

BackupBoxA V100R023C10

Security Maintenance Manual

Issue 01
Date 2023-09-20



Copyright © Huawei Digital Power Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Digital Power Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Digital Power Technologies Co., Ltd. and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied. The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Digital Power Technologies Co., Ltd.

Address: Huawei Digital Power Antuoshan Headquarters
Futian, Shenzhen 518043
People's Republic of China

Website: <https://e.huawei.com>

Contents

1 Change History.....	1
2 Security Maintenance Overview.....	2
3 Device Layer Security.....	3
3.1 Mobile App Maintenance Suggestions.....	3
3.1.1 Maintenance Suggestions.....	3
3.1.2 Procedure.....	3
3.1.3 Exception Handling.....	5
3.2 Serial Port Maintenance Suggestions.....	5
3.3 Upgrade and Maintenance Suggestions.....	5
3.3.1 Maintenance Suggestions.....	5
3.3.2 Procedure.....	5
3.4 Log Maintenance Suggestions.....	10
3.4.1 Maintenance Suggestions.....	10
3.4.2 Procedure.....	10
4 Software Integrity Protection.....	15
4.1 Manually Verifying the Digital Signature of Software Packages.....	15
4.2 Software Integrity Protection.....	19

1 Change History

Version	Date	Description
01	2023-08-30	This issue is the first official release.

2 Security Maintenance Overview

Photovoltaic (PV) operators need to establish a security maintenance mechanism to ensure that their application systems operate properly in a secure environment.

Application systems are now exposed to increasingly severe security threats, which may result in power outages, revenue loss, or system breakdown. Therefore, PV operators need to build and maintain security mechanisms for application systems at several layers to detect and handle any possible security issues.

These threats cannot be all prevented by technology. To address these issues, PV operators need to establish a security management system based on security maintenance suggestions and security issues found in routine maintenance, thereby ensuring that application systems operate securely and properly.

3 Device Layer Security

[3.1 Mobile App Maintenance Suggestions](#)

[3.2 Serial Port Maintenance Suggestions](#)

[3.3 Upgrade and Maintenance Suggestions](#)

[3.4 Log Maintenance Suggestions](#)

3.1 Mobile App Maintenance Suggestions

The BackupBox does not have a WiFi module. Therefore, you need to connect the mobile app to the EMMA of the BackupBox to perform security maintenance.

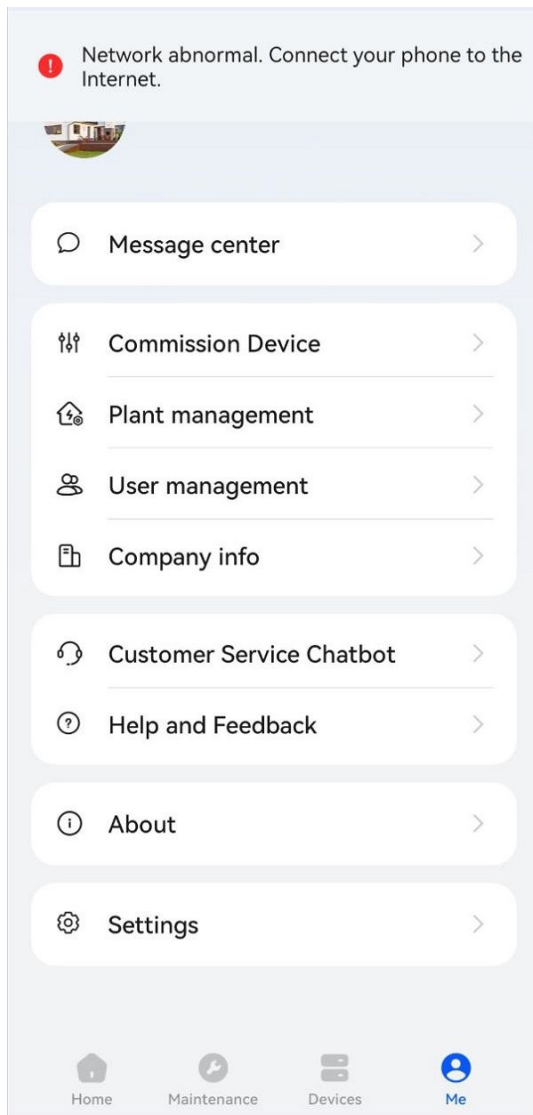
3.1.1 Maintenance Suggestions

- After a BackupBox is deployed for the first time or you log in to the mobile app for the first time, set the passwords for the users (**user** and **installer**).
- Avoid using weak passwords, which are prone to attacks and cracking by unauthorized users. To ensure system security, the password length and complexity must meet the security requirements. A password must meet the following requirements:
 - The password must contain at least eight characters.
 - The password can consist of digits, uppercase letters, and lowercase letters.
- Leaving a password unchanged for a long time increases the risk of password compromise. Change the password at least once every six months.
- To ensure security, you are advised to disable the data connection when using the mobile app.
- You are advised to use a mobile phone that has not been rooted to reduce the risk of information leakage.
- The mobile phone logs are saved in the app directory. Export and back up the mobile phone logs when you need to use them.

