Mobile Security

Quick Start

Quick Start

Activate service

Activate the Mobile Security service upon your first visit.

Procedure

Log on to the Alibaba Cloud console.

Click **Mobile Security** service under **Security**.

Ensure that you have read and agreed to the Mobile Security Terms of Service before checking the box on the **Overview** page.

Click **Activate Now** to complete your service activation.

Upgrade to the Professional Edition

Upgrade your Mobile Security services to the Professional Edition in order to access the full range of Mobile Security functions.

Vulnerability scan and app hardening follow the same procedure to achieve the best performance. The vulnerability scan process is explained as follows.

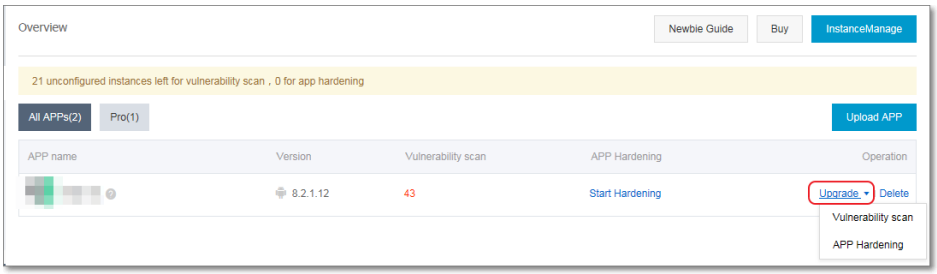
Note: Make sure you have purchased an instance before getting started.

Procedure

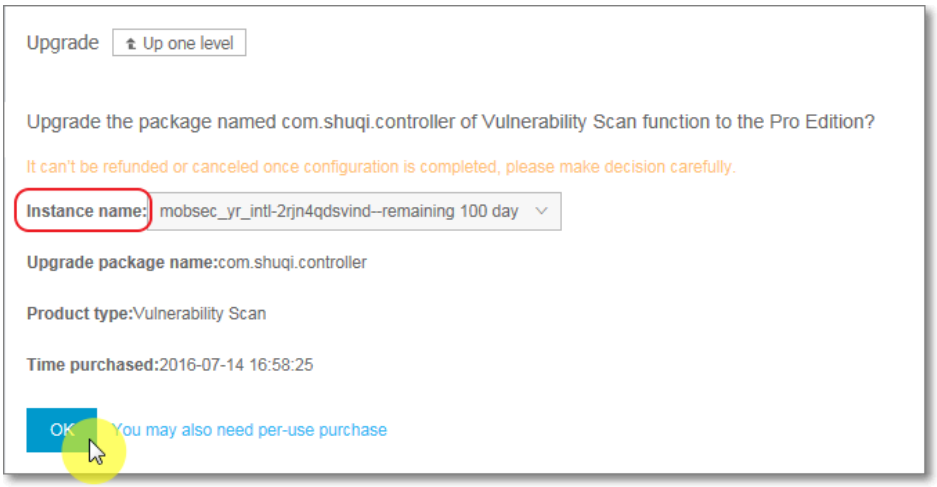
Log on to the **Alibaba Cloud console**.

Click **Mobile Security** service under **Security**.

On the **Overview** page, expand the drop-down box under the operating app, and select the service to be upgraded (in this case, select **Vulnerability scan**).



On the displayed prompt, select the instance to be used for the operation and click **OK** to confirm the operation.



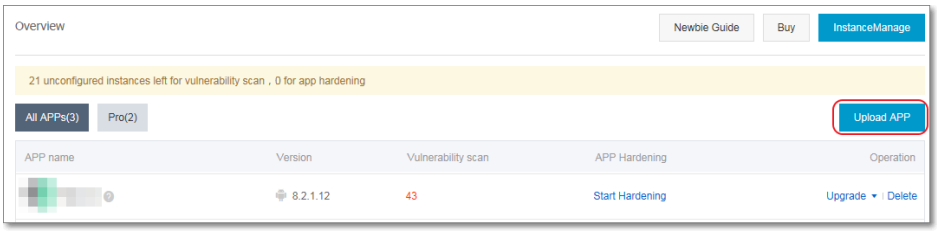
Vulnerability scan

Upload an application

Log on to the Alibaba Cloud console.

