uBreakiFix Samsung Guide Contents

Portal: In-Warranty Portal Flow

Pricing Website > Samsung > Guides > Samsung Guides > IW Portal Flow

Systems: Samsung Guides

Pricing Website > Samsung > Guides > Samsung Guides > Samsung Guides SharePoint

This has TONS of information regarding Samsung common errors, work order flow, credentials management, ect. This SharePoint is maintained by corporate, and thus is always the most up-to-date resource.

Process: How to Keep Credentials Active (Daily Checklist)

- Generate OTP on GSPN on SIvI account
  - GSPN > Knowledge > Hover over Engineer > Mobile Authorization (under Mobile SVC)
  - Enter the Certificates Password on the left side and login
    - The "Plugin Error" messages can be IGNORED; close it out by clicking OK and Done
  - Click the Reissue button to generate your OTP
- Generate MOTP on GSPN on M account
  - GSPN > Admin (top right) > M-OTP Management > Generate
- Confirm Engineer on GSPN on M account
  - GSPN > Admin (top right) > M-OTP Management > Engineer Management > Enter SIvI account > Confirm
    - You must search for your **full** SIvI account name (ex. uBiFXXXSIvI01).

GD Tool: Common Resolutions

- Confirm Fenrir and GD Tool are not both open at the same time.
    - They can both “fight” for USB permissions.
- Try a different USB cable on a different PC port
- Confirm device has enough storage (> 3gb)
- Unplug, revoke USB debugging authorizations, toggle USB debugging off and back on
- Use Fenrir to reinstall Samsung USB drivers.
- Android System Web View
    - Settings > Apps > and search for "WebView". Once you find that app, tap the 3 dots on the top right and Uninstall Updates
- Restart PC
- Uninstall and reinstall GD Tool
- Try using #help channel on Slack
- Use chat function in lower right of ZenDesk

OJT: MOTP GSPN

Introduction

This document is intended for Admin technicians who need to set up the MOTP device. Read through this guide before attempting to create a new MOTP device. Launch date is set for 11/26/2024.

Information

Prerequisites

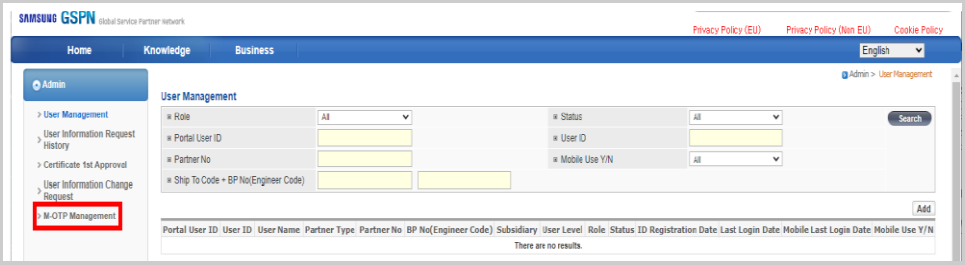
- Only Admins (not regular users) can be assigned to generate the one-time password
- Multiple users can't generate the password
- Set up will delete any previous person previously able to create passwords
- Just like a user can't have multiple GSPN accounts, it's the same with MOTP
- If the MOTP Admin is not at work, a new Admin user needs to be approved and the both accounts updated

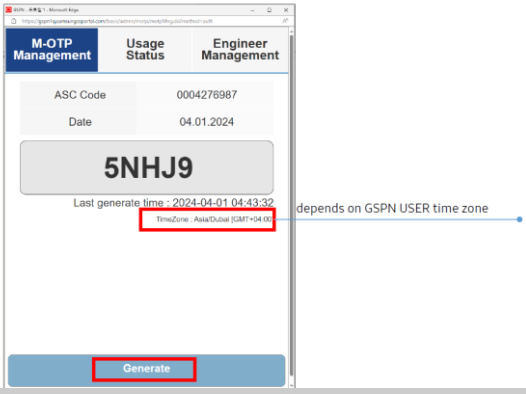
Resolution

Set up a new MOPT user in GSPN (must already have Admin privileges)

New MOPT User

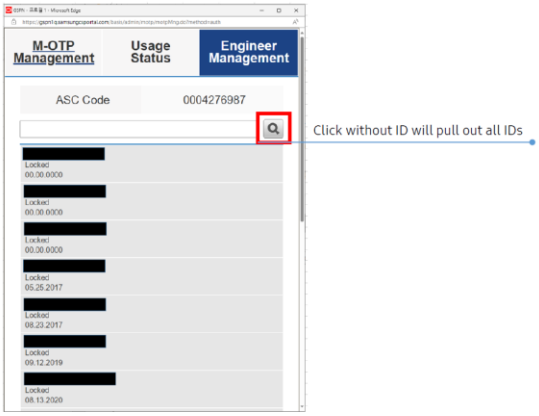
Step	Action
1.	GSPN > Admin > MOTP Management
2.	☐ M-OTP Management
3.	Usage Status Tab

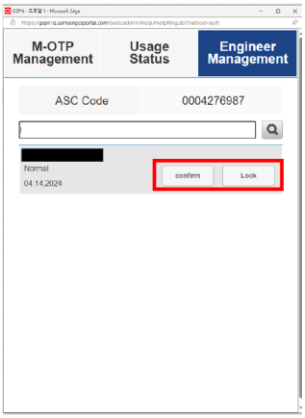




Revised October 28, 2024

4. Engineer Management Tab

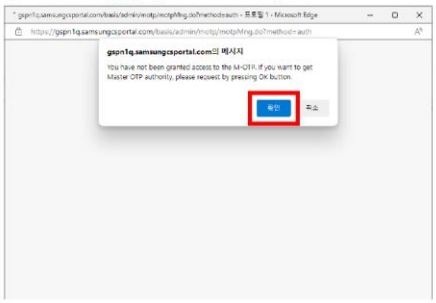




How to sign up for MOTP authority

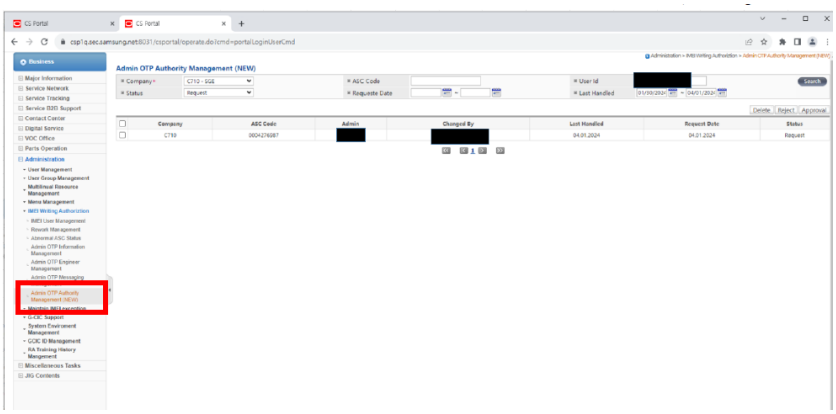
1. Only one person can apply for MOTP authority
2. To apply

① Confirm on applying M-OTP authority



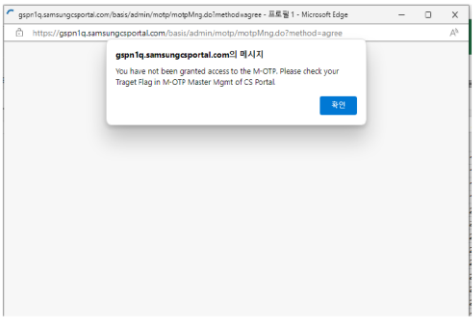
② You need to consent on security complian

3. New Menu in CS Portal (CSP)

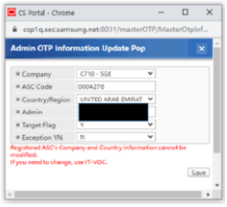


Error Messages

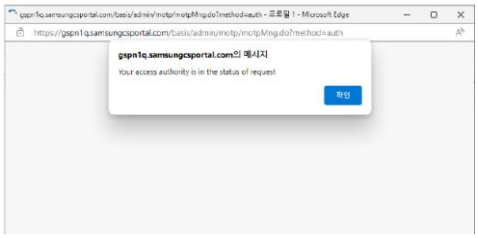
1. If you get an error message, your GSPN ID is not assigned to access MOTP. Contact your CS Portal Admin for access



CS Portal > Administration
> IMEI Writing Authorization
> Admin OTP Information Management



2. You can't access the MOTP until access is approved



FAQs

Q. What to do if the MOTP user is absent?

A. Since only one user is authorized to create a MOTP at a time, if the main MOTP user is absent an alternative user will have to be set up.

1. CS Portal > Business > Administrator > IMEI Writing Authorization > Admin OTP Information Management
   - The updated user must also be an Admin User so you have to replace that user, then request a new one > have it approved

2. When the alternate user tries to open MOTP menu, GSPN will ask the user to request the MOTP. Since this can't be done, you have to request a new MOTP authority and have it approved
   - CS Portal > Business > Administration > IMEI Writing Authorization > Admin OTP Authority (New)

Revision History

The following table lists the revisions made to this OJT resource.

Version	Released	Revision
1	10/25/2024	• First published edition of this document.

Samsung Warranty Policy and Check In Procedure

Overview

This guide will walk you through step by step on how a technician should inspect, troubleshoot and repair Samsung mobile devices with specific focus on how to accurately identify and maintain a Samsung device's warranty status based on the condition of the device.

ubreakifix BY asurion

Index

ubreakifix BY asurion

Physical Condition

Overview

ubreakifix BY asurion

Overview

The first step in warranty eligibility is to verify that the customers device does not have any physical damage that will void their warranty status.

Flip and Fold Devices

For foldable devices you will need to take a deeper look at the device to determine if there is any physical damage that will void the device's warranty status. Similar to the Galaxy S devices, we want to ensure the back glass, outer display, camera deco, etc. are all free from damage on the outside of the device. Detailed examples found on slides 7 through 25.

Once you have inspected the outside of a foldable device, please go to slide 12 for a more in-depth analysis on the inner display inspection process.

Galaxy S and A Series

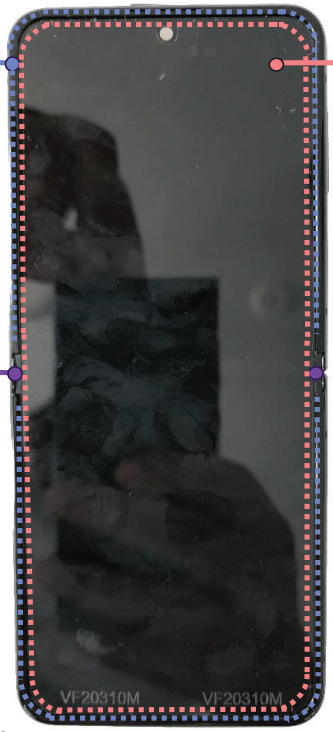
For non-foldable devices, any degree of physical damage will void the warranty. This includes cracked or broken back glass, camera deco, front glass, or the LCD being cracked underneath. Detailed examples found on slides 27 through 33.

For both repair types, techs should also be careful to not damage or break the screen during disassembly to avoid risk of chargebacks.

Damage Inspection Point Glossary

Front Deco

P-CAP



Display Panel Assembly

ALL INSPECTION POINTS REQUIRE PROPER EXAMINATION TO QUALIFY FOR IN-WARRANTY SERVICE

Protect Cover & Frame Housing

Hinge Housing

ubreakifix BY asurion

Flip & Fold

Physical Condition

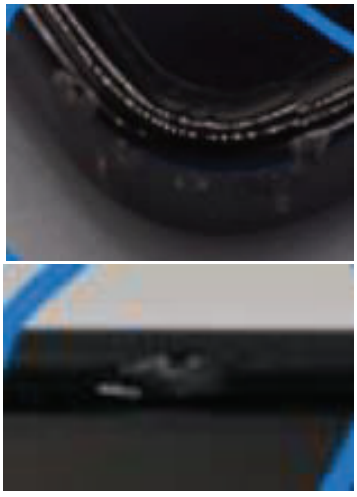
Deco & P-Cap

ubreakifix BY asurion

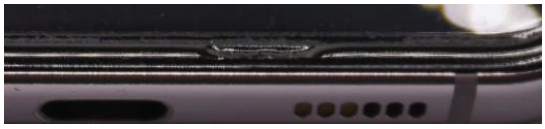
Deco & P-Cap Overview

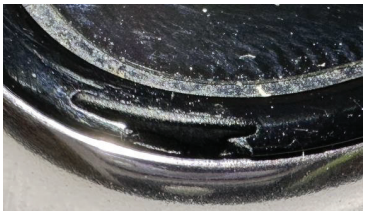
IMPORTANT – You must remove the film protector from a flip or fold device to properly inspect the display. Failure to do so will impact your ability to make the proper determination which could result in a charge back.

1. Any damage to the deco and/or p-caps will result in an out of warranty status. All examples below would be out of warranty repairs



All of the chips present on the example on the left would make the repair OOW

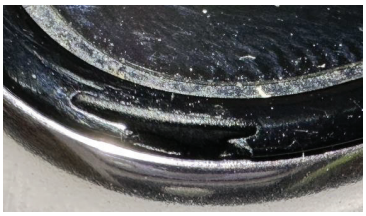




If the deco or p-cap has any chips, cracks, or missing pieces the repair is considered out of warranty and should be charged to the customer

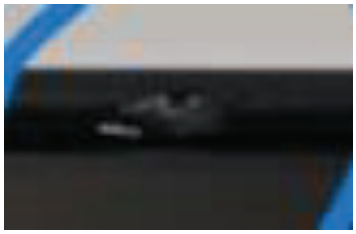
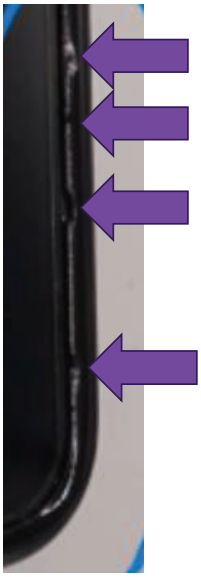
ubreakifix BY asurion

Deco Damage

IW	OOW
 Minor cosmetic scratches should be considered IW	   Any cracks, chips, gouges, or missing pieces of the deco should be considered OOW

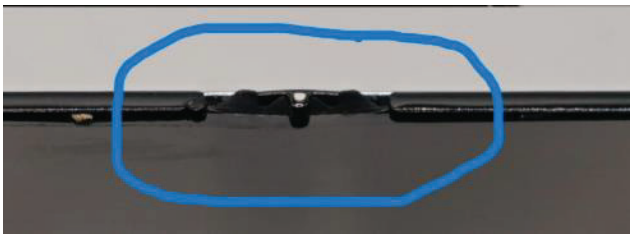
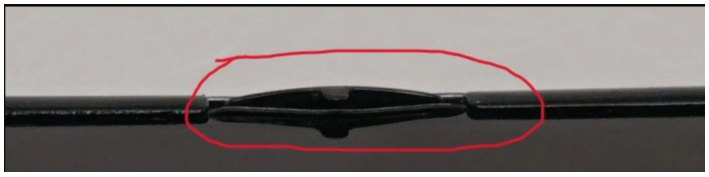
ubreakifix BY asurion

Deco Damage Continued

IW	OOW
   Minor cosmetic scratches should be considered IW	   Any cracks, chips, gouges, or missing pieces of the deco should be considered OOW

ubreakifix BY asurion

P-Cap Damage

IN WARRANTY	OUT OF WARRANTY
	 Damage present on P-Cap (misalignment of ribbon)
	 P-Cap protruding out more than usual

ubreakifix BY asurion

Flip & Fold

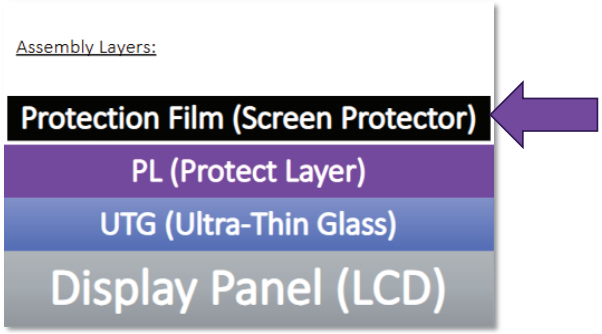
Physical Condition

Inner Display Cracks

ubreakifix BY asurion

Inner Display Cracks Overview

Once you have verified that there is no damage to the deco or p-cap we will need to inspect the display itself.



This image portrays how the different layers of a foldable display are laid out and why it is so important to remove the screen protector first.

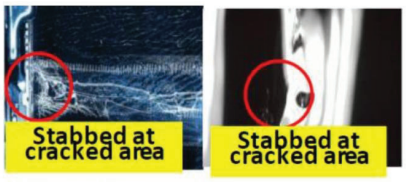
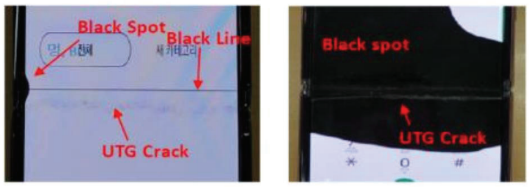
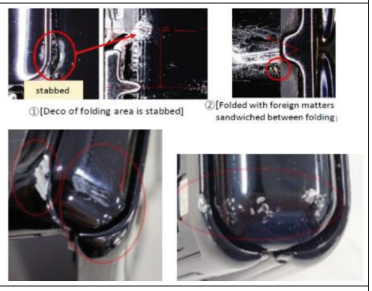
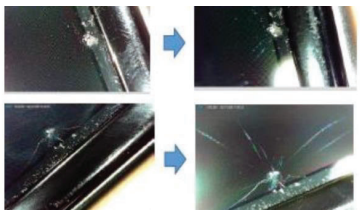
Once removed, you will then be able to fully inspect the PL (protective layer) and have a better look at any potential UTG (ultra thin glass) or LCD cracks underneath.

The next few slides will help you understand the different variations of screen issues on the UTG (Ultra Thin Glass).

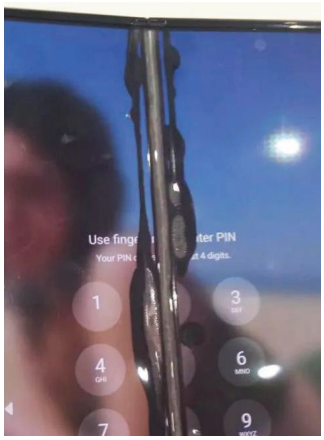
ubreakifix BY asurion

Ultra-Thin Glass (UTG) Crack

Identifying IW vs. OOW

Symptom	IN WARRANTY	OUT OF WARRANTY
UTG Crack Only	UTG cracks in the folding area appear as multiple inconsistent lines. 	Torn surfaces are rough to the touch; stabs are not symmetrical 
Black/Gray Spot, White Line	If the folding area has any of these or other types of damage, check for physical drop damage 	Examine the deco, P CAP and hinge carefully for stabs/scratches/presses  
Damage away from the crack 	No tear on the screen or radial cracks (a crack that spreads in multiple directions from a single impact or pressure point) 	 Use a light source to check for radial cracks even if the damage is away from the UTG symptom. These are OOW cases even if the crack is not near the symptom

Ultra-Thin Glass (UTG) Crack (Continued)

IN WARRANTY	OUT OF WARRANTY
  	  

ubreakifix BY asurion

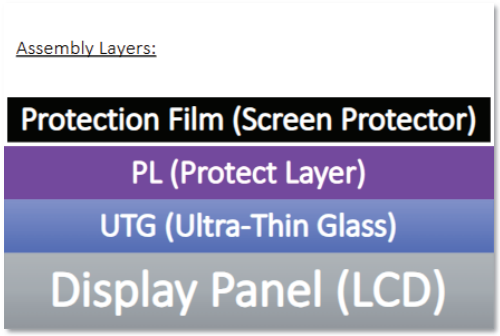
Identifying Types of Cracks

There may be times that a device looks like it has a UTG crack, but it is a different layer of the display that is damaged.

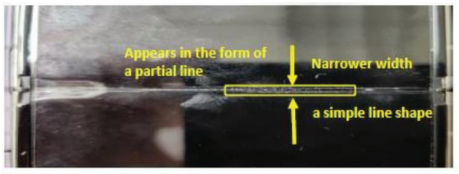
Use this section as a tool to assist in troubleshooting the type of repair needed.

A device that has a crack in the Protective Film (PF) may look like it has a crack in the UTG. To determine which it is, follow these steps:

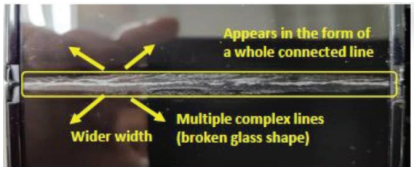
1. Remove the Protective Film
2. Remove any remaining adhesive
3. If the UTG is normal, recommend replacing the Protective Film



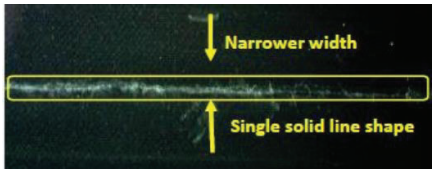
Protection Film Crack -> Replace Film Only



UTG Crack -> Follow In-Warranty Troubleshooting on slides 7 and 8



Display Panel (LCD) -> Out of Warranty



ubreakifix BY asurion

Flip & Fold

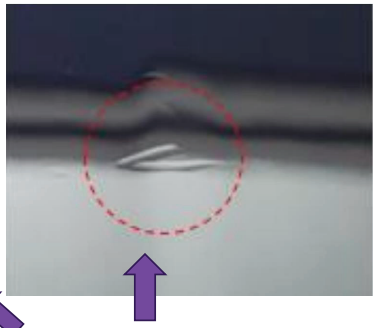
Physical Condition

Inner Display Screen Defects

ubreakifix BY asurion

Inner Display LCD Defects Overview

When determining if screen defects such as dead pixels, black spots, white lines, etc. are covered under warranty there are a few things we need to inspect. As you will see throughout the next few slides, identifying marks in the PL (protective layer) will be key in determining if the identified blemishes were a direct result on the screen malfunction.



Any screen malfunctions on around marks/blemishes like this should be considered out of warranty and be at the cost of the customer.

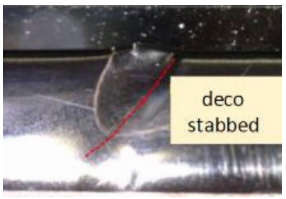
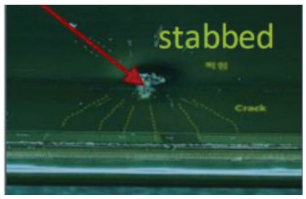
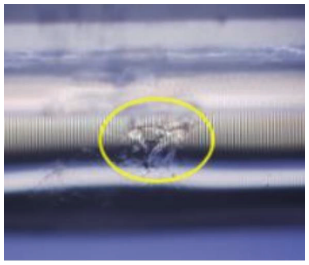
If the screen is blank or you are unable to separate any blemishes from the malfunction you will need consider the repair out of warranty.

Excessive damage to the outside of the device, especially on or around the hinge can also directly void the warranty of the display on the other side.

ubreakifix BY asurion

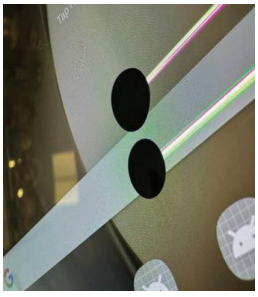
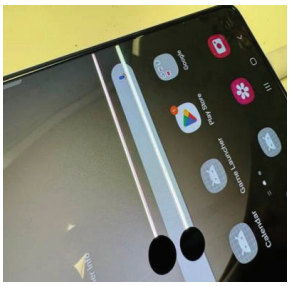
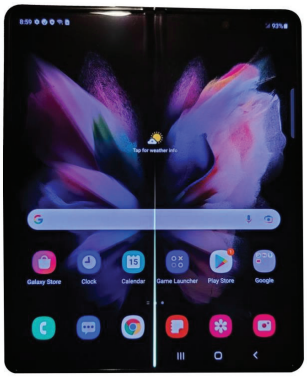
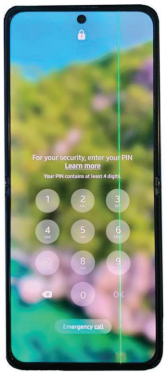
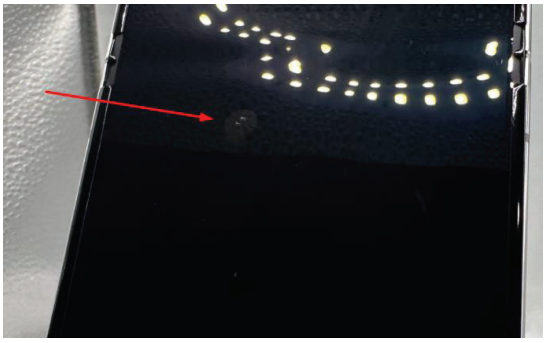
White Line

Identifying IW vs. OOW

Symptom	IN WARRANTY	OUT OF WARRANTY
At fold		The white line symptom at the folded area should be handled as Out-Of-Warranty when there is a stab, scratch, or press Examine the P CAP, Deco, and Hinge area for physical damage   

ubreakifix BY asurion

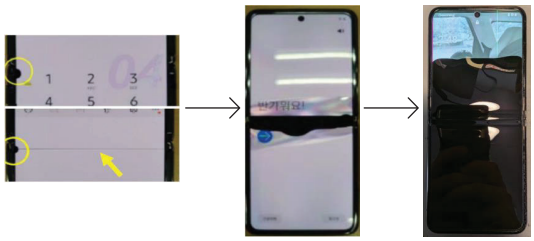
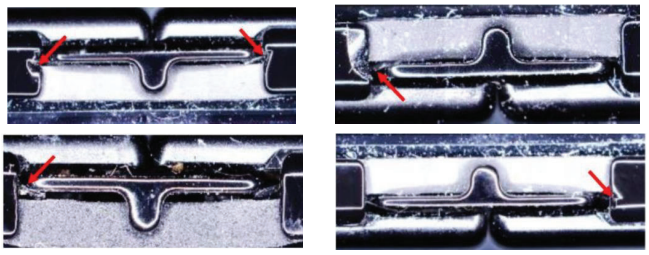
White Line (Continued)

IN WARRANTY	OUT OF WARRANTY
    	 

ubreakifix BY asurion

Black Spot

Identifying IW vs. OOW

Symptom	IN WARRANTY	OUT OF WARRANTY
At fold	  A small black spot may grow over time and can even cause the LCD to go completely blank	1. Inspect the hinge area for damage  2. Visual inspection on or near the P CAP area for damage  Black Spot due to physical damage (on/near the hinge area, P CAP, Deco or at the spot of the symptom) should be handled as Out of Warranty

ubreakifix BY asurion

Bright Dots

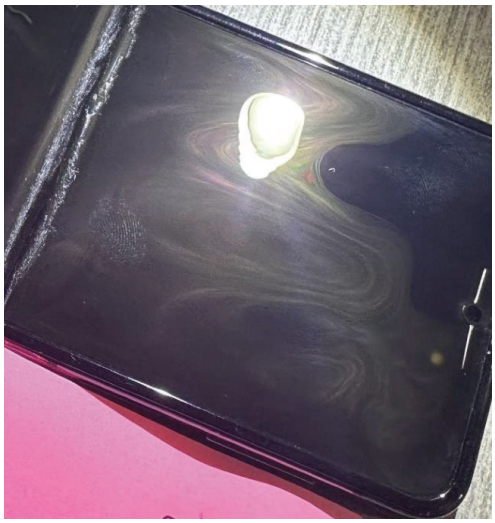
Identifying IW vs. OOW

Symptom	IN WARRANTY	OUT OF WARRANTY
Single bright dot		 
Multiple bright dots		If there is any direct damage trace (Stabbed/Scratched/Pressed) on the Bright dots of the screen, it should be handled as Out of Warranty   [cave in]

ubreakifix BY asurion

Black Screen

Identifying OOW (screen lifting)

Symptom	OUT OF WARRANTY	
Device power turns on, but there is no working display (only vibration or sound work)	In some cases, the Display assembly will begin to lift or peel from the frame (deco and p-cap). This is strictly an out of warranty case and should be charged to the customer. Causes: • IC Crack due to strong pressure of the surface • Corrosion of display parts due to water damage • Screen scratched, display damage due to drop 	

Flip & Fold

Physical Condition

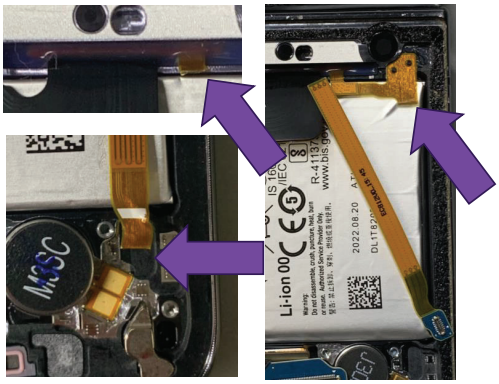
Chargeback Avoidance

ubreakifix BY asurion

Flip and Fold Chargeback Common Occurrences

Once you have properly deemed a Samsung device In-Warranty we need to ensure we are using proper repair techniques. If you DIP (Damaged in Process) an In-Warranty core your location will be subject to a chargeback. Below you will see some common occurrences that resulted in chargebacks.

1. Torn or missing flex cables



2. LCD burn/damage during camera on ear speaker removal

LCD Burn

Punctured camera window

ubreakifix BY asurion

Flip & Fold Display Warranty Determination Flowchart

Whenever a Galaxy Z series foldable device is presented for repair, it is important to complete the appropriate troubleshooting on the device **BEFORE** beginning the repair. Completing the needed troubleshooting in the correct way will help to ensure that there is no unnecessary part consumption, and that the repair is properly identified as In-Warranty or Out-of-Warranty.

Please utilize this warranty process below for any potential foldable display repairs:

1. Inspect the device carefully looking for physical damage. Make sure each of these areas below are examined

- Hinge housing
- Front Deco
- Protect Cover
- Front P-CAP
- Back Glass
- Outer LCD

2. Inspect the display symptom(s) reported by the customer

1. Ask customer when the symptom started to occur
2. Remove Screen Protector
3. Run GD Tool Incoming Quality Control if possible

3. Determine the classification of the symptom type below

- Ultra-Thin Crack
- Black Spot
- Bright Dots
- White Line
- Black Screen

4. Warranty Judgement

- If no damage at all: IW
- If damage on or near defect area: **OOW**

5. Repair

Ensure you are performing the repair properly and avoiding scenarios below as they are subject to chargeback

- Burn the LCD
- Torn Flex's
- Breaking the UB Display
- Damaging other components

ubreakifix BY asurion

Galaxy A & S Series

Physical Condition

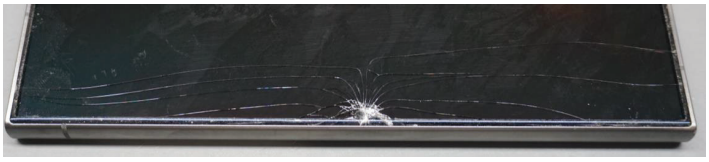
Display Determination

ubreakifix BY asurion

Galaxy A and S Series Display Cracks

For non-foldable devices, any degree of physical damage will void the warranty. This includes, but is not limited to, cracked or broken back glass, camera deco, front glass, or the LCD being cracked underneath. Below are some examples of what would be considered OW:

Even if the damage seems obvious, always be sure to thoroughly check the rest of the phone for any additional damage. In this case, the frame is chipped near the impact point.

