# Breezeway Fire.ONE V1.0
# User Manual V1.0

SSNC Co., Ltd.

# Document Information

| | |
|---|---|
| **Document Title** | Breezeway Fire.ONE V1.0<br>User Manual V1.0 |
| **Revision Number** | Rev.1.3 |
| **Product Name** | Breezeway Fire.ONE V1.0 |

# Revision History

| Revision Number | Date of Amendment | Amendment Details | Author |
|---|---|---|---|
| Rev.1 | June 10, 2025 | Initial Author | Kim Gu-won/Lee Shin-woo |
| Rev.1.1 | 2025.08.29 | Phase 1 Revision | Platform Research Team |
| Rev.1.2 | 2025.09.24 | Product Feature List Revision | Kim Gu-won |
| Rev.1.3 | 2025.12.02 | Reference and Revision of Defect Report | Platform Research Team/Future Technology Research Team |
| | | | |

# 1. Product Overview

## 1.1 Overview

Manually managing firewalls leads to persistent **user inconvenience, operational inefficiency, and security** risks.
Fire.ONE is a **policy management automation** solution designed to revolutionize and improve this manual workflow structure.
It digitizes and automates the entire firewall operation process**, eliminating human error, reducing operational complexity, and significantly enhancing security**.

## 1.2 Fire.ONE Product

Fire.ONE automates every step of firewall policy operations, **fundamentally eliminating the inefficiencies, delays, errors, and security risks inherent in manual management**.

### 1.2.1. Core Value of Fire.ONE Automation

1) User-Friendly Automation

- Fully automated processing from policy request → approval → application
- Automatic calculation of policy application time and real-time status display
- Automatic policy synchronization upon IP changes, eliminating the need for re-application

2) Maximized Operational Efficiency

- Systematize manual Excel and email tasks to eliminate repetitive work and user errors
- Reduce operational workload through automated policy approval and deployment
- Improve operational quality with automated policy structure analysis and organization

3) Enhanced Security

- Automatic detection and blocking of unnecessary policies
- Automatic verification of security-violating policies and compliance adherence
- Automatic generation of audit response reports

### 1.2.2. Firewall Policy Auto-Application Process

- **Application Information Analysis:** During application creation and approval, application information is analyzed in real-time to perform formatting checks per firewall (IP, Port, Protocol format checks).
- **Policy Optimization and Auto-Fixing:** Automated task list classification and rule generation per operator account. Optimizes policies through duplicate checks of application information and comparison with existing firewall policies, performing Auto Fixing (grouping, merging, etc.).
- **Rule Auto-Application:** Rules are automatically applied to each firewall manufacturer's tool via scheduled tasks.
- **Application and Rollback:** Policy application occurs either immediately or via scheduled application. Rollback is possible if an application is incorrect.

### 1.2.3. Firewall Policy Security Verification and Analysis (Analyzer)

- **Pre-Analyzer (Pre-Application Verification):** Prevents the application of unnecessary rules (duplicate rules, unused rules) through pre-verification.
- **Analyzer (Post-Application Verification):** Performs policy security verification and diagnosis by checking the status of unnecessary policies (duplicate policies, unused policies) before and after application.
- Generates reports evaluating policy utilization, compliance with security standards, and service safety through analysis of base rule status, duplicate/permanent policy analysis, and service association analysis.
- Continuous improvement is enabled through diagnostic section-specific scoring and vulnerability remediation guidance.

### 1.2.4. Topology View

Fire.ONE's Topology View visually represents networks and firewalls, enabling users to grasp network structures and policy flows at a glance and analyze risk segments.

- **Network Topology Diagram Creation:** Create a network topology diagram resembling the actual operational environment, including network devices and firewalls. Networks are displayed divided into Zones, allowing you to intuitively identify connection relationships and risk points per network.
- **Firewall Path Analysis:** Select the source and destination on the topology, and it automatically calculates the path through each firewall segment, visually displaying the actual traffic flow.

- **Risk Analysis for Policies:** Analyzes applied policies based on the calculated path, scores the risk level per policy and per path, and provides an analysis report measuring compliance status and the risk level per segment.

### 1.2.5. Automatic Policy Application Based on Risk Analysis

1) Traffic Analysis
   - Collects and visualizes firewall traffic by time period and service.
   - Detects anomalies (e.g., traffic spikes, concentration in specific segments) compared to normal patterns.
2) Risk Assessment
   - Classify detected traffic based on attack type, service criticality, and historical records.
   - Presents the results as threat type/severity distributions (e.g., pie charts) to show at a glance which areas are vulnerable.
3) Policy Generation and Implementation
   - For segments identified as high-risk traffic through analysis, it automatically calculates necessary blocking/permission criteria and generates the content as firewall policies for deployment to devices.
   - Operators can review and approve the proposed policies, enabling rapid reinforcement of defense policies without manual intervention.

### 1.2.6. Compliance Support

- **Supports compliance with various international/domestic standards** (e.g., ISO/IEC 27001, GDPR, NIST SP, Basel-II, BSI 200, Financial Services Commission FSI, Personal Information Protection Act, etc.).
- You can generate compliance reports by selecting firewalls or policies.
- Standardize and manage security scores within Fire.ONE, providing customized management per compliance requirement.

### 1.2.7 Fire.ONE Role-Based Work Processes

| | Step | Task Description | Detailed Description |
|---|---|---|---|
| **Engineer** | 1 | OS Installation and Initial Setup | Package configuration, account/permission setup |
| | 2 | Fire.ONE and DB Installation | |

| | | | |
|---|---|---|---|
| | 3 | Register Firewall Device Information in Fire.ONE | Firewall IP/Account/Key Registration, Device Integration Configuration |
| | 4 | Compliance Storage | Internal Security Rule and Policy Standard Storage |
| | 5 | Topology Creation | Network zone configuration, service flow modeling |
| | 6 | HR information integration and Admin account setup | HR Integration, Administrator Account Creation |
| **Administrator** | 7 | User Menu Access Group/Page Permission Settings | Permission Group Configuration, Assign Work Groups/Approval Groups |
| | 8 | Custom Object Settings | Register frequently used IP/port/server information |
| **User** | 9 | Firewall Request | |
| **Approver** | 10 | Firewall Approval and Authorization | |
| **Firewall Manager** | 11 | Firewall-Specific Policy Commit/Non-Reflection Processing | |
| | 12 | Security Analysis and Report Review | |
| | 13 | Rollback Request and Application | |

## 1.3 Product Information and Supplier Information

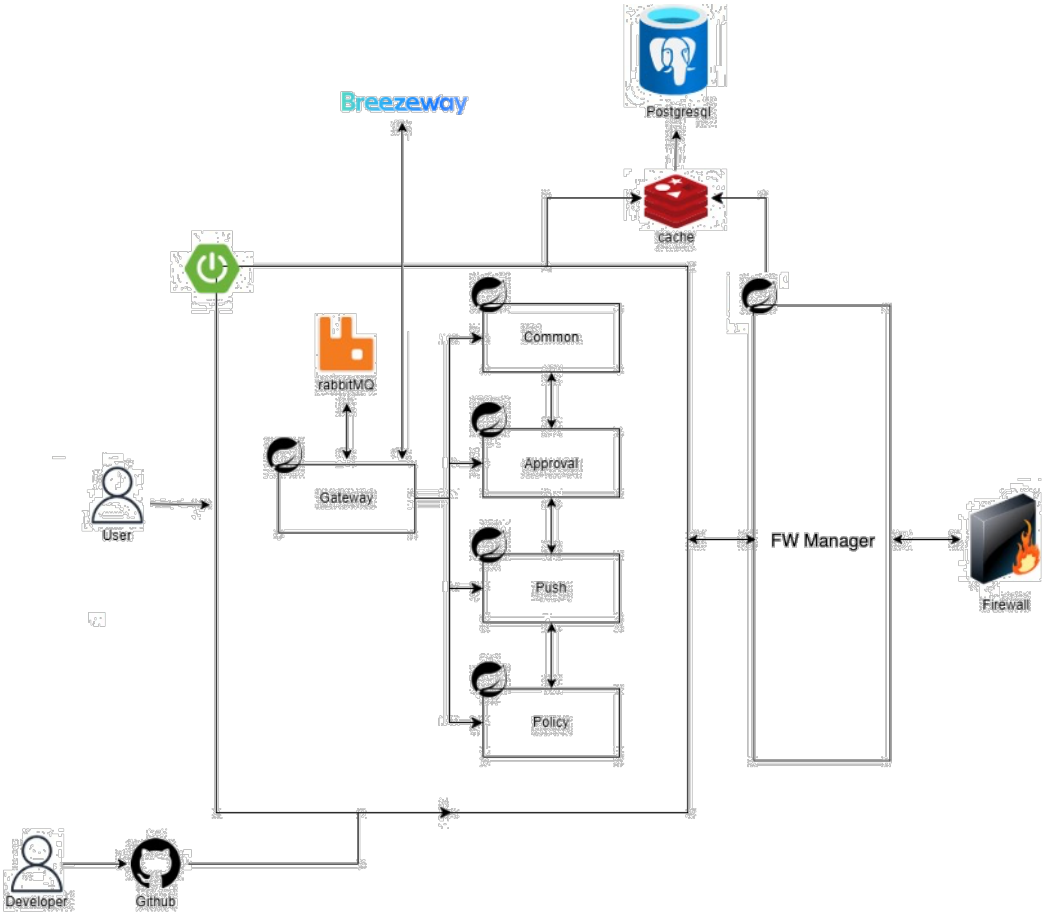
| **Product Name** | **Firewall Integrated Management System<br>Breezeway Fire.ONE V1.0<br>User Manual V1.0** |
|---|---|
| **Version** | V1.0 |
| **Components** | 1) Fire.ONE V1.0 - Operating System<br>2) Fire.ONE V1.0 - Diagnostic/Analysis System |
| **Release Date** | October 1, 2025 |
| **Manufacturer and Supplier** | SSNC Co., Ltd. |
| **Manufacturer and Supplier Address** | Address: 43 Iljik-ro, Gwangmyeong-si, Gyeonggi-do, GIDC Building C, Units 1114-1119<br>Website: https://www.ssnc.co.kr/ |

| | |
|---|---|
| | Phone: 02-6925-2550<br>Email: sales@ssnc.co.kr<br>Fax: 02-6925-2551 |

## 1.4 Copyright Policy

- This product is a work protected by copyright law and may not be reproduced or distributed. In principle, the copyright belongs to SSNC Co., Ltd.

## 1.5 Product Operating Environment



Classification

| Category | | Fire.ONE V1.0 - Operating System | Fire.ONE V1.0 - Diagnostic/Analysis System |
|---|---|---|---|
| Software | OS | Linux (Red Hat 9 or higher, Ubuntu 24 or higher) | |
| | 3rd Party | • DBMS:<br>- PostgreSQL 14.1<br>• JDK<br>- OpenJDK 17 or later<br>• WEB<br>- jQuery 3.7.1<br>- AdminLTE 3.2.0<br>- Chart.js 3.1.1<br>• SpringBoot<br>- 3.3.2 | • WEB<br>- React 19.2.1<br>- Next.JS 16.0.8<br>- Rechart 3.5.1<br>• Storage<br>- Elasticsearch 9.1.1 |
| Hardware | Specifications | Based on Fire.ONE Server Configuration 1.5.1 | |

### 1.5.1 Fire.ONE Server Configuration Standards

Fire.ONE system specifications for CPU, memory, and storage (storage space) vary as follows depending on the number of servers to be processed.

| Scale (Number of Servers) | CPU (vCore) | Memory | Storage | Remarks |
|---|---|---|---|---|
| **50 units** | 8 cores | 32GB | 600GB | |
| **100 units** | 16 cores | 48GB | 1TB | |
| **200 units** | 20 cores | 64GB | 1.2TB | |
| **300 units** | 32 cores | 64GB | 1.6TB | |
| **500 units** | 32 cores | 128GB | 3TB | |

Additional Considerations:

- **High-Performance Workloads:** For tasks such as **daily resource synchronization, rule analysis, and continuous compliance pre-checks**, we recommend configuring with double **the base specifications.**

### 1.5.2 Diagnostic (Log) Collection/Analysis Server Configuration Criteria

The log collection and analysis server is configured to handle **10,000 session logs per second**.

| Scale (Number of Servers) | CPU (vCore) | Memory | Storage | Standard |
|---|---|---|---|---|
| **50 units** | 16 cores | 32GB | 2TB | Based on 10,000 session logs per second |

## 1.6 Standards and Recommendations

1.6 Standards and Recommendations
The technical standards referenced during Fire.ONE development are as follows.

Data Communication Protocols:

- RFC 791 (IPv4),
- HTTP / HTTPS
- JSON Schema Draft 2020-12
- OpenAPI Specification 3.1
- RFC 5424 — Syslog Protocol

Cryptography:

- RFC 4634 - US Secure Hash Algorithms (SHA and HMAC-SHA)
- RFC 8017 — PKCS #1 (RSA Cryptography): RSA-OAEP(SHA256)
- SALT, NONCE

Database Encryption:

- PG Crypto Extension Module - Symmetric-key cryptography functions in OpenPGP format

Web

- Spring Framework, Spring Security, W3C (CSS/HTML)

SBOM

- CycloneDX

# 2. Product Details

## 2.1 Key Features

### 2.1.1 Key Services

This product is an integrated management system that enables the centralized management of multiple firewalls. The services provided to operate the integrated system are as follows.

- **Login**: A function that allows users to authenticate their identity by entering their ID and password and securely access the system
- **Electronic Approval**: A function that manages electronic approvals for firewall policies, from application to approval.
  (Related Menus: Request, Approval, Object)
- **Firewall Policy Management**: Functionality for managing submitted firewall policies
  (Related menus: Policy, Governance)
- **Dashboard and Report Generation**: A function that provides dashboards visualizing key metrics based on collected data and generates detailed reports
  (Related menus: Report, Diagnostic)
- **Asset (Equipment) Management**: Functions to query/manage network equipment such as firewall devices
  (Related Menu: Device)
- **Administrator**: Functions to query and manage various users accessing the software
  (Related menus: Workgroup Management, Permission Group Management, Role Group Management, Policy Status List)
- **Settings**: Functionality allowing users to directly configure/manage the software's overall default environment
  Related Menu: IP ACL, Menu Permission Settings, API Integration List)

### 2.1.2 Firewall Policy

In this system, "Firewall Policy" refers to the rules (ACLs) applied to the firewall and the entire process surrounding them—request, approval, and application. That is, it encompasses both of the following elements:

1) Network Perspective

Refers to firewall rules (ACL) that determine whether to allow or block specific traffic based on the following criteria:

- Source IP or IP range
- Destination IP or IP range
- Service/Port Information
- Protocol (TCP, UDP, ICMP)
- Operation Mode: Allow/Block

In other words, it means "a set of rules defining how specific traffic should behave under certain conditions."

2) Business Process Perspective

This concept encompasses the entire procedure required to apply firewall rule sets to an actual environment.

- Policy Application Details
- Supporting Documents (Security Request Form, Design Document, etc.)
- Pre-verification (compliance checks, duplicate policy check results)
- Approval and Sign-off History
- Commit/Rollback status on actual firewall equipment

In other words, it manages "the entire information flow of rules + requests + verification + approval + application as a single policy."

**Firewall Policy Main Menu**

1) Application Menu

- This menu enables integrated registration of policy requests for specific traffic (source/destination IP, service/port, protocol) across all associated firewalls.
- The Verify button performs duplicate rule checks and compliance checks.

2) Approval Menu

- Applicants can check the progress of policies they have applied for.
- Security personnel can review and approve policies submitted for their approval.

3) Policy Menu

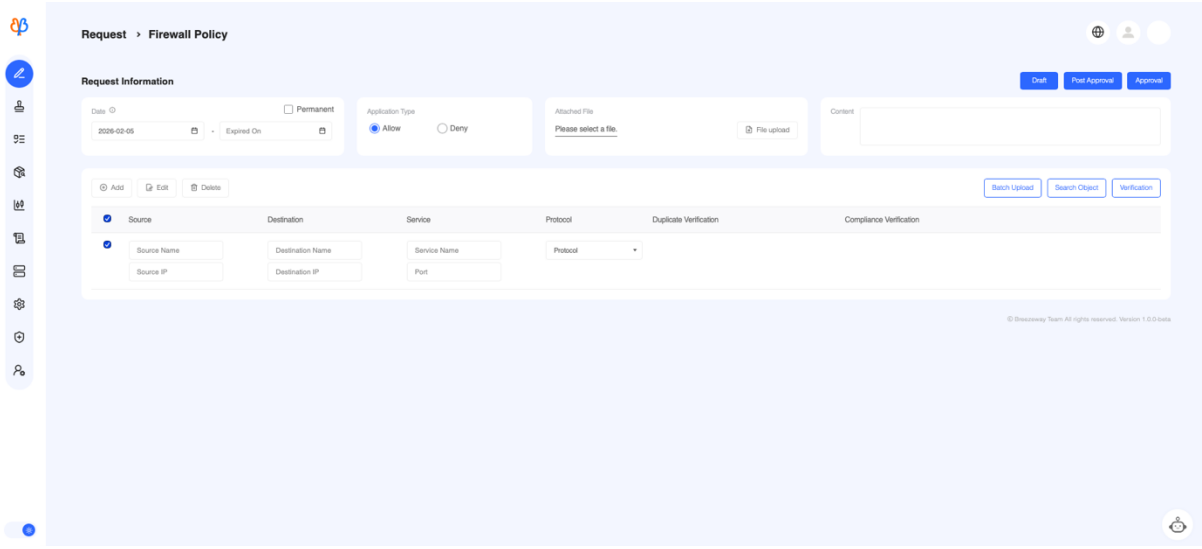
- This menu actually applies policies to the firewall.
- Approved policies can be committed to the firewall device by the

responsible personnel.
- The responsible person can check the policy status.

### 2.1.3 Firewall Policy Request

#### 1) Firewall Policy

This feature allows general users to submit applications for firewall policies. It not only handles simple applications but also provides pre-validation for entered policies, preventing incorrect information input or applications for security violation items in advance.

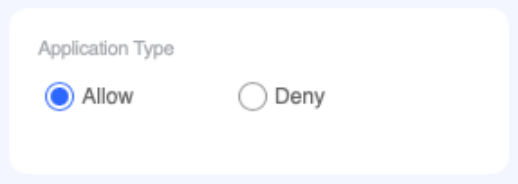



〈Firewall Policy Request Screen〉

#### 2) Attachment


This feature allows attaching documents (security request forms, work request forms, design documents, security review documents, etc.) to substantiate the basis for the required firewall policy when applying. Adding supporting documents enables verification during audits and provides reference material for approvers when assessing policy validity.

#### 3) Application Type




Select whether the requested policy allows (Allow) or blocks (Deny) specific traffic. This requires precise selection as it directly impacts the behavior of the generated firewall rule and the verification/approval process.

4) Temporary Save

This function allows you to temporarily save the application details you are writing. If there is temporarily saved data, you can retrieve the existing data when entering the firewall policy page. Temporary saving is one-time only; supporting documents are not saved.

5) Post-Approval

This function allows applying the policy to the firewall without going through the approval process. When Post-Approval is selected, the policy is urgently applied to the firewall. Additionally, un-submitted approval items are processed as 'Unsubmitted Approvals' and moved to the 'Unsubmitted' folder, where you can generate submission documents from that menu. However, if pre-verification fails, use of this function is restricted.

6) Approval

This function applies firewall policies after processing the standard approval procedure. If the approval function is selected, you will be directed to the approval submission screen to utilize electronic approval. However, if pre-verification fails, use of this function will be restricted.

7) Batch Upload

Uploading the Excel (.xlsx) template file provided on the web allows you to register multiple application details in bulk.

8) Object Search

Firewall operators can retrieve predefined objects for use during the application stage. This allows general users to easily apply firewall policies without needing precise technical knowledge.

- Address Object - Predefined addresses can be used as source or destination.

- Service Object - Predefined services can be used with specified service and protocol information.
- System Object - Predefined addresses and services can be used with specified information.
- Group Object - Predefined group information can be used.

* Service objects are used only for services.

9) Verification

This feature automatically checks the firewall policy information entered by the system. Users can use the verification function to check for input errors or security violations in advance.

| Validation Items | Role | Purpose |
|---|---|---|
| **Duplicate Verification** | Verify conflicts or duplication with existing completed policies | Prevent policy duplication, manage policies/prevent security incidents |
| **Verify compliance** | Verify compliance with regulations, security policies, and prohibited zones | Verify compliance with internal and external security regulations |

- Duplicate verification

○ Function Purpose

Verifies whether a new policy has identical conditions to an existing firewall policy.

○ Verification Items

- Source IP/range match
- Destination IP/Range Match
- Port matching
- Protocol match
- Action (Allow/Deny) Match

○ Validation Error Messages and Solutions

| Error Message | Meaning | Resolution |
|---|---|---|
| **[0034] Service is None or Invalid** | Service/port value is invalid | Must be a valid service/port value between 0 and 65535 |
| **[0036] Source is None** | The source IP is not in IPv4 format or is not registered in the address object | Use a valid IPv4 format |

| | | |
|---|---|---|
| **[0038] Destination is None** | Destination IP is not IPv4 or is not already registered in the address object | Use a valid IPv4 format |
| **[0041] Source, Destination is all any** | Both source IP and destination IP are set to any, resulting in an overly open state | Change either the source or destination to a specific IP address |
| **[0042] Firewall Path List is Empty** | The requested traffic does not have a valid path | Verify the requested traffic path is correct and revalidate |
| **[0043] FromIP is null** | The source IP lacks routing information for its IP range in the firewall routing data traversed | The source IP is likely incorrect; verify the routing information and revalidate |
| **[0044] ToIP is null** | The destination IP lacks routing information for that IP range at a specific firewall in the firewall routing information it traverses | The destination IP is likely incorrect. Verify the routing information and revalidate. |
| **[0054] ExpireName is None** | The expiration date format is invalid. | Verify that the application was submitted through the proper application page |
| **[0091] FromIP and ToIP are the same** | The source IP and destination IP exist on the same interface, meaning they are within the same network/subnet/Zone. Therefore, the firewall policy does not apply. | This traffic cannot be applied. It does not match the firewall policy. |
| **[0200] Dup Ruleset fw_name = {firewall name} AND rulebase_id = {rulebase ID}** | For traffic applied with Allow, a policy exists where the source IP, destination IP, service, and protocol all match (duplicate for the rule policy ID in the rule policy for a firewall with a specific firewall name). | Since this traffic is already managed by an allow policy, apply an exclude policy for this traffic. |
| **[0201] Dup Ruleset fw_id = {firewall ID} AND rulebase_id = {rulebase ID}** | For traffic applied for as allow, a policy exists where the source IP, destination IP, service, and protocol all match (duplicate for the rule | Since this traffic is already managed by an allow policy, apply an exclude policy for this traffic. |

| | | |
|---|---|---|
| | policy with the rule policy ID on a firewall without a firewall name) | |
| **[0202] Deny Ruleset fw_name = {firewall name} AND rulebase_id = {rulebase ID}** | For traffic applied with Deny, a policy exists where the source IP, destination IP, service, and protocol all match (duplicate for the rule policy with the rule policy ID on a firewall with a specific firewall name). | Since this traffic is already managed by a deny policy, apply an exclusion policy for this traffic |
| **[0203] Deny Ruleset fw_id = {firewall ID} AND rulebase_id = {rulebase ID}** | For traffic applied with Deny, a policy exists where the source IP, destination IP, service, and protocol all match (duplicate for the rule policy with the rule policy ID on a firewall without a firewall name) | Since this traffic is already managed by a deny policy, apply an exclusion policy for this traffic. |

- Compliance Verification

○ Function Purpose

- This feature preemptively checks for violations of internal and external security regulations, blocking risks at the policy application stage.

○ Verification Items

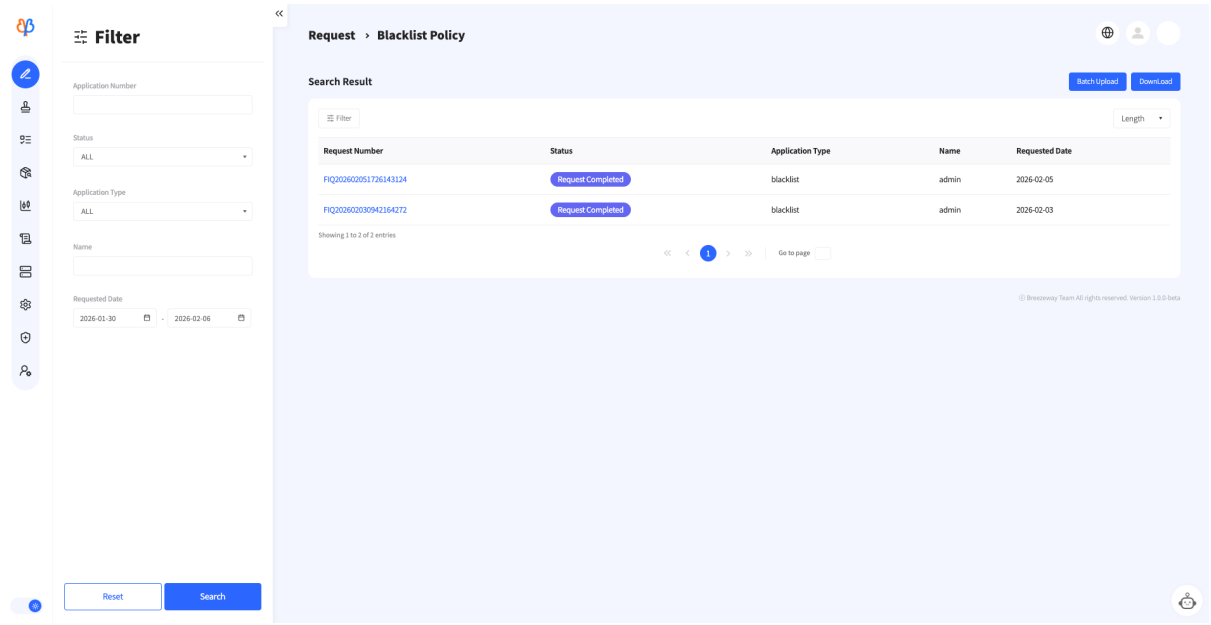
- Compliances added under the 'Governance 〉Compliance' menu

○ Verification Error Message

- Fail =〉 Traffic filtered out by registered compliance rules and therefore unusable

10) Blacklist Policy

Blacklist policies are applied separately from standard firewalls. You can view existing blacklist applications through the menu.



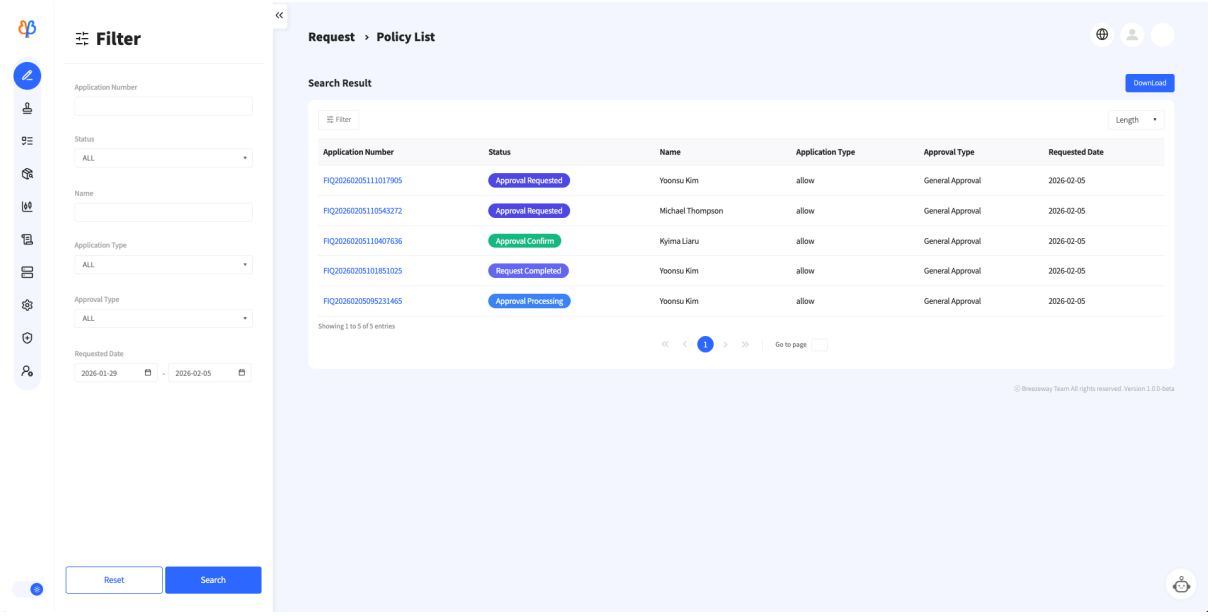

〈Blacklist Policy Inquiry Screen〉

11) Upload

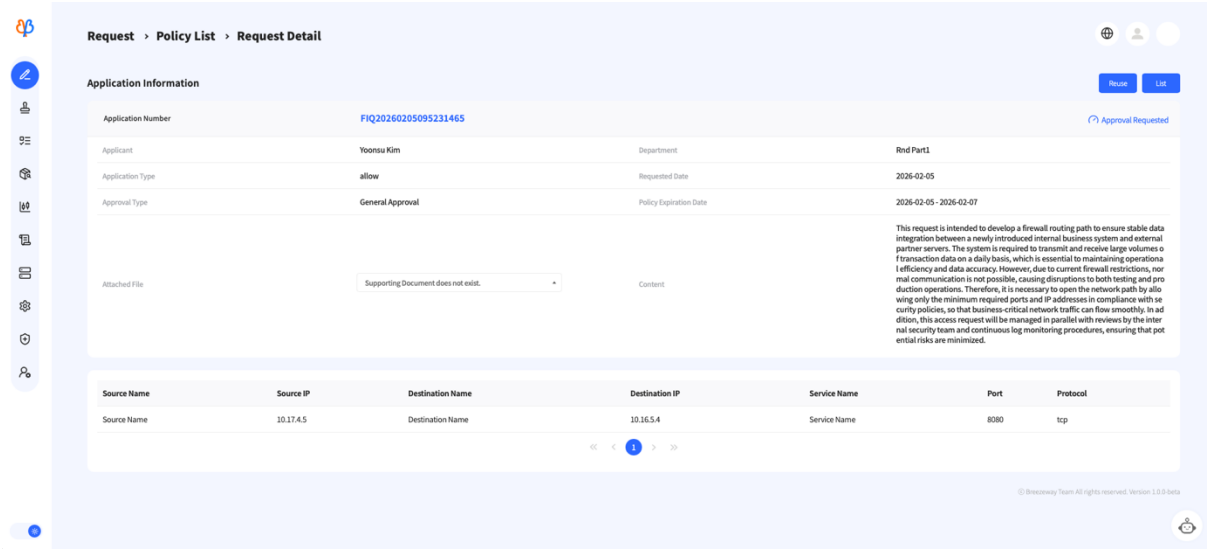
Uploading the Excel (.xlsx) template file provided on the web allows you to batch register multiple blacklist application details.

12) Policy List

Users can view the status and processing steps of previously submitted firewall policies. Clicking an application number in the policy list displays the detailed information for the selected policy. However, user verification results conducted during the application stage cannot be viewed.




〈Application Policy List Screen〉




〈Application Policy Details Screen〉

- Status Bar

Intuitively check the processing stage of the selected policy.

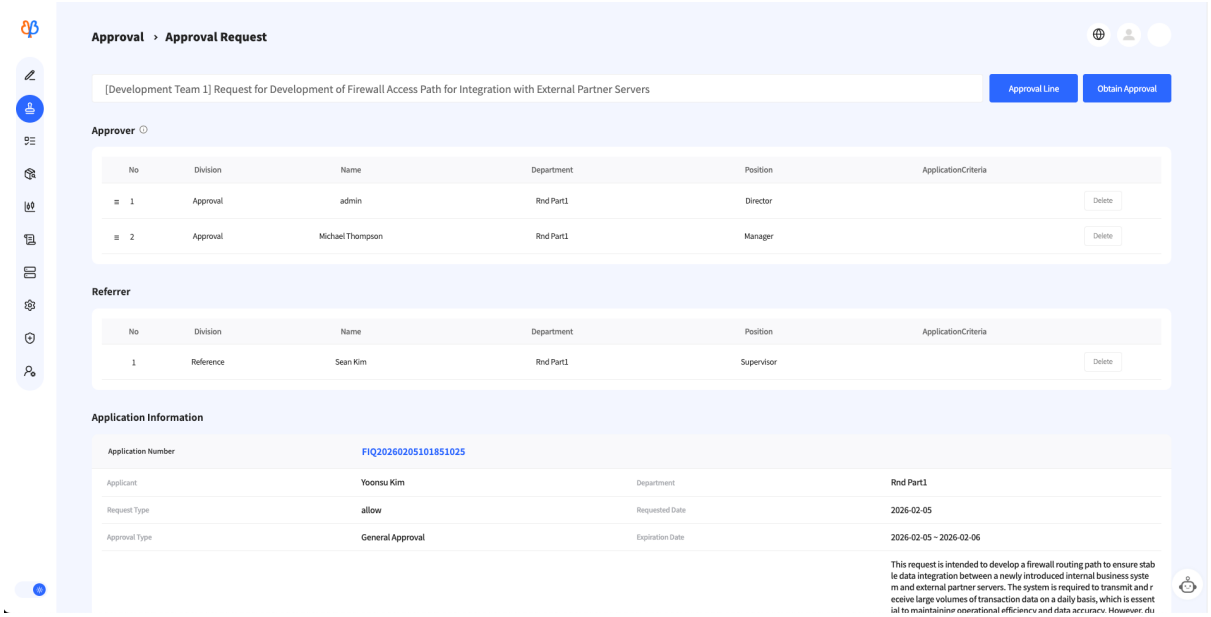
- Reuse

The reuse feature automatically applies existing policies to the application page, reducing repetitive input.

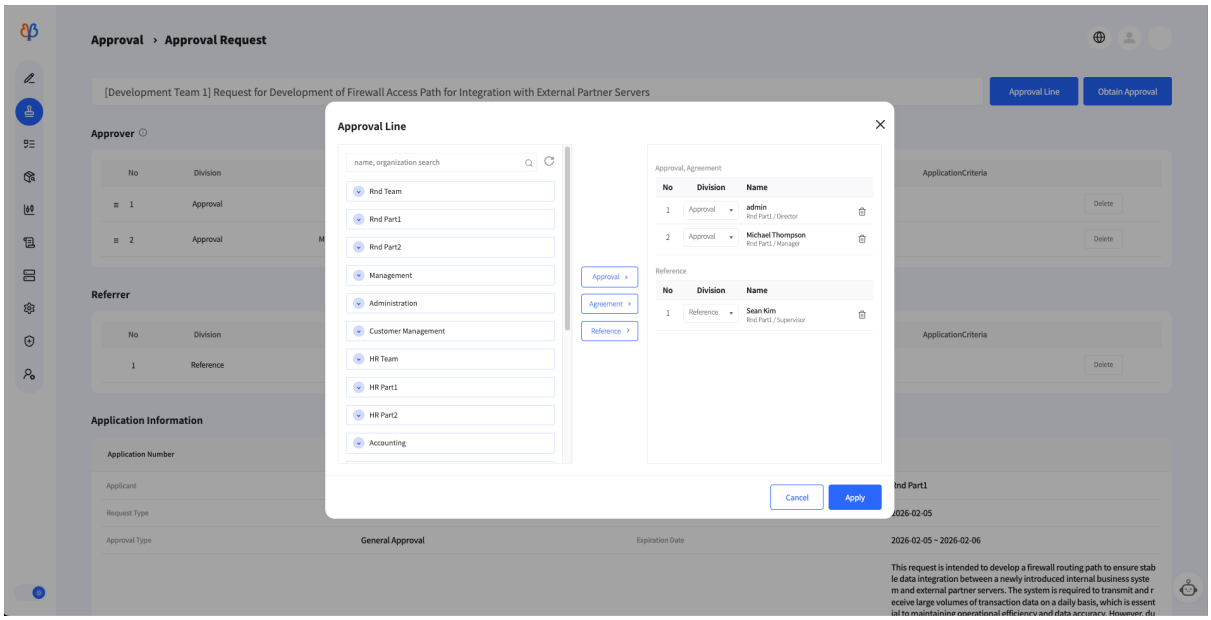
### 2.1.4 Approval

The created firewall policy application form is automatically utilized when submitting for approval, allowing general users to easily proceed with the approval process. To this end, it provides the basic functions required for approval and supports integration not only with internal approval systems but also with external groupware.

1) Approval Submission




〈Approval Submission Screen〉




〈Approval Route Designation Modal Screen〉

2) Automatic Application of Request Information

The firewall policy application form is automatically reflected on the approval submission page. Regular users can proceed with the submission process after designating the approval route without needing to rewrite the application details.

3) Approval Chain

Approvers, consenter and references can be designated via the approval chain modal. Designated approvers are reflected on the approval submission page.

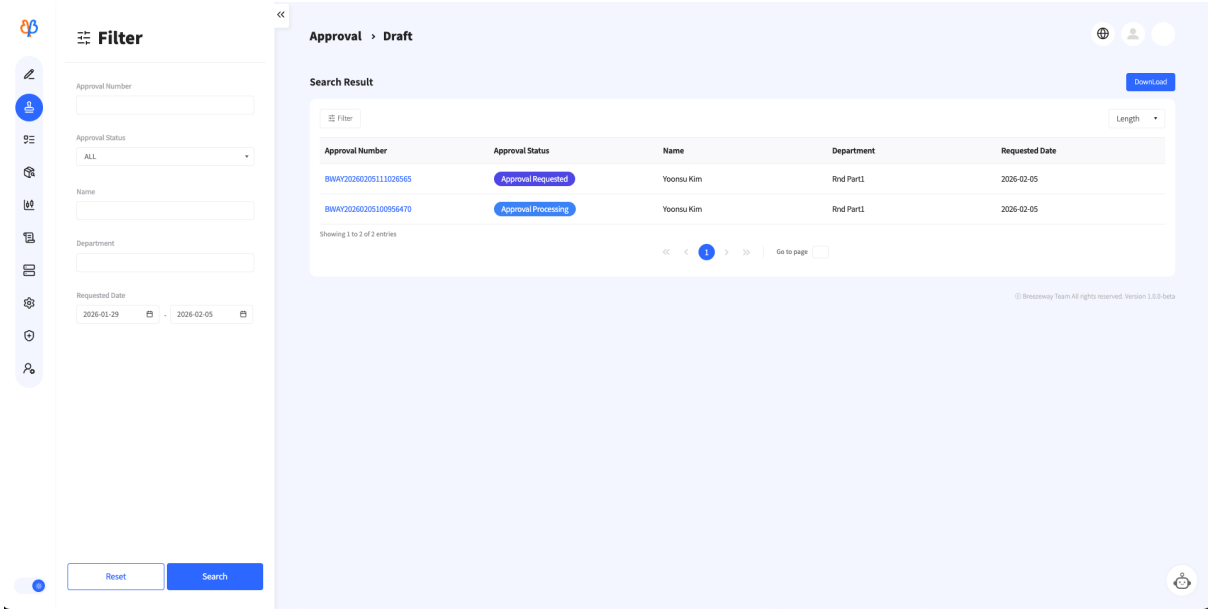
Additionally, approvers manually designated via the approval chain modal can be modified within the submission page. However, fixed approval chains cannot be deleted or modified.

4) Submission

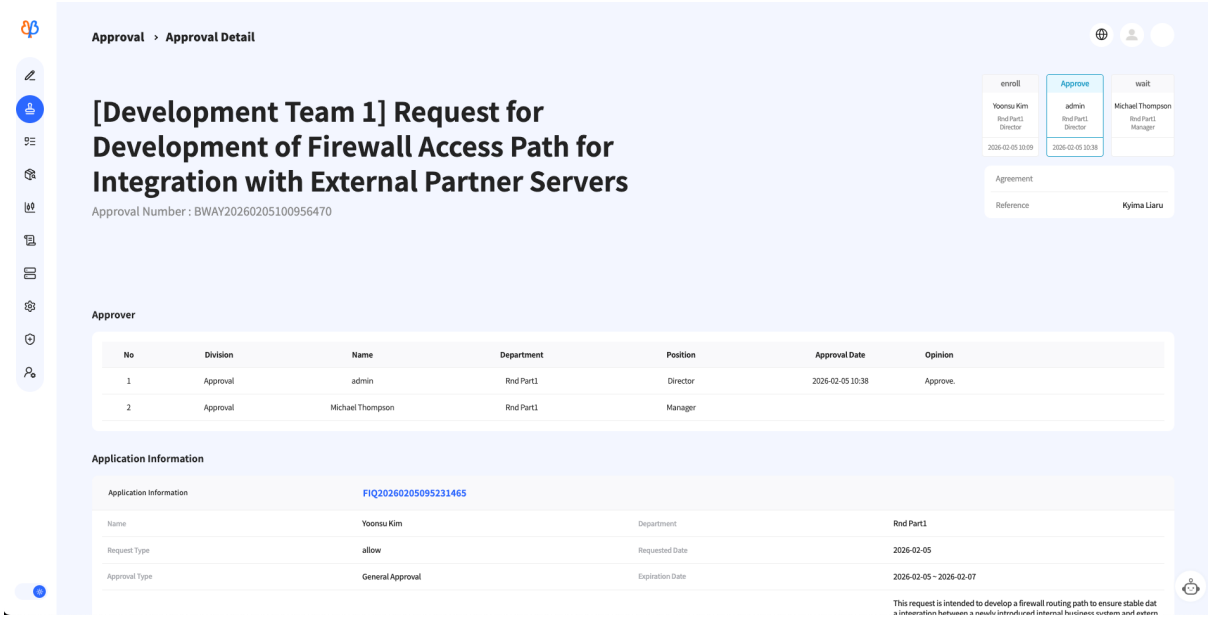
Users submit the approval request and can view the details in the Drafts folder after submission. Approvers, consenter, and references review the submitted details and process approvals via the Approval folder.

5) Draft Folder

Approval submissions can be viewed in the Drafts folder. The Drafts folder displays the list of approvals you have submitted, and you can check the progress status of each approval from this screen. Clicking an approval number allows you to view the detailed approval information.



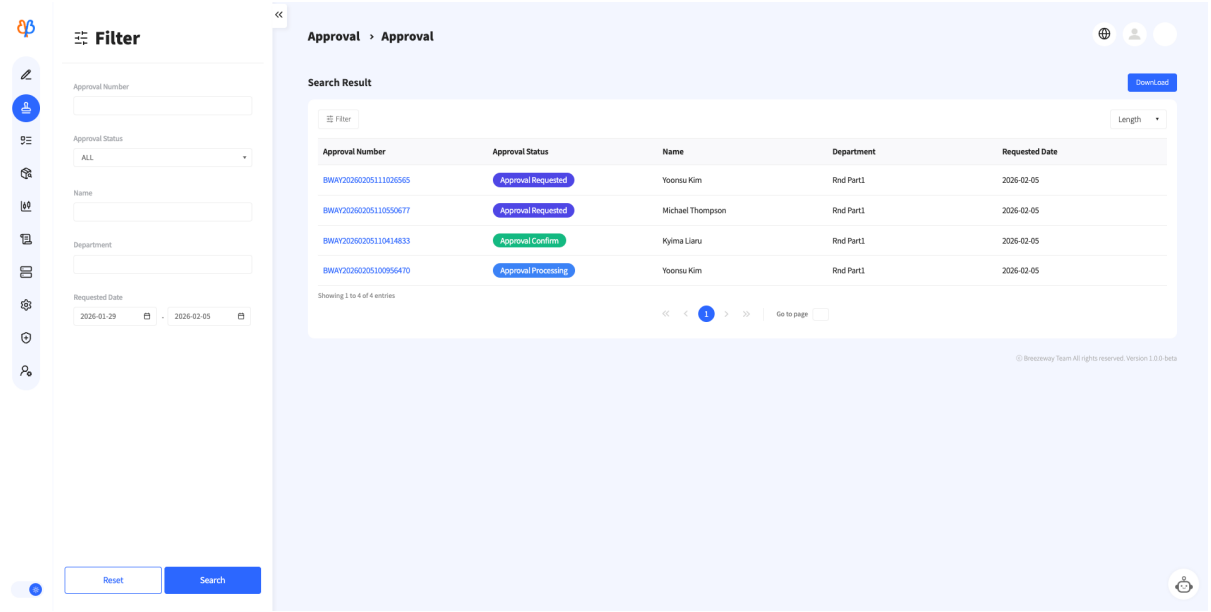

〈Drafts List Screen〉



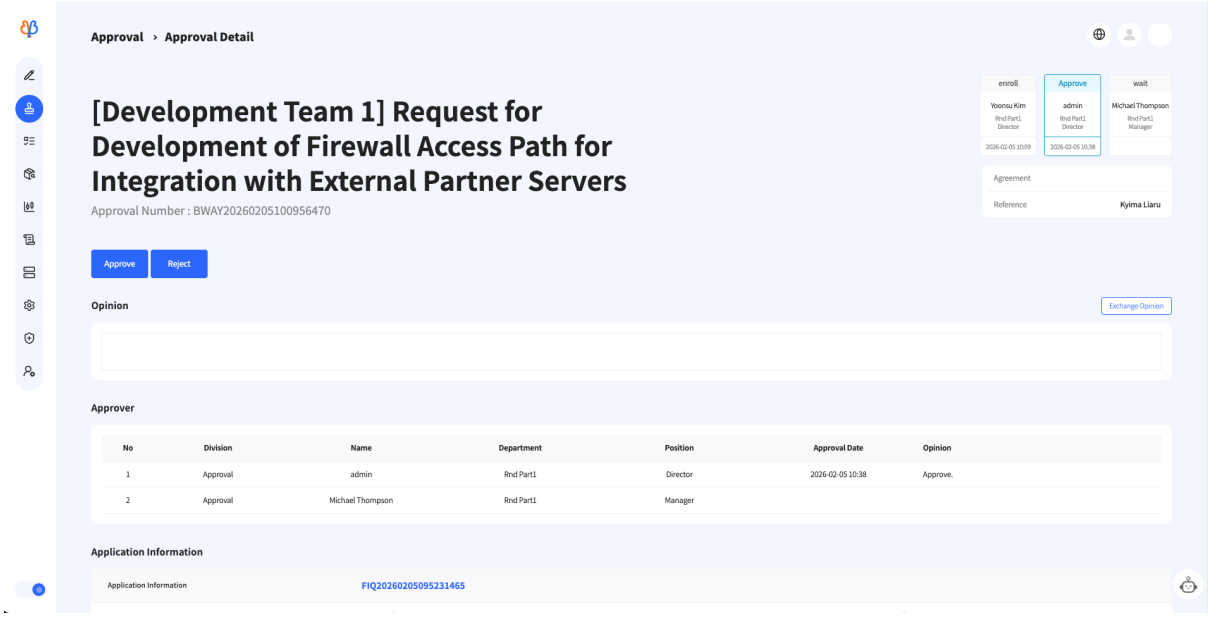

〈Draft Folder Details Screen〉

6) Approval Inbox

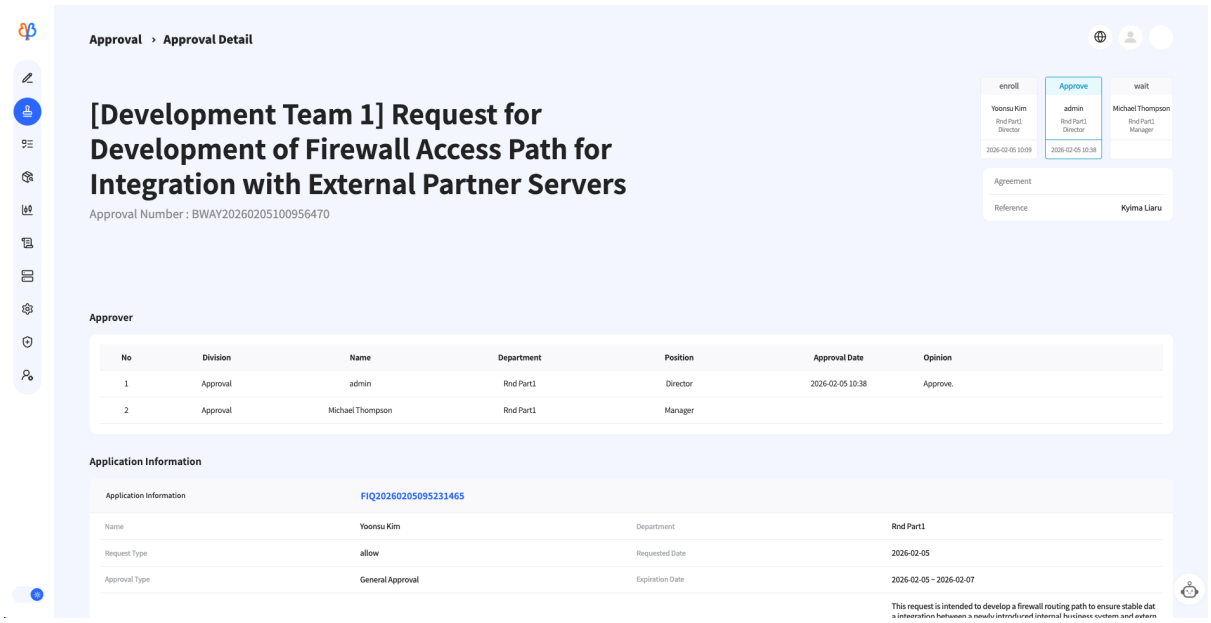
You can only view approvals where you are designated as the approver, co-approver, or reference recipient. You can check the approval stage through the application status (Approval, Approval in Progress, Approved, Rejected). Clicking the approval number allows you to view the detailed approval information. Depending on the approver's decision, you can view the submitter's information, submission details, and the approver's decision result in the upper-right corner of the approval details screen.




〈Approval Queue List Screen〉




〈Approval Details Screen - Approver〉




〈Approval Details Screen - Recipient〉

7) View Approval Details

- Submission Information

You can view the submitter's information and submission date in the upper right corner of the screen.

- Approver Information

You can view approver information (approvers, consenters, and referrers) and the current approval status in the top-right corner of the screen.

- Firewall Policy Application Form

You can view the basic application details (applicant information, application type, approval type, application date, expiration date, application content, attachments) and the detailed firewall policy information (source, destination, service, protocol, verification result).

8) Approval

This function allows the approver to approve the pending approval item. Clicking the Approve button updates the approval status in the approval list and on the details page. The approval process is completed when the final approver approves.

9) Reject

This function allows the approver to reject the approval item. Clicking the Reject button immediately terminates the approval process, and the approval result is reflected in the approval list and detail page.

10) Approval Comments

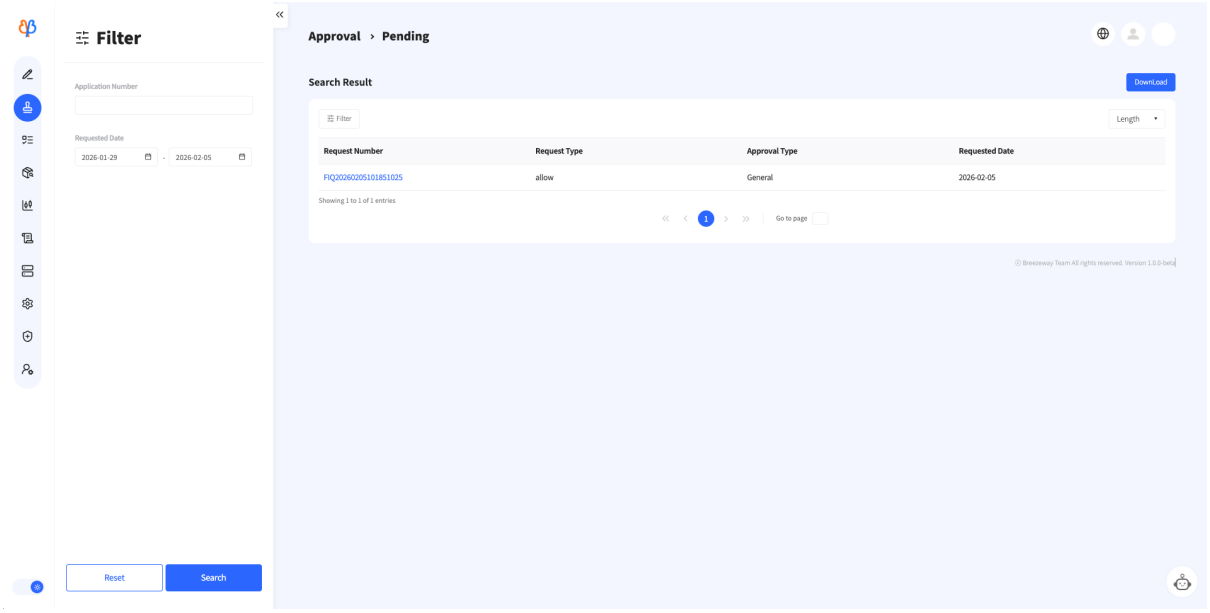
Approvers can write their opinions on the approval item in the approval comments field. Written approval comments can be viewed by the requester, approvers, consenters, and references on the approval details page.

11) Exchange Opinions

If discussion is needed regarding an approval item, opinions can be exchanged via the opinion exchange chat. Participants in the opinion exchange for that approval item include the applicant, approver, co-approver, and referrer designated for that item.

12) Notification

If you applied for a firewall policy using post-approval or closed the submission without submitting documents on the approval submission page, you can process it from the Unsubmitted Items list. Clicking the application number will take you to the approval submission screen to proceed with the submission steps.



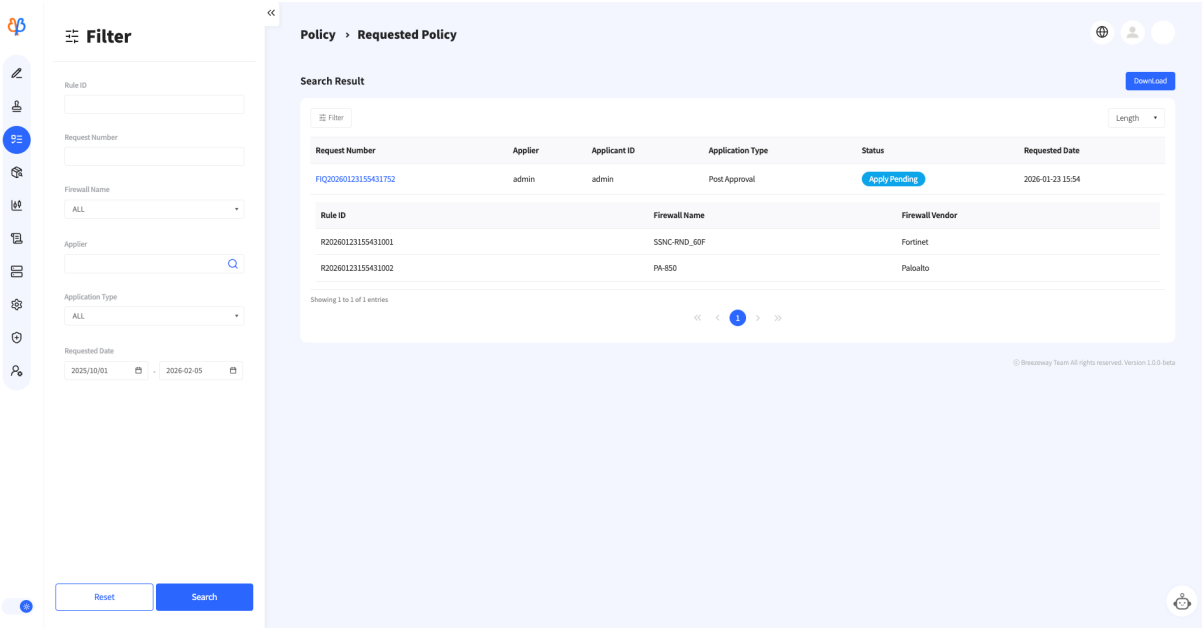

〈Unsubmitted List Screen〉

### 2.1.5 Firewall Policy Application

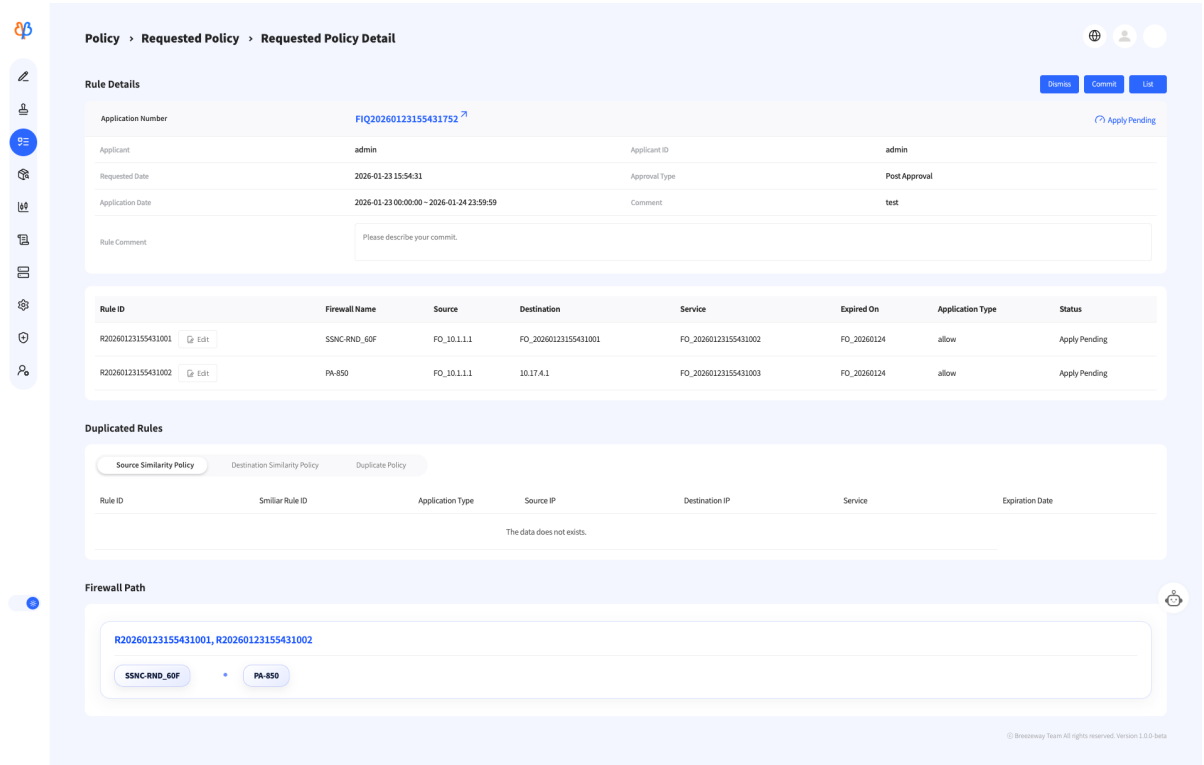
Security administrators can manage policies for each firewall they oversee. A single firewall policy request submitted by a general user is automatically split by the system into multiple policies per firewall. Security administrators can review and process only the request policies corresponding to the firewalls under their responsibility.

1) Application Policy

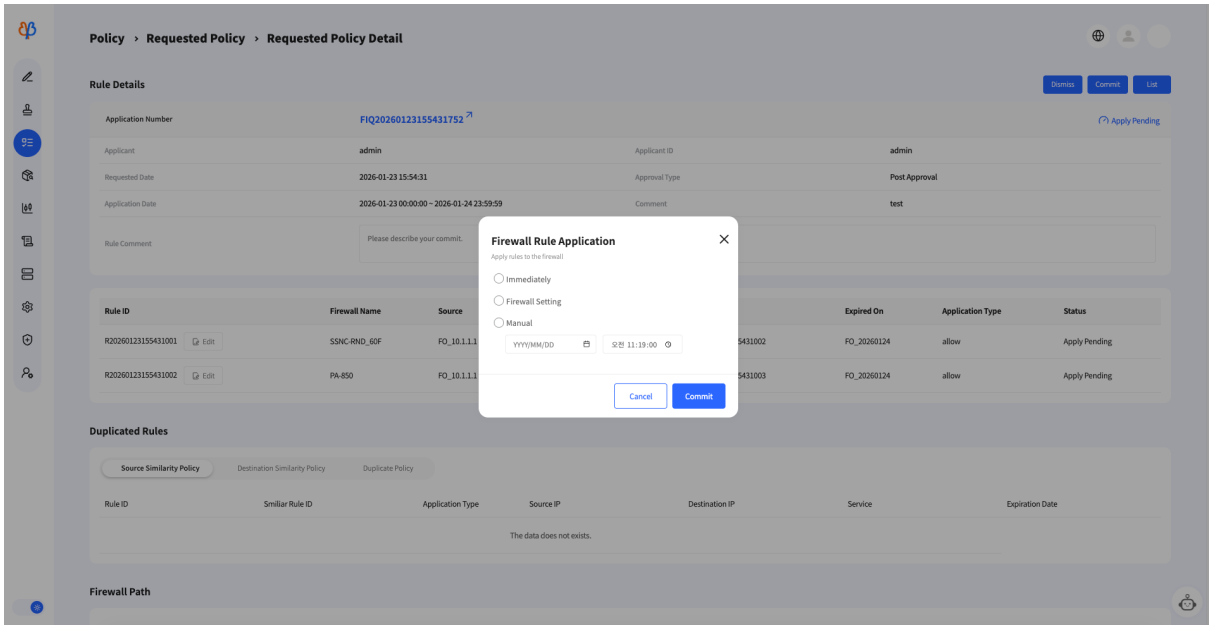
Once approval processing is complete or the policy is immediately reflected through post-approval, the firewall administrator can review the policies separated by their assigned firewall from the application policy and decide whether to apply them.




