MONITORAPP

APPLICATION INSIGHT™ WAF

Release Notes

Version 5.0.2_2
March 07, 2022

Table of Contents

1. Introduction

- Thank you for using APPLICATION INSIGHT WAF (hereafter AIWAF) V5.0.2_2.
- This AIWAF V5.0.2_2 patch is a recommended patch that contains bug patches and functional requirements of AIWAF V5.0.2. It is recommended to keep your system up-to-date by adding improved security features to your system.
- Before using the AIWAF V5.0.2_2 please refer this document.

2. Known Limitation

- A system reboot is required after the patch is completed.
- For use of the patch package, AIWAF V5.0.2 must be installed on the system.

3. Supported Version and Platforms

- Software version
  - AIWAF V5.0.2

- Platforms
  - APPLICANCE (Based on AIOS V5.0.0)
    AIWAF-100_Y17, AIWAF-200_Y17, AIWAF-500_Y17, AIWAF-1000_Y17, AIWAF-2000_Y17, AIWAF-4000_Y17, AIWAF-1000_Y17 R, AIWAF-2000_Y17 R, AIWAF-4000_Y17 R, AIWAF8000_Y18 AIWAF-100_Y20, AIWAF-200_Y20, AIWAF-500_Y20, AIWAF-1000_Y20, AIWAF-2000_Y20, AIWAF-4000_Y20, AIWAF-8000_Y20, AIWAF-1000_Y20 R, AIWAF-2000_Y20 R, AIWAF4000_Y20 R

  - Virtual Edition (Based on Ubuntu 18.04 LTS)
    Virtual Machine, General Server

4. Installation Procedures

4.1. Installation Preparation

- Default product access information
  - AI Manager Console ID: aiadmin
    AI Manager Console PW: number1aiwaf
    AI Manager Web ID: administrator
    AI Manager Web PW: _appleader
  - GUI ID: administrator
    GUI PW: _appleader

- Upload the patch package file to AIWAF.
  - For the patch package, use Patch management > Patch in AI Manager Web.

- Check the hash value of the patch package.
  - Patch package
    AIOS_V5.0.0_B46_AIWAF_V5.0.2_2_B2373_AIMANAGER_V2.1.0_B130_update_220303.tgz
    Sha256sum value : c8571f62c439c1bbb6d8cb7128e6938788ba04bf366a469842b01a81fe11a818