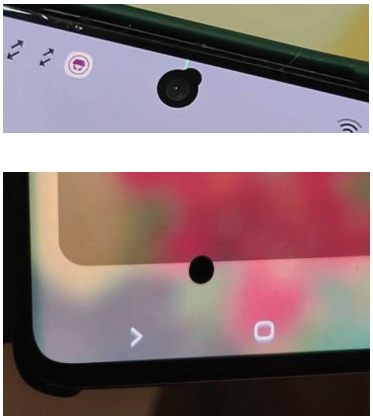


ubreakifix BY asurion

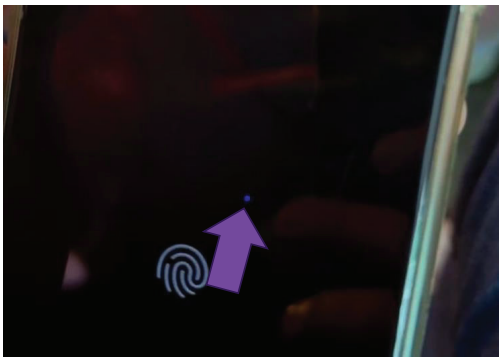
Galaxy A and S Series Display Defects

Any display defects that show no signs of physical damage that could be causing the issue should be classified as IW.

White Lines



Black Spots



Dead Pixels

ubreakifix BY asurion

Galaxy A & S Series

Physical Condition

Cracked Backglass

ubreakifix BY asurion

Galaxy A and S Series Cracked Backglass

If the backglass of the device is cracked, the repair would be OOW.

Remember that not all cracked backglasses will be easily noticeable. Conducting a thorough inspection of the backglass will help you make a well-informed assessment.

When repairing a device with a severely damaged backglass, be aware that components underneath, like the Main and/or Sub PBA and rear cameras, may also be affected and should be inspected thoroughly.

ubreakifix BY asurion

Galaxy A & S Series

Physical Condition

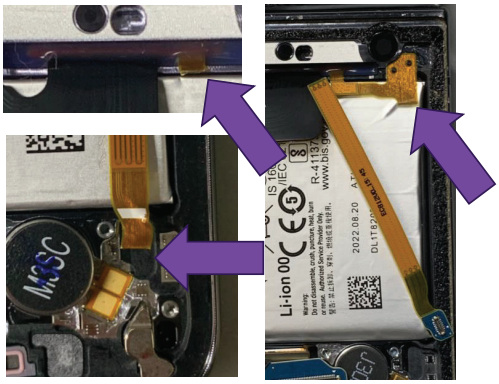
Chargeback Avoidance

ubreakifix BY asurion

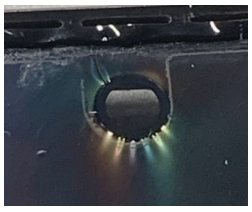
Galaxy A & S Series Chargeback Common Occurrences

Once you have properly deemed a Samsung device In-Warranty we need to ensure we are using proper repair techniques. If you DIP (Damaged in Process) an In-Warranty core your location will be subject to a chargeback. Below you will see some of the more common occurrences we have noticed.

1. Torn or missing flex cables



2. LCD burn/damage during camera or ear speaker removal



LCD Burn

Punctured camera window

ubreakifix BY asurion

A & S Series Display Warranty Determination Flowchart

Whenever an A and/or S Series device is presented for repair, it is important to complete the appropriate troubleshooting on the device **BEFORE** beginning the repair. Completing the needed troubleshooting in the correct way will help to ensure that there is no unnecessary part consumption, and that the repair is properly identified as In-Warranty or Out-of-Warranty.

Please utilize this warranty process below for any potential A & S display repairs:

1. Inspect the device carefully looking for physical damage. Make sure each of these areas below are examined

- LCD
- Backglass
- Frame
- Front camera
- Back camera deco

2. Inspect the display symptom(s) reported by the customer

1. Ask customer when the symptom started to occur
2. Run GD Tool Incoming Quality Control if possible

3. Determine the classification of the symptom type below

- Black Spot
- Bright Dots
- White Line
- Black Screen

4. Warranty Judgement

- If no damage at all: IW
- If damage is present: **OOW**

5. Repair

Ensure you are performing the repair properly and avoiding scenarios below as they are subject to chargeback

- Burn the LCD
- Torn Flex's
- Breaking the UB Display
- Damaging other components

ubreakifix BY asurion

Samsung Warranty Determination: **Customer Talking Points**

Use this guide when talking with a customer about the warranty determination at your store.

Remember to use soft skills and express sympathy and understanding with the customer, but maintain confidence in your decision to determine their warranty status based on condition inspection. You are the tech expert responsible for determining a device's warranty status based on condition.

What NOT to say to a customer:

- "We don't do in-warranty Samsung repairs"
- Mention any detailed, backend processes such as:
  - "Samsung doesn't pay us"
  - "If we don't make the right determination, we will get a chargeback"

What TO share with a customer:

1. Explain the differences in how In-Warranty validation works: In-Warranty by Date versus In-Warranty based on Condition differences.
2. Explain how the physical inspection validation applies to the customer's device: Device condition checks can render a device out of warranty even if it is still In-Warranty by the date.

See next slides for detailed responses

Samsung Warranty Determination: **Customer Talking Points**

1. Explain to the Customer How In-Warranty Validation Works

There are two types of In Warranty validations on your Samsung device.

- ***In Warranty by date*** (typically 1-year) that starts from the date you purchased your device
- ***In Warranty by condition*** – your device must be **free of** defects/damage/imperfections to be considered In Warranty by Samsung
  - Samsung can't determine physical condition of a device over the phone or chat and relies on us as to determine whether a device's condition should be In Warranty

Note for the tech (<u>not</u> customer-facing):

Because our stores are Samsung Authorized Service Centers, Samsung commonly refers customers to our stores. However, it is important to note that Samsung agents should only validate with a customer whether a device is in warranty by date, <u>not based on condition</u>.

A customer's device can be In Warranty by date, but Out of Warranty based on condition.

****Warranty condition validation can only be performed by the Service Center the customer is getting their device fixed at.****

Samsung Warranty Determination: **Customer Talking Points**

2. Explain to the Customer <u>How</u> the Validation Applies to Their Device

- "[Customer Name] Unfortunately, even though your device is In Warranty based on date of purchase, based on the current condition of your device, this device cannot be covered as an In-Warranty repair. *(Show the customer the device, point to areas of designation and explain)."*
- "We are happy to repair your device still, but it would not be covered Under Warranty. "
- "I understand that this is probably upsetting and confusing, but my warranty determination decision is based off the condition of the device today, as outlined based on the checkpoints we are given from Samsung."

Samsung Warranty Determination: **Customer Talking Points**

3. If a Customer Pushes Back on the Out of Warranty Decision

- "I understand your disappointment and frustration."
- "While your device is covered from the purchase date, it is not covered based on its current condition. We consider this decision carefully based on the device's appearance and state. Unfortunately, due to [Damage/Condition], this device is not covered. "

If a Customer mentions Samsung Reference #

- "Thank you for this information. I can share it with the Samsung team to make them aware of your situation. However, the Samsung customer service team can only confirm **your warranty by device date, not current condition.**"

Samsung Warranty Determination: **Validation Point Information**

Note for the tech (<u>not</u> customer-facing):

Two primary validation points will assist you with determining the correct warranty status:

- **1st validation** point is the inspection of the deco and p-caps on the device.
    - If the device has any damage to the deco or damage to the p-caps, regardless of what symptom the device is experiencing – warranty determination by the store should always be Out of Warranty.

If the device does NOT have any damage to the deco or NO damage to the p-caps – the store should proceed with an inspection of the display itself.

- **2nd validation** point will be inspecting the display itself, which will involve two considerations.
    - Cosmetic imperfections examples
        - Ex) Fingernail indents, pitting, scratching, etc.
    - Symptoms of the device
        - Ex) No touch on the display, black splotches on the LCD, missing image, etc).

If the devices' symptoms are **<u>on or near</u>** the cosmetic imperfections, the warranty determination should be considered Out of Warranty.

If the cosmetic imperfections **<u>are separate</u>** from the device symptoms (EG: no touch on the upper portion of the display, but fingernail indent on the bottom half of the display) then the warranty determination should be <u>considered In Warranty.</u>

Fold / Flip Screen Protector Quick Reference Guide

This guide is intended to be a trimmed down version of the full guide which can be found here: https://portal.ubif.net/kbase/article/10509. The full guide is recommended for those who are new to using Portal and checking-in devices.

Collect the customer information and check-in the device as OOW (Out-of-Warranty)

- Before you begin, verify if the customer's device is **In-Warranty by date**.
  - *Customers outside the warranty date should be charged $19.99 MSRP for the protector replacement.*
- **Run IQC** with the customer in store to share the results for transparency before check-in
- Once you've verified the customer is within their warranty period, you will *still* need to check-in the device as **OOW (Out-of-Warranty)**
- DO NOT ever check-in screen protector replacements as IW (In-Warranty)!
- Click on Select Device Symptoms and choose the following **Symptom Codes**
  - L1 - **Screen Protector**
  - 14 - **Screen Protector**
  - Symptom 3 can be any choice relevant to the status of the protector
- Under the "Reason for Out of Warranty Status" menu, select **Protection File**
- Click on the Out of Warranty button to proceed

Add Protection Film SKU to Portal WO and Create GSPN Ticket

- It's important to add the parts to the Portal WO before GSPN Ticket creation
- Once parts are attached and IQC is complete you can **create the GSPN Ticket**
  - It's recommended to only start the GSPN ticket when beginning the screen protector replacement

Submit the FOC (Free-of-Charge) SAW Request

- On the right side of the Portal WO, open the "Work Order Actions" menu and select **Open SAW Tools**
- Under the "Select SAW Type" menu, click on **FOC**
  - *If the option for "**FOC**" is missing, please ensure the device was checked in as OOW!*
- After you select FOC, click on the **Submit SAW button**
  - *Portal should confirm with a pop-up stating "SAW request was created successfully"*
- Next, click on the **View SAW Requests** button to confirm the SAW was attached
- The SAW status *should* read as "**Pending**" which indicates a Sprinklr ticket will need to be submitted in order to receive approval.
  - Issue Type: **Process Requests** > **SAW** > **[VOID] Warranty Cost Full Cover**
  - After submitting the ticket, monitor your email for a response from **FSS**
  - Once FSS confirms the SAW was approved, move to the next step

If the SAW Status shows "Approved" right after attachment, there is no need to submit a Sprinklr ticket.

Attach the Samsung In-Warranty Company

- On the Portal WO, open the "Work Order Actions" menu and select **Open SAW Tools**
- Click on the **View SAW Requests button**
- Here you can see the status of your SAW Request which should be marked **Approved**
  - If SAW still shows "Pending" please resubmit or reply back to the Sprinklr Ticket
- Click the green check box that says "**Convert to I**W" to attach the Samsung In-Warranty company

Moving the WO to Repaired-RFP

- After completing the Screen Protector replacement, you need to complete **Fenrir SVC** and **OQC**
  - When running OQC, you can select "**External**" since the phone **was NOT opened**
- Proceed to moving the WO to Repaired-RFP status using the following **Defect Codes**
  - Check "**OOW**" Box
  - Protection File
  - Cosmetic
  - Protect Film Defect – OOW

If you receive an error when moving the WO to Repaired-RFP, submit a JIRA Ticket right away!

Frequently Asked Questions

Q: Can I facilitate more than one screen protector replacement for the customer?

A: Samsung allows one free protective film replacement during the manufacturer's warranty period. Customer's are also eligible for a free replacement within 7-days of a previous film replacement. Devices outside the warranty will need to be charged for the screen protector.

Q: How much should I charge the customer for a screen protector if the device is outside the warranty period?

A: MSRP is $19.99 (plus tax)

Q: I do not see the option for "FOC" in the SAW Tools menu, how do I proceed?

A: The most common cause for this is due to the device being checked-in as In-Warranty. Screen protector replacements must always be checked in as Out-of-Warranty, even if the customer is

within the warranty period. If you accidentally checked the device in as In-Warranty, mark the Portal Work Order as “Declined-RFP” and recreate the work order.

Q: Do I need to submit a Sprinklr ticket if the SAW Status already shows “Approved”?

A: No. In some cases, the SAW may be auto-approved for various reasons. It’s recommended to always check the SAW status right after attachment to check if a Sprinklr ticket is needed.

Q: What if FSS declines the FOC SAW request?

A: If the customer is out of warranty by date, then the customer should be charged for the screen protector. If this is a customer escalation, please let FSS know of the situation. FSS can check the customer notes to see if a screen protector was promised by Samsung customer service. In which case, the SAW can be approved.

Q: Why are we attaching the “Samsung In Warranty” company if the repair is Out of Warranty?

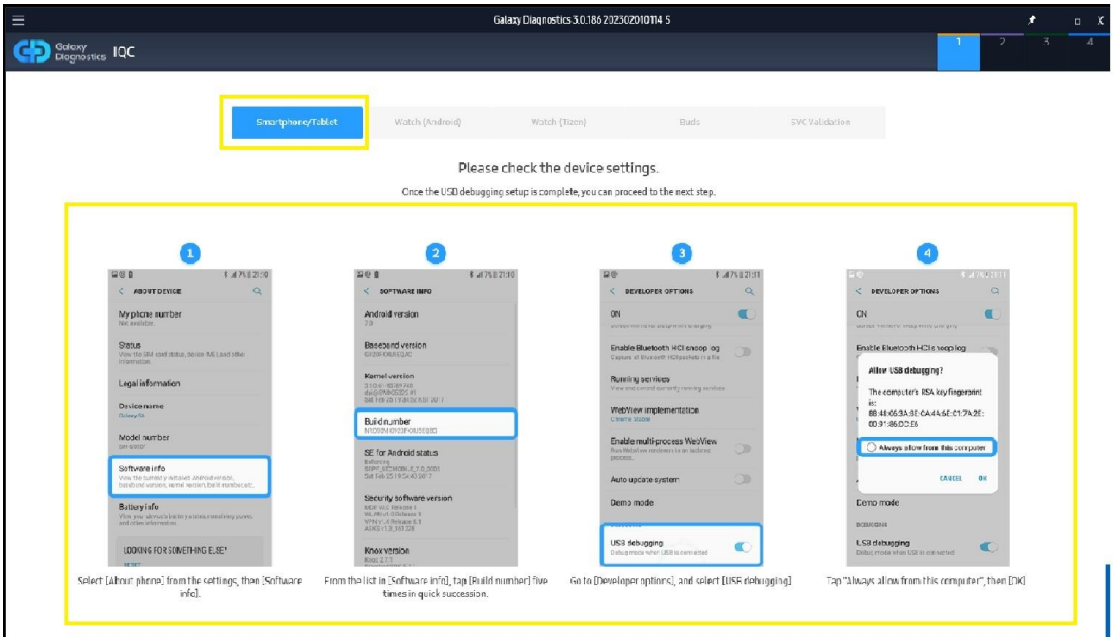
A: While the protector is covered by Samsung, it’s tracked as an Out-of-Warranty repair. If the customer returns with an IW issue (blank screen, connection issues, etc.), then the IW ticket will NOT be tracked as a bounce. This is why it's important to ensure these are checked in correctly according to the guide. This will not void the customer’s device warranty.

Q: What does the error “Work order cannot be changed to this function” mean? How do I resolve it?

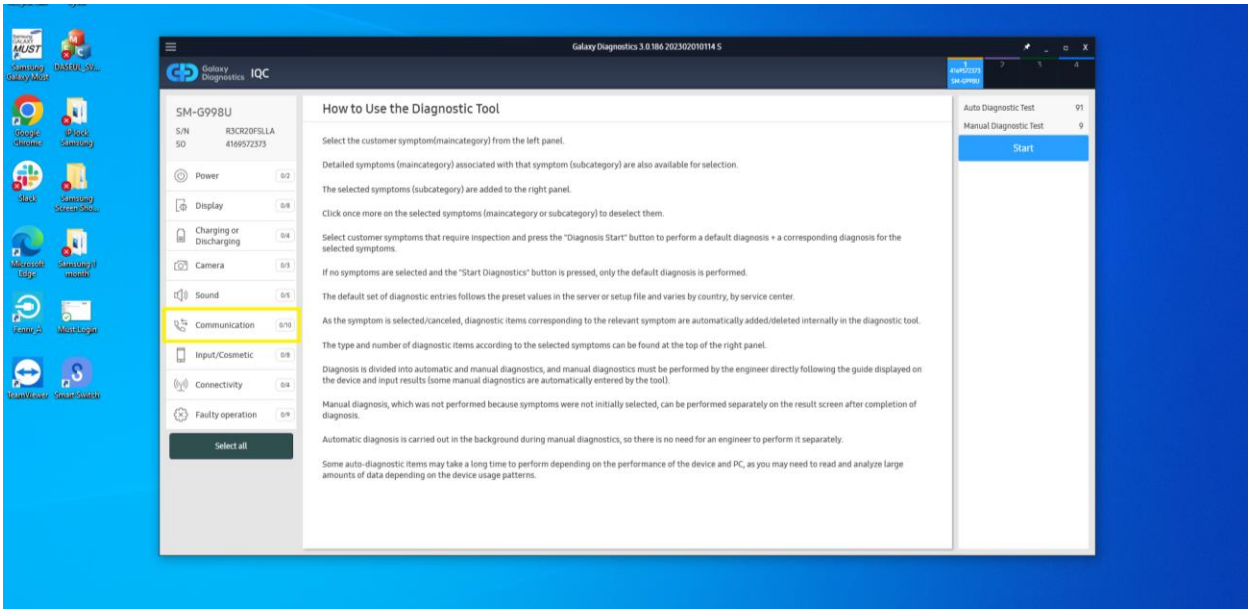
A: This error indicates that there is a Warranty Error on the GSPN ticket that needs to be resolved internally. The quickest way to resolve this is to submit the appropriate JIRA Ticket using the link below. The support agents will provide direction on how to clear the error.

GD Tool: Service Issue IQC Guide

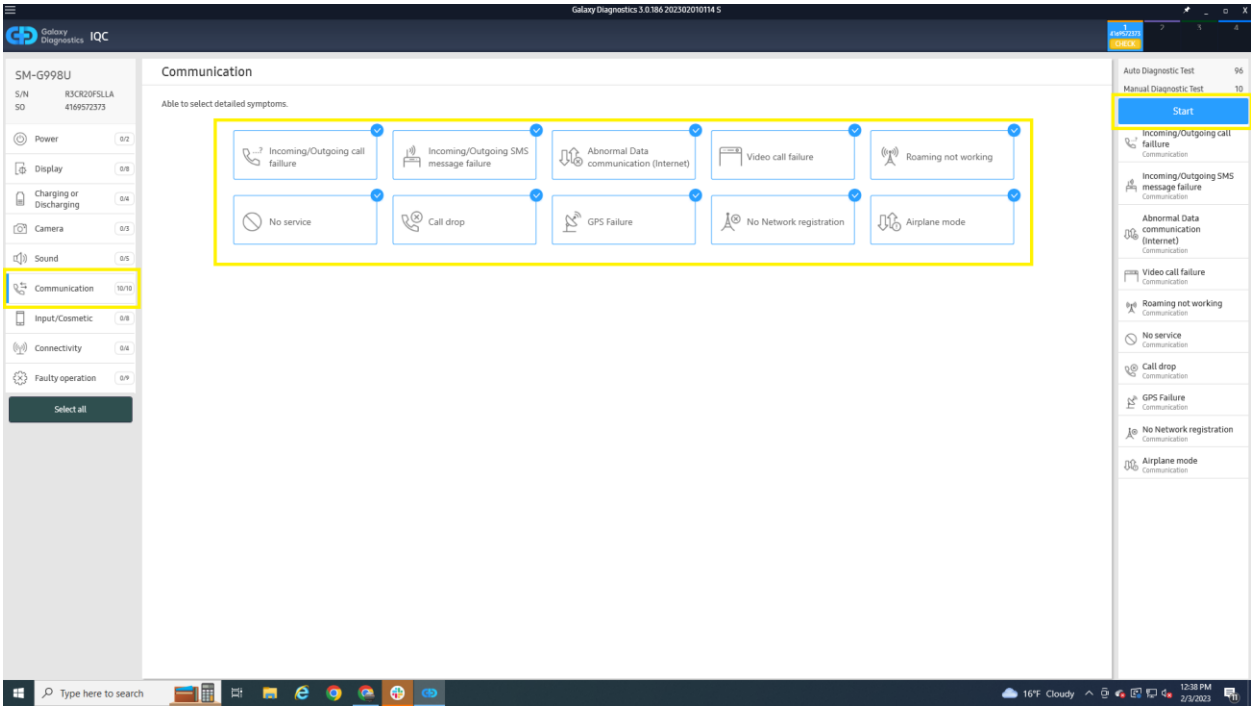
When customers are coming into the store because they are experiencing service issues on Samsung devices, below are the steps to pull the call/SMS and data drops. This allows us to show the customer whether the issue is carrier-related or hardware. This is all done in IQC, and we can either print or show the customer the results depending on where your IQC computer is located.



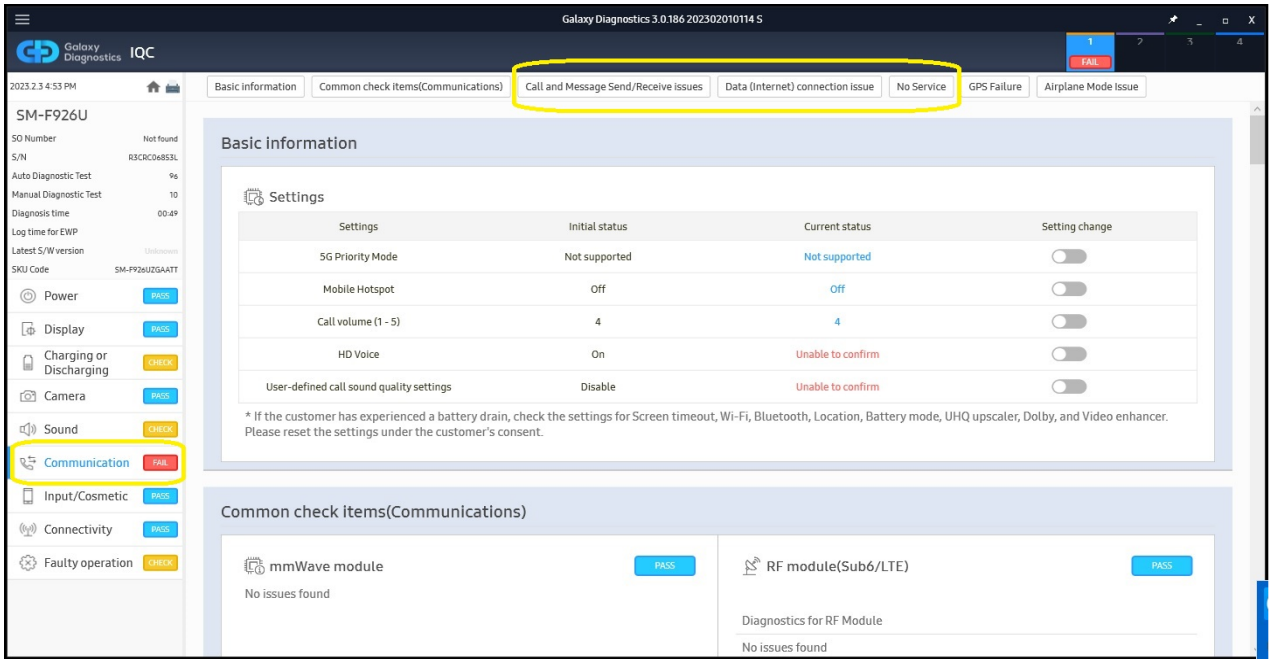
Open IQC from GSPN and follow the steps to get the device ready.



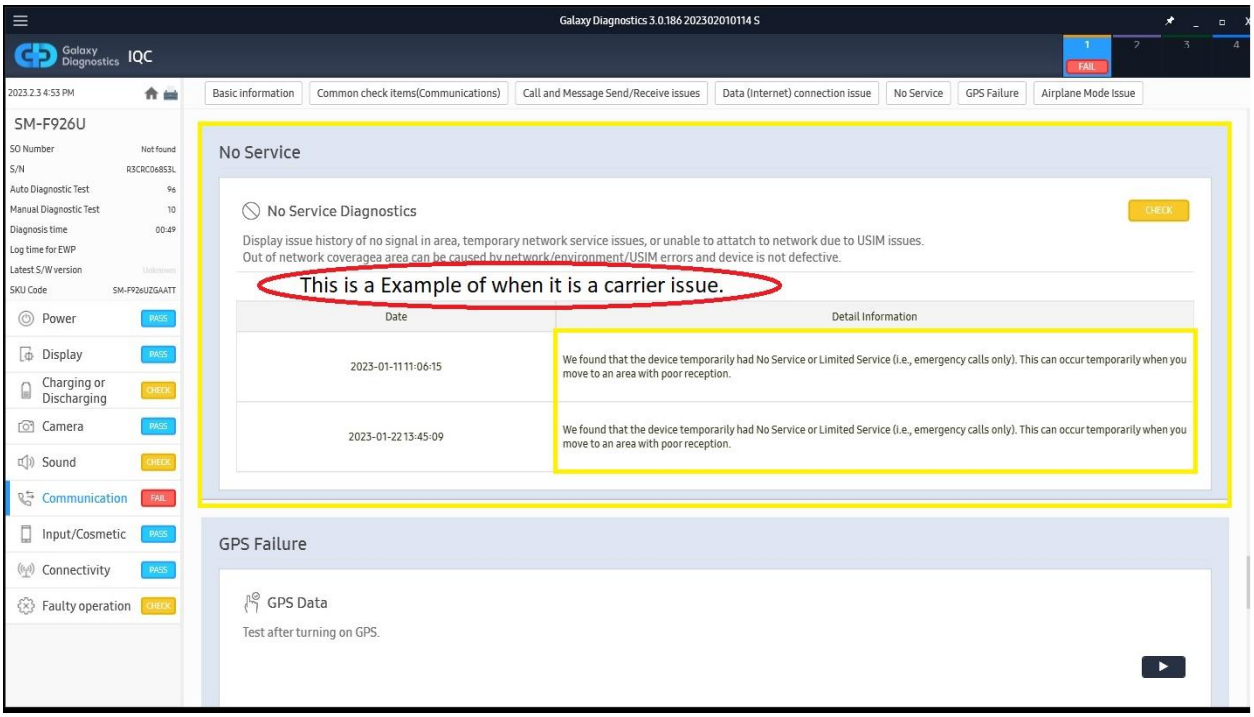
Connect device and follow prompts on the screen to start IQC testing. Select "Connectivity" on the right-hand side.



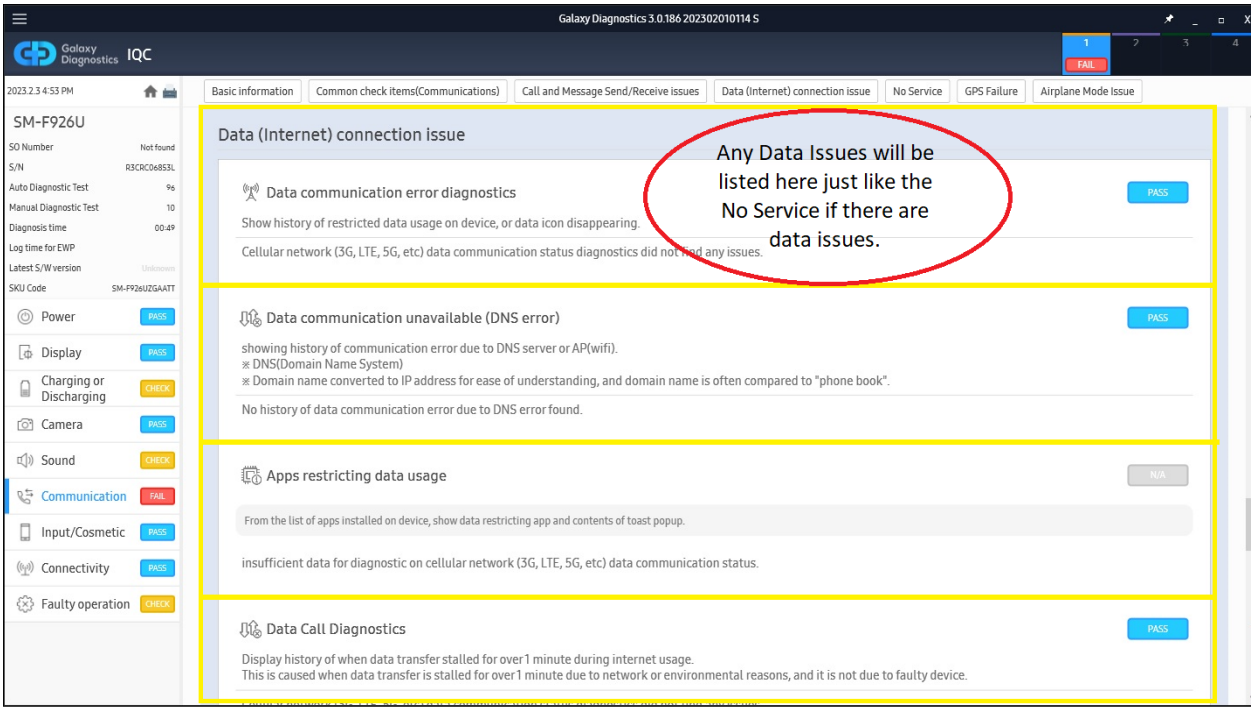
Select all tests under "Connectivity" and press "Start"

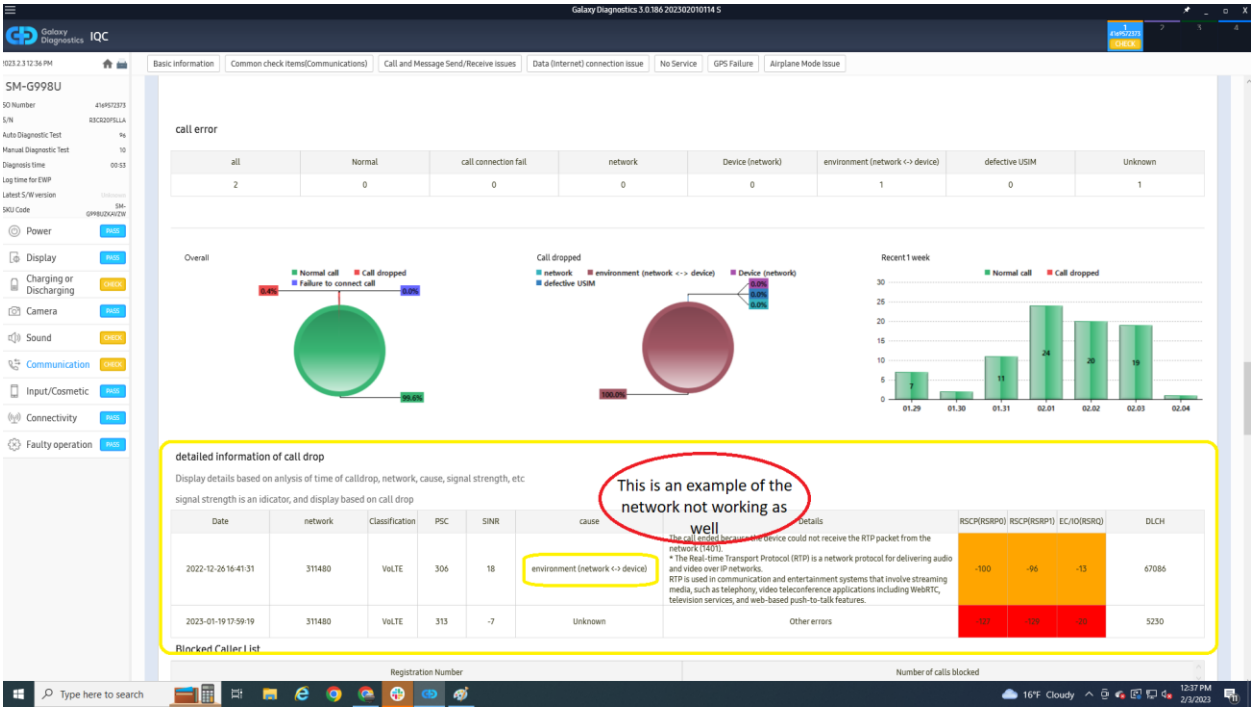


Most tests should run automatically on my devices. Just watch the device and follow any prompts that appear. At the Results Screen make sure to select "Connectivity" on the left hand side and at the top you will see quick links to the info we need.



