PIOLINK Web Application Firewall

# WEBFRONT-K

## 애플리케이션 구성 설명서

Rev 1.2

PIOLINK

## 등록 상표

PIOLINK는 ㈜파이오링크의 등록 상표입니다.

## 일러두기




WEBFRONT-K 애플리케이션 구성 설명서 Rev 1.2 (2017.09.)





전화: 02-2025-6900  Web Page: www.piolink.com

# 설명서 소개

이 WEBFRONT-K 애플리케이션 구성 설명서는 WEBFRONT-K가 제공하는 애플리케이션 보안 기능을 설정하는 방법을 소개합니다. 애플리케이션 보안 기능은 WEBFRONT-K를 네트워크에 설치하고 WEBFRONT-K를 동작시키기 위한 기본적인 설정 작업들을 완료한 후에 설정합니다.

## 대상 독자

이 설명서는 WEBFRONT-K의 애플리케이션 보안 기능을 구성하고 모니터링할 수 있는 통합 관리자, 사이트 관리자, 애플리케이션 관리자 권한을 가진 독자를 대상으로 작성되었습니다.

## PLOS 버전

이 설명서는 PLOS v2.0.58.0.8 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. 최신 버전의 PLOS로 업데이트하는 방법은 이 설명서와 함께 제공되는 <**WEBFRONT-K 시스템 구성 설명서**>의 [**제7장 시스템 및 사용자 관리**]에 설명되어 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. |

## 관련 문서

이 설명서와 함께 다음과 같은 설명서가 추가로 제공됩니다.

- WEBFRONT-K 소개서 (Overview Guide)

  WEBFRONT-K 를 도입해야 하는 필요성과 WEBFRONT-K 를 사용한 네트워크 구성, 그리고 WEBFRONT-K 가 제공하는 기능에 대해 상세하게 소개하는 설명서입니다. WEBFRONT-K 가 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-K 를 사용하기 위해 필수적인 설치 및 구성 과정을 설명하는 설명서입니다. 이 설명서를 참고하면 어떤 과정을 거쳐서 WEBFRONT-K 를 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-K 의 앞면, 뒷면, 옆면에 있는 각 부분의 기능을 소개하고, WEBFRONT-K 를 랙에 설치한 후 각 포트에 장비를 연결하는 방법을 알려주는 설명서입니다. WEBFRONT-K 의 하드웨어 사양과 장비 연결시 사용하는 케이블에 대한 상세한 사양도 이 설명서에서 볼 수 있습니다.

- WEBFRONT-K 시스템 구성 설명서 (System Configuration Guide)

  WEBFRONT-K Web Manager 의 System 메뉴에 대해 설명하고 있는 설명서입니다. WEBFRONT-K Web Manager 는 WEBFRONT-K 를 관리하는 GUI 인터페이스입니다. System 메뉴는 WEBFRONT-K 의 통합 관리자와 사이트 관리자만 사용할 수 있는 메뉴로, System 메뉴를 사용하여 WEBFRONT-K 시스템을 설정하거나 네트워크 설정, 애플리케이션과 사용자 관리 및 WEBFRONT-K 와 전체 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): 1544-9890
- E-mail: support@piolink.com

# 설명서 구성

이 설명서의 각 장은 다음과 같은 내용으로 구성되어 있습니다.

### 제1장 시작하기 전에

이 장에서는 애플리케이션 관리자 또는 애플리케이션 모니터가 WEBFRONT-K에 로그인하는 방법과, WEBFRONT-K에 접속하였을 때 나타나는 시작 화면, 애플리케이션 설정 메뉴, 설정 화면과 설정 버튼에 대해 소개합니다. 애플리케이션 보안 기능을 설정하기 전에 이 부분을 참고하면, 보다 쉽게 설정 메뉴와 화면 구성을 이해할 수 있고, 기능을 설정하는데 도움이 될 수 있습니다.

### 제2장 애플리케이션 기본 설정

이 장에서는 등록한 애플리케이션마다 기본적으로 설정해야 하는 일반 설정과 응답 설정을 하는 방법과 애플리케이션의 각 보안 기능을 설정할 때 사용되는 정규식을 정의하는 방법, 세션 연결 유지를 위한 세션 정보 설정 방법, 인코딩 방식을 설정하는 방법을 소개합니다.

### 제3장 요청 검사 기능 설정

요청 검사는 WEBFRONT-K가 클라이언트로부터 웹 서버로 보내는 요청이 정상적인 요청인지, 공격자가 보낸 공격인지를 검사하여 대응하는 조치를 취하도록 하는 기능입니다. 이 장에서는 WEBFRONT-K에서 제공하는 각 요청 검사 기능을 설정하는 방법에 대해 소개합니다.

### 제4장 컨텐트 보호 기능 설정

컨텐트 보호는 WEBFRONT-K가 웹 서버가 클라이언트로 보내는 응답 메시지를 검사하여, 응답 메시지에 기밀 정보를 포함하고 있거나, 응답 웹이 변조된 경우에 대응하는 조치를 취하도록 하는 응답 검사 기능입니다. 이 장에서는 WEBFRONT-K에서 제공하는 각 컨텐트 보호 기능을 설정하는 방법에 대해 상세하게 소개합니다.

### 제5장 학습 기능 설정

학습 기능은 클라이언트가 웹 서버로 보내는 요청 패킷 중에서 WEBFRONT-K에 설정한 요청 검사 정책에 의해 허용되지 않는 요청 패킷에 대한 정보를 기록하는 기능입니다. 관리자는 학습을 통해 얻은 정보를 이용하여 WEBFRONT-K에 요청 검사 기능에 대한 정책을 설정할 수 있습니다. WEBFRONT-K는 애플리케이션 접근 제어 학습, 폼 필드 학습 2가지 종류의 학습 기능을 제공합니다. 이와 같은 학습 기능을 사용하는 방법은 모두 동일합니다. 그러므로, 이 장에서는 각각의 학습 기능 사용 방법을 설명하지 않고, 접근 제어 학습 기능을 사용하는 방법을 예를 들어 학습 기능을 설정하는 방법과 학습 기능을 통해 얻은 정보를 사용하는 방법을 소개합니다.

### 제6장 위장 기능 설정

위장은 클라이언트와의 연결에 사용되는 URL을 웹 서버의 실제 URL과 다르게 변환하거나, 중요한 웹 서버의 정보를 숨김 또는 변환하는 기능입니다. 이 장에서는 WEBFRONT-K에서 지원하는 URL 정보 위장 기능과 서버 정보 위장 기능을 설정하는 방법에 대해 상세하게 소개합니다.

### 제7장 부하 분산 기능 설정

서버 부하 분산은 자신을 통해 전송되는 인터넷 트래픽을 IP 패킷 데이터의 영역까지 검사하여 트래픽을 가장 적절한 웹 서버로 보내고, 서비스를 제공하지 않을 트래픽은 차단시켜주는 L7 부하 분산 기능입니다. 이 장에서는 WEBFRONT가 제공하는 서버 부하 분산 기능을 설정하는 방법을 상세하게 설명합니다.

### 제8장 SSL 기능 설정

SSL(Secure Sockets Layer) 기능은 WEBFRONT-K를 통해 전송되는 패킷을 암호화(encryption)하거나 복호화(decryption)하여 패킷의 안전성과 신뢰성을 보장할 수 있는 기능입니다. 이 장에서는 WEBFRONT-K가 제공하는 SSL 기능을 설정하는 방법을 상세하게 설명합니다.

### 제9장 애플리케이션 로그

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

### 제10장 애플리케이션 모니터링

이 장에서는 WEBFRONT-K의 애플리케이션 모니터링 기능을 통해 WEBFRONT-K의 애플리케이션 보안 기능의 상태와 통계 정보 등을 파악하는 방법에 대해 설명합니다.

# 목차

# 제1장 시작하기 전에

이 장에서는 애플리케이션 관리자가 WEBFRONT-K에 로그인하는 방법과 WEBFRONT-K에 접속하였을 때 나타나는 시작 화면, 애플리케이션 설정 메뉴와 설정 화면, 그리고 설정 버튼에 대해 소개합니다. 애플리케이션 보안 기능을 사용하기 전에 이 장의 내용을 참고하여 메뉴와 화면 구성, 버튼의 기능 등을 이해해두면 기능을 설정하는데 많은 도움이 될 수 있습니다.

이 장은 다음 내용으로 구성되어 있습니다.



**참고:** WEBFRONT-K의 웹 애플리케이션 보안 기능을 사용하기 위해서는 먼저 WEBFRONT-K에 대상 웹 애플리케이션을 등록해야 합니다. 웹 애플리케이션 등록은 시스템 관리자가 [**System-애플리케이션-애플리케이션 관리**] 메뉴를 사용하여 할 수 있습니다. 웹 애플리케이션을 등록하는 방법은 이 설명서와 함께 제공되는 **WEBFRONT-K 시스템 구성 설명서**의 [**제4장 애플리케이션**]을 참고합니다.

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

# 로그인하기

애플리케이션 보안 기능을 설정을 하기 위해 WEBFRONT-K에 접속하고 WEBFRONT-K의 Web Manager로 로그인하는 방법은 다음과 같습니다.

**참고:** WEBFRONT-K를 설치하고 최초로 Web Manager에 접속한 경우에는 제품 라이센스 등록이 필요합니다. 제품 라이센스를 등록하는 방법은 이 설명서와 함께 제공되는 **WEBFRONT-K 시스템 구성 설명서**의 [**제1장 시작하기 전에 – 라이센스 등록**]절을 참고합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | WEBFRONT-K로 접속할 사용자 PC를 준비합니다. 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. |
| 2 | 사용자 PC에 인터넷 익스플로러나 크롬과 같은 웹 브라우저를 실행합니다. 그리고, 웹 브라우저의 주소 입력란에 'https://WEBFRONT-K의 IP 주소:8443'을 입력한 후 [**Enter**] 키를 누르거나 [**이동**] 버튼을 클릭합니다. WEBFRONT-K의 IP 주소는 관리용 인터페이스나 VLAN 인터페이스의 IP 주소를 사용하면 됩니다.<br>  <br><br>**주의:** 주소를 입력할 때 **https** 대신 **http**를 입력하지 않았는지 확인합니다. http로 입력하면 WEBFRONT-K에 접속할 수 없습니다.<br>**참고:** 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. |
| 3 | WEBFRONT-K의 Web Manager로 로그인하기 위해 로그인 ID와 암호를 입력하고 언어를 선택하는 화면이 나타납니다. ID와 Password 항목에 각각 시스템 관리자한테서 부여 받은 로그인 ID와 암호를 입력합니다. 그리고, Language 항목을 클릭한 후 원하는 언어를 선택합니다. 각 항목들을 모두 설정하였으면 [**Login**] 버튼을 클릭합니다. |
| 4 | Web Manager에 정상적으로 로그인하면 시작 화면이 나타납니다. 시작 화면은 로그인 ID의 사용자 종류(통합 관리자, 시스템 관리자, 애플리케이션 관리자-관리자/모니터 권한, 모니터 관리자)에 따라 달라집니다. 다음 화면은 관리자 권한을 가진 애플리케이션 관리자로 로그인한 경우에 나타나는 화면입니다.<br>  <br> |

**참고: 모니터 권한을 가진 애플리케이션 관리자로 로그인한 경우**


모니터 권한을 가진 애플리케이션 관리자로 로그인한 경우에는 화면에 Application 메뉴가 모두 표시되지 않습니다. 왼쪽 그림과 같이 모니터링할 수 있는 2개의 메뉴(로그, 모니터링)만 표시됩니다.

**참고: Web Manager에서 로그아웃하기**

WEBFRONT-K Web Manager에서 로그아웃하려면 Web Manager 화면의 오른쪽 위에 있는 **Logout**을 클릭하면 됩니다.

# 시작 화면 구성

애플리케이션 관리자로 로그인했을 때 볼 수 있는 Web Manager의 시작 화면은 다음과 같은 부분으로 구성됩니다.


**참고:** 이 설명서는 애플리케이션 관리자가 애플리케이션 메뉴를 사용하는 경우를 가정하고 작성되었습니다. 따라서, 화면 구조나 메뉴들도 애플리케이션 관리자로 로그인했을 때 나타나는 화면을 기준으로 설명합니다. 통합 관리자나 시스템 관리자로 로그인했을 때 볼 수 있는 시작 화면의 구성이나 메뉴 등은 **WEBFRONT-K 시스템 구성 설명서**를 참고합니다

각 부분의 기능은 다음과 같습니다.

❶ 애플리케이션 보안 기능을 설정할 수 있는 Application 메뉴입니다. Application 메뉴는 시스템 관리자가 사용자를 등록할 때 각 애플리케이션에 지정한 사용자 권한에 따라 조금 다릅니다. 애플리케이션을 관리할 수 있도록 지정한 경우에는 앞의 시작 화면에서와 같이 애플리케이션을 설정하는 메뉴와 모니터링 메뉴가 모두 나타납니다. 애플리케이션을 모니터만 할 수 있도록 지정한 경우에는 다음과 같이 애플리케이션 모니터링 관련 메뉴만 나타납니다.


❷ 현재 선택된 메뉴의 위치를 나타내는 부분입니다. 작업 화면의 설정 화면이 어느 메뉴에 해당되는 내용인지를 쉽게 알 수 있습니다.

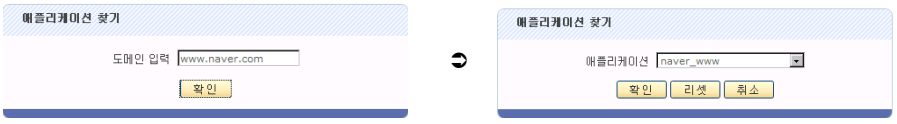
❸ 현재 WEBFRONT-K로 로그인한 사용자의 ID를 보여주고 로그아웃(Logout)하거나 혹은 사용자 환경을 설정(Preference)할 수 있는 부분입니다. Preference를 클릭하면 사용자 환경을 설정할 수 있는데, 바로가기를 설정하거나 기본 메뉴 모드와 로그인 유지시간, 로그인 암호를 변경할 수 있습니다.

❹ 설정하거나 모니터링할 애플리케이션을 선택하는 부분입니다.  아이콘을 클릭하면 애플리케이션을 선택할 수 있는 팝업 창이 나타납니다.


애플리케이션 드롭다운 목록에는 시스템 관리자가 등록해 놓은 애플리케이션이 나타납니다. 이 애플리케이션 중에서 설정하거나 모니터링할 애플리케이션을 선택한 후 [**확인**] 버튼을 클릭합니다.

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

❻ WEBFRONT-K에 등록된 애플리케이션을 검색하는 아이콘입니다. 이 아이콘을 클릭하면 <**애플리케이션 찾기**> 팝업 창이 나타납니다. 이 창에서 찾고자 하는 애플리케이션의 도메인을 입력한 후 [**확인**]을 클릭하면 해당 도메인의 애플리케이션이 표시해줍니다.




다른 애플리케이션을 검색하려면 [**리셋**]을 클릭한 후 다시 도메인을 입력하면 됩니다.

# 애플리케이션 메뉴

이 절에서는 각 Application 메뉴의 기능에 대해 간략하게 소개합니다.

## 기본 메뉴 모드

### 애플리케이션

애플리케이션 메뉴는 애플리케이션의 기본 정보를 설정할 수 있는 다음과 같은 메뉴로 구성되어 있습니다.

| 메뉴 | 설명 |
|---|---|
| 일반 설정 | 동작 모드, IP 주소/포트, 보조 도메인 등 장비가 동작하기 위해 필요한 기본적인 항목을 설정합니다. |
| 응답 설정 | 애플리케이션 보안 기능의 각 정책이 허용하지 않는 패킷을 발견한 경우에 해당 패킷을 전송한 클라이언트에게 패킷이 차단되거나 에러가 발생하였음을 알려주는 방식을 설정합니다. |
| 기타 설정 | 인코딩 방식과 세션 지속 연결 기능, 애플리케이션 URL의 대소문자 구분, 쿼리스트링 검사, 쿠키 매개변수 검사, 사용자 IP 표기 헤더명 변경, XML 요청 검사, 매개변수 검사 길이 제한, 프로토콜 정보 검사를 수행할지 여부를 지정합니다. |

### 요청검사

요청 검사 메뉴는 클라이언트의 요청을 검사하는 데 사용할 규칙을 정의할 수 있는 다음 메뉴들로 구성되어 있습니다. 요청 검사 기능을 설정하는 방법은 이 설명서의 [**제 3 장 요청 검사 기능 설정**]에 상세히 설명되어 있습니다.

| 메뉴 | 기능 |
|---|---|
| 접근 제어 | 웹 서버에서 제공하는 어플리케이션 중에서 사용자가 접근할 수 있는 URL 목록을 설정하여, 목록에 설정된 URL에만 접속이 가능하게 하는 애플리케이션 접근 제어 기능을 설정합니다. |
| 폼필드 검사 | 클라이언트가 웹 서버로 보내는 요청 웹 페이지에 포함된 폼 필드가 변조되었는지를 검사하는 폼 필드 검사 기능을 설정합니다. |
| 과다 요청 제어 | 클라이언트에서 웹 서버로 보내는 요청 패킷 수가 지정한 시간 동안 일정한 양을 초과하지 않도록 요청 패킷의 양을 적절하게 제한해주는 과다 요청 제어 기능을 설정합니다. |
| 쿠키 보호 | 클라이언트가 웹 서버로 보내는 요청 패킷에 포함된 쿠키를 검사하여 쿠키의 변조 여부를 검사하는 쿠키 보호 기능을 설정합니다. |
| 버퍼 오버플로우 차단 | 클라이언트가 웹 서버로 보내는 요청 패킷의 HTTP 헤더, URL, 쿠키의 길이를 지정한 길이와 비교하거나, HTTP 요청에 포함된 쉘 코드의 유형을 검사해내는 버퍼 오버플로우 기능을 설정합니다. |
| SQL 삽입 차단 | 클라이언트가 웹 서버로 보내는 폼 필드 문자열에 지정한 SQL 키워드가 포함되었는지를 검사하여 SQL 삽입 공격 여부를 검사하는 SQL 삽입 차단 기능을 설정합니다. |
| 스크립트 삽입 차단 | 클라이언트가 웹 서버로 보내는 폼 필드의 문자열에 비정상적인 스크립트(Cross Site Scripting(XSS)공격과 관련된 코드)가 포함되어있는지를 검사하는 스크립트 삽입 차단 기능을 설정합니다. |
| 업로드 검사 | 클라이언트가 웹 서버로 업로드하려는 파일을 검사하여 공격 가능성이 있는 파일을 업로드하지 못하도록 제한하는 업로드 검사 기능을 설정합니다. |
| 다운로드 검사 | 특정한 이름의 파일이나 특정 확장자를 가진 파일을 웹 서버에서 다운로드하지 못하도록 차단하는 다운로드 검사 기능을 설정합니다. |
| 디렉토리 리스팅 차단 | '/'로 끝나는 URL을 입력했을 때 해당 디렉토리에 있는 모든 파일과 디렉토리 목록이 출력되는 것을 막기 위해 해당 요청을 차단하는 디렉토리 리스팅 차단 기능을 설정합니다. |
| 요청 형식 검사 | 클라이언트가 웹 서버로 보내는 요청 패킷의 형식을 검사하여 정상적인 요청 패킷인지를 검사하는 형식 검사 기능을 설정합니다. |
| 검사 회피 차단 | 요청 검사를 회피하여 공격을 수행할 가능성이 있는 요청 URL을 찾아내어 차단하는 검사 회피 차단 기능을 설정합니다. |

| | |
|---|---|
| 인클루드 인젝션 차단 | 클라이언트가 웹 서버로 보내는 요청 패킷에 인클루드 인젝션 공격 구문이 포함되었는지를 검사하는 인클루드 인젝션 차단 기능을 설정합니다. |
| 웹 공격 프로그램 차단 | 웹 공격에 사용되는 웹 스캐너, 웹 크롤러, 프록시 툴 등의 프로그램을 사용하여 공격하는 것을 차단하기 위한 웹 공격 프로그램 차단 기능을 설정합니다. |
| HTTP POST 공격 차단 | HTTP POST 메서드를 사용하여 웹 서버와의 커넥션을 장시간 유지하는 L7 DDoS 공격을 차단하기 위한 HTTP POST 차단 기능을 설정합니다. |
| Slowloris 공격 차단 | HTTP 헤더를 느리게 전송하여 세션을 장시간 유지하는 Slowloris 공격 차단 기능을 설정합니다. |
| Slow Read 공격 차단 | 매우 작은 수신 버퍼를 사용하여 웹 서버의 데이터를 천천히 읽음으로써 자원을 고갈시키는 HTTP Slow Read 공격 차단 기능을 설정합니다. |
| 금칙어 차단 | 클라이언트가 웹 서버로 보내는 요청 패킷에 비방, 광고, 욕설, 선정적 내용과 같이 규칙에 어긋나는 단어가 포함되었는지를 검사하는 금칙어 차단 기능을 설정합니다. |
| 신용카드정보 유입 차단 | 클라이언트가 웹 서버로 보내는 요청 내용에 신용카드 정보가 포함되었는지 검사하여, 포함된 경우에 이를 차단하는 신용카드정보 유입 차단 기능을 설정합니다. |
| 주민등록정보 유입 차단 | 클라이언트가 웹 서버로 보내는 요청 내용에 주민등록 정보가 포함되었는지 검사하여, 포함된 경우에 이를 차단하는 주민등록정보 유입 차단 기능을 설정합니다. |
| WISE 요청 필터 | 클라이언트가 웹 서버로 보내는 요청 패킷에 대한 항목, 변수, 값, 조건 등 필터의 규칙을 세부적으로 설정하여 요청 패킷을 필터링하는 WISE 요청 필터를 설정합니다. |

### 컨텐트보호

컨텐트 보호 메뉴는 웹 서버의 응답을 검사하는 데 사용할 규칙을 정의할 수 있는 다음 메뉴들로 구성되어 있습니다. 컨텐트 보호 기능을 설정하는 방법은 이 설명서의 [**제4장 컨텐트 보호 기능 설정**]에 상세히 설명되어 있습니다.

| 메뉴 | 기능 |
|---|---|
| 신용카드정보 유출 차단 | 웹 서버가 클라이언트로 보내는 응답에 신용 카드 정보가 포함되었는지 검사하여, 포함된 경우에는 이를 특정 문자로 변환한 후 전송하거나 응답을 차단하는 신용카드 정보 유출 차단 기능을 설정합니다. |
| 주민등록정보 유출 차단 | 웹 서버가 클라이언트로 보내는 응답에 주민 등록 정보가 포함되었는지 검사하여, 포함된 경우에는 이를 특정 문자로 변환한 후 전송하거나 응답을 차단하는 주민 등록 정보 유출 차단 기능을 설정합니다. |
| 계좌번호정보 유출 차단 | 웹 서버가 클라이언트로 보내는 응답에 계좌 번호 정보가 포함되었는지 검사하여, 포함된 경우에는 이를 특정 문자로 변환한 후 전송하거나 응답을 차단하는 계좌번호 정보 유출 차단 기능을 설정합니다. |
| 웹 변조 방지 | WEBFRONT-K가 웹 서버의 컨텐트를 저장하고 있다가 클라이언트로부터 요청이 오면 웹 서버 대신 WEBFRONT-K가 응답을 보냄으로써 웹 페이지가 변조되는 것을 방지하는 웹 변조 방지 기능을 설정합니다. |
| 응답 형식 검사 | 웹 서버가 클라이언트로 보내는 응답 패킷의 형식을 검사하여 형식에 맞는 응답 패킷인지를 검사하여, 지정한 처리 방식에 따라 해당 응답을 처리하도록 하는 응답 형식 검사 기능을 설정합니다. |
| 코드 노출 차단 | 웹 서버가 클라이언트로 보내는 응답 패킷에 HTML 주석, 스크립트 주석이 포함되었는지를 검사하여, 지정한 처리 방식에 따라 처리하도록 하는 코드 노출 차단 기능을 설정합니다. |
| WISE 컨텐트 필터 | 웹 서버가 클라이언트로 보내는 응답 패킷에 대한 항목, 변수, 값, 조건 등 필터의 규칙을 세부적으로 설정하여 응답 패킷을 필터링하는 WISE 컨텐트 필터를 설정합니다. |

### 학습

학습 메뉴는 접근 제어와 폼 필드 검사 기능을 설정하기 위해 관련 정보를 학습할 수 있는 하위 메뉴로 구성되어 있습니다. 각 하위 메뉴에서는 학습 기능을 통한 학습 결과를 확인할 수 있고, 학습 결과를 각 기능에 적용할 수 있습니다. 그리고, 사이트의 URL 구조를 분석하여 트리 형태로 보여주는 URL 구조 분석 기능도 학습 메뉴에 포함되어 있습니다. 학습 기능을 설정하는 방법과 URL 구조 분석 기능을 통해 URL 구조를 출력하는 방법은 이 설명서의 [**제 5 장 학습 기능 설정**]에 상세히 설명되어 있습니다.

## 위장

위장 메뉴는 URL 정보 위장 기능과 서버 정보 위장 기능을 설정할 수 있는 다음 메뉴로 구성되어 있습니다. 위장 기능을 설정하는 방법은 이 설명서의 [**제6장 위장 기능 설정**]에 상세히 설명되어 있습니다.

| 메뉴 | 기능 |
|---|---|
| URL 정보 위장 | 클라이언트가 웹 서버로 요청하는 URL이나 웹 서버가 클라이언트로 응답하는 URL을 변환하여, 내부의 웹 서버에서 사용되는 URL 정보가 외부에 유출되지 않도록 하는 URL 정보 위장 기능을 설정합니다. |
| Server 정보 위장 | 웹 서버의 중요한 정보들을 변환, 숨김, 삭제하여 외부에 유출되는 것을 방지하는 서버 정보 위장 기능을 설정합니다. |

## 부하분산

부하 분산 메뉴는 애플리케이션의 트래픽을 여러 서버로 분산시키는 데 필요한 패턴, 실제 서버, 그룹, 규칙, 장애감시 등을 설정할 수 있는 다음 메뉴들로 구성되어 있습니다. 부하 분산 기능을 설정하는 방법은 이 설명서의 [**제7장 부하 분산 설정**]에 상세히 설명되어 있습니다.

| 메뉴 | 기능 |
|---|---|
| 소스 NAT | One-Armed 방식의 네트워크 구성을 사용하는 경우, 요청 패킷의 출발지 주소를 변경할 소스 NAT IP 주소를 설정하는 메뉴입니다. |
| 패턴 | 부하 분산 기능을 적용할 URI, 호스트, 쿠키, 사용자 에이전트, Accept-Language를 설정하는 메뉴입니다. |
| 실제 서버 | 부하 분산 기능을 적용할 실제 서버(real server)들의 정보(실제 IP와 실제 포트)를 설정하는 메뉴입니다. |
| 그룹 | 동일한 부하 분산 알고리즘과 장애 감시를 사용할 실제 서버의 그룹을 정의하는 메뉴입니다. |
| 규칙 | 그룹에서 사용할 패턴과 부하 분산 알고리즘, 장애 감시 방법 등에 대한 규칙을 설정하는 메뉴입니다. |
| 장애 감시 | 실제 서버의 동작 상태를 파악하는 장애 감시 방법을 설정하는 메뉴입니다. |

## SSL

SSL 메뉴에서는 WEBFRONT-K 를 통해 전송되는 패킷을 암호화(encryption)하거나 복호화(decryption)하여 패킷의 안전성과 신뢰성을 보장할 수 있는 SSL 기능을 설정할 수 있는 다음 4 개의 하위 메뉴로 구성되어 있습니다. SSL 기능을 설정하는 방법은 이 설명서의 [**제 8 장 SSL 기능 설정**]에 상세히 설명되어 있습니다.

| 메뉴 | 기능 |
|---|---|
| 일반 설정 | SSL 기능의 사용 여부와 백엔드 기능의 사용 여부 및 세션 재사용, 최대 접속, 통과 기능을 설정하는 메뉴입니다. |
| 인증서 관리 | 인증서와 키를 등록하거나 등록된 인증서와 키의 정보를 보거나 파일로 다운로드하거나 삭제하는 메뉴입니다. |
| 임시인증서 생성 | 테스트용이나 CSR로 사용할 수 있는 임시 인증서를 생성하는 메뉴입니다. |
| SSL 프로토콜 검사 | SSL 프로토콜의 대표적인 취약점을 검사하고, SSL 접속 준비 과정(SSL handshaking)에서의 과다 요청을 제어하는 메뉴입니다. |

## 로그

로그 메뉴는 애플리케이션과 관련된 로그를 검색할 수 있는 하위 메뉴로 구성되어 있습니다. 로그 메뉴를 사용하여 애플리케이션 로그를 검색하는 방법은 이 설명서의 [**제 9 장 애플리케이션 로그**]에 상세히 설명되어 있습니다.

| 메뉴 | 기능 |
|---|---|
| 보안 로그 | 수신된 패킷이 WEBFRONT-K에 설정된 애플리케이션 보안 규칙에 위배되는 경우 패킷에 대한 정보와 어떤 규칙에 의해 위배되었는지를 기록하는 로그입니다. |
| 감사 로그 | 애플리케이션 관리자가 WEBFRONT-K에서 조회한 애플리케이션 보안 설정 정보와 변경한 애플리케이션 보안 설정 정보를 기록하는 로그입니다. |
| 접근 로그 | WEBFRONT-K로 웹 요청 패킷이 수신될 때마다 발생하는 로그로, 웹 요청 패킷에 대한 정보가 기록되는 로그입니다. |

## 모니터링

모니터링은 일정 기간 동안 모니터링한 애플리케이션의 트래픽 양과 애플리케이션에 설정된 보안 기능에 의해 차단되거나 학습된 정보의 통계 정보, 그리고 부하 분산 통계 정보를 보여주는 메뉴입니다. 모니터링 메뉴는 모니터링된 모든 정보를 간략하지만 한꺼번에 보여주는 하위 메뉴와 각 보안 기능의 상세 모니터링 정보를 보여주는 6 개의 하위 메뉴로 구성되어 있습니다. 모니터링 메뉴를 사용하여 애플리케이션과 관련된 각종 정보를 모니터링하는 방법은 이 설명서의 [**제 10 장 애플리케이션 모니터링**]에 상세히 설명되어 있습니다.

| 메뉴 | 기능 |
|---|---|
| 애플리케이션 통합 | 최근 25분 동안 WEBFRONT-K를 통해 송수신된 애플리케이션의 트래픽 양과 각 웹 보안 기능에 의해 차단된 웹 공격에 대한 정보, 그리고 학습 기능을 통해 학습된 정보, 각 실제 서버로 부하 분산된 트래픽 양을 보여주는 메뉴입니다. |
| 요청 검사 모니터링 | 일주일 동안 애플리케이션의 요청 검사 기능에 의해 차단된 웹 공격에 대한 정보를 볼 수 있는 메뉴입니다. 특정 요청 검사 기능이나 특정 시간 동안 모니터링한 정보만 출력할 수도 있습니다. |
| 컨텐트 보호 모니터링 | 일주일 동안 애플리케이션의 컨텐트 보호 기능에 의해 차단된 웹 공격에 대한 정보를 볼 수 있는 메뉴입니다. 특정 컨텐트 보호 기능이나 특정 시간 동안 모니터링한 정보만 출력할 수도 있습니다. |
| 학습 모니터링 | 일주일 동안 애플리케이션의 학습 기능에 의해 학습된 웹 공격에 대한 정보를 볼 수 있는 메뉴입니다. 특정 요청 검사 기능에 대한 학습 정보만 조회할 수 있고, 특정 시간 동안의 학습 정보만 출력할 수도 있습니다. |
| 위장 모니터링 | 일주일 동안 애플리케이션의 위장 기능에 의해 정보가 변환된 횟수를 모니터링할 수 있는 메뉴입니다. 특정 위장 기능이나 특정 시간 동안 모니터링한 정보만 출력할 수도 있습니다. |
| 부하분산 모니터링 | 일주일 동안 애플리케이션의 부하 분산 기능에 의해 각 실제 서버로 전송된 트래픽 양을 모니터링할 수 있는 메뉴입니다. 특정 실제 서버나 특정 시간 동안 모니터링한 정보만 출력할 수도 있습니다. |

# OWASP TOP 10 메뉴 모드

OWASP TOP 10 메뉴 모드는 애플리케이션 메뉴를 OWASP TOP 10 취약점을 기준으로 다시 배치한 모드입니다.

| 주 메뉴 | 하위 메뉴 |
|---|---|
| A1 인젝션 | - 버퍼 오버플로우 차단<br>- SQL 삽입 차단 |
| A2 훼손된 인증/세션 | 쿠키 보호 |
| A3 XSS | 스크립트 삽입 차단 |
| A4 직접 객체 참조 | - 다운로드 검사<br>- 웹 공격 프로그램 차단 |
| A5 잘못된 보안 설정 | - 디렉토리 리스팅 차단<br>- 검사 회피 차단 |
| A6 중요 정보 노출 | - 신용 카드 정보 유출 차단<br>- 주민등록 정보 유출 차단<br>- 계좌번호 유출 차단 |
| A7 기능 접근 제어 미비 | - 접근 제어<br>- 폼필드 검사 |
| A8 CSRF | WISE 요청 필터 |
| A9 취약한 컴포넌트 사용 | - 접근 제어<br>- 버퍼 오버플로우 차단<br>- SQL 삽입 차단<br>- 스크립트 삽입 차단 |
| A10 미확인 리다이렉션 | 인클루드 인젝션 차단 |
| etc 기타 | - 업로드 검사<br>- 과다 요청 제어<br>- 요청 형식 검사<br>- HTTP POST 공격 차단<br>- Slow Read 공격 차단<br>- 웹 변조 방지<br>- 응답 형식 검사<br>- 코드 노출 차단<br>- WISE 컨텐트 필터 |

주 메뉴는 OWASP TOP 10 취약점들이고, 하위 메뉴는 해당 취약점을 막기 위해 사용할 수 있는 기능들입니다. 하위 메뉴의 기능들은 기본 모드에서와 동일하게 설정할 수 있고 동작도 동일합니다. 가장 아래에 있는 etc 기타 메뉴는 보안 기능 중 OWASP TOP 10 취약점과 무관한 기능들로 구성되어 있습니다.

기본 메뉴에서 제공되는 기능 중에서 일반 설정, 응답 설정, 기타 설정, SSL, 로그, 모니터링 기능은 OWASP TOP 10 모드에서 표시되지 않습니다.

### OWASP TOP 10 취약점 @@

OWASP TOP 10은 OWASP(Open Web Application Security Project) 에서 발표한 다음과 같은 웹 애플리케이션의 대표적인 10가지 취약점입니다.

| 취약점 | 설명 |
|---|---|
| A1 인젝션 | 인젝션은 사용자가 제공한 데이터가 인터프리터 형식의 명령어나 질의문으로 보내질 때 발생합니다. 악의적인 공격자의 데이터에 대해 인터프리터는 의도하지 않은 명령어를 실행하거나 데이터를 변경할 수 있습니다. 인젝션 취약점, 특히 SQL 인젝션 취약점은 웹 애플리케이션에서 매우 흔합니다. |
| A2 훼손된 인증/세션 | 자격 증명과 세션 토론은 종종 적절히 보호되지 못합니다. 공격자는 다른 사용자인 것처럼 보이게 하기 위하여 비밀번호, 키, 혹은 인증 토큰을 손상시킵니다. |
| A3 XSS<br>(크로스 사이트 스크립팅) | XSS 취약점은 컨텐츠를 암호화나 검증 절차 없이 애플리케이션에 받아 들이거나 웹 브라우저로 보낼 때 발생합니다. XSS는 공격자가 희생자의 브라우저 내에서 스크립트를 실행하게 허용함으로써 사용자 세션을 가로채거나 웹 사이트를 손상하거나 웜을 심는 것을 가능하게 할 수 있습니다. |
| A4 직접 객체 참조 | 직접 객체 참조는 개발자가 파일, 디렉토리, 데이터베이스 기록 혹은 키와 같은 내부 구현 객체에 |

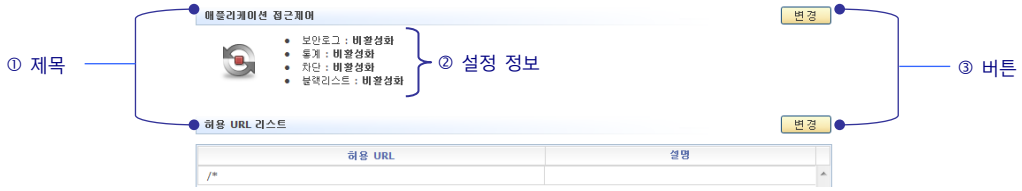
| | |
|---|---|
| | 대한 참조를 URL이나 폼 매개변수로 노출시킬 때 발생합니다. 공격자는 이러한 참조를 조작하여 승인 없이 다른 객체에 접속할 수 있습니다. |
| A5 잘못된 보안 설정 | 바람직한 보안은 애플리케이션, 프레임워크, 웹 애플리케이션 서버, 웹 서버, 데이터베이스 서버와 플랫폼에 대한 보안 구성이 정의되고 적용되기를 요구합니다. 기본 보안 설정은 대부분 안전하지 않기 때문에 새롭게 정의 및 실행하고 유지되어야 합니다. 또한 소프트웨어는 최신의 상태를 유지해야 합니다. |
| A6 중요 정보 노출 | 대다수의 웹 애플리케이션은 카드번호 등과 같은 개인정보를 적절하게 보호하고 있지 않기 때문에, 개인정보유출과 같은 취약점이 발생되고 있습니다. 이를 보완하기 위해서는 데이터저장 시 암호화 및 데이터 전송 시에도 SSL등을 이용하여야 합니다. |
| A7 기능 접근 제어 미비 | 가상적으로는 UI 에서 보여지는 특정기능을 수행 전, 기능접근제한권한을 검증해야 하나, 어플리케이션은 각 기능에 대한 접근 시 동일한 접근통제검사 수행이 요구됩니다. 만일 적절하게 수행되지 않는 경우 공격자는 비인가된 기능에 접근하기 위해, 정상적인 요청을 변조할 수도 있습니다. |
| A8 CSRF<br>(크로스 사이트 요청) | CSRF 공격은 로그온한 희생자의 브라우저가 사전 승인된 요청을 취약한 웹 애플리케이션에 보내도록 함으로써 희생자의 브라우저가 공격자에게 이득이 되는 악의적인 행동을 수행하도록 합니다. CSRF는 자신이 공격하는 웹 애플리케이션이 강력할수록 더 강력해집니다. |
| A9 취약한 컴포넌트 사용 | 슈퍼유저권한으로 운영되는 취약한 라이브러리, 프레임워크 및 기타 다른 소프트웨어 모듈로 인해 데이터유실 및 서버 권한획득과 같은 취약성이 존재합니다. |
| A10 미확인 리다이렉션 | 웹 애플리케이션은 종종 사용자들을 다른 페이지로 리다이렉트하거나 포워드합니다. 그러나, 목적 페이지를 결정하기 위해 신뢰지 않는 데이터를 사용하는 경우에는 적절한 확인이 없다면, 공격자는 피해자를 피싱사이트나 악의적인 사이트로 리다이렉트 할 수 있고, 접근 권한이 없는 페이지의 접근을 위해 사용할 수 있습니다. |

# 애플리케이션 설정 화면

애플리케이션 보안 기능에 속하는 각 기능들을 설정하는 설정 정보 화면, 변경 화면, 추가 화면 등 화면의 구성은 동일한 부분이 많이 있으므로, 해당 절의 내용을 참고로 하여 각 기능을 설정합니다.

