Mobile Security

Quick Start

Quick Start

Activate the Mobile Security service upon your first visit.

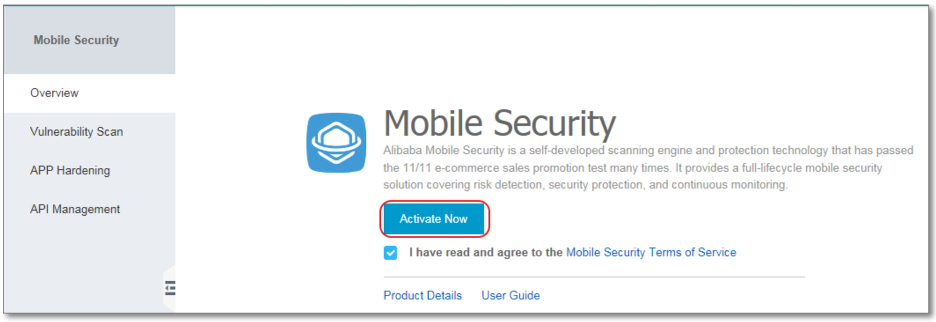
Procedure

Log on to the Alibaba Cloud Security 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.



Alibaba Mobile Security is a self-developed scanning engine and protection technology that has passed the 11/11 e-commerce sales promotion test many times. It provides a full-lifecycle mobile security solution covering risk detection, security protection, and continuous monitoring.

☑ I have read and agree to the Mobile Security Terms of Service

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.

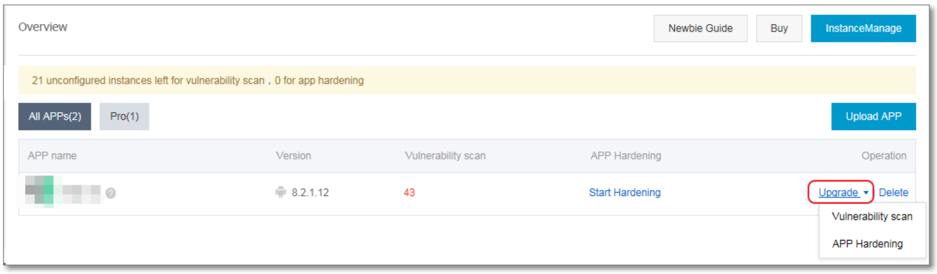
Note: Make sure you have purchased an instance before getting started.

Procedure

Log on to the Alibaba Cloud Security console.

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

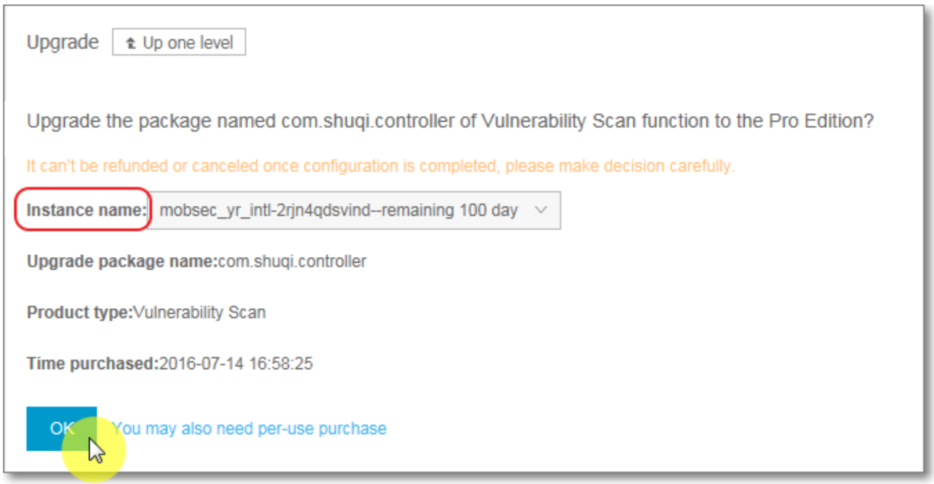
On the **Overview** page, expand the drop-down box under the operating app, and select the service to be upgraded (in this case, select **Vulnerability scan**).



21 unconfigured instances left for vulnerability scan , 0 for app hardening

APP name	Version	Vulnerability scan	APP Hardening	Operation
[redacted]	8.2.1.12	43	Start Hardening	Upgrade ▾ Delete

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



Upgrade the package named com.shuqi.controller of Vulnerability Scan function to the Pro Edition?

It can't be refunded or canceled once configuration is completed, please make decision carefully.