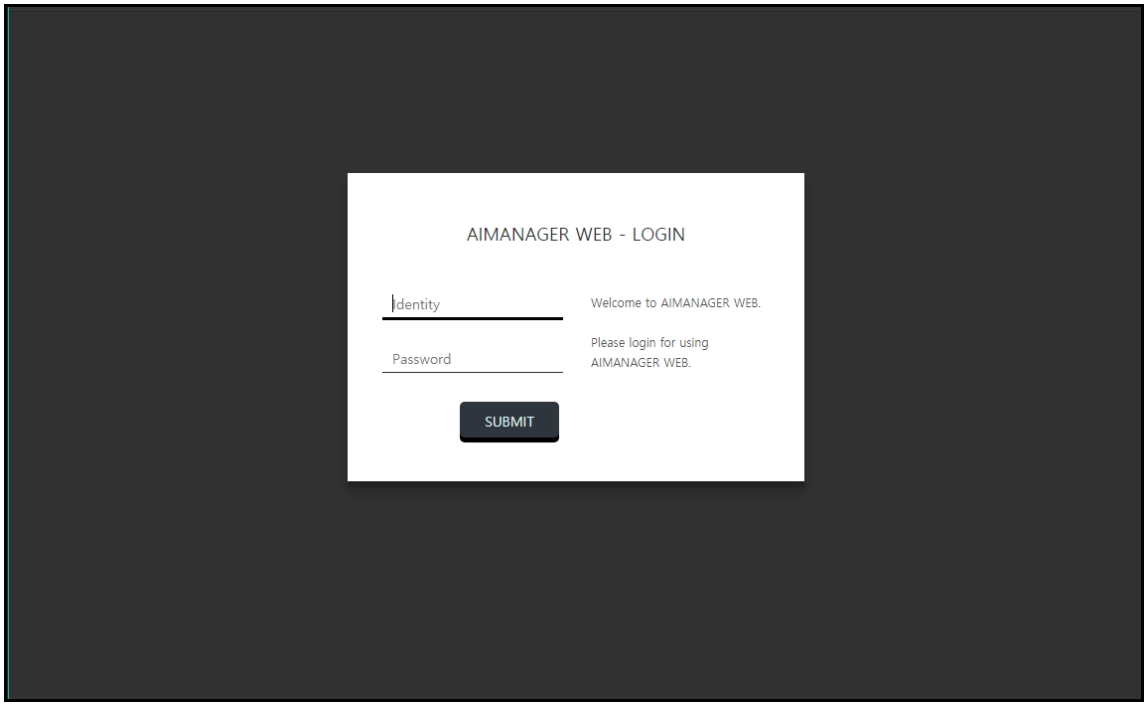
4.2. Patch

4.2.1. Patch

This update patch process explanation works the same for APPLIANCE and Virtual Edition.

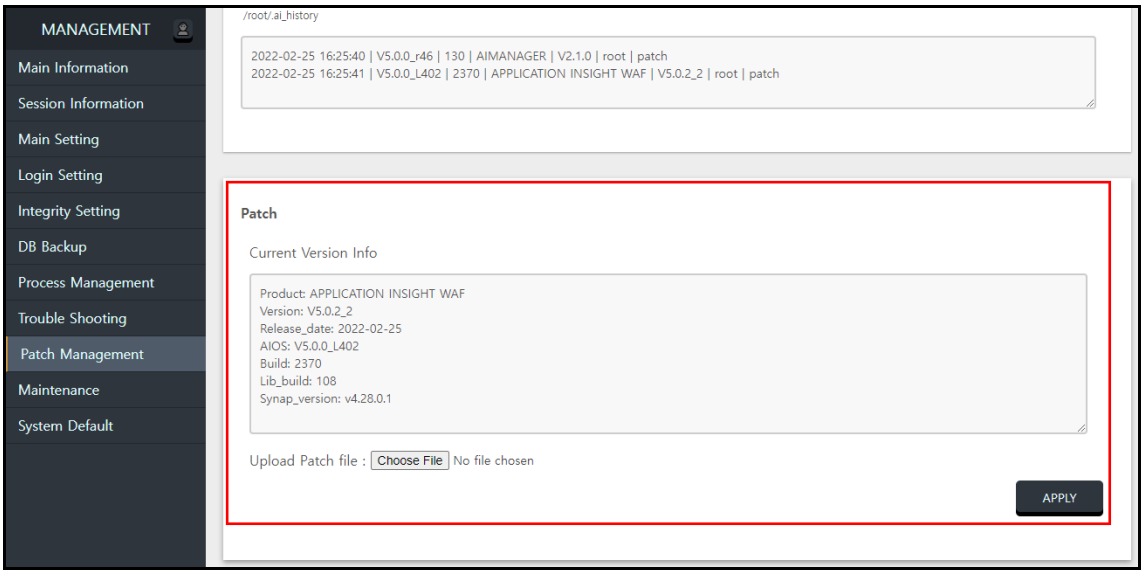
① Access AI Manager Web.