Click **Mobile Security** service under **Security**.

Click **Upload APP** on the top-right corner of the **Overview** page.

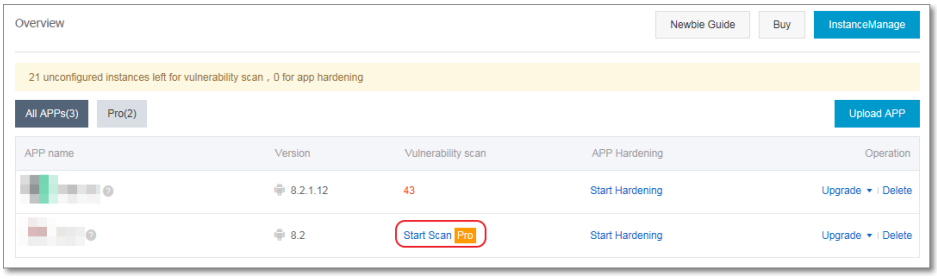


Select the application to be uploaded, and then click **open** to upload it. Wait until the application is uploaded successfully. The application will be added to the APP list.

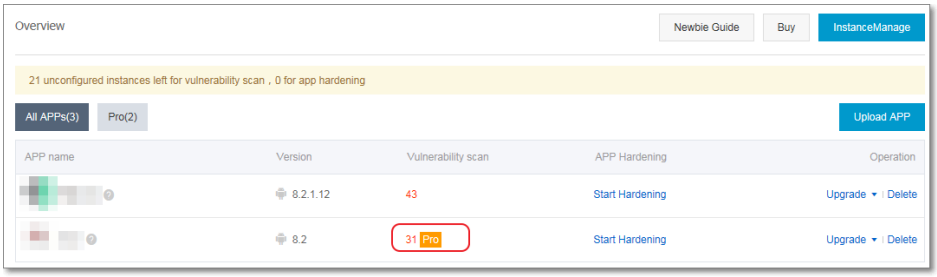
Conduct vulnerability scan

Note: Available for applications that are included in the APP list.

On the **Overview** page, select **Start Scan** under the application to be scanned in the **Vulnerability scan** column. Wait until the scanning is completed. An indicative result (either the total number of vulnerabilities or error message) will be generated in the **Vulnerability scan** column.

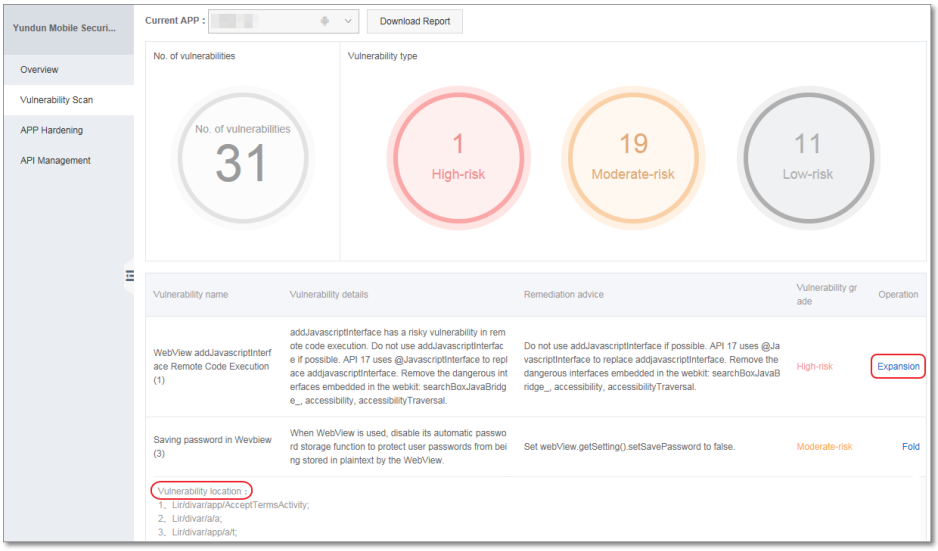


Select the result to view details.



