gånger. Exakt hur många antivirusmotorer som körs och hur många kontroller som görs beror på flera saker, exempelvis hur många som är uppsatta i Impex-stationen och på ett antal inställningar som sätts från administrationsservern.

Eftersom Impex läser filer många gånger så kan stora medier, lagringsmedia med många eller stora filer på, gamla och långsamma lagringsmedia eller i värsta fall kombinationer av dessa, göra att kontrollen tar lång tid att genomföra. Ett sätt för att snabba på arbetet är att Impex försöker läsa in filer på den interna, snabba, lagringsytan i Impex när det går. För att visa att arbete pågår så visas en indikator över förloppet längst ner på skärmen.

1.2 Impex och ICC

En eller flera Impex-stationer sitter anslutna till en server, Impex Control Center, ICC. Från ICC kan man sätta inställningar i Impex-stationen. Beroende på ändringar som är gjorda i ICC så kan den Impex-station som du skall använda se annorlunda ut eller fungera annorlunda.

Till ICC skickas information från Impex-stationen, exempelvis information om en kontroll och genomsökning av ett flyttbart media samt andra loggar.

1.3 Impex och tillbehör

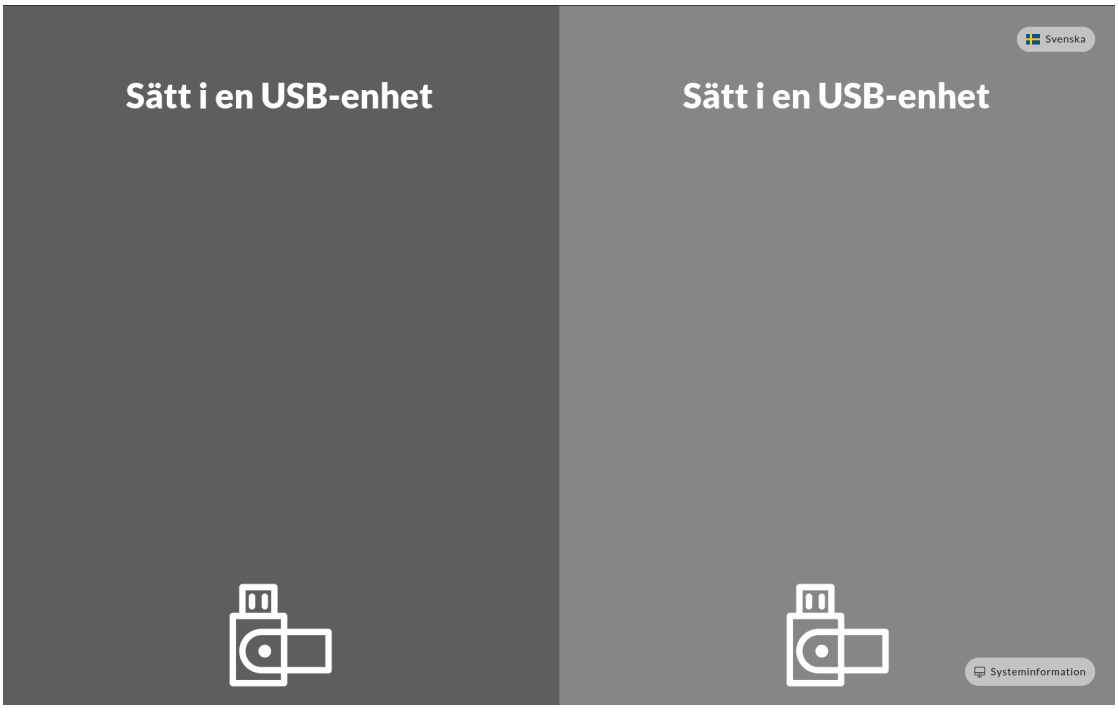
Impex kan utrustas med flera tillbehör. Ett vanligt tillbehör är en kvittoskrivare, till vilket resultatet av en kontroll skrivs ut. På så sätt får man ett fysiskt och konkret bevis på att en kontroll har gjorts. Andra tillbehör är vägghängare och olika mediehanterare, exempelvis DVD-läsare eller SD-kortläsare.

1.4 Impexanvändning i din organisation

Många organisationer har tagit fram speciella styrdokument, riktlinjer och rutiner för hur flyttbara medier får användas, hur de skall kontrolleras, hur de måste skyddas, etc. Det är viktigt att du får kunskap om sådant såsom vilka typer av minnen och diskar som får användas, vilka som får kopieras från eller till, vad som skall göras ifall Impex larmar om att skadlig kod har hittats samt hur digitala eller fysiska kvitton skall hanteras.

2 Genomsöka och överföra filer från en USB-enhet till en annan

Det här kapitlet innehåller steg-för-steg vägledningar för att genomsöka flyttbara medier som till exempel en USB-sticka, för att undersöka om det finns någon skadlig kod (dator virus, trojanska hästar eller annan skadlig kod). Om ingen skadlig kod hittas, överförs innehållet till den andra USB-enheten.



Initial vy

I exemplet nedan så ansluts källmedian i vänster port. IMPEX stödjer givetvis att källmedia och målmedia i vanliga fall kan anslutas till valfri port. Dessa friheter att använda mediet kan dock ändras från administrationsservern ICC, så att vissa media bara får användas på visst sätt.

Innan det går att starta kommer det visas en bild som berättar att en USB-enhet ska anslutas till Impex stationen. I det här skeded är det möjligt att ändra till önskat språk som ska användas i de dialoger som ska visas. Impex har stöd för de flesta av de vanligaste förekommande språken.

1. Anslut den USB-enhet som ska vara källan i den vänstra porten

2. Anslut den USB-enhet som ska vara mottagare i den högra porten

Skärmen visar nu både USB-enheter som anslutits, märke, modell och serienummer. Notera att om serienumret är längre än 30 tecken kommer den att kortas av till att bara visa de sista 30 tecknen.

Tryck på “Visa Innehåll”-knappen för att visa den aktuella enhetens innehåll.

Två enheter anslutna

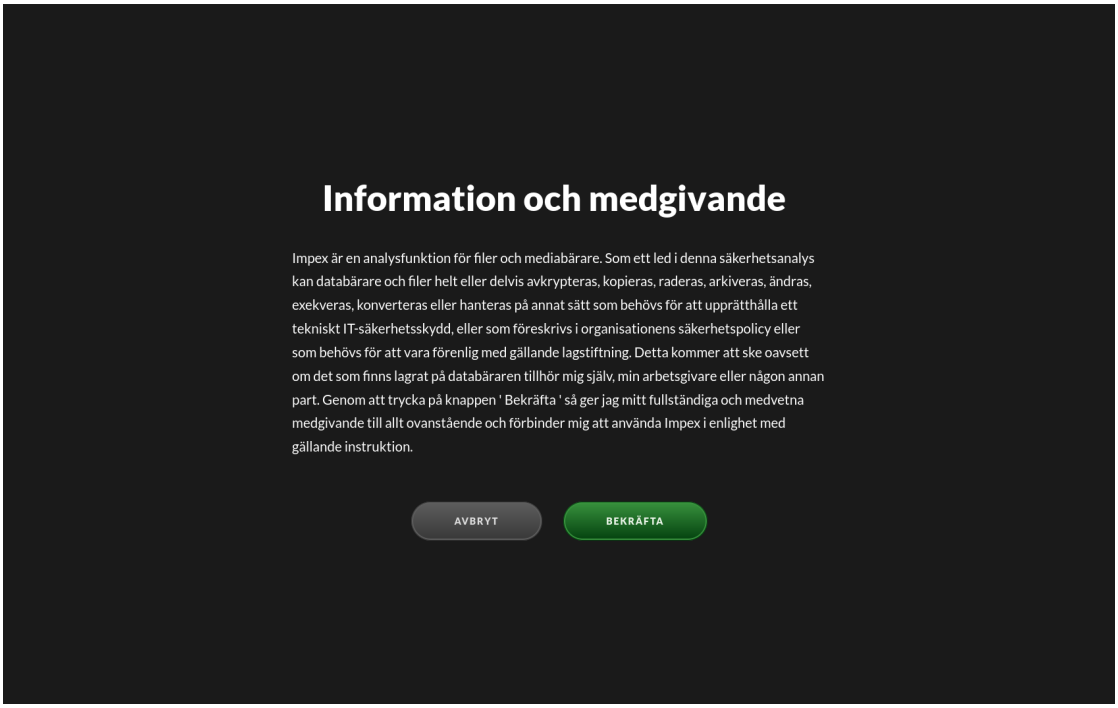
3. Tryck på den vänstra pilen för att överföra filer till den högra enheten

Notera att den högra sidans enhet kommer att bli raderad och rensad (formaterad) för att säkerställa att den är tom innan nya filer kopieras över. Om käll-enheten är en CD eller DVD kommer mottagarenheten att få filsystemet **exfat**.

4. Beroende på den lokala säkerhetspolicyn som stationen är konfigurerad att använda kan det behövas identifikation. Denna skrivs in med hjälp av ett virtuellt tangentbord på pek-skärmen. Avsluta med retur-tangenten för att fortsätta

Identifikationsvyn

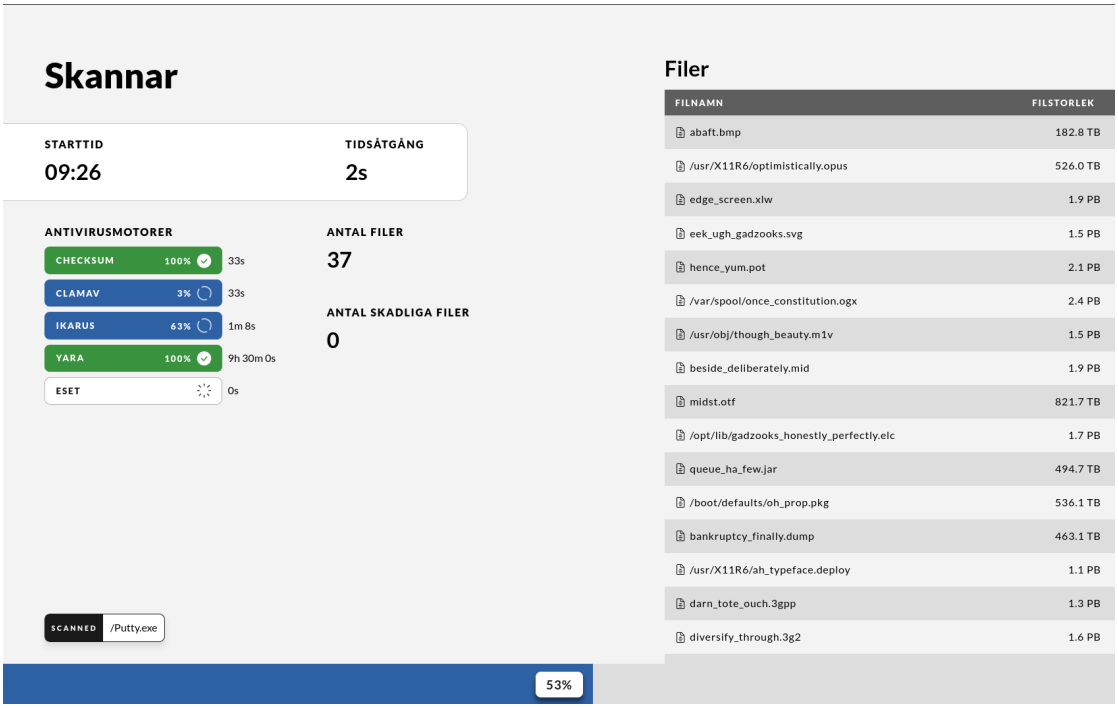
Det här är en vy på skärmen som identifikationen ska fyllas i, exempelvis e-postadress. Stationen kan även vara konfigurerad för att ha automatisk ifyllning av identifikation genom en fördefinierad lista på stationen som användaren kan välja ifrån. Denna lista kan göra att det går lättare samt fortare att fylla identifikationen för en användare. Detta innebär att du börjar skriva ditt namn, sedan kommer Impex visa en lista över namn som innehåller de bokstäver du matat in hittills. Om namnet finns i listan så kan du bara välja det genom att peta på skärmen med fingret på namnet, så fylls det namnet i automatiskt för vem det är som använder Impex-stationen.