Under those tabs will be all the information we need. Most importantly will be "No Service", "Data Connection issue" and "Call Drop Data". This will tell you if the issue is with the carrier or with the device.





*You can either print the results with the printing icon on the left side of the results screen. Make sure to **ONLY** print the pages needed. If not, you will get 20-30 pages printed out.*

GD Tool: Common Resolutions

- Confirm Fenrir and GD Tool are not both open at the same time.
    - They can both “fight” for USB permissions.
- Try a different USB cable on a different PC port
- Confirm device has enough storage (> 3gb)
- Unplug, revoke USB debugging authorizations, toggle USB debugging off and back on
- Use Fenrir to reinstall Samsung USB drivers.
- Android System Web View
    - Settings > Apps > and search for "WebView". Once you find that app, tap the 3 dots on the top right and Uninstall Updates
- Restart PC
- Uninstall and reinstall GD Tool
- Try using #help channel on Slack
- Use chat function in lower right of ZenDesk

GD Tool: Blue WRT Test

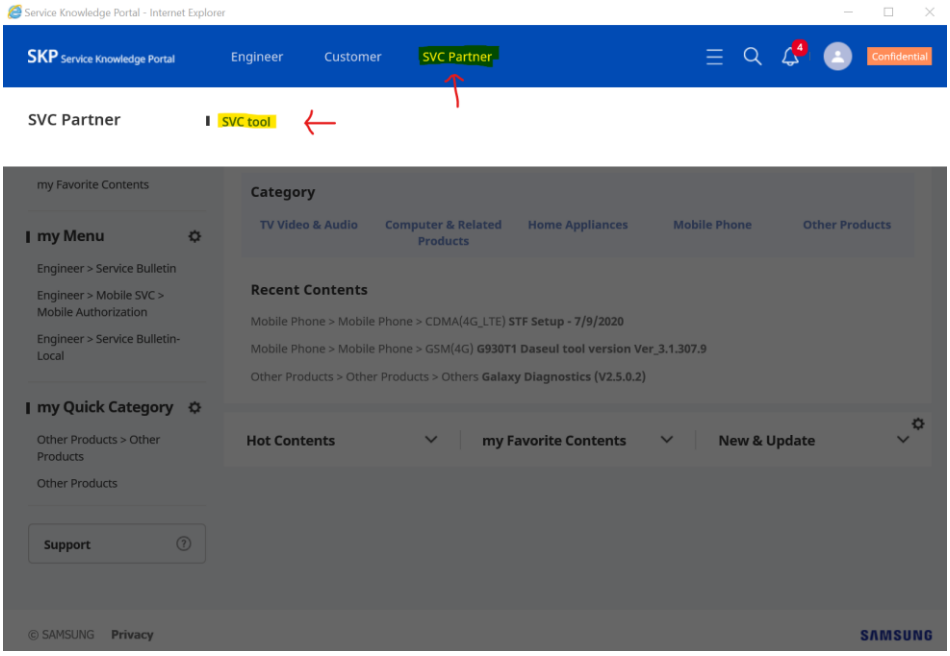
- Turn on and pair sensor
- Verify o-ring is sealed with p-sensor inside
- Put syringe in down position
- Start test
    - If the test does not start, select restart. If you cannot select restart, then restart GD testing
- While sealing the end of tube with your finger, put syringe in upward position and wait with your finger on the end of the tube

GD Tool: Uninstalling and Reinstalling

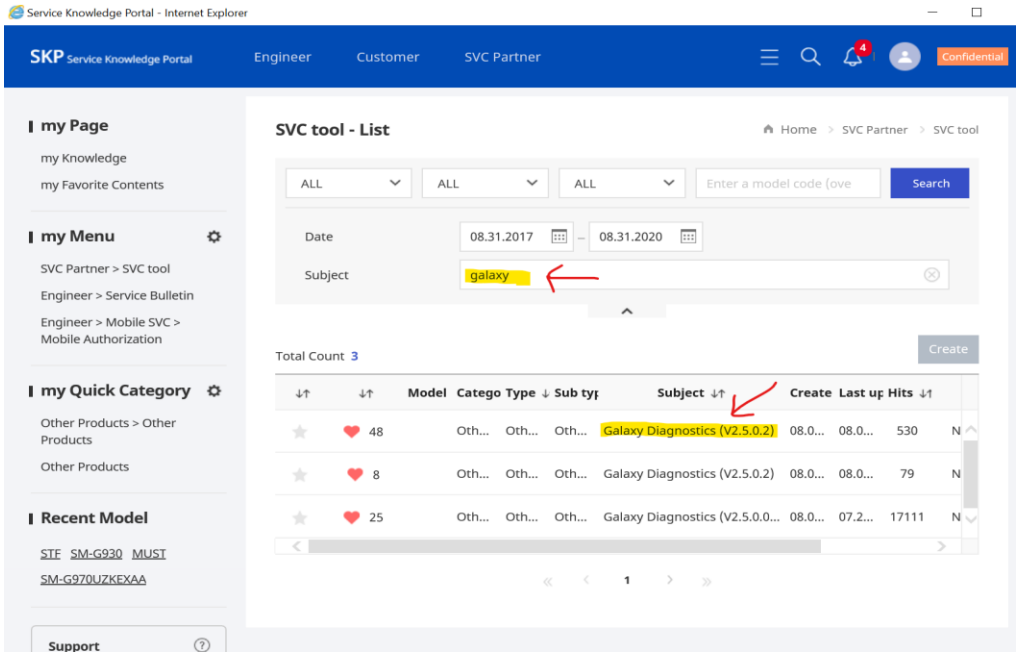
Step	Action
1.	Navigate to Start > Control Panel > Programs and Features on the GD PC
2.	Select the previous installation of Galaxy Diagnostics
3.	Click the "Uninstall" button at the top of the window to uninstall the application
4.	Navigate in Windows Explorer to C:\ and DELETE the GalaxyDiagnostics folder
5.	Reboot the GD PC
6.	Log in to G-SPN
7.	Navigate to Knowledge > Others > SVC Tool
8.	Click **Search** **Note:** There is no need to enter any search criteria to load results.

GSPN: Finding Samsung Software

Galaxy Diagnostics

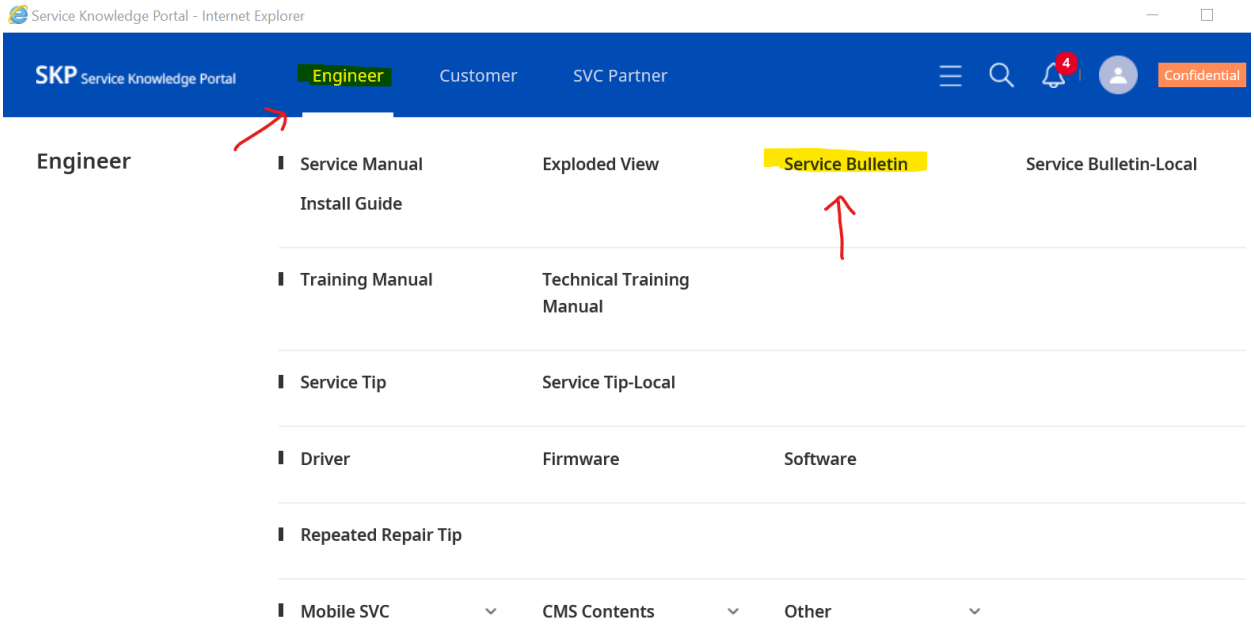


Hover over "SVC Partner" and click "SVC Tool"

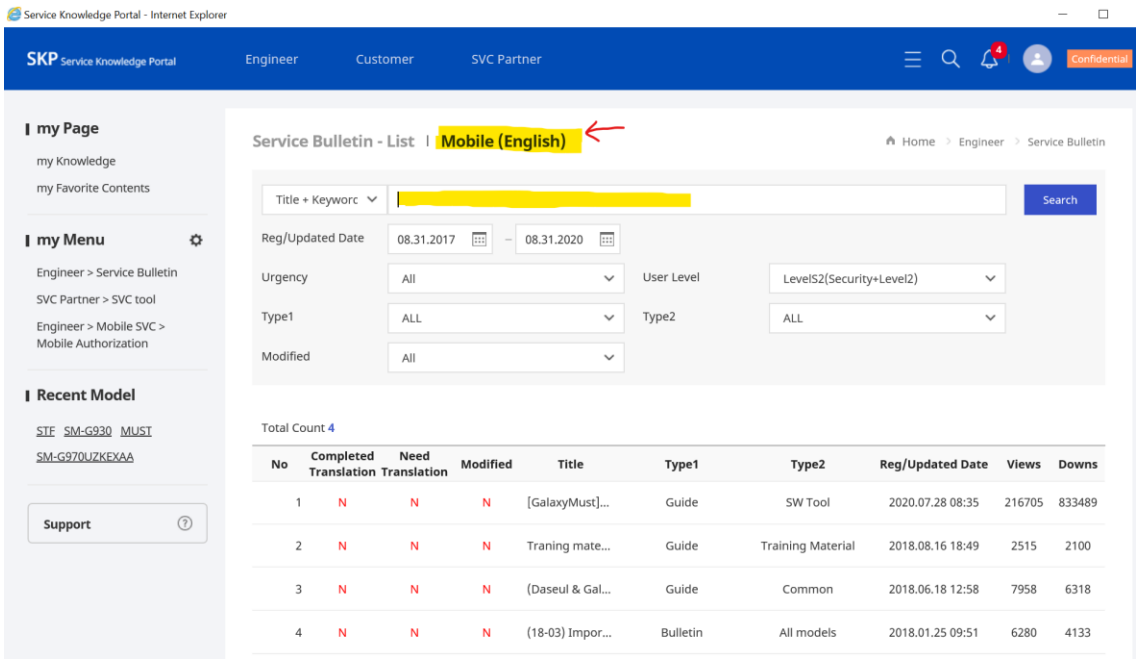


Search "galaxy" in the subject and select the latest version and date.

Fenrir/Daseul

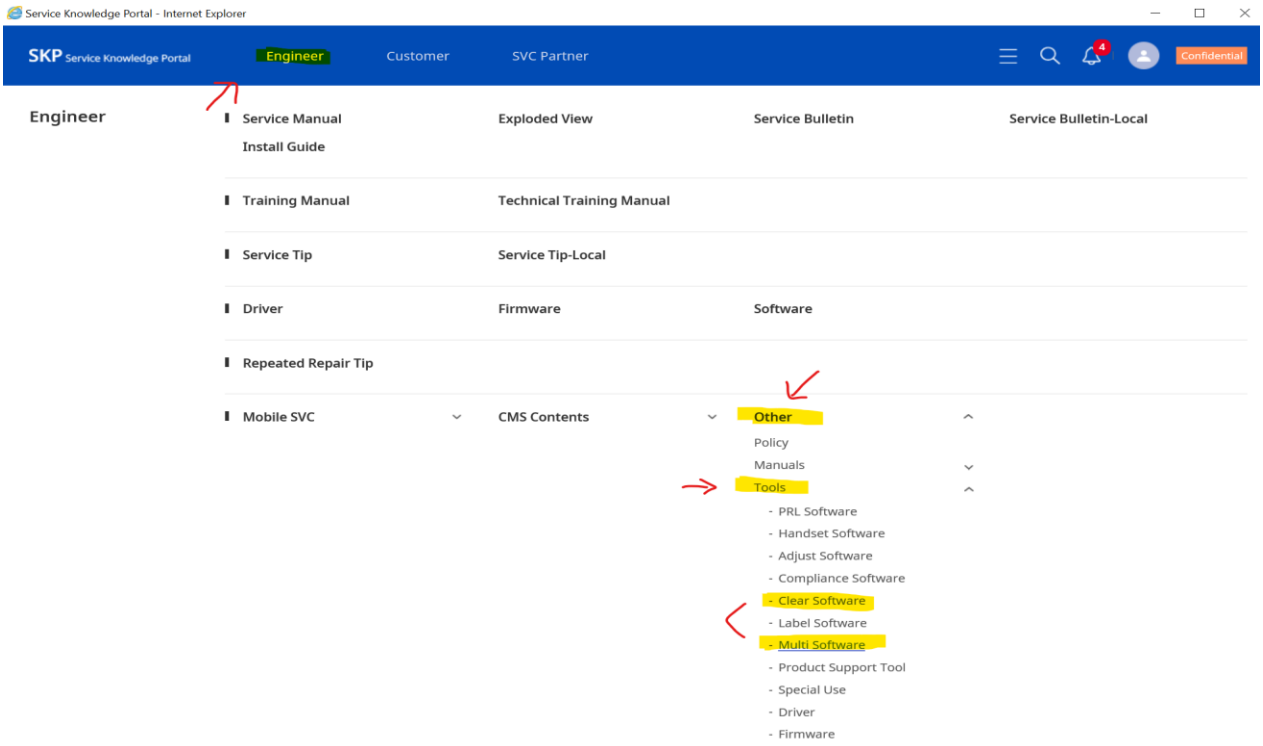


Navigate to Engineer - Service Bulletin

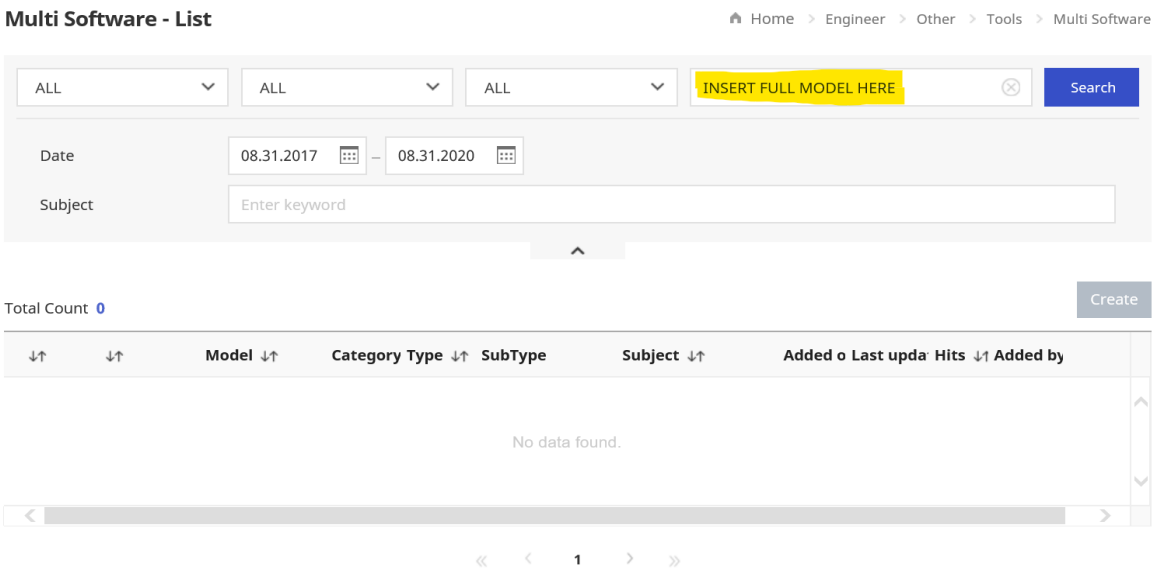


Select "Mobile English" when you do this you will get moved to enter your certificate tool password as full level S2 is required to obtain these. In the yellow field "Title" you will enter MUST, Fenrir, Daseul, etc.

PBA Files



Navigate to Engineer - Other -



Tools and then either Multi or Clear, usually the files will be in Multi-Software.

Insert FULL model code here. Ex: SM-G950UZKAVZW

(SAW) SERVICE ACTION WORK ORDER

PURPOSE

To reduce the OOW (out of warranty) judgement criteria for customer satisfaction in cases where the customer raises escalation concerns. There is a high chance of customer escalation being raised from these cases:

- Unit is recently OOW by purchase date or production date
- Unit determined OOW by condition but difficulties in finding customer fault

WHEN TO REQUEST SAW

The following customer escalation cases qualifies for reduction of OOW judgement criteria for customer satisfaction.

- One-time warranty allowance (warranty extension)
- Minor Physical damage
- Minor Liquid damage

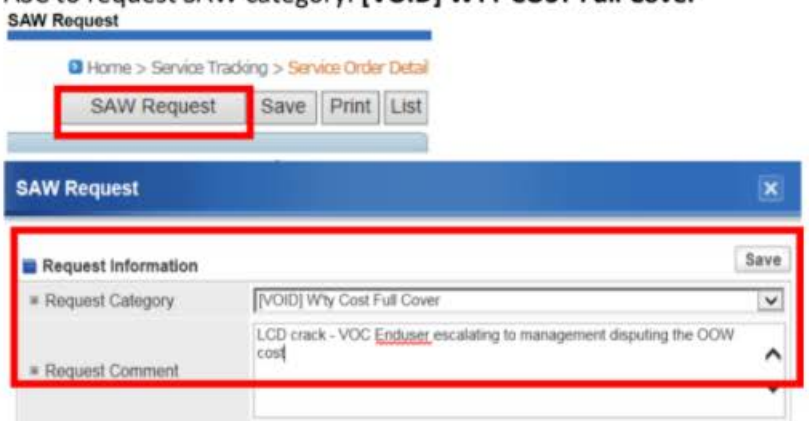
PROCESS

1. **One-time warranty allowance: Warranty grace period 3 months**
   Customer escalating a scene at your ASC location requesting warranty extension

   - Device under repair must be in-warranty by physical condition (no cracks/no liquid damage)
   - Device must be within 3 months of expiration of warranty by Purchase/Manufacturing Date.
   - POP required if using Purchase Date
   - ASC to educate the customer that device is **OOW and requires approval from Samsung Head Office**
   - ASC to **email/notify** SECA (Samsung working hours only 8am-6pm) that device on hand requires **One-time warranty allowance – Grace period** and provide detailed reason for request
   - Once SECA Acknowledge, ASC to create GSPN service order
   - **SECA MUST CREATE SAW, ASC IS NOT TO CREATE SAW**
   - Device warranty status updated to L/P, follow normal warranty repair (Fenrir/QR code scanning/U-Class Label)

2. **Minor physical damage**
   Customer escalating a scene at your ASC location requesting relaxation of OOW judgement with physical damage

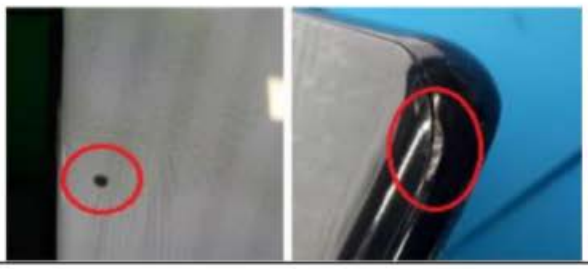
- **Device must be under Manufacturer's warranty**
- ASC to educate the customer that device is OOW and requires approval from Samsung Head Office
- ASC to create GSPN service order then set **WTY Exception: VOID1 Impact Damaged**
  Warranty Term: **OW**
- ASC to take picture and upload to GSPN service order
- ASC to request SAW category: **[VOID] WTY COST Full Cover**



- ASC to email SECA with detailed reason for request that device on hand requires SAW approval
- **SECA must approve SAW request before ASC can update service order to repair completed**
- **Follow normal warranty repair (Fenrir/QR code scanning/U-Class Label)**
- **Use Defect code: F46**

Conditions that qualify as minor physical damage/unable to determine customer fault. SECA review pictures before SAW request approval.

INTERNAL CRACK – Under glass, no signs of impact	HAIRLINE CRACK – minor glass crack, no signs of impact
	

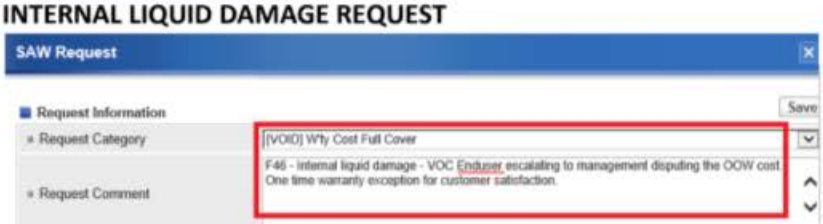
POINT OF IMPACT – Flickering display	POINT OF IMPACT – Black dot/dead pixel
	

BLEEDING OCTA/LCD	CAMERA WINDOW CRACK
	

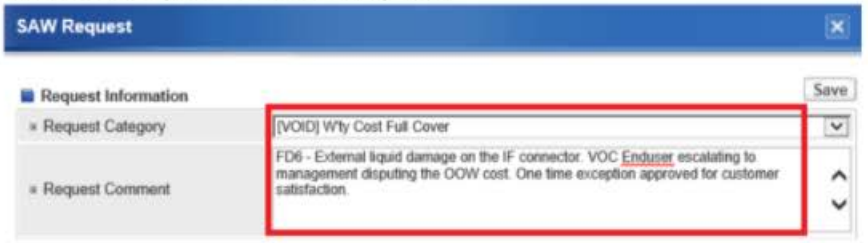
3. **Liquid damage**
   End-user escalating a scene at your ASC location requesting relaxation of OOW Judgement for Liquid damage

   - Device must be under Manufacturer's warranty
   - ASC to Educate the end-user that Defect is OOW that requires approval from Samsung Head Office
   - **ASC to take picture and upload on GSPN before repair of Liquid damaged area**
   - ASC to create GSPN SO ticket then set **WTY Exception: VOID2 Liquid Damaged**
     Warranty Term: **OW**
   - ASC to request SAW category**: [VOID] WTY COST Full Cover**

INTERNAL LIQUID DAMAGE REQUEST



EXTERNAL LIQUID DAMAGE REQUEST



- ASC to **email** SECA with the detailed reason for request that device on hand requires SAW approval for Liquid damage
- **Defect code: F46 (Liquid damaged device)**
- **Defect code: FD6 (IF Connector/charging port only)**

- **SECA must approve SAW request before ASC can update SO ticket status to repair completed**
- **Follow normal warranty repair (Fenrir/QR code scanning /U-Class label)**

ASC Findings	Physical Condition	Disposition	Action	
Color change on litmus liquid damage indicators on device and/or battery.		Warranty void - OOW Take pictures as evidence of Liquid Damage	ASC determines the cost of repair	
No color change on litmus liquid damage indicators on device and/or battery. ASC observes sign of possible liquid damage or corrosion on device	Device DO NOT exhibits dents/No point of impact (maintained in good appearance condition)	GSPN SO ticket set to **WTY Exception: VOID2 Liquid Damaged** Warranty Term: **OW** ASC to request SAW category: **[VOID] WTY COST Full Cover**	Take pictures as evidence of Liquid Damage Take pictures as evidence of physical condition of device Take pictures of litmus liquid damage indicator **Defect code: F46**	
No color change on litmus liquid damage indicators on device and/or battery. ASC observes sign of possible liquid damage or corrosion on device	Device EXHIBITS dents/ point of impact/deep scratches	Warranty void - OOW Take pictures as evidence of Liquid Damage	ASC determines the cost of repair	
No color change on litmus liquid damage indicators on device and/or battery. ASC observes sign of possible liquid damage or corrosion on IF connector/USB charging PORT only (external LD only)	Device DO NOT exhibits dents/No point of impact (maintained in good appearance condition)	**GSPN SO ticket set to WTY Exception: VOID2 Liquid Damaged** **Warranty Term: OW** **ASC to request SAW category: [VOID] WTY COST Full Cover**	**Clean** **Defect code: FD6**	**PASS – Complete Repair** **FAIL – Replace Sub PBA or IF connector**

Process: Ticketing Overview

Is this a JIRA / Support / Help Desk ticket or an FSS / ZenDesk ticket?

Zendesk is run by the Samsung FSS (Field Service Support). The FSS team can approve error requests and Exception requests and is the only team capable of doing so. Please keep in mind that depending on the error you receive, the FSS team/agent may require you to do basic troubleshooting and/or have you provide screenshots of the errors, the about menu of the device, proof of purchase, etc.

JIRA is run by UBIF Asurion ServiceDesk team and can be escalated to the Samsung Partnership team when necessary. Stores first step should be to reach out to the ServiceDesk team if you get a portal error. You can file a ticket using the support tab on portal. The ServiceDesk team is capable of applying requests and determining warranty errors (WERs). The ServiceDesk team is also capable of answering basic troubleshooting questions.

Process: GSPN & Portal Work Order Errors

[Fenrir] [#] There is no history of FENRIR connection in FUS server.

Description

This error occurs when Fenrir was not executed on the device. Work Orders with this error cannot proceed to Repaired-RFP until SVC Connection is executed on the device or having a Fenrir Exception approved. Fenrir [4] and Fenrir[8] are the only 2 errors eligible for Fenrir Exceptions.

Causes

- The device was disconnected from **Fenrir** prematurely; ensure that Fenrir has finished processing the **SVC connection** before disconnecting the cable.
- The device was **not recognized** by FENRIR. This can occur from a **dirty or damaged charging port** or **bad charging cable**. In rare cases, it's the device failing to send data to the PC.
- If the error is **[Fenrir] [4]** that means the **binary** is not downloaded onto the PC so the update could not be installed. This is only seen on **In-Warranty repairs** only.

Solution

Execute Fenrir on the device again. Use "SVC Connection" for BOTH OOW & IW repairs. "S/W Update" is also required for all IW repairs.

If Fenrir cannot be executed on the device or the customer refused a software update, you can submit a Fenrir Exception via ZenDesk Ticket Request. Please note that FSS will NOT approve exceptions for Fenrir if you did not run "SVC Connection" on the device. You will need a screenshot of "SVC Connection" being run on the device in order to receive approval for this request.

If FSS declines this exception request, you can try reaching out to your designated Samsung rep for a one time exception.

[Fenrir] [8] The PBA UN in Phone is not matched to PBA UN in MPTS.

Description

This error occurs when GSPN believes there is a non-OEM motherboard on the device.

Causes

- The device is an "**End-of-Life**" device. EoL devices are considered to be **S7 series and older**.
- The PBA is **non-OEM (or being detected as such)**.

Solution

You can submit a Fenrir Exception via ZenDesk Ticket Request. Include a full screenshot of the error and ensure the WO is visible in the screenshot.

[GCIC] GD Error

Description

This error occurs when Portal has detected a FAIL or MISSING GD Tool Result. Work Orders with this error cannot proceed to Sale Complete without retesting the device or requesting a GD Exception.

Causes

- **IQC** was not executed based on the **defect code selected** upon check-in.
- **OQC** is showing a **FAIL result**; OQC will need to be executed on device again
- **OQC** showing **NO GD result**. This can occur if the GSPN Ticket was not created when testing was executed. This can also occur if the WO has not been set to **Repair-in-Progress** status.
- The WO was not set to **Sale Complete** before 14 days. It's important to not let tickets sit unresolved or opened for more than 24 to 48 hours if possible.

Solution

Execute GD Tool on the device again.

If you cannot resolve this error using the step above, you need to reach out by creating a ZenDesk Ticket Request. If FSS does not resolve the issue, you can try reaching out to your designated Samsung rep for a one time exception.

*** Help Desk and JIRA Support cannot help with GD Tool/OQC Exception approval. ***

[GCIC] [OCTA:F]

Description

This error occurs when Portal has detected a FAIL or MISSING GD Tool Result. Work Orders with this error cannot proceed to Sale Complete without retesting the device or requesting a GD Exception.

Causes

- **Fenrir** was executed before the OCTA was replaced on the device; execute Fenrir again to resolve the error.
- **Fenrir** failed to **send the logs to the FUS server**; ensure the device is **not prematurely disconnected** from **Fenrir**.
- Fenrir was executed on a **previous ticket** that was marked **Repaired** or **Sale Complete** (even if the part is no longer attached to the WO).
- The previous ticket is still **open/not canceled**; if the previous GSPN ticket is **not set to Repaired**, cancel the ticket that had this part attached (even if the part is no longer attached to the WO).
- Part was **removed from the WO** after the status was **changed to Repaired-RFP**.
- Part was **returned into inventory** after processing a **refund**, then reused on another device.

Solution

Execute Fenrir again. If the error persists, replace the OCTA and RMA the current one. After OCTA replacement, execute Fenrir again to clear the error.

If the above does not resolve the issue, reach out to your Samsung rep to get clarification as to why the error is occurring. You can also submit a JIRA ticket for clarification on the reasoning behind the error here: Samsung General Question.

*** Outside of the above solutions, there are no workarounds to this error. If the device was released before this error was resolved, you need to mark this Declined-RFP and absorb the cost of parts used ***

[GCIC] Not created new job.

There was an error creating the Repair Ticket.

[GCIC] Not created new job.

Description

The error occurs when a pending ticket for the device exists on GSPN. The GSPN Ticket can be linked to UBREAKIFIX or another Samsung service provider.

Causes

- There's an open ticket on Portal with the device attached. You can validate this by searching the IMEI in Portal.
- A pending ticket could have been created via 1-800-SAMSUNG if they were contacted prior to the device arriving.
- A pending ticket may exist under another Samsung Authorized Service Center or Partner.

Solution

You can first contact Help Desk if you cannot find the open ticket in Portal.

If it can not be resolved by Help Desk, you can submit a ZenDesk Ticket Request and ask FSS to cancel any pending tickets on their end.

If FSS cannot help, submit a JIRA Ticket.

[GCIC] Ticket is locked, the other user is using this ticket.

There was an error creating the Repair Ticket.

[GCIC] Ticket is locked, the other user is using this ticket.

Description

The error occurs when the GSPN Ticket is being used on the GSPN side by another user.

Causes

- The GSPN ticket is currently being edited at the time of the error.
- The GSPN Ticket could be in an opened internet browser tab. Most of the time, it's someone on the Samsung side.

Solution

Wait and try again. This will likely resolve itself within the hour.

Submit a JIRA Ticket if the issue continues.

ASC Job No already exists.

There was an error creating the Repair Ticket.

ASC Job No already exists.

Description

This error occurs when GSPN detects that the WO number (ASC Job No) has a GSPN Ticket already attached.