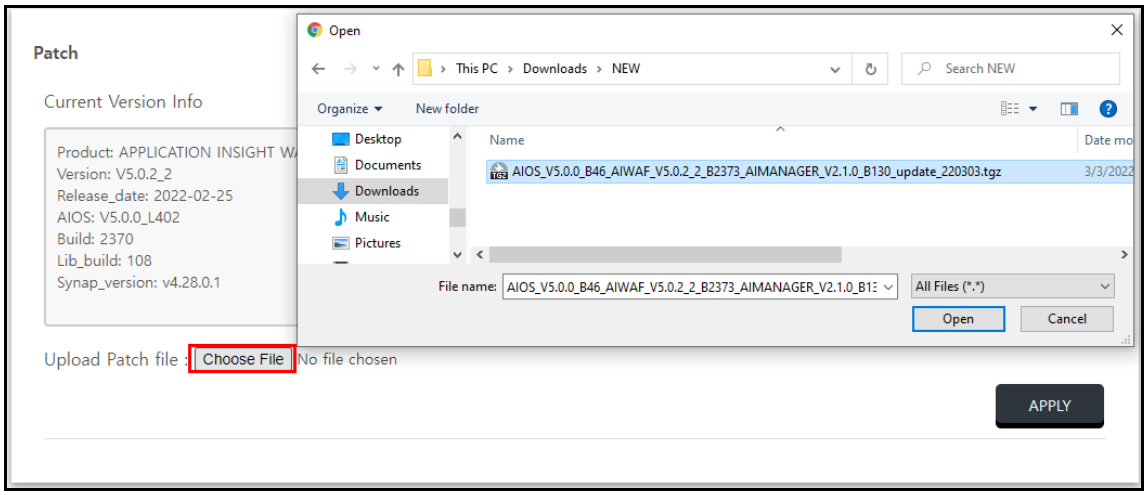
- Enter the AI Manager Web URL (https://[AIWAF IP]:333).
- Log in to AI Manager Web.



② Upload the patch file in Patch Management > Patch.

- Select a file in Patch Management > Patch.

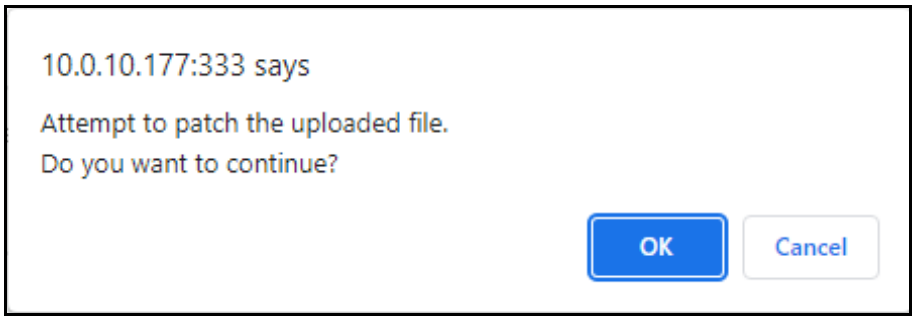




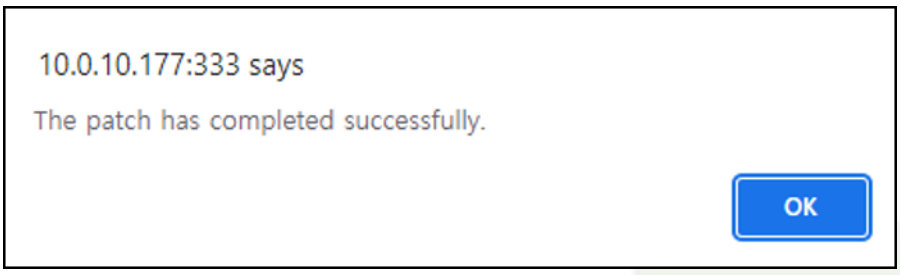
③ Proceed the patch.

- Check the selected file and click on “APPLY” button to proceed the patch.

- The patch message will pop up. Please click on “OK” button if proceed the patch.