〈Application Policy List Screen〉




〈Application Policy Details Screen〉




〈Application Policy Commit Modal Screen〉

2) Policy List Inquiry

View the basic information of the firewall policy. Clicking the application number allows you to view the basic information of the firewall policy.

3) Policy Details View

View detailed information about the applied firewall policy. You can check for duplication with existing policies. You can also view the firewall path for the applied policy.

4) Not Applied

If you decide not to apply the requested policy to the firewall after review, click the Not Applied button.

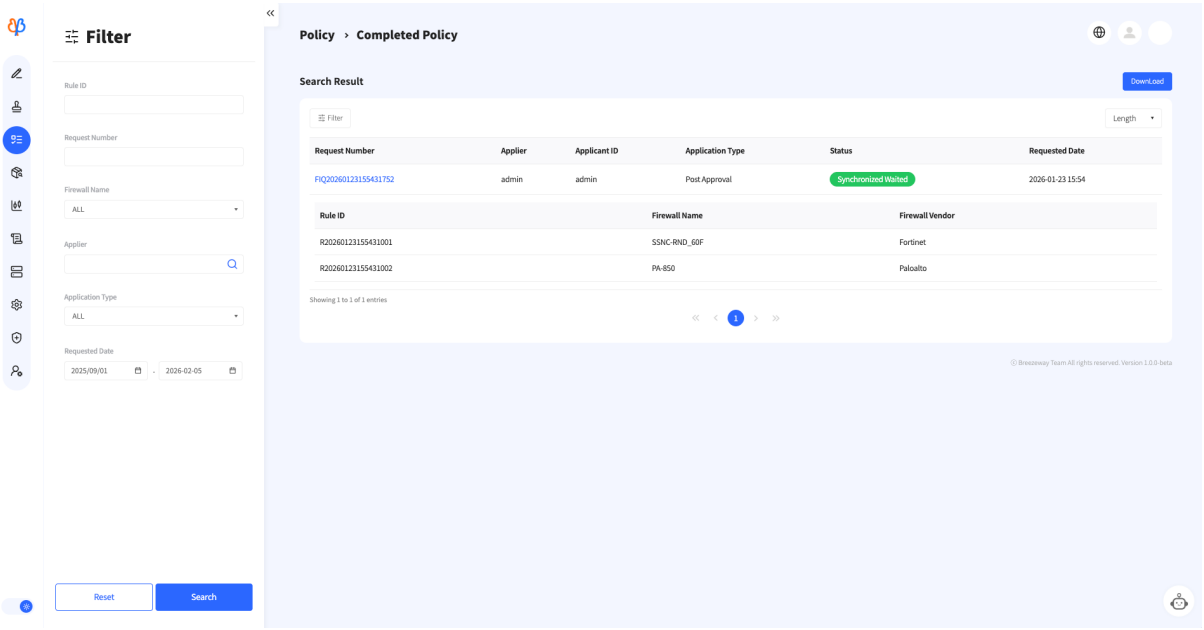
5) Commit

After reviewing the requested policy, if you decide to apply it to the firewall, click the Commit button. The commit methods available in Fire.ONE are as follows.

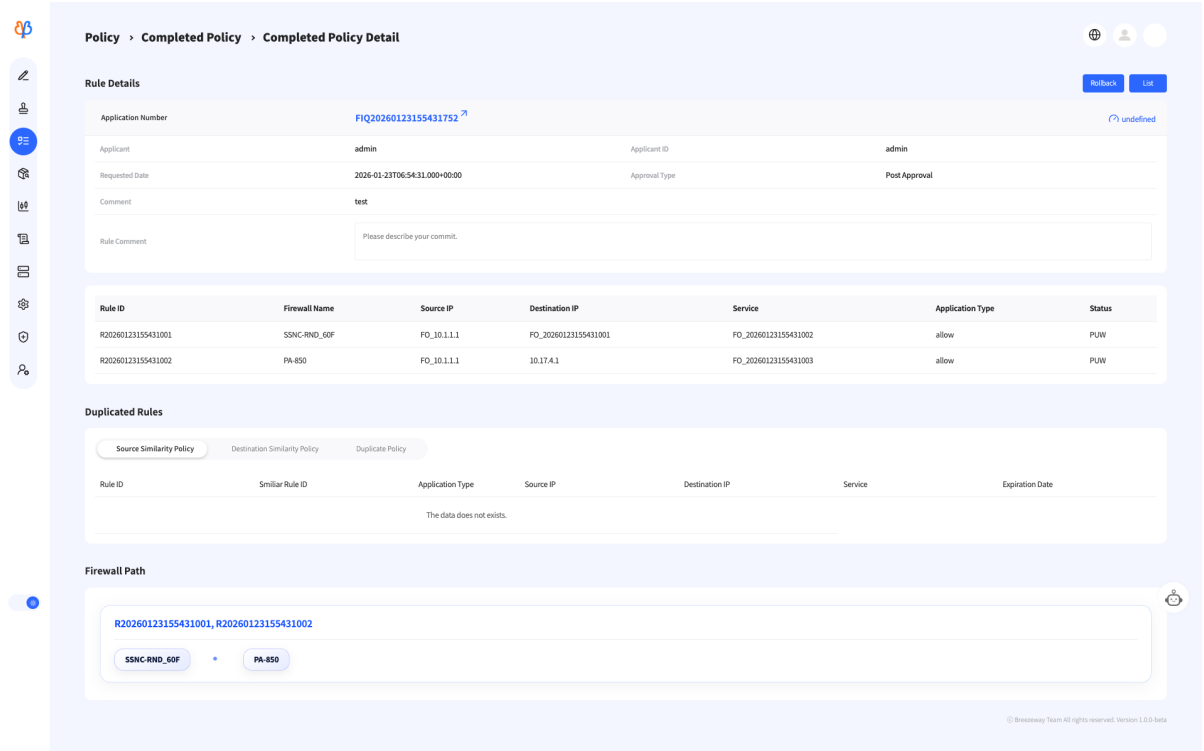
| Method | Description |
|---|---|
| **Immediate Application** | Applies the policy to the firewall immediately. |
| **Firewall Schedule** | When registering the firewall, automatically applies policies according to predefined cron-style schedules. |
| **Manual** | The security administrator applies policies by specifying the desired date and time. |

### 6) Task Completion Policy

You can view the list of policies whose firewall commit (application) has been completed. Clicking a rule ID allows you to view the policy details screen. If an issue occurs with a policy whose firewall application has been completed, a rollback request is possible.




〈Completed Policy List Screen〉




〈Completed Policy Details Screen〉

### 7) Policy List View

View the basic information of the firewall policy. Clicking the application number allows you to view the basic information of the firewall policy.

8) Policy Details View

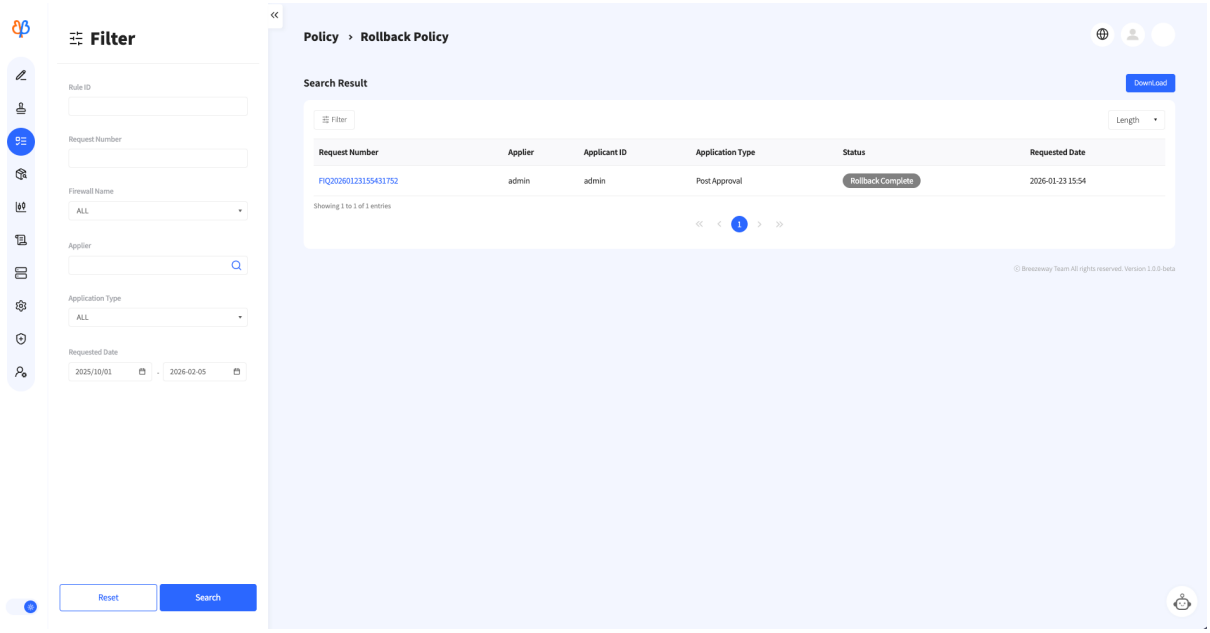
View detailed information about committed firewall policies. You can also check the current firewall application status of the policy (Pending Application, Application Complete, Rollback).
Clicking the application number takes you to the application form to view the detailed application information.

9) Rollback

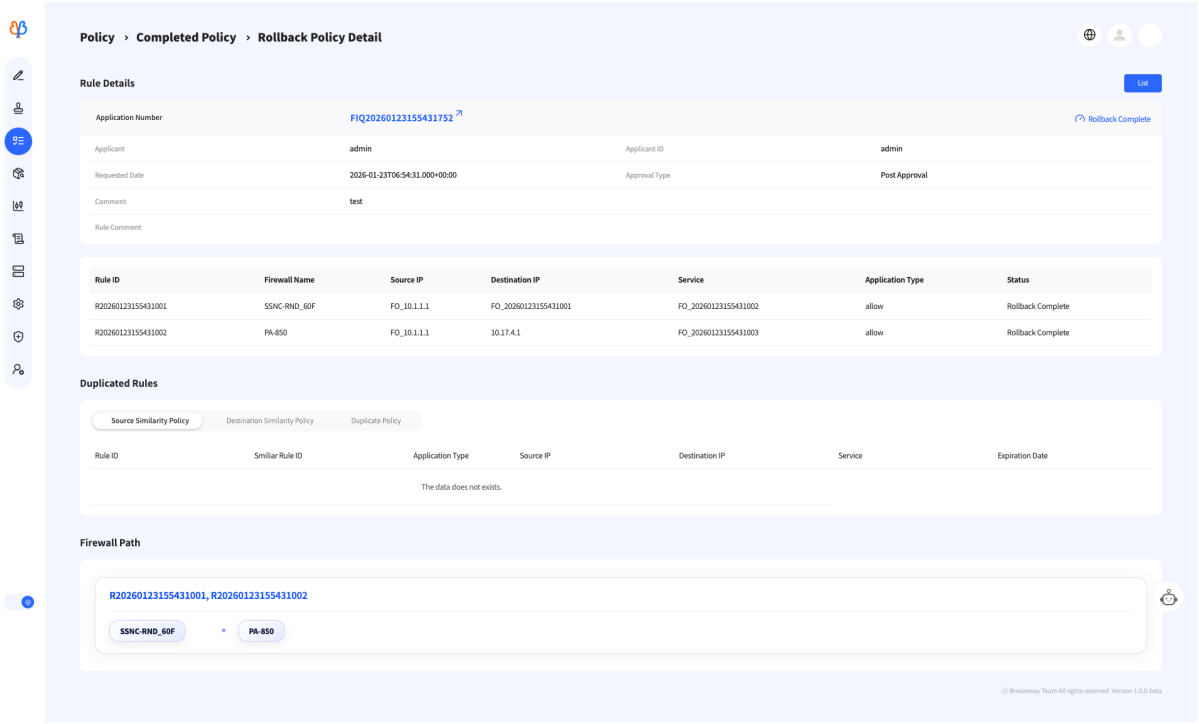
If an issue occurs with a completed policy, you can request a rollback. During rollback, the policy is restored to its state before being applied to the firewall, allowing you to re-evaluate its validity.

10) Rollback Policies

Security administrators can view the list of rolled back policies on the Completed Tasks Details page. Clicking a policy number allows you to view the detailed information for the selected rolled back policy.




〈Rollback Policy List Screen〉




〈Rollback Policy Details Screen〉

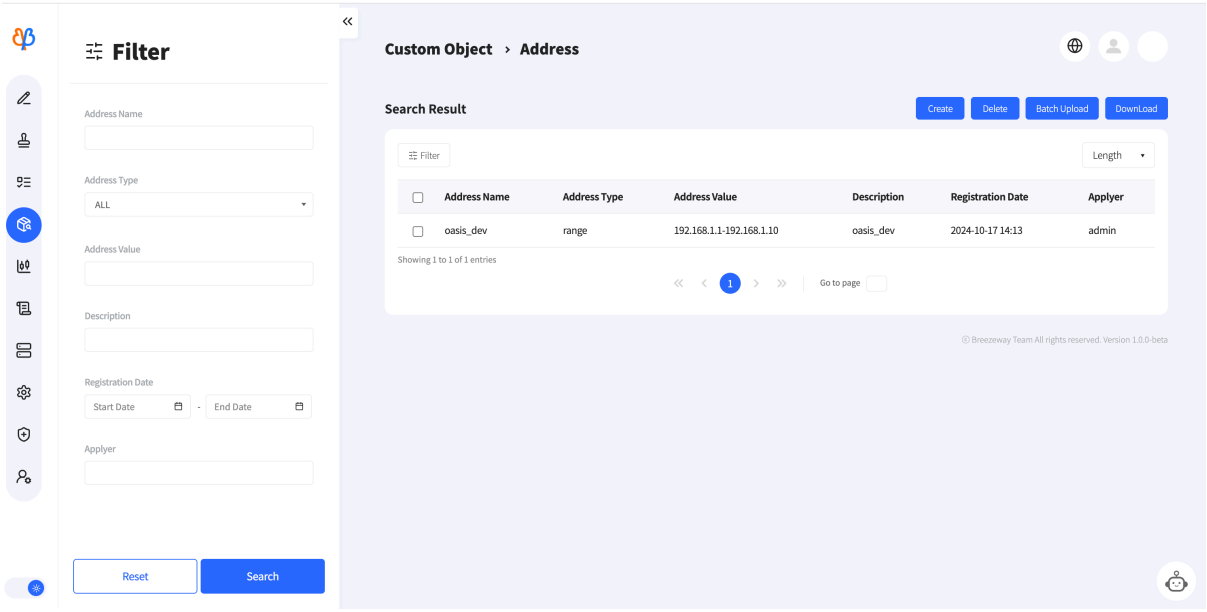
## 2.1.6 Custom Object Management

Pre-create custom objects to be used when applying for a firewall. General users can search for and use custom objects suited to their situation without manually entering IP, service, or protocol information.

**What is a Custom Object?**

Custom objects are a feature that allows administrators to save frequently used IP, port, and server information under names.
When registering policies, users can quickly and accurately select saved objects instead of manual input.

To use a created custom object, click the Object Search button on the Application 〉 Firewall Policy screen and select it from the pop-up window.

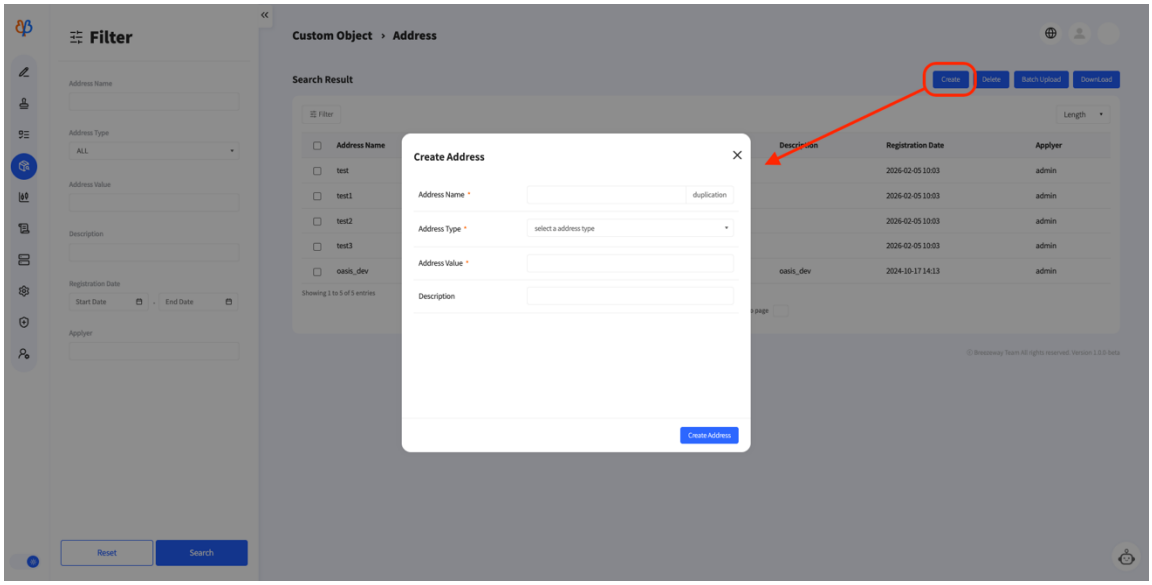



〈Address Object List Screen〉

| Type | Description |
|---|---|
| **Address** | IPv4, range-type IP object |
| **Service** | Port object defined as TCP or UDP type |
| **System** | Object defined as IP+port |
| **Group** | An object that groups one or more objects by address, service, or system |

※ The group object creation function differs from address, service, and system object creation. All other functions are identical.

1) Custom Object Creation



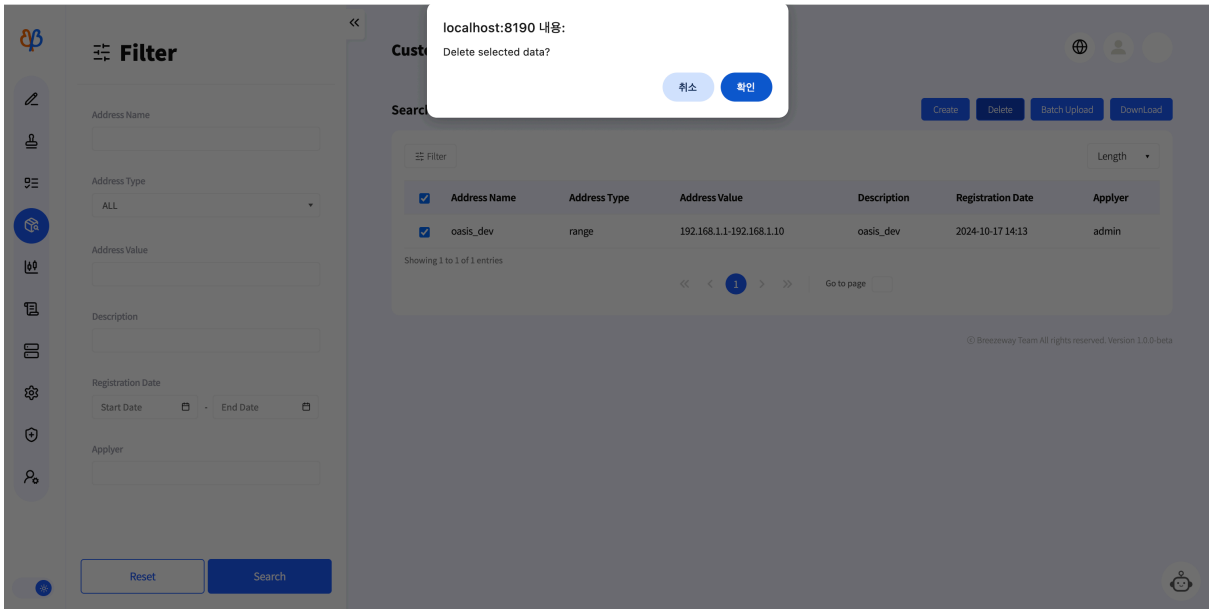

〈Custom Object Creation Screen〉

Click the Create button in the top menu, then create the object in the New Registration pop-up window. The object name must be unique; a duplicate check is mandatory before creation.

2) Custom Object Modification

The object modification function is not provided.

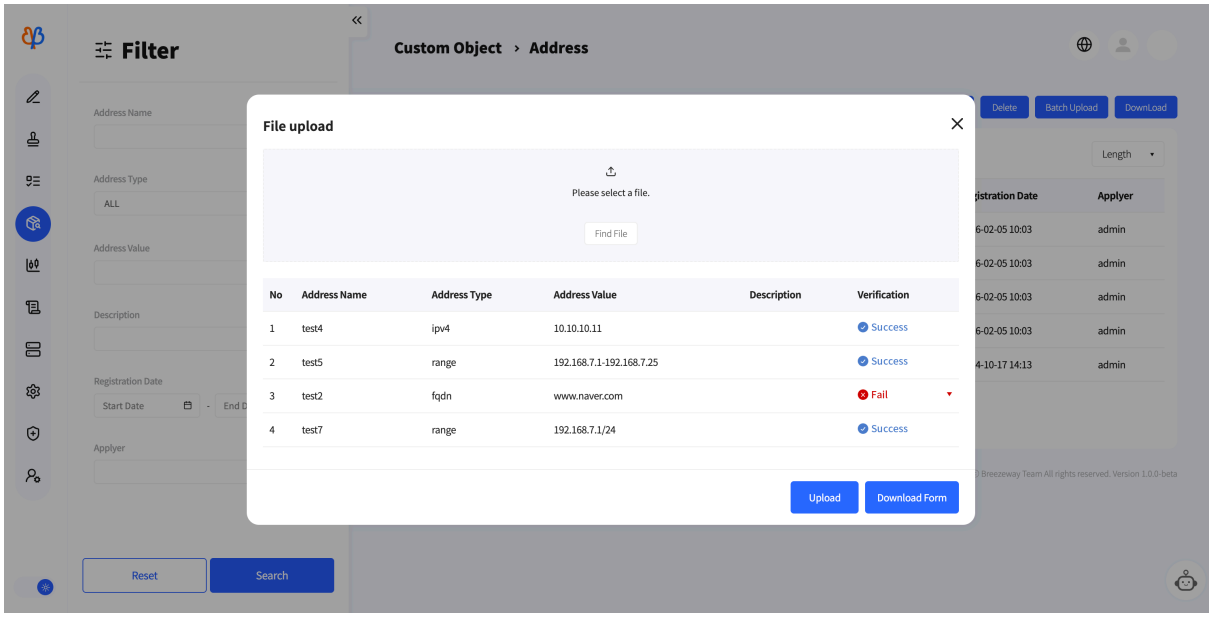
3) Deleting Custom Objects




〈Custom Object Deletion Screen〉

Select the checkbox for the object you wish to delete from the object list, then click the Delete button.

4) Bulk Upload



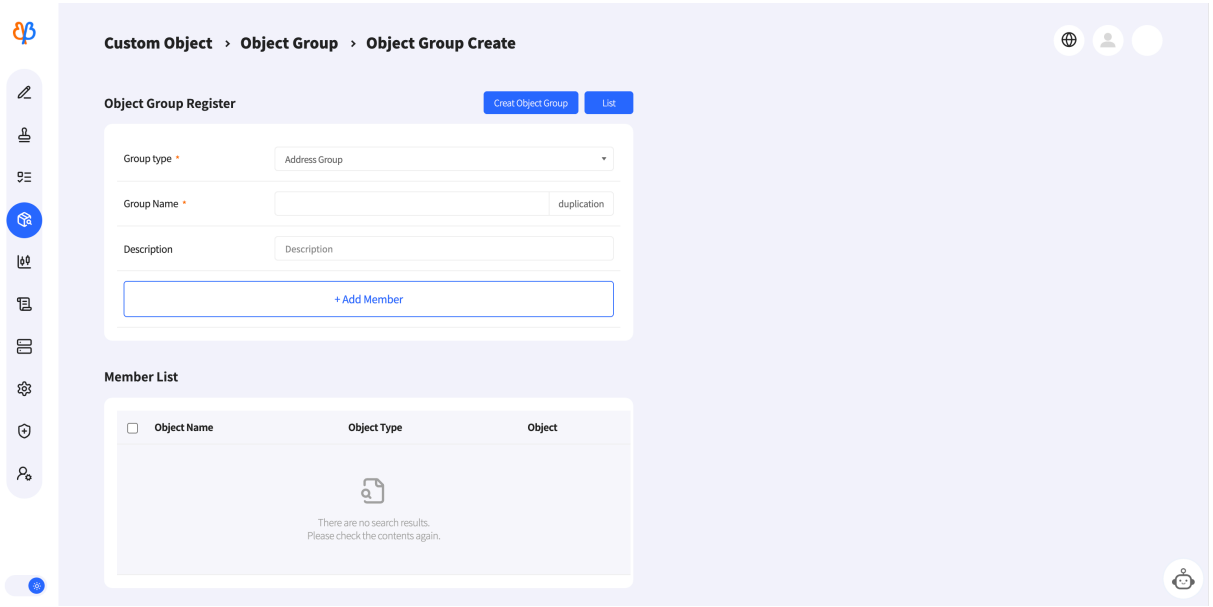

〈Bulk Upload Screen for Custom Objects〉

Upload an Excel file created according to the provided bulk upload file format.

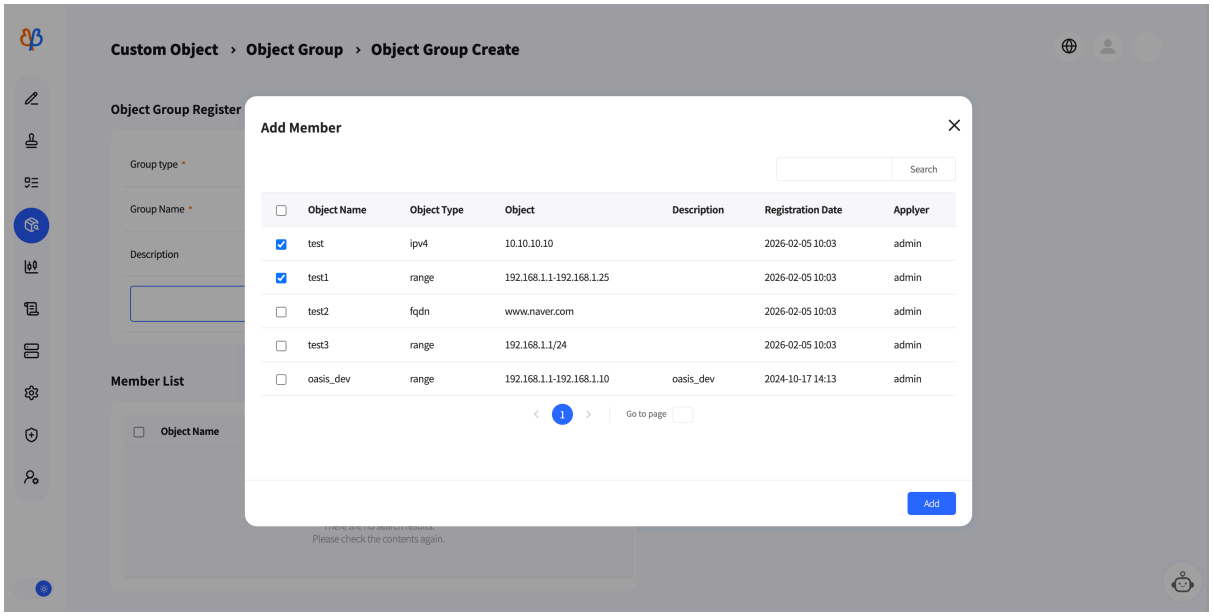
5) Download

Processes the download for the currently displayed table.

6) Group Object Creation




〈Group Object Creation Screen〉

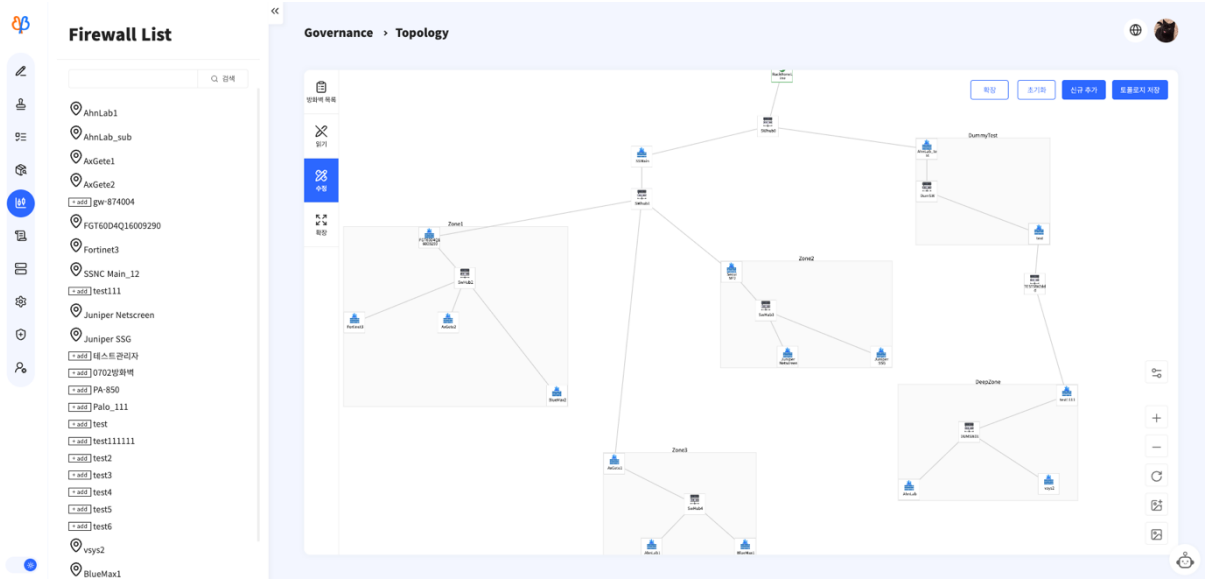



〈Group Object Member Add Modal Screen〉

Clicking the Create button in the upper-right corner of the Group Object List page takes you to the Group Object Creation page.
On the Group Object Creation page, select the group type, group name, notes (description), and choose individual objects to include in the group object using the Add Members button. After confirming the selected objects are correctly reflected in the member list table, click the Register Group Object button to create the object.

## 2.1.7 Topology

Firewall administrators can use the topology creation feature to grasp the entire network configuration structure at a glance.




〈Topology Screen〉

1) Firewall List

The Firewall List displays the list of firewalls managed through the product. The icons preceding the firewall names have the following meanings:

| Icon | Description |
|---|---|
|  | Reflected in the topology. Clicking moves you to that location. |
|  | Adds a firewall to the topology. |

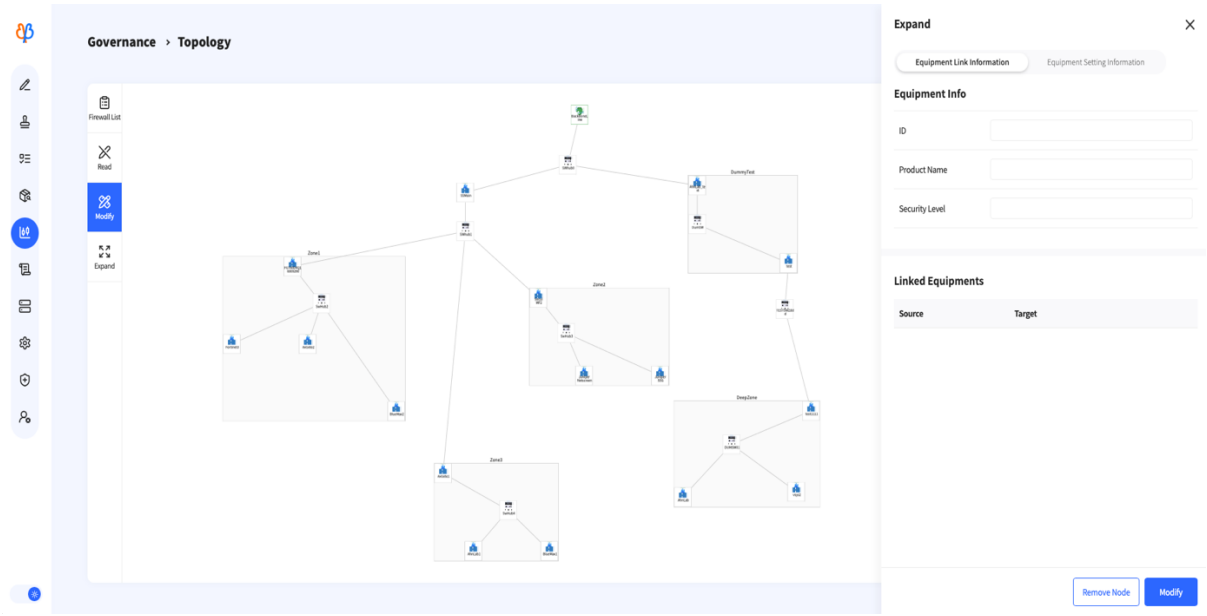
2) Topology

The topology operates in four modes. The behavior per mode is as follows.

| Mode | Description | Features Provided |
|---|---|---|
| **Read** | Only topology lookup is possible; modification is not allowed. | • Topology View |
| **Edit** | Topology modification is possible; selecting this displays the Advanced tab. | • Topology View<br>• Topology Modification<br>• Topology Initialization<br>• New Addition<br>• Save Topology |
| **Expand** | Topology modification and path analysis are possible. Analysis mode is displayed upon selection. | • Topology Query<br>• Modify Topology |

| | | |
|---|---|---|
| | | • Topology Initialization<br>• New Addition<br>• Save Topology<br>• Path Analysis |
| **Analysis** | Firewall path analysis results are scored and calculated, then visualized as a graph. | • Path Analysis |

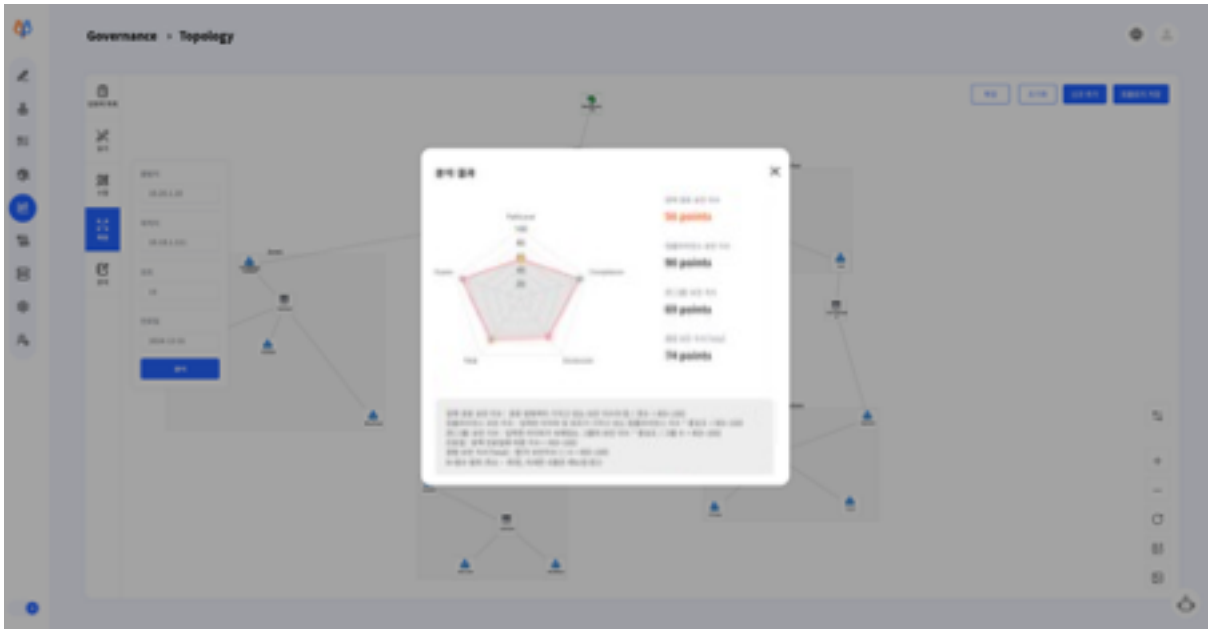
3) Expand




〈Topology Expansion Tab Screen〉

The Extension tab allows you to view, modify, and delete information about nodes.

4) Analysis




〈Topology Path Analysis Screen〉

Analysis is performed on four items based on the source, destination, and port. Once analysis is complete, the results are displayed graphically. (Refer to Appendices 6.1 and 6.2 for the calculation formulas of each security index)

5) Initialization

This function reverts the topology to its state before modification.

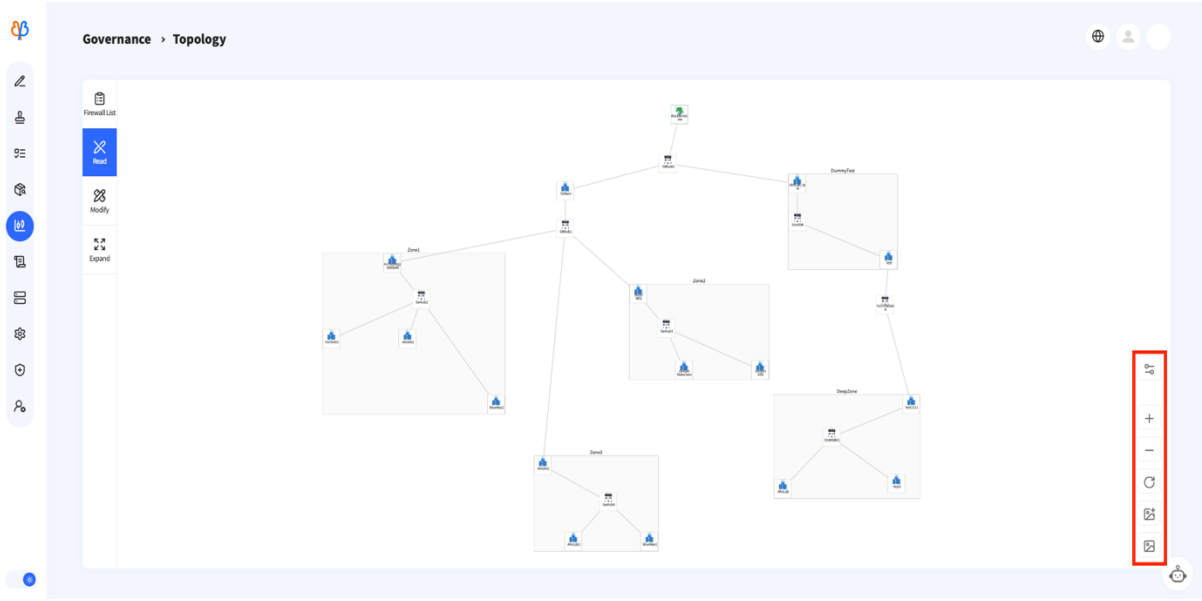
6) New Addition

This function adds a new firewall.

7) Save Topology

This function saves the final modified information. If not saved, the currently modified and reflected data will not be stored.

8) Topology Auxiliary Functions




The buttons in the lower right corner of the topology provide auxiliary functions for viewing the screen. The functions provided by each icon are as follows.

| Icon | Description |
|---|---|
| | Changes the line type and color used in the topology. |
| | Zooms in on the screen. |
| | Zoom out the screen. |
| | Restores the zoomed-in/out screen to its original state. |
| | Saves the current topology screen zoomed in as a file. |
| | Saves the current topology screen as a file. |

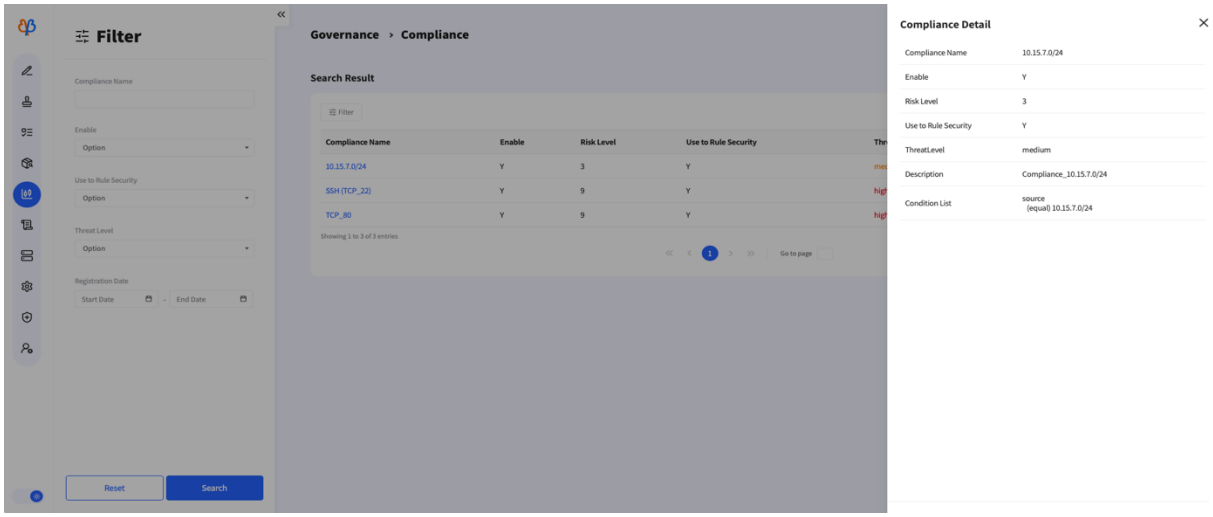
### 2.1.8 Compliance

Security administrators register compliance rules so that when general users verify firewall policies, they can check for violations against pre-registered compliance rules.

What is compliance?

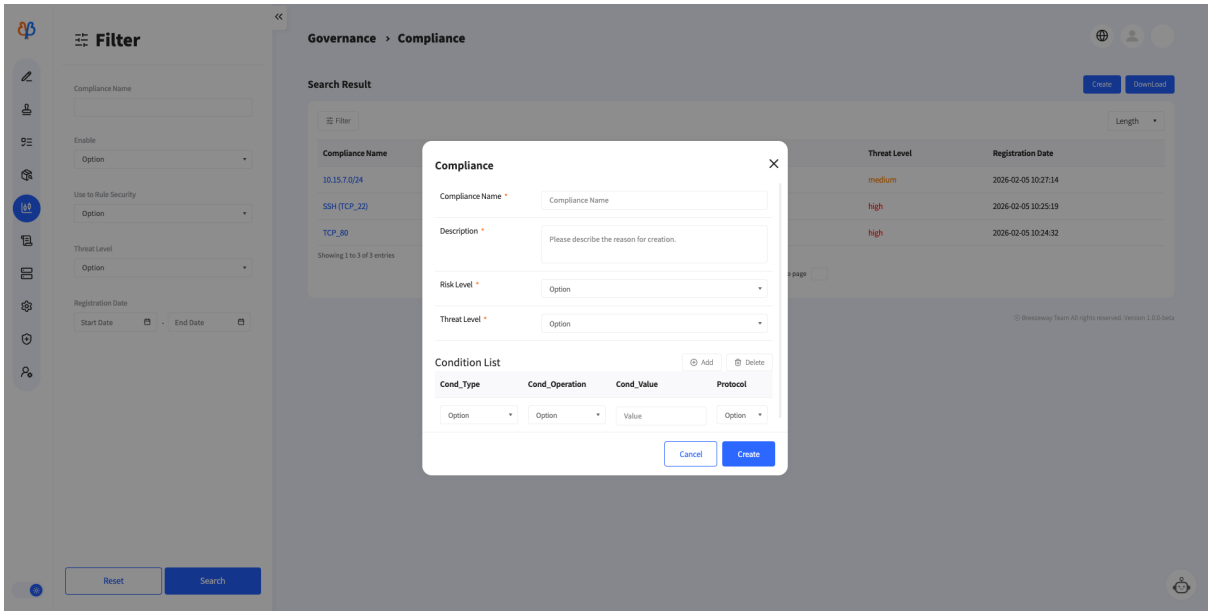
When applying for a firewall policy, compliance is a pre-check standard that automatically verifies whether the policy is secure according to company and security regulations. For example, if access to internal port 22 is requested from outside, it automatically checks for policy violations and determines whether it is "Dangerous" or "Approval Possible".

In other words, it is a protective mechanism that preemptively filters out policies that violate security rules, eliminating the need for manual verification.




〈Compliance Screen〉

- Compliance Name: Compliance Category Name
- Enable: Whether enabled
- Violation Count: Number of requests violating this compliance rule
- Security Analysis Usage: Determines whether to use in security analysis reports
- Remarks: Additional explanation
- Condition: Rule for compliance
  Ex) The condition statement "source address (equal) IP_10.20.1.10" expresses the case where the source address is 10.20.1.10




〈Compliance Registration Screen〉

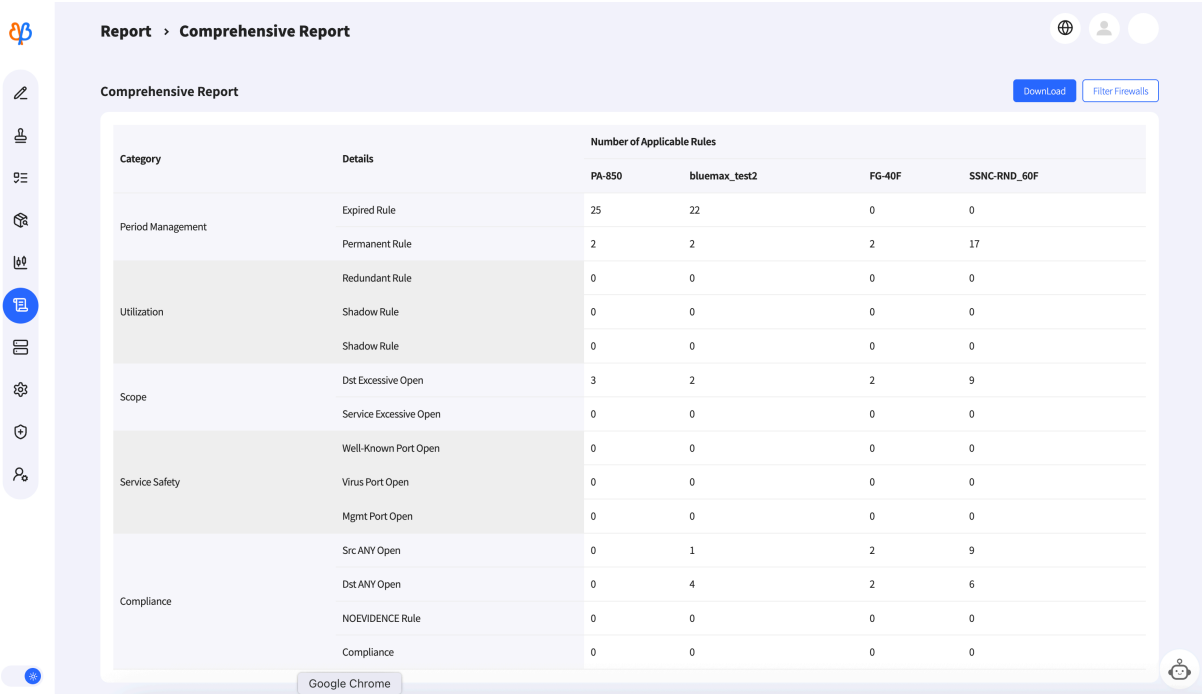
- Compliance Name: Compliance category name
- Remarks: Additional description
- Risk Level: Risk score setting (1~10 points)
- Threat Level: Threat level setting (high, medium, low)
- Condition List: Rule Settings for Compliance
    - Cond_Type: Compliance Type Setting (source, destination, service, expire)
    - Cond_Operation: Compliance rule condition setting
    - Cond_Value, Protocol: Enter source address, destination address, service, and expiration date

### 2.1.9 Dashboard and Report Generation

We provide dashboards that visualize key metrics based on collected data and generate detailed reports.
The dashboard enables real-time visualization of core metrics at a glance for swift monitoring and response. Detailed reports facilitate granular filtering and analysis, enabling root cause identification and serving as documentation for compliance purposes.

### 2.1.10 Report

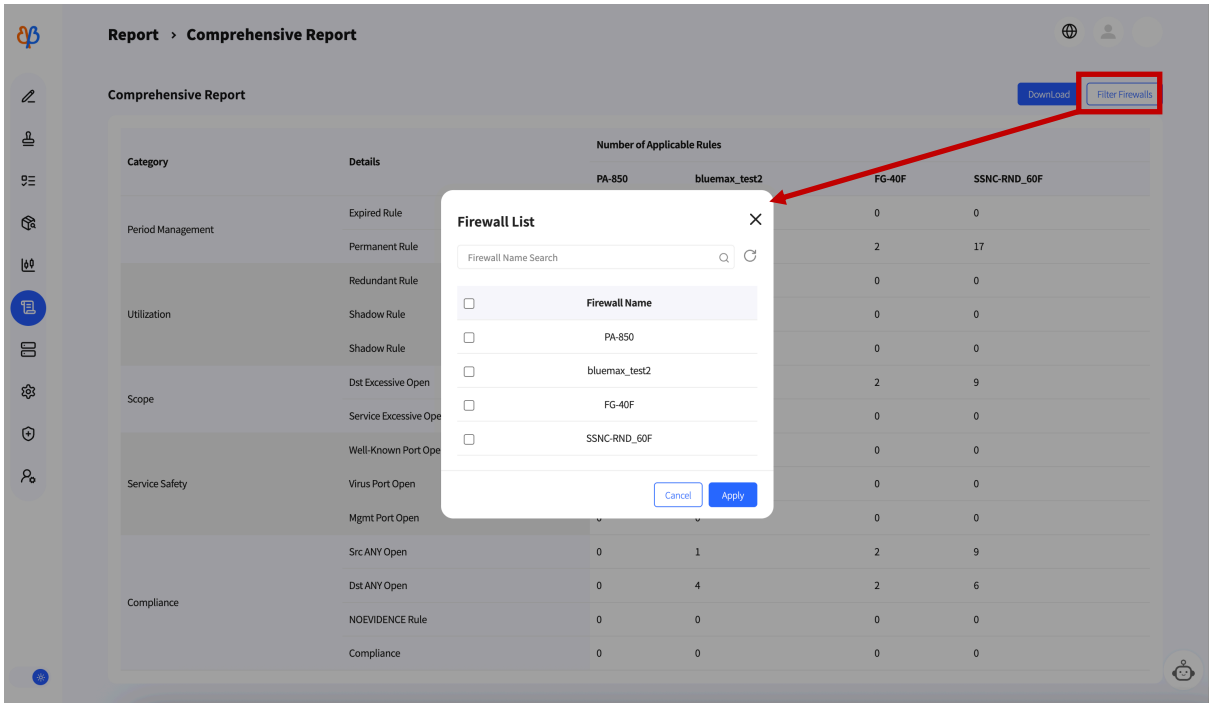
1) Policy Report




〈Policy Report Screen〉

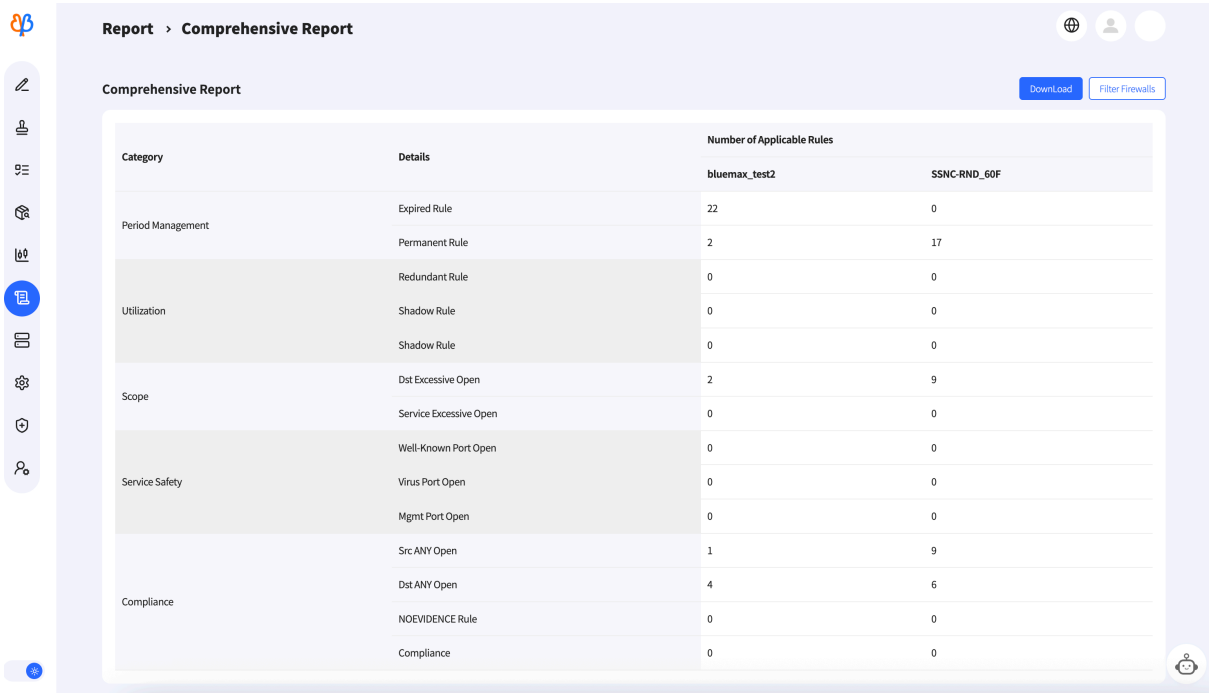
You can see the classification status of rules for each firewall at a glance. Detailed items are grouped by category, and you can easily grasp the number of policies for each item per firewall.

- Policy Report - Filter Application




〈Policy Report Screen - Firewall Filter Modal〉

Use the 'Firewall Filter' button in the upper right corner of the screen to select the firewalls to display in the consolidated report.



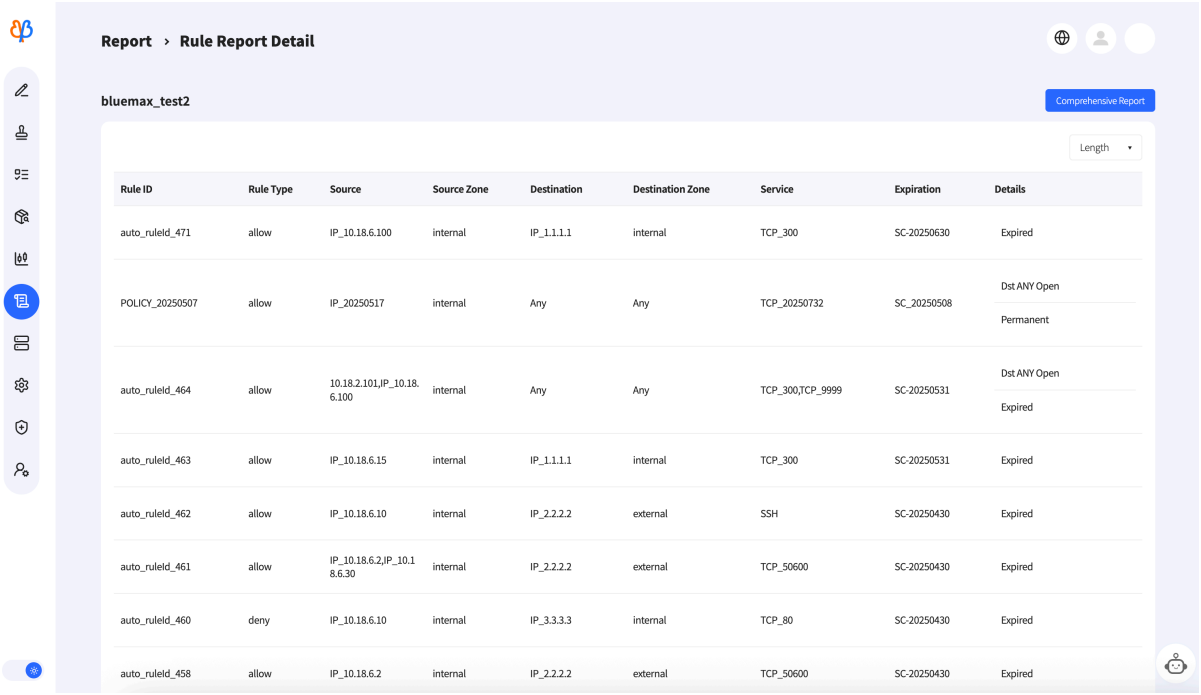

| Category | Details | Number of Applicable Rules | |
|---|---|---|---|
| | | bluemax_test2 | SSNC-RND_60F |
| Period Management | Expired Rule | 22 | 0 |
| | Permanent Rule | 2 | 17 |
| Utilization | Redundant Rule | 0 | 0 |
| | Shadow Rule | 0 | 0 |
| | Shadow Rule | 0 | 0 |
| Scope | Dst Excessive Open | 2 | 9 |
| | Service Excessive Open | 0 | 0 |
| Service Safety | Well-Known Port Open | 0 | 0 |
| | Virus Port Open | 0 | 0 |
| | Mgmt Port Open | 0 | 0 |
| Compliance | Src ANY Open | 1 | 9 |
| | Dst ANY Open | 4 | 6 |
| | NOEVIDENCE Rule | 0 | 0 |
| | Compliance | 0 | 0 |

〈Policy Report Results Screen After Applying Firewall Filter〉

- Excel Download

Click the 'Excel Download' button in the top-right corner of the screen and select the desired firewalls to download their reports. The downloaded Excel file includes one sheet listing the number of policies per item for each firewall in the same format as the table displayed on the screen. Additionally, it provides a separate sheet for each firewall that has at least one item with detailed information.

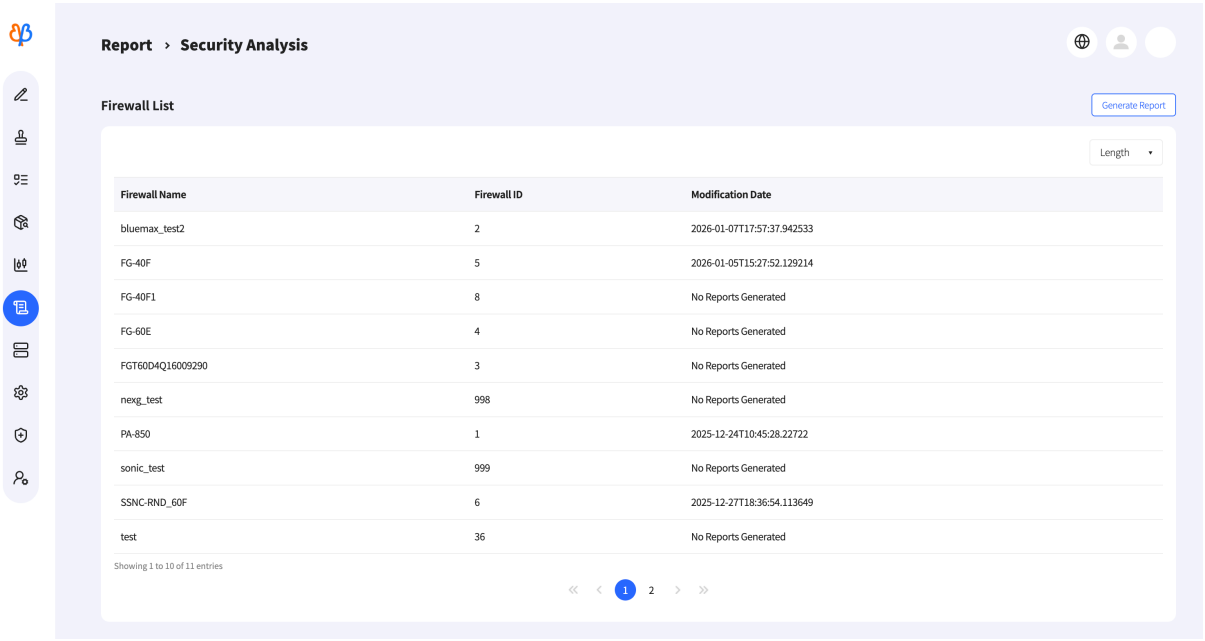
- Policy Report Details




〈Policy Report Details Screen〉

Clicking on a firewall name in the policy report results screen takes you to the detailed report page for that firewall. The policy report details screen displays a list of detailed information for policies that correspond to the specific details within that firewall's policies.
You can return to the initial policy report screen by clicking the "Comprehensive Report" button in the upper right corner.