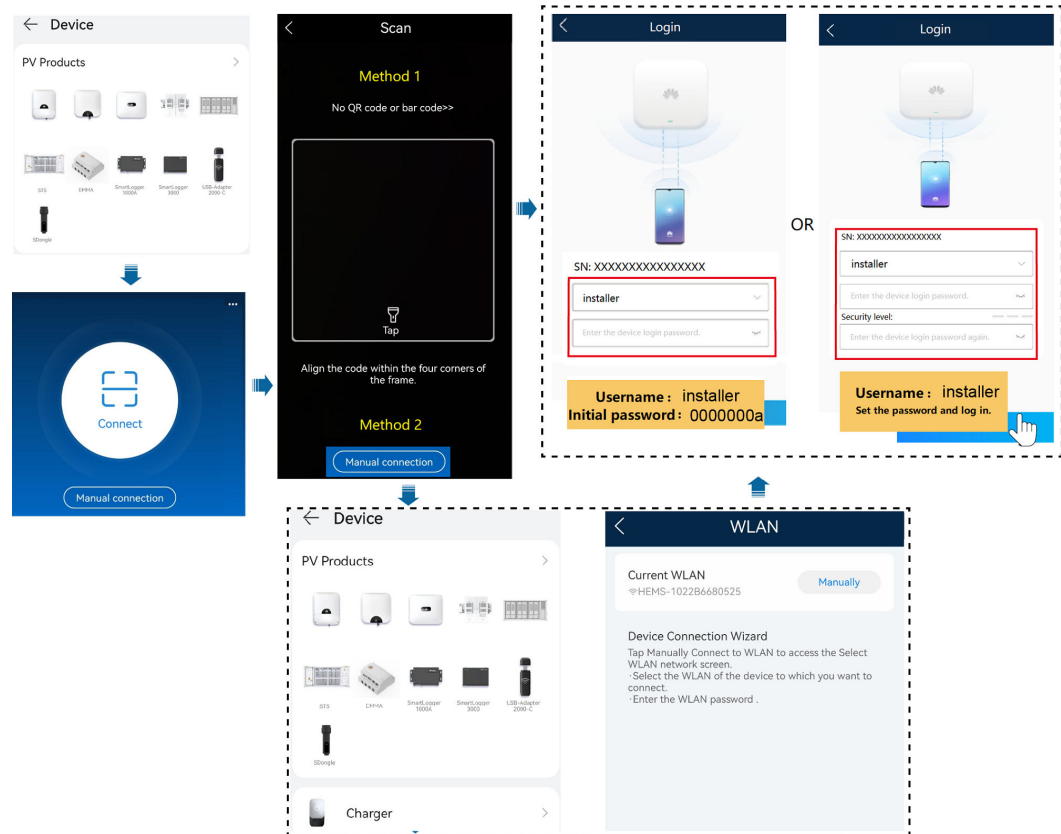
3.1.2 Procedure

To log in to the mobile app for the first time, perform the following steps:

Step 1 Log in to the FusionSolar app and choose **Commission Device**.



Step 2 Log in to the app.



----End

3.1.3 Exception Handling

- Keep the password properly. If the password is lost, you cannot log in to the system.

3.2 Serial Port Maintenance Suggestions

The commissioning serial port has been removed.

3.3 Upgrade and Maintenance Suggestions

3.3.1 Maintenance Suggestions

- Upgrading the BackupBox to the latest version helps update functions, eliminate problems in earlier versions, and improve device security performance.

3.3.2 Procedure

You can upgrade devices such as the EMMA and BackupBox to the latest versions over the mobile app. The upgrade procedure is as follows:

- Step 1** On the operation console menu, choose **Maintenance > Upgrade**. The **Select device** screen is displayed.

Select the corresponding device, select the upgrade file, and tap **NEXT** to check the version.

After confirming that the information is correct, tap **UPLOAD**. After the package is uploaded, tap **Update Now** to start the upgrade.