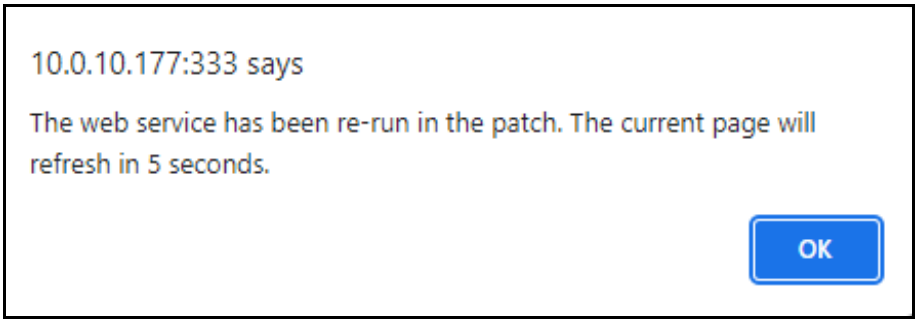
- When the patch is completed, the patch complete message will pop up. To finish the patch process, click on “OK” button.



※ Sometimes The web service of AI Manager Web is re-run in the patch.

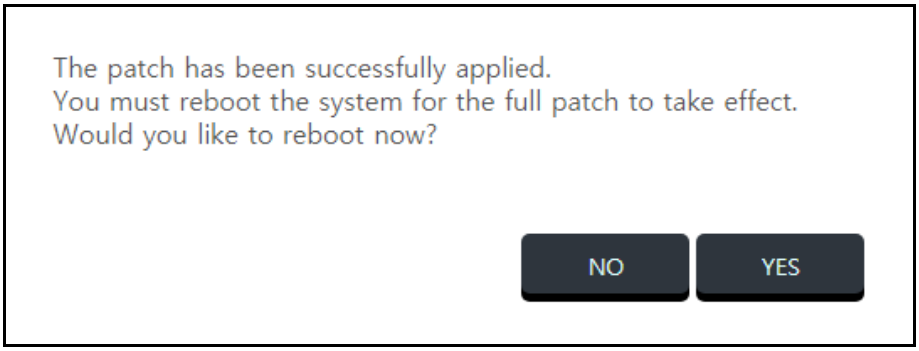
The page refreshed but patch in progress.

In this case, Reboot is not activate automatically.



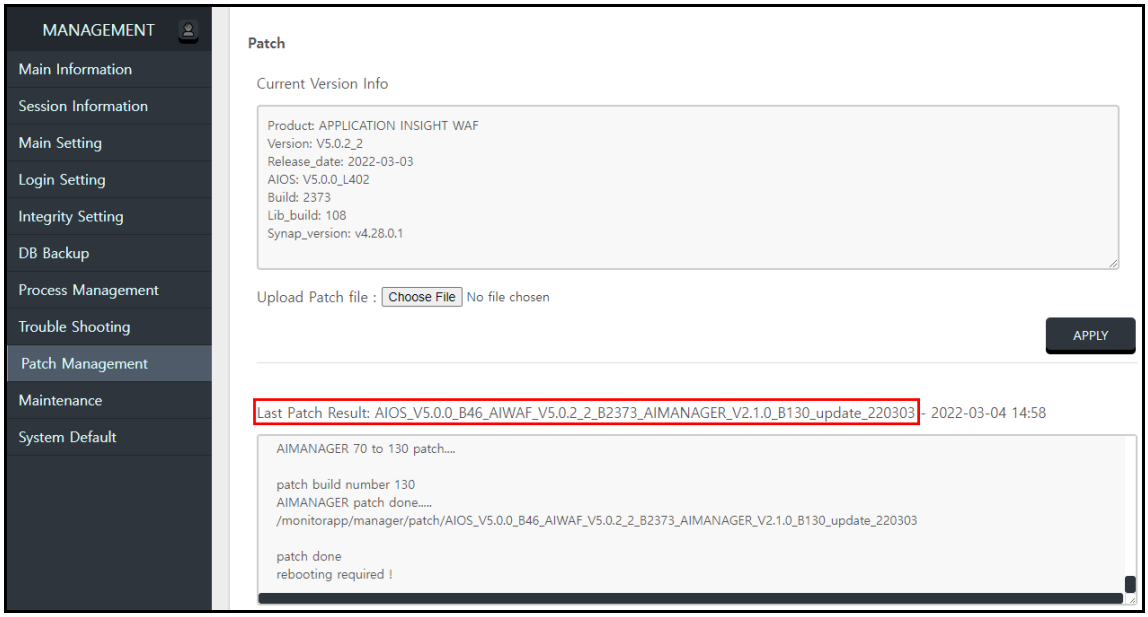
④ Reboot the system.

