

PIOLINK Web Application Firewall

# WEBFRONT-K

시스템 구성 설명서

Rev 1.3

## 등록 상표

---

PIOLINK 는 ㈜파이오링크의 등록상표입니다.

## 일러두기

---

- 이 설명서의 저작권은 ㈜파이오링크에 있습니다. 이 설명서는 저작권법에 의하여 법적으로 보호받고 있으며, 저작권자의 사전 서면 허가 없이는 어떠한 이유에서든 무단으로 전체 혹은 일부분의 내용을 발췌하거나 어떠한 형태로든 복제할 수 없습니다.
- 이 설명서는 제품의 기능 향상과 인쇄상의 오류 수정 등으로 인하여 예고 없이 변경될 수 있습니다.
- 이 설명서 및 그 내용에 의해 직접, 간접으로 발생될 수 있는 피해 및 재산상 손해에 대해 ㈜파이오링크는 법적인 책임이 없음을 밝힙니다.

---

WEBFRONT-K 시스템 구성 설명서 Rev 1.3 (2019.07.)  
© PIOLINK, Inc. All rights reserved.  
전화: 02-2025-6900 / 홈페이지: <http://www.piolink.com>

---

# 설명서 소개

이 설명서는 WEBFRONT-K Web Manager의 System 메뉴에 대해 설명하고 있는 설명서입니다. WEBFRONT-K Web Manager의 System 메뉴는 WEBFRONT-K 시스템을 설정하거나 네트워크 설정, 애플리케이션과 사용자 관리 및 WEBFRONT-K와 전체 애플리케이션을 모니터링할 때 사용하는 메뉴로, WEBFRONT-K의 통합 관리자와 사이트 관리자만 사용할 수 있습니다. WEBFRONT-K가 설치된 네트워크를 관리하는 네트워크 관리자나 WEBFRONT-K의 시스템 관리자는 이 설명서를 참고하여 WEBFRONT-K를 설치한 후 사용하기 위해 필요한 구성 작업을 수행할 수 있습니다.

## 대상 독자

이 WEBFRONT-K 시스템 구성 설명서는 WEBFRONT-K가 설치된 네트워크를 관리하는 네트워크 관리자나 WEBFRONT-K 시스템을 설정하고 관리하는 사이트 관리자를 대상으로 작성되었습니다.

## PLOS 버전

이 설명서는 PLOS v2.0.61.0.3 버전이 설치된 WEBFRONT-K를 기준으로 작성되었습니다. 이전 버전의 PLOS가 설치되어 있는 경우에는 이 사용 설명서에서 설명하는 기능이 지원되지 않을 수 있고, 설명에 맞게 설정한 경우에도 정상적으로 동작하지 않을 수 있습니다.

## 설명서의 표기법

다음은 이 설명서에서 사용하는 참고 및 주의 표시에 대한 설명입니다.

### 참고 및 주의 표기

이 사용 설명서에서 사용자에게 특별히 전달하고자 하는 내용을 다음과 같은 아이콘과 글꼴을 사용하여 표시합니다.



**참고:** 설명서의 내용과 관련하여 함께 알아두면 유용한 사항이나 제품을 사용하면서 도움이 될 만한 참고 사항과 관련 자료 등을 소개합니다.



**주의:** 데이터를 손실하거나 혹은 제품이 잘못 동작할 수 있는 상황을 설명하고, 그 상황에 대한 대처 방법을 알려줍니다.

## 제품 아이콘

아이콘	예
	구성도나 제품 설명 등에 사용되는 제품 아이콘으로, WEBFRONT-K를 나타냅니다.

## 설정 화면

각 설정 화면은 WEBFRONT-K3200을 기준으로 작성되었습니다. 제품에 따라 포트 개수나 포트 위치가 상이할 수 있습니다.

## 관련 문서

이 설명서와 함께 다음과 같은 설명서가 추가로 제공됩니다.

- **WEBFRONT-K 소개서(Overview)**

WEBFRONT-K를 도입해야 하는 필요성과 WEBFRONT-K를 사용한 네트워크 구성, 그리고 WEBFRONT-K가 제공하는 기능에 대해 상세하게 소개하는 설명서입니다. WEBFRONT-K가 어떤 장비이고 어떤 기능을 제공하며 어떻게 활용해야 하는지를 이 설명서를 통해 알 수 있습니다. 다른 설명서를 읽기 전에 가장 먼저 참고하는 것이 좋습니다.

- **WEBFRONT-K 시작 설명서(Getting Started Guide)**

WEBFRONT-K를 사용하기 위해 필수적인 설치 및 구성 과정을 설명하는 설명서입니다. 이 설명서를 참고하면 어떤 과정을 거쳐서 WEBFRONT-K를 설치하고 구성하여 사용할 수 있게 되는지를 파악할 수 있습니다. 이 설명서는 필수적이지만 기본적인 기능에 대해서만 다루고 있고 또 다루는 기능에 대해서도 상세히 설명되어 있지 않습니다. 각 기능에 대한 상세한 설명은 시스템 구성 설명서나 애플리케이션 구성 설명서를 참고하도록 합니다.

- **WEBFRONT-K 설치 설명서(Installation Guide)**

WEBFRONT-K의 앞면, 뒷면, 옆면에 있는 각 부분의 기능을 소개하고, WEBFRONT-K를 랙에 설치한 후 각 포트에 장비를 연결하는 방법을 알려주는 설명서입니다. WEBFRONT-K의 하드웨어 사양과 장비 연결시 사용하는 케이블에 대한 상세한 사양도 이 설명서에서 볼 수 있습니다.

- **WEBFRONT-K 애플리케이션 구성 설명서(Application Configuration Guide)**

WEBFRONT-K Web Manager의 Application 메뉴에 대해 설명하고 있는 설명서입니다. Application 메뉴는 WEBFRONT-K의 통합 관리자, 사이트 관리자, 애플리케이션 관리자가 사용할 수 있는 메뉴입니다. Application 메뉴를 사용하여 애플리케이션을 설정하거나 웹 보안 기능을 설정하고 애플리케이션을 모니터링할 수 있습니다.

## 서비스 지원

고객 서비스나 기술 지원, 혹은 기술 교육에 관한 자세한 정보가 필요한 경우에는 다음 연락처로 문의하시면 필요한 도움을 받을 수 있습니다.

- 기술지원센터(TAC): 544-9890
- E-mail: suport@piolink.com

# 설명서 구성

이 설명서의 각 장은 다음과 같은 내용으로 구성되어 있습니다.

## 제1장 시작하기 전에

이 장에서는 사이트 관리자가 WEBFRONT-K에 접속하고 로그인하는 방법과 WEBFRONT-K의 화면 구성 및 메뉴의 기능, 그리고, WEBFRONT-K를 사용하기 위한 알아야 할 기본적인 사용 방법에 대해 소개합니다.

## 제2장 대시보드

이 장에서는 WEBFRONT-K의 하드웨어 및 애플리케이션 상태를 실시간으로 확인할 수 있는 대시보드에 대해 설명합니다.

## 제3장 통합 모니터링

이 장에서는 WEBFRONT-K의 모니터링 기능을 통해 WEBFRONT-K의 상태 정보와 통계 정보, 시스템 정보 등을 파악하는 방법에 대해 설명합니다.

## 제4장 시스템 모니터링

이 장에서는 WEBFRONT-K 시스템의 기본적인 정보와 상태 정보를 조회하고, 포트의 실시간 트래픽 정보를 모니터링하는 방법에 대해 살펴봅니다.

## 제5장 통합 로그

이 장에서는 WEBFRONT-K의 로그 기능에 대해 살펴본 후, 로그를 설정하는 방법과 사용자가 원하는 로그만을 보여주는 로그 필터를 정의하고 사용하는 방법, 그리고 로그를 화면에 출력하는 방법에 대해 설명합니다.

## 제6장 통합 보고서

이 장에서는 WEBFRONT-K의 보고서 기능에 대해 살펴본 후, 보고서를 생성하는 방법과 주기별 보고서 생성 방법에 대해 설명합니다.

## 제7장 애플리케이션

이 장에서는 WEBFRONT-K의 웹 보안 기능으로 보호할 애플리케이션을 등록하고 관리하는 방법과 애플리케이션의 각 보안 기능을 설정할 때 사용되는 정규식을 정의하는 방법, 그리고, 웹 보안 기능에서 사용하는 시그니처를 업데이트하는 방법에 대해서 알아보십시오.

## 제8장 방화벽

WEBFRONT-K는 자체 보호를 위해 지정된 호스트에서만 WEBFRONT-K로 접근할 수 있도록 하는 시스템 접근 제어 기능을 제공합니다. 그리고 WEBFRONT-K에 연결된 네트워크를 보호하기 위해 다양한 조건의 필터를 사용하여 불필요한 트래픽이 송수신되지 않도록 하는 방화벽 기능을 지원합니다. 이 장에서는 WEBFRONT-K의 시스템 접근 제어 기능과 방화벽 기능에 대해 살펴본 후, 이 기능을 사용하기 위한 설정 방법에 대해 알아보도록 합니다.

## 제9장 사용자 관리

이 장에서는 WEBFRONT-K에 등록된 애플리케이션을 관리할 수 있는 사용자를 등록하고 관리하는 방법을 설명합니다.

## 제10장 일반 설정

이 장에서는 WEBFRONT-K의 기본적인 구성 작업에 대해 알아보십시오. WEBFRONT-K는 출하될 때 이미 기본적인 구성이 되어 있는 상태이기 때문에 이 장에서 설명하는 구성 작업을 하지 않고 제품을 바로 사용할 수 있습니다. 하지만 사용자의 네트워크 환경에 맞게 장비의 설정을 변경해야 하는 경우에는 이 장의 내용을 참고하여 원하는 환경으로 구성하도록 합니다.

## 제11장 네트워크

이 장에서는 WEBFRONT-K의 네트워크 구성 작업에 대해 알아보십시오. VLAN, IP 주소, 포트와 같은 기본적인 네트워크 설정과 더불어 루프(loop)를 방지하기 위한 STP, 장비 포트에 대한 정보를 수집하기 위한 포트 미러링, 포트 모니터링 등 다양한 네트워크 기능을 사용하는 방법에 대해 소개합니다.

## 제12장 HA

이 장에서는 WEBFRONT-K는 안정적인 서비스를 제공하기 위해 HA(High Availability) 기능을 제공합니다. 이 장에서는 WEBFRONT-K의 HA 기능에 대해 살펴본 후, 이 기능을 사용하기 위한 설정 방법에 대해 알아보도록 합니다.

# 목차

<b>WEBFRONT-K 시스템 구성 설명서 .....</b>	<b>1</b>
설명서 소개 .....	3
설명서 구성 .....	5
목차 .....	7
<b>제 1 장 시작하기 전에 .....</b>	<b>12</b>
라이선스 등록 .....	12
라이선스 발급받기 .....	13
라이선스 등록하기 .....	15
관리자 계정 생성 .....	16
로그인/로그아웃 .....	17
로그인하기 .....	17
로그아웃하기 .....	18
시스템 메뉴 .....	19
WEBFRONT-K Web Manager 화면 구성 .....	23
메인 화면 .....	23
설정 화면 .....	24
사용자 환경 설정하기 .....	26
기본 메뉴 모드 설정 .....	26
로그인 유지 시간 설정 .....	27
로그인 암호 변경 .....	27
<b>제 2 장 대시보드 .....</b>	<b>28</b>
개요 .....	29
대시보드 사용하기 .....	29
기본 대시보드 .....	29
사용자 정의 대시보드 .....	31
<b>제 3 장 통합 모니터링 .....</b>	<b>34</b>
시스템 통합 모니터링 .....	35
모니터링 화면 구조 .....	36
트래픽 양에 대한 모니터링 정보 .....	38
웹 공격 횟수에 대한 모니터링 정보 .....	39
요청 검사에 대한 모니터링 정보 .....	39
콘텐츠 보호에 대한 모니터링 정보 .....	40
학습 기능에 대한 모니터링 정보 .....	41
위장 기능에 대한 모니터링 정보 .....	42
요청 검사 모니터링 .....	43
콘텐츠 보호 모니터링 .....	45
학습 모니터링 .....	47
위장 모니터링 .....	49
<b>제 4 장 시스템 모니터링 .....</b>	<b>51</b>
시스템 정보 .....	52
시스템 상태 .....	52
시스템 자원 상태 정보 .....	53

시스템 하드웨어 상태 정보.....	53
포트 모니터링 .....	55
포트의 실시간 트래픽 양 보기.....	55
<b>제 5 장 통합 로그 .....</b>	<b>57</b>
로그 개요.....	57
통합 로그 설정.....	61
로그 레벨 설정하기.....	61
로그 삭제 용량 설정하기.....	61
시스로그 포맷 설정하기.....	62
시스로그 서버 설정하기.....	62
사용자 정의 보안로그 포맷 설정하기.....	63
로그 백업.....	64
로그 내보내기.....	66
보안 로그.....	67
감사/시스템 로그.....	69
방화벽 로그.....	70
접근 로그.....	71
<b>제 6 장 통합 보고서 .....</b>	<b>72</b>
통합 보고서 생성하기.....	73
통합 보고서 스케줄 설정하기 .....	75
<b>제 7 장 애플리케이션 .....</b>	<b>76</b>
애플리케이션 관리.....	76
개요.....	77
애플리케이션 보기.....	77
직접 애플리케이션 추가하기.....	78
마법사로 애플리케이션 추가하기.....	78
애플리케이션 전체 세션 삭제.....	81
도메인 학습.....	82
애플리케이션 설정 보기.....	83
개요.....	83
설정 출력하기.....	84
설정 비교하기.....	85
설정 다운로드하기.....	85
설정 출력 화면.....	86
애플리케이션 설정 간편화.....	88
개요.....	88
애플리케이션 별 보기.....	88
기능 별 보기.....	89
보안 기능 bypass 상태 설정하기.....	90
고급 첨부파일 검사 설정.....	91
고급 첨부 파일 검사 설정 정보 변경하기.....	91
고급 첨부 파일 검사 상태 설정하기.....	91
시그니처 관리.....	92
개요.....	92
시그니처 관리 화면.....	94
시그니처 버전 조회.....	95
시그니처 업데이트.....	96
시그니처 액션 설정.....	98

사용자 정의 시그니처 설정하기.....	101
시그니처 에이징 설정하기.....	102
시그니처 내보내기.....	103
정규식 설정.....	104
정규식.....	104
정규식 등록하기.....	105
블랙리스트 관리.....	106
설정 개요.....	106
블랙리스트 설정하기.....	108
화이트리스트 관리.....	113
설정 개요.....	113
화이트리스트 설정하기.....	114
<b>제 8 장 방화벽.....</b>	<b>115</b>
시스템 접근 제어.....	115
개요.....	116
시스템 접근 제어 설정하기.....	116
Snort 설정.....	118
개요.....	118
Snort 설정하기.....	118
방화벽.....	119
개요.....	119
방화벽 설정하기.....	120
<b>제 9 장 사용자 관리.....</b>	<b>124</b>
사용자 관리 개요.....	125
사용자 추가하기.....	126
현재 로그인 실패 횟수 변경하기.....	128
계정 관리 설정하기.....	129
중복 로그인 허용 설정하기.....	130
기본 사용자 설정하기.....	131
RADIUS 설정하기.....	132
사용자 접근 IP 리스트 관리.....	133
<b>제 10 장 일반 설정.....</b>	<b>134</b>
설정 관리.....	135
개요.....	135
설정 관리 화면.....	137
설정 자동 백업 설정하기.....	138
현재 설정 저장하기(SDRAM → SSD).....	139
설정 다운로드/업로드하기.....	139
설정 삭제하기.....	140
다음 부팅시 사용할 설정 지정하기.....	141
설정 동기화하기.....	141
설정 실시간 동기화하기.....	142
설정 복사하기.....	143
기술 지원 도우미.....	145
시스템 동작 로그 정보 저장하기.....	145
시스템 동작 로그 정보 다운로드하기.....	146
서버 장애 감시.....	147
개요.....	147

서버 장애 감시 활성화하기.....	147
시스템 감시.....	149
시스템 감시 사용 여부와 감시 주기 설정.....	149
CPU 감시 설정.....	149
메모리 감시 설정.....	150
포트 감시 설정.....	150
SNMP.....	151
개요.....	151
SNMP 설정하기.....	152
라이선스 관리.....	156
유지보수 라이선스 설정.....	156
라이선스 설정.....	156
국가별 IP.....	157
국가별 IP 업데이트.....	157
PLOS 관리.....	158
시간 관리.....	160
NTP(Network Time Protocol) 서버.....	160
직접 시스템 시간 설정하기.....	160
시간대 조정하기.....	160
NTP 서버 사용하기.....	161
DNS 관리.....	162
개요.....	162
DNS 설정하기.....	162
리포터 설정.....	163
리포터 IP 정보 설정.....	163
리포터 관련 정보 설정.....	163
리포터 사용 여부 설정.....	164
E-mail 알람.....	165
개요.....	165
E-mail 알람 설정하기.....	165
보안 이벤트 알람.....	166
무결성 검사.....	167
개요.....	167
무결성 검사 설정하기.....	167
환경 변수.....	169
프록시 ARP.....	169
저장 MAC 응답.....	170
HTTP 파라미터.....	171
부팅 중 포트 상태.....	172
TOS 설정.....	173
통계 기간 설정.....	174
개요.....	174
통계 기간 설정하기.....	174
시스템 관리 설정.....	175
웹 매니저 설정.....	175
SSH 설정.....	175
Telnet 설정.....	176
호스트 이름 설정.....	177
시스템 재시작.....	177

## 제 11 장 네트워크 ..... 178

포트 바운더리.....	179
--------------	-----

개요.....	179
포트 바운더리 설정 하기.....	181
IP 주소.....	183
IP 설정 정보 보기.....	183
VLAN 인터페이스의 IP 주소 설정.....	184
기본 게이트웨이 추가.....	184
고정 경로 추가.....	185
VLAN.....	186
개요.....	186
VLAN 생성하기.....	187
포트.....	188
개요.....	188
포트 설정하기.....	189
링크싱크.....	191
개요.....	191
링크싱크 설정하기.....	192
미러링.....	193
트렁킹.....	194
개요.....	194
포트 트렁킹 설정시 주의 사항.....	194
STP.....	196
개요.....	196
STP 설정하기.....	199
STP 상태 설정하기.....	199
ARP.....	201
개요.....	201
정적 ARP 리스트 설정하기.....	201
ARP 타임아웃 설정.....	201

## 제 12 장 HA..... 202

HA 개요.....	203
HA.....	203
Failover.....	203
Dead 간격.....	204
우선 순위.....	204
가상 IP 주소와 서비스 가상 IP 주소.....	205
백업 시 차단 포트.....	205
HA 설정하기.....	206
설정하기 전에.....	206
VRRP 그룹 설정하기.....	206
백업 시 차단 포트 설정하기.....	208
HA 기능 활성화하기.....	208

# 제1장 시작하기 전에

이 장에서는 사이트 관리자가 WEBFRONT-K에 접속하여 라이선스를 등록하고, 로그인하는 방법과 WEBFRONT-K의 화면 구성 및 메뉴의 기능, 그리고, WEBFRONT-K를 사용하기 위해 알아야 할 기본적인 사용 방법에 대해 소개합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 라이선스 등록
- 관리자 계정 생성
- 로그인/로그아웃
- 시스템 메뉴
- WEBFRONT-K Web Manager 화면 구성
- 사용자 환경 설정하기



**참고:** WEBFRONT-K의 Web Manager를 최적의 상태로 사용하기 위해서는 Microsoft의 Internet Explorer 11 이상 또는 Google의 Chrome을 권장합니다.



# 라이선스 등록

WEBFRONT-K를 사용하려면 먼저 WEBFRONT-K에 라이선스를 등록해야 합니다. 제품구입 후 당사의 파트너 포탈 홈페이지(http://partner.piolink.com)에서 제품을 등록하시면 해당 제품의 라이선스를 발급 받을 수 있습니다. 이 절에서는 WEBFRONT-K를 사용하기 위해 필요한 라이선스를 발급 받는 방법과 등록하는 방법에 대해 알아봅니다.



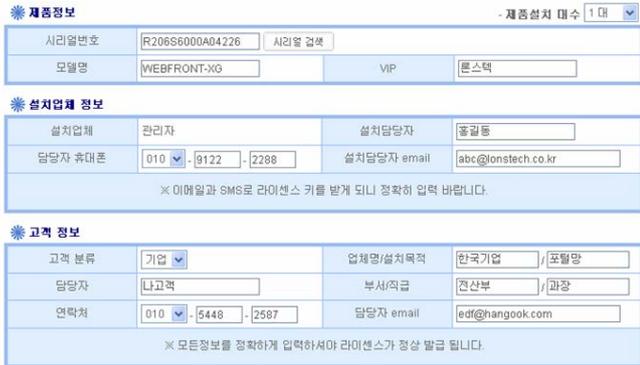
**주의:** 라이선스를 등록하지 않으면 WEBFRONT-K를 설정할 수 있는 Web Manager에 로그인할 수 없습니다. 제품 설치후 다음 설명을 참고하여 라이선스 발급과 등록 과정을 반드시 수행하도록 합니다.



**참고:** 제품 라이선스 발급과 관련된 상세한 정보는 제품의 구입처나 당사 기술지원센터(TAC: 1544-9890)로 문의하시기 바랍니다.

## 라이선스 발급받기

WEBFRONT-K의 제품 라이선스를 발급받는 방법은 다음과 같습니다.

순서	설정 과정
1	인터넷 익스플로러나 파이어폭스와 같은 웹 브라우저를 실행합니다. 그리고, 웹 브라우저의 주소 입력란에 'http://partner.piolink.com'을 입력한 후 <b>[Enter]</b> 키를 누르거나 <b>[이동]</b> 버튼을 클릭합니다.
2	다음과 같은 화면이 나타나면 ID와 PASSWARD를 입력하고 <b>[로그인]</b> 버튼을 클릭합니다.  <p>참고: ID가 없는 경우 <b>[회원가입]</b> 버튼을 클릭한 후 회원 가입 신청을 합니다. 가입 신청 후 관리자 승인이 이루어져야 로그인을 할 수 있습니다.</p>
3	화면 좌측에 있는 <b>제품등록</b> 메뉴를 클릭합니다.
4	제품 라이선스 발급 화면에서 다음 설명을 참고하여 각 항목을 작성한 후 <b>[라이선스 발급]</b> 버튼을 클릭합니다.  <p><b>제품설치 대수</b>      등록할 제품의 수를 드롭다운 목록에서 선택합니다. 1 ~ 5대까지 선택이 가능하며, 선택한 제품 수 만큼 제품 정보 부분이 추가됩니다.</p> <p><b>제품정보</b>            <b>[시리얼 검색]</b> 버튼을 클릭하면 다음과 같은 팝업 창이 나타납니다. 제품 박스 및 뒷면에 붙어있는 시리얼 번호의 뒷자리 5자리를 입력하고 <b>[검색]</b> 버튼을 클릭합니다.</p>

※ Serial No.의 **끝부분 5자리** 숫자를 입력하십시오.

예) R206S6000A**01234**

▶ 01234

- **설치업체 정보**      제품 설치 담당자의 정보를 입력합니다. 입력한 휴대폰 번호와 이메일 주소로 라이선스 키를 전송하므로 정확한 정보를 입력해야 합니다.
- **고객 정보**        제품을 구입한 고객의 정보를 입력합니다.

5 화면 좌측에 있는 등록완료 리스트 메뉴를 클릭합니다.

제품 등록 리스트 화면 에서 시리얼 번호를 클릭합니다.

6

제품명	Serial NO.	VIP(ID)	설치업체(ID)	고객명	등록일	만료일	발송
WEBFRONT-XG	R206S6000A04228	론스텍	관리자	한국기업	2009-08-26	2010-08-26	SMS email
inFRONT 1000	IN1000D	론스텍	관리자	test	2009-08-25	2009-07-07	SMS email



**참고: SMS email**을 클릭하면 제품등록시 입력한 휴대폰 번호와 이메일 주소로 라이선스 키가 발송됩니다.

제품 등록 정보 화면에서 라이선스 키를 확인합니다.

▶ 제품 등록 정보 ◀

7

※ **상품정보**

모델명	WEBFRONT-XG	시리얼번호	R206S6000A04228
OS버전	R206S6000A	SSL여부	없음

※ **설치정보**

설치업체(ID)	관리자 (pioadmin)	설치담당자	홍길동
설치담당자 연락처	010-9122-2288	설치담당자 email	abc@ionstech.co.kr

※ **고객정보**

고객분류	기업	고객업체명	한국기업
고객 담당자	나고객	고객 연락처	010-5448-2587
고객 email	edf@hangoon.com		

※ **라이선스 정보**

라이선스	00ED 2B3CB ECE37 7E3E		
라이선스 발급일	2009-08-26	라이선스 종료일	2010-08-26

※ **담당자 정보**

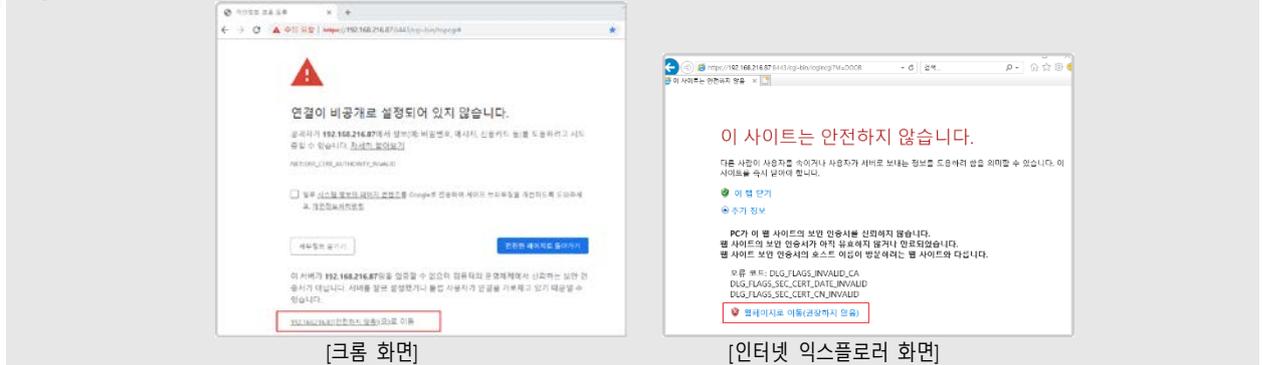
관리 담당자	홍길동	관리 담당자 연락처	010-9122-2288
--------	-----	------------	---------------

← 리스트로 돌아가기

# 라이선스 등록하기

WEBFRONT-K의 제품 라이선스를 등록하는 방법은 다음과 같습니다.

**참고:** Web Manager 접속시 사용자 PC의 보안 설정에 따라 다음과 같은 보안 경고 창이 나타날 수 있습니다. 이러한 창이 나타나면 **[웹페이지로 이동]**을 클릭하면 됩니다.



[크롬 화면]

[인터넷 익스플로러 화면]

순서	설정 과정
1	<p>사용자 PC에 인터넷 익스플로러나 크롬과 같은 웹 브라우저를 실행합니다. 그리고, 웹 브라우저의 주소 입력란에 'https://WEBFRONT-K의 IP 주소:8443'을 입력한 후 <b>[Enter]</b> 키를 누릅니다. WEBFRONT-K의 IP 주소는 관리용 인터페이스나 VLAN 인터페이스의 IP 주소를 사용하면 됩니다.</p>  <p><b>참고:</b> WEBFRONT-K를 구입한 후 관리용 IP 주소를 변경하지 않고 최초로 로그인하는 경우에는 관리용 인터페이스에 기본으로 설정되어 있는 IP 주소인 192.168.100.1/24를 사용합니다. 192.168.100.1/24를 통해 WEBFRONT-K에 접속하려면 사용자 PC의 IP 주소가 192.168.100.1/24와 동일한 네트워크에 속해야 합니다. 즉, 192.168.100.0~192.168.100.255/24 범위에 속하는 IP 주소로 설정되어 있어야 합니다.</p> <p><b>주의:</b> 주소를 입력할 때 https 대신 http를 입력하지 않았는지 확인합니다. http로 입력하면 WEBFRONT-K에 접속할 수 없습니다.</p>
2	<p>라이선스 입력 화면이 나타나면 다음 설명을 참고하여 라이선스를 입력한 후 <b>[확인]</b> 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• 유지보수 라이선스      제품 등록후 발급받은 라이선스 키를 입력합니다.</li> <li>• S/N                        WEBFRONT-K의 시리얼 번호가 출력됩니다. 라이선스 키는 시리얼 번호를 사용하여 생성한 값이기 때문에 라이선스를 다른 장비에 등록할 수 없습니다. 2대 이상의 WEBFRONT-K를 사용하는 경우에는 출력된 시리얼 넘버를 확인한 후 해당 장비의 라이선스 키를 입력하도록 합니다.</li> </ul>

# 관리자 계정 생성

WEBFRONT-K 설치 후 최초로 접속한 경우에는 라이선스 등록 후 사용자 계정을 생성해야 합니다. 최초 접속 시 관리자 계정을 생성하는 방법은 다음과 같습니다.



**참고:** WEBFRONT-K는 기본으로 제공하는 계정이 없습니다. 그러므로 최초 설치 또는 장비를 초기화한 경우에는 Web Manager로 접속하여 관리자 계정을 생성해야 합니다.

순서	설정 과정
1	<p>사용자 PC에서 웹 브라우저를 실행합니다. 그리고, 웹 브라우저의 주소 입력란에 'https://192.168.100.1:8443'을 입력한 후 [Enter] 키를 누르거나 [이동] 버튼을 클릭합니다.</p>
2	<p>계정 생성 화면이 나타나면 다음 설명을 참고하여 각 항목을 입력한 후 [확인] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>사용자 ID</b>    사용자의 로그인 이름을 입력합니다. 알파벳이나 숫자, 특수문자를 조합한 5~16 자의 문자열을 입력합니다. 알파벳은 대소문자를 구분하여 사용해야 합니다.</li> <li>• <b>패스워드</b>    사용자의 로그인 암호를 입력합니다. 알파벳 대문자, 소문자, 숫자, 특수문자 중 3가지 이상의 조합으로 9~20자의 문자열을 지정합니다.</li> <li>• <b>패스워드 확인</b>                   로그인 암호를 다시 한번 입력합니다.</li> <li>• <b>이메일 주소</b>    사용자의 이메일 주소를 입력합니다.</li> </ul>



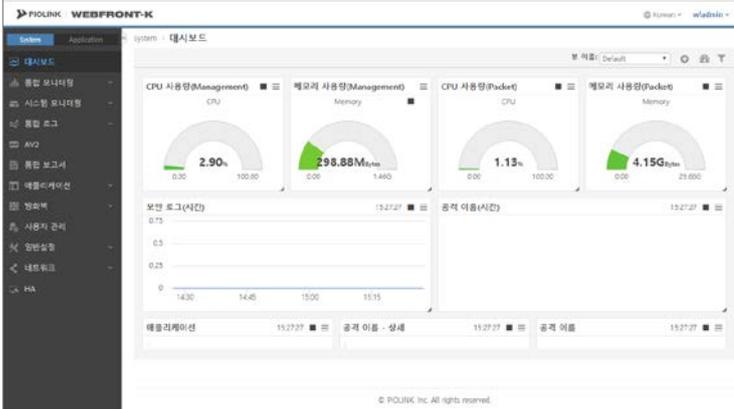
**참고:** 위 방법은 최초 설치 시 또는 장비를 초기화한 경우에만 사용할 수 있습니다. 운용 중 관리자 계정을 추가하는 방법은 이 설명서의 [제9장 사용자 관리 - 사용자 추가하기] 절을 참고하기 바랍니다.

# 로그인/로그아웃

이 절에서는 WEBFRONT-K를 모니터링하고 설정할 수 있는 WEBFRONT-K Web Manager로 로그인하는 방법과 로그아웃하는 방법에 대해 알아봅니다.

## 로그인하기

WEBFRONT-K에 접속하고 WEBFRONT-K의 Web Manager로 로그인하는 방법은 다음과 같습니다.

순서	설정 과정
1	<p>웹 브라우저의 주소 입력란에 'https://WEBFRONT-K의 IP 주소:8443'을 입력한 후 <b>[Enter]</b> 키를 누르거나 <b>[이동]</b> 버튼을 클릭합니다. WEBFRONT-K의 IP 주소는 관리용 인터페이스나 VLAN 인터페이스의 IP 주소를 사용합니다.</p>  <p><b>주의:</b> 주소를 입력할 때 https 대신 http를 입력하지 않았는지 확인합니다. http로 입력하면 WEBFRONT-K에 접속할 수 없습니다.</p> <p><b>참고:</b> WEBFRONT-K를 구입한 후 관리용 IP 주소를 변경하지 않고 최초로 로그인하는 경우에는 관리용 인터페이스에 기본으로 설정되어 있는 IP 주소인 192.168.100.1/24를 사용합니다. 192.168.100.1/24를 통해 WEBFRONT-K에 접속하려면 사용자 PC의 IP 주소가 192.168.100.1/24와 동일한 네트워크에 속해야 합니다. 즉, 192.168.100.0 ~ 192.168.100.255/24 범위에 속하는 IP 주소로 설정되어 있어야 합니다.</p> <p><b>참고:</b> 이 설명서의 화면 예제는 인터넷 익스플로러 버전 11을 사용한 경우입니다. 다른 종류의 웹 브라우저나 다른 버전의 인터넷 익스플로러를 사용하는 경우에는 나타나는 팝업 창이나 화면 형태가 약간 다를 수 있습니다.</p>
2	<p>로그인 정보를 입력하는 화면이 출력되면 <b>사용자 ID</b>와 <b>패스워드</b>를 입력하고 언어를 선택한 후 <b>[확인]</b> 버튼을 클릭합니다.</p>  <p><b>참고:</b> Web Manager의 언어는 사용자 PC의 언어 설정이 자동으로 적용됩니다. 사용자 PC에 설정된 언어와 다른 언어를 사용하려면, 언어 선택 드롭다운 메뉴에서 지정하도록 합니다.</p>
3	<p>Web Manager에 정상적으로 로그인하면 시작 화면이 나타납니다. 시작 화면은 로그인 ID의 사용자 종류(통합 관리자, 시스템 관리자, 애플리케이션 관리자, 모니터)에 따라 달라집니다. 아래 화면은 통합 관리자나 시스템 관리자로 로그인한 경우에 나타나는 화면입니다.</p> 

## 로그아웃하기

WEBFRONT-K Web Manager에서 로그아웃한 후 다른 사용자 계정으로 로그인하려면, WEBFRONT-K Web Manager 화면의 오른쪽 위에 있는 [Logout]을 클릭합니다.



그러면 WEBFRONT-K Web Manager 화면이 닫히고 새로운 계정으로 로그인할 수 있는 화면이 나타납니다.

A screenshot of the WEBFRONT-K login page. The page features the PIOLINK logo and 'WEBFRONT-K' text at the top. Below the logo, the text '로그인' (Login) is displayed, followed by the instruction '아이디와 비밀번호를 입력하여 주세요.' (Please enter your ID and password). There are two input fields: '사용자 ID' (User ID) and '패스워드' (Password). A blue '확인' (Confirm) button is located below the input fields. At the bottom of the page, there is a copyright notice '© PIOLINK WEB Application Firewall' and a language selection option 'Korean'.

# 시스템 메뉴

이 절에서는 각 **System** 메뉴의 기능에 대해 간략하게 소개합니다.



**참고:** 통합 관리자나 사이트 관리자로 로그인하면 **System** 메뉴뿐만 아니라 **Application** 메뉴까지 모두 사용할 수 있습니다. **Application** 메뉴의 사용 방법은 이 설명서와 함께 제공되는 **애플리케이션 구성 설명서**에 설명되어 있으므로 이 설명서에서는 다루지 않습니다.

**System** 메뉴는 12개의 메뉴 항목으로 구성되어 있습니다. 각 메뉴에 대해 상세하게 살펴봅니다.

## 대시보드

대시보드는 WEBFRONT-K와 WEBFRONT-K에 의해 보호되고 있는 애플리케이션의 현재 상태를 실시간으로 보여주는 메뉴입니다. 관리자는 대시보드에 표시된 정보를 통해 빠르게 WEBFRONT-K 및 애플리케이션의 상태를 파악할 수 있고, 필요한 경우 적절한 조치를 즉시 취할 수 있습니다.

## 통합 모니터링

통합 모니터링은 일정 기간 동안 모니터링한 WEBFRONT-K의 트래픽 양과 보안 기능에 의해 차단되거나 학습된 정보에 대한 통계 정보를 보여주는 메뉴입니다. 통합 모니터링 메뉴는 모니터링된 모든 정보를 간략하지만 한꺼번에 보여주는 하위 메뉴와 각 보안 기능의 상세 모니터링 정보를 보여주는 하위 메뉴들로 구성되어 있습니다.

메뉴	기능
시스템 통합 모니터링	최근 시간 동안 WEBFRONT-K를 통해 송수신된 트래픽의 양과 각 웹 보안 기능에 의해 차단된 웹 공격에 대한 정보, 그리고 학습 기능을 통해 학습된 정보를 보여주는 메뉴입니다.
요청 검사 모니터링	요청 검사 기능에 대해서 상세하게 모니터링할 수 있는 메뉴입니다. 특정 애플리케이션이나 특정 요청 검사 기능에 대한 정보, 혹은 특정 형식의 정보만 조회할 수 있습니다. 그리고, 특정 시간 동안 모니터링한 정보만 출력하는 것도 가능합니다.
컨텐츠 보호 모니터링	컨텐츠 보호 기능에 대해서 상세하게 모니터링할 수 있는 메뉴입니다. 특정 애플리케이션이나 특정 컨텐츠 보호 기능에 대한 정보, 특정 형식의 정보만 조회할 수 있습니다. 그리고, 특정 시간 동안 모니터링한 정보만 출력할 수도 있습니다.
학습 모니터링	학습 기능에 대해서 상세하게 모니터링할 수 있는 메뉴입니다. 특정 애플리케이션이나 특정 요청 검사 기능에 대한 학습 정보만 조회할 수 있고, 특정 시간 동안의 학습 정보만 출력할 수도 있습니다.
위장 모니터링	위장 기능에 대해서 상세하게 모니터링할 수 있는 메뉴입니다. 특정 애플리케이션이나 특정 위장 기능에 대한 정보, 특정 형식의 정보만 조회할 수 있습니다. 그리고, 특정 시간 동안 모니터링한 정보만 출력할 수도 있습니다.

## 시스템 모니터링

시스템 모니터링은 WEBFRONT-K 시스템의 기본/상태 정보를 조회하고, 포트의 실시간 트래픽 정보를 모니터링하는 메뉴로 구성되어 있습니다.

메뉴	기능
시스템 정보	WEBFRONT-K 장비의 이름이나 일련 번호, MAC 주소, 소프트웨어 버전 등의 기본적인 시스템 정보와 CPU와 메모리 등의 주요 자원의 현재 사용 상태, 그리고 시스템 온도, 냉각 팬 및 전원 공급기의 동작 상태 등 시스템 하드웨어의 상태 정보를 조회하는 메뉴입니다.
포트 모니터링	WEBFRONT-K의 이더넷 포트를 통해서 송수신되는 트래픽에 대한 정보를 실시간으로 모니터링하는 메뉴입니다.

## 통합 로그

통합 로그 메뉴는 로그에 관한 설정 작업을 하거나 WEBFRONT-K에 저장된 로그를 검색할 수 있는 하위 메뉴들로 구성 되어 있습니다.

메뉴	기능
통합 로그 설정	로그를 저장하고 로그를 외부의 시스로그 서버로 전송하는 데 필요한 설정 작업을 수행하는 메뉴입니다.
로그 내보내기	WEBFRONT-K에 저장된 로그를 관리자 PC로 다운로드하는 메뉴입니다.
보안로그	WEBFRONT-K에 설정된 웹 보안 규칙에 위배되는 경우, 패킷에 대한 정보와 어떤 규칙에 의해 위배되었는지 확인할 수 있는 메뉴입니다.
감사/시스템 로그	관리자가 WEBFRONT-K에서 조회하고 변경한 설정에 대한 정보를 확인할 수 있는 메뉴입니다.
방화벽 로그	WEBFRONT-K에 설정된 방화벽 정책에 위배되는 경우, 패킷에 대한 정보와 어떤 규칙에 의해 위배되었는지 확인할 수 있는 메뉴입니다.
접근 로그	WEBFRONT-K에서 수신한 웹 요청 패킷의 정보를 확인할 수 있는 메뉴입니다.

## AV2

WEBFRONT-K는 수집된 각종 보안 정보를 분석하여 다양한 종류의 상세 리포트와 추세 분석 리포트를 만들어 이를 관리자에게 일정 기간마다 자동으로 보내주는 리포팅 도구인 Analyzer를 제공합니다. Analyzer는 별도로 서버에 설치할 수 있는데, AV2 메뉴를 사용하여 Analyzer가 설치된 서버로 접속할 수 있습니다. Analyzer에 대한 정보는 [일반설정 - 리포터 설정] 메뉴에서 설정할 수 있습니다.

## 통합 보고서

통합 보고서는 WEBFRONT-K의 종합적인 정보를 요약하여 장비 현황과 네트워크 상태를 손쉽게 파악할 수 있는 기능입니다. 관리자는 보고서를 생성한 후 PDF, HTML, Word 형식의 파일로 다운로드 받을 수 있습니다.

## 애플리케이션

네트워크 메뉴는 애플리케이션 관리와 웹 보안 시그니처 관리에 관련된 하위 메뉴들로 구성되어 있습니다. 각 하위 메뉴를 사용하여 수행할 수 있는 작업은 다음과 같습니다.

메뉴	기능
애플리케이션 관리	애플리케이션을 등록하고, 등록된 애플리케이션을 삭제 혹은 수정할 수 있는 메뉴입니다. 애플리케이션을 등록하고 나면 Application 메뉴를 사용하여 애플리케이션에 대한 기본적인 설정 작업을 해주어야 하는 데, 애플리케이션 마법사를 사용하면 이러한 기본 설정 작업까지 함께 수행할 수 있습니다.
애플리케이션 설정 보기	WEBFRONT-K에 등록된 애플리케이션의 정보와 각 애플리케이션의 일반 설정, 요청 검사, 콘텐츠 보호, 위장 기능에 대한 설정 정보를 화면이나 파일로 출력하는 메뉴입니다.
애플리케이션 설정 간편화	WEBFRONT-K에 등록된 애플리케이션의 상태와 각 애플리케이션의 요청 검사, 콘텐츠 보호, 위장 기능의 상태를 한 화면에서 설정할 수 있는 메뉴입니다.
고급 첨부 파일 검사 설정	웹 서버에서 클라이언트로 전송되는 파일을 검사하여 고객 정보가 유출되는 것을 방지하는 고급 첨부 파일 검사를 설정하는 메뉴입니다.
시그니처 관리	시그니처를 최신 버전으로 업데이트하거나 시그니처의 적용 여부를 지정하는 메뉴입니다.
시그니처 내보내기	시그니처를 관리자 PC로 다운로드하는 메뉴입니다.
정규식 설정	애플리케이션 보안 기능을 설정할 때 정규식을 입력할 필요가 있는 경우에 편리하게 선택할 수 있도록 미리 정규식을 정의합니다.
블랙리스트관리	웹 공격을 자주 시도하는 클라이언트의 접근을 제한하기 위한 블랙리스트 기능을 설정하는 메뉴입니다.
화이트리스트관리	특정 클라이언트와 서버에 대해 보안 기능을 바이패스(Bypass)하는 화이트리스트 기능을 설정하는 메뉴입니다.

## 방화벽

방화벽 메뉴는 지정한 호스트에서만 WEBFRONT-K로 접근할 수 있도록 하는 시스템 접근 제어 기능과 WEBFRONT-K에 연결된 네트워크를 보호하기 위해 다양한 조건의 필터를 사용하여 불필요한 트래픽이 송수신되지 않도록 하는 방화벽 기능을 위한 하위 메뉴들로 구성되어 있습니다.

메뉴	기능
시스템 접근	시스템 접근 제어 기능을 사용하기 위해 시스템 접근 규칙을 정의하고, 정의된 시스템 접근 규칙을 수정하거나 삭제하고 시스템 접근 규칙의 적용 여부를 지정하는 메뉴입니다.
Snort	WEBFRONT-K를 통과하는 네트워크 트래픽이 유해트래픽인지 검사하기 위한 규칙을 설정하는 메뉴입니다.
컨텐츠	방화벽에서 특정 문자열을 가진 패킷을 필터링하기 위한 컨텐츠(content)를 정의하고, 정의된 컨텐츠를 수정하거나 삭제하는 메뉴입니다.
컨텐츠 그룹	방화벽에서 컨텐츠를 편리하게 관리할 수 있도록 여러 개의 컨텐츠를 하나의 컨텐츠 그룹으로 정의하는 메뉴입니다.
필터	방화벽에서 특정 출발지/목적지 IP 주소나 출발지/목적지 포트 번호, 프로토콜의 패킷이나 특정 컨텐츠나 컨텐츠 그룹의 조건을 만족하는 패킷을 필터링하기 위한 필터를 정의하는 메뉴입니다. 필터에는 이러한 조건들과 함께 패킷의 처리 방법(Accept, Drop, Reject, Rate Limit)이 포함됩니다.
필터 그룹	방화벽에서 필터를 편리하게 관리할 수 있도록 여러 개의 필터를 하나의 필터 그룹으로 정의하는 메뉴입니다.
정책	어떤 인터페이스에 어떤 필터나 필터 그룹을 적용할지를 나타내는 방화벽 정책을 정의하고, 정책을 활성화하거나 비활성화합니다. 방화벽 정책이 활성화되면 정책에 설정된 인터페이스를 통해 송수신되는 패킷을 정책의 필터나 필터 그룹의 조건에 따라 필터링합니다.

## 사용자 관리

사용자 관리는 WEBFRONT-K로 접속하여 WEBFRONT-K의 기능을 사용할 수 있는 사용자 계정을 관리하는 메뉴입니다. 사용자 관리 메뉴를 통해 새로운 사용자의 계정을 추가하거나 기존에 등록된 사용자 계정의 정보를 수정할 수 있고, 삭제할 수도 있습니다. 사용자에는 통합 관리자, 사이트 관리자, 애플리케이션 관리자, 모니터 관리자의 4가지 종류가 있는데, 통합 관리자는 4가지 종류의 사용자를 모두 관리할 수 있고, 사이트 관리자는 통합 관리자를 제외한 나머지 3가지 종류의 사용자를 관리할 수 있습니다.

## 일반설정

일반설정 메뉴는 가장 기본적인 WEBFRONT-K 시스템 설정과 관련된 하위 메뉴들로 구성되어 있습니다.

메뉴	기능
설정 관리	WEBFRONT-K의 설정(configuration)과 관련된 작업을 할 수 있는 메뉴입니다. 이 메뉴를 사용하여 부팅 후에도 현재 설정이 계속 유지될 수 있도록 SDRAM의 설정을 SSD로 저장하거나 백업을 위해 SSD에 저장된 설정을 사용자 PC의 하드 디스크로 저장할 수 있습니다. 그리고, 사용자 PC의 하드 디스크에 백업해둔 설정 파일을 다시 업로드하여 WEBFRONT-K의 설정으로 사용할 수도 있습니다. 이 밖에 WEBFRONT-K의 현재 설정을 모두 삭제하고 출하 시 기본 설정으로 복구하는 것도 이 메뉴를 통해 할 수 있습니다.
기술 지원 도우미	WEBFRONT-K의 장애 발생 원인을 분석하기 위한 시스템 동작 로그 정보를 다운로드할 수 있는 메뉴입니다.
서버장애 감시	등록된 애플리케이션 서버의 통신 상태를 주기적으로 확인하고 결과를 보여주는 메뉴입니다.
시스템 감시	WEBFRONT-K의 주요 자원인 CPU와 메모리, 포트의 사용 상태를 감시하는 시스템 감시 기능을 설정하는 메뉴입니다. 시스템 감시 기능의 사용 여부와 이상 여부를 판단하는 기준인 임계값을 지정할 수 있습니다.
SNMP	SNMP 상태와 SNMP 관련 정보(시스템 정보), SNMP 트랩 및 SNMP 에이전트를 설정할 수 있는 메뉴입니다.
라이선스 관리	WEBFRONT-K의 유지보수 라이선스를 관리하기 위한 메뉴입니다.
국가별 IP	웹 서버로 접근하는 클라이언트 IP 주소의 국가를 확인할 수 있는 국가별 IP 주소 파일을 업데이트할 수 있는 메뉴입니다.

PLOS 관리	WEBFRONT-K에 설치된 PLOS를 다른 버전으로 업그레이드할 수 있는 메뉴입니다.
시간 관리	WEBFRONT-K의 시간과 관련된 설정을 위한 메뉴입니다. 직접 WEBFRONT-K의 시간을 지정하거나 WEBFRONT-K가 시간을 동기화할 NTP 서버를 지정할 수 있고, WEBFRONT-K를 사용 중인 지역에 맞도록 시간대를 변경할 수 있습니다.
DNS 관리	WEBFRONT-K에서 IP 주소 대신 호스트 이름을 활용하기 위해 DNS 서버를 등록할 수 있는 메뉴입니다.
리포터 설정	외부에 설치된 Analyzer에 접속하는 데 필요한 설정 작업을 하는 메뉴입니다. 리포터 사용 여부와 리포터 접속 및 통신에 필요한 정보를 설정할 수 있습니다.
E-mail 알람	관리자 로그인 실패, 로그 저장소(HDD) 포화, 무결성 손상, 웹 변조 방지 기능에 의한 웹 페이지 변조 탐지 시 관리자에게 경고 메일을 발송하기 위한 메뉴입니다.
무결성 검사	WEBFRONT-K 자체의 보안성을 조사하기 위해 WEBFRONT-K의 설정 정보와 동작 중인 프로그램이 비정상적으로 변조되었는지를 검사하여 이상 여부를 판단합니다.
환경변수	프록시 ARP, 저장 MAC 응답, HTTP 파라미터, 부팅 중 포트 상태, TOS 기능을 설정하는 메뉴입니다.
통계 기간 설정	WEBFRONT-K의 모니터링 기능 및 보고서의 근거 데이터가 되는 통계 데이터의 저장 기간을 설정할 수 있는 메뉴입니다.
시스템 관리 설정	WEBFRONT-K와 관리자 PC 사이의 통신에 사용되는 SSL 프로토콜과 암호 알고리즘을 설정할 수 있는 메뉴입니다.
호스트이름 설정	WEBFRONT-K의 호스트 이름을 설정하는 메뉴입니다. 호스트 이름은 EMS나 NMS에서 WEBFRONT-K를 구분하거나 텔넷 등을 통해 WEBFRONT-K에 접속했을 때 어떤 장비에 접속했는지 나타낼 때 사용됩니다.
시스템 재시작	WEBFRONT-K 장비를 원격으로 리부팅합니다.

## 네트워크

네트워크 메뉴는 포트와 네트워크 설정에 관련된 하위 메뉴들로 구성되어 있습니다. 각 하위 메뉴를 사용하여 수행할 수 있는 작업은 다음과 같습니다.

메뉴	기능
포트 바운더리	수신되는 패킷 중 보안 엔진에서 처리할 패킷을 지정하기 위한 포트 바운더리를 설정하는 메뉴입니다.
IP 주소	VLAN 인터페이스의 IP 주소와 기본 게이트웨이, 고정 경로를 설정하는 메뉴입니다.
VLAN	VLAN을 설정하고 각 포트의 PVID를 지정하는 메뉴입니다.
포트	WEBFRONT-K 기가빗 이더넷 포트의 속도, 전송 모드(duplex), MDI/MDIX, 흐름 제어, Admin 상태(사용 여부)를 지정하는 메뉴입니다.
링크싱크	모니터 포트와 싱크 포트를 감시하여 링크 상태를 동기화하기 위한 링크싱크를 설정하는 메뉴입니다.
미러링	특정 포트에 송수신되는 모든 패킷들의 복사본을 다른 포트에 전달하는 포트 미러링 기능을 사용하기 위해 필요한 설정 작업을 하는 메뉴입니다.
트렁킹	트렁크 그룹으로 사용할 포트와 트렁크 그룹에 속한 포트에 트래픽을 분산할 부하 분산 알고리즘을 지정하는 메뉴입니다. 트렁킹 방식에 따라 포트 트렁킹과 LACP를 설정할 수 있습니다.
STP	각 VLAN별로 STP를 설정하는 메뉴입니다.
ARP	WEBFRONT-K의 ARP 테이블에 특정 IP 주소에 대한 MAC 주소를 수동으로 매핑하여 저장하는 메뉴입니다.

## HA

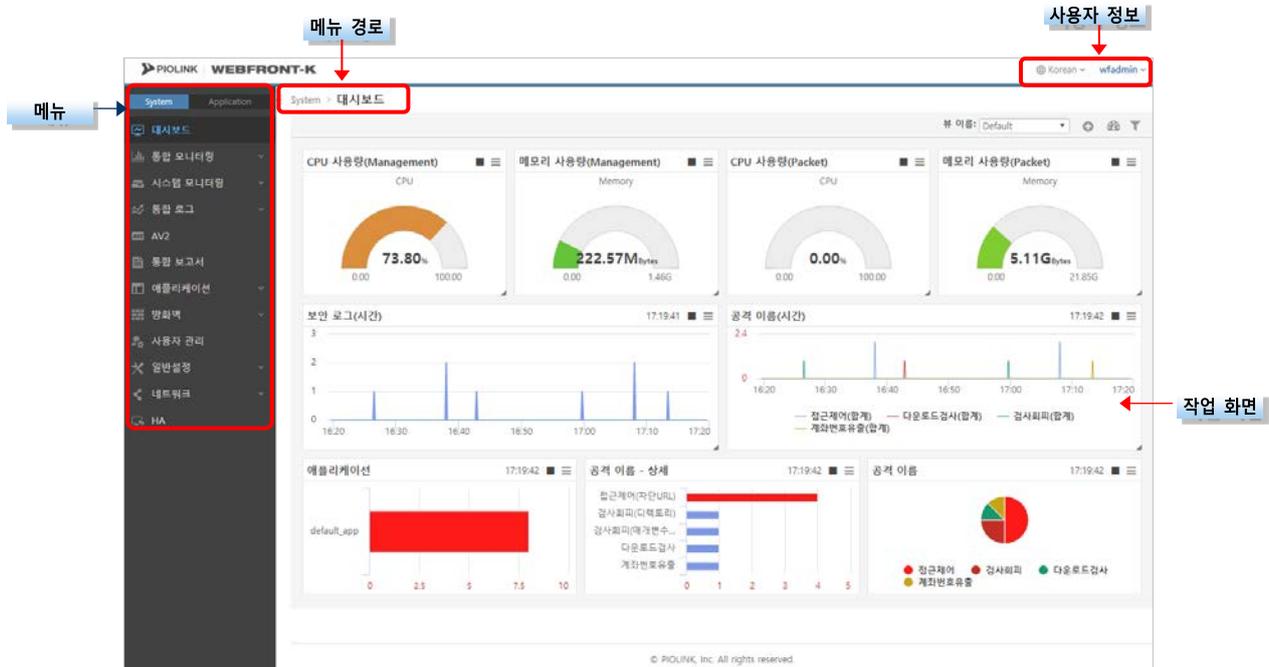
WEBFRONT-K는 안정적인 서비스를 제공하기 위해 2대를 사용하여 이중화(redundancy)할 수 있습니다. HA 메뉴는 WEBFRONT-K를 이중화했을 때 사용하는 메뉴로, WEBFRONT-K의 Failover 정보에 필요한 설정 작업을 할 수 있습니다.

# WEBFRONT-K Web Manager 화면 구성

이 절에서는 WEBFRONT-K Web Manager 메인 화면의 구성과 메뉴를 선택했을 때 볼 수 있는 각종 설정 화면들의 구성에 대해 살펴봅니다.

## 메인 화면

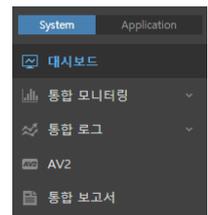
- 다음은 WEBFRONT-K Web Manager 메인 화면을 구성하는 부분들입니다. 이 부분은 어떤 메뉴가 선택되더라도 사라지지 않고 항상 화면에 표시되기 때문에 언제든지 사용할 수 있습니다.



각 부분의 기능을 메뉴에서부터 시작하여 시계 반대 방향으로 차례로 살펴봅니다.

### 메뉴

시스템 관리 및 네트워크 기능을 설정할 수 있는 메뉴들입니다. WEBFRONT-K에는 일반 메뉴 모드와 고급 메뉴 모드가 있는데, 고급 메뉴 모드일 때에는 모든 메뉴가 모두 나타나고, 일반 메뉴 모드로 설정한 경우에는 오른쪽과 같은 메뉴만 나타납니다.



### 작업 화면

선택한 메뉴에 대한 작업을 수행할 수 있는 부분입니다. 선택한 메뉴에 따라 다른 화면이 나타납니다.

### 사용자 정보

현재 WEBFRONT-K로 로그인한 사용자의 ID를 보여주고 로그아웃(Logout)하거나 혹은 사용자 환경을 설정(Preference)할 수 있는 부분입니다. Preference를 클릭하면 사용자 환경을 설정할 수 있는데, 기본 메뉴 모드와 로그인 암호를 변경할 수 있습니다. 사용자 환경을 설정하는 방법은 이 장의 '사용자 환경 설정하기' 절을 참고합니다.

### 메뉴 경로

사용자가 선택한 메뉴를 보여주는 부분입니다. 네트워크 메뉴에서 IP 주소 메뉴를 선택한 경우에는 오른쪽 그림과 같이 메뉴 경로가 표시됩니다. 설정 작업을 하다 보면 어떤 메뉴를 선택하였는지 혼동될 때가 있습니다. 이럴 때 메뉴 경로를 참고하면 선택한 메뉴를 바로 알 수 있습니다.

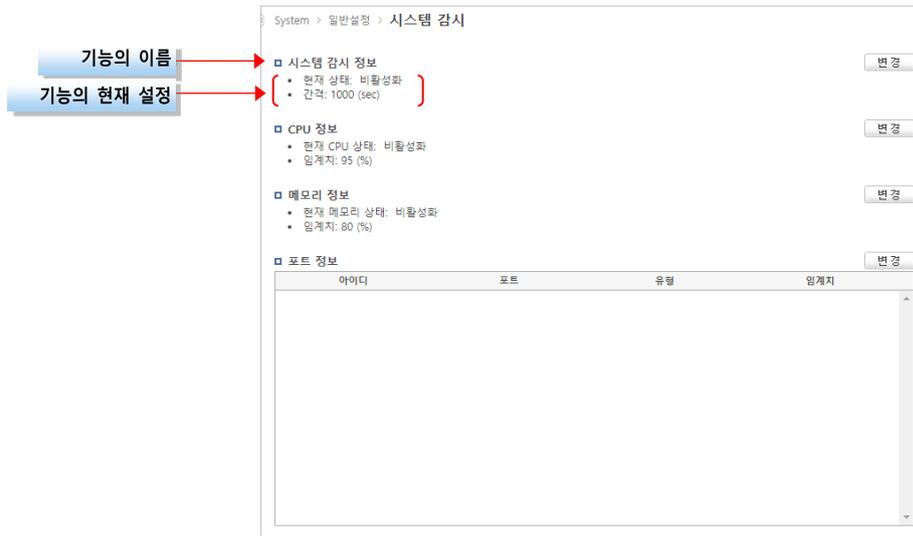


## 설정 화면

WEBFRONT-K의 기능을 사용하면서 사용자가 볼 수 있는 각종 화면의 구성에 대해 살펴봅니다.

### 현재 상태 화면

메인 화면에서 메뉴를 선택하면 작업 화면은 선택한 메뉴의 기능을 수행할 수 있는 화면으로 바뀝니다. 일반적으로 메뉴를 클릭하면 현재의 상태를 보여주는 다음과 같은 형태의 화면이 나타납니다.



위 화면은 **일반설정 - 시스템 감시** 메뉴를 클릭했을 때 나타나는 화면입니다. 위 화면을 통해 시스템 감시 기능은 총 4가지 기능으로 구성되어 있고, 현재 각 기능은 모두 비활성화 상태이고 설정된 포트 정보가 없음을 알 수 있습니다.

### 설정 변경 화면

현재 설정을 변경하려면 각 기능의 오른쪽에 있는 **[변경]** 버튼을 클릭해야 합니다. 그러면, 기능에 따라 다른 형태의 화면이 나타납니다.

#### 항목의 값을 변경하는 화면

앞의 그림에서 시스템 감시 정보나 CPU 정보와 오른쪽과 같이 항목의 값을 변경하는 경우에는 팝업 창이 나타납니다.



#### 리스트 화면

포트 정보와 같이 여러 항목으로 구성된 '리스트'인 경우에는 **[변경]** 버튼을 클릭하면 작업 화면이 다음과 같이 바뀝니다.



항목을 추가하는 경우에는 [추가] 버튼을, 수정하거나 삭제하는 경우에는 리스트에서 항목을 선택한 후 [수정] 혹은 [삭제] 버튼을 클릭하면 됩니다. [추가] 버튼을 클릭하면 항목의 값을 지정할 수 있는 팝업 창이 나타납니다.



팝업 창의 항목들을 설정한 후에는 [확인]을 클릭해야 합니다. 그러면, 입력한 항목이 리스트에 추가됩니다. 일반적으로 추가 팝업 창에 있는 항목 중에서 설명 항목은 값을 입력하지 않아도 됩니다. 나머지 항목들은 기본 값이 설정되어 있는 경우를 제외하고는 대부분 필수적으로 설정해야 합니다.

리스트에서 항목을 선택할 때에는 항목을 왼쪽 마우스 버튼으로 한번 클릭하면 됩니다. 선택된 항목은 하늘색으로 표시 됩니다. 선택된 항목을 다시 한번 클릭하면 선택이 해제됩니다. 여러 항목을 선택하는 경우에는 상황에 따라 [Ctrl] 키나 [Shift] 키를 사용하도록 합니다.

- 연속적인 여러 항목을 선택하는 경우  
첫 항목을 클릭한 후 [Shift] 키를 누른 상태에서 마지막 항목을 클릭합니다.
- 연속적이지 않은 여러 항목을 선택하는 경우  
[Ctrl] 키를 누른 상태에서 원하는 항목을 계속 클릭합니다.

## 버튼

설정 화면은 항목들과 함께 여러 개의 버튼으로 구성되어 있습니다. 다음은 설정 화면에서 볼 수 있는 버튼들의 기능입니다.

버튼	기능
	[추가] 버튼은 리스트에 새로운 항목을 추가할 때 사용합니다. [추가] 버튼을 클릭하면, 해당 항목을 추가할 수 있는 팝업 창이 나타납니다.
	[수정] 버튼은 리스트에 추가되어 있는 하나의 항목을 수정할 때 사용합니다. 리스트에서 수정할 항목을 선택한 후 [수정] 버튼을 클릭하면, 선택한 항목을 수정할 수 있는 팝업 창이 나타납니다.   <b>참고:</b> 수정 팝업 창의 항목은 [추가] 버튼을 클릭했을 때 나타나는 팝업 창의 항목과 동일하기 때문에 이 설명서는 수 화면에 나타나는 항목들을 따로 설명하지 않습니다. 항목을 수정하는 경우에는 해당 항목을 추가하는 부분의 설명 참고하도록 합니다.
	[삭제] 버튼은 리스트에 추가되어 있는 항목(들)을 삭제할 때 사용합니다. 리스트에서 항목(들)을 선택한 후 [삭제] 버튼을 클릭하면 선택한 항목(들)이 삭제됩니다.
	[적용] 버튼은 항목의 값을 지정하거나 변경한 후 이를 WEBFRONT-K에 적용할 때 사용합니다.
	[취소] 버튼은 지정하거나 변경한 항목의 값을 무시하고 이전 화면으로 돌아가고자 할 때 사용합니다.
	[리셋] 버튼은 항목의 값을 이전 설정(팝업 창이 나타났을 때 표시되었던 값)으로 설정하고자 할 때 사용합니다. 이 버튼을 클릭한 후에는 반드시 [적용] 버튼을 클릭해야 합니다.
	설정을 저장한 후 이전 화면으로 돌아가려는 경우에 이 버튼을 클릭합니다.

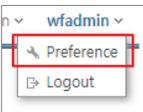
# 사용자 환경 설정하기

이 절에서는 사용자가 쉽게 메뉴를 실행할 수 있게 해주는 바로가기를 설정하거나 메뉴 모드와 로그인 암호, 로그인 유지 시간을 변경하는 방법에 대해 알아봅니다.

## 기본 메뉴 모드 설정

사용자 계정으로 로그인했을 때 표시되는 메뉴의 종류는 기본 메뉴 모드에 따라 결정됩니다. 기본 메뉴 모드에는 고급 설정 모드와 일반 모드가 있는데, 고급 설정 모드를 선택하면 모든 메뉴가 나타나고, 일반 모드를 선택하면 모니터링 메뉴만 나타납니다. 설정 작업을 끝내고 상태 정보와 통계 정보 등을 보려는 경우에는 일반 모드를 사용하면 메뉴가 단순해져서 사용하기가 편리합니다. 기본으로 지정된 메뉴 모드는 고급 설정 모드입니다.

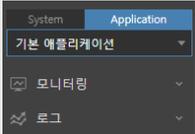
기본 메뉴 모드를 지정하는 방법을 다음과 같습니다.

순서	설정 과정
1	<p>WEBFRONT-K 화면의 오른쪽 위에 있는 드롭다운 목록에서 <b>Preference</b>를 클릭합니다.</p> 
2	<p>&lt;기본 메뉴 모드&gt;의 [변경] 버튼을 클릭합니다.</p>
3	<p>&lt;기본 시작 메뉴 모드 변경&gt; 화면에서 고급 설정 모드와 일반 모드 중에서 하나를 선택한 후 [적용] 버튼을 클릭합니다.</p> 

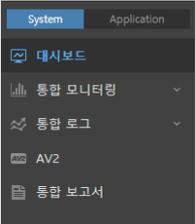


**참고:** 메뉴 모드는 다음 로그인부터 적용됩니다. 일반 모드로 설정한 경우 로그아웃한 후 같은 사용자 계정을 사용하여 다시 로그인하면, 메뉴가 다음과 같이 일반 모드 형태로 나타납니다.

일반 메뉴 모드일 때의 Application 메뉴:



일반 메뉴 모드일 때의 System 메뉴:



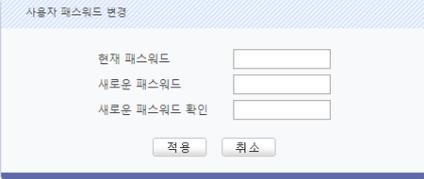
## 로그인 유지 시간 설정

WEBFRONT-K는 지정한 시간(로그인 유지 시간) 동안 사용자의 입력이 없을 경우 자동으로 로그아웃되는 기능을 제공합니다. 로그인 유지 시간을 변경하는 방법은 다음과 같습니다. 변경한 로그인 유지 시간은 다음 로그인시부터 적용됩니다.

순서	설정 과정
1	WEBFRONT-K 화면의 오른쪽 위에 있는 드롭다운 목록에서 <b>Preference</b> 를 클릭합니다.
2	<로그인 유지 시간>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;로그인 유지 시간 변경&gt; 화면의 시간 항목에 설정할 로그인 시간을 입력한 후 [적용]을 클릭합니다. '0'을 입력하면 로그인 시간이 제한되지 않습니다.</p> <div style="text-align: center;">  </div> <p> <ul style="list-style-type: none"> <li>• GUI 제한 시간 Web Manager 에서 사용자 입력이 없어도 로그인을 유지시킬 시간 간격을 입력합니다. '0'을 입력하면 사용자 입력이 없어도 자동으로 로그아웃되지 않습니다. (설정 범위: 0~1440, 기본값 5분)</li> <li>• 터미널 제한 시간 콘솔 접속 화면에 대해 사용자 입력이 없어도 로그인을 유지시킬 시간 간격을 입력합니다. '0'을 입력하면 사용자 입력이 없어도 자동으로 로그아웃되지 않습니다. (설정 범위: 0~65535, 기본값 5분)</li> </ul> </p>

## 로그인 암호 변경

현재 로그인한 사용자 계정의 암호를 변경하는 방법은 다음과 같습니다.

순서	설정 과정
1	WEBFRONT-K 화면의 오른쪽 위에 있는 드롭다운 목록에서 <b>Preference</b> 를 클릭합니다.
2	<패스워드 변경>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;사용자 패스워드 변경&gt; 팝업 창에서 다음 설명을 참고하여 각 항목에 값을 입력하고 [적용] 버튼을 클릭합니다. 화면에는 입력한 암호가 점(•)으로 표시되기 때문에 바르게 입력하였는지 확인할 수 없으므로 주의를 기울여서 입력합니다.</p> <div style="text-align: center;">  </div> <p> <ul style="list-style-type: none"> <li>• 현재 패스워드 현재 사용하고 있는 패스워드</li> <li>• 새로운 패스워드 알파벳 대문자, 소문자, 숫자, 특수문자 중 3가지 이상의 조합으로 9~20자의 문자열을 입력</li> <li>• 새로운 패스워드 확인 새로운 패스워드를 한번 더 입력</li> </ul> </p>

## 제2장 대시보드

이 장에서는 WEBFRONT-K의 하드웨어 및 애플리케이션 상태를 실시간으로 확인할 수 있는 대시보드에 대해 설명합니다.

이 장은 다음 내용으로 구성됩니다.