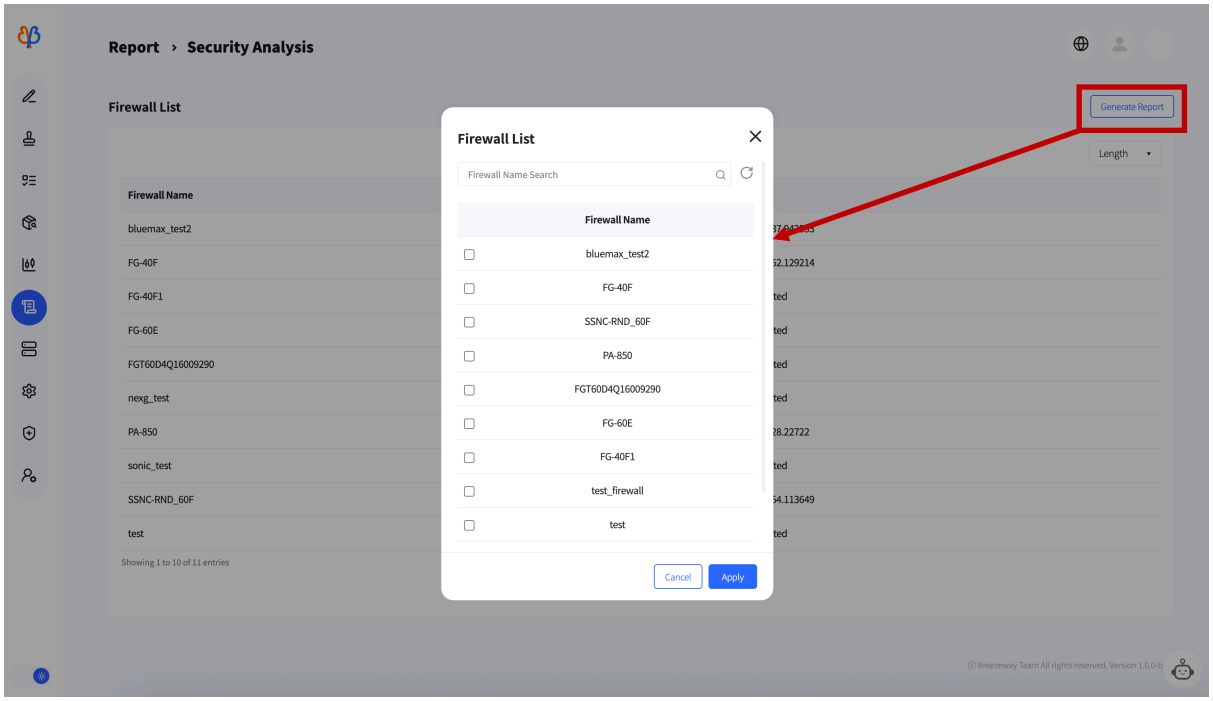
### 2) Security Analysis




〈Security Analysis Screen〉

You can check the status of security analysis report generation for each firewall. The third column of the table displays the date and time of the last generated report. For firewalls where no report has been generated yet, it displays "No Reports Generated".

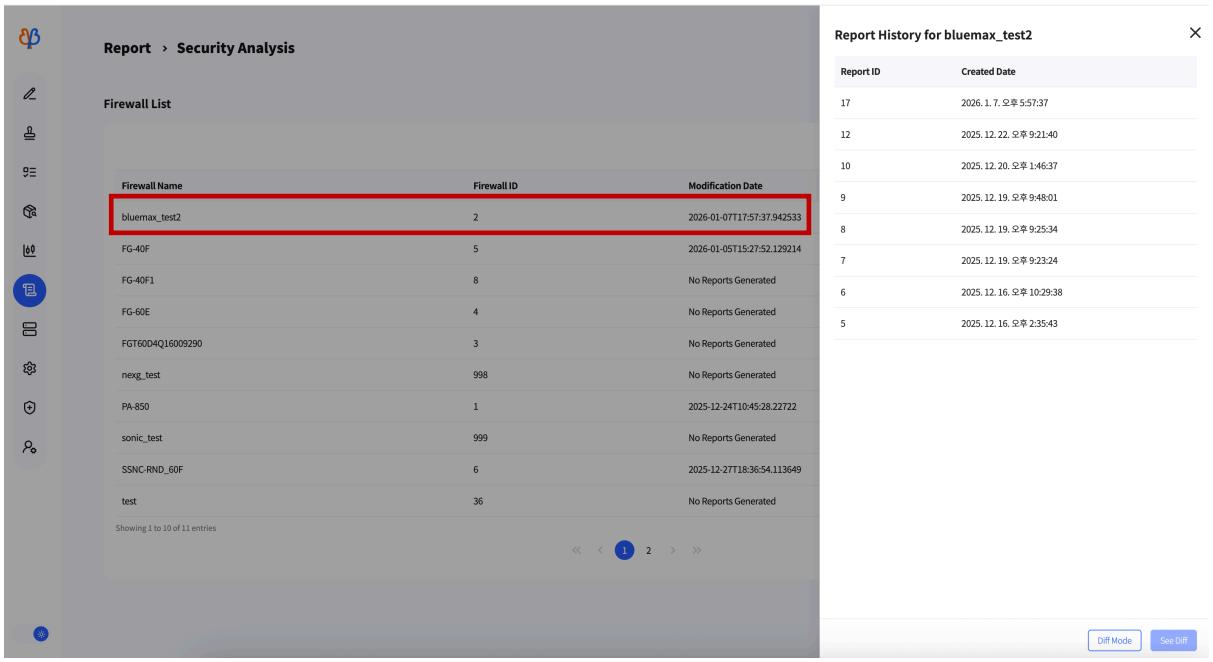
- Security Analysis - Report Generation




〈Report Generation Modal Screen〉

Clicking the "Generate Report" button in the upper-right corner of the screen displays a modal window. Select the firewall for which you want to generate a report in this modal window, then click the "Apply" button at the bottom of the modal window to generate the report. Once report generation is complete, the page refreshes, and the date and time of the last generated report are updated in the third column of the firewall list table for that firewall.

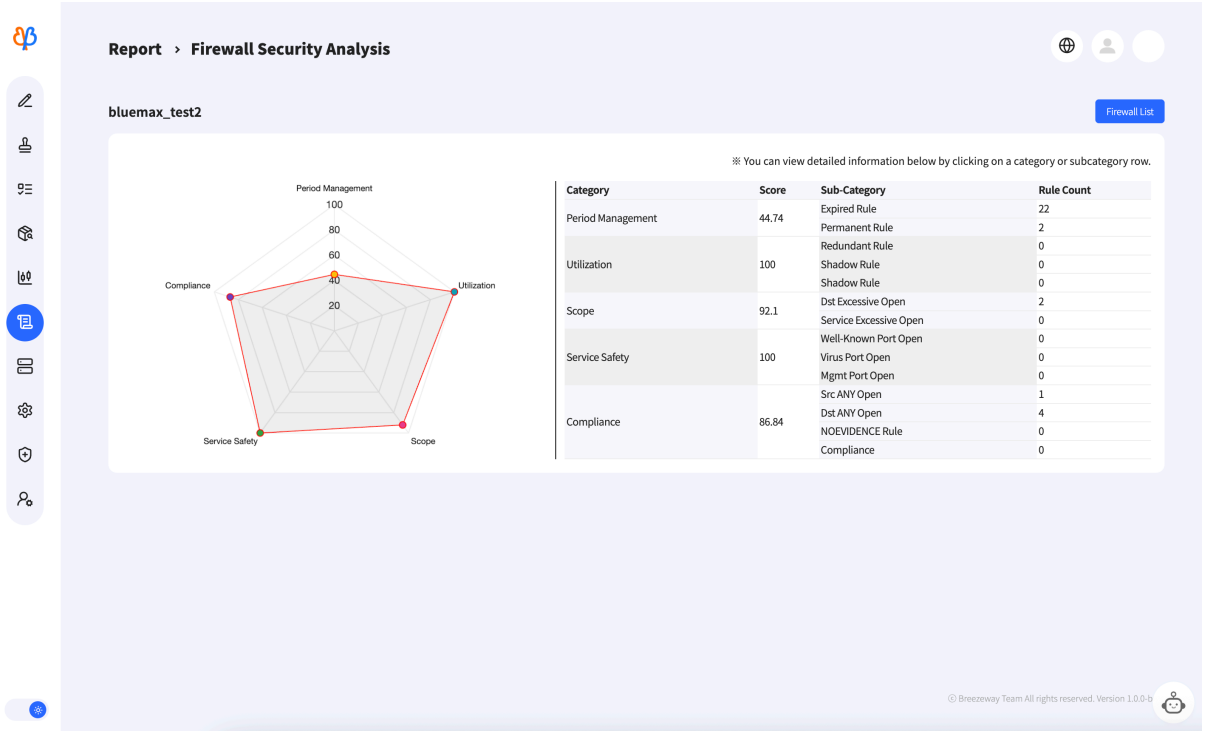
- Security Analysis - Report Generation History




〈Report Generation History Modal Screen〉

Clicking a row in the firewall list table displays a modal window on the right side of the screen containing the report generation history information for that firewall. Clicking a row in the report list takes you to the firewall policy analysis page.

- Security Analysis - Firewall Policy Analysis

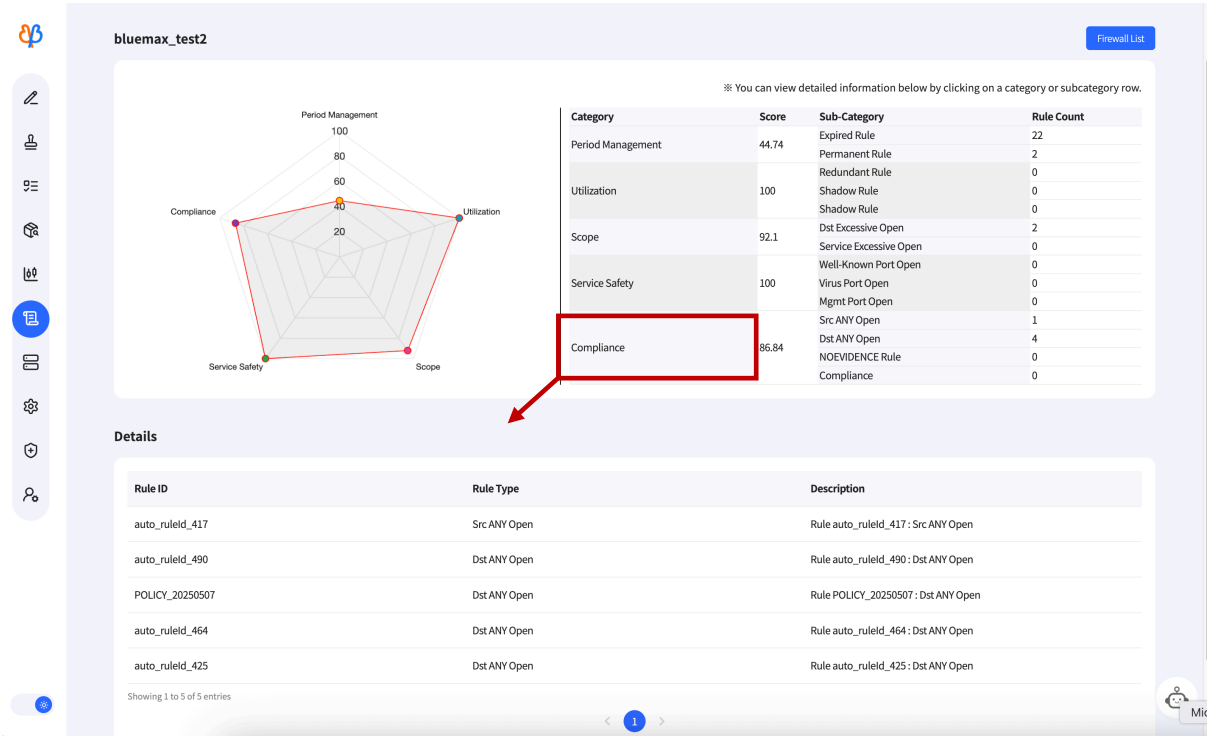



〈Firewall Policy Analysis Screen〉

On the left side of the screen, you can see a radar chart displaying scores for each category. On the right side, a table shows the security score for each category of the corresponding firewall and the number of policies per detail. Click the "Firewall List" button in the top-right corner to return to the <Security Analysis Screen>.

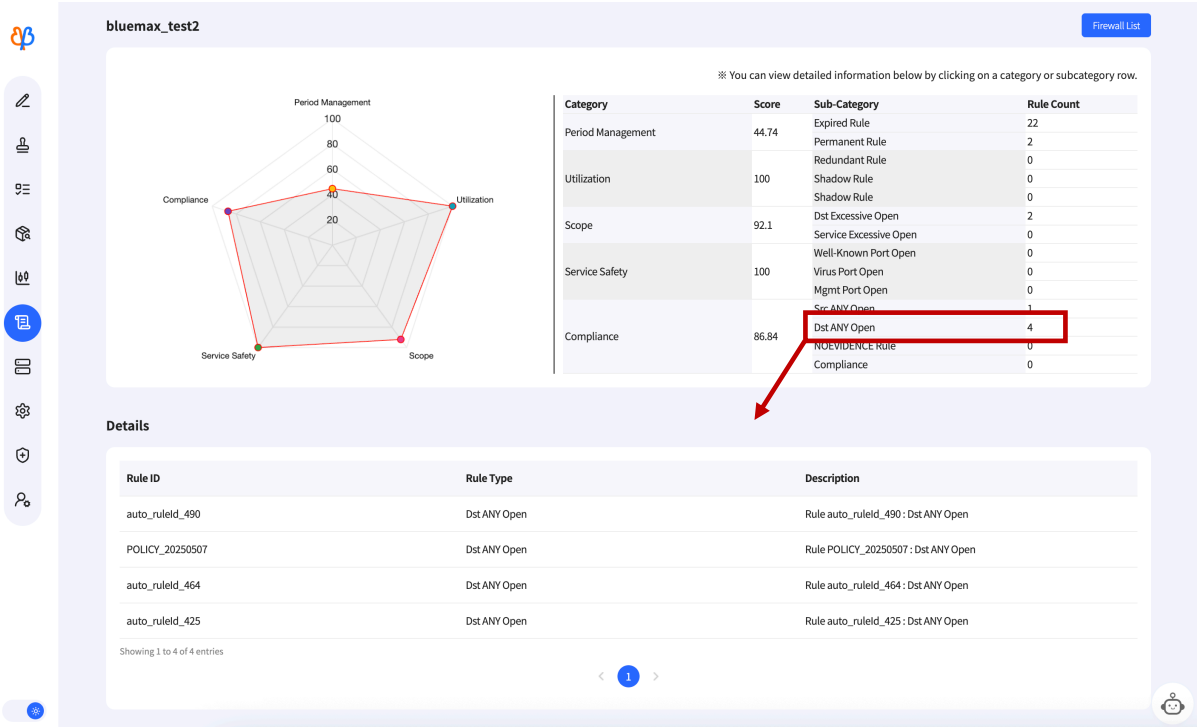
The radar chart on the left displays scores for five categories: Period Management, Usage, Scope, Service Stability, and Compliance. Other details are excluded from the radar chart as they have minimal impact on firewall security. Hovering your mouse over the chart reveals the exact score for that category.

The table on the right side of the screen has a format similar to the <Policy Report Screen>. A higher score for each item indicates a better security status, while a lower score indicates the presence of a violation policy for that specific item. The weight value for each detail can be set in the "Settings -> Weight" screen.




<Firewall Policy Analysis - When Clicking a Major Category Name>

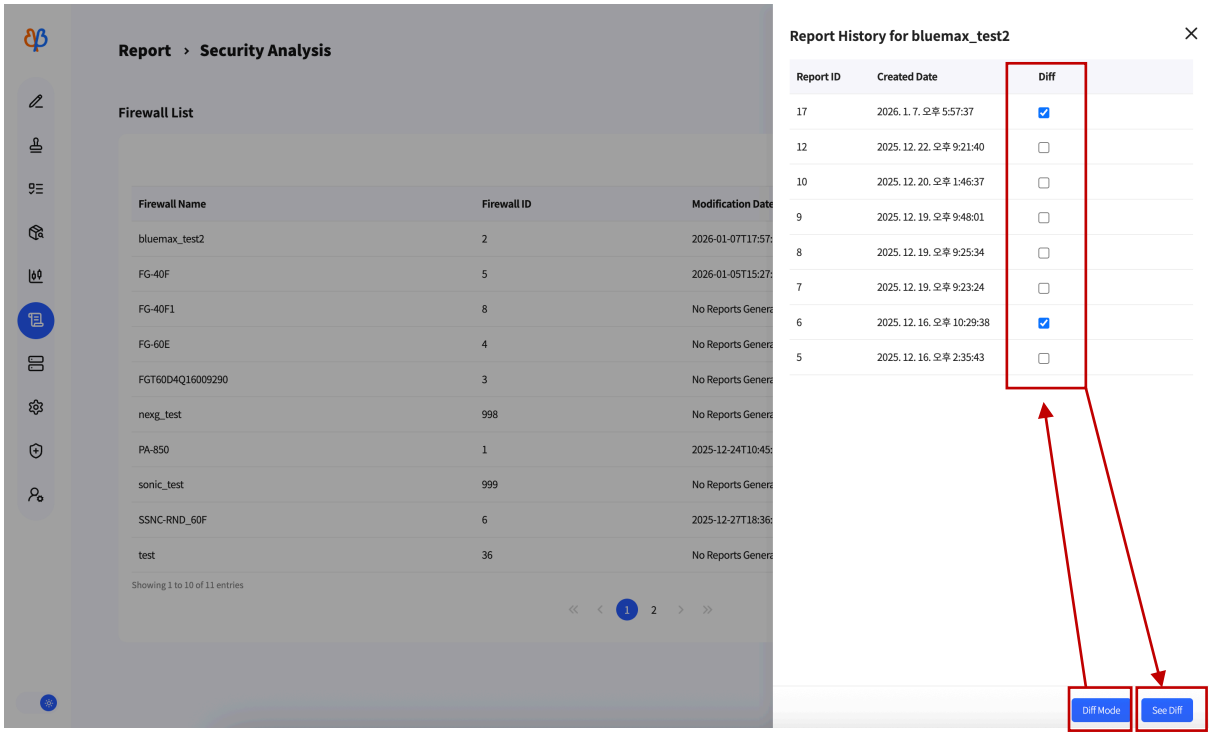
Clicking a major category name in the right table of the <Firewall Policy Analysis Screen> displays a policy list table at the bottom of the screen containing the details classified under that category.




〈Firewall Policy Analysis - When clicking a subcategory detail name〉

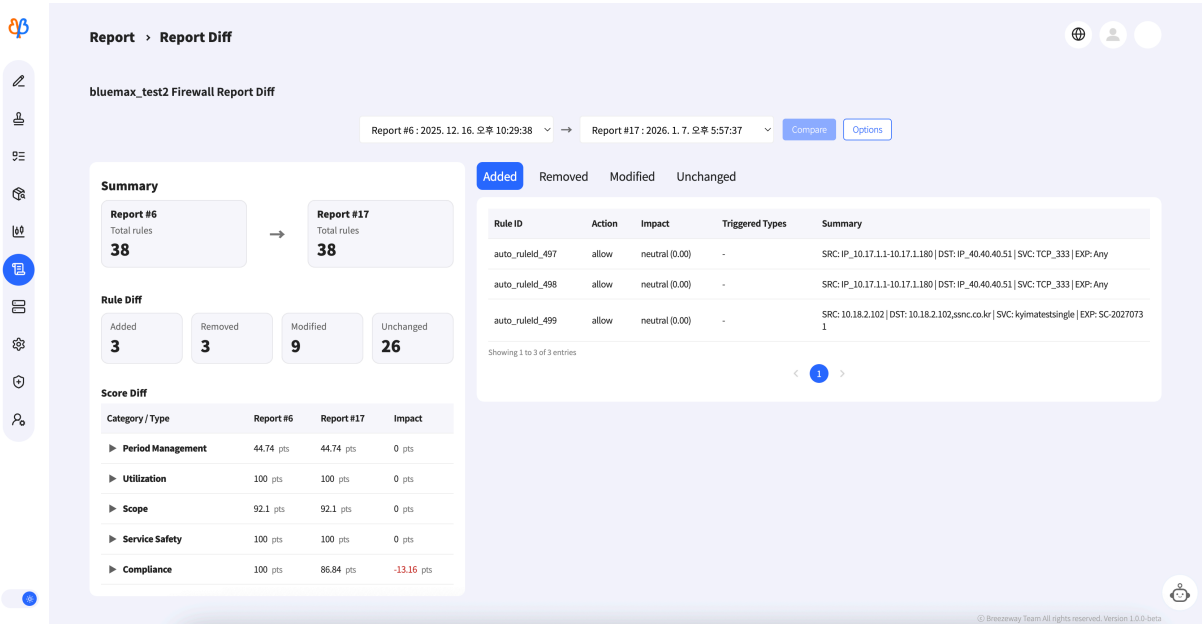
Clicking a subcategory detail name in the right table of the 〈Firewall Policy Analysis Screen〉 displays a policy list table at the bottom of the screen containing policies included in that detail within the category.

- Security Analysis - Firewall Report Difference Analysis




〈Firewall Policy Analysis - When Clicking Diff Mode〉

This feature allows you to analyze differences for generated reports. Select Diff Mode, choose the report for difference analysis, and click See Diff.




〈Firewall Policy Analysis - Report Difference Analysis〉

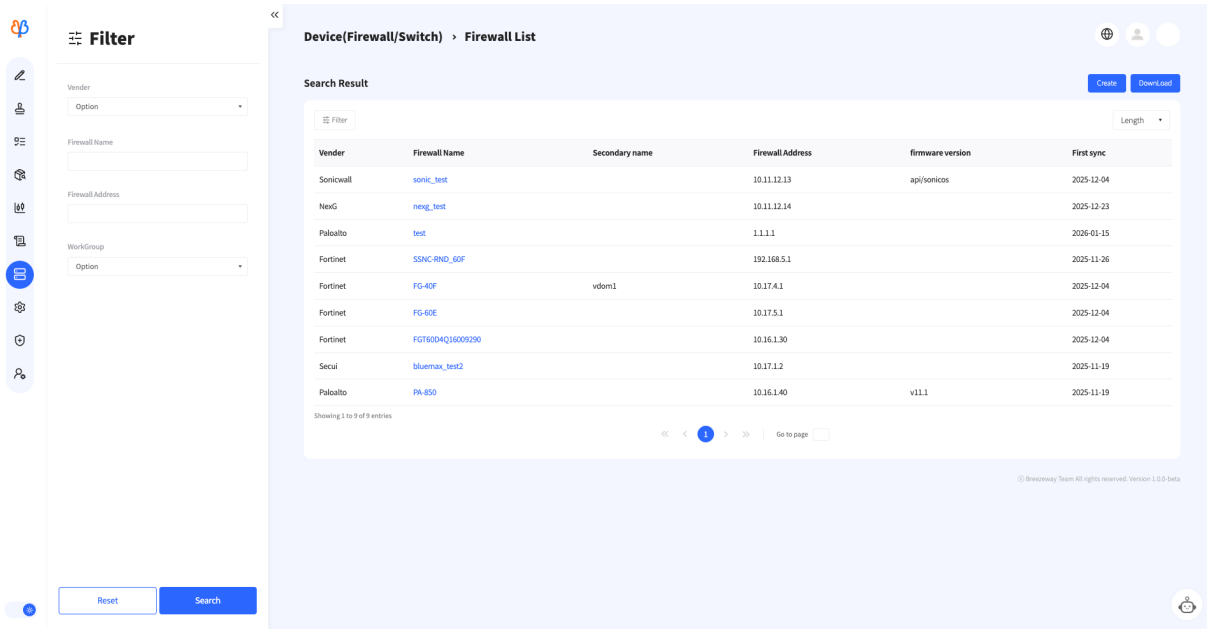
You can view policy changes when comparing two reports. It displays added policies, removed policies, modified policies, and unchanged policies. It also shows the firewall security score impact of these changes.

- Note: Security analysis reports analyze the firewall security status at a snapshot and are not automatically updated. To view the latest information, you must generate a new report.

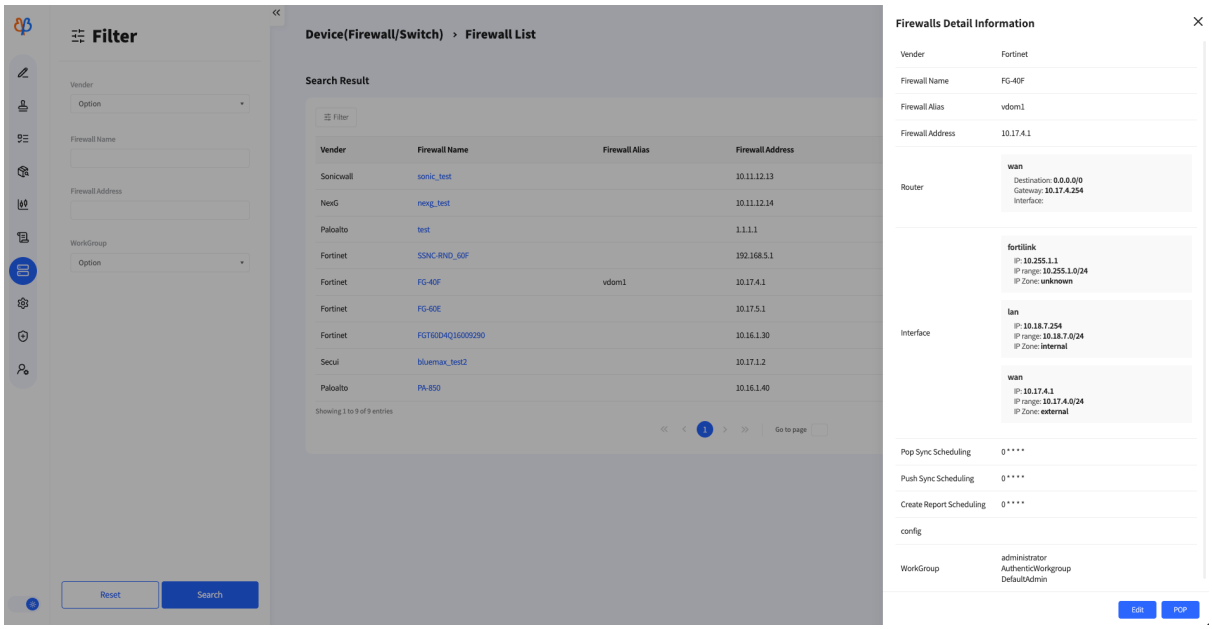
### 2.1.11 Equipment (Firewall) Management

Security administrators can register and manage firewalls and network equipment.

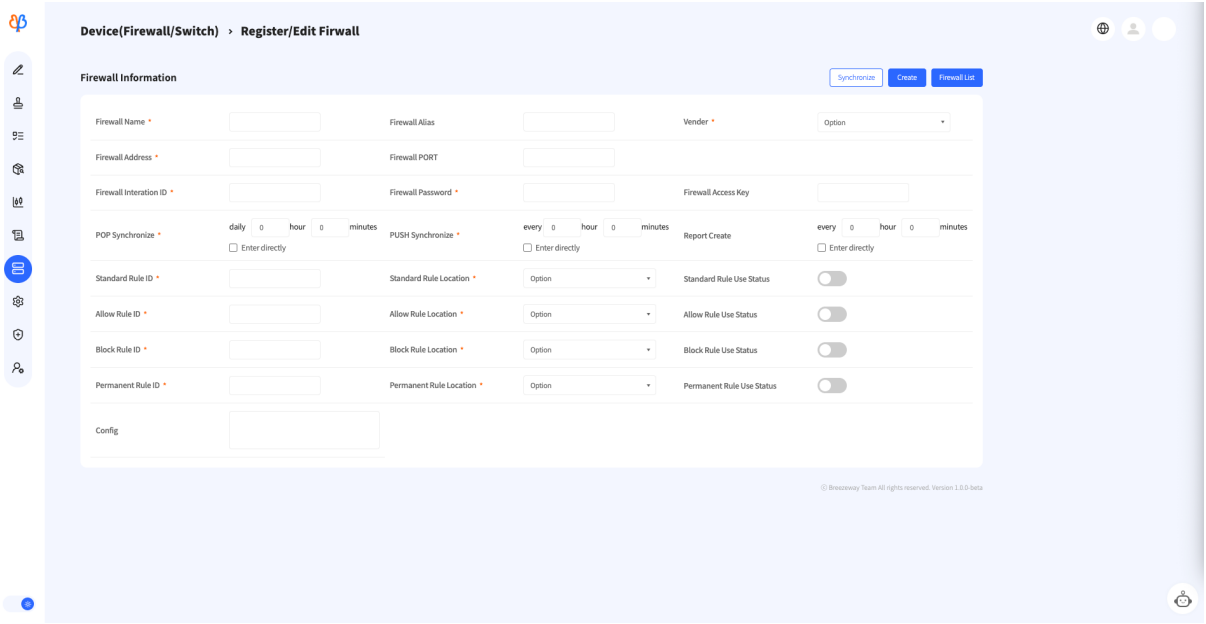
#### 1) Firewall List




〈Firewall List Screen〉




〈Firewall Details Screen〉




〈Firewall Registration Screen〉

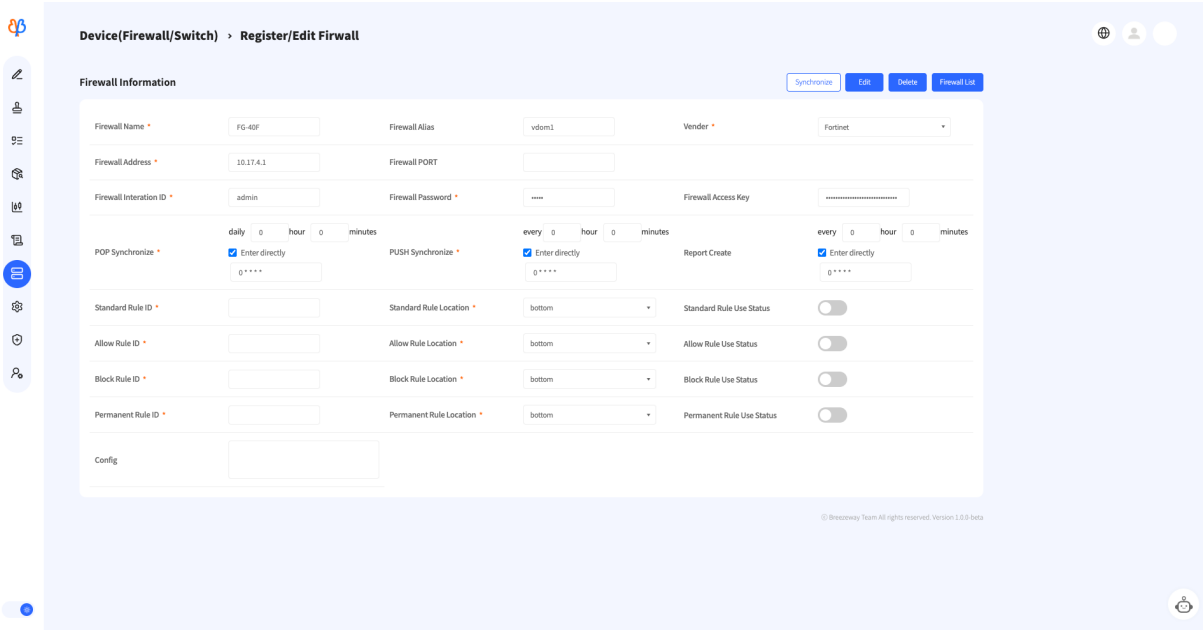
Clicking a firewall name displays its detailed information. Manual POP and firewall information can be modified via the modal on the right side of the details. Additionally, a new firewall can be added using the Create button.

- Firewall Registration/Edit Screen Input Fields

| Required | Item Name | Description |
|---|---|---|
| * | Firewall Name | Name of the firewall to be registered |
| | Firewall Secondary Name | Firewall name to register when using VDOM |
| * | Manufacturer | Select the manufacturer from the dropdown menu |
| * | Firewall Address | Enter the firewall's IP address |
| | Firewall Port | Enter the firewall port number |
| * | Firewall Link ID | Enter the integration ID provided by the firewall |
| * | Firewall Password | Enter the integration password provided by the firewall |
| * | Firewall access key | Enter the key (token) required for firewall integration |
| * | POP Synchronization | Write the firewall data synchronization time in crontab format |

| | | |
|---|---|---|
| * | PUSH Synchronization | Write the firewall data transmission time in crontab format |
| | Schedule report generation tasks | Write the automatic report generation cycle in crontab format<br>(*Currently unsupported) |
| * | Base Rule ID | Specify the firewall policy to be used as the baseline when generating the initial firewall report |
| * | Reference Rule Location | Select the direction for applying the specified baseline rule |
| * | Whether to use the base rule | Select whether to use the standard rule |
| * | Allow Rule ID | Specify the allow firewall policy to be used as the baseline when generating the initial firewall report |
| * | Allow Rule Position | Select the direction for applying the specified allow rule criteria |
| * | Enable/Disable Allow Rules | Select whether to use the allow rule |
| * | Block Rule ID | Specify the baseline blocking firewall policy when generating the initial firewall report |
| * | Block rule location | Select the direction for applying the specified block rule |
| * | Block rule usage status | Select whether to use the block rule |
| * | Permanent Rule ID | Specify the permanent firewall policy to be used as the basis when generating the initial firewall report |
| * | Permanent Rule Location | Select the application direction based on the specified permanent rule |
| * | Permanent rule usage | Permanent Rule Usage Selection |
| * | Config | Additional Information Config Settings (JSON format supported) |

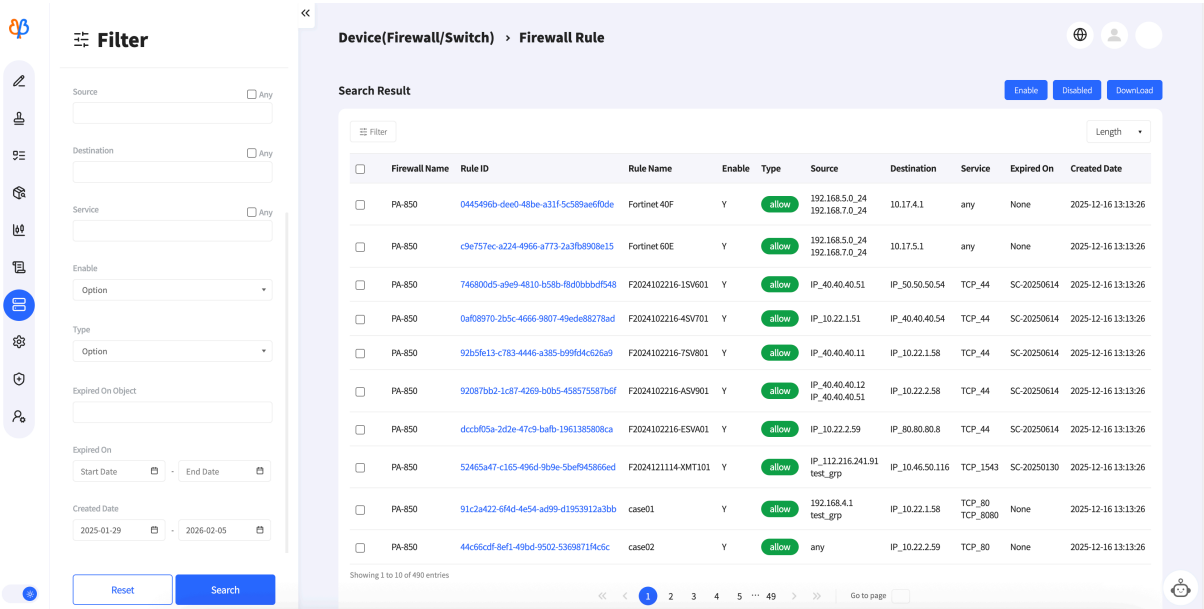
- Modify/Delete Firewall



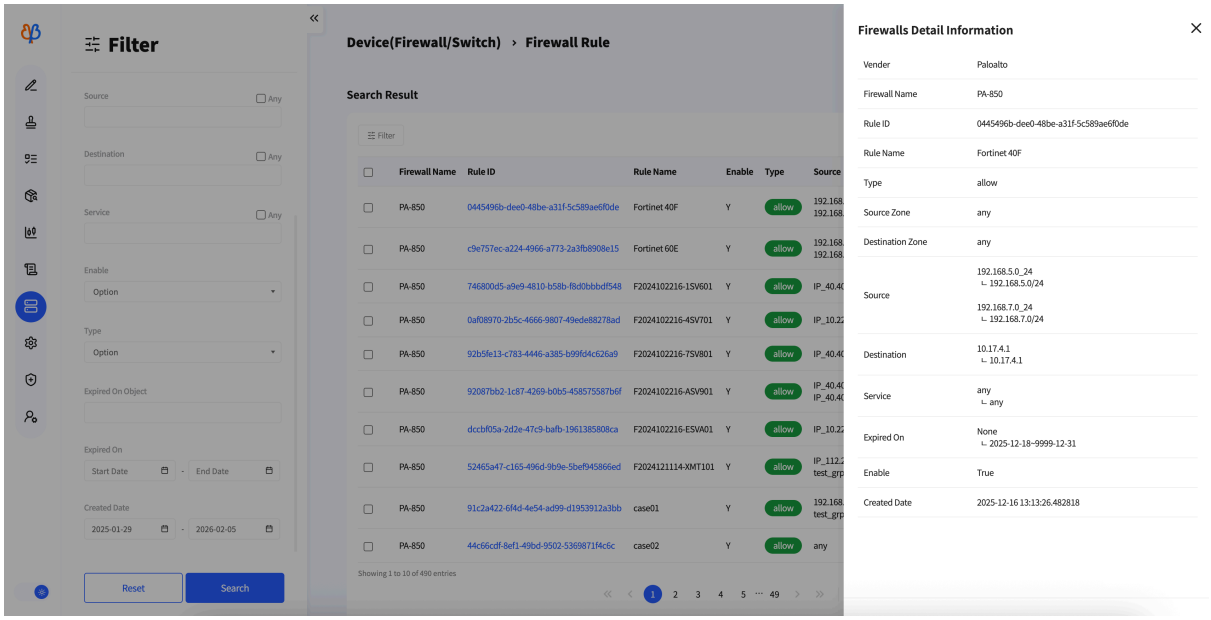

〈Firewall Edit/Delete Screen〉

The firewall edit/delete function can be accessed by clicking the 'Edit' button in the firewall details tab.

- Firewall Policy



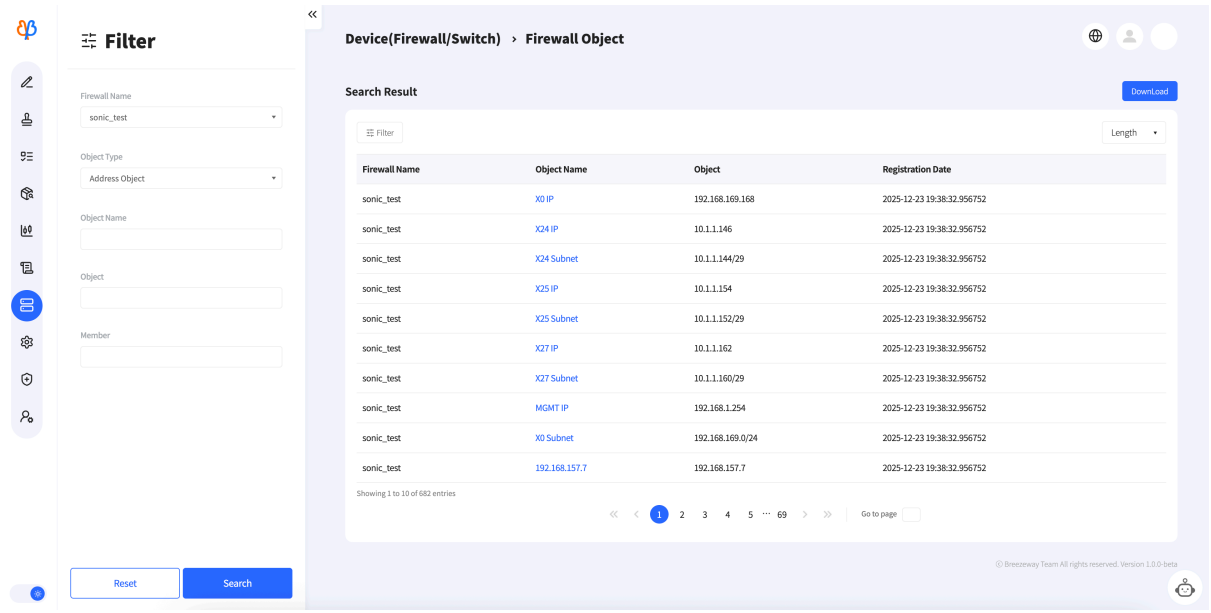

〈Firewall Policy List Screen〉



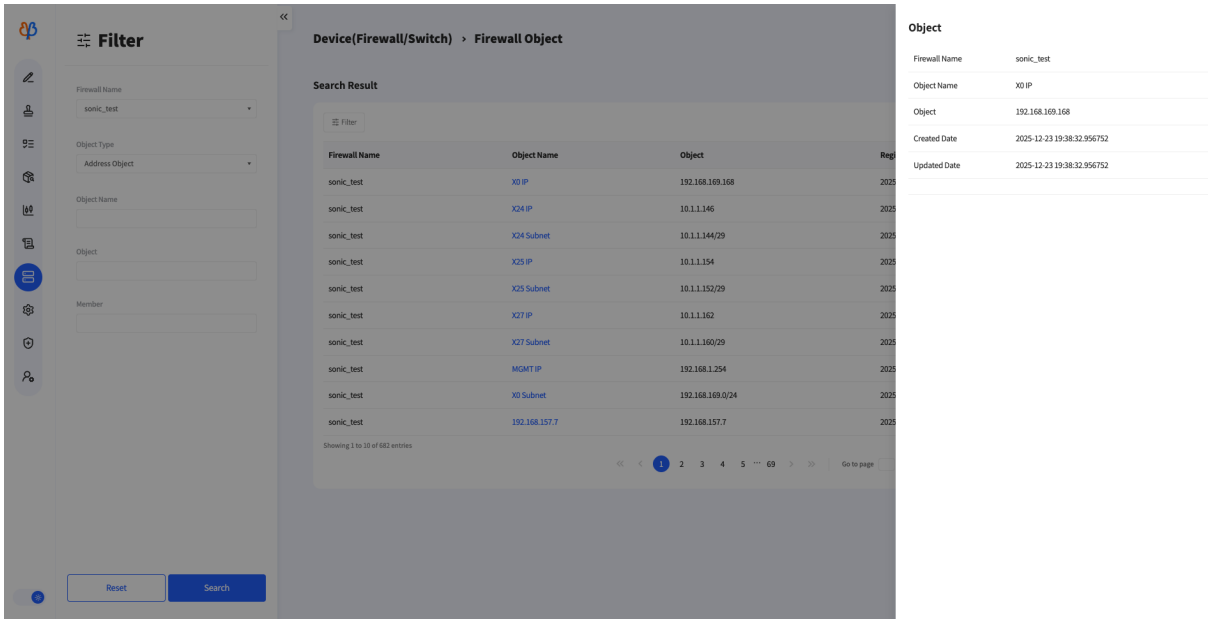

〈Firewall Policy Details Screen〉

You can view policies registered on the firewall by firewall. Clicking a rule ID allows you to view the policy's detailed information.

- Firewall Objects




〈Firewall Object List Screen〉



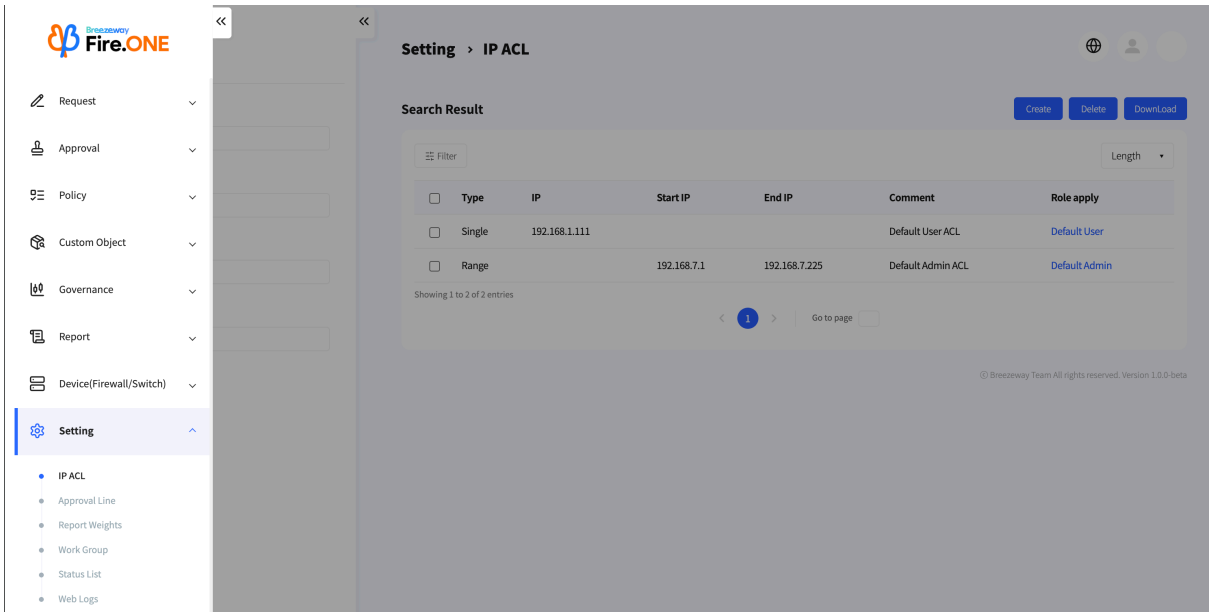

〈Firewall Object Details Screen〉

You can synchronize and view the list of objects registered on the firewall. You can filter and view by firewall, object type, object name, object, or member. Clicking an object name allows you to view the object's detailed information.

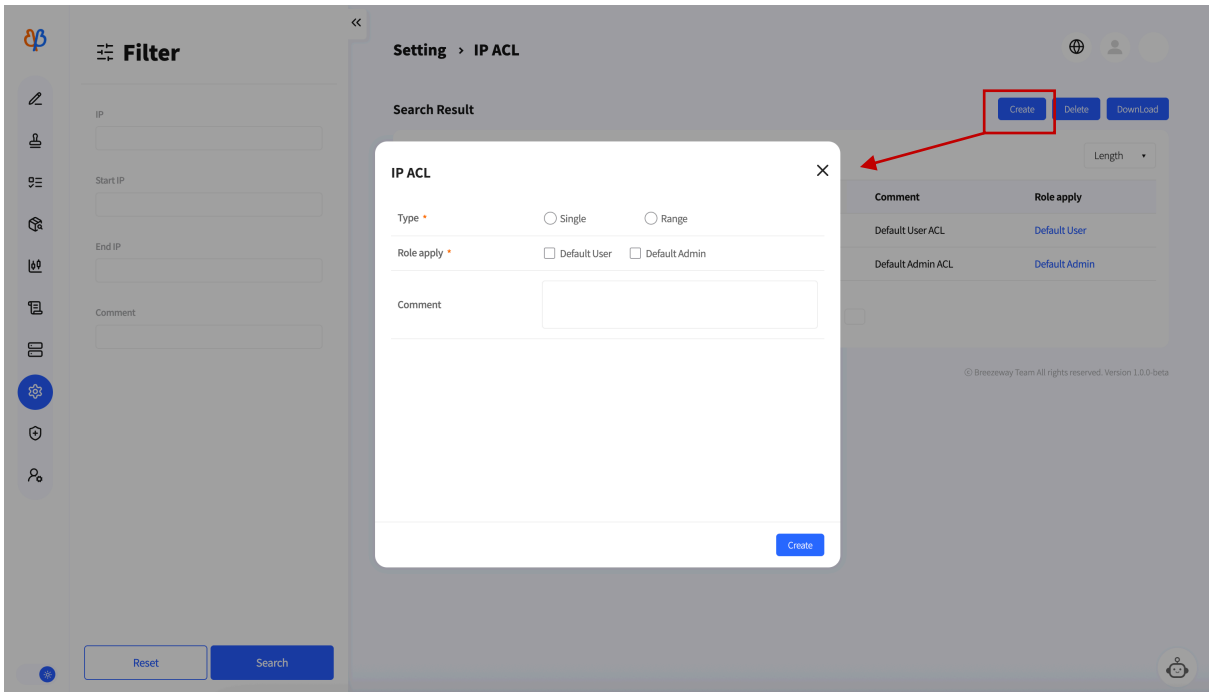
## 2.1.12 Settings

Configure general elements required for website operation when using the product.

### 1) Access Restriction



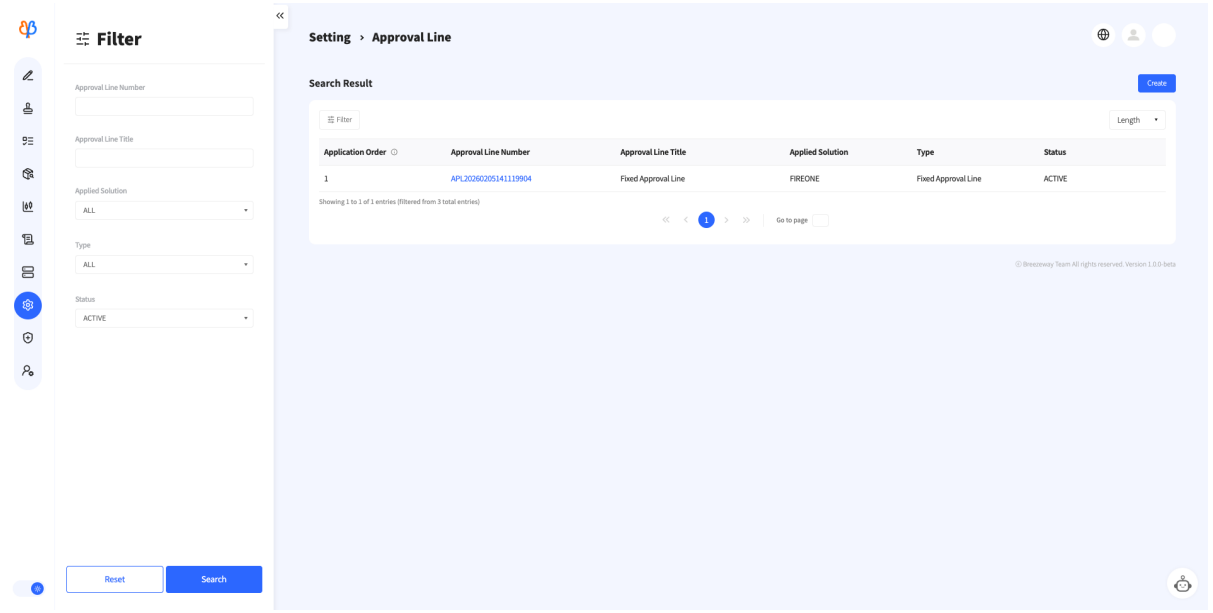

〈Access Restriction List Screen〉



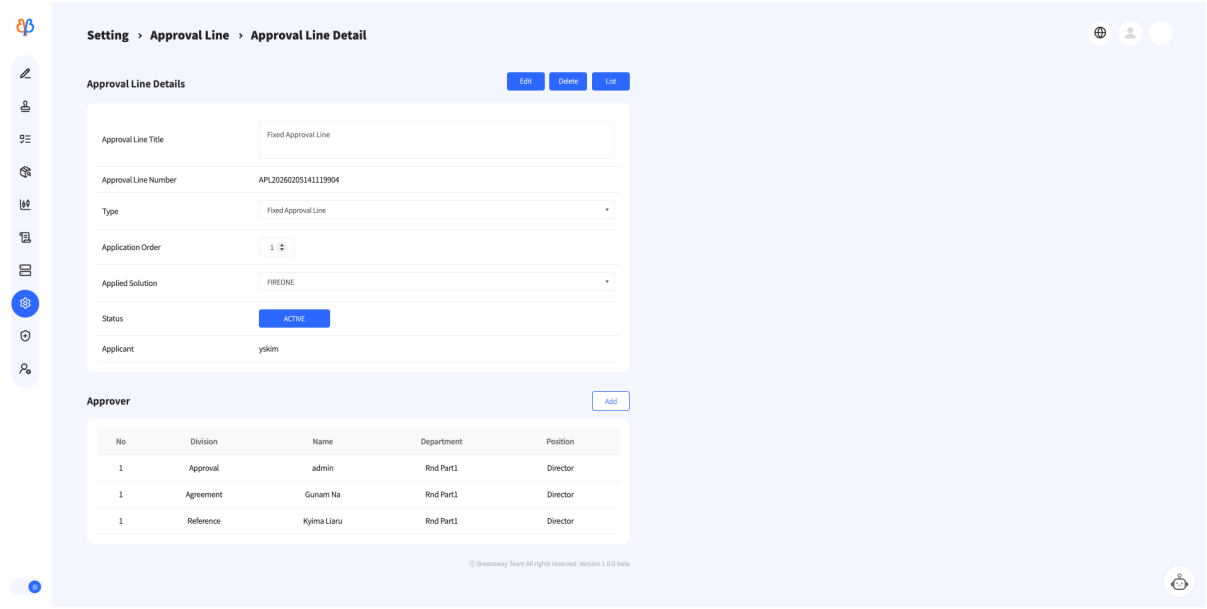

〈Access Restriction Creation Screen〉

Configure access allow/block settings for specific IP addresses or network ranges. You can create a new access restriction using the Create button in the upper-right corner of the screen. You can select users to whom the access restriction will apply by 'Menu Access Restriction Group'.

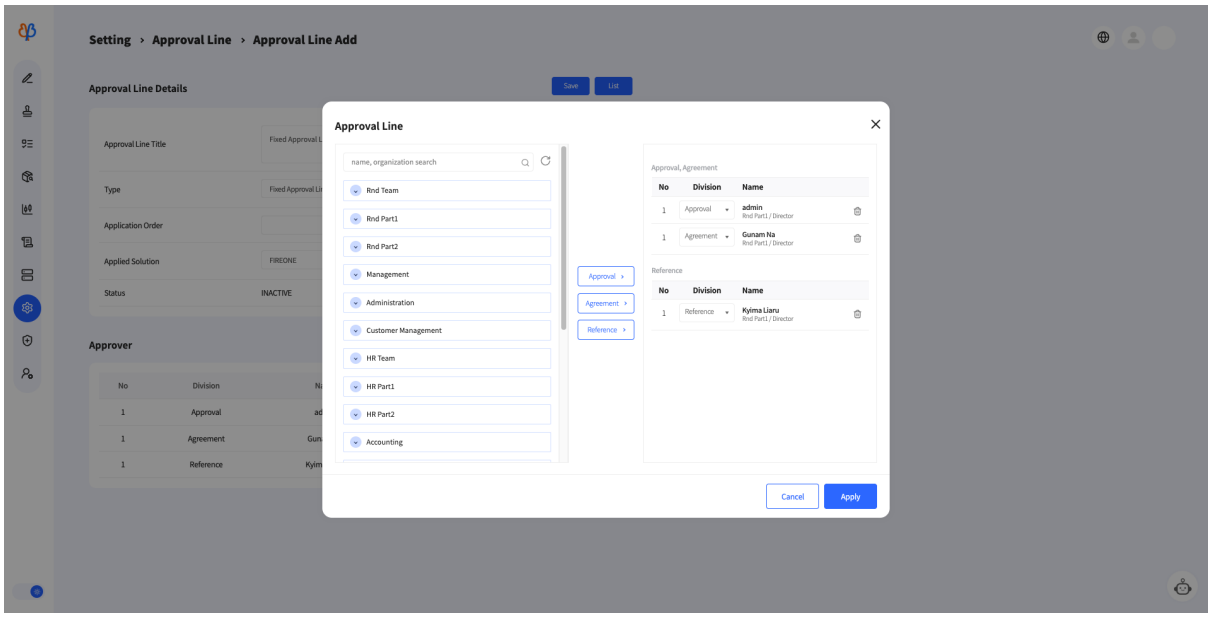
2) Fixed Approval Chain




〈Fixed Approval Chain List Screen〉




〈Fixed Approval Route Details Screen〉




〈Fixed Approval Line Approver Designation Modal Screen〉

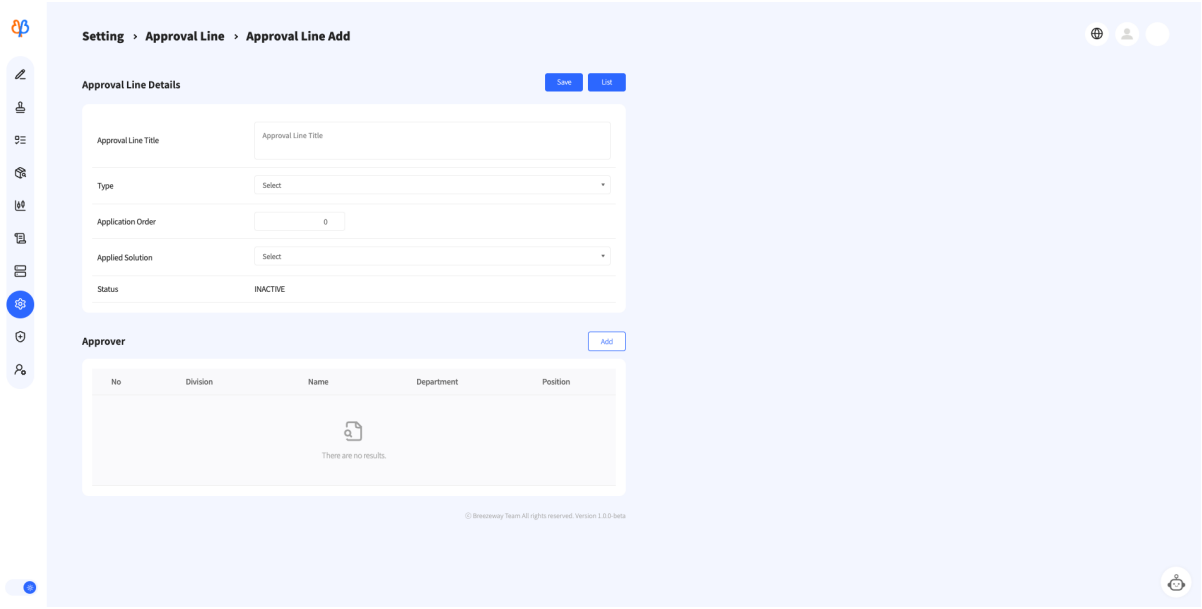
When approval from specific individuals is mandatory, use a fixed approval line to prevent users from arbitrarily excluding those approvers.
By default, only one fixed approval route can be used per solution. When activated, it automatically applies to all approval submissions within that solution.

- View Fixed Approval Line

You can view the basic information of created fixed approval lines and the designated approvers, consensus members, and reference members. Fixed

approval lines are only reflected on the approval submission page when their status is 'Active'.

- Creating a Fixed Approval Line




〈Fixed Approval Route Creation Screen〉

Clicking the 'Create' button located at the top right of the Fixed Approval Line List screen takes you to the Fixed Approval Line Add page. You can specify the fixed approval line's basic information (name, type, application order, applied solution) and approver information.
When creating a fixed approval line, it is created in an inactive state by default. When you enter all the information you need and press the ‘Save’ button, a notification will appear asking if you want to activate the fixed approval Line.

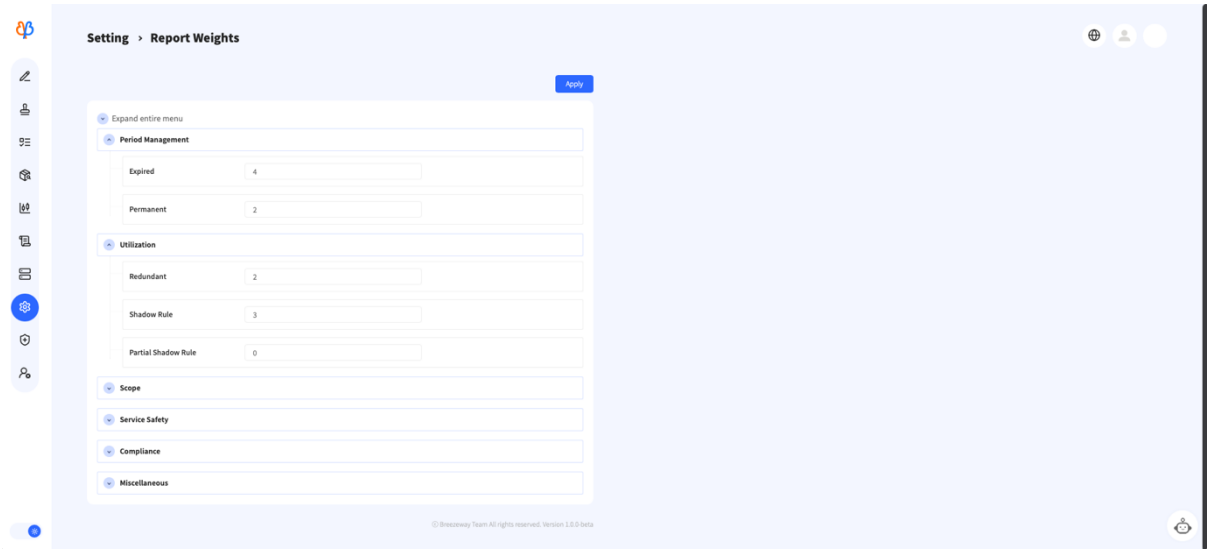
- Modifying Fixed Approval Routes

You can modify the approval route's basic information and approver details on the Fixed Approval Route details page. Clicking the Modify button applies the changes.

- Deleting a Fixed Approval Line

Clicking the Delete button on the fixed approval route detail page will delete the fixed approval route.

