Mobile App Security Scanner by Code Creator

Customer Instructions for AWS Marketplace

Private mobile application security analysis in your AWS account

Item	Value
Base platform	Ubuntu 24.04 LTS on Amazon EC2
Core engine	Mobile Security Framework MobSF v4.5.1
Deployment model	Docker Compose with Caddy HTTPS reverse proxy
Validated scope	Static analysis through the MobSF web workspace
Public ports	80 and 443 only

Important usage notice

Use this AMI only to test mobile applications, packages, and source code that you own or are authorized to assess. The product provides automated security analysis to assist developers, auditors, and AppSec teams. It does not replace a full manual penetration test, legal compliance review, or production security certification.

1. Launch the instance

Recommended launch configuration

- Recommended instance type: m7i.xlarge for initial use and larger instances for heavier scan workloads.
- Use the default root volume included with the AMI unless your organization needs additional storage.
- Enable a public IPv4 address if you want the automatic public-IP-based HTTPS setup.
- Use a new EC2 key pair for SSH access and **ubuntu** as user.

Security group rules

Port	Protocol	Source	Purpose
22	TCP	Your IP only	SSH administration
80	TCP	0.0.0.0/0	HTTP redirect and certificate validation
443	TCP	0.0.0.0/0	Secure web access

Do not open ports 8000, 1337, or 5432 to the public internet. MobSF, its internal proxy port, and PostgreSQL are kept private behind the HTTPS reverse proxy.

2. Wait for first boot to finish

After the instance launches, first boot may take several minutes. During this time, the system generates fresh credentials, discovers the instance public IP address, creates a public-IP-based HTTPS hostname, starts PostgreSQL, MobSF, the scan worker, and Caddy, then writes the customer login file.

Check status with:

```
mobile-security-scanner-status
```

The expected first-boot state is complete, with HTTPS health returning ok.

3. Retrieve the login information

Run this command after first boot completes:

```
cat /home/ubuntu/FIRST_LOGIN.txt
```

The file contains the secure workspace URL, administrator username, generated password, helpful commands, security notes, and open-source notices link.

Default administrator username:

```
ccadmin
```

4. Open the secure workspace

Use the URL shown in FIRST_LOGIN.txt or run:

```
mobile-security-scanner-url
```

The URL will normally look similar to:

```
https://PUBLIC-IP-WITH-DASHES.nip.io/
```

Sign in with username ccadmin and the generated password from FIRST_LOGIN.txt. Change the administrator password after your first successful sign-in.

5. Run a static mobile app scan

1. Open the HTTPS workspace in your browser.
2. Sign in with the generated ccadmin credentials.
3. Drag and drop an authorized APK, AAB, IPA, APPX, JAR, AAR, SO, dylib, or source archive into the upload area.
4. Wait for MobSF to analyze the package.
5. Review the report sections for permissions, manifest findings, certificate details, code findings, trackers, files, and security warnings.
6. Export or save the report as needed for your internal review process.

Validated scope for version 1.1

Version 1.1 is validated for static analysis through the MobSF web workspace. MobSF includes dynamic analysis features upstream, but this AMI does not include a configured Android emulator, iOS device, or separate dynamic-testing infrastructure. Do not market this AMI as a ready-to-use dynamic-analysis lab unless a later version adds and validates that capability.

6. Useful commands

Task	Command
Show URL	**mobile-security-scanner-url**
Show service health and containers	**mobile-security-scanner-status**
Read first login details	**cat /home/ubuntu/FIRST_LOGIN.txt**
Show Docker services	**sudo docker compose --project-directory /opt/mobile-**

	security-scanner --env-file /opt/mobile-security-scanner/.env -f /opt/mobile-security-scanner/compose.yaml ps

7. Stop and start behavior

If the instance is stopped and later started, AWS may assign a new public IPv4 address unless you use an Elastic IP. The included network refresh service detects the current public IP and updates the public-IP-based hostname and FIRST_LOGIN.txt automatically.

After a stop and start, run:

```
mobile-security-scanner-status
```

8. Security and data handling

- Uploaded packages and scan results remain on the EC2 instance and attached EBS storage unless you delete them.
- Restrict SSH access to your administrator IP address.
- Use HTTPS only for the web workspace.
- Change the generated administrator password after first sign-in.
- Upload only applications and source code that you are authorized to test.
- Do not expose internal application ports directly to the internet.

9. Open-source notices

This product includes Mobile Security Framework MobSF v4.5.1. MobSF is licensed under the GNU General Public License version 3. The AMI includes the MobSF GPL license and corresponding MobSF v4.5.1 source bundle at:

- /usr/share/doc/mobile-security-scanner/MobSF-GPL-3.0.txt
- /usr/share/doc/mobile-security-scanner/THIRD_PARTY_NOTICES.txt
- /usr/share/mobile-security-scanner/source/MobSF-v4.5.1-source.tar.gz

The open-source notice page is available on the running instance at:

```
https://PUBLIC-IP-WITH-DASHES.nip.io/open-source-notices.html
```

10. Troubleshooting

Problem	What to check
Browser cannot connect	Confirm ports 80 and 443 are open in the security group and the instance has a public IPv4 address.
FIRST_LOGIN.txt is missing	Wait a few more minutes, then run mobile-security-scanner-status and check the first-boot service result.
Certificate is not ready	Confirm port 80 is open for validation and the public hostname in FIRST_LOGIN.txt matches the instance public IP.
Login fails	Use username ccadmin and the password exactly as shown in FIRST_LOGIN.txt. Avoid copying extra spaces.
Large uploads fail	Use a larger instance or confirm browser/network stability. For very large packages, increase instance resources before heavy use.
Need the API	Open the MobSF API page from the authenticated workspace and use the customer-specific API key shown there.

11. Support and learning resources

- MobSF project: https://github.com/MobSF/Mobile-Security-Framework-MobSF
- MobSF live documentation and API reference: https://mobsf.live/
- OWASP MASVS: https://mas.owasp.org/MASVS/
- AWS security groups: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-security-groups.html
- AWS Marketplace AMI policies: https://docs.aws.amazon.com/marketplace/latest/userguide/product-and-ami-policies.html