Selecting the number directs you to the diagnostic report, where you can view the vulnerability type and distribution, with detailed description and remediation advice for each vulnerability. To view specific vulnerability locations, operate the **Expansion** button in the **Operation** column.

Note: Only the professional service can access to the location information. Refer to upgrade to the professional edition.



Selecting the error message directs you to the error report, where you can acknowledge the cause of failure, and then act accordingly.

Note: Alternatively, you can perform the whole procedure on the **Vulnerability Scan** page.

App hardening

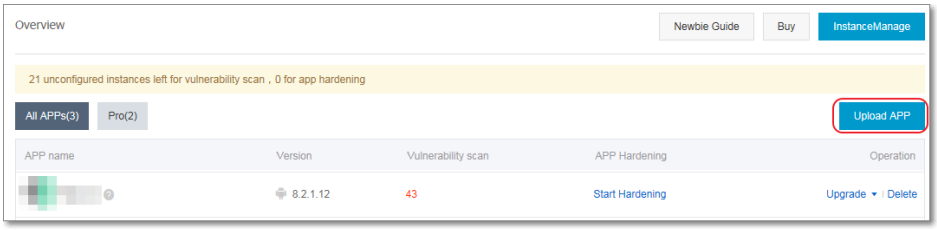
The Mobile Security offers app hardening service for apps included in the Alibaba Cloud.

Upload an application

Log on to the **Alibaba Cloud console**.

Click **Mobile Security** service under **Security**.

Click **Upload app** in the top-right corner of the **Overview** page.

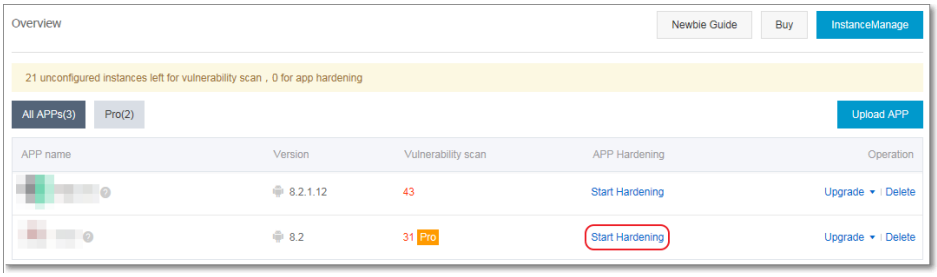


Select the app to be uploaded, and click **Open**. Once the app is successfully uploaded, it will be added to the app list.

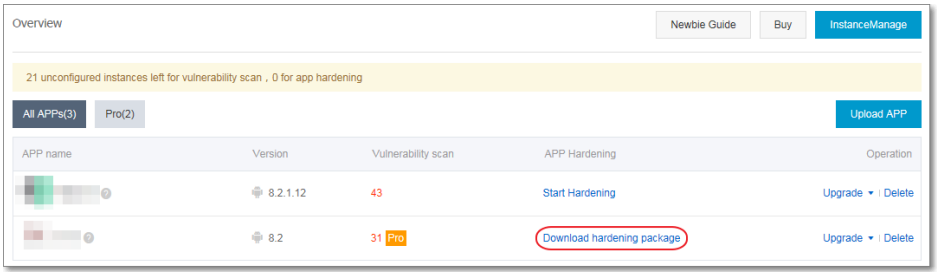
Conduct App hardening

Note: App hardening is only available for apps included in the app list.

On the **Overview** page, select **Start Hardening** under the app to be hardened in the **App Hardening** column and wait until the hardening is completed.