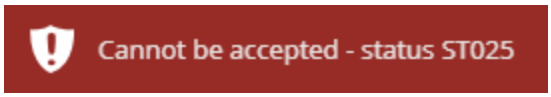
Causes

- This is usually caused by a **miscommunication/disconnect** between the **Portal WO and GSPN Ticket** while attempting to create the GSPN Ticket; this is at no fault of the store.
- There may have been a slight disruption in the **internet connection** while creating the ticket.

Solution

Submit a JIRA Ticket to have this resolved.

Cannot be accepted - status ST025



Description

This error occurs when the GSPN Ticket attached to the Portal Work Order has been canceled.

Causes

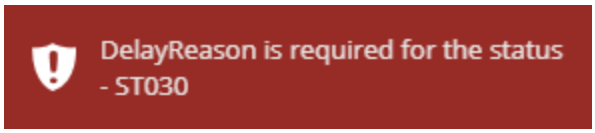
- GSPN Tickets can be canceled by the **Samsung Field Support Team** due to **inactivity**. Tickets that go unresolved for more than 72 hours without an attempt at resolution end up in LTP (Long Pending Ticket) status. This typically only affects **In-Warranty repairs**.

Solution

If the ticket has been canceled on an In-Warranty repair, you will need to recreate a new WO to properly get reimbursed for the repair. Canceled tickets cannot be reopened via the old WO. Exceptions are not guaranteed for the new WO depending on the circumstances.

If the WO needs to be closed due to no repair being completed, you can submit a Work Order Issue Form.

DelayReason is required for the status - ST030



Description

This error occurs when the GSPN ticket is in "Pending" status with no "Reason" selected.

Causes

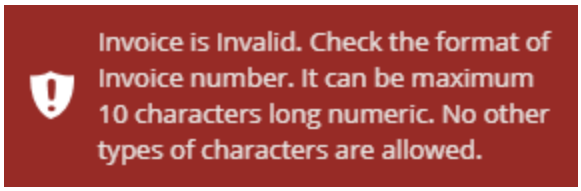
- This could happen if the Portal WO is moved to **"Awaiting Device/Awaiting Customer"** status.

Solution

Try to move the WO to "Repair in Progress" status. This will usually resolve the issue.

Submit a JIRA Ticket if the above does not work.

Invoice is Invalid. Check the format of Invoice number.



Description

The error occurs when a part attached to the Work Order has an invalid OEM Invoice number.

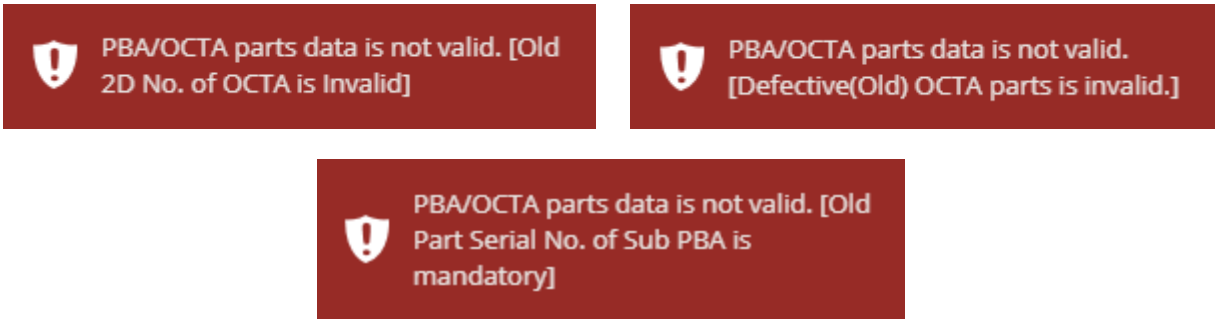
Causes

- Distro's OEM invoice for the Part does not match the invoice number on GSPN. This is at no fault of the store.

Solution

Reach out to Help Desk to resolve this issue.

PBA/OCTA parts data is not valid.



Description

This error occurs when an OCTA or PBA QR code does not match its respective part. Items that require QR scans are: OCTA Kits, Batteries, Camera Modules, and Main PBAs.

Causes

- **Scanning the wrong QR code**. It can be confusing since there are **multiple QR codes** on some parts.
- Running IQC after replacing the parts. **Do NOT ever do this under any circumstance**.

Solution

Execute GD Scan the proper QR codes. If you are absolutely certain you scanned the correct QR codes, take pictures of both QR codes on both old and new parts. You will need to submit these for a SAW (Service Action Work) request for a Parts S/N exception. Please double and triple check the QR codes on the part before reaching out to support as most of these are resolvable without support.

*** If you are rescanning the parts, ensure Portal is updating the codes correctly. If you have issues with Portal updating the scans, please remove the part from the WO and add it back with the proper scans. ***

If the above does not resolve the issue, you can use the SAW Tools module under “Work Order Actions” within Portal. A guide on how to use this tool can be found here: SAW Tool Guide

Once the SAW is attached, you then will need to submit a ZenDesk Ticket Request. For Issue Type select “Process Request” > “SAW” > “Parts and S/N” along with the appropriate WO information. Once approved, you can proceed the WO.

Service request cannot be created.

There was an error creating the Repair Ticket.

Service request cannot be created. Please direct the customer to contact the carrier for repair concerns.

Description

This error occurs when attempting to create a GSPN Ticket for a device with a Carrier not Supported by Samsung.

Causes

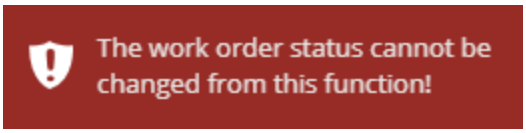
- The device carrier may be **TracFone, Straight Talk, or another unsupported carrier**.
- The device may be an **International Model**. Please check the model code.

Solution

The current resolution is to use International Samsung Work Flow. After the WO is created, submit a request to have the Samsung International Company attached.

This should only be used for Out-of-Warranty repairs. In-Warranty will need to be directed to the device's carrier. Please note that you will only receive GRADED CREDIT for these devices.

The work order status cannot be changed from this function!



Description

This error usually appears for In-Warranty GSPN Tickets that have a Warranty Error (WER). WOs cannot proceed until these are resolved.

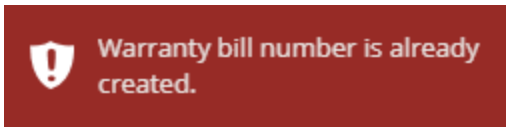
Causes

- The GSPN ticket has a Warranty Error (WER). You can review This Guide for more information on these.

Solution

Submit this JIRA Ticket for WER for help resolving these errors.

Warranty bill number is already created.



Description

This error occurs when a confirmation number for a closed (Goods Delivered) GSPN ticket already exists.

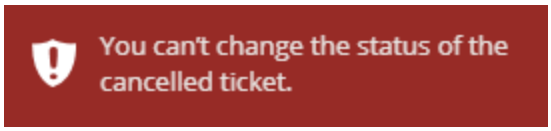
Causes

- This is usually caused by a **miscommunication/disconnect** between the **Portal WO and GSPN Ticket**; this is at no fault of the store.

Solution

Reach out to Help Desk to resolve this issue.

You can’t change the status of the cancelled ticket.



This error is also a variation of “Cannot be accepted - status ST025”

Description

This error occurs when the GSPN Ticket attached to the Portal Work Order has been canceled.

Causes

- GSPN Tickets can be canceled by the **Samsung Field Support Team** due to **inactivity**. Tickets that go unresolved for more than 72 hours without an attempt at resolution end up in LTP (Long Pending Ticket) status. This typically only affects **In-Warranty repairs**.
- GSPN desync. Although it’s rare, it’s possible that GSPN did not properly communicate with the active WO and needs to be synchronized.

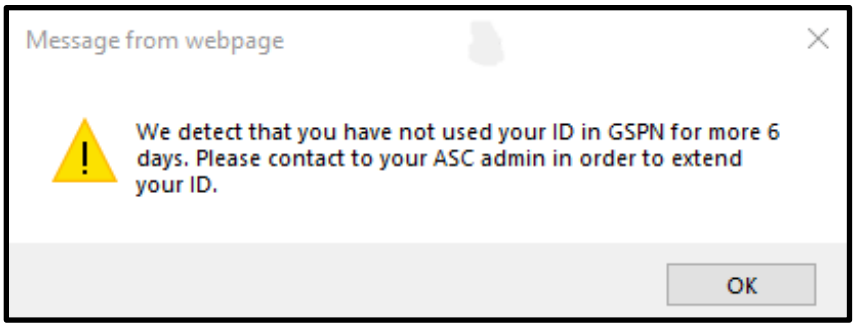
Solution

If the ticket has been canceled on an In-Warranty repair, you will need to recreate a new WO to properly get reimbursed for the repair. Canceled tickets cannot be reopened via the old WO. Exceptions are not guaranteed for the new WO depending on the circumstances.

If the WO needs to be closed due to no repair being completed, you can submit a Work Order Issue Form.

Process: GSPN Errors & Resolutions

GSPN – Account Lock



Error Message

"We detect that you have not used your ID in GSPN for more than 6 days. Please contact to your ASC admin in order to extend your ID."

Cause

The GSPN account was not logged in for at least 6 days.

Solution

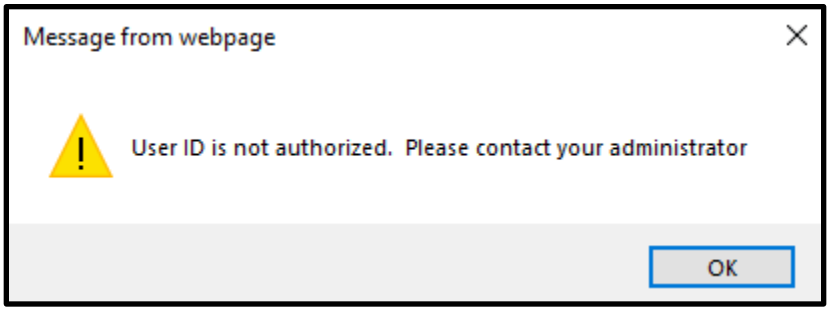
Submit a ZenDesk Ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new

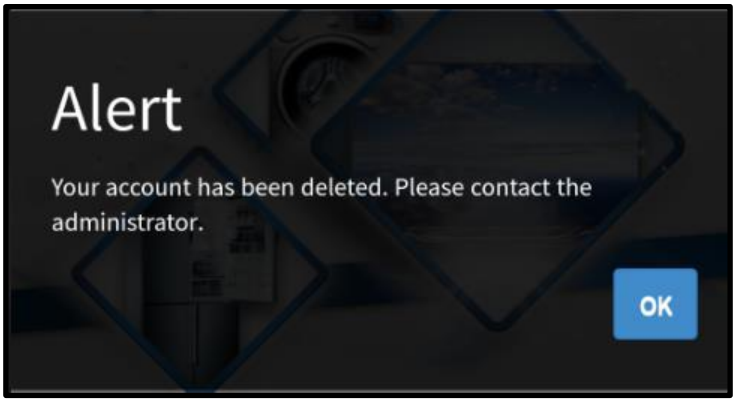
Issue Type: Systems Credentials Support > Expired or Locked GSPN

Description: Explain that your account is locked and include the GSPN account name.

Prevention Measures: Log into your GSPN accounts every day.

GSPN – Account Deleted





Error Message

"User ID is Not Authorized. Please contact your system administrator"

"Your account has been deleted. Please contact the administrator."

Cause

The GSPN account was not logged in for at least 30 days.

Solution

Submit a ZenDesk Ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new

Issue Type: Systems Credentials Support > New GSPN Account

Description: Explain you need a new account to access GSPN. You may need to request both accounts be reactivated (both SIvl and M accounts)

Prevention Measures: Log into your GSPN accounts every day.

GSPN – GD Certificate Approval

Error Message

"The certificate has not been approved yet. Please run GalaxyDiagnostics after the certificate is approved. [530]"

Cause

GD Tool was accessed on another PC. GD Tool can only run on 1 PC per GSPN account. You can request additional accounts via a ZenDesk ticket if you need GD Tool on another computer.

This can also happen if the main Samsung computer was wiped or the hard drive was replaced

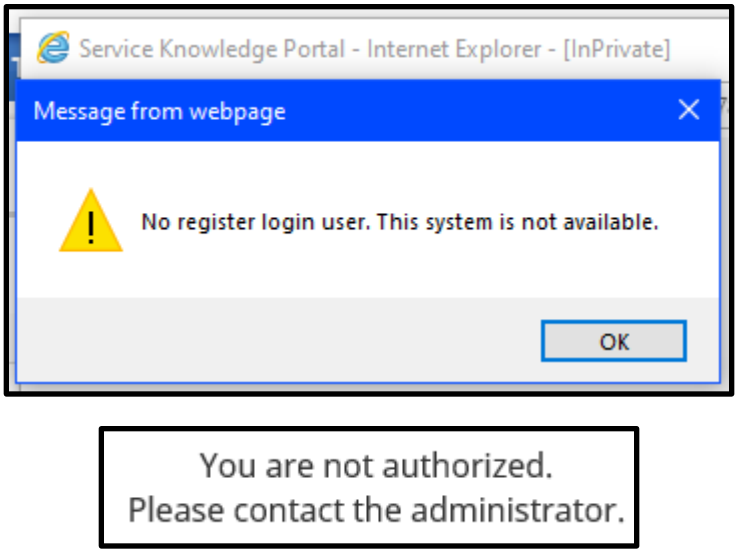
Solution

A guide already exists for this process here: Samsung Systems & Credentials Setup

Go to the GALAXY DIAGNOSTIC SETUP section and scroll down to Step 3.

Prevention Measures: Do not attempt to access GD Tool on another PC if possible.

SKP – Knowledge Tab Lock



Error Message

"No register login user. This system is not available."

Cause

Attempting to access the "Knowledge" tab without entering the certificates password in over 14 days.

Solution

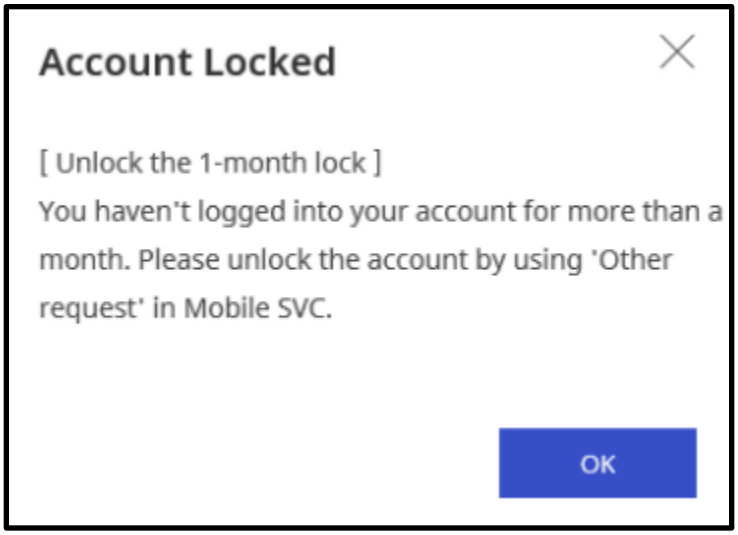
Submit a ZenDesk Ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new

Issue Type: Systems Credentials Support > Knowledge Tab Access Request

Description: Explain that you no longer have access to the Knowledge Tab in GSPN

Prevention Measures: Enter the certificate password everyday in the Mobile SVC section in the Knowledge Tab

SKP – Unlock the 1-Month lock



Error Message

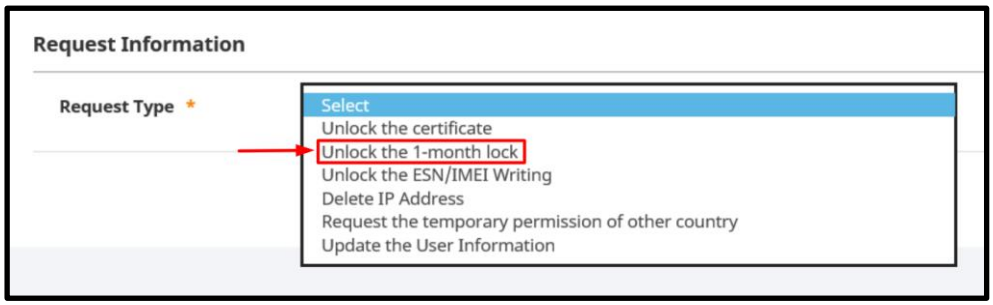
"You haven't logged into your account for more than a month. Please unlock the account by using 'Other request' in Mobile SVC."

Cause

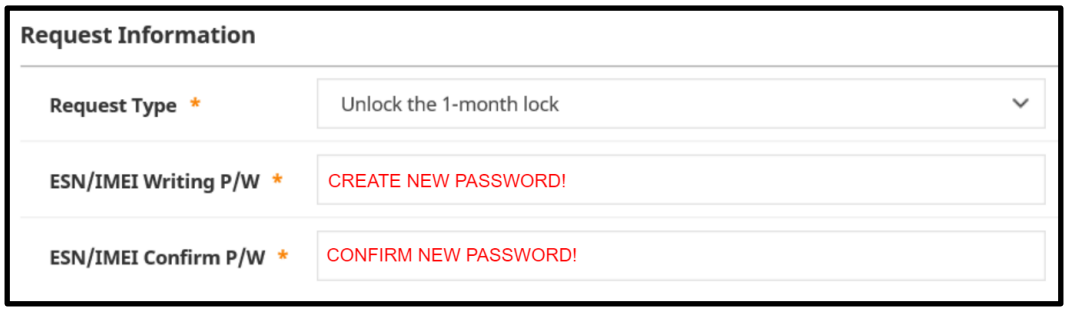
Not generating the OTP code under Mobile SVC within the GSPN Knowledge tab.

Solution

- Access Knowledge Tab on your main GSPN Account (SLVL Account)
- Navigate to Engineer > Mobile SVC > Other Request
- For Request Type select Unlock the 1-month lock



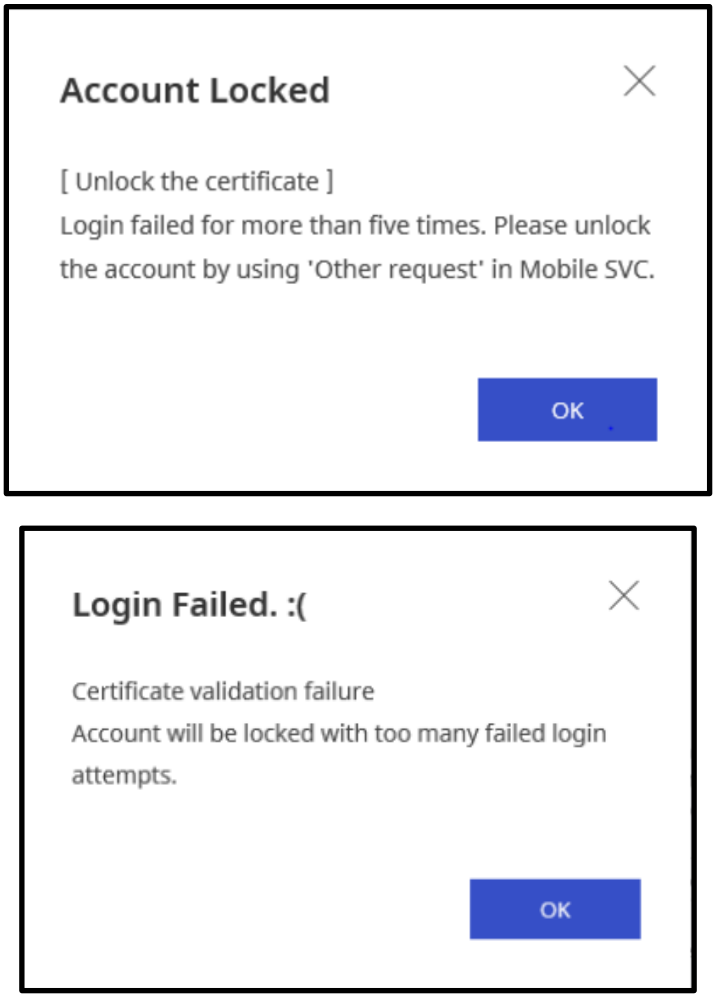
- Create a new ESN/IMEI Writing Password (and take note of it)



- Click on the Request button and then click the Go to Request Page button
- Take a screenshot of Mobile SVC Request Status page
- Submit a ZenDesk ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new
  - Issue Type: System Credentials Support > Unlock the 1-Month Lock
  - Screenshots Required: 3
  - Screenshot of Mobile SVC Request Status Page
  - Screenshot of IP Address from whatismyipaddress.com
  - Screenshot of MAC Address from Windows Command Prompt

Prevention Measures: Enter the certificate password and reissue the OTP code everyday in the Mobile SVC section in the Knowledge Tab

SKP – Unlock the certificate / Login Failed.



Error Message

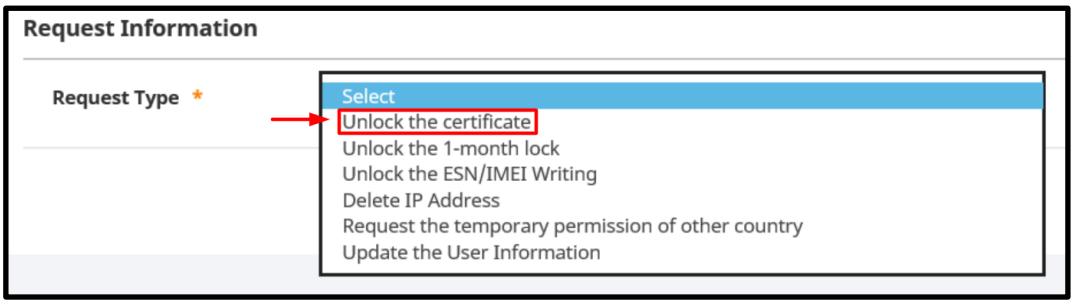
"Login failed for more than five times. Please unlock the account by using 'Other request' in Mobile SVC."
"Certificate validation failure. Account will be locked with many failed login attempts."

Cause

Too many failed login attempts using the Certificates Password.

Solution

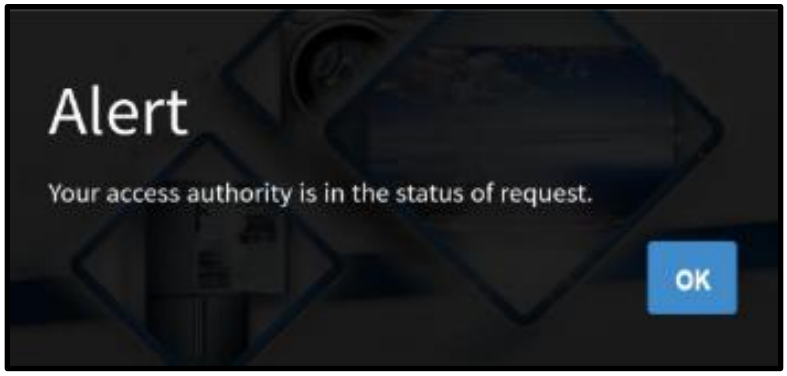
- Access Knowledge Tab on your main GSPN Account (SLVL Account)
- Navigate to Engineer > Mobile SVC > Other Request
- For Request Type select Unlock the Certificate



- Click on the Request button and then click the Go to Request Page button
- Take a screenshot of Mobile SVC Request Status page
- Submit a ZenDesk ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new
    - Issue Type: System Credentials Support > Unlock the Certificate
    - Screenshots Required: 1
    - Screenshot of Mobile SVC Request Status Page

Prevention Measures: Please ensure your passwords are up to date and properly noted somewhere for easy access.

MOTP – Approval Request



Error Message

“Your access authority is in the status of request.”

Cause

The physical MOTP device needs to be approved for mobile GSPN usage. This error should only occur when first setting up the device.

Solution

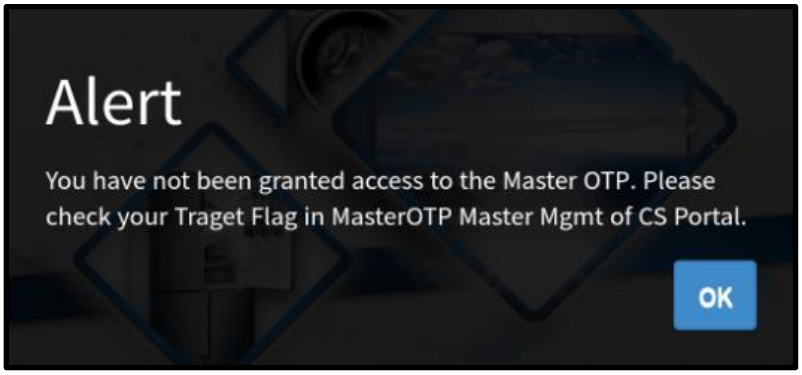
Submit a ZenDesk Ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new

Issue Type: Systems Credentials Support > MOTP Approval Request

Description: Explain that this device needs access to mobile GSPN. Attach a screenshot of the error.

Prevention Measures: N/A

MOTP – Target Flag



Error Message

"You have not been granted access to the Master OTP. Please check your Traget Flag in MasterOTP Master Mgmt of CS Portal"

Cause

The mobile GSPN account has not been assigned to this device. This can happen if you had a new account created due to your previous account being deleted.

Example: Your account may have been named uBiF123**M01** but the new account is now named uBiF123**M02**. This can only be changed by submitting a ZenDesk ticket.

Solution

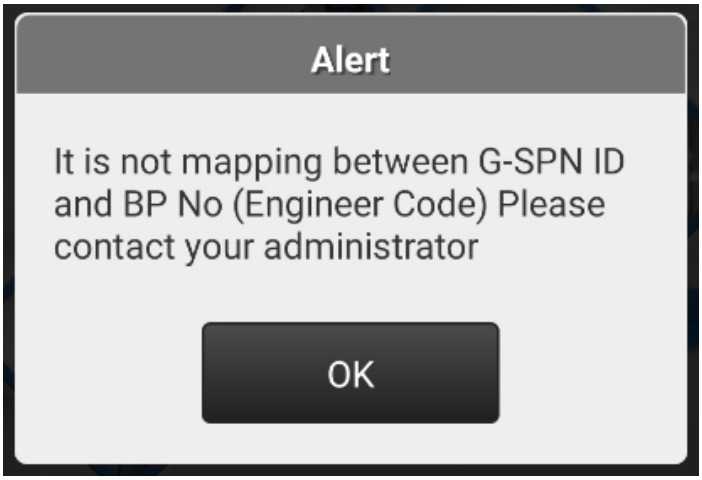
Submit a ZenDesk Ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new

Issue Type: Systems Credentials Support > Target Flag

Description: Explain that the account is not assigned to this MOTP device. Attach a screenshot of the error.

Prevention Measures: N/A

MOTP – Not Mapping between G-SPN ID and BP No



Error Message

"It is not mapping between G-SPN ID and BP No (Engineer Code) Please contact your administrator"

Cause

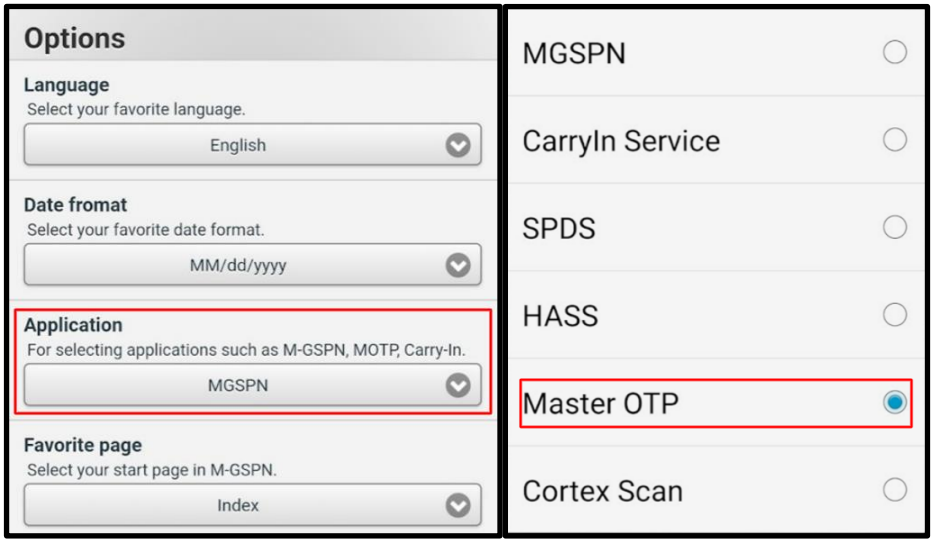
The mobile GSPN application type is not configured correctly.

Solution

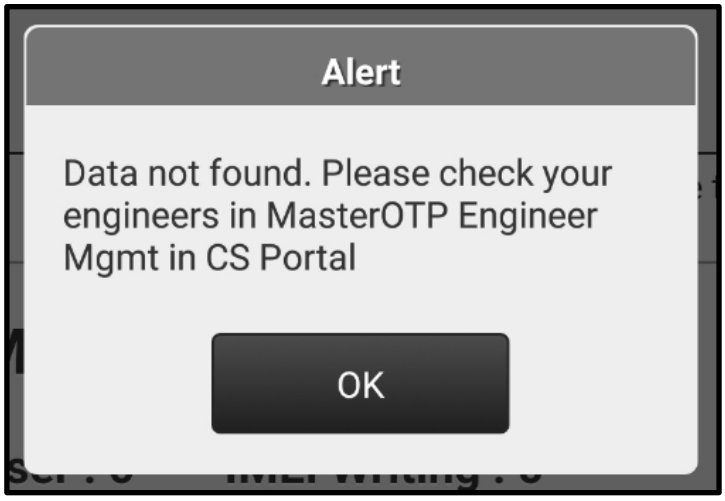
- Open the Mobile GSPN app
- Click the gear icon in the top right corner to access the Options menu
- Under the Application section, click the drop-down and select Master OTP
- Exit the Options menu by clicking the SAVE button

Prevention Measures: N/A


SAMSUNG
MOBILE
G-SPN


Options
Language
Select your favorite language.
English
Date fromat
Select your favorite date format.
MM/dd/yyyy
Application
For selecting applications such as M-GSPN, MOTP, Carry-In.
MGSPN
Favorite page
Select your start page in M-GSPN.
Index
MGSPN
CarryIn Service
SPDS
HASS
Master OTP
Cortex Scan

MOTP – Data Not Found



Error Message

"Data not found. Please check your engineers in MasterOTP Engineer Mgmt in CS Portal"

Cause

Your Level S2 access on your main GSPN account has been revoked or expired.

Solution

A guide already exists for this process here: Samsung Systems & Credentials Setup

Go to the LEVEL S2+ REQUEST section and complete the entire section.

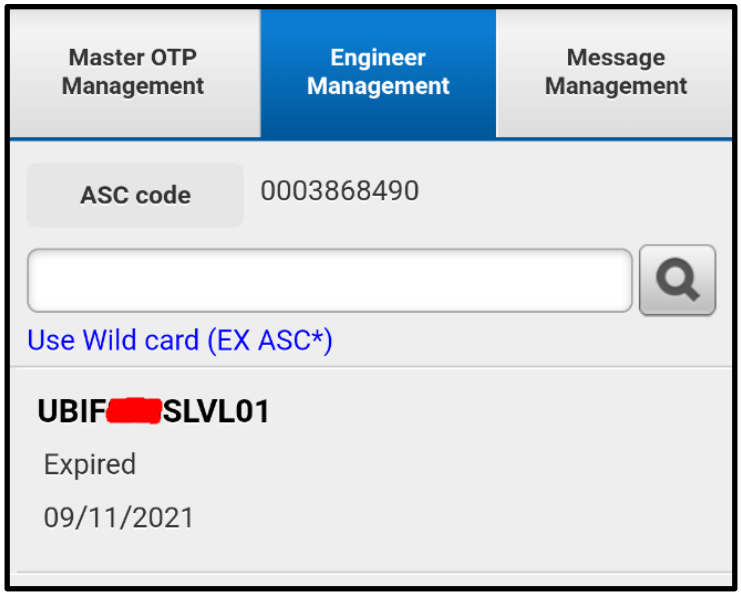
Submit a ZenDesk Ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new

Issue Type: Systems Credentials Support > New Certificate / Level S2

Description: Explain that this device needs access to mobile GSPN.