Instance name: mobsec_yr_intl-2rjn4qdsvind--remaining 100 day

Upgrade package name:com.shuqi.controller

Product type: Vulnerability Scan

Time purchased:2016-07-14 16:58:25

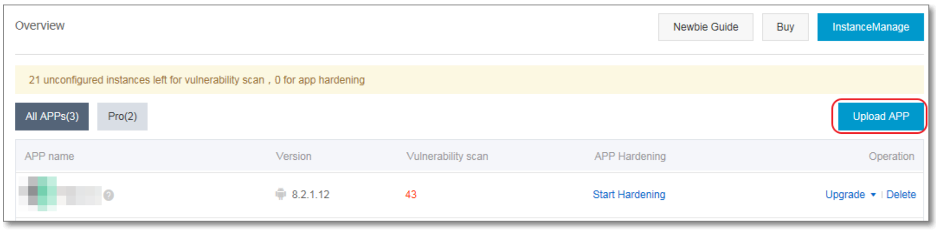
The Mobile Security offers vulnerability scan service for apps that are uploaded to Alibaba Cloud.

Upload an app

Log on to the Alibaba Cloud Security console.

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

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



21 unconfigured instances left for vulnerability scan，0 for app hardening

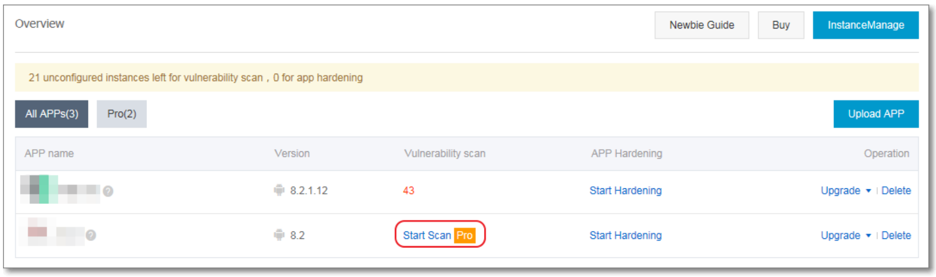
APP name	Version	Vulnerability scan	APP Hardening	Operation
	8.2.1.12	43	Start Hardening	Upgrade ▾ | Delete

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

Conduct vulnerability scan

Note: A vulnerability scan is only available for apps included in the app list.

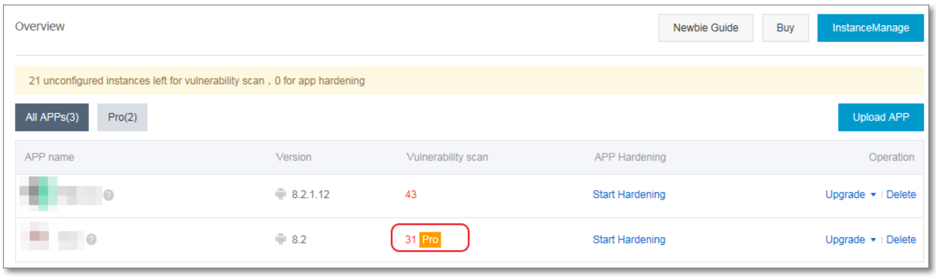
On the **Overview** page, select **Start Scan** under the app to be scanned in the **Vulnerability scan** column. Once the scan is completed, the result (either the total number of vulnerabilities or an error message) will be generated in the **Vulnerability scan** column.



21 unconfigured instances left for vulnerability scan，0 for app hardening

APP name	Version	Vulnerability scan	APP Hardening	Operation
	8.2.1.12	43	Start Hardening	Upgrade ▾ | Delete
	8.2	Start Scan Pro	Start Hardening	Upgrade ▾ | Delete

Select your result to view its details.