## 설정 정보 화면

특정 애플리케이션 보안 기능을 설정하기 위해 해당 메뉴를 클릭하면, 작업 화면에는 해당 기능의 현재 설정 정보를 보여주는 화면이 나타납니다. 이 부분에서는 **Application** - **요청검사** - **접근제어** 설정 화면을 예를 들어, 애플리케이션 보안 기능을 설정하는 화면의 일반적인 구성에 대해 소개합니다.




설정 정보를 보여주는 화면은 일반적으로 다음과 같은 부분으로 구성되어 있습니다.

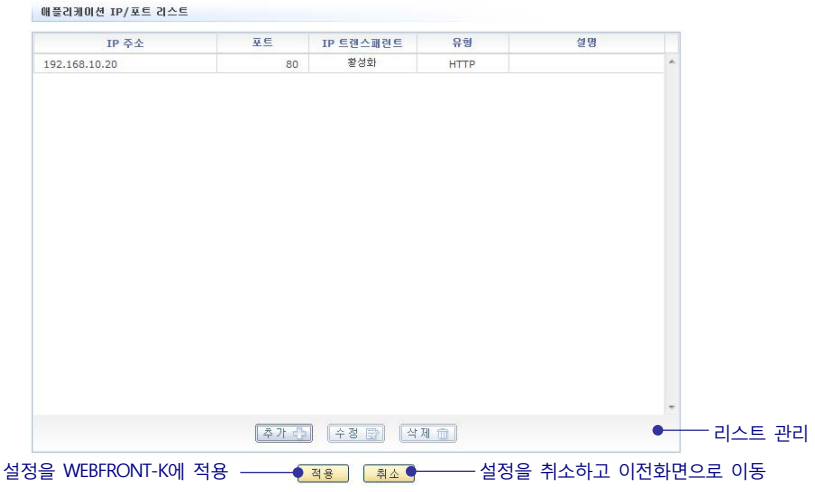
① 제목 — 이 부분은 각 보안 기능에 대한 세부 기능의 제목입니다. 각 애플리케이션 보안 기능마다 한가지 이상의 세부 기능이 있습니다.

② 설정 정보 — 이 부분에서는 각 세부 기능의 설정 정보를 보여줍니다. 일부 세부 기능에 대한 설정 정보는 간단하게 보여주거나, 보여주지 않는 경우가 있습니다.

③ 버튼 — [**변경**] 버튼은 해당 애플리케이션 보안 기능의 세부 기능을 설정하려는 경우에 사용됩니다. [**변경**] 버튼을 클릭하면, 해당 세부 기능을 설정할 수 있는 변경 화면이 나타납니다.

## 변경 화면

설정 정보 화면에서 세부 기능을 설정하기 위해 [**변경**] 버튼을 클릭하면 해당 세부 기능을 설정할 수 있는 화면이 나타납니다. 세부 기능을 설정하는 화면에서는 주로 기능의 상태를 설정하거나(활성화 혹은 비활성화), 항목의 값을 설정하거나, 리스트를 관리(항목을 추가, 삭제, 수정)하게 됩니다. 세부 기능 설정 화면에서 변경한 설정을 WEBFRONT-K에 적용하기 위해서는 마지막에 반드시 [**적용**] 버튼을 클릭해야 합니다. 이 부분에서는 **Application** - **일반설정** - **애플리케이션 IP/포트 리스트** 설정 화면을 예를 들어 설명합니다.




리스트의 항목을 수정하거나 삭제하려면 해당 항목을 선택해야 합니다. 여러 개의 항목을 선택해야 하는 경우에는 [**Shift**] 키나 [**Ctrl**] 키를 사용하면 편리합니다. 연속적인 여러 항목을 선택할 때에는 첫 항목을 클릭한 후 [**Shift**] 키를 누른 상태에서 마지막

항목을 클릭합니다. 연속적이지 않은 여러 항목을 선택할 때에는 [**Ctrl**] 키를 누른 상태에서 원하는 항목을 계속 클릭하면 됩니다.

### 항목 추가 화면

변경 화면의 리스트에서 [**추가**] 버튼을 클릭하면 추가할 항목에 대한 정보를 입력할 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.


# 애플리케이션 설정 버튼

다음은 애플리케이션 설정 화면에 있는 버튼들의 기능입니다.

| | |
|---|---|
| 추가 | [**추가**] 버튼은 하나의 항목을 추가하는 경우에 사용됩니다. 이 버튼을 클릭하면, 해당 항목을 추가할 수 있는 추가 팝업 창이 나타납니다. |
| 수정 | [**수정**] 버튼은 이미 추가된 항목을 수정하려는 경우에 사용됩니다. 먼저 수정하려는 항목을 선택한 후 [**수정**] 버튼을 클릭하면, 해당 항목을 수정할 수 있는 팝업 창이 나타납니다. 수정 팝업 창에서 수정할 수 있는 항목은 [**추가**] 버튼을 클릭하여 나타나는 항목과 동일합니다. 그러므로, 이 매뉴얼에서는 각 항목을 수정하는 방법을 따로 설명하지 않습니다. 해당 항목을 수정하려는 경우에는, 해당 항목을 설정하는 부분의 설명을 참고하여 수정하면 됩니다. |
| 삭제 | [**삭제**] 버튼은 이미 추가된 항목을 삭제하려는 경우에 사용됩니다. 먼저 삭제하려는 항목을 선택한 후, 이 버튼을 클릭하면 됩니다. |
| 적용 | 이 버튼은 설정을 완료한 후 설정을 시스템에 적용하려는 경우에 클릭합니다. 설정을 시스템에 적용하지 않으면, 지금까지 설정한 내용은 적용되지 않고, 마지막으로 적용된 설정 상태로 돌아가게 됩니다. |
| 취소 | 설정을 시스템에 적용하지 않고 이전 화면으로 돌아가려는 경우에 이 버튼을 클릭합니다. |
| 리셋 | 설정 내용을 수정한 후, 이 버튼을 클릭하면 현재 화면의 설정이 원래의 설정 상태로 되돌려집니다. 그러므로, 수정한 사항을 적용하지 않고 원래의 설정으로 복구하려는 경우에는 이 버튼을 클릭한 후 [**적용**] 버튼을 클릭하면 됩니다. |
| 확인 | 설정을 저장한 후 이전 화면으로 돌아가려는 경우에 이 버튼을 클릭합니다. |

# 제2장 애플리케이션 기본 설정

이 장에서는 등록한 애플리케이션마다 기본적으로 설정해야 하는 일반 설정과 응답 설정을 하는 방법과 세션 연결 유지를 위한 세션 정보 설정 방법, 인코딩 방식을 설정하는 방법 등을 소개합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 일반 설정
- 응답 설정
- 기타 설정

**참고:** WEBFRONT-K의 웹 애플리케이션 검사 기능을 사용하기 위해서는 먼저, WEBFRONT-K에 검사를 수행할 웹 애플리케이션을 등록해야 합니다. 웹 애플리케이션은 [**System-애플리케이션-애플리케이션 관리**] 메뉴에서 등록할 수 있습니다. 웹 애플리케이션을 등록하는 방법은 이 설명서와 함께 제공되는 **WEBFRONT-K 시스템 구성 설명서**의 [**제4장 애플리케이션**] 부분을 참고합니다.

# 일반 설정

WEBFRONT-K의 웹 보안 기능을 사용하기 위해서는 먼저 웹 보안 기능으로 보호할 웹 애플리케이션을 WEBFRONT-K에 등록해야 합니다. 웹 애플리케이션은 통합 관리자나 사이트 관리자가 System 메뉴에서 등록할 수 있습니다. 웹 애플리케이션을 등록하는 방법은 이 설명서와 함께 제공되는 WEBFRONT-K 시스템 구성 설명서의 [**제4장 애플리케이션**] 장을 참고합니다.

애플리케이션을 등록한 후에는 Application 메뉴의 **애플리케이션** - **일반설정** 메뉴를 사용하여 반드시 애플리케이션에 대한 기본적인 설정을 해야 합니다. 이 절에서는 이러한 애플리케이션의 기본 설정 방법에 대해 살펴봅니다.

## 일반 애플리케이션과 기본 애플리케이션

애플리케이션에는 사용자가 등록한 '일반' 애플리케이션과 WEBFRONT-K에 기본적으로 등록되어 있는 '기본' 애플리케이션이 있습니다. 이 두 애플리케이션에 기본적으로 설정해야 하는 항목들은 서로 다르기 때문에 각각 살펴보도록 합니다.

### 일반 애플리케이션

다음은 일반 애플리케이션의 일반 설정 화면입니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **애플리케이션** 애플리케이션의 활성화 상태가 표시됩니다.
- **애플리케이션 일반 설정 정보** 애플리케이션의 동작 모드, 도메인 무시, 압축 방지, 클라이언트 MSS, 서버 MSS, CPS 제한, 동시 세션 제한, BPS 제한 기능의 상태가 표시됩니다.
- **애플리케이션 도메인 리스트** 애플리케이션의 도메인 목록이 표시됩니다.
- **애플리케이션 IP/포트 리스트** 애플리케이션 접속 시 사용하는 애플리케이션의 IP 주소와 포트가 표시됩니다.
- **예외 IP/포트 정보** 애플리케이션을 적용하지 않을 IP 주소와 포트가 표시됩니다.
- **URL Prefix 매칭 리스트** URL Prefix 매칭 기능을 적용할 URL 정보가 표시됩니다. URL Prefix 매칭은 IP 주소, 포트, 도메인이 동일할 경우, 설정한 URL을 통해 애플리케이션을 구분할 수 있는 기능입니다.

일반 애플리케이션의 일반 설정 화면에서 기본적으로 설정해야 하는 값들은 다음과 같습니다.

- **모드** WEBFRONT-K는 일반 모드, 부하 분산 모드, 고속 모드, 미러링 모드로 동작할 수 있습니다. WEBFRONT-K를 일반적인 용도로 사용할 경우, '일반' 모드로, 웹 서버에 부하 분산 기능을 적용하는 경우에는 '부하 분산' 모드로 설정합니다. 일반 모드에 비해 사용할 수 있는 기능은 제한되지만 보다 빠른 속도로 서비스를 제공해야 하는 경우에는 '고속' 모드로, WEBFRONT-K를 IDS 장비와 같이 미러링된 패킷을 검사하는 용도로 사용할 경우에는 '미러링' 모드로 설정합니다. 부하 분산 모드로 설정한 경우에는 WEBFRONT-K의 L7 부하 분산 기능을 설정해야 합니다. L7 부하 분산 기능의 설정 방법은 이 설명서의 [**제7장 부하 분산 설정**]을 참고합니다.
- **도메인 무시** 도메인 무시 기능의 상태를 설정합니다. 도메인 무시 기능이 '활성화'된 경우에는 도메인 정보 설정 여부와 관계없이 설정한 애플리케이션의 IP 주소/포트로 수신되는 트래픽에 보안정책을 적용합니다.
- **압축 방지** 압축 방지 기능의 상태를 설정합니다. 압축 방지 기능이 '활성화'된 경우에는 클라이언트의 요청 패킷에서 웹 페이지 압축을 요청하는 Accept-Encoding 헤더를 삭제하여 웹 페이지 압축이 수행되지 않도록 합니다. 웹 페이지 압축이 수행되면 응답 패킷의 바디에 대한 보안 기능이 정상적으로 적용되지 않습니다.
- **클라이언트 MSS** 클라이언트 구간에 대한 TCP MSS(Maximum Segment Size)를 설정합니다. MSS는 최대 세그먼트 크기를 의미합니다.
- **서버 MSS** 서버 구간에 대한 TCP MSS를 설정합니다.
- **CPS 제한** 애플리케이션에서 허용하는 초당 커넥션 수를 설정합니다.
- **동시세션 제한** 애플리케이션에서 허용하는 동시 세션 수를 설정합니다.
- **BPS 제한** 애플리케이션에서 허용하는 초당 비트 수를 설정합니다.
- **도메인** 애플리케이션의 도메인 이름을 등록합니다. 여러 개의 도메인 이름을 등록할 수 있습니다.
- **IP 주소/포트** 애플리케이션의 IP 주소와 포트를 등록합니다.

애플리케이션의 동작 모드는 기본적으로 일반 모드로 설정되어 있고 도메인 무시 기능과 압축 방지 기능은 비활성화 상태로 설정되어 있습니다. 그리고, 기본적으로 설정되어 있는 도메인이나 IP 주소, 포트는 없습니다. 애플리케이션을 활성화하기 위해서는 먼저 도메인과 IP 주소/포트를 반드시 설정해야 합니다.

**참고:** 고속 모드 또는 미러링 모드 사용 시, 제한되는 기능은 다음과 같습니다.

- 마스킹 기능, 폼 필드 검사의 매개변수 보호 기능, 쿠키 무결성 검사 기능, 고급 첨부파일 검사 기능, 웹 변조 방지 기능, 코드 노출 차단 기능, 위장 기능, 부하 분산 기능

## 기본 애플리케이션(default application)

기본 애플리케이션은 WEBFRONT-K에 기본으로 만들어져 있는 애플리케이션으로, 일반 애플리케이션에 속하지 않는 트래픽에 적용됩니다. 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. 이러한 트래픽 조건은 여러 개를 설정할 수 있습니다. 트래픽이 이 조건 중 하나만 만족하면 기본 애플리케이션이 적용됩니다.
기본 애플리케이션이 적용되는 트래픽 중 일부 트래픽에는 기본 애플리케이션을 적용하지 않으려는 경우 해당 트래픽을 '예외' 트래픽으로 지정할 수 있습니다. '예외' 트래픽도 클라이언트의 IP 주소와 포트, 서버 IP 주소와 포트를 사용하여 설정합니다. 예외 트래픽의 조건 역시 여러 개를 지정할 수 있고, 조건 중 하나만 만족하면 기본 애플리케이션이 적용되지 않습니다.

일반 애플리케이션에 속하지 않고, 기본 애플리케이션도 적용되지 않는 트래픽은 WEBFRONT-K의 기능이 적용되지 않고 라우팅 테이블을 참고하여 라우팅됩니다.

다음은 기본 애플리케이션의 일반 설정 화면입니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **애플리케이션** 기본 애플리케이션의 활성화 상태가 표시됩니다.
- **애플리케이션 일반 설정 정보** 기본 애플리케이션의 압축 방지 기능 상태가 표시됩니다.
- **기본 애플리케이션 IP/포트 리스트** 기본 애플리케이션을 적용할 트래픽의 조건이 출력됩니다.
- **예외 IP/포트 정보** 기본 애플리케이션을 적용하지 않을 트래픽의 조건이 출력됩니다.

기본 애플리케이션의 일반 설정 화면에서 설정해야 하는 값들은 다음과 같습니다.

- **압축 방지** 압축 방지 기능의 상태를 설정합니다. 압축 방지 기능이 '활성화'된 경우에는 클라이언트의 요청 패킷에서 웹 페이지 압축을 요청하는 Accept-Encoding 헤더를 삭제하여 웹 페이지 압축이 수행되지 않도록 합니다. 웹 페이지 압축이 수행되면 응답 패킷의 바디에 대한 보안 기능이 정상적으로 적용되지 않습니다.
- **IP 주소/포트** 기본 애플리케이션을 적용할 트래픽을 설정합니다. 트래픽을 설정할 때에는 트래픽을 전송한 클라이언트의 IP 주소와 포트, 그리고 트래픽을 수신한 서버의 IP 주소와 포트를 사용합니다.
- **예외 IP/포트** 기본 애플리케이션을 적용하도록 설정된 트래픽 중에서 예외로 할(기본 애플리케이션을 적용하지 않을) 트래픽을 설정합니다. 예외 트래픽도 트래픽을 전송한 클라이언트의 IP 주소와 포트, 그리고 트래픽을 수신한 서버의 IP 주소와 포트를 사용하여 설정합니다.

# 일반 애플리케이션 설정하기

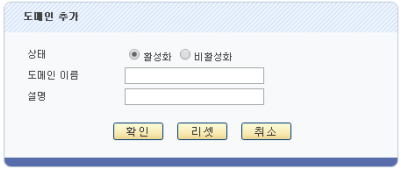
## 애플리케이션의 일반 설정 정보 설정하기

애플리케이션의 일반 설정 정보를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 일반 설정 정보**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 일반 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **모드**<br>– 일반: 애플리케이션이 실행되는 웹 서버에 부하 분산 기능을 적용하지 않는 경우 (기본값)<br>– 부하분산: 애플리케이션이 실행되는 웹 서버에 부하 분산 기능을 적용하는 경우<br>– 고속: 일반 모드에 비해 사용할 수 있는 보안 기능은 제한되지만 보다 빠른 속도로 서비스를 제공해야 하는 경우<br>– 미러링: WEBFRONT-K를 IDS 장비와 같이 미러링된 패킷을 검사하는 용도로 사용하는 경우<br>• **도메인 무시**<br>– 활성화: 애플리케이션의 도메인 리스트 설정과 관계없이 IP 주소/포트로 수신되는 트래픽에 보안정책을 적용하는 경우<br>– 비활성화: 애플리케이션의 도메인 리스트와 함께 IP 주소/포트로 수신되는 트래픽에 보안정책을 적용하는 경우(기본값)<br>• **압축 방지**<br>– 활성화: 클라이언트의 요청을 수정하여 서버에서 웹 페이지 압축을 하지 않도록 하는 경우<br>– 비활성화: 클라이언트의 웹 페이지 압축 요청을 허용하는 경우. 서버의 설정에 따라 압축 여부가 결정됨. (기본값)<br>• **클라이언트 MSS** 클라이언트 구간에 대한 TCP MSS를 설정합니다. (설정 범위: 0 ~ 65535, 기본값: 1460)<br>• **서버 MSS** 서버 구간에 대한 TCP MSS를 설정합니다. (설정 범위: 0 ~ 65535, 기본값: 1460)<br>• **CPS 제한** 클라이언트 구간에 대한 초당 커넥션 수를 설정합니다. (설정 범위: 100 ~ 1,000,000, 기본값: 비활성화)<br>• **동시세션 제한** 클라이언트 구간에 대한 동시 세션 수를 설정합니다. (설정 범위: 100 ~ 20,000,000, 기본값: 비활성화)<br>• **BPS 제한** 클라이언트 구간에 대한 초당 비트 수를 설정합니다. (설정 범위: 100 ~ 1,000,000, 기본값: 비활성화) |

## 애플리케이션 도메인 설정하기

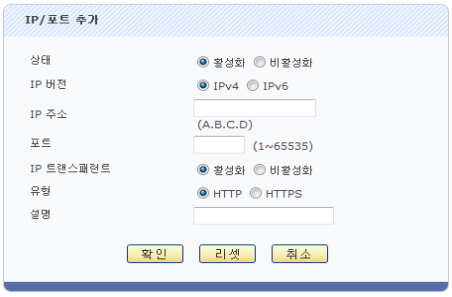
애플리케이션의 도메인을 설정하는 방법은 다음과 같습니다. 하나의 애플리케이션에는 최대 256개의 도메인을 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 도메인 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**도메인 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 지정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 도메인의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **도메인 이름** 도메인의 이름을 입력합니다. 도메인 이름은 알파벳과 '.' 등의 기호로 구성된 256 글자의 문자열로 지정할 수 있습니다.<br>• **설명** 도메인에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열로 지정할 수 있습니다. (선 |

| | |
|---|---|
| | 택 설정) |
| 4 | 도메인을 모두 추가하였으면 [**적용**] 버튼을 클릭합니다. |

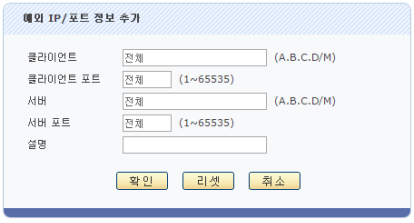
## 애플리케이션 IP 주소와 포트 설정

애플리케이션의 IP 주소와 포트를 설정하는 방법은 다음과 같습니다. 애플리케이션에는 최대 1024개의 IP 주소/포트를 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 IP/포트 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**IP/포트 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 지정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 IP 주소와 포트의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **IP 버전** 애플리케이션의 IP 버전을 지정합니다. (기본값: IPv4)<br>• **IP 주소** 애플리케이션으로 접속할 때 사용할 IP 주소를 입력합니다.<br>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.<br>• **포트** 애플리케이션으로 접속할 때 사용할 포트 번호를 입력합니다. (설정 범위: 1 ~ 65535)<br>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.<br>• **IP 트랜스패런트** 입력한 IP 주소와 포트가 가상(virtual)의 값인지 실제 값인지를 지정합니다. 애플리케이션 모드가 부하 분산 모드일 경우에는 '활성화'를, 그 이외의 모드에서는 '비활성화'를 선택합니다. (기본값: 활성화)<br>• **유형** 애플리케이션의 패킷 유형이 HTTP 인지 HTTPS인지를 지정합니다. SSL 기능을 통해 암호화된 트래픽이 송수신되는 경우에는 'HTTPS'를, 그 이외에는 'HTTP'를 선택합니다. (기본값: HTTP)<br>• **설명** IP 주소와 포트에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열로 지정할 수 있습니다. (선택 설정) |
| 4 | IP 주소와 포트를 모두 추가하였으면 [**적용**] 버튼을 클릭합니다. |

## 예외 트래픽 설정하기

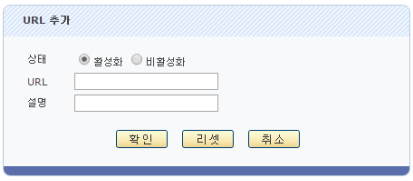
예외 IP 주소와 포트를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 2 | <**예외 IP/포트 정보**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**예외 IP/포트 정보 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다. 해당 조건을 사용하지 않으려면 '전체'를 입력합니다. (기본값: 전체)<br>  |

| | | |
|---|---|---|
| | • **클라이언트** | 애플리케이션을 적용하지 않을 트래픽의 출발지 IP 주소(트래픽을 전송한 클라이언트의 IP 주소)를 1.1.1.1/24와 같은 형식으로 입력합니다. |
| | • **클라이언트 포트** | 애플리케이션을 적용하지 않을 트래픽의 출발지 포트 번호(클라이언트가 트래픽 전송 시 사용한 포트 번호)를 입력합니다. (설정 범위: 1 ~ 65535) |
| | • **서버** | 애플리케이션을 적용하지 않을 트래픽의 목적지 IP 주소(트래픽을 수신할 서버의 IP 주소)를 입력합니다. |
| | • **서버 포트** | 애플리케이션을 적용하지 않을 트래픽의 목적지 포트 번호(서버가 트래픽 수신 시 사용할 포트 번호)를 입력합니다. (설정 범위: 1 ~ 65535) |
| | • **설명** | 설정 중인 트래픽 조건에 대한 설명을 입력합니다. 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | [**확인**] 버튼을 클릭합니다. | |

## URL Prefix 매칭 리스트

URL Prefix 매칭 기능을 적용할 URL을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 2 | <**URL Prefix 매칭 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 지정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** URL Prefix 매칭 기능의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 애플리케이션의 URL을 입력합니다. 애플리케이션 설정의 도메인 이름, IP 주소, 포트와 함께 '/' 이후의 해당 URL이 일치하면 매칭되는 애플리케이션으로 판단합니다. 대소문자는 구분하지 않습니다.<br>• **설명** 설정 중인 URL Prefix 매칭에 대한 설명을 입력합니다. |
| 4 | [**확인**] 버튼을 클릭합니다. |

## 애플리케이션 상태 설정

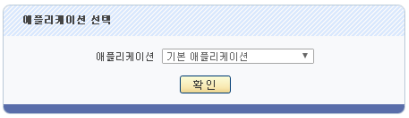
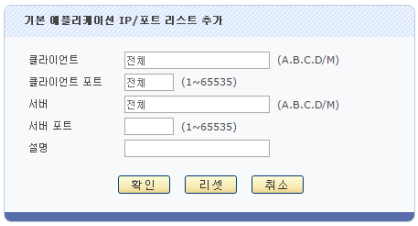
기본적으로 애플리케이션은 비활성화 상태로 설정됩니다. 애플리케이션을 활성화하려면 먼저 애플리케이션의 도메인과 IP 주소/포트를 설정해야 합니다. 애플리케이션의 도메인과 IP 주소/포트를 설정한 후에는 다음과 같은 방법으로 애플리케이션을 활성화할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 상태 설정**> 팝업 창에서 상태를 활성화로 변경한 후 [**적용**]을 클릭합니다. (기본값: 비활성화)<br>  |

# 기본 애플리케이션 설정하기

## 기본 애플리케이션을 적용할 트래픽 설정하기

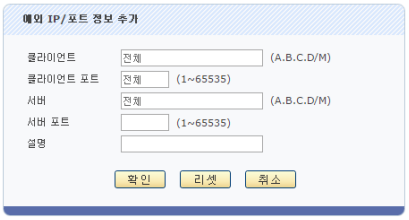
기본적으로 기본 애플리케이션은 IPv4 주소와 '80' 포트로 수신된 트래픽에만 적용됩니다. 다른 트래픽도 기본애플리케이션을 적용하도록 하려면 다음과 같은 방법으로 해당 트래픽에 대한 정보를 설정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | 화면 오른쪽 위에 있는 '**애플리케이션**' 목록의 아이콘을 클릭합니다. |
| 2 | <**애플리케이션 선택**> 팝업 창이 나타나면 애플리케이션 목록에서 기본 애플리케이션을 선택하고 [**확인**] 버튼을 클릭합니다.<br>  |
| 3 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 4 | <**기본 애플리케이션 IP/포트 리스트**> 부분의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 5 | <**기본 애플리케이션 IP/포트 리스트 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목들을 입력한 후 [**확인**] 버튼을 클릭합니다. 해당 조건을 사용하지 않으려면 '전체'를 입력합니다. (기본값: 전체)<br>  <br>• **클라이언트** 기본 애플리케이션을 적용할 트래픽의 출발지 IP 주소(트래픽을 전송한 클라이언트의 IP 주소)를 1.1.1.1/24와 같은 형식으로 입력합니다. (기본값: 전체)<br>• **클라이언트 포트** 기본 애플리케이션을 적용할 트래픽의 출발지 포트 번호(클라이언트가 트래픽 전송시 사용한 포트 번호)를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 전체)<br>• **서버** 기본 애플리케이션을 적용할 트래픽의 목적지 IP 주소(트래픽을 수신할 서버의 IP 주소)를 1.1.1.1/24와 같은 형식으로 입력합니다.<br>• **서버 포트** 기본 애플리케이션을 적용할 트래픽의 목적지 포트 번호(서버가 트래픽 수신 시 사용할 포트 번호)를 입력합니다. (설정 범위: 1 ~ 65535)<br>• **설명** 설정 중인 트래픽 조건에 대한 설명을 입력합니다. 최대 128 글자의 문자열을 입력할 수 있고, 한글도 가능합니다. (선택 설정) |
| 6 | 기본 애플리케이션을 적용할 트래픽에 대한 조건을 모두 추가한 후 설정 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 예외 트래픽 설정하기

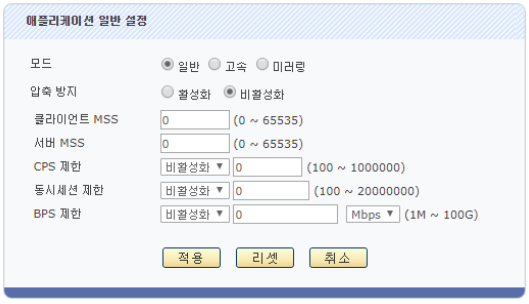
기본 애플리케이션을 적용하지 않을 예외 트래픽에 대한 정보를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | 화면 오른쪽 위에 있는 '**애플리케이션**' 목록의 아이콘을 클릭합니다. |
| 2 | <**애플리케이션 선택**> 팝업 창이 나타나면 애플리케이션 목록에서 기본 애플리케이션을 선택하고 [**확인**] 버튼을 클릭합니다.<br>  |
| 3 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 4 | <**예외 IP/포트 정보**> 부분의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 5 | <**예외 IP/포트 정보 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목들을 입력한 후 [**확인**] 버튼을 클릭합니다. |

| | |
|---|---|
| |  <br><br>• **클라이언트** 기본 애플리케이션을 적용하지 않을 트래픽의 출발지 IP 주소(트래픽을 전송한 클라이언트의 IP 주소)를 1.1.1.1/24와 같은 형식으로 입력합니다. 이 조건을 사용하지 않으려면 '전체'를 입력합니다. (기본값: 전체)<br>• **클라이언트 포트** 기본 애플리케이션을 적용하지 않을 트래픽의 출발지 포트 번호(클라이언트가 트래픽 전송시 사용한 포트 번호)를 입력합니다. 이 조건을 사용하지 않으려면 '전체'를 입력합니다.<br>(설정 범위: 1 ~ 65535, 기본값: 전체)<br>• **서버** 기본 애플리케이션을 적용하지 않을 트래픽의 목적지 IP 주소(트래픽을 수신할 서버의 IP 주소)를 입력합니다. 이 조건을 사용하지 않으려면 '전체'를 입력합니다.<br>• **서버 포트** 기본 애플리케이션을 적용하지 않을 트래픽의 목적지 포트 번호(서버가 트래픽 수신시 사용할 포트 번호)를 입력합니다. (설정 범위: 1 ~ 65535)<br>• **설명** 설정 중인 트래픽 조건에 대한 설명을 입력합니다. 최대 128 글자의 문자열을 입력할 수 있고, 한글도 가능합니다. (선택 설정) |
| 6 | 예외 트래픽에 대한 조건을 모두 추가하였으면 설정 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

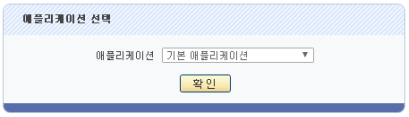
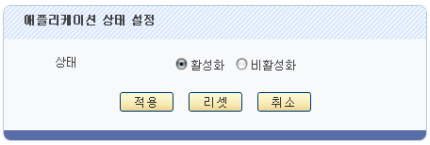
## 기본 애플리케이션의 일반 설정 정보 설정하기

기본 애플리케이션의 일반 설정 정보를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 일반 설정 정보**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 일반 설정**> 팝업 창에서 다음 설명을 참고하여 압축 방지 기능의 상태를 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **모드**<br>– 일반: 애플리케이션이 실행되는 웹 서버에 부하 분산 기능을 적용하지 않는 경우 (기본값)<br>– 고속: 일반 모드에 비해 사용할 수 있는 기능은 제한되지만 보다 빠른 속도로 서비스를 제공해야 하는 경우<br>– 미러링: WEBFRONT-K를 IDS 장비와 같이 미러링된 패킷을 검사하는 용도로 사용하는 경우<br>• **압축 방지**<br>– 활성화: 클라이언트의 요청을 수정하여 서버에서 웹 페이지 압축을 하지 않도록 하는 경우<br>– 비활성화: 클라이언트의 웹 페이지 압축 요청을 허용하는 경우. 서버의 설정에 따라 압축 여부가 결정됨. (기본값)<br>• **클라이언트 MSS** 클라이언트 구간에 대한 TCP MSS를 설정합니다. (설정 범위: 0 ~ 65535, 기본값: 1460)<br>• **서버 MSS** 서버 구간에 대한 TCP MSS를 설정합니다. (설정 범위: 0 ~ 65535, 기본값: 1460)<br>• **CPS 제한** 클라이언트 구간에 대한 초당 커넥션 수를 설정합니다. (설정 범위: 100 ~ 1,000,000, 기본값: 비활성화)<br>• **동시세션 제한** 클라이언트 구간에 대한 동시 세션 수를 설정합니다. (설정 범위: 100 ~ 20,000,000, 기본값: 비활성화)<br>• **BPS 제한** 클라이언트 구간에 대한 초당 비트 수를 설정합니다. (설정 범위: 100 ~ 1,000,000, 기본값: 비활성화) |

## 기본 애플리케이션 상태 설정

기본적으로 기본 애플리케이션은 비활성화 상태로 설정됩니다. 기본 애플리케이션을 활성화하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | 화면 오른쪽 위에 있는 '**애플리케이션**' 목록의  아이콘을 클릭합니다. |
| 2 | <**애플리케이션 선택**> 팝업 창이 나타나면 애플리케이션 목록에서 기본 애플리케이션을 선택하고 [**확인**] 버튼을 클릭합니다.<br>  |
| 3 | **Application** - **애플리케이션** - **일반설정** 메뉴를 클릭합니다. |
| 4 | <**애플리케이션**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 5 | <**애플리케이션 상태 설정**> 팝업 창에서 상태를 활성화로 변경하고 [**적용**] 버튼을 클릭합니다.<br>  |

# 응답 설정

WEBFRONT-K는 애플리케이션에 설정한 보안 정책에 위배되는 클라이언트의 요청을 탐지하였을 경우, 해당 요청을 송신한 클라이언트에게 패킷이 차단되거나 에러가 발생하였음을 알려주는 응답 기능을 제공합니다.

응답 설정 기능에는 차단된 패킷을 전송한 클라이언트에게 응답을 보내는 차단 응답 설정과 에러가 발생하면 발생한 에러의 코드에 따라 서로 다른 응답을 보내는 에러 코드 별 응답 설정이 있습니다. 아래에 이 두 가지 응답 설정 방법 대해 살펴봅니다.

### 차단 응답 설정

차단된 패킷을 전송한 클라이언트에게 전송할 응답 형식에는 다음과 같은 다섯 가지가 있습니다. 관리자는 이 차단 응답 형식 중에서 한가지를 선택하여 설정할 수 있습니다.

| 응답 형식 | 설명 |
|---|---|
| 일반 | 기본적으로 설정된 응답 메시지를 보냅니다. |
| 응답 없음 | 아무런 응답 메시지를 보내지 않습니다. |
| 접속 종료 | 해당 클라이언트와의 접속을 종료합니다. |
| 리다이렉트 | 요청한 URL을 보내지 않고, 사용자가 설정한 다른 URL (에러 페이지, 시작 페이지 등)을 보냅니다. |
| 사용자 정의 | 사용자가 직접 정의한 응답 메시지를 보냅니다. |

### 에러 코드 별 응답 설정

에러 코드 별 응답은 발생한 에러 코드 별로 응답 방식을 지정하여, 에러가 발생하면 해당 에러에 지정한 응답 메시지를 클라이언트에게 전달하는 방식입니다.

에러 코드 별 응답 방식에는 '리다이렉트' 방식과 '사용자 정의' 응답 방식이 있습니다. 리다이렉트 방식을 선택하면 클라이언트에게 보내줄 URL을 입력하면 되고, 사용자 정의 응답 방식을 선택하면 에러가 발생한 경우에 전송할 응답 메시지를 사용자가 직접 작성하면 됩니다.

에러 코드 별 응답 기능 동작 시, 해당 이력에 대한 로그를 남길 수 있습니다. 또한 서버에서 클라이언트로 전송되는 응답을 WEBFRONT-K가 차단할 수 있습니다.