- 대시보드 사용하기



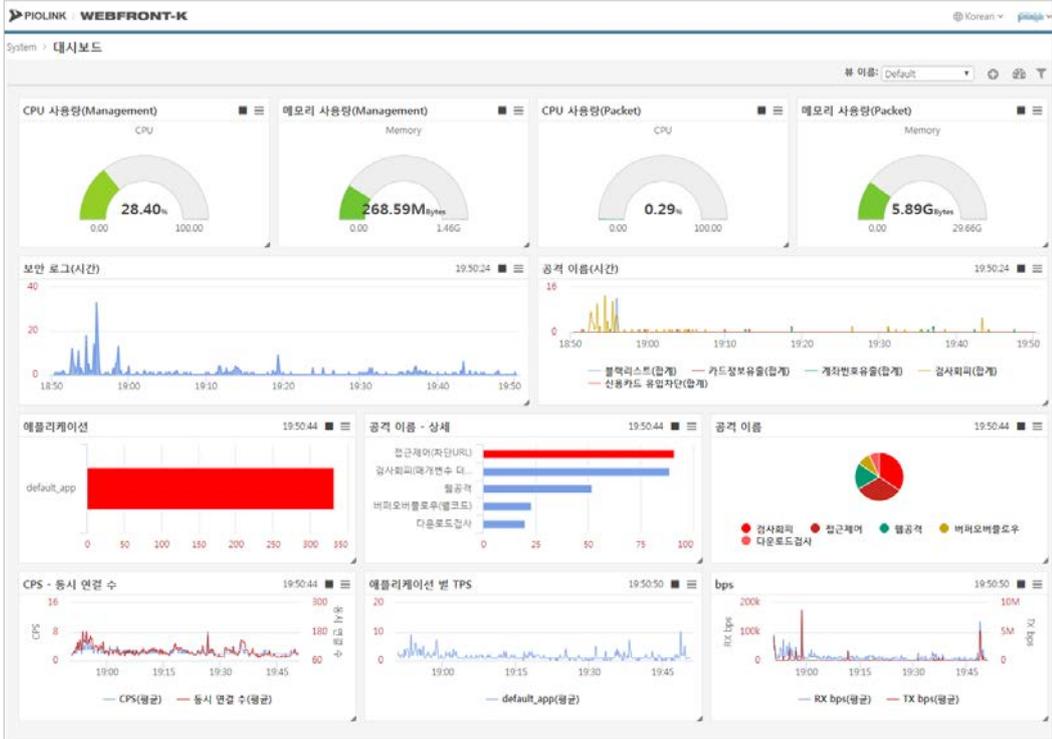
# 개요

WEBFRONT-K에 로그인하면 대시보드(Dashboard)가 시작 화면으로 출력됩니다. 대시보드는 WEBFRONT-K와 WEBFRONT-K에 의해 보호되고 있는 애플리케이션의 현재 상태를 실시간으로 보여주는 기능입니다. 사용자는 대시보드에 표시된 정보를 통해 빠르게 WEBFRONT-K 및 애플리케이션의 상태를 파악할 수 있고, 필요한 경우 적절한 조치를 즉시 취할 수 있습니다.

## 대시보드 사용하기

### 기본 대시보드

대시보드에는 WEBFRONT-K 하드웨어의 상태와 최근 1시간 동안의 공격 정보, 애플리케이션의 정보 등이 표시됩니다. WEBFRONT-K에서 기본적으로 제공하는 대시보드를 조회하는 방법을 설명합니다.

순서	설정 과정															
1	<p><b>System - 대시보드</b> 메뉴를 클릭합니다.</p> <p>다음은 WEBFRONT-K 대시보드의 초기 화면(뷰)입니다.</p>  <p>The screenshot shows a dashboard with several panels: CPU and Memory usage (Management and Packet), Security logs (보안 로그(시간) and 공격 이음(시간)), Application status (애플리케이션), Attack types (공격 이음 - 상세), CPS and TPS (CPS - 동시 연결 수, 애플리케이션 별 TPS), and Network traffic (bps). A legend at the bottom right identifies attack types like 검사회피, 침입탐지, etc.</p>															
2	<p>관리자는 WEBFRONT-K 대시보드를 구성하고 있는 각각의 패널을 드래그 앤 드롭(Drag &amp; drop)하여 원하는 뷰(View)로 변경할 수 있습니다. 또한 대시보드 항목을 추가하거나 삭제할 수 있습니다.</p> <p>다음은 대시보드 우측 상단의 4개 항목에 대한 설명입니다.</p> <table border="1"> <thead> <tr> <th>항목</th> <th>이름</th> <th>설명</th> </tr> </thead> <tbody> <tr> <td></td> <td>뷰 이름: Default</td> <td>드롭다운 버튼을 클릭하여 뷰 선택 (기본값: Default)</td> </tr> <tr> <td></td> <td>패널 추가</td> <td>패널을 추가할 수 있는 버튼</td> </tr> <tr> <td></td> <td>뷰</td> <td>뷰를 추가, 수정 삭제할 수 있는 버튼</td> </tr> <tr> <td></td> <td>필터</td> <td>필터를 추가, 수정, 삭제할 수 있는 버튼</td> </tr> </tbody> </table> <p>다음은 패널 우측 상단의 2개 항목에 대한 설명입니다.</p>	항목	이름	설명		뷰 이름: Default	드롭다운 버튼을 클릭하여 뷰 선택 (기본값: Default)		패널 추가	패널을 추가할 수 있는 버튼		뷰	뷰를 추가, 수정 삭제할 수 있는 버튼		필터	필터를 추가, 수정, 삭제할 수 있는 버튼
항목	이름	설명														
	뷰 이름: Default	드롭다운 버튼을 클릭하여 뷰 선택 (기본값: Default)														
	패널 추가	패널을 추가할 수 있는 버튼														
	뷰	뷰를 추가, 수정 삭제할 수 있는 버튼														
	필터	필터를 추가, 수정, 삭제할 수 있는 버튼														

항목	이름	설명
	정지	해당 패널의 동작 정지 버튼
	닫기	패널 닫기 버튼. 해당 아이콘 후, close 버튼을 클릭하면 패널이 닫힘.

다음은 대시보드의 패널에 대한 설명입니다.

- CPU 사용량(Management)                      장비 관리에 대한 CPU의 사용량
- 메모리 사용량(Management)              장비 관리에 대한 메모리 사용량
- CPU 사용량(Packet)                          패킷 처리에 대한 CPU 사용량
- 메모리 사용량(Packet)                      패킷 처리에 대한 메모리 사용량
- 보안 로그(시간)                              최근 1시간 동안 발생한 보안 로그
- 공격 이름(시간)                              탐지한 공격
- 애플리케이션                                  (시간 확인) 공격당한 애플리케이션
- 공격 이름 - 상세                              상세한 공격 이름
- 공격 이름                                      공격 이름
- CPS - 동시 연결 수                          최근 1시간 동안의 초당 커넥션 수
- 애플리케이션 별 TPS                      애플리케이션 별 초당 트랜잭션 수
- bps    최근 1시간 동안 송수신된 초당 비트 수

## 사용자 정의 대시보드

WEBFRONT-K는 기본으로 제공하는 대시보드 외에 사용자 정의 대시보드 생성 기능을 제공하여, 다양한 종류의 패널을 추가하거나 삭제, 수정할 수 있고 각 패널의 배치와 크기를 조절할 수 있습니다.



**참고:** 대시보드 설정 저장은 별도로 동작하여 **System - 일반설정 - 설정 관리** 메뉴 기능을 적용받지 않습니다. 이에 따라 대시보드 설정은 설정 초기화, 설정 동기화 기능에서 제외됩니다.

### 대시보드 뷰 추가

사용자 정의 대시보드를 추가하는 방법을 설명합니다.

순서	설정 과정
1	<b>System - 대시보드</b> 메뉴를 클릭합니다.
2	오른쪽 상단 메뉴에서  (뷰 추가) 아이콘을 클릭합니다.
3	메뉴를 선택하는 팝업 창이 나타나면 <b>[추가]</b> 를 클릭합니다.
4	<p>&lt;뷰(추가)&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 <b>[적용]</b> 버튼을 클릭합니다.</p> <div style="text-align: center;"> </div> <ul style="list-style-type: none"> <li><b>뷰 이름</b> 새로 생성할 대시보드 이름을 입력합니다.</li> <li><b>Default</b> 기본 대시보드로 지정합니다. 기본 대시보드로 지정시 WEBFRONT-K에 로그인하면 시작 화면으로 출력됩니다.</li> </ul> <p> <b>참고:</b> 새로 생성된 대시보드의 패널 구성은 기본 대시보드와 같습니다. 새로운 패널을 추가하려면 다음 절의 <b>대시보드 패널 추가</b> 절을 참고합니다.</p>

### 대시보드 패널 추가

WEBFRONT-K는 모니터링할 주요 정보를 패널 형태로 제공하고 있으며, 사용자는 다양한 종류의 패널을 구성할 수 있습니다. 각 대시보드에 패널을 추가하는 방법을 설명합니다.

순서	설정 과정
1	<b>System - 대시보드</b> 메뉴를 클릭합니다.
2	오른쪽 상단에 있는 <b>뷰 이름</b> 메뉴에서 드롭다운 목록을 클릭한 후, 대시보드 이름을 선택합니다.
3	오른쪽 상단에 있는  (패널 추가) 아이콘을 클릭합니다.
4	패널 화면에서  아이콘을 클릭합니다.
5	<내용 추가> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 <b>[적용]</b> 버튼을 클릭합니다.

내용 추가
✕

이름:

공격/트래픽/리소스:  
 공격  트래픽  리소스

데이터:

합계  평균

차트 / 데이터 테이블:  
 차트  데이터 테이블

차트 종류(합계):

차트 종류(평균):

3D 차트

최근:

간격:

평균 시간:

갱신:

필터 이름:

범례 수:

- **이름**      패널의 이름을 설정합니다. 이름은 패널 화면 맨 위에 표시되며 입력하지 않으면 '데이터' 항목 이름이 표시됩니다.
- **공격/트래픽/리소스**  
 패널의 유형을 지정합니다. 지정 값에 따라 다음 설정 메뉴가 활성화 또는 비활성화됩니다.
  - 공격: WEBFRONT-K에서 탐지 및 차단한 웹 공격 정보를 제공하는 패널입니다.
  - 트래픽: WEBFRONT-K 인터페이스를 통해 처리된 트래픽 정보를 제공하는 패널입니다.
  - 리소스: WEBFRONT-K 시스템 상태 정보를 제공하는 패널입니다.
- **데이터**  
 패널에 표시될 데이터 종류와 값(합계/평균)의 형식을 선택합니다. 데이터는 바로 위에서 지정한 **공격/트래픽/리소스** 지정 값에 따라 선택할 수 있는 목록이 나타납니다.

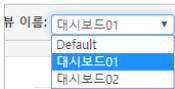
공격/트래픽/리소스	데이터
공격	<ul style="list-style-type: none"> <li>• 보안 로그(시간)</li> <li>• 공격 이름(시간)</li> <li>• 공격 이름 - 상세 (시간)</li> <li>• 공격 이름</li> <li>• 공격 이름 - 상세</li> <li>• 애플리케이션</li> </ul>
트래픽	<ul style="list-style-type: none"> <li>• CPS</li> <li>• 애플리케이션 별 CPS</li> <li>• CPS - 동시 연결 수</li> <li>• TPS</li> <li>• 애플리케이션 별 TPS</li> <li>• bps</li> <li>• 캐시 히트율</li> <li>• 캐시 수</li> </ul>
리소스	<ul style="list-style-type: none"> <li>• CPU 사용량</li> <li>• 메모리 사용량</li> <li>• 저장공간 사용량</li> <li>• CPU 사용량 (Management)</li> <li>• CPU 사용량 (Packet)</li> <li>• 메모리 사용량 (Management)</li> <li>• 메모리 사용량 (Packet)</li> </ul>

- 합계: 패널에 간격 별 합계를 표시합니다.
- 평균: 패널에 간격 별 평균 값을 표시합니다.
- **차트/데이터 테이블**  
 데이터 표시 방법을 차트와 데이터 테이블 중에서 선택합니다.
- **차트 종류(합계), 차트 종류(평균)**  
 차트 종류를 선택합니다. **데이터** 지정 값에 따라 선택할 수 있는 목록이 나타납니다.
  - Spline, Line, Column, Area spline, Area, Pie, Bar
- **3D 차트**  
 3D 차트로 출력할지 여부를 선택합니다.
- **최근**  
 대상 데이터의 기간을 지정합니다. 최근 [1분, 5분, 10분, 30분, 1시간, 6시간, 12시간, 1일] 동안의 데이터로 차트 및 테이블을 생성합니다.

• <b>간격</b>	패널의 차트/데이터 테이블에 데이터를 표시할 간격을 지정합니다. (기본 값: 10초)
• <b>평균 시간</b>	차트/데이터 테이블 생성 평균 시간을 지정합니다. '데이터' 항목이 '평균'인 경우에만 선택할 수 있습니다. (기본 값: 1초)
• <b>갱신</b>	패널의 업데이트 주기를 지정합니다. (설정 범위: 5초, 10초, 30초, 1분, 5분, 10분, 기본 값: 5초)
• <b>필터 이름</b>	필터를 선택합니다.
• <b>범례 수</b>	차트/테이블에 표시할 범례 수를 지정합니다.

## 대시보드 필터 추가

대시보드 필터를 추가하는 방법을 설명합니다.

순서	설정 과정
1	<b>System - 대시보드</b> 메뉴를 클릭합니다.
2	오른쪽 상단에 있는 <b>뷰 이름</b> 메뉴에서 드롭다운 목록을 클릭한 후, 대시보드 이름을 선택합니다. 
3	오른쪽 상단에 있는  (필터) 아이콘을 클릭합니다.
4	<필터 추가(추가)> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 <b>[적용]</b> 버튼을 클릭합니다.  <ul style="list-style-type: none"> <li>• <b>필터 이름</b> 필터 이름을 선택합니다.</li> <li>• <b>필터 이름</b> 필터 이름을 입력합니다.</li> <li>• <b>필터 종류</b> 필터 종류를 선택합니다. <ul style="list-style-type: none"> <li>- 공격: WEBFRONT-K에서 탐지 및 차단한 웹 공격 정보</li> <li>- 트래픽: WEBFRONT-K 인터페이스를 통해 처리된 트래픽 정보</li> </ul> </li> <li>• <b>애플리케이션</b> 애플리케이션을 선택합니다.</li> <li>• <b>공격 이름</b> 공격 이름을 선택합니다.</li> </ul>

## 제3장 통합 모니터링

통합 모니터링은 일정 기간 동안 모니터링한 WEBFRONT-K의 트래픽 양과 보안 기능에 대한 정보를 보여줍니다. 통합 모니터링을 통해 볼 수 있는 정보는 다음과 같습니다.

- WEBFRONT-K의 인터페이스를 통해 송수신된 트래픽의 양
- WEBFRONT-K에 등록된 애플리케이션에 취해진 웹 공격 횟수
- 요청 검사 기능을 통해 차단된 웹 공격 횟수
- 콘텐츠 보호 기능을 통해 차단된 웹 공격 횟수
- 학습 기능을 통해 학습된 정보 개수
- 위장 기능을 통해 변경된 정보 개수

WEBFRONT-K는 위 정보들을 한꺼번에 보여주는 시스템 통합 모니터링 기능과 각 보안 기능별로 모니터링 정보를 보다 상세하게 조회할 수 있는 상세 모니터링 기능을 제공합니다. 시스템 통합 모니터링 화면에서는 최근 25분 동안 수집된 모든 종류의 정보를 볼 수 있습니다. 상세 모니터링 화면에서는 각 기능에 대해 최근 일주일 동안 수집된 정보 중에서 특정한 기간이나 특정 애플리케이션의 특정 기능에 대한 정보만 따로 출력할 수 있어 사용자가 필요로 하는 정보만 필터링하여 볼 수 있습니다.

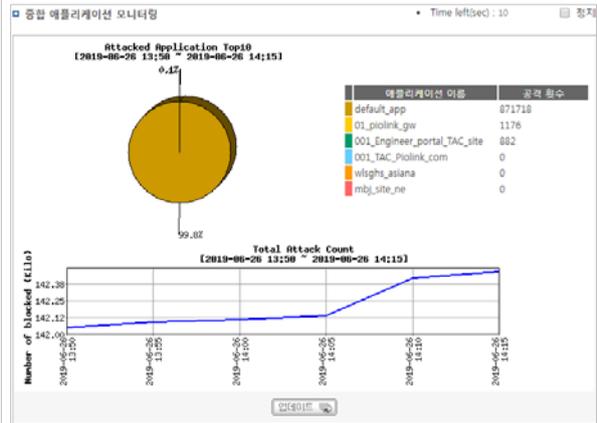
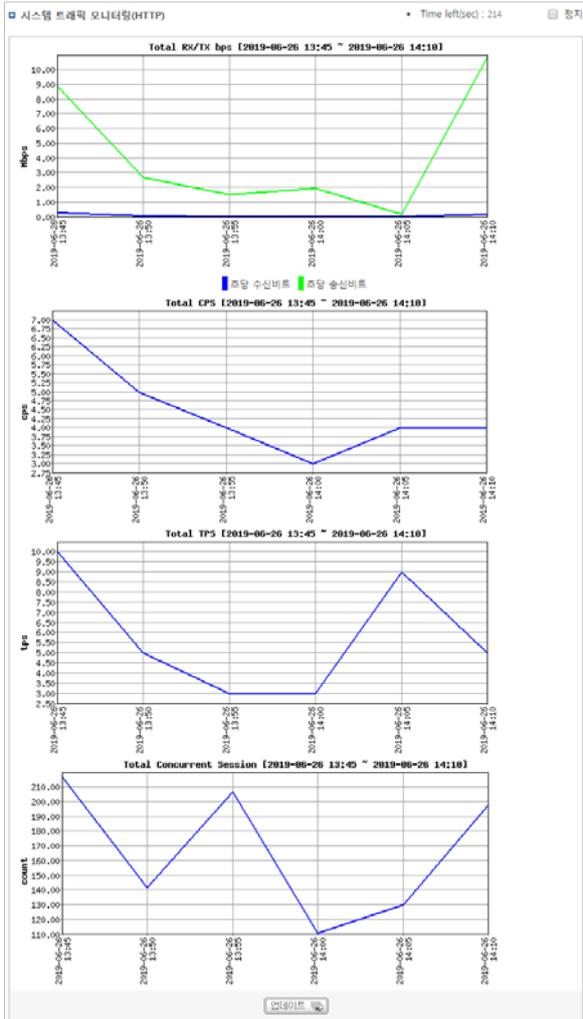
이 장은 다음 내용으로 구성됩니다.

- 시스템 통합 모니터링
- 요청 검사 모니터링
- 콘텐츠 보호 모니터링
- 학습 모니터링
- 위장 모니터링

The logo for PIOLINK, featuring the word "PIOLINK" in a large, bold, sans-serif font. The letters are light gray and have a subtle shadow effect, giving them a three-dimensional appearance. The logo is positioned on the right side of the page, partially overlapping the list of contents.

# 시스템 통합 모니터링

최근 25분 동안 WEBFRONT-K를 통해 송수신된 트래픽의 양과 각 웹 보안 기능에 의해 차단된 웹 공격에 대한 정보를 출력하려면 **System** 메뉴에서 **통합 모니터링 - 시스템 통합 모니터링** 메뉴를 클릭합니다. 시스템 트래픽 정보와 웹 공격에 대한 정보(일부)를 보여주는 화면이 나타납니다.

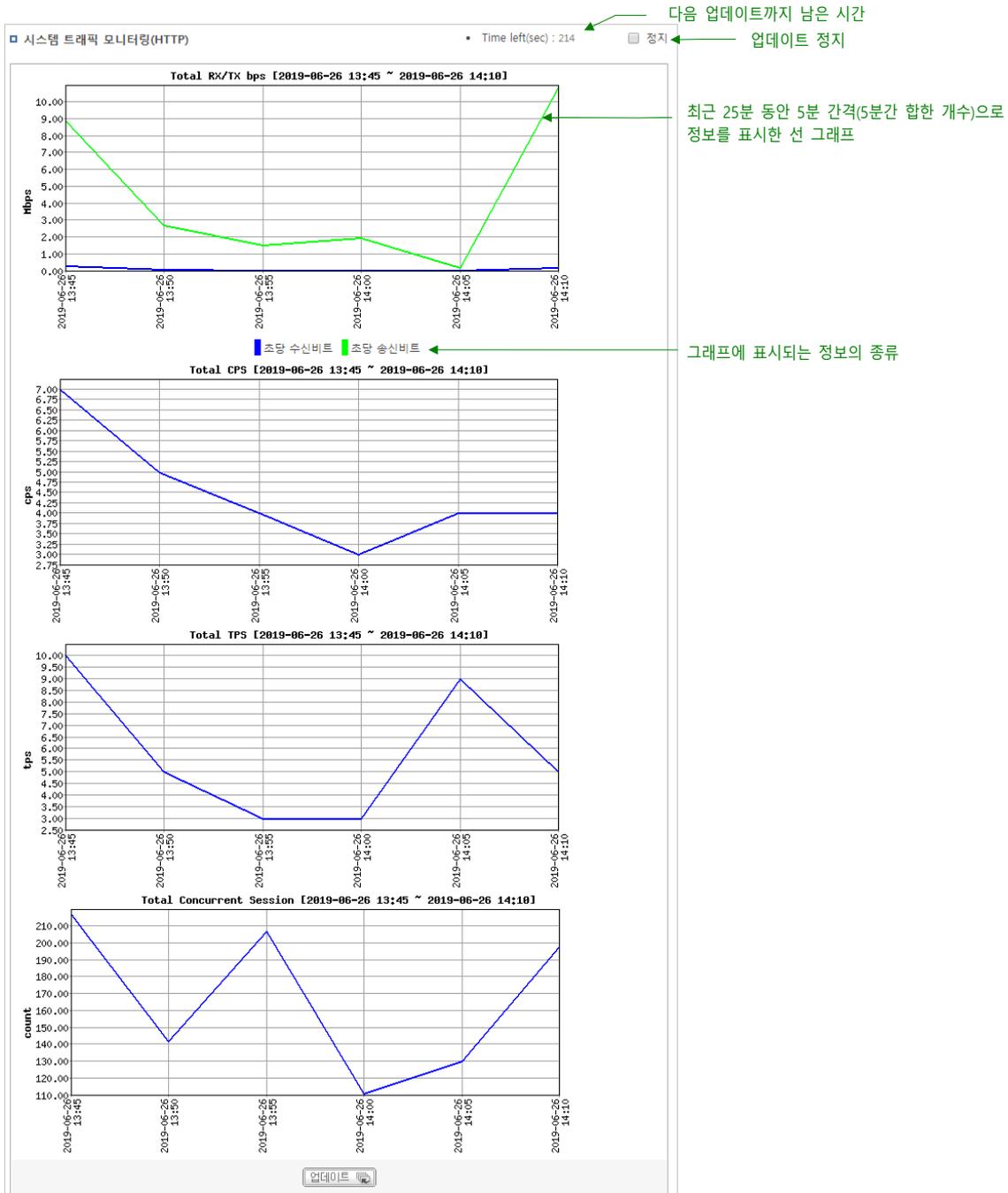


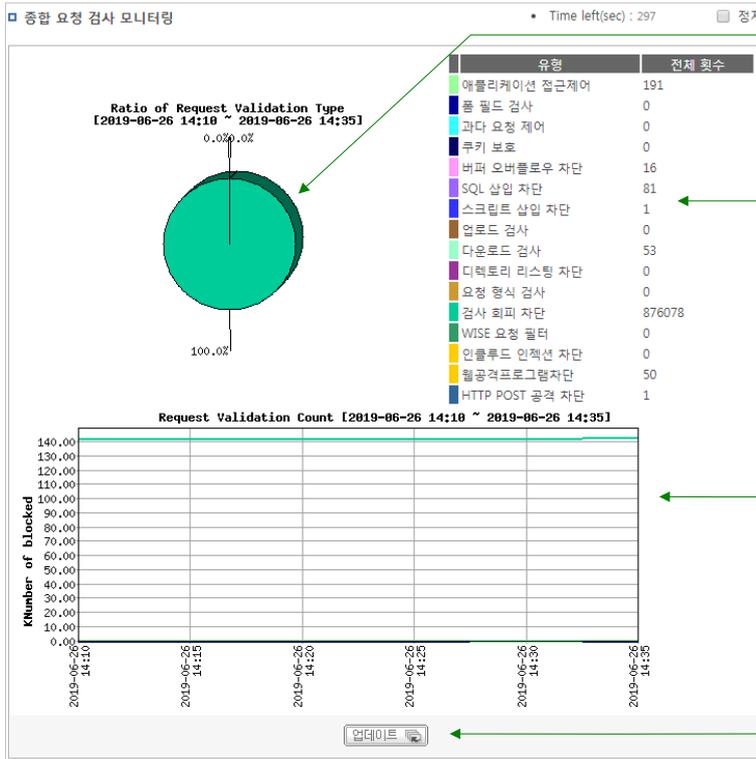
스크롤 바를 사용하여 화면을 아래쪽으로 내리면 웹 공격(나머지)과 요청 검사, 콘텐츠 보호, 학습, 위장에 대한 모니터링 결과를 볼 수 있습니다.

# 모니터링 화면 구조

시스템 통합 모니터링에서는 6종류의 모니터링 화면을 볼 수 있습니다. 가장 위에 트래픽 양에 대한 정보를 보여주는 모니터링 화면이 있고, 아래 쪽에 차례로 애플리케이션, 요청 검사, 콘텐츠 보호, 학습, 위장에 대한 모니터링 화면이 있습니다. 6종류의 모니터링 화면은 거의 동일한 구성으로 이루어져 있으므로 각 화면을 살펴보기 전에 먼저 2가지 모니터링 화면을 예로 들어, 모니터링 화면의 공통적인 부분부터 살펴보도록 합니다.

다음은 <시스템 트래픽 모니터링> 화면과 <종합 요청 검사 모니터링> 화면입니다.





보안 기능의 종류별로 차단한 웹 공격의 비율을 보여주는 파이 그래프

보안 기능의 종류별로 차단한 웹 공격의 횟수를 보여주는 표

최근 25분 동안 5분 간격(5분간 합한 개수)으로 정보를 표시한 선 그래프

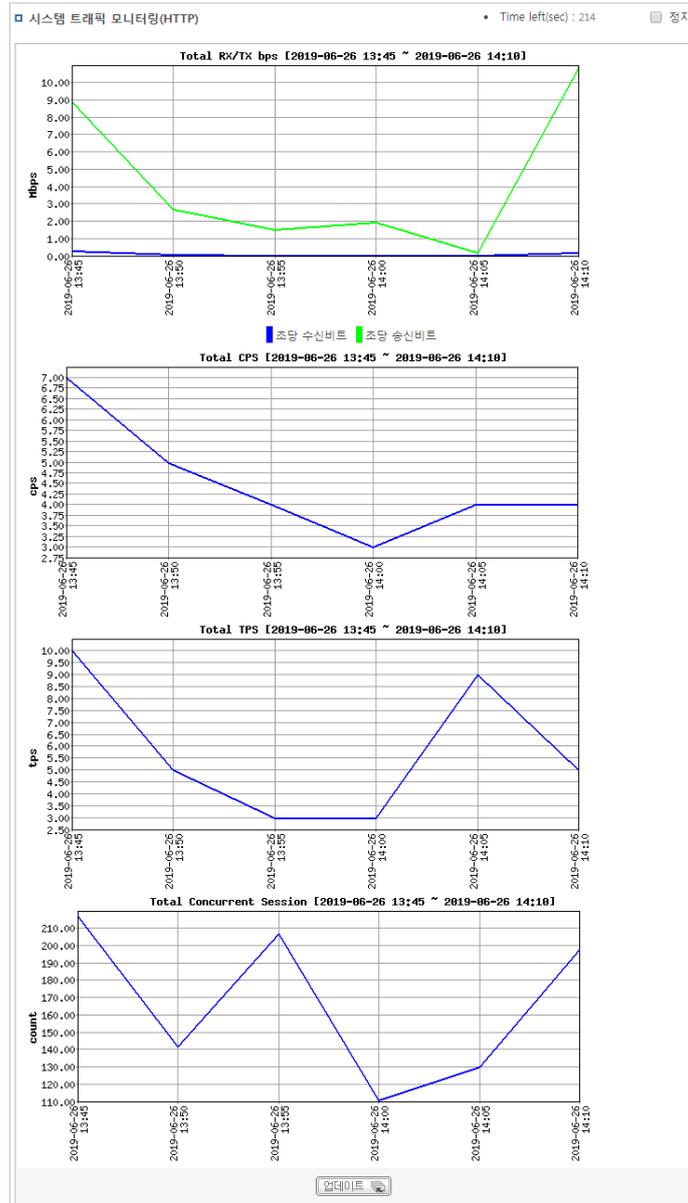
[업데이트] 버튼

두 화면에서 공통적으로 볼 수 있는 꺾은 선 그래프에는 최근 25분 동안 수집한 정보가 5분 간격으로 표시됩니다. 그래프의 가로축은 시간이고, 세로축은 5분 동안 수집한 정보의 합입니다. WEBFRONT-K가 시작된 지 25분이 경과하지 않은 경우에는 WEBFRONT-K가 시작되기 이전까지의 값이 표시되지 않습니다. 5분마다 그래프에 값을 표시하기 때문에 그래프는 5분 간격으로 업데이트됩니다. 다음 업데이트될 때까지 남은 시간은 그래프의 오른쪽 위에 있는 Time left에 표시됩니다. 업데이트를 멈추려면 Time left의 오른쪽에 있는 정지 항목을 클릭합니다. 정지 항목이 체크되어 있는 동안 Time left의 시간이 정지되어 업데이트가 발생하지 않습니다. 정지 항목을 다시 클릭하여 체크되지 않도록 하면 Time left의 시간이 다시 줄어들기 시작합니다. 그래프 아래의 [업데이트] 버튼을 클릭하면 최신 정보로 그래프를 즉시 변경합니다.

두번째 화면의 왼쪽에 있는 파이 그래프는 최근 25분 동안 요청 검사의 각 보안 기능별로 발견한 웹 공격의 비율을 보여줍니다. 오른쪽에 있는 표는 최근 25분 동안 각 보안 기능에 의해 발견된 웹 공격의 횟수를 보여줍니다. 이러한 공통적인 부분을 제외하고, 각 모니터링 화면에서만 볼 수 있는 정보에 대해 살펴봅니다.

# 트래픽 양에 대한 모니터링 정보

<시스템 트래픽 모니터링> 부분에는 WEBFRONT-K의 인터페이스를 통해 송수신된 트래픽 양에 대한 정보가 출력됩니다.

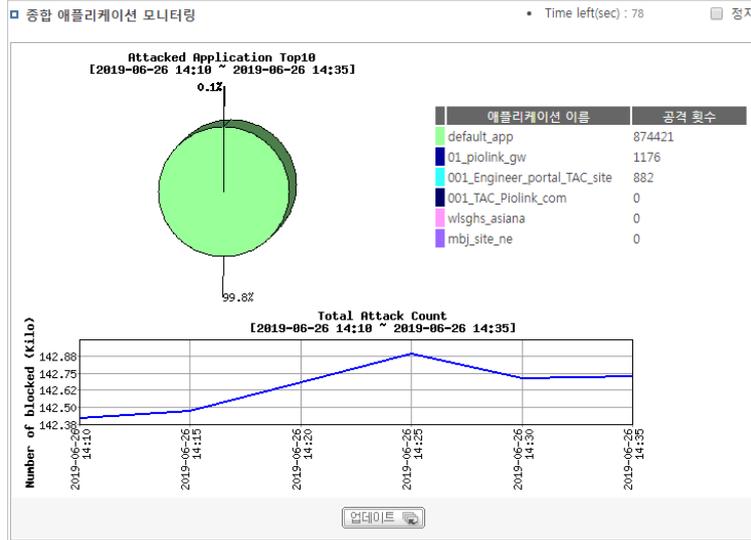


이 부분의 그래프에는 트래픽의 양과 관련된 다음과 같은 4가지 정보가 출력됩니다. 각 정보는 사용자가 쉽게 구분할 수 있도록 모두 다른 색상으로 표시됩니다.

항목	설명
Total RX/TX bps	<ul style="list-style-type: none"> <li>초당 수신 패킷 양(Rx bit per second, 파란색) : 1초 동안 WEBFRONT-K의 모든 인터페이스로 수신된 패킷의 총 bit 수</li> <li>초당 전송 패킷 양(Tx bit per second, 초록색) : 1초 동안 WEBFRONT-K의 모든 인터페이스를 통해 전송된 패킷의 총 bit 수</li> </ul>
Total CPS	<ul style="list-style-type: none"> <li>초당 생성된 TCP 커넥션 수(Connection Per Second) : 1초 동안 WEBFRONT-K가 TCP 커넥션을 정상적으로 수립하고 에러 없이 종료한 수</li> </ul>
Total TPS	<ul style="list-style-type: none"> <li>초당 처리된 트랜잭션 수(Transaction Per Second) : 1초 동안 WEBFRONT-K가 HTTP 요청과 응답을 정상적으로 처리한 수</li> </ul>
Total Concurrent Session	<ul style="list-style-type: none"> <li>초당 생성된 TCP 세션 수 : 1초 동안 WEBFRONT-K에서 동시에 생성한 TCP 세션 수</li> </ul>

## 웹 공격 횟수에 대한 모니터링 정보

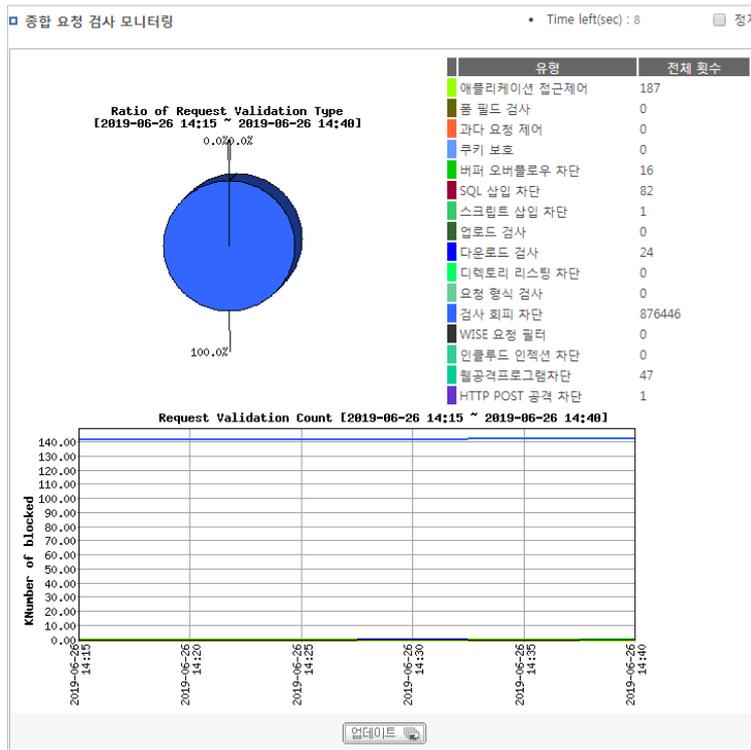
<종합 애플리케이션 모니터링> 부분에서는 WEBFRONT-K에 등록된 애플리케이션으로 행해진 웹 공격의 횟수에 대한 정보를 볼 수 있습니다. 애플리케이션에 설정된 모든 웹 보안 기능에 의해 최근 25분 동안 차단된 웹 공격의 횟수가 이 화면에 출력됩니다.



화면의 오른쪽에 있는 표는 WEBFRONT-K에 등록된 애플리케이션과 각 애플리케이션에 설정된 웹 보안 기능에 의해 차단된 웹 공격의 횟수를 보여줍니다. 애플리케이션별 웹 공격 횟수를 쉽게 비교할 수 있도록 화면의 왼쪽에는 파이 그래프가 있습니다. 그리고, 아래에 있는 꺾은 선 그래프는 WEBFRONT-K의 모든 애플리케이션에서 차단한 총 웹 공격의 횟수를 5분 간격으로 보여줍니다. 이 그래프를 통해서 WEBFRONT-K가 차단한 웹 공격의 시간별 추이를 알 수 있습니다.

## 요청 검사에 대한 모니터링 정보

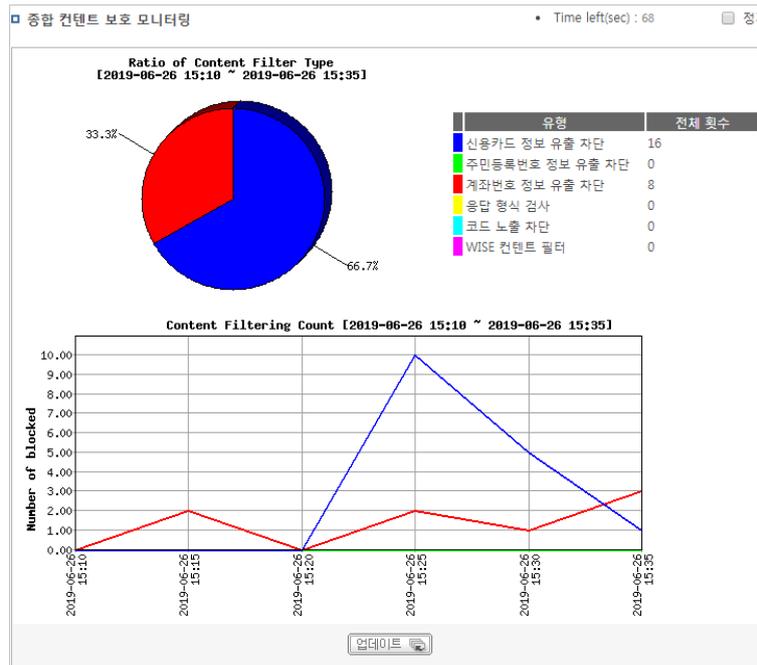
<종합 요청 검사 모니터링> 부분에는 WEBFRONT-K에 설정된 요청 검사 기능을 통해 최근 25분 동안 차단된 웹 공격에 대한 정보가 출력됩니다. 화면의 오른쪽에 있는 표는 요청 검사 기능의 종류와 각 종류의 요청 검사 기능이 차단한 웹 공격의 횟수입니다.



요청 검사 기능의 종류 별로 웹 공격의 횟수를 비교할 수 있도록 화면의 왼쪽에는 오른쪽 표를 변환한 파이 그래프가 있습니다. 그리고, 아래에는 모든 요청 검사 기능을 통해 차단된 총 웹 공격의 횟수를 5분 간격으로 보여주는 꺾은 선 그래프가 있습니다.

## 컨텐츠 보호에 대한 모니터링 정보

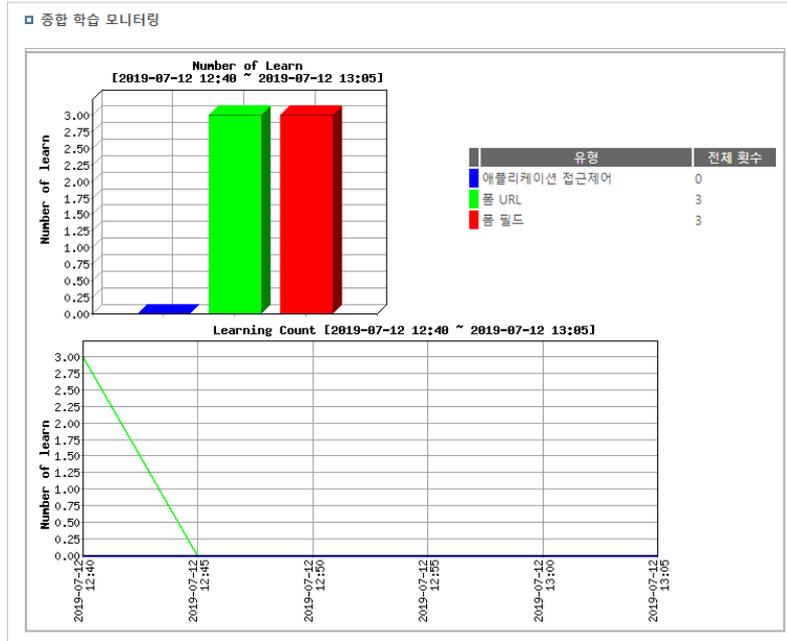
<종합 컨텐츠 보호 모니터링> 부분에는 WEBFRONT-K에 설정된 컨텐츠 보호 기능을 통해 최근 25분 동안 차단된 웹 공격에 대한 정보가 출력됩니다. 화면의 오른쪽에 있는 표는 컨텐츠 보호 기능의 종류와 각 종류의 컨텐츠 보호 기능이 차단한 웹 공격의 횟수입니다.



왼쪽의 파이 그래프는 컨텐츠 보호 기능의 종류 별로 차단한 웹 공격 횟수의 상대적인 비율을 보여줍니다. 그리고, 아래에 있는 꺾은 선 그래프는 모든 컨텐츠 보호 기능을 통해 차단된 총 웹 공격의 횟수를 5분 간격으로 보여줍니다.

## 학습 기능에 대한 모니터링 정보

<종합 학습 모니터링> 부분에는 WEBFRONT-K에 설정된 학습 기능에 의해 최근 25분 동안 학습한 정보의 개수가 출력됩니다. 화면의 오른쪽에 있는 표는 요청 검사 기능의 종류와 각 요청 검사 기능에 설정된 학습 기능에 의해 학습된 정보의 개수입니다.



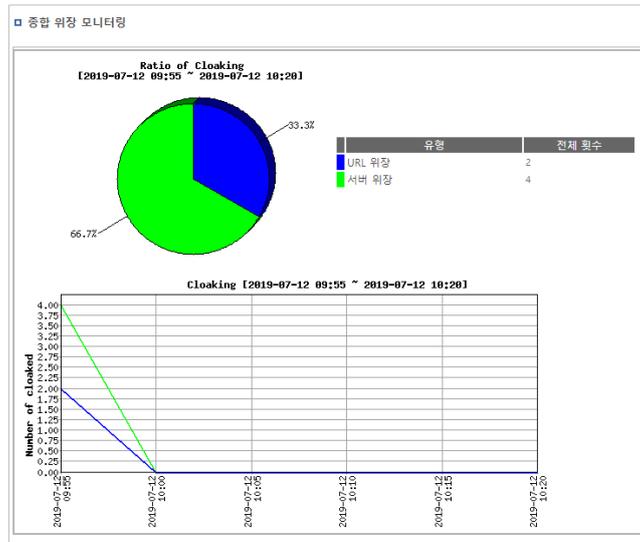
화면의 왼쪽에 있는 막대 그래프는 오른쪽 표의 정보를 그래프 형태로 보여줍니다. 이 그래프를 통해 종류 별로 학습한 정보의 개수를 쉽게 비교할 수 있습니다. 그리고, 아래에 있는 꺾은 선 그래프에서는 학습 기능을 통해 학습된 정보의 총 개수를 볼 수 있습니다.



**참고:** 학습(learning)은 각 요청 검사 기능에 설정된 정책에 어긋나는 패킷에 대한 정보를 기록하는 기능입니다. 학습 기능에 의해 기록된 정보는 이후 애플리케이션 관리자가 요청 검사 기능의 정책을 보완할 때 유용하게 사용할 수 있습니다. 학습 기능에 대한 상세한 설명은 이 설명서와 함께 제공되는 **애플리케이션 구성 설명서**를 참고합니다.

## 위장 기능에 대한 모니터링 정보

<종합 위장 모니터링> 부분에는 WEBFRONT-K에 설정된 위장 기능에 의해 최근 25분 동안 정보가 변경된 횟수가 출력됩니다.



화면의 오른쪽에 있는 표는 위장 기능의 종류와 각 종류의 위장 기능이 정보를 변경한 횟수입니다. 아래에 있는 꺾은 선 그래프는 모든 위장 기능을 통해 차단된 총 웹 공격의 횟수를 5분 간격으로 보여줍니다.



**참고:** 위장(cloaking)은 웹 서버의 주요 정보가 외부로 노출되지 않도록 해주는 기능입니다. 위장 기능을 통해 클라이언트와의 연결에 사용되는 URL을 웹 서버의 실제 URL과 다르게 변환하거나 클라이언트로 전송하는 응답 중에 포함된 웹 서버의 정보를 숨기거나 혹은 다른 값으로 바꿀 수 있습니다. 위장 기능에 대한 상세한 설명은 이 설명서와 함께 제공되는 **애플리케이션 구성 설명서**를 참고합니다.

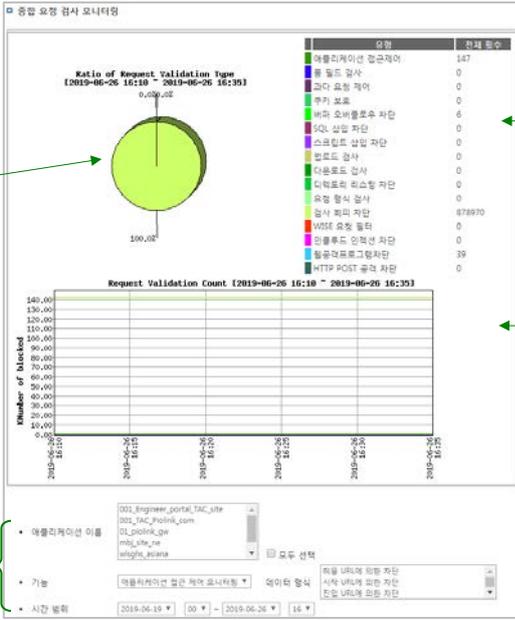
# 요청 검사 모니터링

시스템 통합 모니터링 화면에서는 요청 검사 기능별 차단 웹 공격 횟수나 모든 애플리케이션의 요청 검사 기능에 의해 차단된 총 웹 공격 횟수를 볼 수 있습니다. 볼 수 있는 정보는 최근 25분 동안 수집된 정보로 한정됩니다.

이와 달리 요청 검사 상세 모니터링 화면에서는 일주일간 수집된 정보를 볼 수 있고, 다음과 같이 사용자가 여러 옵션을 선택하여 원하는 정보만 조회할 수 있습니다.

- 특정 애플리케이션의 요청 검사 기능에 대한 정보만 조회
- 특정 요청 검사 기능에 대한 정보만 조회(예: 접근 제어 기능에 대한 정보만 출력)
- 요청 검사의 종류에 따라 원하는 정보만 조회(예: 접근 제어 기능의 시작 URL에 의해 차단된 웹 공격에 대한 정보만 출력)
- 특정 시간 동안 모니터링한 정보만 출력

요청 검사 상세 모니터링 화면에서 요청 검사 정보를 조회하는 방법은 다음과 같습니다.

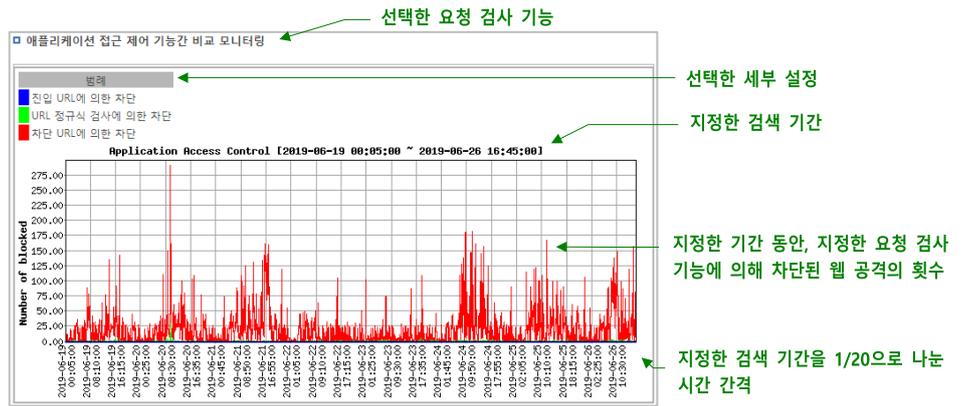
순서	설명
1	<p><b>System - 통합 모니터링 - 요청검사 모니터링</b> 메뉴를 클릭합니다.</p>
2	<p>요청 검사 상세 모니터링 화면이 나타납니다. 화면의 위 부분에는 모든 애플리케이션에 설정된 요청 검사 기능에 의해 최근 25분 동안 차단된 웹 공격에 대한 정보가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 정보를 검색할 때 지정하는 조건들입니다.</p>  <p>요청 검사 기능별 차단 웹 공격의 횟수</p> <p>요청 검사 기능별로 차단된 웹 공격의 비율</p> <p>요청 검사 기능의 모니터링 정보 검색 조건</p> <p>최근 25분 동안 5분 간격 (5분간 합한 개수)으로 모든 요청 검사 기능에 의해 차단된 웹 공격 횟수를 표시한 그래프</p>
3	<p>다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 <b>[보기]</b> 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>애플리케이션 이름</b> 이 항목에는 현재 WEBFRONT-K에 등록된 모든 애플리케이션의 이름이 표시됩니다. 특정 애플리케이션의 요청 검사 기능에 대한 정보만 출력하려면 해당 애플리케이션을 목록에서 클릭합니다. <b>[Shift]</b> 키나 <b>[Ctrl]</b> 키를 사용하여 여러 개의 애플리케이션을 선택할 수도 있습니다. 모든 애플리케이션을 선택하려는 경우에는 항목의 오른쪽에 있는 '모두 선택'을 클릭합니다.</li> <li>• <b>기능</b> 특정 요청 검사 기능에 대한 정보만 출력하려면 이 항목에서 드롭다운 목록을 클릭한 후 원하는 요청 검사 기능을 선택합니다.</li> <li>• <b>데이터 형식</b> 기능 항목에서 요청 검사 기능의 종류를 선택하면 이 항목에는 선택한 요청 검사 기능의 세부 설정 정보가 표시됩니다. 특정 세부 설정에 의해 차단된 웹 공격에 대한 정보만 출력하려는 경우에는 원하는 항목을 선택합니다. <b>[Shift]</b> 키나 <b>[Ctrl]</b> 키를 사용하여 여러 개의 항목을 지정할 수도 있습니다.</li> <li>• <b>시간 범위</b> 특정 기간에 수집된 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다.</li> </ul>



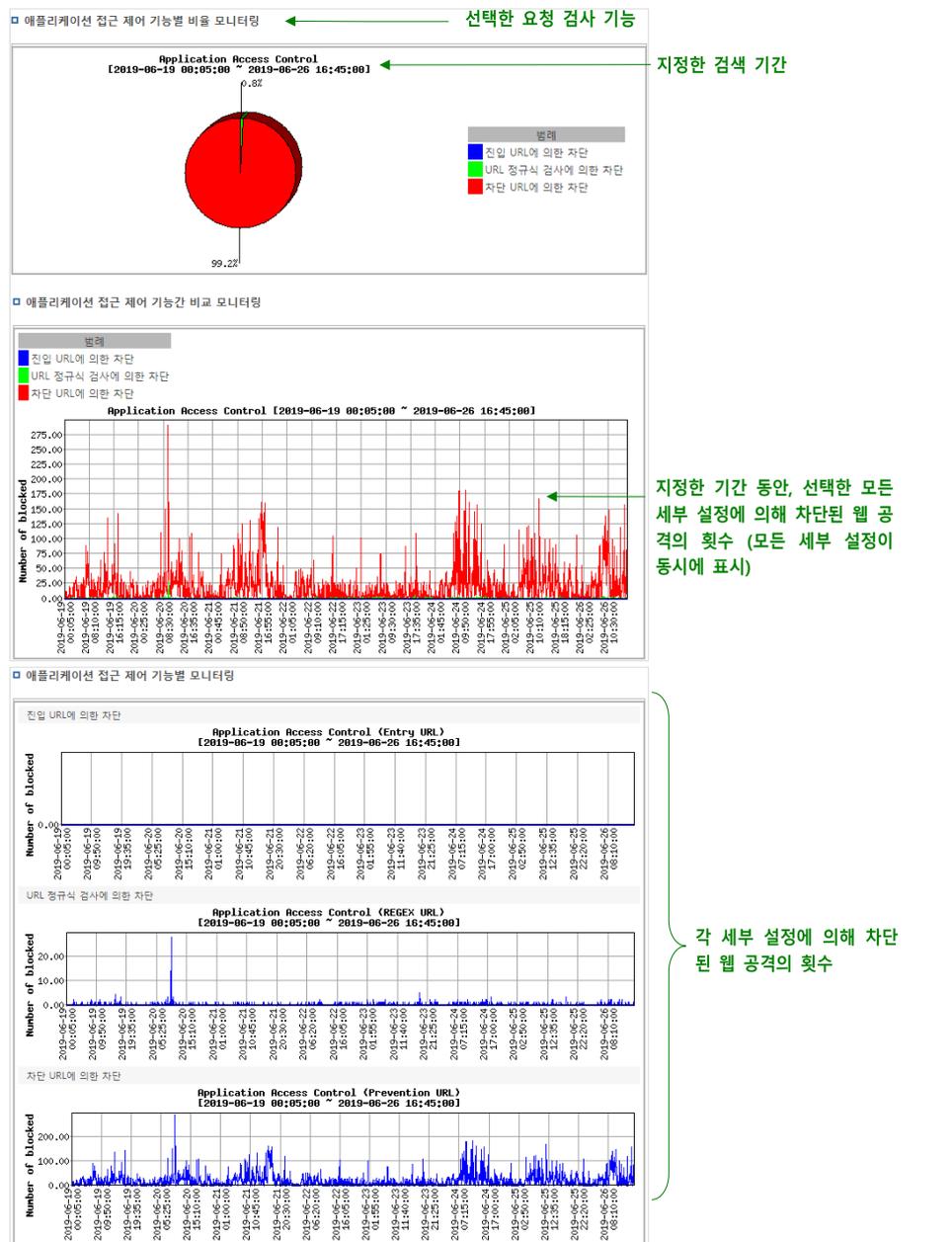
**참고:** WISE 요청 필터에 대한 모니터링 정보는 **Application** 메뉴의 **모니터링 - 요청 검사 모니터링** 메뉴에서만 볼 수 있습니다. 그러므로, '기능' 드롭다운 목록에 WISE 필터 항목이 표시되지 않습니다.

지정한 검색 조건에 따라 다음 세가지 형태 중 하나의 그래프가 나타납니다.

- 검색 조건으로 하나의 애플리케이션과 하나의 세부 설정을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.



- 검색 조건으로 여러 개의 세부 설정을 선택한 경우에는 다음과 같이 맨 위에 파이 그래프가 출력되고 아래에는 선택한 세부 설정의 개수만큼 얇은 선 그래프가 출력됩니다.



- 검색 조건으로 여러 개의 애플리케이션을 선택한 경우에는 애플리케이션마다 위 그림과 같은 정보가 출력됩니다.

# 컨텐츠 보호 모니터링

시스템 통합 모니터링 화면에서는 컨텐츠 보호 기능별 차단 웹 공격 횟수나 모든 애플리케이션의 컨텐츠 보호 기능에 의해 차단된 총 웹 공격 횟수를 볼 수 있습니다. 볼 수 있는 정보는 최근 25분 동안 수집된 정보로 한정됩니다.

이와 달리 컨텐츠 보호 모니터링 화면에서는 일주일간 수집된 정보를 볼 수 있고, 다음과 같이 사용자가 여러 옵션을 선택하여 원하는 정보만 조회할 수 있습니다.

- 특정 애플리케이션의 컨텐츠 보호 기능에 대한 정보만 조회
- 특정 컨텐츠 보호 기능에 대한 정보만 조회(예: 신용카드 정보 차단 기능에 대한 정보만 출력)
- 컨텐츠 보호의 종류에 따라 원하는 정보만 조회(예: 응답 형식 검사 기능의 허용 헤더 설정에 의해 차단된 웹 공격에 대한 정보만 출력)
- 특정 시간 동안 모니터링한 정보만 출력

컨텐츠 보호 모니터링 화면에서 컨텐츠 보호 정보를 조회하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 통합 모니터링 - 컨텐츠 보호 모니터링 메뉴를 클릭합니다.
2	<p>컨텐츠 보호 모니터링 화면이 나타납니다.</p> <p>컨텐츠 보호 기능별 차단 웹 공격의 횟수</p> <p>컨텐츠 보호 기능별로 차단된 웹 공격의 비율</p> <p>최근 25분 동안 모든 컨텐츠 보호 기능에 의해 차단된 웹 공격 횟수를 표시한 그래프</p> <p>컨텐츠 보호 기능의 정보 검색 조건</p>
3	<p>화면의 위 부분에는 모든 애플리케이션에 설정된 컨텐츠 보호 기능에 의해 최근 25분 동안 차단된 웹 공격에 대한 정보가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 정보를 검색할 때 지정하는 조건들입니다.</p> <p>다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 [보기] 버튼을 클릭 합니다.</p> <ul style="list-style-type: none"> <li>• 애플리케이션 이름 이 항목에는 현재 WEBFRONT-K에 등록된 모든 애플리케이션의 이름이 표시됩니다. 특정 애플리케이션의 컨텐츠 보호 기능에 대한 정보만 출력하려면 해당 애플리케이션을 목록에서 클릭합니다. [Shift] 키나 [Ctrl] 키를 사용하여 여러 개의 애플리케이션을 선택할 수도 있습니다. 모든 애플리케이션을 선택하려는 경우에는 항목의 오른쪽에 있는 '모두 선택'을 클릭합니다.</li> <li>• 기능 특정 컨텐츠 보호 기능에 대한 정보만 출력하려면 이 항목에서 드롭다운 목록을 클릭한 후 원하는 컨텐츠 보호 기능을 선택합니다.</li> <li>• 데이터 형식 기능 항목에서 컨텐츠 보호 기능의 종류를 선택하면 이 항목에는 선택한 컨텐츠 보호 기능의 세부 설정이</li> </ul>

표시됩니다.

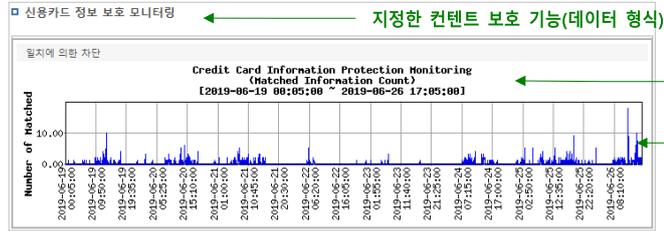
- **시간 범위** 특정 기간에 수집된 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다.



**참고:** WISE 콘텐츠 필터에 대한 모니터링 정보는 **Application** 메뉴의 **모니터링 - 콘텐츠 보호 모니터링** 메뉴에서만 볼 수 있습니다. 그러므로, '기능' 드롭다운 목록에 WISE 필터 항목이 표시되지 않습니다.

지정한 검색 조건에 따라 다음 형태 중 하나의 그래프가 나타납니다.

- 검색 조건으로 하나의 애플리케이션과 하나의 세부 설정을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.



← 지정한 콘텐츠 보호 기능(데이터 형식)

← 사용자가 지정한 검색 기간  
← 지정한 기간 동안 선택한 콘텐츠 보호 기능에 의해 차단된 웹 공격의 횟수를 보여주는 그래프

- 검색 조건으로 여러 개의 세부 설정을 선택한 경우에는 맨 위에 파이 그래프가 출력되고 아래에는 선택한 세부 차단 종류 개수만큼 꺾은 선 그래프가 출력됩니다.
- 검색 조건으로 여러 개의 애플리케이션을 선택한 경우에는 애플리케이션마다 위 그림과 같은 정보가 출력됩니다.

4

# 학습 모니터링

시스템 통합 모니터링 화면에서는 각 요청 검사 기능별로 학습된 정보의 개수나 모든 애플리케이션에 설정된 학습 기능에 의해 학습된 정보의 총 개수를 볼 수 있습니다. 볼 수 있는 정보는 최근 25분 동안 수집된 정보로 한정됩니다.

이와 달리 학습 기능 상세 모니터링 화면에서는 일주일간 수집된 정보를 볼 수 있고, 다음과 같이 사용자가 여러 옵션을 선택하여 원하는 정보만 조회할 수 있습니다.

- 특정 애플리케이션에 설정된 학습 기능에 대한 학습 정보만 조회
- 특정 요청 검사 기능에 대한 학습 정보만 조회(예: 접근 제어 기능의 학습 기능에 의해 기록된 정보의 개수만 출력)
- 특정 시간 동안의 학습 정보만 출력

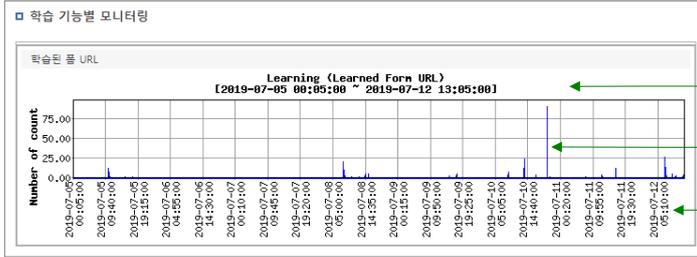
학습 기능 상세 모니터링 화면에서 학습 정보를 조회하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 통합 모니터링 - 학습 모니터링 메뉴를 클릭합니다.
2	<p>학습 기능 상세 모니터링 화면이 나타납니다.</p> <p>학습 기능 별 학습된 정보 개수</p> <p>학습 기능의 종류와 학습된 정보의 개수</p> <p>학습 기능의 정보 검색 조건</p> <p>최근 25분 동안 모든 학습 기능을 통해 학습된 정보의 총 개수를 표시한 그래프</p>
3	<p>화면의 위 부분에는 애플리케이션의 요청 검사 기능에 설정된 학습 기능에 의해 최근 24 시간 동안 학습된 정보의 개수가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 학습에 관한 정보를 검색할 때 지정하는 조건들입니다.</p> <p>다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 [보기] 버튼을 클릭합니다.</p> <ul style="list-style-type: none"> <li>• 애플리케이션 이름 이 항목에는 현재 WEBFRONT-K에 등록된 모든 애플리케이션의 이름이 표시됩니다. 특정 애플리케이션의 학습 기능에 대한 정보만 출력하려면 해당 애플리케이션을 목록에서 클릭합니다. [Shift] 키나 [Ctrl] 키를 사용하여 여러 개의 애플리케이션을 선택할 수도 있습니다. 모든 애플리케이션을 선택하려는 경우에는 항목의 오른쪽에 있는 '모두 선택'을 클릭합니다.</li> <li>• 데이터 형식 특정한 요청 검사 기능의 학습 기능에 대한 정보만 출력하려는 경우에는 여기에서 원하는 요청 기능을 선택합니다. [Shift] 키나 [Ctrl] 키를 사용하여 여러 개의 항목을 지정할 수도 있습니다.</li> <li>• 시간 범위 특정 기간에 수집된 학습 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니</li> </ul>

다.

지정한 검색 조건에 따라 다음 형태 중 하나의 그래프가 나타납니다.

- 검색 조건으로 하나의 애플리케이션과 하나의 학습 기능을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.

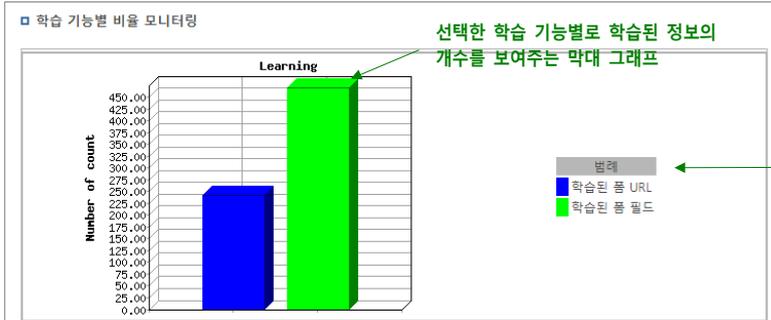


사용자가 지정한 검색 기간

지정한 기간 동안 선택한 학습 기능에 의해 학습된 정보의 개수를 표시한 그래프

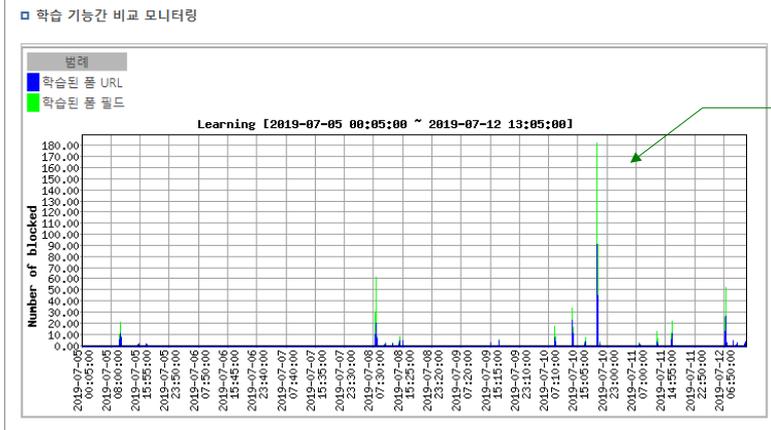
시간 간격

- 검색 조건으로 여러 개의 학습 기능을 선택한 경우에는 다음과 같이 맨 위에 파이 그래프가 출력되고 아래에는 선택한 요청 검사 기능의 개수만큼 겹친 선 그래프가 출력됩니다.



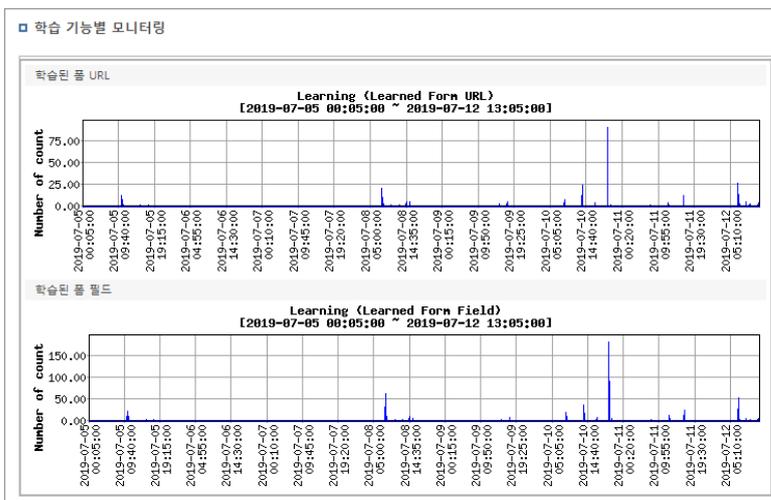
선택한 학습 기능별로 학습된 정보의 개수를 보여주는 막대 그래프

막대 그래프에 학습 정보가 표시되는 보안 기능



지정한 기간 동안 선택한 학습 기능에 의해 학습된 정보의 개수(모든 학습 기능의 정보가 동시에 표시)

4



각 요청 검사 기능의 학습 기능에 의해 학습된 정보의 개수

- 검색 조건으로 여러 개의 애플리케이션을 선택한 경우에는 애플리케이션마다 위 그림과 같은 정보가 출력됩니다.

# 위장 모니터링

시스템 통합 모니터링 화면에서는 위장 기능별 차단 웹 공격 횟수나 모든 애플리케이션의 위장 기능에 의해 차단된 총 웹 공격 횟수를 볼 수 있습니다. 볼 수 있는 정보는 최근 25분 동안 수집된 정보로 한정됩니다.

이와 달리 위장 상세 모니터링 화면에서는 일주일간 수집된 정보를 볼 수 있고, 다음과 같이 사용자가 여러 옵션을 선택하여 원하는 정보만 조회할 수 있습니다.

- 특정 애플리케이션의 위장 기능에 대한 정보만 조회
- 특정 위장 기능에 대한 정보만 조회(예: 서버 위장 기능이나 URL 서버 위장 기능에 대한 정보만 출력)
- 특정 위장 형식에 대한 정보만 조회(예: 버전 위장이나 날짜 위장에 대한 정보만 출력)
- 특정 시간 동안 모니터링한 정보만 출력

위장 상세 모니터링 화면에서 정보를 조회하는 방법은 다음과 같습니다.

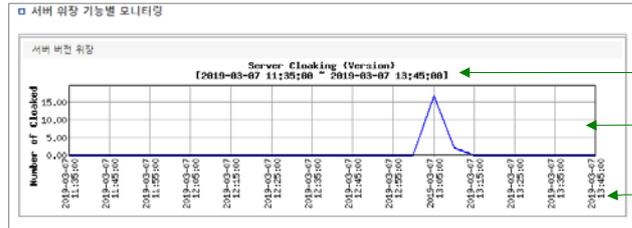
순서	설정 과정
1	<p><b>System - 통합 모니터링 - 위장 모니터링</b> 메뉴를 클릭합니다.</p> <p>위장 상세 모니터링 화면이 나타납니다. 화면의 위 부분에는 최근 25분 동안 모든 애플리케이션에 설정된 위장 기능에 의해 차단된 웹 공격에 대한 정보가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 정보를 검색할 때 지정하는 조건들입니다.</p> <div data-bbox="316 891 1465 1621"> <p>위장 기능별 정보의 변환 비율</p> <p>위장 기능별 정보의 변환 횟수</p> <p>최근 25분 동안 모든 위장 기능에 의해 변환된 횟수를 5분 간격(5분간합한 개수)으로 표시한 그래프</p> <p>위장 기능의 정보 검색 조건</p> </div>
3	<p>다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 <b>[보기]</b> 버튼을 클릭합니다.</p> <div data-bbox="491 1664 1201 1798"> </div> <ul style="list-style-type: none"> <li>• <b>애플리케이션 이름</b> 이 항목에는 현재 WEBFRONT-K에 등록된 모든 애플리케이션의 이름이 표시됩니다. 특정 애플리케이션의 위장 기능에 대한 정보만 출력하려면 해당 애플리케이션을 목록에서 클릭합니다. <b>[Shift]</b> 키나 <b>[Ctrl]</b> 키를 사용하여 여러 개의 애플리케이션을 선택할 수도 있습니다. 모든 애플리케이션을 선택하려는 경우에는 항목의 오른쪽에 있는 '모두 선택'을 클릭합니다.</li> <li>• <b>기능</b> 특정 위장 기능에 대한 정보만 출력하려면 이 항목에서 드롭다운 목록을 클릭한 후 원하는 위장 기능을 선택합니다.</li> <li>• <b>데이터 형식</b> 기능 항목에서 위장 기능의 종류를 선택하면 이 항목에는 선택한 위장 기능의 세부 설정이 표시됩니다. 특정</li> </ul>

세부 설정에 의해 차단된 웹 공격에 대한 정보만 출력하려는 경우에는 여기에서 원하는 항목을 선택합니다.  
 [Shift] 키나 [Ctrl] 키를 사용하여 여러 개의 항목을 지정할 수도 있습니다.

- **시간 범위** 특정 기간에 수집된 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다.

지정한 검색 조건에 따라 다음 세가지 형태 중 하나의 그래프가 나타납니다.

- 검색 조건으로 하나의 애플리케이션과 하나의 세부 설정을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.