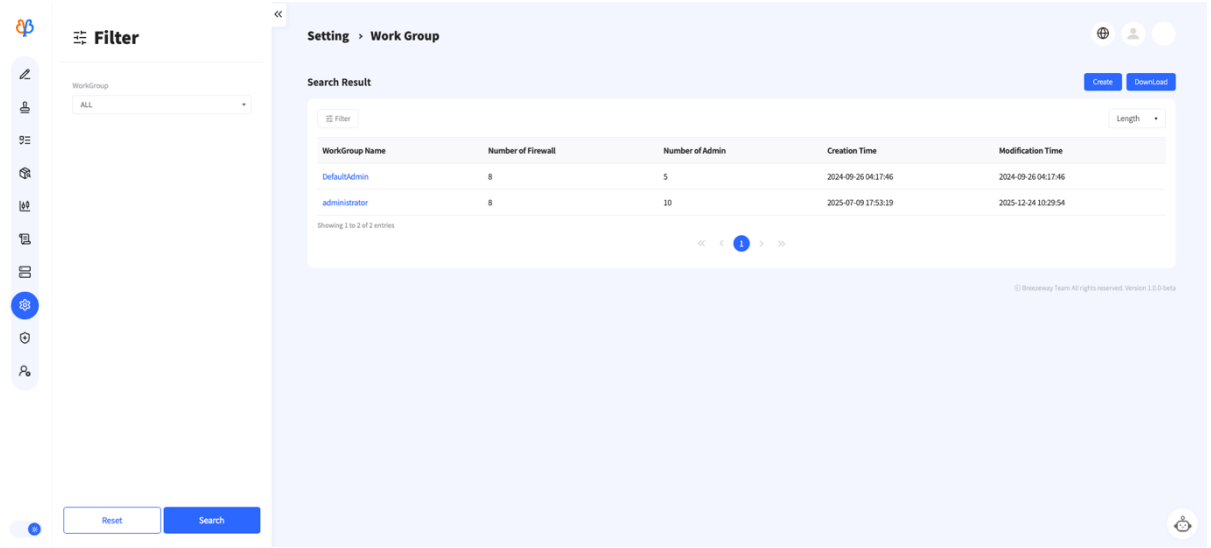
3) Weight



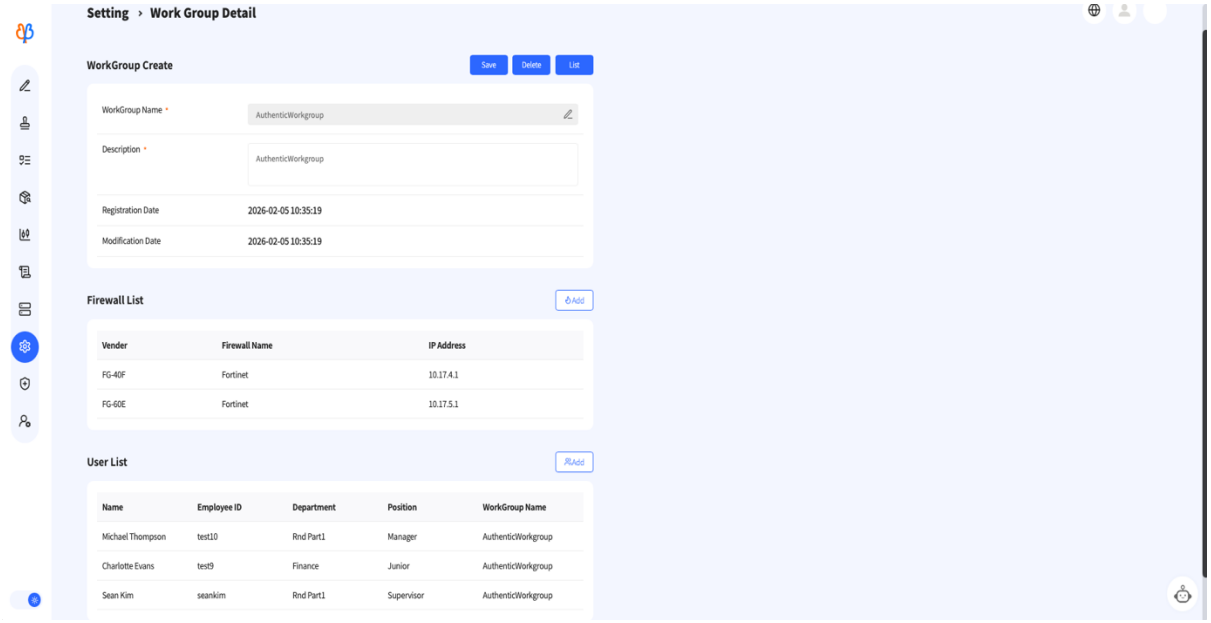

〈Weight Screen〉

This screen registers the weights used in score calculations during report security analysis. After entering weights, clicking the Apply button reflects them when generating reports.

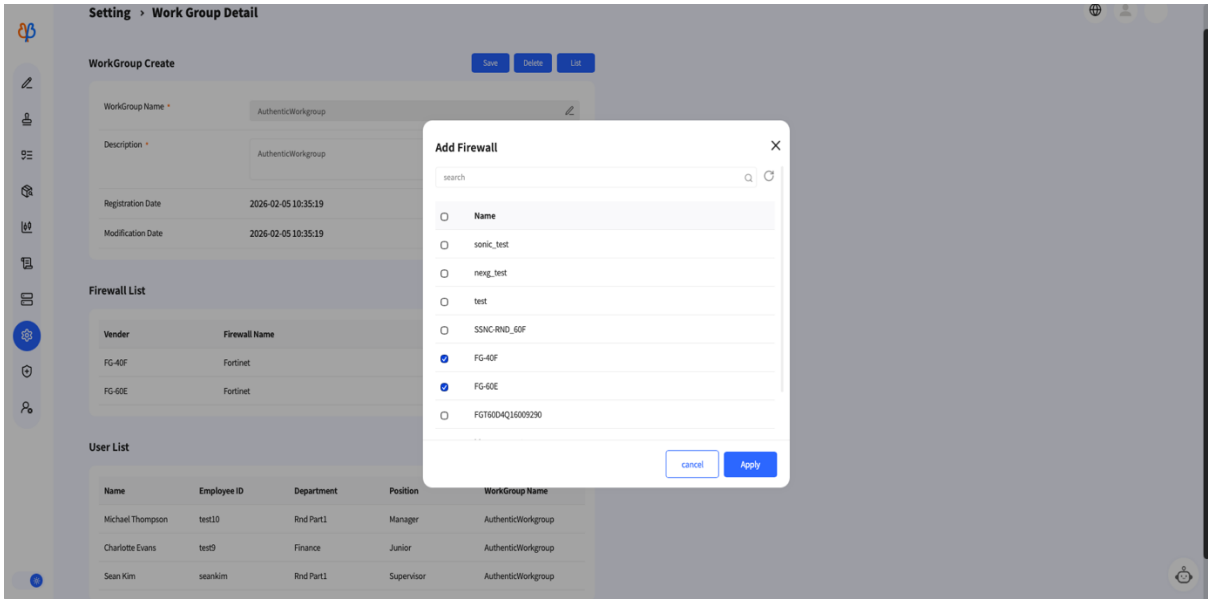
4) Work Group



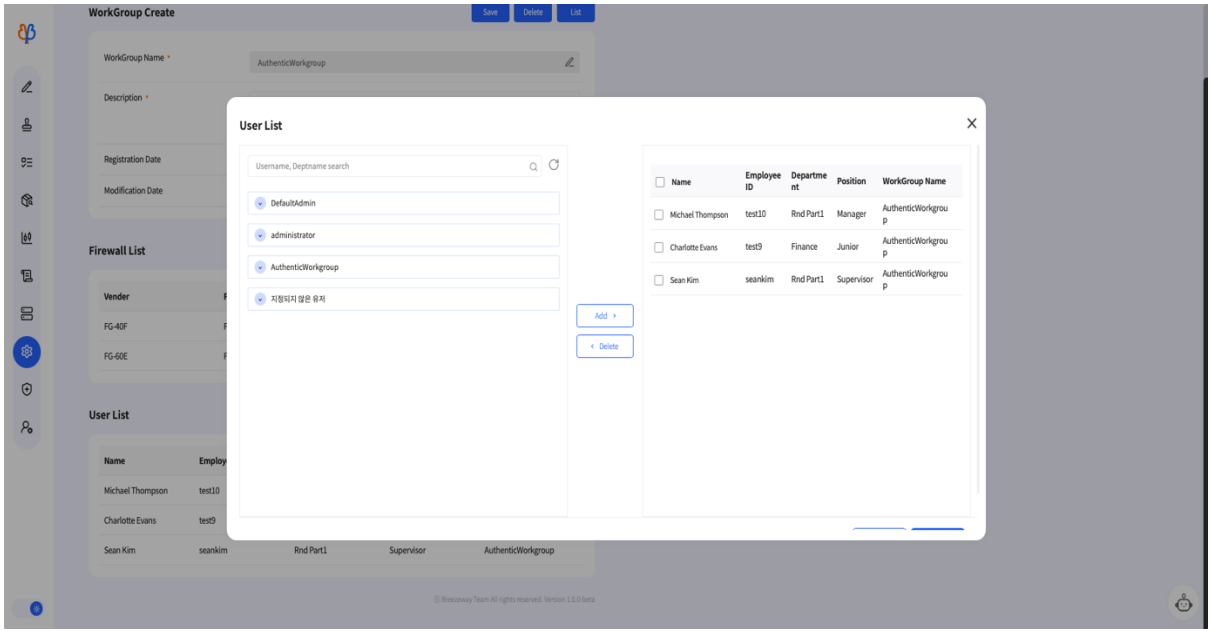

〈Work Group List Screen〉




〈Work Group Details Screen〉




〈Work Group Firewall Assignment Modal〉



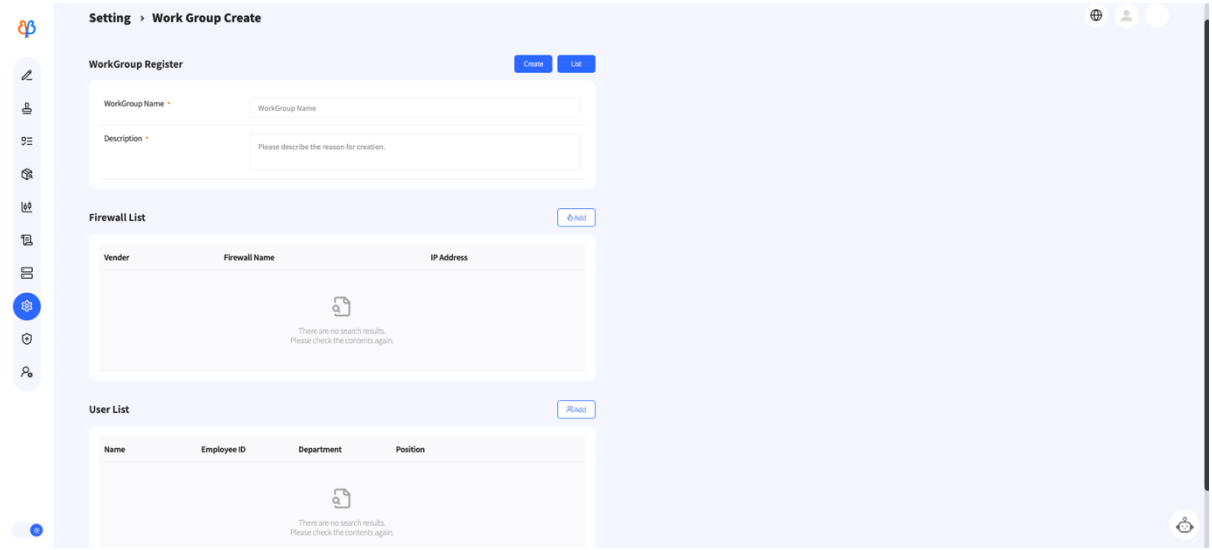

〈Work Group User Assignment Modal〉

Within a workgroup, the firewall administrator can assign the firewall they will manage. The firewall administrator can only view information related to the firewalls assigned to them based on the workgroup, such as in the Policy or Equipment menus.

- View Workgroup Details

You can view the basic information (name, remarks) of the created workgroup, along with the assigned firewall and user information.

- Create Workgroup




〈Workgroup Creation Screen〉

Clicking the Create button in the upper-right corner of the workgroup list takes you to the workgroup creation page. You can create a workgroup by entering the basic workgroup information and adding firewalls and users.

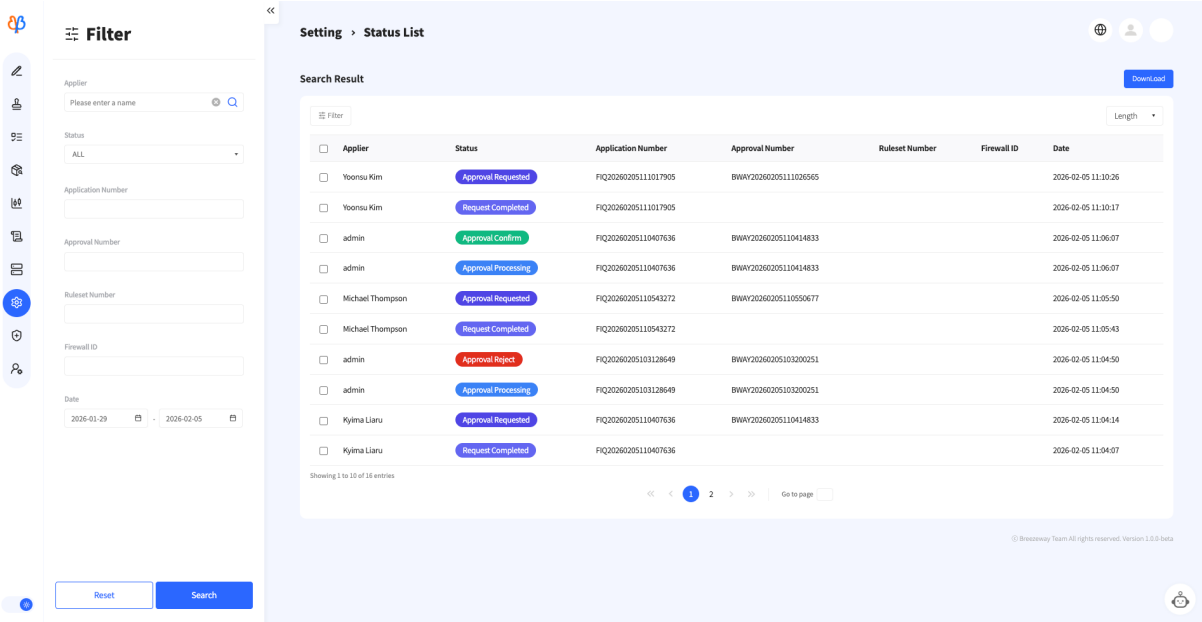
- Modify Workgroup

You can modify the workgroup's basic information and users on the workgroup details page. Clicking the Modify button applies the changes to the workgroup.

- Deleting a Workgroup

Clicking the Delete button on the workgroup details page will delete the specified workgroup.

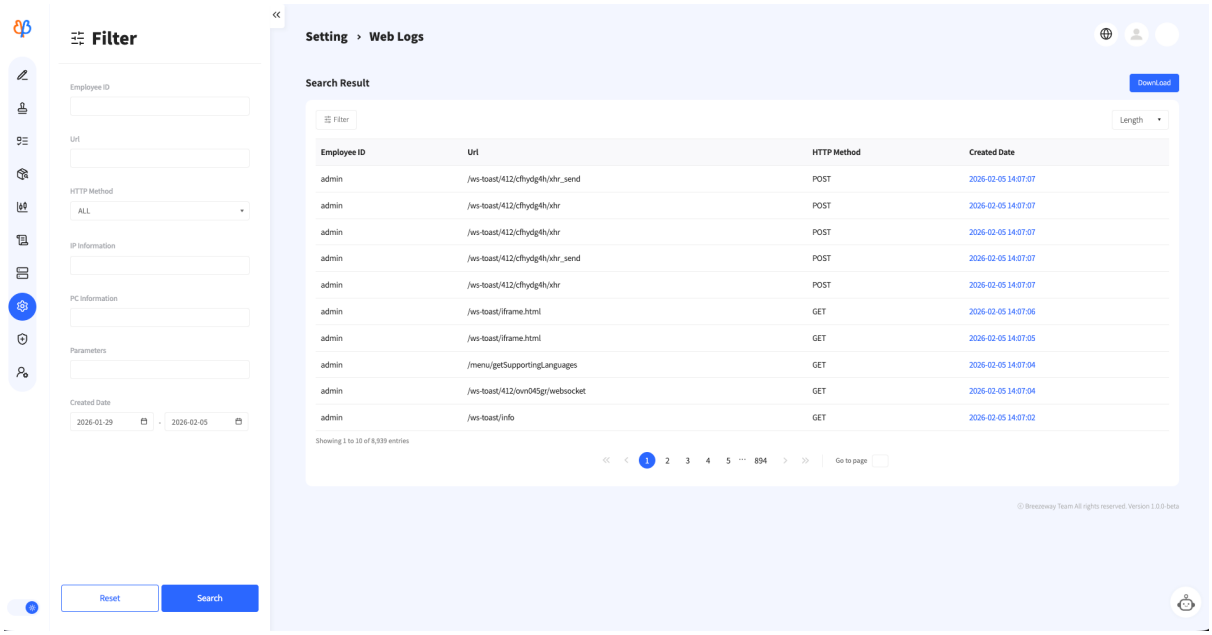
5) Task Processing History



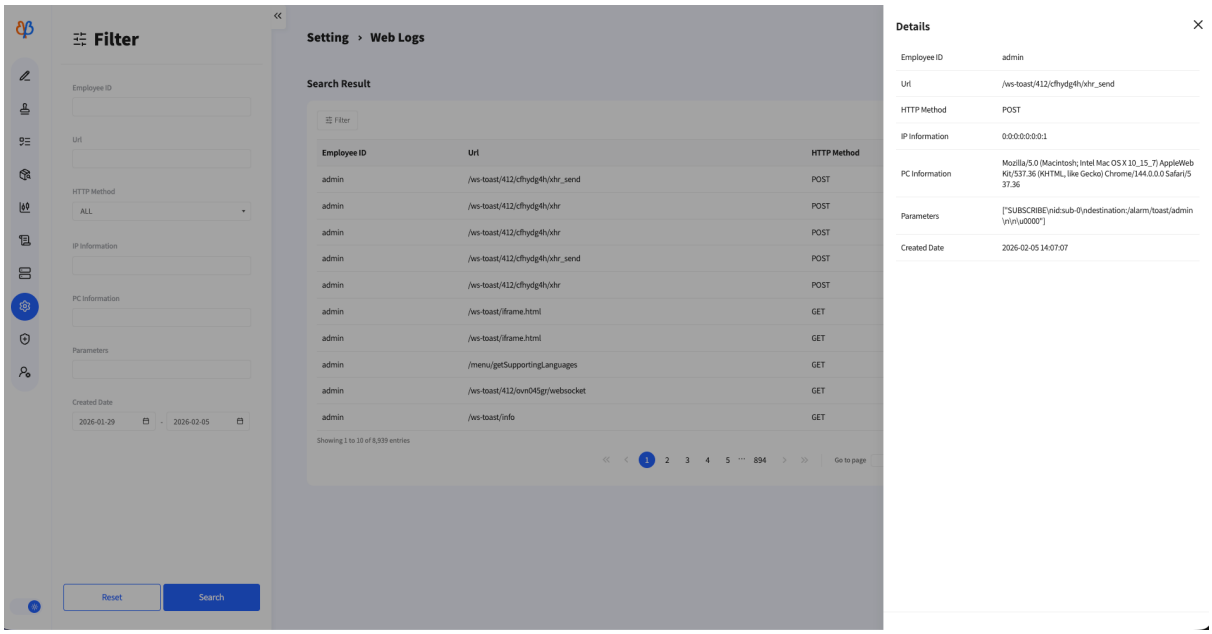

〈Task Processing History Screen〉

You can view the task processing history for all users. The task processing history is updated each time the application, approval, and implementation steps for applying the firewall policy are performed.

6) Web Log




〈Web Log Screen〉



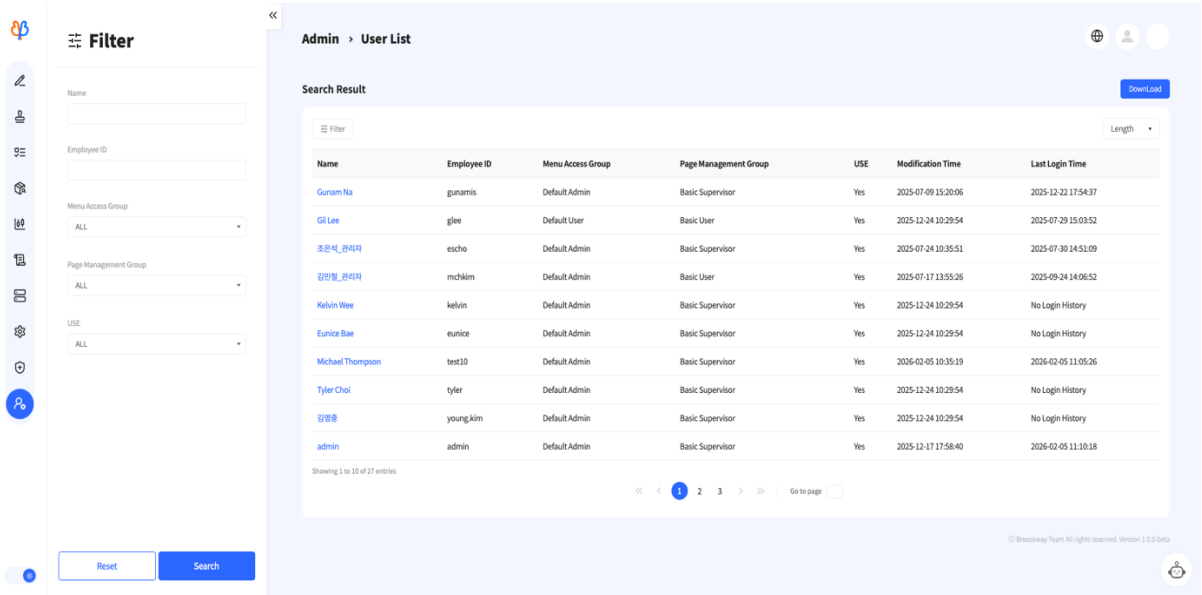

〈Web Log Details Modal Screen〉

You can view the web action logs for all users. All requests originating from the client side are recorded, and the history is updated in real-time. Clicking the creation date allows you to view details about the request.

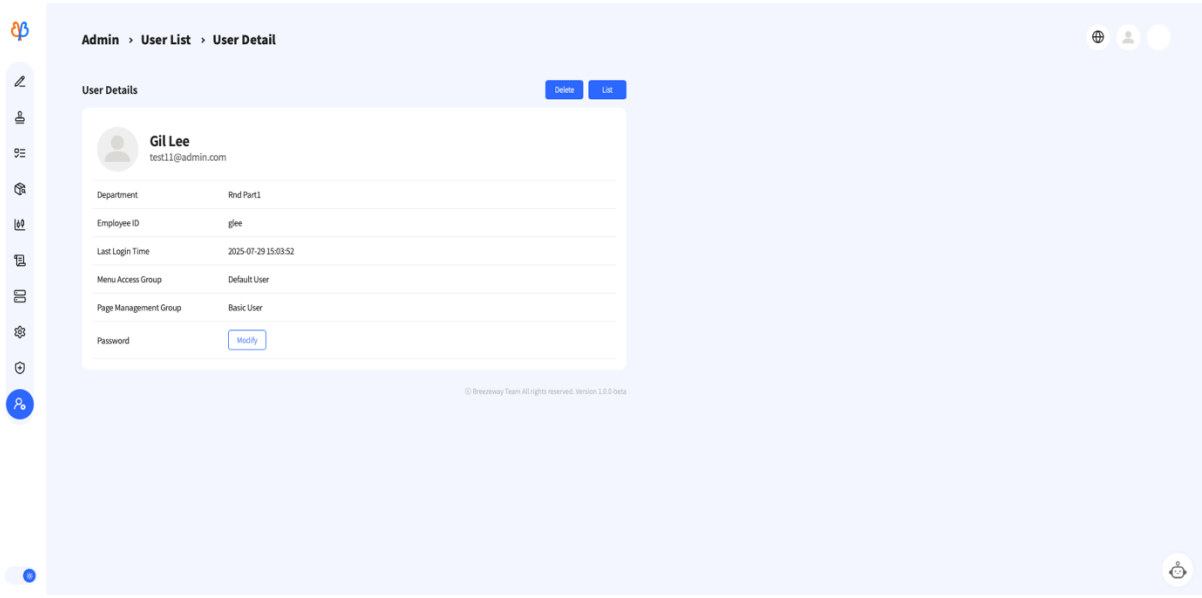
### 2.1.13 Administrator

Administrators can perform tasks that require management/supervision when using the product.

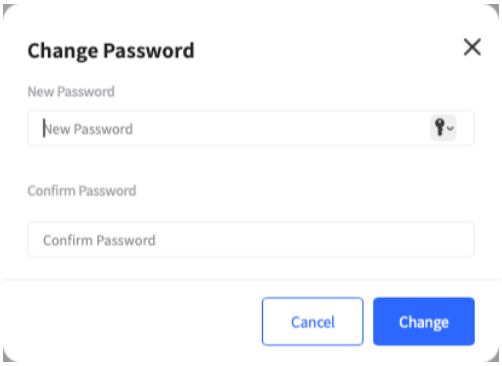
## 1) User List



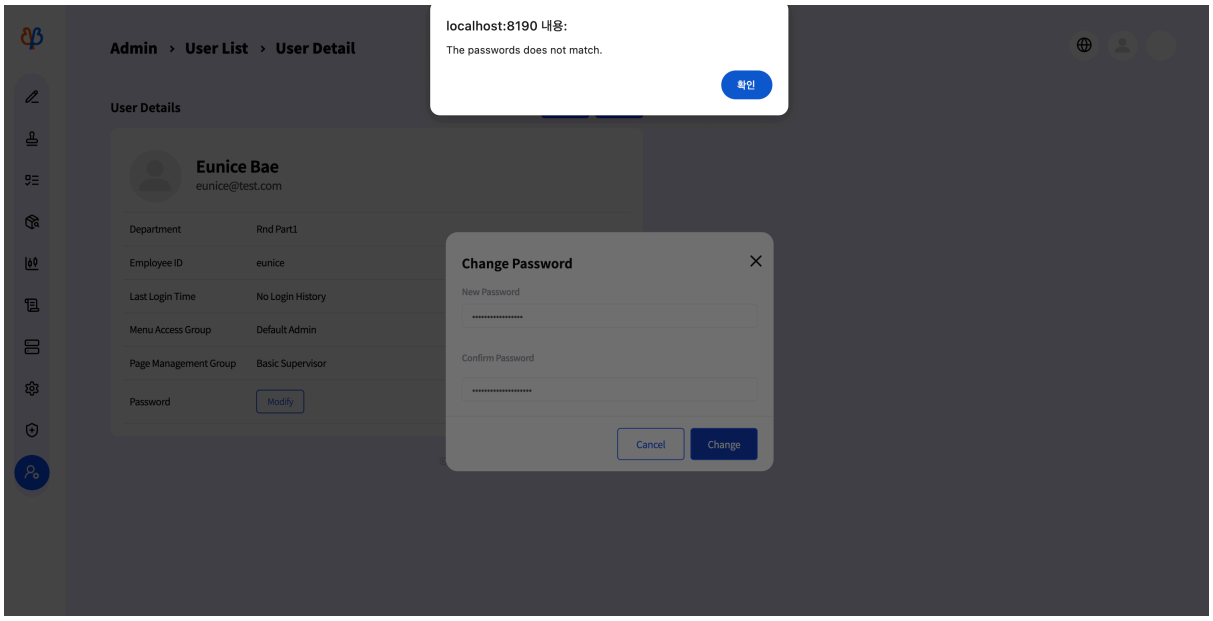

〈User List Screen〉




〈User Details Screen〉




〈Password Change Popup〉




〈If the existing password does not match〉

User accounts can only be created through HR information linkage. On the user list inquiry screen, you can view the list of user accounts registered in the system and the user's activity history. Click a user's name in the list to view their detailed information.

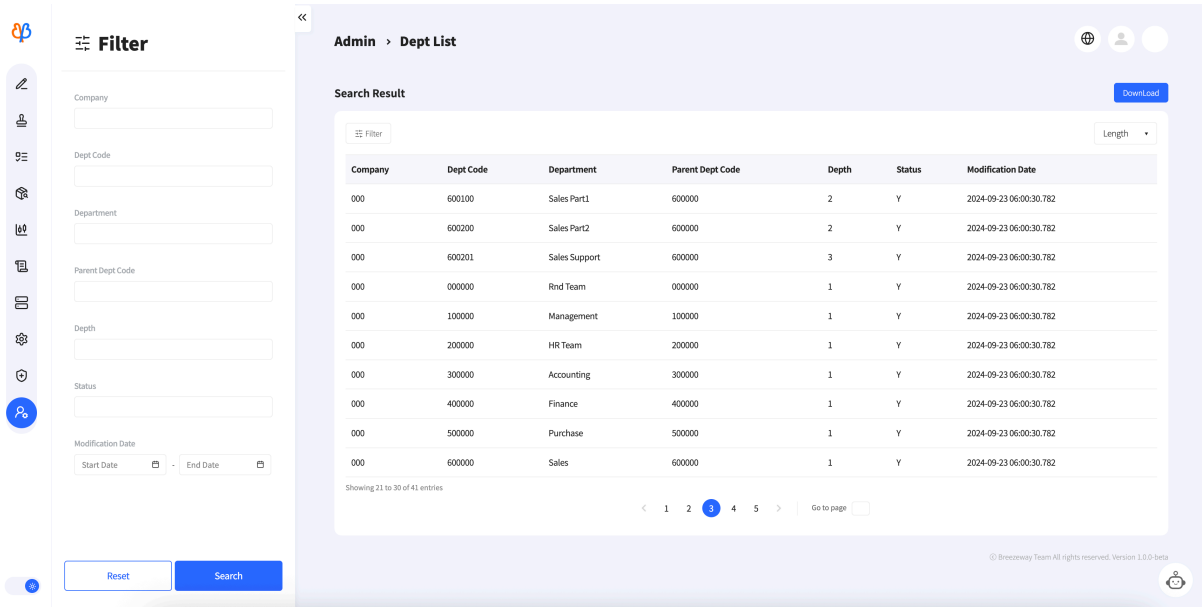
2) User Information Lookup

Quickly view user information such as name, employee number, and email based on HR information linkage.

3) User Information Modification

Since user accounts are created through HR information linkage, name, employee ID, and email information cannot be modified. If a user wishes to change their password or has forgotten it, they can request a password reset from the administrator. Additionally, profile photos can be changed or reset. If no photo is specified, the system's default photo will be used.

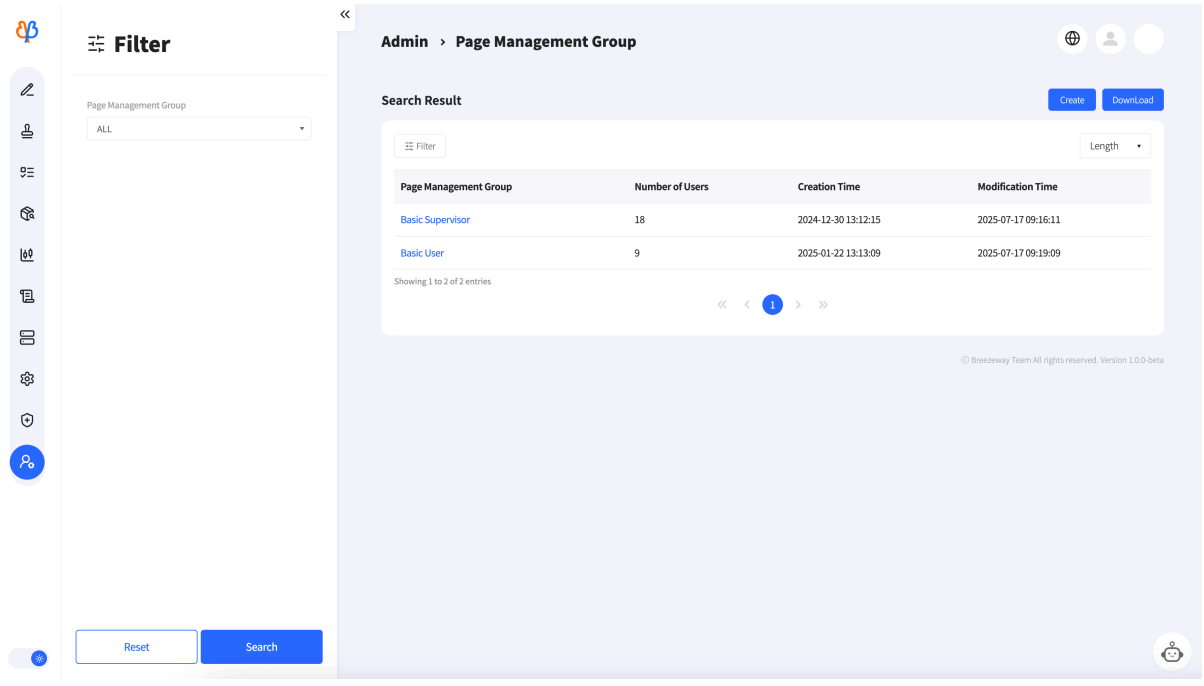
- Department List



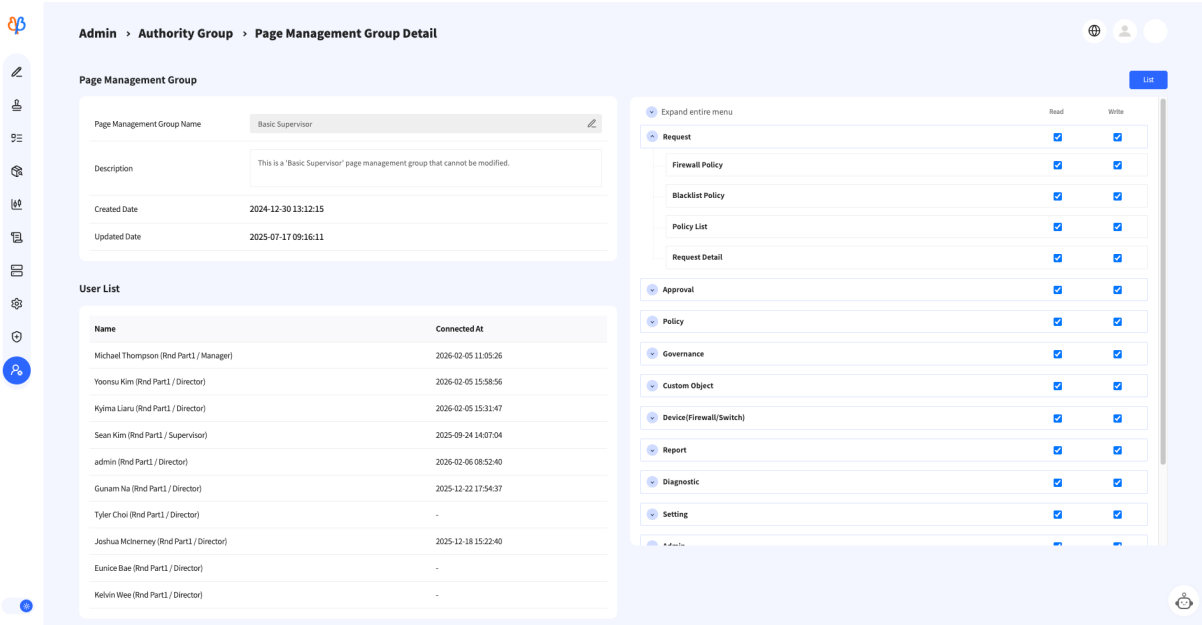

〈Department List Screen〉

You can view department information linked to HR data.

### 4) Page Management Group




〈Page Management Group List Screen〉



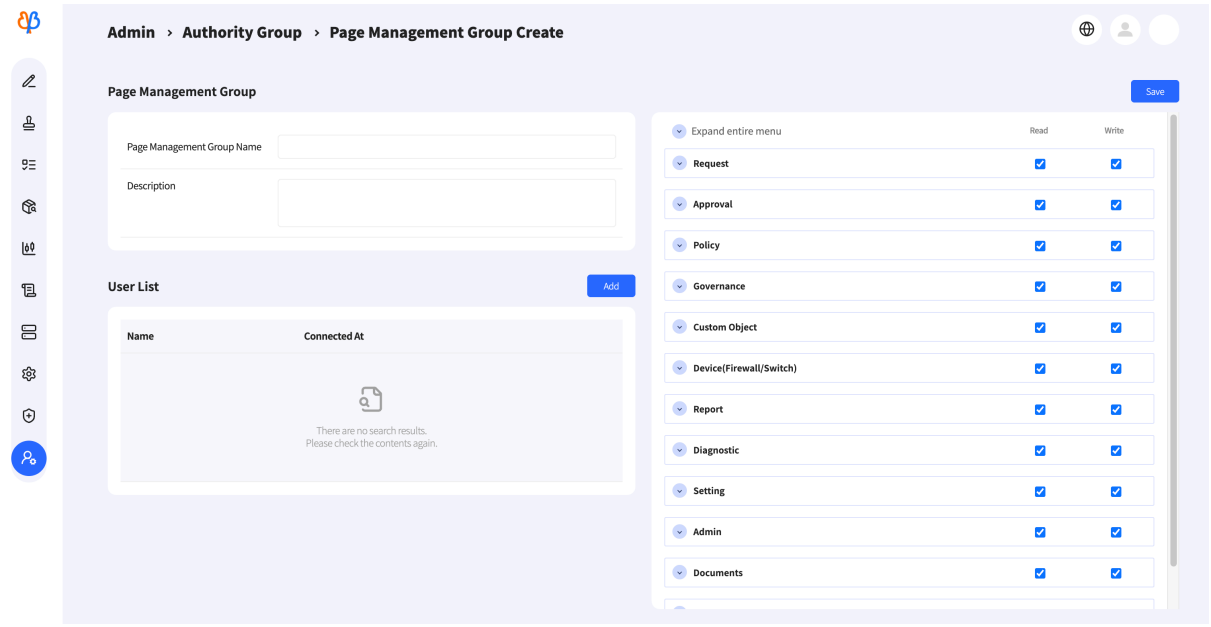

〈Page Management Group Details Screen〉

Restrict user access to features through Page Management Groups. If read or write options are disabled, users cannot utilize the features of that page.

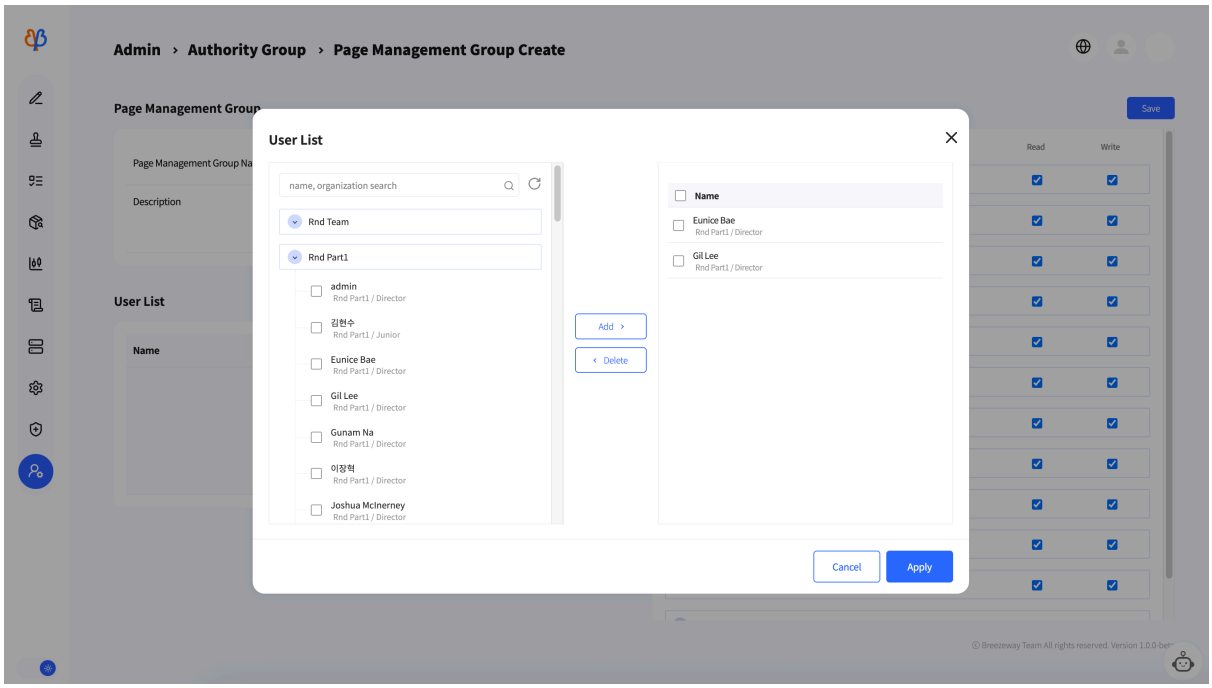
- Page Management Group Inquiry

You can view the basic information of a Page Management Group. Clicking the Page Management Group name takes you to the Page Management Details page. On the details page, you can view the basic information of the Page Management Group, the assigned user information, and the applied functions per menu.

- Page Management Group Creation




〈Page Management Group Creation Screen〉




〈Page Management Group User List Modal Screen〉

Clicking the Create button in the upper-right corner of the Page Management Group List page takes you to the Page Management Group Creation page. You can create a Page Management Group by entering its basic information, adding a user list, specifying functions per page, and saving.

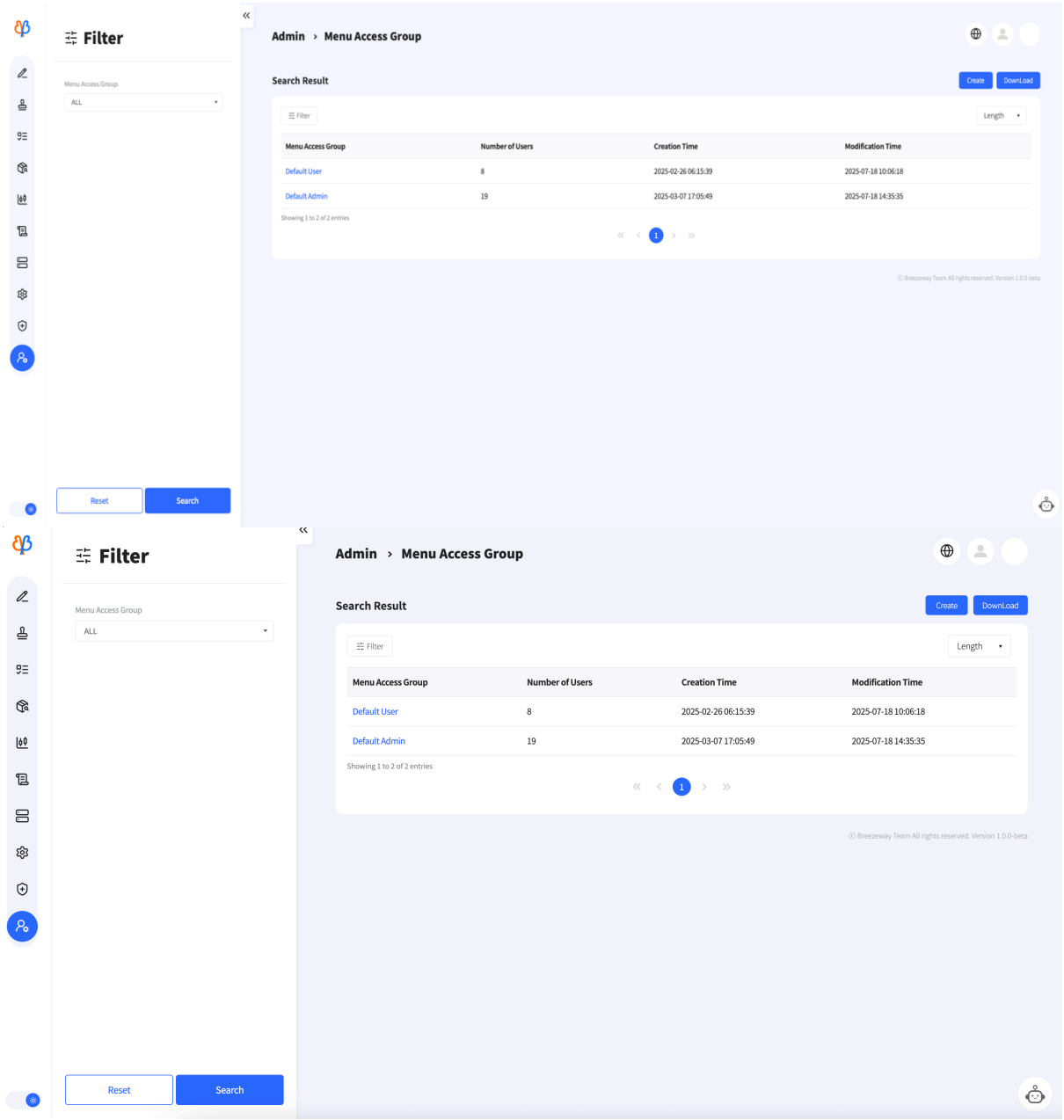
- Modifying a Page Management Group

You can modify relevant information on the page management group details page. Clicking the Edit button applies the changes.

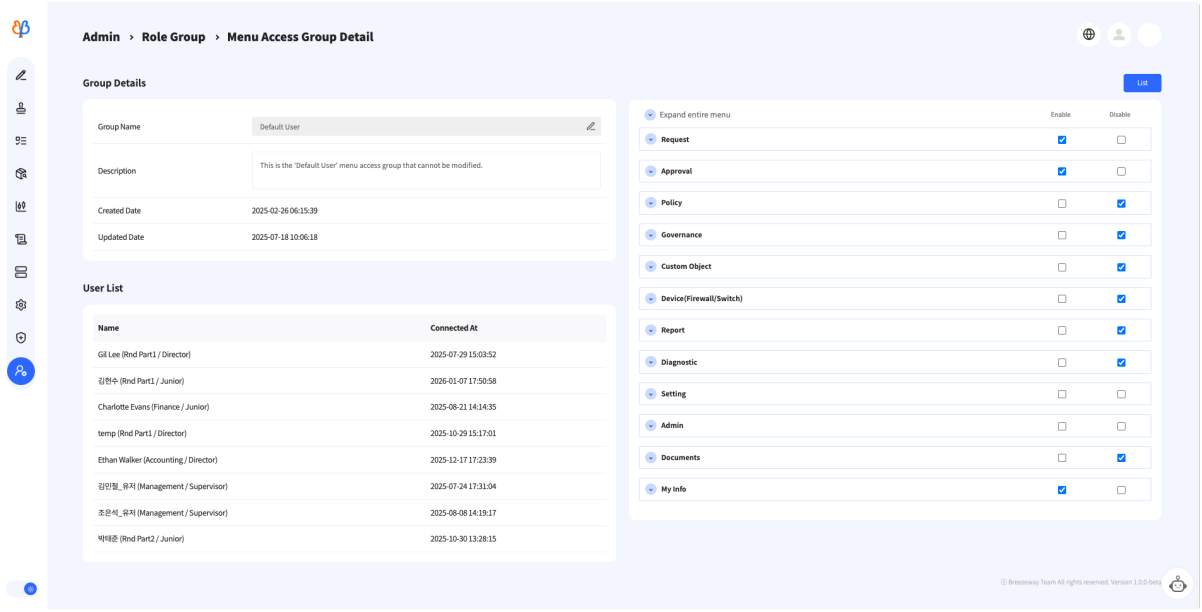
- Deleting a Page Management Group

Clicking the Delete button on the Page Management Group details page will delete that Page Management Group.

5) Menu Access Group




〈Menu Access Group List Screen〉



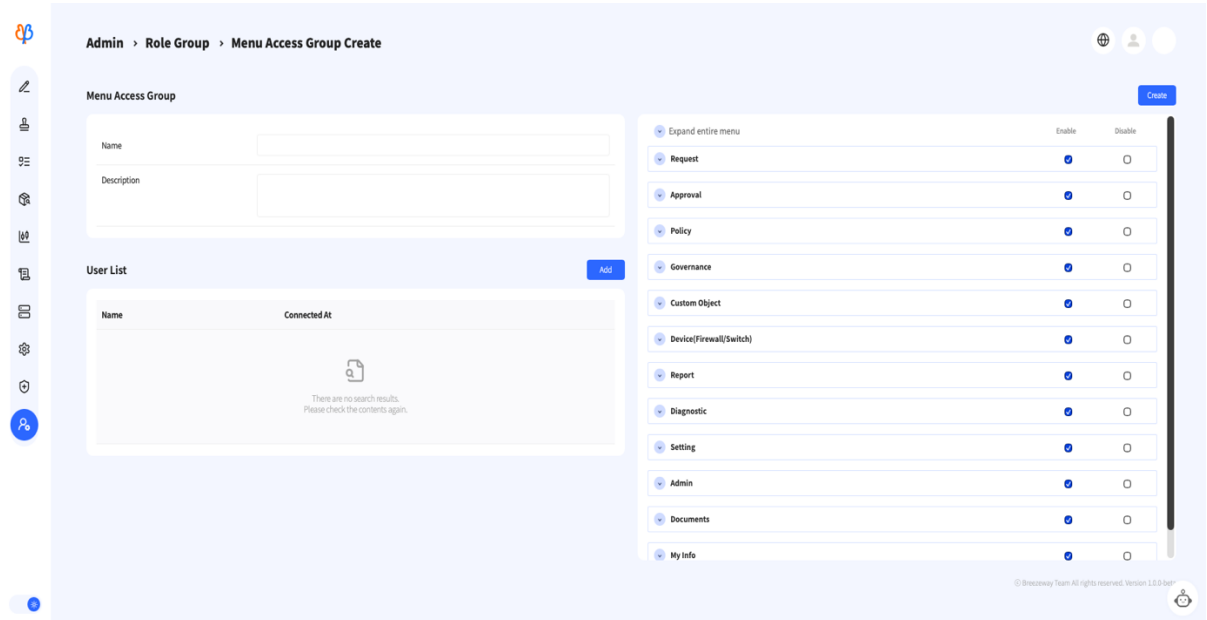

〈Menu Access Group Details Screen〉

Menu access groups restrict which menus users can access. If menu access is disabled, users belonging to that menu access group cannot access the disabled menu.

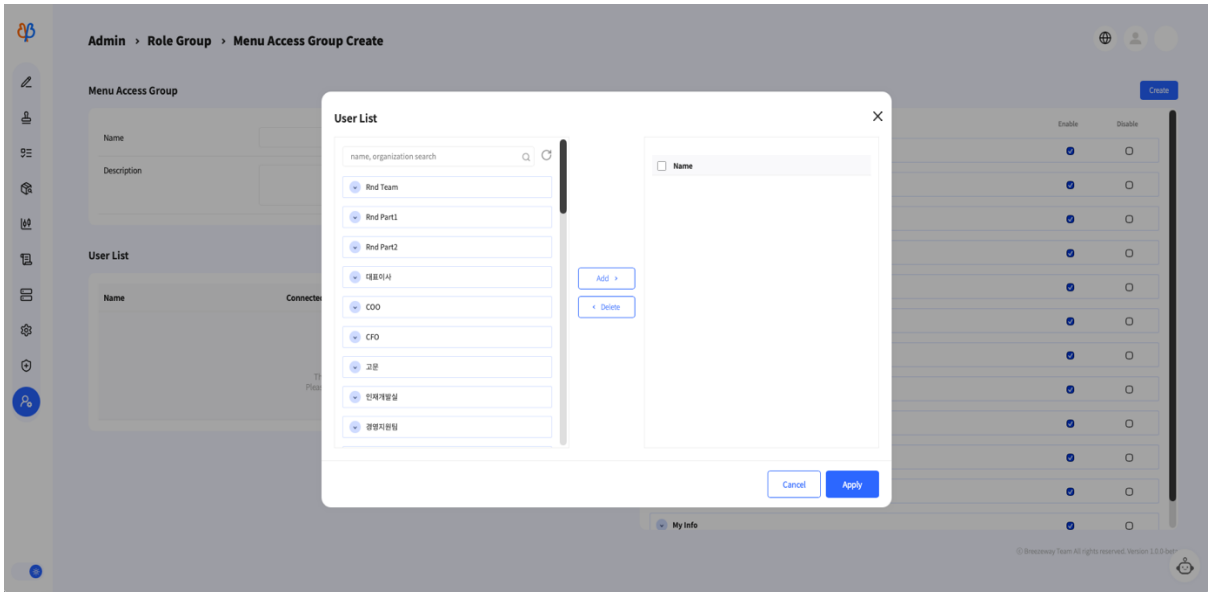
- Menu Access Group Inquiry

You can view the basic information of a Menu Access Group. Clicking the Menu Access Group name takes you to the Menu Access Group Details page. On the details page, you can view the Menu Access Group's basic information, assigned user information, and access information per menu.

- Create Menu Access Group



〈Menu Access Group Creation Screen〉




〈Menu Access Group User List Modal Screen〉

Clicking the Create button in the upper-right corner of the Menu Access Group list page takes you to the Menu Access Group creation page. You can create a menu access group by entering its basic information, adding a user list, specifying access permissions per menu, and saving.

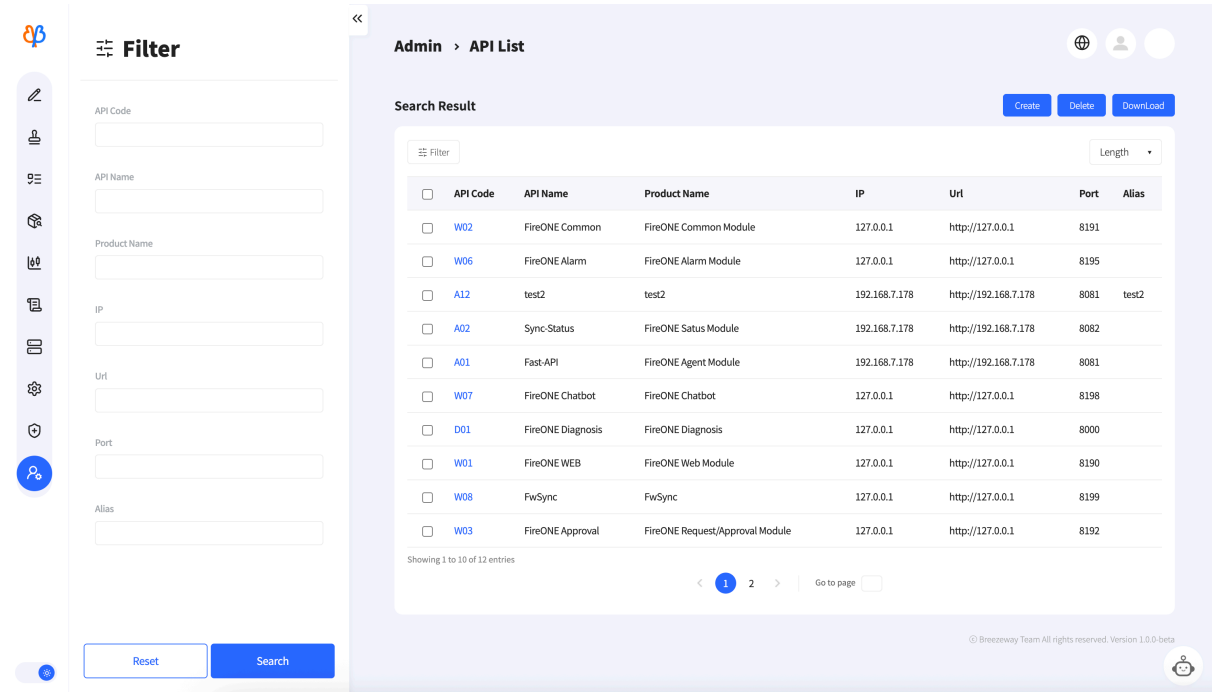
- Modifying a Menu Access Group

You can modify relevant information on the menu access group details page. Clicking the Edit button applies the changes.

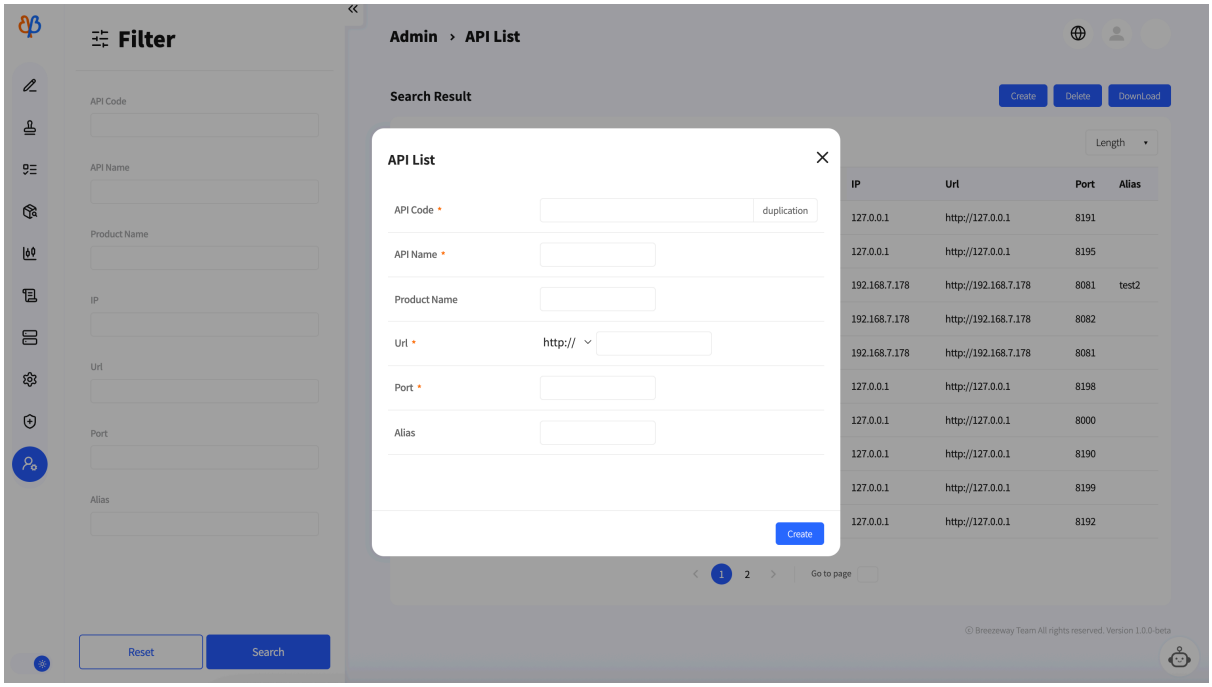
- Deleting a Menu Access Group

Clicking the Delete button on the Menu Access Group details page will delete that menu access group.

6) API List




〈API List Screen〉




〈API List Creation Modal Screen〉

Stores and manages API information used in the product. You can manage the IP, Address, and Port information of APIs currently in use within the product. The Fire.ONE product provides services with each function modularized, but it can be customized by integrating with the customer's application/approval module or alarm module, etc., as needed.

If the address where the product module is installed changes, the address can be updated in the database without redeploying the source code. This aims to reduce failures caused by module-to-module calls.

- Key API module information currently used in the product

| Product Name | Module Description | Address | port |
|---|---|---|---|
| **Fire.ONE Alarm** | Fire.ONE Alarm Module | http://127.0.0.1 | 8195 |
| **Fire.ONE Approval** | Fire.ONE Request/Approval Module | http://127.0.0.1 | 8192 |
| **Fire.ONE Push** | Fire.ONE Push Module | http://127.0.0.1 | 8193 |
| **Fire.ONE Policy** | Fire.ONE Policy Module | http://127.0.0.1 | 8194 |
| **Fire.ONE Common** | Fire.ONE Common Module | http://127.0.0.1 | 8191 |
| **Fire.ONE WEB** | Fire.ONE Web Module | http://127.0.0.1 | 8190 |
| **Fire.ONE FwSync** | Fire.ONE Agent Module | http://127.0.0.1 | 8199 |
| **Fire.ONE Diagnosis** | Fire.ONE Diagnosis | http://127.0.0.1 | 8000 |

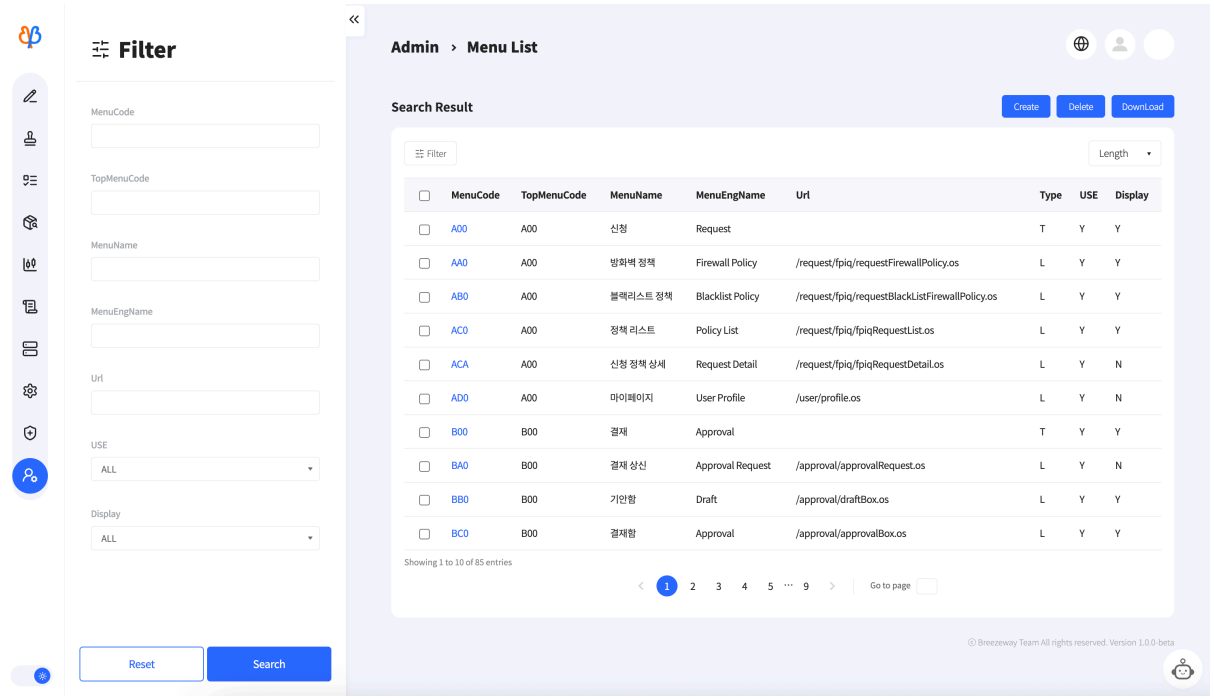
- Create API List

If additional APIs are used, you can add API information by clicking the Create button in the upper right corner of the API List page.