Bekräftelsevyn

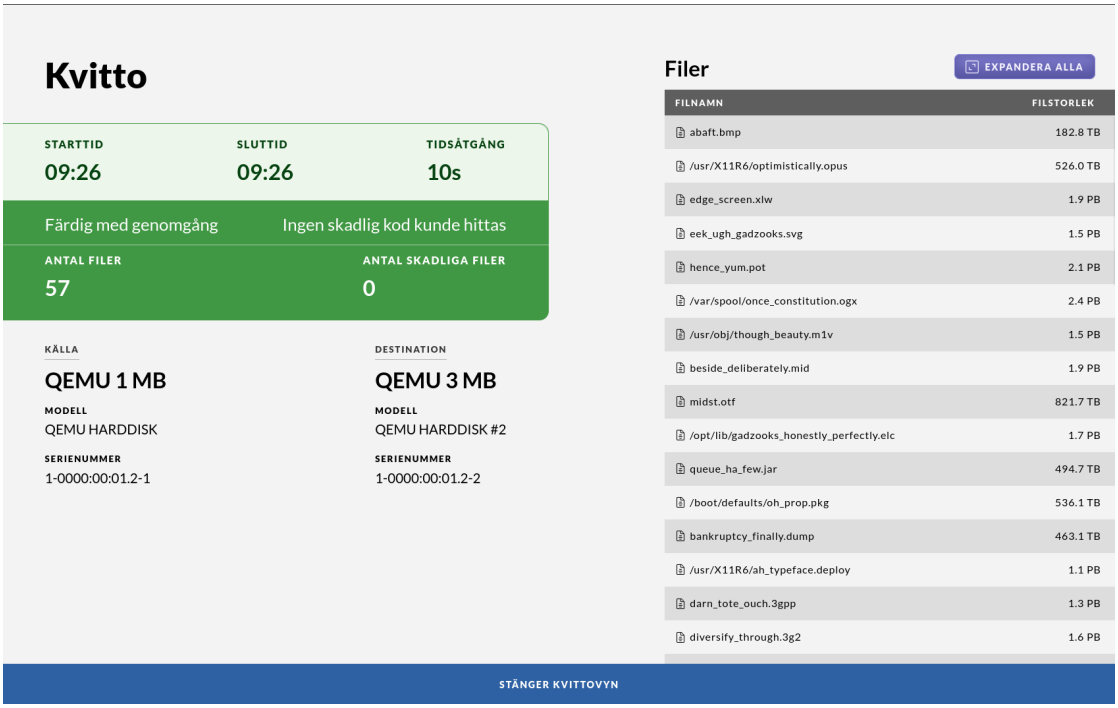
Bekräftelsevyn visar information som beskriver processen som används samt vilka ageranden som Impex gör. Denna bekräftelse måste accepteras innan stationen kan fortsätta.

Filerna från USB-källan kommer nu att analyseras för att söka efter virus, trojanska hästar och annan oönskad kod. Under den här processen kommer dess status visualiseras genom en grov tidsuppskattning på återstående tid.



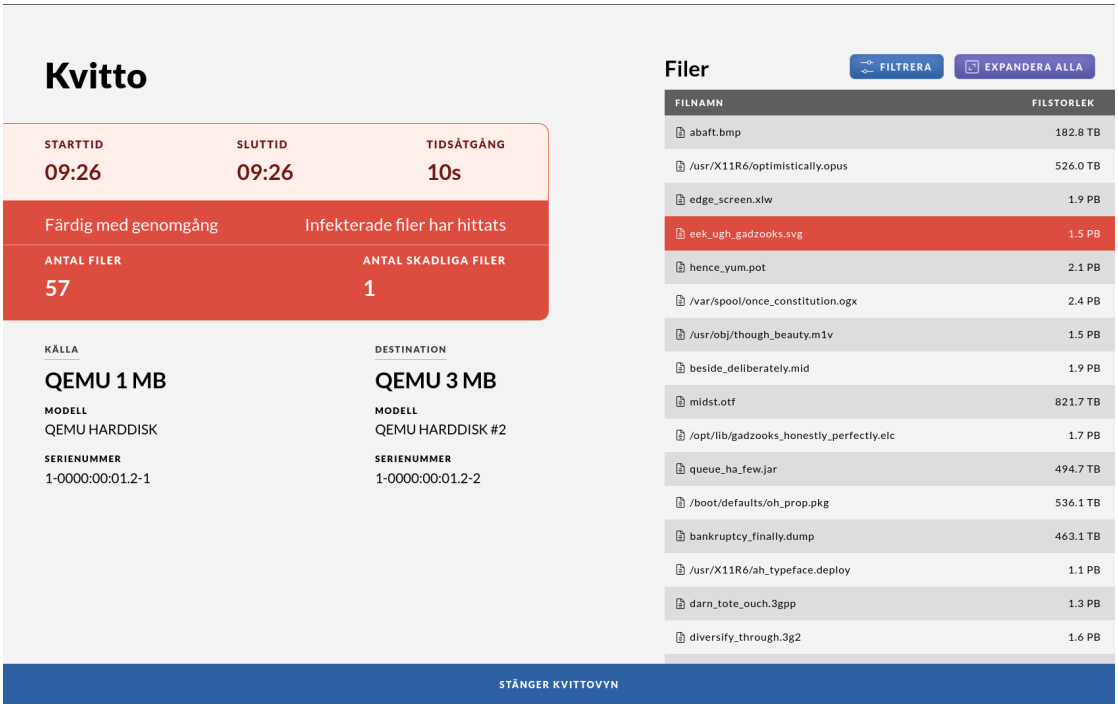
Statusvyn

Om ingen skadlig kod har detekterats kommer en grön vy visas tillsammans med ett kvitto som visar en överblick av vilka filer som har blivit skannade samt deras unika checksumma. Om en skrivare är ansluten kommer även ett kvitto att skrivas ut med en sammanställning.



Sammanställningsvyn

I fallet när oönskad kod detekteras kommer skärmen bli röd och resultatet innehåller även vilken eller vilka filer som har oönskad kod. Notera att det i det här fallet inte kommer överföras några filer till mottagarsidan och den enheten kommer vara tom. Om en skrivare är ansluten och aktiverad kommer även ett kvitto skrivas ut. För att endast visa filer med oönskad kod går det att trycka på knappen filtrera. Källan som innehåller den oönskade koden kommer inte bli modifierad eller rensad av systemet.



Vy när Impex funnit skadlig kod

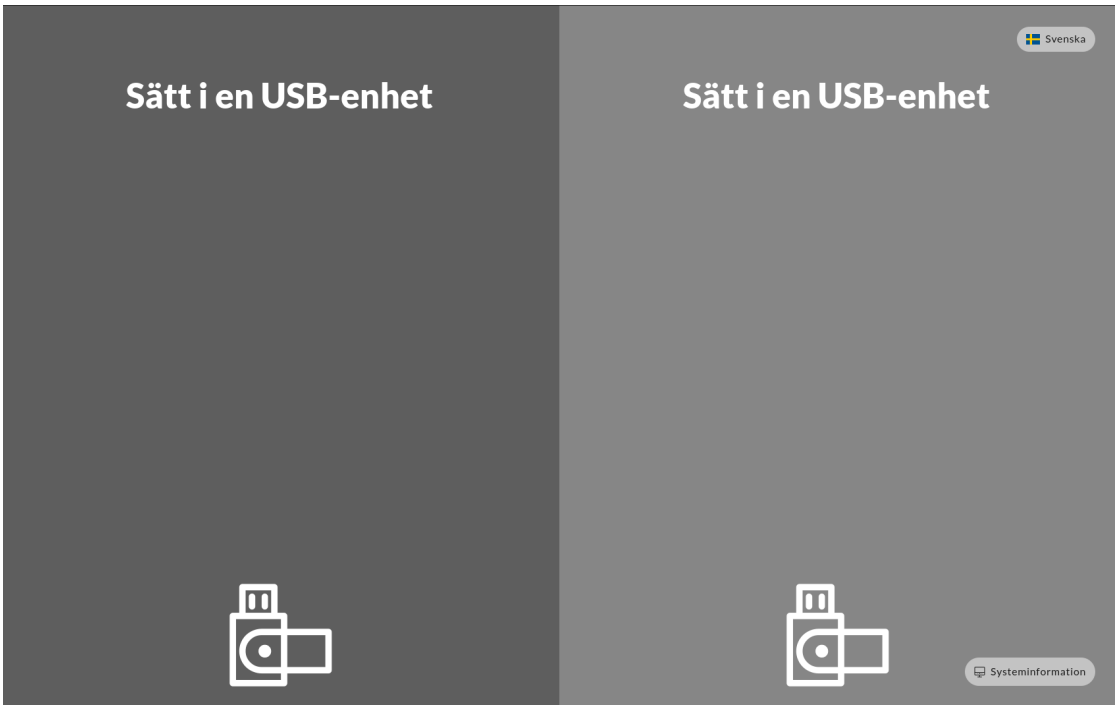
Den lokala säkerhetspolicyn bör berätta vad som ska ske med källenheten i de fall det upptäcks skadlig kod.

5. För att avsluta skanningen tryck på knappen “Avluta” och ta ur USB-enheterna

Om det vid något skede finns behov av att avbryta processen är det bara att ta bort USB-enheterna från portarna. Det finns inget krav på att överföring måste ske från vänster till höger, båda riktningarna fungerar. Riktningen för överföringar kan i vissa fall vara tydligare åt det andra hållet beroende på hur stationen är placerad.

3 Genomsöka/överföra från USB-enhet med Bitlocker till en annan enhet

Det här kapitlet innehåller steg-för-steg vägledningar för att genomsöka flyttbara medier som till exempel en USB-sticka, för att undersöka om det finns någon skadlig kod (dator virus, trojanska hästar eller annan skadlig kod). Om ingen skadlig kod hittas, överförs innehållet till den andra USB-enheten.



Initial vy

I exemplet nedan så ansluts källmedian i vänster port. IMPEX stödjer givetvis att källmedia och målmedia i vanliga fall kan anslutas till valfri port. Dessa friheter att använda mediat kan dock ändras från administrationsservern ICC, så att vissa media bara får användas på visst sätt.

Innan det går att starta kommer det visas en bild som berättar att en USB-enhet ska anslutas till Impex stationen. I det här skeded är det möjligt att ändra till önskat språk som ska användas i de dialoger som ska visas. Impex har stöd för de flesta av de vanligaste förekommande språken.

1. Anslut den USB-enhet som ska vara källan i den vänstra porten

2. Anslut den USB-enhet som ska vara mottagare i den högra porten

Skärmen visar nu både USB-enheter som anslutits, märke och modell. Tryck på “Visa Innehåll”-knappen för att visa den aktuella enhetens innehåll.

Två enheter anslutna

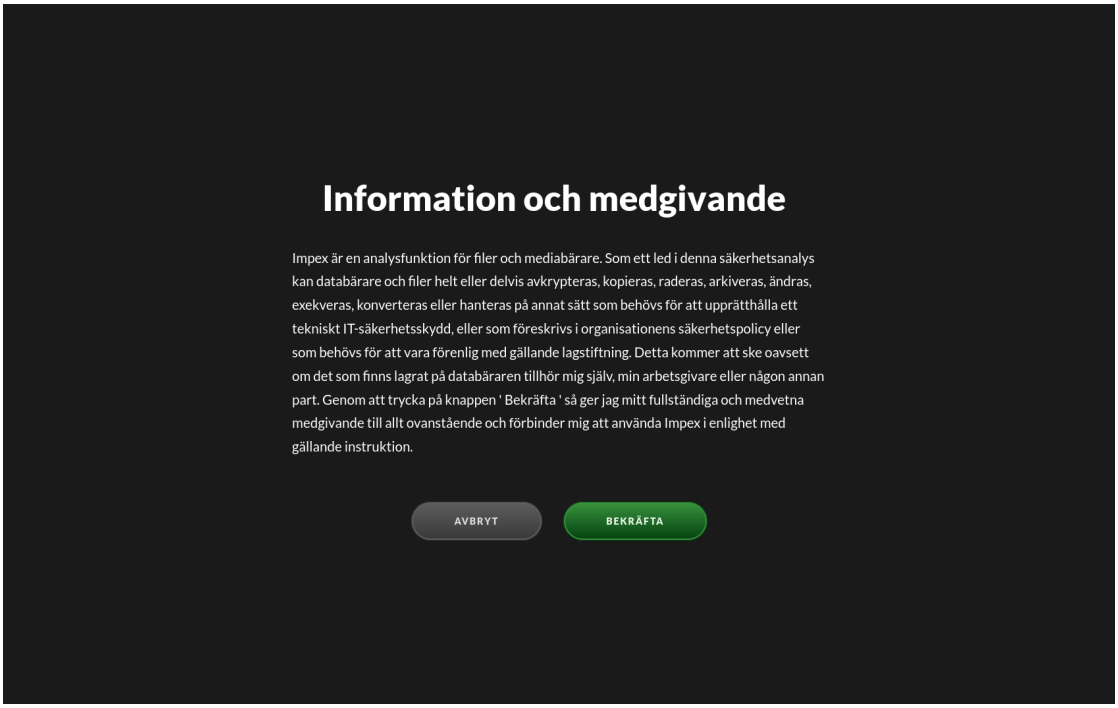
3. Tryck på den vänstra pilen för att överföra filer till den högra enheten

Notera att den högra sidans enhet kommer att bli raderad och rensad (formaterad) för att säkerställa att den är tom innan nya filer kopieras över. Om käll-enheten är en CD eller DVD kommer mottagarenheten att få filsystemet **exfat**.

