1. Requirements

Sensitive Information Storage

- User account information is managed locally with strong hashing and SALT applied.
- All log data is stored in a local database with access control applied, in encoded form.

Data Encryption Settings

To enable data encryption, follow these steps:

```
> sudo vi /monitorapp/aiwaf/conf/ui_conf.php
> Change is_klib_crypto = '1'
> Execute pwd
```

Data Decryption Method

Data decryption occurs automatically when the user references data via the Web Console.
e.g., Logging into AISWG-VE Web Console

Independent Data Storage

Log data is stored locally by default. To configure remote backup, follow these steps in the Web Console:

- Navigate to: System > Device Settings > Log DB Settings > Backup Server Settings > Add Backup Server
- Enter required information depending on server type (FTP/SFTP, AWS S3, MS Azure, GCP). For AWS S3, provide Bucket name and Access key/Secret Key.
- Verify the added server in the backup server list, then go to Log Backup Settings > Select Backup Server, add (+) the server, and click Apply.
- In Log Backup Settings > Change Log Backup Settings, set log backup to Enabled, specify backup cycle and target, then click Apply.
- Click Immediate Backup and Transfer to verify proper operation.

To configure automatic log deletion along with periodic backup:

- Navigate to: Log Backup Settings > Change DB Data Backup and Auto Deletion
- Configure auto deletion conditions (disk partition usage threshold or retention period).
- If backup must occur before deletion, set Transfer to Backup Server to Enabled.
- Select logs to delete and click Apply.
- Click Immediate Check to verify operation. (If current conditions do not meet the threshold, no action will occur.)

To restore log data:

- Upload backup files to the product via SFTP. Refer to 3. Usage Instructions for account and connection details.
- Set file ownership and permissions:

```
> sudo chown postgres:postgres /home/jin/users.csv
> sudo chmod 644 /home/jin/users.csv
```

- Connect to the PostgreSQL database:

```
> psql -U postgres aiswg_db
```

- Restore the uploaded file:

```
> COPY users FROM 'file path' DELIMITER ',';
```

- Verify restored log data in Web Console > Log menu.

Application Status Check

To check instance status in AWS Console:

- Navigate to EC2 > Instances > Status Checks. Review the following results:

> System Status Check – Passed
> Instance Status Check – Passed
> Navigate to EC2 > Instances > Monitoring. Confirm system resources and network I/O remain at normal levels.
> Navigate to EC2 > Instances > Storage. Verify block device volume status is in-use and attachment status is attached.

AWS Service Quota Management

This product is provided as BYOL. To scale up, follow these steps:
- Confirm supported instance types. Officially supported: m5 family.
- Stop the instance: AWS Console > EC2 > Instance State > Stop Instance
- Change instance type: Actions > Instance Settings > Change Instance Type > Select New Instance Type
- Start the instance: AWS Console > EC2 > Instance State > Start Instance
- Once boot is complete, verify instance status using the Application Status Check procedure above.

Cost Information

This product is BYOL. Officially supported instance family: m5. On-demand pricing is as follows:
- m5.large — 0.118 USD/hour
- m5.xlarge — 0.236 USD/hour
- m5.2xlarge — 0.472 USD/hour
- m5.4xlarge — 0.944 USD/hour
- m5.8xlarge — 1.888 USD/hour

2. Release Notes

Release notes for all commercial versions are accessible directly via the Web Console:
- Log in to the product via Web Console, then click Shortcut > Manual in the upper-right corner.
- Use the left-hand menu to select the version and item to view.

3. Usage Instructions

Web Console Access

- In your browser, enter: https://AISVA-VE_IP:222
- Enter login credentials in the right-hand login form.

> Default ID: administrator
> Default PW: [Instance ID]*

- On first login, you must change these credentials. The system will redirect you to a page to update ID and PW.
- After login, you will access the Web Console dashboard, where system information and network flow can be monitored.
- Use the top menu bar to navigate:

> Log: View log data in real time
> Report: Generate reports based on system information or log data
> Policy: Configure protected user information and create security policies
> System: Configure detailed settings such as log backup

* Instance ID: You can check this in the following sections of the AWS EC2 Console.
EC2 > Instances > Details > Instance summary > Instance ID

SSH Console Access

AISVA-VE does not recommend CLI configuration via SSH.
Most system configurations are provided through the Web Console.
If SSH access is required, please refer to the information below to connect.
- Connect via SSH client using the following information:

> host: AISWG-VE_IP
> port: 22
> username: aiadmin
> PW: number1aiswg // OR use [SSH Key pair]*

* SSH Key pair: When creating an instance, use the selected Key pair file under the Key pair (login) section.
Once a Key pair file is lost, it cannot be regenerated, so please manage it carefully.
To create a Key pair, follow these steps:
(When creating an instance) Click Create new key pair under the Key pair (login) section.
Enter the Key pair name, set Key pair type to RSA and Private key file format to .ppk, then click Create key pair.
(In the EC2 - Key Pairs menu) EC2 > Network & Security > Key Pairs > Create key pair

Enter the Name, set Key pair type to RSA and Private key file format to .ppk, then click Create key pair.

Initial Configuration
- Register protected users in: Policy > General > User Management. You may register users by department or import via .csv file.
- Configure basic security policy in: Policy > Web > Security Filter > Category Filter.
- Click Add Rule, enter required fields (department, filter name, user, category via drag-and-drop), then click Apply.
- Click Shortcut in the policy change notification banner, navigate to the menu, and click Apply Policy to finalize.

4. Upgrade Instructions

Direct version upgrades by users are not recommended.
If upgrades are required for feature enhancements, please contact technical support.
During upgrades, all data and settings are preserved, and rollback to previous versions is possible if needed.

5. CloudFormation Delivery Instructions

CloudFormation is not officially supported.