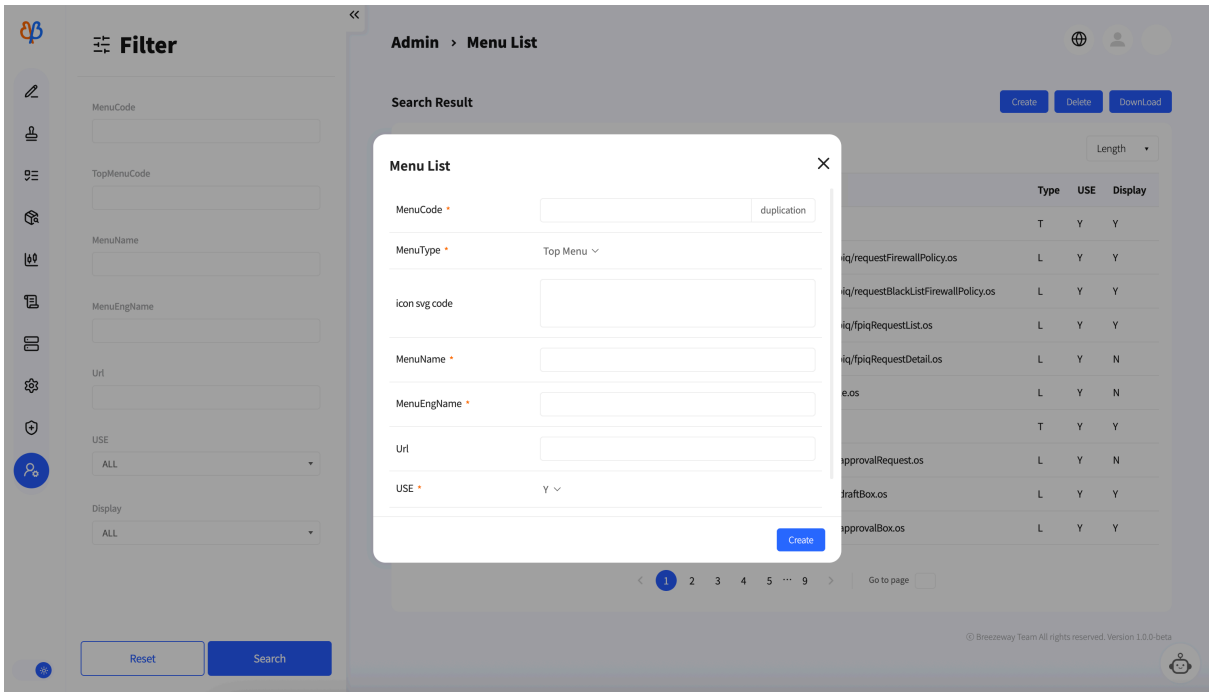
- Download

You can download the list of currently used APIs in Excel format.

7) Menu List




〈Menu List Screen〉




〈Menu List Creation Modal Screen〉

You can view, create, edit, and delete menus used on the webpage.

- Creating a Menu List

You can add a new menu to the menu list by clicking the Create button in the upper-right corner of the menu list page.

- Edit Menu List

Click a menu code in the menu list to edit its detailed information. Click the Edit button in the bottom-right corner of the modal to apply the changes.

- Deleting Menu List

Select the checkbox for the menu you wish to delete from the menu list and click the Delete button to remove that menu.

- Download

You can download the menu list for the current product in Excel file format.

❖ Menu Code Generation Rules

- A 3-digit code composed of a combination of uppercase letters A-Z and 2 digits
- The parent code consists of A-Z + 00, and the menu structure has two levels.
- The top-level code A00 does not require a menu URL, but its submenus do have URLs.


〈System Status Screen〉

Real-time monitoring of system memory, disk, CPU usage, and API connection status is available.

- WAS Memory Usage Status
  Views used memory and available memory.

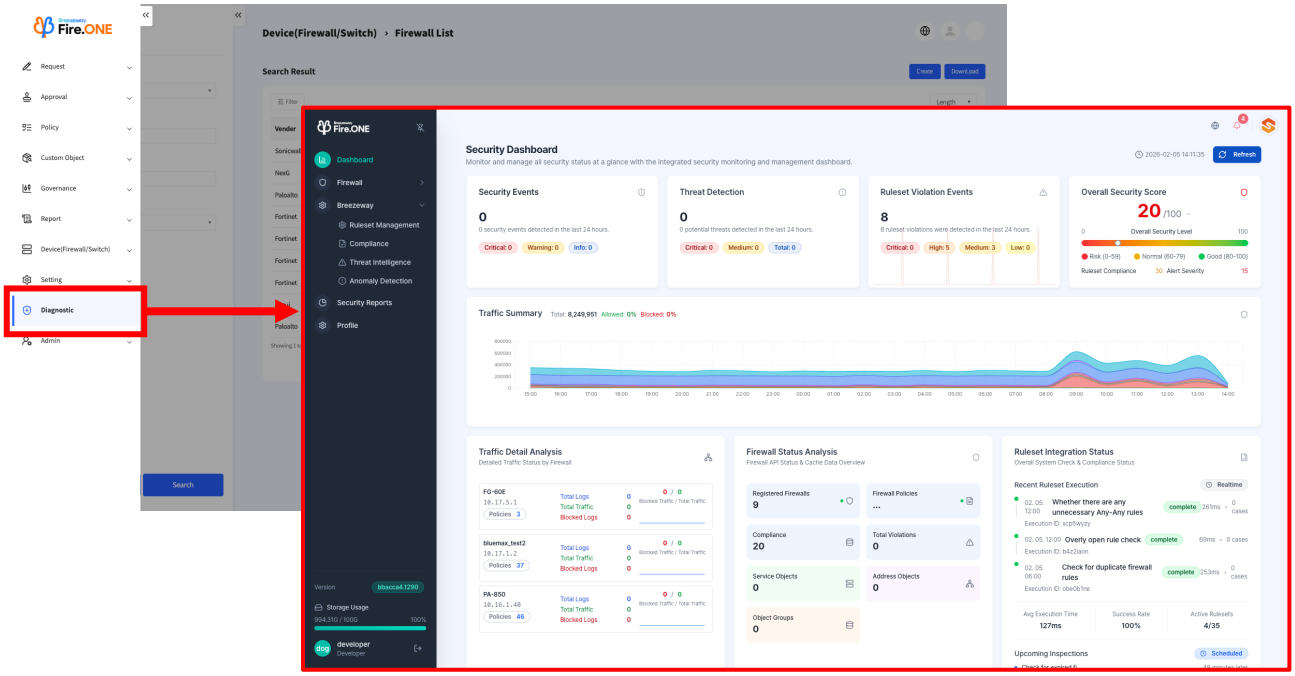
- Disk Usage
  Check the used disk space and available disk space.

- CPU check
  Check the hardware CPU usage and Java Virtual Machine CPU usage.

- API
  Verify the execution status of each module (COMMON, WEB, APPROVAL, PUSH, POLICY, FWSYNC, ALARM).

## 2.2 Diagnostics Function

Fire.ONE's diagnostics function comprehensively utilizes firewall logs, rule-based traffic analysis, policy checks, anomaly detection, and threat intelligence to diagnose the overall security status.

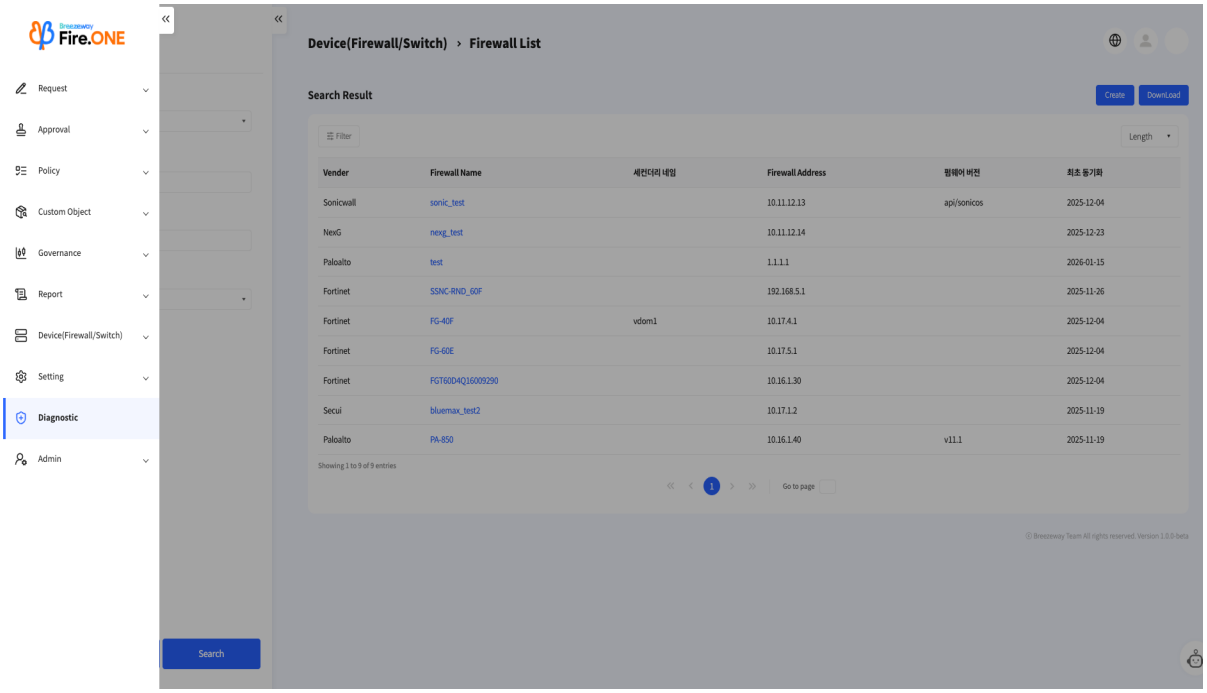



〈Fire.ONE → Diagnostics Access〉

Clicking the Diagnostics menu in Fire.ONE opens the diagnostics screen in a separate window.

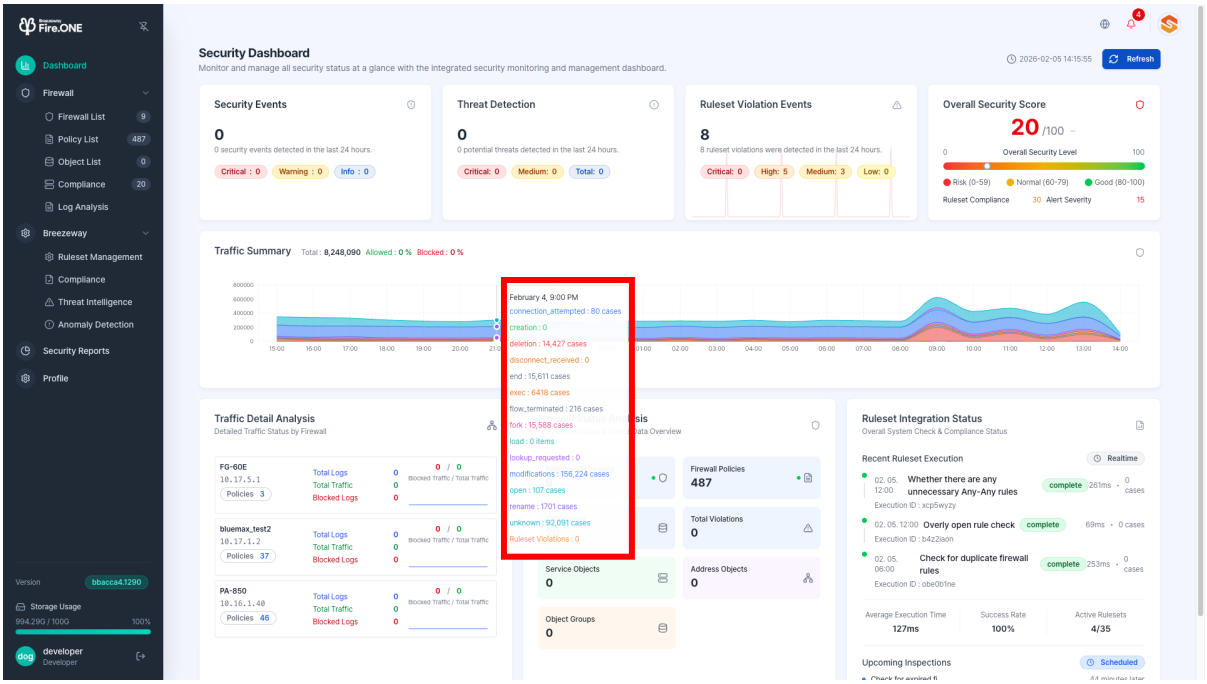
### 2.2.1 Security Dashboard

The dashboard provides an at-a-glance view of the overall security status.



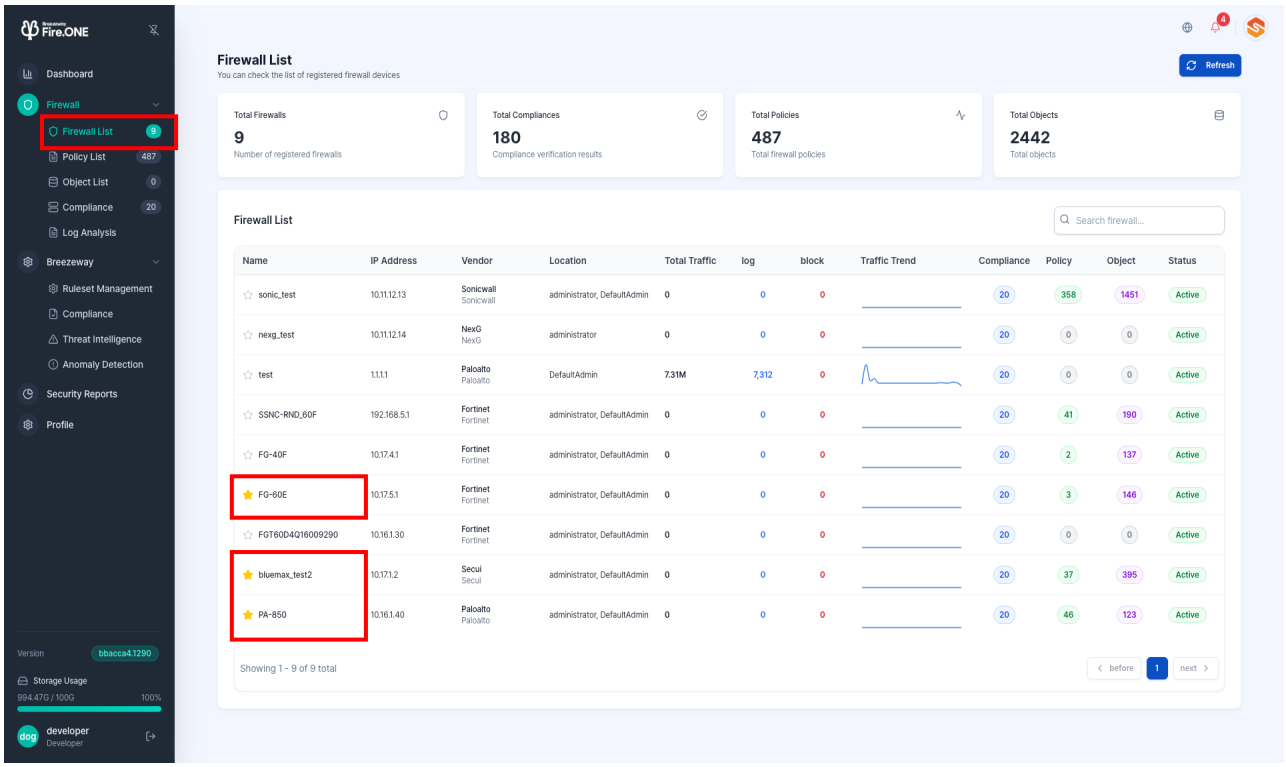

〈Diagnostic Dashboard Screen〉

1) Security Events: Displays the total number of security events collected over the past 24 hours. Events occurring during this period are categorized into info, warning, error, notice, and warn, with corresponding graphs shown.
2) Threat Detection: Displays the number of potential threats detected over the past 24 hours. It summarizes threats by severity level (Critical, Medium, Total), enabling assessment of the current attack landscape.
3) Rule-Based Events: Shows the status of rule violation events over the past 24 hours. Displays the number of events by risk level: Critical, High, Medium, Low.
4) Overall Security Score: A metric converting the current infrastructure's overall security status into a score (0-100). It indicates Risky (0-59), Moderate (60-79), or Good (80-100) status. It also displays the rule set compliance score and alert severity score.
5) Traffic Summary: Displays the overall traffic flow, types, and distribution over the past 24 hours in a time-based graph. Hovering the mouse over a specific time allows you to view detailed information.

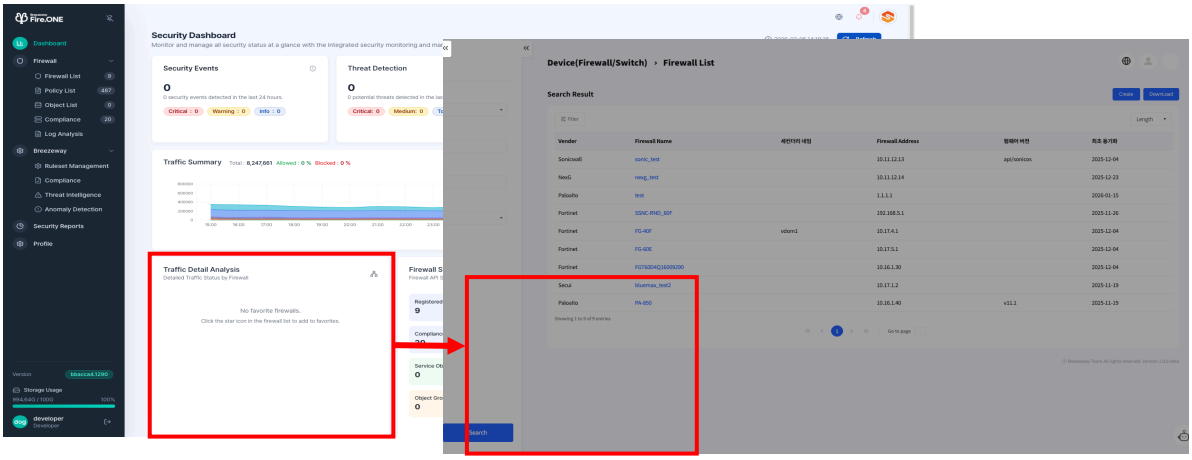



〈Traffic Summary - Detailed View〉

6) Traffic Detailed Analysis: This section displays detailed information about firewalls marked as favorites in the firewall list. It shows detailed logs, traffic, and blocking status for each firewall.




〈Favorite Settings Screen for Firewalls in the Firewall List〉

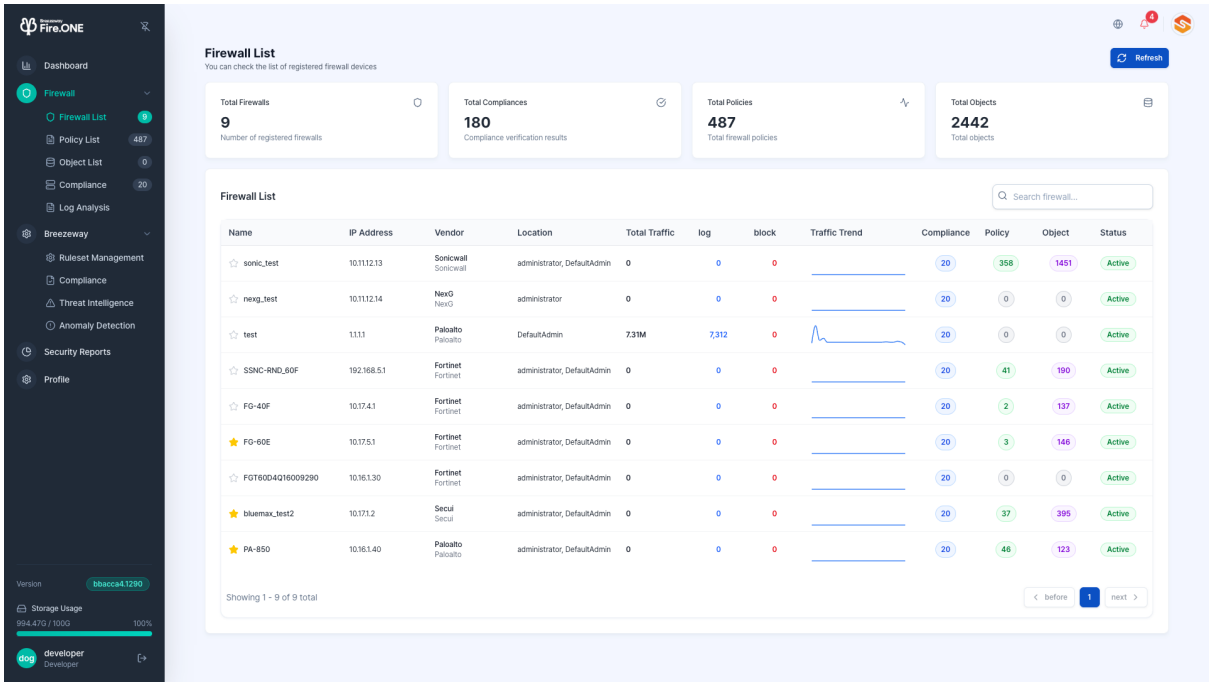



〈Applied Firewall Detailed Traffic Status Screen〉

7) Firewall Status Analysis: Displays the firewall API status and cache data status. Specifically, it shows the status of registered firewalls, firewall policies, compliance, total violations, service objects, address objects, and object groups.
8) Rule Set Trend Status: Displays the overall system inspection and compliance status. Shows recent rule set execution history, allowing you to check the average execution time, success rate, active rule sets, and the next inspection.

### 2.2.2 Fire.ONE - Firewall List

View the list of registered firewall devices, traffic, and associated compliance, policies, and objects.




〈Firewall Status Screen〉

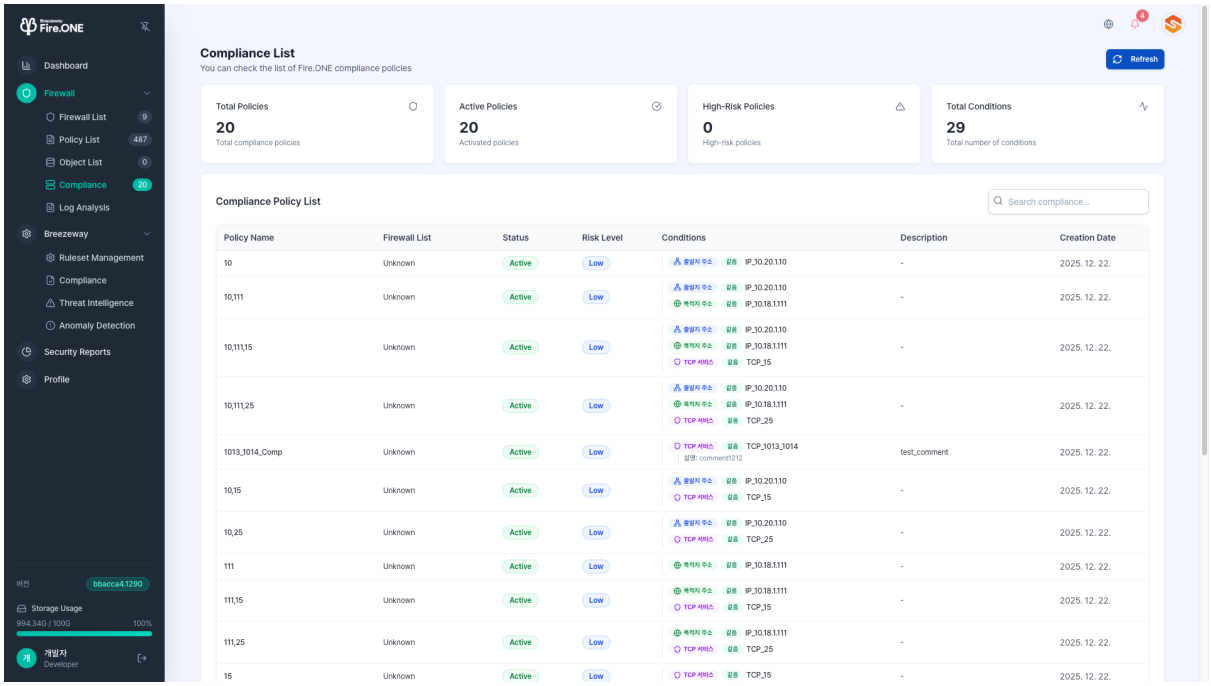
1) All Firewalls
   - Displays the number of firewall devices registered in the system.
   - Provides an at-a-glance view of the number of firewalls currently under management.
2) Total Compliance
   - Displays the aggregate results of compliance checks (policy adherence) performed on all firewalls.
   - This metric provides an overall level check to confirm whether settings comply with regulations or security guidelines.
3) Total Policies
   - Shows the total number of policies applied to currently registered firewalls.
   - It allows you to understand how many rules/policies are in operation on each firewall and the overall policy scale.
4) Total Objects
   - This shows the total number of objects (such as address objects and service objects) used in firewall policies.
   - This metric indicates the complexity of resources used in policy configuration and helps gauge the management scale.
5) Firewall List

| Column Name | Description |
|---|---|

| | |
|---|---|
| **Name** | The logical name of the firewall device. This is an identifier used by administrators to distinguish between devices. |
| **IP Address** | Displays the management IP or primary IP address of the firewall device. |
| **Manufacturer** | Indicates the vendor information of the firewall device (e.g., AhnLab, Bluemax, Fortinet, Palo Alto, etc.). |
| **Location** | Shows the physical/logical location where the firewall is installed. |
| **Total Traffic** | Displays the amount of traffic passing through the firewall. |
| **Traffic Trend** | This area displays traffic changes over time as a mini-graph. It allows you to intuitively identify points of sudden traffic spikes or drops. |
| **Compliance** | The number of compliance checks performed on the device. |
| **Policy** | The number of policies applied to this firewall. |
| **Object** | The number of objects in use on this firewall. |
| **Status** | Displays the active or inactive status of the firewall device. |

### 2.2.3 Fire.ONE - Compliance List

This feature allows you to check the Fire.ONE compliance status. It displays the total number of policies, active policies, high-risk policies, total conditions, and a list of compliance policies. This enables you to quickly grasp how many compliance policies are currently defined, how many policies are actually in operation, and how many policies carry a high risk level.




〈Compliance List Screen〉

1) Compliance Policy List

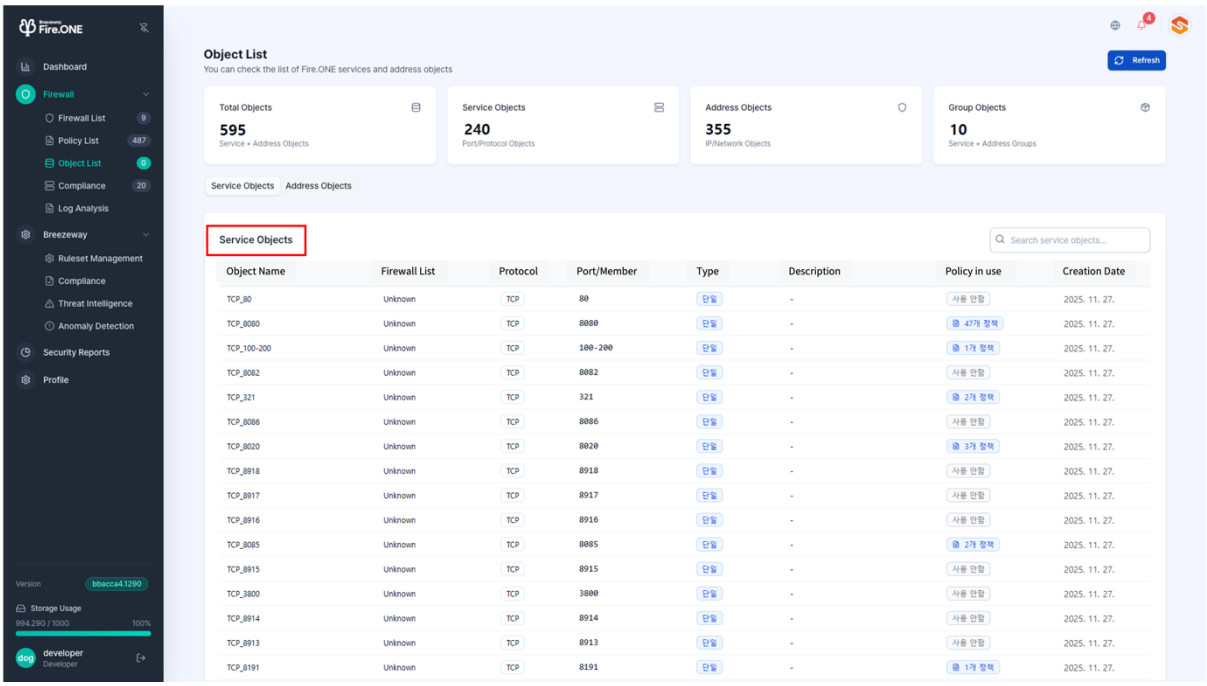
| Column Name | Description |
|---|---|
| **Policy Name** | The name of the compliance policy. It should be expressed in a way that allows administrators to intuitively distinguish what type of policy it is. |
| **Firewall List** | Indicates the target firewall to which this policy applies. |
| **Status** | Displays the operational status of the policy. (Active and Inactive) |
| **Risk Level** | Indicates the risk level of the violations addressed by the policy. For example: Low, Medium, High, etc., allowing prioritization. |
| **Conditions** | A list of detailed conditions the policy uses to determine violations. Specific filter conditions like expiration period, service/port, source/destination address, and protocol are displayed. |
| **Description** | An area for additional notes or comments about the policy. Useful for recording policy intent or operational guidelines. |

| | |
|---|---|
| **Creation Date** | Displays the date this compliance policy was first created. This can be referenced to manage the policy's implementation date and change history. |

### 2.2.4 Fire.ONE - Object List

The Object List provides an at-a-glance view of the total number of objects, service objects, address objects, and group objects (which bundle services and addresses). This allows you to quickly understand how many objects are currently defined for use in the policy configuration and the relative proportions by type.

1) Service Objects

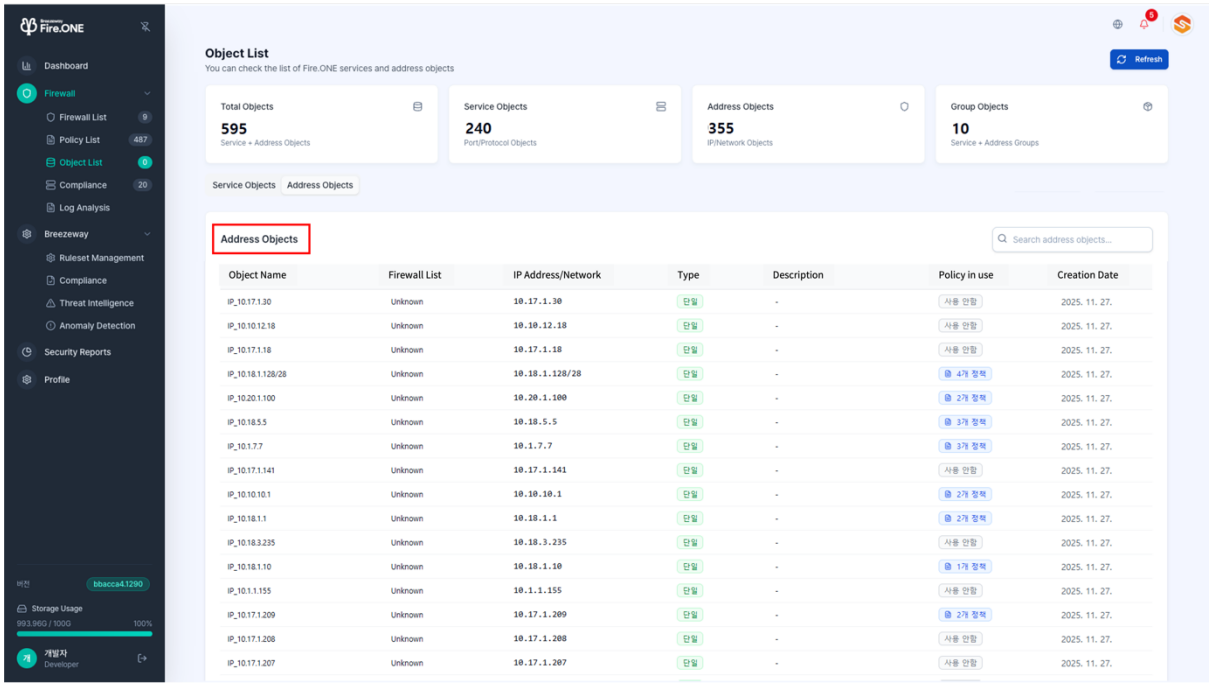



〈Object List - Service Objects Screen〉

| Column Name | Description |
|---|---|
| **Object Name** | The name of the service object. This is the identifier used when referencing it in policies. |
| **Firewall List** | Displays the firewall to which the object belongs. |
| **Protocol** | Displays the protocol information for the object. |
| **Port/Member** | Displays the port and member information for the object. |

| | |
|---|---|
| **Type** | The type of the object. Distinguishes whether it is a single object or a group, etc. |
| **Description** | This area records additional descriptions/notes about the object. You can leave details about its purpose or precautions. |
| **Policies in Use** | Shows whether policies actually reference this object and how many exist. Can be used to identify candidates for cleaning up unused objects. |
| **Creation Date** | This is the date the object was first registered in the system. It can be used as a reference for determining the object's introduction date and when maintenance may be required. |

1) Address Object



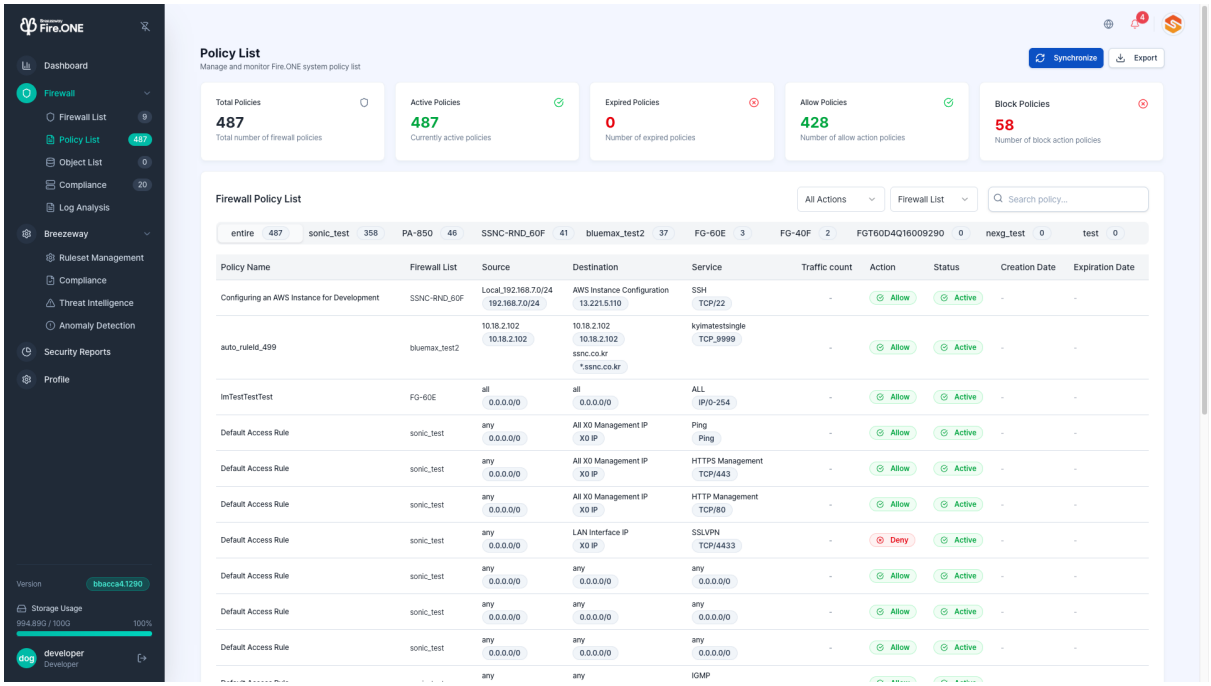

〈Object List - Address Object Screen〉

| Column Name | Description |
|---|---|
| **Object Name** | The name of the address object. This serves as an identifier when referenced in policies, clearly indicating the IP range or purpose. |

| | |
|---|---|
| **Firewall List** | Displays the firewall device to which the address object belongs. |
| **IP Address/Network** | IP information mapped to the object. Displays the IP address and network status. |
| **Type** | The type of the address object. Distinguishes whether it is a single address or a group of multiple addresses. |
| **Description** | This area records additional descriptions/notes for the object. Example: "External DNS server," "Headquarters internal network range," etc. |
| **Active Policies** | Indicates whether policies currently reference this address object and the number of such policies. If not in use, it may be subject to cleanup as an unused object. |
| **Creation Date** | The date this address object was first registered in the system. Useful for determining the creation time and management history. |

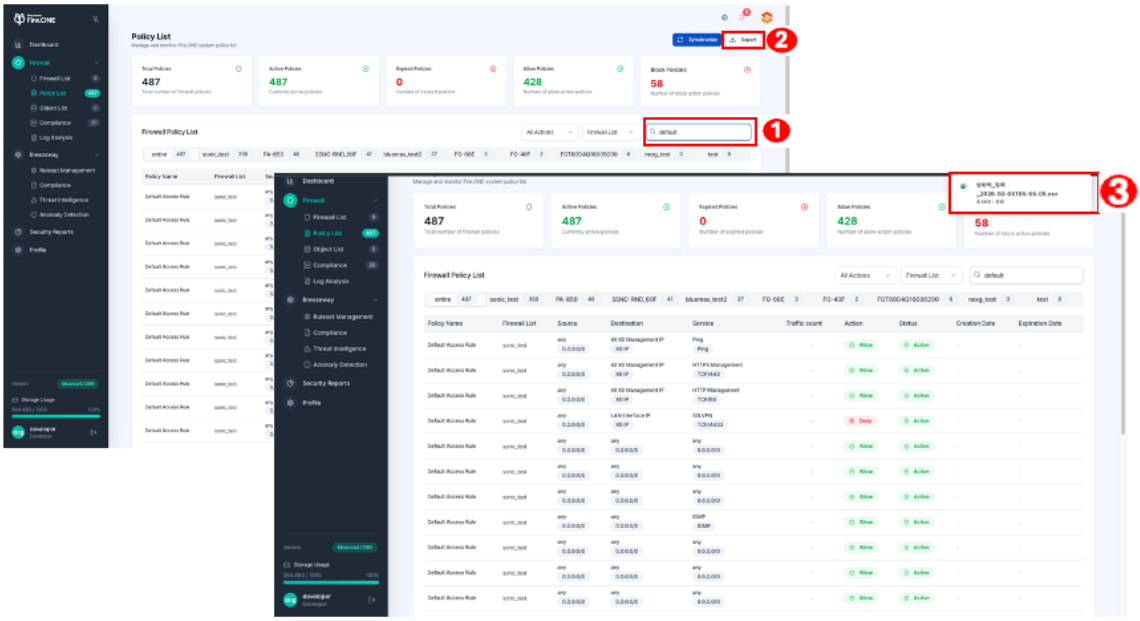
### 2.2.5 Fire.ONE - Policy List

This feature manages and monitors the policy list within the Fire.ONE system, providing an at-a-glance view of the total policies, currently active policies, expired policies, allowed policies, blocked policies, and the firewall policy list. This allows for quick verification of the scale of currently operating policies, the ratio of allowed to blocked policies, and the presence of expired policies.




〈Policy Analysis Screen〉

Additionally, searched policies can be exported as CSV files for download.




〈Policy List Search and Download Process〉

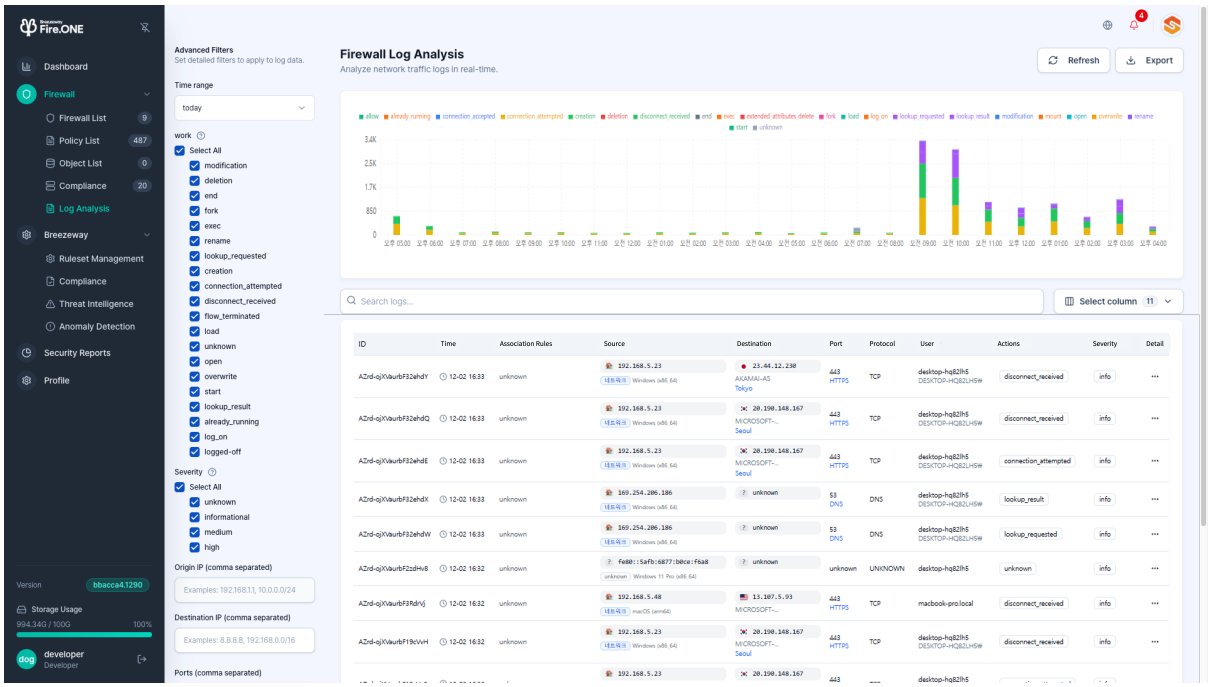
1) Firewall Policy List

| Column Name | Description |
|---|---|
| **Policy Name** | The identification number or name of the firewall policy. It serves as the primary key to distinguish each policy. |

| | |
|---|---|
| **Firewall** | The name of the firewall device to which this policy applies. This allows you to determine which device a policy is applied to. |
| **Source** | The source address/network of the traffic. Expressed as IP, range, any, etc. |
| **Destination** | The destination address/network of the traffic. |
| **Service** | The service (port/protocol) information for the firewall policy. |
| **Action** | Indicates whether the policy will allow or block traffic. This represents the actual direction of the policy action. |
| **Status** | The current operational status of the policy. Example: Active (applied), Inactive (not applied) |
| **Creation Date** | The date this policy was first created. Used to track when the policy was introduced and manage change history. |
| **Expiration Date** | The effective end date of the policy. Used to manage policies that automatically expire after a specific date and is displayed alongside the D-Day. |

### 2.2.6 Log Analysis

This feature monitors network traffic patterns and security events by analyzing firewall logs using filters.




〈Log Analysis Screen〉

1) Advanced Filter Area (Left)

- Time Range: Select 'Today, Yesterday, Last Week, Last Month, Custom' to view logs only for that time period.
- Action: Automatically displayed based on logs. Checkboxes allow selection of various event types such as modification, exec, end, fork, deletion, creation, connection_attempted, disconnect_received, etc. Use [Select All] to select/deselect all events at once.
- Severity: Automatically populated based on the log. You can select the severity criteria for the log using checkboxes.
- Source IP (comma-separated): Filter traffic from specific source ranges by entering single IPs or subnets, e.g., (192.168.1.1, 10.0.0.0/24).
- Destination IP (comma-separated): Example: 8.8.8.8, 192.168.0.0/16. Specify destination IPs or ranges to view only logs destined for targets of interest.
- Port (comma-separated): Example: Enter one or more port numbers like 80, 443, 22 to view only traffic on those specific ports.
- User (comma-separated): Directly enter a username to view logs generated only by a specific user/device.
- Protocol: Automatically displayed based on the log. You can select supported protocols like TCP or UDP via checkboxes to analyze only the desired communication protocols.

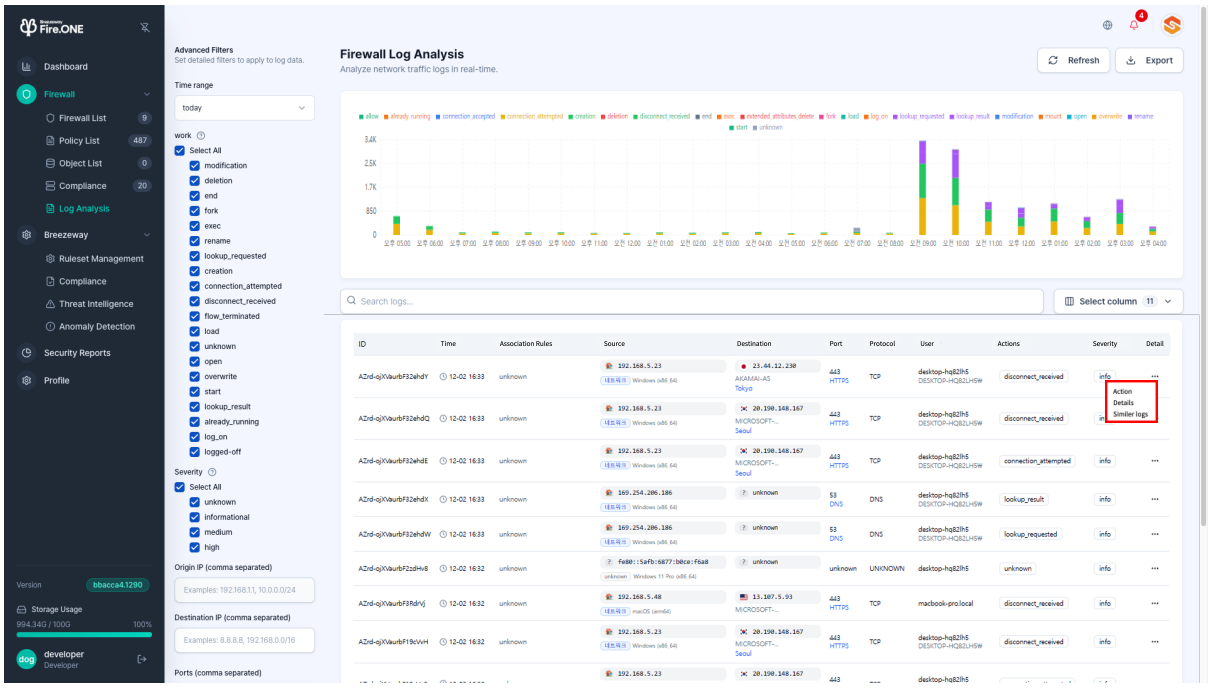
2) Log Analysis Chart (Top Center)

- Displays the number of events within the selected time range in the "Log Analysis" area as a bar graph by time period.
- Color legends for each operation type (e.g., already_running, connection_accepted, connection_attempted, creation, deletion, disconnect_received, modification, start, query, unknown) are displayed at the top, allowing you to quickly identify which events occurred most frequently.
- Changing the filter conditions on the left updates the chart content accordingly.
- Use the [Refresh] button in the upper right to retrieve the latest logs, and the [Export] button to download the current query results as a CSV file.

3) Log Search and Log List (Bottom)

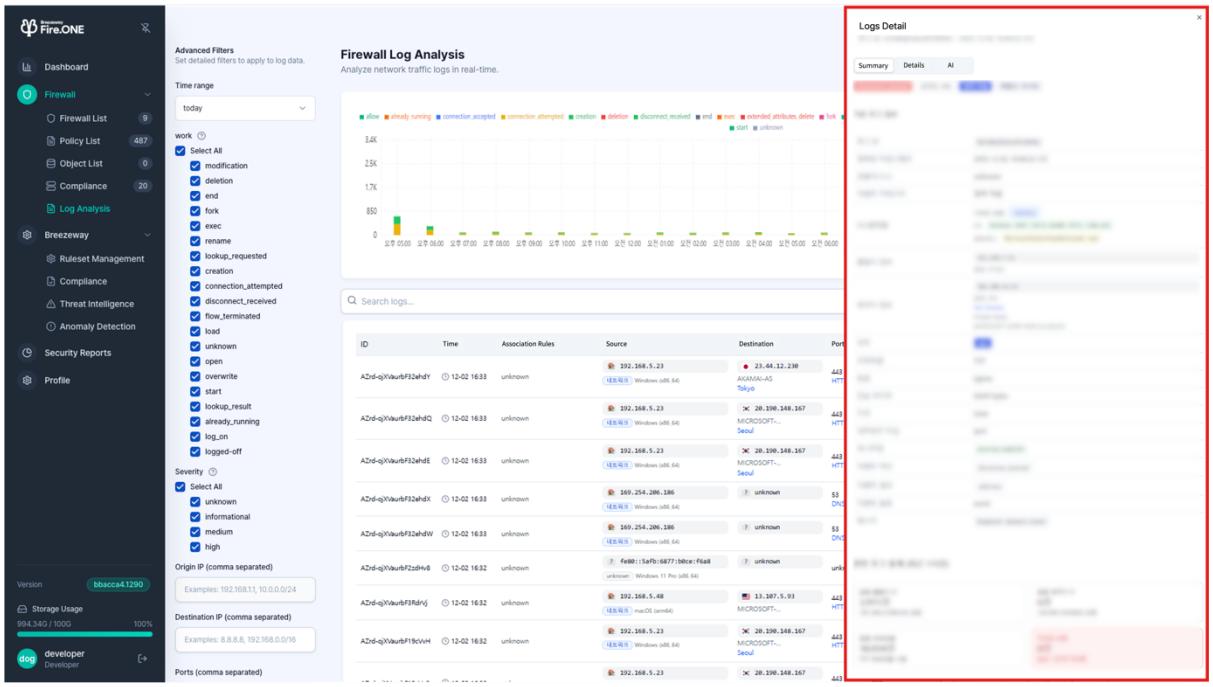
- Log Search: Enter keywords, IP addresses, domains, usernames, etc., in the top search bar to quickly find desired items within the entire log list.

- Log List:
  - ID: A unique identifier distinguishing each collected log event.
  - Time: Displays the time the log was recorded.
  - Associated Rule: Shows the name of the detection/policy rule that triggered the event.
  - Source: Displays the source IP address and OS/device information (e.g., network, Windows, macOS, etc.).
  - Destination: Provides the destination IP along with the provider/service name, region information, etc.
  - Port: Displays the port number used for communication (e.g., 80, 443, 995).
  - Protocol: Indicates the network protocol information, such as TCP.
  - User: Displays the user account or terminal hostname that generated the traffic.
  - Action: Shows the event handling status, such as disconnect_received or connection_attempted.
  - Severity: Displays the risk/importance level, such as info, in a badge format.
  - Details: Clicking the [...] button on the right allows you to view the action, detailed information, and search for similar logs for the selected log.



〈When clicking the log analysis detail screen〉

Selecting a specific log from the log list opens the log details panel on the right.




〈Log Details - Overview Screen〉

The Overview provides a detailed summary of the selected log and related statistics based on the last hour on a single screen.

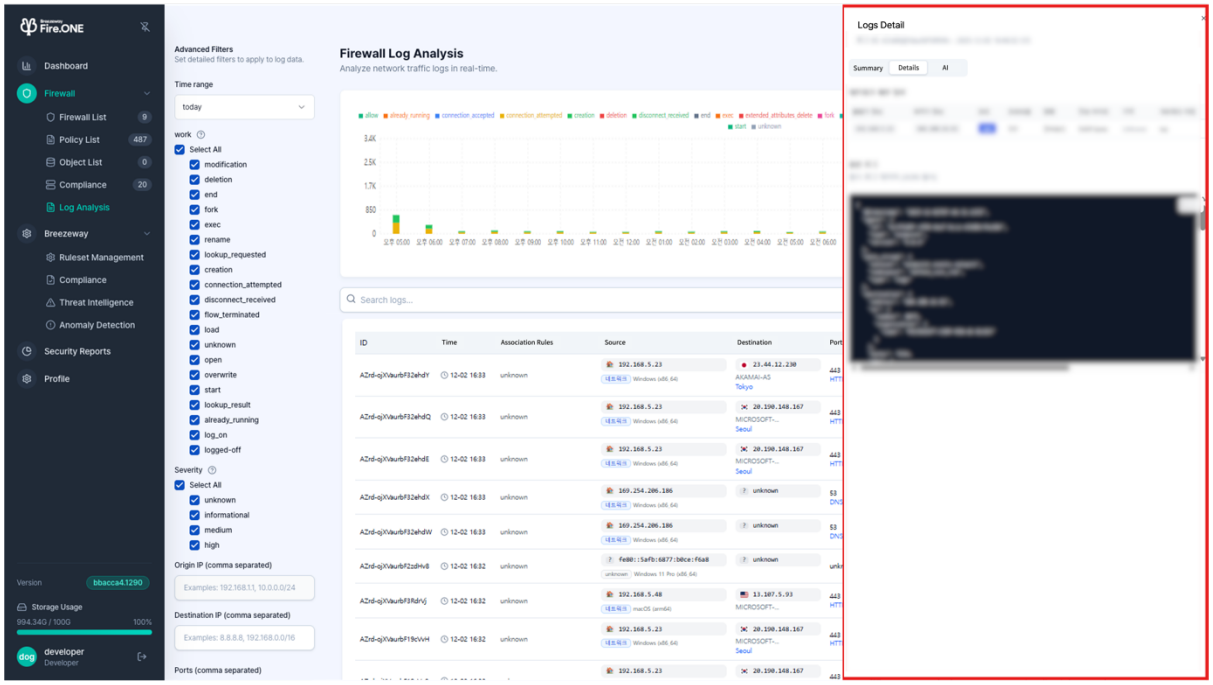
- Basic Log Information
  - Log ID: The unique identifier for the log currently being viewed in detail.
  - Exact Timestamp: Displays the precise time the event occurred and was collected, e.g., 2025-12-02 16:46:32.125.
  - Observer/Source and Event Category: Key metadata classifying the event, such as the observer source and event category, is displayed.
  - Event Type and Platform Information: Event type, OS/platform, and process name allow identification of the device and process generating the event.
  - Source/Destination Information: Source IP and port, destination IP and port, city/country, and carrier/ASN information are displayed together, enabling identification of both ends of the communication and path characteristics.
  - Communication Characteristics Information: Detailed session characteristics are visible at a glance through port (e.g., 443), protocol

(TCP), direction (egress/ingress), transmitted bytes, region, network type (IPv4/IPv6), and hostname.

- Event Result Information: Event action, event result, event type, and message indicate the processing status and meaning of the log.
- Additional Summary Badge: The badge at the top of the screen summarizes the event action, severity, policy application status, and threat score (e.g., 10/100).

- Related log statistics (last hour)
- Displays the total number of traffic events based on the same source IP address.
- Provides the number of connections based on the same destination IP.
- Displays the number of occurrences based on the same protocol (e.g., TCP 443).
- Displays the number of blocked logs (blocked requests) occurring during the same time period.

  → This can be used to determine at a glance whether a specific log is a one-off occurrence, if the same pattern is repeating, and whether it was blocked.




〈Log Details - Details Screen〉

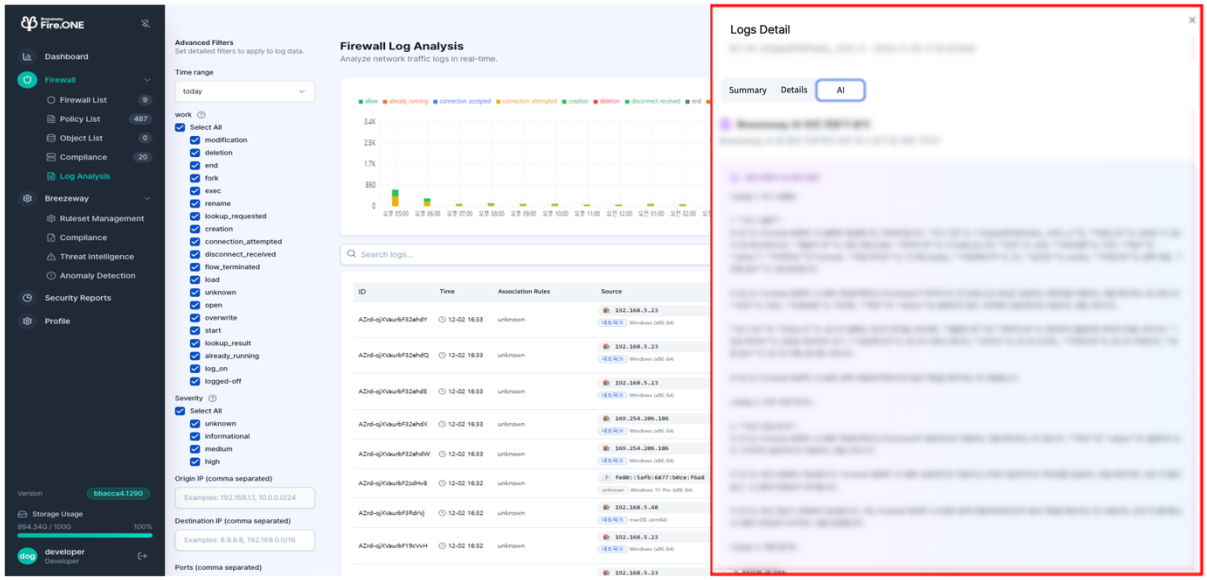
The Details tab provides more specific information broken down by network field.

1) Network Details

- Source and Destination Information: IP and domain information.
- Port and Protocol: The port number used by the session and the protocol type (e.g., TCP/UDP).
- Direction: Indicates the network direction, such as inbound.
- Transmitted Bytes: Allows you to check the traffic volume based on the amount of data transmitted.
- Region: Indicates the geographic location where the network activity originated.
- Network Type: TCP/UDP, etc. This section allows detailed identification of what type of communication a log corresponds to on the actual network.

2) Raw Log (JSON Format)

- The original data (JSON) of the collected log is displayed as-is at the bottom.
- Beyond the summary information at the top, you can directly view all fields necessary for analysis and integration.
- If needed, you can copy the JSON using the Copy button and paste it into external analysis tools or ticket systems.

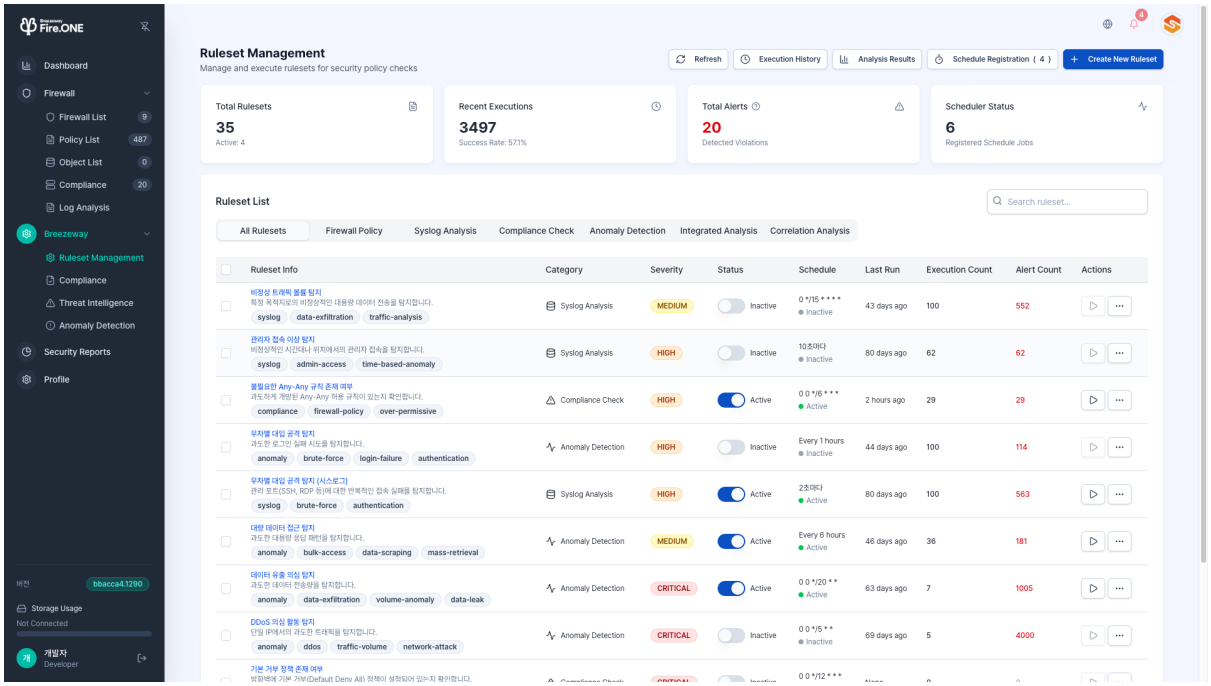



〈Log Details - AI Analysis Screen〉

AI Analysis provides professional security log analysis and response guidance through Breezeway AI.

## 2.2.7 Breezeway Diagnostics - Ruleset Management

This feature manages and executes rulesets for security policy checks.