○ The reboot message will pop up. Click on “YES” button to reboot the system.
(Please reboot the system for proper operation of the product.)



⑤ Check if the patch has completed successfully in Main Information > Product Version Detail after the patch is completed.

- Check Product Version Detail in Main Information > Product Version Detail.



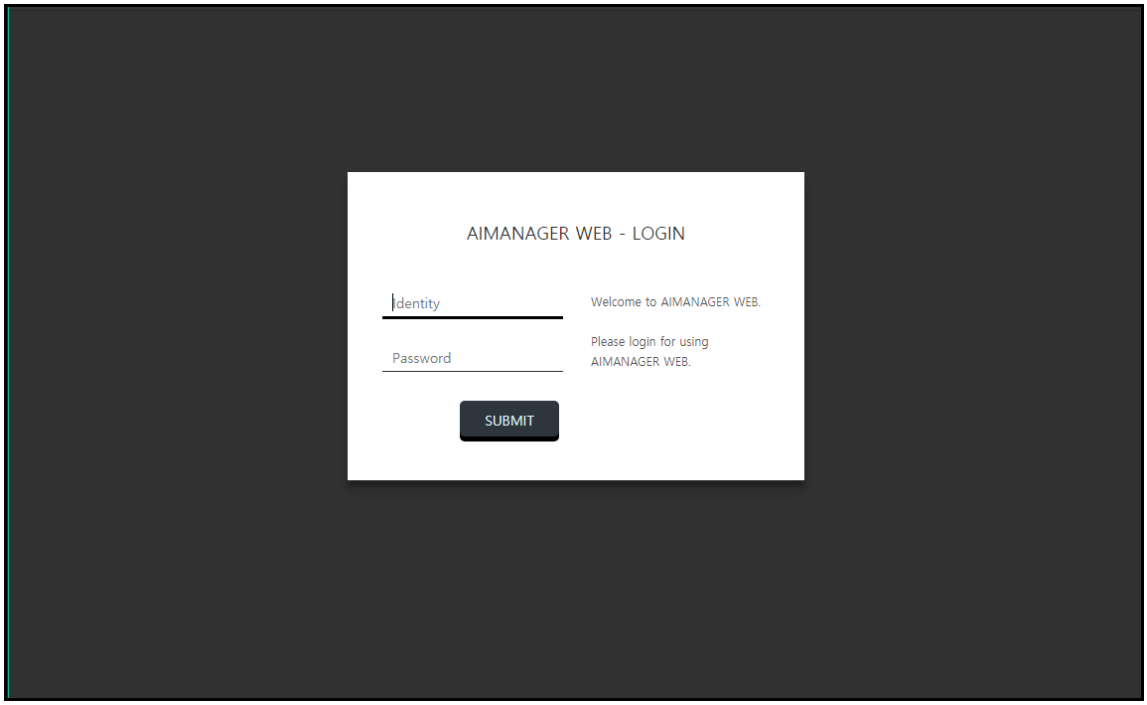
4.2.2. Restore

If you want to restore the system to the previous system state after patch the system, you can restore the system by proceeding Restore.

This Restore process explanation works the same for APPLIANCE and Virtual Edition.