4. Beroende på den lokala säkerhetspolicyn som stationen är konfigurerad att använda kan det behövas identifikation. Denna skrivs in med hjälp av ett virtuellt tangentbord på pekskärmen. Avsluta med retur-tangenten för att fortsätta

Identifikationsvyn

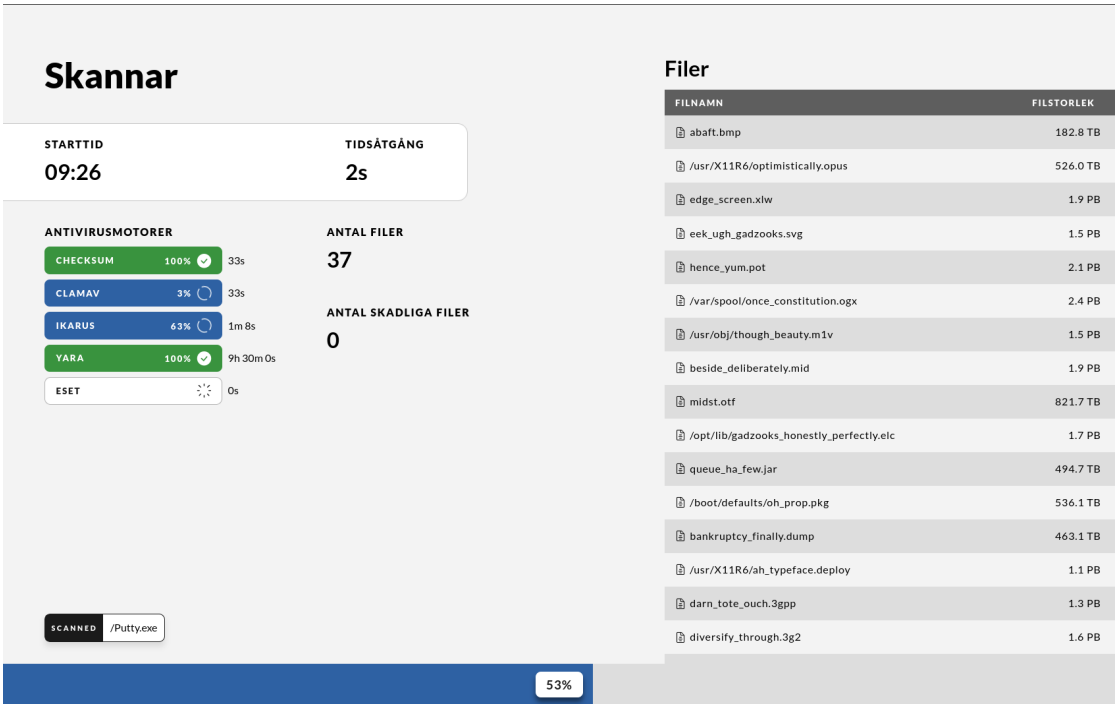
Det här är en vy på skärmen som identifikationen ska fyllas i, exempelvis e-postadress. Stationen kan även vara konfigurerad för att ha automatisk ifyllning av identifikation genom en fördefinierad lista på stationen som användaren kan välja ifrån. Denna lista kan göra att det går lättare samt fortare att fylla identifikationen för en användare. Detta innebär att du börjar skriva ditt namn, sedan kommer Impex visa en lista över namn som innehåller de bokstäver som hittils har matats in. Om namnet finns i listan så kan du bara välja det genom att peta på skärmen med fingret på namnet, så fylls det namnet i automatiskt för vem det är som använder Impex-stationen.



Bekräftelsevyn

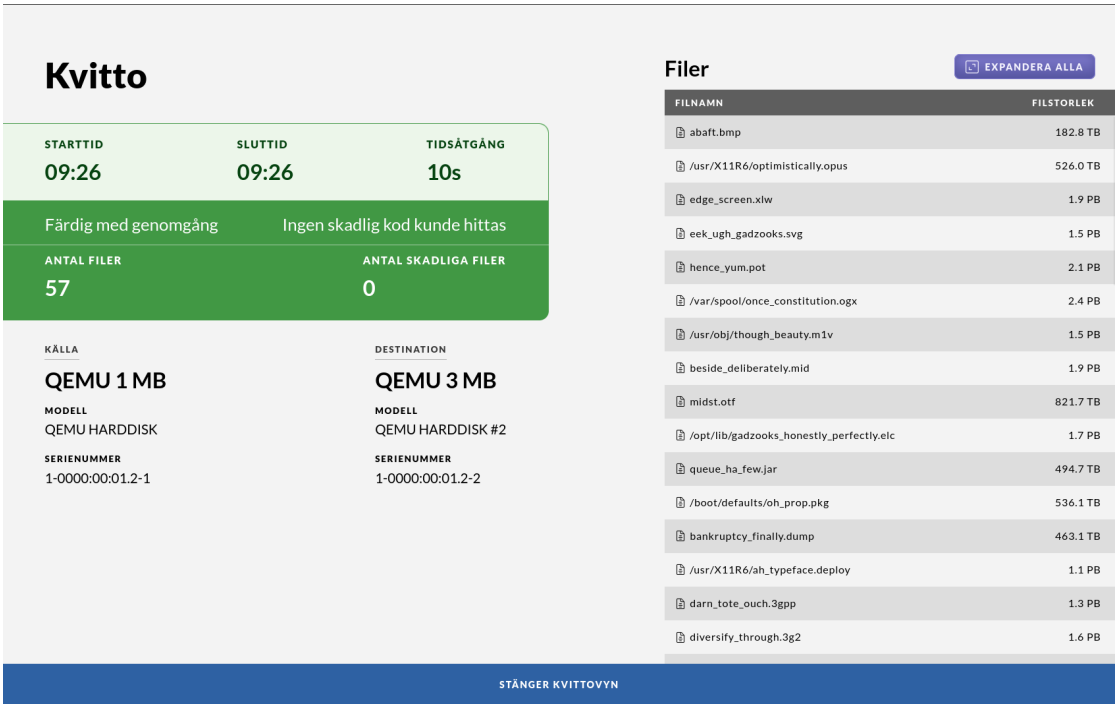
Bekräftelsevyn visar information som beskriver processen som används samt vilka ageranden som Impex gör. Denna bekräftelse måste accepteras innan stationen kan fortsätta.

Filerna från USB-källan kommer nu att analyseras för att söka efter virus, trojanska hästar och annan oönskad kod. Under den här processen kommer dess status visualiseras genom en grov tidsuppskattning på återstående tid.



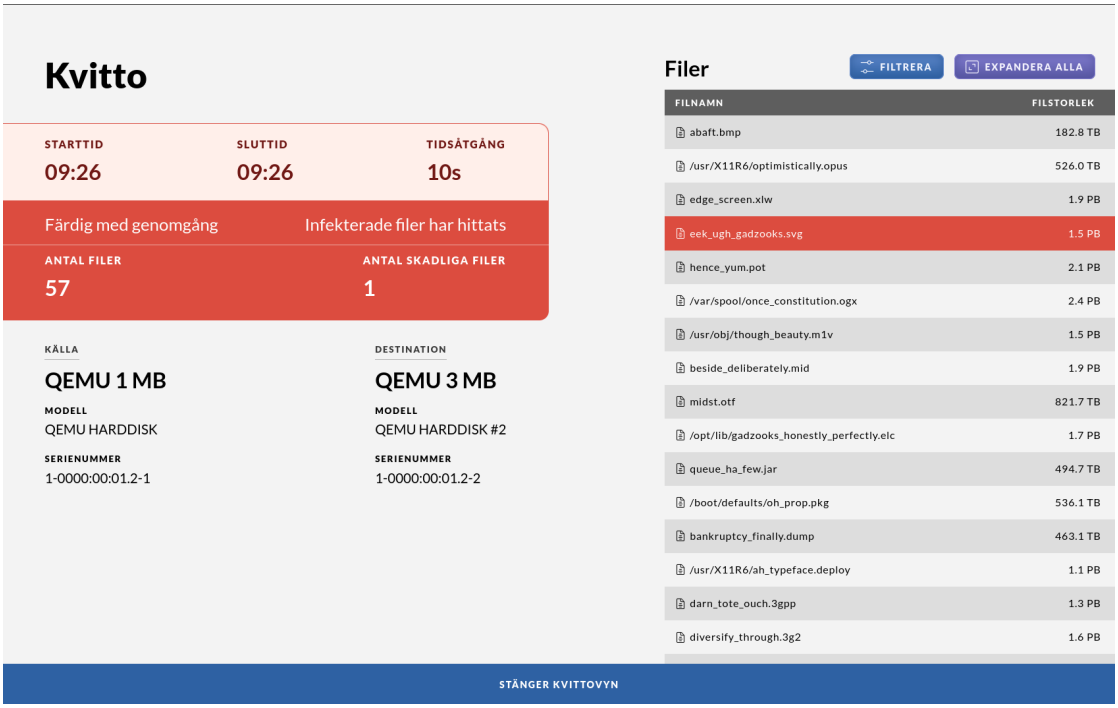
Status vyn

Om ingen skadlig kod har detekterats kommer en grön vy visas tillsammans med ett kvitto som visar en överblick av vilka filer som har blivit skannade samt deras unika checksumma. Om en skrivare är ansluten kommer även ett kvitto att skrivas ut med en sammanställning.



Sammanställningsvyn

I fallet när oönskad kod detekteras kommer skärmen bli röd och resultatet innehåller även vilken eller vilka filer som har oönskad kod. Notera att det i det här fallet inte kommer överföras några filer till mottagarsidan och den enheten kommer vara tom. Om en skrivare är ansluten och aktiverad kommer även ett kvitto skrivas ut. För att endast visa filer med oönskad kod går det att trycka på knappen filtrera. Källan som innehåller den oönskade koden kommer inte bli modifierad eller rensad av systemet.



Skadlig kod funnen. vy

Den lokala säkerhetspolicyn bör berätta vad som ska ske med källenheten i de fall det upptäcks skadlig kod.

5. För att avsluta skanningen tryck på knappen “Avluta” och ta ur USB-enheterna

Om det vid något skede finns behov av att avbryta processen är det bara att ta bort USB-enheterna från portarna. Det finns inget krav på att överföring måste ske från vänster till höger, båda riktningarna fungerar. Riktningen för överföringar kan i vissa fall vara tydligare åt det andra hållet beroende på hur stationen är placerad.

4 Formatera en USB-enhet

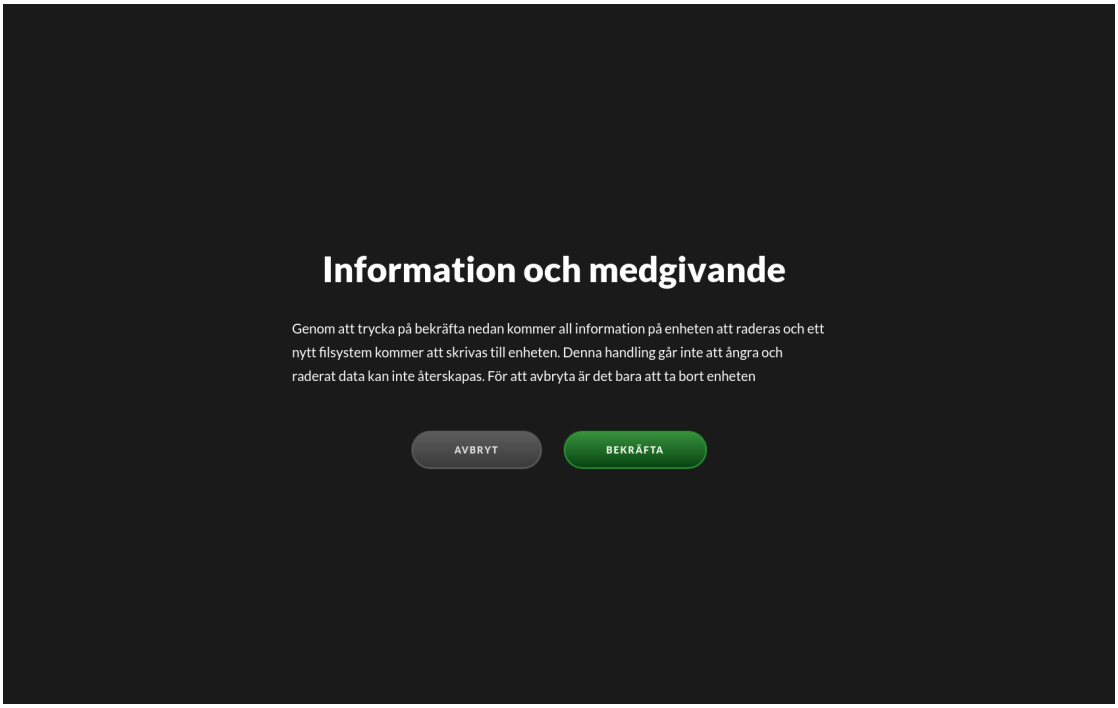
Om inställningen “Tillåt endast formatering” har blivit aktiverat i IMPEX Control Center är det även möjligt att på stationen endast formatera en enhet. När konfigurationen är aktiverad kommer ytterligare en knapp visas när endast en enhet är ansluten. Det spelar ingen roll vilken port USB-enheten är ansluten till.

4.1 Formatera en Bitlocker-USB-enhet

Om USB-enheten är en Bitlocker-sticka kan man formatera den på två sätt. Om stickan är upplåst, dvs man har matat in lösenordet, så skapas det ett nytt NTFS filsystem innuti Bitlocker-containern när man klickar på Format. Om man istället väljer att inte låsa upp Bitlocker-container, t.ex genom att klicka Avbryt vid lösenordsinmatningen, så formateras hela stickan och Bitlocker-containern förstörs.