## 설정 개요

### 설정 화면

**애플리케이션** - **응답설정** 메뉴를 클릭하면 애플리케이션 응답 설정 정보를 출력하고 변경할 수 있는 응답 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **응답 설정 정보** 이 부분에서는 현재 설정된 응답 방식이 표시됩니다.
- **응답설정 에러 코드 리스트** 이 부분에서는 현재 설정된 에러 코드 별 응답 설정 정보가 표시됩니다.

**설정 과정**

앞의 설정 화면에서 각 세부 기능의 변경 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 애플리케이션 응답 설정을 하는 과정은 다음과 같습니다.

❶ 응답 방식 설정

애플리케이션 보안 기능의 각 정책이 허용하지 않는 패킷을 발견한 경우에 해당 패킷을 전송한 클라이언트에게 패킷이 차단되거나 에러가 발생하였음을 알려주는 방식을 설정합니다. 응답 방식에는 일반, 응답 없음, 접속 종료, 리다이렉트와 사용자 정의 등 5가지가 있습니다. 기본적으로는 일반으로 지정됩니다.

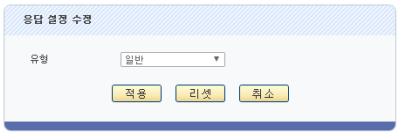
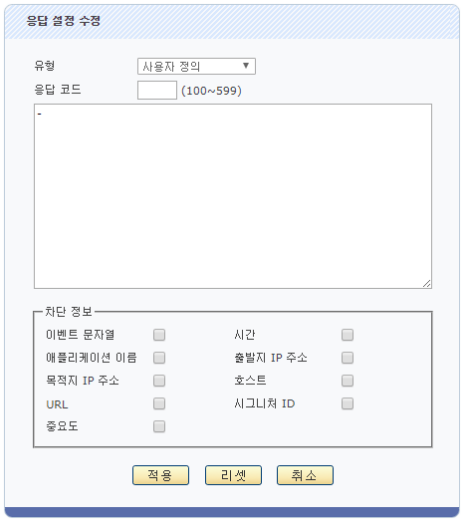
❷ 에러 코드 별 응답 설정

발생한 에러 코드 별로 응답 방식을 지정하여, 에러가 발생하면 해당 에러에 지정한 응답 메시지를 클라이언트에게 전달하는 방식을 설정합니다.

# 응답 설정하기

## 차단 응답 방식 설정

다음은 애플리케이션의 요청 패킷을 차단한 경우 클라이언트에게 어떻게 응답할지를 설정하는 방법입니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **응답설정** 메뉴를 클릭합니다. |
| 2 | <**응답 설정 정보**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**응답 설정 수정**> 팝업 창에서 다음 설명을 참고하여 각 항목들을 입력한 후 [**적용**] 버튼을 클릭합니다. 선택한 응답 방식에 따라 설정 항목이 조금 다르므로 각 응답 방식에 대한 설명은 아래의 설명을 참고합니다. 기본적으로는 기본 응답 페이지를 전송하는'일반'으로 지정됩니다.<br>  <br><br>• **일반** 기본적으로 설정된 응답 메시지를 보냅니다.<br>• **응답 없음** 아무런 응답 메시지도 보내지 않습니다.<br>• **접속 종료** 해당 클라이언트와의 접속을 종료합니다.<br>• **리다이렉트** 요청한 URL을 보내지 않고, 사용자가 설정한 다른 URL(에러 페이지, 시작 페이지 등)을 보내려는 경우에 이 항목을 선택합니다. 이 항목을 선택하면 URL을 설정할 수 있는 항목이 나타납니다. URL 항목에 요청한 URL 대신 전송할 URL을 입력합니다. 입력 가능한 URL의 최대 길이는 256 자 입니다.<br>• **사용자 정의** 사용자가 직접 정의한 응답 메시지를 보내려는 경우에 이 항목을 선택합니다. 이 항목을 선택하면 응답 코드를 입력하는 항목과 사용자가 응답 메시지를 정의할 수 있는 항목, 차단 정보 항목이 다음과 같이 나타납니다.<br>  <br><br>응답 코드 항목에 100~599 범위의 응답 코드 번호를 입력하고, 아래 텍스트 박스에는 클라이언트에게 전송할 페이지 내용을 입력합니다. 사용자 정의 응답 메시지에는 알파벳과 한글로 이루어진 최대 1024글자의 문자열을 |

| | |
|---|---|
| | 입력할 수 있습니다. 화면 하단의 차단 정보 항목을 선택할 경우, 클라이언트의 응답 페이지에 선택된 항목의 정보가 함께 출력됩니다.<br>• **HTTPS 리다이렉트** '리다이렉트'와 동일하게 동작하지만, 사용자가 설정한 URL에 대해 HTTP가 아닌 HTTPS 페이지를 보내줍니다. |
| 4 | 설정을 완료한 후 [**적용**] 버튼을 클릭합니다. |

## 에러 코드 별 응답 설정

각 에러 코드별로 전송할 응답을 설정하는 방법은 다음과 같습니다. 애플리케이션에는 최대 256개의 응답 설정을 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** - **응답설정** 메뉴를 클릭합니다. |
| 2 | <**응답 설정 에러 코드 리스트**>의 [**변경**] – [**추가**]버튼을 클릭합니다. |
| 3 | <**에러 코드 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목들을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 에러 코드의 사용 여부를 지정합니다. 기본적으로는 비활성화로 설정됩니다.<br>• **에러 코드** 응답 방식을 설정할 에러 코드를 입력합니다. 에러 코드의 입력 범위는 100~999입니다.<br>• **유형** 지정한 에러 코드에 해당되는 에러가 발생하면 클라이언트에게 보낼 응답의 형식을 지정합니다. 응답 형식에는 다음과 같은 리다이렉트와 사용자 정의 2가지가 있습니다. 기본적으로는 사용자 정의로 선택됩니다.<br>– 사용자 정의 사용자가 직접 정의한 응답 메시지를 보내려는 경우에 사용자 정의로 지정합니다. 이 경우에는 응답 코드 항목에 대한 설명을 참고하여 응답 코드를 지정합니다.<br>– 리다이렉트 요청한 URL을 보내지 않고, 사용자가 설정한 다른 URL(에러 페이지, 시작 페이지 등)을 보내려는 경우에 리다이렉트를 선택합니다. 리다이렉트를 선택한 경우에는 URL 항목이 나타납니다. URL 항목에 요청한 URL 대신 전송할 URL을 입력합니다. URL은 최대 256 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>– HTTPS 리다이렉트 'HTTPS 리다이렉트'와 동일하게 동작하지만, 사용자가 설정한 URL에 대해 HTTP가 아닌 HTTPS 페이지를 보내줍니다.<br>• **응답 코드** 응답 코드 항목에 100~599 범위의 응답 코드 번호를 입력하고, 아래 텍스트 박스에 클라이언트에게 전송할 페이지 내용을 입력합니다. 사용자 정의 응답 메시지에는 알파벳과 한글로 이루어진 최대 1024글자의 문자열을 입력할 수 있습니다. |
| 4 | 응답 설정을 모두 추가한 후에는 상태 항목에서 활성화, 차단, 보안 로그 사용 여부를 지정하고 [**적용**] 버튼을 클릭합니다. |

# 기타 설정

이 절에서는 WEBFRONT-K의 기타 설정 메뉴에서 설정하는 기능들에 대해 살펴봅니다. 기타 설정 메뉴에서는 다음과 같은 기능들을 설정할 수 있습니다.

- **애플리케이션 인코딩 정보**
  WEBFRONT-K는 인코딩 방식으로 UTF-8과 EUC-KR 인코딩을 지원합니다. 기본 인코딩 방식은 EUC-KR 로 설정되어 있습니다. WEBFRONT-K의 인코딩 방식은 애플리케이션 서비스를 제공하는 웹 서버의 인코딩 방식과 동일해야 됩니다. 인코딩 방식이 서로 다른 경우 한글을 포함하는 패킷을 WEBFRONT-K에서 인식할 수 없으므로 보안 기능을 수행할 수 없습니다. 그러므로, WEBFRONT-K를 운용하기 전에 웹 애플리케이션 관리자에게 문의하여 웹 서버의 인코딩 방식을 확인한 후 이와 동일하게 WEBFRONT-K의 인코딩 방식을 설정해야 합니다.

- **애플리케이션 세션 정보**
  WEBFRONT-K는 특정 클라이언트가 요청하는 모든 연결을 동일한 애플리케이션 세션을 통해 수행하는 '세션 지속 연결' 기능을 제공합니다. WEBFRONT-K는 IP주소를 기준으로 하여 동일한 클라이언트에서 전송한 요청 패킷인지 판단합니다. 이전과 동일한 클라이언트로부터의 요청인 경우에는 이전에 생성한 세션을 그대로 사용합니다. 이러한 세션 지속 연결 기능은 사용자가 지정한 시간(타임아웃) 동안에만 적용됩니다. 세션 지속 연결 기능은 WEBFRONT-K의 요청 검사 기능 중에서 세션 별 과다 요청 제어 기능과 같이 세션을 기반으로 하는 기능에 적용되고 부하 분산 기능에서 동일한 클라이언트의 요청을 동일한 서버로 전송할 수 있게 해줍니다.

- **애플리케이션 URL 대소문자 구분 정보**
  윈도우 웹 서버는 애플리케이션 URL의 대소문자를 구분하지 않습니다. 하지만, 리눅스 웹 서버는 애플리케이션 URL의 대소문자를 구분하는 경우가 있습니다. 이런 경우에는 WEBFRONT-K도 URL의 대소문자를 구분하도록 설정해야 합니다.

- **애플리케이션 쿼리스트링 검사 정보**
  쿼리스트링은 URL의 일부로 클라이언트의 정보를 웹 애플리케이션에 전달하기 위해 사용되며, 물음표(?)로 시작하여 name=value 형식으로 구성됩니다. 쿼리스트링 검사를 활성화하게 되면 물음표 이후의 쿼리스트링 전체에 대해서 버퍼 오버플로우 차단, SQL 삽입 차단, 스크립트 삽입 차단 기능이 적용됩니다. 그러나, 쿼리 스트링 검사 기능을 사용하면 오탐이나 성능 저하의 문제가 발생할 수 있습니다. 이런 경우에는 쿼리스트링 검사를 비활성화로 설정해야 합니다.

- **애플리케이션 쿠키 매개변수 검사 정보**
  클라이언트와 웹 서버간의 연결을 유지하기 위해 사용되는 쿠키에 SQL 삽입, 스크립트 삽입 등의 공격 구문이 포함되었는지를 검사하려면 쿠키 매개변수 검사 기능을 사용합니다. 쿠키 매개변수 검사를 활성화하면 쿠키의 매개변수 값에 대해서 버퍼 오버플로우 차단, SQL 삽입 차단, 스크립트 삽입 차단, 업로드 검사, 다운로드 검사 기능이 적용됩니다.

- **애플리케이션 사용자 IP 표기 헤더명 변경 정보**
  클라이언트의 IP 주소를 표기하는 X-Forwarded-For 헤더명이 일부 네트워크 장비에 의해 임의의 값으로 변경된 경우, 로그 뷰어에서 클라이언트의 IP 주소 정보를 출력할 수 없습니다. 이런 경우 사용자 IP 표기 헤더명 변경 기능을 사용하면, WEBFRONT-K가 변경된 헤더명을 인식하여 클라이언트 IP 주소가 정상적으로 출력됩니다.

- **애플리케이션 XML 요청 검사 정보**
  WEBFRONT-K는 기본적으로 클라이언트가 POST 메서드를 사용하여 전송한 요청 패킷의 바디가 XML인 경우, XML에 대한 요청 검사를 수행하지 않습니다. XML에 대한 요청 검사를 수행하려면 XML 요청 검사를 활성화해야 합니다. XML 요청 검사를 활성화하면 XML에 대해 버퍼 오버플로우 차단(쉘 코드 검사), SQL 삽입 차단, 스크립트 삽입 차단, 다운로드 검사, 인클루드 인젝션 차단 기능이 적용됩니다.

- **애플리케이션 매개변수 검사 정보**
  요청 패킷에 포함된 매개변수 값의 길이가 긴 경우, 해당 요청 패킷에 대한 요청 검사 수행 시간이 많이 소요되어 웹 서비스가 지연될 수 있습니다. 이런 경우에는 매개변수 검사 길이를 설정하여 요청 검사를 수행할 매개변수의 최대 길이를 지정하면 웹 서비스가 지연되는 현상을 방지할 수 있습니다.

- **애플리케이션 프로토콜 정보**
  패킷의 시퀀스가 순서대로 수신되는지를 검사하는 시퀀스 검사 수행 여부와 HTTP/1.1의 다중메서드(pipelining)를 사용하는 클라이언트의 요청에 대한 보안 검사 수행 여부를 선택합니다. 시퀀스 검사를 활성화 한 경우 네트워크 환경에 따라 서비스가 지연될 가능성이 있으므로, 이러한 경우에는 시퀀스 검사를 비활성화로 설정합니다. 또한 다중 메서드를 사용한 요청을 보안 검사하는 과정에서도 서비스가 지연되는 문제가 발생할 수 있으므로, 이러한 경우에는 다중 메서드 검사를 비활성화 합니다.

- **애플리케이션 소스 포트 NAT 정보**
  출발지 포트를 NAT하려면 애플리케이션 소스 포트 NAT 정보를 활성화합니다.

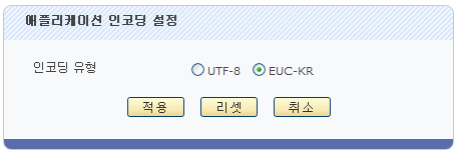
- **애플리케이션 비정상 요청 bypass**
  WEBFRONT-K에 연결된 세션이 연결 중간에 보안 엔진으로 접속될 경우 세션을 bypass 처리할 것인지, 차단 응답(reset)을 보낼 것인지 선택합니다. 기능을 활성화하면 bypass 처리하게 되고, 비활성화하면 차단 응답을 전송합니다.

- **애플리케이션 MIME 요청 검사 정보**
  애플리케이션별로 MIME(Multipurpose Internet Mail Extensions) 요청을 검사하려면 애플리케이션 MIME 요청 검사 정보를 활성화합니다.

- **애플리케이션 JSON 요청 검사 정보**
  JSON(JavaScript Object Notation) 형식의 요청을 검사하려면 애플리케이션 JSON 요청 검사 정보를 활성화합니다.

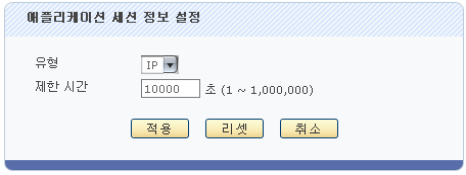
## 인코딩 방식 설정하기

애플리케이션의 인코딩 방식을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 인코딩 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 인코딩 설정**> 팝업 창에서 인코딩 방식을 선택한 후 [**적용**] 버튼을 클릭합니다. 인코딩 방식은 애플리케이션 서비스를 제공하는 웹 서버의 인코딩 방식과 동일해야 됩니다. (기본값: EUC-KR)<br>  |

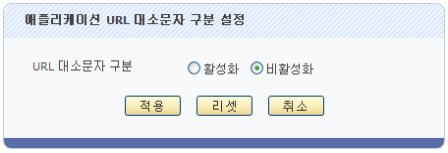
## 세션 지속 연결 제한 시간 설정하기

애플리케이션의 세션 지속 연결 제한 시간을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 세션 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 세션 정보 설정**> 팝업 창에서 아래의 설명을 참고하여 제한 시간을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **제한 시간** 동일한 클라이언트와 연결된 세션을 유지할 타임 아웃 시간을 지정합니다. 타임 아웃 시간이 경과한 후에는 동일한 클라이언트로부터 요청이 오더라도 새로운 세션을 형성합니다.<br>(설정 범위: 1 ~ 1,000,000, 기본값: 10,000초) |

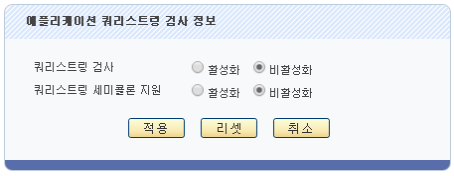
## URL 대소문자 구분 여부 설정하기

애플리케이션의 URL 대소문자 구분 여부를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 URL 대소문자 구분 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 URL 대소문자 구분 설정**> 팝업 창에서 URL 대소문자 구분 여부를 지정한 후 [**적용**] 버튼을 클릭합니다. (기본값: 비활성화)<br>  |

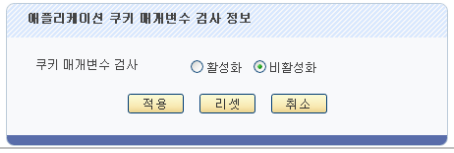
## 쿼리스트링 검사 여부 설정하기

애플리케이션의 쿼리스트링 검사 여부를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 쿼리스트링 검사 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 쿼리스트링 검사 정보**> 팝업 창에서 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **쿼리스트링 검사** 쿼리스트링 검사 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **쿼리스트링 세미콜론 지원** 쿼리스트링 세미콜론 지원의 사용 여부를 지정합니다. 기능을 활성화하면 URL에서 인코딩되어 있지 않은 물음표(?) 또는 앰퍼샌드(&)를 세미콜론(;)으로 분류합니다. (기본값: 비활성화) |

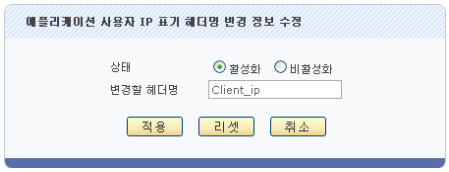
## 쿠키 매개변수 검사 여부 설정하기

애플리케이션의 쿠키 매개변수 검사 여부를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 쿠키 매개변수 검사 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 쿠키 매개변수 검사 정보**> 팝업 창에서 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다. (기본값: 비활성화)<br>  |

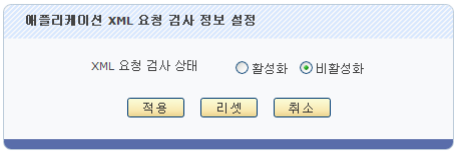
## 사용자 IP 표기 헤더명 변경 설정하기

애플리케이션의 사용자 IP 표기 헤더명 변경을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션 – 기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 사용자 IP 표기 헤더명 변경 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 사용자 IP 표기 헤더명 변경 정보 수정**> 팝업 창에서 다음 설명을 참고하여 사용 여부와 변경할 헤더명을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 사용자 IP 표기 헤더명 변경 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **변경할 헤더명** 네트워크 장비에 의해 변경된 헤더명을 입력합니다. 최대 64 글자의 영문자와 숫자, 그리고 '_', '-' 기호를 입력할 수 있습니다. |

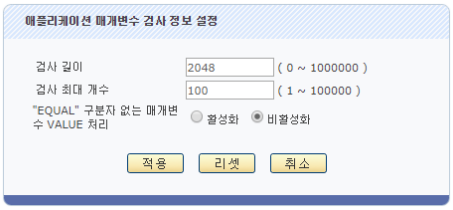
## XML 요청 검사 설정하기

애플리케이션의 XML 요청 검사 여부를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션 – 기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 XML 요청 검사 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 XML 요청 검사 정보 설정**> 팝업 창에서 XML 요청 검사 상태를 여부를 지정한 후 [**적용**] 버튼을 클릭합니다. (기본값: 비활성화)<br>  <br> |

## 매개변수 검사 정보 설정하기

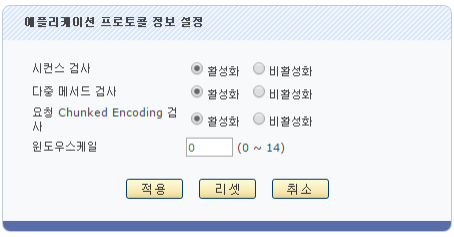
애플리케이션의 매개변수 검사 정보를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션 – 기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 매개변수 검사 길이 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 매개변수 검사 길이 정보 설정**> 팝업 창에서 다음 설명을 참고하여 매개변수 검사 길이와 검사 최대 개수를 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **검사 길이** 요청 검사를 수행할 매개변수 값의 길이를 지정합니다. '0'으로 설정한 경우에는 매개 변수의 모든 값을 검사합니다. (설정 범위: 0 ~ 1,000,000, 기본값: 2048)<br>• **검사 최대 개수** 검사할 매개변수의 최대 개수를 지정합니다. 지정한 값을 초과하면 더 이상 검사하지 않습니다. (설정 범위: 1 ~ 100,000, 기본값: 100)<br>• **"EQUAL" 구분자 없는 매개변수 VALUE 처리** 매개변수에 Equal(=) 구분자가 없는 경우에 대한 검사 여부를 지정합니다. |

| | | |
|---|---|---|
| | | 기능을 활성화하면 Equal 구분자가 없는 경우에도 검사를 수행합니다.<br>(기본값: 비활성화) |

## 애플리케이션 프로토콜 정보 설정하기

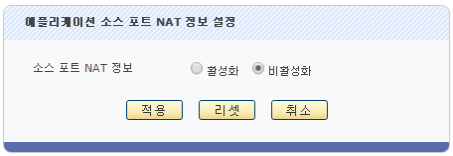
애플리케이션의 프로토콜 정보를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 프로토콜 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 프로토콜 정보 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **시컨스 검사** 시컨스 검사 여부를 지정합니다. (기본값: 활성화)<br>• **다중 매서드 검사** 다중 매서드 검사 여부를 지정합니다. (기본값: 활성화)<br>• **요청 Chunked Encoding 검사** 요청 Chunked Encoding 검사 여부를 지정합니다. (기본값: 활성화)<br>• **윈도우 스케일** 윈도우 스케일 크기를 지정합니다. '0'으로 지정하면 기능이 비활성화됩니다.<br>(설정 범위: 0 ~ 14, 기본값: 0) |



## 소스 포트 NAT 정보 설정하기

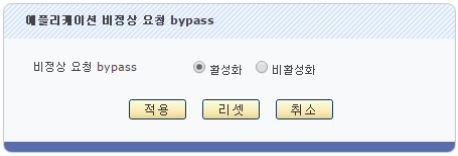
소스 포트에 NAT 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 소스 포트 NAT 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 소스 포트 NAT 정보 설정**> 팝업 창에서 소스 포트 NAT 정보의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다.<br>(기본값: 비활성화)<br>  |



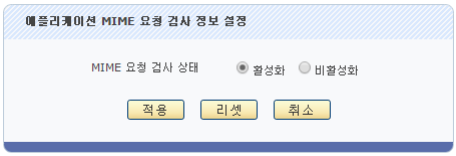
## 비정상 요청 bypass 설정하기

비정상 요청 bypass를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 비정상 요청 bypass**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 비정상 요청 bypass**> 팝업 창에서 비정상 요청 bypass의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다.<br>(기본값: 활성화)<br>  |

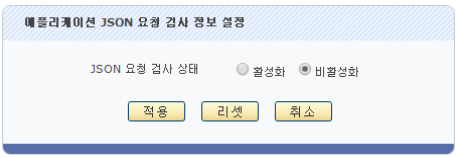
## MIME 요청 검사 정보 설정하기

MIME 요청 검사를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 MIME 요청 검사 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 MIME 요청 검사 정보 설정**> 팝업 창에서 MIME 요청 검사의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다.<br>(기본값: 활성화)<br>  |

## JSON 요청 검사 정보 설정하기

JSON 요청 검사를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **애플리케이션** – **기타 설정** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 JSON 요청 검사 정보**> 부분의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 JSON 요청 검사 정보 설정**> 팝업 창에서 JSON 요청 검사의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다.<br>(기본값: 비활성화)<br>  |

# 제3장 요청 검사 기능 설정

요청 검사는 WEBFRONT-K가 클라이언트로부터 웹 서버로 보내는 요청이 정상적인 요청인지, 공격자가 보낸 공격인지를 검사하여 대응하는 조치를 취하도록 하는 기능입니다. 이 장에서는 WEBFRONT-K에서 제공하는 각 요청 검사 기능을 설정하는 방법에 대해 소개합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 접근 제어 기능 설정
- 폼 필드 검사 기능 설정
- 과다 요청 제어 기능 설정
- 쿠키 보호 기능 설정
- 버퍼 오버플로우 차단 기능 설정
- SQL 삽입 차단 기능 설정
- 스크립트 삽입 차단 기능 설정
- 업로드 검사 기능 설정
- 다운로드 검사 기능 설정
- 디렉토리 리스팅 차단 기능 설정
- 요청 형식 검사 기능 설정
- 검사 회피 차단 기능 설정
- 인클루드 인젝션 차단 기능 설정
- 웹 공격 프로그램 차단 기능 설정
- HTTP POST 공격 차단 기능 설정
- Slowloris 공격 차단 기능 설정
- Slow Read 공격 차단 기능 설정
- 금칙어 차단 기능 설정
- 신용카드 정보 유입 차단 기능 설정
- 주민등록 정보 유입 차단 기능 설정
- WISE 요청 필터 설정



**참고:** 요청 검사 기능에 대한 상세한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 - 요청 검사 (Request Validation)**] 부분을 참고합니다.

# 접근 제어 기능 설정

접근 제어는 웹 서버가 제공하는 애플리케이션 중에서 클라이언트가 접근할 수 있는 URL 목록을 지정하여, 지정된 URL에만 접속이 가능하게 하는 기능입니다. 애플리케이션 접근 제어 기능은 차단 URL, 시작 URL, 허용 URL, 진입 URL, 보호 URL을 등록하여 클라이언트가 웹 서버에 접근하는 것을 제한합니다.

이 기능은 지정한 URL 유형과 보안 수준에 따라 '**기본**' 애플리케이션 접근 제어와 '**고급**' 애플리케이션 접근 제어로 나눌 수 있습니다. 기본 애플리케이션 접근 제어에서는 차단 URL과 허용 URL을 지정하여 차단 URL에 속하지 않으면서 허용 URL에는 포함된 URL에만 접근할 수 있게 합니다. 고급 애플리케이션 접근 제어에서는 URL 정규식 검사를 설정하여 보다 다양한 차단 URL 시그니처를 설정할 수 있고, 시작 URL과 진입 URL, 보호 URL을 추가로 설정하여 여러 단계에 거쳐 애플리케이션에 대한 접근을 제한하므로 보안을 한층 더 강화할 수 있습니다.

고급 애플리케이션 접근 제어에서는 허용 URL로 가기 위해 반드시 거쳐야 하는 시작 URL을 지정할 수 있고, 기본 애플리케이션 접근 제어에서 설정한 허용 URL을 허용 URL과 보안이 더 필요한 보호 URL로 구분하여 설정할 수 있습니다. 보호 URL은 시작 URL뿐만 아니라 진입 URL까지도 통과해야만 접근할 수 있습니다. 시작 URL은 자체적으로 여러 단계를 거치도록 할 수 있습니다. 여러 개의 시작 URL을 추가하고 단계를 지정하면(기본적으로는 추가한 순서대로 단계가 정해집니다) 각 단계별 URL을 차례로 통과해야만 허용 URL로 접근할 수 있습니다. 시작 URL은 최대 10단계까지 설정할 수 있습니다.

관리자는 먼저 기본 접근 제어 기능을 사용할지, 고급 접근 제어 기능을 사용할지를 결정하고, 각 URL 목록에 등록할 URL 정보를 정한 후 애플리케이션 접근 제어 기능을 설정하도록 합니다.

이 절에서는 애플리케이션 접근 제어 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 실제로 애플리케이션 접근 제어 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **접근제어** 메뉴를 클릭하면 애플리케이션 접근 제어 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **애플리케이션 접근제어** 애플리케이션 접근 제어 기능의 활성화 상태와 애플리케이션 접근 제어 기능과 관련된 기능의 활성화 상태가 표시됩니다. 애플리케이션 접근 제어 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **허용 URL 리스트** 현재 등록된 허용 URL 목록이 표시됩니다.
- **고급 애플리케이션 접근 제어** URL 정규식 검사, 시작 URL 접근 제어, 고급 접근 제어, 국가별 접근제어 상태, 접근 로그, 확장자 없는 URL 허용의 활성화 상태가 표시됩니다.

## 설정 과정

기본 애플리케이션 접근 제어 기능과 고급 애플리케이션 접근 제어 기능을 설정하는 과정은 각각 다음과 같습니다.

### 기본 애플리케이션 접근 제어 기능

1. 차단 URL 등록
   클라이언트의 접근 시도에 가장 먼저 적용할 차단 URL 시그니처를 설정합니다. 차단 URL 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.
2. 허용 URL 등록
   차단 URL 다음으로 적용할 허용 URL을 등록합니다. 허용 URL에 등록된 URL로의 접근은 허용됩니다. 단, 시작 URL이 설정되어 있는 경우에는 시작 URL을 통과한 접근만 허용됩니다. 기본적으로 허용 URL에 모든 URL을 의미하는 '/*'가 등록되어 있습니다. 허용 URL이 100개 이상인 경우에는 Web Manager 화면에서 일일이 등록하기보다는 파일을 사용하는 것이 편리하고 속도도 더 빠릅니다.
3. 관련 기능의 활성화 상태 설정
   애플리케이션 접근 제어 기능의 사용 여부와 이 기능에 대한 보안 로그, 학습, 차단, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

### 고급 애플리케이션 접근 제어 기능

1. URL 정규식 검사 설정
   URL 정규식 검사의 사용 여부를 설정하고 URL 정규식 검사 시그니처를 설정합니다. URL 정규식 검사 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.
2. 시작 URL 등록
   허용 URL 목록에 등록된 URL에 접근하기 전에 미리 통과해야 하는 시작 URL을 등록합니다. 시작 URL은 필수적으로 지정하지 않아도 됩니다. 시작 URL을 지정하지 않은 경우에는 클라이언트가 직접 허용 URL 목록에 있는 URL에 접근할 수 있습니다. 기본적으로 등록된 시작 URL은 없습니다. 시작 URL은 최대 10개(10단계)까지 등록할 수 있습니다. 시작 URL을 등록할 때에는 해당 URL을 요청할 때 추가로 허용 URL로 등록할 URL(종속 URL)을 지정할 수 있습니다. 예를 들어, 시작 URL로 등록하고자 하는 /index.html에서 사용하는 그림 파일이 /*.jpg URL에 저장되어 있다면 /*.jpg를 종속 URL로 등록해야 합니다.
3. 진입 URL과 보호 URL 등록
   진입 URL과 보호 URL을 등록합니다. 진입 URL은 보호 URL에 등록된 URL에 접근하기 전에 미리 통과해야 하는 URL입니다. 보호 URL은 허용 URL보다 한층 더 강화된 보안이 필요한 URL로, 진입 URL을 통과해야만 접근할 수 있습니다. 일반적으로는 웹 서버에 로그인하기 위한 URL을 진입 URL 목록에 등록하고, 웹 서버에 로그인한 후 접근할 수 있는 URL을 보호 URL로 등록합니다.
4. 접근 로그 상태 설정
   모든 클라이언트 요청에 대한 기록을 저장할지 여부(접근 로그)를 설정합니다.

# 애플리케이션 접근 제어 설정하기

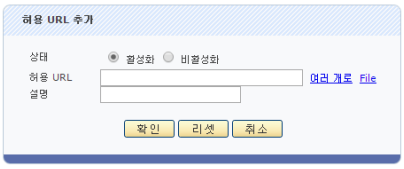
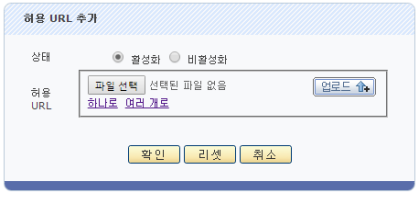
이 절에서는 기본적인 애플리케이션 접근 제어 기능을 사용하기 위해 필요한 설정 작업에 대해 살펴봅니다.

## 차단 URL 등록

차단 URL은 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 차단 URL을 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정, 사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

## 허용 URL 등록

허용 URL 목록에 허용 URL을 등록하는 방법은 다음과 같습니다. 허용 URL은 65536개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**허용 URL 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**허용 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 현재 등록하고 있는 허용 URL을 실제로 클라이언트가 접근할 수 있도록 허용할 것인지를 지정합니다. 허용하려는 경우에는 '활성화'를 선택하고, 허용하지 않으려는 경우에는 '비활성화'를 선택합니다. 허용 URL을 비활성화로 지정하면, 허용 URL 목록에 등록되어 있더라도, 클라이언트가 이 URL에 접근할 수 없습니다. (기본값: 활성화)<br>• **허용 URL** 추가하려는 허용 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다. 여러 개의 허용 URL을 입력하거나 파일에 저장되어 있는 허용 URL을 입력하려는 경우에는 다음 설명을 참고합니다.<br>– **여러 개 입력하기**<br>여러 개의 허용 URL을 입력하려는 경우에는 '여러 개로' 옵션을 클릭합니다. 그러면, 입력란의 형태가 여러 개를 입력할 수 있는 형태로 바뀝니다. 입력란을 클릭한 후 원하는 URL을 입력합니다. URL을 입력한 후에는 [**Enter**] 키를 눌러 다음 줄로 이동한 다음 계속해서 다른 URL을 입력합니다.<br>  <br><br>**참고:** '여러 개로' 옵션을 클릭하여 허용 URL을 입력하는 경우에는 URL이 100개가 넘지 않도록 합니다. 100개 이상의 허용 URL을 입력하면 허용 URL을 등록하는 데 시간이 많이 걸리게 되므로, 이런 경우에는 파일로 업로드 하는 것이 좋습니다.<br>– **파일로 업로드하기**<br>URL로 구성된 파일을 사용하여 허용 URL을 입력하려면 'File' 옵션을 클릭합니다. 그러면, 파일을 선택할 수 있는 [**찾아보기...**] 버튼이 나타납니다. 이 버튼을 클릭한 후 원하는 파일을 선택합니다. 그런 후에 [**업로드**] 버튼을 클릭합니다.<br>  <br><br>파일이 정상적으로 업로드되면 파일에 속한 URL에 대한 정보가 표시됩니다. |

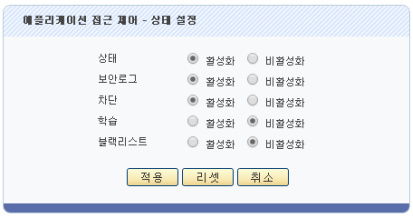

**참고:** 한 글자의 한글이 포함된 URL 의 경우, 해당 URL이 정상적으로 설정되지 않을 수 있습니다. 이런 문제가 발생하는 것을 방지하기 위해서는 알파벳과 기호로만 이루어진 URL을 사용하거나 UTF-8 인코딩된 텍스트 파일을 사용해야 합니다.

- **설명** 입력한 허용 URL에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)

4 허용 URL을 모두 등록하였으면, 설정한 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다.

## 관련 기능의 활성화 상태 설정

애플리케이션 접근 제어 기능의 사용 여부와 애플리케이션 접근 제어 기능과 관련된 보안 로그, 차단, 학습, 블랙리스트 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 접근제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 접근 제어 - 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 접근 제어 기능을 활성화할 것인지 지정합니다. 이 항목을 활성화해야만 애플리케이션 접근 제어 기능이 동작할 수 있습니다.<br>• **보안 로그** 접근 제어 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 접근 제어 기능에 의해 접근이 제한된 요청 패킷을 차단할 것인지 지정합니다. 이 항목을 활성화하면, 접근 제어 정책을 위반한 요청 패킷은 모두 차단됩니다. 만약, 이 항목을 비활성화하면, 접근 제어 정책을 위반한 요청 패킷은 차단되지 않고 웹 서버로 전달되게 됩니다. 일반적으로, 장비를 처음 설치하여 애플리케이션 접근 제어 기능을 설정하지 않았을 경우에, 이 항목을 비활성화로 설정하여 모든 요청에 대하여 학습하는 동시에 서비스도 이루어 지도록 합니다.<br>• **학습** 접근 제어 기능에 학습 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 클라이언트가 접속을 요청한 URL, 매개변수를 전달하는 URL, 매개변수의 형식과 길이 정보를 기록합니다. 학습 정보는 **[Application - 학습 - 접근제어 학습]** 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 접근 제어 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 접근 제어 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

**참고:** 차단 URL 기능의 차단 설정은 각 시그니처 액션 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '시스템 구성 설명서'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**] 부분을 참고합니다.

# 고급 애플리케이션 접근 제어 설정하기

이 절에서는 고급 애플리케이션 접근 제어 기능인 URL 정규식 검사를 설정하는 방법, 확장자 없는 URL 허용을 설정하는 방법, 시작 URL을 설정하는 방법, 진입 URL과 보호 URL을 설정하는 방법, 국가별 접근제어를 설정하는 방법, 그리고 접근 로그의 상태를 설정하는 방법에 대해 알아봅니다.