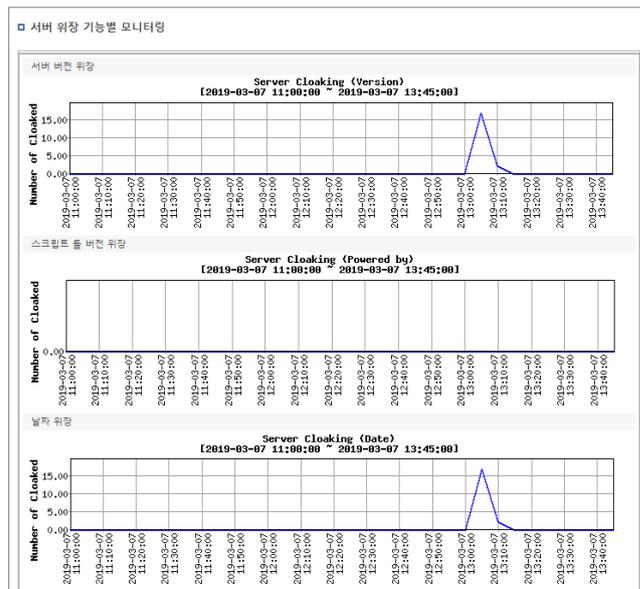
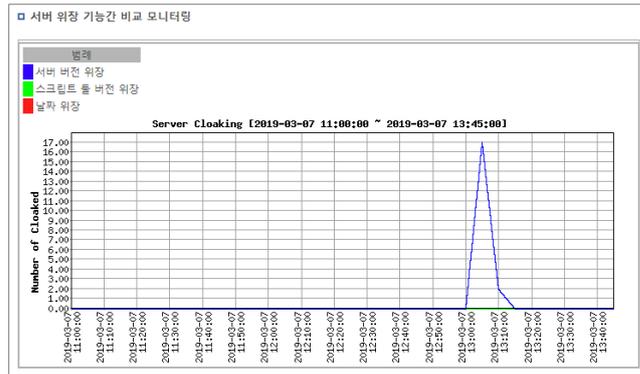
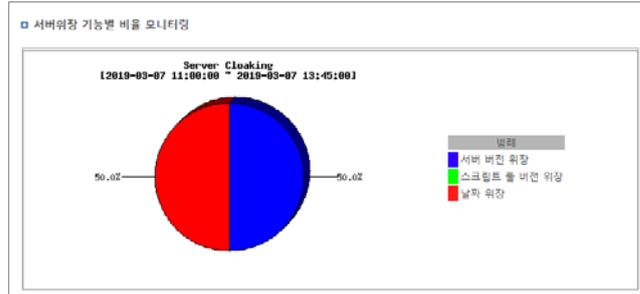


사용자가 지정한 검색 기간

지정한 기간 동안, 지정한 위장 기능에 의해 정보가 변환된 횟수

시간 간격

- 검색 조건으로 여러 개의 세부 설정을 선택한 경우에는 다음과 같이 맨 위에 파이 그래프가 출력되고 아래에는 선택한 세부 차단 종류 개수만큼 꺾은 선 그래프가 출력됩니다.



- 검색 조건으로 여러 개의 애플리케이션을 선택한 경우에는 애플리케이션마다 위 그림과 같은 정보가 출력됩니다.

## 제4장 시스템 모니터링

이 장에서는 WEBFRONT-K 시스템의 기본적인 정보와 상태 정보를 조회하고, 포트의 실시간 트래픽 정보를 모니터링하는 방법에 대해 살펴봅니다.

이 장은 다음 내용으로 구성됩니다.

- 시스템 정보
- 포트 모니터링



# 시스템 정보

WEBFRONT-K의 '시스템 정보' 보기 기능을 사용하면, 장비의 이름이나 일련 번호, MAC 주소, 소프트웨어 버전 등의 기본적인 시스템 정보와 CPU와 메모리 등의 주요 자원의 현재 사용 상태, 그리고 시스템 온도, 냉각 팬 및 전원 공급기의 동작 상태 등 시스템 하드웨어의 상태 정보를 한꺼번에 볼 수 있습니다.

WEBFRONT-K의 **System** 메뉴에서 **시스템 모니터링 - 시스템 정보** 메뉴를 클릭합니다. 그러면, 각종 시스템 정보를 보여주는 화면이 나타납니다.

□ 시스템 상태			
제품 이름	WEBFRONT-K3200-v2.0.61	모델명	WEBFRONT-K3200
소프트웨어 버전	v2.0.61	Build	.0.3
Storage 크기	239GB (available:193GB)	Storage 크기(2nd)	1000GB (available:662GB)
관리용 MAC 주소	00:06:c4:92:04:fe	관리용 IP 주소	192.168.216.38/24.192.168.100.1/24
SDRAM 크기	32768MB	일련 번호	0211K11000AB1290
시스템 가동시간	2 days 20 hours 23 minutes 40 seconds	PLD Version	10
웹 보안 엔진 가동시간	2 days 20 hours 22 minutes 40 seconds		

□ 시스템 자원 상태 정보			
항목	관리 시스템	패킷 프로세서	
CPU 사용률	27.50 %	4.49 %	4.49 %
메모리 사용률	20.66 %	14.00 %	14.00 %
전체 메모리	1536000 kB	31101256 kB	31101256 kB
사용 중인 메모리	317288 kB	4353952 kB	4353952 kB
남은 메모리	1218712 kB	26747304 kB	26747304 kB

□ 시스템 하드웨어 상태 정보			
CPU 온도(Core 0)	52.0 C (high:82.0 C / crit:104.0 C)	CPU 온도(Core 1)	52.0 C (high:82.0 C / crit:104.0 C)
CPU 온도(Core 2)	52.0 C (high:82.0 C / crit:104.0 C)	CPU 온도(Core 3)	52.0 C (high:82.0 C / crit:104.0 C)
Power1	On	Power2	Off
Fan	1(On) 2(On) 3(On) 4(On)	RAID Status	sdb (active sync) / sda (active sync)

각 부분에 대해 살펴봅니다.

## 시스템 상태

<시스템 정보> 화면의 시스템 상태 부분에서는 기본적인 시스템 정보가 출력됩니다.

□ 시스템 상태			
제품 이름	WEBFRONT-K3200-v2.0.61	모델명	WEBFRONT-K3200
소프트웨어 버전	v2.0.61	Build	.0.3
Storage 크기	239GB (available:193GB)	Storage 크기(2nd)	1000GB (available:662GB)
관리용 MAC 주소	00:06:c4:92:04:fe	관리용 IP 주소	192.168.216.38/24.192.168.100.1/24
SDRAM 크기	32768MB	일련 번호	0211K11000AB1290
시스템 가동시간	2 days 20 hours 23 minutes 40 seconds	PLD Version	10
웹 보안 엔진 가동시간	2 days 20 hours 22 minutes 40 seconds		

시스템 상태 부분의 항목은 다음과 같은 정보를 나타냅니다.

항목	설명
제품 이름	장비의 제품 이름
모델명	장비의 모델 이름
소프트웨어 버전	현재 설치된 PLOS의 버전
Build	현재 설치된 PLOS의 세부 빌드 버전
Storage 크기	Storage의 전체 크기와 사용 가능한 크기
Storage 크기(2nd)	장비에 추가로 장착한 Storage의 전체 크기와 사용 가능한 크기
관리용 MAC 주소	관리 이더넷 포트의 MAC 주소
관리용 IP 주소	관리 이더넷 포트에 설정된 IP 주소
SDRAM 크기	SDRAM의 크기(MB)
일련 번호	장비의 일련 번호
시스템 가동 시간	장비가 부팅된 이후부터 지금까지 경과한 시간

PLD Version	현재 설치된 PLD의 버전
웹 보안 엔진 가동시간	웹 보안 엔진이 동작한 이후부터 지금까지 경과한 시간

## 시스템 자원 상태 정보

<시스템 정보> 화면의 시스템 자원 상태 정보 부분에서는 자원 모니터링 기능에 의해 수집된 CPU와 메모리 등의 주요 자원의 현재 사용 상태가 표시됩니다.

항목	관리 시스템	패킷 프로세서
CPU 사용률	27.50 %	4.49 %
메모리 사용률	20.66 %	14.00 %
전체 메모리	1536000 kB	31101256 kB
사용 중인 메모리	317288 kB	4353952 kB
남은 메모리	1218712 kB	26747304 kB

시스템 자원 상태 정보 부분의 항목은 다음과 같은 정보를 나타냅니다.

항목	설명
관리 시스템	관리 시스템의 CPU와 메모리 사용 정보
패킷 프로세서	패킷 프로세서(보안 엔진)의 CPU와 메모리 사용 정보
CPU 사용률	해당 시스템의 현재 CPU의 사용률(utilization, %)
메모리 사용률	해당 시스템의 현재 메모리 사용률(%)
전체 메모리	해당 시스템의 총 메모리 크기
사용 중인 메모리	현재 사용중인 메모리의 크기
남은 메모리	해당 시스템에서 사용할 수 있는 메모리의 크기

## 시스템 하드웨어 상태 정보

<시스템 정보> 화면의 시스템 하드웨어 상태 정보 부분에서는 자원 모니터링 기능에 의해 수집된 온도 정보와 냉각 팬과 전원 공급기 등과 같은 주요 시스템 하드웨어의 상태 정보가 표시됩니다.

CPU 온도(Core 0)	52.0 C (high:82.0 C / crit:104.0 C)	CPU 온도(Core 1)	52.0 C (high:82.0 C / crit:104.0 C)
CPU 온도(Core 2)	52.0 C (high:82.0 C / crit:104.0 C)	CPU 온도(Core 3)	52.0 C (high:82.0 C / crit:104.0 C)
Power1	On	Power2	Off
Fan	1(On) 2(On) 3(On) 4(On)	RAID Status	sdb (active sync) / sda (active sync)

시스템 하드웨어 상태 정보 부분의 항목은 다음과 같은 정보를 나타냅니다.

항목	설명
CPU 온도	각 CPU의 온도. 괄호 안에 표시된 온도는 설정된 임계 온도입니다. CPU의 개수는 제품마다 다르게 표시됩니다.
Power 1~2	각 전원 공급기의 동작 상태
Fan	각 냉각 팬의 동작 상태입니다. 냉각 팬의 개수는 제품마다 다르게 표시됩니다.

CPU 온도가 설정된 임계 온도보다 높거나 낮아지는 경우, 냉각 팬의 동작이 멈춰지거나 다시 시작되는 경우 시스템 로그 메시지가 생성됩니다.

### 하드웨어 상태 정보를 통해 판단하는 장비의 문제

시스템 하드웨어 상태 정보 부분에 출력되는 다음과 같은 정보를 통해서 현재 장비에 어떤 문제가 발생했는지 판단할 수 있습니다.

- CPU 온도

CPU 온도가 WEBFRONT-K의 정상적인 동작 온도의 범위인 0 ~ 77°C를 벗어나는 경우에는 장비의 동작에 영향을 줄 수 있습니다. 장비의 이상 동작이 발생하였을 때 CPU 온도가 매우 높게 표시된다면 온도로 인해 발생한 오동작인지 조사할 필요가 있습니다. (CPU 온도가 97°C를 초과하는 경우에는 장비가 정상적으로 동작하지 않습니다.)

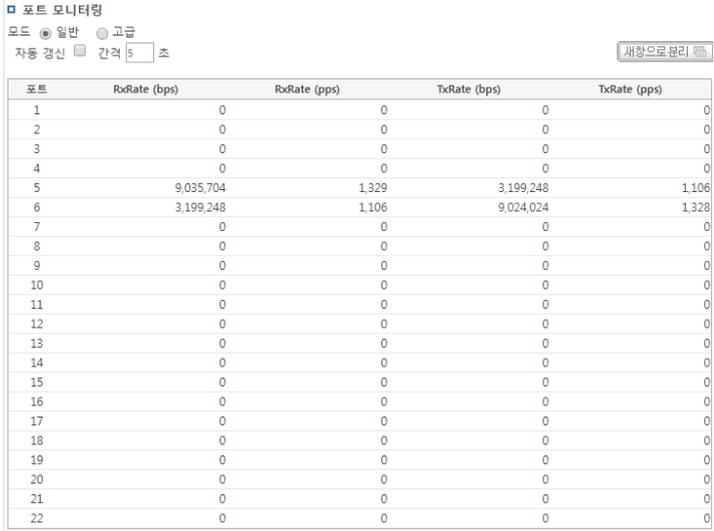
# 포트 모니터링

## 포트의 실시간 트래픽 양 보기

WEBFRONT-K는 각기가넷 이더넷 포트를 통해서 송수신되는 트래픽에 대한 정보를 실시간으로 보여주는 '포트 모니터링' 기능을 제공합니다. 포트 모니터링 기능은 '일반' 모드와 '고급' 모드, 2가지 모드를 지원합니다. 일반 모드에서는 각 포트의 초당 송수신 패킷 수와 byte 수가 출력되고 고급 모드에서는 지정한 포트의 트래픽에 대한 다양한 통계 정보가 출력됩니다.

포트 모니터링 기능은 '자동 갱신' 옵션을 지원하는 데, 이 옵션을 사용하면 포트 모니터링 화면의 정보가 사용자가 설정한 시간(초)마다 최신 정보로 업데이트됩니다. 포트 모니터링 화면을 새 창으로 분리하면, WEBFRONT-K 메인 화면과 별도의 창이 나타납니다. WEBFRONT-K의 다른 기능을 사용하면서 동시에 포트의 트래픽 정보를 지속적으로 관찰하려면 자동 갱신 옵션을 선택한 후 포트 모니터링 화면을 새 창으로 분리하면 됩니다.

포트 모니터링 기능을 사용하는 방법은 다음과 같습니다.

순서	설정 과정										
1	<p><b>System - 시스템 모니터링 - 포트 모니터링</b> 메뉴를 클릭합니다.</p> <p>포트의 실시간 트래픽 정보를 보여주는 &lt;포트 모니터링&gt; 화면이 나타납니다. 기본적으로 포트 모니터링은 '일반' 모드로 설정되어 있습니다.</p> 										
2	<p>일반 모드의 &lt;포트 모니터링&gt; 화면에는 다음과 같은 정보가 출력됩니다.</p> <table border="1"> <thead> <tr> <th>포트</th> <th>포트 번호</th> </tr> </thead> <tbody> <tr> <td>RxRate(bps)</td> <td>해당 포트로 1초 동안 수신된 비트 수</td> </tr> <tr> <td>RxRate(pps)</td> <td>해당 포트로 1초 동안 수신된 패킷 수</td> </tr> <tr> <td>TxRate(bps)</td> <td>해당 포트에서 1초 동안 전송한 비트 수</td> </tr> <tr> <td>TxRate(pps)</td> <td>해당 포트에서 1초 동안 전송한 패킷 수</td> </tr> </tbody> </table>	포트	포트 번호	RxRate(bps)	해당 포트로 1초 동안 수신된 비트 수	RxRate(pps)	해당 포트로 1초 동안 수신된 패킷 수	TxRate(bps)	해당 포트에서 1초 동안 전송한 비트 수	TxRate(pps)	해당 포트에서 1초 동안 전송한 패킷 수
포트	포트 번호										
RxRate(bps)	해당 포트로 1초 동안 수신된 비트 수										
RxRate(pps)	해당 포트로 1초 동안 수신된 패킷 수										
TxRate(bps)	해당 포트에서 1초 동안 전송한 비트 수										
TxRate(pps)	해당 포트에서 1초 동안 전송한 패킷 수										
3	<p>모드 항목을 '고급'으로 선택하면 각종 통계 정보를 보여주는 고급 모드 화면으로 바뀝니다. 포트 드롭다운 목록에서 원하는 통계 정보를 출력하려는 포트를 선택할 수 있습니다.</p>										

□ 포트 모니터링

모드  일반  고급

포트

자동 갱신  간격  초 [새창으로 분리]

RxBytes	0	RxPackets	0
RxErrs	0	RxDrop	0
RxMulticast	0		

TxBytes	0	TxPackets	0
TxErrs	0	TxDrop	0

고급 모드의 <포트 모니터링> 화면에는 다음과 같은 정보가 출력됩니다.

- **RxBytes** 수신한 패킷의 바이트 수
- **RxPackets** 수신한 패킷의 수
- **RxErrs** 수신한 패킷 중 에러가 발생한 패킷의 수
- **RxDrop** 수신 누락된 패킷의 수
- **RxMulticast** 멀티 캐스트로 수신한 패킷의 수
- **TxBytes** 송신한 패킷의 바이트 수
- **TxPackets** 송신한 패킷의 수
- **TxErrs** 송신한 패킷 중 에러가 발생한 패킷의 수
- **TxDrop** 송신 누락된 패킷의 수

4

자동 갱신 항목의 체크 박스를 클릭한 후 오른쪽에 있는 입력란에 갱신 주기(초)를 입력하면 지정한 주기마다 화면의 정보가 자동으로 업데이트됩니다. 업데이트되기까지 남은 시간이 자동 갱신 항목의 오른쪽에 표시됩니다.

□ 포트 모니터링

모드  일반  고급

포트

자동 갱신  간격  초 3 초 남음

5

[새창으로 분리] 버튼을 클릭하면 별도의 포트 모니터링 화면이 나타납니다. 이 화면에서는 모드를 바꿀 수는 없고 자동 갱신 기능을 설정할 수 있습니다.

□ 고급 포트 모니터링

포트

자동 갱신  간격  초

RxBytes	0	RxPackets	0
RxErrs	0	RxDrop	0
RxMulticast	0		

TxBytes	0	TxPackets	0
TxErrs	0	TxDrop	0

## 제5장 통합 로그

이 장에서는 WEBFRONT-K의 로그 기능에 대해 살펴본 후, 로그를 설정하는 방법과 보안 로그, 감사 로그, 방화벽 로그, 접근 로그와 같은 WEBFRONT-K의 다양한 로그를 확인하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성됩니다.

- 로그 개요
- 통합 로그 설정
- 로그 내보내기
- 보안 로그
- 감사/시스템 로그
- 방화벽 로그
- 접근 로그



## 로그 개요

로그(log)는 WEBFRONT-K의 동작 중에 발생하는 각종 이벤트들을 기록한 것입니다. WEBFRONT-K는 동작 중에 어떤 이벤트들이 일어났는지 사용자가 알 수 있도록 이벤트에 대한 정보를 모두 로그로 저장할 수 있습니다. 어떤 사용자가 언제 WEBFRONT-K로 로그인하거나 로그오프했는지, 어떤 기능이 언제 수행되었는지 문제가 발생하지는 않았는지, 어떤 보안 기능에 의해 어떤 클라이언트가 보낸 요청이 차단되었는지, 전원 공급기나 냉각 팬이 켜졌거나 꺼졌는지 등의 이벤트에 대한 정보를 저장된 로그를 통해서 확인할 수 있습니다. 로그는 장비에 문제가 발생했을 때 그 원인을 알아내기 위해 사용됩니다. 로그가 저장되지 않거나 충분하지 않을 경우에는 문제의 원인을 알아내는 데 큰 어려움을 겪을 수 있으므로, 로그를 저장하고 관리하는 데 많은 주의를 기울여야 합니다.

### 이벤트 레벨

WEBFRONT-K에는 짧은 시간 동안 매우 많은 이벤트가 발생합니다. 모든 이벤트들이 다 중요한 것은 아니기 때문에 이벤트의 중요도에 따라 어떤 것은 즉각적인 조치가 필요할 수 있고 어떤 것은 관리자가 굳이 알 필요가 없을 수도 있습니다. 그래서, WEBFRONT-K는 이벤트를 다음과 같은 7개의 레벨로 분류하여 이벤트의 중요도를 구분할 수 있도록 하였습니다.

레벨	설명
Emergency	시스템에 치명적인 이벤트
Alert	즉각적인 조치가 필요한 이벤트
Critical	중대한 에러에 해당되는 이벤트
Error	비교적 중대하지 않은 에러에 해당되는 이벤트
Warning	경고에 해당되는 이벤트
Notice	중요하지 않은 일반 이벤트
Information	정보에 해당하는 이벤트

WEBFRONT-K는 사용자가 지정한 레벨 이상의 이벤트만 로그로 기록합니다. 기본적으로는 WEBFRONT-K는 Notice 레벨 이상의 이벤트만 로그로 저장하도록 설정되어 있습니다.

### 로그 종류

WEBFRONT-K는 이벤트의 종류에 따라 로그 메시지를 다음 4가지 종류로 구분합니다.

- 보안 로그(security log)  
수신된 패킷이 WEBFRONT-K에 설정된 웹 보안 규칙에 위배되는 경우 패킷에 대한 정보와 어떤 규칙에 의해 위배되었는지를 기록하는 로그
- 감사/시스템 로그(audit/system log)  
관리자가 WEBFRONT-K에서 조회한 설정 정보와 변경한 설정 정보에 대한 정보를 기록하는 로그
- 방화벽 로그(firewall log)  
수신된 패킷이 WEBFRONT-K에 설정된 방화벽 정책에 위배되는 경우, 패킷에 대한 정보와 어떤 규칙에 의해 위배되었는지를 기록하는 로그
- 접근 로그(access log)  
WEBFRONT-K로 웹 요청 패킷이 수신될 때마다 웹 요청 패킷에 대한 정보가 기록되는 로그.

## 로그 메시지의 내용

다음은 WEBFRONT-K에 저장된 각 로그 메시지의 예입니다.

### 보안 로그

PIOLINK | WEBFRONT-K Korean wfadmin

System > 통합 로그 > 보안로그

[필터 관리](#)
[상세 필터](#)
[사용자 정의](#)
[내보내기](#)
[조기화](#)
[저장](#)
[적용](#)

날짜	공격 이름	애플리케이션	SIG 위험도	공격 위험도	호스트	URL	클라이언트 IP/PORT	서버 IP/PORT	국가	다음
2019/06/26 10:45:00	XSS	http	중간	중간	192.168.216.112	/index.html?cdf=kkk&abc=<script>&asdf=sdffe	192.168.227.111:38540	192.168.216.112:80		서단

### 감사/시스템 로그

PIOLINK | WEBFRONT-K Korean wfadmin

System > 통합 로그 > 감사/시스템 로그

[필터 관리](#)
[상세 필터](#)
[사용자 정의](#)
[내보내기](#)
[조기화](#)
[저장](#)
[적용](#)

날짜	사용자 아이디	애플리케이션	메시지	결과
2019/06/26 11:21:02	statistics		애플리케이션 일반 설정의 정보를 확인합니다	성공

### 방화벽 로그

PIOLINK | WEBFRONT-K Korean wfadmin

System > 통합 로그 > 방화벽 로그

[필터 관리](#)
[상세 필터](#)
[사용자 정의](#)
[내보내기](#)
[조기화](#)
[저장](#)
[적용](#)

날짜	필터 명	출발지 IP	목적지 IP	프로토콜	메시지	대응
2019/06/26 11:33:31	firewall_filter	192.168.227.111	192.168.216.112	ANY	PSM 방화벽 - 방화벽에 의해 세션이 차단되었습니다	Drop

### 접근 로그

PIOLINK | WEBFRONT-K Korean wfadmin

System > 통합 로그 > 접근로그

[필터 관리](#)
[상세 필터](#)
[사용자 정의](#)
[내보내기](#)
[조기화](#)
[저장](#)
[적용](#)

날짜	애플리케이션	HTTP(S)	HTTP(ver)	호스트	URL	클라이언트 IP/PORT	서버 IP/PORT	메소드
2019/06/26 10:45:00	http	HTTP	HTTP/1.1	192.168.216.112	/index.html?cdf=kkk&abc=<script>&asdf=sdffe	192.168.227.111:38540	192.168.216.112:80	POST

## 시스로그 서버

로그 버퍼에 저장되는 로그는 일정한 시간이 경과하면 로그 순환 기능에 의해 삭제됩니다. 로그는 장비의 문제를 해결하는 데 있어서 필수적인(때로는 유일한) 정보이기 때문에 일부만 삭제되어도 문제를 제대로 해결할 수 없는 경우가 많습니다. 그러므로, 반드시 로그를 백업해두어야 합니다.

가장 일반적으로 사용되는 로그 백업 방법은 외부의 시스로그(syslog) 서버로 로그를 전송하는 것입니다. 윈도우나 유닉스, 리눅스 등 운영체제에 관계 없이 시스로그 서버 프로그램이 동작하고, 충분한 용량의 저장 장치(하드 디스크와 같은)를 가지고 있고, WEBFRONT-K에서 네트워크를 통해 접속할 수 있지만 어떤 서버도 시스로그 서버로 사용할 수 있습니다.

WEBFRONT-K에 시스로그 서버와 시스로그 서버로 전송할 이벤트의 레벨을 설정하면, WEBFRONT-K는 설정된 레벨 이상의 이벤트가 발생할 때마다 이벤트에 대한 로그를 시스로그 서버로 전송합니다. 일반적으로 시스로그 서버의 저장 장치는 WEBFRONT-K의 로그 버퍼에 비해 매우 크기 때문에 로그 버퍼에 저장할 이벤트의 레벨보다 낮은 레벨을 지정하는 것이 좋습니다. WEBFRONT-K에는 최대 256개의 시스로그 서버를 설정할 수 있고, 시스로그 서버마다 이벤트의 레벨을 다르게 지정할 수 있습니다.



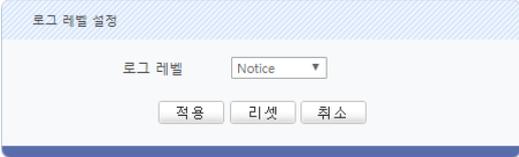
**참고:** Analyzer를 사용하는 경우에는 Analyzer 서버로 모든 로그가 전송되므로 Analyzer 서버를 시스로그 서버처럼 활용할 수 있습니다.

## 통합 로그 설정

로그를 저장하고 로그를 외부의 시스로그 서버로 전송하는 데 필요한 설정 작업을 수행하는 방법을 살펴봅니다.

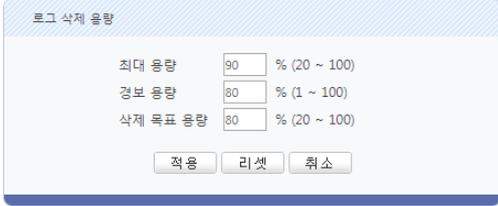
### 로그 레벨 설정하기

기본적으로 WEBFRONT-K의 로그 레벨은 'Notice'로 설정되어 있어서 발생하는 이벤트 중 Notice 레벨 이상만 로그로 저장합니다. 로그 레벨을 다른 값으로 변경하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 통합 로그 - 통합 로그설정 메뉴를 클릭합니다.
2	<로그 레벨>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;로그 레벨 설정&gt; 팝업 창의 드롭다운 목록에서 원하는 로그 레벨을 선택한 후 [적용] 버튼을 클릭합니다. 로그 레벨은 Emergency, Alert, Critical, Error, Warning, Notice, Information 중에서 선택할 수 있습니다. 변경한 로그 레벨은 이후에 발생하는 이벤트부터 바로 적용됩니다. (기본값: Notice)</p> 

### 로그 삭제 용량 설정하기

WEBFRONT-K의 로그 저장 공간이 부족한 경우, 삭제할 로그 용량을 설정할 수 있습니다. 설정한 '최대 용량'을 초과하면 '삭제 목표 용량'이 될 때까지 오래된 로그부터 삭제하며, '경보 용량'이 되면 이메일로 알람을 전송합니다. 로그 삭제 용량을 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 통합 로그 - 통합 로그설정 메뉴를 클릭합니다.
2	<로그 삭제 용량>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;로그 삭제 용량&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [적용] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>최대 용량</b> 저장할 최대 용량 (기본값: 90%)</li> <li>• <b>경보 용량</b> 관리자에게 알람을 전송할 용량 (기본값: 80%)</li> <li>• <b>삭제 목표 용량</b> 최대 용량에 도달한 이후의 목표치 용량 (기본값: 70%)</li> </ul>

## 시스로그 포맷 설정하기

WEBFRONT-K에서 시스로그 서버로 전송되는 로그의 포맷을 설정할 수 있습니다. 시스로그 포맷 설정 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 통합 로그 - 통합 로그설정</b> 메뉴를 클릭합니다.
2	<시스로그 포맷>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;시스로그 포맷 설정&gt; 팝업 창에서 다음 설명을 참고하여 시스로그 포맷을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">시스로그 포맷 설정</p> <p>시스로그 포맷 <input type="text" value="%TIMESTAMP% %\$year% &lt;%pri%&gt; (%syslogseverity-text%) %s"/></p> <p style="text-align: center;"> <input type="button" value="적용"/> <input type="button" value="리셋"/> <input type="button" value="취소"/> </p> </div> <ul style="list-style-type: none"> <li>• 시스로그 포맷           <ul style="list-style-type: none"> <li>- 기본값: %TIMESTAMP% %\$year% &lt;%pri%&gt; (%syslogseverity-text%) %syslogtag%msg%#n</li> <li>- 길이: 1 ~ 1024바이트</li> </ul> </li> </ul> <p> <b>참고:</b> 시스로그 포맷 설정 방법은 아래의 홈페이지 내용을 참고합니다.  <a href="http://www.rsyslog.com/doc/v8-stable/configuration/properties.html">http://www.rsyslog.com/doc/v8-stable/configuration/properties.html</a></p> <p> <b>주의:</b> 시스로그 포맷 설정은 시스로그 기능 전체에 영향을 미치게 되므로 설정에 주의해야 합니다.</p>

## 시스로그 서버 설정하기

WEBFRONT-K에 시스로그 서버가 등록되어 있으면, 이벤트가 발생할 때마다 이벤트에 대한 로그가 등록된 시스로그 서버로 전송됩니다. WEBFRONT-K에 기본적으로 등록되어 있는 시스로그 서버는 없습니다. 다음과 같은 과정을 통해 시스로그 서버를 등록할 수 있습니다. WEBFRONT-K에는 시스로그 서버를 256개까지 추가할 수 있습니다.

순서	설정 과정
1	<b>System - 통합 로그 - 통합 로그설정</b> 메뉴를 클릭합니다.
2	<시스로그 서버 리스트>의 [변경] - [추가] 버튼을 클릭합니다.
3	<p>&lt;시스로그 서버 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [확인] 버튼을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">시스로그 서버 추가</p> <p>상태 <input type="radio"/> 활성화 <input checked="" type="radio"/> 비활성화</p> <p>IP 주소 <input type="text"/></p> <p>포트 <input type="text" value="514"/></p> <p>프로토콜 <input type="text" value="TCP"/></p> <p>레벨 <input type="text" value="Notice"/></p> <p>이벤트 종류 <input type="text" value="없음"/></p> <p>설명 <input type="text"/></p> <p style="text-align: center;"> <input type="button" value="확인"/> <input type="button" value="리셋"/> <input type="button" value="취소"/> </p> </div> <ul style="list-style-type: none"> <li>• <b>상태</b> 현재 설정 중인 시스로그 서버의 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• <b>IP 주소</b> 시스로그 서버의 IP 주소를 입력합니다.</li> <li>• <b>포트</b> 시스로그 서버에서 사용하는 포트를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 514)</li> <li>• <b>프로토콜</b> 시스로그 서버로 로그를 전송할 때 전송 프로토콜을 지정합니다. 프로토콜은 TCP와 UDP 중에서 선택할 수 있습니다. (기본값: TCP)</li> <li>• <b>레벨</b> 시스로그 서버로 전송할 이벤트의 레벨을 지정합니다. 지정한 레벨 이상의 이벤트에 대한 로그만 시스로그 서버로 전송됩니다. 로그 레벨은 emergency, alert, critical, error, warning, notice, information 중에서 선택할 수 있습니다. (기본값: notice)</li> <li>• <b>이벤트 종류</b> 시스로그 서버로 로그를 전송할 때 로그의 facility로 사용할 값을 선택합니다. Facility는 시스로그 서버에서 여러 장비로부터 로그를 수신하는 경우, 어떤 장비로부터 수신한 로그인지를 구분하기 위해 사용하는 값입니다. '없음'을 지정하면 이벤트 종류에 관계없이 모든 로그가 시스로그 서버로 전송됩니다.</li> </ul>

	(기본값: 없음)
	• 설명 시스로그 서버에 대한 설명을 입력합니다. (선택 설정)
4	시스로그 서버를 모두 추가한 후에는 [적용] 버튼을 클릭합니다.

## 사용자 정의 보안로그 포맷 설정하기

WEBFRONT-K에서 시스로그 서버로 전송되는 보안 로그의 항목과 순서를 설정할 수 있습니다. 사용자 정의 보안 로그 포맷의 설정 방법은 다음과 같습니다.

순서	설정 과정
1	System - 통합 로그 - 통합 로그설정 메뉴를 클릭합니다.
2	<사용자 정의 보안로그>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;사용자 정의 보안로그&gt; 영역에서 다음 설명을 참고하여 보안 로그 포맷을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div data-bbox="450 667 1230 1258" data-label="Image"> </div> <p>• 지원 리스트 &lt;지원 리스트&gt;에 있는 필드 값을 선택한 후 [추가]버튼을 클릭하면 &lt;보안로그 형식&gt;에 추가됩니다. 선택시 [Ctrl] 키나 [Shift] 키를 사용하면 여러 개의 필드를 선택할 수 있습니다. &lt;보안로그 형식&gt;에 추가된 필드를 삭제하려면 필드를 선택한 후 [삭제]버튼을 클릭합니다.</p> <ul style="list-style-type: none"> <li>- app_name 애플리케이션의 이름</li> <li>- app_id 애플리케이션의 ID</li> <li>- src_ip 클라이언트의 IP 주소</li> <li>- src_port 클라이언트의 포트 번호</li> <li>- dest_ip 서버의 IP 주소</li> <li>- dest_port 서버의 포트 번호</li> <li>- protocol 프로토콜 (HTTP 또는 HTTPS)</li> <li>- host HTTP Host 헤더값</li> <li>- url HTTP URL 경로</li> <li>- url_param URL 쿼리값</li> <li>- forwarded_for X-forwarded-for 헤더값</li> <li>- sigid 시그니처 ID (시그니처 탐지 시에만 참조)</li> <li>- sig_warning 시그니처 위험도 (시그니처 탐지 시에만 참조)</li> <li>- block 탐지, 차단, 마스크 등의 숫자</li> <li>- owasp OWASP Top10 구분 (2017년도 기준)</li> <li>- detected_time 탐지 시간</li> <li>- desc 내부 탐지 설명 (매칭된 부분으로 표현되지 않는 길이와 같은 부분 설명)</li> <li>- field 탐지된 데이터의 구분자 (예: 쿼리 또는 Payload의 이름)</li> <li>- data 탐지된 데이터</li> <li>- raw_length 증거 데이터의 길이</li> <li>- raw_data 증거 데이터</li> </ul>

• Delimiter

- 필드 구분자로 '/'(슬래시) 또는 '+'(더하기) 기호 중에서 선택합니다. (기본값: , )

• 로그 예제

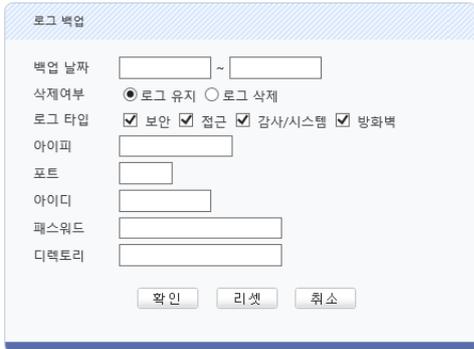
- 설정한 로그 필드와 필드 구분자가 실제로 어떻게 출력되는지 예제를 보여줍니다.

## 로그 백업

로그 메시지는 장비에 발생한 문제를 발견하고 해결하는 데 중요한 역할을 합니다. WEBFRONT-K는 로그의 유실을 예방하기 위해 로그 백업 기능을 제공합니다.

### 로그 수동 백업

WEBFRONT-K 시스템에서 생성 및 저장된 로그를 원격에 있는 SFTP 서버로 백업할 수 있습니다. 로그를 수동으로 백업하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 통합 로그 - 통합 로그설정 메뉴를 클릭합니다.
2	<로그 백업>의 [다운로드] 버튼을 클릭합니다.
	<로그 백업> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [확인] 버튼을 클릭합니다.
	
3	<ul style="list-style-type: none"> <li>• <b>백업 날짜</b> 백업할 로그의 생성 날짜를 선택합니다. 가장 오래된 로그의 날짜부터 현재 시간의 전날까지 지정할 수 있습니다.</li> <li>• <b>삭제 여부</b> 백업된 로그를 WEBFRONT-K에 유지할 것인지 선택합니다. (기본값: 로그 유지) <ul style="list-style-type: none"> <li>- 로그 유지: 백업된 로그를 WEBFRONT-K에서 삭제하지 않습니다.</li> <li>- 로그 삭제: 백업된 로그를 WEBFRONT-K에서 삭제합니다.</li> </ul> </li> <li>• <b>로그 타입</b> 백업할 로그의 종류를 선택합니다. (기본값: 보안, 접근, 감사/시스템, 방화벽)</li> <li>• <b>아이피</b> 로그를 저장할 SFTP 서버의 IP 주소를 입력합니다. 'A.B.C.D' 형식으로 입력합니다.</li> <li>• <b>포트</b> 로그를 저장할 SFTP 서버의 포트 번호를 입력합니다. (설정 범위: 1 ~ 65535)</li> <li>• <b>아이디</b> 로그를 저장할 SFTP 서버로 로그인할 수 있는 ID를 입력합니다. 1~12자까지 입력할 수 있습니다.</li> <li>• <b>패스워드</b> 로그를 저장할 SFTP 서버로 로그인할 수 있는 패스워드를 입력합니다. 1~31자까지 입력할 수 있습니다.</li> <li>• <b>디렉토리</b> 로그가 저장될 경로를 입력합니다. SFTP 서버의 루트 디렉토리를 기준으로 입력합니다. 첫 문자는 반드시 '/'로 시작해야 하고, 1~1024자까지 입력할 수 있습니다. 백업 파일은 압축(tar)파일이며, 압축을 풀면 로그 타입별로 디렉토리가 만들어져 있습니다.</li> </ul>

## 로그 자동 백업

WEBFRONT-K 시스템에서 생성 및 저장된 로그를 지정된 주기마다 원격에 있는 백업서버로 전송합니다. 로그 자동 백업 로그를 기능을 사용하기 위한 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 통합 로그 - 통합 로그설정</b> 메뉴를 클릭합니다.
2	<로그 자동 백업>의 [변경]-[추가] 버튼을 클릭합니다.
	<로그 자동 백업 설정> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [확인] 버튼을 클릭합니다.
	 <p>로그 자동 백업 설정 팝업 창은 다음과 같은 구성을 가지고 있습니다:</p> <ul style="list-style-type: none"> <li>상태: <input checked="" type="radio"/> 활성화 <input type="radio"/> 비활성화</li> <li>로그 타입: <input checked="" type="checkbox"/> 보안 <input checked="" type="checkbox"/> 접근 <input checked="" type="checkbox"/> 감사/시스템 <input checked="" type="checkbox"/> 방화벽</li> <li>주기: [매일] (드롭다운) [ ] 시</li> <li>아이피: [ ]</li> <li>포트: [ ]</li> <li>아이디: [ ]</li> <li>패스워드: [ ]</li> <li>디렉토리: [ ]</li> <li>버튼: [확인] [리셋] [취소]</li> </ul>
3	<ul style="list-style-type: none"> <li>• <b>상태</b> 로그 자동 백업 기능의 사용 여부를 지정합니다. (기본값: 활성화)</li> <li>• <b>로그 타입</b> 백업할 로그의 종류를 선택합니다. (기본값: 보안, 접근, 감사/시스템, 방화벽)</li> <li>• <b>주기</b> 로그 자동 백업을 수행할 주기와 시간을 지정합니다. 기본 주기는 '매일'입니다. 시간은 1시~24시 중에서 입력할 수 있습니다. 설정 주기마다 주기 동안 생성된 로그를 백업합니다. 사용 예는 다음과 같습니다. <ul style="list-style-type: none"> <li>- 매일 10일로 설정할 경우, 지난달 9일~이달 9일까지 생성된 로그가 전송됩니다.</li> <li>- 매주 화요일로 설정할 경우, 저번 주 월요일부터 이번 주 월요일까지 생성된 로그가 전송됩니다.</li> </ul> </li> <li>• <b>아이피</b> 로그를 저장할 SFTP 서버의 IP 주소를 입력합니다. 'A.B.C.D' 형식으로 입력합니다.</li> <li>• <b>포트</b> 로그를 저장할 SFTP 서버의 포트 번호를 입력합니다. (설정 범위: 1 ~ 65535)</li> <li>• <b>아이디</b> 로그를 저장할 SFTP 서버로 로그인할 수 있는 ID를 입력합니다. 1~12자까지 입력할 수 있습니다.</li> <li>• <b>패스워드</b> 로그를 저장할 SFTP 서버로 로그인할 수 있는 패스워드를 입력합니다. 1~31자까지 입력할 수 있습니다.</li> <li>• <b>디렉토리</b> 로그가 저장될 경로를 입력합니다. SFTP 서버의 루트 디렉토리를 기준으로 입력합니다. 첫 문자는 반드시 '/'로 시작해야 하고, 1~1024자까지 입력할 수 있습니다. 백업 파일은 압축(tar)파일이며, 압축을 풀면 로그 타입 별로 디렉토리가 만들어져 있습니다.</li> </ul>

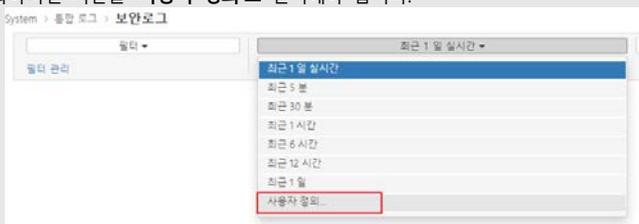
## 로그 파일 업데이트

백업한 로그 파일을 WEBFRONT-K로 업로드할 수 있습니다. 로그 파일을 업데이트하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 통합 로그 - 통합 로그설정</b> 메뉴를 클릭합니다.
2	<로그 파일 업데이트>에서 [파일 선택]을 클릭합니다.
	업로드할 로그 파일을 선택한 후 [파일업로드]를 클릭합니다.
3	 <b>참고:</b> 업로드 파일의 형식은 압축(tar)파일이어야 하고, 업로드 파일의 로그와 WEBFRONT-K 로그의 생성일자가 같으면 업로드한 로그로 대체됩니다.

# 로그 내보내기

로그 내보내기는 WEBFRONT-K에서 검색된 로그를 사용자 PC로 다운로드하는 기능입니다. 로그 내보내기를 하는 방법은 다음과 같습니다.

순서	설정 과정
1	<p><b>System - 통합 로그 - [로그 종류] 메뉴를 클릭합니다.</b></p> <ul style="list-style-type: none"> <li>로그 종류: 보안로그, 감사/시스템 로그, 방화벽 로그, 접근로그</li> </ul> <p>로그 화면에서 검색 조건을 선택한 후, <b>[적용]</b> 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.</p>
2	 <p>The screenshots show the search interface for different log types:         <ul style="list-style-type: none"> <li><b>보안로그 (Security Log):</b> Shows a table with columns for Date, Application, Method, Status, Host, URL, Client IP/Port, Server IP/Port, and Country. A sample entry is shown for an XSS attack.</li> <li><b>감사/시스템 로그 (Audit/System Log):</b> Shows a table with columns for Date, User ID, Application, Message, and Result. A sample entry shows an XML configuration change.</li> <li><b>방화벽 로그 (Firewall Log):</b> Shows a table with columns for Date, Filter Name, Source IP, Destination IP, Protocol, and Message. A sample entry shows a blocked connection.</li> <li><b>접근로그 (Access Log):</b> Shows a table with columns for Date, Application, HTTP(S), HTTP(ver), Host, URL, Client IP/Port, Server IP/Port, and Method. A sample entry shows a GET request for a favicon.</li> </ul> </p>
3	<p><b>[내보내기] 버튼을 클릭합니다.</b></p> <p> <b>참고:</b> [내보내기] 버튼을 활성화하려면 기간을 '사용자 정의'로 선택해야 합니다.</p> 
4	<p>&lt;로그 내보내기&gt; 팝업 창에서 파일 이름을 입력한 후 <b>[저장]</b> 버튼을 클릭합니다. 파일명은 최대 20 글자의 영문자와 숫자, 그리고 <code>w/:*?&lt;&gt; #%</code>를 제외한 특수 문자로 구성될 수 있습니다.</p> 
5	<p><b>System - 통합 로그 - 로그 내보내기 메뉴를 클릭합니다.</b></p> <p>저장한 로그 종류별 메뉴를 클릭한 후 <b>[다운로드]</b> 버튼을 클릭합니다.</p>
6	<p> <b>참고:</b> 다운로드 파일의 형식은 엑셀파일입니다. 하나의 엑셀파일은 최대 10개의 워크시트로 구성되고, 워크시트 당 10,000개의 로그가 기록됩니다. 로그 개수가 100,000개 이상이면 한 개 이상의 엑셀파일이 생성되는데, 이럴 경우 <b>[전체 다운로드]</b> 버튼을 클릭하면 하나의 파일로 압축해서 다운로드됩니다.</p>



## 보안 로그

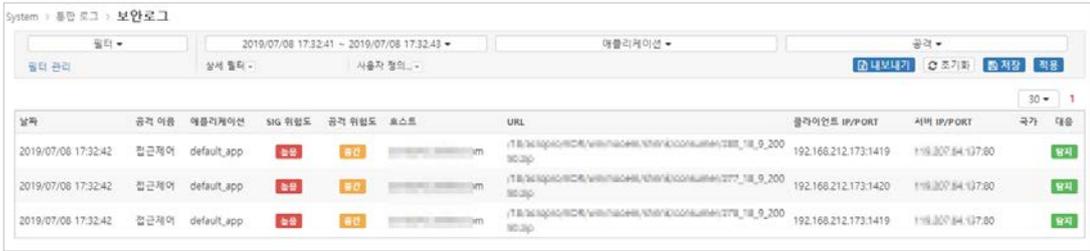
보안 로그는 수신된 패킷이 WEBFRONT-K의 웹 보안 규칙에 위배되는 경우, 패킷에 대한 정보와 어떤 규칙에 의해 위배되었는지 기록하는 로그입니다. WEBFRONT-K의 보안 로그를 조회하는 방법은 다음과 같습니다.

순서	설정 과정
1	<p><b>System - 통합 로그 - 보안로그</b> 메뉴를 클릭합니다.</p> <p>보안 로그 화면에서 필터, 기간, 애플리케이션, 공격 종류를 선택한 후, <b>[적용]</b> 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.</p>
2	<ul style="list-style-type: none"> <li>• 날짜: 로그가 발생한 날짜</li> <li>• 공격 이름: 클라이언트의 공격 이름 또는 공격 종류</li> <li>• 애플리케이션: 대상 애플리케이션의 이름</li> <li>• SIG 위험도: 시그니처 위험도</li> <li>• 공격 위험도: 공격 위험도</li> <li>• 호스트: HTTP 요청 헤더의 호스트 헤더 정보</li> <li>• URL: 클라이언트가 접근을 시도한 URL</li> <li>• 클라이언트 IP/PORT: 클라이언트의 IP 주소와 포트 번호</li> <li>• 서버 IP/PORT: 서버의 IP 주소와 포트 번호</li> <li>• 국가: 클라이언트의 IP 주소에 근거한 국가 정보</li> <li>• 대응: 해당 로그를 처리하였을 때의 대응 방법 (탐지/차단/마스킹/통과(WISE)/검사(WISE))</li> </ul>
3	<p>특정 로그에 대한 상세 정보를 확인하려면 해당 로그를 클릭합니다.</p>

No.	36	날짜	2019/06/26 10:45:00	공격 이름	XSS
공격 이름(자세히)	XSS	애플리케이션	http	App 아이디	2
SIG ID	XSS-00130	SIG 위함도	중간	공격 위함도	중간
호스트	192.168.216.112				
URL	/index.html?cdf=kkk&abc=<script>&asdf=sdwfe;				
클라이언트 IP/PORT	192.168.227.111:38540	서버 IP/PORT	192.168.216.112:80	HTTP(S)	HTTP
WISE ID	-	국가	-	Forwarded for	-
대응	차단	암지여지	요청 바디	필드이름	(%23req%3d%23context.get(%27co%27%2b%27m.open%27%2b%27symphony.xwo%27%2b%27rk2.disp%27%2b%27atcher.Ht
암지여지	<script				
설명	script tag				

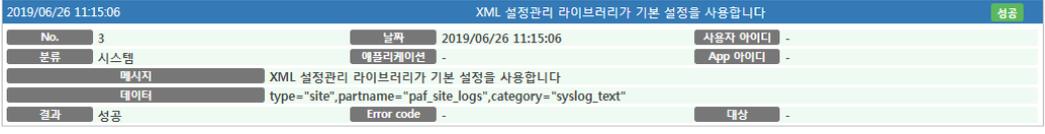
## 시그니처 액션 설정

클라이언트 요청이 시그니처로 탐지 및 차단된 경우 보안 로그의 상세 정보에 해당 시그니처 ID(SIG ID)가 표시됩니다. 이 시그니처 ID를 통해 시그니처 액션을 설정할 수 있습니다. 시그니처 액션은 차단, 탐지, 예외 세가지로 구분됩니다. 다음은 보안 로그 상세화면에서 시그니처의 액션을 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 통합 로그 - 보안로그</b> 메뉴를 클릭합니다.
2	보안 로그 화면에서 필터, 기간, 애플리케이션, 공격 종류를 선택한 후, <b>[적용]</b> 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다. 
3	상세 정보를 조회할 로그를 클릭합니다.
4	상세 정보 화면에서 SIG_ID 항목의 시그니처 아이디를 클릭합니다. 
5	<시그니처> 팝업 창에서 다음 설명을 참고하여 시그니처의 액션을 설정한후 <b>[저장]</b> 버튼을 클릭합니다.  <ul style="list-style-type: none"> <li>• <b>상태</b> 해당 시그니처의 액션을 차단, 탐지, 예외 중에서 지정합니다.</li> <li>• <b>애플리케이션</b> 해당 시그니처의 상태를 적용할 애플리케이션을 선택합니다. <ul style="list-style-type: none"> <li>- 애플리케이션: 해당 공격이 탐지된 애플리케이션에만 적용합니다.</li> <li>- 전체 애플리케이션: 전체 애플리케이션에 적용합니다.</li> </ul> </li> </ul> <p> <b>참고:</b> 설정 내용은 <b>System - 애플리케이션 - 시그니처 관리 - 시그니처 리스트 [변경] - [상세보기]</b> 메뉴에서 확인할 수 있습니다.</p>

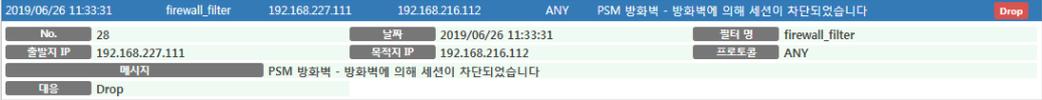
# 감사/시스템 로그

감사/시스템 로그는 관리자가 WEBFRONT-K에서 설정 조회 및 변경에 대한 내용이 기록되어 있는 로그입니다. WEBFRONT-K의 감사/시스템 로그를 조회하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 통합 로그 - 감사/시스템 로그</b> 메뉴를 클릭합니다.
2	<p>감사/시스템 로그 화면에서 필터, 기간, 애플리케이션, 분류를 선택한 후, [적용] 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.</p>  <p> <ul style="list-style-type: none"> <li>• 날짜: 로그가 발생한 날짜</li> <li>• 사용자 아이디: 클라이언트의 공격 이름 또는 공격 종류</li> <li>• 애플리케이션: 대상 애플리케이션의 이름</li> <li>• 메시지: 처리 결과에 대한 설명</li> <li>• 결과: 해당 로그를 처리하였을 때의 설정 결과</li> </ul> </p>
3	<p>특정 로그에 대한 상세 정보를 확인하려면 확인할 로그를 클릭합니다.</p> 

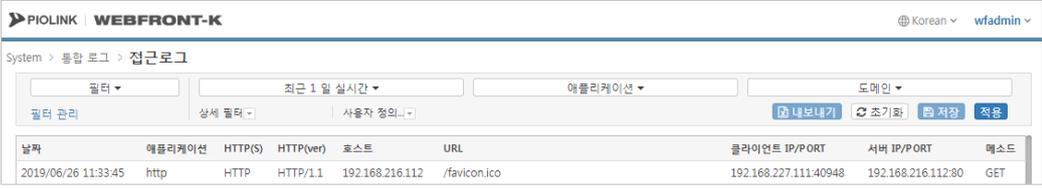
# 방화벽 로그

방화벽 로그는 수신된 패킷이 WEBFRONT-K에 설정된 방화벽 정책에 위배되는 경우, 패킷에 대한 정보와 어떤 규칙에 의해 위배되었는지를 기록하는 로그입니다. WEBFRONT-K의 방화벽 로그를 조회하는 방법은 다음과 같습니다.

순서	설정 과정
1	<p><b>System - 통합 로그 - 방화벽 로그</b> 메뉴를 클릭합니다.</p> <p>방화벽 로그 화면에서 필터, 기간, 프로토콜, 대응을 선택한 후, <b>[적용]</b> 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.</p> 
2	<ul style="list-style-type: none"> <li>• <b>날짜</b>            로그가 발생한 날짜</li> <li>• <b>필터명</b>        방화벽 필터 이름</li> <li>• <b>출발지 IP</b>    패킷의 출발지 IP 주소</li> <li>• <b>목적지 IP</b>    패킷의 목적지 IP 주소</li> <li>• <b>프로토콜</b>    방화벽 필터에 의해 탐지된 패킷의 프로토콜 (TCP/UDP/ICMP)</li> <li>• <b>메시지</b>        해당 대응에 대한 설명</li> <li>• <b>대응</b>          방화벽 필터에 정의된 액션(Permit, Drop, Reject, Rate Limit)</li> </ul>
3	<p>특정 로그에 대한 상세 정보를 확인하려면 <b>확인할 로그</b>를 클릭합니다.</p> 

# 접근 로그

접근 로그는 WEBFRONT-K로 클라이언트의 요청 패킷이 수신될 때마다 해당 패킷에 대한 정보를 기록하는 로그입니다. WEBFRONT-K의 접근 로그를 조회하는 방법은 다음과 같습니다.

순서	설정 과정
1	<p><b>System - 통합 로그 - 접근로그</b> 메뉴를 클릭합니다.</p> <p>접근 로그 화면에서 필터, 기간, 애플리케이션, 도메인을 선택한 후, <b>[적용]</b> 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.</p> 
2	<ul style="list-style-type: none"> <li>• 날짜: 로그가 발생한 날짜</li> <li>• 애플리케이션: 대상 애플리케이션의 이름</li> <li>• HTTP(S): 전송 프로토콜</li> <li>• HTTP(ver): HTTP 버전</li> <li>• 호스트: 클라이언트 헤더의 Host 필드값</li> <li>• URL: 클라이언트가 접근을 시도한 URL</li> <li>• 클라이언트 IP/PORT: 클라이언트의 IP 주소와 포트 번호</li> <li>• 서버 IP/PORT: 서버의 IP 주소와 포트 번호</li> <li>• 메소드: 클라이언트가 사용한 HTTP 메소드</li> </ul>
3	<p>특정 로그에 대한 상세 정보를 확인하려면 확인할 로그를 클릭합니다.</p> 

## 제6장 통합 보고서

통합 보고서는 WEBFRONT-K의 종합적인 정보를 요약하여 장비 현황과 네트워크 상태를 손쉽게 파악할 수 있는 기능입니다. 관리자는 보고서를 생성한 후 PDF, HTML, Word 형식의 파일로 다운로드 받을 수 있습니다.

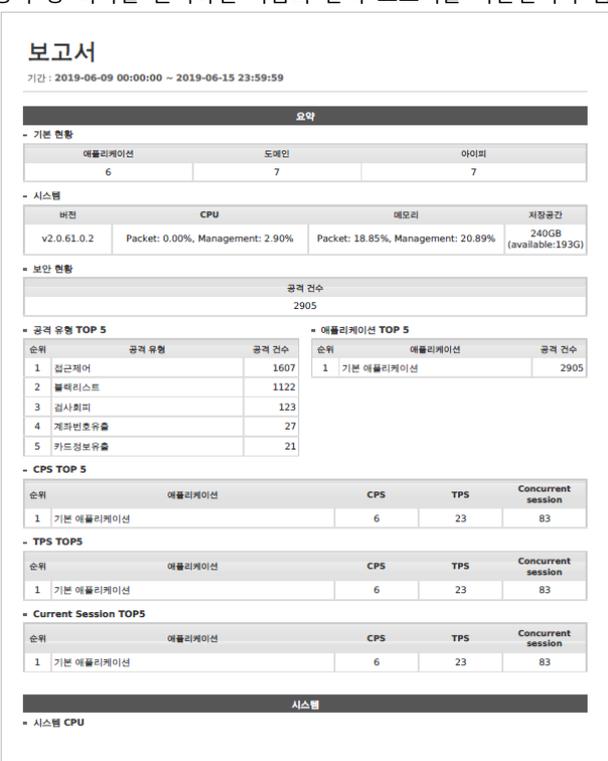
이 장은 다음 내용으로 구성됩니다.

- 통합 보고서 생성하기
- 통합 보고서 스케줄 설정하기



# 통합 보고서 생성하기

통합 보고서를 생성하는 방법은 다음과 같습니다.

순서	설정 과정
1	<p><b>System - 통합 보고서</b> 메뉴를 클릭합니다.</p>
2	<p>&lt;통합 보고서&gt;의 기간과 애플리케이션을 지정한 후 [추가] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>기간</b> 보고서를 생성할 기간을 년, 월, 일 순서로 지정합니다.</li> <li>• <b>애플리케이션</b> 보고서를 생성할 애플리케이션을 선택합니다. 모두 선택하려면 <input type="checkbox"/>모두 선택 옵션에 체크표시를 합니다.</li> </ul>
3	<p>&lt;통합 보고서 리스트&gt;에 추가한 보고서가 표시됩니다. 파일 항목의 상태가 '대기' → PDF 생성 중 → PDF, HTML, DOC, XLSX 중 원하는 형태의 파일을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>순서</b> 보고서가 생성된 순서입니다.</li> <li>• <b>목록</b> &lt;통합 보고서&gt;에서 지정한 보고서의 기간입니다.</li> <li>• <b>요청 시간</b> 보고서 생성을 요청한 시간입니다.</li> <li>• <b>완료 시간</b> 보고서 생성을 완료한 시간입니다.</li> <li>• <b>파일</b> 보고서의 파일 형식을 선택합니다. (PDF, HTML, DOC, XLSX)</li> <li>• <b>삭제</b> &lt;통합 보고서 리스트&gt;에서 특정 보고서를 삭제하려면 [삭제] 버튼을 클릭합니다.</li> </ul>
4	<p>파일 항목에서 보고서의 파일 형식 중 하나를 클릭하면 다음과 같이 보고서를 다운받거나 웹 페이지로 열 수 있습니다.</p>  <p>보고서에 포함되는 내용은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>• <b>요약</b> <ul style="list-style-type: none"> <li>- 기본 현황: 애플리케이션/도메인/아이피 주소 현황이 표시됩니다.</li> <li>- 시스템: 시스템에 설치된 PLOS버전과 시스템의 CPU/메모리/저장공간이 표시됩니다.</li> </ul> </li> </ul>

- 보안 현황: WEBFRONT-K가 탐지 및 차단한 총 공격 건수가 표시됩니다.
- 공격 유형 TOP 5: WEBFRONT-K에서 탐지 및 차단된 공격 유형 TOP 5가 표시됩니다.
- 애플리케이션 TOP 5: WEBFRONT-K에서 탐지 및 차단된 공격 건수에 대한 애플리케이션 TOP 5가 표시됩니다.
- CPS TOP 5: 애플리케이션별 CPS TOP 5가 표시됩니다.
- TPS TOP 5: 애플리케이션별 TPS TOP 5가 표시됩니다.
- Current Session TOP 5: 애플리케이션별 Current Session TOP 5가 표시됩니다.

• 시스템

- 시스템 CPU: WEBFRONT-K 시스템의 CPU 사용량에 대한 그래프가 표시됩니다.
- 시스템 메모리: WEBFRONT-K 시스템의 메모리 사용량에 대한 그래프가 표시됩니다.
- 시스템 저장공간: WEBFRONT-K 시스템의 저장공간 사용량에 대한 그래프가 표시됩니다.

• 보안 현황

- 공격 유형: 공격 유형별 공격 건수를 나타내는 표와 그래프가 표시됩니다.
- 애플리케이션: 애플리케이션별 공격 건수를 나타내는 표와 그래프가 표시됩니다.
- 애플리케이션: 기본 애플리케이션(공격 유형): 기본 애플리케이션의 공격 건수를 나타내는 표와 그래프가 표시됩니다.
- 애플리케이션: [애플리케이션 이름](공격 유형): 애플리케이션 이름별 공격 건수를 나타내는 표와 그래프가 표시됩니다.

• 네트워크 상태

- [애플리케이션 이름] CPS/TPS/Concurrent session: 애플리케이션 이름별 CPS/TPS/Concurrent session를 나타내는 표와 그래프가 표시됩니다.
- 기본 애플리케이션 CPS/TPS/Concurrent session: 기본 애플리케이션의 CPS/TPS/Concurrent session를 나타내는 표와 그래프가 표시됩니다.

# 통합 보고서 스케줄 설정하기

WEBFRONT-K의 통합 보고서를 스케줄에 따라 자동으로 생성할 수 있습니다. 보고서 스케줄을 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 통합 보고서</b> 메뉴를 클릭합니다.
2	<통합 보고서 일정>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;통합 보고서 일정&gt; 팝업 창에서 보고서가 생성되는 일정을 지정한 후, [적용] 버튼을 클릭합니다. 일정은 복수 선택이 가능합니다.</p> <div data-bbox="598 519 1093 728" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• <b>전체</b>      일단위, 주단위, 월단위로 각각 보고서를 생성합니다.</li> <li>• <b>일단위</b>    매일 오전 3시에 하루 전 데이터를 이용한 보고서를 생성합니다.</li> <li>• <b>주단위</b>    매주 일요일 오전 3시에 지난 일요일부터 토요일까지의 데이터를 이용한 보고서를 생성합니다.</li> <li>• <b>월단위</b>    매월 1일 오전 3시에 이전 달 데이터를 이용한 보고서를 생성합니다.</li> </ul>

## 제7장 애플리케이션

이 장에서는 WEBFRONT-K의 웹 보안 기능으로 보호할 애플리케이션을 등록하고 관리하는 방법과 애플리케이션의 각 보안 기능을 설정할 때 사용되는 정규식을 정의하는 방법, 그리고, 웹 보안 기능에서 사용하는 시그니처를 업데이트하는 방법에 대해서 알아봅니다.

이 장은 다음 내용으로 구성됩니다.

- 애플리케이션 관리
- 애플리케이션 설정 보기
- 애플리케이션 설정 간편화
- 고급 첨부파일 검사 설정
- 시그니처 관리
- 시그니처 내보내기
- 정규식 설정
- 블랙리스트 관리
- 화이트리스트 관리



# 애플리케이션 관리

이 절에서는 WEBFRONT-K의 보안 기능으로 보호할 애플리케이션을 등록하는 방법을 살펴봅니다.

## 개요

WEBFRONT-K의 기본적인 시스템 설정이나 네트워크 설정을 끝낸 후에는 애플리케이션을 등록하고 설정해야 합니다. 애플리케이션은 WEBFRONT-K의 웹 보안 기능을 적용하는 단위로, 각 애플리케이션 별로 적용할 보안 정책과 관리자를 설정할 수 있습니다.

애플리케이션은 웹 페이지 그룹입니다. www.piolink.com과 같이 웹 사이트의 모든 웹 페이지일 수도 있고, www.piolink.com/korea와 같이 웹 사이트의 일부 웹 페이지만으로 구성될 수도 있고, www.piolink.com/support.html과 같이 하나의 웹 페이지로 이루어질 수도 있습니다.

애플리케이션은 통합 관리자나 사이트 관리자가 WEBFRONT-K의 System 메뉴를 사용하여 등록하거나 수정 및 삭제할 수 있습니다. 애플리케이션을 등록하고 나면, 애플리케이션 관리자가 Application 메뉴를 사용하여 애플리케이션과 관련된 각종 설정 작업을 수행할 수 있습니다 (물론, 통합 관리자나 사이트 관리자도 애플리케이션을 설정할 수 있습니다). Application 메뉴를 사용하여 설정 작업을 하는 방법은 이 설명서와 함께 제공되는 **WEBFRONT-K 애플리케이션 구성 설명서**를 참고합니다.

## 애플리케이션 생성 마법사(Wizard)

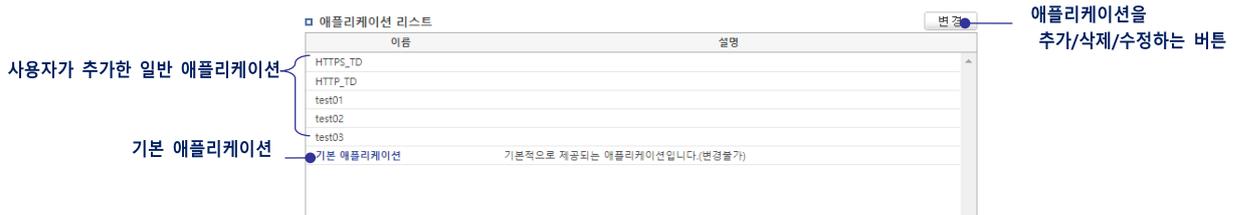
WEBFRONT-K는 좀더 간편하게 애플리케이션을 등록하고 설정할 수 있는 애플리케이션 생성 마법사(wizard)를 지원합니다. 마법사를 사용하지 않으면 애플리케이션을 추가한 후, Application 메뉴들(일반 설정, 응답 설정 등)을 사용하여 애플리케이션을 설정해야 합니다. 마법사를 사용하면 Application 메뉴에서 설정해야 하는 애플리케이션의 IP 주소와 포트, 도메인 정보와 같은 일반 설정과 웹 공격에 대한 응답 설정까지 한꺼번에 할 수 있습니다.

## 기본 애플리케이션

WEBFRONT-K에는 기본적으로 기본 애플리케이션(default application)이 등록되어 있습니다. 기본애플리케이션은 사용자가 등록한 일반 애플리케이션에 해당하지 않는 트래픽에 적용되는 애플리케이션입니다. 기본적으로 일반 애플리케이션에 속하지 않는 트래픽 중에서 '80' 포트를 통해 수신된 트래픽에 기본 애플리케이션이 적용됩니다. 하지만, 클라이언트의 IP 주소와 포트, 서버 IP 주소와 포트를 사용하여 기본 애플리케이션을 적용할 트래픽의 조건을 지정할 수 있습니다. 그러면, 해당 IP 주소와 포트의 클라이언트가 전송하고, 해당 IP 주소와 포트의 서버가 수신한 트래픽에만 기본 애플리케이션이 적용됩니다. 기본 애플리케이션을 설정하는 방법은 **WEBFRONT-K 애플리케이션 구성 설명서**의 [제6장 애플리케이션 기본 설정]을 참고합니다.

## 애플리케이션 보기

현재 WEBFRONT-K에 등록되어 있는 애플리케이션을 보려면 **System** 메뉴 중에서 **애플리케이션 - 애플리케이션 관리** 메뉴를 클릭합니다. 그러면, 현재 등록된 애플리케이션 목록을 보여주는 <애플리케이션 리스트> 화면이 나타납니다.



위 화면에는 여러 개의 애플리케이션이 등록되어 있지만, 기본적으로 가장 아래에 있는 '기본 애플리케이션'만 등록되어 있습니다.

## 직접 애플리케이션 추가하기

WEBFRONT-K에 애플리케이션을 추가하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 애플리케이션 관리</b> 메뉴를 클릭합니다.
2	<애플리케이션 리스트>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<애플리케이션 설정> 화면에서 <b>[추가]</b> 버튼을 클릭합니다.
4	<p>&lt;애플리케이션 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 <b>[확인]</b> 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li><b>이름</b> 애플리케이션의 이름을 입력합니다. 애플리케이션의 이름은 알파벳과 숫자, '_'를 사용하여 1 ~ 255 자의 문자열로 지정해야 합니다.</li> <li><b>설명</b> 애플리케이션에 대한 설명을 입력합니다. 한글과 알파벳, 숫자, 특수 문자 등을 사용하여 최대 128자까지 입력할 수 있습니다. (선택 설정)</li> </ul>
5	<p>다른 애플리케이션을 더 추가하려는 경우에는 3~4번 과정을 반복합니다.</p> <p> <b>참고:</b> 애플리케이션의 최대개수는 장비 모델별로 다르게 적용됩니다. 다음 설명을 참고하여 애플리케이션을 추가하도록 합니다.</p> <ul style="list-style-type: none"> <li>• WEBFRONT-K1800: 50개</li> <li>• WEBFRONT-K3200: 250개</li> <li>• WEBFRONT-K4300: 500개</li> <li>• WEBFRONT-K4600: 500개</li> <li>• WEBFRONT-K5200: 1000개</li> <li>• WEBFRONT-K5600: 1000개</li> <li>• 이외 모델: 255개</li> </ul>
6	애플리케이션을 모두 추가한 후에는 <b>[적용]</b> 버튼을 눌러 추가한 애플리케이션 정보를 저장하고 시스템에 적용합니다.



**참고: Application - 애플리케이션 - 애플리케이션 관리** 메뉴에서 직접 애플리케이션을 추가하는 경우, 해당 애플리케이션의 보안 기능(요청검사, 콘텐츠보호)과 시그니처 상태는 기본값이 적용됩니다.

- 보안 기능: 전체 기능 비활성화
- 시그니처 상태: 기본 시그니처

## 마법사로 애플리케이션 추가하기

이번에는 애플리케이션 생성 마법사를 사용하여 간편하게 애플리케이션을 추가하고 애플리케이션의 기본 설정 작업까지 수행하는 방법을 살펴봅니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 애플리케이션 관리</b> 메뉴를 클릭합니다.
2	<애플리케이션 생성 마법사>의 <b>[마법사 실행]</b> 버튼을 클릭합니다.
3	애플리케이션 생성 마법사의 첫 화면에서는 애플리케이션의 일반 설정 정보를 지정할 수 있습니다. 다음 설명을 참고하여 각 항목의 값을 입력한 후 <b>[IP/포트 리스트]</b> 버튼이나 오른쪽아래에 있는  버튼을 클릭합니다.



- **이름** 애플리케이션의 이름을 입력합니다. 애플리케이션의 이름은 알파벳과 숫자, '\_'를 사용하여 1 ~ 255 자의 문자열로 지정해야 합니다.
- **상태** 애플리케이션의 상태를 지정합니다. 애플리케이션을 추가하는 즉시 활성화하려면 '활성화'를, 그렇지 않으면 '비활성화'를 지정합니다. (기본값: 활성화)
- **모드** 애플리케이션의 동작 모드를 지정합니다. 다음 모드 중 하나를 선택합니다.
  - 일반: 애플리케이션이 실행되는 웹 서버에 부하 분산 기능을 적용하지 않는 경우(기본 설정)
  - 부하분산: 애플리케이션이 실행되는 웹 서버에 부하 분산 기능을 적용하는 경우
  - 고속: 일반 모드에 비해 사용할 수 있는 보안 기능은 제한되지만 보다 빠른 속도로 서비스를 제공해야 하는 경우
  - 미러링: WEBFRONT-K를 IDS 장비와 같이 미러링된 패킷을 검사하는 용도로 사용하는 경우
- **설명** 애플리케이션에 대한 설명을 입력합니다. 한글과 알파벳, 숫자, 특수 문자 등을 사용하여 최대 128자까지 입력할 수 있습니다. (선택 설정)

4 애플리케이션의 IP 주소와 포트를 설정할 수 있는 화면에서 [추가] 버튼을 클릭합니다.