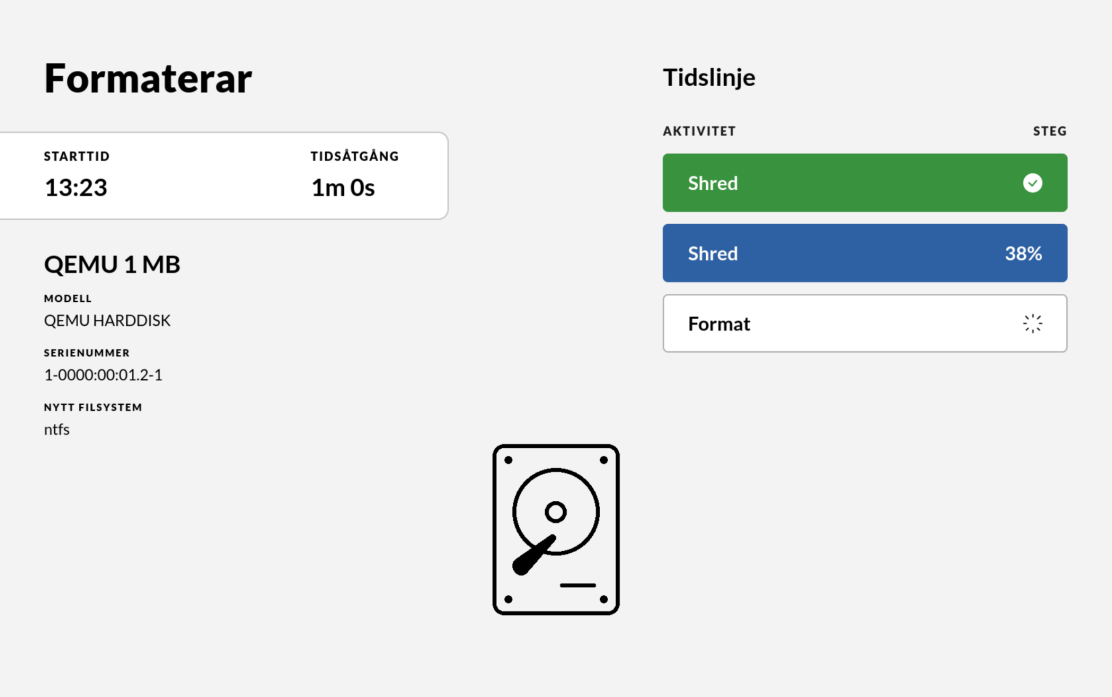
Vy efter att ha anslutit en enhet i den högra porten

1. **Anslut en USB-enhet**
2. **Tryck på knappen “Formatera enhet”**
3. **Läs informationstexten och bekräfta på knappen”**



Bekräftelsevyn

Den här vyn kommer att visa en text som beskriver de handlingar som ska ske. Om det bekräftas kommer nästa steg att formatera den anslutna USB-enheten. Om du vill avbryta är det bara att ta bort USB-enheten för att återgå.

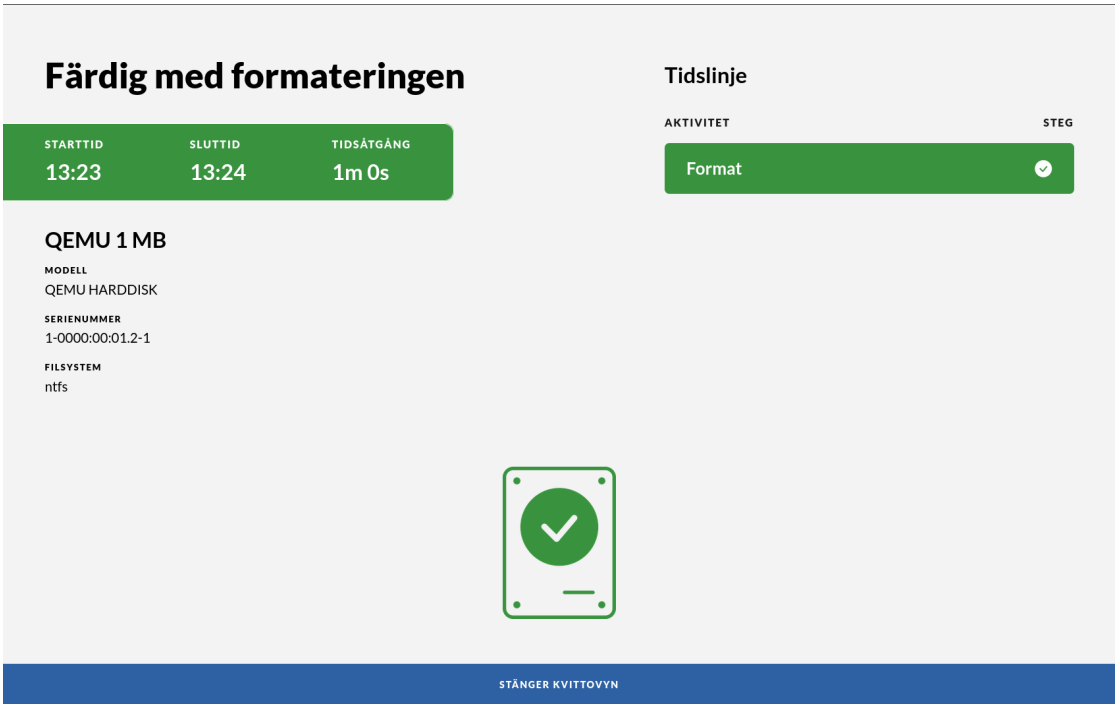


Status vyn

Den förloppsmätare som visas visar processen över formateringen.

Efter bekräftelse att användaren förstår att USB-enheten kommer att raderas och all information kommer gå förlorad kommer enheten formateras med ett nyskapat **FAT32** filsystem per default. Om enheten är större än 2TB kommer den partitioneras med **GPT** och filsystemet kommer vara **exfat**. Default-filsystemet kan ändras till **exfat** eller **NTFS** i ICC.

Efter processen kommer en slutgiltig vy innehållande ett kvitto att visas med information om USB-enheten.



Kvittovyn

Kvittot visas i den högra delen av skärmen. Kvittodelen kommer att innehålla information som:

- Märke och modell av den anslutna USB-enheten
- Namn på den anslutna USB-enheten
- Storlek på den anslutna USB-enheten
- Serienummer på den anslutna USB-enheten

4. Tryck på “Klar” och ta bort USB-enheten

USB-enheten är nu formaterad och tömd och kan användas i valfritt system.

5 Skanna en USB-enhet

Om konfigurationen “Skanna enbart” har blivit aktiverat i IMPEX Control Center kan IMPEX användas för att endast skanna en enhet utan att överföra dess innehåll till en annan enhet. Om aktiverad, kommer ytterligare en knapp visas som heter “Genomsök enhet” när endast en enhet är inkopplad. Det spelar ingen roll vilken port USB-enheten är ansluten till.

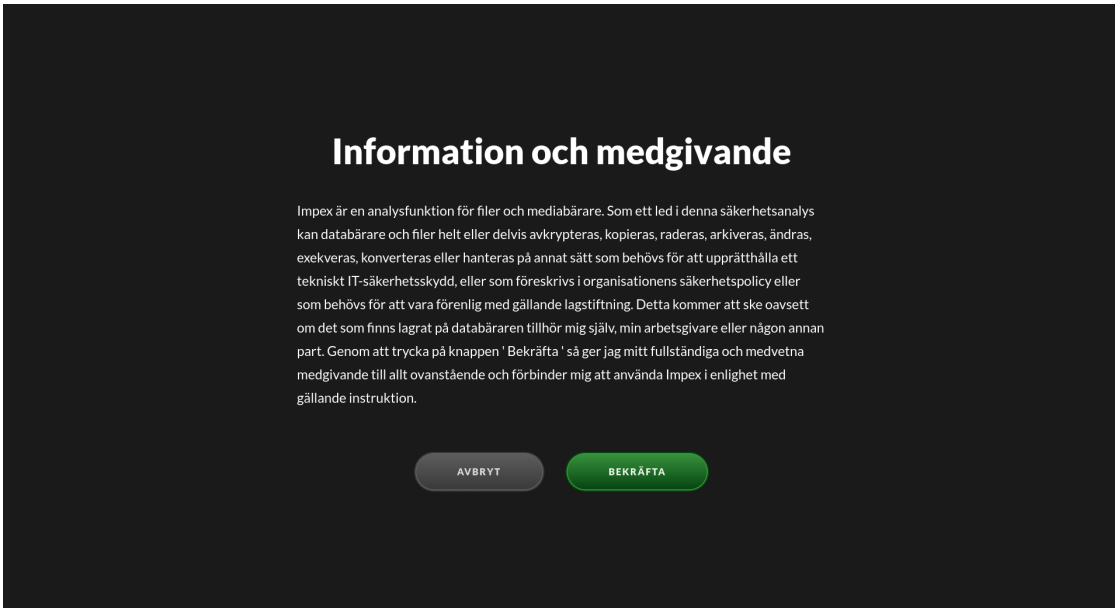
Vyn efter att ha anslutit en enhet i den högra porten

1. **Anslut en USB-enhet**
2. **Tryck på knappen “Genomsök enhet”**

Beroende på den lokala säkerhetspolicyn kan det behövas skrivas in identifikation på det virtuella tangentbordet och avsluta med “Bekräfta”-knappen för att fortsätta.

Identifikationsvyn

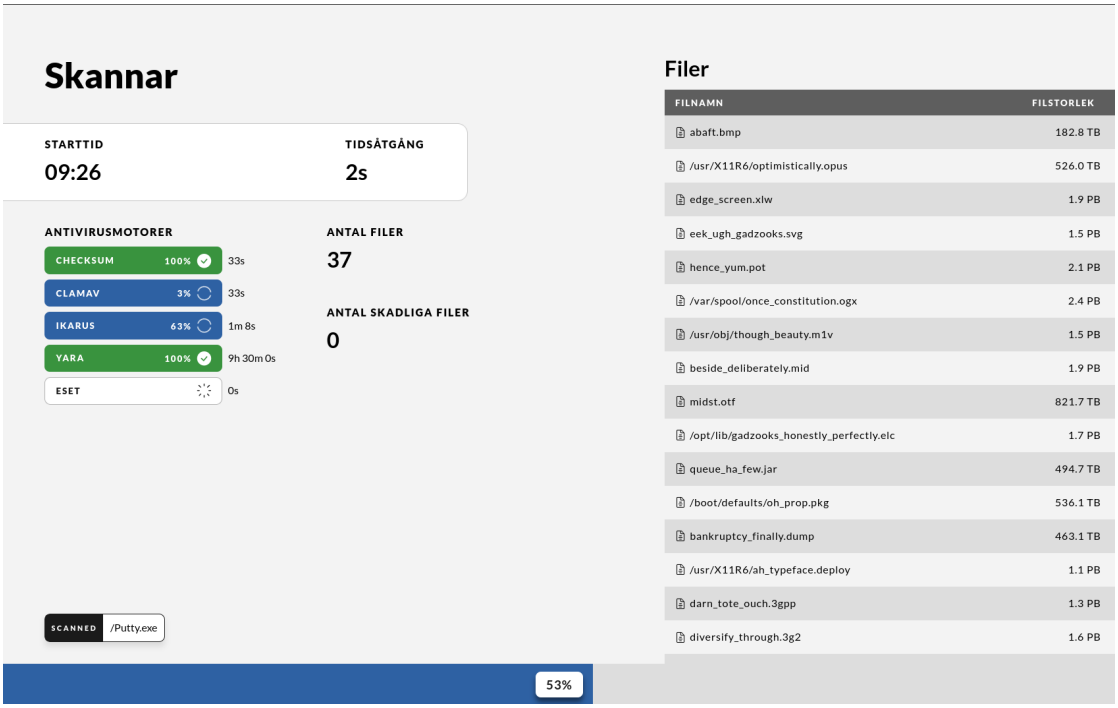
Denna vy som används för att fylla i identifikation. Om stationen har blivit konfigurerad, är det möjligt att vyn har snabblänkar för att fylla i identifikation genom förladdade namn som är möjliga att välja bland.



Bekräftelsevyn

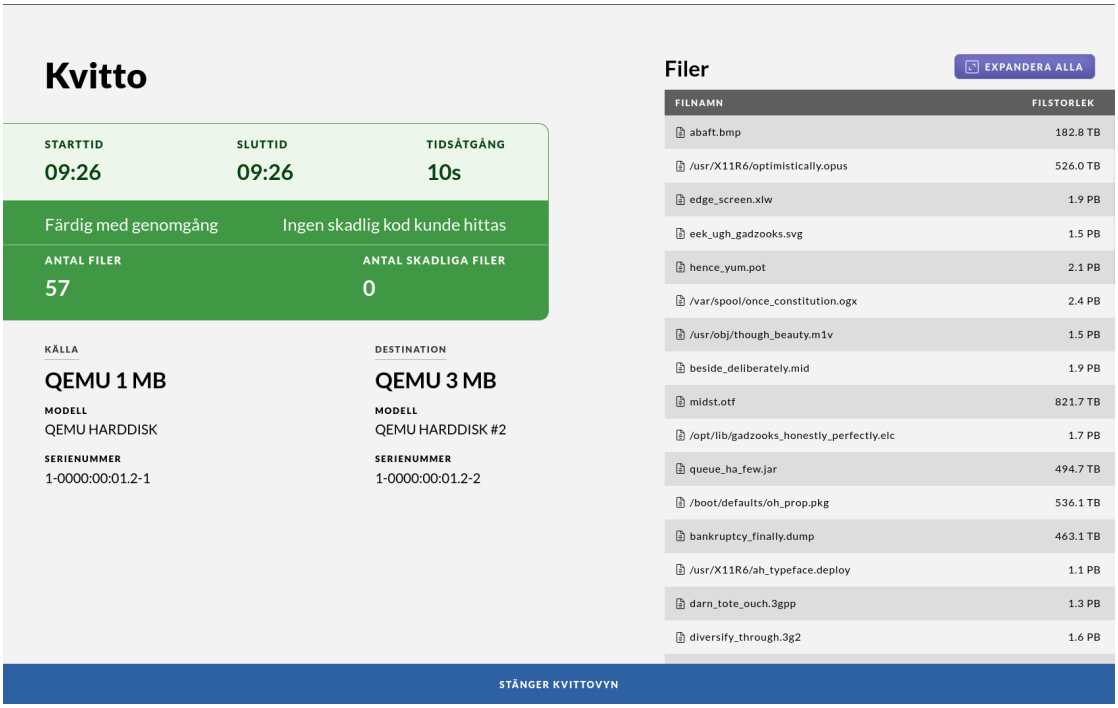
Bekräftelsevyn visar information som beskriver processen som kommer att ske. Det måste bekräftas genom att trycka på knappen för att processen ska fortsätta.