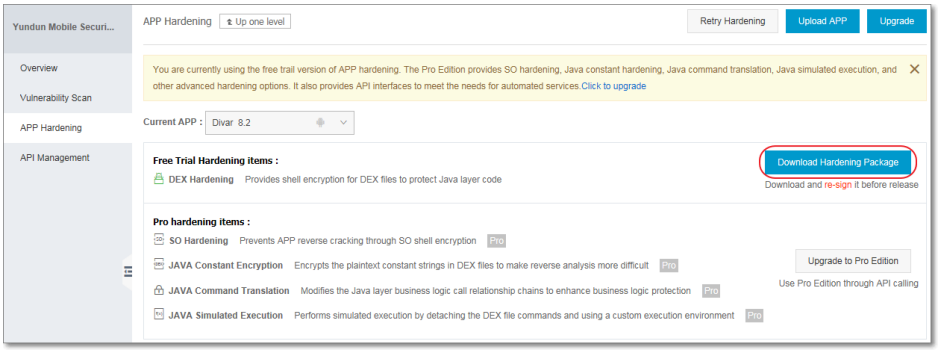


Select **Download hardening package** in the **App Hardening** column, and select the package to be downloaded on the displayed **App Hardening** page.



Only **DEX Hardening** is available in the Free Trial Edition.

To apply advanced hardening options, such as **SO Hardening**, **JAVA Constant Encryption**, **Java Command Translation**, and **Java Simulated Execution**, first upgrade to the Professional Edition.



Re-sign the downloaded hardening package before releasing it. Refer to re-sign an app.

Note: Alternatively, you can perform the entire procedure on the **App Hardening** page.

Re-sign an app

After app hardening, the hardened app is provided in the type of a hardening package. It has to be re-signed before being released.

Use jarsigner to re-sign a hardening package

When re-signing a hardening package, it is recommended to employ the same keystore used for the previous signing. Otherwise, inconsistent signatures may cause failure in uploading the app to the app market.

Follow the jarsigner operating syntax:

jarsigner -digestalg SHA1 -sigalg MD5withRSA -verbose -keystore [your_keystore_path] -signedjar [signed_apk_name] [unsigned_apk_name] [your_keystore_alias]