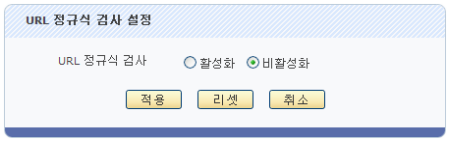
## URL 정규식 검사 설정

URL 정규식 검사는 차단 URL을 보완하기 위한 기능으로 정규식 시그니처를 설정할 수 있다는 점만 다르고, 기본적인 동작과 기능은 차단 URL과 같습니다. 차단 URL은 URL 형식의 시그니처만 설정할 수 있어 시그니처 작성에 제약사항이 있지만 URL 정규식 검사는 정규식 형식의 시그니처를 지원하여 차단 URL 보다 다양한 시그니처를 설정할 수 있습니다. URL 정규식 검사를 사용하려면 먼저, URL 정규식 검사 상태를 활성화하고 URL 정규식 검사 시그니처를 설정해야 합니다.

**참고:** URL 정규식 검사는 차단 URL보다 다양한 시그니처를 설정할 수 있지만 검사 시간이 많이 소요되기 때문에 필요한 경우에만 사용하도록 합니다.

### URL 정규식 검사 상태 설정

URL 정규식 검사 상태를 설정하는 방법은 다음과 같습니다. URL 정규식 검사는 기본적으로 비활성화되어 있습니다.

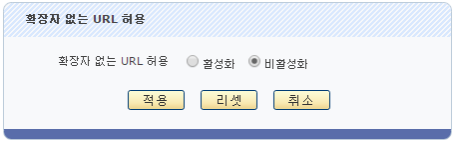
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**고급 애플리케이션 접근 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**URL 정규식 검사 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <**URL 정규식 검사 설정**> 팝업 창에서 URL 정규식 검사 항목을 활성화로 변경하고 [**적용**] 버튼을 클릭합니다.<br>  |

### URL 정규식 검사 시그니처 설정

URL 정규식 검사 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. URL 정규식 검사 시그니처를 설정하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**, **사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

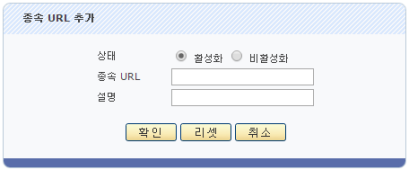
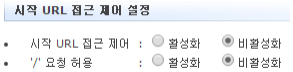
## 확장자 없는 URL 허용 상태 설정

확장자 없는 URL 허용 기능은 URL에 확장자가 없을 경우, 허용 URL 리스트에 존재하지 않아도 해당 URL에 대한 요청을 허용하는 기능입니다. 확장자 없는 URL 허용 상태를 설정하는 방법은 다음과 같습니다. 해당 기능은 기본적으로 비활성화되어 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**고급 애플리케이션 접근 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**확장자 없는 URL 허용**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <**확장자 없는 URL 허용**> 팝업 창에서 확장자 없는 URL 허용 항목을 활성화로 변경하고 [**적용**] 버튼을 클릭합니다.<br>  |

### 시작 URL 등록

시작 URL을 등록하는 방법은 다음과 같습니다. 시작 URL은 10개까지 등록할 수 있습니다. 시작 URL을 등록할 때마다 단계가 하나씩 증가합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**고급 애플리케이션 접근 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**시작 URL 접근 제어 설정**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**시작 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 시작 URL을 실제로 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **시작 URL** 추가하려는 시작 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **설명** 시작 URL에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>• **종속 URL 리스트** 시작 URL를 요청할 때 허용 URL에 추가시킬 종속 URL을 등록합니다. 다음은 종속 URL을 등록하는 방법입니다.<br>❶ 종속 URL 리스트의 [**추가**] 버튼을 클릭합니다.<br>❷ <**종속 URL 추가**> 팝업 창에서 다음 설명을 참고하여 팝업 창의 각 항목을 입력한 후 [**확인**]을 클릭합니다.<br>  <br>– 상태 설정 중인 종속 URL의 사용 여부를 지정합니다.<br>– 종속 URL 종속 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있고 반드시 '/'로 시작해야 합니다.<br>– 설명 설정 중인 종속 URL에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 5 | 시작 URL 접근 제어 항목에서 시작 URL 기능의 사용 여부를 지정합니다. 그리고, '/' 요청 허용 항목에서 '/'을 1단계의 시작 URL로 사용할 것인지를 지정합니다. 기본적으로 두 항목은 모두 비활성화로 설정되어 있습니다.<br>  <br>**참고:** 대부분의 도메인은 도메인 이름 뒤에 '/'를 입력하면 /index.html을 기본적으로 불러옵니다. 이러한 도메인에서는 1단계 시작 URL로 /index.html과 '/'을 모두 등록해야 합니다. 하지만, WEBFRONT-K는 각 단계의 시작 URL을 하나만 설정할 수 있기 때문에 두 URL을 모두 1단계 시작 URL로 등록할 수 없습니다. 그러므로, 이런 경우에는 1단계 시작 URL은 /index.html 로 설정하고, '/' 요청 허용 항목을 활성화하도록 합니다. |
| 6 | 설정한 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

### 시작 URL 단계 변경하기

등록한 시작 URL의 단계를 변경하려면 시작 URL 리스트에서 시작 URL을 선택한 후 다음 4개의 아이콘을 사용하여 URL을 원하는 단계로 옮기면 됩니다.

 1단계로  한 단계 위로  한 단계 뒤로  마지막 단계로

### 시작 URL 상세 정보 보기

시작 URL 리스트에서 [**상세 보기**] 버튼을 클릭하면 해당 시작 URL에 대한 상세 설정 정보를 보여주는 팝업 창이 나타납니다.


## 진입 URL과 보호 URL 등록

진입 URL과 보호 URL을 등록하는 방법은 다음과 같습니다. 진입 URL과 보호 URL은 각각 65536개까지 등록할 수 있습니다.

**참고:** 진입 URL과 보호 URL을 등록하는 방법은 거의 동일하므로 이 절에서 함께 설명합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**고급 애플리케이션 접근 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**고급 접근 제어 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | 진입 URL을 추가하려면 위쪽에 있는 [**추가**] 버튼을 클릭하고, 보호 URL을 추가하려면 아래쪽에 있는 [**추가**] 버튼을 클릭합니다. |
| 5 | 각각 <**진입 URL 추가**>, <**보호 URL 추가**> 팝업 창이 나타납니다. 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL을 실제로 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **URL** 추가하려는 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 6 | 진입 URL과 보호 URL을 모두 등록한 후에는, 고급 접근 제어 항목에서 고급 애플리케이션 접근 제어 기능의 사용 여부를 지정합니다. (기본값: 비활성화) |
| 7 | 설정한 고급 애플리케이션 접근 제어 기능을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

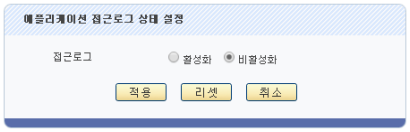
## 국가별 접근제어 설정

국가별 접근제어는 국가별 IP 주소 대역을 기준으로 애플리케이션 접근을 허용 또는 차단하는 기능입니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**고급 애플리케이션 접근 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**국가별 접근제어 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <**지원 국가 리스트**>에서 국가를 선택한 후 [**추가**] 버튼을 클릭합니다. 추가한 국가는 <**선택된 국가 리스트**>에서 확인할 수 있습니다.<br>  |
| 5 | <**국가별 접근제어**> 항목에서 기능의 사용 여부와 접근제어 정책을 지정합니다. (기본값: 비활성화 / 블랙리스트)<br>  <br>• **국가별 접근제어 상태** 국가별 접근제어 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **선택된 국가 접근제어 정책** 접근제어 방식을 지정합니다. 블랙리스트는 선택된 국가만 차단하고 나머지 국가는 허용합니다. 화이트리스트는 선택된 국가만 허용하고 나머지 국가는 차단합니다. (기본값: 블랙리스트) |
| 6 | 설정한 국가별 접근제어 기능을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 접근 로그의 상태 설정

고급 애플리케이션 접근 제어의 기능 중 '접근 로그' 기능은 모든 클라이언트의 접근 요청에 대한 정보를 접근 로그로 저장하는 기능입니다. 이 기능은 기본적으로 비활성화되어 있는데, 다음과 같은 방법으로 활성화할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**고급 애플리케이션 접근 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 접근 로그 정보**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <지원 국가 리스트>에서 접근로그 항목을 활성화로 변경하고 [**적용**] 버튼을 클릭합니다.<br>  |

**주의:** 접근 로그는 다른 종류의 로그에 비해 발생하는 양이 훨씬 많습니다. 따라서, 접근 로그를 활성화하면 로그 버퍼의 대부분이 접근 로그로 채워지게 되어 주요한 보안 로그들이 삭제될 수 있습니다. 그러므로, 반드시 필요한 경우에만(URL 구조 분석 기능을 사용하는 등의 접근 로그를 활성화하는 것을 권장합니다.

# 폼 필드 검사 기능 설정

폼 필드 검사는 클라이언트가 웹 서버로 보내는 요청 웹 페이지에 포함된 폼 필드 입력 내용이 허용 범위인지 또는 변조되었는지 검사하는 기능입니다. 폼 필드 검사는 액션 URL 검사 기능, 취약한 비밀 번호 검사 기능, 매개 변수 보호 기능으로 구성되어 있습니다. 일반적으로 많이 사용되는 액션 URL 검사 기능은 '기본 폼 필드 검사 기능'이고, 취약한 비밀 번호 검사 기능과 매개 변수 보호 기능은 '고급 폼 필드 검사 기능'으로 분류되어 있습니다.

액션 URL 검사 기능은 WEBFRONT-K에 설정된 액션 URL의 폼 필드 정보와 클라이언트가 웹 서버로 보내는 액션 URL을 비교하여 액션 URL의 폼 필드가 변조되었는지를 검사하는 기능입니다. 취약한 비밀 번호 검사 기능은 공격자가 쉽게 예상 가능한 비밀 번호를 설정하지 않도록 방지해주는 기능이고, 매개 변수 보호 기능은 클라이언트가 매개 변수의 값을 이용하여 공격하는 것을 암호화와 일치성 검사를 통해 차단하는 기능입니다.

이 절에서는 폼 필드 검사 기능을 설정하는 화면과 설정하는 과정을 살펴본 후, 각 폼 필드 검사 기능을 설정하는 방법에 대해 알아봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **폼필드검사** 메뉴를 클릭하면 폼 필드 검사 기능을 설정할 수 있는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **폼 필드 검사** : 폼 필드 검사 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 폼 필드 검사 기능의 사용 여부는 아이콘으로 표시됩니다. (초록색)은 활성화 상태를 나타내고, (빨간색)는 비활성화 상태를 나타냅니다.
- **액션 URL 리스트** : 액션 URL 검사 기능이 수행되는 액션 URL 목록이 표시됩니다.
- **고급 폼 필드 검사** : 매개 변수 보호 기능과 취약한 비밀 번호 검사 기능의 활성화 상태가 표시됩니다.
- **사용자 정의 학습 패턴** : 사용자가 정의한 학습 패턴 목록이 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 폼 필드 검사 기능을 설정하는 과정은 각각 다음과 같습니다.

❶ 액션 URL 설정

액션 URL 검사 기능을 사용할 경우, 이 기능을 적용할 액션 URL과 액션 URL에 포함되는 폼 필드의 정보를 등록해야 합니다. 등록해야 하는 폼 필드 정보는 각 폼 필드의 이름, 필수 항목 여부, 형식, 최소 길이, 최대 길이, 설명, 필드값 개수가 있습니다.

❷ 고급 폼 필드 검사 기능 설정

- 매개변수 보호 기능
  매개 변수 보호 기능을 사용할 경우에는 이 기능을 적용할 액션 URL과 소스 URL, 그리고 암호화 기능을 수행할 것인지 일치성 검사를 수행할 것인지를 설정해야 합니다. 암호화 기능을 수행하는 경우에는 암호화 시 사용할 키를 지정해야 합니다.

- 취약한 비밀번호 검사 기능
  취약한 비밀 번호 검사 기능을 사용할 경우에는 검사 규칙을 정의해야 하는데, 검사 규칙은 기능을 적용할 액션 URL과 비밀 번호 필드, 검사 방식, 리다이렉트 URL 항목으로 구성됩니다. 하나의 액션 URL에 대해 여러 개의 검사 규칙을 정의할 수 있습니다.

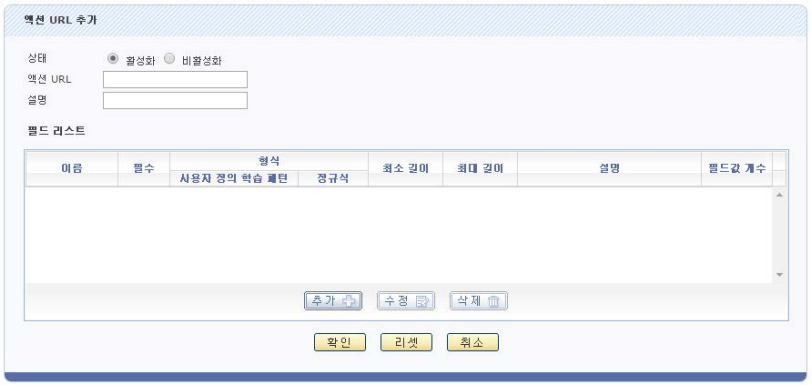
❸ 관련 기능의 활성화 상태 설정
폼 필드 검사 기능의 사용 여부와 이 기능에 대한 보안 로그, 차단, 증거, 학습, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다. 폼 필드 검사 기능이 활성화되어 있어도 차단 기능이 비활성화되어 있으면 설정된 폼 필드 검사 기능에 의해 변조된 폼 필드가 포함된 액션 URL을 발견하더라도 이 URL이 차단되지 않습니다.

**참고:** 매개 변수 보호 기능은 처리하는 정보가 많기 때문에 효율이 떨어지고 장비의 성능을 저하시킬 수 있습니다. 그러므로, 높은 보안 수준이 요구되는 경우에만 사용하는 것이 좋습니다.

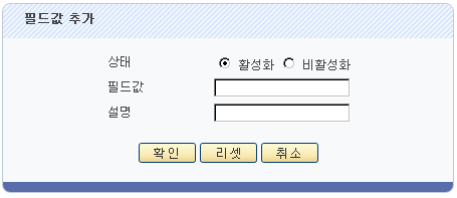
# 폼 필드 검사 설정하기

## 액션 URL 설정

액션 URL 검사 기능을 수행할 액션 URL과 액션 URL에 포함된 폼 필드의 정보를 등록하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **폼필드검사** 메뉴를 클릭합니다. |
| 2 | <**액션 URL 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**액션 URL 추가**> 팝업 창에서 다음 설명을 참고하여 등록할 액션 URL의 정보를 입력합니다.<br>  <br>• **상태** 현재 등록하고 있는 액션 URL을 적용할 것인지 지정합니다. (기본값: 활성화)<br>• **액션 URL** 검사하려는 액션 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** 액션 URL에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>• **필드 리스트** 액션 URL에 포함된 폼 필드의 정보를 추가합니다. 하나의 액션 URL에는 최대 512개 폼 필드의 정보를 추가할 수 있습니다. 폼 필드의 정보를 추가하는 방법은 4번 과정을 참고합니다. |
| 4 | 3번 과정에서 필드 리스트 부분에 있는 [**추가**] 버튼을 클릭하면 <**필드 추가**> 팝업 창이 나타납니다. 다음 설명을 참고하여 추가할 폼 필드에 대한 정보를 입력하고 [**확인**] 버튼을 클릭합니다. |

<table>
<tr><td></td><td>


<ul>
<li>• 상태 현재 등록하고 있는 폼 필드를 적용할 것인지 지정합니다. 적용하려는 경우에는 '활성화'를, 적용하지 않으려는 경우에는 '비활성화'를 선택합니다. (기본값: 활성화)</li>
<li>• 이름 폼 필드의 이름을 입력합니다. 알파벳과 숫자, 특수 문자로 이루어진 최대 256 글자의 문자열을 입력할 수 있습니다.</li>
<li>• 필수 클라이언트가 반드시 입력해야 하는 필드인지를 지정합니다. 반드시 입력해야 하는 필드이면 'Yes', 생략이 가능한 필드이면 'No'를 선택합니다. (기본값: No)</li>
<li>• 최소 길이 폼 필드에 입력 가능한 값의 최소값 혹은 문자열의 최소 길이를 지정합니다. (설정 범위: 0 ~ 2,147,418,112)</li>
<li>• 최대 길이 폼 필드에 입력 가능한 값의 최대값 혹은 문자열의 최대 길이를 지정합니다. (설정 범위: 0 ~ 2,147,418,112)</li>
<li>• 설명 폼 필드에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)</li>
<li>• <b>필드값 리스트</b> 폼 필드에 반드시 입력되어야 하는 값이 있는 경우에는 [<b>추가</b>] 버튼을 클릭한 후 이 값을 등록합니다. [<b>추가</b>] 버튼을 클릭하면 <<b>필드값 추가</b>> 팝업 창이 나타납니다. 아래의 설명을 참고하여 필드 값을 추가합니다. 필드 값은 최대 1024개까지 추가할 수 있습니다.</li>
</ul>


<ul>
<li>– 상태 현재 등록하고 있는 필드값을 실제로 적용할 것인지를 지정합니다. (기본값: 활성화)</li>
<li>– 필드값 필드 값을 입력합니다. 알파벳, 숫자와 특수 문자로 구성된 최대 1024 글자의 문자열을 입력할 수 있습니다.</li>
<li>– 설명 필드 값에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)</li>
</ul>
</td></tr>
<tr><td>5</td><td>폼 필드를 모두 추가하였으면 [확인] 버튼을 클릭합니다.</td></tr>
<tr><td>6</td><td>액션 URL을 모두 추가하였으면 [적용] 버튼을 클릭합니다.</td></tr>
</table>

## 고급 폼 필드 검사 설정

### 매개변수 보호 기능 설정

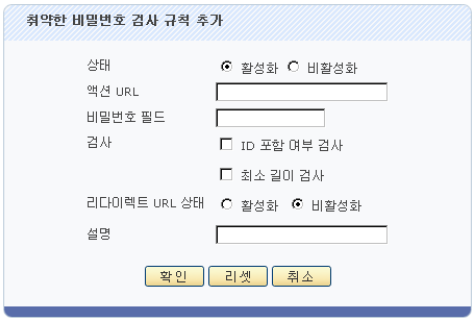
매개변수 보호 기능을 설정하는 방법은 다음과 같습니다. 매개 변수 보호 기능을 적용할 액션 URL은 256개까지 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **폼필드검사** 메뉴를 클릭합니다. |
| 2 | <**고급 폼필드 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**매개변수 보호**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**고급 액션 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL에 매개 변수 보호 기능을 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **액션 URL** 매개 변수 보호 기능을 수행할 액션 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **일치성 검사** 액션 URL에 일치성 검사를 수행할지 여부를 지정합니다. (기본값: 비활성화)<br>• **암호화** 웹 서버가 전송하는 매개 변수의 값을 암호화하는 암호화 기능의 수행 여부를 지정합니다. (기본값: 비활성화)<br>• **설명** 액션 URL에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>• **소스 URL 리스트** 등록 중인 액션 URL의 링크가 포함된 소스 URL을 등록합니다. 적어도 하나의 소스 URL을 등록해야 합니다. 소스 URL 리스트 부분에 있는 [**추가**] 버튼을 클릭하면, <**소스 URL 추가**> 팝업 창이 나타납니다. 팝업 창에서 소스 URL의 사용 상태, 소스 URL과 설명을 입력한 후 [**확인**] 버튼을 클릭합니다. 소스 URL은 256개까지 등록할 수 있습니다.<br>**참고:** 일치성 검사와 암호화는 동시에 수행될 수 없으므로 두 항목을 모두 '활성화' 시킬 수 없습니다. |
| 5 | 액션 URL을 모두 등록하였으면, 매개변수 보호 기능 상태 항목을 '활성화'로 지정하고, 4번 과정에서 암호화 항목을 활성화한 경우에는 암호화 키 항목에 암호화시 사용할 키를 입력합니다. 암호화 키는 영문자와 숫자로 구성된 5~16자의 문자열을 입력하면 됩니다. 항목의 값을 설정한 후 [**적용**] 버튼을 클릭합니다. |

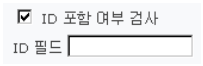
### 취약한 비밀번호 검사 기능 설정

취약한 비밀번호 검사 기능을 설정하는 방법은 다음과 같습니다. 취약한 비밀 번호 검사 규칙은 256개까지 추가할 수 있습니다.

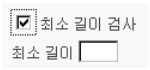
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **폼필드검사** 메뉴를 클릭합니다. |
| 2 | <**고급 폼필드 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**취약한 비밀번호 검사**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**취약한 비밀번호 검사 규칙 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [**확인**] 버튼을 클릭합니다. |




- **상태** 현재 설정 중인 취약한 비밀번호 검사 규칙을 적용할 것인지를 지정합니다. (기본값: 활성화)
- **액션 URL** 취약한 비밀번호 검사 기능을 수행할 액션 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.
- **비밀번호 필드** 액션 URL에 속한 필드 중에서 비밀번호가 입력되는 필드의 이름을 지정합니다.
- **검사** 클라이언트가 비밀번호 필드에 입력한 값에 대해 어떤 검사를 수행할 것인지 지정합니다. 아래 두 검사를 모두 수행할 수도 있습니다.
  - ID 포함 여부 검사 이 검사는 특정 필드의 내용이 비밀번호에 포함되어 있는지를 검사하고, 포함되어 있으면 비밀번호로 허용하지 않습니다. 이 항목을 선택했을 때 나타나는 ID 필드 항목에는 액션 URL에 속한 필드 중에서 포함 여부를 검사할 필드를 지정합니다.




  - 최소 길이 검사 이 검사는 비밀번호의 길이가 지정한 값보다 짧을 경우 비밀번호로 허용하지 않습니다. 이 항목을 선택했을 때 나타나는 최소 길이 항목에는 허용할 비밀번호의 최소 길이를 입력합니다.




- **리다이렉트 URL 상태** 리다이렉트 URL은 규칙에 설정된 검사 결과, 클라이언트가 입력한 비밀번호가 허용될 수 없는 경우 클라이언트에게 보여줄 URL입니다. 리다이렉트 URL을 사용하려면 '활성화'를 선택한 후 리다이렉트 URL 항목이 나타나면 클라이언트에게 보여줄 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.

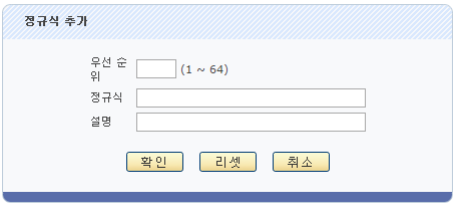
**참고:** 리다이렉트 URL을 설정하지 않으면 **애플리케이션 응답 설정**에 설정된 방법에 따라 액션 URL이 처리됩니다
(폼 필드 검사 기능의 차단 항목이 '활성화'로 설정되어 있는 경우).

- **설명** 등록 중인 규칙에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)

5 비밀 번호 검사 규칙을 모두 등록하였으면, 취약한 비밀번호 검사 기능 상태 항목을 활성화로 지정하고 [**적용**] 버튼을 클릭합니다.

## 사용자 정의 학습 패턴

사용자 정의 학습 패턴을 등록하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **폼필드검사** 메뉴를 클릭합니다. |
| 2 | <**사용자 정의 학습 패턴**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**정규식 추가**> 팝업 창에서 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **우선 순위** 사용자 정의 학습 패턴의 우선 순위를 입력합니다. 설정 범위는 1 ~ 64이고, 숫자가 작을수록 우선 순위는 높습니다.<br>• **정규식** 등록할 정규식을 입력합니다. 정규식을 정의하는 방법은 WEBFRONT-K 시스템 구성 설명서의 [**제4장 애플리케이션 - 정규식 설정**] 부분을 참고합니다.<br>• **설명** 정규식에 대한 설명을 입력합니다. 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 4 | 학습 패턴을 모두 추가하였으면 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

폼 필드 검사 기능의 사용 여부와 폼 필드 검사 기능과 관련된 보안 로그, 차단, 증거, 학습, 블랙리스트 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **폼필드검사** 메뉴를 클릭합니다. |
| 2 | <**폼 필드 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**폼 필드 검사 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 폼 필드 검사 기능을 활성화할 것인지 지정합니다. 이 항목을 활성화해야만 폼 필드 검사 기능이 동작합니다.<br>• **보안로그** 폼 필드 검사 정책을 위반한 요청 패킷에 대해 보안 로그를 기록할 것인지 지정합니다. 기록된 보안 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 폼 필드 검사 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다. 이 항목을 활성화하면, 폼 필드 검사 정책을 위반한 요청 패킷은 모두 차단됩니다. 이 항목을 비활성화하면, 폼 필드 검사 정책을 위반한 요청 패킷이라도 차단되지 않고 웹 서버로 전달됩니다. 일반적으로, WEBFRONT-K를 처음 설치하여 폼 필드 검사 기능을 설정하지 않았을 경우에는 이 항목을 비활성화로 설정하여, 모든 요청에 대하여 학습하는 동시에 서비스도 이루어지도록 합니다.<br>• **증거** 폼 필드 검사 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보를 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 폼 필드 검사 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 폼 필드 검사 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

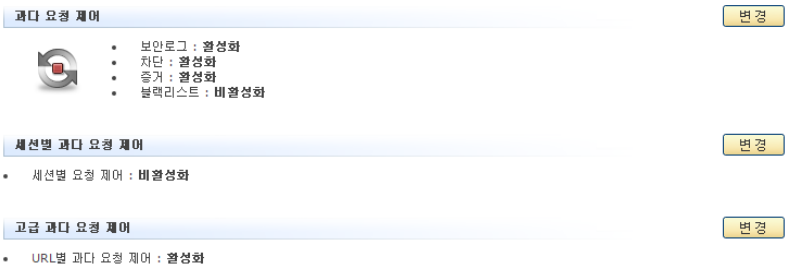
# 과다 요청 제어 기능 설정

과다 요청 제어 기능은 클라이언트에서 웹 서버로 보내는 요청 패킷 수가 지정한 시간(1분/1초) 동안 일정한 양을 초과하지 않도록 요청 패킷의 양을 적절하게 제한해주는 기능입니다. WEBFRONT-K의 과다 요청 제어 기능은 특정 세션을 통해 전송되는 세션 별 요청의 수를 제한하는 세션별 과다 요청 제어와 특정 URL에 대한 요청의 수를 제한하는 URL별 과다 요청 제어를 지원합니다. 이 절에서는 과다 요청 제어 기능을 설정하는 과정에 대해 살펴본 후, 과다 요청 제어 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**요청검사** - **과다요청제어** 메뉴를 클릭하면 과다 요청 제어 기능을 설정하는 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **과다 요청 제어** 과다 요청 제어 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 과다 요청 제어 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **세션별 과다 요청 제어** 세션 별 과다 요청 제한 기능의 설정 정보가 표시됩니다.
- **고급 과다 요청 제어** URL 별 과다 요청 제한 기능의 사용 여부가 표시됩니다.

### 설정 과정

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

❶ 세션 별 과다 요청 제한 설정

세션을 IP 주소 별로 구분할 수 있는 경우에 각 세션 별로 초당 요청 횟수를 제한하는 세션 별 과다 요청 제한 기능의 사용 여부와 최대 요청 횟수를 설정합니다. 세션 별 요청 제한 기능은 기본적으로 비활성화되어 있고, 기본 최대 요청 횟수는 30/초입니다.

❷ URL 별 과다 요청 제한 설정

특정 세션에 대하여 URL 별로 초당 요청 횟수를 제한하는 URL 별 요청 제한 기능의 활성화 상태, 요청 속도를 제한할 URL과 최대 요청 횟수를 설정합니다. 이 방식도 세션을 IP 주소 별로 구분할 수 있는 경우에 사용할 수 있습니다. URL 별 요청 제한 기능은 기본적으로 활성화되어 있습니다.

❸ 관련 기능의 활성화 상태 설정

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

# 과다 요청 제어 설정하기

## 세션 별 과다 요청 제한 설정

과다 요청 제어 기능 중에서 세션 별 과다 요청 제한 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **과다요청제어** 메뉴를 클릭합니다. |
| 2 | <**세션별 요청 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**세션별 과다 요청 제어 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **상태** 세션 별 요청 제한 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **시간 단위** 세션 별 최대 요청 횟수에 적용할 시간 단위를 지정합니다. (기본값: 초)<br>• **세션별 최대 요청 횟수** 세션 별로 서비스가 되도록 허용하는 최대 요청 수를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 30) |

## URL 별 과다 요청 제한 설정

과다 요청 제어 기능 중에서 URL 별 과다 요청 제한 기능을 설정하는 방법은 다음과 같습니다. 과다 요청 제어를 적용할 URL은 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **과다요청제어** 메뉴를 클릭합니다. |
| 2 | <**고급 과다 요청 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**URL별 과다 요청 제어**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL 에 대해 과다 요청 제어를 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **URL** URL 과다 요청 제어 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **시간 단위** 최대 요청 횟수에 적용할 시간 단위를 지정합니다. (기본값: 초)<br>• **최대 요청** 등록하고 있는 URL에 대한 초당 최대 요청 수를 지정합니다. (설정 범위: 1 ~ 65535)<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | URL별 과다 요청 제어 상태를 '활성화' 상태로 지정하고 [**적용**] 버튼을 클릭합니다. |

### 관련 기능의 활성화 상태 설정

과다 요청 제어 기능의 사용 여부와 과다 요청 제어 기능과 관련된 보안 로그, 차단, 증거, 블랙리스트 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **과다요청제어** 메뉴를 클릭합니다. |
| 2 | <**과다 요청 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**과다 요청 제어 상태 변경**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 과다 요청 제어 기능을 활성화할 것인지 지정합니다.<br>• **보안로그** 과다 요청 제어 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 과다 요청 제어 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다. 이 항목을 활성화하면, 과다 요청 제어 정책을 위반한 요청 패킷은 모두 차단됩니다.<br>• **증거** 과다 요청 제어 정책을 위반한 요청 패킷에 대한 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보를 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 과다 요청 제어 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 과다 요청 제어 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

# 쿠키 보호 기능 설정

쿠키 보호는 클라이언트가 웹 서버로 보내는 요청 패킷에 포함된 쿠키를 검사하여 쿠키의 변조 여부를 검사하는 기능입니다. WEBFRONT-K가 제공하는 쿠키 보호 기능은 쿠키 무결성 검사, 쿠키 형식 검사, 쿠키 하이재킹 차단 등의 방법을 통해 쿠키를 보호합니다. 이 절에서는 쿠키 보호 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 쿠키 보호 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **쿠키보호** 메뉴를 클릭하면, 쿠키 보호 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **쿠키 보호 상태** 쿠키 보호 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 쿠키 보호 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다. 다음 항목들은 쿠키가 변조되었거나 잘못된 형식이거나 하이재킹으로 판단될 경우 어떤 작업을 수행할지 여부를 표시합니다.
- **쿠키 무결성 검사** 쿠키 무결성 검사 기능의 현재 설정 정보가 표시됩니다.
- **예외 쿠키 리스트** 쿠키 보호 기능을 적용하지 않는 예외 쿠키 목록이 표시됩니다.
- **쿠키 보호 고급 설정** 쿠키 형식 검사 기능과 쿠키 하이재킹 검사 기능의 사용 여부가 표시됩니다.

### 설정 과정

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

❶ 쿠키 무결성 검사 설정
쿠키 무결성 검사 기능의 사용 여부와 쿠키가 변조되었다고 판단되는 경우의 대응 방법, 그리고 쿠키 암호화 기능의 사용 여부 및 쿠키 암호화 기능을 활성화한 경우 사용할 암호를 설정합니다. 기본적으로는 모두 비활성화되어 있고, 암호는 'admin'으로 설정되어 있습니다.

❷ 쿠키 무결성 검사 예외 쿠키 설정
쿠키 무결성 검사를 수행하지 않을 예외 쿠키를 지정합니다. 기본적으로 지정된 예외 쿠키는 없습니다.

❸ 쿠키 형식 검사 설정
클라이언트가 보낸 쿠키와 비교할 쿠키의 형식을 지정합니다. WEBFRONT-K는 쿠키 형식 검사를 수행할 요청 패킷을 받으면 요청

패킷의 쿠키 형식이 등록된 쿠키 형식 목록에 있는지를 검사하고 쿠키 형식 목록에 있으면 쿠키의 형식을 검사합니다. 기본적으로 등록된 쿠키 형식은 없습니다.

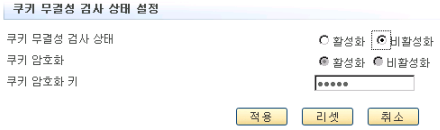
❹ 쿠키 하이재킹 차단 설정
쿠키 하이재킹 공격을 차단하는 기능의 사용 여부를 지정합니다. 쿠키 하이재킹은 공격자가 인증 과정을 거친 클라이언트의 쿠키를 훔쳐 이 클라이언트와 동일한 권한을 가지고 웹 애플리케이션에 접근하는 공격입니다. 기본적으로는 사용하지 않도록 비활성화되어 있습니다.

❺ 관련 기능의 활성화 상태 설정
쿠키 보호 기능의 사용 여부와 이 기능에 대한 보안 로그, 쿠키 삭제, 증거, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# 쿠키 무결성 검사 설정하기

## 쿠키 무결성 검사 기능 설정

쿠키 무결성 검사 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **쿠키보호** 메뉴를 클릭합니다. |
| 2 | <**쿠키 무결성 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**쿠키 무결성 검사 상태 설정**> 화면에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **쿠키 무결성 검사 상태** 쿠키 무결성 검사 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **쿠키 암호화** 쿠키를 암호화할 것인지 지정합니다. 암호화하려면 '활성화'를 암호화하지 않으려면 '비활성화'를 선택합니다. (기본값: 비활성화)<br>• **쿠키 암호화 키** 이 항목은 위 두 항목 중 하나를 '활성화'로 설정해야 입력 가능한 상태로 바뀝니다. 쿠키 암호화시 사용할 암호화 키를 입력합니다. 암호화 키는 최대 16글자의 알파벳과 숫자로 구성될 수 있습니다. (기본값: admin) |

## 쿠키 무결성 검사 예외 쿠키 설정

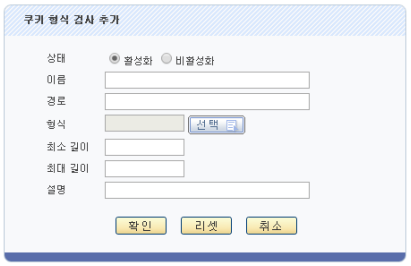
쿠키 무결성 검사를 활성화하면 수신되는 모든 쿠키에 대해 변조 여부를 검사합니다. 클라이언트의 스크립트에 의해 생성된 쿠키와 같이 쿠키 변조 검사를 수행하지 않을 예외 쿠키를 등록하는 방법은 다음과 같습니다. 예외 쿠키는 256개까지 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **쿠키보호** 메뉴를 클릭합니다. |
| 2 | <**예외 쿠키 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 3 | <**쿠키 보호 예외 쿠키 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 예외 쿠키를 실제로 적용할 것인지를 지정합니다. (기본값: 비활성화)<br>• **이름** 쿠키 검사를 수행하지 않을 쿠키의 이름을 입력합니다. 영문자와 숫자로 이루어진 최대 1256 글자의 문자열을 입력할 수 있습니다.<br>• **설명** 예외 쿠키에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 |

| | |
|---|---|
| | 설정) |
| 4 | 예외 쿠키를 모두 추가한 후에는 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

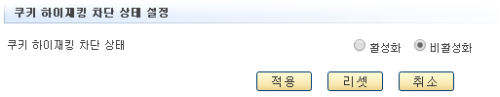
## 쿠키 형식 검사 기능 설정

쿠키 형식 검사 기능을 설정하는 방법은 다음과 같습니다. 쿠키 형식은 256개까지 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **쿠키보호** 메뉴를 클릭합니다. |
| 2 | <**쿠키 보호 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**쿠키 형식 검사 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**쿠키 형식 검사 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 쿠키 형식을 적용할 것인지를 지정합니다. 비활성화로 지정하면, 쿠키 형식이 등록되어 있더라도 쿠키 형식 검사 기능이 적용되지 않습니다. (기본값: 활성화)<br>• **이름** 현재 등록하고 있는 쿠키의 이름을 입력합니다. 쿠키의 이름은 알파벳과 숫자, '-', '_' 문자로 이루어진 최대 256 글자의 문자열을 사용할 수 있습니다.<br>• **경로** 쿠키의 경로를 입력합니다. 쿠키 경로는 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **형식** [**선택**] 버튼을 클릭합니다. 현재 등록된 정규식 목록에서 추가할 정규식을 선택한 후 [**확인**]을 클릭합니다. 추가할 정규식이 목록에 없는 경우에는 먼저 [**변경**] 버튼을 클릭한 후 원하는 정규식을 추가하도록 합니다. 정규식을 정의하는 방법은 이 설명서와 함께 제공되는 WEBFRONT-K 시스템 구성 설명서의 [**제4장 애플리케이션 - 정규식 설정**] 부분을 참고합니다. 쿠키의 형식이 선택한 정규식과 일치하지 않으면 변조된 쿠키로 간주합니다.<br>• **최소 길이** 쿠키의 최대 길이를 지정합니다. (설정 범위: 0 ~ 2,147,418,112)<br>• **최대 길이** 쿠키의 최소 길이를 지정합니다. (설정 범위: 0 ~ 2,147,418,112).<br>• **설명** 쿠키 형식에 대한 설명을 입력합니다. 영문자, 한글, 숫자, 특수 문자로 구성된 최대 128 글자의 문자열을 입력합니다. (선택 설정) |
| 5 | 예외 쿠키를 모두 추가한 후에는 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |
| 6 | 상태 항목에서 쿠키 형식 검사 기능의 사용 여부를 지정합니다. |
| 7 | 설정 내용을 시스템에 적용하기 위해 화면의 맨 아래에 있는 [**적용**] 버튼을 클릭합니다. |

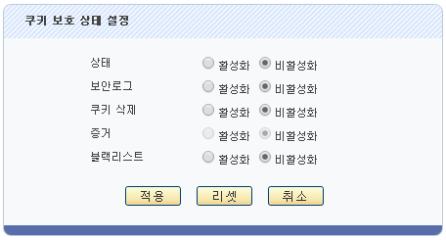
## 쿠키 하이재킹 차단 기능 설정

쿠키 하이재킹 차단 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **쿠키보호** 메뉴를 클릭합니다. |
| 2 | <**쿠키 보호 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**쿠키 하이재킹 차단 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <**쿠키 하이재킹 차단 상태 설정**> 화면에서 쿠키 하이재킹 검사 기능의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다.<br>  |

### 관련 기능의 활성화 상태 설정

쿠키 보호 기능의 사용 여부와 이 기능과 관련된 보안 로그, 쿠키 삭제, 증거, 블랙리스트 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **쿠키보호** 메뉴를 클릭합니다. |
| 2 | <**쿠키 보호 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**쿠키 보호 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 쿠키 보호 기능을 활성화할 것인지 지정합니다. 이 항목을 활성화해야만 쿠키 보호 기능이 동작할 수 있습니다.<br>• **보안 로그** 설정된 쿠키 보호 정책을 위반한 요청 패킷에 대한 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **쿠키 삭제** 설정된 쿠키 보호 정책을 위반한 요청 패킷에서 쿠키를 삭제할 것인지 지정합니다. 이 항목을 활성화하면 쿠키 보호 정책을 위반한 요청 패킷의 쿠키를 삭제한 후 웹 서버로 전송합니다.<br>• **증거** 설정된 쿠키 보호 정책을 위반한 요청 패킷에 대한 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보를 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안 로그**의 상태를 활성화한 경우에만 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 쿠키 보호 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 쿠키 보호 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

# 버퍼 오버플로우 차단 기능 설정

버퍼 오버플로우 차단은 클라이언트가 웹 서버로 보내는 요청 패킷의 HTTP 헤더, URL, 쿠키의 길이가 지정한 길이보다 큰지 검사하거나 HTTP 요청에 포함된 쉘 코드의 유형을 검사하는 기능입니다. 이 절에서는 버퍼 오버플로우 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 버퍼 오버플로우 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** – **버퍼오버플로우차단** 메뉴를 클릭하면 버퍼 오버플로우 차단 기능을 설정하는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **버퍼 오버플로우 차단 상태** 버퍼 오버플로우 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 버퍼 오버플로우 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **버퍼 오버플로우 고급 설정** HTTP, 쿠키, URL의 길이 제어 설정 정보와 MIME 예외, 쿼리스트링 차단 기능의 활성화 여부가 표시됩니다.
- **쉘 코드 검사 예외 URL 리스트** 쉘 코드 검사 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

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

❶ 버퍼 오버플로우 고급 설정

길이 제어를 위한 HTTP 헤더, 쿠키, URL의 최대 길이를 항목별로 설정하고, 쉘 코드 검사의 MIME 예외와 쿼리스트링 차단 옵션 사용 여부를 선택합니다. WEBFRONT-K는 요청 패킷을 받으면 요청 패킷의 HTTP 헤더의 길이, 쿠키의 길이, URL의 길이를 설정한 각 항목의 최대 길이와 비교하여 단 한 항목이라도 최대 길이를 초과하는 경우에는 버퍼 오버플로우 공격 패킷으로 간주합니다. 기본적으로 MIME 예외 옵션은 활성화되어 있고, 쿼리스트링 차단은 비활성화되어 있습니다.