Figure 3-1 Select device screen

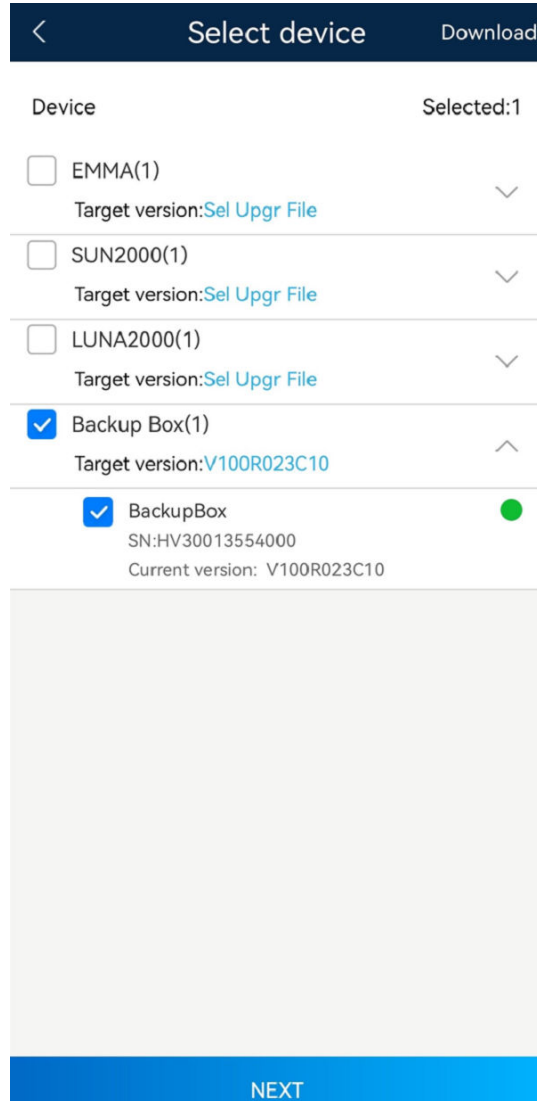


Figure 3-2 Check screen



Figure 3-3 Upgrade package loading screen

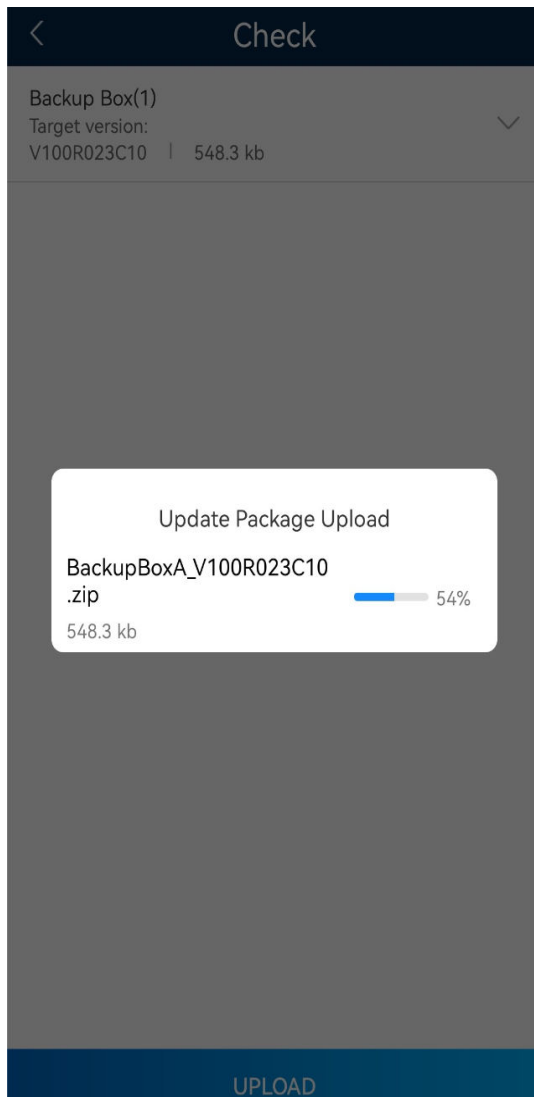


Figure 3-4 Upgrade confirm screen

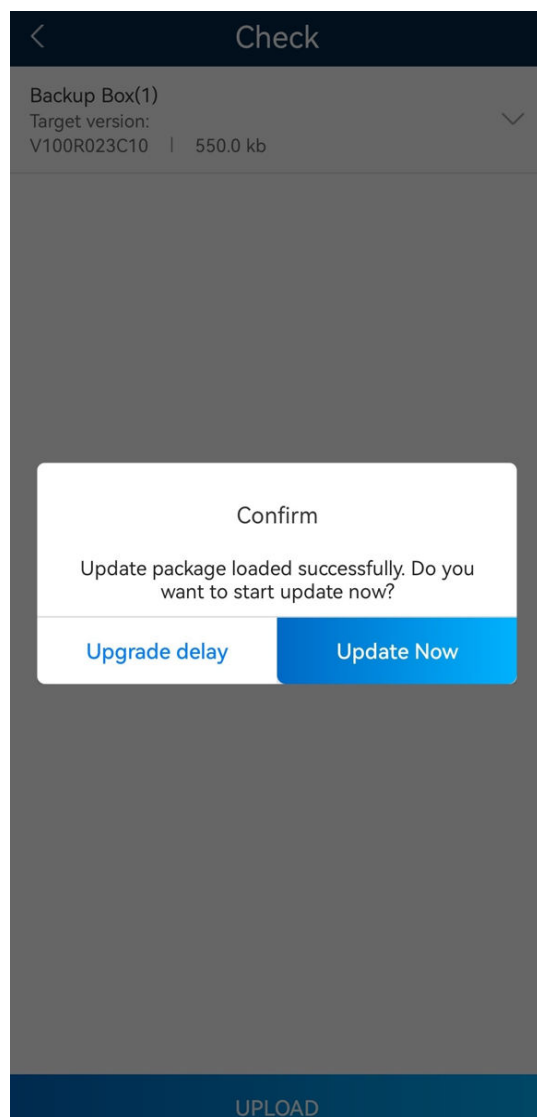
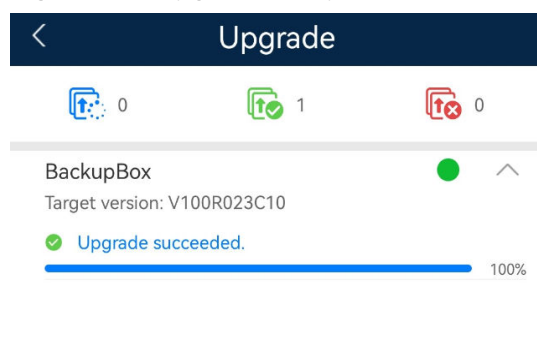
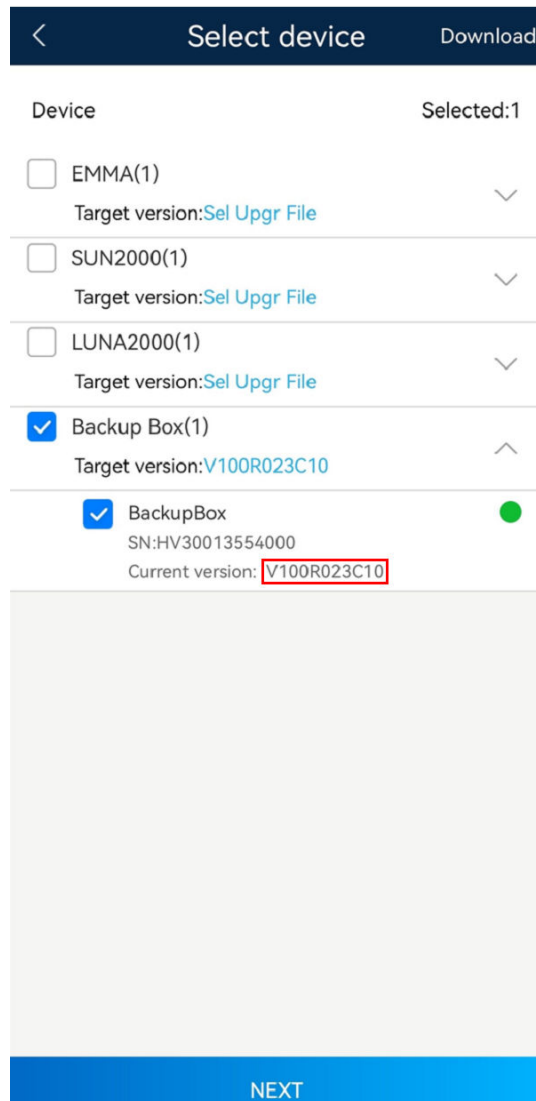