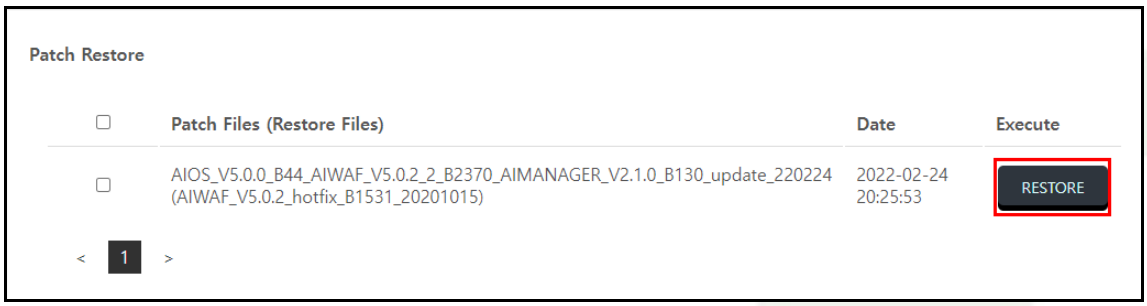
① Access AI Manager Web.

- Enter the AI Manager Web URL (https://[AIWAF IP]:333).
- Log in to AI Manager Web.



② Check the patch file to restore.

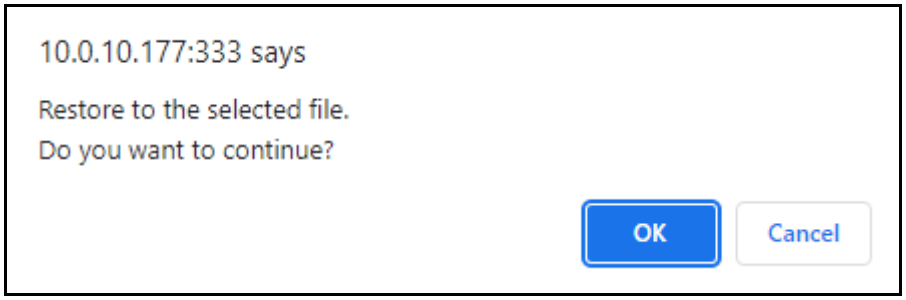
- Check the patch file to restore in Patch Management > Patch Restore.
- When click on “RESTORE” button, AIWAF will be restored to V5.0.2 from V5.0.0_2.



✓ AIOS is excluded from the restoration.

③ Proceed the Restore process.

- The Restore message will pop up. Please click on “OK” button if proceed the restoration.



④ When the restoration is completed, check whether the restoration is successful in Main Information > Product Version Detail.

- Check the restoration result in Main Information > Product Version Detail.

5. Patch Contents

5.1. Added Features

- Add ‘Port’ option in Protected Web Server > Protocol HTTPS > SSL Information > SSL Automatic selection of versions and algorithms.

- Protected Web Server > Protocol HTTPS supports Mutual TLS, OCSP Stapling.
  - Add ‘TODO’ on Protected Web Server > Protocol HTTPS.
  - Depending on the result of "TODO" setting, different "Extension function" will be provided.

    ① When select ‘Client’ in ‘DOTO’
    - Request Client Certificate (= Mutual TLS)
    - Server HTTP/2 Support

TODO	◉ Client	○ Server
Extension function	☐ Request Client Certificate	☐ Server HTTP/2 Support

    ② When select ‘Server’ in ‘DOTO’
    - TODO (OCSP Stapling)
      - ※Only supported on TP, SYN TP
    - Verify Server HTTP/2 Support

TODO	○ Client	◉ Server
Extension function	☐ TODO	☐ Verify Server HTTP/2 Support

  - Deleted **“HTTP/2 Use/Not use”** options, Depending on the existing settings, it's set up in two cases below.