Prevention Measures: Enter the certificate password and reissue the OTP code everyday in the Mobile SVC section in the Knowledge Tab

MOTP - Engineer Expired



Error Message

"Engineer Management - Expired"

Cause

You have not clicked "Confirm" under the Engineer Management Tab in over 14 days.

Solution

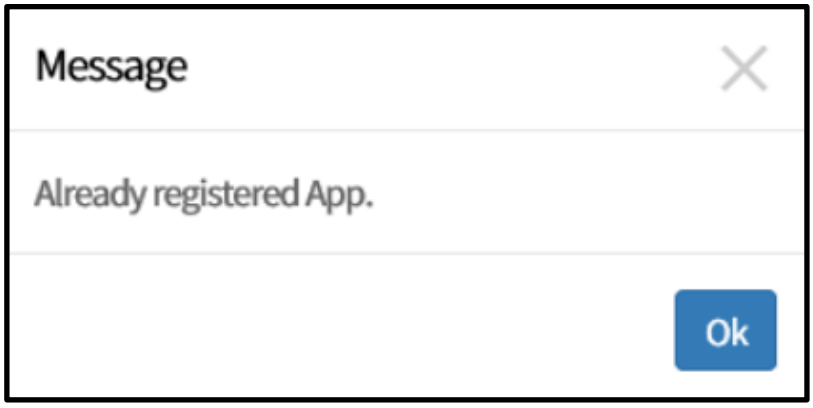
Submit a ZenDesk Ticket: https://ubifsupport.zendesk.com/hc/en-us/requests/new

Issue Type: Systems Credentials Support > Engineer Extension (MGSPN)

Description: Explain that your Engineer access has expired on the MOTP device

Prevention Measures: Click the "Confirm" button under the Engineer Management tab on the MOTP device.

MFA – Already registered App.



Error Message

"Already registered App."

Cause

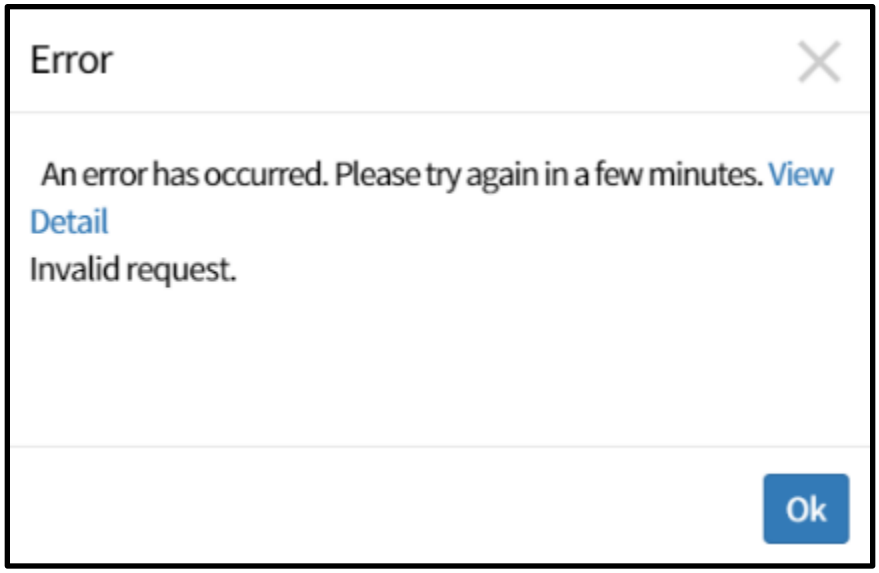
The device and app is already registered to another GSPN account. The Authentication ID you typed in can only be used once per account.

Solution

- Ensure you are logging into the correct account.
- It's worth noting that you need an **separate MFA device** (a total of two devices) for both GSPN accounts
  - One device and app is needed for your **main account** (SLVL account)
  - One device and app is needed for your **MOTP account** (M account)
    - The MOTP device can have the MFA app installed on it as well
    - The 2nd device can be either an iOS or Android device of your choice

Prevention Measures: You need an MFA device for each GSPN login. You can also review the MFA setup guide here: https://portal.ubif.net/kbase/article/10216

MFA – Invalid Request



Error Message

"An error has occurred. Please try again in a few minutes. View Detail > Invalid Request."

Cause

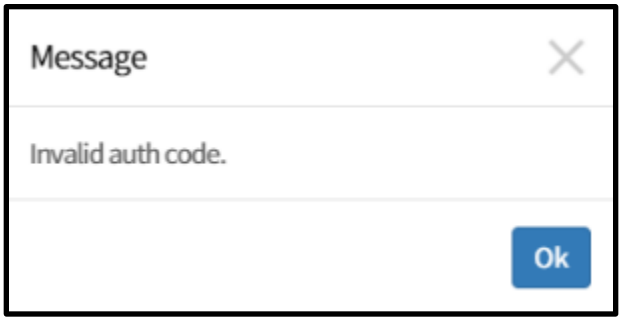
- The device is not connected to the internet.
- The device was connected to Wi-Fi after the app was opened.
- The app session has timed out.

Solution

- Reconnect the device to Wi-Fi and force close and reopen the app.
- If the above does not work, log out of GSPN and log back into the account

Prevention Measures: N/A

MFA – Invalid auth code.



Error Message

“Invalid auth code.”

Cause

- The device is tied to another GSPN account.
- The device is not connected to the internet.

Solution

- Ensure you are logging into the correct account.
- Reconnect the device to Wi-Fi and force close and reopen the app.

Prevention Measures: N/A

OJT: Z Flip4 Digital Hall IC Calibration

Introduction

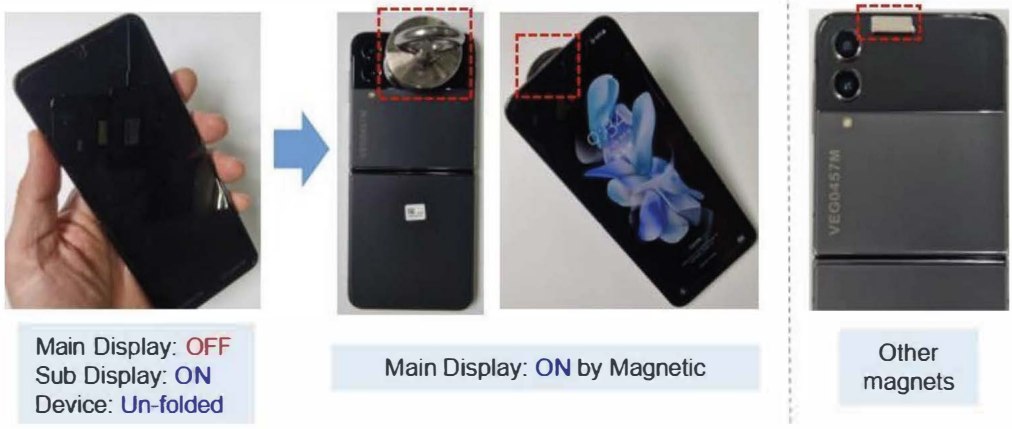
This document is intended to guide technicians in completing Digital Hall IC Calibration on Galaxy Z Flip4 devices.

Turning On the Main Display – Table Magnet

If the Main Display is not turning on after Main PBA or Front Assembly repair, the Main Display can be turned on manually using the instructions in the step table below.

- A Table Magnet (GH81-18190A) is required to manually turn on the Main Display
- When the device is unfolded, the Main Display will be OFF and the Sub Display will be ON

GH81-18190A



Main Display: OFF
Sub Display: ON
Device: Un-folded

Main Display: ON by Magnetic

Other magnets

Note: If the Main Display turns off after the Booting animation (Samsung & Carrier logos) have been shown through Main Display, then there is no hardware defect.

Step	Action
1.	Place the Table Magnet at the top center side of the Sub Display on the Rear • The Magnet will be held to the Rear of the Sub Display by the embedded magnet on that side of the device
2.	When the Table Magnet sticks in place to the Rear of the Sub Display, the Main Display will turn on

Revised September 21, 2022

SAMSUNG Care

Turning On the Main Display – Key Combination

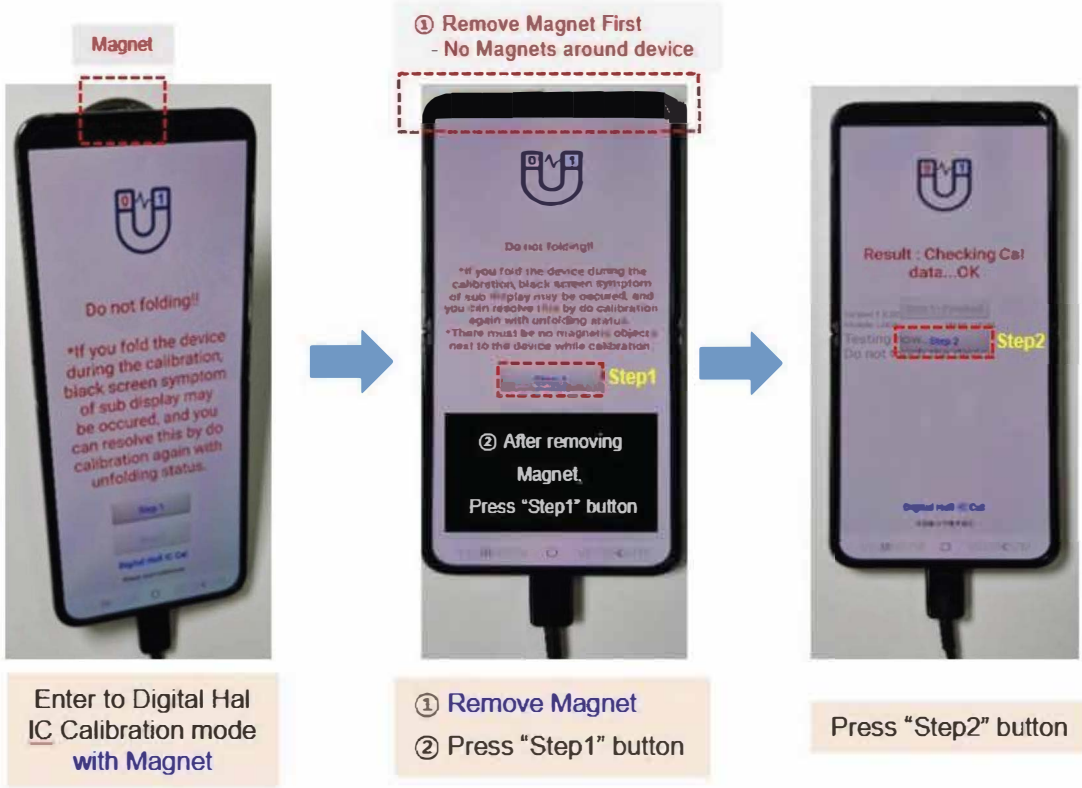
After MR1 has been installed on Galaxy Flip4 devices, the Main Display may be enabled using a keypress combination.

After connecting a USB cable to the device:

1. Press and hold the **Power** key
2. Short-press (press and let go) **Volume Up (+)** once (1x)
3. Short-press (press and let go) **Volume Down (-)** twice (2x)

Completing Digital Hall IC Calibration

Use the instructions in the step table below to use Galaxy Diagnostics for Digital Hall IC Calibration:



Revised September 21, 2022

SAMSUNG Care

Note: There cannot be any magnetic objects around the device to complete Digital Hall IC Calibration successfully; once the device has been placed in Digital Hall IC Calibration mode, remove the Table Magnet (if used) and make sure it is placed far from the device so that it does not impact calibration.

Step	Action
1.	Enter Digital Hall IC Calibration mode, then remove the Table Magnet (if used) and place it far away from the device
2.	After the Table Magnet has been removed, press **Step 1** to start Digital Hall IC Calibration
3.	Press **Step 2** to finish calibration

Revision History

The following table lists the revisions made to this OJT resource.

Version	Released	Revision
1	09/13/2022	• First published edition of this document.

OJT: IMEI Cloud Tool Pilot

Introduction

This document is intended to instruct technicians in the proper installation and usage of the IMEI Cloud Client application on the Service PC in support of the IMEI Cloud Tool pilot.

What is the IMEI Cloud Tool?

Samsung is excited to introduce the new IMEI Cloud Tool for use during this pilot. This tool has been designed to complete the IMEI rewrite process on supported models. The IMEI Cloud Tool is designed to serve as a streamlined, semi-automated process that will help expedite the IMEI rewrite process.

The IMEI Cloud Tool will:

- Reduce the setup and configuration time for IMEI rewrite
- Eliminate the need to manually download associated files (i.e. POT files)
- Eliminate the need to maintain local file directories for required files
- Decrease turnaround time for repairs requiring IMEI rewrite
- Positively impact the customer experience

The IMEI Cloud Tool has been built to reduce the amount of configuration, setup, and maintenance required for the IMEI rewrite process. The new streamlined process is designed to be intuitive, effortless, and fast.

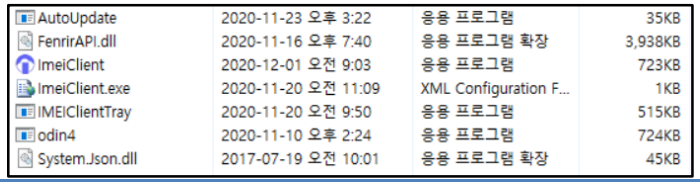
Prerequisites

The following are required to use the IMEI Cloud Client:

- Service PC running Fenrir
  - Make sure that the most up to date binaries have been downloaded in Fenrir for the device being serviced
- Ensure that any VPN connection is disconnected prior to initializing the **ImeiClient.exe**
- Only certain models are supported using the IMEI Cloud Client application at this time.

Download & File Extraction

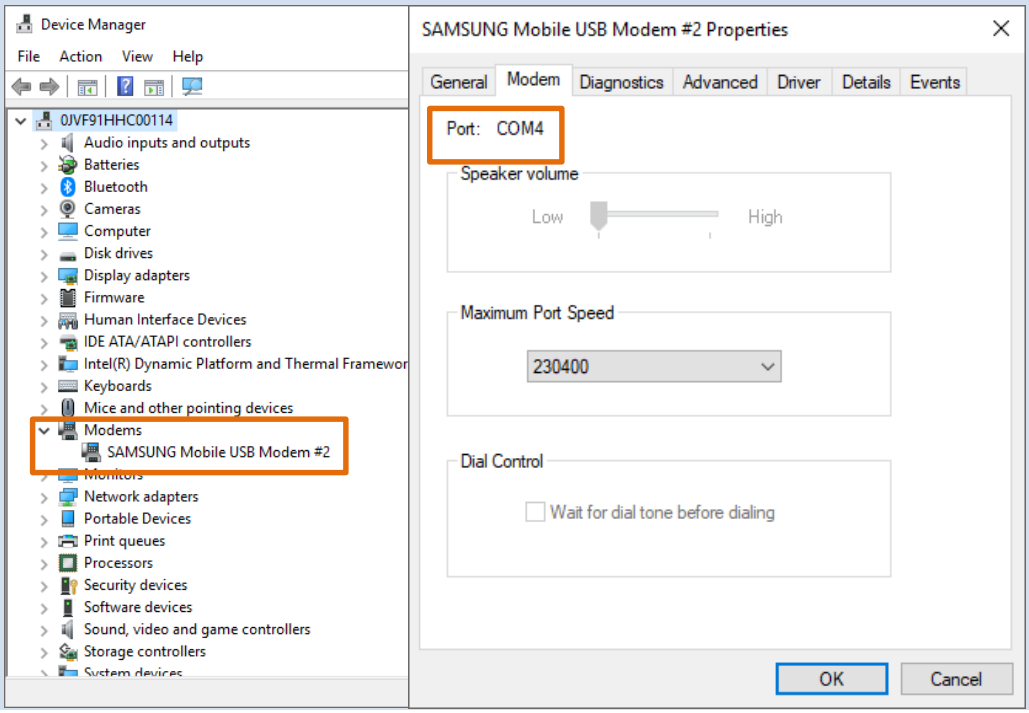
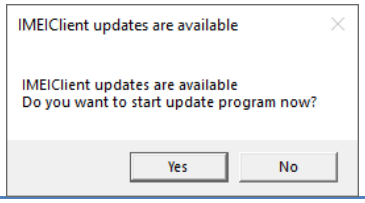
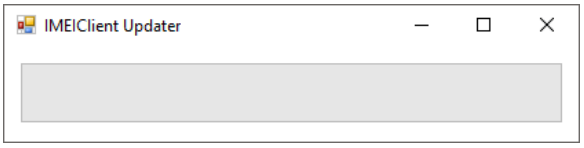
Follow the instructions in the step table below to download and extract the IMEI Cloud Client:

Step	Action
1.	Using an Internet browser, navigate to https://api.secmobilesvc.com/client/GSPN.zip to download the zip archive **IMEI Client GSPN**
2.	Navigate to the downloaded zip archive **IMEI Client GSPN**: • Right click on the zip archive • Select Extract All • Select a location for file extraction • The following items are included in the zip archive: 

Using IMEI Cloud Client via the USB Method (Page 2-6)

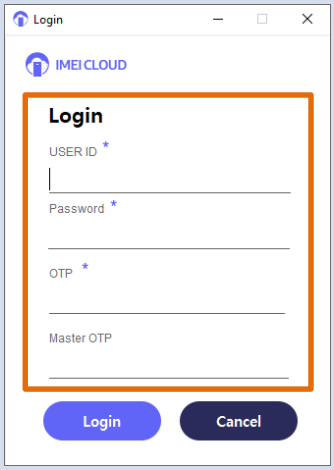
Follow the instructions in the step table below to configure and use the IMEI Cloud Client:

Note: When changing from one model to another, the IMEI Cloud Client tool does not require that the user exit and restart the tool.

Step	Action
1.	Attach the mobile phone to the Service PC using a USB cable • Take note of the COM Port assigned to the device using the Windows Device Manager (Launch Device Manager › Select arrow beside Modems to reveal devices › Right click and select Properties › Activate the Modem tab › Note Port): 
2.	Using Windows Explorer, navigate to the location of the extracted IMEI Cloud Client, and run **ImeiClient.exe** to start the IMEI Cloud Client **Required:** If the IMEI Cloud Client tool needs to be updated, please update as prompted:  

3. Enter the following information into the IMEI Cloud login screen:

   - G-SPN User ID
   - Service Tool Password
   - OTP
   - Master OTP



4. Click the **Login** button to log in to the tool

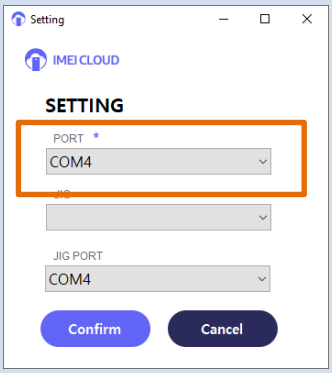
   Note: After successfully logging in, users won't be required to login unless the IMEI Cloud Client tool has been closed or the OTP has expired

5. Set the COM Port for the mobile device based on step 1 for the USB method.

   If unable to use the USB method, proceed using the Anyway Jig (Using the IMEI Cloud Client via the Anyway Jig).

   - Configuration is not required after the first time the IMEI Cloud Client is used

   Note: The COM Port assigned to the mobile device may change if the USB cable is moved to a different port and/or if the Service PC is rebooted



Ensure you are using a compatible Samsung authorized USB cable when utilizing the USB method.

6. Input the device IMEI and the G-SPN Ticket NO:

Note: You can input the IMEI via the barcode scanner or by manually typing in the IMEI.

7. Click the IMEI Write button to complete the IMEI write.

Note: The IMEI Write should be completed followed by the Fenrir D/L option prior to completing the IMEI check.

8. The IMEI Cloud Tool will automatically complete the IMEI rewrite process. A pass message will be displayed once completed successfully.

9. **Ensure the required factory binary has already been installed and is available prior to this step.**

After successfully completing the IMEI Write process in the IMEI Cloud tool, use the Fenrir D/L button within the IMEI Cloud tool to complete a factory binary on the customer's device.

Note: After clicking the Fenrir D/L option, the connected device will automatically be restarted in download mode.

10. Select the correct model, carrier, and S/W version using the three provided drop down fields and click **OK**.

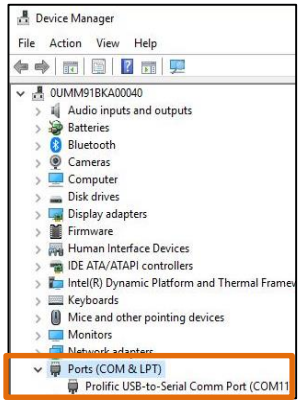
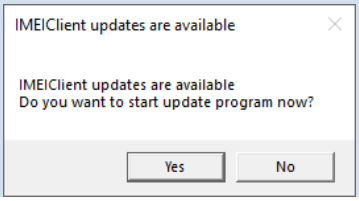
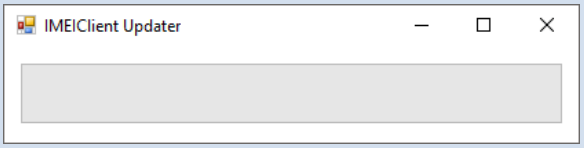
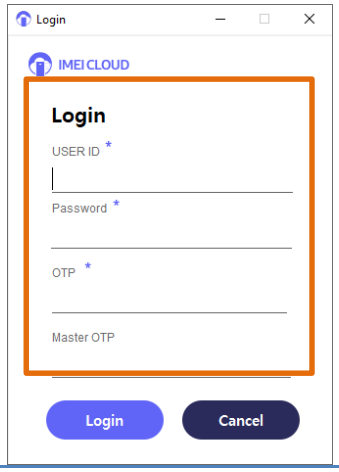
The factory binary will automatically initialize and complete, the device will restart.

11. Click the IMEI Check button to complete the IMEI check.

12. Complete Warranty Validation using Fenrir and proceed with closing the ticket as normal.

Using IMEI Cloud Client via the Anyway Jig (Page 6-11)

If the USB method is unstable, you can alternatively use the Anyway Jig to complete the IMEI Rewrite process using the IMEI Cloud Tool. Use the steps below to complete the IMEI Write and IMEI Check process using the Anyway Jig method.

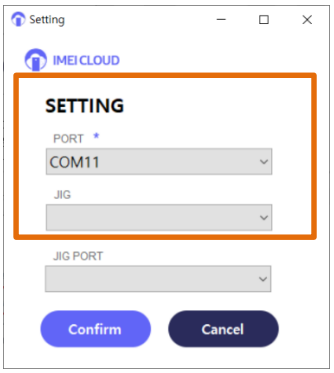
Step	Action
1.	Turn on the S103 Anyway Jig and connect the Anyway Jig to the 5V power supply. Connect the Anyway Jig to the Service PC using the serial to USB cable. **Note:** Do not connect the device to the Anyway Jig
2.	Verify the COM port number of the Anyway Jig in the Device Manager (Launch Device Manager > Select arrow beside Ports to reveal devices > Note the Port beside the **Prolific USB-to-Serial Comm** Port option, i.e. COM11): 
3.	Using Windows Explorer, navigate to the location of the extracted IMEI Cloud Client, and run **ImeiClient.exe** to start the IMEI Cloud Client **Required:** If the IMEI Cloud Client tool needs to be updated, please update as prompted:  
4.	Enter the following information into the IMEI Cloud login screen: • G-SPN User ID • Service Tool Password • Master OTP • OTP 

5. Click the **Login** button to log in to the tool

   Note: After successfully logging in, users won't be required to login unless the IMEI Cloud Client tool has been closed or the OTP has expired

6. Set the COM Port for the Anyway Jig based on step 2. The port setting for the Anyway Jig should be entered in the first Port drop down. Select the Jig in use (i.e. S103) under the Jig dropdown.

   Note: The "Jig port" will be grayed out when using the Anyway Jig method. The port from the Anyway Jig should be entered using the first Port drop down.



7. Input the device IMEI and the G-SPN Ticket NO:

   Note: You can input the IMEI via the barcode scanner or by manually typing in the IMEI.

8. Turn the device off and plug the I/F cable into the device, wait for the device to fully boot on.

9. Click the IMEI Write button to complete the IMEI write.

Note: The IMEI Write should be completed followed by the Fenrir D/L option prior to completing the IMEI check.

10. The IMEI Cloud Tool will automatically complete the IMEI rewrite process. A pass message will be displayed once completed successfully.

11. **Do not close the IMEI Cloud Rewrite Tool.**

Ensure the required factory binary has already been installed and is available prior to this step.

After successfully completing the IMEI Write process in the IMEI Cloud tool, use the Fenrir D/L button within the IMEI Cloud tool to complete a factory binary on the customer's device.

Note: After clicking the Fenrir D/L option, the connected device will automatically be restarted in download mode.

12. Select the correct model, carrier, and S/W version using the three provided drop down fields and click **OK**.

The factory binary will automatically initialize and complete, the device will restart.

13. Turn off the device and plug the I/F cable into the device, wait for the device to fully boot on.

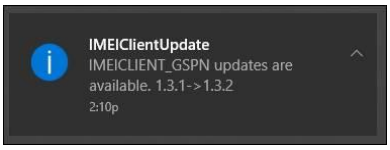
    Click the IMEI Check button to complete the IMEI check.

14. Complete Warranty Validation using Fenrir and proceed with closing the ticket as normal.

Troubleshooting

Q: I've seen a message on my service PC advising an IMEIClientUpdate as available, what should I do?

A: This message indicates there is an update required for the IMEI Cloud Tool. To initialize the update, please click the notification and complete the update wizard. Updates ensure that the tool is running the latest version to ensure the supported processes function correctly.



Q: I'm being prompted to enter a CAPTCHA, why is this occurring?

A: If you've failed to enter the correct login information when trying to access the IMEI Cloud Tool, you may be required to enter a CAPTCHA to validate your login attempt. To complete, type the CAPTCHA in as requested and click OK.

Q: I've received an error E1016 advising an invalid username or password has been entered. What should I do?

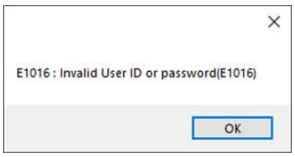
A: Ensure you've entered the proper credentials and try to login again. Your login credentials are:

Username – G-SPN Username

Password – Service Tool password

OTP – OTP generated in G-SPN

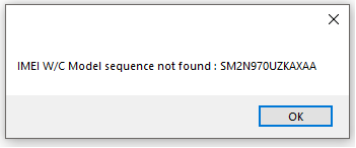
Master OTP – Master OTP generated using Mobile GSPN tool



Q: Which devices are supported by the IMEI Cloud Tool during the initial pilot?

A: The initial list of devices supported by the IMEI Cloud Tool during the pilot include the A21 (SM-A215U), Note10 (SM-N970U), Note10+ (SM-N975U), Note10 Ultra (SM-N976U), Note10 Ultra (SM-N976V)

In the event that an unsupported device/IMEI is detected, an error will be displayed.



Q: What else should I know about error codes and the IMEI Cloud Tool?

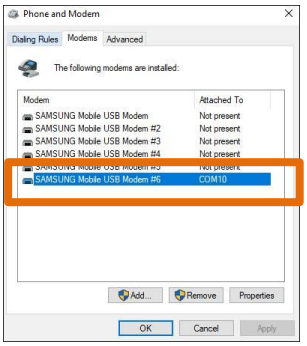
A: The IMEI Cloud Tool uses the same error code types used in Dasuel.

Q: When I use Device Manager to detect the COM port number for the device, I am having trouble validating which port is associated with my device.

A: In the event that you are unable to use the Device Manager to validate the port number of the device you are using, you may need to use the Phone and Modem setting within the Control Panel to validate.

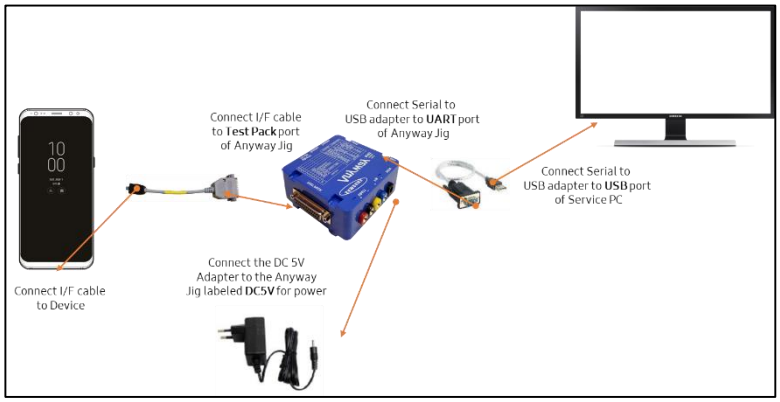
Launch the Control Panel › Type in Phone and Modem in the search field › Once the Phone and modem option launches, if prompted enter your local 3 digit area code › Click the Modems tab › Connect your device › Note the "attached to" column for your device to verify the COM port.

In the event that 20 or more Samsung Mobile USB modem options are displayed, you may need to remove devices that are not in use.



Q: When running the IMEI Write and IMEI Check function via the Anyway Jig method, how should the configuration of the equipment appear?

A: Remember to follower the steps of the Anyway Jig method to ensure the process functions correctly.



Q: When attempting the Fenrir D/L option, I'm getting an unexpected error or failure, what should I check?

A: Remember the required factory binary must be downloaded in Fenrir prior to using the Fenrir D/L option in the IMEI Cloud Tool.

OJT: FRP Unlock Tool Migration

Introduction

This document is intended to educate technicians about migration to the new FRP Unlock function built into the IMEI Cloud Client tool.

About FRP Unlock Tool Migration

Effective August 19, 2024, Samsung is migrating FRP Unlock functionality into the IMEI Cloud Client tool. This is a part of ongoing system consolidation effort to simplify Samsung Repair Process. This migration of FRP Unlock to IMEI Cloud will allow technicians to use the IMEI Cloud Client tool to complete FRP Unlock on devices operating on Android OS.