<IP/포트 추가> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 지정한 후 [확인] 버튼을 클릭합니다. IP 주소와 포트를 더 추가하려면 4 ~ 5번 과정을 동일하게 수행합니다. 애플리케이션에는 최대 1024개의 IP 주소/포트를 추가할 수 있습니다.



- **상태** 현재 등록하고 있는 IP 주소와 포트의 사용 여부를 지정합니다. (기본값: 활성화)
- **IP 버전** 애플리케이션의 IP 버전을 지정합니다. (기본값: IPv4)
- **IP 주소** 애플리케이션으로 접속할 때 사용할 IP 주소를 입력합니다. 애플리케이션의 동작 모드를 '부하 분산'으로 지정한 경우에는 가상 IP 주소를 입력할 수 있습니다. 가상 IP 주소를 입력하는 경우에는 'IP 트랜스패런트' 항목을 '비활성화'로 설정해야 합니다.
- **포트** 애플리케이션으로 접속할 때 사용할 포트 번호를 입력합니다. 애플리케이션의 동작 모드를 '부하 분산'으로 지정한 경우에는 가상 포트 번호를 입력할 수 있습니다. 가상 포트를 입력하는 경우에는 'IP 트랜스패런트' 항목을 '비활성화'로 설정해야 합니다. (설정 범위: 1 ~ 65535)
- **IP 트랜스패런트** 입력한 IP 주소와 포트가 가상(virtual)의 값인지 실제 값인지를 지정합니다. 실제 값이면 '활성화'를, 가상의 값이면 '비활성화'를 선택합니다. (기본값: 활성화)
- **유형** 애플리케이션의 패킷 유형이 HTTP 인지 HTTPS인지를 지정합니다. SSL 기능을 통해 암호화된 트래픽이 송수신되는 경우에는 'HTTPS'를, 그 이외에는 'HTTP'를 선택합니다. (기본값: HTTP)
- **설명** IP 주소와 포트에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열로 지정할 수 있습니다.

6 IP 주소와 포트를 모두 추가하였으면 [도메인 리스트] 버튼이나 버튼을 클릭합니다.

7 애플리케이션의 도메인을 설정할 수 있는 화면에서 [추가] 버튼을 클릭합니다.

8 <도메인 추가> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [확인] 버튼을 클릭합니다. 도메인을 더 추가

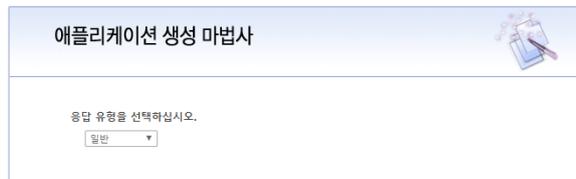
하려면 8 ~ 9번 과정을 동일하게 수행합니다. 하나의 애플리케이션에는 최대 256개의 도메인을 추가할 수 있습니다.



- **상태** 현재 등록하고 있는 도메인의 사용 여부를 지정합니다. (기본값: 활성화)
- **도메인 이름** 도메인의 이름을 입력합니다. 도메인 이름은 알파벳과 '.' 등의 기호로 구성된 최대 256 글자의 문자열로 지정할 수 있습니다.
- **설명** 도메인에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열로 지정할 수 있습니다. (선택 설정)

9 도메인을 모두 추가하였으면 [응답 설정] 버튼이나 버튼을 클릭합니다.

애플리케이션의 응답 방법을 설정할 수 있는 화면에서 드롭다운 목록을 클릭하여 응답 방식을 지정한 후 필요한 값을 설정합니다.



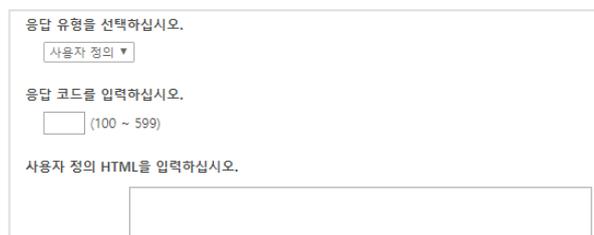
다음 5가지 유형 중에서 애플리케이션을 대상으로 한 웹 공격을 발견했을 때 취할 조치의 유형을 선택합니다.

- **일반** 기본적으로 설정된 응답 메시지를 보냅니다. (기본 설정)
- **응답 없음** 아무런 응답 메시지도 보내지 않습니다.
- **접속 종료** 해당 클라이언트와의 접속을 종료합니다.
- **리다이렉트** 클라이언트가 요청한 URL 대신 사용자가 설정한 다른 URL(에러 페이지, 시작 페이지 등)을 보냅니다. 이 항목을 선택하면 URL을 설정할 수 있는 항목(리다이렉트 URL)이 나타납니다. 리다이렉트 URL 항목에 요청한 URL 대신 전송할 URL을 입력합니다. 입력 가능한 URL의 최대 길이는 256자입니다.

10



- **사용자 정의** 사용자가 직접 정의한 응답 메시지를 보냅니다. 이 항목을 선택하면 응답 코드를 입력하는 항목(응답 코드)과 사용자가 응답 메시지를 정의할 수 있는 항목(사용자 정의 HTML)이 나타납니다. 응답 코드 항목에 100~599 범위의 응답 코드 번호를 입력하고, 사용자 정의 HTML 항목에는 클라이언트에게 전송할 페이지 내용을 알파벳과 한글로 이루어진 최대 1024글자의 문자열로 입력합니다.



11 응답설정을 모두 추가하였으면 [상태/모드] 버튼이나 버튼을 클릭합니다.

12 보안 기능 및 시그니처의 상태를 지정합니다.

## 애플리케이션 생성 마법사



보안기능 상태를 선택하십시오.

- 전체 기능 비활성화    기본 기능 활성화    애플리케이션 복사    전체 기능 활성화

시그니처의 상태를 선택하십시오.

- 기본 시그니처 상태    시그니처 전체 탐지    시그니처 전체 차단

### • 보안기능 상태

보안 기능의 활성화 상태를 지정합니다. 보안 기능은 **Application** 메뉴의 **요청검사, 콘텐츠보호**입니다.

- 전체 기능 비활성화: 전체 보안 기능을 비활성화합니다. (기본값)
- 기본 기능 활성화: 기본 보안 기능을 활성화합니다. 기본 보안 기능 메뉴는 다음과 같습니다.

매뉴 이름				
Application	요청검사	접근제어	신용카드정보유입차단	
		디렉토리리스팅차단	주민등록정보유입차단	
		검사회피차단	다운로드검사	
		요청형식검사	금치어차단	
		웹공격프로그램차단	업로드검사	
		SQL삼입차단	과다요청제어	
		스크립트삼입차단	WISE 요청필터	
		인클루드인젝션차단		
		콘텐츠보호	신용카드정보유출차단	주민등록번호유출차단
			계좌번호정보유출차단	

- 애플리케이션 복사:      선택한 애플리케이션의 보안 기능 상태와 설정을 그대로 적용합니다.
- 전체 기능 활성화:      전체 보안 기능을 활성화합니다.

### • 시그니처 상태

시그니처 상태(탐지/차단)를 지정합니다. 시그니처 상태는 **System - 애플리케이션 - 시그니처관리 - 시그니처 리스트** 메뉴에 적용됩니다.

- 기본 시그니처 상태: 시그니처의 액션을 기본값으로 적용합니다. (기본값)
- 시그니처 전체 탐지: 전체 시그니처의 액션을 '탐지'로 지정합니다.
- 시그니처 전체 차단: 전체 시그니처의 액션을 '차단'으로 지정합니다.

13 애플리케이션 응답 설정 항목들을 모두 설정하였으면 [적용] 버튼을 클릭합니다.

## 애플리케이션 전체 세션 삭제

애플리케이션 전체 세션 삭제는 WEBFRONT-K에 연결되어 있는 전체 세션을 삭제하는 기능입니다.

다음은 애플리케이션 전체 세션을 삭제하는 방법입니다.

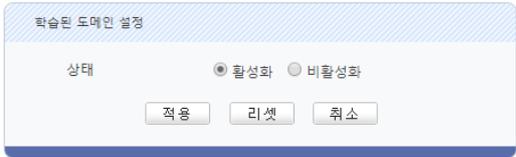
순서	설정 과정
1	<b>System - 애플리케이션 - 애플리케이션 관리</b> 메뉴를 클릭합니다.
2	<애플리케이션 전체 세션 삭제>에서 [지움] 버튼을 클릭합니다.
3	전체 애플리케이션 세션 정보 삭제 확인 팝업 창이 나타나면 [확인]을 클릭합니다.

## 도메인 학습

도메인 학습은 클라이언트의 요청 도메인 정보를 기록하는 기능으로, 도메인 이름, 애플리케이션 이름, 서버 IP 주소, 서버 포트 정보를 기록합니다. 관리자는 학습을 통해 얻은 정보를 이용하여 애플리케이션별 접속 정보 및 애플리케이션에 등록되지 않은 접속 정보까지 확인할 수 있습니다.

### 도메인 학습 상태 설정하기

다음은 도메인 학습 기능의 상태를 설정하는 방법입니다.

순서	설정 과정
1	System - 애플리케이션 - 애플리케이션 관리 메뉴를 클릭합니다.
2	<도메인 학습>의 [변경] 버튼을 클릭합니다.
3	<도메인 학습> 에서 [변경] 버튼을 클릭합니다.
4	<p>&lt;학습된 도메인 설정&gt; 팝업 창에서 상태를 설정한 후 [적용] 버튼을 클릭합니다.</p>  <p>팝업 창 '학습된 도메인 설정'의 상태 설정 화면입니다. '상태' 섹션에 '활성화'와 '비활성화' 두 옵션이 있으며, '활성화'가 선택되어 있습니다. '적용', '리셋', '취소' 버튼이 하단에 배치되어 있습니다.</p>

### 도메인 학습 내용 조회하기

다음은 도메인 학습 기능으로 학습된 도메인을 조회하는 방법입니다.

순서	설정 과정																
1	System - 애플리케이션 - 애플리케이션 관리 메뉴를 클릭합니다.																
2	<도메인 학습>의 [변경] 버튼을 클릭합니다.																
3	<p>&lt;학습된 도메인&gt;을 확인합니다.</p>  <p>도메인 학습 관리 화면의 '학습된 도메인' 섹션입니다. '도메인 학습' 항목이 활성화된 상태(활성화)로 표시되어 있습니다. '학습된 도메인' 목록은 다음과 같습니다.</p> <table border="1"> <thead> <tr> <th>도메인 이름</th> <th>애플리케이션 이름(ID)</th> <th>아이피</th> <th>포트</th> </tr> </thead> <tbody> <tr> <td>172.16.200.251</td> <td>00_HTTP_redmine(1)</td> <td>172.16.200.251</td> <td>80</td> </tr> <tr> <td>172.16.200.251</td> <td>default_app(255)</td> <td>172.16.200.251</td> <td>80</td> </tr> <tr> <td>172.16.200.251</td> <td>00_HTTPS_redmine(2)</td> <td>172.16.200.251</td> <td>443</td> </tr> </tbody> </table>	도메인 이름	애플리케이션 이름(ID)	아이피	포트	172.16.200.251	00_HTTP_redmine(1)	172.16.200.251	80	172.16.200.251	default_app(255)	172.16.200.251	80	172.16.200.251	00_HTTPS_redmine(2)	172.16.200.251	443
도메인 이름	애플리케이션 이름(ID)	아이피	포트														
172.16.200.251	00_HTTP_redmine(1)	172.16.200.251	80														
172.16.200.251	default_app(255)	172.16.200.251	80														
172.16.200.251	00_HTTPS_redmine(2)	172.16.200.251	443														

# 애플리케이션 설정 보기

이 절에서는 WEBFRONT-K의 애플리케이션 설정 보기 기능에 대해 알아봅니다.

## 개요

WEBFRONT-K의 애플리케이션 설정 보기 기능은 등록된 애플리케이션의 정보와 각 애플리케이션의 일반 설정, 요청 검사, 콘텐츠 보호 기능에 대한 설정 정보를 화면이나 파일로 출력하는 기능입니다. 이 설정 보기 기능은 다음과 같은 세부 기능들로 구성되어 있습니다.

- 설정 출력 기능
- 현재 설정과 SSD 메모리에 저장된 설정 비교 기능
- 설정 다운로드 기능

각 기능에 대해 알아봅니다.

### 설정 출력

설정 출력 기능은 SDRAM에 있는 현재 설정이나 SSD 메모리의 특정 저장 공간(공간 #1, #2, #3)에 저장된 설정 정보를 화면에 출력해주는 기능입니다. 전체 설정 정보를 출력할 수도 있고 특정 기능에 대한 설정 정보만 출력할 수도 있습니다. 설정 정보는 애플리케이션 단위로 출력되고, 출력되는 순서는 메뉴 트리에 있는 메뉴의 순서와 설정 화면에 출력되는 항목의 순서와 동일합니다. 이 기능을 사용하면 애플리케이션 설정 정보를 애플리케이션 별로 한꺼번에 일목요연하게 볼 수 있습니다.

### 설정 비교

설정 비교 기능은 SDRAM에 있는 현재 설정과 SSD 메모리의 특정 저장 공간에 저장된 설정 정보를 비교할 수 있도록 두 설정 정보를 모두 보여주는 기능입니다. 출력하는 방법에는 2가지가 있는데, 두 설정 전체를 메뉴 별로 나란히 보여주는 방법과 두 설정 중 동일한 이름의 애플리케이션 설정을 비교하여 서로 다른 부분만 보여주는 방법이 있습니다. 서로 다른 설정을 보여주는 경우에는 이름이 같은 애플리케이션 간에만 비교하기 때문에 만약 두 설정에 같은 이름의 애플리케이션이 없으면 출력되는 정보는 없습니다.

설정 비교 기능에 의해 출력된 설정 정보는 색상을 통해 정보의 종류를 나타냅니다.

- 흰색: 하위 항목까지 포함하여 설정이 완전히 동일한 항목
- 분홍색: 항목은 같지만 설정은 다른 경우
- 하늘색: 현재 설정에는 있지만 SSD의 설정에는 없는 항목
- 연두색: SSD의 설정에는 있지만 현재 설정에는 없는 항목

설정 비교 기능은 전체 설정을 모두 비교하여 출력할 것인지 일부 항목의 설정만 비교할 것인지를 선택할 수 있습니다. 설정 비교 기능은 현재 설정이 SSD에 저장한 설정과 어떤 부분이 다른지 확인하여 어떤 설정 작업이 이루어졌는지를 알아내고자 할 때 사용하면 유용합니다.

### 설정 다운로드

설정 보기 기능을 통해 출력되는 설정 정보는 화면으로 출력할 뿐만 아니라 HTML 파일 형태로 다운로드할 수 있습니다. HTML 파일에 저장되는 설정 정보는 화면으로 출력되는 설정 정보와 내용 및 순서가 동일합니다.

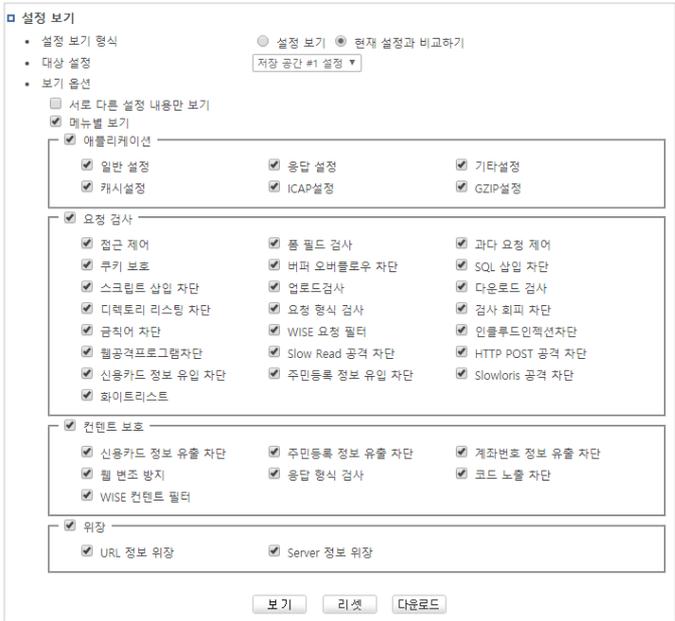
# 설정 출력하기

현재 설정이나 SSD의 특정 저장 공간에 저장된 설정 정보를 출력하는 방법은 다음과 같습니다.

순서	설정 과정																																									
1	<p><b>System - 애플리케이션 - 애플리케이션 설정 보기를 클릭합니다.</b></p>																																									
2	<p>&lt;설정 보기&gt; 화면에서 다음 설명을 참고하여 각 항목을 설정한 후 [보기] 버튼을 클릭합니다.</p> <div data-bbox="507 409 1184 999" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p><b>□ 설정 보기</b></p> <ul style="list-style-type: none"> <li>• 설정 보기 형식 <span style="float: right;"><input checked="" type="radio"/> 설정 보기 <input type="radio"/> 현재 설정과 비교하기</span></li> <li>• 대상 설정 <span style="float: right;">현재 설정 ▼</span></li> <li>• 보기 옵션</li> </ul> <p><input checked="" type="checkbox"/> 메뉴별 보기</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p><input checked="" type="checkbox"/> 애플리케이션</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td><input checked="" type="checkbox"/> 일반 설정</td> <td><input checked="" type="checkbox"/> 응답 설정</td> <td><input checked="" type="checkbox"/> 기타설정</td> </tr> <tr> <td><input checked="" type="checkbox"/> 캐시설정</td> <td><input checked="" type="checkbox"/> ICAP설정</td> <td><input checked="" type="checkbox"/> GZIP설정</td> </tr> </table> </div> <p><input checked="" type="checkbox"/> 요청 검사</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td><input checked="" type="checkbox"/> 접근 제어</td> <td><input checked="" type="checkbox"/> 폼 필드 검사</td> <td><input checked="" type="checkbox"/> 과다 요청 제어</td> </tr> <tr> <td><input checked="" type="checkbox"/> 쿠키 보호</td> <td><input checked="" type="checkbox"/> 바피 오버플로우 차단</td> <td><input checked="" type="checkbox"/> SQL 삽입 차단</td> </tr> <tr> <td><input checked="" type="checkbox"/> 스크립트 삽입 차단</td> <td><input checked="" type="checkbox"/> 업로드검사</td> <td><input checked="" type="checkbox"/> 다운로드 검사</td> </tr> <tr> <td><input checked="" type="checkbox"/> 디렉토리 리스팅 차단</td> <td><input checked="" type="checkbox"/> 요청 형식 검사</td> <td><input checked="" type="checkbox"/> 검사 회피 차단</td> </tr> <tr> <td><input checked="" type="checkbox"/> 공격어 차단</td> <td><input checked="" type="checkbox"/> WISE 요청 필터</td> <td><input checked="" type="checkbox"/> 인클루드인젝션차단</td> </tr> <tr> <td><input checked="" type="checkbox"/> 헬공격프로그램차단</td> <td><input checked="" type="checkbox"/> Slow Read 공격 차단</td> <td><input checked="" type="checkbox"/> HTTP POST 공격 차단</td> </tr> <tr> <td><input checked="" type="checkbox"/> 신용카드 정보 유출 차단</td> <td><input checked="" type="checkbox"/> 주민등록 정보 유출 차단</td> <td><input checked="" type="checkbox"/> Slowloris 공격 차단</td> </tr> <tr> <td><input checked="" type="checkbox"/> 화이트리스트</td> <td></td> <td></td> </tr> </table> <p><input checked="" type="checkbox"/> 콘텐츠 보호</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td><input checked="" type="checkbox"/> 신용카드 정보 유출 차단</td> <td><input checked="" type="checkbox"/> 주민등록 정보 유출 차단</td> <td><input checked="" type="checkbox"/> 계좌번호 정보 유출 차단</td> </tr> <tr> <td><input checked="" type="checkbox"/> 웹 변조 방지</td> <td><input checked="" type="checkbox"/> 응답 형식 검사</td> <td><input checked="" type="checkbox"/> 코드 노출 차단</td> </tr> <tr> <td><input checked="" type="checkbox"/> WISE 콘텐츠 필터</td> <td></td> <td></td> </tr> </table> <p><input checked="" type="checkbox"/> 위장</p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td><input checked="" type="checkbox"/> URL 정보 위장</td> <td><input checked="" type="checkbox"/> Server 정보 위장</td> </tr> </table> <p style="text-align: center;"> <input type="button" value="보기"/> <input type="button" value="리셋"/> <input type="button" value="다운로드"/> </p> </div> <ul style="list-style-type: none"> <li>• <b>설정 보기 형식</b> '설정 보기'를 선택합니다.</li> <li>• <b>대상 설정</b> 어떤 설정을 출력할 것인지를 선택합니다. SDRAM의 설정을 출력하려면 '현재 설정'을, SSD 메모리에 저장된 설정을 출력하려면 해당 저장 공간을 선택합니다.</li> <li>• <b>보기 옵션</b> 출력할 설정 항목을 선택합니다. '메뉴별 보기' 옵션을 선택하면 기능 별로 항목의 이름이 나타납니다. 이 중에서 설정을 출력하고자 하는 항목들을 클릭하여 체크합니다. 모든 항목을 출력하려면 메뉴별 보기 옵션을 선택하지 않거나 모든 항목들을 체크하면 됩니다. 기본적으로는 모든 항목이 출력되도록 설정되어 있습니다.</li> </ul>	<input checked="" type="checkbox"/> 일반 설정	<input checked="" type="checkbox"/> 응답 설정	<input checked="" type="checkbox"/> 기타설정	<input checked="" type="checkbox"/> 캐시설정	<input checked="" type="checkbox"/> ICAP설정	<input checked="" type="checkbox"/> GZIP설정	<input checked="" type="checkbox"/> 접근 제어	<input checked="" type="checkbox"/> 폼 필드 검사	<input checked="" type="checkbox"/> 과다 요청 제어	<input checked="" type="checkbox"/> 쿠키 보호	<input checked="" type="checkbox"/> 바피 오버플로우 차단	<input checked="" type="checkbox"/> SQL 삽입 차단	<input checked="" type="checkbox"/> 스크립트 삽입 차단	<input checked="" type="checkbox"/> 업로드검사	<input checked="" type="checkbox"/> 다운로드 검사	<input checked="" type="checkbox"/> 디렉토리 리스팅 차단	<input checked="" type="checkbox"/> 요청 형식 검사	<input checked="" type="checkbox"/> 검사 회피 차단	<input checked="" type="checkbox"/> 공격어 차단	<input checked="" type="checkbox"/> WISE 요청 필터	<input checked="" type="checkbox"/> 인클루드인젝션차단	<input checked="" type="checkbox"/> 헬공격프로그램차단	<input checked="" type="checkbox"/> Slow Read 공격 차단	<input checked="" type="checkbox"/> HTTP POST 공격 차단	<input checked="" type="checkbox"/> 신용카드 정보 유출 차단	<input checked="" type="checkbox"/> 주민등록 정보 유출 차단	<input checked="" type="checkbox"/> Slowloris 공격 차단	<input checked="" type="checkbox"/> 화이트리스트			<input checked="" type="checkbox"/> 신용카드 정보 유출 차단	<input checked="" type="checkbox"/> 주민등록 정보 유출 차단	<input checked="" type="checkbox"/> 계좌번호 정보 유출 차단	<input checked="" type="checkbox"/> 웹 변조 방지	<input checked="" type="checkbox"/> 응답 형식 검사	<input checked="" type="checkbox"/> 코드 노출 차단	<input checked="" type="checkbox"/> WISE 콘텐츠 필터			<input checked="" type="checkbox"/> URL 정보 위장	<input checked="" type="checkbox"/> Server 정보 위장
<input checked="" type="checkbox"/> 일반 설정	<input checked="" type="checkbox"/> 응답 설정	<input checked="" type="checkbox"/> 기타설정																																								
<input checked="" type="checkbox"/> 캐시설정	<input checked="" type="checkbox"/> ICAP설정	<input checked="" type="checkbox"/> GZIP설정																																								
<input checked="" type="checkbox"/> 접근 제어	<input checked="" type="checkbox"/> 폼 필드 검사	<input checked="" type="checkbox"/> 과다 요청 제어																																								
<input checked="" type="checkbox"/> 쿠키 보호	<input checked="" type="checkbox"/> 바피 오버플로우 차단	<input checked="" type="checkbox"/> SQL 삽입 차단																																								
<input checked="" type="checkbox"/> 스크립트 삽입 차단	<input checked="" type="checkbox"/> 업로드검사	<input checked="" type="checkbox"/> 다운로드 검사																																								
<input checked="" type="checkbox"/> 디렉토리 리스팅 차단	<input checked="" type="checkbox"/> 요청 형식 검사	<input checked="" type="checkbox"/> 검사 회피 차단																																								
<input checked="" type="checkbox"/> 공격어 차단	<input checked="" type="checkbox"/> WISE 요청 필터	<input checked="" type="checkbox"/> 인클루드인젝션차단																																								
<input checked="" type="checkbox"/> 헬공격프로그램차단	<input checked="" type="checkbox"/> Slow Read 공격 차단	<input checked="" type="checkbox"/> HTTP POST 공격 차단																																								
<input checked="" type="checkbox"/> 신용카드 정보 유출 차단	<input checked="" type="checkbox"/> 주민등록 정보 유출 차단	<input checked="" type="checkbox"/> Slowloris 공격 차단																																								
<input checked="" type="checkbox"/> 화이트리스트																																										
<input checked="" type="checkbox"/> 신용카드 정보 유출 차단	<input checked="" type="checkbox"/> 주민등록 정보 유출 차단	<input checked="" type="checkbox"/> 계좌번호 정보 유출 차단																																								
<input checked="" type="checkbox"/> 웹 변조 방지	<input checked="" type="checkbox"/> 응답 형식 검사	<input checked="" type="checkbox"/> 코드 노출 차단																																								
<input checked="" type="checkbox"/> WISE 콘텐츠 필터																																										
<input checked="" type="checkbox"/> URL 정보 위장	<input checked="" type="checkbox"/> Server 정보 위장																																									

## 설정 비교하기

현재 설정과 SSD의 특정 저장 공간에 저장된 설정 정보를 비교하여 출력하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 애플리케이션 설정 보기를 클릭합니다.
2	<p>&lt;설정 보기&gt; 화면에서 다음 설명을 참고하여 각 항목을 설정한 후 [보기] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>설정 보기 형식</b> : 현재 설정과 비교하기</li> <li>• <b>대상 설정</b> : 저장 공간 #1 설정</li> <li>• <b>보기 옵션</b> <ul style="list-style-type: none"> <li><input type="checkbox"/> 서로 다른 설정 내용만 보기</li> <li><input checked="" type="checkbox"/> 메뉴별 보기</li> <li><input checked="" type="checkbox"/> 애플리케이션                             <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 일반 설정</li> <li><input checked="" type="checkbox"/> 캐시설정</li> <li><input checked="" type="checkbox"/> 응답 설정</li> <li><input checked="" type="checkbox"/> ICAP설정</li> <li><input checked="" type="checkbox"/> 기타설정</li> <li><input checked="" type="checkbox"/> GZIP설정</li> </ul> </li> <li><input checked="" type="checkbox"/> 요청 검사                             <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 접근 제어</li> <li><input checked="" type="checkbox"/> 쿠키 보호</li> <li><input checked="" type="checkbox"/> 스크립트 삽입 차단</li> <li><input checked="" type="checkbox"/> 디렉토리 리스팅 차단</li> <li><input checked="" type="checkbox"/> 글꼴이 차단</li> <li><input checked="" type="checkbox"/> 웹공격프로그램차단</li> <li><input checked="" type="checkbox"/> 신용카드 정보 유출 차단</li> <li><input checked="" type="checkbox"/> 화이트리스트</li> <li><input checked="" type="checkbox"/> 톰 필드 검사</li> <li><input checked="" type="checkbox"/> 버퍼 오버플로우 차단</li> <li><input checked="" type="checkbox"/> 업로드검사</li> <li><input checked="" type="checkbox"/> 요청 형식 검사</li> <li><input checked="" type="checkbox"/> WISE 요청 필터</li> <li><input checked="" type="checkbox"/> Slow Read 공격 차단</li> <li><input checked="" type="checkbox"/> 주민등록 정보 유출 차단</li> <li><input checked="" type="checkbox"/> 과도 요청 제어</li> <li><input checked="" type="checkbox"/> SQL 삽입 차단</li> <li><input checked="" type="checkbox"/> 다운로드 검사</li> <li><input checked="" type="checkbox"/> 검사 회피 차단</li> <li><input checked="" type="checkbox"/> 인출루드인젝션차단</li> <li><input checked="" type="checkbox"/> HTTP POST 공격 차단</li> <li><input checked="" type="checkbox"/> Slowloris 공격 차단</li> </ul> </li> <li><input checked="" type="checkbox"/> 컨텐츠 보호                             <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 신용카드 정보 유출 차단</li> <li><input checked="" type="checkbox"/> 웹 변조 방지</li> <li><input checked="" type="checkbox"/> WISE 컨텐츠 필터</li> <li><input checked="" type="checkbox"/> 주민등록 정보 유출 차단</li> <li><input checked="" type="checkbox"/> 응답 형식 검사</li> <li><input checked="" type="checkbox"/> 계좌번호 정보 유출 차단</li> <li><input checked="" type="checkbox"/> 코드 노출 차단</li> </ul> </li> <li><input checked="" type="checkbox"/> 위장                             <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> URL 정보 위장</li> <li><input checked="" type="checkbox"/> Server 정보 위장</li> </ul> </li> </ul> </li> </ul> <p>• <b>설정 보기 형식</b> '현재 설정과 비교하기'를 선택합니다.</p> <p>• <b>대상 설정</b> 현재 설정과 비교할 SSD 메모리의 저장 공간을 선택합니다.</p> <p>• <b>보기 옵션</b></p> <ul style="list-style-type: none"> <li>- 서로 다른 설정 내용만 보기 - 두 설정에서 동일한 이름의 애플리케이션들 간에 설정 내용이 다른 부분만 출력하고자 할 때 이 옵션을 체크합니다. 이 옵션을 체크하지 않으면 전체 설정이 나란히 출력됩니다.</li> <li>- 메뉴별 보기 - 출력할 설정 항목을 선택합니다. '메뉴별 보기' 옵션을 선택하면 기능 별로 항목의 이름이 나타납니다. 이 중에서 설정을 출력하고자 하는 항목들을 클릭하여 체크합니다. 모든 항목을 출력하려면 메뉴별 보기 옵션을 선택하지 않거나 모든 항목들을 체크하면 됩니다. 기본적으로는 모든 항목이 출력되도록 설정되어 있습니다.</li> </ul>

## 설정 다운로드하기

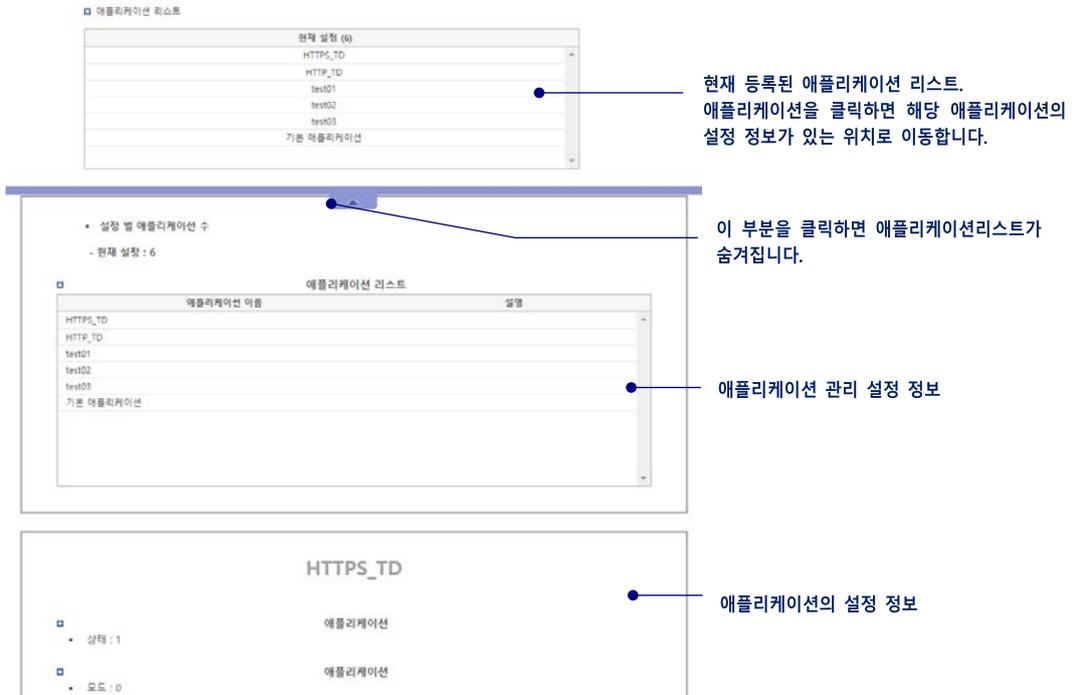
설정 출력이나 설정 비교를 통해 출력되는 설정 정보를 화면이 아닌 HTML 파일로 다운로드 하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 애플리케이션 설정 보기를 클릭합니다.
2	<설정 보기> 화면에서 설정 출력하기와 설정 비교하기 절의 내용을 참고하여 어떤 내용을 파일로 다운로드 할지를 설정한 후 [다운로드] 버튼을 클릭합니다.
3	<파일 다운로드> 팝업 창에서 [저장] 버튼을 클릭합니다.
4	<다른 이름으로 저장> 팝업 창에서 파일을 저장할 폴더의 위치와 파일의 이름을 지정한 후 [저장] 버튼을 클릭합니다. 파일 이름은 기본적으로 configuration.html이 사용됩니다.

# 설정 출력 화면

## 현재 설정 출력 화면

다음은 '설정 보기' 기능을 사용하여 현재 설정 전체를 출력했을 때 나타나는 화면입니다.



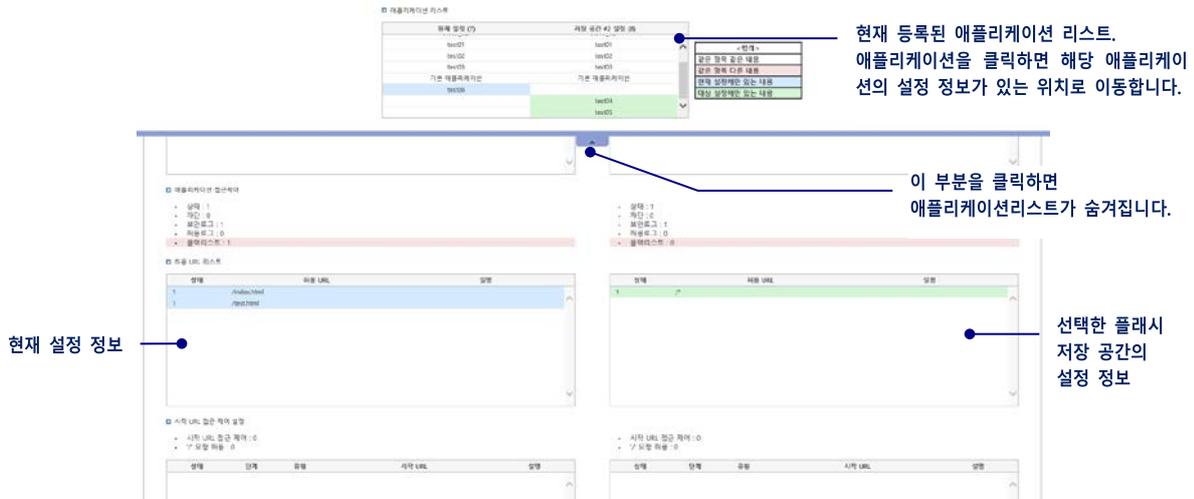
화면의 맨 위 부분에는 애플리케이션의 목록이, 아래 쪽에는 각 애플리케이션 설정이 출력됩니다. 애플리케이션의 설정은 리스트 상의 애플리케이션 순서대로 출력됩니다. 세로 스크롤 바를 움직여서 아래에 있는 설정 정보들을 볼 수 있습니다. 애플리케이션 리스트는 스크롤 바를 내려도 가려지지 않습니다. 애플리케이션 리스트를 숨기려면 중앙의  부분을 클릭합니다. 이 부분을 한번 더 클릭하면 다시 애플리케이션 리스트가 나타납니다.

애플리케이션 리스트에서 현재 설정 뒤의 ( )에 표시된 숫자는 현재 등록된 애플리케이션의 개수입니다. 리스트에서 애플리케이션의 이름을 클릭하면, 해당 애플리케이션의 설정 정보가 있는 위치로 이동합니다.

## 설정 비교 출력 화면

### 두 설정을 모두 출력한 경우

현재 설정과 사용자가 선택한 SSD 저장 공간의 설정을 모두 출력한 경우의 화면입니다.



사용자의 모니터 크기를 감안하여 처음에 나타나는 화면은 위 그림과 달리 하나의 설정 정보만 출력되는 크기입니다. 화면의 크기를 조정하여 두 설정이 모두 보이도록 하는 것이 편리합니다.

화면의 맨 위에는 두 설정의 애플리케이션 리스트가 출력됩니다. 이 리스트는 스크롤 바를 클릭해도 사라지지 않습니다. 리스트를 숨기려면 중앙의 ▲ 부분을 클릭합니다. 이 부분을 한번 더 클릭하면 다시 애플리케이션 리스트가 나타납니다. 리스트에 있는 애플리케이션의 이름을 클릭하면, 해당 애플리케이션의 설정 정보가 있는 위치로 이동합니다.

설정이 표시되는 부분에서 왼쪽 부분에 출력된 설정은 현재 설정이고, 오른쪽에 출력된 설정은 사용자가 지정한 SSD 저장 공간의 설정입니다. 앞서 설명한 대로, 하위 항목까지 설정이 같은 항목은 흰색, 서로 다른 경우에는 분홍색, 하늘색, 연두색 등으로 표시됩니다.

### 설정이 서로 다른 부분만 출력한 경우

설정이 서로 다른 부분만 출력하도록 하는 경우의 출력 화면도 앞의 화면과 화면 구성이 동일합니다. 하지만, 설정이 완전히 같거나 애플리케이션이 모두 다른 경우(같은 이름의 애플리케이션이 없는 경우)에는 '서로 다른 설정 내용이 없습니다'라는 메시지가 표시됩니다.



# 애플리케이션 설정 간편화

애플리케이션 설정 간편화는 등록된 애플리케이션의 상태와 각 애플리케이션의 요청 검사, 콘텐츠 보호 기능에 대한 상태를 간편하게 설정할 수 있는 기능입니다. 이 절에서는 애플리케이션 별, 기능 별로 설정 간편화 기능을 설정하는 방법을 살펴봅니다.

## 개요

여러 애플리케이션 및 웹 보안 기능의 상태를 설정하려면 애플리케이션을 선택하고 각 보안 기능메뉴로 이동해야하는 불편함이 있습니다. 이러한 불편함을 줄이기 위해 WEBFRONT-K는 한 화면에서 애플리케이션과 웹 보안 기능의 상태를 설정할 수 있는 애플리케이션 설정 간편화 기능을 제공합니다. 이 절은 다음과 같은 내용으로 구성됩니다.

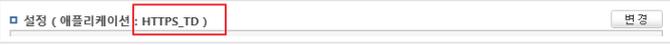
- 애플리케이션 별 보기
- 기능 별 보기

## 애플리케이션 별 보기

애플리케이션 설정 간편화 기능은 애플리케이션 별 보기, 기능 별 보기의 두가지 보기 형식을 지원합니다. 애플리케이션 별 보기를 선택한 경우, <애플리케이션 리스트>에서 선택한 애플리케이션 별 각 보안 기능의 상태, 차단, 보안로그, 통계, 증거 설정을 한 화면에서 할 수 있습니다. 또한 동시에 여러 애플리케이션의 상태 설정을 하거나 선택한 애플리케이션의 설정을 다른 애플리케이션에 적용할 수 있습니다. 이 절에서는 애플리케이션 별 보안 기능의 상태 설정, 애플리케이션의 상태 설정, 같은 설정을 다른 애플리케이션에 적용하는 방법에 대해 알아보도록 합니다.

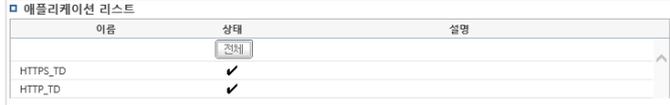
### 애플리케이션의 보안 기능 상태 설정하기

애플리케이션의 각 보안 기능 상태를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 애플리케이션 설정 간편화 메뉴를 클릭합니다.
2	<보기 형식>에서 [애플리케이션 별 보기]를 선택합니다. 기본적으로 선택되어있습니다.
3	<애플리케이션 리스트>에서 애플리케이션을 선택합니다. 선택한 애플리케이션 이름이 <설정>에 나타납니다. 
4	<설정>의 [변경] 버튼을 클릭합니다.
5	상태를 변경할 기능의 [상태], [차단], [보안로그], [증거], [학습], [블랙리스트] 항목을 클릭합니다. ✓ 표시는 활성화 상태를, N/A는 해당 항목이 존재하지 않음을 의미합니다. [전체] 버튼을 사용하면 모든 기능의 상태를 한번에 변경할 수 있습니다. 
6	설정이 완료되면 [적용] 버튼을 클릭합니다.

## 애플리케이션 상태 설정하기

애플리케이션 상태를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 애플리케이션 설정 간편화</b> 메뉴를 클릭합니다.
2	<보기 형식>에서 [ <b>애플리케이션 별 보기</b> ]를 선택합니다. 기본적으로 선택되어있습니다.
3	< <b>애플리케이션 리스트</b> >의 [ <b>변경</b> ] 버튼을 클릭합니다.
4	상태를 변경할 애플리케이션의 [ <b>상태</b> ] 항목을 클릭합니다. <input checked="" type="checkbox"/> 표시는 활성화 상태를 의미합니다. <b>[전체]</b> 버튼을 사용하면 < <b>애플리케이션 리스트</b> >에 있는 모든 애플리케이션의 상태를 한번에 변경할 수 있습니다. 
5	설정이 완료되면 [ <b>적용</b> ] 버튼을 클릭합니다.

## 같은 설정을 다른 애플리케이션에 적용하기

애플리케이션의 각 기능 상태 설정을 다른 애플리케이션에 적용하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 애플리케이션 설정 간편화</b> 메뉴를 클릭합니다.
2	<보기 형식>에서 [ <b>애플리케이션 별 보기</b> ]를 선택합니다. 기본적으로 선택되어있습니다.
3	< <b>애플리케이션 리스트</b> >에서 원본 애플리케이션을 선택하고 화면 아래의 < <b>같은 설정 다른 애플리케이션에 적용</b> > 버튼을 클릭합니다.
4	< <b>설정 복사</b> > 팝업 창에서 대상 애플리케이션을 선택하고 [ <b>적용</b> ] 버튼을 클릭합니다.

## 기능 별 보기

애플리케이션 설정 간편화의 보기 형식을 기능 별 보기로 선택한 경우, <기능 리스트>에서 항목을 선택한 후 여러 애플리케이션의 해당 기능에 대한 상태, 차단, 보안로그, 통계, 증거 설정을 동시에 할 수 있습니다. 이 절에서는 보안 기능 별로 상태를 설정하는 방법에 대해 알아보도록 합니다.

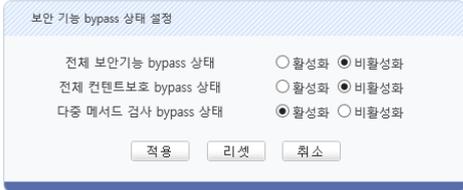
## 보안 기능 별 상태 설정하기

각 보안 기능 상태를 애플리케이션에 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 애플리케이션 설정 간편화</b> 메뉴를 클릭합니다.
2	<보기 형식>에서 [ <b>기능 별 보기</b> ]를 선택합니다.
3	< <b>기능 리스트</b> >에서 상태를 변경할 보안 기능을 선택합니다. 선택한 보안 기능 이름이 <설정>에 나타납니다.
4	<설정>의 [ <b>변경</b> ] 버튼을 클릭합니다.
5	상태를 변경할 기능의 [ <b>상태</b> ], [ <b>차단</b> ], [ <b>보안로그</b> ], [ <b>증거</b> ], [ <b>학습</b> ], [ <b>블랙리스트</b> ] 항목을 클릭합니다. <input checked="" type="checkbox"/> 표시는 활성화 상태를, N/A는 해당 항목이 존재하지 않음을 의미합니다. <b>[전체]</b> 버튼을 사용하면 모든 애플리케이션의 기능 상태를 한번에 변경할 수 있습니다. 
6	설정이 완료되면 [ <b>적용</b> ] 버튼을 클릭합니다.

# 보안 기능 bypass 상태 설정하기

보안 기능의 bypass 상태를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 애플리케이션 설정 간편화 메뉴를 클릭합니다.
2	<보안 기능 bypass 상태>에서 [변경] 버튼을 클릭합니다.
3	<p>&lt;보안 기능 bypass 상태 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 지정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li> <b>전체 보안기능 bypass 상태</b>                      전체 애플리케이션에 대한 보안 기능 사용 여부를 지정합니다. 기능을 활성화하면 각 애플리케이션에 설정된 보안 기능의 활성화 여부와 관계없이 모든 보안 기능이 동작하지 않습니다. WEBFRONT-K에 장애가 발생하였거나 모든 애플리케이션의 보안 기능을 비활성화해야 하는 등의 특수한 경우가 아닐 경우에는 이 기능을 활성화하지 않도록 합니다. (기본값: 비활성화)                 </li> <li> <b>전체 콘텐츠보호 bypass 상태</b>                      전체 애플리케이션에 대한 콘텐츠 보호 사용 여부를 지정합니다. 기능을 활성화하면 각 애플리케이션에 설정된 콘텐츠보호의 활성화 여부와 관계없이 콘텐츠 보호 기능이 동작하지 않습니다. 기능을 비활성화하면 애플리케이션에 콘텐츠 보호 기능이 활성화된 경우에만 동작합니다. (기본값: 비활성화)                 </li> <li> <b>다중 메서드 검사 bypass 상태</b>                      전체 애플리케이션에 대한 다중 메서드 검사 여부를 지정합니다. 기능을 활성화하면 각 애플리케이션에 설정된 다중 메서드 검사의 활성화 여부와 관계없이 다중 메서드 검사가 진행되지 않습니다. 기능을 비활성화하면 애플리케이션에 다중메서드 검사가 활성화된 경우에만 검사를 수행합니다. (기본값: 활성화)                 </li> </ul>

## 고급 첨부파일 검사 설정

WEBFRONT-K는 웹 서버에서 클라이언트로 전송되는 파일을 검사하여 고객정보가 유출되는 것을 방지하는 고급 첨부 파일 검사 기능을 지원합니다. 고급 첨부 파일 검사 기능을 사용하기 위해서는 가상 IP 주소를 설정하고 상태를 활성화해야 합니다.

이 절에서는 고급 첨부 파일 검사 기능의 상태와 가상 IP 주소를 설정하는 방법에 대해 살펴봅니다.

### 고급 첨부 파일 검사 설정 정보 변경하기

다음은 고급 첨부 파일 검사 설정 정보를 변경하는 방법입니다.

순서	설정 과정
1	System - 애플리케이션 - 고급첨부파일검사 설정 메뉴를 클릭합니다.
2	<고급첨부파일검사 설정 정보>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;고급첨부파일검사 설정 정보 변경&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div data-bbox="587 795 1109 1003" data-label="Image"> </div> <p>• <b>검사 파일 크기 제한</b> 검사할 파일의 크기를 지정합니다. (설정 범위: 1KB ~ 10MB, 기본값: 100KB)</p>

### 고급 첨부 파일 검사 상태 설정하기

다음은 고급 첨부 파일 검사 상태를 설정하는 방법입니다.

순서	설정 과정
1	System - 애플리케이션 - 고급첨부파일검사 설정 메뉴를 클릭합니다.
2	<고급첨부파일검사 설정 상태>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;고급첨부파일검사 설정 변경&gt; 팝업 창에서 상태를 설정한 후 [적용] 버튼을 클릭합니다.</p> <div data-bbox="587 1467 1109 1646" data-label="Image"> </div>



**참고:** 고급 첨부 파일 검사 기능을 사용하기 위해서는 신용카드 정보 유출 차단, 주민등록 정보 유출 차단, 계좌번호 유출 차단 상태와 파일 차단 상태가 활성화되어 있어야 합니다. 또한, 각 정보 유출 차단 기능의 정보 보호 방법을 탐지로 설정한 경우에는 고급 첨부 파일 검사 기능이 탐지 모드로 동작하게 되어 응답 패킷은 차단되지 않고, 보안 로그만 기록됩니다.



**참고:** 개인 정보 보호 기능을 사용하려면 고급 첨부 파일 검사 상태가 활성화되어 있어야 합니다.



**참고:** 고급 첨부 파일 검사 기능을 활성화하면 첨부 파일의 수와 용량에 따라 검사에 소요되는 시간이 길어져 클라이언트로의 응답이 늦어질 수 있습니다.

# 시그니처 관리

이 절에서는 시그니처 관리에서 제공하는 기능에 대해 살펴봅니다.

## 개요

시그니처는 웹 공격에 사용되는 패턴을 정의한 것으로 WEBFRONT-K의 웹 보안 기능 중에는 접근 제어나 SQL 삽입 차단 기능과 같이 시그니처를 사용하여 웹 공격을 차단하는 기능이 많습니다. 보안 시그니처 관리 기능은 웹 보안 기능에 사용되는 시그니처의 버전을 관리하고 보안 정책에 반영하도록 설정하는 기능입니다. 이 시그니처 관리 기능은 다음과 같은 세부 기능들로 구성되어 있습니다.

- 시그니처 버전 관리
- 시그니처 리스트 관리
- 시그니처 에이징

각 기능에 대해 알아봅니다.

### 시그니처 버전 관리

WEBFRONT-K의 웹 보안 기능에 사용되는 시그니처의 버전을 관리하기 위한 다음과 같은 기능을 제공합니다.

- 시그니처 버전을 공장 초기 출하 버전으로 초기화하는 기능
- 파이오링크에서 제공하는 시그니처 업데이트 서버로부터 최신 버전의 시그니처로 업데이트하는 기능
- 시그니처 파일을 관리자가 직접 업로드하여 업데이트하는 기능
- 현재 설치된 버전과 최신 시그니처 버전을 조회하는 기능
- 시그니처 릴리즈 노트를 다운로드하는 기능

### 시그니처 리스트 관리

WEBFRONT-K의 웹 보안 기능 중 접근 제어, 버퍼오버플로우 차단, SQL 삽입 차단, 스크립트 삽입차단, 업로드 검사, 다운로드 검사, 인클루드 인젝션, 웹 공격 프로그램 차단 기능을 수행할 때 이 리스트에 포함된 시그니처를 사용합니다. 시그니처 리스트는 사용자가 설정한 보안 레벨에 따라 변경됩니다. 보안 레벨은 높음, 보통, 낮음 세 단계로 구분됩니다. 각각의 시그니처는 차단, 탐지, 예외 세가지 상태를 가지며 사용자는 시그니처 리스트에서 시그니처의 액션을 변경하여 사용 여부를 설정할 수 있습니다. 시그니처 리스트에 필요한 시그니처가 없는 경우 사용자가 직접 시그니처를 작성하여 리스트에 추가할 수 있습니다.

다음은 요청 검사 기능 중 접근 제어 - 차단 URL 기능의 시그니처 리스트를 보여주는 화면입니다. 보안 레벨 설정에 따라 보안 기능에 설정되는 시그니처가 달라지며 드롭다운 목록에서 보안기능을 선택하면 해당 기능에 사용되는 시그니처 리스트를 볼 수 있습니다.

□ 시그니처 리스트 변경

• 보안레벨: 높음 [사용자]  
(의심가는 접근 전체를 차단하지만 일부 정상접근도 차단 될 수 있습니다.)

접근제어 - 차단URL

시그니처 ID	시그니처 정보	위험도	차단	탐지	예외
ACC-00001	설명 : .htaccess 액세스 공격	하		●	
ACC-00002	설명 : /architext_query.pl	하		●	
ACC-00003	설명 : /blabla.ida	상		●	
ACC-00004	설명 : /cgi-bin/global.cgi 취약점	하		●	
ACC-00005	설명 : /etc/rhosts 시스템 파일 접근공격	상		●	
ACC-00006	설명 : /etc/hosts 시스템 파일 접근공격	상		●	
ACC-00007	설명 : /etc/passwd시스템 파일 접근공격	상		●	
ACC-00008	설명 : /sam 샘플일 추출 공격1	하		●	
ACC-00009	설명 : /sam 샘플일 추출 공격2	하		●	
ACC-00010	설명 : /sam 샘플일 추출 공격3	하		●	
ACC-00011	설명 : /test/jsp/declaration/IntegerOverfio접근공격	하		●	
ACC-00012	설명 : /test/jsp/pagelsErrorPage.* 접근공격	하		●	
ACC-00013	설명 : /test/jsp/pagelsThreadSafe.* 접근공격	하		●	
ACC-00014	설명 : /test/jsp/pageSession.* 접근공격	하		●	
ACC-00015	설명 : /././././wint/win.ini 접근 취약점	하		●	
ACC-00016	설명 : 검색 robots 접근 공격	중		●	

## 시그니처 에이징

시그니처 에이징은 시그니처의 유용성 분석 후 시그니처의 액션을 일일이 변경해야 하는 번거로움을 줄여주는 기능입니다. 시그니처 에이징 리스트에 설정된 시그니처는 설정된 에이징 기간 동안 탐지 상태로 동작 하다가 이후 자동으로 차단 상태로 변경됩니다.

다음은 시그니처 에이징 리스트에 시그니처가 등록된 화면 입니다.

□ 시그니처 에이징 리스트 변경

접근제어 - 차단URL

시그니처 ID	시그니처 정보	위험도	에이징기간
ACC-00001	설명 : .htaccess 액세스 공격	하	7일
ACC-00002	설명 : /architext_query.pl	하	7일
ACC-00005	설명 : /etc/rhosts 시스템 파일 접근공격	상	7일
ACC-00006	설명 : /etc/hosts 시스템 파일 접근공격	상	7일

# 시그니처 관리 화면

System 메뉴에서 애플리케이션 - 시그니처관리 메뉴를 클릭하면 다음과 같은 <시그니처관리> 화면이 나타납니다.



화면의 각 부분에서 보여주는 정보와 수행할 수 있는 작업은 다음과 같습니다.

- 시그니처 버전** WEBFRONT-K에 저장된 시그니처의 버전을 보여줍니다. 시그니처 초기화, 네트워크 업데이트, 파일 업데이트 기능, 최신 시그니처 버전 조회, 시그니처 릴리스 노트 다운로드를 수행할 수 있습니다.
- 시그니처 리스트** 보안레벨과 각 보안 기능에 설정된 시그니처의 액션을 보여줍니다. 시그니처 리스트의 보안레벨 설정과 시그니처 액션 설정, 사용자 정의 시그니처 추가를 할 수 있습니다.
- 시그니처 에이징** 시그니처 에이징 기능의 상태와 각 보안기능 별 시그니처 에이징 리스트를 설정할 수 있습니다. 시그니처 에이징 리스트에 등록된 시그니처는 기본 에이징 기간 동안 탐지로 동작하고 이후 차단으로 동작하게 됩니다.

시그니처 리스트의 각 항목에서 보여주는 정보는 다음과 같습니다.

- 시그니처 ID** 시그니처를 구분하는 ID입니다. 기본으로 제공되는 시그니처의 ID는 [보안기능:영문자 3자리]-[숫자 5자리]로 구성되고 사용자 정의 시그니처 ID는 [USER]- [보안기능:영문자 3자리]-[숫자 5자리]로 구성되어 있습니다. 예) ACC-00001, USER-ACC-00001
- 시그니처 정보** 시그니처에 대한 설명입니다. 사용자 정의 시그니처의 경우 시그니처와 설명이 표시됩니다.
- 위험도** 공격이 성공한 경우 시스템에 미치는 위험도입니다. 상/중/하 세가지로 구분됩니다.
- 차단** 해당 시그니처가 요청 패킷에 포함된 경우 요청을 차단합니다.
- 탐지** 해당 시그니처가 요청 패킷에 포함된 경우 요청을 통과시키고 보안로그를 생성합니다.
- 예외** 보안기능에서 해당 시그니처를 검사하지 않습니다.

## 시그니처 버전 조회

WEBFRONT-K는 시그니처 현재 설치 버전과 최신 버전, 최신 릴리스 노트를 제공합니다. 관리자는 제공된 정보를 통해 업데이트가 필요한지 확인할 수 있습니다.

시그니처 버전을 조회하고 릴리스 노트를 다운로드하는 방법을 설명합니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 시그니처관리</b> 메뉴를 클릭합니다.
2	<p>&lt;시그니처 버전&gt;에서 버전을 확인합니다.</p> <div data-bbox="582 517 1107 629" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>□ 시그니처 버전</p> <ul style="list-style-type: none"> <li>• 현재 시그니처 버전: 4.35</li> <li>• <b>최신 시그니처 버전: v4.35</b></li> <li>• 시그니처 릴리스노트: <a href="#">다운로드</a></li> </ul> </div> <ul style="list-style-type: none"> <li>• <b>현재 시그니처 버전</b> WEBFRONT-K에 설치되어 있는 시그니처 버전정보가 표시됩니다.</li> <li>• <b>최신 시그니처 버전</b> 파이오링크 시그니처 업데이트 서버에 게시된 최신 시그니처 버전 정보가 표시됩니다.</li> </ul>
3	시그니처 릴리스 노트를 다운로드 하려면 <b>시그니처 릴리스노트</b> 에서 <b>[다운로드]</b> 버튼을 클릭합니다.
4	시그니처 릴리스 노트 문서가 다운로드됩니다.

## 시그니처 업데이트

파이오링크는 신규 보안 취약점을 분석하여 새로운 시그니처를 개발하고 이를 파이오링크 시그니처 업데이트 서버에 게시합니다. 최신의 시그니처를 업데이트 하려면, 업데이트 서버에 네트워크를 통해 연결하거나 관리자 PC에서 직접 업로드할 수 있습니다.

### 네트워크를 이용한 업데이트하기

다음은 업데이트 서버에서 새로운 시그니처를 다운로드하여 WEBFRONT-K의 시그니처를 업데이트하는 방법입니다.

순서	설정 과정						
1	System - 애플리케이션 - 시그니처관리 메뉴를 클릭합니다.						
2	<시그니처 버전>의 [변경] 버튼을 클릭합니다.						
3	<시그니처 네트워크 업데이트>의 [업데이트] 버튼을 클릭합니다.						
4	<p>&lt;시그니처 버전&gt;의 현재 시그니처 버전 항목에 업데이트된 시그니처의 버전이 표시되고 화면 아래 부분에는 시그니처 버전, 시그니처 업데이트 시간, 시그니처 업데이트 유형이 표시됩니다.</p>  <table border="1" data-bbox="496 1043 1198 1261"> <thead> <tr> <th>시그니처 버전</th> <th>시그니처 업데이트 시간</th> <th>시그니처 업데이트 유형</th> </tr> </thead> <tbody> <tr> <td>4.35</td> <td>2019/06/18 10:54:17</td> <td>시그니처 네트워크 업데이트</td> </tr> </tbody> </table>	시그니처 버전	시그니처 업데이트 시간	시그니처 업데이트 유형	4.35	2019/06/18 10:54:17	시그니처 네트워크 업데이트
시그니처 버전	시그니처 업데이트 시간	시그니처 업데이트 유형					
4.35	2019/06/18 10:54:17	시그니처 네트워크 업데이트					

### 파일 업로드를 이용한 업데이트하기

다음은 새로운 시그니처 파일을 업로드하여 WEBFRONT-K의 시그니처를 업데이트하는 방법입니다.

순서	설정 과정
1	System - 애플리케이션 - 시그니처관리 메뉴를 클릭합니다.
2	<시그니처 버전>의 [변경] 버튼을 클릭합니다.
3	<시그니처 파일 업데이트>의 [파일 선택] 버튼을 클릭합니다.
4	파일 선택 팝업 창에서 업데이트할 시그니처 파일이 저장되어 있는 폴더와 파일을 선택하고 [열기] 버튼을 클릭합니다.
5	<시그니처 파일 업데이트>에 선택한 파일의 경로가 표시되면 [파일업로드] 버튼을 클릭합니다.
6	<시그니처 버전>의 현재 시그니처 버전 항목에 업데이트된 시그니처의 버전이 표시되고 화면 아래 부분에는 시그니처 버전, 시그니처 업데이트 시간, 시그니처 업데이트 유형이 표시됩니다.

### 시그니처 초기화하기

기본적으로 WEBFRONT-K의 PLOS에는 시그니처가 포함되어 있습니다. 시그니처 초기화란 WEBFRONT-K의 시그니처를 PLOS에 포함된 시그니처로 복구시키는 것을 의미 합니다. 시그니처를 초기화하면 앞서 살펴본 시그니처 관리 기능을 통

해 업데이트된 시그니처는 모두 삭제됩니다.

다음은 WEBFRONT-K의 시그니처를 초기화하는 방법입니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 시그니처관리</b> 메뉴를 클릭합니다.
2	<시그니처 버전>의 [변경] 버튼을 클릭합니다.
3	<시그니처 버전>에 있는 [초기화] 버튼을 클릭합니다.
4	시그니처 초기화를 확인하는 팝업 창이 나타납니다. [확인]을 클릭합니다.
5	<p>시그니처를 초기화하는 과정이 잠시 동안 진행됩니다. 초기화가 끝나면 &lt;시그니처 버전&gt;의 현재 시그니처 버전 항목에는 PLOS에 포함되었던 시그니처의 버전이 표시됩니다.</p> 



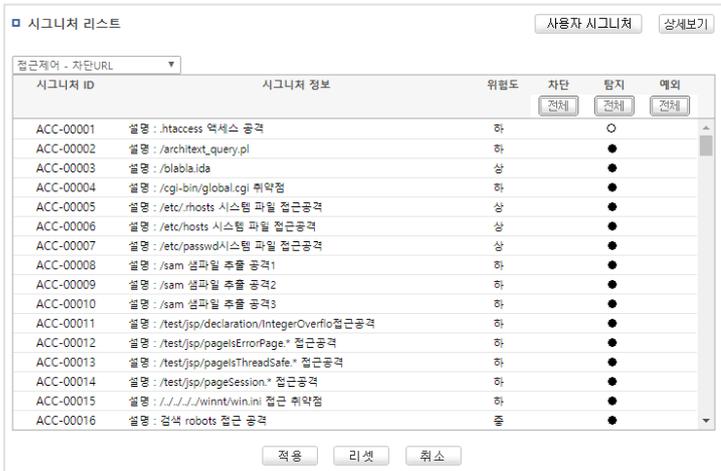
**참고:** PLOS를 업데이트하는 경우 업데이트할 PLOS에 포함된 시그니처가 현재 WEBFRONT-K에 설치된 시그니처보다 더 최신 버전이면 시그니처도 함께 업데이트됩니다. 하지만, 현재 WEBFRONT-K의 시그니처가 업데이트하려는 PLOS에 포함된 시그니처보다 최신인 경우에는 PLOS를 업데이트해도 시그니처는 그대로 유지됩니다.

# 시그니처 액션 설정

시그니처 액션 설정 방법은 '기본 액션 설정', '상세 액션 설정'의 두 가지 방법이 있습니다.

## 기본 액션 설정하기

새로 추가되는 애플리케이션은 기본 액션으로 시그니처 액션이 설정되며, 기본 액션 설정으로 시그니처의 액션을 변경하는 경우 기본 액션과 같은 설정을 가진 모든 애플리케이션의 시그니처에 적용됩니다. 시그니처 액션은 차단, 탐지, 예외 세가지로 구분되며 각각의 시그니처는 서로 다르게 액션을 설정할 수도 있습니다. 다음은 시그니처 리스트에서 시그니처의 기본 액션을 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 시그니처관리</b> 메뉴를 클릭합니다.
2	<시그니처 리스트>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<시그니처 리스트>의 드롭다운 목록에서 설정하고자 하는 보안기능을 선택합니다.
4	<p>액션을 변경할 시그니처의 <b>[차단]</b>, <b>[탐지]</b>, <b>[예외]</b> 항목 중에서 1개를 선택합니다. ● 표시는 모든 애플리케이션의 액션이 기본 액션임을 의미하고, ○ 표시는 시그니처의 기본 액션을 표시 하지만 애플리케이션 마다 서로 다른 액션 설정이 되어있음을 의미합니다. <b>[전체]</b> 버튼을 사용하면 모든 시그니처의 액션을 차단, 탐지 또는 예외로 변경합니다.</p> 
5	시그니처 액션 설정이 완료되면 <b>[적용]</b> 버튼을 클릭합니다.



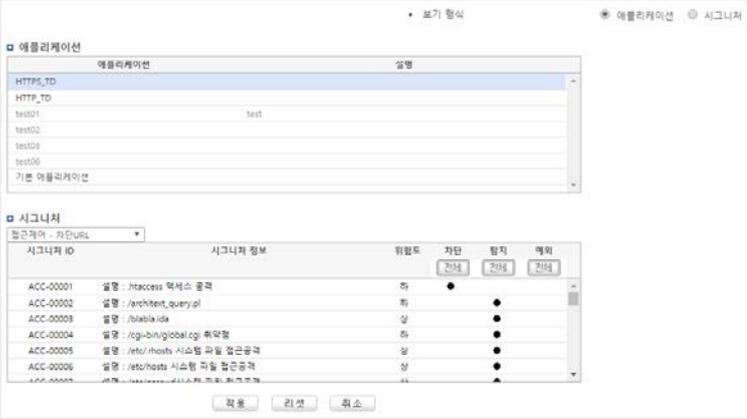
**참고:** ○ 표시된 시그니처의 기본 액션을 변경하면, 동일하게 설정되어 있는 애플리케이션의 시그니처 액션도 같이 변경됩니다.

## 상세 액션 설정

상세 액션 설정은 애플리케이션, 시그니처의 두가지 보기 형식을 지원합니다. 애플리케이션 보기 형식을 선택한 경우에는 애플리케이션을 기준으로 하여 각각의 시그니처 액션을 설정하고 시그니처 보기 형식을 선택한 경우에는 시그니처를 기준으로 각각의 애플리케이션에 해당 시그니처의 액션을 설정하는 방법입니다.

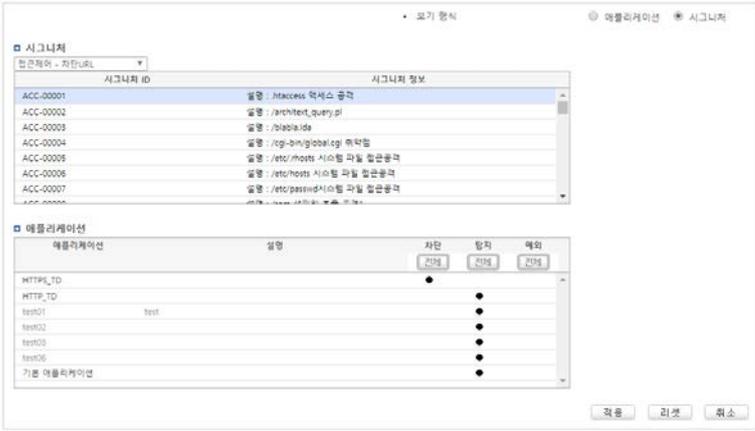
### 애플리케이션 별 액션 설정하기

다음은 애플리케이션 별 시그니처의 액션을 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 시그니처관리</b> 메뉴를 클릭합니다.
2	<시그니처 리스트>의 [변경] 버튼을 클릭합니다.
3	<시그니처 리스트>의 [상세보기] 버튼을 클릭합니다.
4	보기 형식에서 <b>애플리케이션</b> 을 선택합니다.
5	<애플리케이션>에서 시그니처의 액션을 변경할 애플리케이션을 선택합니다.
6	<p>&lt;시그니처&gt;의 드롭다운 목록에서 설정하고자 하는 보안 기능을 선택하고 액션을 변경할 시그니처의 [차단], [탐지], [예외] 항목을 클릭합니다. <b>전체</b> 버튼을 사용하면 모든 시그니처의 액션을 동일하게 설정할 수 있습니다.</p> 
7	설정이 완료되면 [적용] 버튼을 클릭합니다.

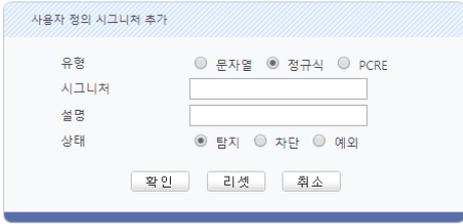
## 시그니처 별 액션 설정하기

다음은 시그니처 별 시그니처의 액션을 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 시그니처관리</b> 메뉴를 클릭합니다.
2	<시그니처 리스트>의 [변경] 버튼을 클릭합니다.
3	<시그니처 리스트>의 [상세보기] 버튼을 클릭합니다.
4	보기 형식에서 <b>시그니처</b> 를 선택합니다.
5	<시그니처>의 드롭다운 목록에서 설정하고자 하는 보안기능을 선택하고 액션을 변경할 시그니처를 선택합니다.
6	<p>&lt;애플리케이션&gt;에서 시그니처의 액션을 변경할 애플리케이션의 [차단], [탐지], [예외] 항목을 클릭합니다. [전체] 버튼을 사용하면 모든 애플리케이션에 동일한 액션 설정을 할 수 있습니다.</p> 
7	설정이 완료되면 [적용] 버튼을 클릭합니다.

## 사용자 정의 시그니처 설정하기

기본으로 제공되는 시그니처 이외의 시그니처가 필요한 경우 사용자가 직접 시그니처를 추가하여 보안기능에 설정할 수 있습니다. 다음은 사용자 정의 시그니처를 설정하는 방법입니다. 시그니처를 더 추가하려면 4 ~ 5번 과정을 반복하면 됩니다. 사용자 정의 시그니처는 256개까지 추가할 수 있습니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 시그니처관리</b> 메뉴를 클릭합니다.
2	<시그니처 리스트>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<시그니처 리스트>의 드롭다운 목록에서 설정하고자 하는 보안기능을 선택합니다.  <b>참고:</b> '업로드 검사 - 파일 내용' 시그니처는 사용자 정의 시그니처를 설정할 수 없습니다.
4	<시그니처 리스트>의 <b>[사용자 시그니처] - [추가]</b> 버튼을 클릭합니다. <사용자 정의 시그니처 추가> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 <b>[확인]</b> 을 클릭합니다.
5	<div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>유형</b>      입력할 시그니처의 유형을 지정합니다. (기본값: 정규식)</li> <li>• <b>시그니처</b>      시그니처를 입력합니다. 최대 256 글자의 문자열을 입력할 수 있습니다. 정규식을 입력할 경우 다음 절인 <b>[정규식 설정]</b> 부분을 참고합니다.</li> <li>• <b>설명</b>      시그니처에 대한 설명을 입력합니다. 최대 128 글자의 문자열을 입력할 수 있습니다. 한글 입력도 가능합니다.</li> <li>• <b>상태</b>      시그니처에 적용할 액션을 선택합니다. (기본값: 탐지)</li> </ul> <p> <b>참고:</b> 접근제어 - 차단 URL, 인클루드 인젝션 차단 기능의 사용자 정의 시그니처는 URL 형식의 시그니처만 입력할 수 있으며, 첫글자는 반드시 '/'를 입력해야 합니다. 두 보안 기능의 사용자 정의 시그니처 설정시 위 그림에서의 유형 항목은 나타나지 않습니다.</p>
6	사용자 정의 시그니처 설정이 완료되면 화면 아래의 <b>[적용]</b> 버튼을 클릭합니다.