Filerna på USB-enheten kommer att bli analyserade för att leta efter skadlig kod, trojanska hästar samt annan oönskad kod. Under genomsökningen kommer tidsåtgång och en grov uppskattning av återstående tid visas.



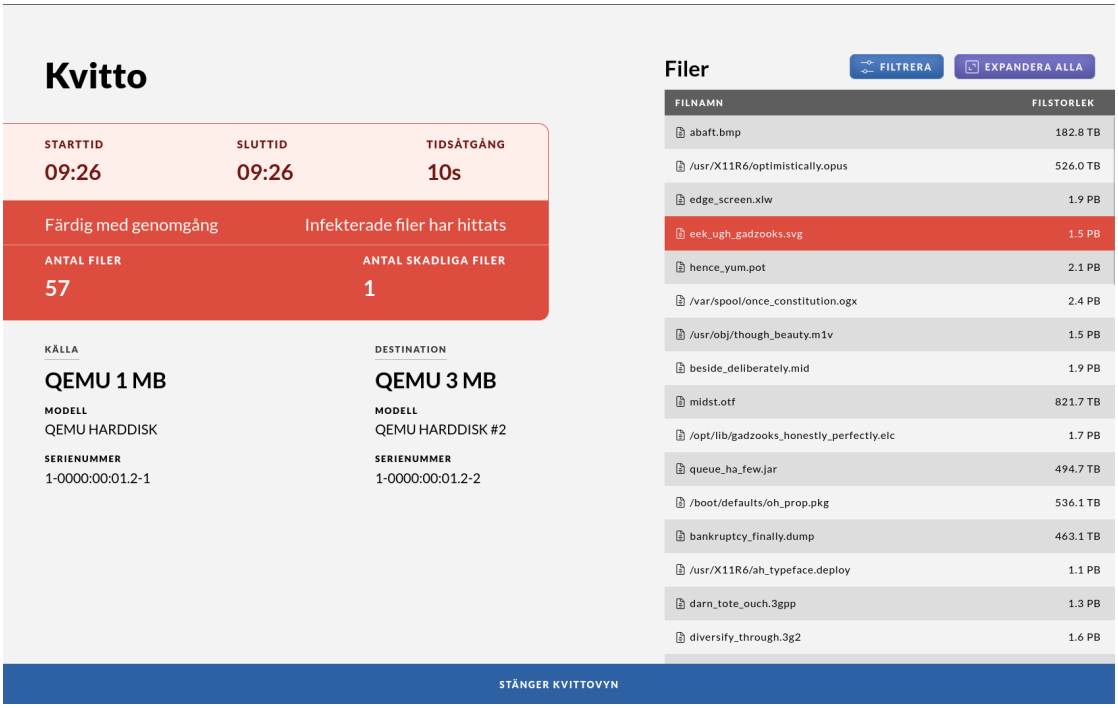
Status vyn

Om ingen skadlig kod har detekterats kommer en grön vy visas tillsammans med ett kvitto som ger en överblick av vilka filer som har blivit skannade samt deras unika checksummor. Om en skrivare är ansluten och aktiverad kommer ett kvitto skrivas ut med en sammanställning.



Sammanställningsvyn

I det fall som oönskad kod detekterats kommer en röd vy visas och fil-listningen visar då vilka filer som kan vara skadliga. Om en skrivare är ansluten och aktiverad kommer ett kvitto skrivas ut. För att endast visa de filer som är skadliga går det att trycka på knappen “filtrera”. Filerna på den genomsökta USB-enheten blir inte modifierade eller rensade från skadlig kod.



Skadlig kod hittad, vy

Den lokala säkerhetspolicyn bör beskriva vad som ska göras med en USB-enhet om skadlig kod detekteras.

3, För att avsluta, tryck på “Avsluta”-knappen eller ta bort USB-enheten.

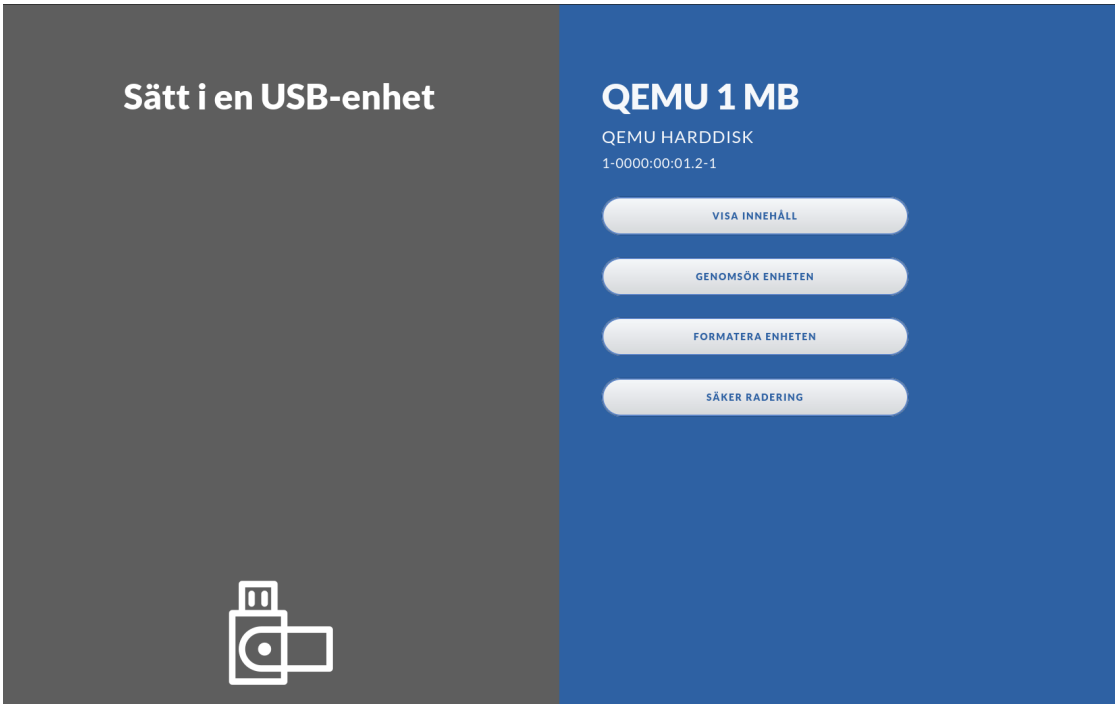
Tryck antingen på “Done” eller ta bort USB-enheten för att avsluta kvitto-vyn. Om USB-enheten tas bort medans kvitto-vyn är aktiv kommer “Done” ersättas med en “countdown” på tio sekunder och när den når noll stängs kvitto-vyn automatiskt.

För att avbryta nedräkningen trycker man på “countdown” och då kommer “Done” att synas igen och kvittot stängs bara genom att trycka på den.

Om det vid något tillfälle måste avbrytas är det bara att ta bort USB-enheten för att återgå.

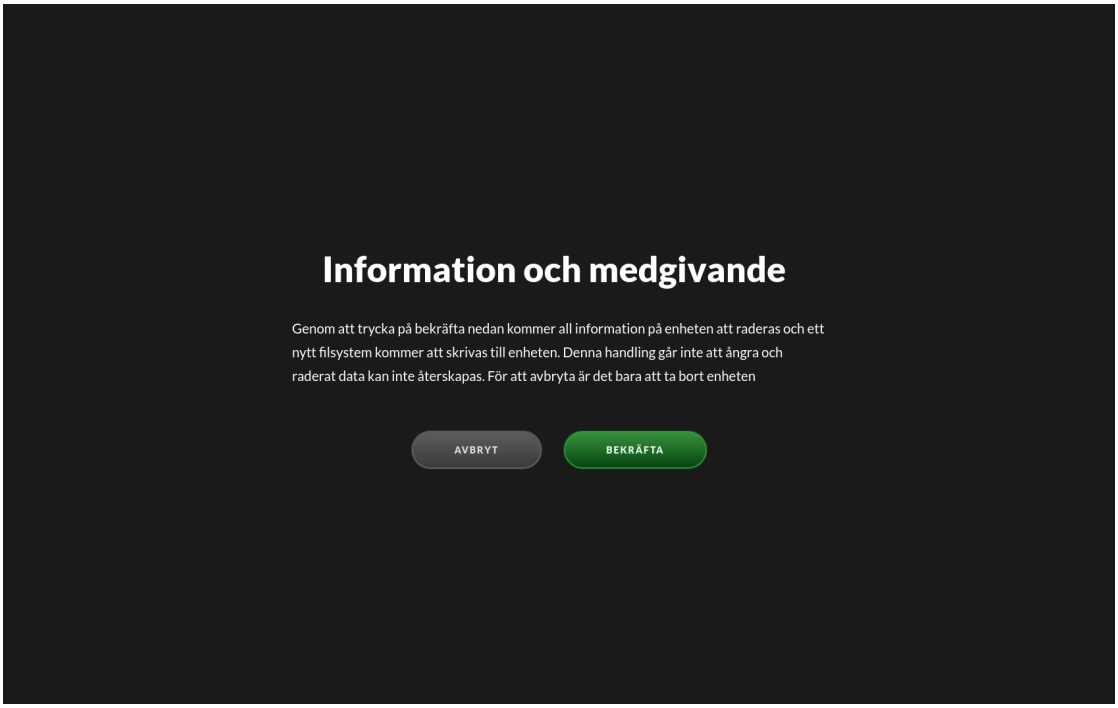
6 Säker radering (shred) av USB-enhet

Om inställningen “Allow shred only” har blivit aktiverat i IMPEX Control Center är det även möjligt att på stationen endast “shredda” en enhet. Med “shredda” menas processen att skriva över sektorer på disken med slumpmässig data. När konfigurationen är aktiverad kommer ytterligare en knapp visas när endast en enhet är ansluten. Det spelar ingen roll vilken port USB-enhet är ansluten till.



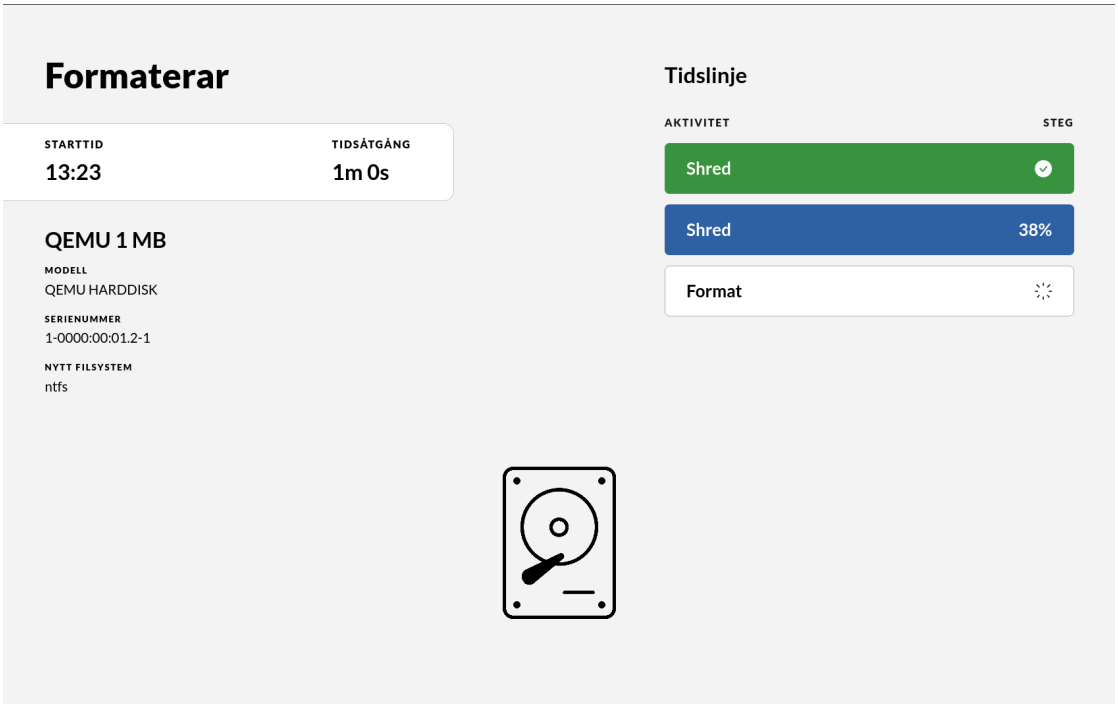
Vy efter att ha anslutit en enhet i den vänstra porten

1. **Anslut en USB-enhet**
2. **Tryck på knappen “Säker radering”**
3. **Läs informationstexten och bekräfta på knappen”**



Bekräftelsevyn

Den här vyn kommer att visa en text som beskriver vad som kommer ske. Om det bekräftas kommer nästa steg att skriva över varje sektor på disken med slumpmässig data och sedan formatera den anslutna USB-enheten. Om du vill avbryta är det bara att ta bort USB-enheten för att återgå.