Figure 3-5 Upgrade completion screen



Step 2 After the upgrade is complete, you can confirm the target version on the upgrade screen or download the run_log file for confirmation. For details about how to download the run_log file, see the next section.



----End

If you have any questions about the upgrade, refer to the upgrade guide or contact Huawei supplier for support.

3.4 Log Maintenance Suggestions

3.4.1 Maintenance Suggestions

- Periodically checking device logs helps you learn about the latest device status and eliminate security risks.

3.4.2 Procedure

Perform the following steps to export logs of the BackupBox over the app:

- Step 1** On the operation console menu, choose **Maintenance > Device logs**. On the displayed **Download logs** screen, tap **DOWNLOAD** to download the current logs.

Figure 3-6 Download logs screen

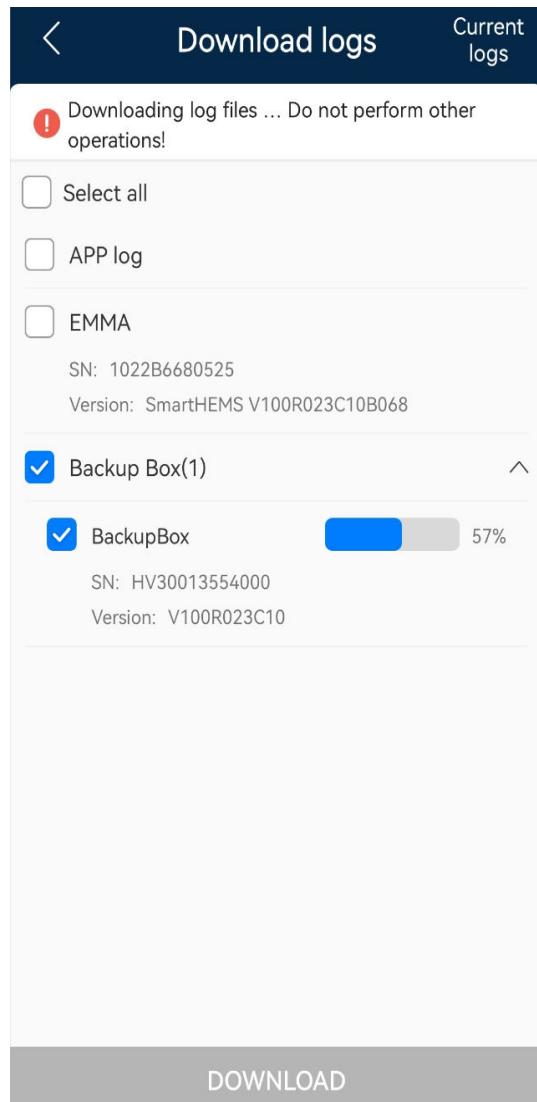
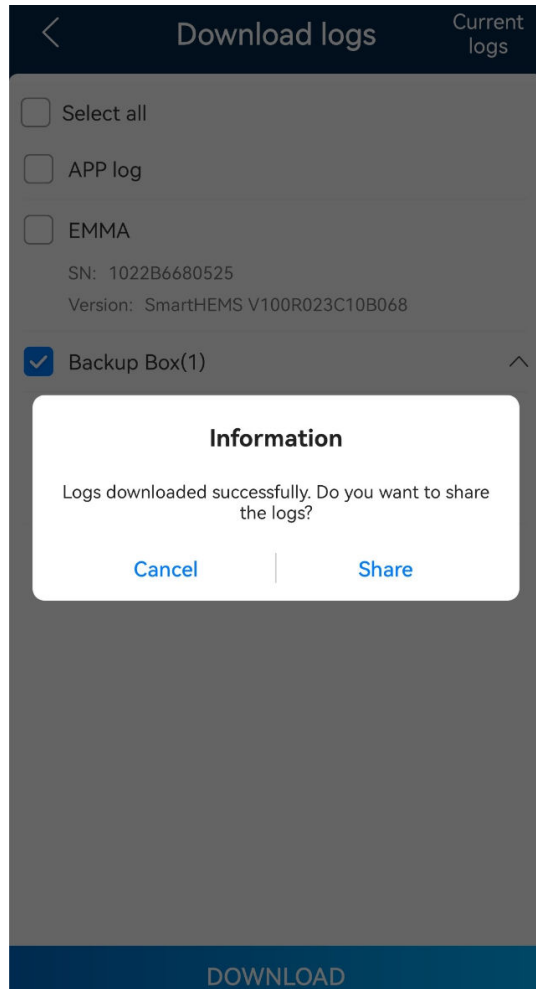
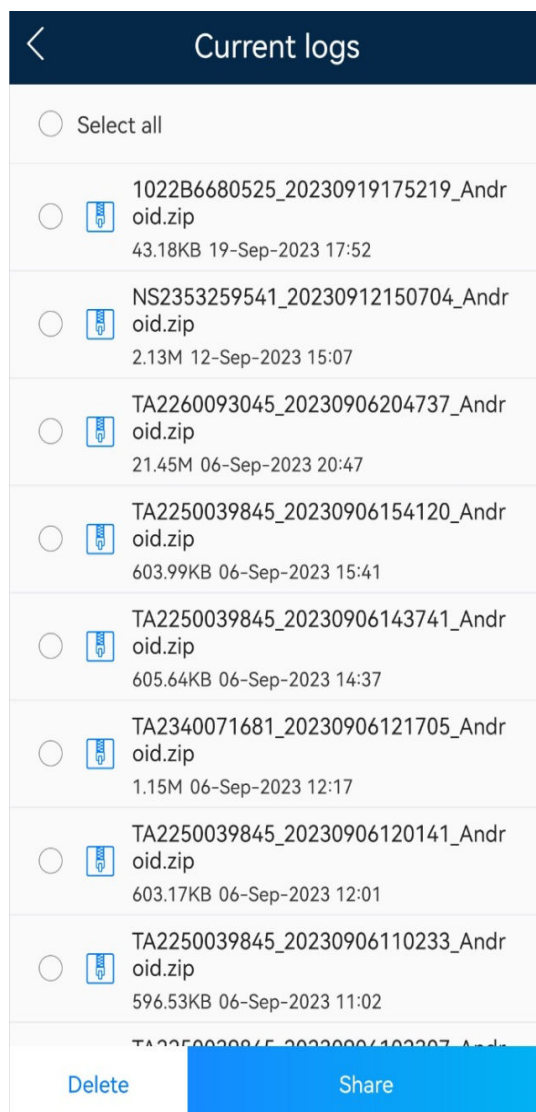