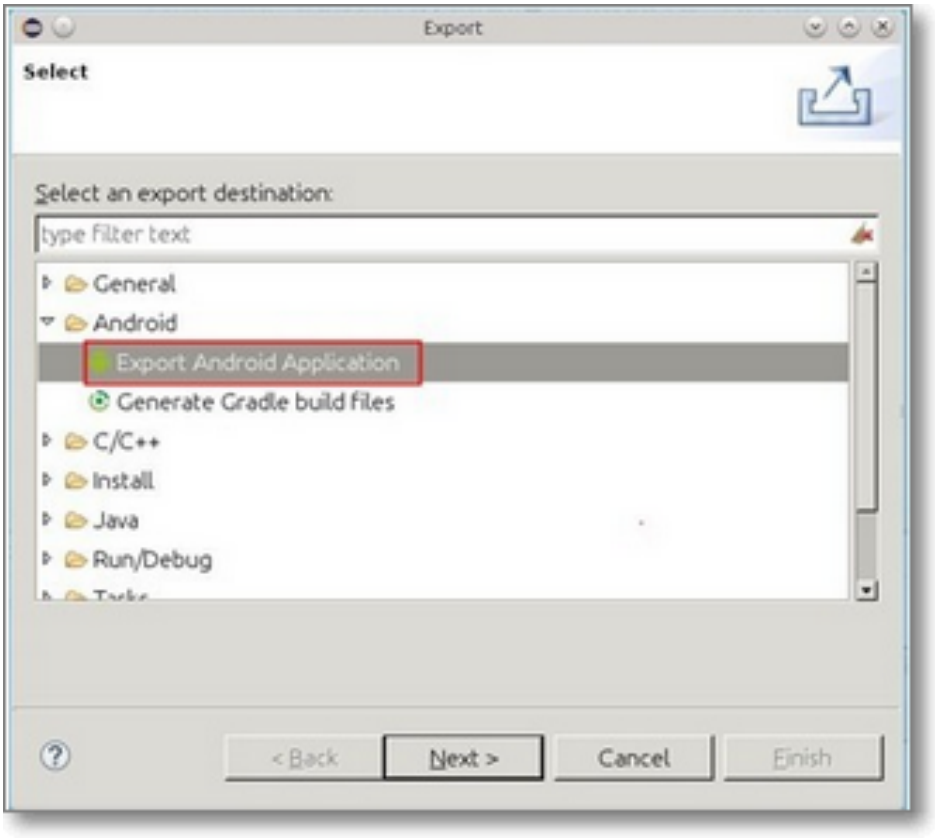
Where,

- your_keystore_path denotes the absolute path of the key.
- signed_apk_name denotes the name of the signed installation package.
- unsigned_apk_name denotes the name of the unsigned installation package.
- your_keystore_alias denotes the key alias.

Get the keystore path

Right-click on the eclipse project.

Select **Export**, and select **Export Android Application**.



Click **Next** to confirm the operation.

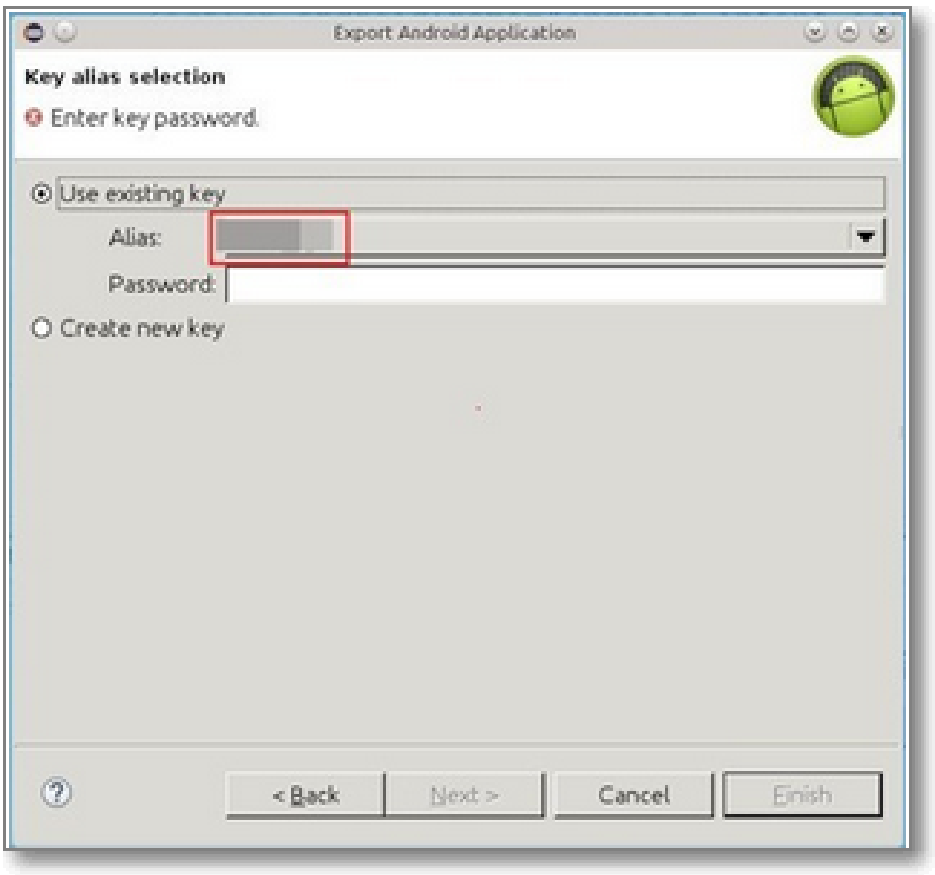
Copy the path filled in the location entry, which is the absolute path of the previous keystore.

Replace your_keystore_path in the syntax with the copied key path.

Get the key alias

On the **Keystore** page, click **Next** to access the **Key alias selection** page.

Through the **Alias** drop-down box, view all existing keys kept in the keystore, and select the one used in the previous app signature.



Replace your_keystore_alias in the syntax with the selected key alias.