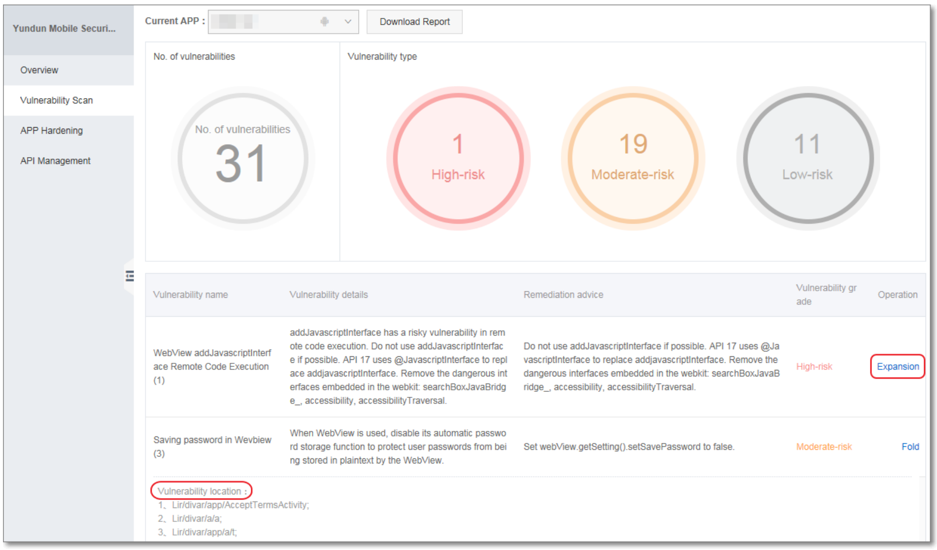


21 unconfigured instances left for vulnerability scan，0 for app hardening

APP name	Version	Vulnerability scan	APP Hardening	Operation
	8.2.1.12	43	Start Hardening	Upgrade ▾ | Delete
	8.2	31 Pro	Start Hardening	Upgrade ▾ | Delete

Selecting the number of vulnerabilities will direct you to the diagnostic report. This includes the vulnerability type and distribution, with detailed descriptions and remediation advice for each vulnerability. To view specific vulnerability locations, select the **Expansion** button in the **Operation** column.

Note: Only the Professional Edition service can access location information. Refer to upgrade to the Professional Edition for details.



Vulnerability name	Vulnerability details	Remediation advice	Vulnerability grade	Operation
WebView addJavascriptInterface Remote Code Execution (1)	addJavascriptInterface has a risky vulnerability in remote code execution. Do not use addJavascriptInterface if possible. API 17 uses @JavascriptInterface to replace addjavascriptInterface. Remove the dangerous interfaces embedded in the webkit: searchBoxJavaBridge_, accessibility, accessibilityTraversal.	Do not use addJavascriptInterface if possible. API 17 uses @JavascriptInterface to replace addjavascriptInterface. Remove the dangerous interfaces embedded in the webkit: searchBoxJavaBridge_, accessibility, accessibilityTraversal.	High-risk	Expansion
Saving password in Wevbiew (3)	When WebView is used, disable its automatic password storage function to protect user passwords from being stored in plaintext by the WebView.	Set webView.getSetting().setSavePassword to false.	Moderate-risk	Fold

Vulnerability location :
1、Lir/divar/app/AcceptTermsActivity;
2、Lir/divar/a/a;
3、Lir/divar/app/a/t;

Selecting the error message will direct you to the error report, where you can view the cause of failure, and act accordingly.

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

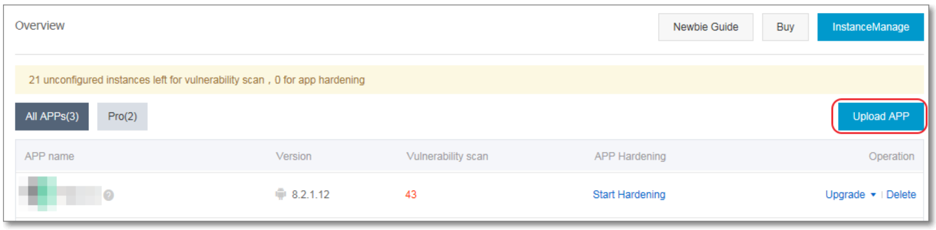
The Mobile Security offers app hardening service for apps that are uploaded to the Alibaba Cloud.

Upload an application

Log on to the Alibaba Cloud Security console.

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

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



21 unconfigured instances left for vulnerability scan , 0 for app hardening

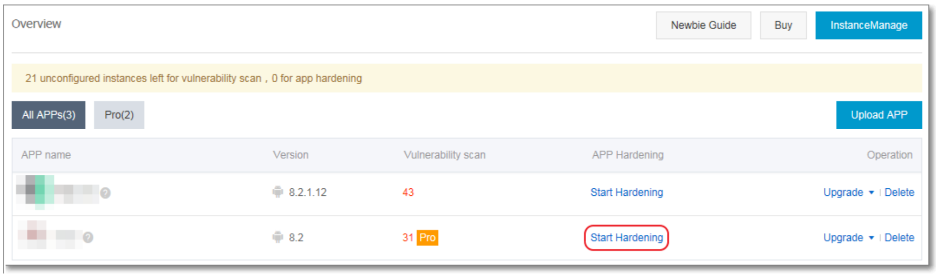
APP name	Version	Vulnerability scan	APP Hardening	Operation
[redacted]	8.2.1.12	43	Start Hardening	Upgrade ▾ | Delete

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.