〈Rule Set Management Screen〉

1) Top Screen

- Total Rulesets: Displays the number of rulesets registered in the system and the number of active rulesets among them.
- Recent Executions: Displays the number of times the ruleset was executed and its success rate during the selected period.
- Total Notifications: Total number of all notifications generated in the last 7 days.
- Scheduler Status: Shows how many rulesets have schedules set by displaying the number of currently registered scheduled execution tasks.

The following function buttons are located in the upper right corner:

- Create New Ruleset: Registers a new ruleset.
- Refresh: Updates the current status to the latest information.
- Execution History: View the execution records and results of the ruleset.
- Analysis Results: View detected violations and security issues from rule set execution.
- Schedule Registration: Register a new schedule.

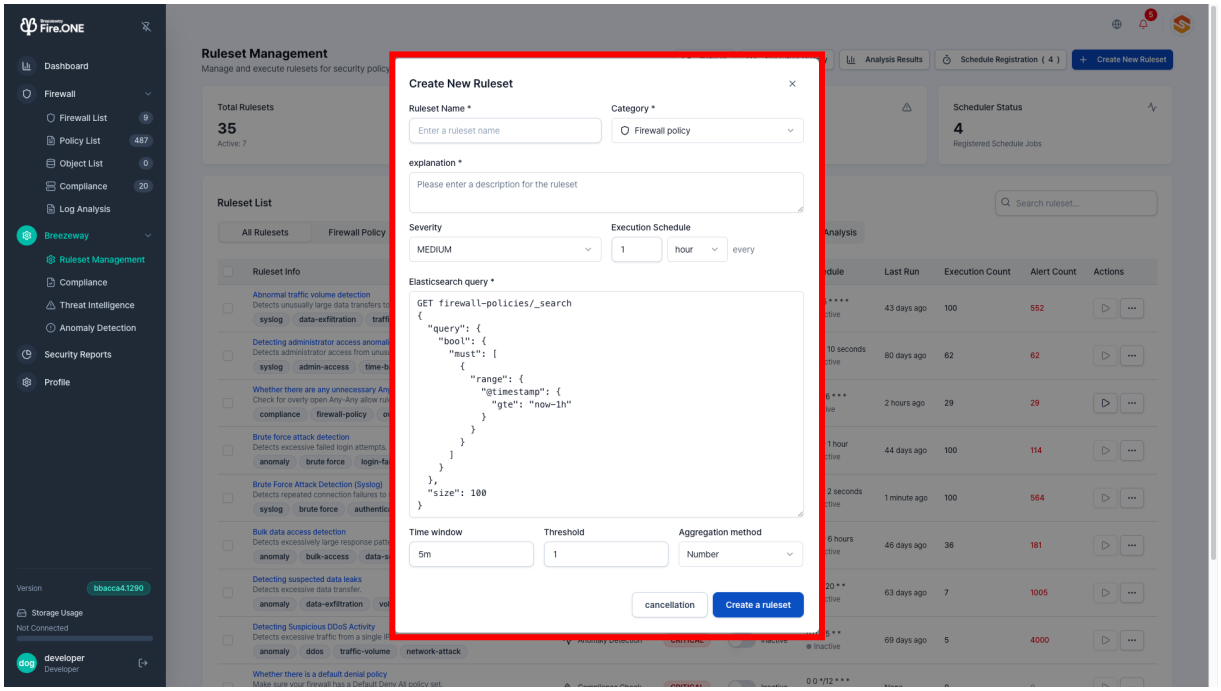
2) Rule Set List

The rule set list is displayed in the center of the screen. You can view not only all rule sets but also those related to firewall policies, syslog analysis, compliance checks, anomaly detection, integrated analysis, and correlation analysis. Details are as follows.

| Column Name | Description |
|---|---|
| **Rule Set Information** | The rule set name, brief description, and tags (e.g., syslog, data-exfiltration) are displayed together. This allows you to quickly understand the purpose of each rule. |
| **Category** | Indicates the analysis category to which the ruleset belongs. Examples: syslog analysis, compliance checks, anomaly detection, etc. |
| **Severity** | The risk level assigned when an event detected by the ruleset occurs. Examples: MEDIUM, HIGH, CRITICAL, etc. |
| **Status** | Indicates and allows modification of the rule set's active/inactive status. Scheduled execution and notifications do not occur when inactive. |
| **Schedule** | Indicates the frequency at which the rule set runs. Examples: Every hour, Inactive, etc. |
| **Last Run, Run Count, Notification Count** | Shows the time of the most recent execution, the cumulative number of executions, and the number of notifications generated by that ruleset. |
| **Actions** | You can execute, modify, duplicate, or delete a ruleset. You can also view its execution history. |

3) Create New Rule Set

To register a new rule set, click the [Create New Rule Set] button to open the pop-up, then enter the following items in order.



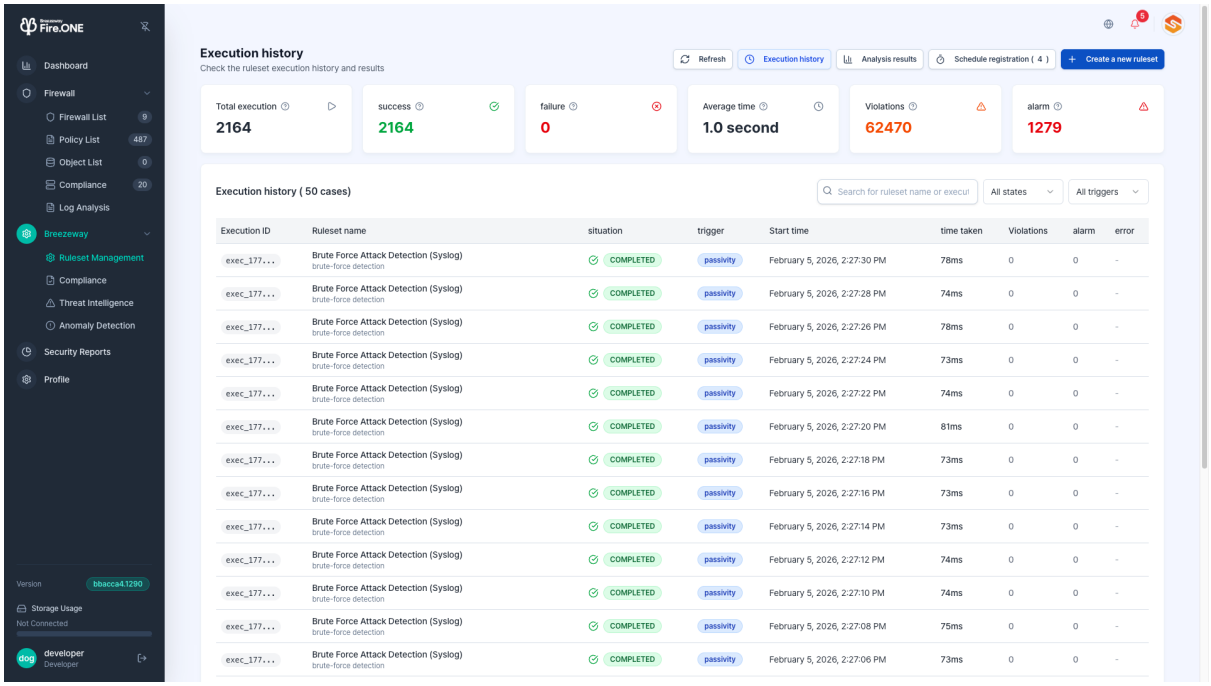

〈New Ruleset Creation Screen〉

- Rule Set Name: Enter the name for the new rule set.
- Category: Select the policy type to which the rule set belongs.
- Description: Briefly enter the purpose, detection conditions, and usage methods for this rule set. Write it so operators can easily understand the intent when viewing the rule set in the list.
- Severity: Select the risk level to assign upon detection.
- Execution Schedule: Set the frequency at which the rule set will run.
- Elasticsearch Query: Enter the Elasticsearch DSL query defining the detection criteria. In this section, define all fields and conditions that determine what is considered a detection target.
- Time Window: Set the time range used as the basis for detection.
- Threshold: Set the minimum number of occurrences required to determine detection.
- Aggregation Method: Select the method for aggregating logs.

Then click the [Create Rule Set] button to save the new rule set with the entered content. The saved rule set will automatically run according to the configured execution schedule and will be reflected in notifications and diagnostic results when conditions are met. Clicking the [Cancel] button closes the window without saving the current input.

4) Execution History

The Execution History screen displays the execution records for each diagnostic rule set in chronological order. You can quickly see which rules were executed at specific points in time, whether they completed successfully, and how many risks were detected. The top area provides a summary of the total number of executions, successful/failed counts, average execution time, and the number of violations and notifications.




〈Execution History Screen〉

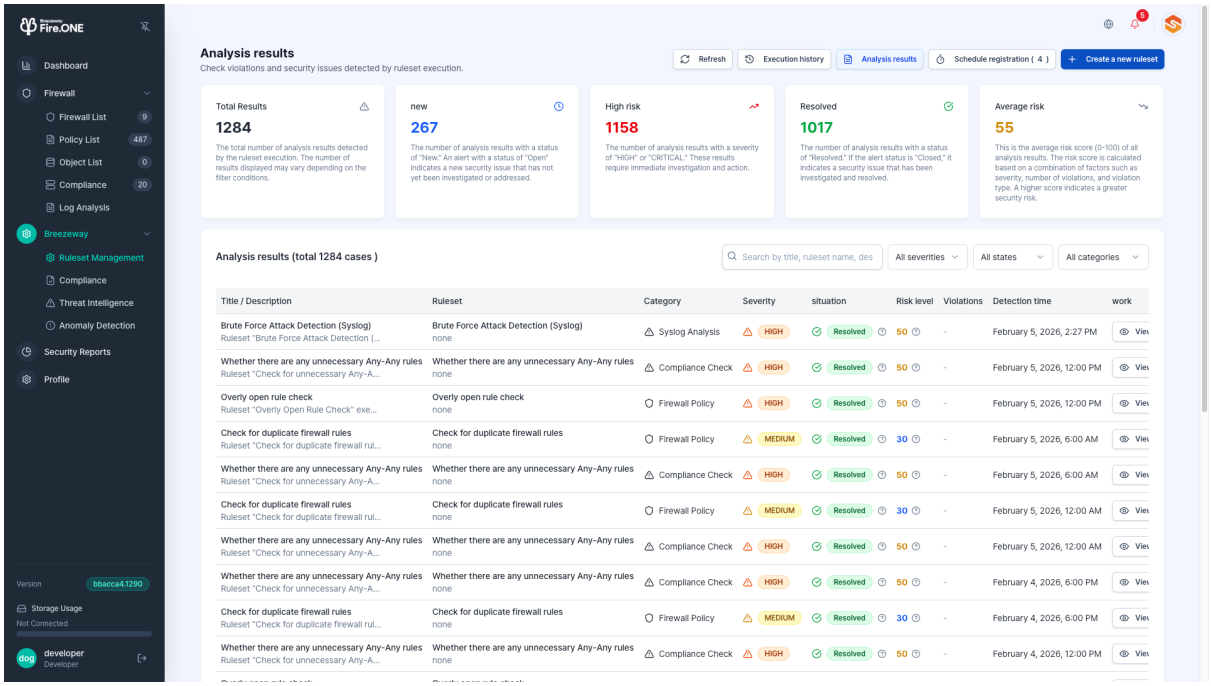
- Execution History (50 entries)

| Column Name | Description |
|---|---|
| **Execution ID** | An identifier distinguishing individual executions. |
| **Rule Set Name** | The name of the executed diagnostic rule. Example: Brute-Force Attack Detection, Advanced Port Scanning Detection, etc. |
| **Status** | Indicates the execution result. COMPLETED means normal completion, FAILED means failure due to an error. |
| **Trigger** | Indicates how execution was initiated. Shows whether it was manually executed by the user or automatically executed by a schedule. |
| **Start Time** | The exact time the diagnostic actually started execution. |
| **Duration** | The time taken for the diagnostic to complete. This allows you to check performance and whether there was any delay. |

| | |
|---|---|
| **Violations** | The number of violations detected during this run. |
| **Notifications** | The number of notifications sent because risk thresholds were met. |
| **Error** | If the execution failed, a summary of the error cause is displayed. If completed successfully, it is marked as '-'. |

5) Analysis Results

The analysis results section provides an overview of security issues and risks detected through rule set execution. It summarizes the number of issues by risk level, new occurrences, and resolved issues. The list below displays detailed information for each detected event.




〈Analysis Results Screen〉

- Analysis Results (Total Count)

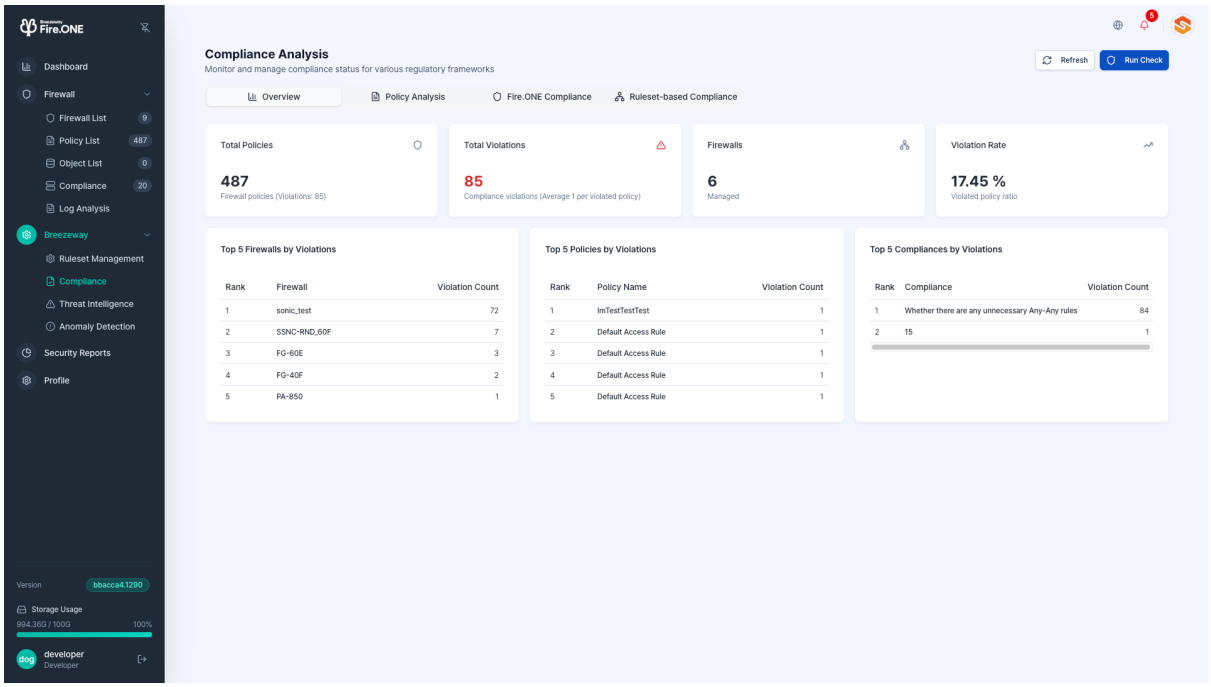
| Column Name | Description |
|---|---|
| **Title / Description** | The title and brief description of the detected event. This allows you to quickly understand what type of abnormal behavior occurred. |
| **Rule Set** | The name of the ruleset that detected this event. |
| **Category** | The category to which the rule set belongs. Types are distinguished as anomaly_detection, policy_violation, etc. |
| **Severity** | The risk level of the event. Displayed as LOW / MEDIUM / HIGH / CRITICAL. |

| | |
|---|---|
| **Status** | The current processing status of this issue. Examples: Resolved, New, etc. |
| **Risk Level** | The risk score assigned to the detected event. A higher score indicates greater security impact. |
| **Violations** | The actual number of detected events or related sessions/log entries. |
| **Detection Time** | The actual time when the security event was detected. |
| **Action** | This button allows you to view the details of the detected event. Clicking it takes you to the detailed analysis screen. |

### 2.2.8 Breezeway Diagnostics - Compliance Analysis

The compliance analysis screen monitors how well firewall policies adhere to internal regulations and security guidelines via a dashboard and table format.

1) Overview: Provides summary metrics such as total policy count, violation count, firewall count, and violation rate.




〈Compliance Analysis - Overview Screen〉

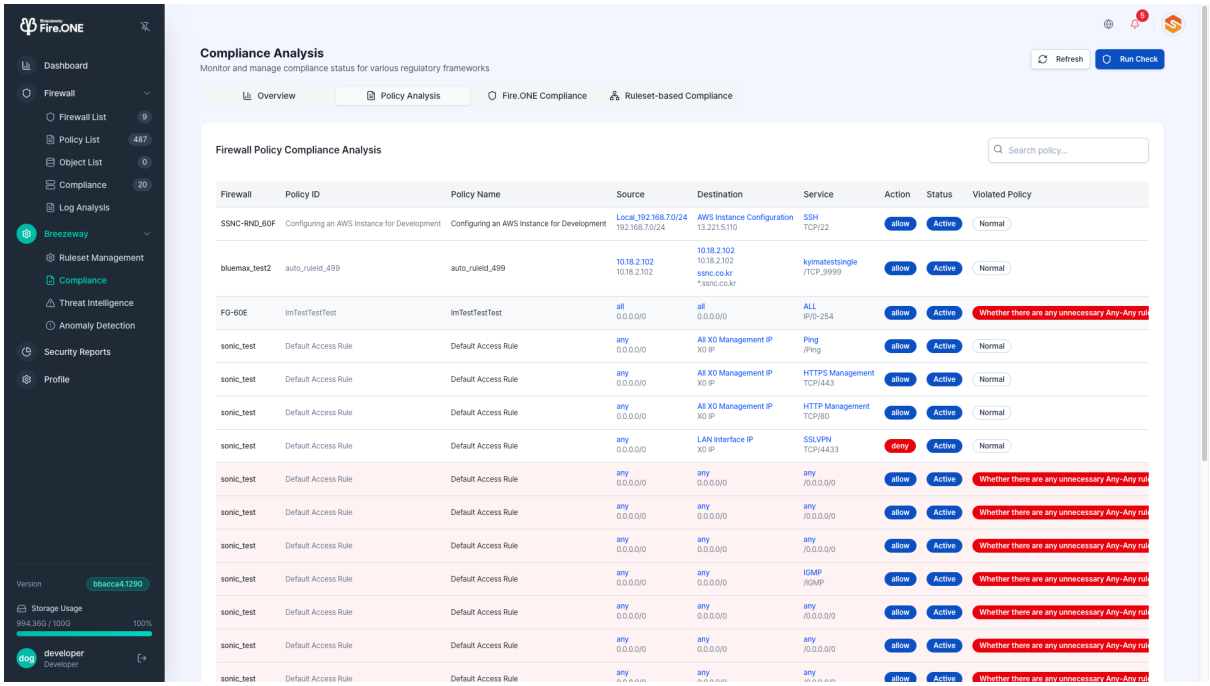
| Item | Description |
|---|---|
| **Total Policies** | The number of firewall policies currently subject to compliance inspection. (Includes violations and normal policies) |

| | |
|---|---|
| **Total Violations** | The number of policies found to be non-compliant during the inspection. (Displays both the number of non-compliant policies and the average number of violations per policy) |
| **Number of Firewalls** | The number of firewall devices included in the compliance inspection. |
| **Violation rate** | The percentage of policies determined to be in violation out of all policies. This intuitively shows the compliance level of the current environment. |

Additionally, a Top 5 panel is provided to identify items with concentrated violations.

- Top 5 Violations by Firewall: Displays firewall devices in order of highest violation counts.
- Top 5 Violations by Policy: Displays policies that are frequently violated at the top.
- Top 5 Violations by Compliance: Allows you to see which compliance regulations (items) are frequently violated.

2) Policy Analysis: The Policy Analysis tab allows you to review compliance results for each individual policy actually applied to the firewall.

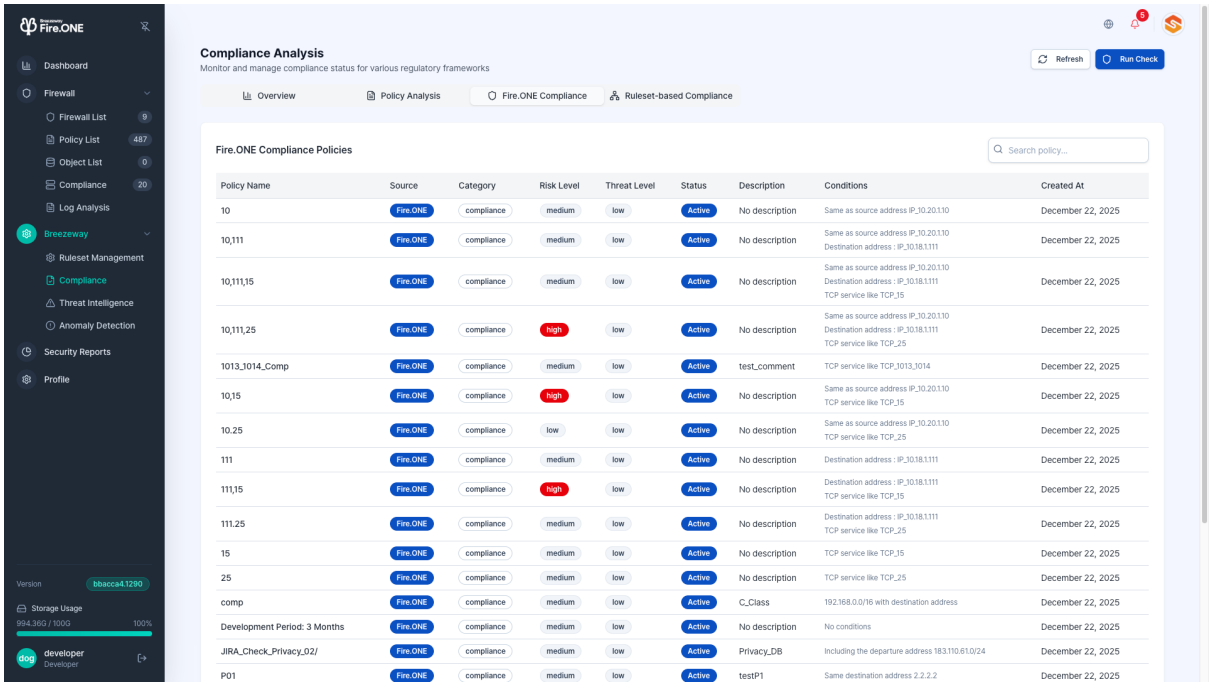



〈Compliance - Policy Analysis Screen〉

- Firewall Policy Compliance Analysis

| Column Name | Description |
|---|---|
| Firewall | The name of the firewall device to which this policy is applied. |
| Policy ID | The policy identification number used by the firewall. |
| Policy Name | The name or alias of the policy. |
| Source | The source address/network configured in the policy. Displayed as IP, range, any, etc. |
| Destination | The destination address/network configured in the policy. |
| Service | Information about the services (ports/protocols) that the policy allows or blocks. Example: HTTPS, TCP/8193-8194, etc. |
| Action | The setting value determining whether the policy allows or blocks the corresponding traffic. |
| Status | The operational status of the policy. Example: Active, Inactive. |
| Violation Policy | The determination of whether this policy is compliant or non-compliant based on the compliance check result. |
| Reason for Violation | A summary explanation of which rule was violated and how, if the policy was determined to be in violation. |
| Description | This area allows you to add additional notes about the policy if needed. |

3) Fire.ONE Compliance: The Fire.ONE Compliance tab displays a list of compliance policies defined within the system and the characteristics of each policy.

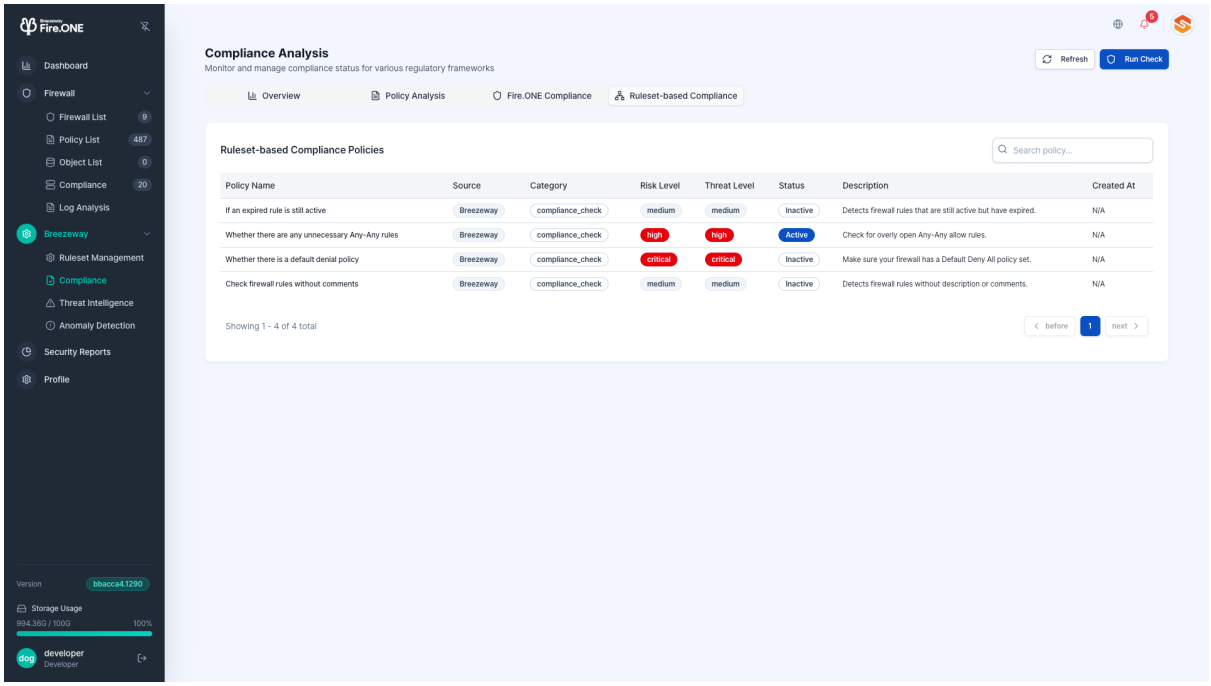



〈Compliance Analysis - Fire.ONE Compliance Screen〉

- Fire.ONE Compliance Policy

| Column Name | Description |
|---|---|
| **Policy Name** | This is the name of the compliance policy. Example: Cannot apply for over 1 year, destination ANY, etc. |
| **Source** | Indicates the policy group or source to which the policy belongs. (e.g., FPMS) |
| **Category** | Classification information for the policy. Example: compliance, compliance_check, etc. |
| **Risk Level** | The default risk level assigned when this compliance is violated. |
| **Threat Level** | The threat severity level applied when an actual violation occurs. (Typically set to match the risk level) |
| **Status** | Indicates whether the policy is active or inactive. Only active policies are used for compliance checks. |
| **Description** | Text describing what the item checks. |
| **Conditions** | The detailed conditions the policy uses for checks. Examples: Based on expiration date, include/exclude specific objects, port conditions, etc. |
| **Creation Date** | The date the compliance policy was registered in the system. (May be marked as N/A) |

4) Rule Set-Based Compliance: The Rule Set-Based Compliance tab displays the results of policy checks performed using inspection items provided by external/recommended rule sets (e.g., Breezeway).




〈Compliance Analysis - Rule Set-Based Compliance Screen〉

- Rule Set-Based Compliance Policy

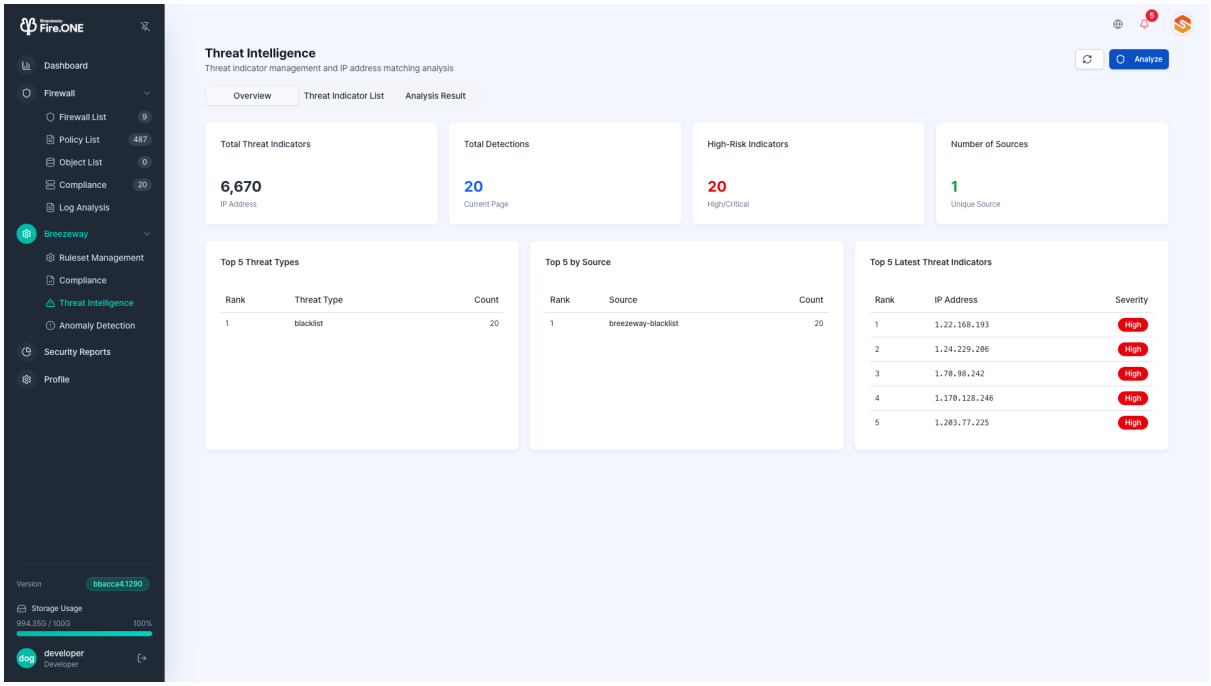
| Column Name | Description |
|---|---|
| **Policy Name** | The name of the compliance check item defined in the ruleset. Example: Whether expired rules remain active, presence of a default deny policy, etc. |
| **Source** | The source of the ruleset providing this check item. Example: Breezeway. |
| **Category** | The classification to which the check item belongs. Example: compliance_check. |
| **Risk Level** | The default risk level assigned when this item is violated. Example: medium, high, critical. |
| **Threat Level** | The threat severity applied when the violation actually occurs. Typically displayed the same as the risk level. |
| **Status** | Indicates whether the check item is enabled. Only active items are included in the actual inspection. |
| **Description** | Text describing what the item checks. |

| Creation Date | The date the check item was registered. (May display as N/A for external rulesets.) |
|---|---|

### 2.2.9 Breezeway Diagnostics - Threat Intelligence

The Threat Intelligence screen manages threat indicators (primarily IP addresses) collected from external and internal sources and analyzes threat IP detection status by matching them with actual traffic logs.

1) Overview: This screen provides a quick overview of the threat indicators currently held by the system and their detection status.



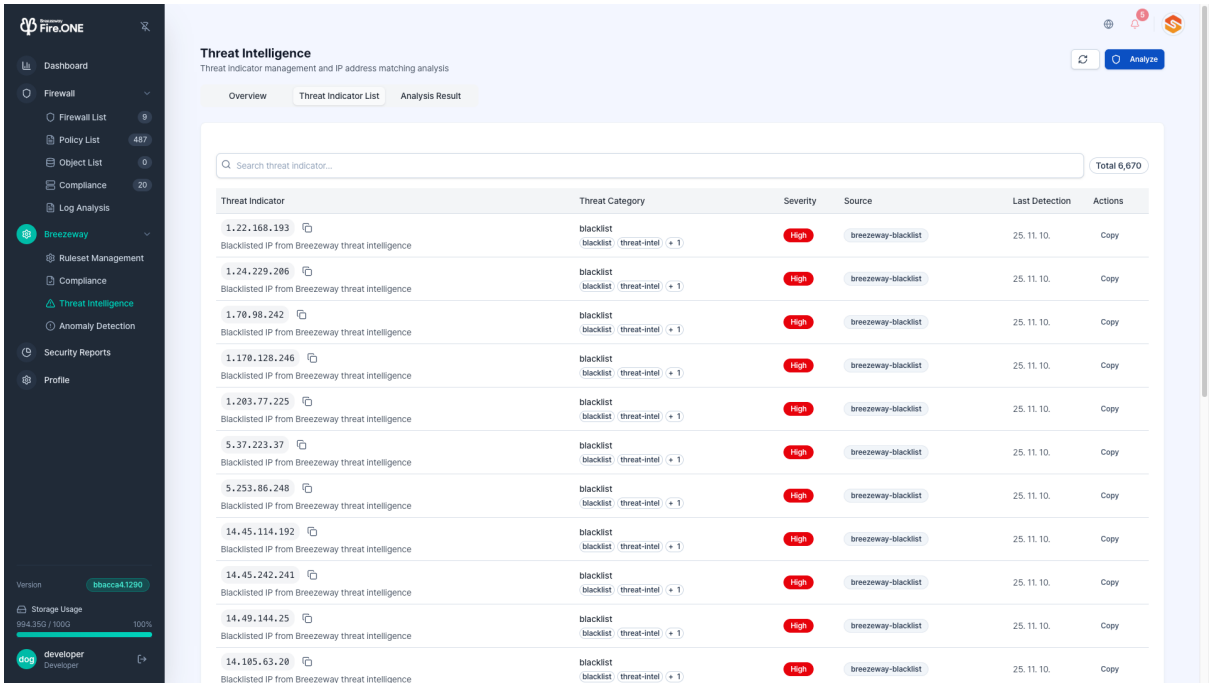

〈Threat Intelligence - Overview Screen〉

| Item | Description |
|---|---|
| **Total Threat Indicators** | The total number of threat indicators currently registered in the system. (Based on IP addresses) |
| **Total Detection Count** | The number of threat detection events matched with threat indicators based on traffic log analysis. |
| **High-Risk Indicators** | The number of threat indicators with a severity level of Critical or High among the registered indicators. |
| **Number of sources** | The number of sources (unique sources) providing threat indicators. |

Below is the Top 5 panel showing the distribution of threat indicators.

- Top 5 Threat Types
  - Displays the top 5 threat types by count, such as malware, C2 servers, spam, and scanning IPs.
  - You can determine which types of threats were collected most frequently.
- Top 5 by Source
  - This displays the top 5 sources with the highest number of collected threat indicators (Feed Source).
  - You can see which sources are contributing the most threat information.
- Top 5 New Threat Indicators
  - Displays recently added threat indicators along with their IP addresses and severity levels.
  - Quickly identify newly added high-risk IPs and incorporate them into separate monitoring.

2) Threat Indicator List: View all threat indicators registered in the system in a tabular format.



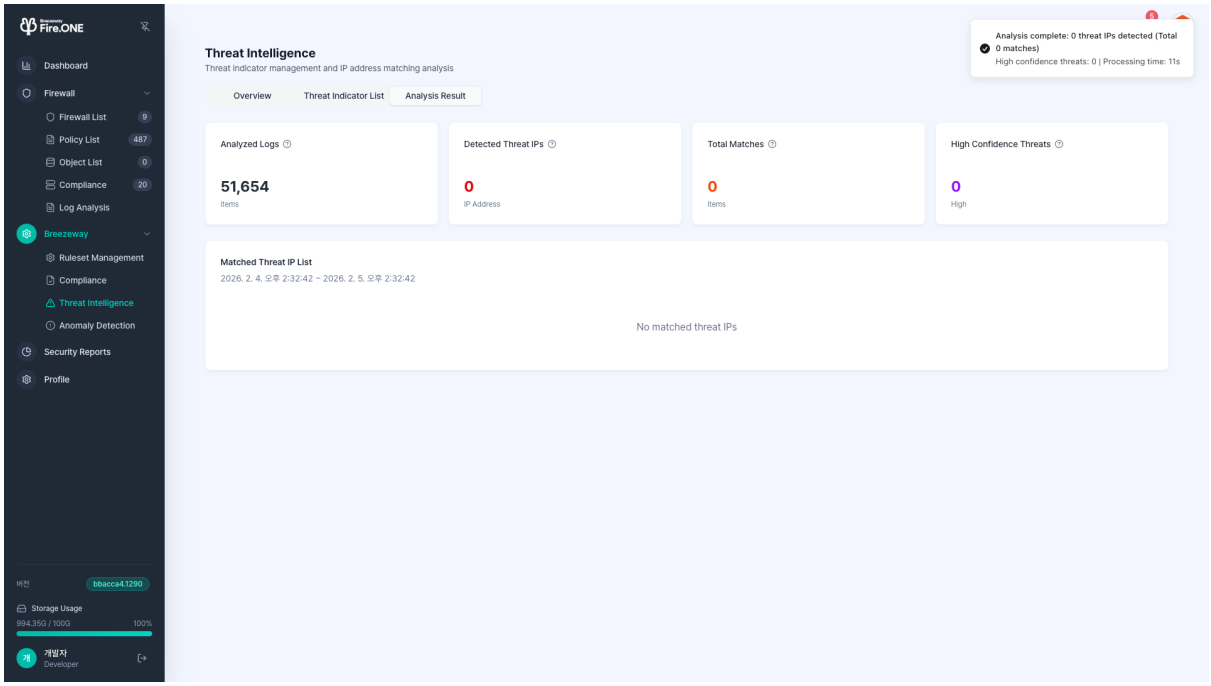

〈Threat Intelligence - Threat Indicator List Screen〉

- Table Details

| Column Name | Description |
|---|---|

| | |
|---|---|
| **Threat Indicator** | IP addresses or domains classified as threats. Each row in the list represents one indicator. |
| **Threat Classification** | Indicates the type of threat associated with the indicator. Example: Blacklist |
| **Severity** | The risk level assigned to the indicator. |
| **Source** | The information source (Threat Feed) that provided the threat indicator. Example: breezeway-blacklist |
| **Last Detected** | The time when the indicator was last detected in actual traffic. This allows you to check if there has been recent activity. |
| **Actions** | This button area allows you to copy the indicator value or perform actions for future expansion, such as linking to detailed views or blocking policies. (Currently provides 'Copy' functionality) |

3) Analysis Results: Clicking the [Analyze] button summarizes the results matched with the threat indicator after analyzing actual logs.




〈Threat Intelligence - Analysis Results Screen〉

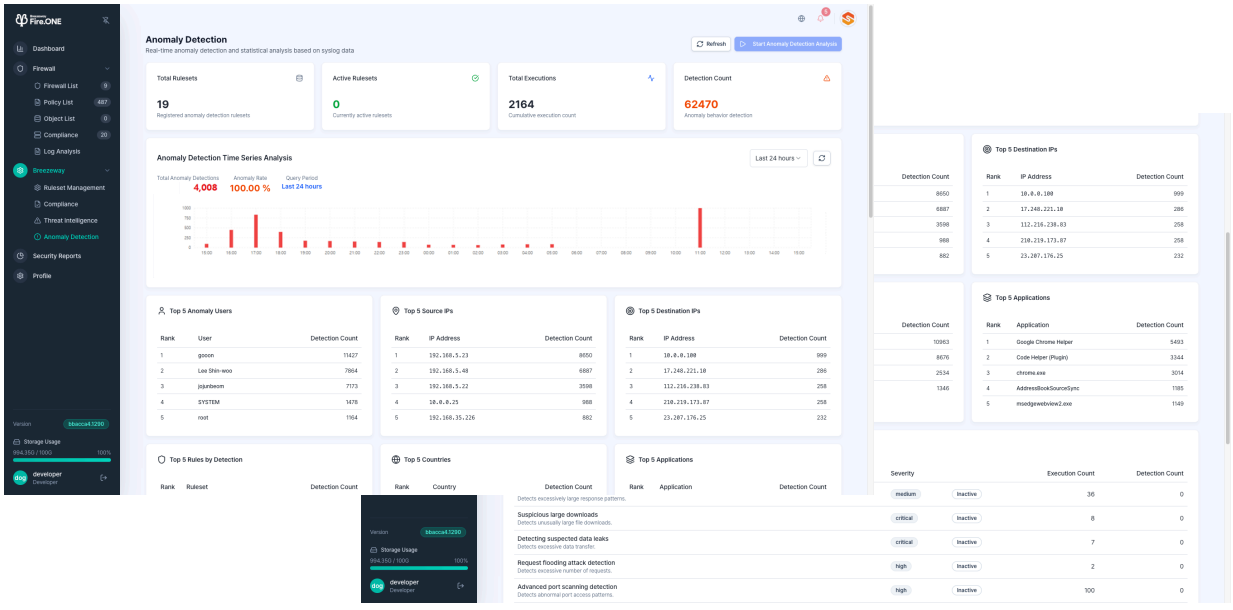
- Details

| Item | Description |
|---|---|
| **Analyzed Logs** | Total number of logs used for threat intelligence analysis. All firewall logs within the specified time |

| | |
|---|---|
| | range are analyzed and matched against threat indicators. |
| **Detected Threat IPs** | The number of unique threat IP addresses found in the logs. This indicates instances where malicious IP addresses registered in the threat intelligence database were detected in actual traffic logs. |
| **Total Match Count** | The total number of times threat IP addresses matched in the logs. If a single threat IP is found in multiple logs, all instances are counted and displayed. |
| **High-severity threats** | The number of threat IPs with a confidence level set to "high" or "critical." High-confidence threats may require immediate security action. |
| **List of matched threat IPs** | The list of matched threat IPs is displayed, along with the analysis period. |

### 2.2.10 Breezeway Diagnostics - Anomaly Detection

The Anomaly Detection screen provides real-time detection and statistical analysis of abnormal behavior (anomalies) based on syslog and traffic data.




〈Anomaly Detection Screen〉

- Top Items

| Item | Description |
|---|---|

| | |
|---|---|
| **Total Ruleset** | The total number of registered anomaly detection rulesets. This indicates the number of detection rules currently available in the system. |
| **Active Rulesets** | The number of rule sets that are currently active and being used for actual detection. Only active rules are reflected in anomaly analysis. |
| **Total Executions** | The cumulative number of executions for all anomaly detection rulesets. This indicates how frequently analysis has been performed. |
| **Detection Count** | The total number of events detected as abnormal behavior. This provides an at-a-glance view of the scale of anomalies in the current environment. |

Click the [Start Anomaly Detection Analysis] button in the upper-right corner to perform anomaly detection analysis on the latest logs based on the configured ruleset. The [Refresh] button reloads the results.

The graph area displays the number of anomaly detections by time period.

- Anomaly Detection Count: Total number of anomalies detected during the selected period
- Anomaly Detection Rate: Percentage of anomaly events relative to total events
- Analysis Period: The time range currently represented by the graph (e.g., last 24 hours)
- The bar graph allows you to intuitively see which time periods show concentrated anomaly activity.
- You can change the analysis period using the dropdown on the right (e.g., "Last 24 Hours").

Below the graph, a Top 5 panel summarizes abnormal behavior from various perspectives.

| Panel Name | Description |
|---|---|
| **Top 5 Users with Abnormal Activity** | Displays the top 5 user accounts with the most anomaly detections. You can view the number of detections per user, helping to identify accounts suspected of misuse or compromise. |

| | |
|---|---|
| **Top 5 Source IPs** | Top 5 source IPs with the highest number of anomaly detections. This helps identify where abnormal activity primarily originates. |
| **Top 5 Destination IPs** | The top 5 destination IPs where the abnormal activity is directed. Use this to identify where the abnormal activity is heading. |
| **Top 5 Detections by Rule** | This shows which anomaly detection rule sets triggered the most detections. By reviewing the rule names and detection counts, you can distinguish specific types of abnormal activity. |
| **Top 5 by Country** | Displays the top 5 countries associated with IPs involved in anomaly detections. This enables monitoring of abnormal traffic from overseas or specific countries. |
| **Top 5 by Application** | The top 5 applications (processes/programs) where most anomaly detections occurred. Examples: chrome.exe, EXCEL.EXE, etc. You can identify which applications are exhibiting abnormal behavior. |

Below, the list of anomaly detection rulesets currently in use on the system is displayed in a table format.

- Anomaly Detection Ruleset List

| Column Name | Description |
|---|---|
| **Rule Set Name** | Displays the name and brief description of the anomaly detection rule set. |
| **Severity** | The risk level assigned when this rule set detects an anomaly. (medium, high, critical) |
| **Status** | The active/inactive status of the rule set. It is used for detection analysis only when active; switching it to inactive prevents it from generating events. |
| **Execution Count** | The number of times this rule set has performed analysis. This allows you to understand the schedule cycle and actual execution history. |
| **Detection Count** | The number of anomaly detection events generated by the rule set. This can be used as a criterion to distinguish between rules with high detection efficiency and those requiring tuning. |

### 2.2.11 Security Report

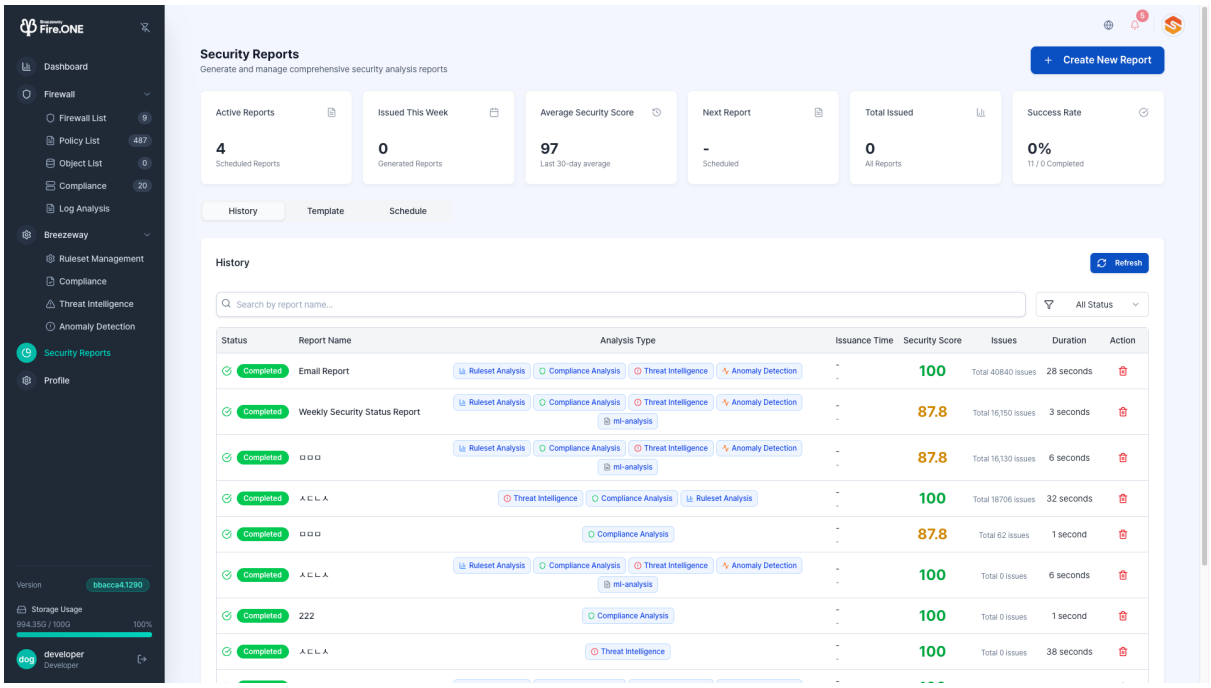
The Security Report screen generates weekly/monthly security status reports based on results collected and analyzed by Fire.ONE, and manages templates and schedules.

The top section always displays the following four items:

| Item | Description |
|---|---|
| **Active Reports** | The number of report templates currently set to be automatically issued according to the schedule. |
| **Issued This Week** | The number of reports generated this week. Includes both manual and scheduled issuances. |
| **Average Security Score** | The average security score of reports generated over the last 30 days. This helps track the overall security level trend of your organization. |
| **Upcoming Reports** | This shows the schedule for reports set to be automatically published in the future. If no reports are scheduled, it displays "None Scheduled". |

1) Issuance History

The Issue History tab displays a list of all security reports generated to date.




〈Security Report - Issue History Screen〉

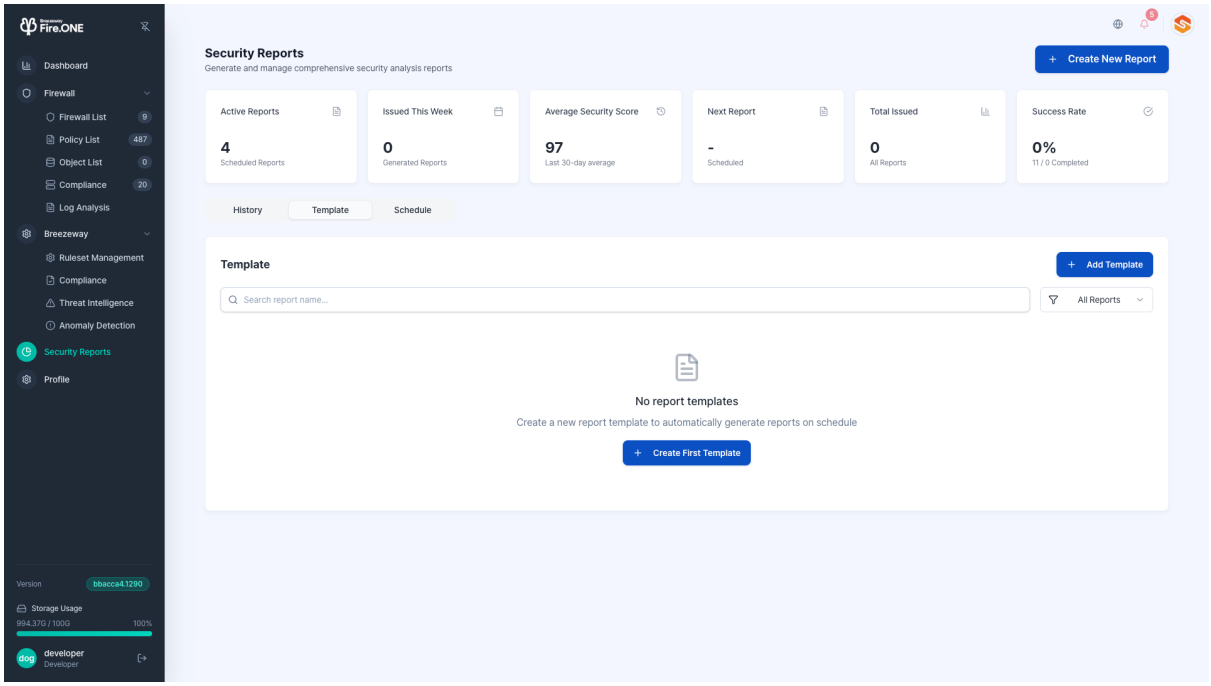
You can view the total number of reports issued, success rate, average security score, and trends at a glance, and also check detailed issuance history for each report.
Below is an explanation of the issuance history.

- You can search by report name in the top search bar.
- Use the [Refresh] button to reload the latest issuance history.
- Issuance History

| Column Name | Description |
|---|---|
| **Status** | The result status of the report generation task. Examples: Completed, Failed, In Progress, etc. |
| **Report Name** | The report title specified by the user. Example: Weekly Security Status Report. |
| **Analysis Type** | The analysis areas that compose the report. Example: Multiple types such as Compliance Analysis, Threat Intelligence, and Anomaly Detection may be displayed together. |
| **Issuance Time** | Displays both the exact time the report was generated and a relative time in the format "n minutes ago". |
| **Security Score** | The overall security score calculated for this report. It represents a combined assessment of multiple analysis results on a scale of 0 to 100 points. |
| **Issues** | The total number of security issues (alerts, violations, etc.) aggregated in the report. |
| **Time Taken** | The time taken to generate the report. It displays the total time required for data collection, analysis, and report rendering in seconds. |
| **Actions** | This area displays icons for subsequent actions, such as deleting reports. (e.g., trash can icon) |

2) Template Management

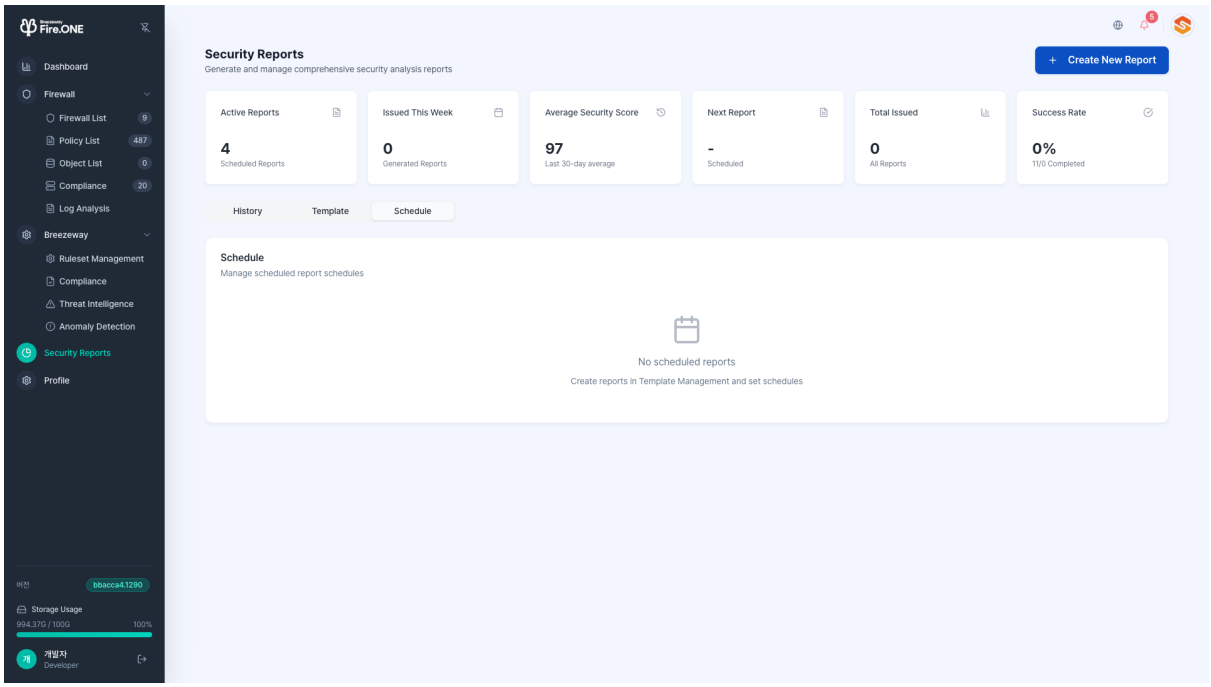
The Template Management screen allows you to modify, activate, deactivate, or delete created reports and templates.




〈Security Report - Template Management Screen〉

3) Schedule Management

The Schedule Management tab is the screen for managing scheduled tasks that automatically generate security reports.

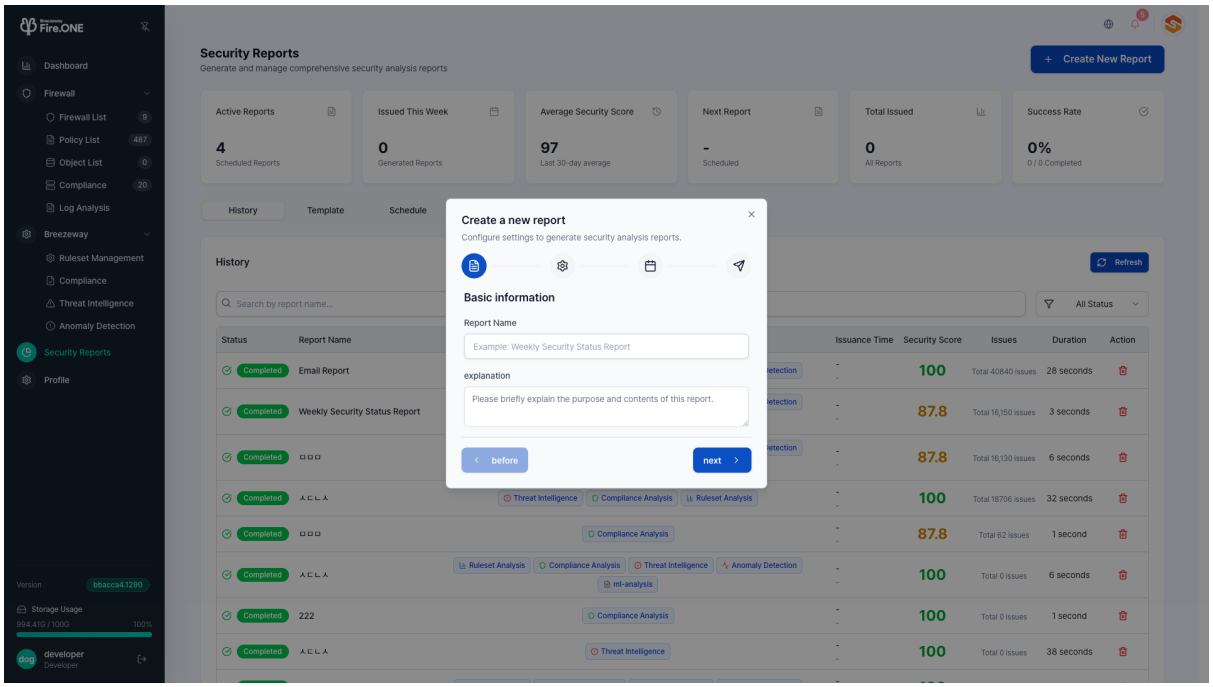



〈Security Report - Schedule Management Screen〉

4) Create New Report

Security reports proceed through a total of 4 steps.

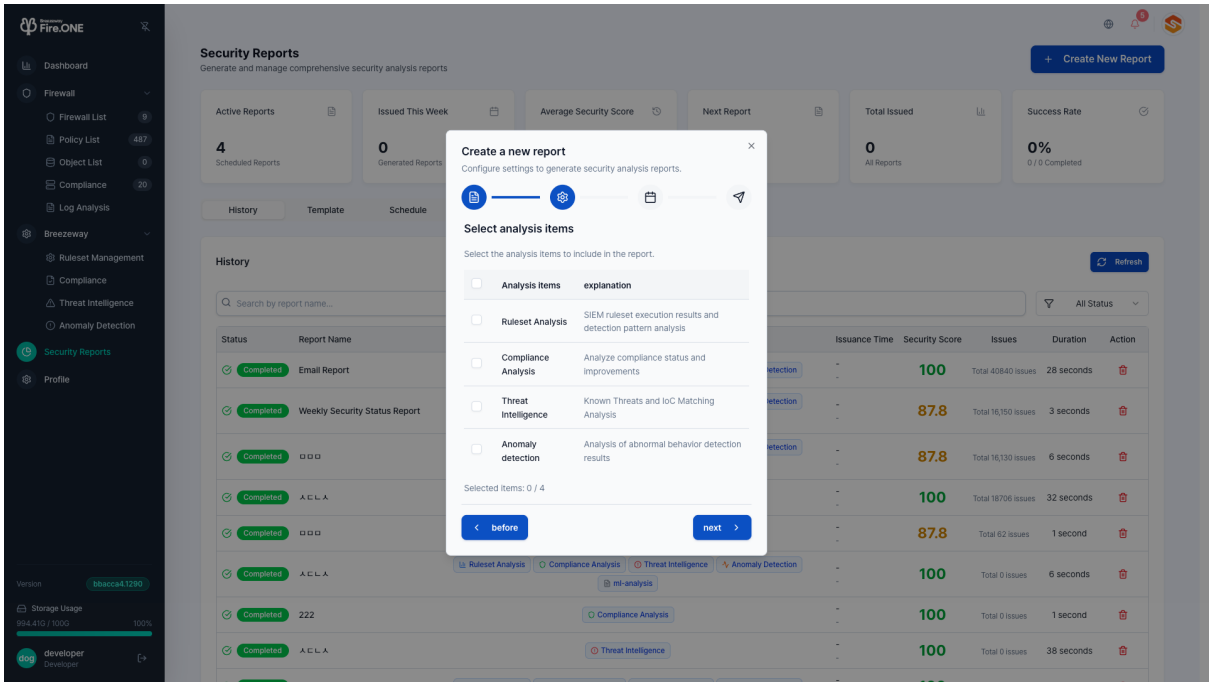
- Step 1: Set Basic Information




〈Basic Information Setup Screen〉

  - Report Name: Enter the report title. Example: Weekly Security Status Report, Monthly Compliance Report, etc.
  - Description: Briefly describe the report's purpose and content. Example: "Summary of Security Issues and Risk Levels Detected in the Past Week"
  - Click the [Next] button to proceed to the analysis item selection stage.