### 참고: [사용자 정의 시그니처 수정/삭제하기]

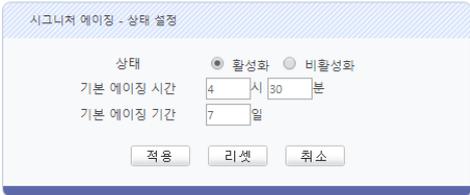
- 사용자 정의 시그니처 리스트에 추가한 시그니처의 내용을 변경하려면 시그니처를 선택하고 **[수정]** 버튼을 클릭합니다.  
<사용자 정의 시그니처 수정> 팝업 창이 나타나면 원하는 항목을 변경한 후 **[확인]**을 클릭합니다.
- 사용자 정의 시그니처 리스트에 추가한 시그니처의 내용을 삭제하려면 시그니처를 선택하고 **[삭제]** 버튼을 클릭합니다.

# 시그니처 에이징 설정하기

다음은 시그니처 에이징 상태 설정과 시그니처 에이징을 설정하는 방법에 대해 살펴봅니다.

## 시그니처 에이징 상태 설정하기

다음은 시그니처 에이징 기능의 상태를 설정하는 방법입니다.

순서	설정 과정
1	System - 애플리케이션 - 시그니처관리 메뉴를 클릭합니다.
2	화면 아래에 있는 <시그니처 에이징>의 [변경] 버튼을 클릭합니다.
3	화면 위에 있는 <시그니처 에이징>의 [변경] 버튼을 클릭합니다.
4	<p>&lt;시그니처 에이징 - 상태 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• 상태: 시그니처 에이징 기능의 사용 여부를 지정합니다. 사용하려는 경우에는 '활성화'를 선택하고, 사용하지 않으려는 경우에는 '비활성화'를 선택합니다. (기본값: 활성화)</li> <li>• 기본 에이징 시간: 에이징 기간을 계산할 시간을 입력합니다. 매일 기본 에이징 시간마다 기본 에이징 기간을 계산하여 하루씩 줄어듭니다. (기본값: 4시 30분)</li> <li>• 기본 에이징 기간: &lt;시그니처 에이징 리스트&gt;에서 시그니처 에이징 설정시 기본으로 설정되는 에이징 기간을 입력합니다. (설정 범위: 1 ~ 30, 기본값: 7일)</li> </ul>

## 시그니처 에이징 설정하기

다음은 시그니처 에이징을 설정하는 방법입니다.

순서	설정 과정
1	System - 애플리케이션 - 시그니처관리 메뉴를 클릭합니다.
2	<시그니처 에이징>의 [변경] 버튼을 클릭합니다.
3	<시그니처 에이징 리스트>의 [변경] 버튼을 클릭합니다.
4	<시그니처 리스트>의 드롭다운 목록에서 설정하고자 하는 보안기능을 선택합니다.
5	에이징 설정을 할 시그니처를 선택하고 [추가]버튼을 클릭합니다.
6	설정이 완료되면 [적용]버튼을 클릭합니다.



<시그니처 에이징 리스트>에서 추가한 시그니처는 시그니처 에이징 상태 설정에서 지정한 기본 에이징 기간으로 설정됩니다. 에이징 기간을 변경하고자 할 경우에는 시그니처를 더블 클릭하여 에이징 상태와 기간을 설정합니다.



시그니처의 에이징 설정을 취소하려면 <시그니처 에이징 리스트>에서 시그니처를 선택하고 [삭제] 버튼을 클릭하거나 시그니처를 더블 클릭한 후 에이징 상태를 비활성화로 변경합니다. 에이징 설정을 취소한 시그니처는 액션이 차단으로 변경됩니다.



<시그니처의 에이징 리스트>의 시그니처 추가/삭제 시 [Ctrl] 또는 [Shift] 키를 사용하여 최대 20개의 시그니처를 한번에 추가/삭제할 수 있습니다.

# 시그니처 내보내기

현재 WEBFRONT-K에 적용된 시그니처를 사용자 PC로 다운로드하는 방법에 대해 살펴봅니다.

순서	설정 과정
1	<p><b>System - 애플리케이션 - 시그니처 내보내기</b> 메뉴를 클릭합니다.</p> <p>&lt;시그니처 내보내기&gt;에서 다음 설명을 참고하여 각 항목을 설정한 후 <b>[내보내기]</b> 버튼을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>▣ 시그니처 내보내기</p> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 10px;">시그니처 ▾</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">애플리케이션 ▾</div> <div style="border: 1px solid #ccc; padding: 2px 10px;">정렬 기준 ▾</div> <div style="background-color: #007bff; color: white; padding: 2px 10px; border-radius: 3px;">내보내기</div> </div> </div>
2	<ul style="list-style-type: none"> <li>• <b>시그니처</b> 다운로드할 WEBFRONT-K 웹 보안 기능의 종류를 선택합니다.</li> <li>• <b>애플리케이션</b> 다운로드할 애플리케이션을 선택합니다.</li> <li>• <b>정렬 기준</b> 시그니처 목록의 정렬 기준을 선택합니다. (기본값: 시그니처)</li> </ul> <p> <b>참고:</b> 시그니처와 애플리케이션을 지정하지 않고 <b>[내보내기]</b> 버튼을 클릭하면, 모든 시그니처와 애플리케이션을 대상으로하여 파일을 생성합니다.</p>
3	<p>&lt;시그니처 내보내기&gt; 팝업 창에서 파일이름을 입력한 후 <b>[저장]</b> 버튼을 클릭합니다. 파일명은 최대 20 글자의 영문자와 숫자, 그리고 ₩/:*?"&lt;&gt; #% 를 제외한 특수 문자로 구성될 수 있습니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0; width: fit-content;"> <p style="text-align: center; font-size: small;">시그니처 내보내기</p> <div style="border: 1px solid #ccc; height: 20px; margin-bottom: 5px;"></div> <div style="display: flex; justify-content: flex-end; gap: 5px;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">닫기</div> <div style="background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">저장</div> </div> </div>
4	<p>시그니처 내보내기 목록에서 <b>[다운로드]</b>버튼을 클릭합니다.</p> <p> <b>참고:</b> 다운로드 파일의 형식은 엑셀파일입니다.</p>

# 정규식 설정

애플리케이션 보안 기능을 설정할 때 정규식을 입력하는 경우가 있습니다. 주로 시그니처를 등록할 때 사용됩니다. 정규식은 구성이 일반 문자의 조합에 비해 복잡하므로 정규식에 대해 익숙하게 알고 있는 관리자가 아닌 경우에는 원하는 값을 바로 정규식으로 정의하기가 어려울 수 있습니다. 그리고, 유사한 형식의 정규식을 여러 군데 사용하는 경우, 그 때마다 정규식을 입력해야 하는 경우도 있습니다. WEBFRONT-K는 이러한 불편함을 줄이기 위해 정규식을 미리 정의해 놓을 수 있습니다. 이렇게 정규식을 미리 정의해두면 실제 정규식을 사용하는 화면(요청검사의 폼필드검사, 쿠키보호)에서는 정의된 정규식을 선택하기만 하면 되므로 편리합니다.

이 절에서는 정규식에 대해 살펴본 후 WEBFRONT-K에 정규식을 정의하는 방법을 소개합니다.

## 정규식

정규식은 일반 문자(영문자)와 메타 문자로 알려진 특수 문자로 구성된 텍스트의 패턴입니다. 패턴은 텍스트를 검색할 때 특정 문자열뿐만 아니라 하나 이상의 다양하고 복잡한 문자열을 검사할 수 있습니다. WEBFRONT-K는 POSIX 1003.2에 정의된 확장 정규식을 지원합니다. 다음은 정규식에서 사용할 수 있는 메타 문자들입니다.

메타 문자	설명
.	어떤 하나의 문자를 매치
\w	^[a-zA-Z0-9_]*와 같은 메타 문자를 보통 문자로 사용하기 위해 사용하는 escape 문자
*	선행 element가 없거나 있을 때 매치
?	선행 element가 없거나 하나일 때 매치
+	선행 element가 하나나 그 이상일 때 매치
^	시작 문자열을 매치
\$	끝 문자열을 매치
[abc] or [a-c]	[ ] 내의 하나의 문자(또는 범위) 매치
[^abc] or [^a-c]	[ ] 내의 리스트를 제외한 어떤 하나의 문자 매치
( )	Expression을 그룹으로 묶어 처리할 때 사용
	OR 연산자. 피연산자 중 하나라도 일치되면 매치
{x}	선행 element가 정확히 x번 발생시 매치
{x,}	선행 element가 적어도 x번 발생시 매치
{x,y}	선행 element가 적어도 x번 발생하고, y보다 많이 발생하지 않는 매치

다음은 자주 사용되는 정규식들입니다. 이 정규식들은 WEBFRONT-K에는 기본적으로 등록되어 있습니다.

- ^[[:alpha:]]\*\$  
알파벳으로 구성된 문자열
- ^[[:digit:]]\*\$  
십진수로 구성된 문자열
- ^[[:alnum:]]\*\$  
알파벳과 십진수로 구성된 문자열
- ^((([A-Za-z0-9]+\_+)|([A-Za-z0-9]+W+)|([A-Za-z0-9]+W+)))\*[A-Za-z0-9]+@((Ww+W+)|(Ww+W+))\*Ww{1,63}W.[a-zA-Z]{2,6}\$  
이메일 주소 형태의 문자열
- ^[[:digit:]]{6}-[[:digit:]]{7}\$  
한국의 주민등록번호 형태의 문자열

## 정규식 등록하기

정규식을 등록하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 정규식 설정 메뉴를 클릭합니다.
2	<정규식 리스트>의 [변경] - [추가] 버튼을 클릭합니다.
3	<p>&lt;정규식 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [확인] 버튼을 클릭합니다.</p> <div data-bbox="624 445 1062 633" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• <b>아이디</b> 정규식의 ID를 1-255 범위의 숫자로 입력합니다. 정규식 ID는 등록된 정규식을 서로 구분하기 위해 사용됩니다.</li> <li>• <b>정규식</b> 등록할 정규식을 입력합니다. 정규식은 이 창의 [정규식 설정 &gt; 정규식]을 참고합니다. 정규식은 최대 1024 문자까지 입력할 수 있습니다.</li> <li>• <b>설명</b> 정규식에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)</li> </ul>
4	등록한 정규식을 장비에 저장하기 위해 [적용] 버튼을 클릭합니다.

# 블랙리스트 관리

블랙리스트는 웹 공격을 자주 시도하는 클라이언트를 구분하여 웹 서버로의 접근을 제한하는 기능입니다. 이 절에서는 블랙리스트 기능을 설정하는 화면과 설정 과정, 그리고 설정하는 방법에 대해 살펴봅니다.

## 설정 개요

### 설정 화면

System - 애플리케이션 - 블랙리스트관리 메뉴를 클릭하면 블랙리스트 기능을 설정하는 화면이 나타납니다.



화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **블랙리스트 상태** 블랙리스트 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 블랙리스트 기능의 활성화 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **블랙리스트 옵션** 블랙리스트 기능 설정 시 사용할 수 있는 옵션과 설정 값이 출력됩니다.
- **블랙리스트 설정(세션 상태)** 블랙리스트 설정(세션 상태) 기능의 사용 여부가 표시됩니다.
- **블랙리스트 고급 설정(프록시 IP 헤더 리스트)** 블랙리스트 고급 설정(프록시 IP 헤더 리스트) 기능의 사용 여부와 프록시 IP 헤더리스트가 표시됩니다.
- **블랙리스트 고급 설정(사용자 정의 IP)** 사용자가 직접 등록한 영구 차단 IP 주소와 블랙리스트 기능에서 제외할 허용 IP 주소가 출력됩니다.
- **블랙리스트 차단 IP 리스트** 허용 공격 수를 초과하여 일시적으로 차단된 IP 주소와 차단이 해제되기 까지 남은 시간이 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [변경] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 블랙리스트 기능을 설정하는 과정은 다음과 같습니다.

- ❶ **블랙리스트 옵션 설정**  
블랙리스트 차단 IP 리스트에 등록하기 위한 기준과 차단 시간, 그리고 추가 차단 옵션을 설정합니다.
- ❷ **블랙리스트 설정 (세션 상태)**  
클라이언트 IP 주소를 기준으로 블랙리스트 옵션 설정을 적용할 것인지 지정합니다. 블랙리스트 차단 IP 리스트에 추가될 클라이언트 IP는 블랙리스트 옵션의 허용 공격 수와 차단 시간 설정에 따라 결정됩니다.

③ 블랙리스트 고급 설정(프록시 IP 헤더 리스트)

HTTP 요청 헤더의 프록시 IP 헤더 값을 기준으로 블랙리스트 옵션 설정을 적용할 것인지 지정하고, 프록시 헤더 값을 등록합니다. 블랙리스트 차단 IP 리스트에 추가될 클라이언트 IP는 프록시 헤더 설정과, 블랙리스트 옵션의 허용 공격 수와 차단 시간 설정에 따라 결정됩니다

④ 블랙리스트 고급 설정(사용자 정의 IP)

블랙리스트 허용 IP 주소와 블랙리스트 영구 차단 IP 주소를 설정합니다. 블랙리스트 허용 IP 주소는 블랙리스트 기능을 적용하지 않을 IP 주소를 설정하고, 블랙리스트 영구 차단 IP 주소는 웹 서버로의 접근을 무조건 차단할 IP 주소를 설정합니다.

⑤ 관련 기능의 활성화 상태 설정

블랙리스트 기능의 사용 여부와 이 기능에 대한 보안 로그, 차단 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

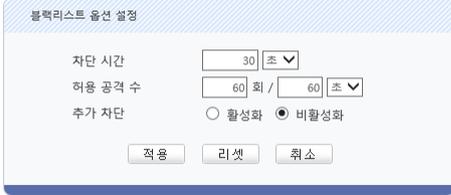
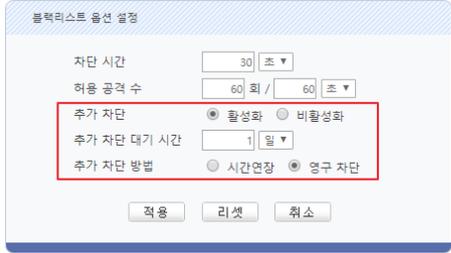
⑥ 블랙리스트 차단 IP 리스트 설정

블랙리스트 기능에 의해 차단된 IP 주소를 블랙리스트 차단 IP 리스트에서 제거하거나 블랙리스트 허용 IP 리스트, 블랙리스트 영구 차단 IP 리스트에 등록합니다.

# 블랙리스트 설정하기

## 블랙리스트 옵션 설정

블랙리스트 옵션을 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 블랙리스트관리 메뉴를 클릭합니다.
2	<블랙리스트 옵션>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;블랙리스트 옵션 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>차단 시간</b> 블랙리스트 차단 IP 리스트에 등록된 IP 주소를 차단할 시간을 입력합니다. (설정 범위: 1초 ~ 30일, 기본값: 30초)</li> <li>• <b>허용 공격 수</b> 블랙리스트 차단 IP 리스트에 등록하기 위한 기준이 되는 단위 시간과 공격 횟수를 입력합니다. 단위 시간 동안 특정 IP 주소의 요청 패킷이 허용 공격 수를 초과하여 요청 검사 기능에 의해 차단되거나 탐지되면, 해당 IP 주소를 블랙리스트 차단 IP 리스트에 등록합니다. (설정 범위: 1 ~ 65535회/1초 ~ 30일, 기본값: 60회/60초)</li> <li>• <b>추가 차단</b> 추가 차단 사용 여부를 설정합니다. 추가 차단을 활성화하면 블랙리스트 차단 IP 리스트에서 해제된 이후 해당 IP 주소가 추가 차단 대기 시간 안에 다시 등록되면 추가 차단 방법 설정에 따라 차단합니다. (기본값: 비활성화)</li> </ul> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>- 추가 차단 대기 시간: 추가 차단 대기 시간을 입력합니다. (설정 범위: 1초 ~ 30일, 기본값: 1일)</li> <li>- 추가 차단 방법: 추가 차단 방법을 선택합니다.             <ul style="list-style-type: none"> <li>* 시간연장: 차단을 연장할 시간을 입력합니다. (설정 범위: 1초 ~ 30일, 기본값: 10초)</li> <li>* 영구 차단: 해당 IP를 영구적으로 차단할 경우 선택합니다.</li> </ul> </li> </ul>

## 블랙리스트 설정(세션 상태)

이 기능은 클라이언트 IP 주소로 공격의 빈도를 확인하여 웹 서버로의 접근을 차단하는 기능입니다. 바로 위에서 설정한 블랙리스트 옵션 조건과 일치하면 해당 클라이언트 IP 주소는 블랙리스트에 추가됩니다. 이 기능을 적용하려면 각 요청 검사(Application - 요청검사)의 블랙리스트 항목을 활성화해야 합니다.

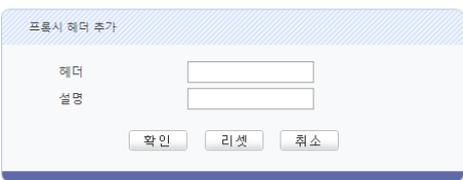
블랙리스트 설정(세션 상태) 기능의 사용 여부를 지정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 블랙리스트관리 메뉴를 클릭합니다.
2	<블랙리스트 설정(세션 상태)>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;블랙리스트 고급 설정(세션 상태)&gt; 팝업 창에서 블랙리스트 세션 상태 기능을 활성화할 것인지 지정합니다. (기본값: 비활성화)</p> 

## 블랙리스트 고급 설정(프록시 IP 헤더 리스트)

이 기능은 HTTP 요청 헤더의 프록시 헤더 값으로 공격의 빈도를 확인하여 해당 클라이언트의 접근을 차단하는 기능입니다. 예를 들어 블랙리스트 고급 설정의 프록시 IP 헤더 리스트에 'x-forwarded-for'가 등록되어 있고, 클라이언트의 HTTP 요청 헤더에 'x-forwarded-for: 1.1.1.1'가 포함되어 있으면 1.1.1.1은 블랙리스트 대상으로 관리됩니다. 이 기능을 적용하려면 각 요청 검사(Application - 요청검사)의 블랙리스트 항목을 활성화해야 합니다.

블랙리스트의 프록시 IP 헤더를 설정하는 방법은 다음과 같습니다.

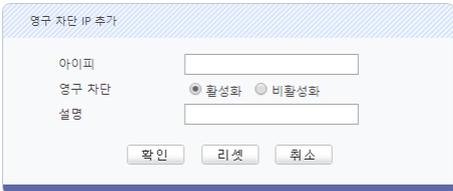
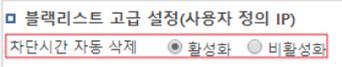
순서	설정 과정
1	System - 애플리케이션 - 블랙리스트관리 메뉴를 클릭합니다.
2	<블랙리스트 고급 설정(프록시 IP 헤더 리스트)>의 [변경] - [변경] - [추가] 버튼을 클릭합니다.
3	<p>&lt;프록시 헤더 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [확인] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>헤더</b> 차단할 프록시 헤더를 입력합니다. 알파벳, 숫자와 '.' 기호로 이루어진 최대 128자의 문자열을 입력할 수 있습니다.</li> <li>• <b>설명</b> 프록시 헤더에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다.</li> </ul>
4	상태 항목에서 등록된 프록시 IP 헤더 리스트의 활성화 여부를 지정합니다. (기본값: 비활성화)
5	설정이 완료되면 [적용] 버튼을 클릭합니다.

## 블랙리스트 고급 설정(사용자 정의 IP)

블랙리스트 고급 설정(사용자 정의 IP)은 블랙리스트 옵션에서 설정한 허용 공격 수와 상관없이 웹 서버로의 접근을 차단 및 허용할 IP 주소를 설정하는 기능입니다. 이 기능은 영구적 또는 일정 시간 동안 접근을 차단할 영구 차단 IP 리스트 설정과 블랙리스트 기능에서 제외할 IP 주소를 설정하는 허용 IP 리스트 설정으로 구성되어 있습니다. 블랙리스트 고급 설정(사용자 정의 IP)에는 차단 및 허용 IP 주소를 최대 1024개까지 등록할 수 있습니다.

### 블랙리스트 영구 차단 IP 리스트 설정

영구 차단 IP 리스트를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 블랙리스트관리 메뉴를 클릭합니다.
2	<블랙리스트 고급 설정(사용자 정의 IP)>의 [변경] 버튼을 클릭합니다.
3	<블랙리스트 영구 차단 IP 리스트>의 [추가] 버튼을 클릭합니다.
4	<p>&lt;영구 차단 IP 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [확인] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>아이피</b> 요청 패킷을 영구적으로 차단할 IP 주소를 입력합니다. IP 주소만 설정할 수도 있고 넷 마스크 비트(bit) 수를 입력하여 IP 주소 대역을 설정할 수도 있습니다. 예) IP 주소: 192.168.200.10, IP 주소 대역: 192.168.200.0/24</li> <li>• <b>영구 차단</b> 영구 차단 적용 여부를 선택합니다. <ul style="list-style-type: none"> <li>- 활성화: 해당 IP 주소에 대해 영구적으로 차단합니다.</li> <li>- 비활성화: 해당 IP 주소에 대해 설정된 차단 시간 동안 차단합니다. 차단 시간을 설정하는 방법은 이 장의 <b>블랙리스트 관리 &gt; 블랙리스트 설정하기 &gt; 블랙리스트 옵션 설정</b> 절을 참고합니다.</li> </ul> </li> <li>• <b>설명</b> 영구 차단 IP 주소에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)</li> </ul>
5	<p>차단시간 자동 삭제 항목에서 자동 삭제 기능의 활성화 여부를 지정합니다. (기본값: 활성화)</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>활성화</b> 차단 시간이 만료된 IP 주소를 블랙리스트 영구 차단 IP 리스트에서 매시간 59분마다 자동으로 삭제합니다. (기본값)</li> <li>• <b>비활성화</b> 차단 시간이 만료된 IP주소는 자동으로 삭제되지 않고, 관리자가 직접 삭제해야 합니다.</li> </ul>
6	블랙리스트 영구 차단 IP 설정이 완료되면 [적용] 버튼을 클릭합니다.

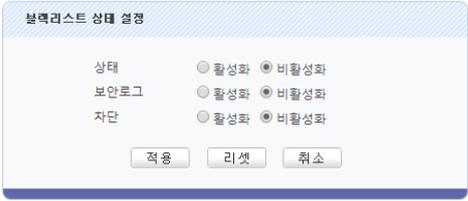
## 블랙리스트 허용 IP 리스트 설정

허용 IP 리스트를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 블랙리스트관리 메뉴를 클릭합니다.
2	<블랙리스트 고급 설정(사용자 정의 IP)>의 [변경] 버튼을 클릭합니다.
3	<블랙리스트 허용 차단 IP 리스트>의 [추가] 버튼을 클릭합니다.
4	<p>&lt;예외 IP 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [확인] 버튼을 클릭합니다.</p> <div data-bbox="609 456 1077 654" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• <b>아이피</b> 블랙리스트 기능에서 제외할 IP 주소를 입력합니다. IP 주소만 설정할 수도 있고 넷 마스크 비트(bit) 수를 입력하여 IP 주소 대역을 설정할 수도 있습니다. 예) IP 주소: 192.168.200.10, IP 주소 대역: 192.168.200.0/24</li> <li>• <b>영구 허용</b> 영구 허용 적용 여부를 선택합니다. <ul style="list-style-type: none"> <li>- 활성화: 해당 IP 주소에 대해 영구적으로 허용합니다.</li> <li>- 비활성화: 해당 IP 주소에 대해 설정된 시간 동안 허용합니다. 시간을 설정하는 방법은 이 장의 <b>블랙리스트 관리 &gt; 블랙리스트 설정하기 &gt; 블랙리스트 옵션 설정</b> 절을 참고합니다.</li> </ul> </li> <li>• <b>설명</b> 허용 IP 주소에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)</li> </ul>
5	블랙리스트 영구 허용 IP 설정이 완료되면 [적용] 버튼을 클릭합니다.

## 관련 기능의 상태 설정

블랙리스트 기능의 사용 여부와 블랙리스트 기능과 관련된 보안 로그, 차단 기능의 상태를 지정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 블랙리스트관리</b> 메뉴를 클릭합니다.
2	<블랙리스트 상태>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;블랙리스트 상태 설정&gt; 팝업 창에서 각 항목의 상태를 지정한 후 <b>[적용]</b> 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>상태</b> 블랙리스트 기능을 활성화할 것인지 지정합니다.</li> <li>• <b>보안로그</b> 블랙리스트 차단 IP 리스트와 영구 차단 IP 리스트에 등록된 클라이언트의 요청에 대한 로그를 기록할 것인지 지정합니다. 기록된 로그는 <b>[System - 통합로그]</b> 메뉴에서 확인할 수 있습니다.</li> <li>• <b>차단</b> 블랙리스트 차단 IP 리스트와 영구 차단 IP 리스트에 등록된 클라이언트의 요청을 차단할 것인지 지정합니다.</li> </ul>

## 블랙리스트 차단 IP 리스트 설정

블랙리스트 차단 IP 리스트에서 등록된 IP 주소의 차단 상태를 해제하거나 영구 차단 IP 리스트, 허용 IP 리스트에 등록하는 방법은 다음과 같습니다.



참고: 블랙리스트 차단 IP 리스트는 블랙리스트 옵션 설정에 따라 자동으로 등록되며 사용자가 직접 추가할 수 없습니다.



참고: 블랙리스트 기능의 상태가 비활성화된 경우에는 블랙리스트 IP 리스트 설정을 할 수 없습니다.

순서	설정 과정
1	<b>System - 애플리케이션 - 블랙리스트관리</b> 메뉴를 클릭합니다.
2	<블랙리스트 차단 IP 리스트>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;블랙리스트 차단 IP 리스트 설정&gt; 화면에서 상태를 변경할 IP 주소의 <b>[제거]</b>, <b>[영구 차단]</b>, <b>[허용]</b> 항목을 클릭합니다. 각 항목을 클릭하면 ● 표시가 나타나며 <b>[전체 선택]</b> 버튼을 사용하면 모든 IP 주소의 상태를 한번에 변경할 수 있습니다.</p> <div style="text-align: center;">  </div>
4	설정이 완료되면 <b>[적용]</b> 버튼을 클릭합니다.

# 화이트리스트 관리

화이트리스트(Whitelist)는 클라이언트와 서버의 IP 주소/포트 번호가 필터와 일치하는 경우, 모든 애플리케이션에 대해 보안 기능만 바이패스(Bypass)하여 접근을 허용하는 기능입니다. 이 절에서는 화이트리스트를 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 화이트리스트를 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

System - 애플리케이션 - 화이트리스트관리 메뉴를 클릭하면 화이트리스트 기능을 설정하는 화면이 나타납니다.



화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **화이트리스트 상태**      화이트리스트 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 화이트리스트 기능의 활성화 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **화이트리스트 목록**      전체 애플리케이션에 대해 보안 기능을 적용하지 않고 허용할 클라이언트 IP 주소와 포트, 서버 IP주소와 포트가 출력됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [변경] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 화이트리스트 기능을 설정하는 과정은 다음과 같습니다.

- ❶ **화이트리스트 목록 설정**  
화이트리스트 기능을 적용할 클라이언트와 서버의 IP 주소/포트 번호를 설정합니다. 화이트리스트에 등록된 IP 주소/포트 번호는 웹 서버로의 접근을 허용합니다.
- ❷ **관련 기능의 활성화 상태 설정**  
화이트리스트 기능의 사용 여부를 지정합니다.

# 화이트리스트 설정하기

## 화이트리스트 목록 설정

화이트리스트 기능을 적용할 클라이언트와 서버의 IP 주소/포트 번호를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 화이트리스트관리 메뉴를 클릭합니다.
2	<화이트리스트 목록>의 [변경] 버튼을 클릭합니다.
3	<화이트리스트 IP/PORT 설정>의 [추가] 버튼을 클릭합니다.
4	<p>&lt;화이트리스트 IP/PORT 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [확인] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• 클라이언트            화이트리스트를 적용할 클라이언트의 IP주소를 1.1.1.1/24와 같은 형식으로 입력합니다. (기본값: 전체)</li> <li>• 클라이언트 포트    화이트리스트를 적용할 클라이언트의 포트번호를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 전체)</li> <li>• 서버                    화이트리스트를 적용할 서버의 IP주소를 1.1.1.1/24와 같은 형식으로 입력합니다. (기본값: 전체)</li> <li>• 서버 포트            화이트리스트를 적용할 서버의 포트번호를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 전체)</li> <li>• 설명                    화이트리스트에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)</li> </ul>
5	화이트리스트 IP/PORT 설정이 완료되면 [적용] 버튼을 클릭합니다.

## 관련 기능의 상태 설정

화이트리스트 기능의 사용 여부를 지정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 애플리케이션 - 화이트리스트관리 메뉴를 클릭합니다.
2	<화이트리스트 상태>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;화이트리스트 상태&gt; 팝업 창에서 상태를 지정한 후 [적용] 버튼을 클릭합니다. 기본적으로 활성화되어 있습니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• 상태                    화이트리스트 기능을 활성화할 것인지 지정합니다.</li> </ul>

## 제8장 방화벽

이 장에서는 WEBFRONT-K의 시스템 접근 제어 기능과 방화벽 기능에 대해 살펴본 후, 이 기능을 사용하기 위한 설정 방법에 대해 알아보도록 합니다. 시스템 접근 제어는 지정한 사용자만 WEBFRONT-K로 접근할 수 있도록 하는 기능입니다. 방화벽 기능은 WEBFRONT-K에 연결된 네트워크를 보호하기 위해 다양한 조건의 필터를 사용하여 불필요한 트래픽이 송수신되지 않도록 합니다.

이 장은 다음과 같은 내용으로 구성되어 있습니다.

- 시스템 접근 제어
- Snort 설정
- 방화벽



# 시스템 접근 제어

이 절에서는 시스템 접근 제어 기능에 대해 살펴본 후 설정 방법에 대해 소개하도록 합니다.

## 개요

시스템 접근 제어 기능은 시스템을 보호하기 위해 지정된 IP 주소와 포트 번호만 WEBFRONT-K로 접속할 수 있도록 제한하는 기능입니다. 시스템 접근 기본 설정은 '차단'이며, 보안 관리를 위한 서비스 포트(TCP 8443/22/23, ICMP)에 대해서만 허용 정책이 등록되어 있습니다. 운영 환경에 맞게 특정한 IP 주소와 포트 번호만 접근할 수 있도록 수정해야 합니다. 만약 사용자 접근 IP 리스트 기능이 활성화되어 있으면, 사용자 접근 IP 리스트에도 IP 주소를 등록해야 WEBFRONT-K 웹 매니저에 접근할 수 있습니다. 사용자 접근 IP 리스트에는 기본적으로 '192.168.100.2'가 등록되어 있으며 **System - 사용자 관리 - 사용자 접근 IP 리스트** 메뉴에서 수정할 수 있습니다.

## 시스템 접근 제어 설정하기

시스템 접근 제어 기능을 사용하기 위해 관리 접근 허용 IP 주소를 설정하는 방법을 살펴봅니다.

### 시스템 접근 규칙 설정

다음은 시스템 접근 규칙을 설정하는 방법입니다. 시스템 접근 규칙은 최대 1024개까지 등록할 수 있습니다.

순서	설정 과정
1	<b>System - 방화벽 - 시스템 접근</b> 메뉴를 클릭합니다.
2	<시스템 접근 규칙 리스트>의 [변경] - [추가] 버튼을 클릭합니다. <시스템 접근 규칙 추가> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [적용] 버튼을 클릭합니다.
3	<div data-bbox="592 1111 1098 1532" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• <b>아이디</b> 시스템 접근 규칙의 ID를 1~1024 범위의 값 중에서 지정합니다.</li> <li>• <b>프로토콜</b> 패킷 비교 조건으로 사용할 프로토콜 종류를 선택합니다.</li> <li>• <b>정책</b> 규칙의 조건에 만족하는 패킷을 허용할 것인지 폐기할 것인지를 지정합니다. 허용하려는 경우에는 '허용'을, 폐기하려는 경우에는 '차단' 항목을 선택합니다. (기본값: 차단)</li> <li>• <b>상태</b> 규칙의 활성화 여부를 선택합니다. '활성화'를 선택하면 접근 규칙이 지정한 인터페이스로 수신되는 패킷에 즉시 적용됩니다. '비활성화'를 선택하면 설정한 접근 규칙이 적용되지 않습니다. (기본값: 활성화)</li> <li>• <b>출발지 IP 주소</b> 패킷 비교 조건으로 사용할 출발지 IP 주소를 지정합니다. 입력 형식은 A.B.C.D/M입니다. A, B, C, D는 각각 1~256 범위의 십진수이고, M은 넷마스크 비트입니다. (기본값: 0.0.0.0/0)</li> <li>• <b>출발지 포트</b> 패킷 비교 조건으로 사용할 출발지 포트 번호나 포트 범위를 지정합니다. 포트 범위를 지정할 때에는 100-150과 같이 입력하면 됩니다. (기본값: 0)</li> <li>• <b>목적지 IP 주소</b> 패킷 비교 조건으로 사용할 목적지 IP 주소를 지정합니다. 입력 형식은 A.B.C.D/M입니다. A, B, C, D는 각각 1~256 범위의 십진수이고, M은 넷마스크 비트입니다. (기본값: 0.0.0.0/0)</li> <li>• <b>목적지 포트</b> 패킷 비교 조건으로 사용할 목적지 포트 번호나 포트 범위를 지정합니다. 포트 범위를 지정할 때에는 100-150과 같이 입력하면 됩니다. (기본값: 0)</li> <li>• <b>인터페이스</b> 인터페이스 목록에서 설정 중인 규칙을 적용할 인터페이스를 선택합니다. 'mgmt' 항목은 관리용 이더넷 포트 인터페이스입니다. 현재 정의되어 있는 VLAN 인터페이스가 없는 경우에는 드롭다운 목록에 mgmt</li> </ul>

	항목만 표시됩니다. 모든 인터페이스에 적용하려면 'any'를 선택합니다. (기본값: any)
4	시스템 접근 규칙을 모두 추가한 후에는 [적용] 버튼을 눌러 추가한 시스템 접근 규칙을 저장하고 시스템에 적용합니다.

### 기본 시스템 접근 정책 설정

기본 시스템 접근 정책은 기본적으로 '차단'으로 설정되어 있습니다. 이 상태에서는 모든 접근을 차단하기 때문에 접근을 허용하려면 시스템 접근 규칙을 설정해야 합니다. 시스템 접근 규칙을 설정하는 방법은 이 장의 [시스템 접근 제어 > 시스템 접근 제어 설정하기 > 시스템 접근 규칙 설정] 절을 참고합니다.

기본 시스템 접근 정책을 '허용'으로 설정하면 모든 접근을 허용하기 때문에 설정된 시스템 접근 규칙이 적용되지 않습니다. 설정된 시스템 접근 규칙대로 WEBFRONT-K로의 접근을 제어하려면 기본 시스템 접근 정책을 '차단'으로 설정해야 합니다.

순서	설정 과정
1	<b>System - 방화벽 - 시스템 접근</b> 메뉴를 클릭합니다.
2	<기본 시스템 접근 정보>의 [변경] 버튼을 클릭합니다.
3	<기본 시스템 접근 정보 설정> 팝업 창에서 상태를 지정한 후 [적용] 버튼을 클릭합니다. (기본값: 차단)



**주의:** 기본 시스템 접근 정책을 '차단'으로 설정하게 되면, 현재 WEBFRONT-K에 접속해 있는 PC가 시스템 접근 규칙을 만족하지 않을 경우 WEBFRONT-K로 접근이 허용되지 않아 WEBFRONT-K와의 접속이 끊어지게 됩니다. 기본 시스템 접근 정책을 차단으로 설정하기 전에 반드시 WEBFRONT-K로 접속할 수 있도록 시스템 접근 규칙을 설정해야 합니다.

# Snort 설정

이 절에서는 Snort 기능에 대해 살펴본 후 설정 방법에 대해 소개하도록 합니다.

## 개요

Snort 기능은 WEBFRONT-K를 통과하는 네트워크 트래픽을 검사하여 유해트래픽인 경우 탐지 또는 차단하는 기능입니다. WEBFRONT-K를 통과하는 트래픽이 사전에 정의된 규칙과 일치하면 공격 또는 비정상 트래픽으로 판단하여 탐지 및 차단합니다. Snort 탐지 규칙은 최대 1024개까지 등록할 수 있습니다.

## Snort 설정하기

Snort 기능을 설정하는 방법을 살펴봅니다.

### Snort 상태 설정

다음은 Snort 기능의 상태를 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 방화벽 - Snort</b> 메뉴를 클릭합니다.
2	< <b>Snort</b> >의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;<b>Snort - 상태 설정</b>&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 <b>[적용]</b> 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>상태</b> Snort 기능을 활성화할 것인지 지정합니다.</li> <li>• <b>모드</b> Snort 탐지 규칙에 매칭된 패킷에 대해 탐지 로그를 생성할 것인지 차단할 것인지 지정합니다. <ul style="list-style-type: none"> <li>- 탐지: 트래픽이 Snort 규칙에 포함된 경우 해당 트래픽을 통과시키고 보안로그를 생성합니다.</li> <li>- 차단: 트래픽이 Snort 규칙에 포함된 경우 해당 트래픽을 차단합니다.</li> </ul> </li> </ul>

### Snort 규칙 업로드

Snort 규칙을 적용하려면 Snort 규칙을 업로드해야 합니다. Snort 규칙은 파일 단위로 업로드하며 한 개의 파일에 최대 1000개의 규칙을 포함할 수 있습니다.

순서	설정 과정
1	<b>System - 방화벽 - Snort</b> 메뉴를 클릭합니다.
2	< <b>Snort 규칙 업로드</b> >의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;<b>Snort 규칙 업로드</b>&gt; 팝업 창에서 <b>[파일 선택]</b> 버튼을 누른 다음 Snort 규칙 파일을 선택한 후 <b>[적용]</b> 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div>



**참고:** Snort 규칙 파일은 Snort 공식 홈페이지(<https://www.snort.org/>)에서 제공하는 규칙과 동일한 형식으로 작성합니다.

- 형식: Action + Protocol + Source IP address + Source Port + Direction + Dest IP address + Dest Port + Options
- 사용 예: alert tcp any any -> 172.16.100.253/24 80 (msg:"yaho"; uricontent:"/abcd"; nocase; content:"HostW: 172.16.100.253";nocase; sid:1199882; rev:0)



**주의:** Snort 공식 홈페이지(<https://www.snort.org/>)에서 제공하는 규칙(rule) 파일을 사용하는 경우 일부만 적용됩니다

# 방화벽

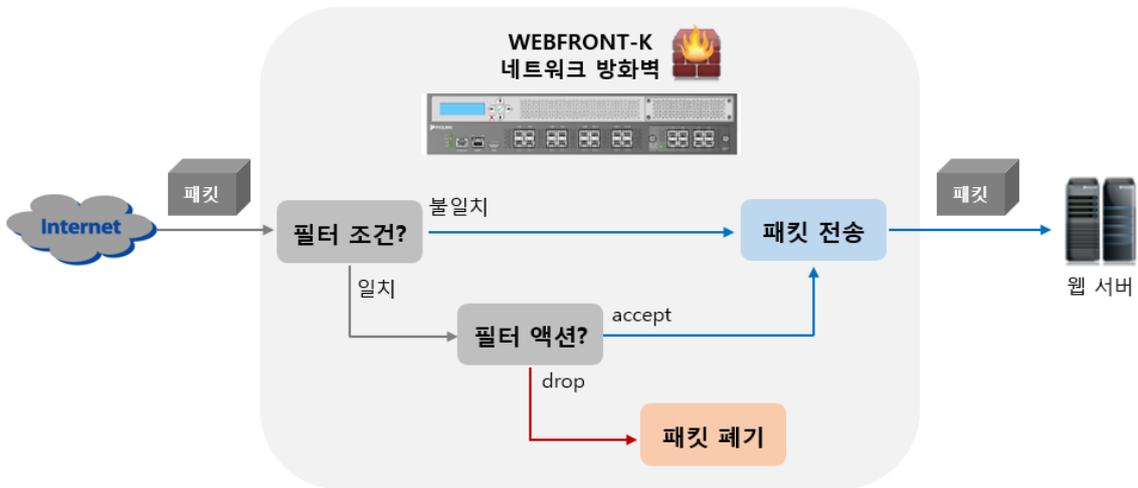
이 절에서는 WEBFRONT-K의 방화벽 기능에 대해 살펴봅니다.

## 개요

방화벽은 내부 네트워크를 보호하기 위해 허가된 네트워크 또는 사용자만 내부 네트워크로 접근할 수 있고 허가되지 않은 외부 네트워크의 접근은 차단하는 기능입니다. 네트워크 관리자는 다양한 보안 정책을 설정하여 지속적으로 발견되고 보고되는 보안상 취약한 부분들을 수정함으로써 네트워크의 보안 수준을 높이는 것이 필요합니다. 방화벽은 네트워크의 보안 수준을 높이는데 꼭 필요한 도구 중에 하나입니다.

WEBFRONT-K는 방화벽의 한 종류인 패킷 필터링 방화벽 기능을 제공합니다. 패킷 필터링 방화벽은 내부 네트워크와 외부 네트워크 간에 송수신되는 패킷들을 모니터링하여 설정된 필터의 조건에 따라 패킷을 필터링합니다. 각 필터는 '조건'과 '동작'으로 구성됩니다. 조건은 패킷을 구분할 때 사용되고 동작은 조건을 통해 구분된(조건을 만족하는) 패킷을 허용(accept)할 것인지 폐기(drop)할 것인지 등을 지정합니다. 이러한 패킷 필터링 방화벽을 사용하면 외부 네트워크에 노출시킬 내부 네트워크를 제한할 수 있고(특정 포트 차단 등을 통해) 내부 네트워크에서 외부로 불필요하게 전송되는 트래픽이나 허용하지 않는 사이트로의 접속을 차단할 수 있습니다.

다음은 외부 네트워크로부터 수신된 패킷이 WEBFRONT-K의 방화벽에 의해 필터링되는 과정을 보여주는 그림입니다.



WEBFRONT-K는 방화벽의 필터링 조건으로 다음과 같은 값을 사용할 수 있습니다.

- 패킷의 프로토콜 종류
- 패킷의 출발지/목적지 IP 주소
- 패킷의 출발지/목적지 포트 번호
- 패킷의 내용(content)
- TCP 플래그(flag)
- 패킷의 길이
- ICMP 유형

WEBFRONT-K는 대부분의 방화벽이 제공하는 필터링 조건인 프로토콜 종류나 IP 주소, 포트 번호뿐만 아니라 패킷의 길이와 패킷의 내용, TCP 플래그 등의 다양한 필터링 조건을 제공함으로써, 보다 다양하고 높은 수준의 보안 정책을 설정할 수 있습니다.

# 방화벽 설정하기

이 절에서는 방화벽을 설정하는 과정과 실제로 방화벽을 설정하는 방법에 대해 살펴봅니다.

## 방화벽 설정 과정

WEBFRONT-K에 방화벽 기능을 설정하는 과정은 다음과 같습니다.

### ① 콘텐츠 정의

패킷의 콘텐츠 중 특정 문자열을 필터링 조건으로 사용하는 경우에 콘텐츠를 정의해야 합니다. 콘텐츠는 검색할 문자열(string)과 검색 위치(offset), 검색 범위(depth), 대소문자 구분 여부(case)로 구성됩니다. 여러 개의 콘텐츠를 필터링 조건으로 사용하는 경우에 이를 하나의 콘텐츠 그룹으로 정의하여 사용하면, 콘텐츠를 편리하게 관리할 수 있습니다.

### ② 필터 정의

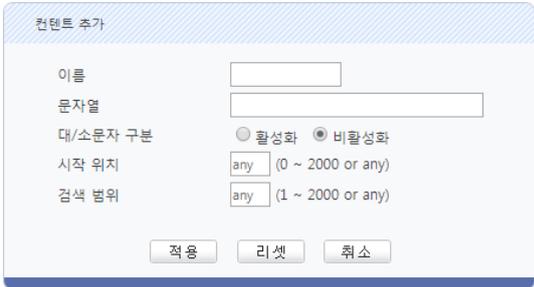
필터에는 패킷을 비교할 조건과 조건을 만족하는 패킷의 처리 방법이 정의됩니다. 패킷을 비교하는 조건으로는 패킷의 출발지/목적지 IP 주소와 출발지/목적지 포트 번호, 프로토콜 종류, 콘텐츠와 콘텐츠 그룹을 사용할 수 있습니다. 조건을 만족하는 패킷의 처리 방법으로는 패킷의 수신(accept), 폐기(drop), 패킷의 전송지로 리셋 메시지 전송(reject), 패킷의 전송 대역폭 제한(ratelimit)이 있습니다. WEBFRONT-K는 여러 필터를 사용할 경우에 하나의 필터 그룹으로 정의하여 사용하면, 여러 필터들을 각각 사용할 때보다 높은 성능 향상을 가져올 수 있습니다.

### ③ 방화벽 정책 정의

방화벽 정책은 필터나 필터 그룹과 이를 적용할 인터페이스로 구성됩니다. 방화벽 정책이 활성화되면 정책에 설정된 인터페이스를 통해 송신 또는 수신되는 패킷을 정책에 포함된 필터나 필터 그룹의 조건에 따라 필터링합니다.

## 콘텐츠 정의

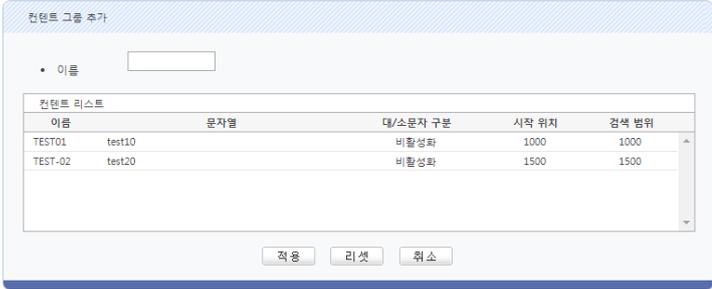
콘텐츠를 정의하는 방법은 다음과 같습니다. WEBFRONT-K에는 최대 256개의 콘텐츠를 정의할 수 있습니다.

순서	설정 과정
1	<b>System - 방화벽 - 콘텐츠</b> 메뉴를 클릭합니다.
2	<콘텐츠 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;콘텐츠 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li><b>이름</b> 정의할 콘텐츠의 이름을 입력합니다. 콘텐츠 이름은 최대 16자의 영문자와 숫자로 구성된 문자열로 첫 글자는 반드시 영문자여야 합니다.</li> <li><b>문자열</b> 패킷의 페이로드에서 검색할 문자열을 지정합니다. 따옴표(""), 인용 부호(), 콜론(:), 세미 콜론(;), 백슬래시(\)은 사용할 수 없습니다. 16진수를 입력하는 경우에는  7082C4 와 같이 16진수의 시작과 끝에  문자를 추가합니다. 문자열은 최대 100자까지 지정할 수 있습니다.</li> <li><b>대/소문자 구분</b> 드롭다운 목록을 클릭한 후 문자열을 검색할 때 대소문자를 구분할지 여부를 지정합니다. 대소문자를 구분하려면 활성화 항목을, 구분하지 않으려면 비활성화 항목을 선택합니다. (기본값: 비활성화)</li> <li><b>시작 위치</b> 문자열을 패킷의 페이로드에서 검색할 때 검색을 시작할 지점을 지정합니다. any로 지정한 경우에는 패킷의 페이로드 처음부터 문자열을 검색합니다. (설정 범위: 0 ~ 2,000 또는 any, 기본값: any)</li> </ul>

- **검색 범위** 페이로드에서 문자열 검색을 종료할 지점을 지정합니다. 이 값은 반드시 '시작 위치'항목에서 지정한 값보다 커야 합니다. any로 지정한 경우에는 패킷의 페이로드 끝까지 문자열을 검색합니다.  
(설정 범위: 1 ~ 2,000 또는 any, 기본값: any)

## 컨텐츠 그룹 정의

컨텐츠를 정의한 후에는 다음과 같은 방법으로 컨텐츠 그룹을 정의할 수 있습니다. WEBFRONT-K에는 최대 256개의 컨텐츠 그룹을 정의할 수 있습니다.

순서	설정 과정
1	<b>System - 방화벽 - 컨텐츠 그룹</b> 메뉴를 클릭합니다.
2	<컨텐츠 그룹 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;컨텐츠 그룹 추가&gt; 팝업 창에서 컨텐츠 그룹의 이름을 설정한 후 [적용] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>이름</b> 정의할 컨텐츠 그룹의 이름을 입력합니다. 컨텐츠 그룹의 이름은 최대 16자의 영문자와 숫자로 구성된 문자열로 지정하되, 첫 글자는 반드시 영문자여야 합니다.</li> <li>• <b>컨텐츠 리스트</b> 이 목록에 표시되는 값들은 현재 WEBFRONT-K에 정의되어 있는 컨텐츠들입니다. 컨텐츠 중에서 컨텐츠 그룹에 포함시킬 컨텐츠 항목을 선택합니다. 하나의 컨텐츠 그룹에는 최대 256개의 컨텐츠를 추가할 수 있습니다.</li> </ul>

## 필터 정의

방화벽 필터를 정의하는 방법은 다음과 같습니다. WEBFRONT-K에는 최대 256개의 방화벽 필터를 정의할 수 있습니다.

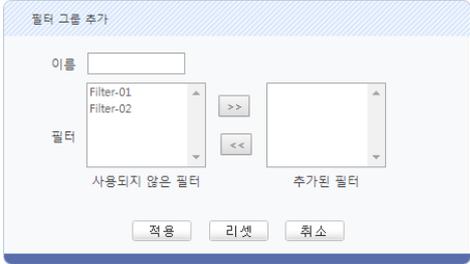
순서	설정 과정
1	<b>System - 방화벽 - 필터</b> 메뉴를 클릭합니다.
2	<필터 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;필터 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [적용] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>이름</b> 정의할 필터의 이름을 입력합니다. 필터의 이름은 최대 16자의 영문자와 숫자로 구성된 문자열로 첫 글자는</li> </ul>

반드시 영문자여야 합니다.

- **액션** 드롭다운 목록을 클릭한 후 다음 항목 중에서 필터의 조건과 일치하는 패킷을 처리할 방법을 지정합니다.
  - Accept: 조건과 일치하는 패킷 허용 (기본값)
  - Drop: 조건과 일치하는 패킷 폐기
  - Reject: 조건과 일치하는 패킷의 출발지 IP 주소로 리셋(Reset) 패킷을 전송
  - Rate Limit: 대역폭 제한 항목에 지정한 대역폭(패킷/초)으로 패킷을 수신
- **대역폭 제한** 제한할 대역폭을 지정합니다. 이 항목은 액션 항목을 'Rate Limit'로 선택한 경우에만 나타납니다. (설정 범위: 1 ~ 65,535(kbps))
- **프로토콜** 드롭다운 목록을 클릭한 후, 패킷을 필터링하는 기준으로 사용할 프로토콜 종류를 선택합니다. 'ANY'를 선택하면 프로토콜을 필터링의 기준으로 사용하지 않습니다. 이 항목에서 선택한 프로토콜의 종류에 따라 설정할 수 있는 항목의 종류가 다음과 같이 달라집니다. 기본으로 설정되는 프로토콜은 'TCP'입니다.
  - TCP: TCP 플래그, TCP 플래그 옵션 (기본값)
  - TCP, UDP: 출발지 포트
  - ICMP: ICMP 유형
- **출발지 IP 주소** 패킷의 필터링 기준으로 사용할 패킷의 출발지 IP 주소를 입력합니다. 출발지 IP 주소를 패킷 필터링 조건으로 사용하지 않으려면 any를 입력합니다. (기본값: any)
- **출발지 포트** 패킷의 필터링 기준으로 사용할 패킷의 출발지 포트 번호를 설정합니다. 먼저, 앞에 있는 드롭다운 목록에서 포트 번호의 비교 방법을 지정합니다. (기본값: any)
  - 같음: 출발지 포트가 입력한 포트와 일치하는지 확인합니다.
  - 보다 큼: 출발지 포트가 입력한 포트보다 큰지 확인합니다.
  - 보다 작음: 출발지 포트가 입력한 포트보다 작는지 확인합니다.
  - 범위: 출발지 포트가 입력한 포트의 범위에 포함되는지 확인합니다.
  - Any: 출발지 포트를 필터링 조건으로 사용하지 않습니다.같음, '보다 큼', '보다 작음'을 선택한 경우에는 드롭다운 목록의 오른쪽에 있는 입력란에 출발지 포트 번호를 입력하고, '범위'를 선택한 경우에는 아래에 나타나는 출발 포트 범위 항목에 비교할 포트의 시작 값과 마지막 값을 입력합니다.  
출발지 포트를 패킷 필터링 조건으로 사용하지 않는 경우에는 드롭다운 목록에서 'Any'를 선택합니다. 이 항목은 프로토콜 항목에서 TCP 또는 UDP를 선택했을 때만 활성화됩니다.
- **목적지 IP 주소** 패킷의 필터링 기준으로 사용할 패킷의 목적지 IP 주소를 입력합니다. 목적지 IP 주소를 패킷 필터링 조건으로 사용하지 않는 경우에는 any를 입력합니다. (기본값: any)
- **목적지 포트** 패킷의 필터링 기준으로 사용할 패킷의 목적지 포트 번호를 설정합니다. 설정하는 방법은 출발지 포트 항목과 동일합니다. (기본값: any)
- **보안로그** 드롭다운 목록을 클릭한 후 이 필터에 의해 패킷이 필터링된 정보를 로그로 남길지 여부를 설정합니다. 필터링 내역을 로그로 남기려면 '활성화'를, 남기지 않으려면 '비활성화'를 선택합니다. (기본값: 비활성화)
- **컨텐츠 / 컨텐츠 그룹**  
컨텐츠나 컨텐츠 그룹을 필터링 조건으로 추가하려면 드롭다운 목록을 클릭한 후 원하는 컨텐츠나 컨텐츠 그룹을 선택합니다. 없음을 선택하면 필터링 조건으로 컨텐츠나 컨텐츠 그룹을 사용하지 않습니다. (기본값: 없음)
- **TCP 플래그** 이 항목은 프로토콜 항목에서 'TCP'를 선택했을 때만 활성화됩니다. 패킷의 필터링 조건으로 사용할 TCP 플래그를 선택합니다. [Ctrl] 또는 [Shift] 키를 이용하여 여러 개의 플래그를 선택할 수 있습니다. 선택한 TCP 플래그를 비교하는 방법은 아래에 있는 TCP 플래그 옵션 항목에서 지정합니다. TCP 플래그를 패킷 필터링 조건으로 사용하지 않는 경우 'None'을 입력합니다. (기본값: None)
- **TCP 플래그 옵션**  
이 항목은 프로토콜 항목에서 'TCP'를 선택했을 때만 활성화됩니다. 드롭다운 목록을 클릭한 후 TCP 플래그 항목에서 선택한 TCP 플래그를 비교할 방법을 선택합니다. (기본값: 일치)
  - 일치: 선택한 모든 TCP 플래그가 '1'로 설정되어 있는지 비교 (기본값)
  - 포함: 선택한 TCP 플래그 중에서 하나라도 '1'로 설정되어 있는지 비교
- **ICMP 유형** 드롭다운 목록을 클릭한 후 ICMP 패킷을 필터링할 때 세부적인 필터링 조건으로 사용할 ICMP 패킷의 종류를 선택합니다. 이 항목은 프로토콜 항목에서 ICMP를 선택한 경우에만 활성화됩니다. ICMP의 유형을 패킷 필터링 조건으로 사용하지 않을 경우에는 'None'을 선택합니다. (기본값: None)
- **길이** 패킷의 필터링 조건으로 사용할 패킷 크기를 byte 단위로 입력합니다. 패킷 크기를 패킷 필터링 조건으로 사용하지 않는 경우에는 'any'를 입력합니다. (설정 범위: 1 ~ 2,000 또는 any, 기본값: any)

## 필터 그룹 정의

필터를 정의한 후에는 다음과 같은 방법으로 필터 그룹을 정의할 수 있습니다. WEBFRONT-K에는 최대 256개의 방화벽 필터 그룹을 정의할 수 있습니다.

순서	설정 과정
1	System - 방화벽 - 필터 그룹 메뉴를 클릭합니다.
2	<필터 그룹 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;필터 그룹 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li><b>이름</b> 정의할 필터 그룹의 이름을 입력합니다. 필터 그룹의 이름은 최대 16자의 영문자와 숫자로 구성된 문자열로 지정하되, 첫 글자는 반드시 영문자여야 합니다.</li> <li><b>필터</b> 왼쪽의 목록에 표시되는 값은 현재 WEBFRONT-K에 정의되어 있는 필터입니다. 필터 그룹에 포함할 필터를 선택한 후, [&gt;&gt;] 버튼을 클릭하면 오른쪽의 추가된 필터 목록으로 이동합니다. 추가된 필터를 선택한 후, [&lt;&lt;] 버튼을 클릭하면 사용되지 않은 필터 항목으로 이동합니다.</li> </ul>

## 정책 정의

필터나 필터 그룹을 정의한 후에는 다음과 같은 방법으로 방화벽 정책을 설정할 수 있습니다.

순서	설정 과정
1	System - 방화벽 - 정책 메뉴를 클릭합니다.
2	<정책 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;정책 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li><b>정책 이름</b> 방화벽 정책의 이름을 입력합니다. 필터의 이름은 최대 16자의 영문자와 숫자로 구성된 문자열을 입력합니다. 첫 글자는 반드시 영문자여야 합니다.</li> <li><b>필터/필터 그룹</b> 드롭다운 목록을 클릭한 후 인터페이스 항목에서 선택한 인터페이스에 적용할 필터나 필터 그룹을 선택합니다. 정책에는 하나의 필터나 필터 그룹을 지정할 수 있습니다.</li> <li><b>인터페이스</b> 드롭다운 목록을 클릭한 후 방화벽 정책을 적용할 인터페이스를 선택합니다. 이 때, 인터페이스는 WEBFRONT-K에 설정된 VLAN 인터페이스입니다.</li> <li><b>상태</b> 드롭다운 목록을 클릭한 후, 방화벽 정책의 사용 유무를 지정합니다. 설정한 방화벽 정책을 사용하려면 활성화, 사용하지 않으려면 비활성화를 선택합니다. (기본값: 활성화)</li> </ul>

## 제9장 사용자 관리

이 장에서는 WEBFRONT-K에 등록된 애플리케이션을 관리할 수 있는 사용자를 관리하는 방법에 대해 설명합니다. 사용자 관리 기능을 통해 새로운 사용자의 계정을 추가하거나 계정을 삭제할 수 있습니다. 또한 로그인 실패 횟수를 조정하거나 중복 로그인의 허용 여부를 설정할 수 있습니다.

이 장은 다음 내용으로 구성됩니다.

- 사용자 관리 개요
- 사용자 추가하기
- 현재 로그인 실패 횟수 변경하기
- 계정 관리 설정하기
- 중복 로그인 허용 설정하기
- 기본 사용자 설정하기
- RADIUS 설정하기
- 사용자 접근 IP 리스트 관리



# 사용자 관리 개요

WEBFRONT-K의 사용자에는 통합 관리자, 사이트 관리자, 애플리케이션 관리자, 모니터 관리자의 4가지 종류가 있습니다. WEBFRONT-K로 로그인할 때 사용한 사용자 계정의 종류에 따라 사용할 수 있는 WEBFRONT-K의 기능이 달라집니다. 다음은 WEBFRONT-K 사용자의 종류와 권한에 대한 설명입니다.

## 통합 관리자(Super User)

통합 관리자는 WEBFRONT-K의 모든 기능을 사용할 수 있는 사용자입니다. 사용자 관리는 물론, 애플리케이션과 시스템을 관리할 수 있고, 등록된 모든 애플리케이션의 관리자 역할을 수행할 수 있습니다. WEBFRONT-K를 처음 설치한 경우에는 유지보수 라이선스 등록 후 통합 관리자 계정을 생성해야 하며, 해당 계정으로 로그인한 후 사이트 관리자와 애플리케이션 관리자 등을 추가해야 합니다.

통합 관리자는 각 사용자 계정마다 최대 로그인 실패 횟수를 지정할 수 있고 현재 로그인 실패 횟수를 볼 수 있습니다.

## 사이트 관리자(Site Administrator)

사이트 관리자는 WEBFRONT-K의 시스템 관리 기능을 사용할 수 있고, 모든 애플리케이션의 애플리케이션 관리자 역할을 할 수 있습니다. 통합 관리자의 기능 중에서 사용자 관리 기능은 사이트 관리자가 수행할 수 없습니다. 따라서, 사이트 관리자로 로그인하면, WEBFRONT-K의 사용자 관리 기능을 제외한 모든 System 메뉴와 모든 Application 메뉴를 사용할 수 있습니다.

## 애플리케이션 관리자(Application Administrator)

애플리케이션 관리자는 특정 애플리케이션의 설정을 조회하거나 변경할 수 있는 사용자입니다. 애플리케이션 관리자는 '관리자' 권한과 '모니터' 권한 중 하나의 권한을 부여 받을 수 있는데 부여 받은 권한에 따라 사용할 수 있는 메뉴가 달라집니다.

- 관리자 권한  
'관리자' 권한을 부여 받은 애플리케이션 관리자는 WEBFRONT-K의 Application 메뉴를 사용할 수 있습니다.
- 모니터 권한  
'모니터' 권한을 부여 받은 애플리케이션 관리자는 Application 메뉴 중에서 로그, 모니터링 메뉴만 사용할 수 있습니다.

애플리케이션 관리자로 로그인하면 System 메뉴를 사용하거나 자신이 관리할 수 없는 애플리케이션을 선택할 수 없습니다. WEBFRONT-K는 애플리케이션 관리자가 여러 애플리케이션을 관리하도록 설정할 수 있으므로 각 애플리케이션마다 애플리케이션 관리자를 지정하지 않아도 됩니다. 그리고, 한 사용자가 특정 애플리케이션의 관리자이면서 동시에 다른 애플리케이션의 모니터가 될 수 있습니다.

## 모니터 관리자(Monitor Administrator)

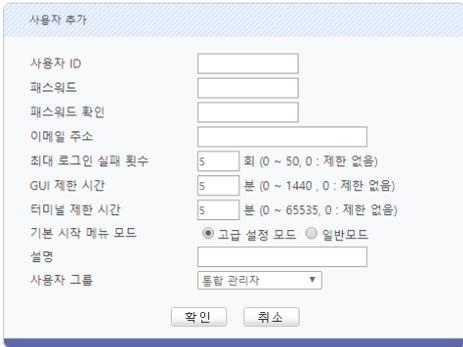
모니터 관리자는 시스템의 정보만 볼 수 있는 사용자로, System 메뉴 중에서 시스템 정보, 포트 모니터링 메뉴만 사용할 수 있고 Application 메뉴는 사용할 수 없습니다.



**참고:** 이 설명서에서 다루는 WEBFRONT-K의 System 메뉴는 통합 관리자와 사이트 관리자, 모니터 관리자만 사용할 수 있습니다. 애플리케이션 관리자가 사용할 수 있는 Application 메뉴에 관한 설명은 이 설명서와 함께 제공되는 WEBFRONT-K 애플리케이션 구성 설명서에 설명되어 있습니다.

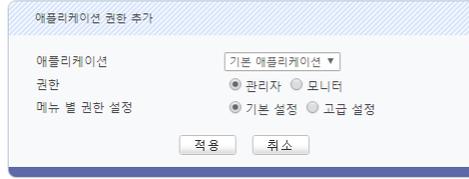
# 사용자 추가하기

새로운 사용자를 추가하려면 다음 과정을 수행합니다. 최대 256 개의 사용자 계정을 추가할 수 있습니다.

순서	설정 과정
1	<b>System - 사용자 관리</b> 메뉴를 클릭합니다.
2	<사용자 리스트>의 [변경] - [추가] 버튼을 클릭합니다. <사용자 추가> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [확인] 버튼을 클릭합니다. <div style="text-align: center;">  </div>
3	<p>아래 항목 중에서 설명 항목을 제외한 나머지 항목들은 반드시 값을 설정해야 하는 필수 항목입니다.</p> <ul style="list-style-type: none"> <li> <b>• 사용자 ID</b>                      사용자의 로그인 이름을 입력합니다. 알파벳이나 숫자, 기호를 조합한 5~16 자의 문자열을 입력합니다. 알파벳은 대소문자를 구분하여 사용해야 합니다.                 </li> <li> <b>• 패스워드</b>                      사용자의 로그인 암호를 입력합니다. 알파벳 대문자, 소문자, 숫자, 특수문자 중 3가지 이상의 조합으로 9~20자의 문자열을 지정합니다.                 </li> <li> <b>• 패스워드 확인</b>                      로그인 암호를 다시 한번 입력합니다.                 </li> <li> <b>• 이메일 주소</b>                      사용자의 이메일 주소를 입력합니다.                 </li> <li> <b>• 최대 로그인 실패 횟수</b>                      허용할 로그인 실패 횟수를 지정합니다. 이 횟수만큼 연속적으로 로그인에 실패한 이후에는 로그인을 시도할 때마다 "로그인 실패 횟수가 한도를 초과하였습니다"라는 팝업 창이 나타납니다. 이런 경우에는 통합 관리자가 현재 로그인 실패 횟수를 최대 로그인 실패 횟수보다 작은 값으로 변경해주어야만 로그인을 할 수 있습니다. 이 항목을 '0'으로 지정하면 로그인 실패 횟수에 상관 없이 계속 로그인을 시도할 수 있습니다. (설정 범위: 1 ~ 1440, 기본값: 10회)                 </li> <li> <b>• GUI 제한 시간</b>                      Web Manager 화면에서 사용자 입력이 없어도 로그인을 유지 시킬 시간 간격을 입력합니다. 이 시간이 경과할 때까지 사용자 입력이 없으면 자동으로 Web Manager에서 로그아웃됩니다.'0'을 입력하면 사용자 입력이 없어도 자동으로 로그아웃되지 않습니다. (설정 범위: 1 ~ 1440, 기본값: 5분)                 </li> <li> <b>• 터미널 제한 시간</b>                      콘솔 화면에서 사용자 입력이 없어도 로그인을 유지 시킬 시간 간격을 입력합니다. 이 시간이 경과할 때까지 사용자 입력이 없으면 자동으로 콘솔에서 로그아웃됩니다.'0'을 입력하면 사용자 입력이 없어도 자동으로 로그아웃되지 않습니다. (설정 범위: 1 ~ 65535, 기본값: 5분)                 </li> <li> <b>• 기본 시작 메뉴 모드</b>                      사용자로 로그인했을 때 나타나는 기본 설정 화면의 종류를 선택합니다.                     <ul style="list-style-type: none"> <li>- <b>고급 설정 모드:</b> 모든 메뉴가 나타나는 모드(기본 설정)</li> <li>- <b>일반 모드:</b> 모니터링 메뉴만 나타나는 모드</li> </ul> </li> <li> <b>• 설명</b>                      사용자의 역할 등 사용자에게 대한 간단한 정보를 입력합니다. 알파벳, 숫자, 한글, 특수 문자 모두 사용할 수 있고 최대 128자까지 입력할 수 있습니다.                 </li> <li> <b>• 사용자 그룹</b>                      드롭다운 목록을 클릭한 후 사용자의 종류를 선택합니다.                     <ul style="list-style-type: none"> <li>- <b>통합 관리자:</b> 모든 메뉴 사용 가능한 사용자(기본 설정)</li> <li>- <b>사이트 관리자:</b> 사용자 관리를 제외한 모든 메뉴 사용 가능한 사용자</li> <li>- <b>애플리케이션 관리자:</b> 지정한 애플리케이션만을 관리할 수 있는 사용자. 이 항목을 선택하면 사용자가 관</li> </ul> </li> </ul>

리할 애플리케이션을 지정할 수 있는 애플리케이션 목록이 나타납니다.

- ❶ 애플리케이션 목록의 [추가] 버튼을 누릅니다.
- ❷ <애플리케이션 권한 추가> 팝업 창에서 다음 두 항목을 설정한 후 [적용] 버튼을 클릭합니다.

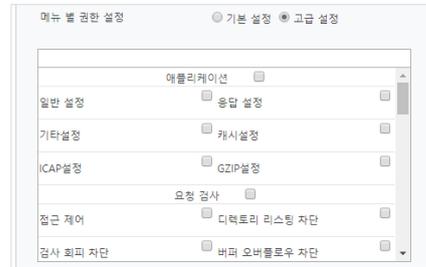


**애플리케이션** 드롭다운 목록(현재 추가된 애플리케이션의 목록)을 클릭한 후 사용자가 관리할 애플리케이션을 선택합니다.

**권한** 사용자의 권한을 지정합니다. 애플리케이션 설정 및 조회를 모두 허용하려면 관리자, 정보 조회만 허용하려면 모니터를 선택합니다.

**메뉴 별 권한 설정** 권한을 관리자로 선택한 경우 설정할 수 있는 Application 메뉴를 선택합니다.

- 기본 설정: 사용자가 모든 Application 메뉴를 설정할 수 있습니다.
- 고급 설정: 고급 설정을 선택하면 다음과 같은 선택 화면이 나타나며 설정 가능한 Application 메뉴를 지정할 수 있습니다.



- ❸ 지정한 애플리케이션이 목록에 추가됩니다. 사용자가 여러 개의 애플리케이션을 관리하는 경우에는 애플리케이션 개수만큼 [추가] 버튼을 클릭하여 애플리케이션을 지정해주면 됩니다.

- **모니터 관리자:** 시스템의 정보만 볼 수 있는 사용자. System 메뉴 중 시스템 정보, 포트 모니터링 메뉴만 사용가능

4 사용자를 모두 추가한 후에는 [적용] 버튼을 눌러 추가한 사용자 정보를 저장하고 시스템에 적용합니다.