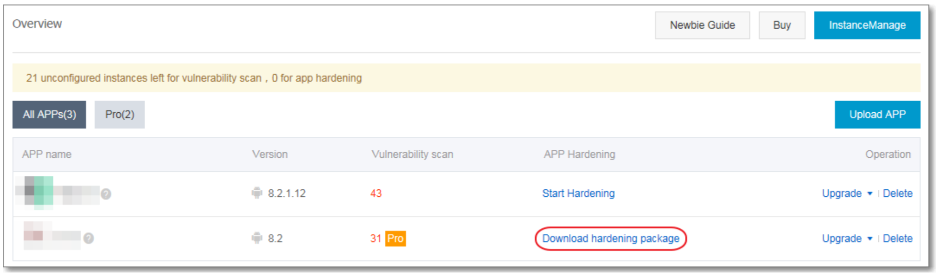
On the **Overview** page, select **Start Hardening** under the app to be hardened in the **App Hardening** column and wait until the hardening is completed.



21 unconfigured instances left for vulnerability scan , 0 for app hardening

APP name	Version	Vulnerability scan	APP Hardening	Operation
	8.2.1.12	43	Start Hardening	Upgrade ▾ | Delete
	8.2	31 Pro	Start Hardening	Upgrade ▾ | Delete

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

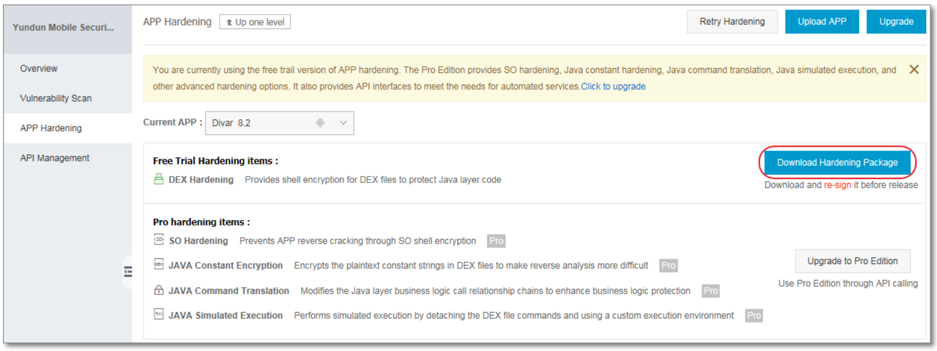


21 unconfigured instances left for vulnerability scan , 0 for app hardening

APP name	Version	Vulnerability scan	APP Hardening	Operation
	8.2.1.12	43	Start Hardening	Upgrade ▾ | Delete
	8.2	31 Pro	Download hardening package	Upgrade ▾ | Delete

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.



You are currently using the free trail version of APP hardening. The Pro Edition provides SO hardening, Java constant hardening, Java command translation, Java simulated execution, and other advanced hardening options. It also provides API interfaces to meet the needs for automated services.Click to upgrade

Current APP : Divar 8.2

Free Trial Hardening items :

DEX Hardening Provides shell encryption for DEX files to protect Java layer code

Download and re-sign it before release

Pro hardening items :

SO Hardening Prevents APP reverse cracking through SO shell encryption Pro

JAVA Constant Encryption Encrypts the plaintext constant strings in DEX files to make reverse analysis more difficult Pro

JAVA Command Translation Modifies the Java layer business logic call relationship chains to enhance business logic protection Pro

JAVA Simulated Execution Performs simulated execution by detaching the DEX file commands and using a custom execution environment Pro

Use Pro Edition through API calling

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, we recommend that you 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]