❷ 쉘 코드 검사 설정

쉘 코드 삽입 공격을 검사하기 위한 쉘 코드 시그니처를 설정합니다. WEBFRONT-K는 많이 사용되는 쉘 코드 시그니처 목록을 제공합니다. WEBFRONT-K는 HTTP 요청 패킷의 매개 변수를 검사하여 쉘 코드가 포함된 경우에는 이 요청 패킷을 버퍼 오버플로우 공격 패킷으로 간주합니다. 쉘 코드 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❸ 쉘 코드 검사 예외 URL 설정

쉘 코드 검사 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

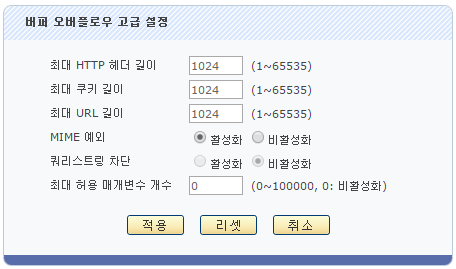
❹ 관련 기능의 활성화 상태 설정

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

# 버퍼 오버플로우 차단 설정하기

## 버퍼 오버플로우 고급 설정

버퍼 오버플로우 차단 기능 중에서 길이 제어 기능과 MIME 예외, 쿼리스트링 차단 옵션을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **버퍼오버플로우차단** 메뉴를 클릭합니다. |
| 2 | <**버퍼 오버플로우 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**버퍼 오버플로우 고급 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **최대 HTTP 헤더 길이** 버퍼 오버플로우 공격을 확인하기 위한 기준이 되는 HTTP 헤더의 길이를 입력합니다. HTTP 헤더가 지정한 길이를 초과하면, 버퍼 오버플로우 공격 패킷으로 간주합니다. (설정 범위: 1 ~ 65535, 기본값: 1024)<br>• **최대 쿠키 길이** 버퍼 오버플로우 공격을 확인하기 위한 기준이 되는 쿠키의 길이를 입력합니다. 쿠키의 길이가 지정한 길이를 초과하면, 버퍼 오버플로우 공격 패킷으로 간주합니다. (설정 범위: 1 ~ 65535, 기본값: 1024)<br>• **최대 URL 길이** 버퍼 오버플로우 공격을 확인하기 위한 기준이 되는 URL의 길이를 입력합니다. URL의 길이가 지정한 길이를 초과하면, 버퍼 오버플로우 공격 패킷으로 간주합니다. (설정 범위: 1 ~ 65535, 기본값: 1024)<br>• **MIME 예외** 쉘 코드 검사의 MIME 예외 옵션 활성화 여부를 설정합니다. MIME 예외 기능을 활성화하면 Content-Type 헤더가 multipart/form-data인 MIME 형식의 요청 패킷은 쉘 코드 검사를 수행하지 않습니다. (기본값: 활성화)<br>• **쿼리스트링 차단** 쉘 코드 검사의 쿼리스트링 차단 옵션 활성화 여부를 설정합니다. 기능을 활성화하면 Value 내용과 파라미터를 모두 탐지하며, 비활성화하면 Value 내용만 탐지합니다. (기본값: 비활성화)<br>• **최대 허용 매개변수 개수** 허용할 매개변수의 개수를 입력합니다. 매개변수가 지정한 개수를 초과하면, 이를 탐지합니다. (설정 범위: 0~ 100,000, 기본값: 0) |



**참고:** 쿼리스트링 차단 옵션은 **Application** – **애플리케이션** – **기타설정** 메뉴에서 쿼리스트링 검사 기능의 상태가 활성화인 경우에만 설정할 수 있습니다. 쿼리스트링 검사 기능을 비활성화하면 쿼리스트링 차단 옵션이 자동으로 비활성화됩니다.

**참고:** 쿼리스트링 차단 옵션 설정은 쿼리스트링 검사 기능 설정과의 관계로 인해 설정 복사가 되지 않습니다.

## 쉘 코드 검사 설정

쉘 코드 검사 기능에 사용되는 쉘 코드 유형은 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 쉘 코드 유형을 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정, 사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

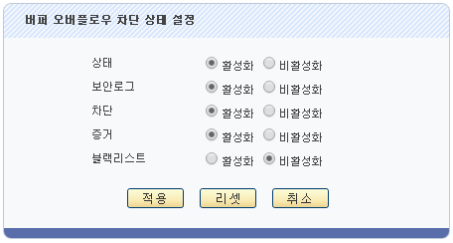
## 쉘 코드 검사 예외 URL 설정

쉘 코드 검사 기능에서 제외할 예외 URL이 있는 경우에는 다음과 같은 방법으로 URL을 등록합니다. 쉘 코드 검사 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **버퍼오버플로우차단** 메뉴를 클릭합니다. |
| 2 | <**쉘코드 검사 예외 URL 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 3 | <**쉘코드 검사 예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 쉘 코드 검사 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 됩니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | **상태** 항목에서 등록한 예외 URL의 활성화 여부를 지정합니다. (기본값: 비활성화) |
| 5 | 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 상태 설정

버퍼 오버플로우 차단 기능의 사용 여부와 버퍼 오버플로우 차단 기능과 관련된 보안 로그, 차단, 증거, 블랙리스트 기능의 상태를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **버퍼오버플로우차단** 메뉴를 클릭합니다. |
| 2 | <**버퍼 오버플로우 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**버퍼 오버플로우 차단 상태 설정**> 팝업 창에서 각 항목의 상태를 설정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 버퍼 오버플로우 차단 기능의 활성화 여부를 지정합니다.<br>• **보안로그** 버퍼 오버플로우 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 버퍼 오버플로우 차단 기능의 길이 제어 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다. 이 항목을 활성화하면 길이 제어 정책을 위반한 요청 패킷은 모두 차단됩니다.<br>• **증거** 버퍼 오버플로우 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안로그는 요청에 대한 주요 정보를 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 버퍼 오버플로우 차단 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 버퍼 오버플로우 차단 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 '**WEBFRONT-K 소개서**'의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

**참고:** 쉘 코드 검사 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**] 부분을 참고합니다.

# SQL 삽입 차단 기능 설정

SQL 삽입 차단은 클라이언트가 웹 서버로 보내는 폼 필드 문자열에 지정한 SQL 삽입 공격 시그니처가 포함되었는지를 검사하는 기능입니다. SQL 삽입 공격 시그니처가 포함된 클라이언트 요청은 지정한 방식에 따라 처리됩니다. 이 절에서는 SQL 삽입 차단 기능의 설정 화면과 설정 과정에 대해 살펴본 후 실제로 SQL 삽입 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **SQL삽입차단** 메뉴를 클릭하면 SQL 삽입 차단 기능을 설정할 수 있는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **SQL 삽입 차단 상태** — SQL 삽입 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. SQL 삽입 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **SQL 삽입 차단 고급 설정** — MIME 예외, 쿼리스트링 차단, 논리연산 공격 차단 활성화 여부가 표시됩니다.
- **SQL 삽입 차단 예외 URL 리스트** — SQL 삽입 차단 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

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

❶ SQL 삽입 차단 시그니처 설정

SQL 삽입 공격을 검사하기 위한 SQL 삽입 차단 시그니처와 논리 연산 차단 시그니처를 지정합니다. WEBFRONT-K는 많이 사용되는 SQL 삽입 공격 시그니처 목록을 제공합니다. WEBFRONT-K는 요청 패킷의 SQL 문자열에 지정한 시그니처가 포함되었는지를 검사하여, 지정한 시그니처가 폼 필드에 포함된 경우에는 SQL 삽입 공격으로 판단합니다. SQL 삽입 차단 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❷ SQL 삽입 차단 고급 설정

MIME 예외, 쿼리스트링 차단 옵션 활성화 여부와 논리 연산 공격 차단 URL을 지정합니다. 기본적으로 MIME 예외 옵션은 활성화되어 있고, 쿼리스트링 차단 옵션은 비활성화되어 있습니다. 또한, 논리 연산 공격 차단 기능은 비활성화되어 있고, 지정된 논리 연산 공격 차단 URL은 없습니다.

❸ SQL 삽입 차단 검사 예외 URL 설정

SQL 삽입 차단 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

❹ 관련 기능의 활성화 상태 설정

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

# SQL 삽입 차단 설정하기

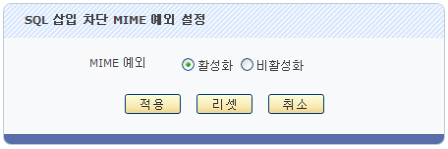
## SQL 삽입 차단 기능 설정

SQL 삽입 차단 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 시그니처를 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정, 사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

## SQL 삽입 차단 고급 설정

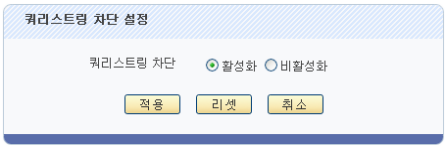
### MIME 예외 설정

MIME 예외 옵션의 상태를 설정하는 방법은 다음과 같습니다. MIME 예외 옵션을 활성화하면 Content-Type 헤더가 multipart/form-data인 MIME 형식의 요청 패킷은 SQL 삽입 차단 검사를 수행하지 않습니다. MIME 예외 옵션은 기본적으로 활성화되어 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **SQL삽입차단** 메뉴를 클릭합니다. |
| 2 | <**SQL 삽입 차단 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**SQL 삽입 차단 MIME 예외 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <**SQL 삽입 차단 MIME 예외 설정**> 팝업 창에서 활성화 여부를 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  |

### 쿼리스트링 차단 설정

쿼리스트링 차단 옵션의 상태를 설정하는 방법은 다음과 같습니다. 쿼리스트링 차단 옵션을 활성화하면 SQL 삽입 차단 기능의 차단 설정은 각 시그니처의 액션 설정과 관계 없이 모두 차단으로 동작합니다. 쿼리스트링 차단 옵션은 기본적으로 비활성화되어 있습니다.

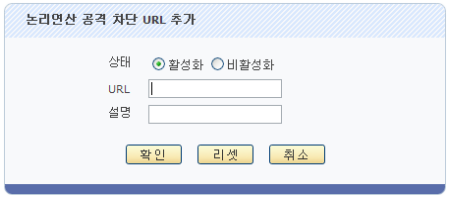
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **SQL삽입차단** 메뉴를 클릭합니다. |
| 2 | <**SQL 삽입 차단 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**쿼리스트링 차단 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <**쿼리스트링 차단 설정**> 팝업 창에서 활성화 여부를 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  |

**참고:** 쿼리스트링 차단 옵션은 **Application** – **애플리케이션** – **기타설정** 메뉴에서 쿼리스트링 검사 기능의 상태가 활성화인 경우에만 설정할 수 있습니다. 쿼리스트링 검사 기능을 비활성화하면 쿼리스트링 차단 옵션이 자동으로 비활성화됩니다.

**참고:** 쿼리스트링 차단 옵션 설정은 쿼리스트링 검사 기능 설정과의 관계로 인해 설정 복사가 되지 않습니다.

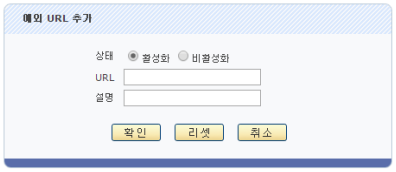
### 논리 연산 공격 차단 URL 리스트 설정

논리 연산 공격 차단 URL 리스트를 설정하는 방법은 다음과 같습니다. 기본적으로 설정된 URL 리스트는 없습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **SQL삽입차단** 메뉴를 클릭합니다. |
| 2 | <**SQL 삽입 차단 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**논리연산 공격 차단 URL 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**논리연산 공격 차단 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가할 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 논리연산 공격 차단 기능을 수행할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 상태 항목에서 등록한 URL의 활성화 여부를 지정합니다. (기본값: 비활성화) |
| 6 | URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

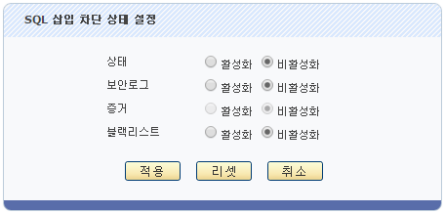
### SQL 삽입 차단 예외 URL 설정

SQL 삽입 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **SQL삽입차단** 메뉴를 클릭합니다. |
| 2 | <**SQL 삽입 차단 예외 URL 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가할 예외 URL의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **URL** SQL 삽입 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 상태 항목에서 등록한 예외 URL의 활성화 여부를 지정합니다. (기본값: 비활성화) |
| 5 | 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 상태 설정

SQL 삽입 차단 기능의 사용 여부와 SQL 삽입 차단 기능과 관련된 보안 로그, 증거, 블랙리스트 기능의 상태를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **SQL삽입차단** 메뉴를 클릭합니다. |
| 2 | <**SQL 삽입 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**SQL 삽입 차단 상태 설정**> 팝업 창에서 각 항목의 상태를 설정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화 되어 있습니다.<br>  <br>• **상태** SQL 삽입 차단 기능의 활성화 여부를 지정합니다.<br>• **보안 로그** SQL 삽입 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** SQL 삽입 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** SQL 삽입 차단 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 SQL 삽입 차단 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |



**참고:** SQL 삽입 차단 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**] 부분을 참고합니다.

# 스크립트 삽입 차단 기능 설정

스크립트 삽입 차단은 클라이언트가 웹 서버로 보내는 폼 필드의 문자열에 크로스 사이트 스크립팅(Cross Site Scripting, XSS) 공격과 관련된 코드가 포함되어있는지를 검사하는 기능입니다. 이 절에서는 스크립트 삽입 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 스크립트 삽입 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **스크립트차단** 메뉴를 클릭하면 스크립트 삽입 차단 기능을 설정할 수 있는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **스크립트 삽입 차단 상태** — 스크립트 삽입 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 스크립트 삽입 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **스크립트 삽입 차단 고급 설정** — 쿼리스트링 차단과 스트럿츠2 취약점 공격 검사의 활성화 여부가 표시됩니다.
- **스크립트 삽입 차단 예외 URL 리스트** — 스크립트 삽입 차단 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

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

❶ 스크립트 삽입 차단 시그니처 설정
스크립트 삽입 공격을 검사하기 위한 스크립트 시그니처를 지정합니다. WEBFRONT-K는 많이 사용되는 스크립트 삽입 시그니처 목록을 제공합니다. WEBFRONT-K는 요청 패킷의 스크립트 문자열에 지정한 시그니처가 포함되었는지를 검사하여, 지정한 시그니처가 스크립트 문자열에 포함된 경우에는 스크립트 삽입 공격으로 판단합니다. 스크립트 삽입 차단 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❷ 스크립트 삽입 차단 고급 설정
쿼리스트링 차단과 스트럿츠2 취약점 공격 검사의 활성화 여부를 지정합니다. 기본적으로 두 옵션 모두 비활성화되어 있습니다.

❸ 스크립트 삽입 차단 검사 예외 URL 설정
스크립트 삽입 차단 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

❹ 관련 기능의 활성화 상태 설정
스크립트 삽입 차단 기능의 사용 여부와 이 기능에 대한 보안 로그, 증거 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

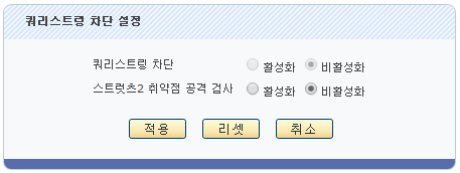
# 스크립트 삽입 차단 설정하기

## 스크립트 삽입 차단 기능 설정

스크립트 삽입 차단 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 시그니처를 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정, 사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

## 스크립트 삽입 차단 고급 설정

스크립트 삽입 차단 기능의 쿼리스트링 차단과 스트럿츠2 취약점 공격 검사 옵션을 설정하는 방법은 다음과 같습니다. 쿼리스트링 차단과 스트럿츠2 취약점 공격 검사 옵션은 기본적으로 비활성화되어 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **스크립트삽입차단** 메뉴를 클릭합니다. |
| 2 | <**스크립트 삽입 차단 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**쿼리스트링 차단 설정**> 팝업 창에서 활성화 여부를 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **쿼리스트링 차단** 쿼리스트링 차단 기능의 활성화 여부를 지정합니다. 기능을 활성화하면 Value 내용과 파라미터를 모두 탐지하며, 비활성화하면 Value 내용만 탐지합니다.<br>• **스트럿츠2 취약점 공격 검사** 스트럿츠2 취약점 공격 검사 기능의 활성화 여부를 지정합니다. 해당 기능을 활성화하면 원격 코드 실행 취약점을 이용한 공격을 탐지할 수 있습니다. |

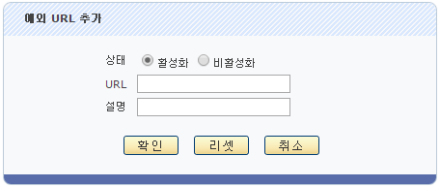


**참고:** 쿼리스트링 차단 옵션은 **Application** – **애플리케이션** – **기타설정** 메뉴에서 쿼리스트링 검사 기능의 상태가 활성화인 경우에만 설정할 수 있습니다. 쿼리스트링 검사 기능을 비활성화하면 쿼리스트링 차단 옵션이 자동으로 비활성화됩니다.

**참고:** 쿼리스트링 차단 옵션 설정은 쿼리스트링 검사 기능 설정과의 관계로 인해 설정 복사가 되지 않습니다.

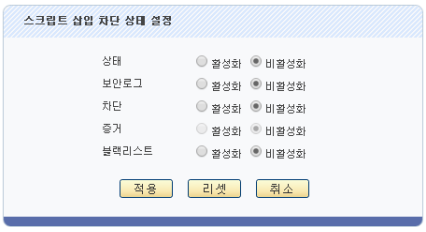
## 스크립트 삽입 차단 예외 URL 설정

스크립트 삽입 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **스크립트차단** 메뉴를 클릭합니다. |
| 2 | <**스크립트 삽입 차단 예외 URL 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가할 예외 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 스크립트 삽입 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 상태 항목에서 등록한 예외 URL의 활성화 여부를 지정합니다. (기본값: 비활성화) |
| 5 | 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

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

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **스크립트삽입차단** 메뉴를 클릭합니다. |
| 2 | <**스크립트 삽입 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**스크립트 삽입 차단 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 스크립트 삽입 차단 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 스크립트 삽입 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 스크립트 삽입 차단 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다.<br>• **증거** 스크립트 삽입 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 스크립트 삽입 차단 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 스크립트 삽입 차단 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 보안 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |



**참고:** 스크립트 삽입 차단 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션** - **시그니처 관리** - **시그니처 액션 설정**] 부분을 참고합니다.

# 업로드 검사 기능 설정

업로드 검사 기능은 클라이언트가 웹 서버로 업로드하려는 파일을 검사하여 공격 가능성이 있는 파일을 업로드하지 못하도록 제한하는 기능입니다. 이 절에서는 업로드 검사 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 업로드 검사 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** – **업로드검사** 메뉴를 클릭하면 업로드 검사 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **업로드 검사** — 업로드 검사 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 업로드검사 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **업로드 검사 URL 리스트** — 업로드를 제한하려는 URL의 목록이 표시됩니다.
- **업로드 검사 예외 URL 리스트** — 업로드 검사 기능에서 제외할 URL의 목록이 표시됩니다.
- **업로드 검사 예외 파일 확장자 리스트** — 업로드 검사의 파일 확장자 검사 기능에서 제외할 파일 확장자 목록이 표시됩니다.
- **개인 정보 보호 검사 대상 파일 정보** — 업로드 검사의 개인 정보 보호 기능에서 지원하는 파일 리스트와 검사 리스트를 확인할 수 있습니다.

### 설정 과정

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

❶ 업로드 검사 시그니처 설정

업로드를 제한할 파일 확장자 시그니처와 파일 내용 시그니처를 설정합니다. WEBFRONT-K는 일반적으로 사용되는 파일 확장자 시그니처 목록과 파일 업로드 공격에 많이 사용되는 파일 내용 시그니처 목록을 제공합니다. 설정된 시그니처는 업로드 검사 URL 리스트에서 **파일 확장자 차단**과 **파일 내용 검사**에 적용됩니다. 업로드 파일 확장자와 파일 내용 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❷ 업로드 검사 URL 등록

파일 업로드를 제한할 URL과 제한 방식을 지정합니다. 제한 방식에는 파일 확장자 차단과 파일 내용 검사, 파일 크기 제한이 있습니다. 기본적으로 설정된 URL은 없습니다.

❸ 업로드 검사 예외 URL 등록

업로드 검사 기능에서 제외할 URL을 지정합니다. 업로드 검사 기능은 업로드 URL 리스트에 설정된 URL에만 적용됩니다. 업로드 URL의 하위 URL 중 업로드 검사에서 제외할 URL을 설정하도록 합니다. 기본적으로 설정된 URL은 없습니다.

❹ 업로드 검사 예외 파일 확장자 등록

업로드 검사의 파일 확장자 차단 기능에서 제외할 파일 확장자를 지정합니다. 기본적으로 설정된 파일 확장자는 없습니다.

❺ 개인 정보 보호 검사 대상 파일 정보 설정

업로드 검사의 개인 정보 보호 검사 대상 파일 확장자를 지정합니다. 기본적으로 설정된 파일 확장자는 doc, docx, xls, xlsx, ppt, pptx, pdf, hwp 입니다.

❻ 관련 기능의 활성화 상태 설정

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

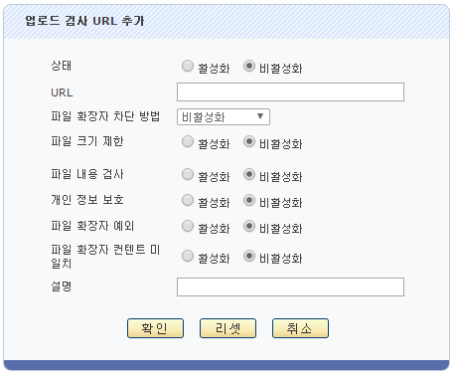
# 업로드 검사 기능 설정하기

## 업로드 파일 이름 시그니처 설정

업로드를 제한하려는 파일 이름 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 업로드 파일 이름 시그니처를 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션** - **시그니처 관리** - **시그니처 액션 설정, 사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

## 업로드 검사 URL 등록

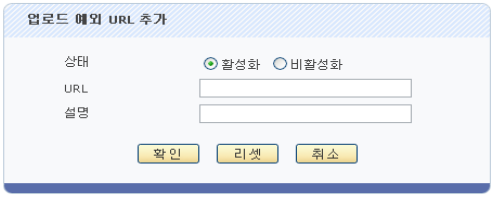
업로드 검사 기능을 적용하여 파일 업로드를 제한할 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 URL을 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **업로드검사** 메뉴를 클릭합니다. |
| 2 | <**업로드 검사 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**업로드 검사 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**업로드 검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL에 대해 업로드 검사 기능을 적용할지를 지정합니다. (기본값: 비활성화)<br>• **URL** 업로드 검사 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **파일 확장자 차단 방법** 드롭다운 목록에서 파일 확장자 차단 방법을 지정합니다. (기본값: 비활성화)<br>– 비활성화: 파일 확장자를 검사하지 않습니다.<br>– 모두 차단: 모든 파일의 업로드를 차단합니다.<br>– 시그니처 차단: **업로드 검사** - **파일 확장자** 시그니처 설정에 따라 업로드를 제한합니다.<br>– 모두 탐지: 모든 파일의 업로드를 허용하고, 보안 로그를 생성합니다.<br>• **파일 크기 제한** 업로드하는 파일의 크기 제한 여부를 지정합니다. '활성화'를 선택한 경우에는 이 항목의 아래에 파일 크기 항목이 추가로 나타납니다. (기본값: 비활성화)<br>  |

| | |
|---|---|
| | 파일 크기 항목에는 업로드할 수 있는 파일의 크기를 입력합니다. 오른쪽의 드롭다운 목록을 클릭하면 파일 크기의 단위를 B(Byte), KB(Kilo Byte), MB(Mega Byte) 중에서 선택할 수 있습니다.<br>(설정 범위: 1 ~ 1024, 기본 단위: B)<br>• **파일 내용 검사** 업로드 파일의 내용 검사 여부를 지정합니다. 이 항목을 활성화하면 **업로드 검사 - 파일내용** 시그니처 설정에 따라 업로드를 제한합니다. (기본값: 비활성화)<br>• **개인 정보 보호** 업로드 파일의 개인 정보 보호 여부를 지정합니다. 개인 정보 보호는 업로드 파일의 내용에 주민등록번호 또는 신용카드번호가 포함되어 있을 경우, 이를 탐지 및 차단합니다. (기본값: 비활성화)<br>  **참고:** 개인 정보 보호 기능을 사용하려면 아래 3가지 항목을 설정해야 합니다.<br>1. 고급첨부파일 검사가 활성화되어 있어야 합니다.<br>- 설정 경로: **System > 애플리케이션 > 고급첨부파일검사 설정 활성화**<br>2. 개인 정보 보호 검사 대상 파일을 설정합니다.<br>- 설정 경로: **Application > 요청검사 > 업로드 검사 > 개인 정보 보호 검사 대상 파일 정보**<br>3. URL 별 개인 정보 보호 기능을 활성화합니다.<br>- 설정 경로: **Application > 요청검사 > 업로드 검사 > 업로드 검사 URL 리스트 설정 > 업로드 검사 URL 추가/수정**<br>  **주의:** 개인 정보 보호 기능 설정 시, 아래 3가지 사항을 유의합니다.<br>1. 업로드 하는 파일 이름에 확장자가 있어야 합니다.<br>2. 대용량 파일의 경우 미탐이 발생할 수 있습니다.<br>3. 검사 URL을 /* 로 설정할 경우 서비스 지연이 발생할 수 있습니다.<br>• **파일 확장자 예외** 파일 확장자 차단 방법을 모두 차단, 시그니처 차단, 모두 탐지로 설정한 경우 업로드 검사 예외 파일 확장자 리스트에 설정한 확장자를 업로드 검사 기능에서 제외할 지 여부를 지정합니다.<br>(기본값: 비활성화)<br>• **파일 확장자 컨텐트 미일치** 업로드 파일의 확장자와 컨텐트의 일치 검사 여부를 지정합니다. 파일 확장자 컨텐트 미일치는 악성 코드 검사를 회피하거나 컨텐트를 위장하기 위해 실제 파일 내용과 다른 확장자 파일을 업로드 하는 경우를 탐지 및 차단합니다. (기본값: 비활성화)<br>  **참고:** HTTP 컨텐트 미일치 검사 기능이 지원하는 파일 포맷은 다음과 같습니다.<br>• 이미지 파일 (JPG, JPEG, TIF, PNG, GIF, BMP, DIB)<br>• Microsoft 워드 (DOC, DOCX)<br>• Microsoft 파워포인트 (PPT, PPTX)<br>• Microsoft 엑셀 (XLS, XLSX)<br>• 한글과 컴퓨터 아래아 한글 (HWP)<br>• Adobe Acrobat (PDF)<br>• Rich Text Format (RTF)<br>• 압축파일 (TGZ, GZ, TAR, XZ, ZIP, JAR)<br>• 소스코드 파일 (C, CPP, XML, CGI, PL, PY, RB)<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 업로드 검사를 수행할 URL을 모두 설정한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 업로드 검사 예외 URL 등록

업로드 검사 기능에서 제외할 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 URL을 등록할 수 있습니다.

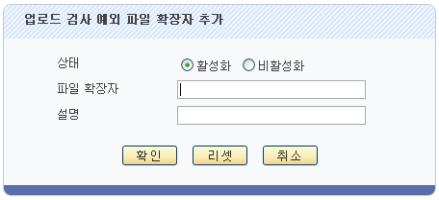
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **업로드검사** 메뉴를 클릭합니다. |
| 2 | <**업로드 검사 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**업로드 검사 예외 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**업로드 예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL을 업로드 검사 기능에서 제외할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 업로드 검사 기능에서 제외할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 업로드 검사에서 제외할 URL을 모두 설정한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |



**참고:** 업로드 URL과 업로드 예외 URL은 중복하여 설정할 수 없습니다. 업로드 예외 URL은 업로드 URL의 하위 URL 중 업로드 검사에서 제외할 URL로 설정하도록 합니다.

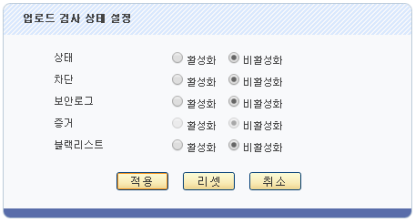
## 업로드 검사 예외 파일 확장자 등록

업로드 검사 기능에서 제외할 파일 확장자를 설정하는 방법은 다음과 같습니다. 최대 256개의 파일 확장자를 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **업로드검사** 메뉴를 클릭합니다. |
| 2 | <**업로드 검사 예외 파일 확장자 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**업로드 검사 예외 파일 확장자 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 파일 확장자를 업로드 검사 기능에서 제외할지 여부를 지정합니다. (기본값: 활성화)<br>• **파일 확장자** 업로드 검사 기능에서 제외할 파일 확장자를 입력합니다. 파일 확장자는 최대 9 글자의 영문자와 숫자, 그리고 '*', '?', ',', ';', '<', '>', '\|'를 제외한 특수 문자로 구성될 수 있습니다. 첫 문자는 반드시 '.'이어야 합니다.<br>• **설명** 파일 확장자에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 업로드 검사에서 제외할 파일 확장자를 모두 설정한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 상태 설정

업로드 검사 기능의 사용 여부와 업로드 검사 기능과 관련된 보안 로그, 증거, 블랙리스트 기능의 상태를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **업로드검사** 메뉴를 클릭합니다. |
| 2 | <**업로드 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**업로드 검사 상태 설정**> 팝업 창에서 각 항목의 상태를 설정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 업로드 검사 기능의 활성화 여부를 지정합니다.<br>• **차단** 업로드 검사 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다. 이 항목을 활성화하면 업로드 검사 정책을 위반한 요청 패킷은 모두 차단됩니다.<br>• **보안로그** 업로드 검사 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** 업로드 검사 정책을 위반한 클라이언트의 요청 패킷에 대한 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 업로드 검사 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 업로드 검사 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |



**참고:** 업로드 검사 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션** - **시그니처 관리** - **시그니처 액션 설정**] 부분을 참고합니다.

# 다운로드 검사 기능 설정

다운로드 검사 기능은 클라이언트가 특정한 이름의 파일이나 특정 확장자를 가진 파일을 웹 서버에서 다운로드하지 못하도록 차단하는 기능입니다. WEBFRONT-K에 다운로드를 차단할 파일에 대한 시그니처를 등록해두면 클라이언트가 해당 파일을 다운로드하기 위한 요청을 보내더라도 WEBFRONT-K는 이 요청을 웹 서버로 전달하지 않습니다. 이 절에서는 이러한 WEBFRONT-K의 다운로드 검사 기능을 설정하는 데 필요한 내용으로 구성되어 있습니다. 먼저, 설정 화면의 구성을 살펴본 후 파일 다운로드 검사 기능을 설정하는 과정과 설정 방법에 대해 살펴봅니다.

## 설정 개요

### 설정 화면

다운로드 검사 기능을 설정하려면 **Application** 메뉴에서 **요청검사** – **다운로드검사** 메뉴를 클릭합니다. 그러면, 다운로드 검사 기능의 현재 설정 정보를 보여주는 설정 화면이 나타납니다.


화면의 각 부분에 출력된 정보는 다음과 같습니다.

- **다운로드 검사** 다운로드 검사 기능의 활성화 상태와 관련 기능(보안 로그, 차단, 증거)의 활성화 상태가 표시됩니다. 다운로드 검사 기능의 활성화 상태는 아이콘으로 표시되는데, 은 활성화 상태를, 는 비활성화 상태를 나타냅니다.
- **다운로드 검사 URL 리스트** 다운로드 검사 기능을 적용할 URL의 목록이 표시됩니다.
- **다운로드 검사 예외 URL 리스트** 다운로드 검사 기능에서 제외할 URL의 목록이 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 다음은 파일 다운로드 검사 기능을 설정하는 과정입니다.

❶ 다운로드 파일 이름 시그니처 설정

다운로드를 차단하려는 파일의 이름이나 확장자의 시그니처를 설정합니다. WEBFRONT-K는 일반적으로 많이 사용되는 파일 확장자의 시그니처를 제공합니다. 다운로드 파일 이름 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❷ 다운로드 검사 URL 등록

<**다운로드 URL 리스트**>에서 등록한 시그니처를 사용하여 파일 다운로드를 제한할 URL을 지정합니다. 기본적으로 설정된 URL은 없습니다.

❸ 다운로드 검사 예외 URL 등록
다운로드 검사 기능에서 제외할 URL을 지정합니다. 다운로드 검사 기능은 다운로드 URL 리스트에 설정된 URL에만 적용됩니다. 다운로드 URL의 하위 URL 중 다운로드 검사에서 제외할 URL을 설정하도록 합니다. 기본적으로 설정된 URL은 없습니다.