**참고: 사용자 삭제 및 수정하기**

추가한 사용자를 삭제하려면 사용자 목록에서 삭제할 사용자(들)를 클릭한 후 [삭제] 버튼을 클릭합니다. 그리고, [적용] 버튼을 누릅니다. 사용자를 수정하려면 사용자 목록에서 수정할 사용자를 클릭한 후 [수정] 버튼을 클릭합니다. 그리고, 원하는 항목의 값을 다시 입력한 후 [적용] 버튼을 누릅니다.



**참고: 상세 사용자 정보 보기**

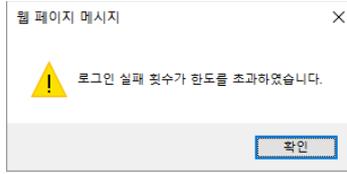
통합 관리자는 사용자 리스트에서 [상세보기] 버튼을 클릭하면 사용자에 대한 상세 정보를 보여주는 팝업 창이 나타납니다.

□ 사용자 리스트						변경
사용자 ID	그룹	현재 로그인 실패 횟수	최대 로그인 실패 횟수	설명	상세 보기	
wfadmin	통합 관리자	0	5	Default User	상세보기	



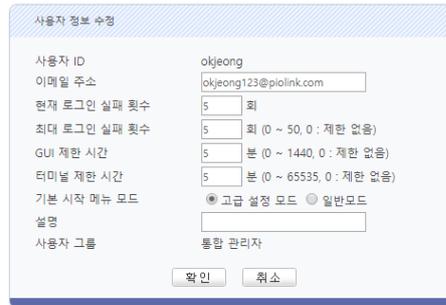
## 현재 로그인 실패 횟수 변경하기

최대 로그인 횟수가 설정되어 있는 사용자는 이 횟수만큼 연속적으로 로그인에 실패하게 되면 이후부터 로그인을 시도 할 때마다 다음과 같은 팝업 창이 나타납니다.



이와 같이 로그인 실패 횟수가 한도를 초과한 사용자가 다시 로그인을 하려면 통합 관리자가 다음과 같은 방법을 통해 해당 사용자의 현재 로그인 실패 횟수를 최대 로그인 실패 횟수보다 작은 값으로 변경해주어야 합니다.

순서	설정 과정
1	<b>System - 사용자 관리</b> 메뉴를 클릭합니다.
2	<사용자 리스트>의 [변경] 버튼을 클릭합니다.
3	<사용자 리스트 수정> 화면에서 현재 로그인 실패 횟수를 변경할 사용자를 선택한 후 [수정] 버튼을 클릭합니다.
4	<사용자 정보 수정> 팝업 창에서 현재 로그인 실패 횟수 항목을 최대 로그인 실패 횟수보다 작은 값으로 변경한 후 [확인] 버튼을 클릭합니다.
5	<사용자 리스트 수정> 화면으로 돌아오면 현재 로그인 실패 횟수가 바르게 변경되었는지 확인한 후 [적용] 버튼을 클릭합니다.



# 계정 관리 설정하기

사용자 계정을 생성한 이후, 장비 접속 및 패스워드 관리 정책을 설정할 수 있습니다. 다음은 계정 관리를 설정하는 과정입니다.

순서	설정 과정
1	<b>System - 사용자 관리</b> 메뉴를 클릭합니다.
2	<계정 관리 설정>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;계정 관리 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 <b>[적용]</b> 버튼을 클릭합니다.</p> <div data-bbox="576 501 1115 703" data-label="Image"> </div> <ul style="list-style-type: none"> <li> <b>최근 사용 패스워드 제한</b>                      최근 사용한 패스워드의 제한 여부를 지정합니다. 기능을 활성화하면 최근 사용한 4개의 패스워드를 사용자 패스워드로 설정할 수 없습니다. (기본값: 비활성화)                 </li> <li> <b>미 사용 계정 만료</b>                      지정한 기간 동안 로그인하지 않은 계정에 대해 Web Manager와 콘솔 접속의 차단 여부를 지정합니다. (설정 범위: 0 ~ 365(일), 기본값: 0)                 </li> <li> <b>패스워드 변경 주기 확인</b>                      지정한 기간 동안 패스워드를 변경하지 않은 사용자가 Web Manager 로그인 시, 알림창 출력 여부를 지정합니다. (설정 범위: 0 ~ 365(일), 기본값: 0)                 </li> <li> <b>최대 로그인 실패 횟수 초과 시 자동 잠금 해제</b>                      최대 로그인 실패 횟수를 초과하여 계정이 잠긴 경우, 지정한 시간 이후에 자동으로 잠금을 해제할 지 여부를 지정합니다. (설정 범위: 0 ~ 1440(분), 기본값: 0)                 </li> </ul>

# 중복 로그인 허용 설정하기

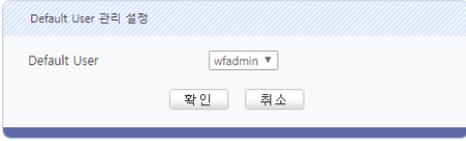
다음은 사용자 계정의 중복 로그인 허용 여부를 설정하는 과정입니다.

순서	설정 과정
1	System - 사용자 관리 메뉴를 클릭합니다.
2	<중복 로그인 허용 설정>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;중복 로그인 허용 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  <p>중복 로그인 허용 설정</p> <p>계정별 중복 로그인      <input checked="" type="radio"/> 허용   <input type="radio"/> 차단</p> <p>설정 변경 사용자의 중복 로그인      <input checked="" type="radio"/> 허용   <input type="radio"/> 차단</p> <p><input type="button" value="적용"/>   <input type="button" value="리셋"/>   <input type="button" value="취소"/></p> </div> <ul style="list-style-type: none"> <li> <b>계정별 중복 로그인</b>                      동일한 계정의 중복 로그인 여부를 지정합니다. (기본값: 허용)                 </li> <li>  <b>참고:</b> 모니터 관리자 계정일 경우, 설정과 관계 없이 중복 로그인을 허용합니다.                 </li> <li> <b>설정 변경 사용자의 중복 로그인</b>                      설정 변경 권한이 있는 사용자의 중복 로그인 여부를 지정합니다. '허용'으로 설정할 경우, 설정 변경 권한이 있는 2명 이상의 관리자가 동시에 접속할 수 있고, '차단'으로 설정할 경우 1명만 접속할 수 있습니다. (기본값: 허용)                 </li> </ul>

# 기본 사용자 설정하기

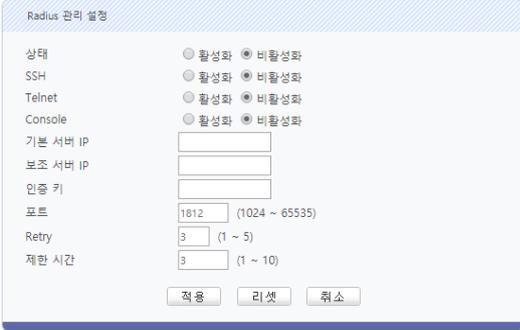
WEBFRONT-K에는 기본적으로 ID가 **wfadmin**인 통합관리자 그룹의 기본 사용자 계정이 등록되어 있습니다. 기본 사용자는 통합관리자 그룹에 속하는 계정에 한해 기본 사용자 계정을 변경할 수 있습니다.

기본 사용자를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 사용자 관리</b> 메뉴를 클릭합니다.
2	< <b>Default User 관리 설정</b> >의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;<b>Default User 관리 설정</b>&gt; 팝업 창의 드롭다운 목록에서 기본 사용자를 선택한 후 <b>[확인]</b> 버튼을 클릭합니다.</p> 
	 <b>참고:</b> Default User 변경은 현재 로그인한 계정이 '통합 관리자'이고 'Default User'인 경우에만 실행할 수 있습니다.

# RADIUS 설정하기

WEBFRONT-K는 RADIUS(Remote Authentication Dial In User Service) 서버를 이용하여 웹 또는 콘솔 등을 통한 외부 접속에 대해 사용자 인증 기능을 제공합니다. 사용자는 RADIUS 서버와 WEBFRONT-K간의 통신 시 사용할 TCP 포트를 지정하고, 인증에 사용되는 인증 키 값을 설정합니다.

순서	설정 과정
1	<b>System - 사용자 관리</b> 메뉴를 클릭합니다.
2	< <b>Radius 관리 설정</b> >의 [ <b>변경</b> ] 버튼을 클릭합니다.
3	<p>&lt;<b>Radius 관리 설정</b>&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [<b>적용</b>] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>상태</b> RADIUS 기능의 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• <b>SSH</b> SSH를 통해 WEBFRONT-K에 접속 시 RADIUS 서버 인증 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• <b>Telnet</b> Telnet을 통해 WEBFRONT-K에 접속 시 RADIUS 서버 인증 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• <b>Console</b> 콘솔을 통해 WEBFRONT-K에 접속 시 RADIUS 서버 인증 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• <b>기본 서버 IP</b> 기본 RADIUS 서버의 IP주소를 설정합니다.</li> <li>• <b>보조 서버 IP</b> 기본 RADIUS 서버가 정상적으로 동작하지 않는 경우에 사용되는 보조 RADIUS 서버 IP주소를 설정합니다.</li> <li>• <b>인증 키</b> RADIUS 서버와 PAS-K와의 인증에 사용되는 인증 키 값을 설정합니다.</li> <li>• <b>포트</b> RADIUS 서버와 PAS-K간의 통신 시 사용할 TCP 포트를 설정합니다. (설정 범위: 1024 ~ 65535, 기본값: 1812)</li> <li>• <b>Retry</b> RADIUS 서버의 응답이 없을 때 RADIUS 서버와 접속을 위해 다시 시도할 접속 횟수를 설정합니다 (설정 범위: 1 ~ 5회, 기본값: 3)</li> <li>• <b>제한 시간</b> RADIUS 서버 응답 타임아웃을 설정합니다. (설정 범위: 1~10초, 기본값: 3)</li> </ul>

# 사용자 접근 IP 리스트 관리

사용자 접근 IP 리스트를 통해 특정 IP 주소만 WEBFRONT-K의 Web Manager에 접속할 수 있도록 설정할 수 있습니다. 사용자 접근 IP 리스트를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 사용자 관리</b> 메뉴를 클릭합니다.
2	<사용자 접근 IP 리스트>의 <b>[변경]</b> - <b>[추가]</b> 버튼을 클릭합니다.
3	<p>&lt;접근 IP 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 <b>[확인]</b> 버튼을 클릭합니다.</p> <div data-bbox="598 497 1093 678" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• <b>아이피</b> Web Manager 접근을 허용할 IP 주소를 1.1.1.1과 같은 형식으로 입력합니다.</li> <li>• <b>설명</b> 애플리케이션에 대한 설명을 입력합니다. 한글과 알파벳, 숫자, 특수 문자 등을 사용하여 최대 128자까지 입력할 수 있습니다. (선택 설정)</li> </ul>
4	<p><b>상태</b> 항목에서 사용자 접근 IP 리스트의 활성화 여부를 지정합니다.</p> <ul style="list-style-type: none"> <li>• <b>활성화</b> 등록된 IP 주소에서만 접근할 수 있습니다.</li> <li>• <b>비활성화</b> 모든 IP 주소에서 접근할 수 있습니다. (기본값)</li> </ul>
5	설정이 완료되면 <b>[적용]</b> 버튼을 클릭합니다.

# 제10장 일반 설정

이 장에서는 WEBFRONT-K를 사용하기 위해 확인하고 설정해야 할 가장 기본적인 설정 작업에 대해 알아봅니다.

이 장은 다음 내용으로 구성됩니다.

- 설정 관리
- 기술 지원 도우미
- 서버 장애 감시
- 시스템 감시
- SNMP
- 라이선스 관리
- 국가별 IP
- PLOS 관리
- 시간 관리
- DNS 관리
- 리포터 설정
- E-mail 알람
- 무결성 검사
- 환경 변수
- 통계 기간 설정
- 시스템 관리 설정
- 호스트 이름 설정
- 시스템 재시작



# 설정 관리

이 장에서는 WEBFRONT-K의 설정(configuration)을 관리하는 방법에 대해 알아봅니다.

## 개요

WEBFRONT-K의 설정은 설정 저장 공간(이하, SSD)에 저장됩니다. SSD는 3개의 저장 공간(저장 공간 #1, #2, #3)으로 분리되어 각각 다른 설정을 저장할 수 있습니다. WEBFRONT-K는 부팅 시 세 저장 공간에 저장된 설정 중 하나를 사용하여 부팅하는 데, 기본적으로 저장 공간 #1의 설정을 사용합니다. 부팅 시 사용할 설정은 사용자가 변경할 수 있습니다. WEBFRONT-K는 각 저장 공간별로 설정 저장, 동기화, 업로드, 다운로드, 적용, 삭제 기능을 지원합니다.

### 설정 저장

WEBFRONT-K는 부팅 시 SSD에 저장된 설정을 SDRAM으로 로딩합니다. SDRAM에 로딩된 설정은 사용자가 WEBFRONT-K의 설정을 바꿀 때마다 변경됩니다. WEBFRONT-K를 다시 시작한 후에도 계속 변경된 설정을 사용하기 위해서는 SDRAM의 설정을 SSD에 저장해야 합니다. WEBFRONT-K는 SDRAM의 설정을 사용자가 지정한 SSD의 영역에 저장하는 기능을 제공합니다.

### 설정 다운로드/업로드

WEBFRONT-K는 SSD에 저장되어 있는 설정이나 SDRAM의 설정을 다운로드하여 사용자 PC에 파일로 저장할 수 있습니다. 그리고, 사용자 PC에 저장된 설정 파일을 SSD의 특정 저장 공간으로 업로드할 수 있습니다. 이러한 설정 다운로드/업로드 기능을 사용하면, 설정을 백업해두었다가 WEBFRONT-K의 설정에 문제가 생기거나 혹은 이전 설정으로 되돌려야 하는 경우에 유용하게 사용할 수 있습니다. 여러 대의 WEBFRONT-K를 동일하게 설정해야 하는 경우에도 이 기능을 활용하면, 모든 WEBFRONT-K를 설정할 필요 없이 하나의 WEBFRONT-K만 설정하고 나머지는 이 WEBFRONT-K의 설정 파일을 업로드하면 됩니다.

### 기본 설정 복구

다음은 WEBFRONT-K의 출하시 기본 설정입니다. WEBFRONT-K를 사용하거나 설정을 변경하는 중에도 언제든지 이러한 출하시의 기본 설정으로 되돌릴 수 있습니다.

항목	기본 설정			
관리용 IP 주소	192.168.100.1/24			
호스트 이름	WEBFRONT-K			
포트	관리자 상태	속도와 전송 모드	MDI/MDI-X	흐름 제어
	활성화	Auto	MDI-X	OFF
사용자	없음			
NTP 클라이언트	상태	간격		
	활성화	3600초		
리포터	상태	리포터 설정		
	비활성화	없음		
프록시 ARP	비활성화			
애플리케이션	기본 애플리케이션			
로그	레벨	시스로그 서버		
	Notice	없음		

## 설정 동기화

WEBFRONT-K는 다른 WEBFRONT-K의 설정을 가져올 수 있는 설정 동기화 기능을 제공합니다. 설정 동기화 기능은 지정된 WEBFRONT-K의 설정 중 네트워크 설정(링크 싱크 제외)과 시스템 감시를 제외한 모든 설정을 복사하여 SSD의 특정 저장 공간에 저장합니다. 여러 WEBFRONT-K의 웹 보안 기능을 동일하게 설정하는 경우에는 하나의 WEBFRONT-K만 설정한 후에 설정 동기화 기능을 사용하여 설정을 가져오기만 하면 됩니다. 설정 동기화 기능은 설치된 PLOS 버전이 동일한 WEBFRONT-K간에만 사용할 수 있습니다.

## 설정 복사

WEBFRONT-K는 특정 애플리케이션의 설정을 다른 애플리케이션으로 복사할 수 있는 설정 복사 기능을 제공합니다. Application 메뉴나 Application 메뉴 화면에서 설정을 복사하고자 하는 기능이나 항목을 선택하고 설정을 복사할 대상 애플리케이션(들)을 지정하면 해당 애플리케이션의 설정이 선택한 기능이나 항목의 설정으로 변경됩니다(overwrite). 설정 복사 기능은 애플리케이션의 자체 정보인 애플리케이션 일반 설정과 이 정보와 관련되어 있는 SSL 일반 설정, 애플리케이션 기타 설정의 애플리케이션 프로토콜 정보, 쿼리스트링 차단 기능(버퍼 오버플로우 차단, SQL 삽입 차단, 스크립트 삽입 차단)은 복사하지 않습니다.

다음은 설정 복사 기능을 효과적으로 활용할 수 있는 경우입니다.

- 애플리케이션에 적용한 시그니처나 설정이 매우 효과적으로 트래픽을 차단하여 다른 애플리케이션에도 확대 적용하려는 경우
- 새로 생성한 애플리케이션에 이미 생성된 애플리케이션의 설정을 그대로 사용하려는 경우

## 설정 자동 백업

WEBFRONT-K는 별도의 서버에 현재 설정을 자동으로 저장하는 설정 자동 백업 기능을 제공합니다. 설정 자동 백업 기능은 WEBFRONT-K의 현재 설정 파일을 지정한 백업 주기마다 백업 서버로 전송합니다. 설정 자동 백업 기능을 사용하기 위해서는 FTP서비스를 제공하는 서버가 필요합니다.

## 설정 적용

WEBFRONT-K는 저장 공간에 저장된 설정을 WEBFRONT-K에 바로 적용하는 기능을 제공합니다. 설정을 적용하고 나면 Web Manager 화면을 초기화하기 위해 Web Manager에서 로그아웃됩니다. 따라서, 설정 적용이 완료되면 로그인 화면이 나타납니다.

## 설정 관리 화면

System 메뉴의 일반설정 - 설정 관리 메뉴를 클릭하면 다음과 같은 설정 관리 화면이 나타납니다.

The screenshot shows a web interface for managing settings. It includes sections for:

- 현재 설정 다운로드** (Download current settings): A button to download system settings to the local drive.
- 설정 자동 백업** (Automatic settings backup): A button to back up current settings.
- 설정 저장 리스트** (Settings save list): A table listing saved settings with columns for '저장공간' (Storage space), '상태' (Status), '저장 일시' (Save time), and '설명' (Description). The first entry is for 'test' settings saved on 2019/05/31. Below the table are buttons for '전체 설정 동기화' (Sync all settings), '다시저장' (Save again), '업로드' (Upload), '다운로드' (Download), '다음부팅사용' (Use on next boot), '설정적용' (Apply settings), and '삭제' (Delete).
- 실시간 동기화** (Real-time sync): A button to sync settings in real-time.
- 시스템 초기화** (System reset): A button to reset all settings to factory defaults.

화면의 각 부분에서 수행할 수 있는 작업은 다음과 같습니다.

- **현재 설정 다운로드**

현재 WEBFRONT-K의 설정을 다운로드하여 사용자의 PC에 파일로 저장합니다.

- **설정 자동 백업**

현재 WEBFRONT-K의 설정을 지정한 주기마다 백업 서버로 전송합니다.

- **설정 저장 리스트**

플래시의 각 저장 공간에 저장되어 있는 설정에 대한 정보를 보여줍니다. 다음은 각 항목과 버튼에 대한 설명입니다.

항목	설명	
상태	저장 공간에 저장된 설정이 사용된 정보. 설정이 저장된 후 한번도 사용되지 않으면 아무런 정보도 표시되지 않습니다.	
저장 일시	저장 공간에 설정이 마지막으로 저장된 날짜와 시간	
설명	저장 공간에 설정을 저장할 때 사용자가 입력한 설명	
버튼	전체 설정 동기화	다른 WEBFRONT-K의 설정을 가져와서 저장 공간에 저장합니다.
	다시 저장	현재 WEBFRONT-K의 설정을 저장 공간에 저장합니다(이전에 저장된 설정은 모두 삭제됩니다).
	업로드	사용자 PC에 저장된 설정 파일을 업로드하여 저장 공간에 저장합니다.
	다운로드	저장 공간에 저장된 설정을 사용자 PC로 다운로드하여 파일로 저장합니다.
	다음 부팅 시 사용	다음 부팅 시 저장 공간에 저장된 설정을 사용하도록 설정합니다.
	설정 적용	저장 공간에 저장된 설정을 WEBFRONT-K에 바로 적용합니다. 설정을 적용하고 나면 Web Manager 화면을 초기화하기 위해 Web Manager에서 로그아웃됩니다. 따라서, 설정 적용이 완료되면 로그인 화면이 나타납니다.
	삭제	저장 공간의 설정을 삭제합니다.



주의: WEBFRONT-K가 동작하는 중에 [설정 적용] 버튼을 클릭하면 새로운 설정이 바로 적용되기 때문에 트래픽의 양이나 동작 상태 등에 따라 WEBFRONT-K가 오동작할 수도 있고 때로 리부팅될 수도 있습니다. 그러므로, WEBFRONT-K를 테스트하거나 매우 적은 양의 트래픽이 처리되는 중일 때에만 [설정 적용] 버튼을 사용하도록 하고 정상적으로 WEBFRONT-K를 운영하는 중에는 사용하지 않도록 합니다.

• **실시간 동기화**

WEBFRONT-K는 다른 WEBFRONT-K의 설정을 실시간으로 가져올 수 있는 실시간 설정 동기화 기능을 제공합니다. 실시간으로 동기화할 메뉴를 설정하면 해당 설정을 복사하여 SSD의 특정 저장 공간에 저장합니다. 실시간 동기화 기능은 설치된 PLOS 버전이 동일한 WEBFRONT-K간에만 사용할 수 있습니다.

• **시스템 초기화**

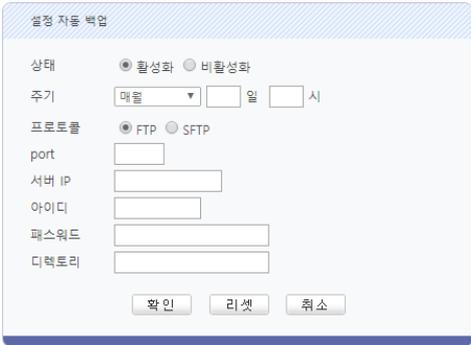
WEBFRONT-K의 설정을 삭제하고 출하시 기본 설정으로 되돌립니다.



참고: 시스템을 초기화해도 기존에 입력했던 라이선스 정보는 그대로 유지됩니다.

## 설정 자동 백업 설정하기

WEBFRONT-K의 설정 자동 백업 기능을 사용하기 위한 방법은 다음과 같습니다. 설정 자동 백업은 최대 32개까지 설정할 수 있습니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<설정 자동 백업>의 [변경] - [추가] 버튼을 클릭합니다. <설정 자동 백업> 팝업 창에서 다음 설명을 참고하여 각 항목들의 값을 설정한 후 [확인]버튼을 클릭합니다.
3	<div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>상태</b> 자동 백업 설정을 사용할 것인지 여부를 지정합니다. (기본값: 활성화)</li> <li>• <b>주기</b> 자동 백업을 수행할 주기와 시간을 지정합니다. 기본 주기는 '매월'입니다. 일자는 1~31, 시간은 1~24 중에서 입력할 수 있습니다.</li> <li>• <b>프로토콜</b> 자동 백업 시 설정 파일을 저장할 백업 서버와의 통신 프로토콜을 선택합니다. (기본값: FTP)</li> <li>• <b>포트</b> 백업 서버의 포트번호를 입력합니다. (설정 범위: 1~65535)</li> <li>• <b>서버 IP</b> 백업 서버의 IP 주소를 입력합니다. 'A.B.C.D' 형식으로 입력합니다.</li> <li>• <b>아이디</b> 백업 서버의 FTP/SFTP 서비스로 로그인할 수 있는 ID를 입력합니다. 1~12자까지 입력할 수 있습니다.</li> <li>• <b>패스워드</b> 백업 서버의 FTP/SFTP 서비스로 로그인할 수 있는 패스워드를 입력합니다. 1~31자까지 입력할 수 있습니다.</li> <li>• <b>디렉토리</b> 설정 파일이 저장될 경로를 입력합니다. FTP/SFTP 서비스의 루트 디렉토리를 기준으로 입력합니다. 첫 문자는 반드시 '/'로 시작해야 합니다. 1~1024자까지 입력할 수 있습니다.</li> </ul> <p> 주의: 설정을 백업할 서버는 반드시 FTP/SFTP 서비스를 제공해야 합니다.</p>
4	설정 자동 백업 설정이 완료되었으면 [적용] 버튼을 클릭합니다.



참고: 설정 파일은 WF-YYYYMMDD-hhmm-서버IP.conf의 형식으로 저장되며 백업된 설정 파일은 이 장의 [설정 다운로드/업로드하기] 절을 참고하여 WEBFRONT-K에 적용할 수 있습니다.

## 현재 설정 저장하기(SDRAM → SSD)

다음은 현재 WEBFRONT-K의 설정을 SSD의 저장 공간에 저장하는 방법입니다. SSD에 설정을 저장하면 부팅 후에도 설정이 계속 유지됩니다.

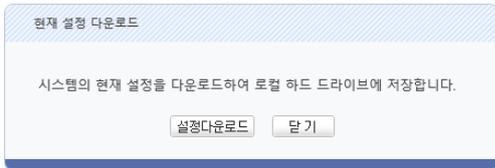
순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<설정 저장 리스트> 부분에서 현재 WEBFRONT-K의 설정을 저장할 SSD의 저장 공간에 있는 <b>[다시저장]</b> 버튼을 클릭합니다.  참고: 저장공간에 설정을 처음으로 저장하는 경우에는 <b>[다시저장]</b> 버튼 대신 <b>[저장]</b> 버튼을 클릭합니다.
3	저장 공간에 저장된 설정을 삭제하고 현재 설정을 저장할 것인지를 확인하는 팝업 창이 나타나면 <b>[확인]</b> 버튼을 클릭합니다.
4	<현재 설정 저장> 팝업 창에서 저장하려는 설정에 대한 간략한 설명을 입력한 후 <b>[적용]</b> 버튼을 클릭합니다. 설명을 입력할 필요가 없는 경우에는 <b>[적용]</b> 버튼만 클릭합니다.

## 설정 다운로드/업로드하기

이 절에서는 현재 WEBFRONT-K의 설정이나 SSD에 저장된 설정을 사용자 PC로 다운로드하는 방법과 사용자 PC에 다운로드했던 설정을 SSD로 업로드하는 방법에 대해 살펴봅니다.

### 현재 설정 다운로드하기

다음은 WEBFRONT-K의 현재 설정을 다운로드하여 사용자 PC에 저장하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<현재 설정 다운로드>의 <b>[설정다운로드]</b> 버튼을 클릭합니다.
3	<현재 설정 다운로드> 팝업 창에서 <b>[설정다운로드]</b> 버튼을 클릭합니다.  현재 설정 다운로드 시스템의 현재 설정을 다운로드하여 로컬 하드 드라이브에 저장합니다. 설정다운로드 닫기
4	파일 다운로드 팝업 창에서 <b>[저장]</b> 버튼을 클릭합니다.
5	다른 이름으로 저장하려면 <b>[다른 이름으로 저장]</b> 버튼을 클릭합니다. 설정 파일을 저장할 폴더와 파일 이름을 지정한 후 <b>[저장]</b> 버튼을 클릭합니다. 설정 파일 이름은 기본적으로 WEBFRONT-K-날짜.conf로 지정됩니다.

### 설정 다운로드하기

다음은 SSD에 저장된 설정을 다운로드하여 사용자 PC에 저장하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<설정 저장 리스트> 부분에서 다운로드할 설정이 저장된 SSD 저장 공간의 <b>[다운로드]</b> 버튼을 클릭합니다.
3	파일 다운로드 팝업 창이 나타나면 <b>[저장]</b> 버튼을 클릭합니다.
4	다른 이름으로 저장하려면 <b>[다른 이름으로 저장]</b> 버튼을 클릭합니다. 설정 파일을 저장할 폴더와 파일 이름을 지정한 후 <b>[저장]</b> 버튼을 클릭합니다. 설정 파일 이름은 기본적으로 WAF_호스트 이름_slot저장 공간의 번호_날짜.conf로 지정됩니다.

## 설정 업로드하기

다음은 사용자 PC에 저장된 설정 파일을 WEBFRONT-K의 SSD로 업로드하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<설정 저장 리스트> 부분에서 설정을 업로드할 SSD 저장 공간에 있는 <b>[업로드]</b> 버튼을 클릭합니다.
3	<설정파일 업로드> 팝업 창에서 <b>[찾아보기]</b> 버튼을 클릭합니다.
4	<파일 선택> 팝업 창에서 업로드할 설정 파일이 저장되어 있는 폴더와 파일을 선택하고 <b>[열기]</b> 버튼을 클릭합니다.
5	<설정파일 업로드> 팝업 창에서 저장공간 설명 항목에 업로드할 설정에 대한 간략한 설명을 입력하고 <b>[적용]</b> 버튼을 클릭합니다. 설명을 입력할 필요가 없는 경우에는 <b>[적용]</b> 버튼만 클릭합니다.

## 설정 삭제하기

이 절에서는 WEBFRONT-K의 설정을 포함하여 SSD의 모든 설정을 삭제하는 방법과 SSD에 저장된 설정을 삭제하는 방법에 대해 살펴봅니다.

### 모든 설정 삭제하기

다음은 WEBFRONT-K의 모든 설정(SSD에 저장된 설정까지 포함)을 삭제하고 출하 시 기본 설정으로 복구하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<시스템 초기화>의 <b>[설정지움]</b> 버튼을 클릭합니다.
3	모든 설정을 삭제할 것인지 확인하는 팝업 창이 나타납니다. <b>[확인]</b> 을 클릭합니다.
4	출하시의 기본 설정이 성공적으로 복구되면 시스템을 다시 시작할지 묻는 팝업 창이 나타납니다. 복구한 기본 설정을 WEBFRONT-K에 적용하려면 <b>[확인]</b> 을 클릭하여 시스템을 다시 시작합니다.

### 설정 삭제하기

다음은 SSD의 저장 공간에 저장된 설정을 삭제하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<설정 저장 리스트> 부분에서 설정을 삭제할 SSD 저장 공간에 있는 <b>[삭제]</b> 버튼을 클릭합니다.
3	저장 공간에 저장된 설정을 삭제할 것인지 확인하는 팝업 창이 나타납니다. <b>[확인]</b> 을 클릭합니다.



**주의:** 현재 사용중인 저장 공간에 저장된 설정은 삭제하지 않도록 주의해야 합니다.

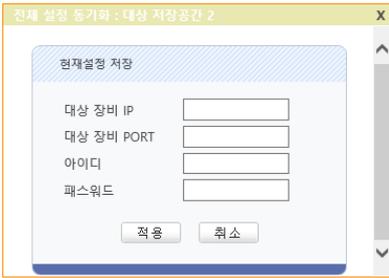
## 다음 부팅시 사용할 설정 지정하기

다음은 SSD의 특정 저장공간에 저장된 설정을 다음 부팅 시부터 사용하도록 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<설정 저장 리스트> 부분에서 다음 부팅 시부터 사용할 설정이 저장된 SSD 저장 공간의 <b>[다음 부팅시 사용]</b> 버튼을 클릭합니다.
3	선택한 저장 공간의 설정을 다음 부팅 시에 사용할 것인지 확인하는 팝업 창이 나타납니다. <b>[확인]</b> 을 클릭합니다.
4	해당 저장 공간의 상태 항목에 '다음 부팅시 사용되도록 설정됨'이라는 메시지가 표시됩니다.

## 설정 동기화하기

다음은 다른 WEBFRONT-K의 애플리케이션 설정을 가져와서 지정한 SSD의 저장 공간에 저장하는 방법입니다. 이 기능을 사용하면 다른 WEBFRONT-K의 '다음 부팅시 사용'으로 지정된 저장공간의 설정을 가져옵니다.

순서	설정 과정
1	<b>System - 일반설정 - 설정 관리</b> 메뉴를 클릭합니다.
2	<설정 저장 리스트> 부분에 있는 3개의 플래시 저장 공간 중에서 다른 WEBFRONT-K로부터 가져온 설정을 저장할 저장 공간의 <b>[전체 설정 동기화]</b> 버튼을 클릭합니다. <현재설정 저장> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 <b>[적용]</b> 버튼을 클릭합니다.
3	<div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>대상 장비 IP</b>                    설정을 가져올 WEBFRONT-K의 IP 주소를 입력합니다.</li> <li>• <b>대상 장비 PORT</b>                설정을 가져올 WEBFRONT-K의 포트 번호를 입력합니다.</li> <li>• <b>아이디</b>                            설정을 가져올 WEBFRONT-K로 로그인할 때 사용할 ID를 입력합니다.</li> <li>• <b>패스워드</b>                        설정을 가져올 WEBFRONT-K로 로그인할 때 사용할 패스워드를 입력합니다.</li> </ul> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p> <b>주의:</b> 설정을 가져올 WEBFRONT-K는 설정 동기화를 수행 중인 WEBFRONT-K와 PLOS 버전이 같아야 합니다.</p> <p> <b>참고:</b> 설정 동기화 기능에서 제외되는 메뉴는 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>• [System - 일반설정 - 시스템 감시] 메뉴</li> <li>• [System - 네트워크] 메뉴에서 링크링크를 제외한 나머지 메뉴(포트 바운더리, IP 주소, VLAN, 포트, 미러링, 트렁킹, STP, ARP)</li> </ul> </div>



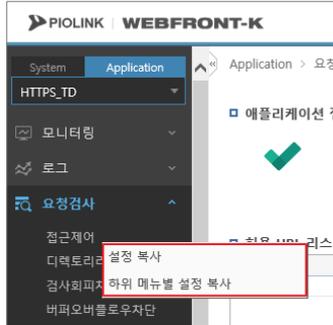
## 설정 복사하기

이 절에서는 현재 선택된 애플리케이션의 설정을 다른 애플리케이션으로 복사하는 방법에 대해 살펴봅니다.

### 복사할 설정 선택하기

다른 애플리케이션으로 복사할 설정을 선택하는 방법에는 2가지 방법이 있습니다.

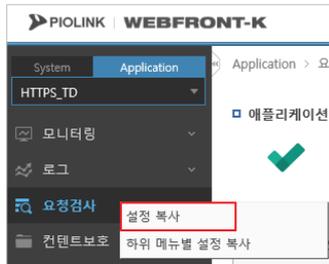
- **Application** 메뉴에서 복사하고자 하는 설정 메뉴를 오른쪽 버튼으로 클릭



**Application** 메뉴의 하위 메뉴에서 오른쪽 버튼을 클릭하면 위와 같이 팝업 메뉴가 나타납니다. 해당 메뉴에 속한 모든 항목들 즉 하위 메뉴를 모두 포함하여 한꺼번에 복사하거나(**설정 복사** 메뉴) 하위 항목 중에서 일부를 선택하여 복사할 수 있습니다(**하위 메뉴별 설정 복사** 메뉴).

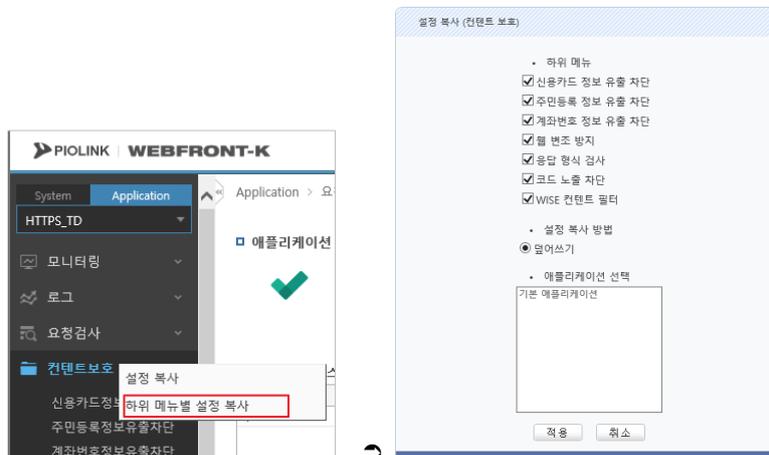
몇 가지 예를 통해 복사할 설정을 선택하는 방법을 살펴봅니다.

- 애플리케이션의 '요청 검사 설정 전체'를 다른 애플리케이션으로 복사하려는 경우  
**Application - 요청 검사** 메뉴를 오른쪽 마우스로 클릭한 후 **설정 복사** 메뉴를 클릭



- 애플리케이션의 '컨텐츠 보호 설정 중 일부'를 다른 애플리케이션으로 복사하려는 경우

**Application - 컨텐츠 보호** 메뉴를 오른쪽 마우스로 클릭한 후 **하위 메뉴별 설정 복사** 메뉴를 클릭 → <설정 복사> 팝업 창의 '하위 메뉴' 항목에서 복사할 항목을 선택



## 설정 복사 방식

WEBFRONT-K가 설정을 복사하는 방식에는 다음과 같은 방식이 있습니다.

- 덮어쓰기(overwrite): 애플리케이션의 기존 설정을 모두 삭제한 후 현재 애플리케이션의 설정을 복사하는 방식.

## 복사되지 않는 설정

설정 복사 기능은 애플리케이션 설정 중에서 다음 설정들은 복사할 수 없습니다.

- 애플리케이션 - 일반 설정
- 애플리케이션 - 기타 설정 - 애플리케이션 프로토콜 정보
- SSL - 일반 설정
- 쿼리스트링 차단 기능(버퍼 오버플로우 차단, SQL 삽입 차단, 스크립트 삽입 차단)

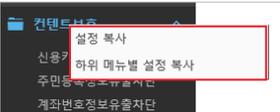
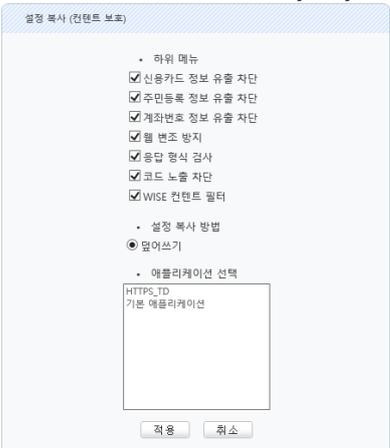
따라서, 위의 메뉴나 설정 화면에서는 오른쪽 마우스 버튼을 클릭해도 설정 복사 팝업 메뉴가 나타나지 않습니다.



**참고:** 설정 복사 기능은 애플리케이션의 '설정'만 복사하는 기능이므로 애플리케이션을 설정하는 메뉴가 아닌 로그, 모니터링, System 메뉴에서는 설정 복사 팝업 메뉴가 나타나지 않습니다.

## 설정 복사하기

다음은 설정 복사하기 기능을 사용하여 현재 애플리케이션의 설정을 다른 애플리케이션으로 복사하는 과정입니다.

순서	설정 과정
1	<p><b>Application</b> 드롭다운 목록에서 설정을 복사할 애플리케이션(원본 애플리케이션)을 선택합니다.</p> 
2	<p><b>복사할 설정 선택하기</b> 절의 내용을 참고하여 복사할 설정을 선택합니다.</p> 
3	<p>&lt;설정 복사&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 <b>[적용]</b> 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• 하위 메뉴: 선택한 메뉴의 하위 메뉴 중에서 설정을 복사할 메뉴를 선택합니다.</li> <li>• 설정 복사 방법: 설정을 복사할 방식은 기본적으로 덮어쓰기로 지정되어 있습니다.</li> <li>• 애플리케이션 선택: 설정을 복사할 대상 애플리케이션을 선택합니다. <b>[Shift]</b> 키나 <b>[Ctrl]</b> 키를 사용하면 여러 애플리케이션을 선택할 수 있습니다.</li> </ul>

## 기술 지원 도우미

WEBFRONT-K에 장애가 발생한 경우, 장애 발생 원인을 파악하기 위해서는 여러 차례 관련 정보(장비 상태 정보 및 로그 정보)를 확인해야 합니다. 이러한 번거로움을 줄이기 위해 WEBFRONT-K는 기술 지원 도우미 기능을 제공합니다.

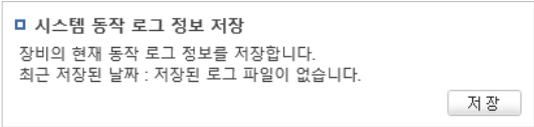
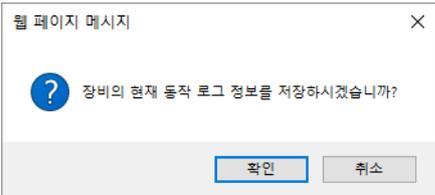
기술 지원 도우미는 다음과 같은 동작 로그 정보를 통합된 하나의 파일로 제공하는 기능입니다.

- 하드웨어 상태 정보
- CPU, 메모리 사용량 정보
- 시스템 정보
- 설정 정보(포트, 인터페이스, 라우팅, 보안, SSL)
- 로그 정보

기술 지원 도우미 기능을 사용하면 장애 발생 시 쉽고 빠르게 정보를 확인하여 원인을 분석할 수 있어, 신속하게 장애에 대응할 수 있습니다.

## 시스템 동작 로그 정보 저장하기

WEBFRONT-K의 메모리에 시스템 동작 로그 정보를 저장하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 기술지원 도우미</b> 메뉴를 클릭합니다.
2	<시스템 동작 로그 정보 저장>의 [저장] 버튼을 클릭합니다. 
3	다음과 같은 팝업 창이 나타나면 [확인] 버튼을 클릭합니다. 

## 시스템 동작 로그 정보 다운로드하기

WEBFRONT-K의 메모리에 저장되어 있는 동작 로그 정보를 Web Manager가 실행중인 사용자의 PC로 다운로드하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 기술지원 도우미</b> 메뉴를 클릭합니다.
2	<p>&lt;시스템 동작 로그 정보 다운로드&gt;의 [다운로드] 버튼을 클릭합니다.</p> <div data-bbox="582 427 1114 551" style="border: 1px solid gray; padding: 5px;"> <p> <input type="checkbox"/> 시스템 동작 로그 정보 다운로드                      저장한 로그 정보를 다운로드합니다.                      다운로드 기능을 이용하기 위해서는 먼저 동작 로그 정보를 저장해야 합니다.                 </p> <p style="text-align: right;"><input type="button" value="다운로드"/></p> </div>
3	<p>다음과 같은 팝업 창이 나타나면 [확인] 버튼을 클릭합니다.</p> <div data-bbox="635 651 1059 842" style="border: 1px solid gray; padding: 10px; width: fit-content; margin: auto;"> <p style="text-align: right;">웹 페이지 메시지 <span style="float: right;">×</span></p> <p style="text-align: center;"> <span style="font-size: 2em; color: blue;">?</span> 저장한 동작 로그 파일을 다운로드하시겠습니까?                 </p> <p style="text-align: center;"> <input type="button" value="확인"/> <input type="button" value="취소"/> </p> </div>



**참고:** 시스템 동작 로그 정보를 다운로드하기 위해서는 먼저 동작 로그 정보를 WEBFRONT-K 메모리에 저장해야 합니다. 동작 로그 정보를 저장하는 방법은 앞 절인 <시스템 동작 로그 정보 저장하기> 부분을 참고합니다.



**참고:** 시스템 동작 로그 정보 파일은 'tech-assist-diag-info.tar.gz' 형식으로 다운로드 됩니다.

# 서버 장애 감시

## 개요

서버 장애 감시 기능은 WEBFRONT-K에 등록된 애플리케이션의 서버의 통신 상태를 감시하는 기능입니다. WEBFRONT-K는 애플리케이션 등록 시 설정한 IP 주소와 포트를 사용하여 애플리케이션 서버들의 통신 상태를 5초마다 검사(장애 감시)하고 그 결과를 화면에 표시해줍니다. 장애 감시 시 사용하는 프로토콜은 TCP이고, 서버에서 3초 이내에 응답을 보내 주지 않으면 장애 감시가 실패한 것으로 판단합니다. 장애 감시 결과가 실패인 경우 다시 장애 감시를 시도하지 않습니다.

다음은 WEBFRONT-K의 서버 장애 감시 기능의 동작 방식을 정리한 표입니다.

항목	값
프로토콜	TCP
IP 주소/포트	애플리케이션에 설정된 IP 주소와 포트
간격	5초
타임아웃	3초
재시도	없음

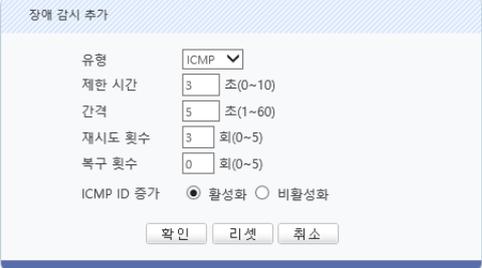
## 서버 장애 감시 활성화하기

다음은 서버 장애 감시 기능을 활성화하는 방법입니다.

순서	설정 과정																												
1	<b>System - 일반설정 - 서버장애 감시</b> 메뉴를 클릭합니다.																												
2	<서버장애감시>의 [변경] 버튼을 클릭합니다.																												
3	<p>&lt;서버장애감시 상태 설정&gt; 팝업 창에서 '활성화'를 선택하고 [적용] 버튼을 클릭합니다. (기본값: 비활성화)</p>  <p>서버장애감시 상태 설정 상태 <input type="radio"/> 활성화 <input checked="" type="radio"/> 비활성화 적용 리셋 취소</p>																												
4	<p>서버 장애 감시 기능을 활성화하면 다음과 같이 서버 상태를 보여주는 테이블이 출력됩니다.</p>  <p>서버장애감시 상태: 활성화</p> <table border="1"> <thead> <tr> <th>IP 주소</th> <th>포트</th> <th>애플리케이션 수</th> <th>상태</th> <th>BYPASS 설정</th> <th>장애 감시 리스트</th> <th>활성화</th> </tr> </thead> <tbody> <tr> <td>172.16.2.201</td> <td>443</td> <td>1</td> <td></td> <td>X</td> <td>0</td> <td></td> </tr> <tr> <td>172.16.2.202</td> <td>443</td> <td>1</td> <td></td> <td>X</td> <td>0</td> <td></td> </tr> <tr> <td>172.16.2.203</td> <td>443</td> <td>1</td> <td></td> <td>X</td> <td>0</td> <td></td> </tr> </tbody> </table> <ul style="list-style-type: none"> <li>• IP 주소: 애플리케이션 등록 시 입력한 IP 주소</li> <li>• 포트: 애플리케이션 등록 시 입력한 포트</li> <li>• 애플리케이션 수: 동일한 IP 주소와 포트를 사용하는 애플리케이션의 개수</li> <li>• 상태: IP 주소와 포트를 사용한 장애 감시 결과</li> <li>• BYPASS 설정: 바이패스 사용 여부. 장애 감시 리스트가 활성화된 상태에서 서버 장애로 판단되면 프록시 처리하지 않고 서버에 직접 패킷 전송</li> <li>• 장애 감시 리스트: 장애 감시 리스트 개수.  아이콘을 클릭하여 수정.</li> <li>• 활성화: 해당 서버에 대한 장애 감시 활성화 여부</li> </ul>	IP 주소	포트	애플리케이션 수	상태	BYPASS 설정	장애 감시 리스트	활성화	172.16.2.201	443	1		X	0		172.16.2.202	443	1		X	0		172.16.2.203	443	1		X	0	
IP 주소	포트	애플리케이션 수	상태	BYPASS 설정	장애 감시 리스트	활성화																							
172.16.2.201	443	1		X	0																								
172.16.2.202	443	1		X	0																								
172.16.2.203	443	1		X	0																								

## 장애 감시 추가

다음은 장애 감시 설정을 추가하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 서버장애 감시</b> 메뉴를 클릭합니다.
2	<서버장애감시>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<서버장애감시 상태 설정> 팝업 창에서 '활성화'를 선택하고 <b>[적용]</b> 버튼을 클릭합니다. (기본값: 비활성화) 
4	서버 장애 감시 기능을 활성화하면 다음과 같이 서버 상태를 보여주는 테이블이 출력됩니다. 장애 감시를 추가할 항목의  아이콘을 클릭합니다. 
5	바이패스와 장애 감시를 설정할 수 있는 창이 출력됩니다. <BYPASS 설정>의 <b>[변경]</b> 버튼을 클릭합니다.
6	<BYPASS 설정> 팝업 창에서 활성화 또는 비활성화를 선택하고 <b>[적용]</b> 버튼을 클릭합니다. (기본값: 비활성화) 
7	<장애 감시 설정>의 <b>[변경]</b> - <b>[추가]</b> 버튼을 클릭합니다.
8	<장애 감시 추가> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 <b>[확인]</b> 버튼을 클릭합니다.  <ul style="list-style-type: none"> <li>• <b>유형</b> 장애 감시의 유형 (ICMP, TCP, HTTP, HTTPS)</li> <li>• <b>제한 시간</b> 장애 여부를 판단하는 타임아웃 값 (설정 범위: 0~10(초), 기본값: 3)</li> <li>• <b>간격</b> 장애 감시 패킷을 서버로 전송하는 주기 (설정 범위: 1~60(초), 기본값: 5)</li> <li>• <b>재시도 횟수</b> 장애 감시 패킷의 재전송 주기 (설정 범위: 0~5, 기본값: 3)</li> <li>• <b>복구 횟수</b> 설정 범위: 0~5, 기본값: 0</li> <li>• <b>ICMP ID 증가</b> 서버로 ICMP 패킷을 전송한 후, ICMP 패킷 ID의 증가 여부. 유형이 'ICMP'인 경우에만 설정. (기본값: 활성화)</li> <li>• <b>Domain</b> 유형이 HTTP, HTTPS인 경우에만 설정</li> <li>• <b>URL</b> 유형이 HTTP, HTTPS인 경우에만 설정</li> <li>• <b>설명</b> 유형이 HTTP, HTTPS인 경우에만 설정</li> </ul>

# 시스템 감시

시스템 감시 기능은 WEBFRONT-K의 주요 자원인 CPU와 메모리, 포트의 사용 상태를 감시하는 기능입니다. 시스템 감시 기능이 활성화되어 있으면, 일정한 주기로 CPU와 메모리의 사용량(usage)과 포트의 실시간 트래픽 양이 지정한 임계값(threshold)을 초과하였는지 확인합니다. 초과한 경우에는 관련 정보를 가진 로그 메시지를 생성하고 저장합니다.



**참고:** 메모리의 사용량은 SDRAM의 사용량을 의미합니다.



**참고:** 시스템 감시 기능을 통해 생성되는 로그의 이벤트 레벨은 'Warning'입니다.

각 자원마다 감시 여부와 임계값을 설정할 수 있습니다. 감시 주기는 모든 자원에 공통적으로 적용됩니다.

## 시스템 감시 사용 여부와 감시 주기 설정

CPU나 포트, 메모리의 감시 기능이 활성화되어 있어도 시스템 감시 기능이 비활성화되어 있으면 이러한 자원의 감시 기능이 동작하지 않습니다. 각 자원의 감시 기능을 활성화한 후에는 반드시 시스템 감시 기능을 활성화해야 합니다. 다음은 시스템 감시 기능을 활성화하고 감시 주기를 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 시스템 감시</b> 메뉴를 클릭합니다.
2	<시스템 감시 정보>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;시스템 감시 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;"> </div> <ul style="list-style-type: none"> <li>• 상태            시스템 감시 기능의 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• 간격            자원의 감시 주기를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 1000초)</li> </ul>

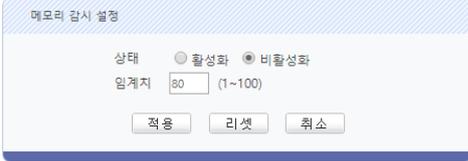
## CPU 감시 설정

CPU 감시 기능의 사용 여부와 임계치를 지정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 시스템 감시</b> 메뉴를 클릭합니다.
2	<CPU 정보>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;CPU 감시 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;"> </div> <ul style="list-style-type: none"> <li>• 상태            CPU 감시 기능의 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• 임계치        CPU 사용률에 대한 임계값을 입력합니다. (설정 범위: 1 ~ 100, 기본값: 95%)</li> </ul>

## 메모리 감시 설정

메모리 감시 기능의 사용 여부와 임계치를 지정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 일반설정 - 시스템 감시 메뉴를 클릭합니다.
2	<메모리 정보>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;메모리 감시 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 [적용] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>상태</b>            메모리 감시 기능의 사용 여부를 지정합니다. (기본값: 비활성화)</li> <li>• <b>임계치</b>        메모리 사용률에 대한 임계값을 입력합니다. (설정 범위: 1 ~ 100, 기본값: 80%)</li> </ul>

## 포트 감시 설정

포트 감시 기능을 적용할 포트를 지정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 일반설정 - 시스템 감시 메뉴를 클릭합니다.
2	<포트 정보>의 [변경] - [추가] 버튼을 클릭합니다.
3	<p>&lt;포트 설정 추가&gt; 팝업 창에서 다음 설명을 참고하여 감시하고자 하는 포트에 대한 정보를 설정한 후 [확인] 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• <b>아이디</b>            ID를 1~32 범위의 값으로 입력합니다.</li> <li>• <b>상태</b>            포트를 감시할 것인지 여부를 지정합니다. (기본값: 활성화)</li> <li>• <b>포트</b>            감시할 포트의 번호를 지정합니다.</li> <li>• <b>유형</b>            포트 감시 기능은 감시 간격마다 포트의 트래픽 양을 확인하여 포트의 상태를 감시합니다. 네 가지 옵션 중 확인할 트래픽의 종류를 선택합니다. <ul style="list-style-type: none"> <li>- RxRate (bps)      초당 수신한 비트 수 (기본 설정)</li> <li>- RxRate (pps)      초당 수신한 패킷 수</li> <li>- TxRate (bps)      초당 전송한 비트 수</li> <li>- TxRate (pps)      초당 전송한 패킷 수</li> </ul> </li> <li>• <b>임계치</b>        포트의 트래픽 양에 대한 임계값을 지정합니다. Kbyte 단위로 입력하려면 K(1K ~ 1024K) 항목을, Mbyte 단위로 입력하려면 M(1M ~ 1024M) 항목을 선택합니다. (설정 범위: 1 ~ 1024, 기본 단위: Kbyte)</li> </ul>
4	감시할 포트를 모두 추가한 후에는 [적용] 버튼을 클릭합니다.

# SNMP

이 절에서는 WEBFRONT-K에서 지원하는 SNMP에 대해 소개하고, WEBFRONT-K에 SNMP와 관련된 설정 작업을 수행하는 방법을 살펴봅니다.

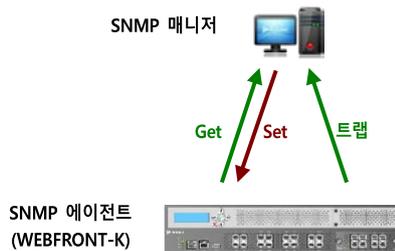
## 개요

SNMP(Simple Network Management Protocol)는 장비와 네트워크를 원격지에서 관리할 수 있도록 해주는 대표적인 관리 프로토콜입니다. SNMP를 지원하는 네트워크 장비는 장비의 현재 상태나 설정을 외부의 호스트에게 알려주거나 호스트가 조회할 수 있게 해주고, 때로는 외부의 호스트에서 장비의 상태나 설정을 변경할 수 있게 해줍니다.

SNMP를 지원하는 네트워크 장비를 'SNMP 에이전트'라고 하고, 장비의 정보를 조회하고 설정하는 외부의 호스트를 'SNMP 매니저'라고 합니다. SNMP 매니저가 조회하고 설정할 수 있는 SNMP 에이전트의 정보는 MIB(Management Information Base)이라는 데이터베이스에 저장되는데, 정보를 조회할 때에는 MIB의 값을 읽어 가고, 정보를 설정할 때에는 MIB의 값을 변경하게 됩니다.

## SNMP 매니저와 에이전트의 통신

SNMP 매니저가 SNMP 에이전트에 접속하여 MIB 정보를 받아오거나 MIB 값을 변경하려면 인증 과정을 거쳐야 합니다. 인증 과정을 위해 SNMP v1과 v2에서는 커뮤니티(community)를 사용하고, SNMP v3에서는 사용자 ID와 MD5 암호, DES 암호를 사용합니다. SNMP 매니저가 에이전트에 접속하면 통신 명령을 사용하여 필요한 정보를 교환할 수 있습니다. 다음은 SNMP 매니저와 에이전트 사이의 통신을 나타내는 그림입니다.



그림에서와 같이 SNMP 매니저가 SNMP 에이전트에서 MIB의 값을 읽어 갈 때에는 Get이라는 명령을 사용하고, MIB의 값을 변경할 때에는 Set 명령을 사용합니다.

트랩(trap)은 SNMP 에이전트에서 사용자 인증 오류나 시스템 재시작, 인터페이스 업/다운 등의 중요한 이벤트가 발생했을 때 SNMP 에이전트가 SNMP 매니저에게 전달하는 메시지입니다. 트랩 메시지에는 발생한 이벤트에 대한 정보가 담겨 있습니다. SNMP 매니저가 트랩 메시지를 수신하려면 SNMP 에이전트에 트랩 호스트로 설정되어 있어야 합니다.

## SNMP 버전

다음은 WEBFRONT-K에서 지원하는 SNMP 버전입니다.

### • SNMP v1

SNMP 버전 1은 RFC 1157에 정의되어 있습니다. SNMP 버전 1에서는 기본적인 MIB-I과 MIB-II를 간략하게 정의하였으며, 시스템, 네트워크, 애플리케이션, 서비스 등에 대한 내용을 포함하고 있습니다. SNMP 버전 1은 커뮤니티 기반의 보안 기능을 지원하며, SNMP 매니저와 에이전트의 커뮤니티 이름이 매칭되어야만 SNMP 매니저와 에이전트 사이의 통신이 가능하게 합니다.

### • SNMP v2c

SNMP 버전 2c는 RFC 1902에 정의되어 있습니다. SNMP 버전 2에서는 SNMP 버전 1의 내용을 포함하고 있을 뿐만 아니라, 데이터 종류, 카운터 크기, 프로토콜 동작 등을 추가하여 보안과 접근 제어(access control) 기능을 강화하였습니다. SNMP 버전 2는 버전 1과 같이 커뮤니티 기반의 보안 기능을 지원합니다.

### • SNMP v3

SNMP 버전 3은 가장 최근의 SNMP 버전이며, RFC 2571~ 2575에 정의되어 있습니다. SNMP 버전 3에서는 비밀 키를

이용하여 사용자 인증을 거친 후 장비에 접근하도록 하고, 데이터를 암호화하여 보안 기능을 크게 강화하였습니다.

## SNMP 기본 설정

기본적으로 WEBFRONT-K에는 SNMP와 관련된 설정이 다음과 같이 설정되어 있습니다.

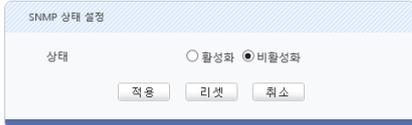
항목	기본 설정
SNMP 상태	비활성화
커뮤니티	없음
사용자	없음
트랩	비활성화
트랩 호스트	없음

## SNMP 설정하기

이 절에서는 SNMP 관련 설정 작업을 수행하는 방법에 대해 소개합니다.

### SNMP 상태 설정

기본적으로 SNMP는 비활성화 상태로 설정되어 있습니다. SNMP 상태를 활성화로 변경하면 설정된 트랩 호스트로 트랩 정보가 전송되고, SNMP 매니저에서 설정된 사용자 ID와 커뮤니티를 사용하여 WEBFRONT-K의 정보를 설정하거나 수신할 수 있습니다. 다음은 SNMP 상태를 변경하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - SNMP</b> 메뉴를 클릭합니다.
2	< <b>SNMP 상태 정보</b> >의 [ <b>변경</b> ] 버튼을 클릭합니다.
3	< <b>SNMP 상태 설정</b> > 팝업 창에서 상태를 선택한 후 [ <b>적용</b> ] 버튼을 클릭합니다. 기본적으로는 '비활성화'로 지정되어 있습니다. 



**주의:** Analyzer 버전 2.0이 설치되어 있는 서버의 경우 WEBFRONT-K의 상태에 관한 정보는 SNMP로 전송됩니다. 따라서 WEBFRONT-K의 SNMP 기능을 반드시 활성화해야 합니다. SNMP를 활성화하려면 최소한 하나 이상의 커뮤니티가 존재해야 하므로 활성화하기 전에 커뮤니티를 추가합니다. Analyzer로 장비 상태에 관한 정보를 보내기 위해서는 커뮤니티 이름이 'public'인 커뮤니티를 생성하고, 커뮤니티가 추가되면 SNMP를 활성화합니다. 커뮤니티를 추가하는 과정에 대한 상세한 설명은 이 장의 **사용자 정보 설정** 절을 참고하도록 합니다.

### SNMP 시스템 정보(이름, 위치, 연락처, 설명) 설정

WEBFRONT-K의 이름과 위치, 연락처는 SNMP 매니저에서 WEBFRONT-K가 어떤 장비이고 어디에 설치되어 있는지, 또 문제가 발생한 경우 어디로 연락을 취해야 하는지 등을 알아내는 데 도움을 줍니다. 기본적으로 WEBFRONT-K에는 SNMP 시스템 정보가 설정되어 있지 않은데, 다음과 같은 방법으로 이 정보를 설정할 수 있습니다.

순서	설정 과정
1	<b>System - 일반설정 - SNMP</b> 메뉴를 클릭합니다.
2	< <b>SNMP 시스템 정보</b> >의 [ <b>변경</b> ] 버튼을 클릭합니다.
3	< <b>SNMP 시스템 설정</b> > 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 [ <b>적용</b> ] 버튼을 클릭합니다.



- **이름** 숫자와 알파벳, '.', '-'로 구성된 최대 8글자의 장비의 이름을 입력합니다. 장비의 이름은 어떤 장비인지, 어떤 용도로 사용 중인지를 쉽게 알 수 있는 문자열을 사용하도록 합니다.
- **위치** 숫자와 알파벳, 그리고 특수 문자(따옴표 제외)로 구성된 최대 64자의 위치 정보를 입력합니다. 위치 정보는 주로 장비가 설치된 곳의 주소를 지정하는 경우가 많습니다.
- **연락처** 숫자와 알파벳, 그리고 특수 문자(따옴표 제외)로 구성된 최대 64자의 연락처를 입력합니다. 연락처는 주로 관리자의 이메일 주소나 전화 번호를 사용합니다.

## SNMP 사용자 정보 설정

SNMP 사용자 정보는 커뮤니티(community) 이름과 사용자 ID입니다. 커뮤니티 이름은 SNMP v1과 v2c에서 인증 시 사용하는 문자열이고, 사용자 ID는 SNMP v3에서 인증 시 암호와 함께 사용됩니다. SNMP 매니저에서 SNMP를 이용해 WEBFRONT-K로 접속하기 위해서는 WEBFRONT-K에 설정된 것과 동일한 커뮤니티나 사용자 ID를 사용해야 합니다. WEBFRONT-K에 기본으로 설정되어 있는 사용자 정보는 없습니다. SNMP 사용자 정보를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - SNMP</b> 메뉴를 클릭합니다.
2	< <b>SNMP 사용자 정보</b> >의 [ <b>변경</b> ] 버튼을 클릭합니다.
3	<p>&lt;<b>SNMP v1, v2c 커뮤니티 이름 정보</b>&gt;에서는 커뮤니티 이름을 추가할 수 있고, 아래에 있는 &lt;<b>SNMP v3 사용자 ID 정보</b>&gt; 부분에서는 사용자 ID와 암호를 추가할 수 있습니다. 추가하고자 하는 항목에 있는 [<b>변경</b>] 버튼을 클릭합니다.</p> <p><b>커뮤니티 추가하기</b></p> <ol style="list-style-type: none"> <li>&lt;<b>SNMP v1, v2c 커뮤니티 이름 설정</b>&gt; 화면 아래에 있는 [<b>추가</b>] 버튼을 클릭합니다.</li> <li>&lt;<b>커뮤니티 이름 추가</b>&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 모두 입력한 후 [<b>확인</b>] 버튼을 클릭합니다. <ul style="list-style-type: none"> <li>• <b>커뮤니티 이름</b> 커뮤니티 이름을 입력합니다.</li> <li>• <b>권한</b> 항목에는 입력한 커뮤니티 이름을 사용할 때 부여할 권한을 지정합니다. SNMP 정보를 읽어들일 수만 있도록 하려면(GET) 'Read-only'를, 읽고 쓸 수 있도록 하려면(GET, SET) 'Read-write'를 선택합니다. (기본값: Read-only)</li> <li>• <b>Limit-Oid</b> SNMP 커뮤니티가 접근할 수 있는 OID를 지정합니다. OID를 지정하면 해당 OID 이하의 OID만 접근할 수 있습니다.</li> </ul> </li> </ol> <div style="text-align: center;"> </div> <ol style="list-style-type: none"> <li>커뮤니티 이름을 더 추가하려면 1 ~ 2번 과정을 반복합니다. 커뮤니티 이름을 모두 추가한 후에는 [<b>적용</b>] 버튼을 클릭합니다.</li> </ol> <p><b>주의:</b> Analyzer 버전 2.0이 설치되어 있는 서버의 경우 WEBFRONT-K의 상태에 관한 정보는 SNMP로 전송됩니다. 따라서 WEBFRONT-K의 SNMP 기능을 반드시 활성화 해야합니다. SNMP를 활성화하려면 최소한 하나 이상의 커뮤니티가 존재해야 하므로 활성화하기 전이 커뮤니티를 추가합니다. Analyzer로 장비 상태에 관한 정보를 보내기 위해서는 커뮤니티 이름이 'public'인 커뮤니티를 생성하고 커뮤니티가 추가되면 SNMP를 활성화합니다. SNMP 기능을 활성화하는 방법에 대한 설명은 이 장의 <b>SNMP 상태 설정</b> 절을 참고합니다.</p> <p><b>사용자 ID 추가하기</b></p> <ol style="list-style-type: none"> <li>&lt;<b>SNMP v3 사용자 ID 설정</b>&gt; 화면 아래에 있는 [<b>추가</b>] 버튼을 클릭합니다.</li> <li>&lt;<b>사용자 ID 추가</b>&gt; 팝업 창에서 다음의 설명을 참고하여 각 항목의 값을 모두 입력한 후 [<b>확인</b>] 버튼을 클릭합니다.</li> </ol>

- **사용자 ID** 인증시 ID로 사용할 문자열을 입력합니다.
  - **SHA Password** 인증에 사용할 암호를 입력합니다. 알파벳 대문자, 소문자, 숫자, 특수문자 중 3가지 이상의 조합으로 9~64 글자의 문자열로 지정합니다.
  - **AES Password** 인증에 사용할 암호를 입력합니다. 알파벳 대문자, 소문자, 숫자, 특수문자 중 3가지 이상의 조합으로 9~64 글자의 문자열로 지정합니다.
- 3) 사용자 ID를 더 추가하려면 1 ~ 2번 과정을 반복합니다. 사용자 ID를 모두 추가한 후에는 [적용] 버튼을 클릭합니다.

## SNMP 트랩 설정

WEBFRONT-K는 장비의 재시작, 인터페이스의 Up/Down, Web Manager로의 로그인/로그아웃과 같은 이벤트가 발생할 때마다 트랩 호스트로 트랩 메시지를 전송합니다. 기본적으로는 이러한 이벤트가 발생해도 트랩 메시지를 전송하지 않도록 설정되어 있고 트랩 호스트도 등록되어 있지 않습니다. 트랩 메시지는 원격지에서 WEBFRONT-K의 상태를 파악하는데 도움이 되므로 필요한 호스트를 트랩 호스트로 등록하고 주요한 이벤트의 트랩 상태도 활성화하는 것이 좋습니다. 다음은 이벤트의 트랩 상태를 변경하고 트랩 호스트를 등록하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - SNMP</b> 메뉴를 클릭합니다.
2	< <b>SNMP 트랩 정보</b> >의 [변경] 버튼을 클릭합니다.  < <b>SNMP 트랩 설정</b> > 화면이 나타납니다. SNMP 트랩 설정 화면에는 각 트랩의 상태와 등록된 트랩 호스트의 목록을 보여줍니다.  <b>트랩 상태 변경하기</b> 1) < <b>SNMP 트랩 타입 정보</b> >의 [변경] 버튼을 클릭합니다. 2) < <b>SNMP 트랩 타입 설정</b> > 팝업 창에서 다음 설명을 참고하여 각 트랩의 상태를 설정한 후 [적용] 버튼을 클릭합니다. 모든 트랩은 기본적으로 '비활성화' 상태로 설정되어 있습니다.
3	<div data-bbox="619 1227 1082 1487" data-label="Form"> </div> <ul style="list-style-type: none"> <li>• <b>Cold Start</b> 리셋 버튼이나 전원 스위치를 눌러서 WEBFRONT-K가 다시 시작된 경우 발생하는 트랩</li> <li>• <b>Interface Up</b> 인터페이스의 링크가 업(up)되었을 때 발생하는 트랩</li> <li>• <b>Interface Down</b> 인터페이스의 링크가 다운(down)되었을 때 발생하는 트랩</li> <li>• <b>Fan</b> 장비의 냉각 팬이 ON/OFF 되었을 때 발생하는 트랩</li> <li>• <b>Power</b> 장비의 전원이 ON/OFF 되었을 때 발생하는 트랩</li> <li>• <b>Temperature</b> 장비의 CPU 온도가 임계값을 초과한 경우 발생하는 트랩</li> </ul> <p><b>트랩 호스트 추가하기</b> 1) &lt;<b>SNMP 트랩 호스트 정보</b>&gt;의 [변경] - [추가] 버튼을 클릭합니다. 2) &lt;<b>트랩 호스트 IP 주소 추가</b>&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [확인] 버튼을 클릭합니다.</p> <div data-bbox="619 1809 1082 2069" data-label="Form"> </div> <ul style="list-style-type: none"> <li>• <b>IP 주소</b> 트랩 메시지를 전송할 호스트의 IP 주소를 입력</li> </ul>

- 버전 트랩 메시지의 버전을 선택 (설정 범위: 1, 2c, 3, 기본값: 2c)
- 커뮤니티 이름 트랩 메시지를 전송할 때 사용할 커뮤니티를 입력 (버전을 1, 2c로 선택한 경우)
- 사용자 트랩 메시지를 전송할 때 인증 ID로 사용할 문자열 입력 (버전을 3으로 선택한 경우)
- 엔진 ID 트랩 메시지를 전송할 트랩 호스트의 엔진 ID를 5~128 글자의 문자열로 입력합니다. (버전을 3으로 선택한 경우)
- SHA 트랩 메시지를 전송할 때 인증에 사용할 암호를 입력. 알파벳 대문자, 소문자, 숫자, 특수문자 중 3가지 이상의 조합으로 9~64글자의 문자열을 지정합니다. (버전을 3으로 선택한 경우)
- AES 트랩 메시지를 전송할 때 인증에 사용할 암호를 입력. 알파벳 대문자, 소문자, 숫자, 특수문자 중 3가지 이상의 조합으로 9~64글자의 문자열을 지정합니다. (버전을 3으로 선택한 경우)

3) 트랩 호스트를 모두 추가한 후에는 [적용] 버튼을 클릭합니다.