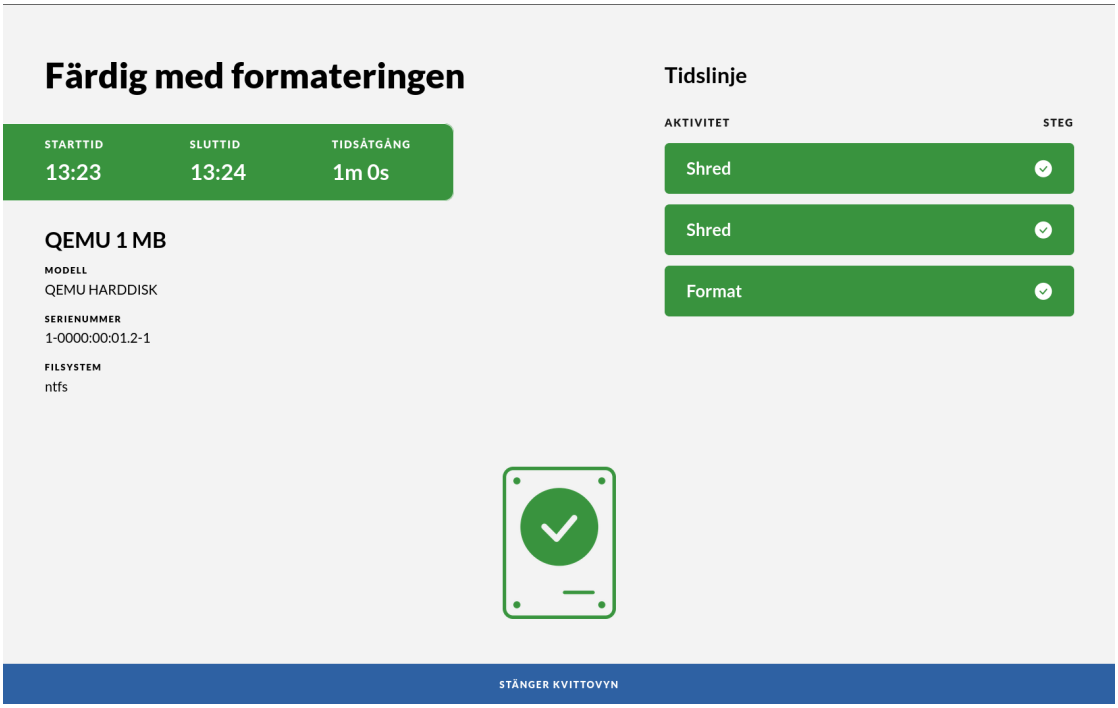


Status vyn

Den förloppsmätare som visas visar processen av överskrivningen och formateringen.

Efter bekräftelse att användaren förstår att USB-enheten kommer att raderas och all information kommer att gå förlorad kommer enheten formateras med ett nyskapat **FAT32** filsystem per default. Om enheten är större än 2TB kommer den partitioneras med **GPT** och filsystemet kommer vara **exfat**. Default-filsystemet kan ändras till **exfat** eller **NTFS** i ICC.

Efter processen kommer en slutgiltig vy innehållande ett kvitto att visas med information om USB-enheten och överskrivningen.



Kvittovyn

Kvittot visas på skärmen. Den innehåller information som:

- Märke och modell av den anslutna USB-enheten
- Namn på den anslutna USB-enheten
- Storlek på den anslutna USB-enheten
- Serienummer på den anslutna USB-enheten
- antal gånger varje sektor blev överskriven

4. Tryck på "Klar" och ta bort USB-enheten

USB-enheten är nu shreddad (överskriven med slumpmässig data) och formaterad och kan användas igen.

5. Viktigt att veta angående SSD och överskrivningar

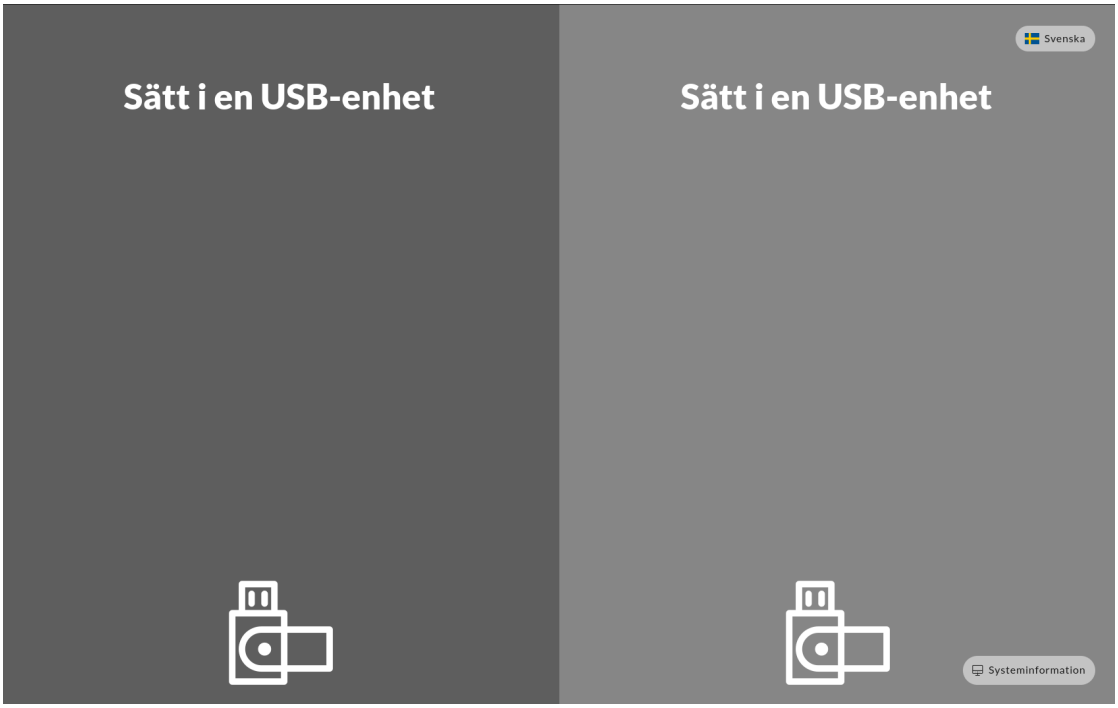
Moderna flashdiskar har inbyggd mjukvara som delegerar skrivningar till olika minnesceller varje gång för att sprida ut skrivningar jämnt över alla minnesceller. Detta kallas "wear leveling" och är en finess för att förlänga livslängden på dessa. Detta gör att även fast det ser ut om alla sektorer skrivits över så är det ingen garanti att det inte finns några minnesceller som fortfarande har känslig data på sig.

6. Bitlocker undantag

Bitlocker diskar kan inte bli shreddade då IMPEX inte kan återskapa bitlocker containern. Om en enhet har Bitlocker-kryptering kommer inte Shred-knappen att visas. Vi rekommenderar att byta Bitlocker lösenordet till något väldigt långt och sedan inte notera det vilket i slutändan i praktiken får samma effekt.

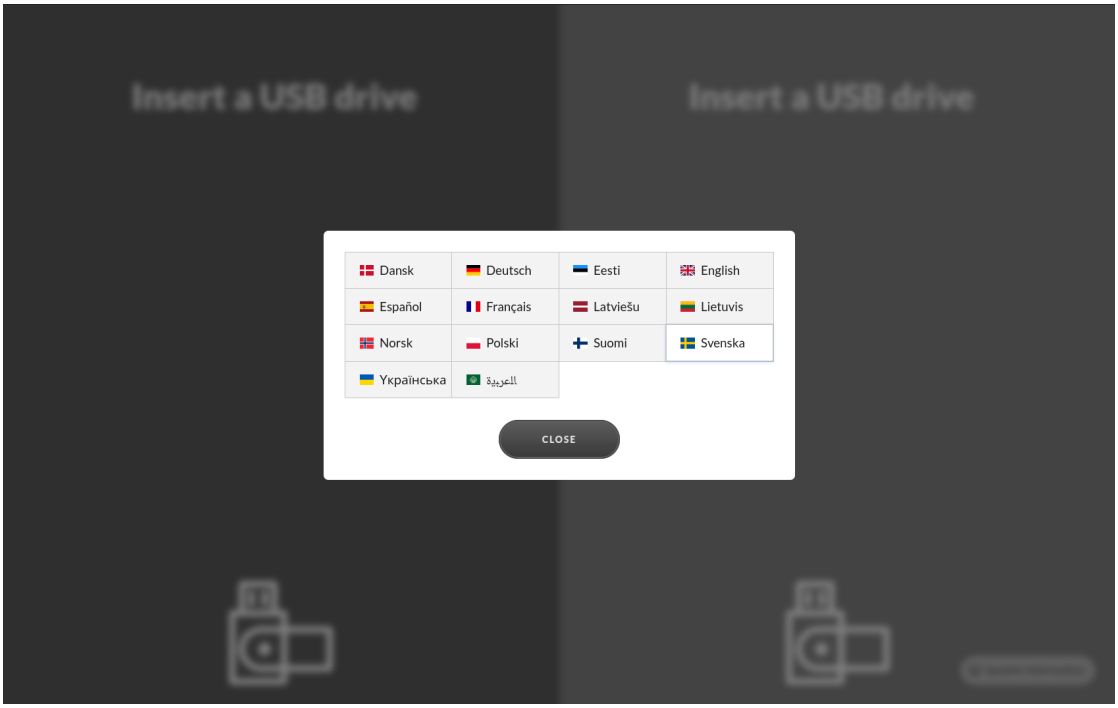
7 Byta språk

IMPEX stationens gränssnitt har support för flera språk. För att byta språk är det bara att trycka på flagg-symbolen i övre högra hörnet och välja det önskade språket.



Flaggsymbolsvyn

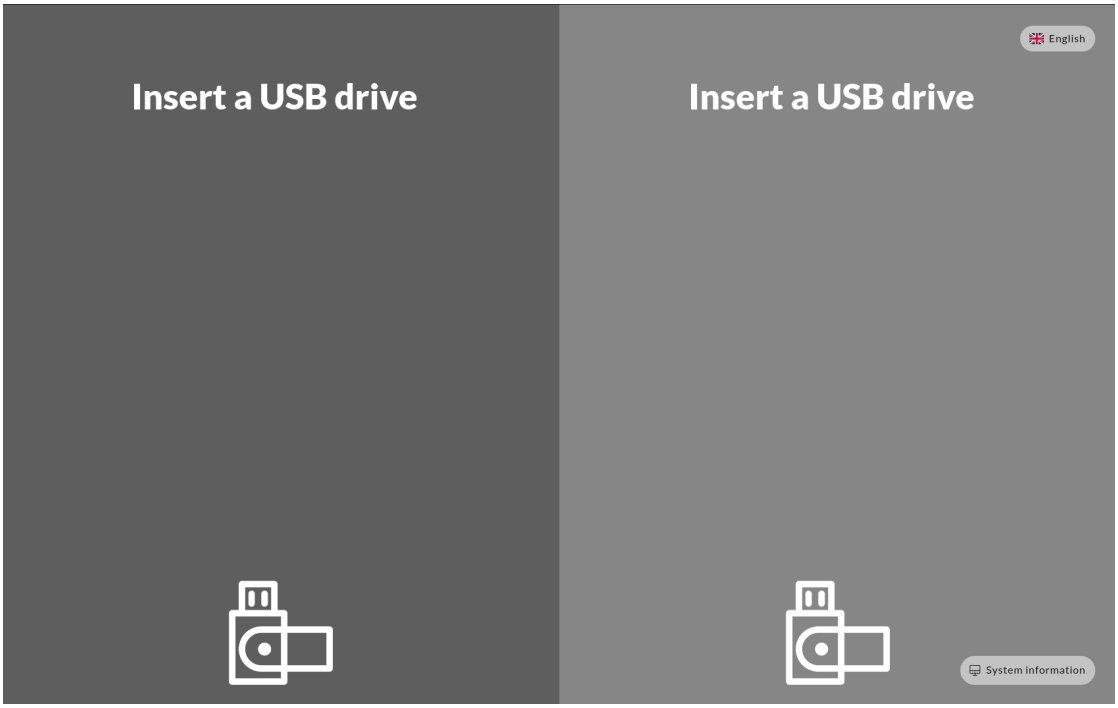
Det här är vyn med flagg-symbolen i det övre högra hörnet. Genom att klicka på den blir det möjligt att byta språk på Impex stationen.



Flaggsymbolsmenyn

När du har klickat på flagg-symbolen kommer en meny att visas. Denna meny visar de olika språk som det går att välja mellan på stationen för att få önskat språk.

Så här ser det ut i gränssnittet efter att språket har ändrats till engelska.