    ① If the previous setting is “HTTP/2 Use”
    - TODO – ‘Server’
    - Server HTTP/2 Support – enabled

    ② If the previous setting is “HTTP/2 Not use”
    - TODO - Client
    - Extension function – all disabled

- (Reverse Proxy) Add ‘Copy information of Web server’ in Protected Web Server > Protocol HTTPS.

- Support 40G NIC on Y20 model.
  - Support models : 1000_Y20, 2000_Y20, 4000_Y20, 8000_Y20
    - ✓ Add option as ‘Q’ in make_model.sh

```
is valid integer type
 ===================================
| LCD  |  S5  |  S6  |  S7  |  S8  |
|      |      |      |      |      |
|      |---------------------------|
| Mgmt |  S1  |  S2  |  S3  |  S4  |
|      |      |      |      |      |
 ===================================

Enter use slot count (1~8) : 1

Enter the slot number : 1
Enter the NIC type of slot 1 (Q, G, T, F) : Q
Do you want to use bonding interface? (yes or no) : no
```

```
#!/bin/sh

MODEL=AI_1020_2Q

EXTERNAL_IF=S1E1
INTERNAL_IF=S1E2
MANAGER_IF=mgmt
HA_IF=ha
ASYNC_IF=

NETWORK_DRIVER1="igb.ko mapping_device=mgmt,ha RSS=4,4"
NETWORK_DRIVER2="i40e.ko mapping_device=S1E1,S1E2"
~
```

- Add new policies & options
  - Admin policy > DoS policy > Slow Read attack detection
  - Admin policy > URL Rewriting policy
    - ✓ URL Rewriting policy > URL Rewriting request rule
    - ✓ URL Rewriting policy > URL Rewriting response rule
  - Add Geo IP option on Domain policy > Group/Block page settings > IP group

- Add options in httpgw.conf
  - sslkeylog
    - ✓ directory /monitorapp/debug/
  - piilog_masking : masking reason on detection log details when the action of personal information policy are detect.

- Add STARTTLS options in Configurations > System Settings > Mail Settings > Mail protocol
  - STARTTLS added for Mail Server that is not support TLS.

- Add option in 'Domain Management' for Proxy Protocol.
  - Add a header has name of **'PROXY'** in **Policy Settings > Domain Management > Origin IP header identification** to identificate Proxy Protocol.

- Add 'IP Blacklist/Whitelist' buttons for 'Origin IP' in **Log analysis > Detection log view > Log detail view**

5.2. Changed Features

- Improve functions in Domain policy
  - Policy settings > Domain management
    - ✓ Expand code range in Error Page Cloaking > Application code (100-999)

- Improve health_check process
  - Change to Optional logic that restart the httpgw process.

- Improve Detection log
  - Improve Log analysis > Detection log view > Show only interest logs
    - ✓ Change to **interest logs** output regardless of the Period.

  - Improve output of detect reason in Log analysis > Detection log view > Log detail view
    - ✓ Add “View detection pattern string” in Request/Response fields that opened pop-up window.

- Add options in Policy settigns > Default settings > System overload auto bypass setting
  - Add “The current status” option that prints bypass status.
  - Add option for bypass off manually.

- Improve ESM
  - Configurations > Log management > ESM settings
    - ✓ Add “MAX: bytes” on “Request/Reply/Audit Log” (MAX: 60,000 bytes)
    - ✓ Add “Reply data” in “Detection log format”
      - It only works for response based policy
    - ✓ Expand length of “Distinguishment ID” : up to 30 bytes

- Improve the function that Protected web server
  - (Reverse Proxy) HTTPS web server settings
    - ✓ Disabled “path” on URL
    - ✓ The values of “path” have to delete, when it has values.
    - ✓ Reason for disabled
      - AIWAF cannot distinguish the target that have “same host + path”.
      - It is because “Protected web server” is selected with “SNI” on AIWAF. And “SNI” does not have “path”.