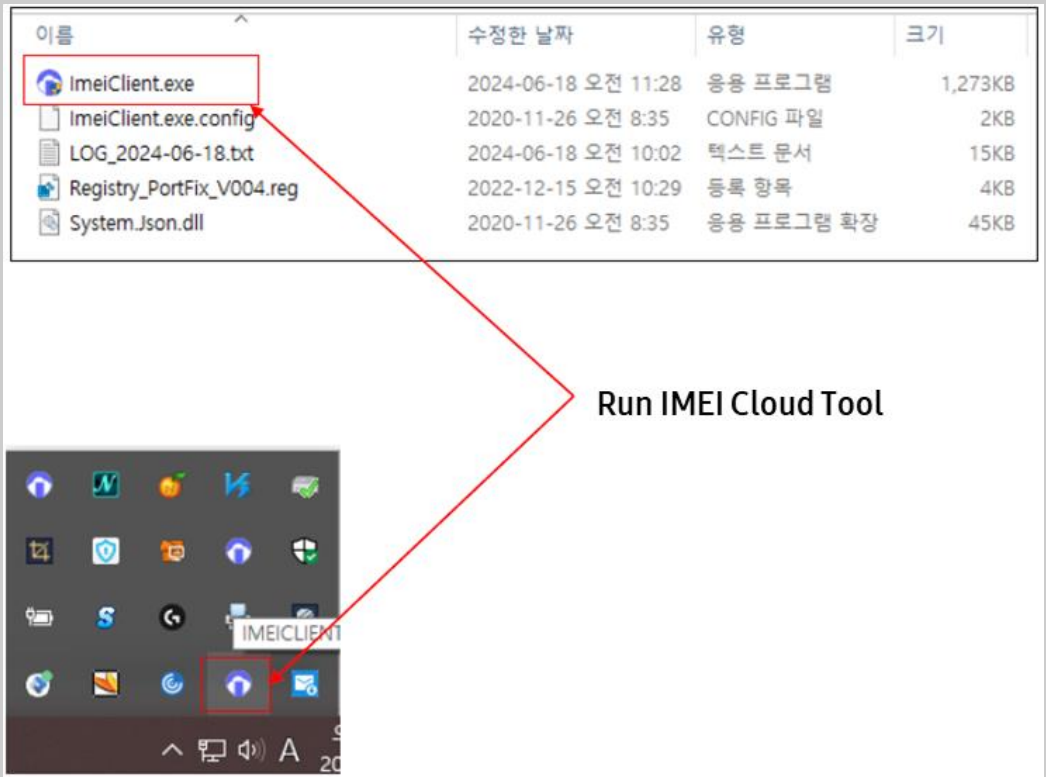
There are several benefits:

- Elimination of Galaxy Must log-in requirement
- No change in IMEI Cloud Client log-in process
- Using an existing tool with an existing process means there should be a quick learning curve for the new method

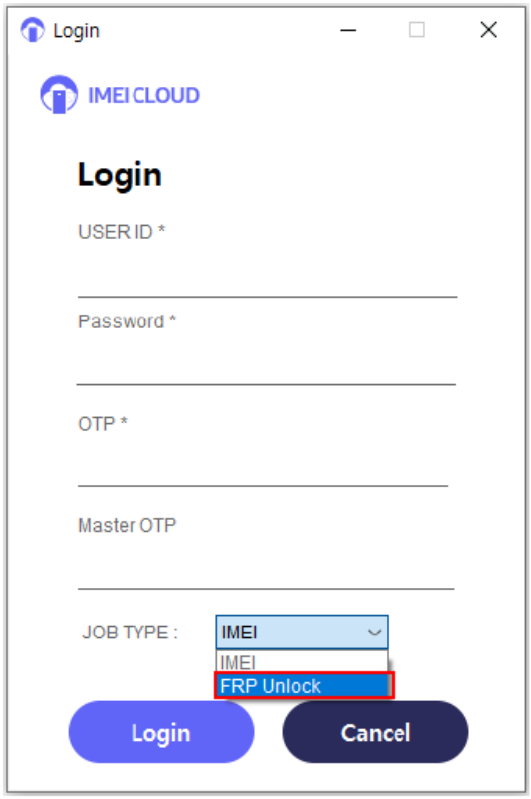
Using IMEI Cloud Client Tool - FRP Unlock

Use the instructions in the step table below to use the IMEI Cloud Client tool to complete FRP Unlock:

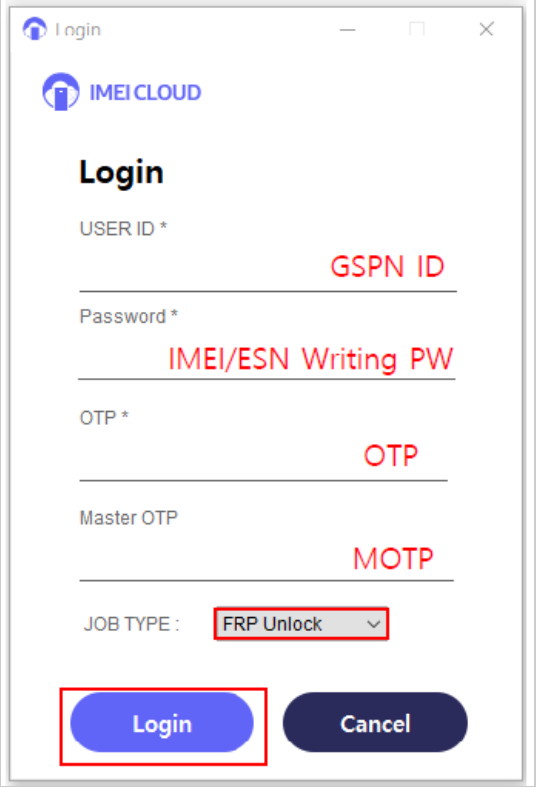
Step	Action
1.	Open the IMEI Cloud Client using either the IMEICLIENT icon or by running "ImeiClient.exe"



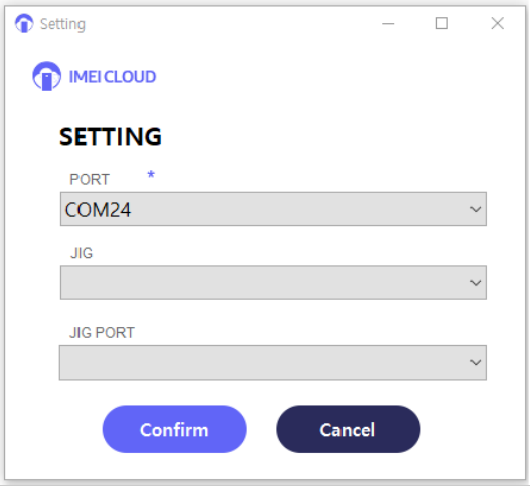
2. Select the **Job Type** (FRP Unlock to complete FRP Unlock)



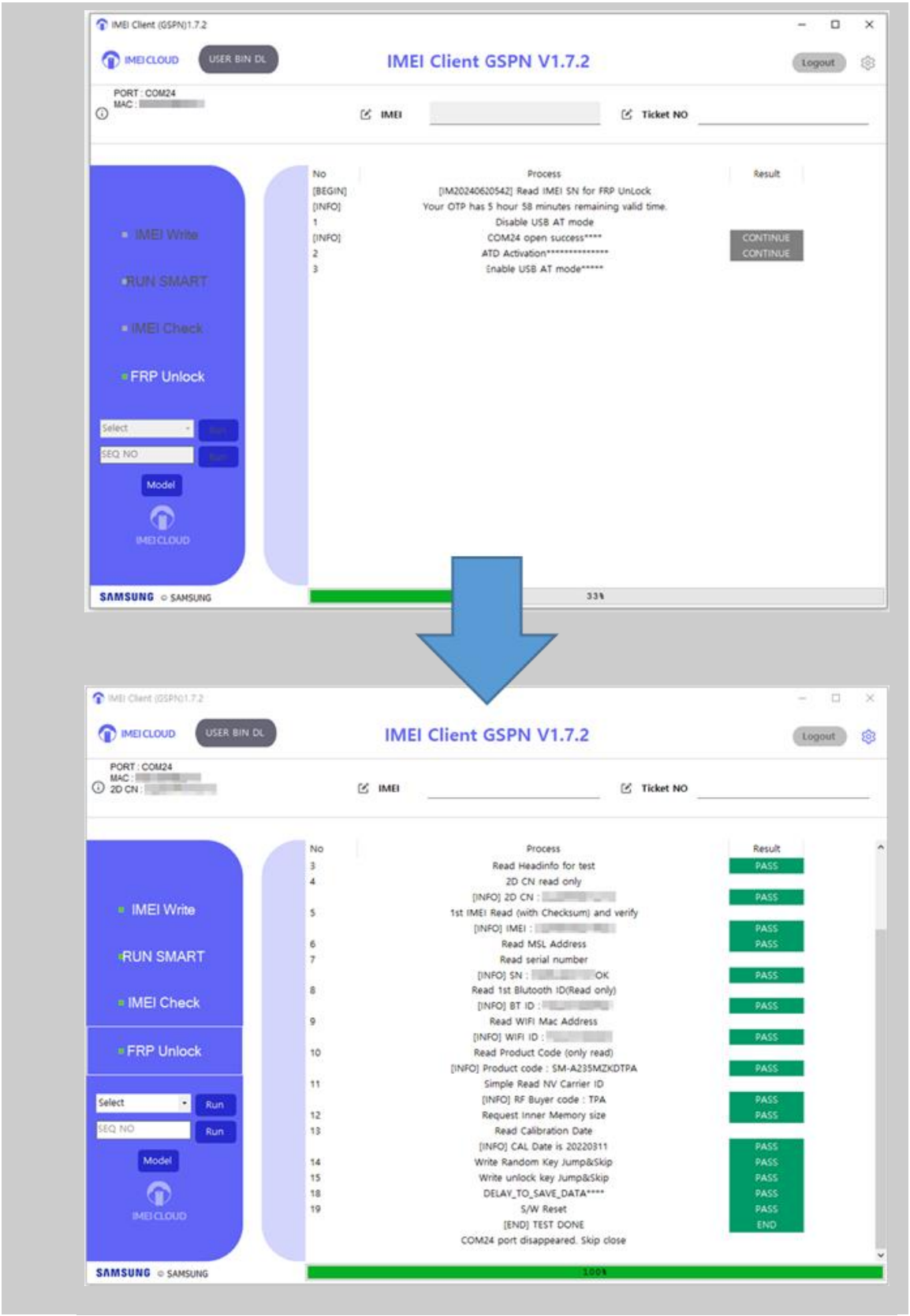
3. Log in with the following information:
   - GSPN ID
   - IMEI Write Password
   - OTP
   - MOTP



4. Select and confirm the COM port number



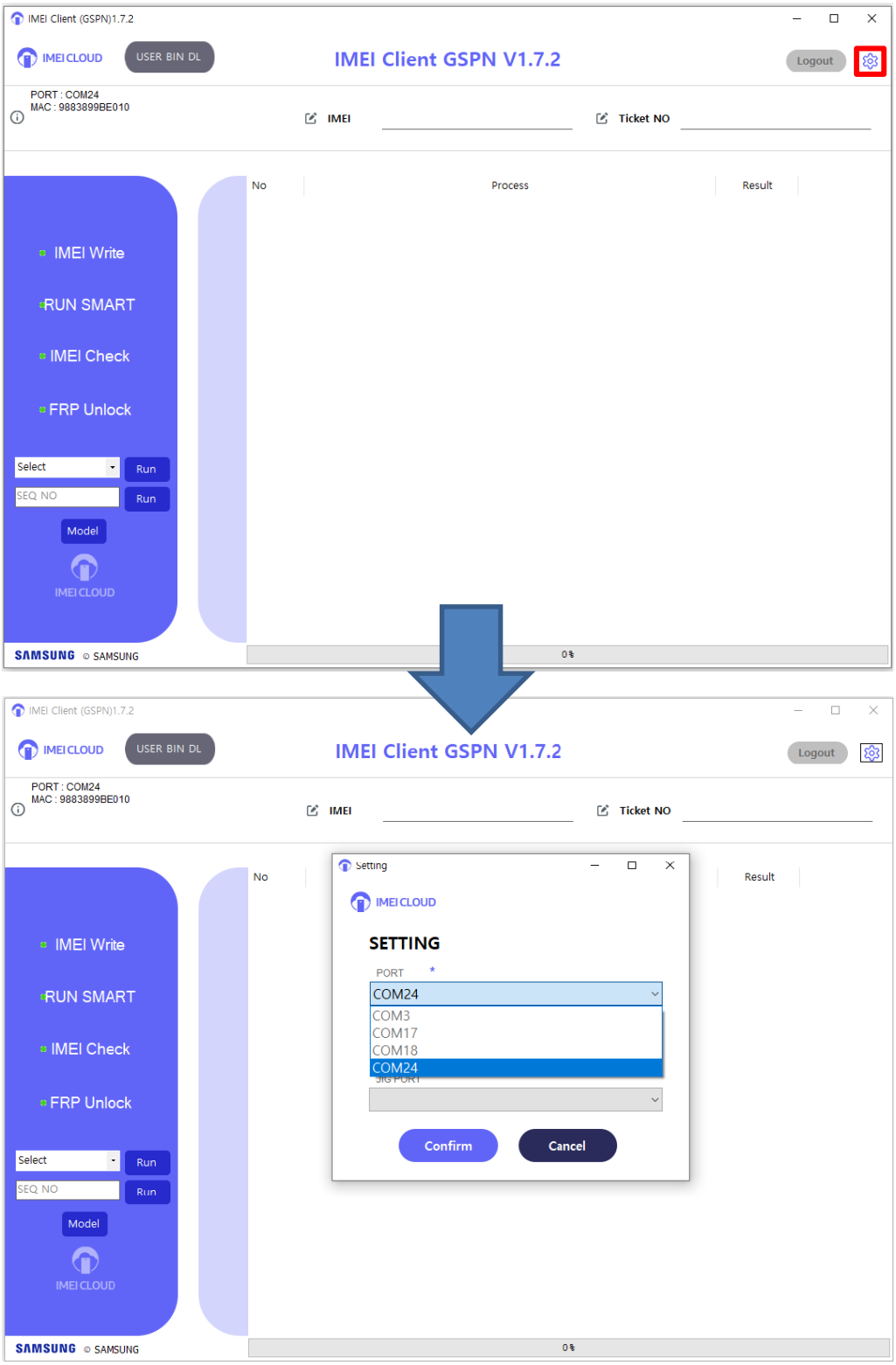
5. Click **FRP Unlock**
   - FRP Unlock will complete automatically
     - Read phone information (Auto)
     - FRP Unlock and check “PASS”



Changing the COM Port

To change the COM port being used by the IMEI Cloud Client tool:

1. Click the **Settings** button at the top right of the UI
2. Select the desired COM port number, then click **Confirm**



Revision History

The following table lists the revisions made to this OJT resource.

Version	Released	Revision
1	08/07/2024	• First published edition of this document.

OJT: Scanning Main PBA QR Codes

Introduction

This document is intended to guide agents on where to find and scan QR codes on the Main PBA. Knowing where to locate and scan the QR codes will enable more accurate parts management during and after repairs.

Topic

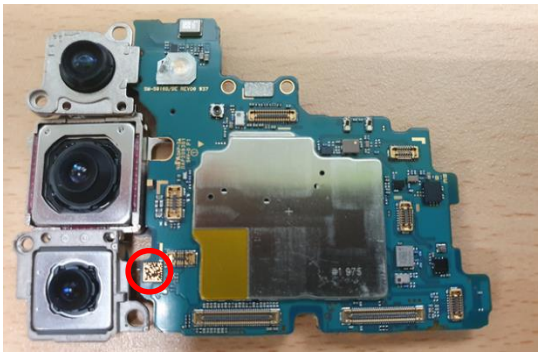
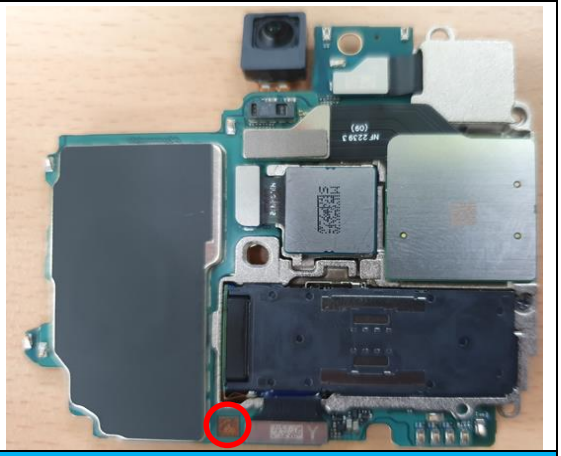
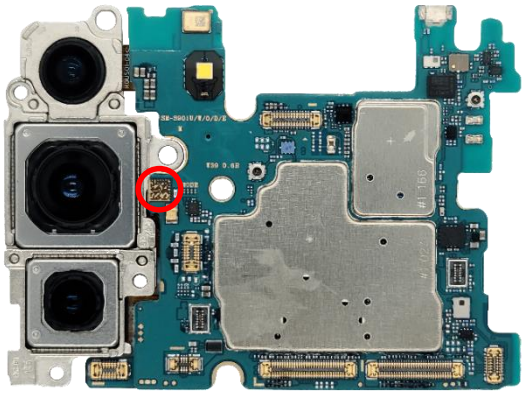
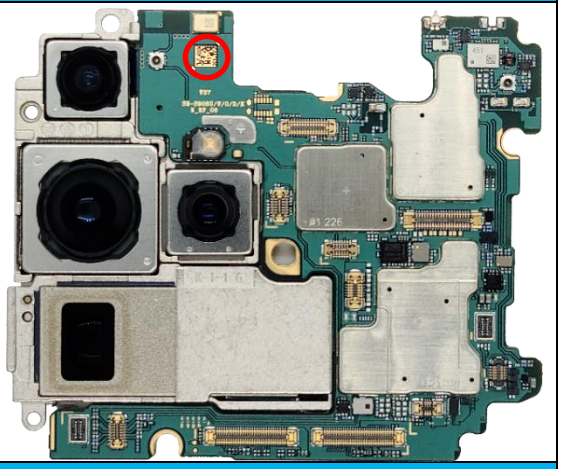
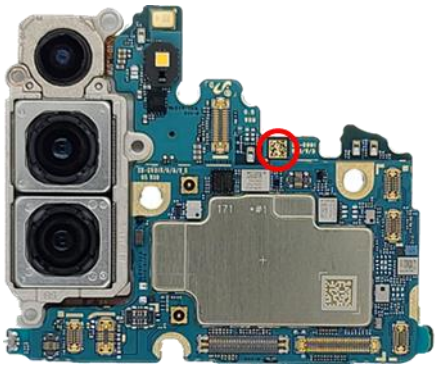
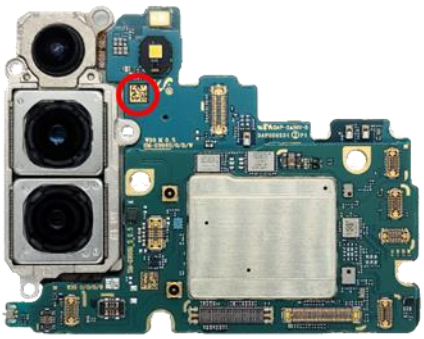
The Main PBAs for Samsung devices feature an embedded QR code that enables the part to be scanned during repairs. Utilizing the QR code allows the unique identifying information for each Main PBA to be tracked and managed effectively. Scanning the QR code helps to reduce the impact of human error when managing parts, and increases the speed at which parts can be tracked and shipped via U-Class.

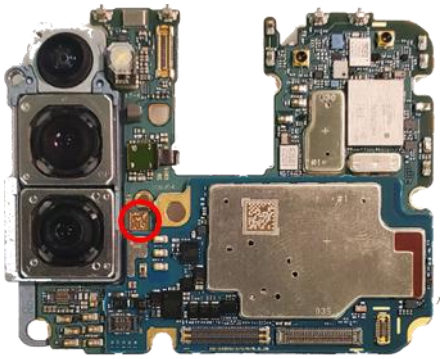
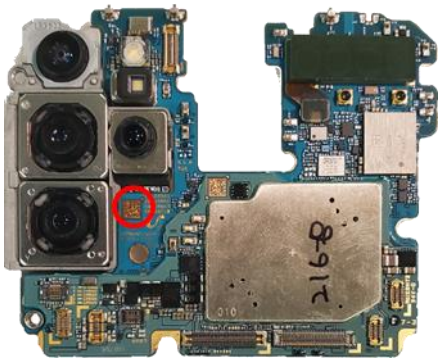
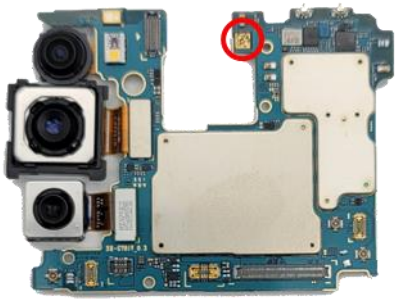
The following device series are listed:

- Galaxy S Series
- Galaxy Note Series
- Galaxy Z Series
- Galaxy A Series
- Additional Devices

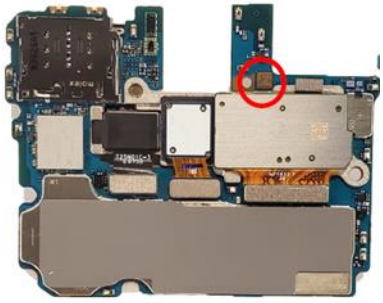
Revised August 15, 2023

Galaxy S Series

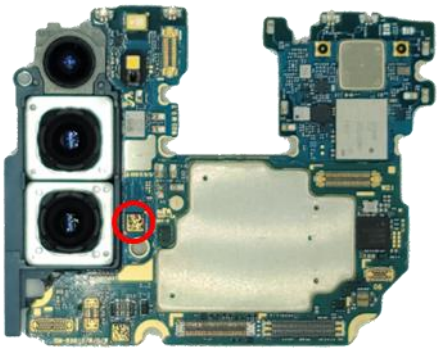
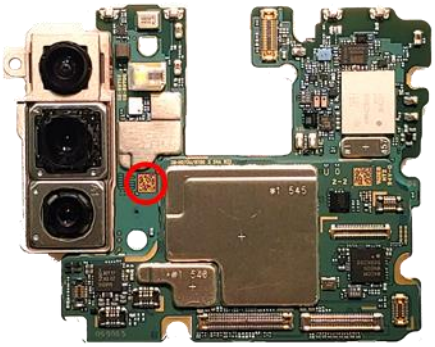
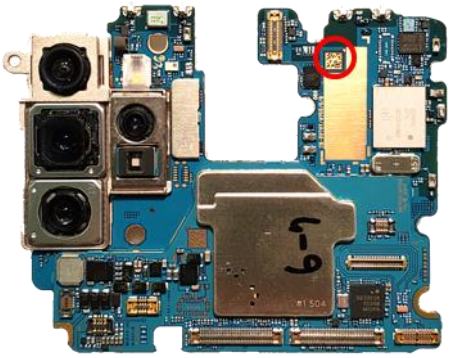
Galaxy S23 & Galaxy S23+	Galaxy S23 Ultra (Rear Side)
	
Galaxy S22 & Galaxy S22+	**Galaxy S22 Ultra**
	
Galaxy S21 5G	**Galaxy S21+ 5G**
	

Galaxy S21 Ultra 5G	Galaxy S20 5G
	
Galaxy S20+ 5G	**Galaxy S20 Ultra 5G**
	
Galaxy S20 FE	**Galaxy S10**
	

Galaxy S10e	Galaxy S10+
	

Galaxy S10 5G (Rear)


Galaxy Note Series

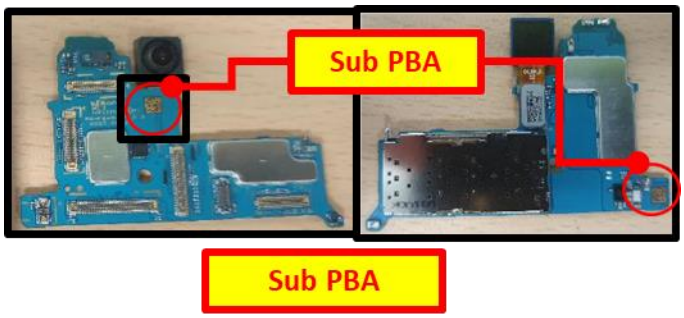
Galaxy Note20 5G	Galaxy Note20 Ultra 5G
	
Galaxy Note10	**Galaxy Note10+**
	

Revised August 15, 2023

SAMSUNG Care

Galaxy Z Series

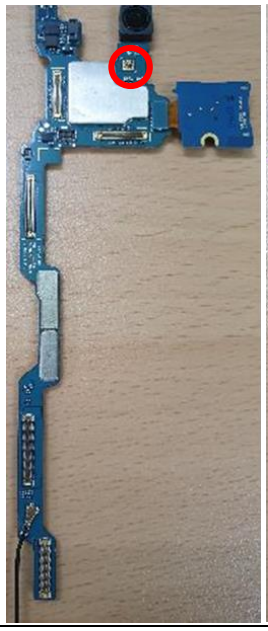
Galaxy Z Fold5



Galaxy Z Fold4

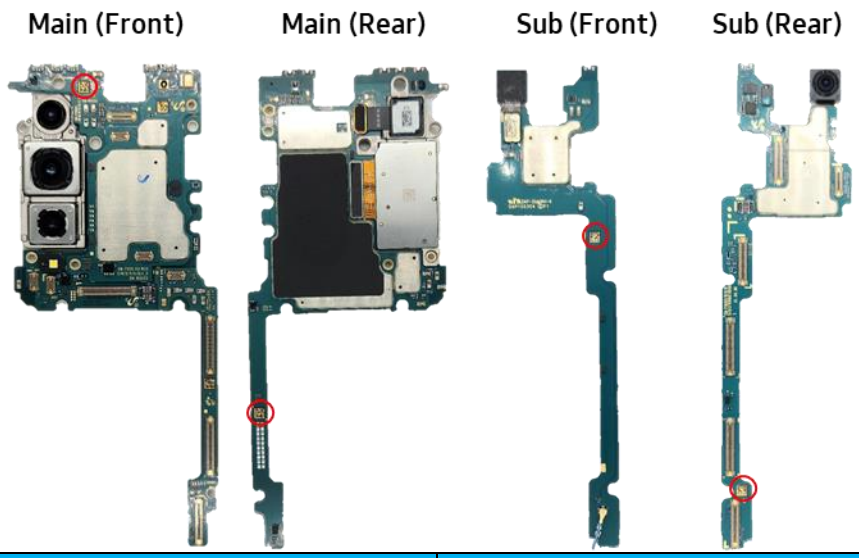
Main

Sub (Rear)



Sub (Front)

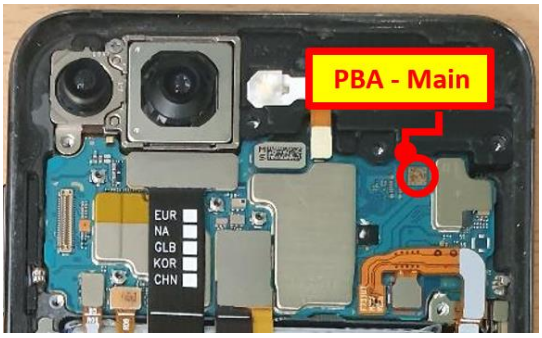
Galaxy Z Fold3 5G



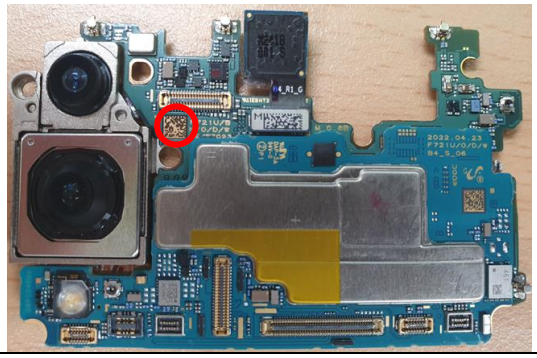
Galaxy Z Fold2 5G

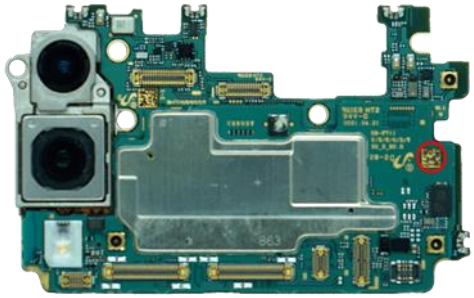
Galaxy Z Fold

Galaxy Z Flip5

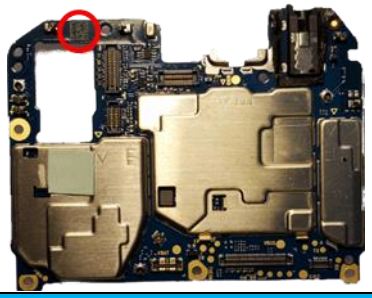
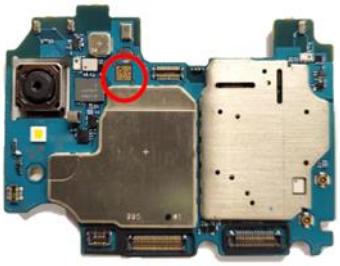
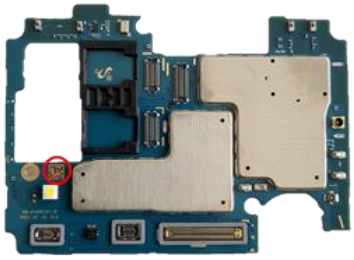
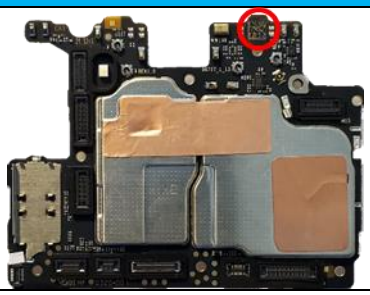
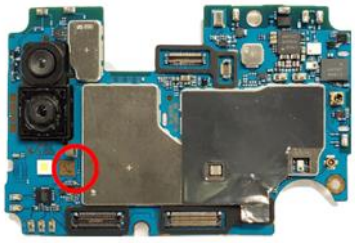


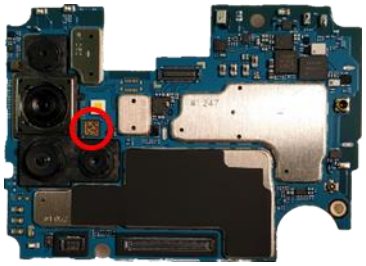
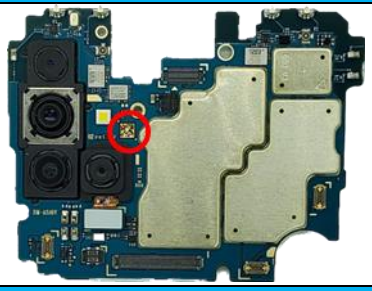
Galaxy Z Flip4



Galaxy Z Flip3 5G	Galaxy Z Flip
	

Galaxy A Series

Galaxy A01	Galaxy A10e
	
Galaxy A11	**Galaxy A12**
	
Galaxy A21	**Galaxy A20**
	

Galaxy A50	Galaxy A51
	
Galaxy A51 5G	**Galaxy A70**
	
Galaxy A70	
	

Additional Devices

Galaxy Watch


Revision History

The following table lists the revisions made to this OJT.

Version	Released	Revision
1.0	2/28/2020	• Initial OJT created
1.1	10/14/2020	• New models added
1.2	12/3/2020	• New models added
1.3	1/25/2021	• New models added
2.0	8/18/2021	• Updated document tables/design, added new models, added hyperlinks
3	2/10/2022	• New models added
4	8/17/2022	• New models added
5	02/14/2023	• New models added
6	07/31/2023	• New models added

QRG: mmWave Calibration – No Power Supply

Introduction

This document is intended to guide repair technicians in performing mmWave Calibration without an ODA2CH power supply.

About mmWave Calibration

mmWave Calibration is performed using Daseul, and must be completed when the following kinds of repair are done on 5G mmWave capable devices:

- IMEI Rewrite (Main PBA Replacement)
- 5G mmWave Antenna Module Replacement

Following successful calibration, Galaxy Diagnostics will test the integrity of each mmWave Module; if any instances fail, the module with the failing instance must be replaced, and mmWave Calibration repeated.

Note: mmWave Calibration is NOT OPTIONAL, and must be completed with these repair types on 5G mmWave capable devices.