Figure 3-7 Logs downloaded successfully screen



Step 2 On the **Download logs** screen, select **Current logs**. The screen for selecting current logs and storage paths is displayed. Select a log, tap **Share**, and select a sharing mode to export the log.

Figure 3-8 Selecting logs and a save path



Step 3 Check logs to learn about the latest device status. Logs contain the following information:

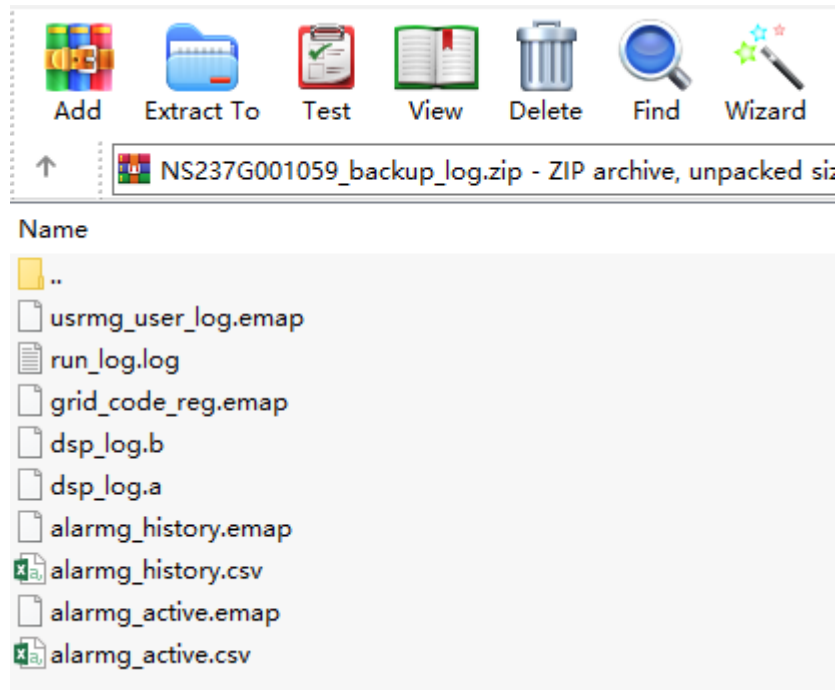
User operation log: records user operations and operation time.

Run log: records the startup and running process of the monitoring system.

Power log: records the startup and running process of the power system.

Alarm log: records active alarms and historical alarms. You can locate faults based on alarm logs.

Figure 3-9 Logs



----End

4 Software Integrity Protection

The integrity of an obtained software package should be checked to prevent PV system network risks that may be caused by malicious tampering or damage during the transmission of the software package. A software package can be installed only after it passes the check.

[4.1 Manually Verifying the Digital Signature of Software Packages](#)

[4.2 Software Integrity Protection](#)

4.1 Manually Verifying the Digital Signature of Software Packages

After downloading software packages during installation and update, users or technical support personnel need to manually verify the integrity of the software packages (PGP package signature). The verification requirements must be specified in the installation manual to remind installation personnel to perform the verification. After the verification is successful, upload the software packages to the device so that the device automatically verifies the integrity of the inner software packages (CMS inner signature).

The software package signature is used to manually verify the integrity of the downloaded software packages. Users or technical support personnel use the integrity verification tool to manually verify the integrity of the software packages.

- Step 1** Log in to <https://support.huawei.com/enterprise/en/tool/software-digital-signature-validation-tool--pgp-verify--TL1000000054>. Click **English** to switch to the English version. (Chinese documents can be downloaded on the Chinese page, and English documents can be downloaded on the English page.)