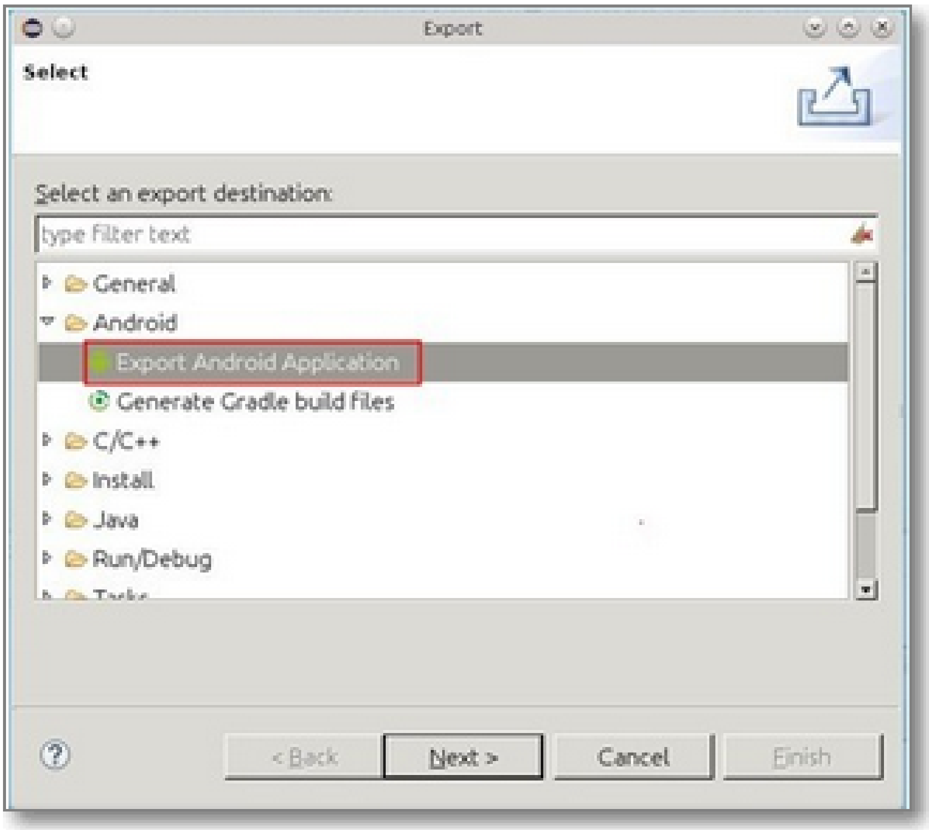
Where,

- 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.

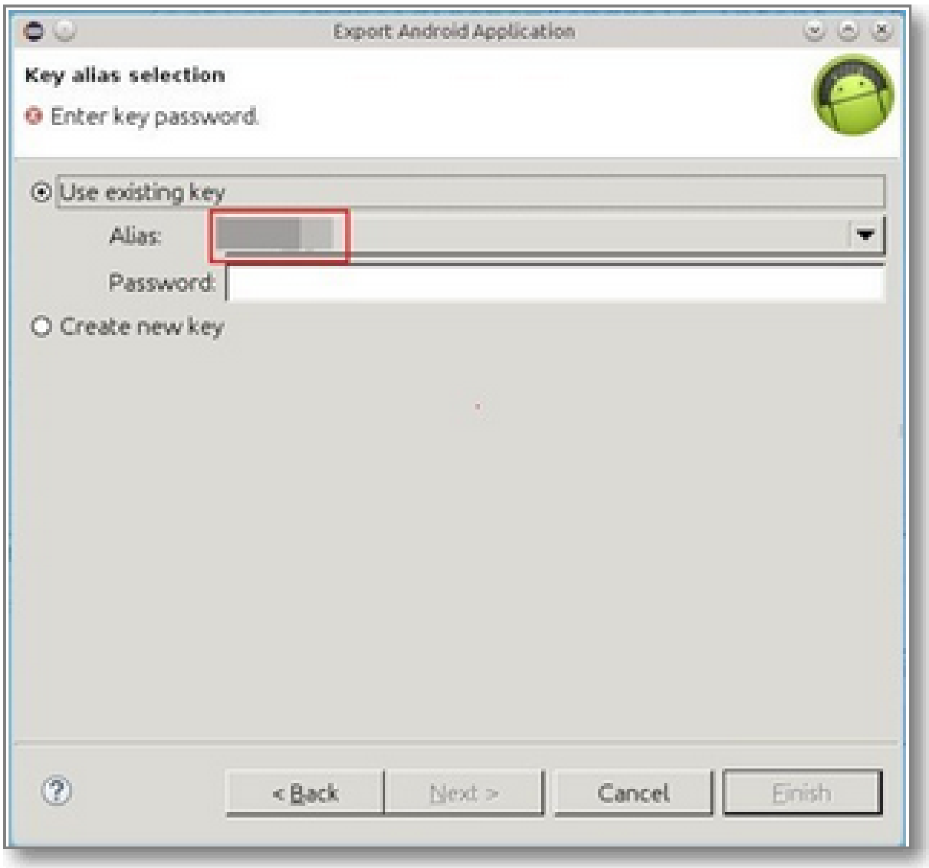
Copy the path filled in the location entry, which is the absolute path of the previous keystore.

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.



Key alias selection

Enter key password.

● Use existing key

Alias: [redacted]

Password:

○ Create new key

Replace your_keystore_alias in the syntax with the selected key alias.