❹ 관련 기능의 활성화 상태 설정
다운로드 검사 기능의 사용 여부와 이 기능에 대한 보안 로그, 증거, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

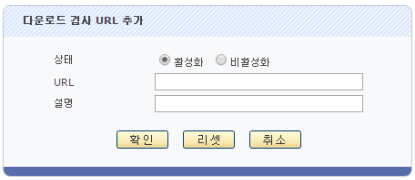
# 다운로드 검사 기능 설정하기

## 다운로드 파일 이름 시그니처 등록

다운로드를 제한하려는 파일 이름 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 다운로드 파일 이름 시그니처를 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션** - **시그니처 관리** - **시그니처 액션 설정, 사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

## 다운로드 검사 URL 등록

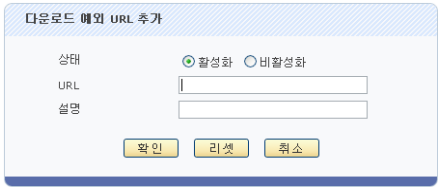
파일 다운로드 검사 기능을 적용할 URL을 설정하는 방법은 다음과 같습니다. WEBFRONT-K에는 다운로드 검사를 수행할 URL을 최대 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **다운로드검사** 메뉴를 클릭합니다. |
| 2 | <**다운로드 검사 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**다운로드 검사 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**다운로드 검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL에 대해 다운로드 검사 기능을 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** 다운로드 검사 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있고, 반드시 '/'로 시작해야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 5 | URL을 모두 추가한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |



## 다운로드 검사 예외 URL 등록

다운로드 검사 기능에서 제외할 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 URL을 등록할 수 있습니다.

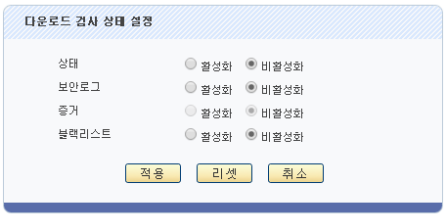
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **다운로드검사** 메뉴를 클릭합니다. |
| 2 | <**다운로드 검사 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**다운로드 검사 예외 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**다운로드 검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL을 다운로드 검사 기능에서 제외할지를 지정합니다. (기본값: 활성화)<br>• **URL** 다운로드 검사 기능에서 제외할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' |

| | |
|---|---|
| | 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 5 | 다운로드 검사에서 제외할 URL을 모두 설정한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

**참고:** 다운로드 검사 URL과 다운로드 검사 예외 URL은 중복하여 설정할 수 없습니다. 다운로드 검사 예외 URL은 다운로드 검사 URL의 하위 URL 중 다운로드 검사에서 제외할 URL로 설정하도록 합니다.

## 관련 기능의 활성화 상태 설정

파일 다운로드 검사 기능의 사용 여부와 다운로드 검사 기능과 관련된 보안 로그, 증거, 블랙리스트 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **다운로드검사** 메뉴를 클릭합니다. |
| 2 | <**다운로드 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**다운로드 검사 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 다운로드 검사 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 다운로드 검사 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** 다운로드 검사 정책을 위반한 요청 패킷에 대한 증거를 기록할 것인지 지정합니다. 이 항목은 **보안 로그**의 상태를 활성화한 경우에만 설정이 가능합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 다운로드 검사 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 다운로드 검사 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |



**참고:** 다운로드 검사 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**] 부분을 참고합니다.

# 디렉토리 리스팅 차단 기능 설정

디렉토리 리스팅 차단 기능은 클라이언트가 http://www.listing.com/admin/과 같이 '/'로 끝나는 URL을 입력했을 때 해당 디렉토리에 있는 모든 파일과 디렉토리 목록이 출력되는 것을 막기 위해 해당 요청을 차단하는 기능입니다.

WEBFRONT-K의 디렉토리 리스팅 차단 기능을 사용하려면 차단 URL을 등록해야 합니다. 차단 URL이 등록되면 해당 URL로의 요청이 모두 차단됩니다. '/'로 끝나기는 하지만 클라이언트가 정상적으로 요청 가능한 페이지인 경우에는 디렉토리 리스팅 차단 기능에서 제외할 예외 URL로 등록할 수 있습니다.

응답 페이지 검사 기능은 응답 페이지에 디렉토리 리스트가 포함된 경우 해당 페이지를 전송하지 않는 기능입니다. 예외 URL을 사용해도 차단할 요청과 허용할 요청을 구분하기 힘든 경우에는 고급 디렉토리 리스팅 차단 기능에서 응답 페이지 검사 기능을 사용합니다.

이 절에서는 디렉토리 리스팅 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 디렉토리 리스팅 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

디렉토리 리스팅 차단 기능을 설정하려면 **Application** 메뉴에서 **요청검사** – **디렉토리리스팅차단** 메뉴를 클릭합니다. 그러면, 디렉토리 리스팅 차단 기능의 현재 설정 정보를 보여주는 설정 화면이 나타납니다.


화면의 각 부분에 출력된 정보는 다음과 같습니다.

- **디렉토리 리스팅 차단** 디렉토리 리스팅 차단 기능의 활성화 상태와 관련 기능(보안 로그, 차단)의 활성화 상태가 표시됩니다. 디렉토리 리스팅 차단 기능의 활성화 상태는 아이콘으로 표시되는데, 은 활성화 상태를, 는 비활성화 상태를 나타냅니다.
- **디렉토리 리스팅 차단 URL 리스트** 디렉토리 리스팅 차단 기능에 의해 요청을 차단할 URL의 목록이 표시됩니다.
- **디렉토리 리스팅 차단 예외 URL 리스트** 차단 URL 중에서 예외적으로 요청을 허용할 URL의 목록이 표시됩니다.
- **고급 디렉토리 리스팅 차단** 응답 페이지 검사 기능의 사용 여부와 응답 페이지 검사 기능에서 사용할 사용자 정의 패턴 목록을 볼 수 있습니다.

### 설정 과정

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

❶ 디렉토리 리스팅 차단 URL 설정(필수)
디렉토리 리스팅 차단 기능을 적용할 URL을 등록합니다. 기본적으로 모든 URL(/*/)이 등록되어 있습니다.

❷ 디렉토리 리스팅 차단 예외 URL 설정
디렉토리 리스팅 차단 URL 중에서 예외적으로 디렉토리 차단 기능에서 제외할 URL을 등록합니다.

❸ 고급 디렉토리 리스팅 차단 기능 설정 – 응답 페이지 검사 기능 및 사용자 정의 패턴 설정
응답 페이지 검사 기능의 활성화 여부를 지정합니다. 별도의 패턴이 필요한 경우 사용자가 직접 패턴을 추가할 수 있습니다.

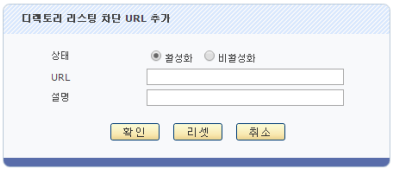
응답 페이지 검사 기능을 활성화하면 WEBFRONT-K의 성능이 낮아지게 되므로 반드시 필요한 경우에만 사용하도록 합니다.

❹ 디렉토리 리스팅 차단 기능 활성화 및 관련 기능 활성화(필수)
디렉토리 리스팅 차단 기능의 사용 여부와 이 기능에 대한 보안 로그, 차단, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 사용하지 않도록 비활성화되어 있습니다.

# 디렉토리 리스팅 차단 설정하기

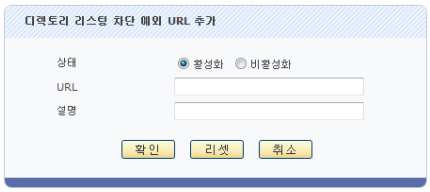
## 디렉토리 리스팅 차단 URL 설정하기

디렉토리 리스팅 차단 기능을 적용할 URL을 추가하는 방법은 다음과 같습니다. WEBFRONT-K에는 디렉토리 리스팅 차단 기능을 적용할 URL을 최대 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **디렉토리리스팅차단** 메뉴를 클릭합니다. |
| 2 | <**디렉토리 리스팅 차단 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**디렉토리 리스팅 차단 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**디렉토리 리스팅 차단 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가하고자 하는 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 디렉토리 리스팅 차단 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있고, 반드시 '/'로 시작해야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | URL을 모두 추가한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

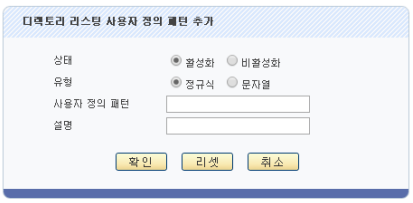
### 디렉토리 리스팅 차단 예외 URL 설정

디렉토리 리스팅 차단 URL 중에서 디렉토리 리스팅 차단 기능에서 제외할 예외 URL을 추가하는 방법은 다음과 같습니다. WEBFRONT-K에는 디렉토리 리스팅 차단 예외 URL을 최대 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **디렉토리리스팅차단** 메뉴를 클릭합니다. |
| 2 | <**디렉토리 리스팅 차단 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**디렉토리 리스팅 차단 예외 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**디렉토리 리스팅 차단 예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가하고자 하는 예외 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 디렉토리 리스팅 차단 기능에서 제외할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있고, 반드시 '/'로 시작해야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 예외 URL을 모두 추가한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

### 고급 기능 설정 – 응답 페이지 검사 기능과 사용자 정의 패턴 설정

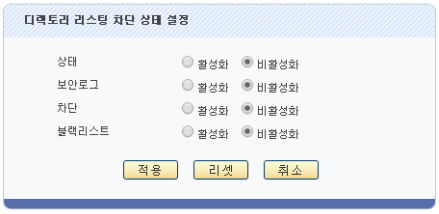
디렉토리 리스팅 차단 기능의 고급 기능인 응답 페이지 검사 기능을 설정하는 방법은 다음과 같습니다. 응답 페이지 검사를 위한 디렉토리 리스팅 사용자 정의 패턴은 256개까지 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **디렉토리리스팅차단** 메뉴를 클릭합니다. |
| 2 | <**고급 디렉토리 리스팅 차단**>의 [**변경**] - [**변경**] 버튼을 클릭합니다. |
| 3 | 응답 페이지 검사 항목을 활성화하고 [**적용**] 버튼을 클릭합니다. 별도의 패턴 설정이 필요한 경우 [**적용**] 버튼을 클릭 하지 않고 다음의 과정을 수행합니다.<br>**참고:** 디렉토리 리스팅 사용자 정의 패턴이란 디렉토리 리스트에 공통적으로 포함된 내용을 사용자가 직접 문자열이나 정규식으로 설정한 것으로 WEBFRONT-K가 응답 페이지에 디렉토리 리스트가 포함되었는지 판단하기 위한 기준으로 사용됩니다.<br>**참고:** WEBFRONT-K는 웹 애플리케이션에서 제공하는 디렉토리 리스트를 판별할 수 있기 때문에 별도의 사용자 정의 패턴을 설정하지 않아도 됩니다. 그러나 별도로 제작한 디렉토리 리스트 페이지를 웹 애플리케이션에 포함시킨 경우에는 사용자 정의 패턴을 설정해야 응답 페이지 검사 기능에서 판별할 수 있습니다. |
| 4 | <**설정된 디렉토리 리스팅 차단 사용자 정의 패턴 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 5 | <**디렉토리 리스팅 차단 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가할 패턴의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **유형** 패턴의 입력 유형을 선택합니다. 패턴 입력 유형에는 문자열과 정규식이 있습니다. (기본값: 정규식)<br>• **사용자 정의 패턴** 유형 항목에서 선택한 유형의 패턴을 입력합니다. '문자열'을 선택한 경우에는 알파벳, 숫자와 문자로 이루어진 최대 1024 글자의 문자열을 입력합니다. '정규식'을 선택한 경우에는 이 설명서와 함께 제공되는 **WEBFRONT-K 시스템 구성 설명서**의 [**제4장 애플리케이션** - **정규식 설정**] 부분을 참고하여 추가하고자 하는 패턴의 정규식을 입력합니다.<br>• **설명** 패턴에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 6 | 응답 페이지 검사 항목에서 등록한 사용자 정의 패턴 리스트의 활성화 여부를 지정합니다. (기본값: 비활성화) |

| | |
|---|---|
| 7 | 패턴을 모두 추가한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

### 관련 기능의 활성화 상태 설정

디렉토리 리스팅 차단 기능의 사용 여부와 이 기능과 관련된 보안 로그, 차단, 블랙리스트 기능의 사용 여부를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **디렉토리리스팅차단** 메뉴를 클릭합니다. |
| 2 | <**디렉토리 리스팅 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**디렉토리 리스팅 차단 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 디렉토리 리스팅 차단 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 디렉토리 리스팅 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 디렉토리 리스팅 차단 정책을 위반한 요청 패킷이나 응답 패킷을 차단할 것인지 지정합니다.<br>• **블랙리스트** 디렉토리 리스팅 차단 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 업로드 검사 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

# 요청 형식 검사 기능 설정

요청 형식 검사는 클라이언트가 웹 서버로 보내는 요청 패킷의 형식을 검사하여 정상적인 요청 패킷인지를 검사하는 기능입니다. 이 절에서는 요청 형식 검사 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 요청 형식 검사 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **요청형식검사** 메뉴를 클릭하면 요청 형식 검사 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **요청 형식 검사** 요청 형식 검사 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 요청 형식 검사 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **허용 메서드 목록** 등록된 허용 메서드 목록이 표시됩니다. 등록된 허용 메서드가 없는 경우에는 '모든 메서드가 허용되었습니다.' 라는 메시지가 출력됩니다.
- **허용 헤더 목록** 등록된 허용 헤더 목록이 표시됩니다. 등록된 허용 헤더가 없는 경우에는 '모든 헤더가 허용되었습니다.' 라는 메시지가 출력됩니다.
- **요청 형식 검사 고급 설정** 필수 헤더 검사, 호스트 헤더 검사 여부가 표시됩니다.

### 설정 과정

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

❶ 허용 메서드 설정

요청 패킷을 검사하기 위한 허용 메서드를 등록합니다. WEBFRONT-K는 요청 패킷이 설정한 허용 메서드를 사용한 요청인지를 검사하여, 허용 메서드를 사용한 경우에만 웹 서버로 전달합니다. 기본적으로 GET과 POST가 허용 메서드로 등록되어 있습니다.

❷ 허용 헤더 설정

요청 패킷의 헤더에 포함되어야 하는 허용 헤더를 등록합니다. WEBFRONT-K는 요청 패킷의 헤더에 설정한 허용 헤더가 포함된 경우에는 요청을 웹 서버로 전달하고, 포함하지 않은 경우에는 요청을 차단합니다. 기본적으로 권장 허용 헤더가 등록되어 있지만, 허용 헤더 상태는 비활성화되어 있습니다.

❸ 호스트 헤더 검사 설정

요청 패킷의 헤더 중 호스트 헤더의 검사 여부를 설정합니다. 호스트 헤더는 하나의 IP주소/포트로 여러 개의 웹 애플리케이션을 서비스 하는 경우 웹 애플리케이션을 구분하기 위한 헤더입니다. 비정상적인 호스트 헤더가 요청 패킷에 포함된 경우에는 요청을 차단합니다. 기본적으로 호스트 헤더 검사 상태는 활성화되어 있습니다.

❹ 필수 헤더 설정

특정 메서드를 사용하는 요청 패킷에 반드시 포함되어야 하는 필수 헤더를 등록합니다. 클라이언트가 필수 헤더가 설정되어 있는 메서드를 통해 웹 서버로 요청 패킷을 보내면 WEBFRONT-K는 요청 패킷에 설정한 필수 헤더가 포함되었는지를 확인합니다. 필수 헤더 기능은 고급 기능으로 반드시 설정하지 않아도 됩니다. 기본적으로 필수 헤더 기능은 비활성화되어 있고, 등록된 필수 헤더가 없습니다.

❺ 관련 기능의 활성화 상태 설정

요청 형식 검사 기능의 사용 여부와 이 기능에 대한 보안 로그, 차단, 증거, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 사용하지 않도록 비활성화되어 있습니다.

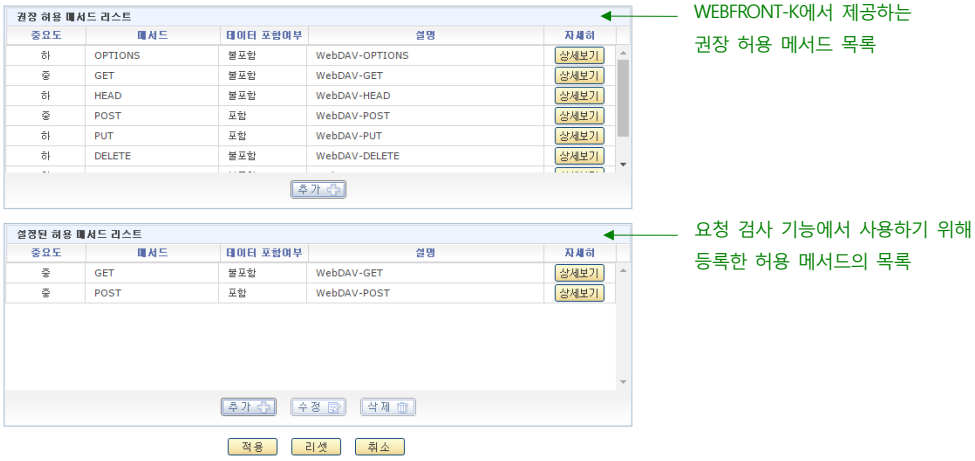
# 요청 형식 검사 설정하기

## 허용 메서드 설정

요청 형식 검사 기능을 수행하기 위한 허용 메서드를 설정하는 방법은 다음과 같습니다. 허용 메서드는 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **요청형식검사** 메뉴를 클릭합니다. |
| 2 | <**허용 메서드 리스트**>의 [**변경**] 버튼을 클릭합니다. |

권장 허용 메서드와 등록된 허용 메서드 목록을 보여주는 화면이 나타납니다. 권장 목록의 허용 메서드를 추가하려면 3번 과정을, 사용자가 직접 허용 메서드를 입력하려면 4 ~ 5번 과정을 수행합니다.

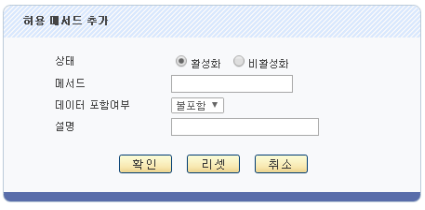



WEBFRONT-K에서 제공하는 권장 허용 메서드 목록

요청 검사 기능에서 사용하기 위해 등록한 허용 메서드의 목록

**참고:** 권장 허용 메서드 목록에 있는 정보는 실제 WEBFRONT-K 화면에서 출력되는 권장 정보와 다를 수 있습니다.

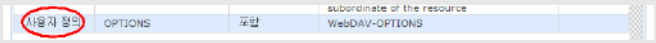
| | |
|---|---|
| 3 | 등록하고자 하는 허용 메서드가 권장 허용 메서드 목록에 있는 경우에는 목록에서 해당 허용 메서드를 선택한 후 [**추가**] 버튼을 클릭합니다. 여러 개의 허용 메서드를 선택할 때에는 [**Ctrl**] 키나 [**Shift**] 키를 누른 상태에서 허용 메서드를 클릭하면 됩니다. 허용 메서드를 선택할 때에는 허용 메서드의 중요도와 상세 정보를 참고하는 것이 좋습니다. 권장 허용 메서드의 중요도와 상세 정보에 대한 설명은 다음 절인 [**권장 허용 메서드 정보 보기**]에 설명되어 있습니다. |
| 4 | 사용자가 직접 허용 메서드를 입력하려면 <**설정된 허용 메서드 리스트**>에 있는 [**추가**] 버튼을 클릭합니다. |
| 5 | <**허용 메서드 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다. |



| | |
|---|---|
| | • **상태** 등록하고 있는 허용 메서드를 실제로 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **메서드** 허용 메서드를 최대 16글자의 알파벳으로 입력합니다.<br>• **데이터 포함 여부** 메서드가 데이터를 포함하는지를 지정합니다. (기본값: 불포함)<br>• **설명** 허용 메서드에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>**참고:** 사용자가 직접 입력한 허용 메서드는 중요도 항목이 '사용자 정의'로 표시됩니다. |
| 6 | 허용 메서드를 모두 설정한 후에는 허용 메서드 설정 상태 항목에서 설정한 허용 메서드의 활성화 여부를 지정합니다. |
| 7 | 메서드를 모두 추가한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

**참고: [설정된 허용 메서드 수정하기]**

• 설정된 허용 메서드 리스트에 추가한 허용 메서드의 내용을 변경하려면 해당 허용 메서드를 선택하고 [**수정**] 버튼을 클릭합니다. <**허용 메서드 수정**> 팝업 창이 뜨면 원하는 항목을 변경한 후 [**확인**]을 클릭합니다. 권장 허용 메서드를 수정한 경우에는 중요도가 '사용자 정의'로 바뀌고 [**상세 보기**] 버튼도 없어집니다.

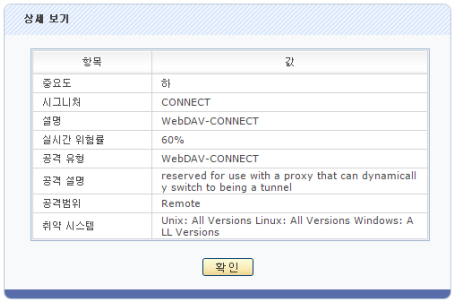



• 설정된 허용 메서드 리스트의 허용 메서드 중, 비공개로 표시된 허용 메서드는 수정할 수 없습니다.

## 권장 허용 메서드 정보 보기

설정된 허용 메서드에 등록할 권장 허용 메서드를 선택할 때에는 허용 메서드의 중요도와 상세 정보를 참고하는 것이 좋습니다. 허용 메서드의 중요도는 상, 중, 하, 세 단계로 표시됩니다. 중요도가 '상'인 허용 메서드는 요청 형식 검사에 필요한 허용 메서드이므로 반드시 설정된 허용 메서드로 추가해야 합니다. 중요도가 '중'이나 '하'인 허용 메서드는 [**상세보기**] 버튼을 클릭하여 허용 메서드의 상세 정보를 확인한 후 추가 여부를 결정하도록 합니다.

허용 메서드의 [**상세보기**] 버튼을 클릭하면 <**상세 보기**> 팝업 창이 나타납니다. <**상세 보기**> 팝업 창에서 보여주는 정보는 다음과 같습니다.




- 중요도
  허용 메서드의 중요도. 상, 중, 하로 표시됩니다.
- 시그니처
  허용 메서드. 비공개 허용 메서드인 경우에는 '시그니처 비공개'로 표시됩니다.
- 설명
  허용 메서드가 차단하는 공격에 대한 설명
- 실시간 위험률
  시그니처에 대한 실제 공격 사용빈도 위험률 (%)
- 공격 유형
  허용 메서드에 의해 차단할 공격의 유형
- 공격 설명
  허용 메서드에 의해 차단할 공격에 대한 설명
- 공격 범위
  공격 방식. remote인 경우에는 원격에서 서버를 공격하는 방식이고, local은 서버에서 직접 공격하는 방식입니다.
- 취약 시스템
  허용 메서드에 의해 차단할 공격에 대해 취약한 시스템

## 허용 헤더 설정

요청 형식 검사 기능을 수행하기 위한 허용 헤더를 설정하는 방법은 다음과 같습니다. 허용 헤더는 256개까지 등록할 수 있습니다.

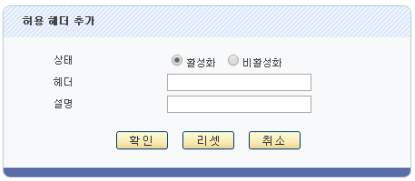
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **요청형식검사** 메뉴를 클릭합니다. |
| 2 | <**허용 헤더 리스트**>의 [**변경**] 버튼을 클릭합니다. |

권장 허용 헤더 목록을 보여주는 <**허용 헤더 리스트 설정**> 화면이 나타납니다. 권장 목록의 허용 헤더를 추가하려면 3번 과정을, 사용자가 직접 허용 메서드를 입력하려면 4 ~ 5번 과정을 수행합니다.


WEBFRONT-K에서 제공하는 권장 허용 헤더 목록

요청 형식 검사 기능을 적용하기 위해 사용자가 등록한 허용 헤더 목록.

**참고:** 권장 허용 헤더 목록에 있는 정보는 실제 WEBFRONT-K 화면에서 출력되는 권장 정보와 다를 수 있습니다.

| | |
|---|---|
| 3 | 등록하고자 하는 허용 헤더가 권장 허용 헤더 목록에 있는 경우에는 목록에서 해당 허용 헤더를 선택한 후 [**추가**] 버튼을 클릭합니다. 여러 개의 허용 헤더를 선택할 때에는 [**Ctrl**] 키나 [**Shift**]키를 누른 상태에서 허용 헤더를 클릭하면 됩니다. 허용 헤더를 선택할 때에는 허용 헤더의 중요도와 상세 정보를 참고하는 것이 좋습니다. 권장 허용 헤더의 중요도와 상세 정보에 대한 설명은 다음 절인 [권**장 허용 헤더 정보 보기**]에 설명되어 있습니다. |
| 4 | 사용자가 직접 허용 헤더를 입력하려면 <**설정된 허용 헤더 리스트**>에 있는 [**추가**] 버튼을 클릭합니다. |
| 5 | <**허용 헤더 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 등록하고 있는 허용 헤더에 대해 요청 형식 검사 기능을 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **헤더** 요청 패킷에 포함된 헤더와 비교할 허용 헤더를 입력합니다. 허용 헤더에는 알파벳, 숫자와 '-' 기호로 이루어진 최대 128자의 문자열을 입력할 수 있습니다.<br>• **설명** 허용 헤더에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>**참고:** 사용자가 직접 입력한 허용 헤더는 중요도 항목이 '사용자 정의'로 표시됩니다. |
| 6 | 허용 헤더를 모두 설정한 후에는 허용 헤더 설정 상태 항목에서 설정한 허용 헤더의 활성화 여부를 지정합니다. |
| 7 | 헤더를 모두 추가한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

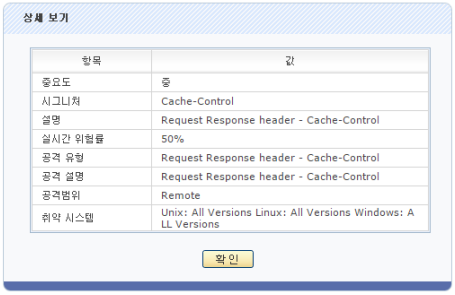
**참고: [설정된 허용 헤더 수정하기]**

- 설정된 허용 헤더 리스트에 추가한 허용 헤더의 내용을 변경하려면 해당 허용 헤더를 선택하고 [**수정**] 버튼을 클릭합니다. <**허용 헤더 수정**> 팝업 창이 뜨면 원하는 항목을 변경한 후 [**확인**]을 클릭합니다. 권장 허용 헤더를 수정한 경우에는 중요도가 '사용자 정의'로 바뀌고 [**상세 보기**] 버튼도 없어집니다.
- 설정된 허용 헤더 리스트의 허용 헤더 중, 비공개로 표시된 허용 헤더는 수정할 수 없습니다.

### 권장 허용 헤더 정보 보기

설정된 허용 헤더에 등록할 권장 허용 헤더를 선택할 때에는 허용 헤더의 중요도와 상세 정보를 참고하는 것이 좋습니다. 허용 헤더의 중요도는 상, 중, 하, 세 단계로 표시됩니다. 중요도가 '상'인 허용 헤더는 요청 형식 검사에 필요한 허용 헤더이므로 반드시 설정된 허용 헤더로 추가해야 합니다. 중요도가 '중'이나 '하'인 허용 헤더는 [**상세보기**] 버튼을 클릭하여 허용 헤더의 상세 정보를 확인한 후 추가 여부를 결정하도록 합니다.

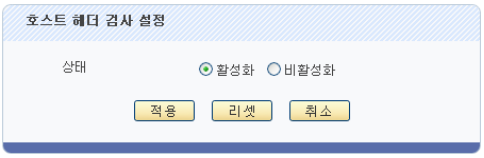
허용 헤더의 [**상세보기**] 버튼을 클릭하면 <**상세 보기**> 팝업 창이 나타납니다. <**상세 보기**> 팝업 창에서 보여주는 정보는 다음과 같습니다.




- 중요도
  허용 헤더의 중요도. 상, 중, 하로 표시됩니다.
- 시그니처
  허용 헤더. 비공개 허용 헤더인 경우에는 '시그니처 비공개'로 표시됩니다.
- 설명
  허용 헤더가 차단하는 공격에 대한 설명
- 실시간 위험률
  시그니처에 대한 실제 공격 사용빈도 위험률 (%)
- 공격 유형
  허용 헤더에 의해 차단할 공격의 유형
- 공격 설명
  허용 헤더에 의해 차단할 공격에 대한 설명
- 공격 범위
  공격 방식. remote인 경우에는 원격에서 서버를 공격하는 방식이고, local은 서버에서 직접 공격하는 방식입니다.
- 취약 시스템
  허용 헤더에 의해 차단할 공격에 대해 취약한 시스템

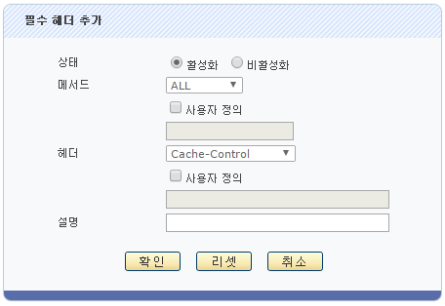
## 호스트 헤더 검사 설정

다음은 요청 패킷의 호스트 헤더 검사 상태를 설정하는 방법입니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **요청형식검사** 메뉴를 클릭합니다. |
| 2 | <**요청 형식 검사 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**호스트 헤더 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 4 | <**호스트 헤더 검사 설정**> 팝업 창에서 상태를 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  |

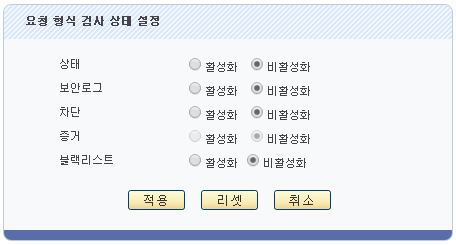
## 필수 헤더 설정

다음은 요청 패킷의 메서드 종류에 따라 요청 패킷에 반드시 포함되어야 하는 필수 헤더를 설정하는 방법입니다. 필수 헤더는 256개까지 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **요청형식검사** 메뉴를 클릭합니다. |
| 2 | <**요청 형식 검사 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**요청 형식 검사 고급 설정 보기**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**필수 헤더 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 등록하고 있는 필수 헤더를 요청 형식 검사 기능에 적용할지를 지정합니다. (기본값: 활성화)<br>• **메서드** 필수 헤더 검사를 수행할 메서드를 지정합니다. 메서드는 다음과 같은 2가지 방법 중의 한 가지 방법으로 지정할 수 있습니다. (기본값: ALL)<br>❶ 드롭다운 목록을 클릭한 후 목록에서 지정하려는 메서드를 선택합니다.<br>❷ 드롭다운 목록에 지정하려는 메서드가 없는 경우에는 '사용자 정의' 항목을 체크한 후 바로 아래의 텍스트 박스에 메서드를 직접 입력합니다. 메서드는 알파벳과 숫자로 이루어진 최대 16자의 문자열을 입력합니다.<br>• **헤더** 지정한 메서드를 사용하는 요청 패킷에 반드시 포함되어야 하는 필수 헤더를 지정합니다. 필수 헤더는 다음과 같은 2가지 중 한 가지 방법으로 지정할 수 있습니다. (기본값: Cache-Control)<br>❶ 드롭다운 목록을 클릭한 후 지정하려는 필수 헤더를 선택합니다.<br>❷ 드롭다운 목록에 지정하려는 헤더가 없는 경우에는 '사용자 정의' 항목을 체크한 후 바로 아래의 텍스트 박스에 헤더를 직접 입력합니다. 필수 헤더는 알파벳, 숫자와 '-' 기호로 이루어진 최대 128자의 문자열로 지정합니다.<br>• **설명** 필수 헤더에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 필수 헤더를 모두 추가하였으면 필수 헤더 기능 상태 항목에서 필수 헤더의 사용 여부를 지정합니다. |
| 6 | 설정 내용을 저장하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

요청 형식 검사 기능의 사용 여부와 요청 형식 검사 기능과 관련된 보안 로그, 차단, 증거, 블랙리스트 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **요청형식검사** 메뉴를 클릭합니다. |
| 2 | <**요청 형식 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**요청 형식 검사 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 요청 형식 검사 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 요청 형식 검사 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 요청 형식 검사 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다.<br>• **증거** 요청 형식 검사 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안 로그**의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 요청 형식 검사 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 요청 형식 검사 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

# 검사 회피 차단 기능 설정

검사 회피 차단은 디렉토리 불법 참조 차단, 더블 인코딩 차단, 불법 UTF-8 인코딩 차단, 매개변수 내 불법 URL 인코딩 차단, 매개변수 중복 차단과 같은 WEBFRONT-K의 검사를 회피하려는 행위를 차단하는 기능입니다. 이 절에서는 검사 회피 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 검사 회피 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **검사회피차단** 메뉴를 클릭하면 검사 회피 차단 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **검사 회피 차단** — 검사 회피 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 검사 회피 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **검사 회피 차단 기능** — 검사 회피 차단 기능의 각 항목의 설정 상태가 표시됩니다.
- **검사 회피 차단 예외 URL 리스트** — 검사 회피 차단 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

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

❶ 검사 회피 차단 기능 설정
검사를 회피하여 공격을 수행할 가능성이 있는 WEBFRONT-K에서 지원하는 항목들을 각각 차단할 것인지 지정합니다. 기본적으로는 차단하지 않도록 비활성화로 지정되어 있습니다.

❷ 검사 회피 차단 예외 URL 설정
검사 회피 차단 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

❸ 관련 기능의 활성화 상태 설정
검사 회피 차단 기능의 사용 여부와 이 기능에 대한 보안 로그, 차단, 증거, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 사용하지 않도록 비활성화되어 있습니다.

# 검사 회피 차단 설정하기

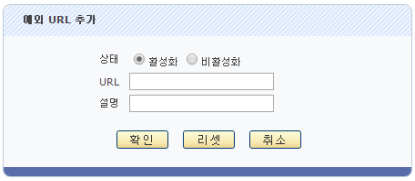
## 검사 회피 차단 기능 설정

검사 회피 차단 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **검사회피차단** 메뉴를 클릭합니다. |
| 2 | <**검사 회피 차단 기능**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**검사 회피 차단 기능 설정**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **디렉토리 불법 참조 차단** 요청 URL에 '~' 또는 './'이 포함된 경우, 요청을 차단합니다. (기본값: 활성화)<br>• **더블 인코딩 차단** 요청 URL이 더블 인코딩된 경우 요청을 차단합니다. (기본값: 활성화)<br>• **더블 인코딩 차단(매개변수)** 요청 URL의 매개변수 및 요청 URL 바디의 매개변수 값이 더블 인코딩된 경우 요청을 차단합니다. (기본값: 비활성화)<br>• **불법 UTF-8 인코딩 차단** 요청 URL이 일반적인 형식에 맞지 않게 UTF-8 인코딩이 된 경우 요청을 차단합니다. (기본값: 활성화)<br>• **매개변수 내 불법 URL 인코딩 차단** 요청 URL 및 폼 필드의 매개변수 값에 URL 인코딩으로 위장한 구문이 포함된 경우 요청을 차단합니다. (기본값: 활성화)<br>• **매개변수 중복 차단** 하나의 요청에 동일한 매개변수가 중복으로 사용된 경우 요청을 차단합니다. (기본값: 비활성화) |

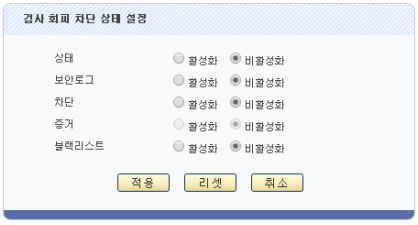
## 검사 회피 차단 예외 URL 설정

검사 회피 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **검사회피차단** 메뉴를 클릭합니다. |
| 2 | <**검사 회피 차단 예외 URL 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가할 예외 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 검사 회피 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | <**예외 URL 리스트**>의 **상태** 항목에서 등록한 예외 URL의 활성화 여부를 지정합니다. (기본값: 비활성화) |
| 5 | 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

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

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **검사회피차단** 메뉴를 클릭합니다. |
| 2 | <**검사 회피 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**검사 회피 차단 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br>• **상태** 검사 회피 차단 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 검사 회피 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 검사 회피 차단 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다.<br>• **증거** 검사 회피 차단 정책을 위반한 요청 패킷에 대한 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안 로그**의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 디렉토리 리스팅 차단 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 업로드 검사 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

# 인클루드 인젝션 차단 기능 설정

인클루드 인젝션 차단 기능은 외부 서버의 파일을 호출하여 실행할 수 있는 인클루드 취약점을 이용한 공격을 검사하는 기능입니다. 인클루드 인젝션 차단 시그니처에 포함된 URL 요청 시 외부 파일을 호출하는 구문이 포함되어 있으면 해당 요청은 지정한 방식에 따라 처리됩니다. 이 절에서는 인클루드 인젝션 차단 기능의 설정 화면과 설정 과정에 대해 살펴본 후 실제로 인클루드 인젝션 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **인클루드인젝션차단** 메뉴를 클릭하면 인클루드 인젝션 차단 기능을 설정할 수 있는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **인클루드 인젝션 상태** 인클루드 인젝션 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 인클루드 인젝션 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **인클루드 인젝션 차단 옵션** 인클루드 인젝션 차단 기능에서 사용하는 옵션의 상태가 표시됩니다.
- **인클루드 인젝션 예외 URL 리스트** 인클루드 인젝션 차단 기능에서 제외할 URL과 매개변수, 매개변수 값이 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 세부 기능의 변경 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 인클루드 인젝션 차단 기능을 설정하는 과정은 다음과 같습니다.