PGP Verify

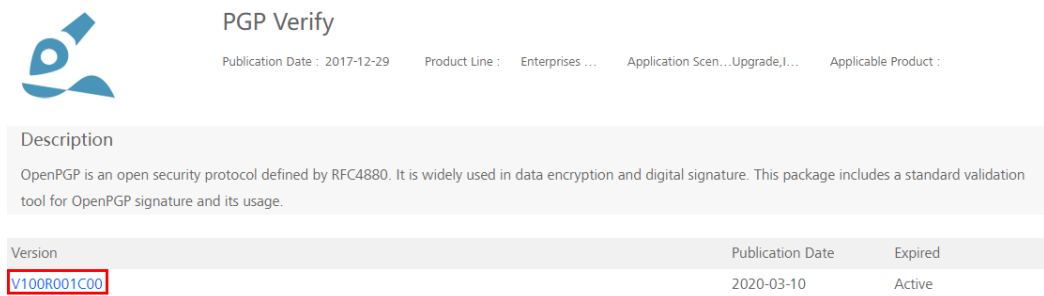
Publication Date : 2017-12-29 Product Line : Enterprises ... Application Scen... Upgrade, I... Applicable Product :

Description

OpenPGP is an open security protocol defined by RFC4880. It is widely used in data encryption and digital signature. This package includes a standard validation tool for OpenPGP signature and its usage.

Version	Publication Date	Expired
V100R001C00	2020-03-10	Active

Step 2 Click **V100R001C00**. The download page is displayed.



PGP Verify

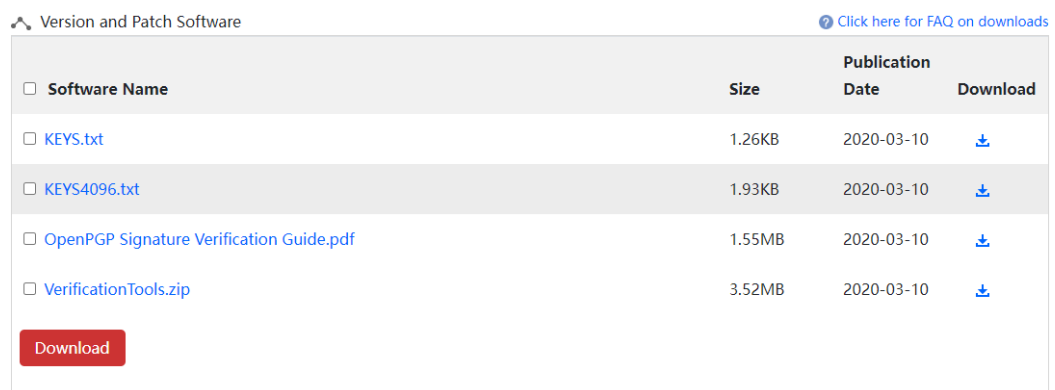
Publication Date : 2017-12-29 Product Line : Enterprises ... Application Scen... Upgrade,1... Applicable Product :

Description

OpenPGP is an open security protocol defined by RFC4880. It is widely used in data encryption and digital signature. This package includes a standard validation tool for OpenPGP signature and its usage.

Version	Publication Date	Expired
V100R001C00	2020-03-10	Active

Step 3 Select **VerificationTools.zip**, **KEYS.txt**, **KEYS4096.txt**, and **OpenPGP Signature Verification Guide.pdf**, and click **Download**.



Version and Patch Software [Click here for FAQ on downloads](#)

<input type="checkbox"/> Software Name	Size	Publication Date	Download
<input type="checkbox"/> KEYS.txt	1.26KB	2020-03-10	↓
<input type="checkbox"/> KEYS4096.txt	1.93KB	2020-03-10	↓
<input type="checkbox"/> OpenPGP Signature Verification Guide.pdf	1.55MB	2020-03-10	↓
<input type="checkbox"/> VerificationTools.zip	3.52MB	2020-03-10	↓

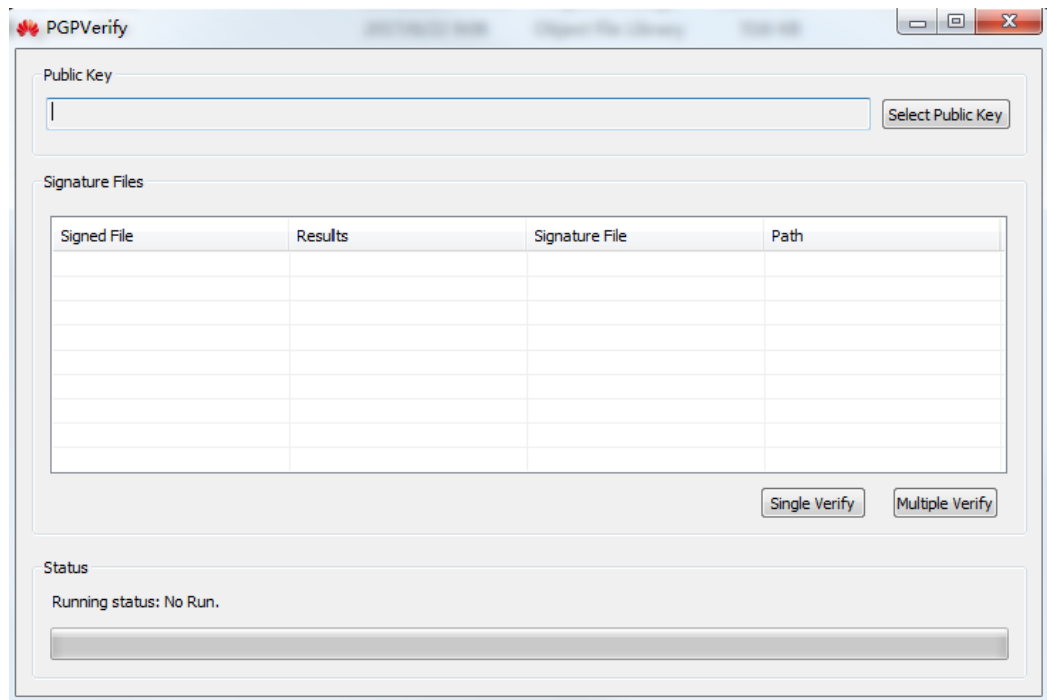
[Download](#)

Step 4 After the download is complete, decompress **VerificationTools.rar** and go to the **VerificationTools > Windows** directory in **VerificationTools** to obtain the PGP verification tool.