## 라이선스 관리

WEBFRONT-K 정식 버전을 사용하려면 제품 구입시 발급받은 라이선스 키를 등록해야 합니다. 라이선스는 아래와 같이 두 가지 종류가 있습니다.

- 유지보수 라이선스

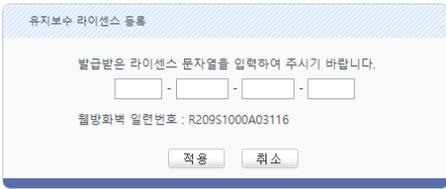
제품 사용을 위한 라이선스로 WEBFRONT-K 설치 후 최초로 접속할 때 등록하고 이후 라이선스가 만료되거나 변경이 필요한 경우 **System - 일반설정 - 라이선스 관리** 메뉴에서 수정할 수 있습니다.

- 라이선스

제품 성능에 대한 라이선스로, 라이선스 종류에 따라 처리율(Throughput)과 TPS가 적용됩니다.

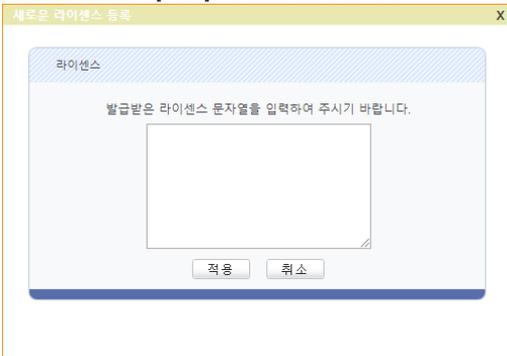
## 유지보수 라이선스 설정

유지보수 라이선스를 등록하는 방법을 설명합니다.

순서	설정 과정
1	<b>System - 일반설정 - 라이선스 관리</b> 메뉴를 클릭합니다.
2	<유지보수 라이선스>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;유지보수 라이선스 등록&gt; 팝업 창에서 라이선스 키를 입력한 후 <b>[적용]</b> 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• 라이선스 키                    제품 구매시 발급받은 라이선스 키를 입력합니다.</li> <li>• 웹방화벽 일련번호            WEBFRONT-K의 일련번호가 출력됩니다.</li> </ul>

## 라이선스 설정

성능 라이선스를 등록하는 방법을 설명합니다.

순서	설정 과정
1	<b>System - 일반설정 - 라이선스 관리</b> 메뉴를 클릭합니다.
2	<라이선스>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<p>&lt;라이선스&gt; 팝업 창에서 라이선스 키를 입력한 후 <b>[적용]</b> 버튼을 클릭합니다.</p>  <ul style="list-style-type: none"> <li>• 라이선스 키                    제품 구매시 발급받은 라이선스 키를 입력합니다.</li> </ul>

# 국가별 IP

국가별 IP는 클라이언트의 IP주소로 접속 국가를 확인하는데 사용되는 파일을 업데이트하는 기능입니다. 국가별 IP 파일은 국가별로 접근제어 정책을 적용하거나 보안 로그에서 접속 국가를 확인하는데 사용됩니다.

이 절에서는 국가별 IP 파일을 업데이트 하는 방법을 살펴봅니다.

## 국가별 IP 업데이트

국가별 IP 파일을 업데이트하는 방법에는 업데이트 서버에 연결하는 방법과 사용자 PC에 저장된 파일을 업로드하는 방법이 있습니다. 국가별 IP 파일을 업데이트하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 국가별 IP</b> 메뉴를 클릭합니다.
2-1	<p>방법1: 국가별 IP 네트워크 업데이트</p> <p>1) &lt;국가별 IP 네트워크 업데이트&gt;에 업데이트 서버의 URL을 입력한 후 [업데이트] 버튼을 클릭합니다.                  2) 기본적으로 GeolIP 공식홈페이지 다운로드 URL이 설정되어 있습니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>□ 국가별 IP 네트워크 업데이트</p> <p><input type="text" value="http://geolite.maxmind.com/download/geoip/databas"/> <input type="button" value="업데이트"/></p> </div>
2-2	<p>방법2: 국가별 IP 파일 업데이트</p> <p>1) &lt;국가별 IP 파일 업데이트&gt;에서 [파일선택] 버튼 클릭하여 업데이트할 국가별 IP 파일 선택합니다.                  2) 파일을 선택한 후 [파일업로드] 버튼을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>□ 국가별 IP 파일 업데이트</p> <p><input type="button" value="파일 선택"/> 선택된 파일 없음 <input type="button" value="파일업로드"/></p> </div> <p> 참고: 국가별 IP 업데이트용 파일은 GeolIP 다운로드 서버에서 배포되는 국가용 압축파일을 사용합니다.</p>
3	업데이트 확인 팝업 창이 나타나면 [확인] 버튼을 클릭합니다.

# PLOS 관리

PLOS는 WEBFRONT-K에 설치되어 있는 소프트웨어입니다. WEBFRONT-K의 PLOS에는 여러 개의 버전이 있으며, 버전마다 제공하는 기능이 다를 수 있습니다. 일반적으로 새로운 PLOS가 출시되었을 때 업그레이드를 위해 PLOS를 업데이트하는 경우가 많습니다. 이 절에서는 PLOS를 업데이트 하는 방법을 살펴봅니다.



**주의:** PLOS의 버전에 따라 이러한 방법으로도 복구되지 않는 설정이 일부 있을 수 있습니다. 이러한 설정은 PLOS를 업데이트한 후 다시 설정 작업을 해야 합니다.

## PLOS 업데이트

PLOS를 업데이트하는 방법에는 업데이트 서버에 연결하는 방법과 사용자 PC에 저장된 파일을 업로드하는 방법이 있습니다. PLOS를 업데이트하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 국가별 IP</b> 메뉴를 클릭합니다.
2-1	<p>방법1: PLOS 네트워크 업데이트</p> <p>1) &lt;PLOS 네트워크 업데이트&gt;에 PLOS가 저장되어 있는 업데이트 서버의 URL을 입력한 후 <b>[업데이트]</b> 버튼을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>□ PLOS 네트워크 업데이트</p> <input style="width: 100%;" type="text"/> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px;">업데이트</span> </div>
2-2	<p>방법2: PLOS 파일 업데이트</p> <p>1) &lt;PLOS 파일 업데이트&gt;에서 <b>[찾아보기...]</b> 버튼을 클릭합니다.</p> <p>2) 업데이트할 PLOS 파일을 선택한 후 <b>[파일업로드]</b> 버튼을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p>□ PLOS 파일 업데이트</p> <p style="text-align: center;"> <span style="border: 1px solid #ccc; padding: 2px 5px;">파일 선택</span> <span style="border: 1px solid #ccc; padding: 2px 5px;">선택된 파일 없음</span> <span style="float: right; border: 1px solid #ccc; padding: 2px 5px;">파일업로드</span> </p> </div> <p>3) PLOS 업로드 확인 팝업 창이 나타나면 <b>[확인]</b> 버튼을 클릭합니다.</p> <p>4) PLOS 업데이트 진행 확인 팝업 창이 나타나면 <b>[적용]</b> 버튼을 클릭합니다.</p>
3	PLOS의 업데이트가 성공적으로 끝나면 시스템 재부팅을 묻는 팝업 창이 나타납니다. <b>[확인]</b> 버튼을 클릭합니다.



**주의:** 상위 버전에서 하위 버전으로 다운그레이드 하는 경우, 반드시 시스템의 설정을 초기화한 후에 진행합니다.

## PLOS 버전 정보 조회

WEBFRONT-K에 설치되어 있는 PLOS의 버전을 확인하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - PLOS 관리</b> 메뉴를 클릭합니다.
2	<p>&lt;PLOS 버전 정보&gt;에서 PLOS 버전을 확인합니다.</p> <ul style="list-style-type: none"> <li>• 현재 PLOS 버전            WEBFRONT-K에 설치되어 있는 PLOS 버전이 출력됩니다.</li> <li>• 최신 PLOS 버전            최신 PLOS 버전이 출력됩니다.</li> </ul>

## PLOS 릴리스 노트 다운로드

PLOS 릴리스 노트는 WEBFRONT-K의 최신 PLOS와 관련된 정보를 제공하는 문서로 릴리스되는 PLOS에 포함된 주요 기능 및 주의 사항들이 설명되어 있습니다. PLOS 릴리스 노트를 다운로드하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - PLOS 관리</b> 메뉴를 클릭합니다.
2	<다운로드 PLOS 릴리즈 노트>에서 다운로드할 서버의 URL을 입력한 후 [다운로드] 버튼을 클릭합니다. 

## 시간 관리

WEBFRONT-K에서 발생한 각종 이벤트나 장애, 사용자에게 의해 실행된 명령 등이 로그로 기록될 때마다 당시의 시스템 시간이 함께 기록됩니다. 이러한 로그들은 시스템에 문제가 발생했을 때 문제를 해결하기 위한 중요한 자료로 사용되므로 시스템의 시간을 정확하게 유지하는 것은 매우 중요합니다.

WEBFRONT-K의 시간은 사용자가 직접 지정할 수도 있고, NTP 클라이언트 기능을 사용하여 주기적으로 NTP 서버로부터 정확한 시간을 받아온 후 자동으로 시간을 맞출 수도 있습니다.

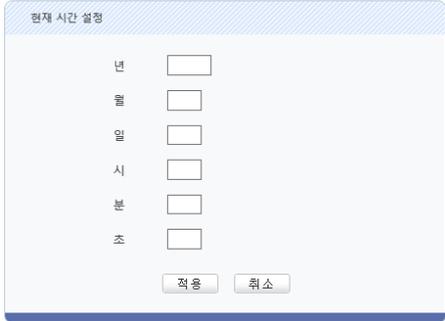
### NTP(Network Time Protocol) 서버

NTP(Network Time Protocol)는 네트워크에 연결된 장비들의 시간을 동기화 시킬 수 있게 해주는 프로토콜입니다. WEBFRONT-K는 NTP 프로토콜을 사용하여 시스템의 시간을 설정할 수 있는 NTP 클라이언트 기능을 지원합니다. NTP 클라이언트 기능이 활성화된 장비들은 NTP 서버로 시간 정보를 요청합니다. 그리고, NTP 서버로부터 받은 시간 정보와 장비의 현재 시간을 비교한 후 차이가 있을 경우에는 그 차이를 조정하여 장비의 시간을 정확하게 맞춥니다. 이러한 과정은 지정된 주기마다 반복되므로 NTP 클라이언트 기능이 활성화되어 있는 장비는 시스템 시간을 계속해서 정확하게 유지할 수 있습니다. WEBFRONT-K에는 이러한 NTP 클라이언트 기능이 기본적으로 비활성화되어 있고, NTP 서버도 설정되어 있지 않습니다.

WEBFRONT-K는 이전 동기화 이후 NTP 서버와의 시간 차이가 큰 경우 16초 간격으로 동기화를 수행하고, 시간 차이가 작은 경우에는 256초 간격으로 동기화를 수행합니다.

### 직접 시스템 시간 설정하기

사용자가 직접 WEBFRONT-K의 시간을 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 시간 관리</b> 메뉴를 클릭합니다.
2	<현재 시간>의 [변경] 버튼을 클릭합니다.
3	<현재 시간 설정> 팝업 창에서 년, 월, 일, 시, 분, 초를 입력한 후 [적용] 버튼을 클릭합니다. 

### 시간대 조정하기

WEBFRONT-K의 시간대(Time Zone)는 기본적으로 한국의 시간대에 맞게 GMT 시간보다 9시간 늦은 GMT +9로 설정되어 있습니다. WEBFRONT-K를 사용하고 있는 지역에 맞도록 시간대를 변경하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 시간 관리</b> 메뉴를 클릭합니다.
2	<GMT 시간차>의 [변경] 버튼을 클릭합니다.

<GMT 시간차 설정> 화면에서 GMT 시간차 항목에 GMT 시간으로부터의 시차를 -12 ~ +13 범위의 값으로 입력하고 [적용] 버튼을 클릭합니다. (기본값: 9시간)

3

## NTP 서버 사용하기

NTP 서버로부터 시간 정보를 받아오도록 하기 위해 WEBFRONT-K를 NTP 클라이언트로 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 일반설정 - 시간 관리 메뉴를 클릭합니다.
2	<NTP 클라이언트 설정>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;NTP 클라이언트 설정&gt; 화면에서 다음 설명을 참고하여 각 항목에 값을 입력하고 [적용] 버튼을 클릭합니다.</p> <ul style="list-style-type: none"> <li>• <b>간격 설정</b> NTP 서버로부터 시간 정보를 수신하는 간격 (설정 범위: 0 ~ 59(분), 기본값: 비활성화) '활성화'로 선택한 경우 아래 항목을 선택합니다. <ul style="list-style-type: none"> <li>- <b>요일</b>: NTP 서버에 접속할 요일을 지정합니다. (기본값: 전체 요일)</li> <li>- <b>날짜</b>: NTP 서버에 접속할 날짜를 지정합니다. 여러 개 입력시 ';' (쉼표)로 구분합니다. 예를들어 1일, 2일, 3일 지정시 '1,2,3'으로 입력합니다. (설정 범위: 1~31, 기본값: * (매일))</li> <li>- <b>시</b>: NTP 서버에 접속할 시간을 지정합니다. 여러 개 입력시 ';' (쉼표)로 구분합니다. (설정 범위: 1~24, 기본값: * (매시간))</li> <li>- <b>간격</b>: NTP 서버 접속 시간 간격을 지정합니다. (기본값: 30분)</li> </ul> </li> </ul> <p> <b>참고</b> 간격 설정시 참고 사항입니다. 요일과 날짜는 각 설정대로 동작하지만, 한 개라도 '전체'를 선택하면 일부분으로 지정된 요일 또는 날짜가 적용됩니다.</p> <ul style="list-style-type: none"> <li>• 요일- 화, 수, 목, 날짜- 10일, 20일 설정시: 매주 화/수/목요일과 10일, 20일에 모두 실행</li> <li>• 요일- *(전체), 날짜- 10일, 20일 설정시: 10일, 20일에 실행</li> <li>• 요일- 토, 일, 날짜- *(전체) 설정시: 매주 토/일요일에 실행</li> </ul> <ul style="list-style-type: none"> <li>• <b>상태</b> NTP 클라이언트 기능 상태 (기본값: 비활성화)</li> <li>• <b>NTP 서버 IP 주소 (primary)</b> NTP 서버의 Primary IP 주소</li> <li>• <b>NTP 서버 IP 주소 (secondary)</b> NTP 서버의 Secondary IP 주소</li> </ul>

# DNS 관리

이 절에서는 DNS(Domain Name System)에 대해 소개하고, WEBFRONT-K에 DNS와 관련된 설정 작업을 수행하는 방법을 살펴봅니다.

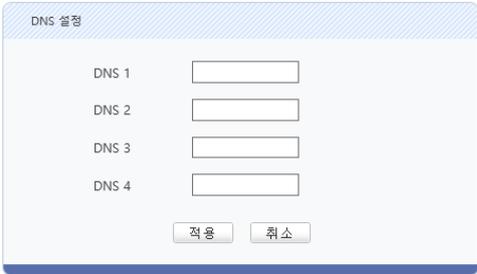
## 개요

DNS(Domain Name System)는 호스트의 이름이나 도메인 이름을 실제 IP 주소로 변환해주는 시스템입니다. WEBFRONT-K에 DNS 서버를 등록하면 사용자는 ping, telnet, traceroute 등의 IP 주소를 이용한 명령을 실행할 때, 복잡한 IP 주소 대신 호스트 이름을 사용하여 보다 편리하게 여러 가지 작업을 수행할 수 있습니다. DNS 서비스를 사용하려면 먼저 사용자의 네트워크에서 사용할 DNS 서버를 등록해야 합니다.

WEBFRONT-K에는 기본 DNS 서버와 보조 DNS 서버를 등록할 수 있습니다. WEBFRONT-K는 먼저 기본 DNS 서버에 DNS 쿼리를 전송하고, 기본 DNS 서버에서 응답이 없을 경우, 보조 DNS 서버에게 쿼리를 전송합니다. WEBFRONT-K에는 하나의 기본 DNS 서버와 3개의 보조 DNS 서버를 지정할 수 있습니다. 기본적으로 DNS 서비스는 기본 DNS 서버가 사용되고, 기본 DNS 서버가 정상적으로 동작하지 않을 때에는 추가한 순서대로 보조 DNS 서버가 사용됩니다.

## DNS 설정하기

WEBFRONT-K의 DNS를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 일반설정 - DNS 관리 메뉴를 클릭합니다.
2	<DNS 설정>의 [변경] 버튼을 클릭합니다.
3	<DNS 설정> 팝업 창에서 DNS 서버의 IP 주소를 입력하고 [적용] 버튼을 클릭합니다. 

## 리포터 설정

리포터는 WEBFRONT-K의 리포팅(reporting) 도구인 WEBFRONT-K Analyzer를 의미합니다. WEBFRONT-K Analyzer는 수집된 각종 보안 정보를 분석하여 다양한 종류의 상세 보고서와 추세 분석 보고서를 만들어 이를 관리자에게 일정 기간마다 자동으로 보내줍니다. WEBFRONT-K Analyzer는 별도로 서버에 설치할 수 있는데, **System - AV2** 메뉴를 사용하여 WEBFRONT-K Analyzer가 설치된 서버로 접속할 수 있습니다.

WEBFRONT-K Analyzer로 접속하여 그 기능을 사용하거나 WEBFRONT-K와 WEBFRONT-K Analyzer가 서로 필요한 정보를 주고 받기 위해서는 리포터 관리 메뉴를 사용하여 다음과 같은 정보를 설정해주어야 합니다.

- 리포터의 IP 주소
- 설치되어 있는 리포터의 버전
- 프로토콜
- WEBFRONT-K에서 리포터로 로그를 전송할 때 암호화 기능 사용 여부
- 암호화 기능에 사용될 암호화 키

이 절에서는 위와 같은 정보를 설정하는 방법에 대해 살펴봅니다.

### 리포터 IP 정보 설정

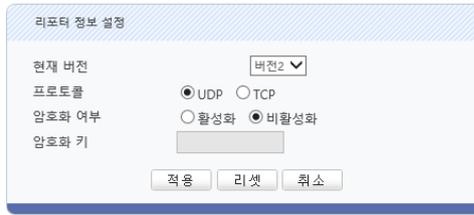
WEBFRONT-K에 여러 대의 리포터 서버를 등록할 수 있습니다. 리포트는 **System - AV2** 메뉴에서 리포터 IP 주소별로 확인할 수 있습니다. 다음은 리포터의 IP 주소를 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 리포터 설정</b> 메뉴를 클릭합니다.
2	<리포터 IP 정보> 의 [변경] 버튼을 클릭합니다.
3	<p>&lt;리포터 IP 설정&gt; 팝업 창에서 리포터 서버의 IP 주소를 입력하고 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  <p>리포터 IP 설정</p> <p>리포터 IP주소 1 <input type="text"/></p> <p>리포터 IP주소 2 <input type="text"/></p> <p>리포터 IP주소 3 <input type="text"/></p> <p>리포터 IP주소 4 <input type="text"/></p> <p>리포터 IP주소 5 <input type="text"/></p> <p>리포터 IP주소 6 <input type="text"/></p> <p>리포터 IP주소 7 <input type="text"/></p> <p>리포터 IP주소 8 <input type="text"/></p> <p>[적용] [리셋] [취소]</p> </div> <p> <b>주의:</b> 리포터 IP 주소 설정 시, 위에서부터 순서대로 입력해야 합니다. 만약 중간에 비어 있는 항목이 있으면, 빈 항목 이전까지의 설정만 적용됩니다.</p>

### 리포터 관련 정보 설정

다음은 리포터로 접속하고 사용하는 데 필요한 정보를 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 리포터 설정</b> 메뉴를 클릭합니다.
2	<리포터 정보>의 [변경] 버튼을 클릭합니다.
3	<리포터 정보 설정> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용]버튼을 클릭합니다.



- **현재 버전** 설치되어 있는 리포터의 버전을 선택합니다. (현재는 '버전2'만 선택 가능합니다.)
- **프로토콜** 로그 전송 시 사용할 프로토콜을 지정합니다. (기본값: UDP)
- **암호화 여부** 로그 정보 전송시 암호화할 지의 여부를 선택합니다. 암호화하려면 활성화를 선택하고, 암호화하지 않으려면 비활성화를 선택합니다. (기본값: 비활성화)
- **암호화 키** 로그 정보를 암호화할 때 사용할 키 값을 입력합니다.

## 리포터 사용 여부 설정

기본적으로 리포터는 사용하지 않는 비활성화 상태로 설정되어 있기 때문에 리포터를 사용하려면 먼저 리포터를 활성화해야 합니다. 리포터를 활성화하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 리포터 설정</b> 메뉴를 클릭합니다.
2	<리포터 상태>의 [변경] 버튼을 클릭합니다.
3	<리포터 상태 설정> 팝업 창에서 활성화를 선택한 후 [적용] 버튼을 클릭합니다.



# E-mail 알람

## 개요

E-mail 알람은 관리자 로그인 실패, 로그 저장소(HDD) 포화, 무결성 검사 결과 변조 발생, 웹 변조 방지 기능에 등록된 웹 페이지의 변조 발생 이벤트 발생 시 관리자에게 경보 메일을 발송하는 기능입니다.

E-mail 알람 기능을 사용하기 위해서는 메일 발송을 위한 SMTP 서버와 보내는 사람, 받는 사람의 이메일 주소를 설정해야 합니다. WEBFRONT-K의 E-mail 알람 기능은 기본적으로 비활성화되어 있으며, 등록된 SMTP 서버 및 보내는 사람, 받는 사람 이메일 주소가 없습니다.

## E-mail 알람 설정하기

다음은 E-mail 알람 기능을 설정하는 방법입니다.

순서	설정 과정
1	System - 일반설정 - E-mail 알람 메뉴를 클릭합니다.
2	<E-mail 알람 정보>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;E-mail 알람 정보&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <p> <ul style="list-style-type: none"> <li>• 상태: E-mail 알람 기능의 활성화 여부를 선택합니다. (기본값: 비활성화)</li> <li>• 보내는 사람 이메일 주소: 이메일로 전송할 때 보내는 사람으로 사용할 이메일 주소를 입력합니다.</li> <li>• 받는 사람 이메일 주소: 경보 메일을 수신할 관리자의 이메일 주소를 입력합니다.</li> <li>• SMTP 서버 IP 주소: 경보 메일을 전송할 때 사용할 SMTP 서버의 IP 주소를 입력합니다.</li> <li>• SMTP 프로토콜: SMTP 프로토콜을 지정합니다. (설정 범위: SMTP, SMTPS, StartTLS, 기본값: SMTP)</li> <li>• SMTP 포트: SMTP 포트 번호를 지정합니다. (기본값: 25)</li> <li>• 인증: SMTP 서버에 대한 인증 여부를 선택합니다. 활성화 시, 계정 정보 필드가 출력됩니다. (기본값: 비활성화)</li> </ul> </p>

## 보안 이벤트 알람

다음은 보안 이벤트 알람 기능을 설정하는 방법입니다.

순서	설정 과정
1	System - 일반설정 - E-mail 알람 메뉴를 클릭합니다.
2	<보안 이벤트 알람>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;보안 이벤트 알람 설정&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div data-bbox="604 472 1082 694" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• 상태: 보안 이벤트 알람 기능의 활성화 여부를 선택합니다. (기본값: 비활성화)</li> <li>• 알람 통계 수집 간격: 알람 통계를 수집하는 시간 간격을 지정합니다. (설정 범위: 5 ~ 1,440(분), 기본값: 5)</li> <li>• 알람 발생 보안 이벤트 개수: 보안 이벤트의 임계치를 설정합니다. 알람 통계 수집 간격 시간동안 해당 임계치를 초과할 경우, 이메일로 알람 전송 로그 최대 개수만큼 로그를 전송합니다. (설정 범위: 1 ~ 10,000,000, 기본값: 1)</li> <li>• 알람 전송 로그 최대 개수: 이메일로 전송할 로그의 최대 개수를 설정합니다. (설정 범위: 1 ~ 1,000, 기본값: 0)</li> </ul>

# 무결성 검사

이 절에서는 무결성 검사 기능에 대해 소개한 후 무결성 검사를 사용하는 방법에 대해 설명합니다.

## 개요

무결성 검사는 WEBFRONT-K가 해킹으로 인해 보안 상 이상이 발생하였는지를 검사하고 판단하는 기능입니다. 무결성 검사는 WEBFRONT-K의 설정 정보와 동작 중인 프로그램이 비정상적으로 변조되었는지를 검사하여 이상 여부를 판단합니다. 무결성 검사를 활성화하면 먼저, 현재 설정과 프로그램 정보를 저장합니다. 그리고, 검사를 실시할 때마다 저장해둔 정보와 현재 정보를 비교하여 차이가 있는지를 확인합니다. Web Manager의 메뉴를 사용하여 정상적으로 설정을 변경하여 발생한 차이점은 무결성 검사에서 변조한 것으로 고려하지 않습니다.

저장해둔 정보와 현재 정보가 다른 경우(정상적인 설정 변경을 제외하)에는 변조가 발생한 것으로 간주하고 감사 로그를 생성함과 동시에 이를 화면에 표시해줍니다. 만약 정상적인 변경을 비정상적인 변조라고 판단한 경우에는 '업데이트' 기능을 통해 현재 설정 정보를 업데이트하고, 이 후에는 변조 여부를 확인할 때 이 정보를 사용하도록 할 수 있습니다.

무결성 검사는 사용자가 설정한 시간 간격마다 주기적으로 자동 수행되도록 할 수도 있고, 사용자가 필요할 때마다 수동으로 검사를 실시할 수도 있습니다.

## 무결성 검사 설정하기

### 무결성 검사 활성화하기

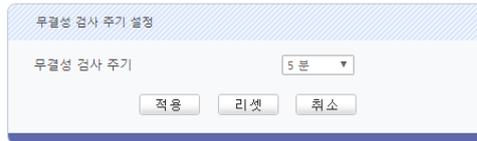
기본적으로 무결성 검사는 비활성화 상태로 설정되어 있습니다. 자동 기능이든 수동 기능이든 무결성 검사를 수행하려면 먼저 무결성 검사를 활성화해야 합니다. 무결성 검사를 활성화하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 무결성 검사</b> 메뉴를 클릭합니다.
2	<무결성 검사 상태>의 [변경] 버튼을 클릭합니다.
3	<무결성 검사 상태 설정> 팝업 창에서 상태 항목을 '활성화'로 선택하고 [적용] 버튼을 클릭합니다. 
4	무결성 검사 상태가 활성화로 표시되고, 설정 파일 리스트와 프로그램 리스트에 변조 여부를 감시할 설정 파일과 프로그램 이름이 표시됩니다. 

## 자동 무결성 검사 주기 설정하기

무결성 검사를 활성화하고 무결성 검사 주기를 설정하면 설정된 주기마다 무결성 검사가 자동으로 수행됩니다. 기본적으로 무결성 검사가 활성화되면 5분 간격으로 무결성 검사를 실시하도록 설정되어 있습니다. 기존에 설정되어 있는 무결성 검사의 검사 주기를 변경하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 일반설정 - 무결성 검사</b> 메뉴를 클릭합니다.
2	<무결성 검사 주기>의 [변경] 버튼을 클릭합니다.
3	<무결성 검사 주기 설정> 팝업 창에서 드롭다운 목록을 클릭한 후 원하는 주기를 선택하고 [적용] 버튼을 클릭합니다. (설정 범위: 5, 10, 30, 60, 기본값: 5분)



## 자동 무결성 검사 해제하기

자동 무결성 검사를 해제하려면 앞의 자동 무결성 검사 주기 설정하기를 참고하여 무결성 검사 주기를 '비활성화'로 설정합니다.

## 수동으로 무결성 검사하기

수동 무결성 검사는 원하는 설정 파일이나 프로그램의 변조 여부를 즉시 검사할 수 있는 기능입니다. 수동 무결성 검사는 다음과 같은 방법으로 수행할 수 있습니다.

순서	설정 과정
1	<b>System - 일반설정 - 무결성 검사</b> 메뉴를 클릭합니다.
2	<설정파일 리스트>나 <프로그램 리스트>에서 무결성 검사를 실시할 설정 파일이나 프로그램을 선택하고 [무결성 검사] 버튼을 클릭합니다. 선택시 [Ctrl] 키나 [Shift] 키를 사용하면 여러 개의 설정 파일 또는 프로그램을 선택할 수 있습니다.

## 무결성 검사 결과 확인하기

무결성 검사가 수행되고 나면, 그 결과가 리스트의 상태 항목에 표시됩니다. 무결성 검사 결과 변조된 부분이 발견되지 않았으면 '정상'으로, 발견되었으면 '변조'로 표시됩니다.

검사 결과가 '변조'로 표시된 경우에는 정상적으로 변경한 설정이 무결성 검사에서 변조로 판단한 것은 아닌지 조사합니다. 만약 정상적인 변경이었다면, [업데이트]나 [전목록 업데이트] 버튼을 클릭하여 이 후에는 해당 변경 사항을 정상 변경으로 인식하도록 해야 합니다.

실제로 해당 정보가 변조되었다면 감사 로그를 분석하여 적절한 조치를 취해야 합니다. 변조가 발생한 경우, **통합로그-감사/시스템 로그** 메뉴에서 다음과 같이 변조된 파일이나 프로그램을 확인할 수 있습니다.

2018/08/23 14:18:10 wfadmin 프로그램이 변조되었습니다 <span style="float:right">성공</span>					
No.	42	날짜	2018/08/23 14:18:10	사용자 아이디	wfadmin
분류	설정	애플리케이션	-	App 아이디	-
메시지	프로그램이 변조되었습니다				
데이터	user="wfadmin",user_ip="192.168.231.70",param_file="ospsfd",result="1",error="0"				
결과	성공	Error code	-	대상	-
2018/08/23 14:18:04 wfadmin 설정파일이 변조되었습니다 <span style="float:right">성공</span>					
No.	39	날짜	2018/08/23 14:18:04	사용자 아이디	wfadmin
분류	설정	애플리케이션	-	App 아이디	-
메시지	설정파일이 변조되었습니다				
데이터	user="wfadmin",user_ip="192.168.231.70",param_file="time.conf",result="1",error="0"				
결과	성공	Error code	-	대상	-

# 환경 변수

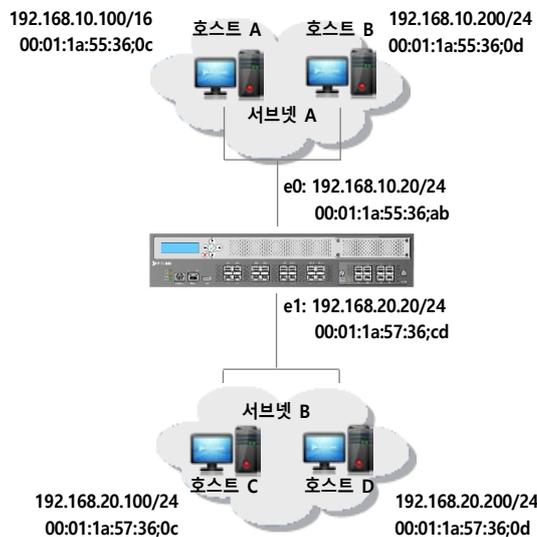
## 프록시 ARP

이 절에서는 프록시 ARP에 대해 소개한 후 WEBFRONT-K에서 프록시 ARP 기능을 활성화하는 방법을 설명합니다.

### 개요

ARP(Address Resolution Protocol)는 네트워크상에서 IP 주소와 물리적인 주소(MAC 주소)를 대응시키기 위해 사용되는 프로토콜입니다. 프록시 ARP는 라우터의 서로 다른 인터페이스에 연결된 호스트가 라우터와 같은 네트워크에 있을 때 호스트 대신 라우터가 ARP 응답을 해주는 기능입니다. 라우터가 ARP 응답을 전송하기 때문에 ARP를 요청한 호스트는 라우터를 목적지 호스트로 판단하고 데이터를 전송하고, 라우터는 실제 목적지 호스트로 데이터를 전송하게 됩니다.

아래와 같이 WEBFRONT-K에 서브넷 A와 서브넷 B가 연결되어 있는 네트워크 구성에서 서브넷 A에 있는 호스트 A가 서브넷 B에 있는 호스트 D로 패킷을 전송하려는 경우를 예로 들어 프록시 ARP의 동작 과정을 보다 상세하게 살펴봅니다.



호스트 A는 호스트 D로 패킷을 전송하기 전에 ARP 요청 패킷을 전송하여 호스트 D의 MAC 주소를 알아내야 합니다. 호스트 A는 넷마스크 비트가 16이기 때문에 IP 주소가 192.168.20.200인 호스트 D를 포함하여 192.168.0.0 대역의 모든 호스트가 같은 네트워크에 속해 있다고 판단합니다. 그래서, 호스트 D에 대한 ARP 요청을 서브넷 A에 브로드캐스팅합니다.

호스트 A가 브로드캐스팅한 ARP 요청은 WEBFRONT-K의 e0 인터페이스를 포함한 서브넷 A에 속한 모든 호스트에게 전송되지만, 다른 서브넷으로는 전송되지 않으므로 서브넷 B에 있는 호스트 D까지 전달될 수 없습니다. 따라서, 호스트 A는 호스트 D로부터 ARP 응답을 받지 못해 패킷을 전송할 수 없게 됩니다. 하지만, 만약 WEBFRONT-K에 프록시 ARP 기능이 활성화되어 있고 WEBFRONT-K의 라우팅 테이블에 호스트 D가 속한 네트워크의 경로가 존재한다면, WEBFRONT-K는 호스트 A로부터 호스트 D에 대한 ARP 요청을 수신했을 때 자신의 MAC 주소(00:01:1a:55:36:ab)가 담긴 ARP 응답을 호스트 A에게 전송합니다. 이 응답을 받은 호스트 A는 호스트 D에게 보내려고 하는 패킷을 00:01:1a:55:36:ab MAC 주소로 전송하게 되고, 패킷을 수신한 WEBFRONT-K는 라우팅 테이블의 정보를 이용하여 이 패킷을 다시 호스트 D로 보내게 됩니다.

이와 같이 프록시 ARP 기능은 다른 네트워크에 있는 호스트를 마치 같은 네트워크에 있는 호스트처럼 통신할 수 있게 해줍니다. 하지만, 프록시 ARP 기능은 라우팅 테이블에 목적지 호스트로의 경로가 있지만 확인하고 실제 목적지 호스트가 존재하는지는 확인하지 않기 때문에 실제로 존재하지 않는 호스트에 대한 ARP 요청까지 응답할 수도 있습니다. 그리고, WEBFRONT-K로 전송하는 ARP 요청을 가로채어 잘못된 ARP 응답을 요청하는 스푸핑 공격의 대상이 될 수도 있습니다.

## 프록시 ARP 활성화하기

기본적으로 WEBFRONT-K에는 프록시 ARP 기능이 동작하지 않습니다. 프록시 ARP 기능을 동작시키거나 혹은 동작 중인 프록시 ARP 기능을 중단시키고자 할 때에는 다음과 같은 과정을 수행하면 됩니다.

순서	설정 과정
1	System - 네트워크 - 환경변수 메뉴를 클릭합니다.
2	<프록시 ARP>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;프록시 ARP 설정&gt; 화면에서 '활성화'를 선택하고 [적용] 버튼을 클릭합니다. (기본값: 비활성화)</p> 

## 저장 MAC 응답

### 개요

저장 MAC 응답 기능은 클라이언트가 전송한 요청 패킷의 출발지 MAC 주소와 목적지 MAC 주소를 저장해두었다가 응답 패킷을 전송할 때 저장된 MAC 주소를 그대로 사용합니다. 저장 MAC 응답 기능을 사용하지 않으면 응답 패킷을 보낼 때마다 라우팅을 수행합니다.

저장 MAC 응답 기능은 WEBFRONT-K의 성능을 향상시키고자 할 때 사용합니다. 저장 MAC 응답 기능을 사용하면 응답 패킷을 보낼 때 라우팅을 수행하지 않으므로 WEBFRONT-K의 성능이 눈에 띄게 높아지는 것을 느낄 수 있습니다.

저장 MAC 응답 기능을 사용하기 위해서는 요청 패킷의 출발지/목적지 MAC 주소가 응답 패킷에 그대로 사용할 수 있는 환경이어야 합니다. 기본적으로 저장 MAC 응답 기능은 비활성화 되어 있습니다.

### 저장 MAC 응답 기능 활성화하기

다음은 저장 MAC 응답 기능 상태를 설정하는 방법입니다.

순서	설정 과정
1	System - 네트워크 - 환경변수 메뉴를 클릭합니다.
2	<저장 MAC 응답>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;저장 MAC 응답 설정&gt; 화면에서 '활성화'를 선택하고 [적용] 버튼을 클릭합니다. (기본값: 비활성화)</p> 

# HTTP 파라미터

## 개요

HTTP 요청 및 응답에는 다양한 파라미터 속성값이 포함되어 있습니다. 관리자는 WEBFRONT-K에서 다음과 같은 HTTP 파라미터 항목을 설정할 수 있습니다.

- **HTTP 요청 타임아웃** 3-way Handshake 이후, 요청이 도착하기까지의 타임아웃 시간입니다. 지정시간 이내에 요청이 도착하지 않을 경우, 세션 정보가 삭제됩니다.
- **HTTP 요청 헤더 최대 길이** WEBFRONT-K에서 허용하는 HTTP 요청 헤더의 최대 길이입니다. 허용 범위를 초과한 요청에 대해서는 보안 기능이 동작하지 않습니다.
- **HTTP 응답 헤더 최대 길이** WEBFRONT-K에서 허용하는 HTTP 응답 헤더의 최대 길이입니다. 허용 범위를 초과한 응답에 대해서는 보안 기능이 동작하지 않습니다.

## HTTP 요청/응답 헤더의 길이 설정 하기

다음은 HTTP 요청/응답 헤더의 길이를 설정하는 방법입니다.

순서	설정 과정
1	System - 네트워크 - 환경변수 메뉴를 클릭합니다.
2	<HTTP 파라미터>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;HTTP 파라미터 설정&gt;화면에서 다음 정보를 입력한 후 [적용] 버튼을 클릭합니다.</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>□ HTTP 파라미터 설정</p> <p>HTTP 요청 타임아웃 <input type="text" value="40"/> 초</p> <p>HTTP 요청 헤더 최대 길이 <input type="text" value="16384"/> 바이트</p> <p>HTTP 응답 헤더 최대 길이 <input type="text" value="16384"/> 바이트</p> <p style="text-align: right;"> <input type="button" value="적용"/> <input type="button" value="리셋"/> <input type="button" value="취소"/> </p> </div> <ul style="list-style-type: none"> <li>• <b>HTTP 요청 타임아웃</b> HTTP 요청이 도착하기까지의 타임아웃 시간을 지정합니다. (설정 범위: 10 ~ 3600, 기본값: 40)</li> <li>• <b>HTTP 요청 헤더 최대 길이</b> HTTP 요청 헤더의 최대 길이를 지정합니다. (설정 범위: 16,384~4,194,304, 기본값: 16,384)</li> <li>• <b>HTTP 응답 헤더 최대 길이</b> HTTP 응답 헤더의 최대 길이를 지정합니다. (설정 범위: 16,384~4,194,304, 기본값: 16,384)</li> </ul>

## 부팅 중 포트 상태

### 개요

부팅 중 포트 상태는 WEBFRONT-K의 전원이 켜진 이후, 포트가 활성화(Up)되는 시점을 설정하는 기능입니다. 관리자는 다음과 같은 2가지의 시점 중 하나를 선택할 수 있습니다.

- **부팅 중 포트 상태 UP** 부팅이 진행되는 과정에서 포트가 활성화됩니다.
- **부팅 중 포트 상태 Down** 부팅이 완료되고 기존 설정이 복원된 이후에 포트가 활성화됩니다.

기본적으로 WEBFRONT-K의 부팅 중 포트 상태는 활성화로 지정되어 있습니다.

### 부팅 중 포트 상태 설정하기

다음은 부팅 중 포트 상태를 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 네트워크 - 환경변수</b> 메뉴를 클릭합니다.
2	<부팅 중 포트 상태>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<부팅 중 포트 상태 설정>에서 상태를 지정한 후 <b>[적용]</b> 버튼을 클릭합니다. (기본값: UP) 

# TOS 설정

## 개요

TOS 설정은 보안 검사 대상이 되는 패킷의 IP 헤더에 ToS(Type of Service)를 설정하는 기능입니다. TOS 상태를 활성화하면 IP헤더의 ToS에 바운더리 값(ALL, 서버, 클라이언트)이 설정됩니다. 바운더리 값은 포트를 통해 전송되는 패킷의 방향으로 이 값이 서버인 패킷은 서버로 전송되어야 하고, 클라이언트인 패킷은 클라이언트로 전송되어야 합니다. 만약 패킷의 전송 방향이 이 값과 다르면 차단됩니다. 바운더리 값은 **System - 네트워크 - 포트 바운더리** 메뉴에서 설정합니다

이 기능은 네트워크 환경에서 VLAN의 트랜스패런트 브릿지 모드가 활성화 되어 있을 때 불필요한 패킷 플루딩(Flooding)으로 인해 맥 플래핑(MAC Flapping)이 발생하는 것을 방지하기 위해 사용됩니다.

## TOS 상태 설정하기

다음은 TOS 상태를 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 네트워크 - 환경변수</b> 메뉴를 클릭합니다.
2	<TOS>의 <b>[변경]</b> 버튼을 클릭합니다.
3	<TOS 설정>에서 상태를 지정한 후 <b>[적용]</b> 버튼을 클릭합니다. (기본값: 비활성화) 
	 <b>주의:</b> 네트워크 망에서 ToS 값으로 4와 12를 사용할 경우, TOS 상태를 비활성화해야 합니다.

# 통계 기간 설정

## 개요

WEBFRONT-K의 모니터링 기능과 보고서 기능은 WEBFRONT-K에 축적되어 있는 통계 데이터를 기반으로 제공됩니다. 따라서 특정 기간에 대해 모니터링 하거나 보고서를 생성하려면, 해당 기간 동안의 데이터가 WEBFRONT-K에 남아 있어야 합니다.

관리자는 통계 기간 설정 기능을 통해 데이터가 저장되는 기간을 일 단위로 설정할 수 있습니다. 기본적으로 통계 데이터가 저장되는 기간은 3일입니다.

## 통계 기간 설정하기

다음은 통계 기간을 설정하는 방법입니다.

순서	설정 과정
1	System - 일반설정 - 통계 기간 설정 메뉴를 클릭합니다.
2	<통계 기간 설정>의 [변경] 버튼을 클릭합니다.
3	<통계 기간 설정> 팝업 창에서 통계 기간을 지정한 후 [적용] 버튼을 클릭합니다. (설정 범위: 1 ~ 62(일), 기본값: 3) 

# 시스템 관리 설정

WEBFRONT-K가 부팅되면 관리자는 관리 서비스를 통해 장비를 설정할 수 있습니다. 관리 접근 서비스의 종류에는 HTTPS(Web Manager)를 이용하는 GUI(Graphic User Interface)와 SSH, Telnet와 같은 CLI(Command Line Interface)가 있습니다.

이 절에서는 WEBFRONT-K와 관리자 PC 사이의 관리 서비스 통신에 사용되는 웹매니저, SSH, Telnet 서비스를 설정하는 방법을 설명합니다.

## 웹 매니저 설정

관리자가 Web Manager에 접속 시, 관리자의 PC와 WEBFRONT-K는 SSL(Secure Socket Layer)을 이용한 암호화 통신을 수행합니다. 만약 공격자가 관리자 PC와 WEBFRONT-K 사이에서 송수신되는 패킷을 탈취하여도 모든 데이터가 암호화되어 있기 때문에 내용 확인이 불가능합니다.

이와 같이 Web Manager로의 모든 접속은 SSL을 이용하도록 설계되어 있으며, 관리자는 네트워크 환경에 적합한 SSL 프로토콜과 SSL 암호 알고리즘을 선택할 수 있습니다. 다음은 SSL 프로토콜과 SSL 암호 알고리즘을 설정하는 방법입니다.

순서	설정 과정
1	<b>System - 일반설정 - 시스템 관리 설정</b> 메뉴를 클릭합니다.
2	<웹매니저 설정>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;웹매니저 설정&gt;에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>□ 웹매니저 설정</p> <p>SSL 프로토콜 <input type="text" value="+ALL -SSLv2 -SSLv3"/></p> <p>SSL 암호알고리즘 <input type="text" value="ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-AES128-GCM-SHA256:AES128-SHA"/></p> <p>Management 포 <input type="text" value="8443"/> ( 포트 범위 : 1 ~ 65535 )</p> <p style="text-align: right;"><input type="button" value="적용"/> <input type="button" value="취소"/></p> </div> <ul style="list-style-type: none"> <li>• <b>SSL 프로토콜</b>                    SSL 프로토콜을 지정합니다. (기본값: +ALL -SSLv2)</li> <li>• <b>SSL 암호알고리즘</b>            SSL 암호 알고리즘을 지정합니다. (기본값: ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:AES128-SHA)</li> <li>• <b>Management 포트</b>            Web Manager에 접속할 때 사용할 포트 번호를 입력합니다. (설정 범위: 1~65535, 기본값: 8443)</li> </ul>

**주의:** SSL 프로토콜 및 암호 알고리즘 설정 시, 다음 사항을 확인합니다.

- SSL 프로토콜 항목에 비정상적인 값이 존재하거나 유효한 값이 하나도 존재하지 않는 경우, 설정이 적용되지 않습니다.
- SSL 암호 알고리즘 항목에는 최소 1개 이상의 유효한 암호 알고리즘이 존재해야 합니다.

## SSH 설정

다음은 원격에서 SSH 관리 서비스로 접속할 때 사용할 포트 번호를 지정하는 방법을 설명합니다.

순서	설정 과정
1	<b>System - 일반설정 - 시스템 관리 설정</b> 메뉴를 클릭합니다.
2	<SSH 설정>의 [변경] 버튼을 클릭합니다.
3	<SSH 설정>에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.

• SSH 포트

SSH 관리 접속 시 사용할 포트 번호를 입력합니다. (설정 범위: 1~65535, 기본값: 22)

## Telnet 설정

다음은 원격에서 Telnet 관리 서비스로 접속할 때 사용할 포트 번호를 지정하는 방법을 설명합니다.

순서	설정 과정
1	System - 일반설정 - 시스템 관리 설정 메뉴를 클릭합니다.
2	<Telnet 설정>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;Telnet 설정&gt;에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div data-bbox="582 719 1109 875" data-label="Form"> </div> <ul style="list-style-type: none"> <li>• Telnet 상태: Telnet 관리 접속 서비스의 사용 여부를 지정합니다. (기본값: 활성화)</li> <li>• Telnet 포트: Telnet 관리 접속 시 사용할 포트 번호를 입력합니다. (설정 범위: 1~65535, 기본값: 23)</li> </ul>

## 호스트 이름 설정

WEBFRONT-K의 호스트 이름은 EMS(Equipment Management System)이나 NMS(Network Management System)에서 장비를 구분할 때 사용되고, 터미널 프로그램을 통해 장비에 접속했을 때 어떤 장비에 접속했는지 나타낼 때에도 사용됩니다.



WEBFRONT-K에 기본적으로 지정되는 호스트 이름은 'WEBFRONT-K'입니다. 여러 대의 WEBFRONT-K가 사용 중이거나 네트워크 상에 많은 장비가 있는 경우, 용도나 설치된 위치 등의 정보를 사용하여 호스트 이름을 지정해두면 각 WEBFRONT-K를 쉽게 구분할 수 있어 편리합니다. WEBFRONT-K의 호스트 이름은 다음과 같은 과정을 통해 변경할 수 있습니다.

순서	설정 과정
1	<b>System - 일반설정 - 호스트이름 설정</b> 메뉴를 클릭합니다.
2	<호스트이름>의 [변경] 버튼을 클릭합니다.
3	<호스트이름> 화면에서 새로 지정할 호스트 이름을 입력하고 [적용] 버튼을 클릭합니다. 호스트 이름은 최대 8자까지 가능하며, 알파벳과 숫자, '_'의 조합으로 구성할 수 있습니다. 첫 글자는 반드시 알파벳이어야 합니다. 

## 시스템 재시작

WEBFRONT-K Web Manager에서는 연결되어 있는 WEBFRONT-K 장비를 원격으로 다시 시작할 수 있습니다. **System** 메뉴에서 **일반설정 - 시스템 재시작** 메뉴를 선택하면 <시스템 재시작> 화면이 나옵니다.



화면의 [재시작] 버튼을 누르면 연결된 WEBFRONT-K가 다시 부팅됩니다. WEBFRONT-K가 부팅되는 동안 WEBFRONT-K와의 접속이 끊어집니다. WEBFRONT-K로 접속하는 방법은 이 설명서의 [제1장 시작하기 전에 - 로그인/로그아웃하기] 절에 설명되어 있습니다.

# 제11장 네트워크

이 장에서는 WEBFRONT-K의 기본적인 네트워크 구성 작업에 대해 알아봅니다. 사용자의 네트워크 환경에 맞게 장비의 설정을 변경하려면 이 장의 내용을 참고하여 원하는 환경으로 구성하도록 합니다.

이 장은 다음 내용으로 구성됩니다.

- 포트 바운더리
- IP 주소
- VLAN
- 포트
- 링크싱크
- 미러링
- 트렁킹
- STP
- ARP

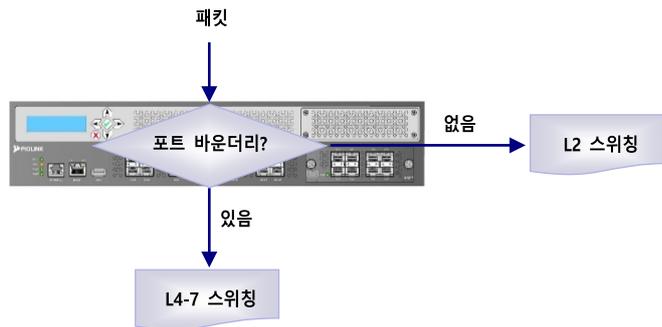


# 포트 바운더리

이 절에서는 WEBFRONT-K의 포트에 포트 바운더리를 설정해야 하는 이유에 대해 상세히 소개한 후, 포트 바운더리를 설정하는 방법에 대해 설명합니다.

## 개요

WEBFRONT-K의 기능 중에서 웹 보안 기능은 L4-7 스위칭을 통해서 수행됩니다. WEBFRONT-K는 수신되는 패킷 중에서 L4-7 스위칭이 필요한 패킷을 구분하기 위해 포트 바운더리(port boundary)를 사용합니다. 포트 바운더리가 설정되어 있는 포트에 수신된 패킷은 L4-7 스위칭을 수행하고, 포트 바운더리가 설정되어 있지 않은 패킷은 L2 스위칭으로만 처리합니다. 따라서, 웹 보안 기능을 적용해야 하는 패킷이 수신되는 포트에는 반드시 포트 바운더리를 설정해야 합니다. 다음 그림은 WEBFRONT-K로 패킷이 수신되었을 때 포트 바운더리의 설정 여부에 따라 패킷이 처리되는 과정을 보여줍니다.



위 그림에서와 같이 패킷이 수신되면 WEBFRONT-K는 먼저 패킷이 수신된 포트에 포트 바운더리가 설정되어 있는지를 확인합니다. 포트 바운더리가 설정되어 있지 않은 포트인 경우에는 L2 스위칭에 의해 처리하고, 포트 바운더리가 설정되어 있는 경우에는 L4-7 스위칭에 의해 패킷을 처리합니다.

## 포트 바운더리의 적용 범위 제한

기본적으로 포트 바운더리는 포트에 송수신되는 모든 패킷에 적용됩니다. 하지만, 필요한 경우에는 출발지(source)나 목적지(destination) IP 대역, 프로토콜 종류, VLAN ID와 같은 조건을 사용하여 포트 바운더리를 적용할 패킷을 구체적으로 지정할 수 있습니다.

- 출발지/목적지 IP 대역  
포트 바운더리에 출발지 IP 대역이나 목적지 IP 대역을 지정하면, 포트를 통해 전송하거나 수신하는 패킷 중에서 출발지 IP 주소나 목적지 IP 주소가 지정한 IP 대역에 속하는 패킷에만 포트 바운더리를 적용합니다.
- 프로토콜  
포트 바운더리에 TCP나 UDP, ICMP 프로토콜을 지정하면, 포트를 통해 송수신되는 패킷 중에서 지정한 프로토콜 종류의 패킷에만 포트 바운더리를 적용합니다.

이 조건들은 하나의 포트 바운더리에서 동시에 사용될 수 있습니다.

## 포트 바운더리의 ID

하나의 포트에는 여러 포트 바운더리가 적용될 수 있습니다. 그런 경우 WEBFRONT-K는 ID가 작은 순으로 포트 바운더리를 적용합니다. 여러 포트 바운더리가 적용된 포트에 패킷이 수신되면 WEBFRONT-K는 먼저 ID가 가장 작은 포트 바운더리를 확인합니다. 패킷이 그 포트 바운더리의 조건에 만족하지 않으면 WEBFRONT-K는 다음 포트 바운더리를 확인합니다. 만약, 패킷이 모든 포트 바운더리의 조건에 해당하지 않으면 포트 바운더리가 설정되어 있지 않은 포트에 수신된 패킷과 마찬가지로 L2 스위칭이 수행됩니다. 이와 같이 포트 바운더리의 ID는 우선 순위와 같은 역할을 합니다.

포트 바운더리의 ID를 지정할 때 유의할 사항은 설정 정보가 구체적인 포트 바운더리일수록 더 낮은(우선 순위는 높은) ID로 지정해야 한다는 점입니다. 다음과 같은 3개의 포트 바운더리에 ID를 설정하는 예를 살펴보도록 합니다.

- ❶ 출발지 IP 대역이 100.1.1.0/24인 포트 바운더리
- ❷ 출발지 IP 대역이 100.1.0.0/16인 포트 바운더리
- ❸ 출발지 IP 대역이 지정되지 않은 포트 바운더리

위 세 포트 바운더리가 하나의 포트에 동시에 적용되는 경우에는 포트 바운더리의 ID를 반드시 ❶ < ❷ < ❸ 이 되는 값으로 지정해야 합니다.

## Promisc 모드와 Include MAC 모드

기본적으로 포트 바운더리가 설정된 포트에 수신되는 모든 패킷은 L4-7 스위칭이 수행됩니다. 이들 패킷 중에서도 L4-7 스위칭이 필요하지 않은 패킷이 포함될 수 있습니다. 이러한 패킷들이 L4-7 스위칭 과정을 거치지 않도록 설정해주면 WEBFRONT-K의 부하를 덜어주어 더 나은 성능을 제공할 수 있습니다. 포트 바운더리가 설정된 포트에 수신된 패킷 중에서 어떤 패킷에 L4-7 스위칭을 수행하고 어떤 패킷에 수행하지 않을 지는 Promisc 모드와 Include MAC 모드를 사용하여 구분할 수 있습니다.

Promisc 모드는 포트에 수신되는 모든 패킷에 L4-7 스위칭을 수행할 것인지 아니면 특정한 패킷만 L4-7 스위칭을 수행하고 나머지 패킷은 포워딩할지를 나타냅니다. Promisc 모드는 on이나 off로 설정할 수 있습니다. Promisc 모드가 on인 포트 바운더리에 속한 포트에 수신되는 모든 패킷은 L4-7 스위칭이 수행됩니다. Promisc 모드가 off인 포트 바운더리에 속한 포트는 수신된 패킷 중에서 패킷의 목적지 MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는 패킷만 L4-7 스위칭이 수행됩니다.

Include MAC 모드는 L4-7 스위칭을 수행할 패킷의 종류(유니캐스트, 멀티캐스트, 브로드캐스트)를 나타냅니다. Include MAC 모드는 none, unicast, multi-broadcast로 설정할 수 있습니다. Include MAC 모드가 none인 이 포트 바운더리에 속한 포트는 promisc 모드의 설정에 따라 패킷의 L4-7 스위칭이 이루어집니다. Include MAC 모드가 unicast인 포트 바운더리에 속한 포트는 목적지 MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는 패킷과 유니캐스트 MAC 주소를 가진 패킷에 L4-7 스위칭이 수행됩니다. Include MAC 모드가 multi-broadcast인 포트 바운더리에 속한 포트는 멀티캐스트나 브로드캐스트 MAC 주소를 가진 패킷만 L4-7 스위칭이 수행됩니다.

다음은 promisc 모드와 Include MAC 모드에 따라 L4-7 스위칭이 수행되는 패킷을 정리한 표입니다.

Promisc 모드	Include MAC 모드	L4-7 스위칭이 수행되는 패킷
off	none	목적지 MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는 패킷
off	unicast	<ul style="list-style-type: none"> <li>• 목적지 MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는 패킷</li> <li>• 유니캐스트 MAC 주소를 가진 패킷</li> </ul>
off	multi-broadcast	멀티캐스트 혹은 브로드캐스트 MAC 주소를 가진 패킷
on	none	포트로 수신되는 모든 IP 패킷

Include MAC 모드를 unicast나 multi-broadcast로 지정한 경우에는 반드시 promisc 모드를 off로 설정해야 합니다. Promisc 모드를 off로 설정하고, Include MAC 모드를 multi-broadcast로 설정한 경우는 Include MAC 모드를 unicast로 설정한 경우와 달리, 목적지 MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는 패킷은 L4-7 스위칭이 수행되지 않습니다.

멀티캐스트나 브로드캐스트 MAC 주소를 가진 패킷과 이러한 패킷(목적지 MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는)의 L4-7 스위칭을 모두 수행하도록 설정하려면 다음과 같은 2개의 포트 바운더리를 정의해야 합니다.

- 포트 바운더리 1  
Promisc 모드'off', Include MAC 모드'none'
- 포트 바운더리 2  
Promisc 모드'off', Include MAC 모드'multi-broadcast'

다음은 4가지 포트 바운더리를 어떤 상황에서 사용해야 하는지를 나타낸 표입니다.

Promisc 모드	Include MAC 모드	이러한 설정이 사용되는 경우
off	none	<ul style="list-style-type: none"> <li>• WEBFRONT-K가 다음 홈이나 게이트웨이로 설정된 경우</li> <li>• 서버 부하 분산 서비스의 가상 IP로 접속하는 경우</li> </ul>
off	unicast	브리지 모드 네트워크 구성인 경우
off	multi-broadcast	서로 다른 VLAN 간에 멀티캐스트 패킷을 송수신하고자 하는 경우
on	none	모든 패킷에 L4-7 스위칭을 수행해야 하는 경우

## 포트 바운더리 설정 하기

WEBFRONT-K의 포트에 포트 바운더리를 설정하는 방법은 다음과 같습니다. 여러 개의 포트 바운더리를 추가하려면 3번 과정을 반복해서 수행합니다. WEBFRONT-K에는 최대 16개의 포트 바운더리(각 포트마다)를 정의할 수 있습니다.

순서	설정 과정
1	<b>System - 네트워크 - 포트 바운더리</b> 메뉴를 클릭합니다.
2	<포트 바운더리 정보> 화면에서 [추가] 버튼을 클릭합니다.
3	<p>&lt;포트 바운더리 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>아이디</b> 포트 바운더리의 ID를 입력합니다. (설정 범위: 1 ~ 16)</li> <li>• <b>포트</b> 포트 바운더리를 적용할 포트를 선택합니다.</li> <li>• <b>프로토콜</b> 드롭다운 목록을 클릭한 후 포트 바운더리를 적용할 패킷의 프로토콜 종류를 선택합니다. TCP나 UDP, ICMP를 선택하면 선택한 프로토콜의 패킷에만 포트 바운더리를 적용하게 됩니다. '전체'를 선택하면 프로토콜 종류에 관계없이 모든 패킷에 포트 바운더리를 적용합니다. (기본값: 전체)</li> <li>• <b>출발지 IP 주소</b> 포트 바운더리를 적용할 패킷의 출발지 IP 대역을 지정합니다. (기본값: 0.0.0.0/0)</li> <li>• <b>목적지 IP 주소</b> 포트 바운더리를 적용할 패킷의 목적지 IP 대역을 입력합니다. (기본값: 0.0.0.0/0)</li> <li>• <b>출발지 포트</b> 바운더리를 적용할 패킷의 출발지 IP 대역을 지정합니다. (설정 범위: 1~65535)</li> <li>• <b>목적지 포트</b> 바운더리를 적용할 패킷의 목적지 IP 대역을 입력합니다. (설정 범위: 1~65535)</li> <li>• <b>Promisc</b> 드롭다운 목록을 클릭한 후 promisc 모드의 상태를 지정합니다. Promisc 모드를 'on'으로 설정하면 포트 바운더리에 속한 포트로 수신되는 모든 패킷에 L4-7 스위칭이 수행되고, 'off'로 설정하면 패킷의 목적지</li> </ul>

	<p>MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는 패킷만 L4-7 스위칭이 수행됩니다. (기본값: off)</p> <ul style="list-style-type: none"> <li>• <b>Include-MAC</b>(Promisc가 off인 경우에만 설정 가능) 드롭다운 목록을 클릭한 후 다음 3가지 값 중에서 Include MAC 모드를 선택합니다. <ul style="list-style-type: none"> <li>- 없음: Promisc 모드의 설정에 따라 패킷의 L4-7 스위칭이 이루어집니다.</li> <li>- unicast: 목적지 MAC 주소가 WEBFRONT-K의 MAC 주소와 일치하는 패킷과 유니캐스트 MAC주소를 가진 패킷에 L4-7 스위칭이 수행됩니다(기본 설정).</li> <li>- multi-broadcast: 멀티캐스트나 브로드캐스트 MAC 주소를 가진 패킷에 L4-7 스위칭이 수행됩니다.</li> </ul> </li> <li>• <b>VLAN</b> 포트 바운더리에 속한 포트가 tagged 포트인 경우, 포트 바운더리를 적용할 패킷의 VLAN을 선택합니다. (기본값: 없음)</li> <li>• <b>상태</b> 드롭다운 목록을 클릭한 후 설정 중인 포트 바운더리의 활성화 여부를 지정합니다. 포트 바운더리를 활성화 하면 포트 바운더리가 바로 적용됩니다. (기본값: 활성화)</li> <li>• <b>바운더리</b> 패킷의 전송 방향을 지정합니다. <ul style="list-style-type: none"> <li>- ALL: 서버/클라이언트로 전송되는 경우에 지정합니다.</li> <li>- 서버: 서버로 전송되는 경우에 지정합니다.</li> <li>- 클라이언트: 클라이언트로 전송되는 경우에 지정합니다.</li> </ul> </li> </ul>
4	항목의 값을 모두 입력한 후 <b>[적용]</b> 버튼을 클릭합니다.

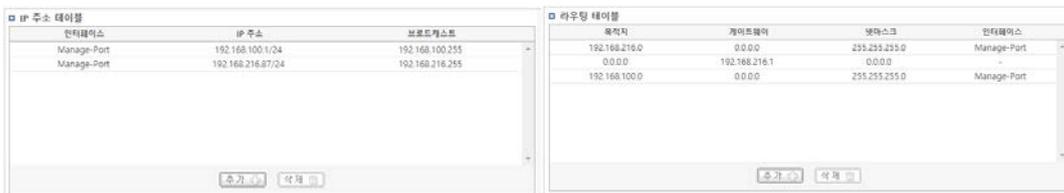
# IP 주소

WEBFRONT-K가 다른 네트워크 장비와 통신하기 위해서는 IP 주소 및 라우팅 정보가 필요합니다. 이 절에서는 다른 네트워크 장비와 통신하기 위해 WEBFRONT-K에 설정해야 하는 항목들에 대해 살펴봅니다.

- VLAN 인터페이스의 IP 주소  
 사용자가 VLAN을 생성한 후, 생성한 VLAN을 이용하여 통신을 하려면 해당 VLAN 인터페이스에 대한 브로드캐스트 주소를 포함한 IP 주소를 할당해야 합니다. 특정 IP 주소는 특수한 사용을 위해 예약되어 있습니다. 이러한 IP 주소는 호스트, 서브넷, 또는 네트워크 주소로 사용할 수 없습니다.
- 기본 게이트웨이  
 기본 게이트웨이는 목적지가 라우팅 테이블에 존재하지 않는 경우 패킷을 전송할 인터페이스입니다.
- 고정 경로  
 고정 경로는 사용자가 정의하는 경로로 출발지와 목적지 사이에서 패킷을 이동하는데 경유하는 특정(지정한) 경로입니다. 고정 경로는 WEBFRONT-K를 특정 목적지 호스트 또는 네트워크를 위한 경로로 설정할 때 필요합니다. 고정 경로는 목적지 IP 주소 및 네트워크 주소, 서브넷 마스크, 게이트웨이 IP 주소로 구성됩니다.

## IP 설정 정보 보기

WEBFRONT-K에 현재 설정된 IP 정보를 보려면 **System** 메뉴에서 **네트워크 - IP 주소** 메뉴를 클릭합니다. 그러면, 각 인터페이스에 설정된 IP 주소와 라우팅 테이블을 보여주는 <IP 주소 테이블>과 <라우팅 테이블>이 나타납니다.



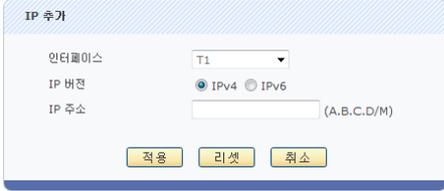
<IP 주소 테이블>에는 WEBFRONT-K에 정의된 인터페이스와 인터페이스에 설정된 IP 주소가 출력됩니다. 기본적으로 WEBFRONT-K에는 관리용 이더넷 포트 인터페이스인 'Manage-Port' 인터페이스가 설정되어 있습니다.

<라우팅 테이블>에는 WEBFRONT-K의 라우팅 테이블에 등록된 라우트 엔트리가 출력됩니다. 각 라우트 엔트리는 다음 항목들로 구성됩니다.

항목	설명
목적지	라우트 엔트리를 통해 도달하는 목적지 네트워크나 호스트의 IP 주소. 이 값이 0.0.0.0이면 인터페이스의 기본 게이트웨이 주소입니다.
게이트웨이	목적지에 도달하기 위해 거쳐가야 하는 다음 노드의 IP 주소.
서브넷 마스크	목적지의 서브넷 마스크. 이 값이 255.255.255.255이면 목적지가 호스트입니다.
인터페이스	목적지로 패킷을 전송할 때 사용하는 WEBFRONT-K의 인터페이스.

## VLAN 인터페이스의 IP 주소 설정

VLAN 인터페이스에 IP 주소를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - IP 주소 메뉴를 클릭합니다.
2	<IP 주소 테이블>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;IP 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정하고 [적용] 버튼을 클릭합니다.</p>  <p>인터페이스 IP 주소를 지정할 VLAN 인터페이스를 선택. (기본값: default)                      IP 버전 VLAN 인터페이스의 IP 버전을 선택. (기본값: IPv4)                      IP 주소 VLAN에 할당할 IP 주소와 넷 마스크 비트(bit) 수를 입력.</p>

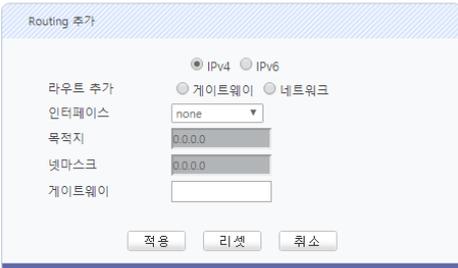
 주의: 인터페이스들은 반드시 서로 다른 네트워크 대역에 존재해야 하므로, 다른 인터페이스의 IP 주소와 동일한 네트워크 대역에 속하는 IP 주소를 입력하지 않도록 합니다.

 참고: VLAN 인터페이스에 IP 주소를 할당하면, 할당된 IP 주소와 VLAN 인터페이스의 MAC 주소를 포함한 ARP 요청 메시지가 WEBFRONT-K와 연결된 모든 네트워크 인터페이스로 전송됩니다. ARP 요청 메시지를 수신한 네트워크 인터페이스는 자신의 IP 주소와 MAC 주소가 담긴 ARP 응답 메시지를 전송합니다. VLAN 인터페이스는 이렇게 수신된 ARP 응답 메시지에 포함된 IP 주소와 MAC 주소를 ARP 테이블에 등록하여 이후 패킷을 전송할 때 사용하게 됩니다.

 참고: VLAN 인터페이스에 지정한 IP 주소를 삭제하려면 VLAN 인터페이스를 선택한 후 [삭제] 버튼을 클릭하면 됩니다. Manage-Port 인터페이스에 설정된 IP 주소는 삭제할 수 없습니다.

## 기본 게이트웨이 추가

인터페이스를 통해 전송되는 패킷 중에서 라우팅 테이블의 정보로는 패킷의 목적지를 알 수 없는 경우가 있습니다. 이런 경우 패킷의 인터페이스에 설정된 기본 게이트웨이로 전송됩니다. WEBFRONT-K의 관리용 이더넷 인터페이스(Manage-Port)의 기본 게이트웨이는 기본적으로 '0.0.0.0'으로 설정되어 있습니다. 인터페이스의 기본 게이트웨이는 다음과 같은 방법으로 설정할 수 있습니다.

순서	설정 과정
1	System - 네트워크 - IP 주소 메뉴를 클릭합니다.
2	<라우팅 테이블>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;Routing 추가&gt; 팝업 창에서 IP 버전을 선택하고, 라우트 추가 항목을 게이트웨이로 지정합니다. 그러면, 기본 게이트웨이 설정에 필요하지 않은 항목들(인터페이스, 목적지, 넷마스크)은 입력할 수 없는 상태로 바뀝니다. 다음 내용을 참고하여 기본 게이트웨이 설정에 필요한 항목들의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p>  <p>• <b>게이트웨이</b> 인터페이스에 지정할 기본 게이트웨이 주소를 입력.</p>

## 고정 경로 추가

고정 경로를 추가하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 네트워크 - IP 주소</b> 메뉴를 클릭합니다.
2	<라우팅 테이블>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;Routing 추가&gt; 팝업 창에서 IP 버전을 선택하고, 라우트 추가 항목을 네트워크로 지정합니다. 그러면, 고정 경로 설정에 필요하지 않은 항목(게이트웨이)은 입력할 수 없는 상태로 바뀝니다. 다음 내용을 참고하여 추가할 고정 경로에 대한 정보를 입력한 후 [적용] 버튼을 클릭합니다.</p> <div data-bbox="614 510 1077 779" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• <b>인터페이스</b> 드롭다운 목록을 클릭한 후 고정 경로를 설정할 VLAN 인터페이스를 선택합니다.</li> <li>• <b>목적지</b> 고정 경로의 목적지 네트워크 주소나 호스트의 IP 주소를 입력합니다.</li> <li>• <b>넷마스크</b> 목적지 항목에 입력한 IP 주소의 서브넷 마스크를 입력합니다.</li> </ul>

# VLAN

이 절에서는 VLAN(Virtual LAN)의 기본적인 개념과 여러 장비에서 VLAN을 공유할 수 있는 802.1Q tagged VLAN에 대해 소개하고, WEBFRONT-K에 VLAN을 설정하는 방법을 설명합니다.