- Improve Admin policy > URL access rule
  - Add confirm message when Client IP or Server URL have default values.

- Others
  - Improve Debug_filter that logs more information.
  - Add functions of html_entities decording on httpgw.
  - Reduce the time of “power off” progress.(=reduce reboot time)
  - Update the cipher_suite_table in HTTPS Web server Settings.
  - Optimize Postgresql options in postgresql.conf.
  - Update Synap: v4.28.0.1
  - Add SSL_OP_NO_RENEGOTIATION to blocking HTTPS reuse.

- Add “FAN check” for AI-200_Y17 model.
- Add “POWER check” for AI-200_Y20 model.

5.3. Bug Patches

- Fix a bug that httpgw process is abnormally stopped when the specific situations

- HTTP
  - Fix a bug that fail to connect specific HTTP/2 pages on IE.
  - Fix a bug that overload CPU when use SSL Offload on specific situations.
  - Fix a bug that fail download chunked data that has huge sizes.

- AWS Auto Scaling
  - Fix a bug that fail Policy synchronization in Scale-Out.
  - Fix a bug that fail Configurations synchronization in Scale-Out.
  - Fix a bug that fail to detecting in Scale-Out with abnormal pattern data.

- Network
  - Fix a bug that fail to Blocking Slow DoS attack in Mirroring mode.
  - Fix a bug that print abnormal frames of Administrator settings with IPv6 GUI.
  - Fix a bug that forwarding packets to kernel when AIWAF received packets have AIWAF's MAC address.

- The functions in Domain policy
  - Policy settings > Domain policy > Domain
    - ✓ Fix a bug that occurs error when access Domain policy with the browser's developer tool.
    - ✓ Fix a bug that detect wrong in 'Malicious code diffusion detection'.
    - ✓ Fix a bug that set abnormally Exception URL in 'Directory access detection'.
    - ✓ Fix a bug that cannot understand extention of '.ai' files as 'pdf' in 'Malicious file upload detection'.
    - ✓ Fix a bug that detect abnormally 'Server URL' in 'Threshold-based security policy> Login fraud attempt'.
    - ✓ Fix a bug that fail to transfer block pages with 'JSON overflow detection'.
    - ✓ Fix a bug that active 'Web Socket detection' when Operation mode is 'Policy Bypass mode'.

- The functions in Protected web server
  - Policy settings > Admin policy > Protected web server
    - ✓ (Reverse Proxy) Fix a bug that fail to lookup host alias on specific situations.
    - ✓ (Reverse Proxy) Fix a bug that fail to Server Load Balancing on specific situations.
    - ✓ (Reverse Proxy) Fix a bug that fail to match Domain ID for 'host' header with 'port'.

- Detection log view
  - Log analysis > Detection log view
    - ✓ Fix a bug that execute scripts in dectection log on specific situations.
    - ✓ Fix a bug that fail to add 'port' of Exception URL when it takes "Exception URL registration" button in Detail detection view.
    - ✓ Fix a bug that disappear 'body of request' in detection log that because response based policy.

- ✓ Fix a bug that fail to output Detection reason in Log detail view with Directory access detection.

- Policy synchronization
  - UI Policy settings > Default settings > Policy synchronization settings
    - ✓ Fix a bug that print non-sync when success Policy synchronization in specific environments.
    - ✓ Fix a bug that sync the Passive Mirror settings.

- VE Environment
  - Fix a bug that can't set DHCP IP on NCP(Naver Cloud Platform)

- Others
  - Fix a bug that program integrity check failed when update GeoIP DB.
  - Fix a bug that had fault on aicc_agent intermittently.
  - Fix a bug that som items in Policy setting report are printed incorrectly.
  - Fix a bug that memory leak occurs when checking(use 'cat' command) a specific file on CLI.
  - Fix a bug that restarted intermittently when activate Web Caching.
  - Fix a bug that do not print Blacklist when activate single_client_ip option.