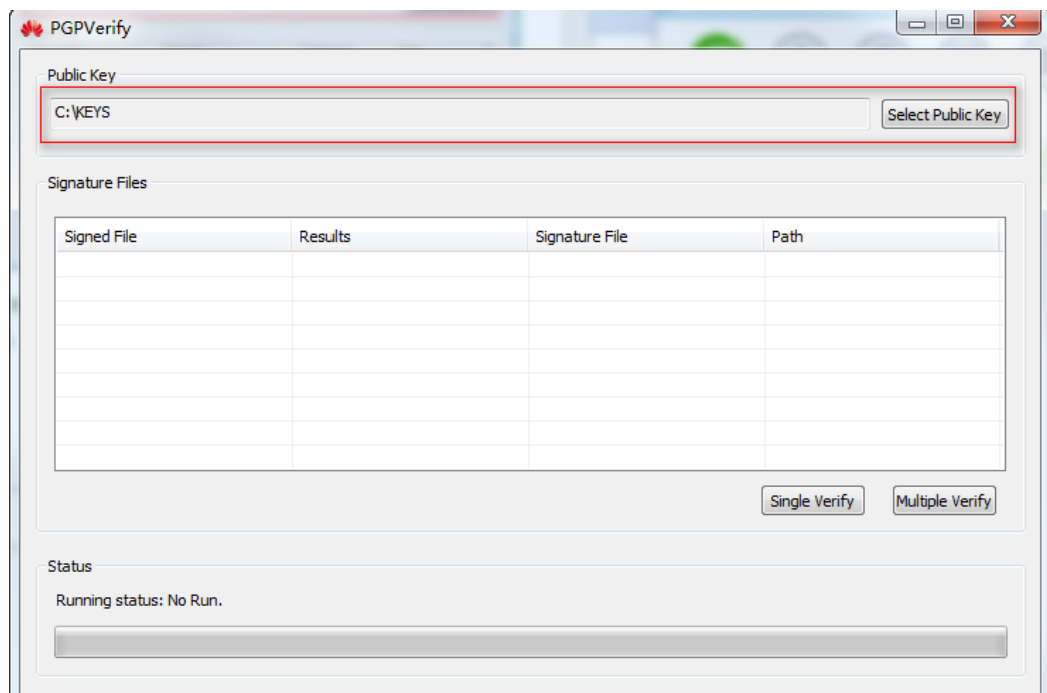
 PGPVerify.exe	2017/12/14 11:36	1,280 KB
 PGPVerify.exe.asc	2017/12/21 14:05	1 KB

Step 5 Log in to the support website of the software product and download the .asc signature file and software package.

Step 6 Double-click **PGPVerify.exe** to start PGPVerify.

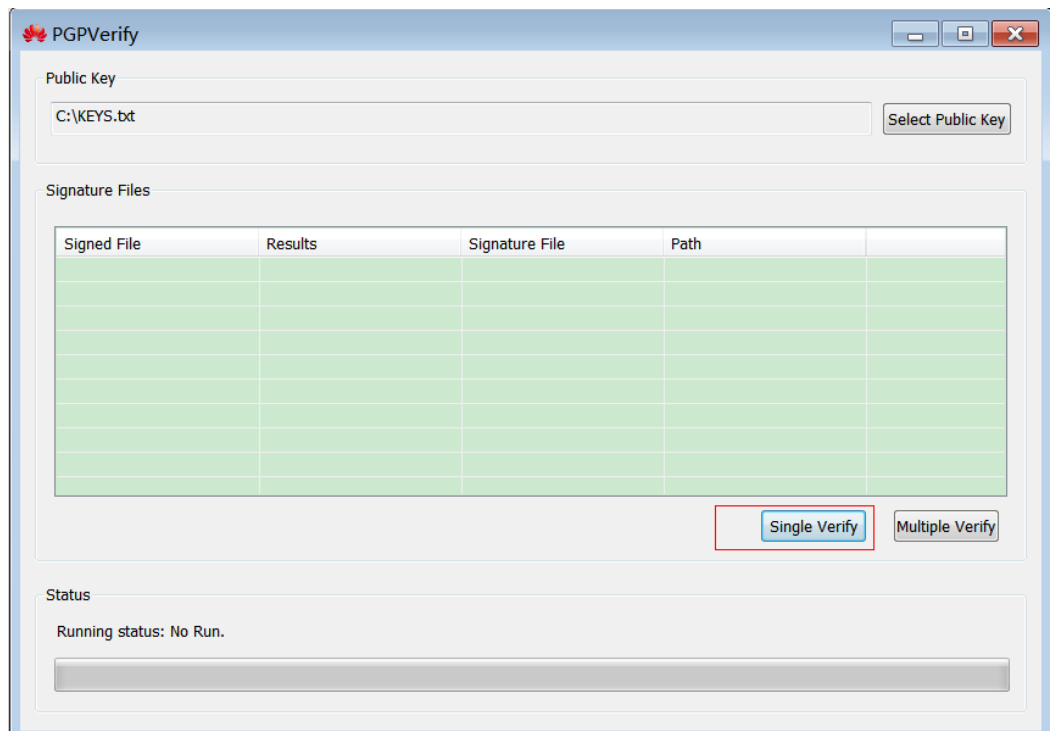


Step 7 Load the public key file as follows: Click **Select Public Key** and select the **KEYS.txt** file downloaded in step 3.