❶ 인클루드 인젝션 차단 시그니처 설정

인클루드 인젝션 공격을 검사하기 위한 시그니처를 지정합니다. WEBFRONT-K는 각각의 시그니처마다 서로 다른 액션(차단, 탐지, 예외) 설정을 할 수 있으며, 설정된 액션에 따라 요청 패킷을 처리합니다. 인클루드 인젝션 차단 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❷ 인클루드 인젝션 차단 옵션 설정

모든 URL 검사 옵션 사용 여부를 지정합니다. 기본적으로 인클루드 인젝션 차단 기능은 시그니처에 정의된 URL을 검사 대상으로 합니다. 이 시그니처는 제로 보드 등의 공개 웹 애플리케이션에 존재하는 취약점 페이지를 대상으로 하기 때문에 별도의 웹 페이지를 검사하려면 모든 URL 검사 옵션을 활성화하거나 사용자 정의 시그니처를 정의해야 합니다.

❸ 인클루드 인젝션 예외 URL 설정

인클루드 인젝션 차단 기능에서 제외할 예외 URL과 매개변수, 값을 지정합니다. 인클루드 인젝션 차단 기능은 시그니처에 설정된

URL에 대해서만 검사를 수행합니다. 그러므로 인클루드 인젝션 예외 URL은 모든 URL 검사 옵션을 활성화한 경우 사용하는 것이 효율적입니다. 기본적으로 지정된 예외 URL은 없습니다.

❹ 인클루드 인젝션 차단 기능과 관련 기능의 활성화 상태 설정
인클루드 인젝션 차단 기능의 사용 여부와 인클루드 인젝션 차단 기능과 관련된 보안 로그, 차단, 증거, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

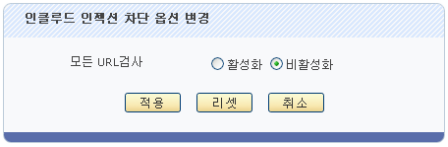
# 인클루드 인젝션 차단 설정하기

## 인클루드 인젝션 차단 시그니처 설정

인클루드 인젝션 차단 기능을 사용하려면 차단하려는 시그니처를 설정해야 합니다. 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 시그니처를 설정하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션** - **시그니처 관리** - **시그니처 액션 설정**, **사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

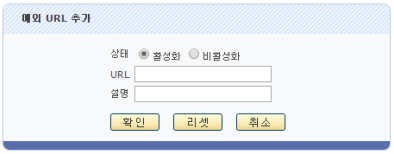
## 인클루드 인젝션 차단 옵션 설정

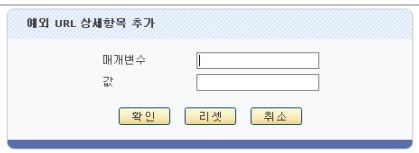
인클루드 인젝션 차단 기능의 옵션을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **인클루드인젝션차단** 메뉴를 클릭합니다. |
| 2 | <**인클루드 인젝션 차단 옵션**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**인클루드 인젝션 차단 옵션 변경**> 팝업 창에서 모든 URL 검사 옵션의 활성화 여부를 설정하고 [**적용**] 버튼을 클릭합니다. (기본값: 비활성화)<br>  |

## 인클루드 인젝션 차단 예외 URL 설정

인클루드 인젝션 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **인클루드인젝션차단** 메뉴를 클릭합니다. |
| 2 | <**인클루드 인젝션 예외 URL 리스트**>의 [**변경**] - [**URL추가**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가할 예외 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 인클루드 인젝션 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** 예외 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 예외 URL을 보다 상세하게 설정 하려면 [**상세항목추가**] 버튼을 클릭합니다. |
| 5 | <**예외 URL 상세항목 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다. |




- **매개변수** 인클루드 인젝션 차단 기능에서 제외할 매개변수 이름을 입력합니다.
- **값** 인클루드 인젝션 차단 기능에서 제외할 매개변수 값을 입력합니다.

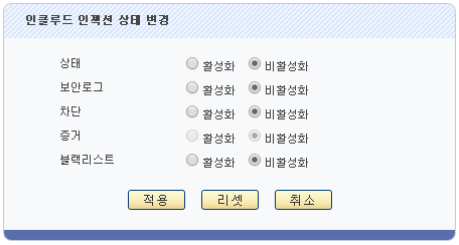
**참고:** 인클루드 인젝션 차단 예외 URL은 설정한 항목에 따라 다르게 동작합니다. 설정항목에 따른 동작 방식은 다음과 같습니다.
- URL만 설정 - 해당 URL을 인클루드 인젝션 차단 기능에서 제외합니다.
- URL과 매개변수를 설정 - 해당 URL에서 설정한 매개변수만 인클루드 인젝션 차단 기능에서 제외합니다.
- URL과 값을 설정 - 해당 URL에서 모든 매개변수에 대해 설정한 값이 요청된 경우 인클루드 인젝션 차단 기능에서 제외합니다.
- URL과 매개변수, 값 모두 설정 - 해당 URL에서 설정한 매개변수에 설정한 값이 요청된 경우만 인클루드 인젝션 차단 기능에서 제외합니다.

6 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다.

## 관련 기능의 활성화 상태 설정

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

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **인클루드인젝션차단** 메뉴를 클릭합니다. |
| 2 | <**인클루드 인젝션 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | **<인클루드 인젝션 상태 설정>** 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다. |




- **상태** 인클루드 인젝션 차단 기능의 활성화 여부를 지정합니다.
- **보안 로그** 인클루드 인젝션 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.
- **차단** 모든 URL 검사 옵션이 활성화된 경우 인클루드 인젝션 공격이 포함된 요청을 차단할 것인지 지정합니다. 모든 URL 검사 옵션이 비활성화된 경우에는 각 시그니처 설정에 따라 차단이 결정됩니다.
- **증거** 인클루드 인젝션 차단 정책을 위반한 요청 패킷에 대한 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보(시간, 클라이언트, URL, 공격 유형 등)만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.
- **블랙리스트** 인클루드 인젝션 차단 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 인클루드 인젝션 차단 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다.

**참고:** 모든 URL 검사 옵션이 비활성화 상태인 경우 인클루드 인젝션 차단 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**] 부분을 참고합니다.

# 웹 공격 프로그램 차단 기능 설정

웹 공격 프로그램 차단은 웹 공격 프로그램(웹 스캐너, 웹 크롤러, 프록시 툴 등)을 사용하여 웹 서버로 보내는 요청을 차단하기 위해 요청 패킷을 검사하는 기능입니다. 웹 공격 프로그램을 통해 보내지는 요청은 시그니처 액션 설정에 따라 처리됩니다. 이 절에서는 웹 공격 프로그램 차단 기능의 설정 화면과 설정 과정에 대해 살펴본 후 실제로 웹 공격 프로그램 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **웹공격프로그램차단** 메뉴를 클릭하면 웹 공격 프로그램 차단 기능을 설정할 수 있는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **웹 공격 프로그램 차단 상태** 웹 공격 프로그램 차단 기능과 관련 기능의 활성화 상태가 표시됩니다. 웹 공격 프로그램 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **웹 공격 프로그램 차단 옵션** 웹 공격 프로그램 차단 기능에서 사용하는 옵션의 상태가 표시됩니다.
- **웹 공격 프로그램 차단 예외 URL 리스트** 웹 공격 프로그램 차단 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 웹 공격 프로그램 차단 기능을 설정하는 과정은 다음과 같습니다.

❶ 웹 공격 프로그램 차단 시그니처 설정
웹 스캔 또는 공격에 이용되는 프로그램을 사용하여 웹 서버로 보내는 요청 패킷을 검사하기 위한 웹 공격 프로그램 차단 시그니처를 지정합니다. WEBFRONT-K는 각각의 시그니처마다 서로 다른 액션(차단, 탐지, 예외) 설정을 할 수 있으며, 설정된 액션에 따라 요청 패킷을 처리합니다. 웹 공격 프로그램 차단 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❷ 웹 공격 프로그램 차단 옵션 설정
웹 공격 프로그램 차단 기능에서 사용할 옵션을 설정합니다.

❸ 웹 공격 프로그램 차단 예외 URL 설정
웹 공격 프로그램 차단 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

❹ 웹 공격 프로그램 차단 기능과 관련 기능의 활성화 상태 설정
웹 공격 프로그램 차단 기능의 사용 여부와 웹 공격 프로그램 차단 기능과 관련된 보안 로그, 차단, 증거, 블랙리스트 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

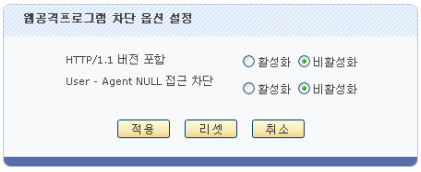
# 웹 공격 프로그램 차단 설정하기

## 웹 공격 프로그램 차단 시그니처 설정

웹 공격 프로그램 차단 기능을 사용하려면 차단하려는 시그니처를 설정해야 합니다. 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정합니다. 시그니처를 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션** - **시그니처 관리** - **시그니처 액션 설정, 사용자 정의 시그니처 설정하기**] 부분을 참고합니다.

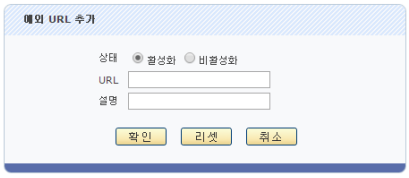
## 웹 공격 프로그램 차단 옵션 설정

웹 공격 프로그램 차단 기능에서 사용할 옵션을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **웹공격프로그램차단** 메뉴를 클릭합니다. |
| 2 | <**웹 공격 프로그램 차단 옵션**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**웹 공격 프로그램 차단 옵션 설정**> 팝업 창에서 다음 설명을 참고하여 각 옵션의 상태를 설정하고 [**적용**] 버튼을 클릭합니다. 각 옵션은 기본적으로 비활성화되어 있습니다.<br>  <br><br>• **HTTP/1.1 버전 포함**<br>웹 공격 프로그램 차단 기능은 기본적으로 HTTP/1.0 버전의 패킷을 검사 대상으로 합니다. HTTP/1.1 버전도 검사 대상에 포함시키려면 옵션을 활성화합니다.<br>• **User – Agent NULL 접근 차단**<br>요청 패킷의 헤더 중 User – Agent 헤더의 값이 비어 있는 경우 요청을 차단합니다. |

## 웹 공격 프로그램 차단 예외 URL 설정

웹 공격 프로그램 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **웹공격프로그램차단** 메뉴를 클릭합니다. |
| 2 | <**웹공격프로그램 차단 예외 URL 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 추가할 예외 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 웹 공격 프로그램 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** 예외 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 예외 URL을 모두 설정한 후에는 상태 항목에서 설정한 예외 URL의 활성화 여부를 지정합니다. |
| 5 | 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

웹 공격 프로그램 차단 기능의 사용 여부와 웹 공격 프로그램 차단 기능과 관련된 보안 로그, 증거, 블랙리스트 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **웹공격프로그램차단** 메뉴를 클릭합니다. |
| 2 | <**웹 공격 프로그램 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**웹 공격 프로그램 차단 상태 설정**>팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 웹 공격 프로그램 차단 기능의 활성화 여부를 지정합니다.<br>• **보안 로그** 웹 공격 프로그램 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** User – Agent NULL 접근 차단 옵션이 활성화된 경우 User – Agent 헤더가 NULL인 요청을 차단할 것인지 지정합니다.<br>• **증거** 웹 공격 프로그램 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보(시간, 클라이언트, URL, 공격 유형 등)만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **블랙리스트** 웹 공격 프로그램 차단 기능에 블랙리스트 기능을 적용할 것인지 지정합니다. 이 항목을 활성화하면 특정 클라이언트가 웹 공격 프로그램 차단 정책을 위반한 횟수를 기록합니다. 이 횟수는 다른 요청 검사 기능의 정책을 위반한 횟수와 함께 블랙리스트 차단 IP 리스트에 등록하기 위한 조건이 됩니다. 블랙리스트 기능에 대한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 블랙리스트**] 부분을 참고하도록 합니다. |

**참고:** 웹 공격 프로그램 차단 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**] 부분을 참고합니다.

# HTTP POST 공격 차단 기능 설정

HTTP POST 공격 차단은 HTTP POST 메서드를 사용하여 웹 서버와의 커넥션을 장시간 유지함으로써 웹 서버가 정상적인 사용자의 접속을 받지 못하게 하는 L7 DDoS 공격을 차단하는 기능입니다. 이 절에서는 HTTP POST 공격 차단 기능의 설정 화면과 설정 과정에 대해 살펴본 후 실제로 HTTP POST 공격 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** – **HTTP POST 공격차단** 메뉴를 클릭하면 HTTP POST 공격 차단 기능을 설정할 수 있는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **HTTP POST 공격 차단 상태** — HTTP POST 공격 차단 기능과 관련 기능의 활성화 상태가 표시됩니다. HTTP POST 공격 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **HTTP POST 공격 차단 고급 설정** — 요청 시간 검사 기능의 활성화 여부와 최대 요청 허용 시간이 표시됩니다.
- **HTTP POST 공격 검사 URL 리스트** — HTTP POST 공격 차단 기능을 적용할 URL이 표시됩니다.
- **HTTP POST 공격 검사 예외 URL 리스트** — HTTP POST 공격 차단 기능에서 제외할 URL과 인증 옵션의 활성화 상태가 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. HTTP POST 공격 차단 기능을 설정하는 과정은 다음과 같습니다.

❶ HTTP POST 공격 차단 고급 설정
요청 시간 검사 기능의 사용 여부와 최대 요청 허용 시간을 설정합니다. 요청 시간 검사 기능을 활성화하면 HTTP POST 공격 차단 검사 URL에 대한 웹 요청이 지정된 최대 요청 허용 시간을 초과하여 지속되는 경우, 해당 요청을 L7 DDoS 공격으로 간주합니다. 기본적으로 요청 시간 검사 기능은 활성화되어 있고, 최대 요청 허용 시간은 5초로 설정되어 있습니다.

❷ HTTP POST 공격 차단 검사 URL 설정
HTTP POST 공격 차단 기능을 적용할 URL을 지정합니다. 기본적으로 모든 URL을 의미하는 '/*'가 등록되어 있습니다.

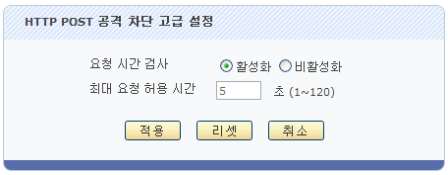
❸ HTTP POST 공격 차단 예외 URL 설정
HTTP POST 공격 차단 기능에서 제외할 예외 URL을 지정하고, 예외 URL에 대한 인증 옵션의 활성화 여부를 설정합니다. 인증 옵션을 활성화하면, 예외 URL로의 접근 시 마우스 클릭을 요구하여 정상적인 요청임을 확인하는 인증 페이지를 클라이언트에게 전송합니다. 인증이 완료되면 해당 요청에 인증 쿠키를 삽입하여 쿠키가 유지되는 동안 요청을 허용합니다. 기본적으로 인증 옵션은 비활성화되어 있고, 지정된 예외 URL은 없습니다.

❹ HTTP POST 공격 차단 기능과 관련 기능의 활성화 상태 설정
HTTP POST 공격 차단 기능의 사용 여부와 HTTP POST 공격 차단 기능과 관련된 로그, 차단 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# HTTP POST 공격 차단 설정하기

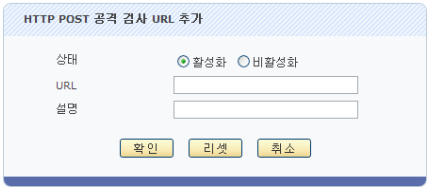
## HTTP POST 공격 차단 고급 설정

요청 시간 검사 기능의 사용 여부와 최대 요청 허용 시간을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **HTTP POST 공격차단** 메뉴를 클릭합니다. |
| 2 | <**HTTP POST 공격 차단 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**HTTP POST 공격 차단 고급 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **요청 시간 검사** 요청 시간 검사 기능의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **최대 요청 허용 시간** 요청을 허용할 시간을 지정합니다. 지정한 시간을 초과하여 요청이 지속되는 경우, 해당 요청을 L7 DDoS 공격으로 간주합니다. (설정 범위: 1 ~ 120, 기본값: 5(초)) |

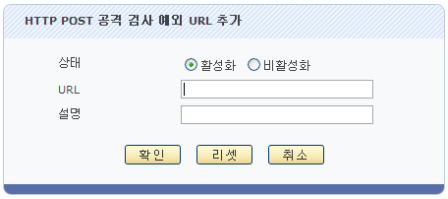
## HTTP POST 공격 차단 검사 URL 설정

HTTP POST 공격 차단 기능을 적용할 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 검사 URL을 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **HTTP POST 공격차단** 메뉴를 클릭합니다. |
| 2 | <**HTTP POST 공격 검사 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**HTTP POST 공격 검사 URL 리스트 설정**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**HTTP POST 공격 검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 현재 등록하고 있는 URL에 대해 HTTP POST 공격 차단 기능을 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** HTTP POST 공격 차단 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있고, 반드시 '/'로 시작해야 합니다.<br>HTTP POST 공격 검사 예외 URL에 설정된 URL은 검사 URL로 설정할 수 없습니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. |

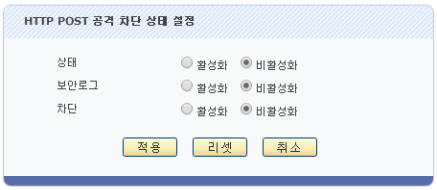
## HTTP POST 공격 차단 예외 URL 설정

HTTP POST 공격 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 예외 URL을 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **HTTP POST 공격차단** 메뉴를 클릭합니다. |
| 2 | <**HTTP POST 공격 검사 예외 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**HTTP POST 공격 검사 예외 URL 리스트 설정**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**HTTP POST 공격 검사 예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 추가할 예외 URL의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **URL** HTTP POST 공격 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다. HTTP POST 공격 검사 URL에 설정된 URL은 예외 URL로 설정할 수 없습니다.<br>• **설명** 예외 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 예외 URL을 모두 설정한 후에는 다음 설명을 참고하여 예외 URL과 인증 옵션의 활성화 여부를 지정합니다.<br>• **상태** HTTP POST 공격 검사 예외 URL 리스트에 등록한 모든 예외 URL의 사용 여부를 지정합니다. 비활성화로 지정하면 각 예외 URL의 상태와 관계없이 모두 비활성화로 동작합니다. (기본값: 비활성화)<br>• **인증** 예외 URL에 대한 인증 옵션의 활성화 여부를 설정합니다. 인증 옵션을 활성화하면, 예외 URL로의 접근 시 마우스 클릭을 요구하여 정상적인 요청임을 확인하는 인증 페이지를 클라이언트에게 전송합니다. 인증이 완료되면 해당 요청에 인증 쿠키를 삽입하여 세션이 유지되는 동안 요청을 허용합니다. |
| 6 | HTTP POST 공격 검사 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

HTTP POST 공격 차단 기능의 사용 여부와 HTTP POST 공격 차단 기능과 관련된 보안 로그, 차단 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **HTTP POST 공격차단** 메뉴를 클릭합니다. |
| 2 | <**HTTP POST 공격 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**HTTP POST 공격 차단 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** HTTP POST 공격 차단 기능의 활성화 여부를 지정합니다.<br>• **보안 로그** HTTP POST 공격 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** HTTP POST 공격 차단 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다. |

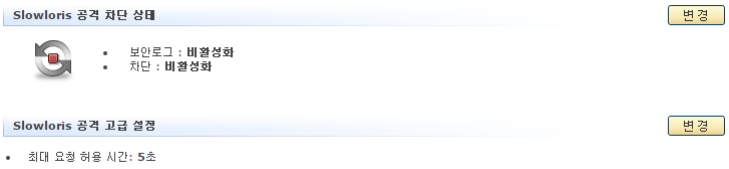
# Slowloris 공격 차단 기능 설정

Slowloris 공격 차단은 HTTP 헤더를 느리게 전송하여 세션을 장시간 유지하는 DoS 공격을 방어하기 위한 기능입니다. 이 절에서는 Slowloris 공격 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, Slowloris 공격 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **Slowloris 공격차단** 메뉴를 클릭하면 Slowloris 공격 차단 기능을 설정할 수 있는 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **Slowloris 공격 차단 상태** — Slowloris 공격 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. Slowloris 공격 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **Slowloris 공격 고급 설정** — Slowloris 공격 차단 기능의 최대 요청 허용 시간이 표시됩니다.

### 설정 과정

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

❶ Slowloris 공격 차단 기능 설정

최대 요청 허용 시간을 지정합니다. WEBFRONT-K는 최대 요청 허용 시간을 초과한 패킷에 대해 Slowloris 공격으로 판단합니다. 기본적으로 최대 요청 허용 시간은 5초로 지정되어 있습니다.

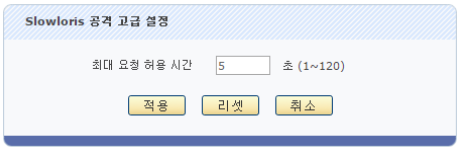
❷ Slowloris 공격 차단 기능의 활성화 상태 설정

Slowloris 공격 차단 기능의 사용 여부와 이 기능에 대한 보안로그, 차단 기능의 사용 여부를 지정합니다. 기본적으로 모두 비활성화되어 있습니다.

# Slowloris 공격 차단 설정하기

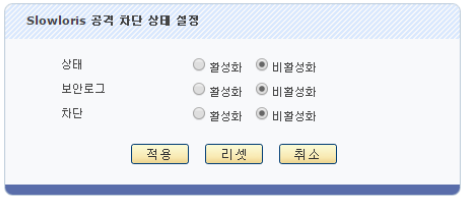
## Slowloris 공격 고급 설정

Slowloris 공격 차단 기능의 최대 요청 허용 시간을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **Slowloris 공격차단** 메뉴를 클릭합니다. |
| 2 | <**Slowloris 공격 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**Slowloris 공격 고급 설정**> 팝업 창에서 최대 요청 허용 시간을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **최대 요청 허용 시간** 요청을 허용할 시간을 지정합니다. 지정한 시간을 초과하여 요청이 지속되는 경우, 해당 요청을 Slowloris 공격으로 간주합니다. (설정 범위: 1 ~ 120, 기본값: 5(초)) |

## 관련 기능의 활성화 상태 설정

Slowloris 공격 차단 기능의 사용 여부와 Slowloris 공격 차단 기능과 관련된 보안 로그, 차단 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **Slowloris 공격차단** 메뉴를 클릭합니다. |
| 2 | <**Slowloris 공격 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**Slowloris 공격 차단 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** Slowloris 공격 차단 기능의 활성화 여부를 지정합니다.<br>• **보안 로그** Slowloris 공격 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** Slowloris 공격 차단 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다. |

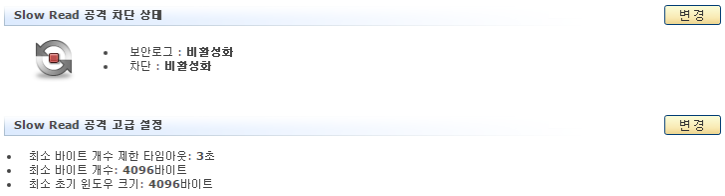
# Slow Read 공격 차단 기능 설정

Slow Read 공격 차단은 매우 작은 수신 버퍼를 사용하여 웹 서버의 데이터를 천천히 읽음으로써 자원을 고갈시키는 HTTP Slow Read 공격을 차단하는 기능입니다. 이 절에서는 Slow Read 공격 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, Slow Read 공격 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **Slow Read 공격차단** 메뉴를 클릭하면 Slow Read 차단 기능을 설정할 수 있는 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **Slow Read 공격 차단 상태** : Slow Read 공격 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. Slow Read 공격 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **Slow Read 공격 고급 설정** : 최소 바이트 개수 제한 타임아웃, 최소 바이트 개수, 최소 초기 윈도우 크기가 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. Slow Read 공격 차단 기능을 설정하는 과정은 다음과 같습니다.

❶ Slow Read 공격 차단 고급 설정

최소 바이트 개수 제한 타임아웃, 최소 바이트 개수, 최소 초기 윈도우 크기를 지정합니다. 최소 바이트 개수 제한 타임아웃 시간동안 최소 바이트 개수로 지정한 값보다 작은 양의 데이터를 전송받을 경우, Slow Read 공격으로 간주합니다. 또한 최초 연결 시, 윈도우 크기가 지정한 최소 초기 윈도우 크기보다 작을 경우에도 공격으로 간주합니다.

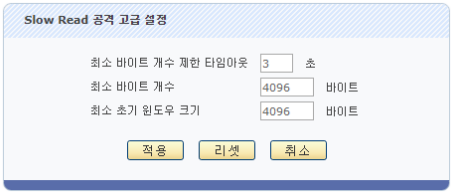
❷ Slow Read 공격 차단 기능과 관련 기능의 활성화 상태 설정

Slow Read 공격 차단 기능의 사용 여부와 Slow Read 공격 차단 기능과 관련된 보안로그, 차단 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# Slow Read 공격 차단 설정하기

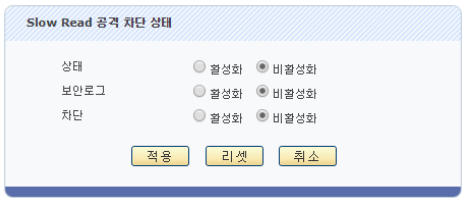
## Slow Read 공격 고급 설정

Slow Read 공격 차단 기능의 최대 요청 허용 시간을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **Slow Read 공격차단** 메뉴를 클릭합니다. |
| 2 | <**Slow Read 공격 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**Slow Read 공격 고급 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **최소 바이트 개수 제한 타임아웃** Slow Read 공격 여부를 판단하기 위한 제한 타임아웃 시간을 지정합니다. (설정 범위: 1 ~ 60, 기본값: 3)<br>• **최소 바이트 개수** 최소 바이트를 지정합니다. 제한 타임아웃 동안 최소 바이트 값보다 적은 양의 데이터를 전송하는 경우, 공격으로 간주합니다. (설정 범위: 1 ~ 65535, 기본값: 4096)<br>• **최소 초기 윈도우 크기** 최초 연결 시에 Slow Read 공격 여부를 판단하기 위한 윈도우 크기를 지정합니다. (설정 범위: 1 ~ 65535, 기본값: 4096) |

## 관련 기능의 활성화 상태 설정

Slow Read 공격 차단 기능의 사용 여부, 보안 로그, 차단 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **Slow Read 공격차단** 메뉴를 클릭합니다. |
| 2 | <**Slow Read 공격 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**Slow Read 공격 차단 상태**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** Slow Read 공격 차단 기능의 활성화 여부를 지정합니다.<br>• **보안 로그** Slow Read 공격 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** Slow Read 공격 차단 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다. |

# 금칙어 차단 기능 설정

금칙어 차단은 클라이언트가 웹 서버로 보내는 폼 필드의 문자열에 욕설, 비방, 광고, 선정적 내용 등이 포함되어있는지를 검사하는 기능입니다. 이 절에서는 금칙어 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 금칙어 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **금칙어차단** 메뉴를 클릭하면 금칙어 차단 기능을 설정할 수 있는 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **금칙어 차단 상태** — 금칙어 차단 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 금칙어 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **금칙어 차단 예외 URL 리스트** — 금칙어 차단 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

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

❶ 금칙어 차단 시그니처 설정
금칙어 삽입을 검사하기 위한 금칙어 시그니처를 지정합니다. WEBFRONT-K는 요청 패킷의 폼 필드에 지정한 시그니처가 포함되었는지를 검사하여, 지정한 시그니처가 폼 필드에 포함된 경우에는 금칙어가 삽입된 것으로 판단합니다. 금칙어 차단 시그니처는 **System** - **애플리케이션** - **시그니처 관리** 메뉴에서 설정할 수 있습니다.

❷ 금칙어 차단 검사 예외 URL 설정
금칙어 차단 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

❸ 관련 기능의 활성화 상태 설정
금칙어 차단 기능의 사용 여부와 이 기능에 대한 통계 기능의 사용 여부를 지정합니다. 기본적으로 모두 비활성화되어 있습니다.

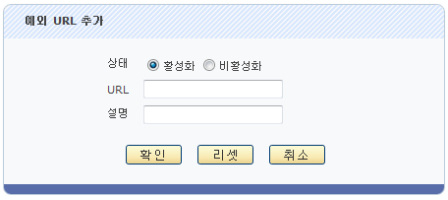
# 금칙어 차단 설정하기

## 금칙어 차단 시그니처 설정

금칙어 차단 시그니처는 **System - 애플리케이션 - 시그니처 관리** 메뉴에서 설정합니다. 시그니처를 등록하는 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 **[제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정, 사용자 정의 시그니처 설정하기]** 부분을 참고합니다.

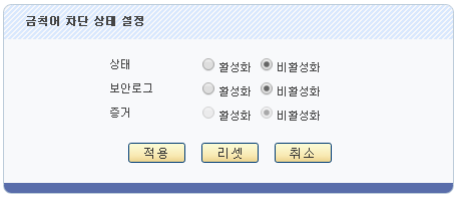
## 금칙어 차단 예외 URL 설정

금칙어 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **금칙어차단** 메뉴를 클릭합니다. |
| 2 | <**금칙어 차단 예외 URL 리스트**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 추가할 예외 URL을 사용할지 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 금칙어차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 상태 항목에서 등록한 예외 URL의 활성화 여부를 지정합니다. (기본값: 비활성화) |
| 5 | 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

금칙어 차단 기능의 사용 여부와 금칙어 차단 기능과 관련된 통계 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **금칙어차단** 메뉴를 클릭합니다. |
| 2 | <**금칙어 차단 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**금칙어 차단 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 금칙어 차단 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 금칙어 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** 금칙어 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보(시간, 클라이언트, URL, 공격 유형 등)만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안로그**의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

**참고:** 금칙어 차단 기능의 차단 설정은 각 시그니처 설정에 따라 적용됩니다. 시그니처 액션 설정 방법은 이 설명서와 함께 제공되는 '**시스템 구성 설명서**'의 [**제4장 애플리케이션 - 시그니처 관리 - 시그니처 액션 설정**] 부분을 참고합니다.

# 신용카드 정보 유입 차단 기능 설정

신용카드 정보 유입 차단 기능은 클라이언트가 웹 서버로 보내는 내용에 신용카드 정보가 포함되었는지 검사하여, 포함된 경우에 이를 차단하는 기능입니다. 이 절에서는 신용카드 정보 유입 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 신용카드 정보 유입 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **신용카드정보유입차단** 메뉴를 클릭하면 신용카드 정보 유입 차단 기능 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **신용카드 정보 유입 차단** 신용카드 정보 유입 차단의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 신용카드 정보 유입 차단의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **검사 URL 리스트** 신용카드 정보 유입 차단 기능을 적용할 URL이 표시됩니다.
- **예외 URL 리스트** 신용카드 정보 유입 차단 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 신용카드 정보 유입 차단 기능을 설정하는 과정은 다음과 같습니다.

❶ 신용카드 정보 유입 차단 검사 URL 설정
신용카드 정보 유입 차단 기능을 적용할 URL을 지정합니다. 기본적으로 지정된 검사 URL은 없습니다.

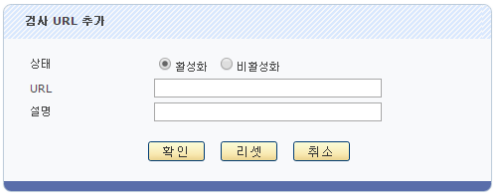
❷ 신용카드 정보 유입 차단 예외 URL 설정
신용카드 정보 유입 차단 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

❸ 신용카드 정보 유입 차단 기능과 관련 기능의 활성화 상태 설정
신용카드 정보 유입 차단 기능의 사용 여부와 신용카드 정보 유입 차단 기능과 관련된 로그, 차단, 증거 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# 신용카드 정보 유입 차단 설정하기

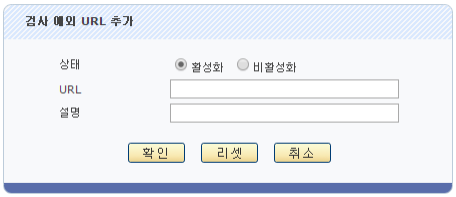
## 신용카드 정보 유입 차단 검사 URL 설정

신용카드 정보 유입 차단 기능을 적용할 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 검사 URL을 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **신용카드 정보 유입 차단** 메뉴를 클릭합니다. |
| 2 | <**검사 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**검사 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 현재 등록하고 있는 URL에 대해 신용카드 정보 유입 차단 기능을 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** 신용카드 정보 유입 차단 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있고, 반드시 '/'로 시작해야 합니다. 예외 URL 리스트에 설정된 URL은 검사 URL로 설정할 수 없습니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |

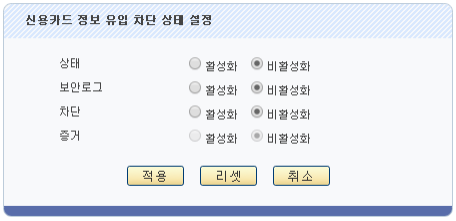
## 신용카드 정보 유입 차단 예외 URL 설정

신용카드 정보 유입 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 예외 URL을 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **신용카드 정보 유입 차단** 메뉴를 클릭합니다. |
| 2 | <**검사 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**검사 예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 추가할 예외 URL의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 신용카드 정보 유입 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다. 신용카드 정보 유입 검사 URL에 설정된 URL은 예외 URL로 설정할 수 없습니다.<br>• **설명** 예외 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 신용카드 정보 유입 차단 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

신용카드 정보 유입 차단 기능의 사용 여부와 신용카드 정보 유입 차단 기능과 관련된 보안 로그, 차단, 증거 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **신용카드 정보 유입 차단** 메뉴를 클릭합니다. |
| 2 | <**신용카드 정보 유입 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**신용카드 정보 유입 차단 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 신용카드 정보 유입 차단 기능의 활성화 여부를 지정합니다.<br>• **보안 로그** 신용카드 정보 유입 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 신용카드 정보 유입 차단 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다.<br>• **증거** 신용카드 정보 유입 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 판단의 근거가 되는 정보를 기록합니다. 로그의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

# 주민등록 정보 유입 차단 기능 설정

주민등록 정보 유입 차단 기능은 클라이언트가 웹 서버로 보내는 내용에 주민등록 정보가 포함되었는지 검사하여, 포함된 경우에 이를 차단하는 기능입니다. 이 절에서는 주민등록 정보 유입 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 주민등록 정보 유입 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **주민등록정보유입차단** 메뉴를 클릭하면 주민등록 정보 유입 차단 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **주민등록번호 유입 차단** 주민등록 정보 유입 차단의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 주민등록 정보 유입 차단의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **검사 URL 리스트** 주민등록 정보 유입 차단 기능을 적용할 URL이 표시됩니다.
- **예외 URL 리스트** 주민등록 정보 유입 차단 기능에서 제외할 URL이 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 주민등록 정보 유입 차단을 설정하는 과정은 다음과 같습니다.

❶ 주민등록 정보 유입 차단 검사 URL 설정
주민등록 정보 유입 차단 기능을 적용할 URL을 지정합니다. 기본적으로 지정된 검사 URL은 없습니다.

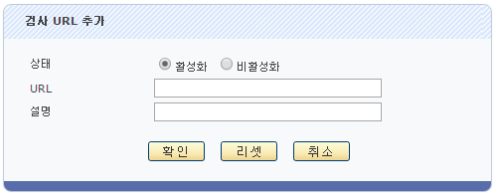
❷ 주민등록 정보 유입 차단 예외 URL 설정
주민등록 정보 유입 차단 기능에서 제외할 예외 URL을 지정합니다. 기본적으로 지정된 예외 URL은 없습니다.