Hardware Configuration

The following equipment is required to complete mmWave Calibration without an ODA2CH power supply:

Category	Item	SVC Jig Code	QTY
Shield Box	AS 3.1, 5G (mmWave) AUTO CAL Shield Box	GH81-17197A	1
Anyway Jig and Cable	• Anyway Jig	GH81-12520B	1
	• Anyway Jig Adaptor	GH81-14495A	1
	• 25pin Serial Cable	GH81-17200A	1
	• USB to Serial Cable	GH81-13470Z	1
I/F Cable	Type-C	GH81-17202A	1
Common Model Jig	• Comm.Radiation JIG_Main Base	GH81-19033A	1
	• Comm.Radiation JIG_Mounting(Variable)	GH81-19033B	3
	• Comm.Radiation JIG_Mounting(Fixed)	GH81-19033C	2
	• Comm.Radiation JIG_LM Unit	GH81-19033D	1
	• PACK HOLDER)Slim Molding Pack Assy)	GH81-17204A	1

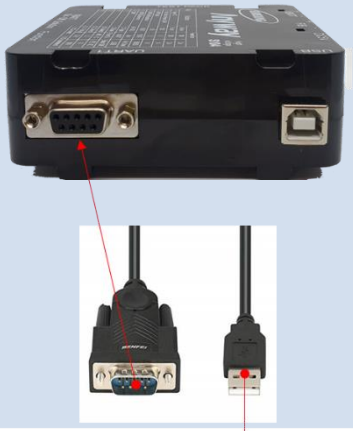
Follow the instructions in the step table below to complete mmWave Calibration when an ODA2CH power supply is not available:

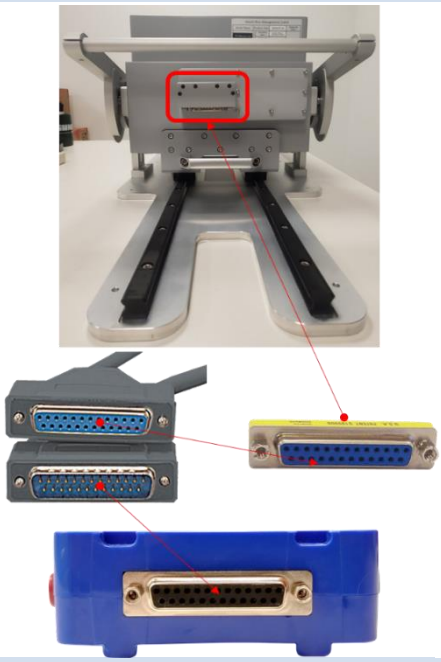
Note: mmWave RF Calibration can be performed without the use of a Power Supply; however, device battery should be charged over 50% before executing the calibration. If the state of charge is less than 50%, the calibration will not start.

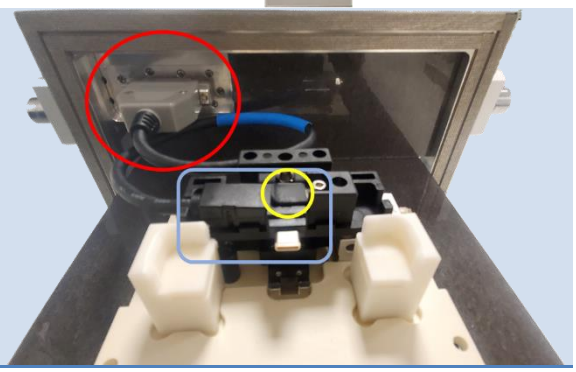
Revised March 16, 2021

SAMSUNG Care

Step	Action
1.	Connect the Anyway Jig to the Service PC: • Connect the serial side of the USB to Serial Cable to the serial UART port on the Anyway Jig • Connect the USB side of the USB to Serial Cable to an open USB port on the Service PC **Note:** Connecting the Anyway Jig to the Service PC will generate a COM Port for the Anyway Jig, which can be found in the Windows Device Manager
2.	Connect the Anyway Jig to the Shield Box: • Connect one end of the 25 pin Serial Cable to the Test Pack port on the Anyway Jig • Connect the other end of the 25 pin Serial Cable to the Anyway Jig Adapter • Connect the 25 pin Serial Cable with the attached adapter to the port on the Shield Box door
3.	Configure the Common Model Jig for the device model being calibrated: • Remove the screws from the holder(s) to be moved • Move the holder(s) to the coordinates labeled for the device model to be tested ¬ Make sure that the screws are facing away from where the device will be positioned ¬ The upper variable holder should be secured so that the device does not move after securing the lower side variable holder • (x, y) are the coordinates on the pegboard where the screws should be fastened ¬ There will be at least two points listed for each variable holder ¬ The points will be listed in sets of two in the format (x, y)/(x,y)





4.	Insert the Common Model Jig into the Shield Box: • Pull open the Shield Box chamber and place the Common Model Jig in the center • Align the notches on the Common Model Jig to the pegs on the Shield Box to secure the Common Model Jig in place **Note:** Do not pull the chamber drawer all the way out; this will derail the chamber from its sliding tracks	
5.	Connect the Common Model Jig to the Shield Box using the I/F Cable: • Connect and secure the I/F cable to the Shield Box port located behind the chamber of the shield box • Slide the I/F plug into the Common Model Jig; be careful not to lift and damage the clip	

Downloading, Configuring Daseul & Calibration

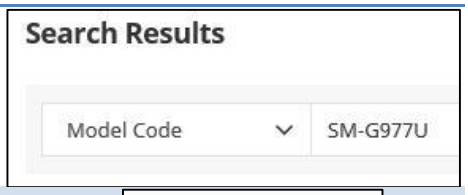
There are three (3) files required to complete mmWave Calibration:

- Daseul Launcher (.exe)
- Calibration Runtime (.cab)
- Model File (SM-GXX.cab)

Follow the instructions in the step table below to download the required files from SKP and configure Daseul:

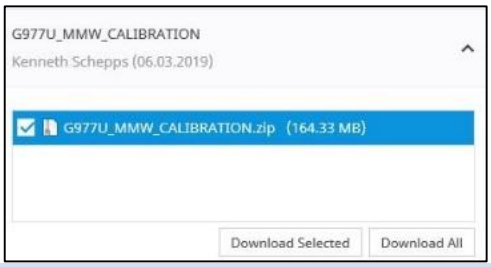
Step	Action
1.	Log in to G-SPN, and click on **Knowledge** from the top menu bar

2. Type the device model number in the **Model Code** search field, and click on **Search**



3. Scroll the scroll bar left until you reach the **Compliance Software** column, and click on the hyperlinked number in the Compliance Software column

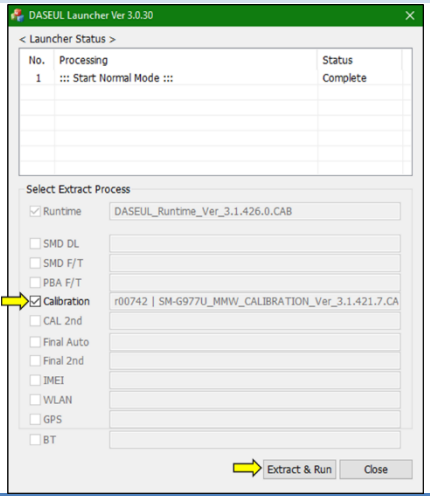
4. Select the file to download and click **Download Selected** to download the .zip file to the Service PC



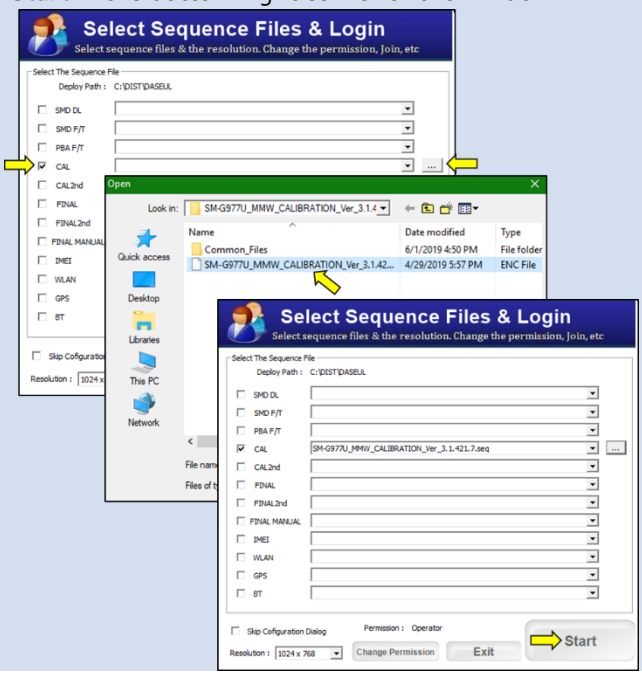
5. Extract the .zip file contents into a folder that will contain all three files

6. Navigate to and open the folder containing the extracted files, then launch the Daseul Launcher

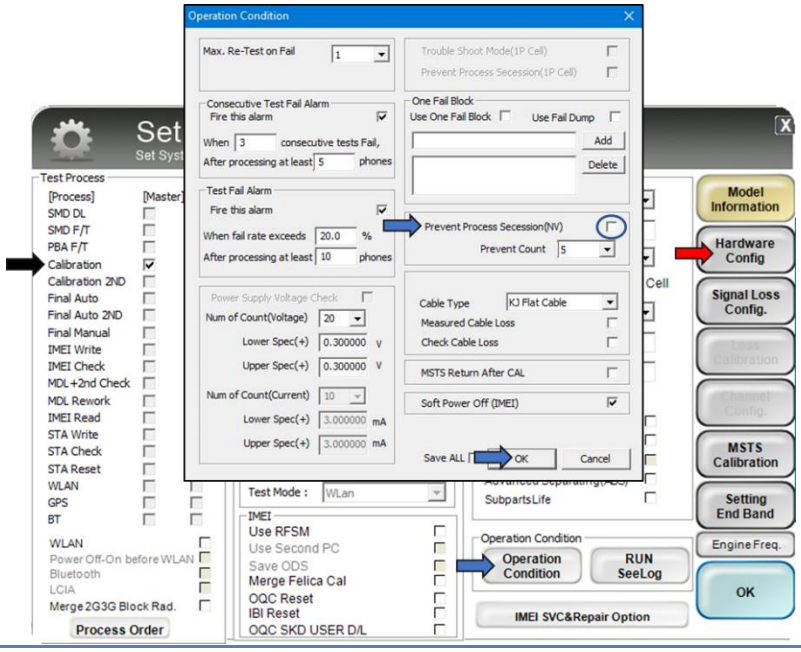
   - With all of the files in the folder, Daseul Launcher should automatically load the same MMW_Calibration file
   - Check the box next to **Calibration**
   - Click **Extract & Run**



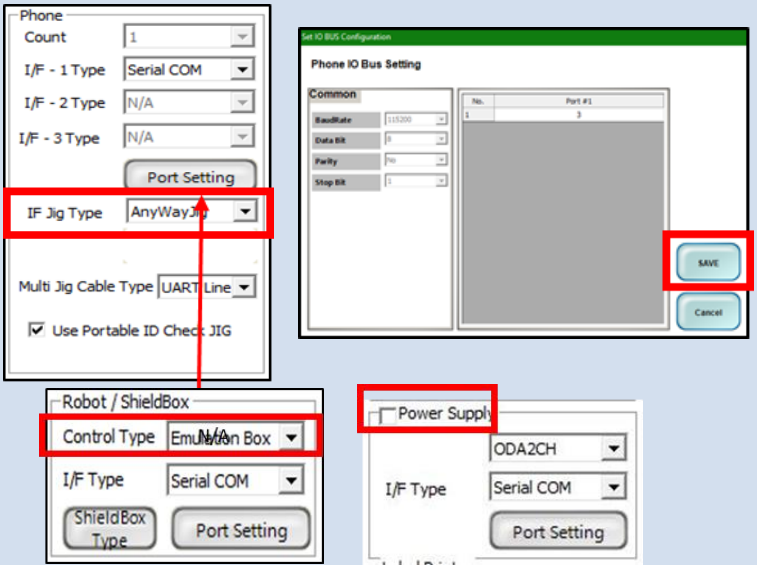
7. Once the extraction process is completed, the **Select Sequence Files & Login** window will appear:
   - Click and check off **CAL**
   - Click the **…** button next to the CAL dropdown
   - Navigate to and select the Model File, then click **Open**
   - Click **Start** in the bottom right corner of the window



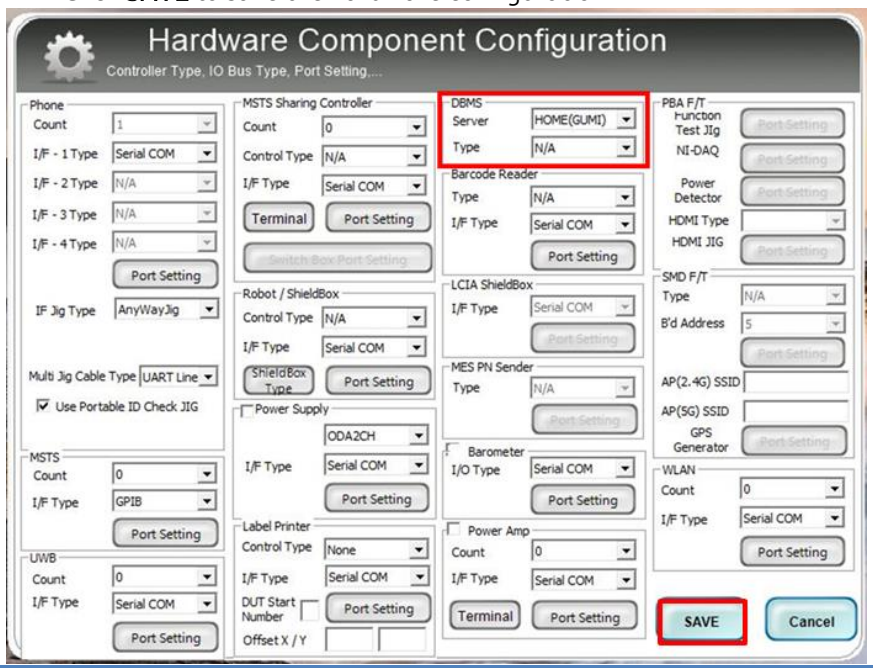
8. The **Set System Configuration** dialog window will open:
   - In the **Test Process** section, select **Calibration**
   - Select **Operation Condition** and ensure **Prevent Process Secession (NV)** is **unchecked**; click **OK**
   - Click **Hardware Config** to continue



9. Configure the Shield Box:
   - Make sure that the Anyway Jig is connected as outlined in the above section, *Hardware Configuration*
   - In the Phone section, select **AnyWay Jig** as the IF Jig Type
   - Click on **Port Setting** to configure the COM Port number (found in the Windows Device Manager), then click **Save**
   - In the **Robot/Shieldbox** section, set the **Control Type** to **N/A** and the **I/F Type** to **Serial COM**
   - In the **Power Supply** section, make sure that the **Power Supply** box is unchecked

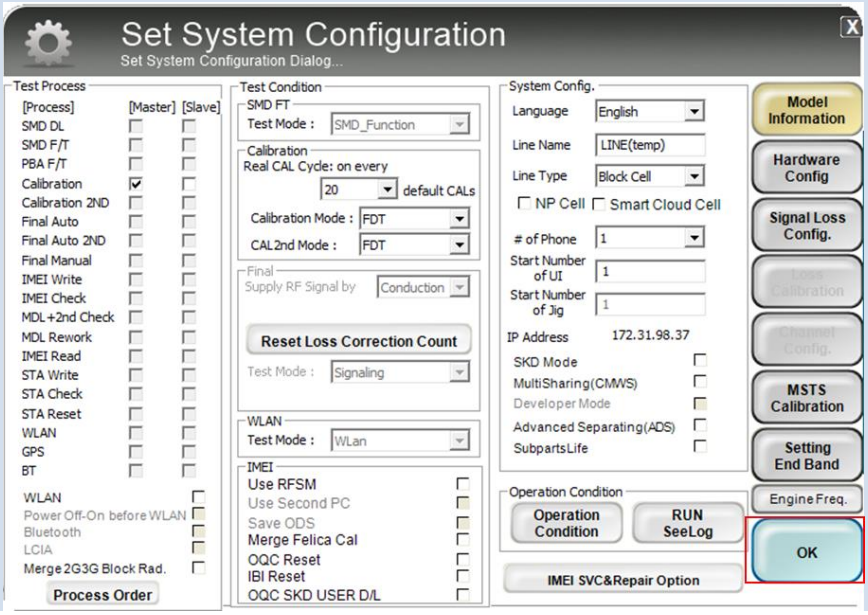


10. Congifure DBMS and Save:
   - In the **Server** section, select **Home(GUMI)**
   - In the **Type** section, select **N/A**
   - Click **SAVE** to save the hardware configuration



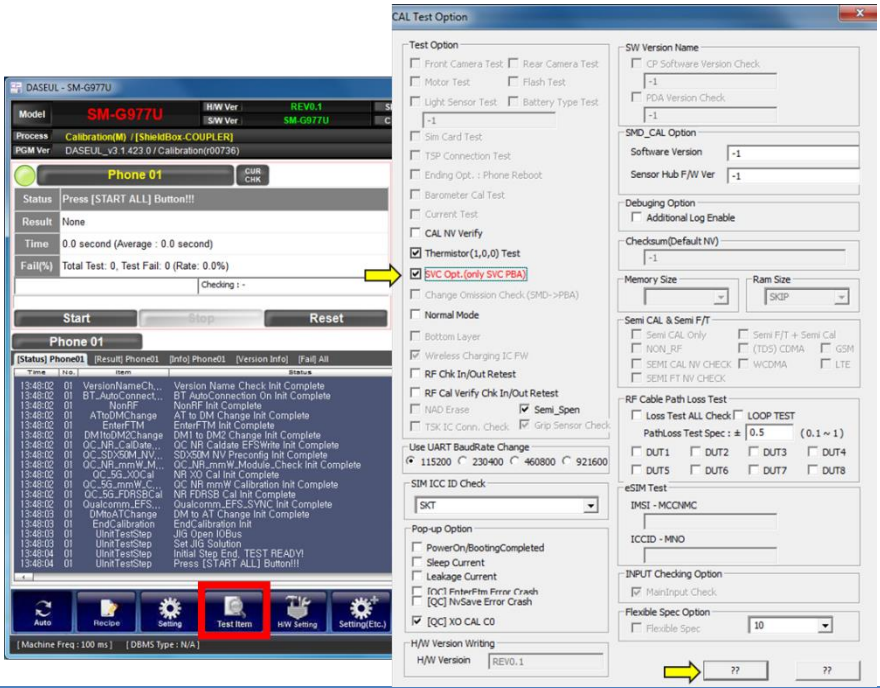
11. Once hardware has been configured, you will return to the Set System Configuration window:

- To save your settings and proceed to Daesul, click **OK**
- You may encounter a MSTS pop-up notification upon clicking OK; disregard this notification and proceed to launching Daseul



12. Configure Daseul:

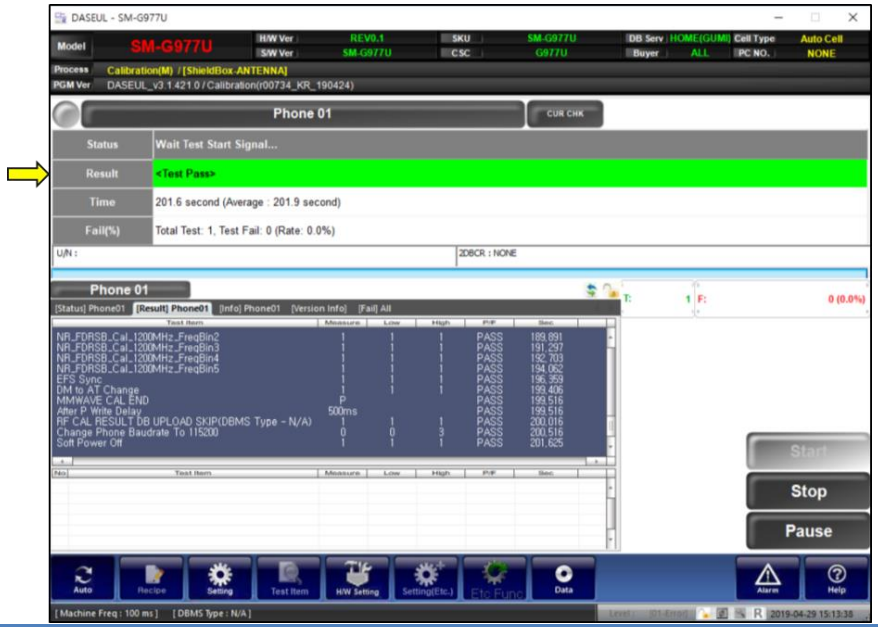
- Click on the **Test Item** option within Daseul, and then select the **SVC Opt. (only SVC PBA)** option in red font
- Save and close your settings by selecting the left **??** option below the **CAL Test Option** settings window



13. Select **Start** :
    - Place the powered off device in the Common Model Jig and connect it to the IF Port
    - Hold the Power Key to turn the device on
    - Close the chamber while the device is booting up, making sure that the Shield Box is closed and locked by pulling **down** on the handle

    Note: If the calibration fails, do not stop the tool; allow Daseul to retest, then power the device off, reconnect it to the IF Port, hold the Power Key to turn the device on and close the chamber again while the device is booting up

14. When calibration completes successfully, Daseul will display **<Test Pass>** in the **Result** section

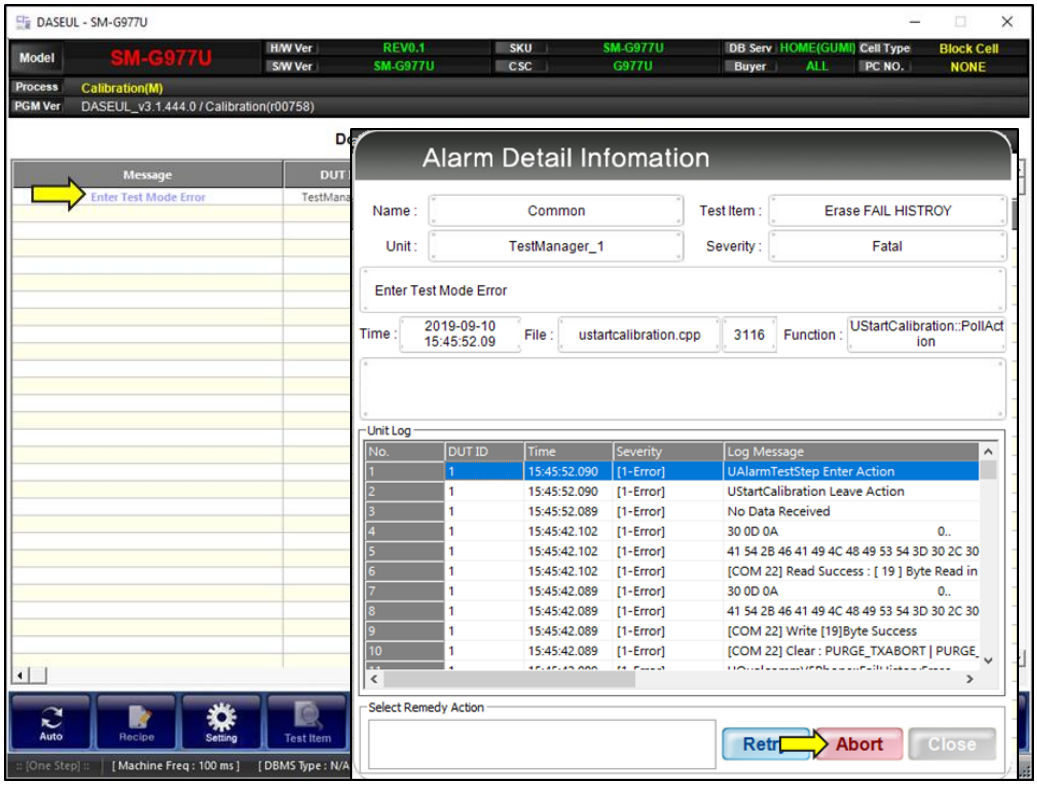


Troubleshooting

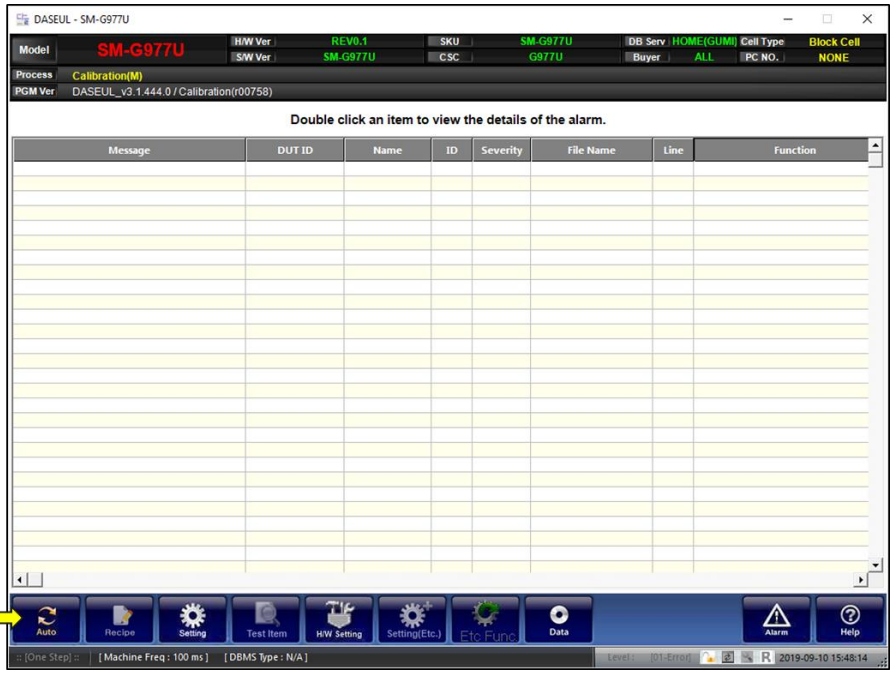
If the tool fails, Daseul will display **Alarm !!!** in the **Result** field; a pop up window will provide details of the failure:

Error	Troubleshooting Steps
Tool failing for "Booting Completed Msg Error"	1. Check Anyway Jig COM Port Mapping/Settings
Tool failing for "StartCalibration Fail to Read Test Items All"	1. Ensure the device does not have Screen Lock turned on
Tool failing for "Erase Fail History"	1. Click Abort on the Alarm Screen and let the tool reset

It is important to make sure that the Fail History is erased manually when a failure occurs; double click on the failure line to view the Alarm Detail, and click the Abort button to clear the failure history. **DO NOT** click Retry, as this will only cause the tool to fail again.



Once the failure history has been cleared, click the **Auto** option and allow Daseul to retest the device:



OJT: Scanning QR Codes on Display Modules

Introduction

This document is intended to guide agents on where to find and scan QR codes on display modules (OCTA). Knowing where to locate and scan the QR codes will enable more accurate parts management during repairs.

Topic

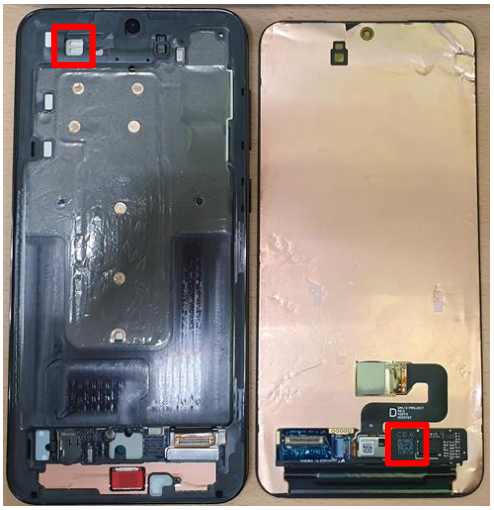
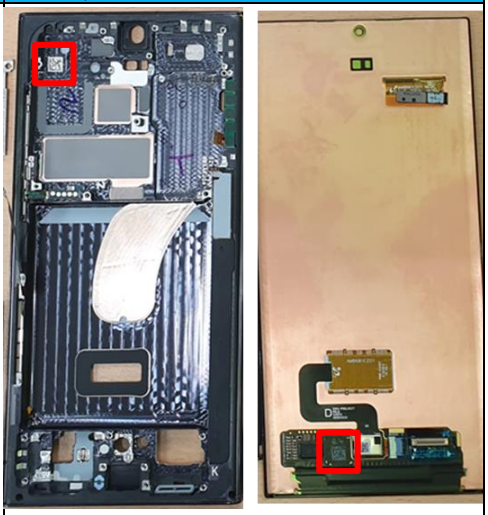
The OCTAs for Samsung devices feature an embedded QR code that enables the part to be scanned during repairs. Utilizing the QR code allows the identifying, unique information for each OCTA to be tracked and managed effectively. Scanning the QR code helps to reduce the impact of human error when managing parts and increases the speed at which parts can be tracked and shipped via U-Class.