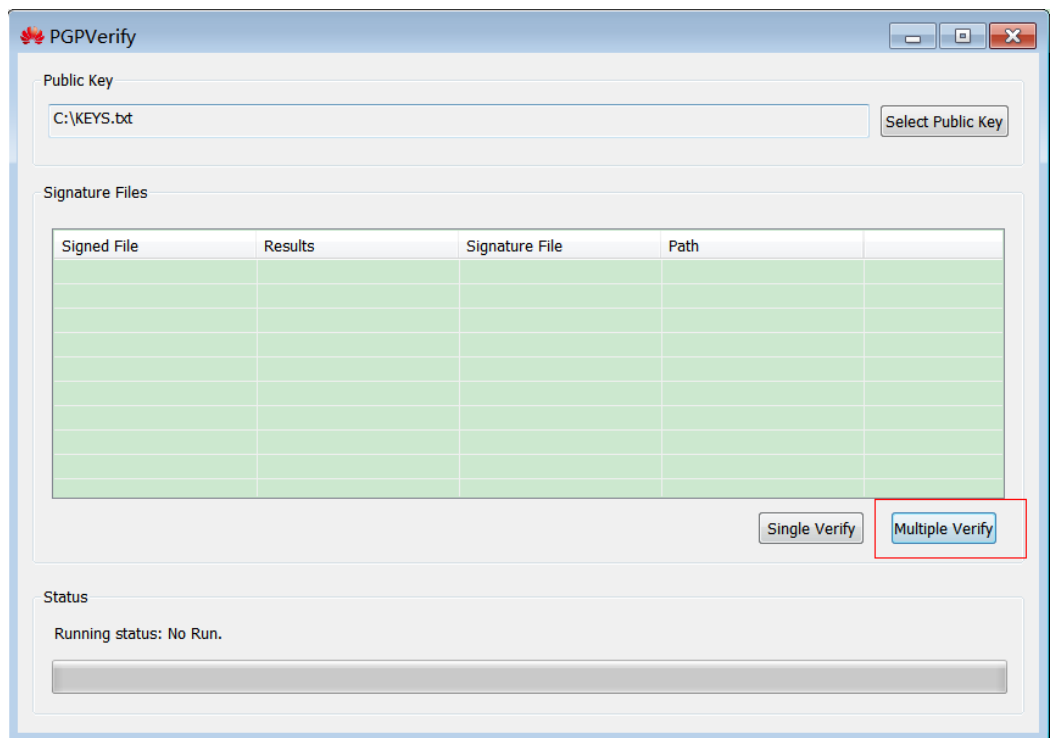


Step 8 Verify the file. Note that the .asc file must be in the same directory as the software package XXX.tar/zip.

- To verify a single file, click **Single Verify** and select the .asc signature verification file.



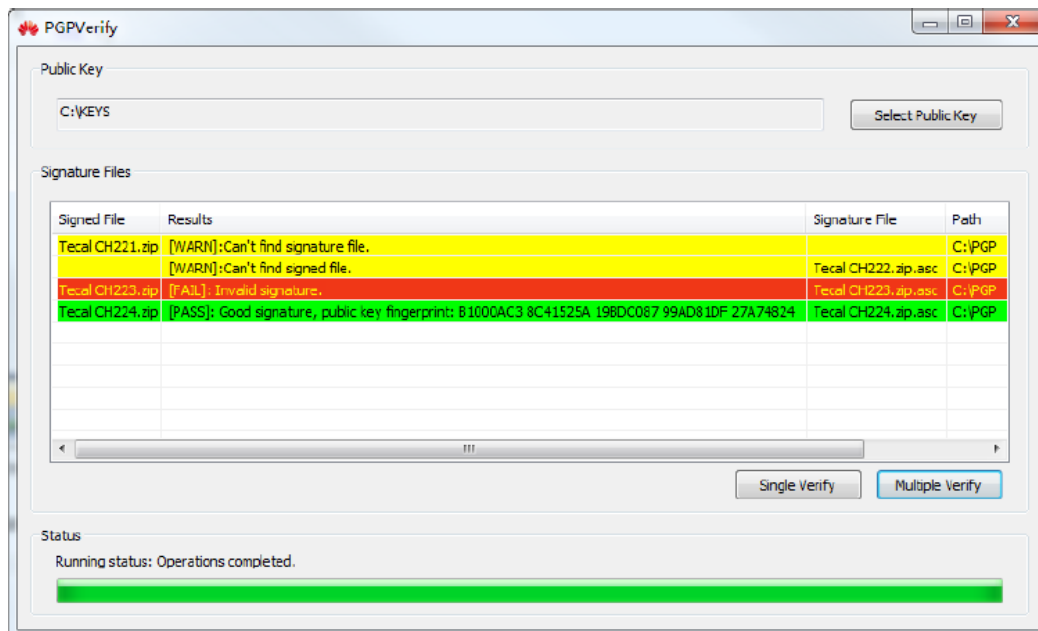
- To verify all files in the directory, click **Multiple Verify** and select the **C:\PGP** directory.



Step 9 Confirm the result.

- If the verification item is yellow and the value of **Results** is **[WARN]**, the signature cannot be verified for certain reasons.
- If the verification item is red and the value of **Results** is **[FAIL]**, the signature verification failed.

- If the verification item is green and the value of **Results** is **[PASS]**, the signature passes the verification using the specified public key.
- If the verification item is green and the value of **public key fingerprint** in the **Results** column is **B1000AC3 8C41525A 19BDC087 99AD81DF 27A74824**, the signature file is a valid signature issued by Huawei. Otherwise, the signature file is untrusted.



Note: If the software package signature verification tool and public key need to be integrated into the products for automatic integrity verification, the public key replacement function must be provided.

----End

4.2 Software Integrity Protection

The preceding features prevent software upgrade packages that have been tampered with from being downloaded to boards and affecting system functions. Only software packages that have not been tampered with can be loaded and used.