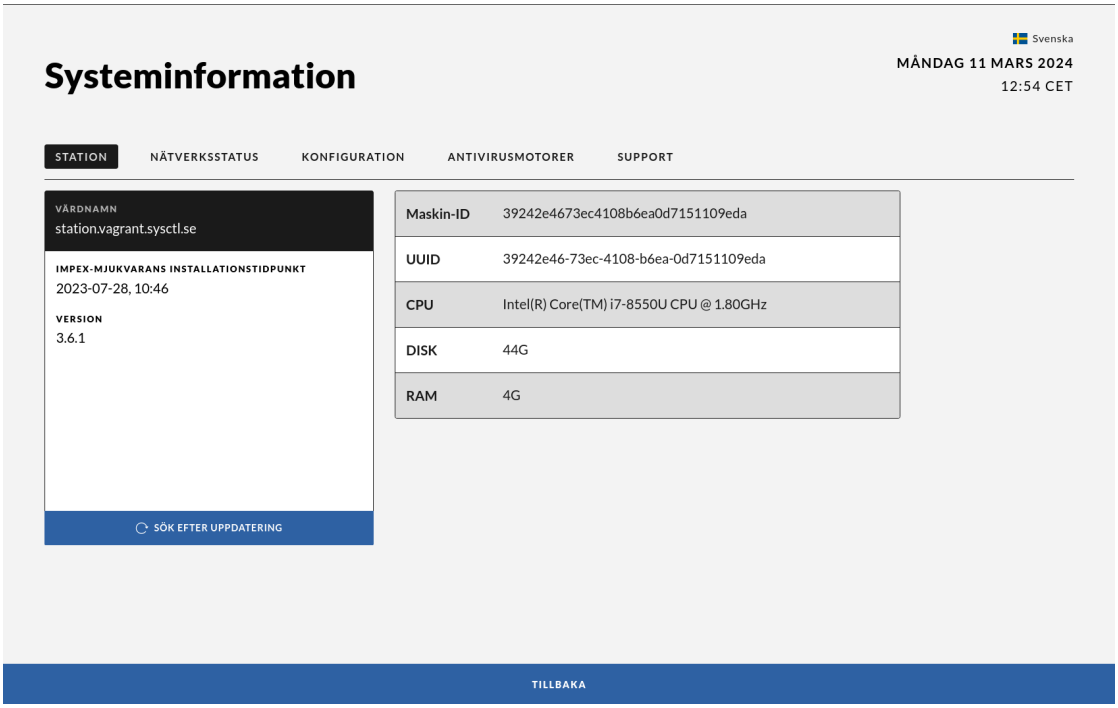


Initialvy efter att ha bytt språk till engelska

8 Systeminformationssidan

Systeminformationssidan innehåller information om konfigurationen för den aktuella stationen.

På den initiala sidan längst ner i högra hörnet är det en länk till informationssidan. Denna länk är grön i de fall Antivirus och stationen är uppdaterad, länken är röd om de inte är uppdaterade.



Syteminformationsvyn

Informationssidan har fyra sektioner. “STATION”-delen innehåller information om vilken version IMPEX-mjukvaran har, stationens identifikation och namnet. Det finns även tidpunkt för senaste hämtning av Antivirus och Operativsystems uppdateringar.

“KONFIGURATION” och “ANTIVIRUS MOTORER” - delarna visar vilka inställningar som är gjorda i Impex Control Center för den aktuella stationen. Dessa inställningar kan endast göras på serverdelen.

“NÄTVERKSSTATUS”-delen visar nätverkskonfiguration och vilken Impex Control Center som stationen är ansluten till.

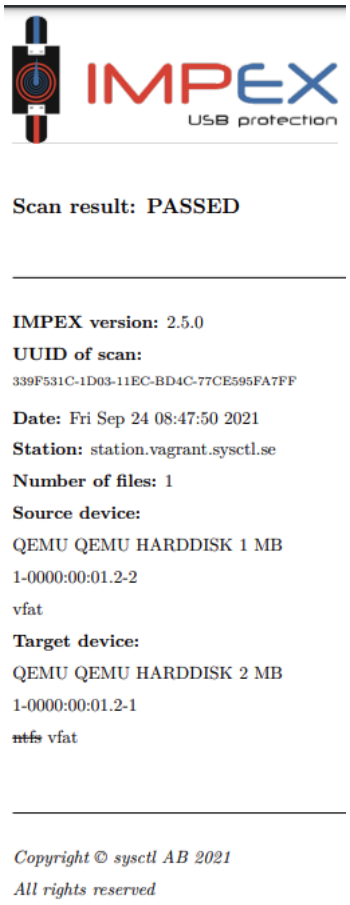
Denna sida är främst ämnad för tekniker, men kan vara användbar för andra också.

9 Exempel med utskrivna kvitton

Nedanstående bilder visar hur det fysiska kvittot ser ut när man får ut det efter en kontroll. Det ena kvittot är från en kontroll där det inte hittades någon skadlig kod och det andra kvittot är från en kontroll då man hittade skadlig kod.

9.1 Kvitto på körning utan funnen skadlig kod

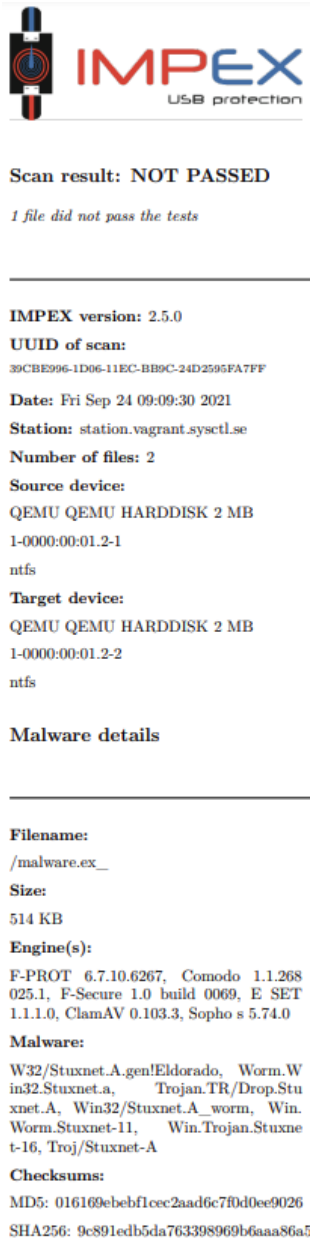
Det här kvittot är ett exempel på en utskrift som blir när Impex inte har hittat någon skadlig kod.



Kvitto på check utan funnen skadlig kod

9.2 Kvitto på körning med funnen skadlig kod

Det här kvittot är ett exempel på en utskrift som blir när Impex har hittat skadlig kod. Notera att kvittot har extra information om vilka AV-motorer som finns på Impex och de olika namn som den skadliga koden fått av de olika AV-motorerna.



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

Kvitto på körning med funnen skadlig kod

10 Skanna och överföra filer från en USB-enhet till en annan (endast textinstruktion)

Den här steg-för-steg manualen är för skanning av en USB-enhet för att upptäcka skadlig kod och om ingen skadlig kod hittas, överföra filerna till en sekundär USB-enhet.

1. Anslut käll-USB-enheten till den vänstra USB porten

2. Anslut destinationsenheten till den högra porten

Skärmen visar nu både USB-enheterna, deras märke och modell. Tryck på "Visa Innehåll"-knappen för att lista innehållet på enheterna.

3. Tryck på den vänstra pilknappen för att överföra filer till den högra enheten.

Notera att den högra enheten kommer att raderas och tömmas(formateras) för att säkerställa att den är tömd. Om käll-enheten är en CD eller DVD kommer mottagarenheten att få filsystemet **exfat**.

4. Beroende på den lokala säkerhetspolicy kan det behövas matas in identifikation på det virtuella tangentbordet. Tryck på "Bekräfta" för att fortsätta.

Filerna på källenheten kommer nu att genomsökas för skadlig kod och annan oönskad kod. Under denna process kommer en grov tidsuppskattning att göras för att visualisera den återstående tiden.

Om inte någon skadlig kod hittas kommer en grön vy visas tillsammans med ett kvitto som visar en överblick av vilka filer som skannats samt deras unika checksummor. Om en skrivare är ansluten och aktiveras kommer ett kvitto med en sammanställning att skrivas ut.

I de fall som oönskad kode hittas kommer vyn bli röd och en listning av vilken eller vilka filer som innehåller skadlig kod visualiseras. Noteras att inga filer blir överförda till mottagarenhet och den kommer därför vara tom. Om en skrivare är ansluten och aktiveras kommer ett kvitto att skrivas ut. För att endast visa de filer som innehåller skadlig kod går det att trycka på knappen "filtrera". Källenheten som innehåller skadlig kod kommer inte att bli modifierad eller rensad från skadlig kod.

Den lokal säkerhetspolicy som finns bör beskriva vad som ska göras med den USB-enhet där skadlig kod hittas.

5. För att avsluta skanningen, tryck på "Avsluta"-knappen och ta bort USB-enheterna.

Om det vid något skede finns behov av att avbryta processen är det bara att ta bort USB-enheterna från portarna. Det finns inget krav på att överföring måste ske från vänster till höger, båda riktningarna fungerar. Riktningen för överföringar kan i vissa fall vara tydligare åt det andra hållet beroende på hur stationen är placerad.

11 Administration

11.1 Uppdateringar och patchning

Impex uppdaterar sig själv automatiskt utan att något behöver utföras på stationen. Det finns två typer av uppdateringar som installeras.

- Signaturfiler
- Systemuppdateringar

11.1.1 Signaturfiler

Signaturfiler hämtas regelbundet och installeras flera gånger per dag för olika motorer. Detta påverkar inte några skanningar.

11.1.2 Systemuppdateringar

Varje natt kontrollerar stationen om det finns nya systemuppdateringar och när dessa finns så kommer de att installeras.

När en uppdatering av systemet pågår så är det inte möjligt att starta en skanning, formatering eller shred.

Om en skanning är pågående eller om det är mindre än tre timmar sedan en skanning, formatering eller shred är avslutad så kommer kontrollen efter uppdateringar att avvakta till natten därpå.

11.2 Veckovis omstart

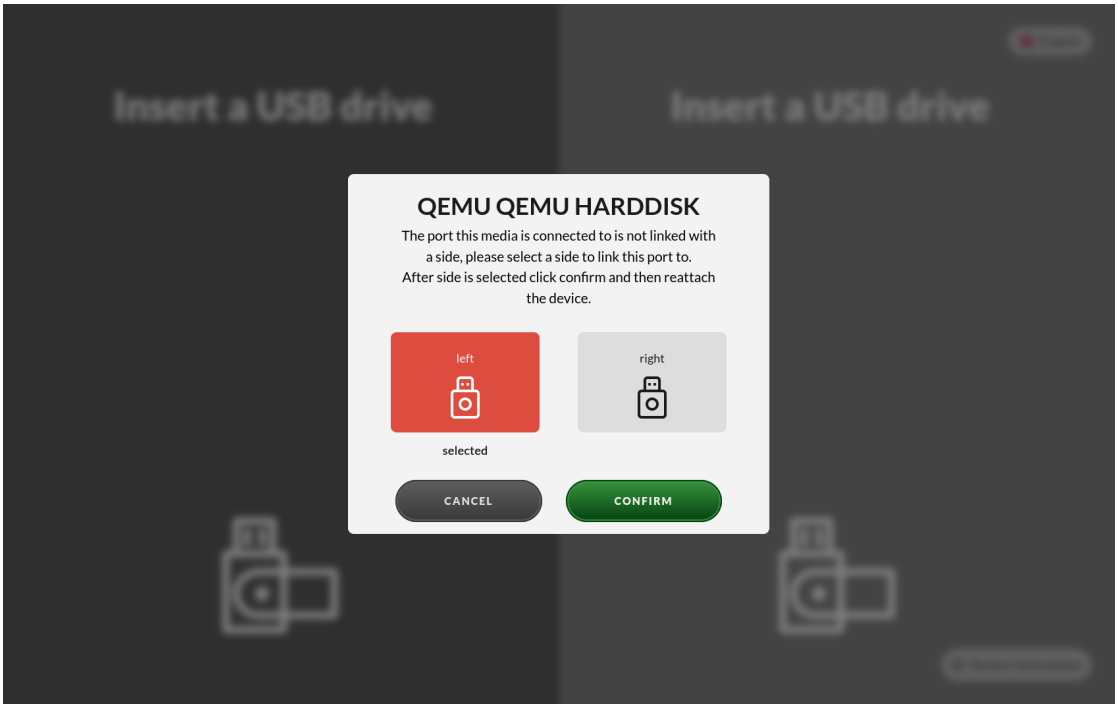
Stationen kommer att starta om en gång i veckan varje söndag klockan 06:01 på morgonen med 10 minuters slumpmässig fördröjning.

Om resultatet från kvittovyn krävs efter en skanning och det har försvunnit på grund av att stationen har startat om och ingen person har varit på plats går det att använda Impex kvittoskrivare alternativt kontrollera resultatet på servern som stationen är kopplad till.

11.3 Konfigurera USB sidor

Impex stationer använder två sidor som visualiseras på skärmen. Dessa sidor är mappade till en USB port och är namngivna som vänster och höger. Det kan finnas flera USB portar mappade mot samma sida men bara en port kan användas per sida åt gången.

I de situationer där en USB port inte är mappad, det sker normalt sätt när stationen är ny eller att sidorna har blivit återställda från ICC, kommer en dialogruta synas och fråga vilken av sidorna den instoppade USB-enheten ska mappas mot. Det är inte den faktiska USB-enheten som mappas mot en sida utan porten som USB-enheten är instoppad i som mappas mot den valda sidan.