- Step 2: Select Analysis Items
  - Select the analysis areas to include in the report. (Maximum of 4)

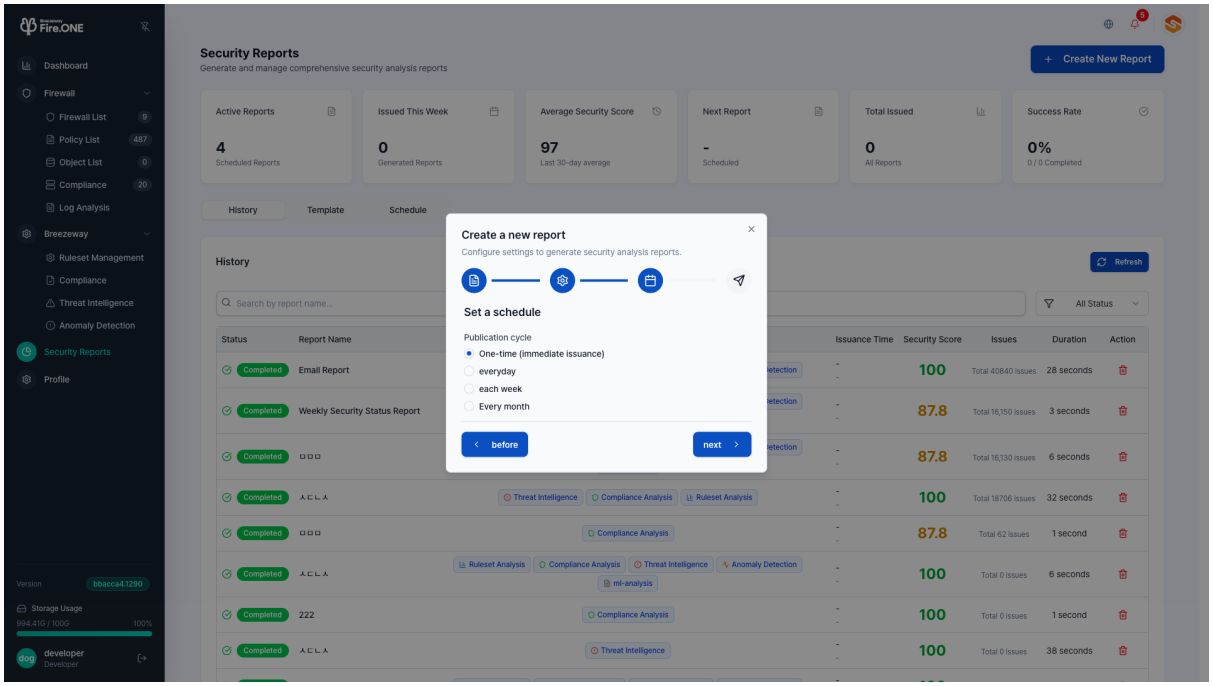



〈Analysis Item Selection Screen〉

- Toolset Analysis: Analysis of SIEM rule set execution results and detection patterns
- Compliance Analysis: Analysis of compliance status and improvement points
- Threat Intelligence: Analysis of external threat intelligence and IOC matching
- Anomaly Detection: Summary of anomaly behavior detection results
- Check the required items and click [Next].

- Step 3: Schedule Settings

Determine when and how often to generate the report.

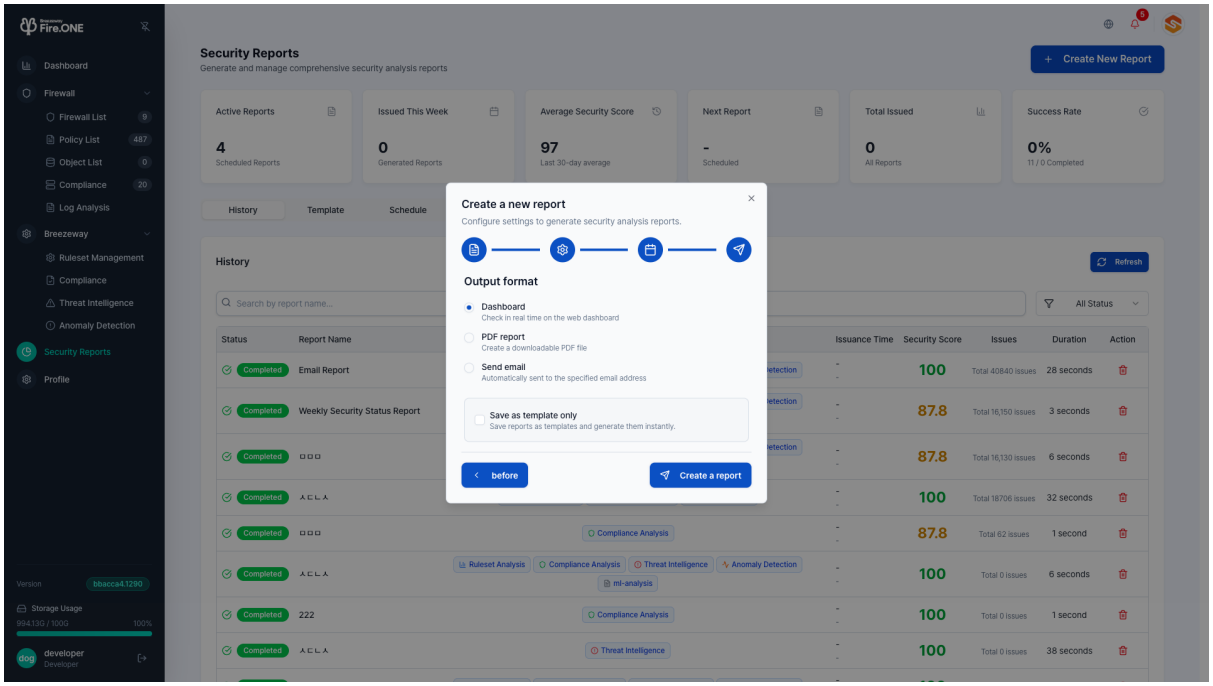



〈Schedule Settings Screen〉

- Issuance Frequency (One-time, Daily, Weekly, Monthly)
- Reports will be automatically generated and published according to the selected cycle.
- After completing the settings, click [Next] to proceed to the output format step.

- Step 4: Select and Generate Output Format

Determine the format in which you will use the report results.




〈Output Format Selection and Creation Screen〉

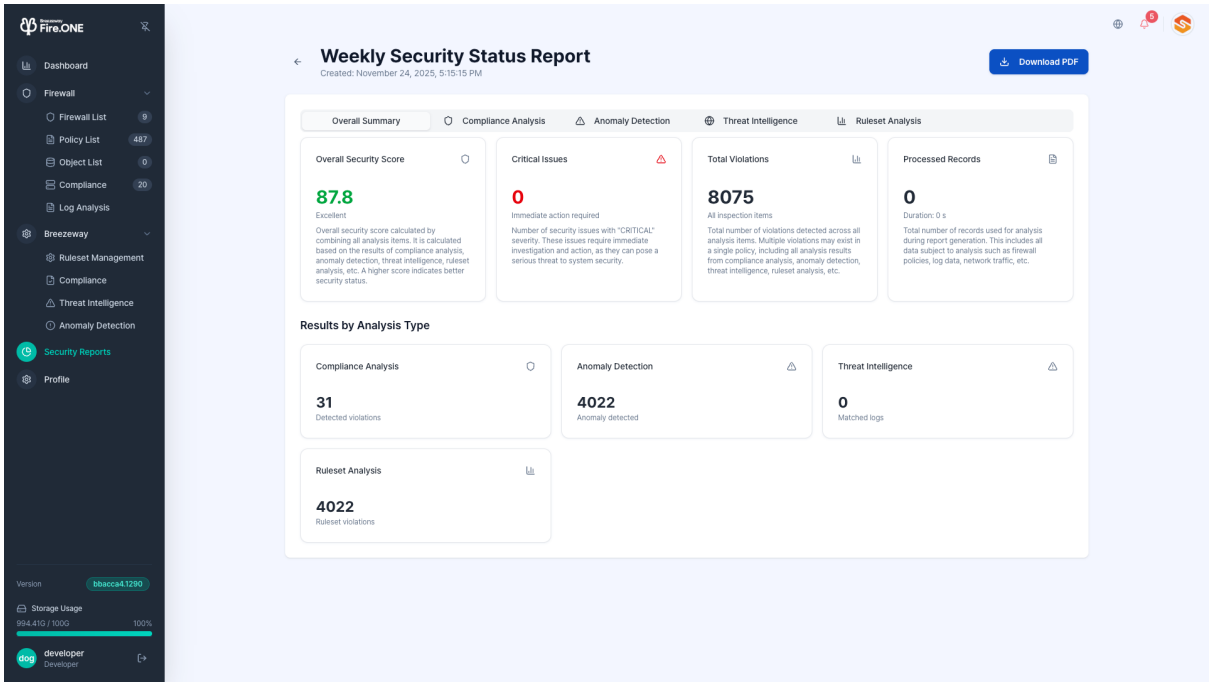
- Dashboard: View in real-time on the web dashboard
- PDF Report: Generate as a downloadable PDF file
- Email Delivery: Automatically send reports to specified email addresses
- Additional Option: Save as Template Only (Saves report settings as a template without immediate issuance)
- After selecting all items, clicking the [Generate Report] button creates the security report and schedules it based on the configured conditions.

5) Generated Security Report

The generated security report is issued based on the analysis items selected by the user and the schedule. The example below shows the security report issued when all analysis items are selected.

- Overall Summary

Displays an overall summary of the generated security report.

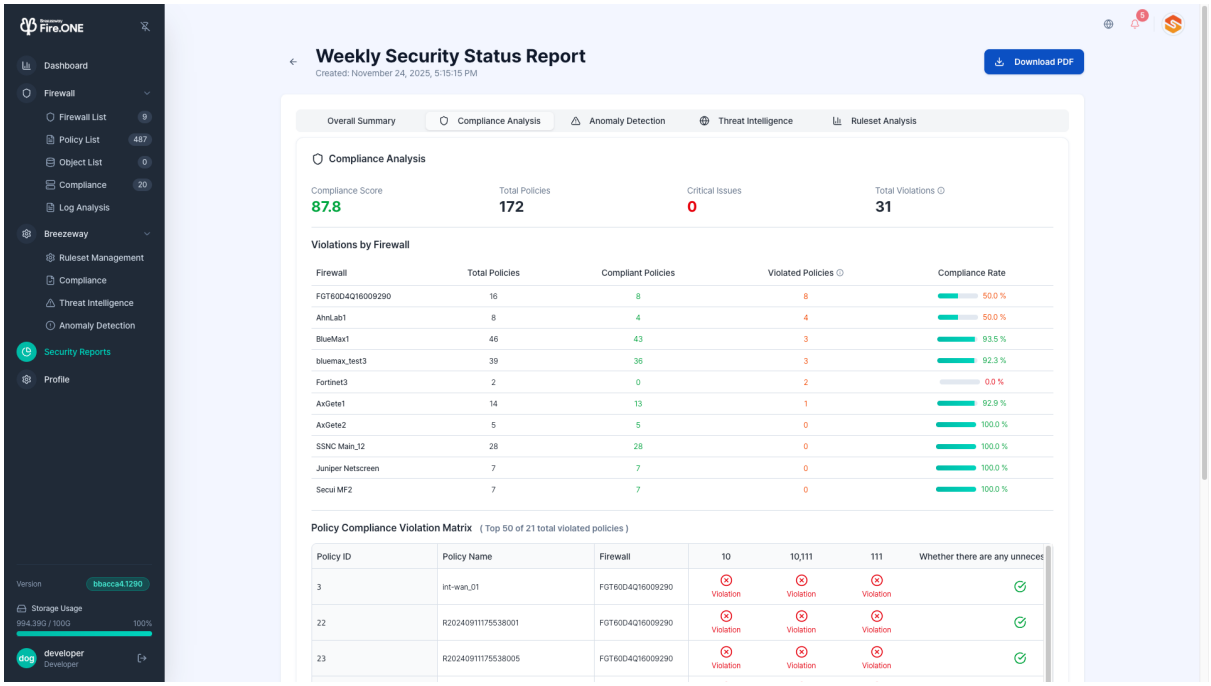



〈Generated Security Report - Overall Summary Screen〉

- Overall Security Score: The comprehensive security score calculated by combining all analysis items. It is determined by synthesizing results from compliance analysis, anomaly detection, threat intelligence, rule set analysis, and more. A higher score indicates a better security posture.
- Critical Issues: The number of security issues with a severity level of "CRITICAL." These issues require immediate investigation and action, as they can pose a serious threat to system security.
- Total Violations: The total number of violations detected across all analysis items. A single policy may have multiple violations, and this includes all analysis results from compliance analysis, anomaly detection, threat intelligence, and ruleset analysis.
- Processed Records: The total number of records used in the analysis when generating the report. This represents the count of all analyzed data, including firewall policies, log data, and network traffic.
- Results by Analysis Item: Shows results for the selected analysis items (currently all selected: compliance analysis, anomaly detection, threat intelligence, ruleset analysis).

- Compliance Analysis

Displays detailed compliance analysis information for the generated report.

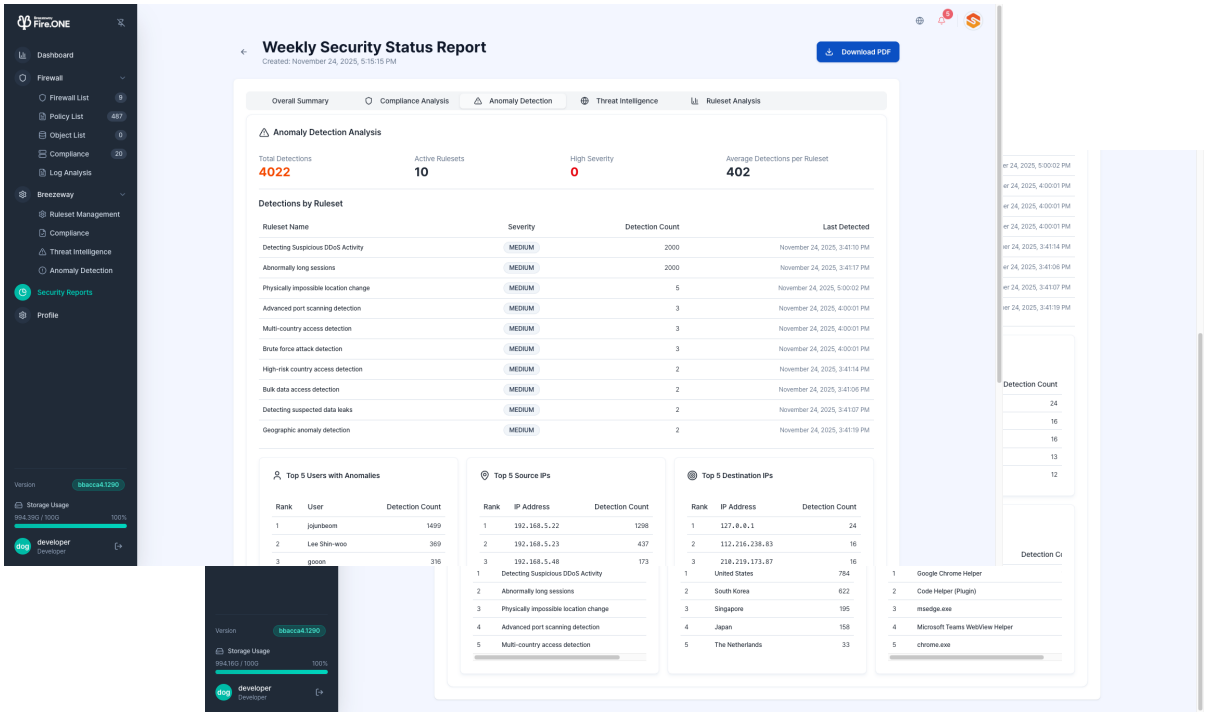



〈Generated Security Report - Compliance Analysis Screen〉

- Compliance Score: The compliance score calculated based on the entire firewall policy. It is displayed as a value between 0 and 100, where 100 indicates that all policies fully comply with the standards.
- Total Policies: The total number of firewall policies analyzed in this report.
- Critical Issues: Represents the number of compliance violation policies classified as 'Critical' according to internal standards.
- Total Violations: Total number of violations; one policy may have multiple violations.
- Violations per Firewall: Shows the compliance status of policies per each firewall device.

- Anomaly Detection

Displays anomaly detection details for the generated report.

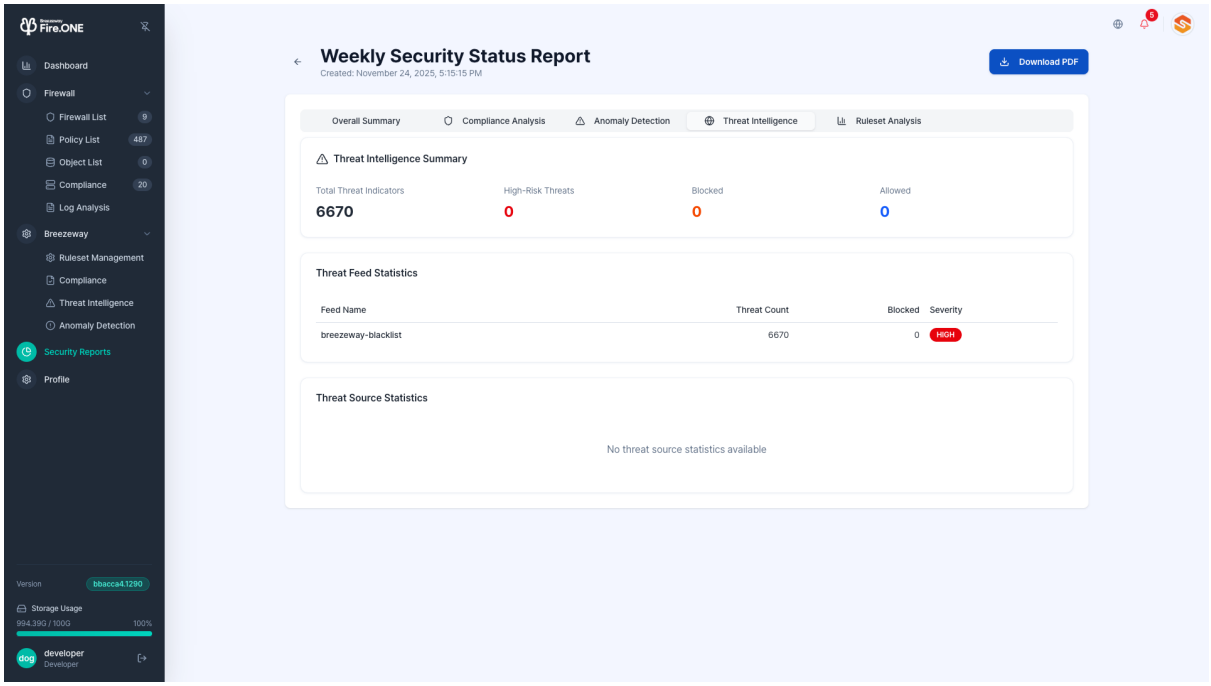



〈Generated Security Report - Anomaly Detection Screen〉

- Anomaly Detection Analysis: Shows total detections, active rulesets, severity score (0 ~ 100), and detections per ruleset.
- Detection Status by Ruleset: Shows the severity level, number of detections, and last detection time for each ruleset.
- Top 5 Detailed Analysis: Shows the top 5 distributions by abnormal user behavior, source IP, destination IP, rule-based detection, country, and application.

- Threat Intelligence

Displays threat intelligence information for the generated report.

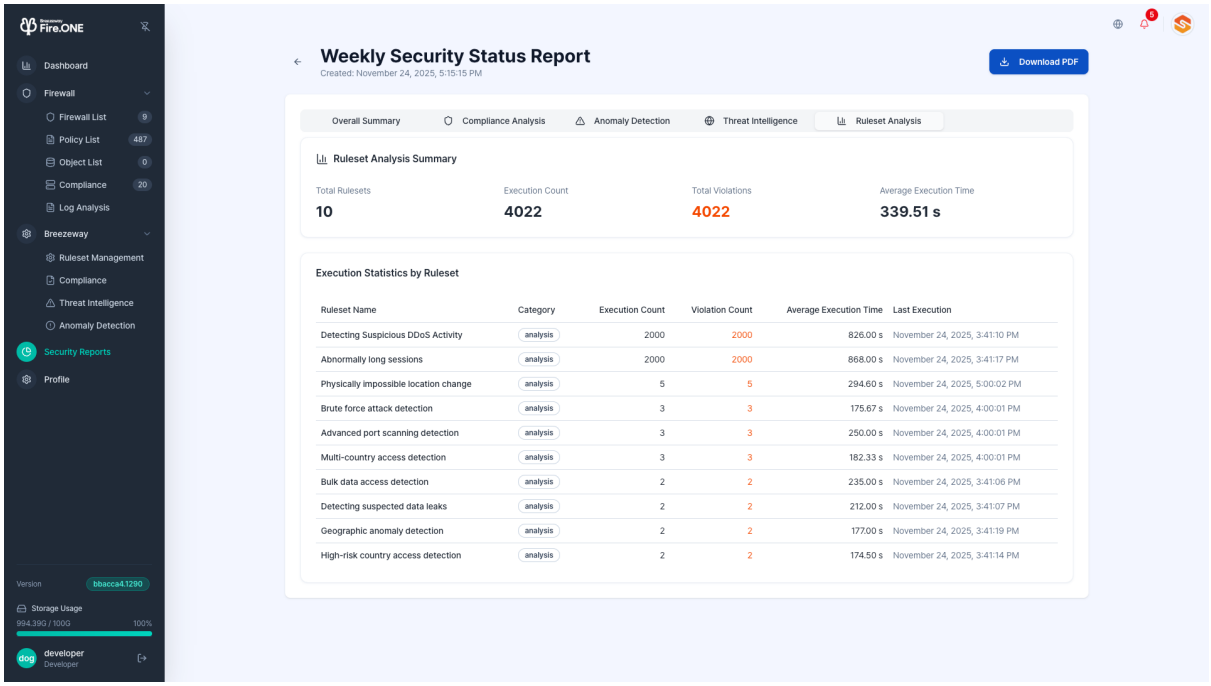



〈Generated Security Report - Threat Intelligence Screen〉

- Threat Intelligence Summary: Provides summary information on total threat indicators, high-risk threats, blocked incidents, and allowed incidents.
- Threat Feed Statistics: Displays the number of threats, blocked incidents, and severity level per threat feed.
- Threat Source Statistics: Provides statistical information by threat source.

- Rule Set Analysis

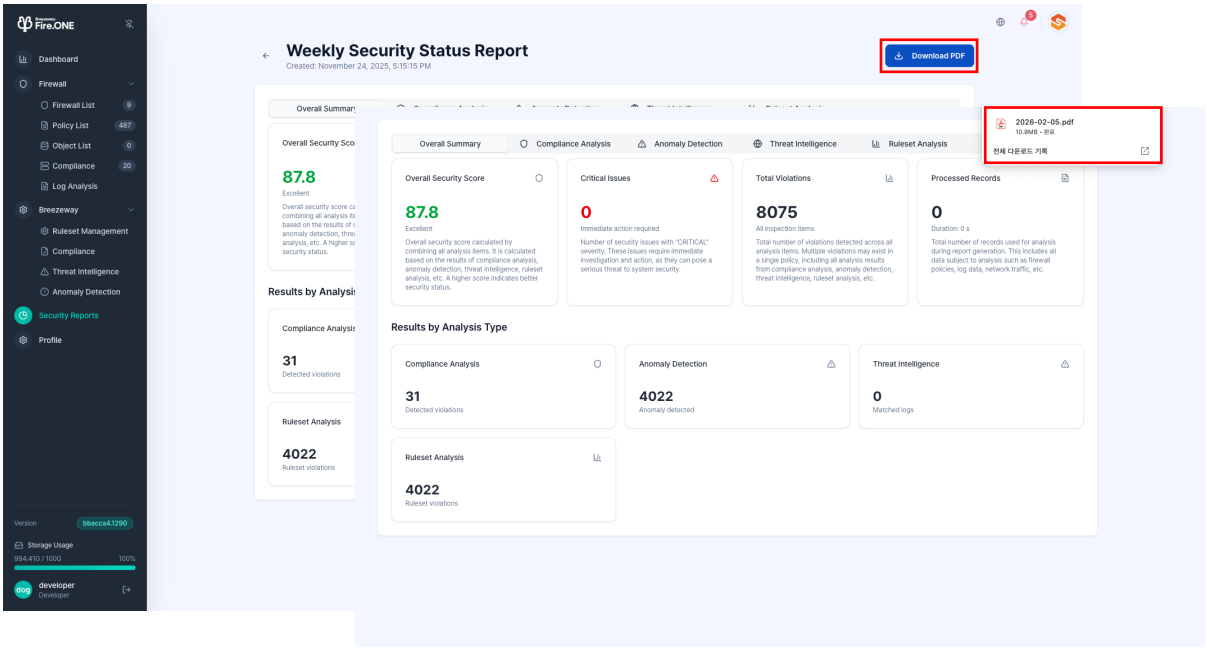
Displays the ruleset analysis for the generated report.




〈Generated Security Report - Ruleset Analysis Screen〉

- Ruleset Analysis Summary: Provides the total number of rulesets, execution count, total violation count, and average execution time.
- Rule Set Execution Statistics: Displays category, execution count, violation count, average execution time, and last execution time per rule set.

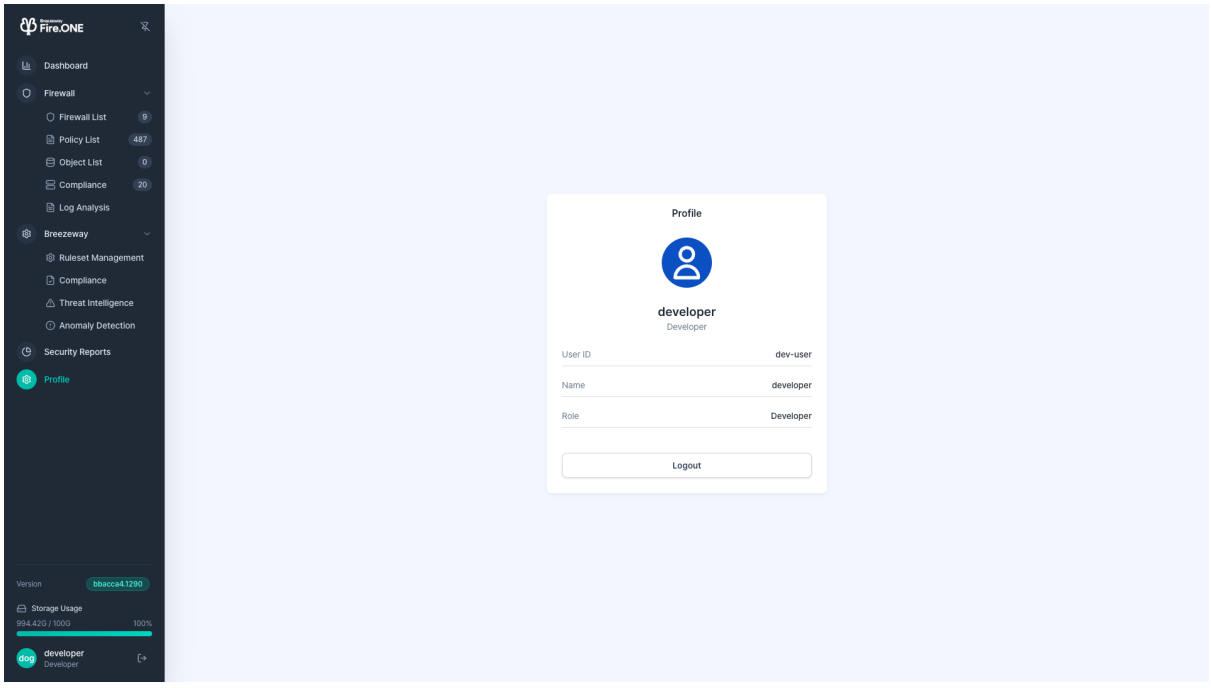
For any generated security report, you can generate a PDF file for the current screen by clicking the [PDF Download] button in the upper right corner of all screens.




〈Generated Security Report - PDF Download Screen〉

## 2.2.12 Profile

This feature allows you to check system user information and log them out.




〈Profile Screen〉

- Details

| Item | Description |
|---|---|

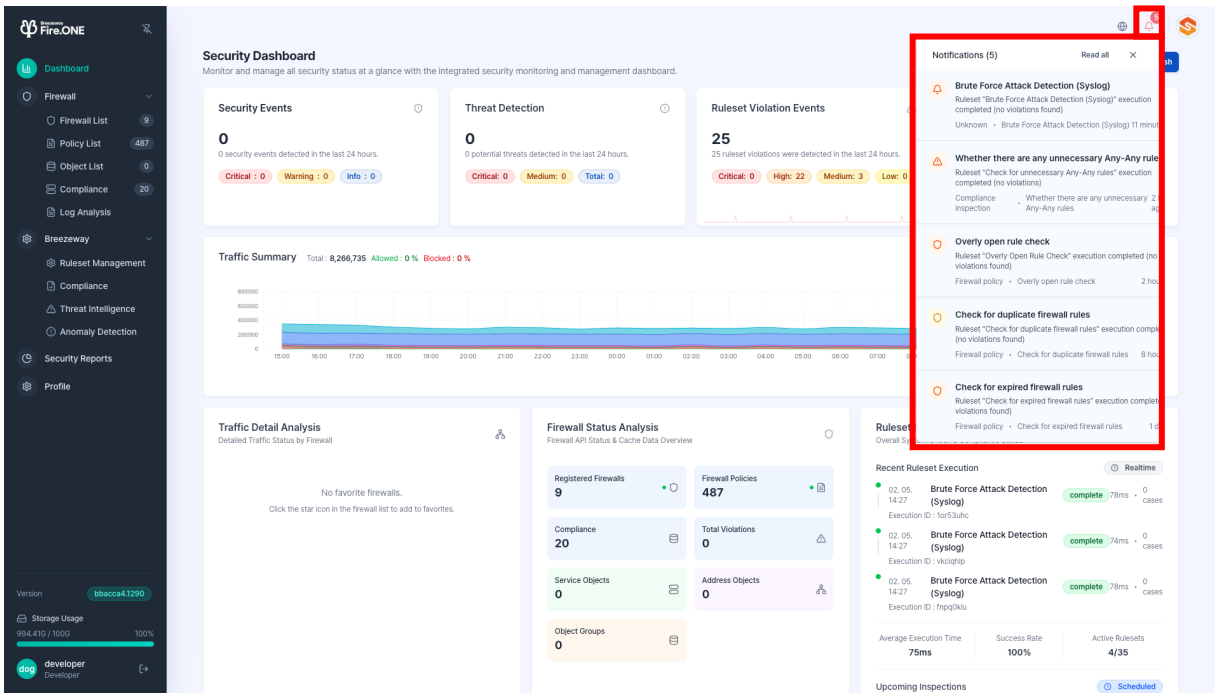
| | |
|---|---|
| **Profile Icon / Name** | Displays the user's profile icon and name (e.g., Developer). |
| **User ID** | The account ID used for login. Example: dev-user. |
| **Name** | The user name registered in the system. |
| **Role** | The permission role assigned to the account. Example: Developer, Administrator, etc. Accessible menus and features vary depending on the role. |

You can log out of your account by clicking the Logout button.

### 2.2.13 Other Features

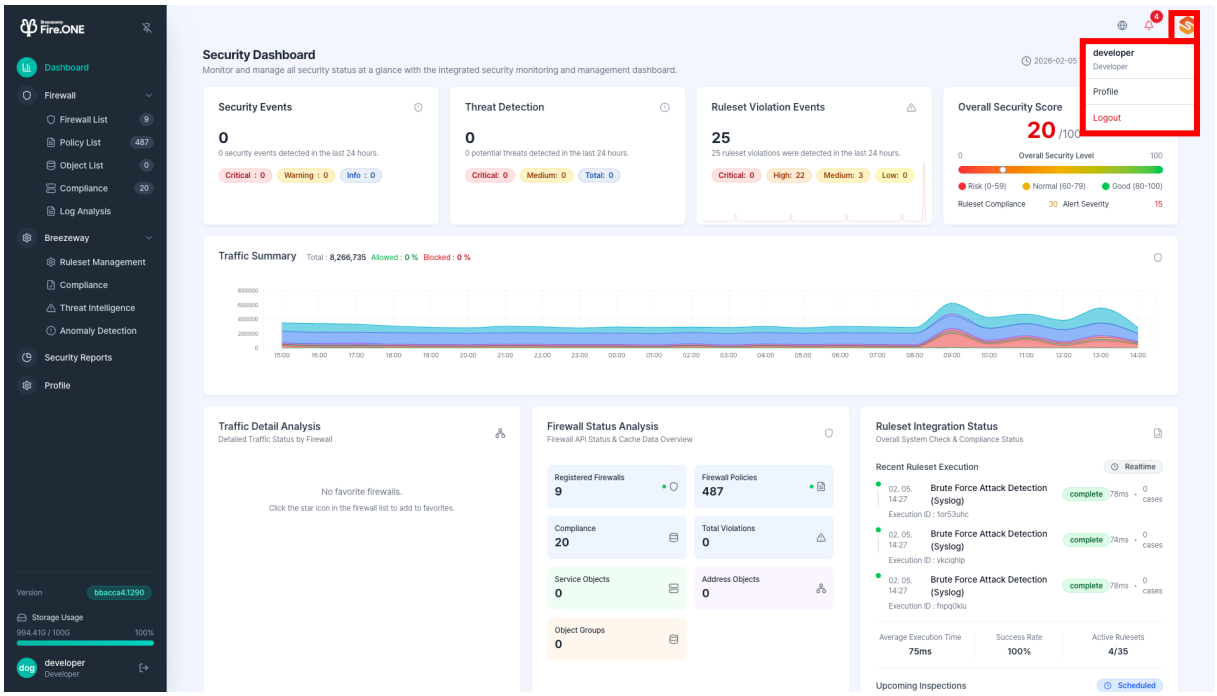
On the diagnostic platform, you can view recent notifications by clicking the notification icon in the upper right corner.

- Notification Content
  - Notification Title: e.g., Detected abnormal traffic volume, Detected brute-force attack, etc.
  - Summary Message: Displays a summary of the notification's content.
  - Occurrence Time: Displays the time the notification was generated.
  - Clicking the [Mark All as Read] button allows you to mark all displayed notifications as read at once.




〈Notification Screen〉

Clicking the SSNC icon to the right of the notification icon opens the My Account menu, where you can go directly to the profile screen or log out.




〈My Account Menu Screen〉

## 2.2.14 Diagnostic Platform Configuration Procedure

This section describes the process of configuring the diagnostic platform to analyze data stored in the security log collector.

The security log collector is configured based on Elasticsearch, with a Fleet Server additionally configured to collect various security data. Kibana is the tool used to visualize the collected data and is configured separately from the diagnostic platform.

### 1) Elasticsearch Installation and Initial Configuration

Install Elasticsearch, which serves as the security log storage and search engine, and apply initial security, cluster, and storage settings.

※ The configuration steps for Elasticsearch, Kibana, Fleet, and the firewall collector are all part of the security log collection configuration phase.

### 2) Kibana Installation and Initial Configuration

Install Kibana for visualizing and managing Elasticsearch data, and configure dashboards, public keys, and authentication.

### 3) Fleet Installation and Initial Setup

Configure Fleet Server to set up agent management, enabling centralized batch management of logs incoming from each firewall device or agent.

4) Firewall Collector Configuration

Configure collectors to gather logs from each firewall device and integrate transmission formats, protocols, log types, etc.

5) Security Log Diagnostic Platform Configuration

Configure the Fire.ONE Log Diagnostic Platform, which performs anomaly detection, policy diagnostics, and risk analysis based on collected logs.

6) Fire.ONE API Integration Setup

Register API communication settings and authentication information to integrate firewall policy information, user information, device lists, etc., from the Fire.ONE API.

※ The Fire.ONE API is used for firewall policy reference purposes.

7) Data Integration Settings

Synchronize data between the security log collection platform and Fire.ONE to enable its use for policy diagnostics, traffic analysis, and anomaly detection.

※ This step involves setting the existing security log collection platform as the integration target.

### 2.2.15 User Perspective Flowchart

1) Login & View Overall Status

- Check the weekly security score and presence of critical issues on the dashboard.
- Check system status in Fire.ONE System Status, including API connections, number of firewalls, number of policies, etc.

2) Anomaly Detection / Threat Detection

- In Log Analysis, investigate specific IP, user, or service traffic.
- In Breezeway Rule Set Management, run diagnostic rule sets and identify violations.
- Review external threat matching results (IPs, domains, etc.) from threat intelligence/analysis.

- Review anomaly behavior statistics (Top 5 users, IPs, countries, apps) based on anomaly detection/analysis results.
- Perform advanced anomaly detection and model analysis using ML analysis when necessary.

3) Compliance & Policy Improvement
- Identify compliance rates and violation policies by framework in compliance analysis.
- Search for problematic firewall policies and download lists.

4) Result Summary & Reporting
- Review issuance history in security reports.
- You can view weekly/monthly security status reports.
- Internal reporting is possible via PDF download or email dispatch.

5) Post-Incident Tracking & Account Management
- Track administrator/user activity logs and risky behaviors in the audit log.
- View account information and log out from the profile.

## 2.3 Limitations and Performance

### 2.3.1 Limitations

This product provides a file registration feature for blacklist and compliance purposes when required. The supported file extension for upload is ".xlsx".

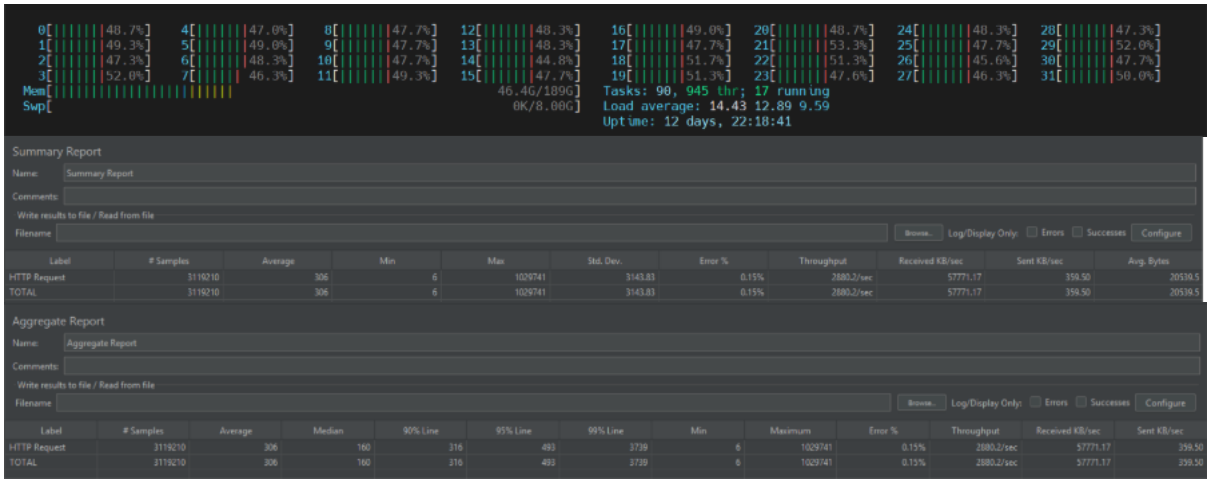
This product provides a function to upload supporting documentation for firewall policy requests. At this time, a maximum of 5 files can be uploaded, each within 500MB ( ), allowing for a total upload size of 2.5GB. There are no file extension restrictions for supporting documentation files.

Other data formats exchangeable between different products include Syslog, HTTP, Rest API, SMTP, Webhook, TLS, JSON, CSV, YAML, CEF, ECS, and SIGMA.

### 2.3.2 Performance

This product guarantees the following performance in the specified operating environment.

| Category | Measurement Result | Remarks |
|---|---|---|
| **Average Response Time** | 669 ms | This is an internal network measurement result; when applied to the internet network, 1000ms |
| **95% Response Time** | 493 ms | |
| **99th percentile response time** | 3739 ms | |
| **Transactions Per Second (TPS)** | 2880 requests per second | High processing performance |
| **CPU usage** | Average around 50% | Resources available |
| **Memory Usage** | Approximately 25% | Resources available |
| **Total requests** | 3.1M | |
| **Error rate** | 0.15% | Low level |
| **Maximum delay time** | 1029 seconds | Limited to some requests; timeout settings require optimization |
| **Concurrent user handling capacity** | Stable even with over 1000 users | |



## 2.4 User Error Prevention

This product provides a feature that checks and alerts users when they attempt incorrect input or actions.

When required values are missing or format errors occur, a confirmation message appears. When validation fails, a guidance message appears. During input, an input method guide is displayed alongside the input field to provide user confirmation messages.

## 2.5 Backup and Recovery

It provides DB backup, full backup, and incremental backup functions.

The DB configuration information is as follows.

- dbuser: argosuser
- dbname: argosdb

### 2.5.1 Automatic Scheduled Full Backup (dump)

- Automatic backup method

- Automatic backup server command

```
0 1 * * * pg_dump -U dbuser -F c -f /backup/db/full_`date +₩%Y₩%m₩%d`.dump dbname
```

  - Uses crontab to perform backups daily at dawn (minimum traffic time).
  - Perform the backup using pg_dump.
  - Perform the backup with dbUser privileges.
  - Specify the backup file format as custom using -F c.
  - Specify the backup file storage path and filename as `/backup/db/full_YYYYMMDD.dump`.

- Manual Backup Method

- Full backup server command

```
pg_dumpall -U postgres -f /backup/all_db_$(date +%Y%m%d).sql
```

  - Perform a full database backup using pg_dumpall.
  - To back up all databases, perform the backup using the superuser account `postgres`.

- Specify the backup file path and filename as /backup/all_db_$(date +%Y%m%d).sql.

- Server command for backing up a specific database

```
pg_dump -U postgres -F c -f /backup/dbname_$(date +%Y%m%d).dump dbname
```

- Specify the target database as dbname to perform a backup of a specific database.

### 2.5.2 Incremental Backup

- WAL Archive Configuration

```
postgresql.conf file
archive_mode = on
archive_command = 'rsync -a %p /backup/wal/%f'
archive_timeout = 60          # Force archive once per minute
```

### 2.5.3 Backup Directory

The location of each data is as follows.

- DB data: /var/lib/postgresql
- WAL Archive: /backup/wal

### 2.5.4 Deleting Backup Files from 7 Days Ago

- File deletion server command

```
$ find /backup/wal -type f -mtime +7 -delete
```

- Specifies files modified more than 7 days ago in the /backup/wal directory as the search target.
- Deletes files matching the search criteria.

### 2.5.5 DB Backup Recovery

- DB Backup Restore Server Command

```
$ pg_restore -U dbuser -d dbname /backup/db/20250101.dump
or
$ psql -U postgres -f /backup/all_db_20250101.sql
```

- Use the pg_restore command to restore a single database.

- Specify the dbuser and dbname for the restore, and specify the path to the backup file to be used for the restore.
- Restore the entire database backed up with pg_dumpall using the psql command.

## 2.6 Security Considerations

This product provides login functionality using ID/PW to ensure only authorized users can use it. It prevents direct URL access to pages accessible only to authorized users.

The encryption algorithms used are as follows: Communication channels (UI access, internal service-to-service communication) are encrypted using the TLS algorithm. Connection information for firewall devices is encrypted using the RSA algorithm because decryption is required. BreezeWay Fire.ONE web access information is stored after being hashed using the SHA256 + Salt algorithm. During authentication, a nonce value is additionally used to compare passwords. Log transmission uses gzip.

## 2.7 Dependent Resources (SW/HW)

None

## 2.8 User Interface

### 2.8.1 Fire.ONE UI

The Fire.ONE UI is a platform designed to enable users to easily and intuitively apply firewall policies, manage devices, and utilize analysis and reporting functions.
The overall design aims for a simple and intuitive UX/UI and features the following characteristics.

- Consistent left-sidebar-based layout:
  All main menus are placed in the left sidebar, allowing users to quickly access desired features.
- Clean screen composition:
  User profile and language change buttons are placed at the top to enhance accessibility.
- Role-Based Access Control (RBAC):
  Automatically controls displayed menus and features based on user permissions, ensuring both security and usability.

### 2.8.2 Menu and Navigation Structure

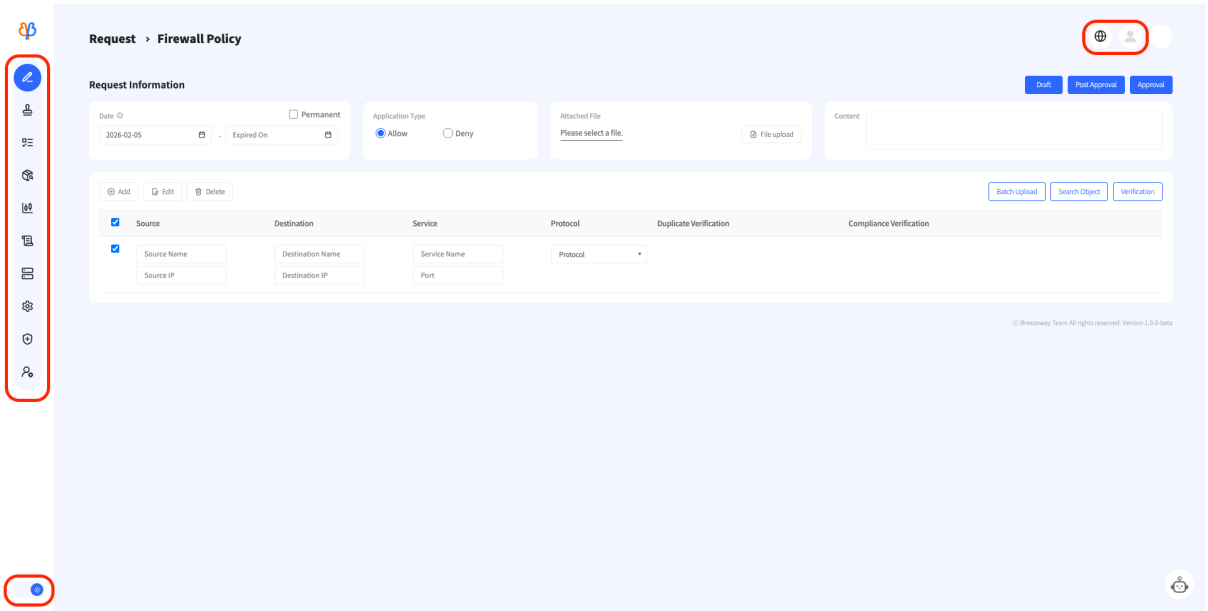
The Fire.ONE menu and navigation structure is centered around the left sidebar (Side Navigation). Each menu allows access to detailed functions through a hierarchical structure.

| Menu | Description |
|---|---|
| **Request** | Submit firewall policies and support efficient policy input through pre-validation, object selection, Excel uploads, and more. |
| **Approval** | Process approvals or rejections for submitted policies by approver, co-approver, and referrer, and review approval history. |
| **Policy** | Review firewall policies that have been applied and approved. Apply (Commit) or reject (Dismiss) policies separately for each firewall. |
| **Custom Objects** | Provides a user-friendly feature to register IPs, services, etc., as objects for convenient selection during policy requests. |
| **Governance** | Integrated management of firewall structure and policy risks, including network topology visualization, risk analysis, and compliance policy verification. |
| **Report** | View currently applied firewall policies and provides visualized diagnostic reports. |
| **Device** | A management menu that allows you to view basic information, rules, objects, etc., for registered firewall devices. |

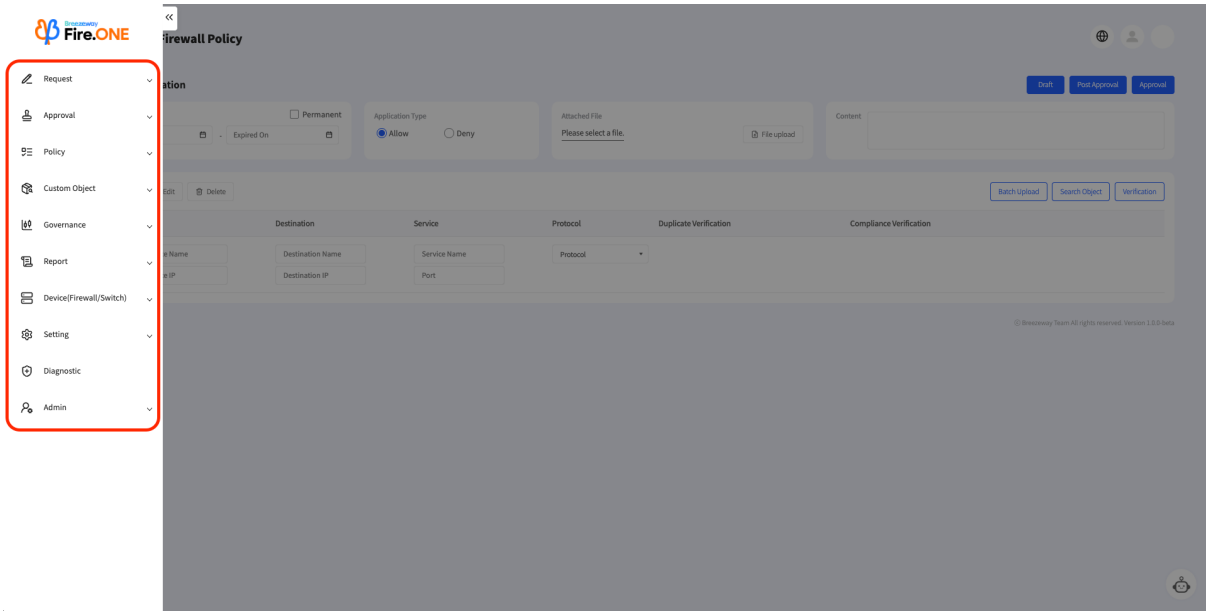
| | |
|---|---|
| **Settings** | View Fire.ONE web environment settings such as allowed IPs, departments, menus, and API lists with administrator privileges. |
| **Diagnostic** | Performs integrated security diagnostics through log and rule-based traffic analysis, policy evaluation, anomaly detection, and threat intelligence. |
| **Administrator** | Includes administrator-only functions such as firewall management settings by user/permission/organization, user activity logs, and application status checks. |

### 2.8.3 Screen Layout

The Fire.ONE interface features key function menus arranged as icons in the left sidebar, enabling users to easily navigate to each function page. Account information can be viewed and configured via the user information button in the top-right corner. The bottom-left corner includes a Dark Mode and Light Mode toggle button, allowing users to freely switch between themes as desired.




〈Screen Layout〉




〈Left Sidebar Open Screen〉

### 2.8.4 Icons and Buttons

Icons and buttons used in Fire.ONE are designed with intuitiveness, consistency, and accessibility in mind. Users can easily recognize the current state through screen components and perform necessary actions intuitively.

- Button Design and Functionality:
  Fire.ONE buttons are designed based on functional color and visual differentiation.

- Button Styles:
  - Primary Button
    - Background Color: Blue (#2C67FF)
    - Usage: Used for primary actions like search, save, submit
    - Visually most prominent; typically only one or a few are placed on a single screen
  - Secondary Button
    - Background color: White with blue border
    - Usage: Used for optional actions like reset or cancel
  - Disabled Button
    - Displayed in gray tones, indicating an unclickable state
    - Automatically disabled when user conditions are not met

- Button Interaction:
  - Hover Effect: When hovering over the button, its color darkens slightly to intuitively indicate actionability
  - Loading State: Displays a spinner icon during major operations to indicate progress

- Icon Design Principles:
  - Consistency: Use the same icon for the same function
  - Intuitive Design: Apply simple line icons to convey menu purpose at a glance
  - Highlighting: The selected menu is highlighted in blue to intuitively indicate the current position

- Icon Style:
  - Line icon centered
  - Single color used
  - Apply blue highlight effect when sidebar is active

# 2.9 User Convenience Features

## 2.9.1 System Access


〈Login Screen〉

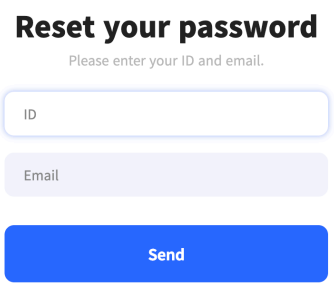
Access Method

1) Access the main URL via a web browser. (for Demo URL: https://Fire.ONE.breezeway.team:8190/)
2) When the 〈Login Screen〉 appears, enter your assigned ID and Password, then click the [LOGIN] button.
3) If the ID and password match the information stored on the server, you will be logged into the system.

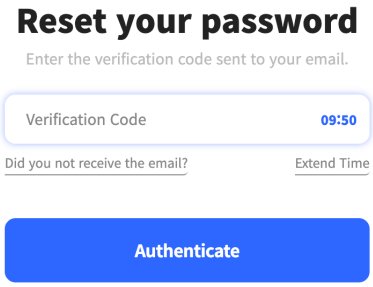
Error Message Pop-up Screen List

〈When ID and Password Do Not Match〉

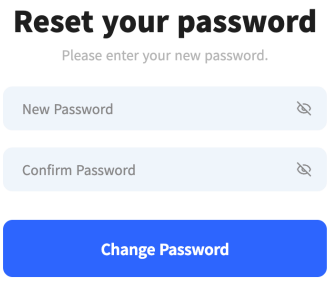
Password Reset Method



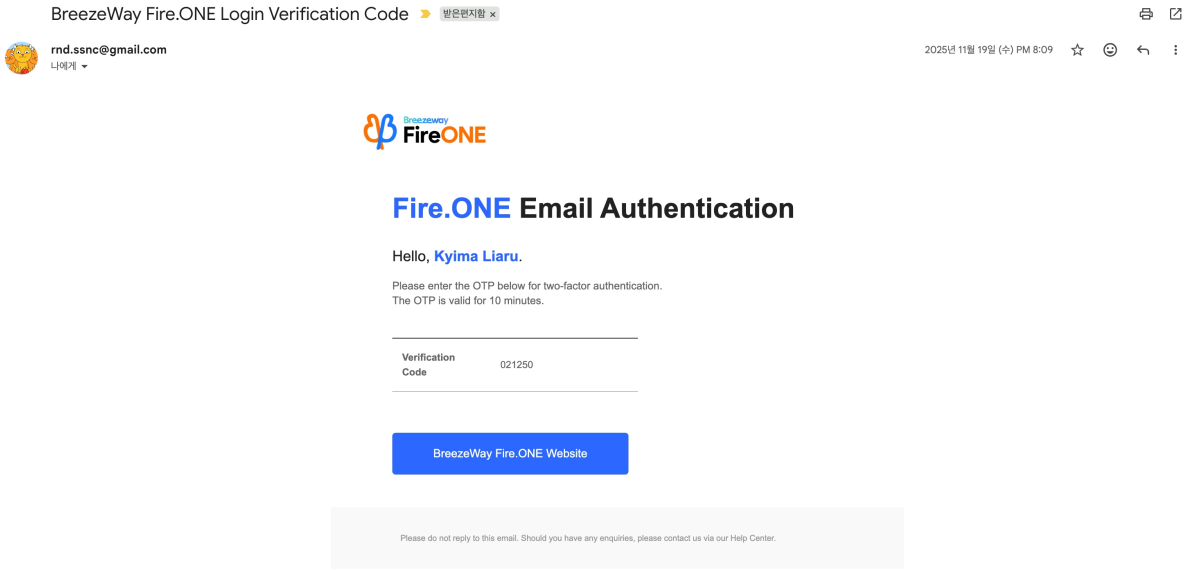

〈Password Reset Screen〉




〈Authentication Code Input Screen〉




〈New Password Input Screen〉



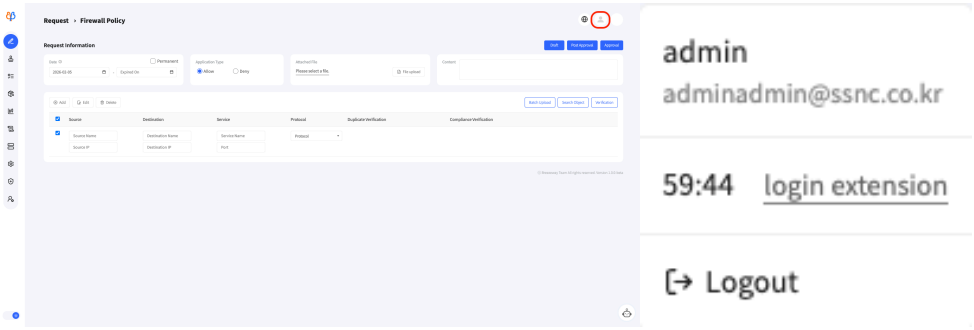

〈Example Screen of Password Reset Authentication Code Email〉

1) Access the Fire.ONE login page.
2) Click the [Forgot your password?] link below the login button.
3) The 〈Password Reset Screen〉 appears.
4) Enter the assigned ID and the email address registered to your account, then click the [Send] button.
5) Shortly after, an email containing the verification code will be sent, and the 〈Verification Code Input Screen〉 will appear.
6) Enter the verification code sent to your email on the screen, then click the [Verify] button.
7) Upon successful verification, the 〈Enter New Password Screen〉 will appear.

8) Enter your new password and click the [Change Password] button. Your password must contain at least one letter, one number, and one special character.
9) The <Login Screen> appears.

### 2.9.2 User Profile

Clicking the profile icon (person icon or profile photo) in the upper-right corner of Fire.ONE allows you to view information about the currently logged-in user and access account-related functions.

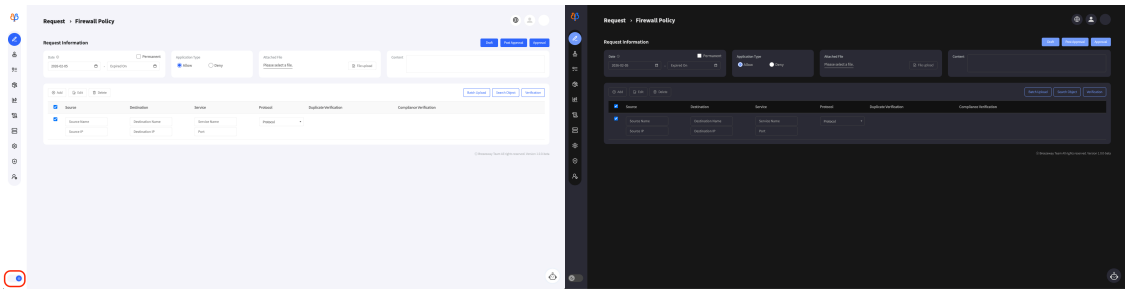



<Profile Information and Logout Screen>

1) The ID and registered email address of the currently logged-in account are displayed.
2) The remaining login time is displayed and can be extended if needed.
3) Clicking the [Logout] button at the bottom will immediately log you out and redirect you to the login screen.

### 2.9.3 Screen Mode Switching

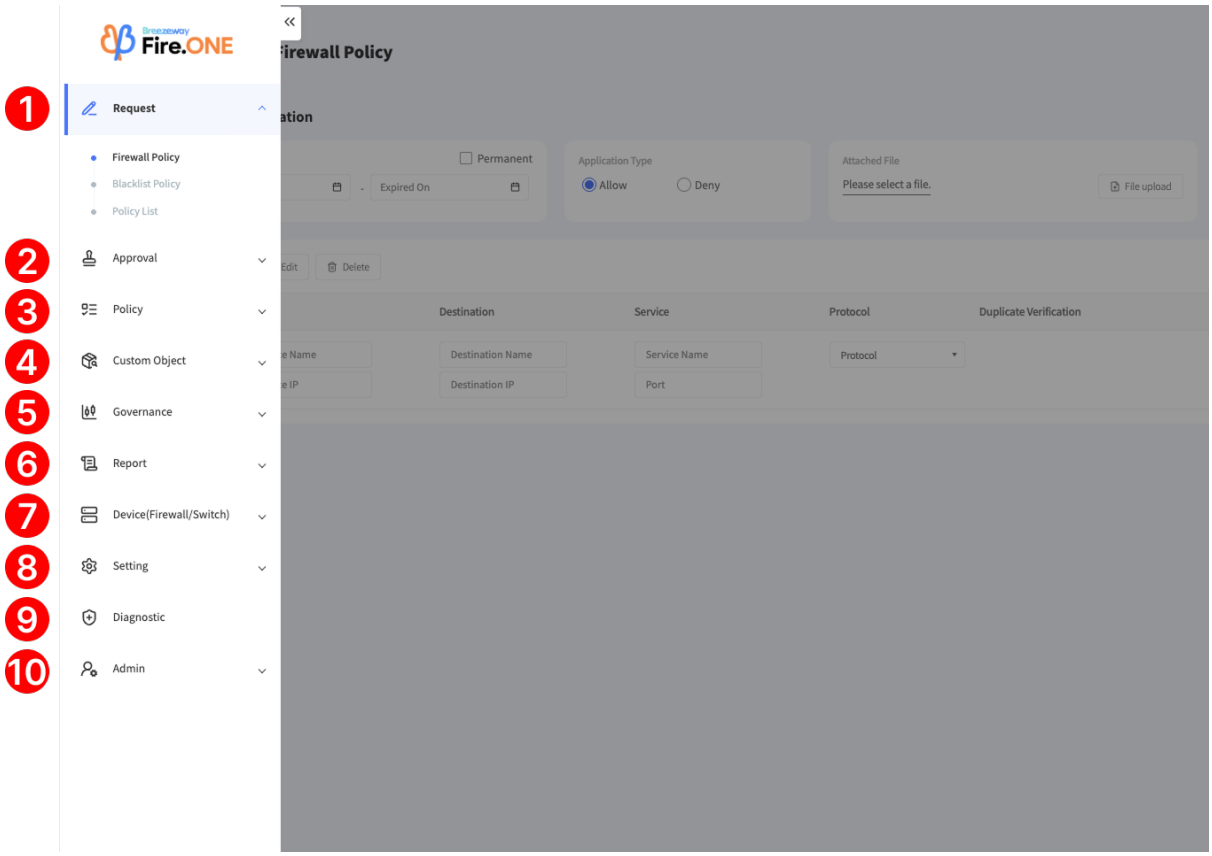
Fire.ONE provides Light Mode by default, and users can switch to Dark Mode for convenience. Each mode automatically adjusts background and text colors to optimize visibility and readability, ensuring a



〈Dark Mode Switch Screen〉

1) Click the button in the bottom left corner
2) Clicking this button immediately switches to Dark Mode.
3) Clicking the button again returns to Light Mode.