## 개요

VLAN은 물리적으로는 다른 LAN 세그먼트에 위치해있지만 논리적으로는 같은 LAN에 속하는 네트워크 장비의 그룹입니다. VLAN에 속한 장비들은 마치 물리적으로 같은 LAN 세그먼트에 있는 것처럼 서로 통신할 수 있습니다. 이러한 VLAN을 사용하면 백본에 연결되어 있는 네트워크를 여러 개의 워크그룹(workgroup)으로 나눌 수 있어, 트래픽을 보다 효과적으로 처리하고 대역폭 활용률을 높일 수 있습니다.

- 기본 VLAN(default VLAN)

WEBFRONT-K에는 기본적으로 이름이 default이고 ID가 1인 VLAN이 만들어져 있습니다. 이 default VLAN에는 모든 포트가 포함되어 있어서, 기본적으로 WEBFRONT-K에 연결된 장비들이 하나의 LAN에 있는 것처럼 통신하게 됩니다. 기본 VLAN은 삭제할 수 없습니다.

- 중복 VLAN(overlapped VLAN)

WEBFRONT-K의 VLAN은 하나의 포트가 여러 VLAN에 동시에 포함될 수 있는 중복 VLAN입니다. 포트는 반드시 하나의 VLAN에는 속해야 하므로, 기본 VLAN을 제외한 다른 모든 VLAN에서 삭제된 포트는 기본 VLAN에 자동으로 추가됩니다.

- 802.1Q Tagged VLAN

WEBFRONT-K는 다른 장비에서 전송한 패킷에 포함된 VLAN ID를 구분할 수 있고, 또한 패킷을 전송할 때 VLAN ID를 포함시킬 수 있는 802.1Q tagged VLAN을 지원합니다. Tagged 포트에 설정된 포트는 포트의 VID(VLAN ID)를 헤더에 추가한 후 패킷을 전송합니다. 그리고, 수신된 패킷의 헤더에서 VID를 식별하여 해당 VLAN으로 패킷을 전송합니다. Untagged 포트에 설정된 포트는 패킷을 전송할 때 VID를 추가하지 않고, 수신한 패킷도 VID가 없는 패킷으로 간주하여 처리합니다.

미러링 패킷이 유입되는 VLAN 인터페이스에는 '미러링 모드 라우팅 정책'을 반드시 Drop으로 설정해야 합니다. Forward로 설정할 경우, 미러링 패킷이 Inline으로 전달되어 네트워크에 문제가 발생할 수 있습니다.

# VLAN 생성하기

새로운 VLAN을 생성하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - VLAN 메뉴를 클릭합니다.
2	<VLAN 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;VLAN 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 모두 입력한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>VLAN 이름</b> 최대 10자의 알파벳, 숫자, '-', '_' 문자로 이루어진 문자열로 지정할 수 있으며 첫 글자는 반드시 알파벳이어야 함.</li> <li>• <b>VLAN ID</b> VLAN에 할당할 ID를 입력. (입력 범위: 2 ~ 4080)</li> <li>• <b>VLAN 상태</b> VLAN의 동작 상태를 지정. (UP: 활성화, Down: 비활성화)</li> <li>• <b>미러링 모드 라우팅 정책</b> 클라이언트의 요청 패킷이 애플리케이션에 의해 서비스되지 않는 경우에 대한 라우팅 정책 설정             <ul style="list-style-type: none"> <li>- Forward: 클라이언트의 요청 패킷이 애플리케이션에 의해 서비스되지 않는 경우, 해당 패킷을 포워딩 함 (기본값)</li> <li>- Drop: 클라이언트의 요청 패킷이 애플리케이션에 의해 서비스되지 않는 경우, 해당 패킷을 폐기함</li> </ul> </li> </ul> <p> <b>주의:</b> 미러링 패킷이 유입되는 VLAN 인터페이스에는 '미러링 모드 라우팅 정책'을 반드시 Drop으로 설정해야 합니다. Forward로 설정할 경우, 미러링 패킷이 Inline으로 전달되어 네트워크에 문제가 발생할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• <b>트랜스패런트 브릿지 모드</b> 트랜스패런트 브릿지 모드의 사용 여부를 지정. (기본값: 비활성화)</li> <li>• <b>Tagged 포트</b> VLAN에 추가할 포트를 선택. Tagged 포트로 설정된 포트를 통해서는 802.1Q에서 정의된 태그 필드가 포함된 프레임(tagged 프레임) 전송가능.</li> <li>• <b>Untagged 포트</b> VLAN에 추가할 포트를 선택. Untagged 포트로 설정된 포트를 통해서는 태그 필드가 포함되지 않은 프레임만 전송할 수 있음.</li> </ul>

 **주의:** 802.1Q를 지원하지 않는 장비나 NIC 등과 연결되어 있는 포트는 반드시 untagged 포트로 지정해야 합니다. 802.1Q를 지원하지 않는 장비로 태그 필드가 포함된 프레임을 전송하면 프레임을 제대로 인식하지 못하거나 혹은 크기 오류(oversize packet)가 발생한 패킷으로 인식하여 폐기하게 됩니다.

 **참고:** 생성한 VLAN을 삭제하려면 <VLAN 정보>에 표시되는 VLAN 목록에서 삭제하려는 VLAN을 선택한 후 [삭제] 버튼을 클릭합니다. VLAN의 정보를 수정하려면 <VLAN 정보>에 표시되는 VLAN 목록에서 수정하려는 VLAN을 선택하고, [수정] 버튼을 클릭한 후 원하는 항목의 값을 다시 입력하면 됩니다. 기본 VLAN인 'default'는 수정하거나 삭제할 수 없습니다.

## 포트

WEBFRONT-K에는 내부 혹은 외부 네트워크의 장비들과 데이터를 송수신할 때 사용하는 이더넷 포트가 있습니다. 각 모델별 포트에 대한 자세한 설명은 이 설명서와 함께 제공되는 <WEBFRONT-K 설치 설명서>를 참고합니다.

WEBFRONT-K의 각 이더넷 포트를 통해서 상대 장비와 정상적으로 통신하기 위해서는 속도나 전송 모드와 같은 포트 특성을 연결되어 있는 상대 장비와 동일하게 설정해야 합니다. 이 절에서는 WEBFRONT-K의 이더넷 포트 특성을 설정하는 방법을 살펴본 후, 각 이더넷 포트를 통해 송수신되는 패킷의 양을 모니터링하는 방법을 살펴봅니다.

## 개요

기가빗 이더넷 포트를 설정하는 것은 다음과 같은 포트 특성을 지정하는 것입니다.

- 속도(speed)  
데이터를 전송하고 수신하는 속도. 100Mbps, 1000Mbps(1Gbps), 10000Mbps(10Gbps)로 설정할 수 있습니다.
- 흐름 제어(flow control)  
포트의 수신 한도를 넘는 데이터가 수신되어 데이터가 분실되지 않도록 데이터의 흐름을 조절하는 기능. 이 기능을 활성화하면 바로 처리할 수 있는 용량보다 더 많은 데이터가 수신되는 경우 상대 장비에게 조절 패킷(pause packet)을 전송하여 데이터를 천천히 전송하도록 유도합니다.
- 포트의 상태  
포트의 동작 여부. 포트의 상태가 활성화된 포트만 동작하고, 비활성화 상태로 설정된 포트는 동작하지 않습니다. 연결된 포트가 비활성화 상태이면 통신이 이루어지지 않습니다.

### 자동 모드 (Auto Negotiation Mode)와 수동 모드 (Forced Mode)

포트의 속도를 설정할 때 100Mbps, 1000Mbps 와 같은 값을 직접 지정할 수도 있지만, WEBFRONT-K의 이더넷 포트는 자동 모드를 지원하기 때문에 자동 모드로 설정할 수도 있습니다. 포트를 자동 모드로 설정하면 상대 포트와의 협상 과정(negotiation)을 통해 두 포트가 통신할 수 있는 최적의 속도로 설정하게 됩니다.

포트를 자동 모드로 설정하기 위해서는 연결된 상대 포트도 반드시 자동 모드를 지원해야 합니다. 상대 장비의 포트가 자동 모드를 지원하지 않는 경우에는 이 절에서 설명하는 방법을 통해 포트의 속도를 사용자가 수동으로 설정해주어야 정상적으로 통신할 수 있습니다.

### 기본 설정

기본적으로 WEBFRONT-K 기가빗 이더넷 Fiber 포트의 특성이 다음과 같이 설정되어 있습니다.

항목	기본 설정		
	10 기가빗 이더넷 Fiber 포트	기가빗 이더넷 Fiber 포트	기가빗 이더넷 Copper 포트
속도	10000Mbps	자동	자동
흐름 제어	off	off	Off
동작 상태	활성화	활성화	활성화

## 포트 설정하기

WEBFRONT-K의 10 기가빗 이더넷 Fiber 포트의 현재 설정을 보는 방법과 포트를 설정하는 방법을 살펴봅니다.

### 현재 포트 설정 보기

WEBFRONT-K 10 기가빗 이더넷 Fiber 포트의 현재 설정 정보를 보려면 **System** 메뉴에서 네트워크 - 포트 메뉴를 클릭합니다. 그러면, 각 포트의 현재 설정 정보를 보여주는 <포트 정보> 화면이 나타납니다.

포트	링크	인터페이스	관리자	속도(Mbps)	Duplex	MDI/MDIX	흐름제어	설명
ge1		Fiber	활성화	자동(1000)	-	-	Off	없음
ge2		Fiber	활성화	자동(1000)	-	-	Off	없음
ge3		Fiber	활성화	자동(1000)	-	-	Off	없음
ge4		Fiber	활성화	자동(1000)	-	-	Off	없음
ge5		Fiber	활성화	자동(1000)	-	-	Off	없음
ge6		Fiber	활성화	자동(1000)	-	-	Off	없음
ge7		Fiber	활성화	자동(1000)	-	-	Off	없음
ge8		Fiber	활성화	자동(1000)	-	-	Off	없음
xg1		Fiber	활성화	10000	-	-	Off	없음
xg2		Fiber	활성화	10000	-	-	Off	없음
xg3		Fiber	활성화	10000	-	-	Off	없음
xg4		Fiber	활성화	10000	-	-	Off	없음
xg5		Fiber	활성화	10000	-	-	Off	없음
xg6		Fiber	활성화	10000	-	-	Off	없음
xg7		Fiber	활성화	10000	-	-	Off	없음
xg8		Fiber	활성화	10000	-	-	Off	없음

화면의 각 항목들은 포트에 대한 다음 정보들을 표시해줍니다.

항목	의미
링크	
	포트의 연결 상태
	케이블이 연결되어 있지 않거나 상대 장비와 연결되어 있지 않은 포트
	상대 장비와 연결되어 있는 포트
인터페이스	포트의 물리적 인터페이스 종류(Copper, Fiber)
관리자	포트의 동작 상태. '활성화' 상태인 포트는 사용하도록 설정된 포트이고, '비활성화' 상태인 포트는 사용하지 않도록 설정된 포트입니다.
속도(Mbps)	포트에 설정된 속도와 포트의 현재 속도(Mbps). 포트의 속도를 '자동' 모드로 설정한 경우 괄호 안에는 현재 연결된 속도가 표시됩니다.
Duplex	포트에 설정된 전송 모드와 현재 전송 모드. 포트의 전송 모드를 '자동' 모드로 설정한 경우 괄호 안에는 현재 전송 모드가 표시됩니다. (기가빗 이더넷 Fiber 포트, 10 기가빗 이더넷 Fiber 포트는 지원하지 않습니다.)
MDI/MDIX	포트가 MDI 혹은 MDIX로 연결되어 있는지 여부. 포트가 상대 장비와 연결되어 있지 않은 경우에는 '연결되지 않음'으로 표시됩니다. (기가빗 이더넷 Fiber 포트, 10 기가빗 이더넷 Fiber 포트는 지원하지 않습니다.)
흐름제어	흐름 제어 기능의 사용 여부. 흐름 제어를 사용할 경우 'On', 사용하지 않을 경우 'Off'로 표시됩니다.
설명	포트에 대한 추가 설명입니다. 사용자가 직접 입력하여 설정합니다.

## 포트 속도 설정

기본적으로 10 기가빗 이더넷 Fiber 포트의 속도는 '10000'모드로 설정되어 있습니다. 포트의 속도를 변경하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - 포트 메뉴를 클릭합니다.
2	<포트 정보> 화면에서 속도를 설정할 포트의 속도 항목을 클릭합니다.
3	<Speed Edit> 팝업 창의 속도 드롭다운 목록에서 지정할 속도를 선택한 후 [적용] 버튼을 클릭합니다. 

## 흐름 제어(flow control) 설정

포트의 흐름 제어를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - 포트 메뉴를 클릭합니다.
2	<포트 정보> 화면에서 흐름 제어 기능을 설정할 포트의 흐름제어 항목을 클릭합니다.
3	포트에 흐름 제어 기능의 사용 여부를 변경할지 묻는 팝업 창이 나타나면 [확인]을 클릭합니다.

## 포트의 동작 상태 설정

포트의 동작 상태를 변경하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - 포트 메뉴를 클릭합니다.
2	<포트 정보> 화면에서 동작 상태를 변경할 포트의 관리자 항목을 클릭합니다.
3	변경 여부를 확인하는 팝업 창이 나타나면 [확인] 버튼을 클릭합니다.



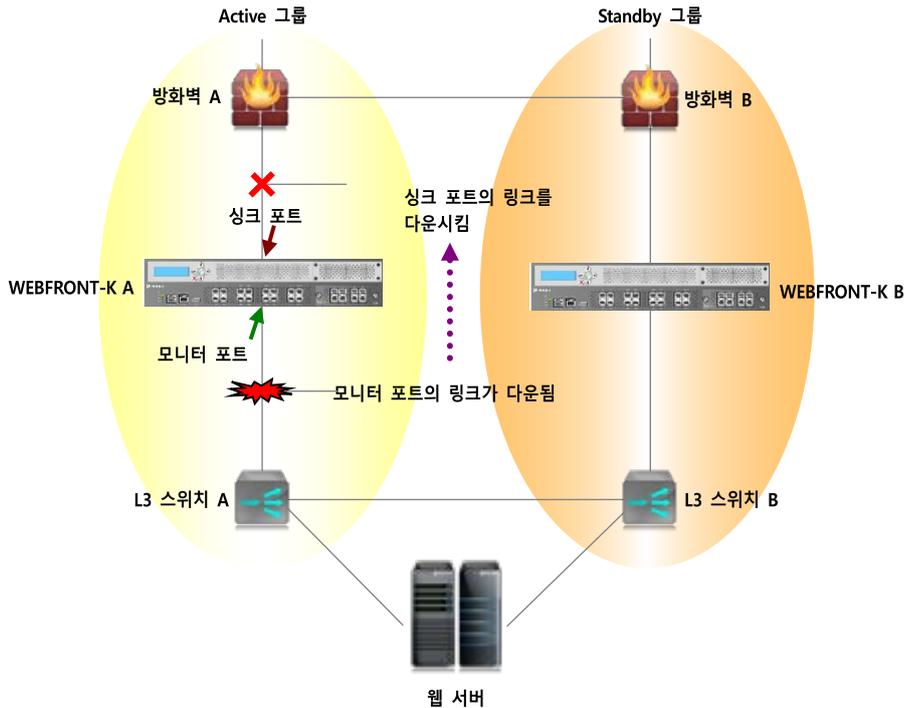
**주의:** 포트의 동작 상태를 비활성화 상태로 설정하면 포트가 사용하지 않는 상태로 변경되므로 해당 포트의 연결이 끊어집니다.

# 링크싱크

이 절에서는 링크싱크 기능에 대해 소개한 후 WEBFRONT-K에서 링크싱크 기능을 설정하는 방법에 대해 설명합니다.

## 개요

링크싱크(Linksync)는 모니터 포트와 싱크 포트의 링크 상태를 주기적으로 감시하여 두 포트간의 링크 상태를 동기화 시켜주는 기능입니다. 링크싱크는 두 가지 모드(단방향 싱크, 양방향 싱크)를 제공하여, 다양한 네트워크 구성을 지원합니다. 다음 그림은 Active 그룹과 Standby 그룹이 있는 Failover 구성에서 링크싱크 기능이 사용되는 예입니다.



먼저 이 구성에서 L3 스위치 A와 WEBFRONT-K A 가 연결된 링크가 다운되더라도 방화벽 A는 WEBFRONT-K A와의 링크가 살아 있기 때문에 요청 패킷을 전송합니다. 그러나 L3 스위치 A와 WEBFRONT-K A 간의 링크가 다운되었기 때문에 요청 패킷은 웹 서버에게 전송될 수 없습니다. 이로 인해 웹 서버는 지속적인 서비스를 제공할 수 없습니다.

한편, 링크싱크 기능을 사용할 경우, WEBFRONT-K는 지속적으로 모니터 포트의 상태를 감시하여 모니터 포트가 다운되었을 경우, 싱크 포트의 링크도 다운시켜 방화벽A가 방화벽 B로 failover됩니다. 이로써, 웹 서버는 WEBFRONT-K B를 통해 지속적인 서비스를 제공할 수 있습니다.

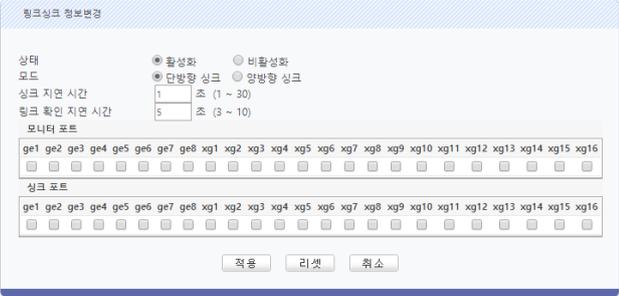
- 단방향 모드  
모니터 포트의 링크 상태를 감시하여 모니터 포트의 링크가 다운될 경우 싱크 포트도 링크 다운시킵니다. 모니터 포트가 링크 업 되면 싱크 포트의 포트도 링크 업 시킵니다.
- 양방향 모드  
기본적인 동작은 단방향 모드와 같지만 모니터 포트와 싱크 포트 모두 링크 상태를 감시한다는 차이점이 있습니다. 양방향 모드의 모니터 포트와 싱크 포트는 서로의 링크 상태에 따라 상태가 변경됩니다. 즉, 앞의 그림에서 싱크 포트의 링크가 다운되면 모니터 포트의 링크도 다운시킵니다. 그렇게 되면, L3 스위치 A로 수신된 패킷이 WEBFRONT-K A로 전송되지 않고 L3 스위치 B로 전송되어 WEBFRONT-K B를 통해 지속적으로 서비스를 제공할 수 있습니다.



**참고:** 하나의 링크싱크 설정에는 여러 개의 모니터 포트와 싱크 포트를 설정할 수 있습니다. 이 경우, 모든 모니터 포트들이 링크 다운되어야 싱크 포트의 모든 포트들도 링크 다운되고 모든 모니터 포트가 링크 업되어야 싱크 포트의 모든 포트들도 링크 업됩니다.

## 링크싱크 설정하기

WEBFRONT-K에 링크싱크 기능을 설정하는 방법은 다음과 같습니다. WEBFRONT-K에는 최대 8개의 링크싱크를 설정할 수 있습니다.

순서	설정 과정
1	<b>System - 네트워크 - 링크싱크</b> 메뉴를 클릭합니다.
2	<링크싱크 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;링크싱크 정보변경&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [적용] 버튼을 클릭합니다.</p>  <p>링크싱크 정보변경 팝업 창에는 상태(활성화/비활성화), 모드(단방향 싱크/양방향 싱크), 싱크 지연 시간(1~30초), 링크 확인 지연 시간(3~10초), 모니터 포트, 싱크 포트가 표시되어 있습니다. 각 항목은 체크박스, 라디오 버튼, 텍스트 입력 필드, 또는 선택 가능한 포트 목록을 통해 설정할 수 있습니다. 하단에는 [적용], [리셋], [취소] 버튼이 있습니다.</p> <ul style="list-style-type: none"> <li>• <b>상태</b> 현재 설정하고 있는 링크싱크 기능의 적용 여부를 선택합니다. (기본값: 활성화)</li> <li>• <b>모드</b> 링크싱크의 모드를 설정합니다. (기본값: 단방향 싱크)</li> <li>• <b>싱크 지연 시간</b> 모니터 포트의 링크 상태가 변경되었을 경우 싱크 포트의 링크 상태를 변경하기까지의 대기 시간을 입력합니다. (설정 범위: 1 ~ 30, 기본값: 1초)</li> <li>• <b>링크 확인 지연 시간</b> 포트 상태를 활성화로 변경한 후 실제 링크 상태가 업으로 인식되기까지의 최대 지연 시간을 입력합니다. (설정 범위: 3 ~ 10, 기본값: 5초)</li> <li>• <b>모니터 포트</b> 링크 상태를 확인할 포트를 선택합니다.</li> <li>• <b>싱크 포트</b> 모니터 포트의 상태에 따라 링크 상태를 변경할 포트를 선택합니다.</li> </ul>



**주의:** 링크싱크 기능에 설정된 포트를 **System - HA** 메뉴에서 백업 시 차단 포트로 설정하게 되면 링크싱크 기능이 정상적으로 동작하지 않을 수 있습니다.



**주의:** Copper 포트를 통해 링크싱크 기능을 사용하는 경우, 해당 Copper 포트와 상대 장비 Copper 포트의 속도, 전송 모드, MDI/MDIX를 수동으로 설정해야 합니다. Copper 포트의 각 설정을 자동으로 지정한 경우에는 포트 정보를 교환하는 과정에서 지연이 발생하여 링크싱크 기능이 오동작할 수 있습니다.



**참고:** 링크싱크는 모드에 관계없이 최대 8개까지 설정할 수 있으며, 하나의 링크싱크에 설정된 포트는 다른 링크싱크 설정에 포함될 수 없습니다.



**참고:** 링크싱크 기능에 설정된 포트는 **System - 네트워크 - 포트** 메뉴에서 포트의 동작 상태를 설정할 수 없으며, **System - 네트워크 - 포트** 메뉴에서 비활성화로 설정된 포트는 링크싱크 기능에 설정할 수 없습니다.



**참고:** 링크싱크 기능은 포트의 인터페이스(Copper, Fiber)의 종류와 관계 없이 둘 중 하나의 인터페이스가 링크 업 상태이면 링크 업 상태로, 두 가지 인터페이스가 모두 링크 다운이면 링크 다운 상태로 판단합니다.

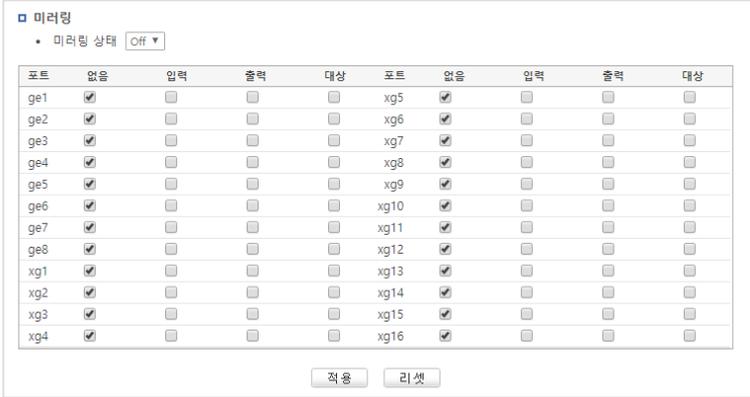
# 미러링

포트 미러링(Port Mirroring)은 특정 포트에 송수신되는 모든 패킷들의 복사본을 다른 포트에 전달하는 기능입니다. 포트 미러링의 대상이 되는 포트를 '모니터 대상 포트(mirrored 포트)'라고 하고, 모니터 대상 포트의 트래픽이 전달되는 포트(패킷의 복사 본을 생성할)를 '모니터 포트(mirroring 포트)'라고 합니다. 포트 미러링은 모니터 포트를 통해 모니터 대상 포트에서 송수신되는 패킷을 조사하여 네트워크에서 발생한 문제를 해결하거나 보다 나은 네트워크 보안을 제공하기 위해 사용됩니다.

관리용 이더넷 포트를 제외한 WEBFRONT-K의 모든 포트를 모니터 포트로 사용할 수 있습니다. 일반적으로는 모니터 포트에는 네트워크 분석기나 RMON 등을 연결하여 패킷을 분석합니다. 모니터 포트는 포트 미러링 기능을 수행하는 동안에는 모니터 대상 포트의 패킷만 수신할 수 있습니다. 포트 미러링 기능이 비활성화되면 다시 정상적으로 패킷을 수신할 수 있습니다. 모니터 포트는 하나만 지정할 수 있지만, 모니터 대상 포트는 여러 개를 지정할 수 있습니다.

## 포트 미러링 설정하기

포트 미러링 기능을 사용하기 위해 모니터 포트와 모니터 대상 포트를 지정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - 미러링 메뉴를 클릭합니다.
2	<p>&lt;미러링&gt; 화면에서 모니터 대상 포트를 지정합니다. 포트에 수신되는 트래픽만 모니터링하려면 입력 항목을 체크하고, 외부로 전송하는 트래픽만 모니터링하는 경우에는 출력 항목을, 양방향 트래픽을 모두 모니터링하려는 경우에는 입력과 출력 항목을 모두 체크합니다. 모니터 대상 포트는 여러 개를 지정할 수 있습니다.</p> 
3	모니터 포트로 지정할 포트의 <b>대상</b> 항목을 체크합니다. 모니터 포트는 하나만 지정할 수 있습니다.
4	모니터 대상 포트와 모니터 포트를 모두 지정한 후 포트 미러링을 시작하기 위해 <b>미러링 상태</b> 드롭다운 목록을 클릭한 후 on을 선택하고 <b>[적용]</b> 버튼을 클릭합니다.

# 트렁킹

## 개요

포트 트렁킹(Port Trunking)은 여러 개의 포트들을 하나의 그룹(트렁크 그룹)으로 설정하여 논리적인 포트로서 사용할 수 있게 하는 기능입니다. WEBFRONT-K는 같은 트렁크 그룹에 속한 포트들에게 트래픽을 분산시켜주는 부하 분산 기능을 제공합니다. 부하 분산 기능을 사용하면 트렁크 그룹 내의 특정 포트가 트래픽을 처리할 수 없는 경우 트래픽은 트렁크 그룹 내의 가용한 다른 포트에게 분산됩니다. 트렁크 그룹에서 트래픽을 분산시킬 포트를 선택하는 부하 분산 알고리즘은 기본적으로 패킷의 출발지와 목적지 MAC 주소의 XOR값을 이용한 해시(hash) 방식이 사용됩니다. 이 방식 외에도 다음과 같은 방식이 지원됩니다.

부하 분산 알고리즘	설명
dest-ip	목적지 IP 주소 기반의 해시 방식
dest-MAC	목적지 MAC 주소 기반의 해시 방식
src-dest-ip	출발지와 목적지 IP 주소의 XOR 값을 이용한 해시 방식
src-dest-MAC	출발지와 목적지 MAC 주소의 XOR 값을 이용한 해시 방식
src-ip	출발지 IP 주소 기반의 해시 방식
src-MAC	출발지 MAC 주소 기반의 해시 방식

## 포트 트렁킹 설정시 주의 사항

WEBFRONT-K에 포트 트렁킹을 설정할 때에는 다음 사항들을 주의합니다.

- WEBFRONT-K에는 총 5개의 트렁크 그룹을 만들 수 있으며, 각 트렁크 그룹에는 2 ~ 8개의 포트를 포함시킬 수 있습니다.
- 하나의 포트는 동시에 둘 이상의 트렁크 그룹에 속할 수 없습니다.
- 트렁크 그룹에 포함되는 포트들은 모두 같은 VLAN에 포함되어 있어야 합니다.
- 포트 트렁킹은 STP와 함께 사용할 수 없습니다. STP가 활성화되어 있으면 포트 트렁킹 설정 화면에 다음과 같은 메시지가 표시되고, 포트 트렁킹 기능을 사용할 수 없습니다.



## 포트 트렁킹 설정하기

WEBFRONT-K에 트렁크 그룹을 추가하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - 트렁킹 메뉴를 클릭합니다.
2	<트렁크 정보>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;트렁크 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <p>• <b>트렁크 이름</b> 추가할 트렁크 그룹의 이름을 트렁크1 ~ 트렁크5 중에서 선택합니다.</p> <p>• <b>규칙</b> 다음 중에서 트렁크 그룹의 부하 분산 시 사용할 알고리즘을 선택합니다.</p> <ul style="list-style-type: none"> <li>- src-mac           출발지 MAC 주소 기반의 해시 방식</li> <li>- dest-mac        목적지 MAC 주소 기반의 해시 방식</li> <li>- src-dest-mac    목적지와 출발지 MAC 주소의 XOR 값을 이용한 해시 방식 (기본 설정)</li> <li>- src-ip           출발지 IP 주소 기반의 해시 방식</li> <li>- dest-ip          목적지 IP 주소 기반의 해시 방식</li> <li>- src-dest-ip     목적지와 출발지 IP 주소의 XOR 값을 이용한 해시 방식</li> </ul> <p>• <b>LACP</b> LACP 동작 모드를 지정합니다.</p> <ul style="list-style-type: none"> <li>- 비활성화        LACP를 사용하지 않음. (기본 설정)</li> <li>- Active          LACP 모드를 active로 지정</li> <li>- Passive         LACP 모드를 passive로 지정. (상대 장비가 active로 동작해야 합니다.)</li> </ul> <p>• <b>포트</b> 트렁크 그룹에 포함시킬 포트를 선택합니다. 2 ~ 8개의 포트를 선택할 수 있습니다.</p>

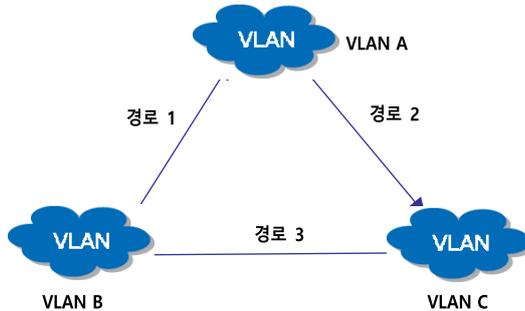
# STP

이 절에서는 STP(Spanning Tree Protocol)의 역할과 STP에서 사용하는 스페닝 트리의 구조, 그리고 STP가 동작 시 사용되는 타이머 등 STP에 대해 상세히 살펴본 후 WEBFRONT-K에 STP를 동작시킬 수 있도록 설정하는 방법에 대해 설명합니다.

## 개요

STP는 스페닝 트리를 사용하여 목적지에 대한 경로가 2개 이상일 때 발생하는 루프(loop)를 방지해주는 프로토콜입니다. 스페닝 트리는 하나의 노드에 둘 이상의 경로가 존재하는 경우, 우선 순위 등을 고려하여 최적의 경로를 선택하여 스페닝 트리에 포함시킵니다. 그리고, 그 경로를 제외한 나머지 경로를 블로킹 상태(blocking state: 프레임을 전송하지 않는 상태)로 처리하여 스페닝 트리에서 제외합니다. 트래픽은 블로킹 상태가 아닌 최적의 경로를 통해서만 전송되므로 루프가 만들어지지 않습니다.

아래와 같이 WEBFRONT-K에 3개의 VLAN이 정의된 경우를 예로 들어 살펴보면, VLAN A에서 VLAN C까지 도달할 수 있는 2개의 경로가 있습니다. 직접 연결된 경로 2와 VLAN B를 경유하여 경로 1과 경로 3을 통해 가는 경로입니다. 이와 같이 한 목적지에 대해 2개 이상의 경로가 존재하면 루프(loop)가 만들어집니다. VLAN A가 패킷을 브로드캐스트하면, VLAN C는 경로 2를 통해 수신한 패킷을 VLAN B로 전송하고, VLAN B는 경로 3을 통해 수신한 패킷을 경로 1을 통해 VLAN A로 전송하기 때문에 루프가 생성됩니다. 반대로 VLAN A-B-C-A의 루프도 생성됩니다.

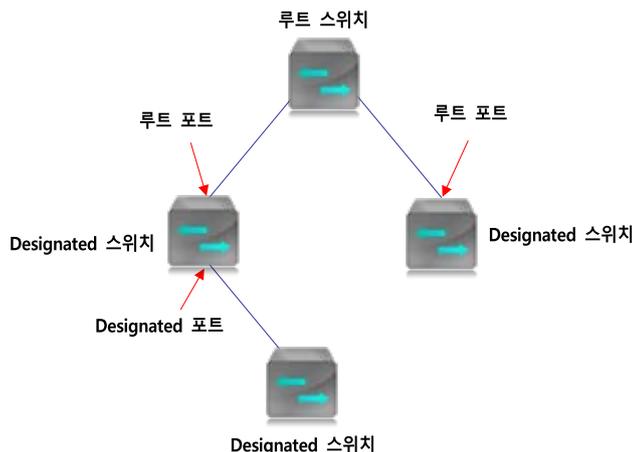


위와 같은 상황에서 STP를 사용하면 경로 3(가장 높은 경로 비용과 우선 순위를 가지고 있다고 가정)이 블로킹 상태가 됩니다. 그러면, VLAN A에서 VLAN C까지의 경로가 오직 하나(경로 2)만 존재하므로 루프가 만들어지지 않습니다.

만약 경로 2에 문제가 발생하면, STP는 블로킹 상태에 있던 경로 3을 포워딩 상태(forwarding state: 트래픽을 전송하는 상태)로 변경하여 VLAN A와 VLAN C간에 트래픽이 문제 없이 전송될 수 있도록 합니다.

## 스패닝 트리의 구조와 BPD(Bridge Protocol Data Unit)

스패닝 트리는 루트 스위치, designated 스위치, 루트 포트, designated 포트 등으로 구성됩니다. 루트 스위치는 스페닝 트리의 가장 윗 부분에 위치하는 스위치로, 루트 스위치를 기준으로 하여 스페닝 트리가 만들어집니다. Designated 스위치는 각 LAN 세그먼트에서 루트 스위치로 패킷을 포워딩할 때 사용되는 스위치입니다. 루트 포트는 designated 스위치에서 루트 스위치로 패킷을 포워딩할 때 사용되는 포트입니다. Designated 포트는 designated 스위치의 포트 중에서 하위의 LAN에 직접 연결되는 포트입니다.



앞의 그림과 같이 스페닝 트리에 참여하는 스위치와 포트를 결정하기 위해, 각 스위치는 BPDU를 교환합니다. BPDU에는 다음과 같은 정보가 포함되어 있습니다.

- BPDU를 전송하는 스위치가 루트 스위치로 알고 있는 스위치의 브리지 ID
- 루트 스위치까지의 경로 비용
- BPDU를 전송하는 스위치의 브리지 ID
- BPDU의 aging 시간
- BPDU를 전송하는 인터페이스의 ID
- 스페닝 트리 타이머 값들(hello, forward delay, max-age)

브리지 ID는 스페닝 트리에서 중심이 되는 스위치인 루트 스위치를 선출할 때 사용되는 값입니다. 브리지 ID는 스위치의 우선 순위(상위 2byte)와 MAC 주소로 구성되어 있는데, 가장 높은 우선 순위를 가진 스위치가 루트 스위치로 선출됩니다. 우선 순위 값이 낮을수록 우선 순위는 높습니다. 만약 모든 스위치의 우선 순위가 동일한 경우에는 MAC 주소를 비교하여 가장 낮은 MAC 주소를 가진 스위치를 루트 스위치로 선택합니다.

경로 비용은 루트 포트와 designated 스위치를 선택할 때 사용되는 값입니다. 스위치가 루트 스위치로 패킷을 전송할 때 가장 좋은 경로(비용이 가장 적음)를 제공하는 포트, 즉, 루트 스위치까지의 경로 비용이 가장 적은 포트가 루트 포트가 됩니다. 그리고, LAN에서 루트 스위치까지 패킷을 포워딩할 때 경로 비용이 가장 낮은 스위치가 designated 스위치가 됩니다. Designated 스위치의 포트 중에서 LAN에 직접 연결되는 포트가 designated 포트가 됩니다.

BPDU에는 3개의 타이머 값(hello, forward delay, max aging)이 포함됩니다. 이 타이머들은 전체 스페닝 트리의 성능에 영향을 미치는 타이머들로 다음과 같은 기능을 합니다.

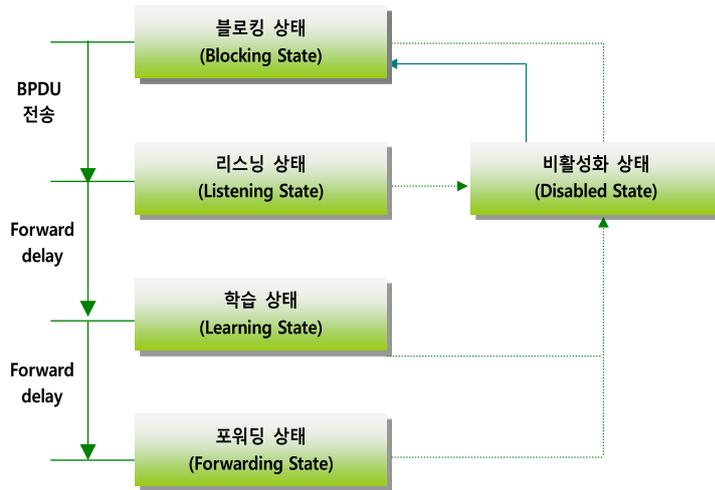
타이머	설명
Hello timer	Hello 메시지 전송 주기. 루트 스위치가 얼마나 자주 BPDU 메시지를 다른 스위치로 브로드캐스트 할지 결정하는 타이머 값
Forward delay timer	리스닝 상태와 학습 상태를 얼마나 오랫동안 유지할 지 결정하는 타이머 값. 리스닝 상태에서 forward delay 시간이 경과되면 학습 상태로 넘어가고, 다시 학습 상태에서 forward delay 시간이 경과하면 포워딩 상태가 됩니다. 이 타이머는 변경된 토폴로지 정보가 스페닝 트리에 충분히 전파 되기 전에 포트가 포워딩 상태로 되어서 루프가 만들어지는 현상을 방지해줍니다.
Max aging timer	BPDU의 Aging 시간(유효 시간). 스위치가 수신한 BPDU를 얼마나 오랫동안 저장할 것인지 결정하는 타이머 값. Max aging 타이머의 시간이 지나면 BPDU를 폐기합니다.

## 포트의 상태

STP는 네트워크 상의 포트를 다음 5가지 상태로 설정합니다.

- 블로킹 상태  
프레임을 전송하지 않는 상태. STP가 동작하는 포트의 기본 상태.
- 리스닝 상태  
블로킹 상태에서 포워딩 상태로 가기 전 처음으로 거치는 상태.
- 학습 상태  
프레임 전송을 준비하는 단계의 상태.
- 포워딩 상태  
트래픽을 전송하는 상태.
- 비활성화 상태  
STP가 비활성화되었거나 프레임 전송이 불가능한 상태.

포트가 이러한 5가지 상태를 거치는 과정을 그림으로 나타내면 다음과 같습니다.



STP가 동작하는 포트는 항상 블로킹 상태에서 시작하게 됩니다. STP가 동작하도록 설정된 스위치는 초기화될 때 자신이 루트 스위치라고 가정하고 모든 포트를 통해 연결된 장비로 BPDU를 전송합니다. 블로킹 상태의 포트는 BPDU를 제외한 모든 프레임을 폐기합니다. BPDU를 수신한 포트는 리스닝 상태가 됩니다.

리스닝 상태의 포트는 다른 장비와 BPDU를 교환하여 루트 스위치를 결정하는 등의 작업을 수행합니다. 그리고 forward delay의 시간이 경과한 후 학습 상태로 바뀝니다. 학습 상태의 포트는 프레임을 전송하기 위해 MAC 주소를 학습합니다. 그리고, forward delay의 시간이 지나면 포워딩 상태가 됩니다. 포트가 포워딩 상태가 되기 전까지 수신된 프레임은 모두 폐기되고, 포워딩 상태가 된 이 후부터는 수신된 프레임이 포트를 통해 전송됩니다. 비활성화 상태의 포트는 스패닝 트리 에 참여하지 않는 포트로서, 포트가 동작하지 않거나 링크가 연결되어 있지 않거나 혹은 STP가 동작하지 않는 포트입니다. 이 상태의 포트는 BPDU를 전송하거나 수신하지도 않고, 프레임을 전송하지도 않습니다.

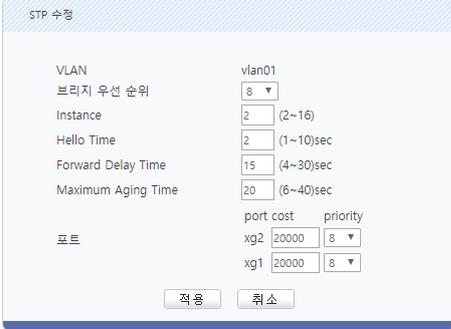
### 경로 선택

STP는 경로를 선택할 때, 즉, 어떤 스위치를 통해서 패킷을 전송할지 결정할 때, 스패닝 트리 알고리즘을 사용합니다. 스패닝 트리 알고리즘은 실제 토폴로지 상에서의 포트 역할을 기준으로 하여 네트워크를 통해 루프가 만들어지지 않는 가장 좋은 경로를 계산합니다.

스위치에 2개의 인터페이스가 루프를 형성하게 되는 경우에는 포트의 우선 순위와 경로 비용에 따라 어떤 인터페이스를 포워딩 상태로 하고 나머지 인터페이스를 블로킹 상태로 할지를 결정하게 됩니다. 포트 우선 순위는 주로 네트워크 상에서 인터페이스의 위치를 나타내고 (트래픽 전송에 얼마나 용이한 위치에 있는지), 경로 비용은 인터페이스의 물리적인 속도(media speed)를 나타냅니다. 스패닝 트리에서 사용하지 않는 여분의 경로는 대기 상태, 즉 블로킹 상태로 설정됩니다. 스패닝 트리의 특정 네트워크 세그먼트가 동작하지 않을 때(링크가 끊어지거나) 다른 여분의 경로가 있는 경우, 스패닝 트리 알고리즘은 스패닝 트리 토폴로지를 다시 계산하여 대기 상태인 여분의 경로를 포워딩 상태로 바꿉니다.

## STP 설정하기

STP는 VLAN별로 하나씩 설정할 수 있습니다. VLAN에 STP를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - STP 메뉴를 클릭합니다.
2	<STP 리스트> 화면에서 [추가] 버튼을 클릭합니다.
3	<p>&lt;STP 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 입력한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>VLAN</b> STP를 추가할 VLAN을 선택합니다.</li> <li>• <b>브리지 우선 순위</b> VLAN에 할당할 브리지 우선 순위를 선택합니다. 브리지 우선 순위는 루트 브리지를 선택할 때 사용되는 값으로, 값이 작을수록 우선 순위가 높습니다. (설정 범위: 0 ~ 15, 기본값: 8)</li> <li>• <b>Instance</b> VLAN을 포함시킬 Instance를 선택합니다. (설정 범위: 2~16)</li> <li>• <b>Hello Time</b> 선택한 VLAN에서 다른 VLAN으로 Hello 메시지를 전송할 주기를 입력합니다. (설정 범위: 1 ~ 10, 기본값: 2초)</li> <li>• <b>Forward Delay Time</b> STP에 포함된 포트의 상태 변화 시간을 지정합니다. 포트의 상태가 변경되려면 최소한 이 시간이 경과해야 합니다. (설정 범위: 4 ~ 30, 기본값: 15초)</li> <li>• <b>Maximum Aging Time</b> 다른 VLAN으로 전송한 BPDU 패킷의 유효 기간을 지정합니다. 이 시간이 경과하면 BPDU 패킷은 폐기됩니다. (설정 범위: 6 ~ 40, 기본값: 20초)</li> <li>• <b>포트</b> STP에 포함된 포트의 비용과 우선 순위를 지정합니다. <ul style="list-style-type: none"> <li>- cost: 포트의 비용을 입력합니다. 비용이 낮은 포트일수록 더 자주 경로(route)로 선택됩니다. (설정 범위: 1 ~ 65535, 기본값: 4)</li> <li>- Priority: 포트의 우선 순위를 선택합니다. VLAN에 속한 포트 중 우선 순위가 가장 낮은 포트를 통해 다른 VLAN으로 트래픽을 전송합니다. 값이 작을수록 우선 순위가 높습니다. (설정 범위: 0, 32, 64, 96, 128, 160, 192, 224, 기본값: 0)</li> </ul> </li> </ul>
4	같은 방법으로 다른 VLAN에서 STP를 설정합니다. STP가 동작하는 중에 STP 설정이 변경되면 WEBFRONT-K는 그 때마다 변경 사항을 반영하여 스페닝 트리를 다시 생성합니다.

## STP 상태 설정하기

STP 기능의 활성화 상태와 모드를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	System - 네트워크 - STP 메뉴를 클릭합니다.
2	<STP 상태>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;STP 상태 설정&gt; 팝업 창에서 다음 설명을 참고하여 상태와 모드를 지정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>상태</b> STP 기능을 활성화할 것인지 지정합니다. (기본값: 비활성화)</li> <li>• <b>포트</b> STP 모드를 지정합니다. 연결된 상태 장비와 같은 모드를 사용해야 합니다.</li> </ul>

- spvst: 표준 PVSTP 모드로 동작합니다. (기본 설정)
- pvst-plus: Cisco사의 PVSTP+ 모드로 동작합니다. 이 모드는 Cisco사의 장비와 연결 시 사용합니다.

# ARP

이 절에서는 ARP(Address Resolution Protocol)에 대해 소개하고, WEBFRONT-K에 ARP와 관련된 설정 작업을 수행하는 방법을 살펴봅니다.

## 개요

ARP(Address Resolution Protocol)는 IP 네트워크 상에서 IP 주소를 MAC 주소로 대응시키기 위해 사용되는 프로토콜입니다. 예를 들어, 장비 A가 장비 B에게 패킷을 전송하려고 할 때, 장비 B의 MAC 주소를 알고 있지 않은 경우에는 ARP 프로토콜을 사용하여 목적지 B의 IP 주소와 MAC 주소 AA:BB:CC:DD:EE:FF를 가지는 ARP 패킷을 전송합니다. 장비 B는 자신의 IP 주소를 가진 ARP 패킷을 받으면 장비 A에게 자신의 MAC 주소를 알려주는 패킷을 보냅니다. 이와 같은 방식으로 수집된 IP 주소와 이에 해당하는 MAC 주소는 장비의 ARP 캐시라고 불리는 메모리에 테이블 형태로 저장됩니다. 저장된 정보는 다음 패킷 전송 시에 사용됩니다.

WEBFRONT-K에서는 위에서 설명한 동적 ARP 기능을 지원할 뿐만 아니라 사용자가 직접 IP 주소와 MAC 주소를 매핑시킬 수 있는 정적 ARP 캐시 기능도 지원합니다. 정적 ARP 캐시 기능을 이용하여 IP 주소와 MAC 주소를 매핑한 경우에는 해당 IP 주소에 대해 동적 ARP 기능이 수행되지 않습니다.

## 정적 ARP 리스트 설정하기

정적 ARP 리스트를 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 네트워크 - ARP</b> 메뉴를 클릭합니다.
2	<정적 ARP 리스트>의 [추가] 버튼을 클릭합니다.
3	<p>&lt;정책 ARP 추가&gt; 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>IP 주소</b> 정적 ARP 리스트에 추가할 IP 주소를 입력합니다. 'A.B.C.D' 형식으로 입력합니다.</li> <li>• <b>MAC 주소</b> IP 주소에 매핑할 MAC 주소를 입력합니다. 'AA:BB:CC:DD:EE:FF' 형식으로 입력합니다.</li> </ul>

## ARP 타임아웃 설정

ARP 타임아웃은 ARP 테이블을 갱신한 이후, 일정 시간 동안 새로운 갱신을 허용하지 않도록 강제하는 기능입니다. ARP 타임아웃을 설정하는 방법은 다음과 같습니다.

순서	설정 과정
1	<b>System - 네트워크 - ARP</b> 메뉴를 클릭합니다.
2	<ARP 타임아웃>의 [변경] 버튼을 클릭합니다.
3	<p>&lt;ARP 타임아웃 설정&gt; 팝업 창에서 다음 설명을 참고하여 타임아웃 값을 설정한 후 [적용] 버튼을 클릭합니다.</p> <div style="text-align: center;">  </div> <ul style="list-style-type: none"> <li>• <b>타임아웃</b> ARP 타임아웃 값을 입력합니다. (설정 범위: 0 ~ 10,000,000, 단위: 1/100(초), 기본값: 100)</li> </ul>

## 제12장 HA

WEBFRONT-K는 안정적인 서비스를 제공하기 위해 HA(High Availability) 기능을 제공합니다. 이 장에서는 WEBFRONT-K의 HA 기능과 함께 이중화된 WEBFRONT-K의 역할이 바뀌는 Failover 방식에 대해 소개한 후, WEBFRONT-K를 이중화하는 데 필요한 설정 작업들을 살펴봅니다.

이 장은 다음 내용으로 구성됩니다.

- HA 개요
- HA 설정하기



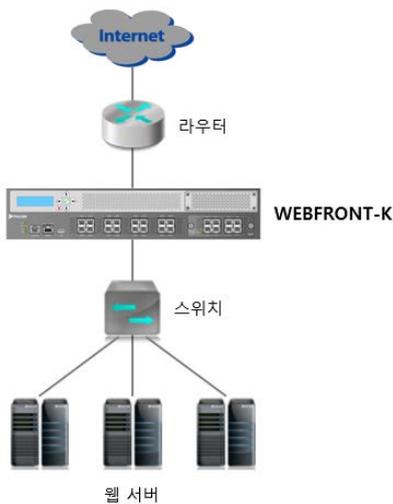
# HA 개요

## HA

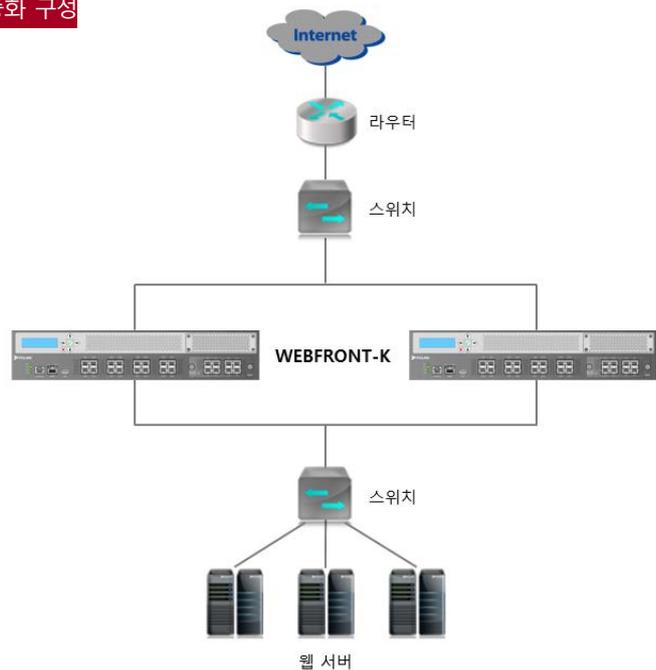
WEBFRONT-K는 장비의 상태에 관계없이 서비스를 지속적으로 제공할 수 있도록 이중화하는 HA(High Availability)를 지원합니다. HA는 2대의 WEBFRONT-K를 사용하여 하나가 비정상적으로 동작하면 나머지 WEBFRONT-K가 비정상적인 WEBFRONT-K의 작업을 이어 받는 기능입니다. 이 기능을 통해 예측할 수 없는 장애가 발생한 경우에도 클라이언트의 요청을 계속 처리할 수 있습니다.

아래 그림 중 왼쪽 그림은 하나의 WEBFRONT-K를 사용하여 구축한 단독 구성(standalone) 네트워크이고, 오른쪽 그림은 2대의 WEBFRONT-K로 이중화한 네트워크입니다.

단독 구성



이중화 구성



[단독 구성과 이중화 구성]

단독 구성에서는 WEBFRONT-K가 정상적으로 동작하지 않는 경우, 클라이언트와 웹 서버 간의 네트워크가 끊어지므로 웹 서버에서 서비스를 제공할 수 없습니다. HA 구성에서는 하나의 WEBFRONT-K가 동작하지 않아도 다른 WEBFRONT-K에 의해 클라이언트와 서버 간의 연결이 계속 유지될 수 있습니다. 이와 같이 이중화된 두 WEBFRONT-K는 직접 연결될 필요 없이 네트워크로 연결되어 서로 통신만 가능하면 됩니다.

## Failover

Failover는 마스터가 정상적으로 동작하지 않을 때, 마스터와 백업의 역할이 서로 바뀌는 과정을 의미합니다. Failover가 발생하면 마스터 WEBFRONT-K를 통해 연결된 세션은 모두 종료되고 백업 WEBFRONT-K에서 새로운 세션을 연결하게 됩니다.

최초에는 2대의 WEBFRONT-K 중에서 먼저 동작한 WEBFRONT-K가 마스터가 됩니다. 이중화로 구성된 WEBFRONT-K가 동작되면, WEBFRONT-K는 통지 간격 동안 상대 WEBFRONT-K로부터 VRRP 패킷을 기다립니다. 그 기간 동안 VRRP 패킷이 수신되지 않으면 자신을 마스터로 설정하게 되고, VRRP 패킷이 수신되면 우선 순위에 따라 그대로 마스터로 동작하거나 혹은 Failover가 발생하게 됩니다.

이 후에는 다음 2가지 상황이 되었을 때 Failover가 발생합니다.

- Dead 간격 동안 마스터로부터 VRRP 패킷이 수신되지 않은 경우
- 마스터의 우선 순위가 백업 우선 순위보다 낮은 경우

Failover가 발생하는 2가지 상황에 대해 살펴봅니다.

## Dead 간격

Failover가 발생하는 첫번째 상황은 백업 WEBFRONT-K가 dead 간격(통지 간격 x 최대 재시도 횟수 + 0.5 x 마스터 ARP 검사 횟수) 이 경과할 때까지 마스터로부터 VRRP 패킷을 수신하지 못한 경우입니다. 이러한 경우, 백업은 마스터가 정상적으로 동작하지 않는 것으로 판단하고 자신이 마스터로 동작하게 됩니다. 마스터가 dead 간격 이내에 VRRP 패킷을 전송할 수 없는 경우는 장비가 다운되었거나 리부팅되었거나 혹은 백업 WEBFRONT-K의 네트워크와 연결된 포트가 동작하지 않는 경우 등이 있습니다.

Dead 간격을 결정하는 3가지 값(통지 간격, 최대 재시도 횟수, 마스터 ARP 검사 횟수)은 각각 다음과 같은 의미를 가집니다.

- 통지 간격                                    마스터가 VRRP 패킷을 전송하는 주기
- 최대 재시도 횟수                         백업이 마스터로 VRRP 패킷의 재전송을 요청하는 횟수
- 마스터 ARP 검사 횟수                 백업이 마스터로 ARP 요청 패킷을 전송하는 횟수

즉, 백업 WEBFRONT-K는 VRRP 패킷 전송 주기가 경과할 때까지 마스터로부터 VRRP 패킷이 도착하지 않으면, 설정된 최대 재시도 횟수만큼 VRRP 패킷의 재전송을 요청합니다. 그리고, 최대 재시도 횟수만큼 VRRP 패킷의 재전송을 요청한 후에도 VRRP 패킷이 도착하지 않을 경우, 마스터 장비가 동작 중인지를 확인하기 위해 다시 ARP 요청 패킷을 마스터 ARP 검사 횟수만큼 마스터로 전송합니다. 그 이후에도 ARP 응답 패킷이 수신되지 않으면 마스터 장비가 동작하지 않는 것으로 판단하게 되는 것입니다. 이 값들은 각각 1초(통지 간격)와 3회(최대 재시도 횟수), 0(마스터 ARP 검사 횟수)으로 지정되어 있는데, 상황에 따라 사용자가 더 적절한 값으로 변경할 수 있습니다.

## 우선 순위

Failover가 발생하는 두번째 상황은 백업 WEBFRONT-K가 수신한 VRRP 패킷에 담긴 마스터의 우선순위가 백업의 우선 순위보다 낮은 경우입니다. 이런 경우에도 Failover가 발생하여 백업이 마스터로, 마스터는 백업으로 동작하게 됩니다. 우선 순위는 다음 공식에 의해 계산됩니다.

$$\text{우선 순위} = \text{기본 우선 순위} + \text{트랙포트 우선 순위}$$

트랙 포트 우선 순위가 설정되어 있는 경우에는 트랙 포트 우선 순위가 기본 우선 순위에 더해집니다.

### 트랙 포트 우선 순위

트랙 포트 우선 순위는 트랙 포트에 설정된 포트에 할당되는 우선 순위입니다. 포트가 정상적으로 연결되어 있는 경우에는 포트의 우선 순위가 기본 우선 순위에 더해지고, 정상적이지 않은 경우에는 더해지지 않습니다. 트랙 포트 우선 순위를 사용하면 포트의 동작 상태를 마스터 선택에 반영할 수 있습니다. 트랙 포트의 우선 순위를 기본 우선 순위에 더하는 방식에는 다음과 같은 '멤버 우선 순위'와 '개별 우선 순위'가 있습니다.

- 멤버 우선 순위

멤버 우선 순위는 두 개 이상의 포트를 하나의 트래크 포트 그룹으로 설정하고, 트래크 포트 그룹에 우선 순위를 부여합니다. 그룹에 속한 모든 포트가 연결되어 있지 않은 경우에만 우선 순위를 더하지 않고, 포트 중 하나라도 정상적으로 연결되어 있으면 기본 우선 순위에서 트래크 포트 그룹의 우선 순위가 더해집니다. 예를 들어, 기본 우선 순위가 100 이고, 포트 1, 2, 3을 하나의 트래크 포트 그룹으로 구성하고 우선 순위를 30으로 설정한 경우, 포트 1, 2, 3 의 연결 상태가 모두 다운되지 않는 이상, 우선 순위는 130으로 유지됩니다.

- 개별 우선 순위

개별 우선 순위는 각 포트마다 우선 순위를 부여하고, 포트의 연결 상태에 따라 기본 우선 순위에서 포트의 우선 순위를 더하거나 혹은 더하지 않는 방식입니다. 예를 들어, 기본 우선 순위가 100 고, 포트 1, 2, 3 각각을 우선 순위가 10 인 트래크 포트에 설정한 경우, 우선 순위는 130 이 됩니다. 만약, 하나의 포트가 연결이 끊어지면 해당 포트의 우선 순위가 더해지지 않으므로 VRRP 그룹의 우선 순위는 10만큼 감소하여 120이 됩니다.

## 가상 IP 주소와 서비스 가상 IP 주소

가상 IP 주소는 WEBFRONT-K에 연결된 호스트나 장비에서 WEBFRONT-K의 인터페이스로 통신하기 위해 사용하는 IP 주소입니다. 마스터와 백업 WEBFRONT-K의 인터페이스에 실제 IP 주소가 설정되어 있지만, 두 WEBFRONT-K 중 어느 장비가 마스터로 동작할지 알 수 없으므로 이러한 가상 IP 주소를 대신 사용하게 됩니다. 일반적으로 WEBFRONT-K의 모든 인터페이스에 가상 IP 주소를 설정합니다.

서비스 가상 IP 주소는 부하 분산 서비스의 가상 IP 주소입니다. 클라이언트는 서비스 가상 IP 주소를 실제 서버의 IP 주소로 인식하고, 서비스 가상 IP 주소를 목적지 IP 주소로 하여 서버로 서비스를 요청합니다. 서비스 가상 IP 주소로 수신된 데이터는 부하 분산 서비스에 의해 서버로 전송됩니다. WEBFRONT-K에는 최대 10개의 서비스 가상 IP 주소를 설정할 수 있습니다.

## 백업 시 차단 포트

브리지 모드의 이중화 구성에서 루프가 만들어지는 것을 방지하기 위해서는 백업 WEBFRONT-K의 특정 포트를 차단할 수 있습니다. 백업 시 차단할 포트를 설정하면 해당 포트의 링크는 up 상태로 유지되지만 데이터가 송수신되지 않기 때문에 루프가 형성되는 것을 방지할 수 있습니다.

루프를 방지하는 데에는 백업 WEBFRONT-K의 포트를 차단하는 방법 외에도 STP를 사용하는 방법이 있습니다. STP를 사용할 경우 속도가 느려질 수 있으므로 이중화 구성에서는 백업 WEBFRONT-K의 포트를 차단하는 방법을 더 권장합니다. 두 방법은 동시에 사용할 수 없으므로, 백업 시 차단할 포트를 설정한 경우에는 반드시 STP를 비활성화해야 합니다.

백업 시 차단 포트가 설정된 WEBFRONT-K가 마스터에서 백업으로 되는 경우, 먼저 해당 포트가 차단되고 이 후에 WEBFRONT-K가 백업이 됩니다. 이 때, 백업 시 차단 포트의 링크가 잠시 Down되었다가 다시 Up 상태가 됩니다. 반대로, 백업에서 마스터로 되는 경우에는 WEBFRONT-K가 마스터가 되고 그 이후에 포트의 차단이 해제됩니다.

# HA 설정하기

두 WEBFRONT-K를 이중화하기 위해 필요한 설정 작업에 대해 살펴봅니다.

## 설정하기 전에

이중화하는 두 WEBFRONT-K는 반드시 설정이 동일해야 합니다. 두 WEBFRONT-K를 동일하게 설정하려면 설정 동기화 기능을 사용하거나 설정을 파일로 저장한 후 다른 WEBFRONT-K로 업로드하면 됩니다.

## VRRP 그룹 설정하기

두 WEBFRONT-K를 동일하게 설정한 후, 다음과 같은 방법으로 VRRP 그룹의 정보를 설정합니다.

순서	설정 과정
1	<b>System - HA</b> 메뉴를 클릭합니다.
2	<b>&lt;Failover 정보&gt;</b> 의 <b>[추가]</b> 버튼을 클릭합니다.
3	<p><b>&lt;Failover 설정&gt;</b>에서 다음 설명을 참고하여 각 항목을 설정합니다.</p>  <ul style="list-style-type: none"> <li>• <b>상태</b> 현재 등록하고 있는 VRRP의 사용 여부를 지정합니다. (기본값: 활성화)</li> <li>• <b>ID</b> VRRP ID를 지정합니다. WEBFRONT-K는 동일한 VRRP ID를 가진 그룹과 VRRP 패킷을 주고 받으므로 이중화하는 WEBFRONT-K와 동일한 값으로 설정해야 합니다. (설정 범위: 1 ~ 254)</li> <li>• <b>모드</b> Failover 동작 모드를 선택합니다.             <ul style="list-style-type: none"> <li>- Active-standby: Active-standby 방식으로 동작</li> <li>- Active-active: Active-active 방식으로 동작</li> </ul> </li> <li>• <b>기본 우선 순위</b> 기본 우선 순위를 지정합니다. (설정 범위: 0 ~ 255, 기본값: 100)</li> <li>• <b>통지 간격</b> VRRP 패킷의 전송 주기를 설정합니다. (설정 범위: 1 ~ 255, 기본값: 1초)</li> <li>• <b>최대 재시도 횟수</b> 통지 간격 항목에 설정된 시간이 경과할 때까지 마스터로부터 VRRP 패킷이 도착하지 않을 경우 VRRP 패킷을 다시 전송하도록 마스터에 요청할 횟수를 지정합니다. (설정 범위: 1 ~ 255, 기본값: 3)</li> <li>• <b>마스터 ARP 검사 횟수</b> 최대 재시도 횟수에 설정된 횟수만큼 VRRP 패킷의 재전송을 요청한 후에도 VRRP 패킷이 도착하지 않을 경우, 마스터 장비가 동작 중인지 확인하기 위해 마스터로 ARP 요청 패킷을 전송할 횟수를 지정합니다. 이 항목에서 설정한</li> </ul>

횟수만큼 ARP 요청 패킷을 전송한 후에도 ARP 응답 패킷이 수신되지 않으면 마스터 장비가 다운된 것으로 판단하고 Failover가 일어납니다. (설정 범위: 0 ~ 255, 기본값: 0)

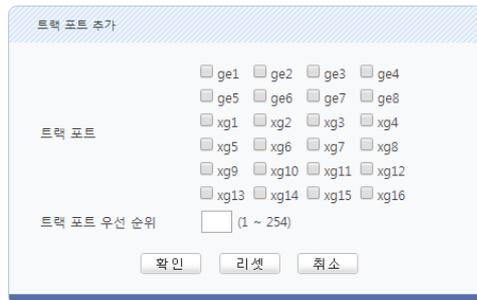
• **가상 MAC 상태**

VRRP 그룹의 가상 IP 주소와 서비스 가상 IP 주소에 대한 MAC 주소로 가상 MAC 주소를 사용할 것인지 인터페이스의 실제 MAC 주소를 사용할 것인지 지정합니다. VRRP 그룹의 ID를 사용하여 자동으로 생성된 가상 MAC 주소를 사용하려면 '활성화'를, 인터페이스의 실제 MAC 주소를 사용하려면 '비활성화'를 선택합니다. (기본값: 활성화)

• **트랙 포트 리스트**

다음과 같은 방법으로 우선 순위 계산 시 사용할 트랙 포트를 추가합니다. 트랙 포트 우선 순위는 8개까지 설정할 수 있습니다.

- ❶ 리스트의 아래에 있는 [추가] 버튼을 클릭합니다.
- ❷ <트랙 포트 추가> 팝업 창이 나타납니다.



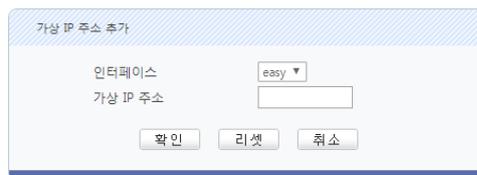
트랙 포트 항목에서 트랙 포트에 추가할 포트를 선택하고 트랙 포트 우선순위 항목에서는 트랙 포트에 할당할 우선 순위를 1~255 범위의 값으로 입력한 후 [확인]을 클릭합니다. 트랙 포트에 하나의 포트만 추가하면 포트가 다운되었을 때 우선 순위는 다운된 포트에 할당된 우선 순위만큼 감소합니다(개별적 우선 순위). 트랙 포트에 여러 개의 포트를 같이 지정하면, 트랙 포트에 속한 모든 포트가 다운되기 전에는 우선 순위는 변경되지 않습니다. 트랙 포트의 모든 포트가 다운되었을 때 트랙 포트에 할당된 우선 순위만큼 전체 우선 순위가 감소하게 됩니다. (멤버 우선순위)

- ❸ 선택한 트랙 포트와 입력한 우선 순위가 리스트에 추가됩니다.

• **가상 IP 주소 리스트(필수)**

다음과 같은 방법으로 인터페이스의 가상 IP 주소를 지정합니다. 하나의 인터페이스에는 최대 8개의 가상 IP 주소를 지정할 수 있습니다.

- ❶ 리스트의 아래에 있는 [추가] 버튼을 클릭합니다.
- ❷ <가상 IP 주소 추가> 팝업 창이 나타납니다.



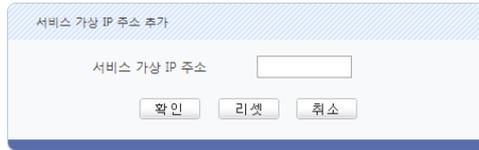
인터페이스 드롭다운 목록을 클릭한 후 가상 IP 주소를 설정할 VLAN 인터페이스를 선택합니다. 그리고, 가상 IP 주소 항목에는 선택한 인터페이스에 지정할 가상 IP 주소를 입력한 후 [확인] 버튼을 클릭합니다.

- ❸ 입력한 인터페이스의 가상 IP 주소가 리스트에 추가됩니다.

• **서비스 가상 IP 주소 리스트**

다음과 같은 방법으로 서비스 가상 IP 주소를 지정합니다. 최대 10개의 서비스 가상 IP 주소를 지정할 수 있습니다.

- ❶ 리스트의 아래에 있는 [추가] 버튼을 클릭합니다.
- ❷ <서비스 가상 IP 주소 추가> 팝업 창이 나타납니다. 서비스 가상 IP 주소 항목에 Failover를 적용할 부하 분산 서비스의 IP 주소를 입력한 후 [확인] 버튼을 클릭합니다.



⑥ 입력한 인터페이스의 가상 IP 주소가 리스트에 추가됩니다.



**주의:** 애플리케이션이 부하 분산 모드로 동작하고 있는 경우에는 반드시 서비스 가상 IP 주소를 입력해야 합니다.

## 백업 시 차단 포트 설정하기

브리지 모드의 이중화 구성에서 WEBFRONT-K가 백업 상태가 되었을 때, 루프를 방지하기 위해 차단할 포트를 지정합니다. 다음은 백업 시 차단 포트를 설정하는 방법입니다.

순서	설정 과정
1	<b>System - HA</b> 메뉴를 클릭합니다.
2	< <b>Failover 정보</b> >의 [ <b>추가</b> ] 버튼을 클릭합니다.
3	< <b>백업 시 차단 포트</b> >에서 백업 시 차단할 포트를 선택한 후 [ <b>적용</b> ] 버튼을 클릭합니다.

백업 시 차단 포트

ge1    ge2    ge3    ge4    ge5    ge6    ge7    ge8    xg1    xg2    xg3    xg4  
 xg5    xg6    xg7    xg8    xg9    xg10    xg11    xg12    xg13    xg14    xg15    xg16

## HA 기능 활성화하기

다음은 HA 기능을 활성화하는 방법입니다.

순서	설정 과정
1	<b>System - HA</b> 메뉴를 클릭합니다.
2	< <b>Failover 리다이렉트 정보</b> >의 [ <b>변경</b> ] 버튼을 클릭합니다.
3	< <b>Failover 리다이렉트 정보 설정</b> >화면에서 '활성화'를 선택하고 [ <b>적용</b> ] 버튼을 클릭합니다. (기본값: 비활성화)

Failover 리다이렉트 정보 설정

• 상태    활성화    비활성화