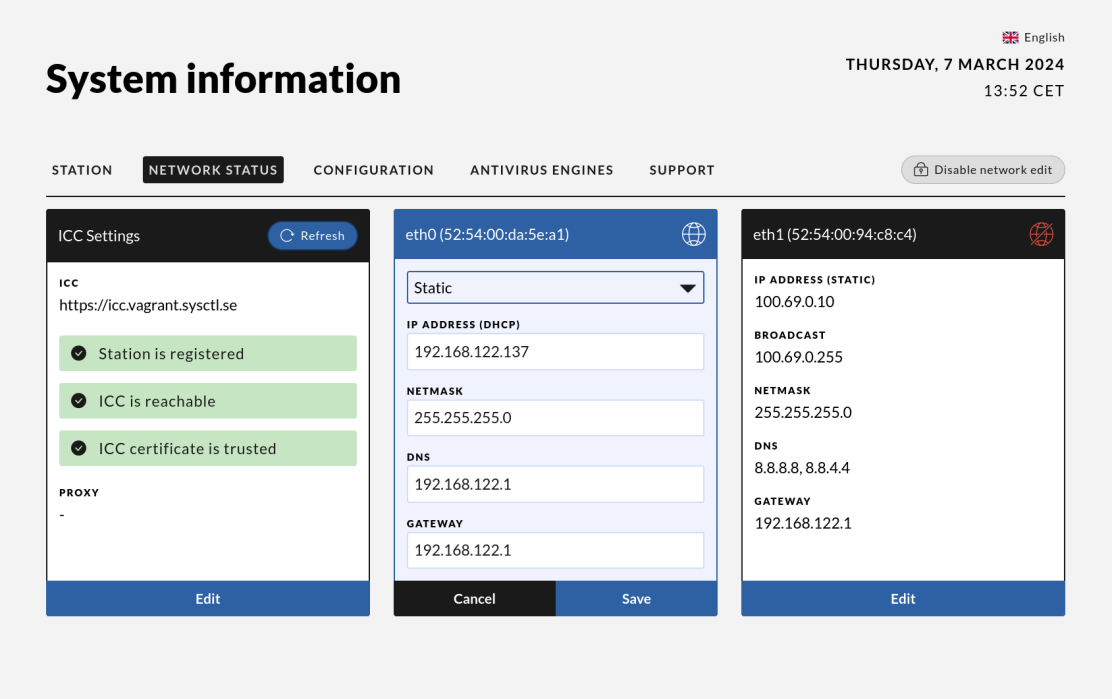


Mappa en USB port till en sida

Vy när vänster sida mappas mot en okonfigurerad USB port.

11.4 Konfigurera nätverksinställningar

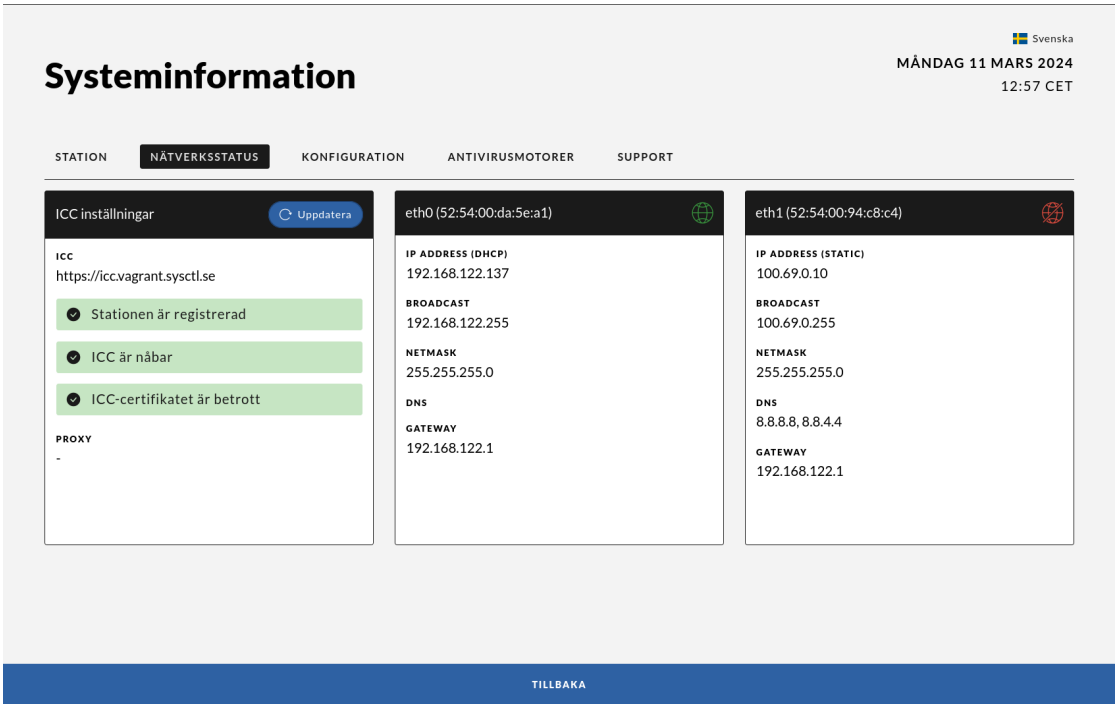
En fungerande nätverksuppkoppling krävs för att en station ska kunna få uppdateringar, konfiguration och skicka rapporter om skanningar/överföringar till ICC. För att konfigurera nätverksinställningar på en station som aldrig blivit uppkopplad mot en ICC så klicka på “Systeminformation” på skärmen och sedan “Nätverksstatus”. Klicka edit på det nätverkskort som ska ändras och välj mellan Auto eller Manual, Auto kräver ingen mer konfiguration medans Manual kräver IP-adress och nätmask. DNS samt gateway beror på det aktuella nätverket.



Konfigurera nätverksinställningar

11.4.1 Ändra nätverksinställningar

Ibland kan det vara önskvärt att ändra en stations nätverksinställningar, till exempel lägga till en proxy eller ändra stationens IP.



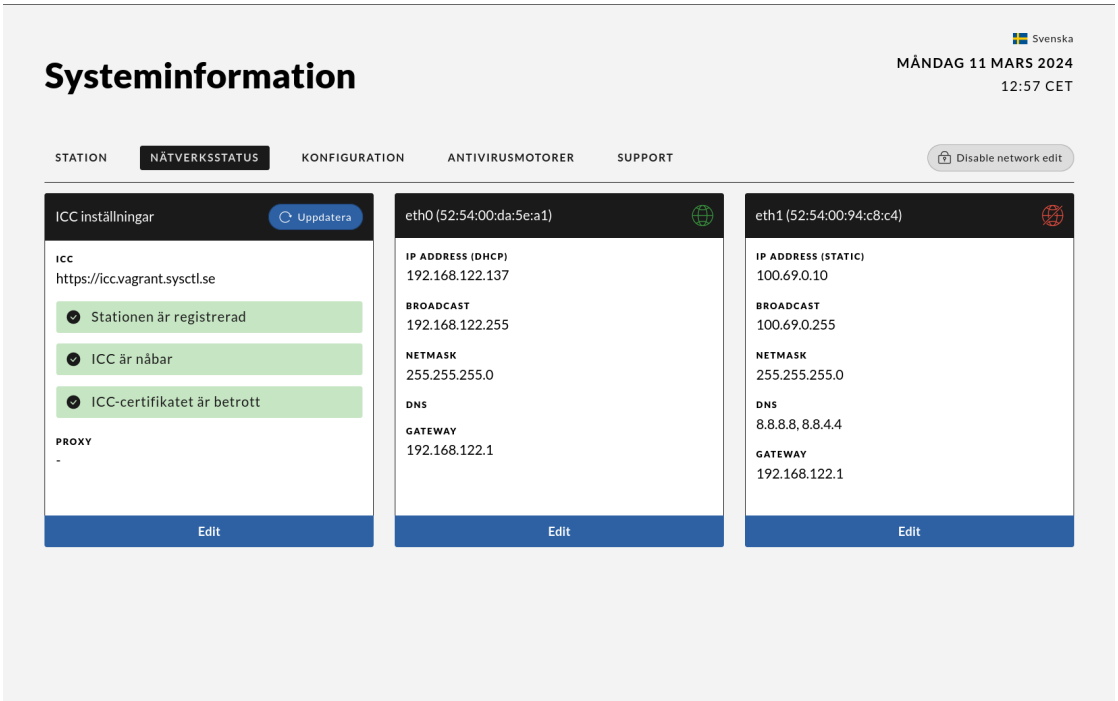
Network status

För att kunna ändra nätverksinställningar behöver du först ladda ner en “station network edit”-signify bundle som finns under server settings på ICC. Unzippa filerna och lägg dom på en USB-sticka som sedan sätts in i stationen.

Tryck sedan på “Install signed bundle from inserted device” och efter det länken för att komma till nätverksstatusvyn. Nätverksvyn kommer nu kunna editeras, både ICC-settings och interfaces.

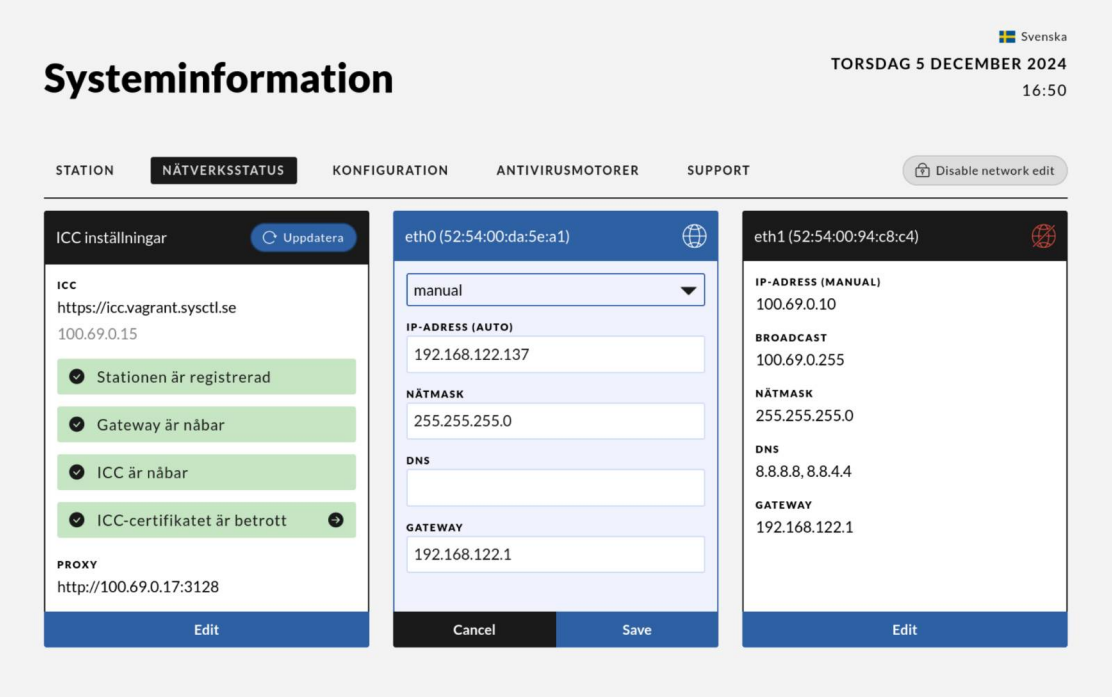
Exekvera signerad bundle

Notera att signify-bundlen bara fungerar på stationer som är kopplade till ICCn den hämtas ifrån. Den har även en tidsbegränsning på en vecka. Det genereras en ny varje måndag morgon.



View after signify-bundle

Tryck “edit” på önskad del att ändra, tryck sedan “save”.



Ändra nätverksinställningar network-settings

När alla önskade ändringar är ändrade och sparade, dra ut stickan och edit-läget kommer att försvinna.

11.5 Koppla upp mot en ICC

Klicka edit på ICC settings och ange den ICC server, användarnamn och lösenord som krävs. Dessa fält är minimum av vad som krävs för att koppla upp stationen mot en ICC. Det finns även möjlighet att mappa en IP mot ett hostname samt använda proxy.

12 Avancerad administration

12.1 Konsolåtkomst

I vissa situationer behöver en systemadministratör använda sig av konsolåtkomst för att ändra specifika systeminställningar i en Impex-station. Konsolåtkomst är enbart möjlig för den privilegierade användaren “root”. Inga vanliga konton existerar eller är användbara på en Impex.

Notera att de åtgärder som beskrivs bara bör utföras efter överenskommelse med Sysctl

Det bör noteras att de flesta administrativa åtgärderna som behövs för att hantera en Impex station kan göras från en server av typen Impex Control Centre, ICC. Det är en webbaserad

managementstation. I vissa särfall kan det dock behövas direktåtkomst till stationen för att hantera udda tekniska ändringar. Via konsolåtkomst kan man bland annat göra följande:

- Ändra lösenord eller inloggningsuppgifter till ett trådlöst nätverk
- Temporärt ändra rootlösenordet på stationen
- Felsöka nätverket
- Förkrav
  - För att kunna få åtkomst till konsolen behövs det ett tangentbord
  - Tangentbord måste vara tillåtet i stationen
  - tangentbord är inte tillåtet som standard

Om stationen inte har kontakt eller åtkomst till sin ICC-server, så är det ändå möjligt att ändra den s.k. UDEV-regeln som spärrar skärmåtkomst.

12.1.1 Singel-boota en station för att sätta ett nytt lösenord

Tangentbordslayouten är engelska i grubmenyn.

1. Anslut tangentbord i en USB-port
2. Starta om stationen genom att trycka en gång på startknappen och vänta till stationen är avstängd
3. Tryck på startknappen igen för att starta upp stationen
4. Tryck på *ESC*-tangenten under uppstart för att kommma in i GRUB
5. Skriv in användarnamnet *root* och grub lösenordet(går att hämta ut från ICC servern
6. Skriv *normal* och enter samt tryck en gång på *ESC*
7. Tryck på “e” för att kunna editera boot-parametrar
8. På raden som börjar med linux, lägg till “rw init=/bin/bash” i slutet på raden
9. Tryck *CTRL+x* för att starta upp i “single user mode”
10. skriv *passwd* för att sätta ett nytt lösenord
11. skriv kommandot *touch /.autorelabel* för att säkerställa att samtliga filer får rätt SELinux-labels
12. skriv kommandot *exec /sbin/init* för att start om stationen

12.1.2 Stänga av UDEV-regelverket manuellt

1. Singel-boota stationen för att sätta ett nytt lösenord
2. Innan omstartskommandot i steg 12:
3. Ändra *“udev_rule”: true* till *false* genom att ändra i filen

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

4. Starta om enligt steg 12