### 2.9.4 Feature Menu



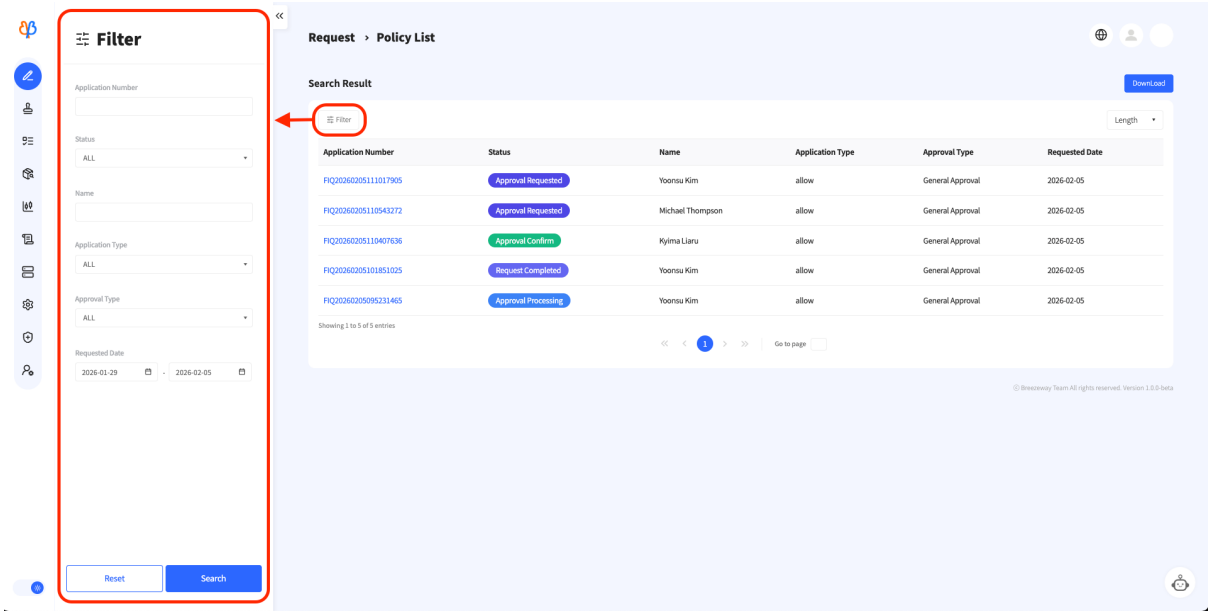

〈Feature Description Screen〉

1) Request: Submit firewall policy requests and support efficient policy input through pre-validation, object selection, Excel uploads, etc.
2) Approval: Process approvals/rejections for submitted policies by approver, co-approver, and referrer, and review approval history.
3) Policy Status: View submitted and approved firewall policies. Apply (Commit) or reject (Dismiss) policies separately for each firewall.
4) Custom Object: Custom Objects allow administrators to save frequently used IP and service information by name.
   It provides a user-friendly feature allowing users to quickly and accurately select saved objects during policy registration instead of manual input.

5) The generated custom objects can be used by clicking the Object Search button on the Application > Firewall Policy screen and then looking them up in the pop-up window.
   Ex) If the project development team pre-creates essential application objects containing the target IPs and service information required for the project, operational staff can easily and securely apply by searching for the object name.
6) Governance: Integrates management of firewall structure and policy risks, including network topology visualization, risk analysis, and compliance policy verification.
7) Report: Queries currently applied firewall policies and provides visualized diagnostic reports.
8) Device: A management menu that allows you to view basic information, rules, objects, and more for registered firewall devices.
9) Settings: View Fire.ONE web environment configuration items such as allowed IPs, departments, menus, and API lists with administrator privileges.
10) Diagnostic Dashboard: Provides a unified security status diagnosis through log and rule-based traffic analysis, policy evaluation, anomaly detection, and threat intelligence.
11) Administrator (Admin): Includes administrator-only functions such as firewall management settings by user/permission/organization, user activity logs, and application status checks.

### 2.9.5 Filter

Search filters help you quickly retrieve data matching desired conditions from the firewall policy request list.




〈Policy List Search Filter〉

1) Open Filter Panel: Click the [Filter] button in the top-left corner of the screen to expand the filter input window on the left.
2) Enter search criteria: Select and enter the following conditions in the expanded filter window.
3) Applicant name, policy status (e.g., Request, Apply, etc.), service name, request date range, other conditions
4) Execute Search: After entering conditions, click the [Search] button at the bottom. The list on the right will automatically filter according to those conditions.
5) Reset: To clear all search conditions, click the [Reset] button to remove all input values at once.

## 2.10 Troubleshooting

### 2.10.1 Fault Isolation

- Each service module (Application, Payment, Apply, etc.) is designed independently to prevent errors in one module from affecting others.
- **Current Scope:** Maintains service isolation levels through modular design.

### 2.10.2 Logging and Monitoring

- Records service operations and errors to enable rapid root cause analysis when issues occur

- **Current scope:** Module-specific logging (SLF4J / Logback)
- Server console, log files, default log level configuration

### 2.10.3 Error Page Provision

- Provides users with detailed error guidance
- **Current scope:** Spring Security default error page provided
- **Example:** Default pages for 404, 500 errors

### 2.10.4 Version rollback

- If issues are discovered after deployment, recovery to a previous stable version is possible
- **Current scope:** Manual rollback (based on Git tags)
- Previous version Git checkout → Server redeployment

### 2.10.5 Session Persistence

- Shares session information across servers to maintain user sessions even during failures
- **Current scope:** Only partially implemented (DB or file-based session storage)

## 2.11 User Permissions and Account Types

The Fire.ONE system utilizes two management menus to flexibly apply user permissions and account types.

1) **Administrator > Menu Access Group Menu**: Groups that manage which menus users can access. The minimum required Default Admin group and Default User group are provided for operation and cannot be deleted. Additional groups can be created and used according to the customer's environment.
2) **Page Management Group Menu**: Groups that manage permissions for specific actions (e.g., create, edit, delete) within particular pages. The Basic Supervisor group and Basic User group are provided and cannot be deleted. Additional groups can be created and used according to the customer's environment.

These two group settings enable efficient application of various permissions and account types across the entire system.

### 2.11.1 Account Types

| Account Type | Description | Primary Functions |
|---|---|---|
| **Admin (Administrator)** | Highest-level administrator managing the entire system | - Create and delete user accounts<br>- Set permissions and approve requests<br>- Review and approve request history<br>- Modify system settings |
| **Approver (Approver)** | Responsible for approving or rejecting requested firewall policies, etc. | - Review and approve requests<br>- Add comments and change status |
| **User (General User)** | General user performing routine tasks like policy requests | - Firewall policy requests<br>- View request history<br>- View request history |
| **Auditor (Optional)** | Account dedicated to log viewing and activity monitoring (Read-only) | - View Approval/Request History<br>- Verify system logs |

### 2.11.2 Permission Scope

| Function Item | Admin | Approver | User | Auditor |
|---|---|---|---|---|
| **User Management (Administrator)** | ✓ | ✖ | ✖ | ✖ |
| **Policy Request (Application)** | ✓ | ✖ | ✓ | ✖ |
| **Request Approval/Rejection (Approval)** | ✓ | ✓ | ✖ | ✖ |
| **System Settings Change (Settings)** | ✓ | ✖ | ✖ | ✖ |

| | | | | |
|---|---|---|---|---|
| View Request History (Policy) | ✓ | ✓ | ✓ | ✓ |
| Audit Log Access | ✓ | ✖ | ✖ | ✓ |

# 3. Installation Guide

## 3.1 Installation

### 3.1.1 Server Installation

**Ubuntu Server Deployment and Project Execution**

1) Install Ubuntu Server (Ubuntu CLI)

Set Ubuntu time zone

- Check Current Time
  - Check using the `timedatectl` command
- Set the server time to Korean Standard Time
  - $ sudo timedatectl set-timezone Asia/Seoul.
- Configure server time to synchronize with Internet standard time (NTP)
  - $ sudo timedatectl set-ntp true

2) Install Java

- Create a folder to install Java
  $ mkdir -p /usr/local/openjdk
- Change the current working directory to the created folder
  $ cd /usr/local/openjdk
- Moving Java source files to the server
  $ scp openjdk-23.0.2_linux-x64_bin.tar root@[server IP address]:/usr/local/openjdk
- Extract the archive
  - $ tar -xvf /usr/local/openjdk/openjdk-23.0.2_linux-x64_bin.tar -C /usr/local/openjdk

3) Install and connect to PostgreSQL (Example: Version 15)

- 3-1) Install required tools
  $ sudo apt install curl ca-certificates

- 3-2) Create PostgreSQL APT key storage location
  $ sudo install -d /usr/share/postgresql-common/pgdg

- 3-3) Download the PostgreSQL Official Signing Key
  $ sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc ₩
  $ --fail https://www.postgresql.org/media/keys/ACCC4CF8.asc

- 3-4) Set the distribution codename as an environment variable (noble for Ubuntu 24.04)
  $. /etc/os-release

- 3-5) Add PostgreSQL APT repository (noble-pgdg)
  $ sudo sh -c "echo 'deb [signed-by=/usr/share/postgresql-common/pgdg/apt.postgresql.org.asc] ₩
  https://apt.postgresql.org/pub/repos/apt${VERSION_CODENAME}-pgdg main' ₩
  > /etc/apt/sources.list.d/pgdg.list"

- 3-6) Update package list
  $ sudo apt update
- 3-7) Install PostgreSQL 15

$ sudo apt install postgresql-15

- 3-8) Start
  $ sudo systemctl enable postgresql
  $ sudo systemctl status postgresql

4) Granting Database Access Permissions

- $ sudo vi /etc/postgresql/15/main/pg_hba.conf
- Open the PostgreSQL configuration file
  $ Locate the following section in the /etc/postgresql/15/main/pg_hba.conf file

```
# ================================
# "local" is for Unix domain socket connections only
local   all                 postgres peer
# ================================
# Modify as follows
# ================================
# "local" is for Unix domain socket connections only
# local   all                 postgres peer
local   all                 postgres md5
# ================================
```

  - Save with Vi editor and reboot the server
    $ sudo systemctl restart postgresql

5) Verify normal DB connection

- $ sudo psql -U postgres

6) Modify deployed service file

- $ sudo vi /etc/systemd/system/Fire.ONE.service

[Unit]
Description=Fire.ONE Service
After=network.target
StartLimitBurst=5
StartLimitBurst=5
[Service]
Type=simple
Environment="KEYSTORE_PASSWORD=[password]" # Add if environment variables are needed (e.g., SSL password)
# EnvironmentFile=/etc/default/myapp # myapp is the environment file
WorkingDirectory=/FIRE.ONE-API
ExecStart=/FIRE.ONE-APIi/argos_run.sh
Restart=on-failure
[Install]
WantedBy=multi-user.target

### 7) Granting Permissions

- Grant permissions to execute Argos_run.sh
  $ sudo chmod +x /FIRE.ONE-API/argos_run.sh

### 8) Service Registration and Execution

- $ sudo systemctl daemon-reload
- $ sudo systemctl enable Fire.ONE.service
- $ sudo systemctl start Fire.ONE.service
- $ sudo systemctl status Fire.ONE.service

Verify 5 services are running normally using `ps -ef | grep SNAPSHOT*`

```
[root@localhost ~]# ps -ef | grep SNAPSHOT*
root      590745       1  0 Oct24 ?        00:23:10 /usr/local/openjdk/jdk-23/bin/java -jar argos-common-0.0.1-SNAPSHOT.jar
root      590811       1  0 Oct24 ?        00:26:02 /usr/local/openjdk/jdk-23/bin/java -jar argos-approval-0.0.1-SNAPSHOT.jar
root      590886       1  0 Oct24 ?        00:26:13 /usr/local/openjdk/jdk-23/bin/java -jar argos-push-0.0.1-SNAPSHOT.jar
root      590939       1  0 Oct24 ?        00:29:18 /usr/local/openjdk/jdk-23/bin/java -jar argos-web-0.0.1-SNAPSHOT.war
root     1593766       1  0 Sep18 ?        00:54:41 /usr/local/openjdk/jdk-23/bin/java -jar /FIREONE-API/argos-policy-0.0.1-SNAPSHOT.jar
root     2904176 2904142  0 19:19 pts/0    00:00:00 grep --color=auto SNAPSHOT*
```

### 9) Diagnostic Installation and Configuration Example

- Elasticsearch configuration file
  - elastic.yml
    cluster.name: elk-cluster
    node.name: node-1
    discovery.type: single-node
    path.data: /home/ssnc/elk/elasticsearch-9.1.1/data

path.logs: /home/ssnc/elk/elasticsearch-9.1.1/logs
network.host: 0.0.0.0
http.port: 9200
discovery.seed.hosts: ["192.168.7.60"]
xpack.security.enabled: true
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.keystore.path:/home/ssnc/elk/elasticsearch-9.1.1/config/certs/http.p12
xpack.security.http.ssl.keystore.password: ""
xpack.security.http.ssl.truststore.path:/home/ssnc/elk/elasticsearch-9.1.1/config/certs/http.p12
xpack.security.http.ssl.truststore.password: ""
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.keystore.path:/home/ssnc/elk/elasticsearch-9.1.1/config/certs/transport.p12
xpack.security.transport.ssl.keystore.password: ""
xpack.security.transport.ssl.truststore.path:/home/ssnc/elk/elasticsearch-9.1.1/config/certs/transport.p12
xpack.security.transport.ssl.truststore.password: ""

- Generate Elastic internal authentication files
  - Create http_ca.p12
    /home/ssnc/elk/elasticsearch-9.1.1/bin/elasticsearch-certutil ca --silent --pass "" -out /home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.p12
  - Generate http.p12
    /home/ssnc/elk/elasticsearch-9.1.1/bin/elasticsearch-certutil cert --silent --ca /home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.p12 --ca-pass "" --name es-http --ip 127.0.0.1 --ip 192.168.7.60 --dns localhost --dns 192.168.1.249 --pass "" -out /home/ssnc/elk/elasticsearch-9.1.1/config/certs/http.p12
  - Generate transport.p12
    /home/ssnc/elk/elasticsearch-9.1.1/bin/elasticsearch-certutil cert --silent --ca /home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.p12 --ca-pass "" --name es-transport --ip 127.0.0.1 --ip 192.168.7.60 --dns localhost --dns 192.168.1.249 --pass "" -out /home/ssnc/elk/elasticsearch-9.1.1/config/certs/transport.p12
  - Generate crt file

openssl pkcs12 -in /home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.p12 -clcerts -nokeys -passin pass: -out /home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.crt

- Run Elasticsearch
  (Proceed to the next step if no errors occur)
  - Set Elastic account password
    /home/ssnc/elk/elasticsearch-9.1.1/bin/elasticsearch-setup-passwords interactive

- For Kibana configuration
  - Generate service token
    /home/ssnc/elk/elasticsearch-9.1.1/bin/elasticsearch-service-tokens create elastic/kibana kibana-token
  - Note: The generated key is one-time use only
    Ex:
    (AAEAAWVsYXN0aWMva2liYW5hL2tpYmFuYS10b2tlbjpfb05WQXdQQVJWS2I3MklNUXI1MDhB)
  - kibana.yml
    server.port: 5601
    server.host: 192.168.7.60
    server.ssl.enabled: false
    elasticsearch.hosts: ["https://192.168.7.60:9200"]
    elasticsearch.serviceAccountToken: "The token value from above"
    elasticsearch.ssl.certificateAuthorities:[“/home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.crt”]
    xpack.encryptedSavedObjects.encryptionKey: "1wAQSW+xKyxN5cFNrPirGoE9/RzHyPQLQUwwp9SlfUA="

- Install Fleet Server (Use the actual token value displayed in the Kibana UI)
  sudo ./elastic-agent install ₩
  --fleet-server-es=https://192.168.7.60:9200 ₩
  --fleet-server-service-token=AAEAAWVsYXN0aWMvZmxlZXQtc2VydmVyL3Rva2VuLTE3NjEyOTI5MzYwMzQ6M0w3MUtfNFZSc210QTBQbmwzOGx2dw ₩
  --fleet-server-policy=fleet-server-policy ₩
  --fleet-server-port=8220 ₩
  --install-servers ₩

--fleet-server-es-ca=/home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.crt

- Issuing Tokens for Fleet Server
  sudo /home/ssnc/elk/elasticsearch-9.1.1/bin/elasticsearch-service-tokens ₩
  create elastic/fleet-server fleet-srv-token
  Remember or save the token value printed once, as it will be used below
  sudo /home/ssnc/elk/elastic-agent-9.1.1-linux-x86_64/elastic-agent install --fleet-server-es=https://192.168.60.207:9200 --fleet-server-service-token="fleet-server service token value" --fleet-server-policy=fleet-server-policy --fleet-server-port=8220 --fleet-server-es-ca=/home/ssnc/elk/elasticsearch-9.1.1/config/certs/http_ca.crt --install-servers

- Elastic Agent Installation (Windows)

### 3.1.2 Firewall Integration

- List of currently supported firewall vendors
  - AhnLab
  - AxGate
  - CheckPoint
  - Fortinet
  - Juniper
  - Palo Alto
  - Secui (Bluemax)

Below are the settings that must be configured on the firewall side to integrate the firewall with Fire.ONE.

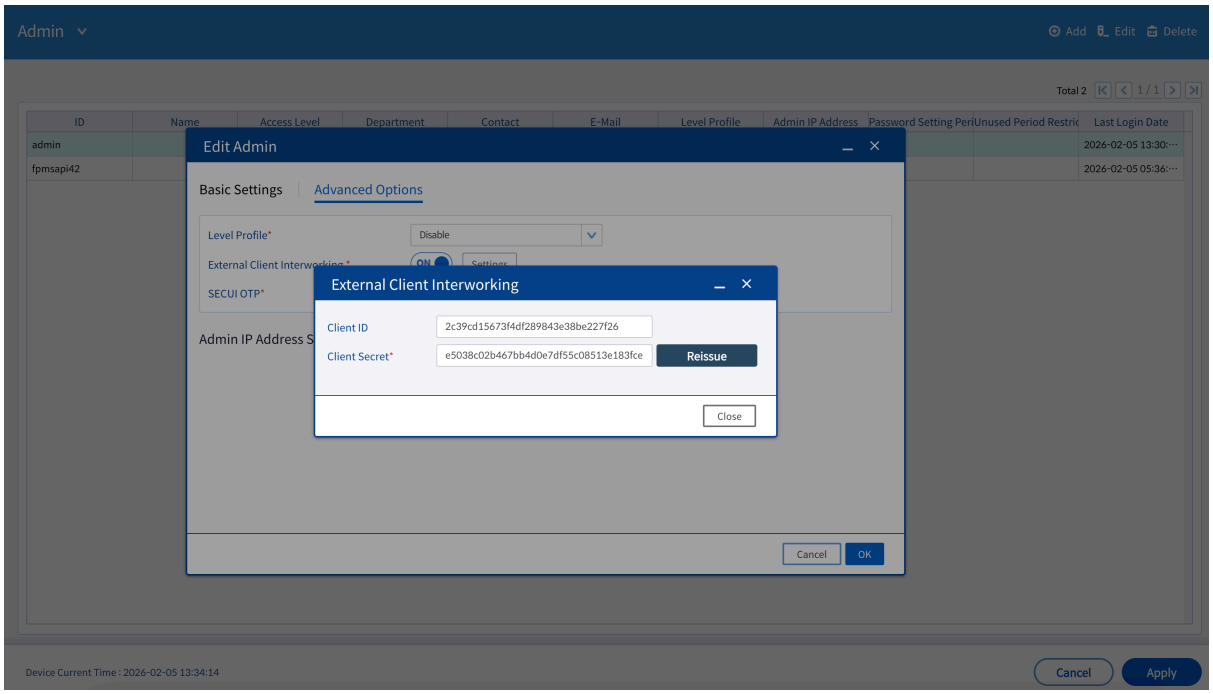
- The screenshots below are from each vendor's firewall GUI, not Fire.ONE's interface.
- Basic integrable features: Firewall API, Syslog

**Secui_blueMax Integration Method**

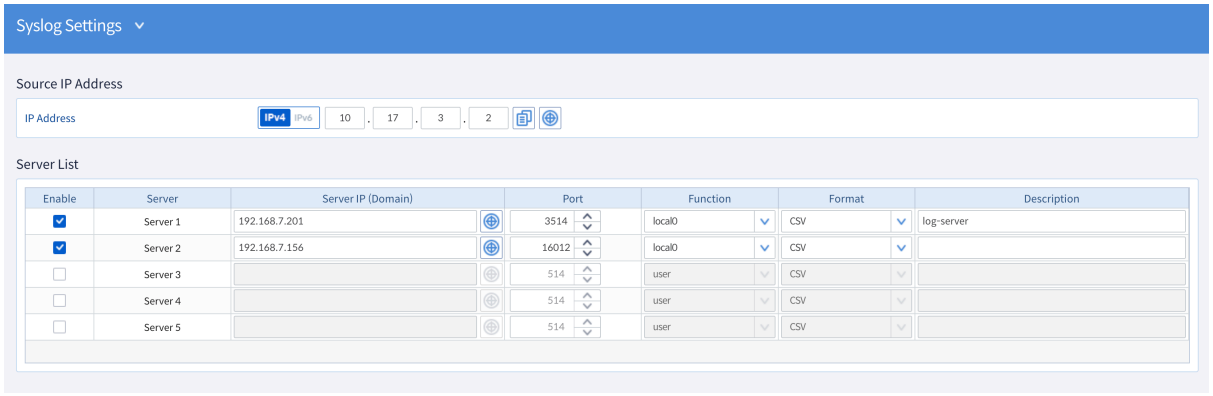
Login > System > Admin Settings > Admin

Click the ID of the logged-in account to pop up the administrator edit screen

Navigate to the Advanced Settings tab and click the External Client Integration Settings button




System > Integration Server > Syslog Settings

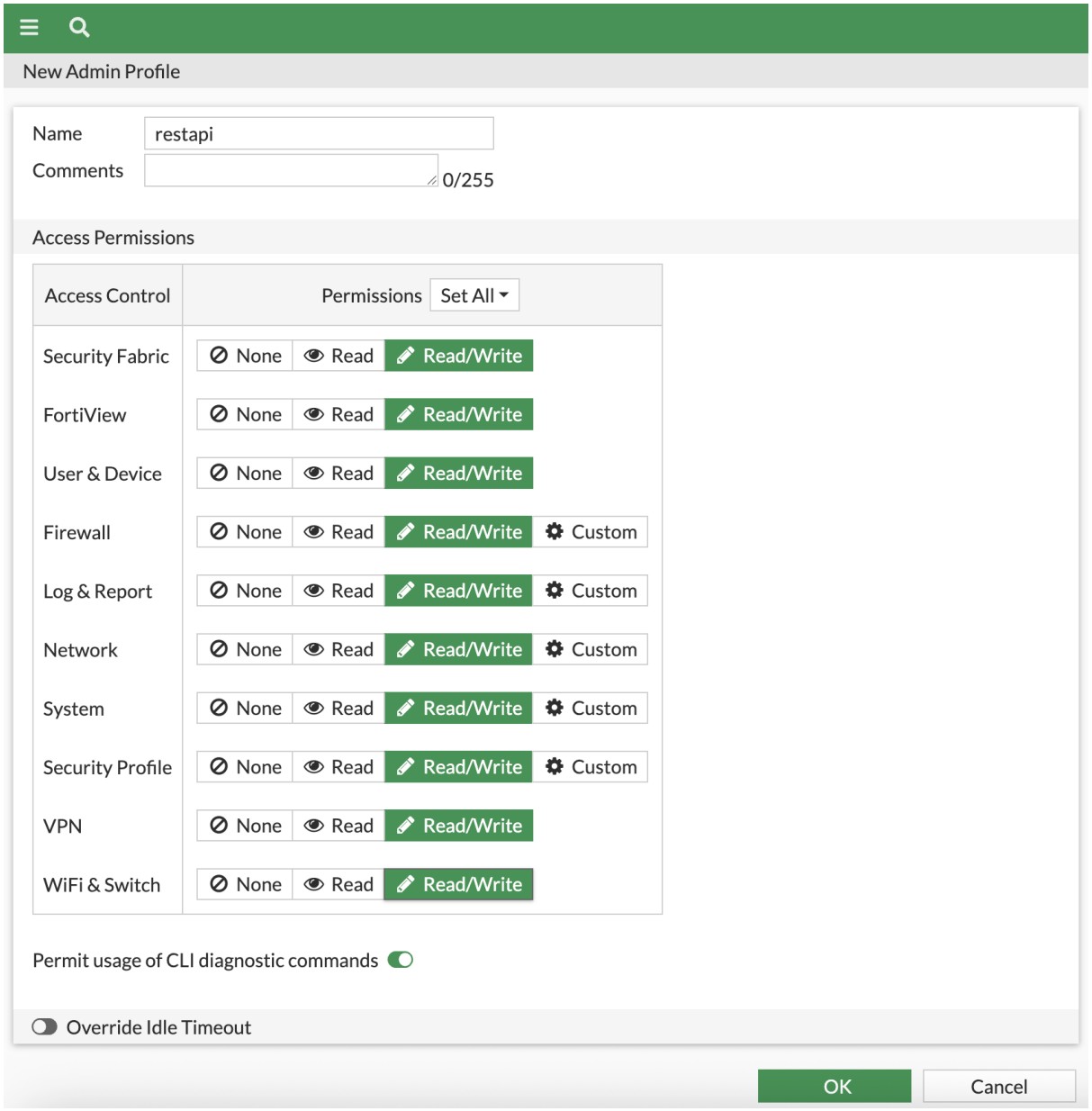



Configure as shown below and apply

- Sender IP Address: Firewall Management IP
- Server List: Enter the destination server IP and port
- Configure other settings as needed

### Forinet Integration Method

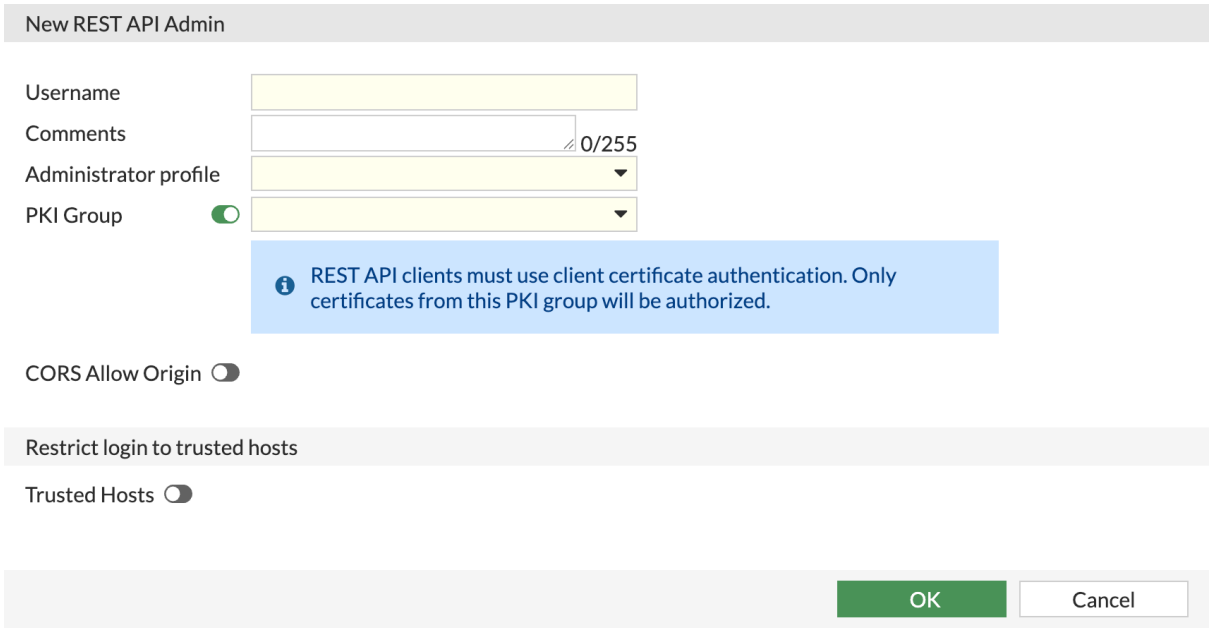
System > Administrator Profile > Create New




Configure as shown below and approve

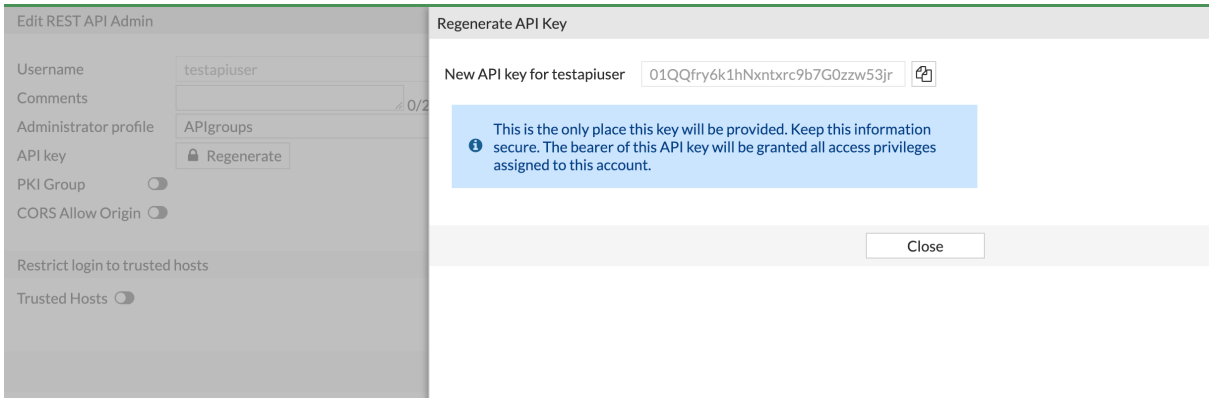
- Name: (Enter desired name)
- Access Permissions: Set All Permissions > Read/Write
- Configure other settings as needed

System > Administrators > Create New > REST API Administrator




Configure as follows and approve

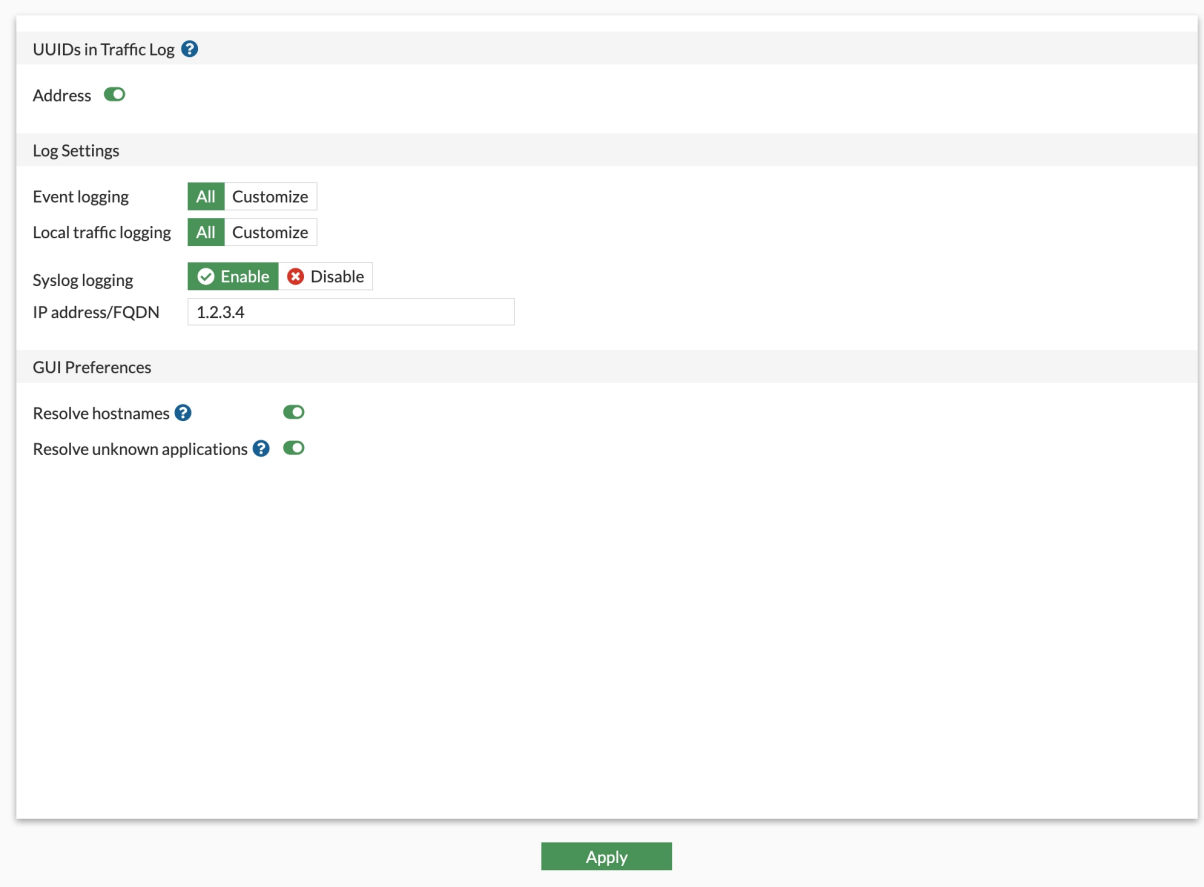
- Name: (Desired name)
- Administrator Profile: Specify the profile created above
- PKI Group: Disable
- Configure other settings as needed




Copy and record the API key displayed after approval

- This key is required for REST API integration
- Reissuance is required if lost or if DB information corruption makes recovery impossible

Log & Reports > Log Settings




Configure as follows and apply

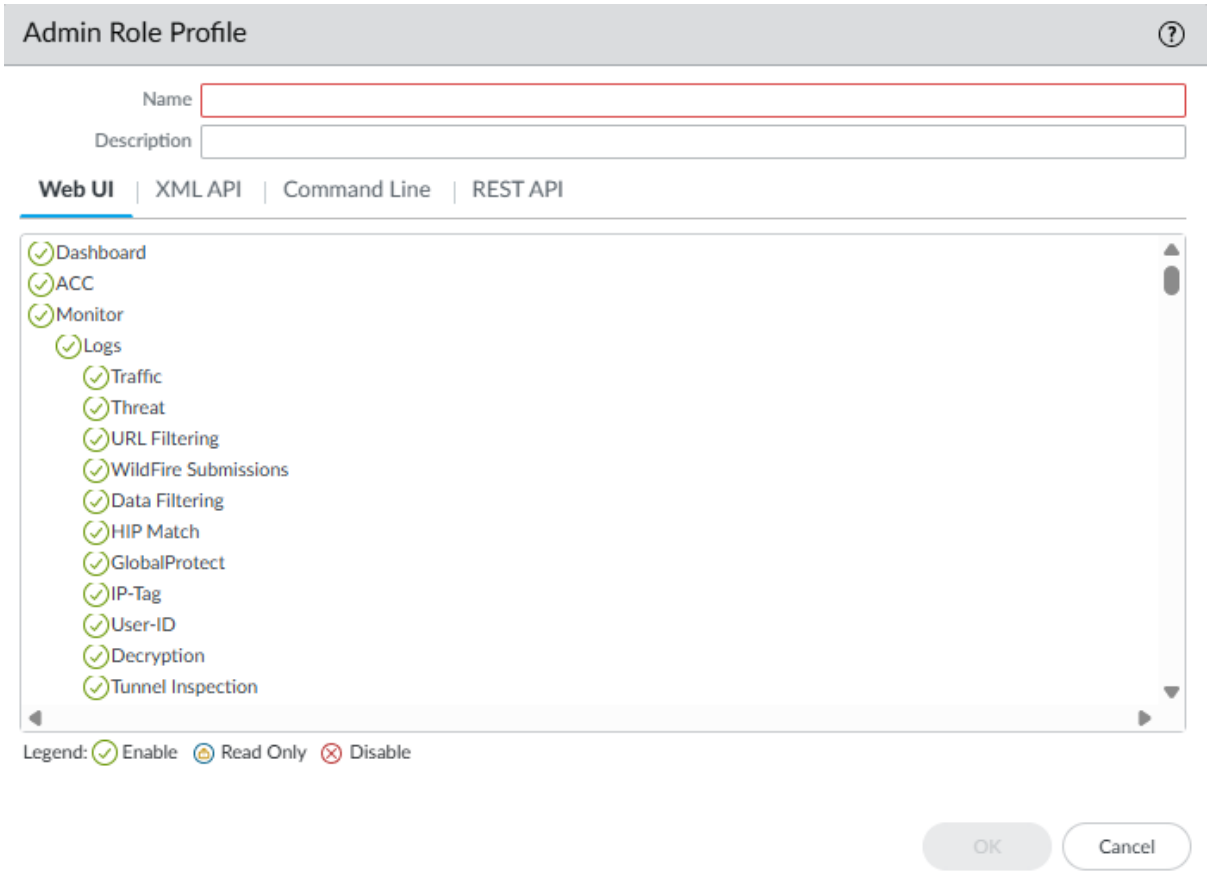
- Syslog logging: Enabled
- IP address/FQDN: Enter the IP address/domain of the syslog server
- Configure other settings as needed

Must change the Syslog format to CSV via CLI access

- config global
- config log syslogd setting
- set format csv
- show full-configuration (verify application)

### Palo Alto Integration Method

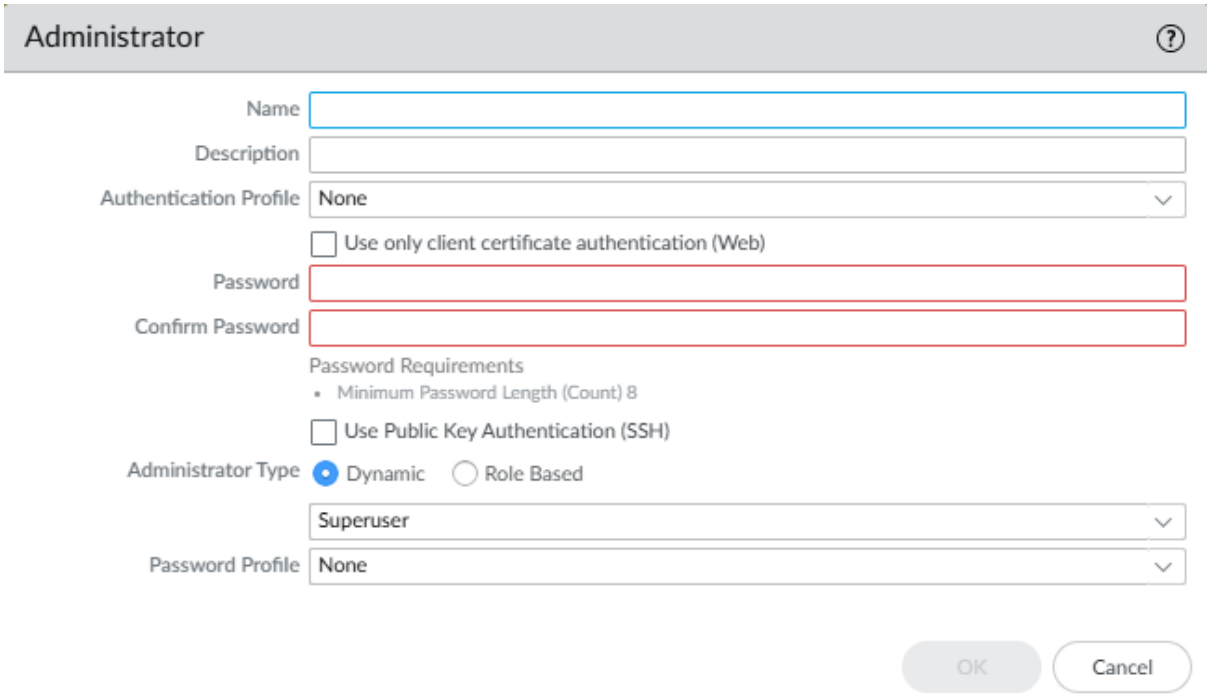
Device > Admin Roles > Add




Configure as shown below and click OK

- Web UI, XML API, REST API: Set all to Enabled
- Configure others as needed

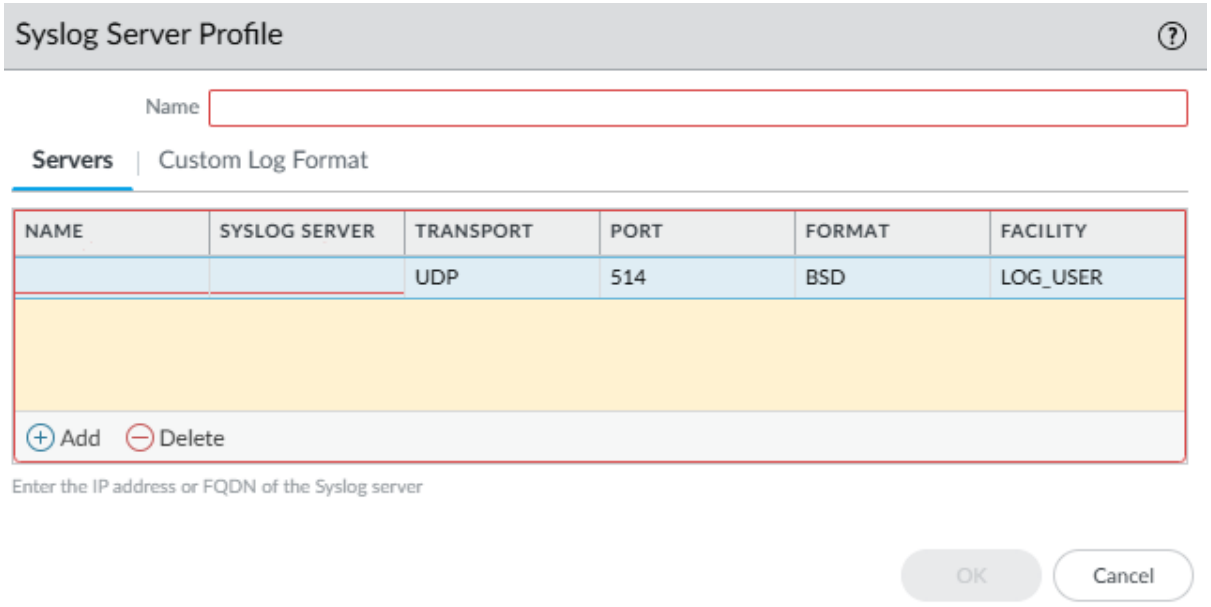
Device > Administrators > Add




Configure as shown below and click OK

- Name: (Desired name)
- Password: (Desired password)
- Confirm Password: (Same password as above)
- Administrator Type: Select Role Based, then assign the profile created earlier
- Configure other settings as needed

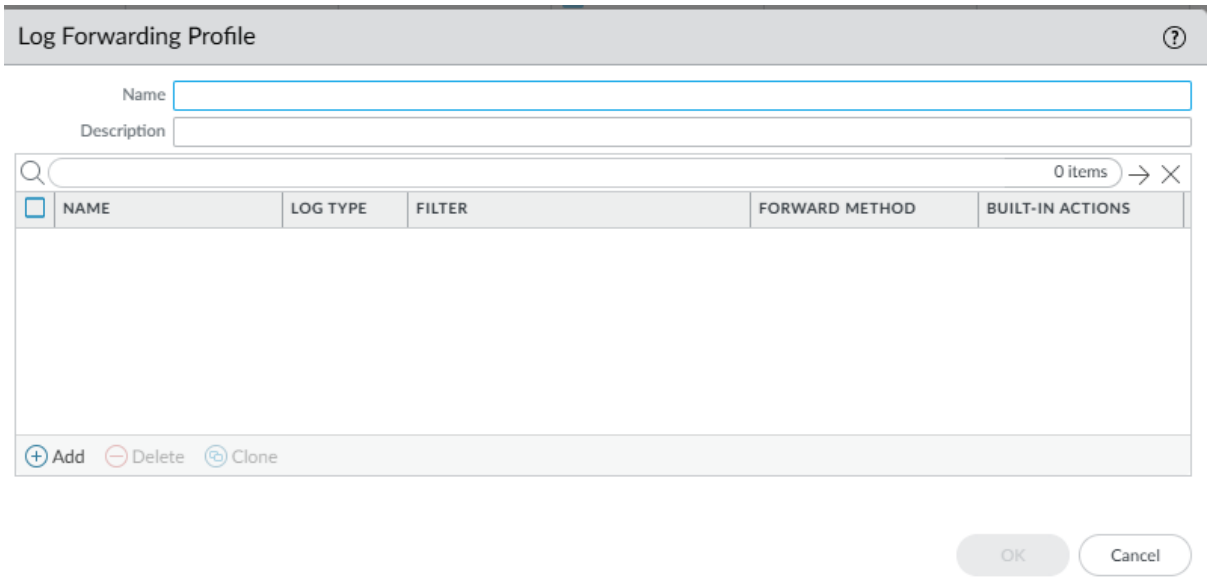
Device > Server Profiles > Syslog > Add




Configure as shown below and click OK

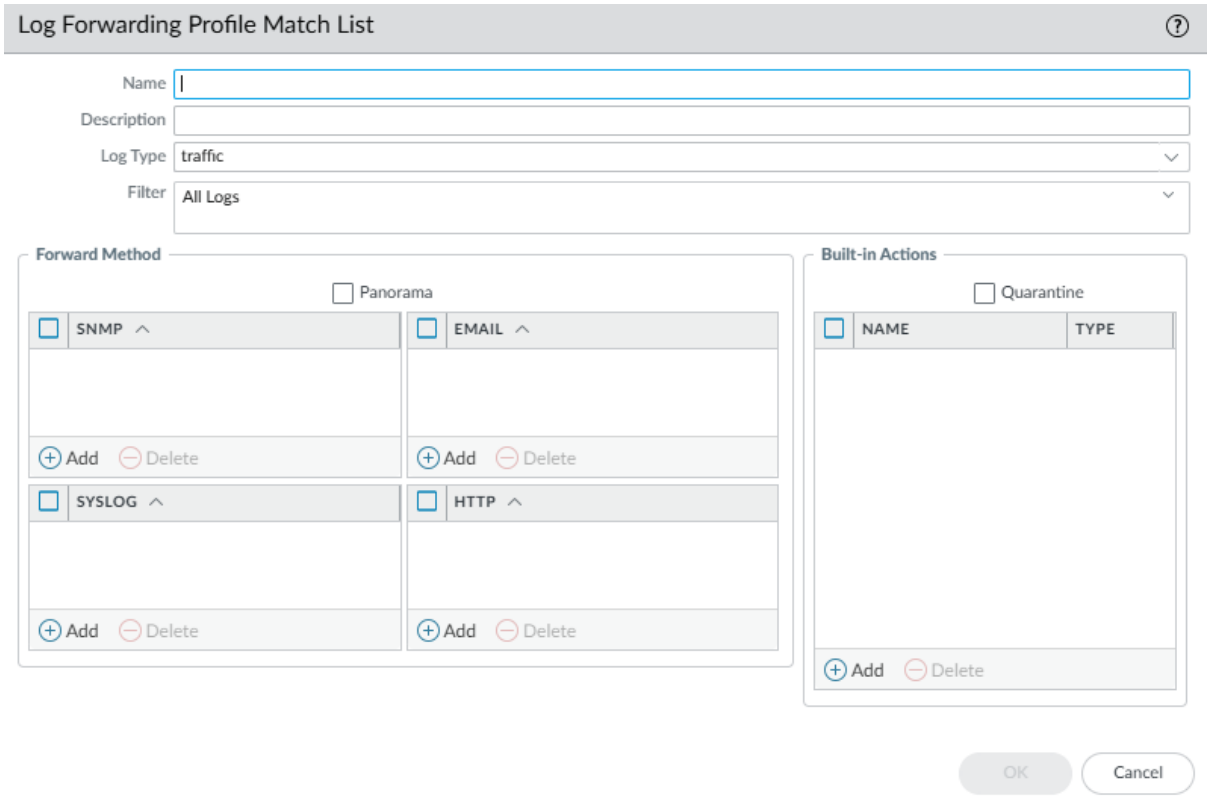
- Name: (Desired name)
- Servers: Enter Name (desired name), Syslog Server (log server address)
- Configure the rest as needed

Objects > Log Forwarding > Add




Configure as follows and click OK

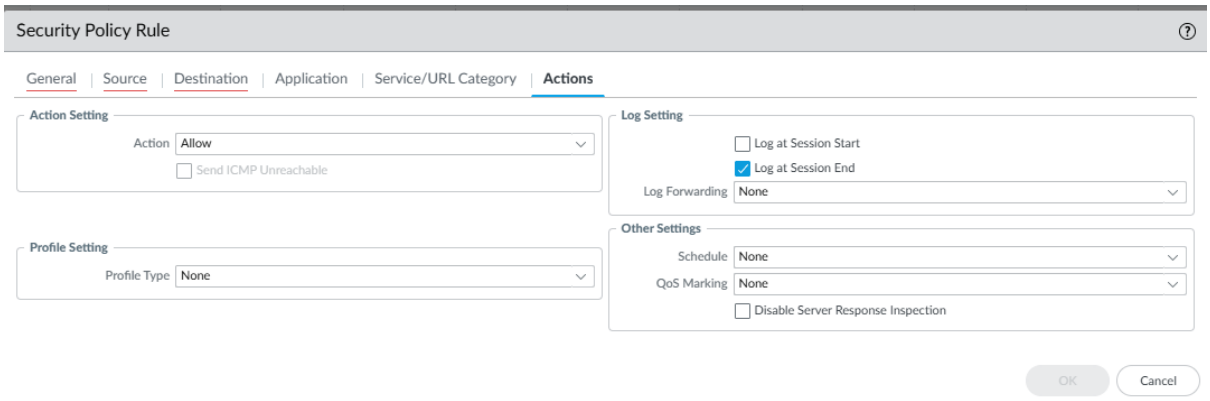
- Name: Desired name
- Click Add




Configure as shown below and click OK

- Name: (Desired name)
- Syslog > Click Add, register the Syslog Server Profile created above
- Configure other settings as needed

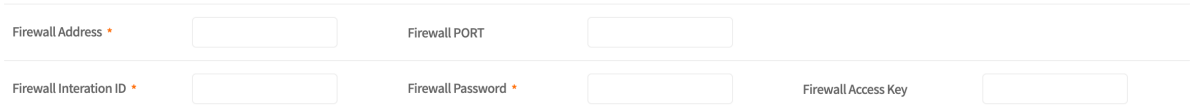
Policies > Add




Configure as follows and click OK

- General, Source, Destination: Enter required values
- Actions:
  - Log Setting > Log Forwarding, specify the Log Forwarding Profile registered above
- Configure other settings as needed

* Palo Alto requires clicking Commit in the upper-right corner after completing all settings to apply changes.




After logging into the Fire.ONE system, click the Create button under Device > Firewall List and enter the Firewall Integration ID and Firewall Password.

### 3.1.3 Personnel Information Integration

This system integrates customer HR information to manage user and department details in real-time.

**Integration Overview and Technical Support**

Fire.ONE utilizes the customer's HR integration data to create logins and approval lines without requiring a separate user registration process.

Technical Support Need: Personnel information integration requires engineer technical support based on the customer's integration method (data format, delivery method, etc.).

### HR Integration Process

HR information integration proceeds through the following steps, with table synchronization automated via functions in the PostgreSQL environment.

| Step | Description | Tables Used |
|---|---|---|
| Step 1: Temporary Data Loading | Data is analyzed based on the client's HR information provision method (file, DB, etc.) and ultimately loaded into a temporary table. | CO_USER_TEMP (User Information) CO_DEPT_TEMP (Department Information) |
| Step 2: Synchronize Main Tables | Using PostgreSQL functions, we compare the data in the temporary tables with the existing data in the main tables. | CO_USER (Final User Information) CO_DEPT (Final Department Information) |
| Step 3: Data Update | Based on the comparison results, new data is inserted using INSERT, and modified data is updated using UPDATE to maintain the latest state of the main table. | |

### Synchronization Cycle and Batch Settings

- **Synchronization Frequency:** HR synchronization runs **once daily** by default.
- **Execution Time:** The execution time is determined in consultation with the client, considering system load, and the batch program is configured to run at that scheduled time.

**Example)**

```
@Scheduled(cron="0 0 7 * * ?") // 매일 7시에 실행
@RequestMapping(value="/insaSync", method={RequestMethod.POST, RequestMethod.GET})
public ResponseEntity<String>  insaSync() throws Exception {
    logger.debug("START INSASYNC");
    int i  = insaServiceImpl.insaSyncFromNACtoSSTOPC();
    return ResponseEntity.ok().body("FINISHED");
}
```

# 4. Customer Support

Issues are received through issue reports submitted by users or the client company.

1) **Issue Reporting**: Users or the client company report issues to the help desk.
2) Help Desk:

- **Receipt and Initial Handling**: Receives the incident, reviews the analysis results, and performs **initial** handling for resolution and inquiries.
- **Issue Escalation**: Issues exceeding the scope of initial handling are escalated to the **maintenance** organization.

3) Maintenance Organization:

- **Issue Resolution and Verification**: Resolves transferred issues, verifies results, and performs **monitoring and emergency** support **for the affected systems**.
- **Transfer to Help Desk**: After resolution, transfer the outcome back to the Help Desk.

## 4.1 Help Desk Operation Plan

| | |
|---|---|
| Working Hours | Weekdays: Operates from 09:00 to 18:00.<br>Saturdays, Nights, and Holidays: Operates via an emergency contact system.<br>(For emergencies, we'll set up another point of contact.) |
| Submission Methods | Phone (02-6925-2550) and emergency contact network.<br>Email: rnd@ssnc.co.kr |
| Services Provided | * Initial Support: Receives and analyzes equipment failures, performs initial handling for simple failures and inquiries.<br>* Fault Escalation: Escalate faults to the responsible maintenance organization and confirm the resolution status.<br>* Reporting: Report situations to the project manager during emergency situations.<br>* Monthly Reporting: Compile and report monthly fault resolution results. |

# 5. Maintenance

## 5.1 Maintenance Support Items

| | |
|---|---|
| Defect Repair | ● Improvement or modification work when functional defects occur<br>● Support provided after mutual agreement between the client and the proposing company for damage caused by user negligence or natural disasters |
| Version Upgrades | ● Patch and update support<br>● Minor version upgrade support |
| Technical Support | ● Q&A via phone/email, online support, etc.<br>● Rapid troubleshooting support during system failures<br>● Submission of incident resolution reports<br>● Regular inspections for fault prevention |
| Training Support | ● Evaluation of operational status, identification of operational issues, and proposal of improvement plans<br>● Technical and training support to resolve issues |

## 5.2 Maintenance Period

- Basic Contract Period: **12 months (1 year)**
- Extension Option: **Renewal in 1-year increments** or long-term contracts possible based on project conditions
- Emergency Contact System: **365-day emergency response capability** during the contract period

## 5.3 Maintenance Costs

- Regular Maintenance Costs (Monthly/Annual Basis)
  - Calculated based on system scale, number of devices, and service complexity

- Maintenance Rate: 15% of supply amount (separate pricing applies after 3-year hardware warranty)

- Additional Development or Feature Enhancement Requests
  - Separate quotation provided (additional work outside maintenance scope)

※ Actual amounts are determined based on consultation or detailed calculation criteria within the proposal.

## 5.4 Maintenance Method

- First-Level Support - Help Desk (Phone/Remote)
  a. Receive and immediately analyze issues
  b. Handling simple issues and inquiries
- Secondary Support - Technical Engineer
  a. System failure root cause analysis
  b. Implementation of patches, service restart, configuration changes, and other specialized actions
- Tier 3 Support - Developer/Specialized Technical Team
  a. Complex Issues, Structural Problems, and Software Error Resolution
  b. Providing development fixes and patches when necessary
- On-site support
  a. Engineer dispatch to the site when issues cannot be resolved remotely
- Remote Monitoring
  a. Implementation of a monitoring system for real-time status checks when required

# 6. Appendix

## 6.1 Detailed Code for Password Hash Algorithm

### 6.1.1 Basic Hash Operation Logic

```
public String sha256Hex(String input) {  1 usage   KyimaLiaru
    try {
        MessageDigest digest = MessageDigest.getInstance( algorithm: "SHA-256");
        byte[] hashBytes = digest.digest(input.getBytes(StandardCharsets.UTF_8));
        return bytesToHex(hashBytes);
    } catch (NoSuchAlgorithmException e) {
        throw new IllegalStateException("SHA-256 Algorithm not available", e);
    }
}

private String bytesToHex(byte[] bytes) {  1 usage   KyimaLiaru
    StringBuilder sb = new StringBuilder( capacity: bytes.length * 2);
    for (byte b : bytes) {
        sb.append(String.format("%02x", b)); // 항상 2자리 16진수
    }
    return sb.toString();
}
```

### 6.1.2 Salt and Nonce Generation Logic

```
@Override  1 usage   KyimaLiaru *
public SaltVo generateRandomKey(SaltVo saltVo) {
    // 랜덤 nonce 생성
    byte[] bytes = new byte[16];
    secureRandom.nextBytes(bytes);
    String randomKey = Base64.getUrlEncoder().withoutPadding().encodeToString(bytes);
    saltVo.setNonce(randomKey);

    // nonce 저장 및 해당 유저의 salt 불러오기
    saltVo.setSalt(loginDao.setRandomKey(saltVo));

    // nonce 와 salt 리턴
    return saltVo;
}
```

### 6.1.3 When setting a password for the first time or changing/resetting it: sha256(salt + password)

Client:

```
$.ajax({
    type: 'POST',
    url: contextPath + '/getRandomKey',
    contentType: 'application/json',
    data: JSON.stringify( value: {"empno":empnoInput}),
    success: async function (response) {
        const data : {empno: string, password: any}  = {
            "empno": empnoInput,
            "password": await sha256(response.salt + newPassword.val())
        };
```

1. Client requests the user's unique salt value from the server
2. Server transmits the corresponding user's salt
3. Client generates a hash value using the SHA256 algorithm with the password and sends it to the server
4. The received hash value is stored on the server

### 6.1.4 When logging in

Client:

```
$.ajax({
    type: 'POST',
    url: contextPath + '/getRandomKey',
    contentType: 'application/json',
    data: JSON.stringify( value: {"empno":$('#username').val()}),
    success: async function (response) {
        const password = $('#password');
        const salted = await sha256(response.salt + password.val());
        const hashed = await sha256(salted + response.nonce);
```

Server:

```
// SHA256(Salt + Pw) 와 nonce 를 합친 문자열의 SHA256 생성 및 비교
SaltVo saltVo = loginDao.getRandomKey(userVo);
String hashed = hashUtil.sha256Hex( input: saltVo.getPassword() + saltVo.getNonce());

UserVo result = loginDao.findUserById(userVo);

// 위에서 계산한 HASH와 클라이언트 비밀번호 비교; 틀리면 기존처럼 return null, 같으면 진행.
if (!userVo.getPassword().equals(hashed)) {
    return null;
}
```

1. Client requests the server for the user's unique salt value and a random nonce
2. Server generates the user's salt value and a nonce that changes with each request (see Appendix 6.1.2), then sends it to the client
3. Generate a hash value using the SHA-256 algorithm with the password
4. Generate a hash value using the hash value created in step 3 and the nonce, then send the login request to the server
5. When the server receives the login request, it generates a hash value using SHA256 with the stored hash value and the nonce

6. If the hash value received in step 4 matches the hash value generated in step 5, process as login successful; if the hash values differ, process as login failed.

## 6.2 Topology Security Index

- Policy Path Security Index

- The operator manually inputs the risk index for each firewall and network device. (Stored in the database)
- Based on the input IP (for lookup), the security score along the network path is calculated.
- Formula: Sum(Firewall.Security Index) + Sum(Network.Security Index) * (Max100)≤ 100
  Ex) If path contains Firewall A (Security Index: 10), Firewall B (Security Index: 5), and Network C (Security Index: 10): Score = 25. If exceeding 100, adjusted to Max 100

- Compliance Security Index

- The operator inputs compliance scores and weights according to internal rules. (Stored in DB)
- Calculates the compliance violation index based on the entered IP (for search), port, and expiration date (for search).
- Formula: Sum(Search Compliance * Score * Weight) * (Max 100)≤ 100

- Zone (Group) Security Index

- The operator manually inputs the security index appropriate for the internal network. (DB storage)
- Based on the input IP (for search), it searches for zones (groups) along the path and calculates the score.
- Formula: Sum(Security Score of Included Zones (Groups)) * (Max100)≤ 100

- Expiration Date Security Index

- Calculates the security index based on the entered expiration date (for search purposes).
- Formula: Expiration Date≤1month=80, Expiration Date ≤ 6 months=60, Expiration Date≤ 12 months=40 Expiration Date≥ Permanent=20

- Comprehensive Security Index

- Provides a comprehensive calculation of the above 4 security indices.
- Formula: Sum of each security index / 4≤ 100

## 6.3 Additional Restrictions for Document Use

- Any **modification, editing, translation, adaptation, or redistribution** (including sharing, forwarding, posting, or uploading) of this document (or any portion of it) **without prior written permission from the distributor** is not permitted.

- This document may be used **only for the specified purpose and within the authorized scope**. Any use beyond such purpose (including commercial use) requires the distributor's prior written permission.

- All copyrights and other intellectual property rights in this document belong to the distributor (or the applicable rights holder). Users may not remove, alter, or obscure any rights notices (including copyright notices).

- Any confidential or sensitive information contained in this document must not be disclosed to any third party, and access must not be granted to any unauthorized person.

- Any derivative works based on this document (including summaries, excerpts, translations, or presentation materials) must not be distributed without the distributor's prior written permission.

- In the event of a violation of these restrictions, the distributor may require immediate cessation of use of the document and may pursue remedies under applicable laws and/or agreements.

- The copyrights, trademarks, logos, and other rights related to third-party products referenced or used in this document belong to their respective owners.

- The contents of this document may vary depending on the time of distribution, and the distributor assumes no responsibility or liability for any matters arising therefrom.

- Users must manage this document securely on a need-to-know basis, and upon the distributor's request or upon completion of the authorized purpose, users must promptly retrieve and delete (or return and destroy) the document.

- Only the most recently distributed version is valid. Prior versions must not be used or retained and must be promptly disposed of.

- If these restrictions conflict with any separate contract, license, or written agreement, the terms of such contract/agreement shall prevail.