The following device series are listed:

- Galaxy S Series
- Galaxy Note Series
- Galaxy Z Series
- Galaxy A Series
- Galaxy Tablets
- Additional Devices

Revised August 15, 2023

Galaxy S Series

Galaxy S23 & Galaxy S23+	Galaxy S23 Ultra
	
Galaxy S22 & Galaxy S22+	**Galaxy S22 Ultra**
	

Revised August 15, 2023

Galaxy S21 5G	Galaxy S21+ 5G
	

Galaxy S21 Ultra 5G	Galaxy S20 5G
	

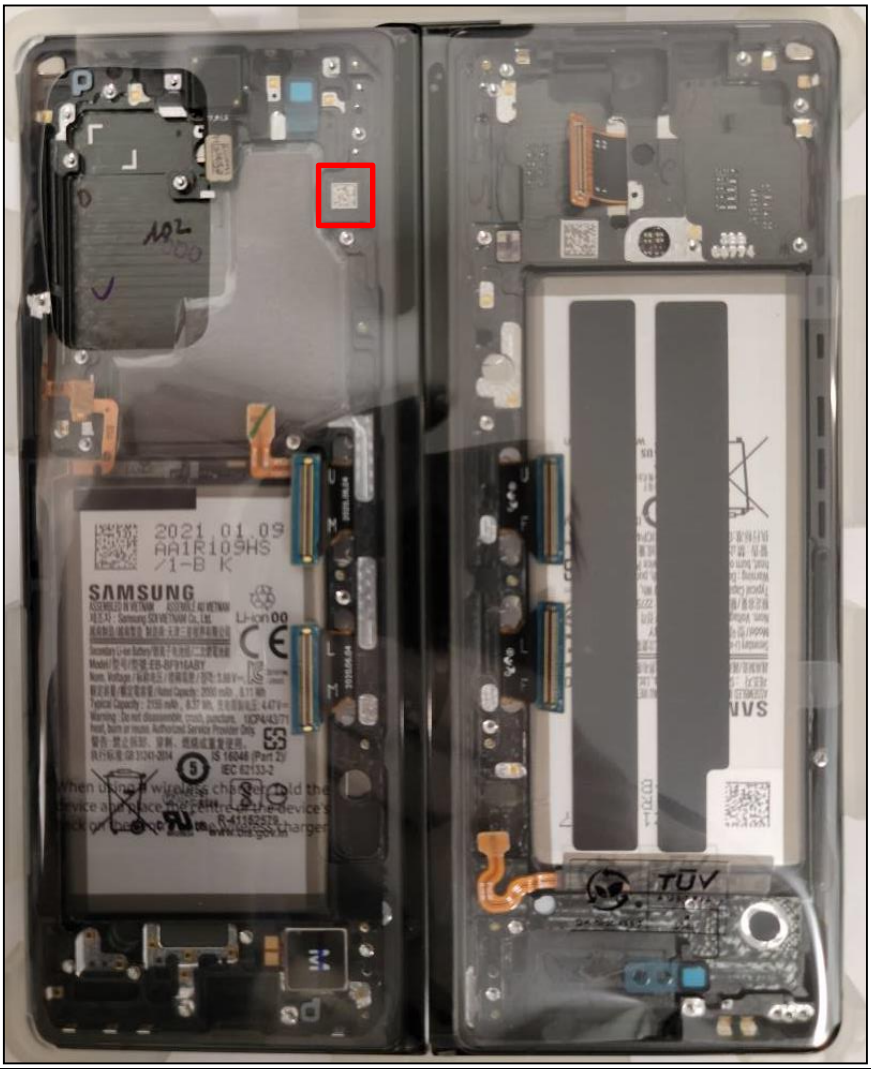
Galaxy S20+ 5G	Galaxy S20 Ultra 5G
	

Galaxy Note Series

Galaxy Note20 5G	Galaxy Note20 Ultra 5G
	

Galaxy Z Series

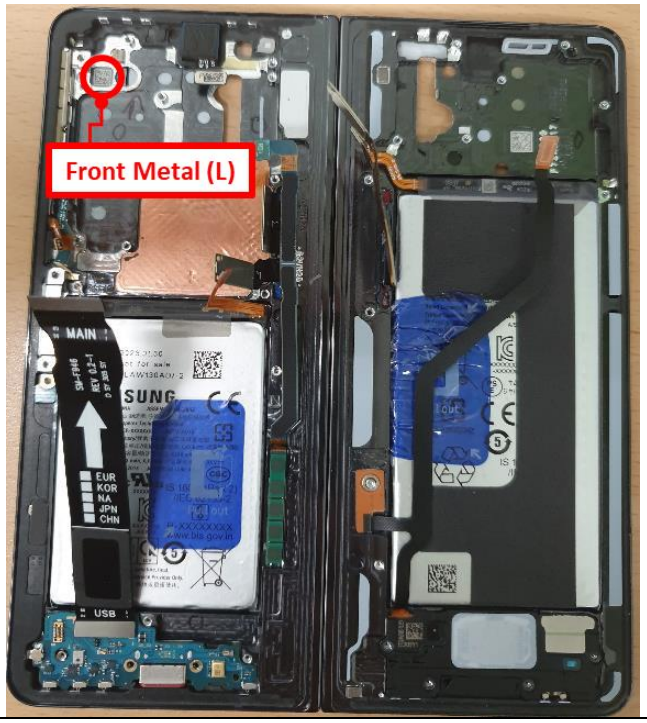
Galaxy Z Fold2 5G



Galaxy Z Fold3 5G

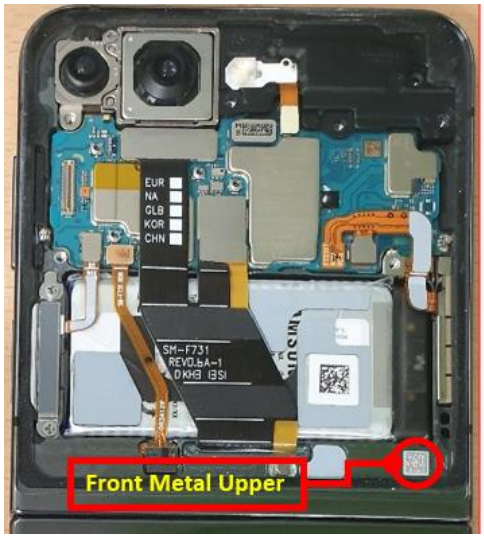
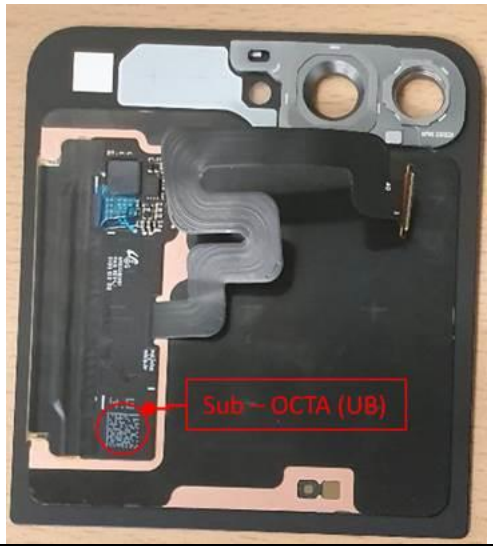
Galaxy Z Fold4

Galaxy Z Fold5



Galaxy Z Flip 5G	Galaxy Z Flip
	

Galaxy Z Flip3 5G	Galaxy Z Flip4
	

Galaxy Z Flip5	
	

Galaxy A Series

Galaxy A01	Galaxy A02
	

Galaxy A02s	Galaxy A10s
	

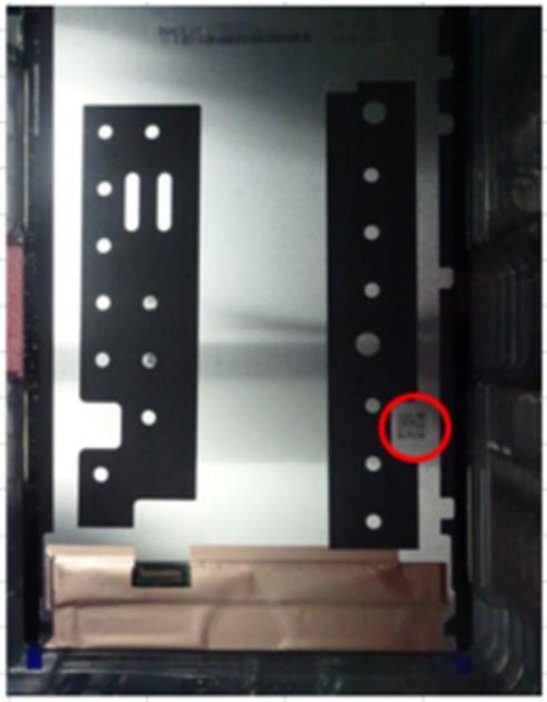
Galaxy A11	Galaxy A20s
	

Galaxy A21	Galaxy A22
	

Galaxy A71	Galaxy A03s
	

Galaxy A03s (International)	Galaxy A03 Core
	

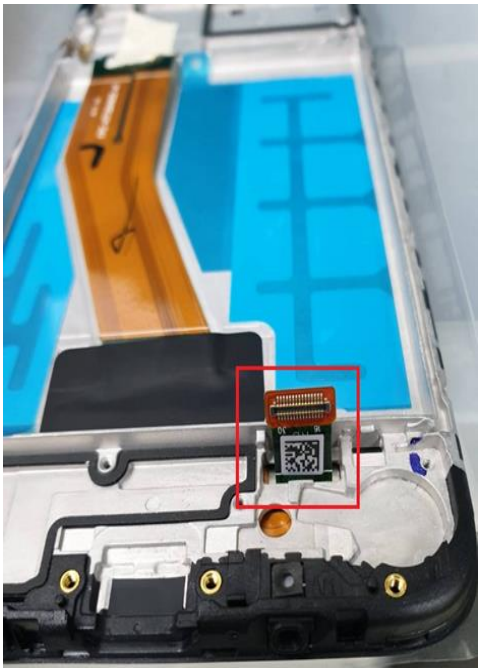
Galaxy Tablets

Galaxy Tab A7	Galaxy Tab A7 Lite
	

Galaxy Tab A8	
	

Additional Devices

Galaxy M01	Galaxy M02
	

Galaxy M11	Galaxy F52
	

QRG: Using Fenrir

Introduction

This document is intended to act as a quick reference guide to technicians when using Fenrir.

About Fenrir

Fenrir is a Samsung repair system used for these parts of the repair process:

- Warranty Validation
- Software Flash (Android OS installation)

This document will outline the following topics related to Fenrir:

Note: It is important to make sure that no other repair tools (e.g. GD) are in use when using Fenrir.

PC Hardware Specifications

These are the required system specifications for use with Fenrir:

- PC running Windows 7/8/10 operating system
- At least 3TB available storage for device binaries
  - More storage allows for more binary storage
  - It is recommended to set up the hard disk drive (HDD) as a single partition
- At least 5Mbps high-speed Internet connection (>7Mbps recommended)
- Firewall open to the following FUS server URLs:
  - Required for binary download and device connection history upload to FUS servers
  - http://cloud-neofussvr.sslcs.cdngc.net
  - http://neofussvr.sslcs.cdngc.net
- Data Cable connected directly to the USB Port on the Mainboard of the Service PC (back ports)
- USB hub with external power source (e.g. Belkin F4U041 or similar) for multiple devices connected directly to the USB Port on the Mainboard of the Service PC (back ports)

Note: The following page includes samples of tables and informational blocks (warnings, cautions, tips and notes) in case you need to use them.

Revised December 2, 2021

Binary Management

In order to use Fenrir with a device, the most up to date binary for that device must be loaded into Fenrir.

There are two (2) types of binary used in Fenrir:

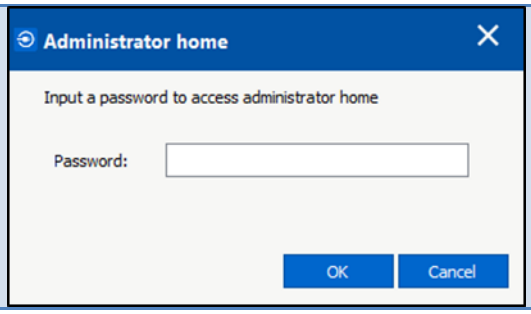
- H (Home) – Attempts to save customer user data
  - **Cannot** be used for IMEI Write/Check processes
  - **Cannot** be used on Tizen devices
- F (Factory) – Erases all customer user data, and sets the device to factory defaults
  - **Required** for use with IMEI Write/Check processes
  - Main screen can be used to flash Tizen watches as well as for the Phone Recovery software option

Fenrir A (All) is an option which combines both the Home and Factory binaries into a single program; this option requires twice the storage and network traffic as the individual components, and allows more room for human error because it is possible for the wrong binary to be applied to the device accidentally, which may cause customer user data to be permanently lost. Tizen watches will not work on the Fenrir A Home screen, but can still be flashed using the Phone software recovery option.

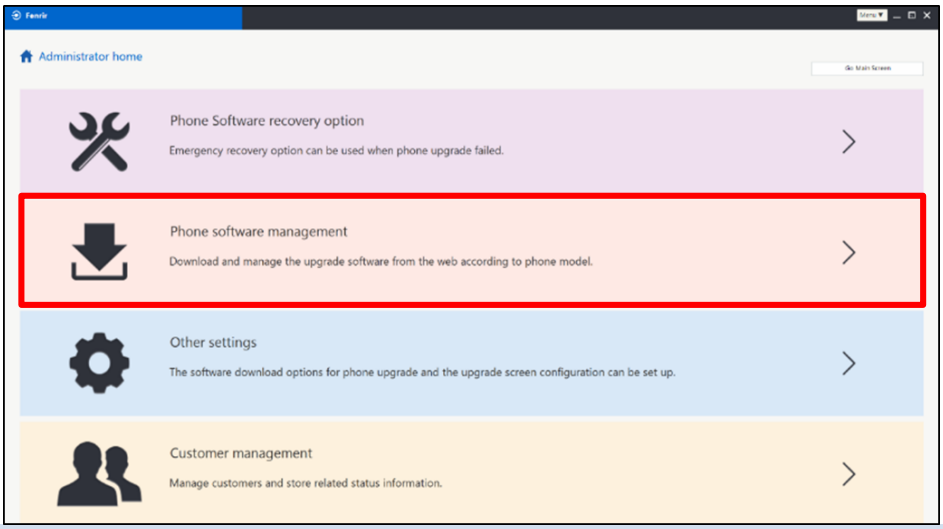
It is important to make sure that the correct binary is used for the wanted outcome.

Use the instructions in the step table below to manage Fenrir binaries:

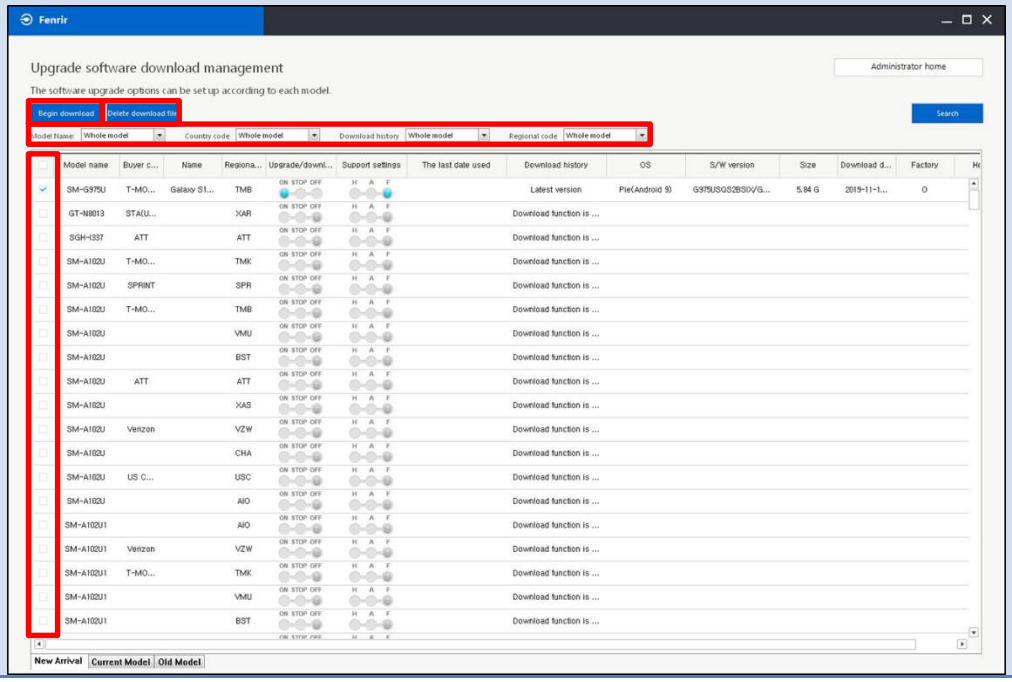
Note: Using out of date binaries with Fenrir may cause device repair systems (e.g. IMEI Cloud Client) or the device software to malfunction, and may render the device inoperable; **DO NOT** attempt to recover a rooted device with Fenrir.

Step	Action	
1.	Launch Fenrir, and access Administrator Home by pressing Alt + F10; enter **smart100** as the password, then click **OK**	

2. Select **Phone software management** to download and manage binaries by phone model



3. The Upgrade software download manager will display:
   - Select the check box next to the device model binaries to update
   - Use the drop down menus to narrow the options down to a specific device model, country code, or regional code
   - Click **Begin download** to download the selected binar(ies)
   - Click **Delete download file** to delete the stored binar(ies)



4. Once the selected binar(ies) have been downloaded, set Fenrir to automatically download updated binar(ies):

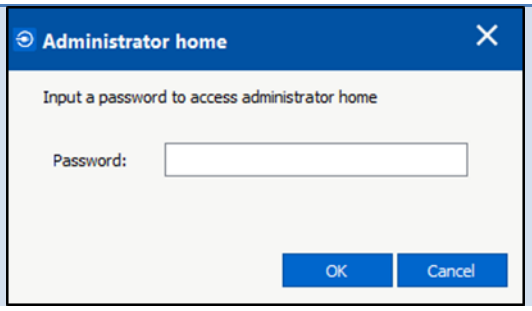
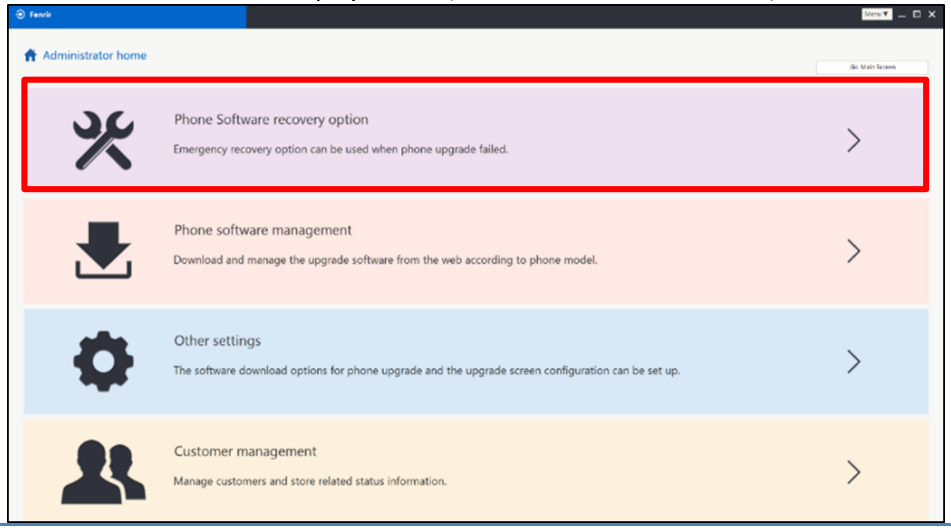
	Web download	S/W Update	Comments
Stop (Orange) 	Ongoing	Not Possible	Set by default (Temporary)
OFF 	Not Possible	Not Possible	
ON 	Possible	Possible	

NOTE: Stop (Orange) will automatically switch to **ON** upon completion of binary download

Using Fenrir: Software Recovery

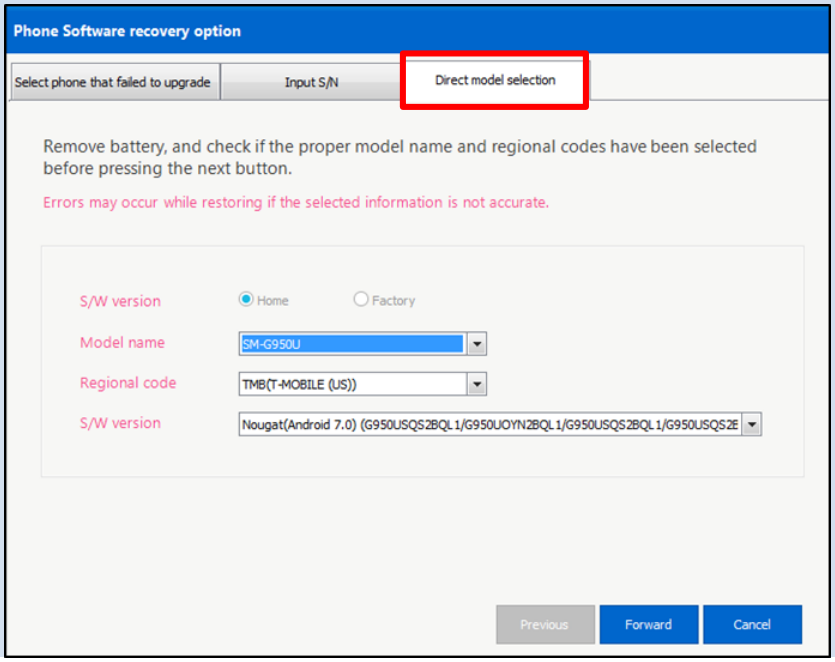
Use the instructions in the step table below to complete a Phone Software recovery on a device:

Note: Do not perform software recovery or update on a rooted device.

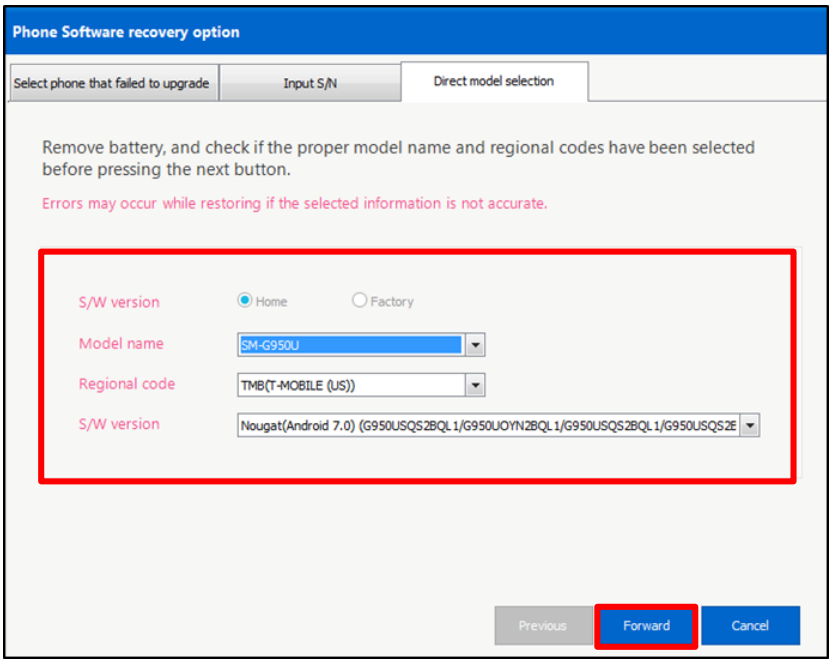
Step	Action	
1.	Launch Fenrir, and access Administrator Home by pressing Alt + F10; enter **smart100** as the password, then click **OK**	
2.	Select **Phone Software recovery option** to perform a software recovery:	

Revised December 2, 2021

3. When the Phone Software recovery option window appears, select the Direct model selection tab:

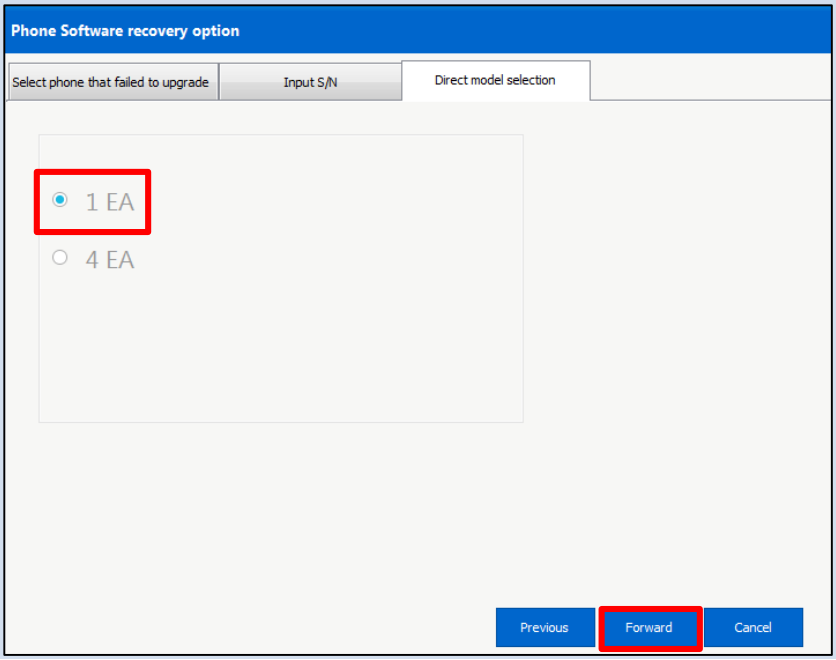


4. Select the following options to install the Home binary to the device, then click **Forward** to continue:

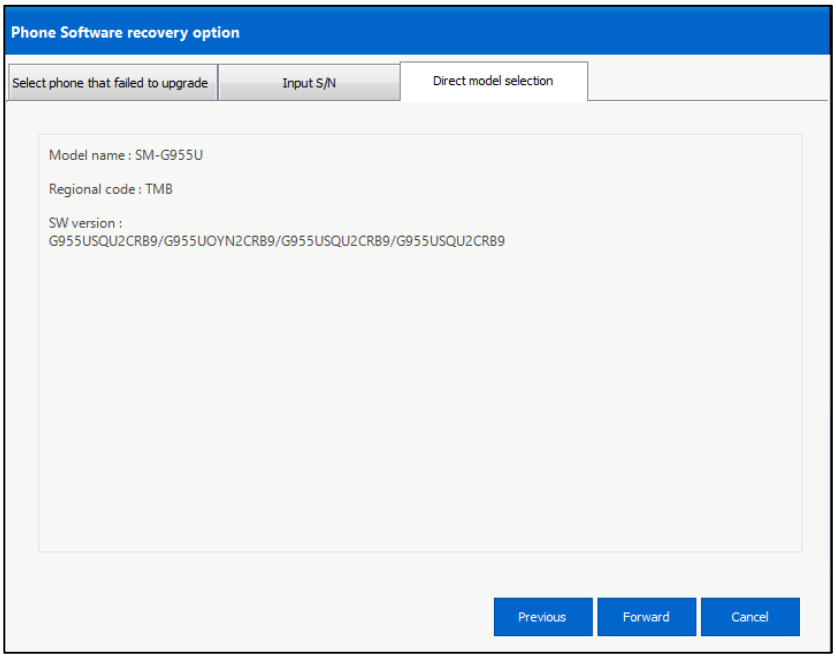


- S/W Version: Home
- Model name: Select the device model from the drop down menu
  - If the device is not listed, the binary is not installed
- Regional code: The original carrier of the device
- S/W version: The current, up to date binary in Fenrir

5. Select **1 EA** to recover one device at a time (recommended), then click **Forward** to continue:

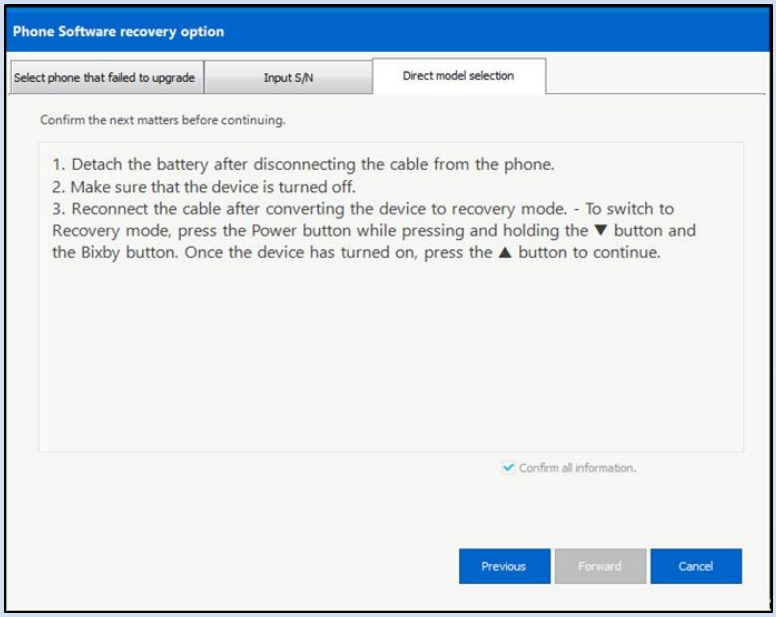


6. Review the selections made before proceeding:



- Press **Previous** to go back and make changes
- Press **Forward** to continue if no changes are needed

7. Place the device in Download Mode using the instructions shown, and confirm the items listed:



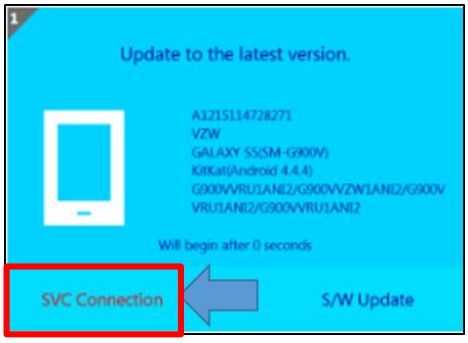
- Make sure the device is charged to **at least 30%**
- Check the **Confirm all information** box
- Click **Forward** to attempt device recovery
- Leave the device connected until the process has completed, and Fenrir has confirmed that the results have been updated to the FUS server

Using Fenrir: SVC Connection

When completing a repair, the device needs to be connected to Fenrir to perform a Warranty Validation, also known as SVC Connection. SVC Connection is required for every repair, whether it is in warranty or out of warranty.

Fenrir needs to log every component used during a repair to FUS. If FUS does not see the components used in the GSPN Service Order for the device, GSPN logic will assume parts were never used. This will stop the GSPN Service Order from being marked Goods Delivered. If this happens, no Warranty Claim will be generated, and the location will not be paid for the repair.

To perform Warranty Validation after a repair, connect the device to PC via USB cable and wait for Fenrir to recognize the device. Once device has been recognized, select SVC Connection and wait for SVC Connection to log the IMEI to the FUS server.



Performance Tips & Tricks

To ensure optimal performance when using Fenrir:

- Make sure that the Service PC meets all minimum system requirements outlined above
- Make sure to use a Samsung charging/data cable to ensure a proper connection between the device and the Service PC
- Make sure that all needed binaries are updated daily to prevent device detection or connection errors
  - Fenrir will not recognize a device if the binary for it has not been downloaded
- Do not use a USB hub to connect the device to the Service PC; this may have negative impacts on data transfer speeds
- Make sure to use the **rear** USB ports on the Service PC for a direct connection to the system BUS
- Make sure to use either the BLUE (USB 3.0) ports on the Service PC, or a USB Type-C port
- Make sure that the cables being used to connect the device to the Service PC are in good condition and working properly
- Make sure to leave the Service PC powered on and logged in so that automatic software downloads can take place as scheduled (The screen may be locked)
- Make sure that the Service PC has a stable connection to the Internet

Revised December 2, 2021

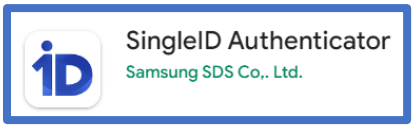
SAMSUNG Care

NEW MFA APP SETUP FOR GSPN LOGIN

Beginning on Tuesday October 22, 2024, GSPN is expected to switch their MFA App over to the **SingleID Authenticator App**. This short guide is meant to be a very brief overview of how to switch the app once the change goes live in GSPN. The steps in this guide assume you already have an MFA device setup for **both GSPN logins** *(Slvl for main account and M0x for MOTP account).* **This process should be completed on both of your GSPN accounts!**

******If you are using an iOS/Apple device, you must first setup a 6-digit passcode BEFORE attempting to register it as an MFA device******

1. Download the **SingleID Authenticator App** from **App Store (iOS)/Play Store (Android)**.



2. Log into GSPN as you normally would to begin setup using the on-screen instructions.
    a. **WARNING: DO NOT SUBMIT AN MFA DELETION REQUEST!!!**
    b. If the **User Consent** page prompts, check **"Accept all"** to continue
3. At the **verification option** page, select **"SingleID Authenticator – PIN"**
4. Click the **"Get started"** button on the **Enroll SingleID Authenticator** page
5. You should now be prompted to install the **SingleID Authenticator** app
    a. For **Android** devices search the app on the **Google Play** store (or use the on screen QR)
    b. For **iOS** devices search the app on the **App Store** (or use the on screen QR)
6. Open the app once it's downloaded to your device and configure it as instructed below
    a. In the **App Permissions** pop-up, click the **"OK"** button
        i. Enabling Push notifications is ideal for authenticating
    b. Press the **"Start"** button at the bottom to be sent to the **Home** page
7. Back on the PC prompt, click the **"Next"** button on the **Install mobile app** page
8. You should be at the **Service registration** page with 2 options to register (QR or Manual)
    a. Scanning the QR will send you right to the next step (Step 9 see below)
    b. To activate the Manual Code, use the app to enter the PIN code
9. In the pop-up that says, **"Would you like to register the following service?"** click **"Registration"**
    a. It should say **GSPN/secdx** or something similar in the message box as well
10. You will then be asked to create a 6-digit PIN. Create a PIN and take note of it somewhere.
11. A pop up will appear saying **"Please register your biometrics/Face ID",** be sure to click **"Cancel"**
    a. This will bypass the biometric requirements
12. GSPN should take you to the **Enrollment completed** screen; at this point you should be able to log into GSPN using the PIN method!

If you are having any issues with the MFA setup, DO NOT SUBMIT AN MFA DELETION REQUEST!!!
Instead, please submit a JIRA Ticket using this form to troubleshoot first:
https://ubreakifix.atlassian.net/servicedesk/customer/portal/6/group/69/create/330

Please include screenshots of the errors you encounter to speed up the process!

FAQ

Forgot your Password? -

When requesting a password reset, make sure you are entering your STG ID and not your UBIF/Asurion email. Password reset can only be initiated by entering your STG ID. If you do not know your STG ID, please reach out to your Franchise Consultant or Corporate District Manager.

I submitted "Forgot your Password?" with my STG ID but still not receiving an email -

Your account may have been deactivated. Submit a Sprinklr ticket for System Credential Support > STG Support and explain the situation. If your account was deactivated, it will take 1-3 days to resolve.