❸ 주민등록 정보 유입 차단 기능과 관련 기능의 활성화 상태 설정
주민등록 정보 유입 차단 기능의 사용 여부와 주민등록 정보 유입 차단 기능과 관련된 로그, 차단, 증거 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# 주민등록 정보 유입 차단 설정하기

## 주민등록 정보 유입 차단 검사 URL 설정

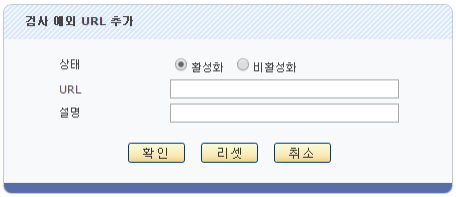
주민등록 정보 유입 차단 기능을 적용할 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 검사 URL을 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **주민등록 정보 유입 차단** 메뉴를 클릭합니다. |
| 2 | <**검사 URL 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**검사 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 URL에 대해 주민등록 정보 유입 차단 기능을 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** 주민등록 정보 유입 차단 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있고, 반드시 '/'로 시작해야 합니다. 예외 URL 리스트에 설정된 URL은 검사 URL로 설정할 수 없습니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |



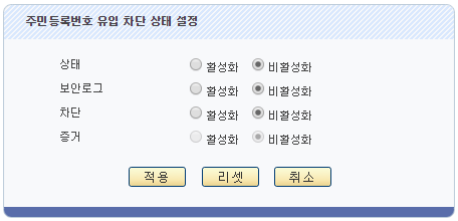
## 주민등록 정보 유입 차단 예외 URL 설정

주민등록 정보 유입 차단 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 최대 256개의 예외 URL을 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **주민등록 정보 유입 차단** 메뉴를 클릭합니다. |
| 2 | <**검사 리스트**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 4 | <**검사 예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 추가할 예외 URL의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **URL** 주민등록 정보 유입 차단 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 됩니다. 주민등록 정보 유입 검사 URL에 설정된 URL은 예외 URL로 설정할 수 없습니다.<br>• **설명** 예외 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 주민등록 정보 유입 차단 예외 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

주민등록 정보 유입 차단 기능의 사용 여부와 주민등록 정보 유입 차단 기능과 관련된 보안 로그, 차단, 증거 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** – **주민등록 정보 유입 차단** 메뉴를 클릭합니다. |
| 2 | <**주민등록번호 유입 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**주민등록번호 유입 차단 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 주민등록 정보 유입 차단 기능의 활성화 여부를 지정합니다.<br>• **보안 로그** 주민등록 정보 유입 차단 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 주민등록 정보 유입 차단 정책을 위반한 요청 패킷을 차단할 것인지 지정합니다.<br>• **증거** 주민등록 정보 유입 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 판단의 근거가 되는 정보를 기록합니다. 로그의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

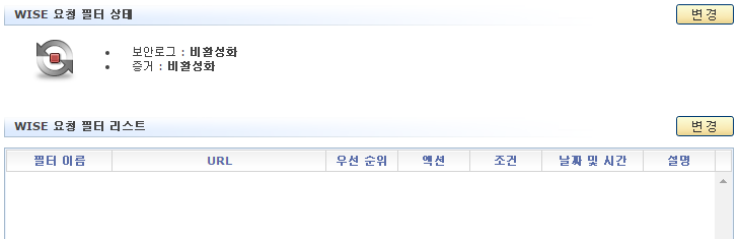
# WISE 요청 필터 설정

WISE(Web Insight Security Enforcement) 요청 필터는 클라이언트가 웹 서버로 보내는 요청 패킷에 대한 항목, 변수, 값, 조건 등 필터의 규칙을 세부적으로 설정하여 요청 패킷을 필터링하는 기능입니다. 이 절에서는 WISE 요청 필터를 설정하는 화면과 설정하는 과정에 대해 살펴본 후, WISE 요청 필터를 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **요청검사** - **WISE 요청필터** 메뉴를 클릭하면 WISE 요청 필터 설정 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **WISE 요청 필터 상태** WISE 요청 필터의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. WISE 요청 필터의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **WISE 요청 필터 리스트** 현재 설정된 WISE 요청 필터의 목록이 표시됩니다.

### 설정 과정

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

❶ WISE 요청 필터 설정

먼저 WISE 요청 필터를 정의합니다. 필터를 정의할 때는 필터의 이름, 활성화 상태, 필터링할 URL, 필터링된 요청 패킷의 처리 방법, 우선 순위 등을 설정합니다. 기본적으로 정의된 WISE 요청 필터는 없습니다. 필터를 정의한 후에는 데이터 유형, 변수, 값, 비교 방법 등 요청 패킷에 대한 필터링 조건을 설정합니다. 기본적으로는 아무런 필터링 조건도 설정되어 있지 않습니다.

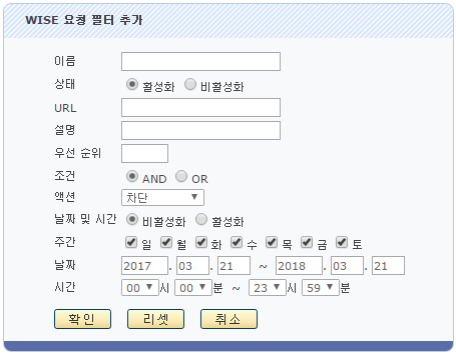
❷ 관련 기능의 활성화 상태 설정

WISE 요청 필터의 사용 여부와 이 기능에 대한 보안 로그, 증거 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# WISE 요청 필터 설정하기

## WISE 요청 필터 추가

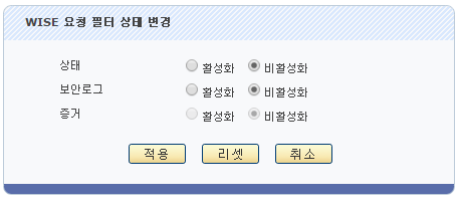
다음과 같은 방법으로 WISE 요청 필터를 정의하고, 필터링 조건을 설정합니다. 하나의 애플리케이션에는 WISE 요청 필터를 1024개까지 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **WISE 요청필터** 메뉴를 클릭합니다. |
| 2 | <**WISE 요청 필터 리스트**>의 [**변경**] - [**필터추가**] 버튼을 클릭합니다. |
| 3 | <**WISE 요청 필터 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **이름** WISE 요청 필터의 이름을 입력합니다. 이름은 알파벳과 숫자로 이루어진 최대 32 글자의 문자열로 지정할 수 있으며, 'filter'는 사용할 수 없습니다.<br>• **상태** 등록하고 있는 WISE 요청 필터를 활성화할 것인지 지정합니다. (기본값: 활성화)<br>• **URL** WISE 요청 필터를 통해 필터링을 수행할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/' 이어야 됩니다.<br>• **설명** WISE 요청 필터 또는 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>• **우선 순위** 현재 등록하고 있는 WISE 요청 필터의 우선 순위를 입력합니다. 우선 순위는 하나의 URL에 대해 여러 개의 WISE 요청 필터가 정의되어 있는 경우, 어떤 필터를 먼저 적용할지 결정할 때 사용됩니다. 우선 순위의 값의 범위는 1~1024이고, 숫자가 작을 수록 우선 순위가 높습니다.<br>• **조건** 검사항목의 만족 조건을 선택합니다. (기본값: AND)<br>– AND: 모든 검사항목을 만족할 경우 해당 요청에 대해 액션을 수행합니다.<br>– OR: 검사항목 중 한 가지 이상 만족할 경우 해당 요청에 대해 액션을 수행합니다.<br>• **액션** 드롭다운 목록을 클릭하여, 현재 등록하고 있는 WISE 요청 필터에 매치된 URL 요청 패킷을 처리할 방법을 선택합니다. 처리 방법에는 차단, 통과, 무로그 통과, 검사, 무로그 검사가 있습니다. (기본값: 차단)<br>– 차단: 해당 요청을 차단합니다.<br>– 통과: 해당 요청을 웹 서버로 전송합니다.<br>– 무로그 통과: '통과'와 액션은 동일하지만 로그는 생성하지 않습니다.<br>– 검사: 해당 요청을 임의로 차단하거나 통과시키지 않고 보안 기능 검사를 수행합니다.<br>– 무로그 검사: '검사'와 액션은 동일하지만 로그는 생성하지 않습니다.<br>• **날짜 및 시간** WISE 요청 필터가 특정 날짜 및 시간에만 동작하도록 할 것인지 지정합니다. (기본값: 비활성화)<br>• **주간** WISE 요청 필터가 동작할 요일 지정<br>• **날짜** WISE 요청 필터가 동작할 연도, 월, 일 지정<br>• **시간** WISE 요청 필터가 동작할 시간, 분 단위 지정 |
| 4 | 추가한 요청 필터의 필터링 조건을 설정하기 위해 필터를 선택한 후 [**검사항목추가**] 버튼을 클릭합니다. 하나의 필터에 최대 16개의 필터링 조건을 추가할 수 있습니다. |
| 5 | <**WISE 요청 필터 검사 항목 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **데이터 형식** WISE 요청 필터 기능을 통해 패킷의 어떤 부분을 검사할 것인지를 지정합니다. 검사할 수 있는 패킷의 부분(데이터 |

| | |
|---|---|
| | 유형)에는 쿠키, 메서드, 헤더, 매개변수, IP 주소, 시그니처 ID 등 6가지가 있습니다. 시그니처 ID를 선택한 경우에는 팝업창 아래 부분에 시그니처 리스트가 나타납니다. (기본값: 매개변수)<br>• **변수** 데이터 형식을 쿠키, 헤더, 매개변수를 선택한 경우에는 해당되는 변수를 입력합니다. 변수는 알파벳, 숫자와 '-' 기호로 이루어진 최대 256자의 문자열로 지정할 수 있습니다. 메서드나 IP 주소를 선택한 경우에는 이 항목을 입력하지 않습니다. 매개변수를 선택한 경우 '*'를 사용하여 해당 URL의 모든 매개변수를 설정할 수 있습니다.<br>• **조건** 드롭다운 목록을 클릭하여 설정한 데이터 형식의 값과 요청 패킷의 해당 데이터 형식의 값을 비교할 조건을 선택합니다. (기본값: 같음)<br>– 같음: 해당 데이터 형식의 값이 값 항목에 설정한 값과 일치하는지 검사합니다.<br>– 포함: 해당 데이터 형식의 값이 값 항목에 설정한 값을 포함하는지 검사합니다.<br>– 포함하지 않음: 해당 데이터 형식의 값이 값 항목에 설정한 값을 포함하지 않았는지 검사합니다.<br>– 정규식: 해당 데이터 형식의 값이 값 항목에 설정한 정규식과 일치하는지 검사합니다.<br>– 매개변수가 존재함: 해당 데이터 형식의 변수가 존재하는지 검사합니다.<br>– 매개변수가 존재하지 않음: 해당 데이터 형식의 변수가 존재하지 않는지 검사합니다.<br>– 값이 존재하지 않음: 해당 데이터 유형의 값이 존재하지 않는지 검사합니다.<br>데이터 형식 항목에서 선택한 유형에 따라 드롭다운 목록에 나타나는 조건이 달라집니다. 쿠키나 헤더, 매개변수를 선택한 경우에는 위의 모든 비교 조건 중에서 선택할 수 있고, 메서드를 선택하면 같음, 포함, 포함하지 않음, 정규식 중에서 선택할 수 있습니다. IP 주소를 선택한 경우에는 포함과 포함하지 않음 중에서만 선택할 수 있습니다.<br>데이터 형식 항목에서 시그니처 ID를 선택한 경우에는 버퍼오버플로우 - 쉘코드 검사, SQL 삽입 차단, SQL 삽입 차단-논리 연산 차단, 스크립트 삽입 차단, 업로드 검사-파일 확장자, 업로드 검사-파일 내용, 다운로드 검사, 인클루드 인젝션 차단을 선택할 수 있습니다. 선택한 항목에 따라 팝업 창 아래 부분의 시그니처 리스트가 변경됩니다.<br>• **값** 데이터 형식의 값을 입력합니다. 변수가 존재하는 데이터 형식의 경우에는 변수에 해당하는 값을 입력합니다.<br>데이터 형식 항목에서 시그니처 ID를 선택한 경우에는 값을 직접 입력하지 않고 시그니처 리스트에서 선택합니다. 시그니처는 하나만 선택할 수 있습니다. |
| 6 | WISE 요청 필터를 모두 추가하였으면 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

WISE 요청 필터 기능의 사용 여부와 WISE 요청 필터 기능과 관련된 로그, 증거 등 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **WISE 요청필터** 메뉴를 클릭합니다. |
| 2 | <**WISE 요청 필터 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**WISE 요청 필터 상태 변경**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** WISE 요청 필터 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** WISE 요청 필터 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** WISE 요청 필터 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

# 제4장 컨텐트 보호 기능 설정

컨텐트 보호는 WEBFRONT-K가 웹 서버에서 클라이언트로 보내는 응답 메시지를 검사하여, 응답 메시지에 기밀 정보를 포함하고 있거나, 응답 웹이 변조된 경우에 대응하는 조치를 취하도록 하는 응답 검사 기능입니다. 이 장에서는 WEBFRONT-K에서 제공하는 각 컨텐트 보호 기능을 설정하는 방법에 대해 상세하게 소개합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 신용카드 정보 유출 차단 기능 설정
- 주민등록 정보 유출 차단 기능 설정
- 계좌번호 유출 차단 기능 설정
- 웹 변조 방지 기능 설정
- 응답 형식 검사 기능 설정
- 코드 노출 차단 기능 설정
- WISE 컨텐트 필터 설정

**참고:** 컨텐트 보호 기능에 대한 상세한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제3장 WEBFRONT-K 웹 보안 기능 – 컨텐트 보호(Content Protection)**] 부분을 참고합니다.

# 신용카드 정보 유출 차단 기능 설정

신용카드 정보 유출 차단 기능은 클라이언트로 보내는 응답에 신용카드 정보가 포함되었는지 검사하여, 포함된 경우에는 이를 특정 문자로 변환한 후 전송하거나 응답을 차단하는 기능입니다. 이 절에서는 신용카드 정보 유출 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 신용카드 정보 유출 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **컨텐트보호** - **신용카드정보유출차단** 메뉴를 클릭하면 신용카드 정보 유출 차단 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **신용카드 정보 유출 차단** : 신용카드 정보 유출 차단 기능의 활성화 상태와 보안 로그 등 관련 기능의 활성화 상태가 표시됩니다. 신용카드 정보 유출 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **신용카드 정보 보호 방법** : 현재 설정되어 있는 신용카드 정보 보호 방법에 대한 설정 정보가 표시됩니다.
- **검사 URL 리스트** : 신용카드 정보 유출 차단 기능을 적용할 URL의 목록이 출력됩니다.
- **예외 URL 리스트** : 신용카드 정보 유출 차단 기능에서 제외할 URL의 목록이 출력됩니다.
- **파일 차단** : 신용카드 정보 보호의 파일 차단에 대한 설정 정보가 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 신용카드 정보 유출 차단 기능을 설정하는 과정은 다음과 같습니다.

❶ 신용카드 정보 보호 방법 설정
웹 서버가 클라이언트로 보내는 응답 패킷에 신용카드 정보가 포함된 경우 해당 정보를 처리할 방법을 설정합니다. 기본적으로 정보 보호 방법은 탐지로 설정되어 있습니다.

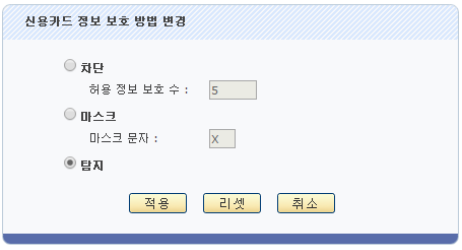
❷ 검사 URL 설정
신용카드 정보 유출 차단 기능을 적용할 검사 URL을 등록합니다. 기본적으로 등록된 URL은 없습니다.

❸ 관련 기능의 활성화 상태 설정
신용카드 정보 유출 차단 기능의 사용 여부와 이 기능에 대한 보안 로그 및 파일 차단 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# 신용카드 정보 유출 차단 설정하기

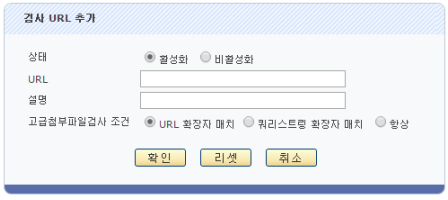
## 신용카드 정보 보호 방법 설정

다음과 같은 방법으로 신용카드 정보 보호 방법을 설정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **신용카드정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**신용카드 정보 보호 방법**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**신용카드 정보 보호 방법 변경**> 팝업 창에서 다음 설명을 참고하여 신용카드 정보가 포함된 응답을 처리할 방법을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br>• **차단** 신용카드 정보를 포함한 응답은 허용 정보 보호 수 항목에서 설정한 개수만큼만 허용되고, 이 개수를 초과하는 패킷은 차단합니다. 허용 정보 보호 수 항목에는 허용할 개수를 입력합니다. (설정 범위: 0 ~ 1024, 기본값: 5)<br>• **마스크** 신용카드 정보를 포함한 응답은 신용카드 정보에서 마지막 4개의 문자를 마스크 문자 항목에서 지정한 문자로 바꾼 후 전송합니다.<br>마스크 문자 항목에는 신용카드 정보를 대체할 문자를 입력합니다. 하나의 문자만 입력할 수 있으며, 알파벳, 숫자와 특수 문자를 모두 입력할 수 있습니다. (기본값: X)<br>• **탐지** 신용카드 정보를 포함한 응답을 모두 허용하고 보안 로그를 기록합니다. |

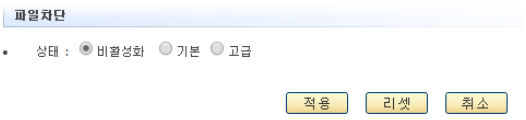
## 검사 URL 설정

신용카드 시그니처를 설정한 후에는 다음과 같은 방법으로 신용카드 정보 유출 차단 기능을 적용할 검사 URL을 등록합니다. 검사 URL은 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **신용카드정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**검사 URL 리스트**>의 [**변경**] – [**추가**]버튼을 클릭합니다. |
| 3 | <**검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 검사 URL을 실제로 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** 검사 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>• **고급첨부파일검사 조건**<br>- **URL 확장자 매치** URL이 **[파일차단 > 고급]** 메뉴에서 설정한 파일 확장자로 끝나는 경우에 검사<br>- **쿼리스트링 확장자 매치** URL 또는 쿼리스트링 값 부분이 **[파일차단 > 고급]** 메뉴에서 설정한 파일 확장자로 끝나는 경우에 검사<br>- **항상** 검사 URL로 설정된 URL을 항상 검사 |
| 4 | 설정 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

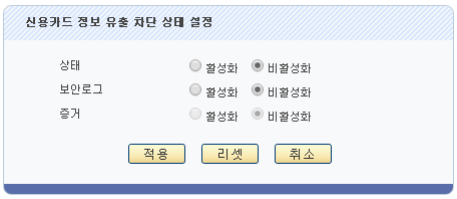
### 파일 차단

파일 차단은 클라이언트가 요청한 파일의 내용 중에 신용카드 정보가 포함되어 있을 경우 해당 응답을 차단하는 기능입니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **신용카드정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**파일 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**파일 차단**>에서 기능의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 파일 차단 상태는 비활성화되어 있습니다.<br>  <br><br>• **비활성화** 파일 차단 기능을 비활성화합니다. (기본값)<br>• **기본** doc, ppt, xls, hwp 파일에 신용카드 정보가 포함되어 있을 경우, 해당 응답을 차단합니다.<br>• **고급** 여러 가지 종류의 파일 확장자 중에서 검사할 확장자를 지정합니다. 지정 리스트의 파일 확장자를 선택한 후, **[추가]** 버튼을 클릭하면 검사 리스트로 이동합니다. |

### 관련 기능의 활성화 상태 설정

신용카드 정보를 등록하고 검사 URL을 설정하고 나면 다음과 같은 방법으로 신용카드 정보 유출 차단 기능의 사용 여부와 신용카드 정보 유출 차단 기능과 관련된 보안 로그, 증거 기능의 활성화 상태를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **신용카드정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**신용카드 정보 유출 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**신용카드 정보 유출 차단 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 신용카드 정보 유출 차단 기능의 사용 여부를 지정합니다.<br>• **보안 로그** 신용카드 정보 유출 차단 기능에 의해 정보가 차단될 때 관련 정보를 로그로 기록할 것인지를 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합 로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** 신용카드 정보 유출 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 판단의 근거가 되는 정보를 기록합니다. 로그의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합 로그**] 메뉴에서 확인할 수 있습니다. |

# 주민등록 정보 유출 차단 기능 설정

주민등록 정보 유출 차단 기능은 웹 서버가 클라이언트로 보내는 응답에 주민등록 정보가 포함되었는지 검사하여, 포함된 경우에는 이를 특정 문자로 변환한 후 전송하거나 응답을 차단하는 기능입니다. 이 절에서는 주민등록 정보 유출 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 주민등록 정보 유출 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **컨텐트보호** - **주민등록정보유출차단** 메뉴를 클릭하면 주민등록 정보 유출 차단 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **주민등록번호 정보 유출 차단** — 주민등록 정보 유출 차단 기능의 활성화 상태와 보안 로그 등 관련 기능의 활성화 상태가 표시됩니다. 주민등록 정보 유출 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **주민등록 번호 정보 보호 방법** — 현재 설정되어 있는 주민등록번호 정보 보호 방법에 대한 설정 정보가 표시됩니다.
- **검사 URL 리스트** — 주민등록 정보 유출 차단 기능을 적용할 URL 목록이 표시됩니다.
- **예외 URL 리스트** — 주민등록 정보 유출 차단 기능에서 제외할 URL의 목록이 표시됩니다.
- **파일차단** — 주민등록 정보 보호의 파일 차단에 대한 설정 정보가 표시됩니다.

### 설정 과정

앞의 설정 화면에서 각 부분의 [**변경**] 버튼을 클릭하면 해당 기능을 설정할 수 있습니다. 주민등록 정보 유출 차단 기능을 설정하는 과정은 다음과 같습니다.

❶ 주민등록번호 정보 보호 방법 설정
웹 서버가 클라이언트로 보내는 응답 패킷에 주민등록번호 정보가 포함된 경우 해당 정보를 처리할 방법을 설정합니다. 기본적으로 정보 보호 방법은 탐지로 설정되어 있습니다.

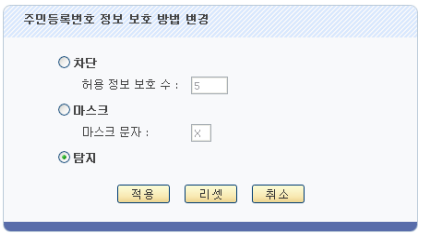
❷ 검사 URL 설정
주민등록 정보 유출 차단 기능을 적용할 검사 URL을 등록합니다. 기본적으로 등록된 URL은 없습니다.

❸ 관련 기능의 활성화 상태 설정
주민등록 정보 유출 차단 기능의 사용 여부와 이 기능에 대한 보안 로그 및 파일 차단 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# 주민등록 정보 유출 차단 설정하기

## 주민등록 정보 처리 방법 설정

다음과 같은 방법으로 주민등록 정보 처리 방법을 설정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **주민등록정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**주민등록번호 정보 보호 방법**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**주민등록번호 정보 보호 방법 변경**> 팝업 창에서 다음 설명을 참고하여 주민등록번호 정보가 포함된 응답을 처리할 방법을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **차단** 주민등록번호 정보를 포함한 응답은 허용 정보 보호 수 항목에서 설정한 개수만큼만 허용되고, 이 개수를 초과하는 패킷은 차단합니다. 허용 정보 보호 수 항목에는 허용할 개수를 입력합니다. (설정 범위: 0 ~ 1024, 기본값: 5)<br>• **마스크** 주민등록번호 정보를 포함한 응답은 주민등록번호 정보에서 마지막 7개의 문자를 마스크 문자 항목에서 지정한 문자로 바꾼 후 전송합니다.<br>마스크 문자 항목에는 주민등록번호 정보를 대체할 문자를 입력합니다. 하나의 문자만 입력할 수 있으며, 알파벳, 숫자와 특수 문자를 모두 입력할 수 있습니다. (기본값: X)<br>• **탐지** 주민등록번호 정보를 포함한 응답을 모두 허용하고 보안 로그를 기록합니다. |

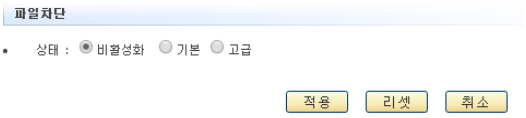
## 검사 URL 설정

주민등록 정보를 설정한 후에는 다음과 같은 방법으로 주민등록 정보 유출 차단 기능을 적용할 검사 URL을 등록합니다. 검사 URL은 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **주민등록정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**검사 URL 리스트**>의 [**변경**] – [**추가**]버튼을 클릭합니다. |
| 3 | <**검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 현재 등록하고 있는 검사 URL을 실제로 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** 검사 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 설정 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

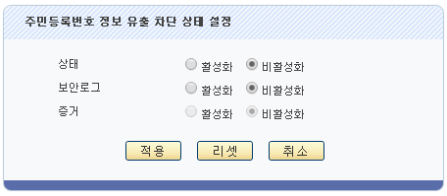
## 파일 차단

파일 차단은 클라이언트가 요청한 파일의 내용 중에 주민등록 정보가 포함되어 있을 경우 해당 응답을 차단하는 기능입니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **주민등록정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**파일 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**파일 차단**>에서 기능의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 파일 차단 상태는 비활성화되어 있습니다.<br>  <br><br>• **비활성화** 파일 차단 기능을 비활성화합니다. (기본값)<br>• **기본** doc, ppt, xls, hwp 파일에 주민등록 정보가 포함되어 있을 경우, 해당 응답을 차단합니다.<br>• **고급** 여러 가지 종류의 파일 확장자 중에서 검사할 확장자를 지정합니다. 지정 리스트의 파일 확장자를 선택한 후, **[추가]** 버튼을 클릭하면 검사 리스트로 이동합니다. |

## 관련 기능의 활성화 상태 설정

주민등록번호 시그니처와 검사 URL을 설정하고 나면, 다음과 같은 방법으로 주민등록 정보 유출 차단 기능의 사용 여부와 이 기능과 관련된 보안 로그, 증거 기능의 활성화 상태를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **주민등록정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**주민등록번호 정보 유출 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**주민등록번호 정보 유출 차단 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 주민등록 정보 유출 차단 기능의 사용 여부를 지정합니다.<br>• **보안 로그** 주민등록 정보 유출 차단 기능에 의해 정보가 차단될 때 관련 정보를 로그로 기록할 것인지를 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합 로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** 주민등록 정보 유출 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 판단의 근거가 되는 정보를 기록합니다. 로그의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합 로그**] 메뉴에서 확인할 수 있습니다. |

# 계좌번호 유출 차단 기능 설정

계좌번호 유출 차단 기능은 웹 서버가 클라이언트로 보내는 응답에 계좌번호 정보가 포함되었는지 검사하여, 포함된 경우에는 이를 특정 문자로 변환한 후 전송하거나 응답을 차단하는 기능입니다. 이 절에서는 계좌번호 유출 차단 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후, 계좌번호 유출 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **컨텐트보호** - **계좌번호유출차단** 메뉴를 클릭하면 계좌번호 유출 차단 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **계좌번호 정보 유출 차단** 계좌번호 유출 차단 기능의 활성화 상태와 로그 등 관련 기능의 활성화 상태가 표시됩니다. 계좌번호 유출 차단 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **계좌번호 정보 보호 방법** 현재 설정되어 있는 계좌번호 정보 보호 방법에 대한 설정 정보가 표시됩니다.
- **검사 URL 리스트** 계좌번호 유출 차단 기능을 적용할 URL 목록이 표시됩니다.
- **예외 URL 리스트** 계좌번호 유출 차단 기능에서 제외할 URL 목록이 표시됩니다.

### 설정 과정

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

❶ 계좌번호 정보 보호 방법 설정
웹 서버가 클라이언트로 보내는 응답 패킷에 계좌번호 정보가 포함된 경우 해당 정보를 처리할 방법을 설정합니다. 기본적으로 정보 보호 방법은 탐지로 설정되어 있습니다.

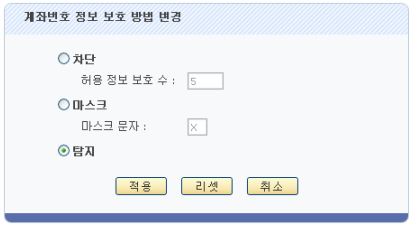
❷ 검사 URL 설정
계좌번호 유출 차단 기능을 적용할 검사 URL을 등록합니다. 기본적으로는 등록된 URL은 없습니다.

❸ 관련 기능의 활성화 상태 설정
계좌번호 유출 차단 기능의 사용 여부와 이 기능에 대한 보안 로그 및 파일 차단 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# 계좌번호 유출 차단 설정하기

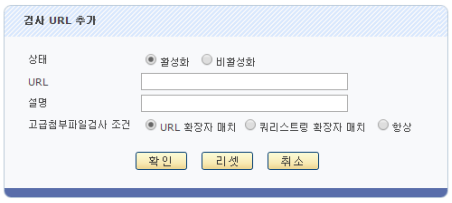
## 계좌번호 정보 처리 방법 설정

다음과 같은 방법으로 계좌번호 정보 처리 방법을 설정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **계좌번호유출차단** 메뉴를 클릭합니다. |
| 2 | <**계좌번호 정보 보호 방법**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**계좌번호 정보 보호 방법 변경**> 팝업 창에서 다음 설명을 참고하여 계좌번호 정보가 포함된 응답을 처리할 방법을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **차단** 계좌번호 정보를 포함한 응답은 허용 정보 보호 수 항목에서 설정한 개수만큼만 허용되고, 이 개수를 초과하는 패킷은 차단합니다. 허용 정보 보호 수 항목에는 허용할 개수를 입력합니다. (설정 범위: 0 ~ 1024, 기본값: 5)<br>• **마스크** 계좌번호 정보를 포함한 응답은 계좌번호 정보에서 마지막 6개의 문자를 마스크 문자 항목에서 지정한 문자로 바꾼 후 전송합니다. 마스크 문자 항목에는 계좌번호 정보를 대체할 문자를 입력합니다. 하나의 문자만 입력할 수 있으며, 알파벳, 숫자와 특수 문자를 모두 입력할 수 있습니다. (기본값: X)<br>• **탐지** 계좌번호 정보를 포함한 응답을 모두 허용하고 보안 로그를 기록합니다. |

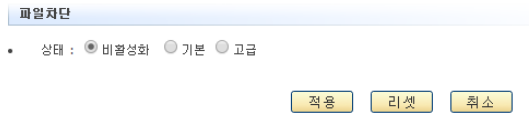
## 검사 URL 설정

계좌번호 시그니처를 설정한 후에는 다음과 같은 방법으로 계좌번호 정보 유출 차단 기능을 적용할 검사 URL을 등록합니다. 검사 URL은 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **계좌번호유출차단** 메뉴를 클릭합니다. |
| 2 | <**검사 URL 리스트**>의 [**변경**] – [**추가**]버튼을 클릭합니다. |
| 3 | <**검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 현재 등록하고 있는 검사 URL을 실제로 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** 검사 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 구성된 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>• **고급첨부파일검사 조건**<br>- **URL 확장자 매치** URL이 **[파일차단 > 고급]** 메뉴에서 설정한 파일 확장자로 끝나는 경우에 검사<br>- **쿼리스트링 확장자 매치** URL 또는 쿼리스트링 값 부분이 **[파일차단 > 고급]** 메뉴에서 설정한 파일 확장자로 끝나는 경우에 검사<br>- **항상** 검사 URL로 설정된 URL을 항상 검사 |
| 4 | 설정 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

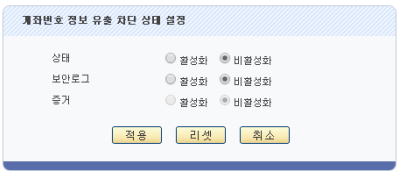
## 파일 차단

파일 차단은 클라이언트가 요청한 파일의 내용 중에 계좌번호 정보가 포함되어 있을 경우 해당 응답을 차단하는 기능입니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **계좌번호정보유출차단** 메뉴를 클릭합니다. |
| 2 | <**파일 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**파일 차단**>에서 기능의 사용 여부를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 파일 차단 상태는 비활성화되어 있습니다.<br>  <br><br>• **비활성화** 파일 차단 기능을 비활성화합니다. (기본값)<br>• **기본** doc, ppt, xls, hwp 파일에 계좌번호 정보가 포함되어 있을 경우, 해당 응답을 차단합니다.<br>• **고급** 여러 가지 종류의 파일 확장자 중에서 검사할 확장자를 지정합니다. 지정 리스트의 파일 확장자를 선택한 후, **[추가]** 버튼을 클릭하면 검사 리스트로 이동합니다. |

## 관련 기능의 활성화 상태 설정

계좌번호 정보를 등록하고 검사 URL을 설정하고 나면, 다음과 같은 방법으로 계좌번호 정보 유출 차단 기능의 사용 여부와 계좌번호 정보 유출 차단 기능과 관련된 로그, 증거 기능의 활성화 상태를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **계좌번호유출차단** 메뉴를 클릭합니다. |
| 2 | <**계좌번호 정보 유출 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**계좌번호 정보 유출 차단 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 계좌번호 유출 차단 기능의 사용 여부를 지정합니다.<br>• **보안 로그** 계좌번호 유출 차단 기능에 의해 정보가 차단될 때 관련 정보를 로그로 기록할 것인지를 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합 로그**] 메뉴에서 확인할 수 있습니다.<br>• **증거** 계좌번호 정보 유출 차단 정책을 위반한 요청 패킷에 대해 증거를 기록할 것인지 지정합니다. 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 판단의 근거가 되는 정보를 기록합니다. 로그의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합 로그**] 메뉴에서 확인할 수 있습니다. |

# 웹 변조 방지 기능 설정

웹 변조 방지 기능은 웹 페이지가 변조되는 것을 방지하기 위해 WEBFRONT-K가 웹 서버의 정보를 저장하고 있다가 클라이언트로부터 요청이 오면 웹 서버 대신 응답을 보내주는 기능입니다. 이 절에서는 웹 변조 방지 기능 설정하는 화면과 설정 과정에 대해 살펴본 후 실제로 웹 변조 방지 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **컨텐트보호** - **웹변조방지** 메뉴를 클릭하면 웹 변조 방지 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **웹변조방지** 웹 변조 방지 기능의 활성화 상태와 보안 로그 등 관련 기능의 활성화 상태가 표시됩니다. 웹 변조 방지 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고, 는 비활성화 상태를 나타냅니다.
- **웹변조방지 체크 주기** 현재 설정된 웹 체크 시간 간격이 표시됩니다.
- **웹변조방지 리스트** 현재 등록된 웹 페이지 목록이 표시됩니다.

### 설정 과정

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

❶ 웹 페이지 등록

먼저 웹 변조 방지 기능을 적용할 웹 페이지를 등록합니다. 그러면, WEBFRONT-K는 해당 웹 페이지의 내용을 웹 서버로부터 받아와서 WEBFRONT-K에 저장합니다. 이 후, 등록한 웹 페이지에 대한 요청이 클라이언트로부터 오면 WEBFRONT-K는 그 요청을 웹 서버에게 전달하는 대신 저장해둔 웹 페이지를 클라이언트에게 보냅니다. 기본적으로는 등록되어 있는 웹 페이지는 없습니다.

❷ 웹 체크 시간 간격 설정

웹 페이지가 변경되었는지를 주기적으로 확인하는 웹 체크 시간 간격을 설정합니다. WEBFRONT-K는 설정한 체크 시간 간격마다 등록된 웹 페이지가 웹 서버에서 변경되었는지를 확인하고 변경된 경우에는 기록을 남깁니다. 이 기록을 통하여 관리자에 의해 웹 페이지가 변경되었는지 아니면 공격자가 변조하였는지를 구분할 수 있습니다. 기본적으로는 5분으로 설정되어 있습니다.

❸ 관련 기능의 활성화 상태 설정

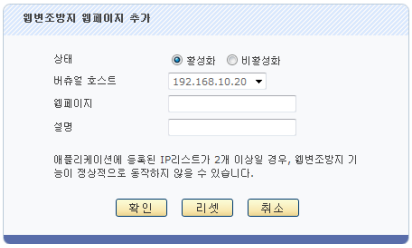
웹 변조 방지 기능의 사용 여부와 이 기능에 대한 보안 로그 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

등록된 웹 페이지는 사용자가 원할 때마다(웹 체크 시간과 무관하게) 변조 여부를 점검할 수 있고, 웹 페이지의 상세한 내용을 확인하거나 웹 페이지를 최신 내용으로 업데이트할 수 있습니다.

# 웹 변조 방지 설정하기

## 웹 페이지 등록

먼저 다음과 같은 방법으로 웹 변조 방지 기능을 적용할 웹 페이지를 등록합니다. 웹 변조 방지 기능을 적용할 웹 페이지는 최대 256개까지 등록할 수 있습니다.

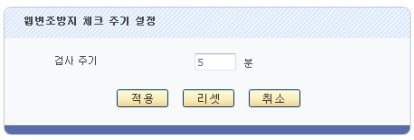
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **웹변조방지** 메뉴를 클릭합니다. |
| 2 | <**웹변조방지 리스트**>의 [**변경**] – [**추가**]버튼을 클릭합니다. |
| 3 | <**웹변조방지 웹페이지 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 웹 페이지에 대하여 웹 변조 방지 기능을 적용할 것인지를 지정합니다. (기본값: 비활성화)<br>• **버츄얼 호스트** 사용자가 등록한 웹 페이지를 서비스하는 서버의 도메인 이름을 입력합니다.<br>• **웹페이지** 웹 변조 방지 기능을 적용하려는 웹 페이지를 입력합니다. 웹 페이지는 최대 1024 글자로 된 URL 형식으로 입력합니다.<br>• **설명** 웹 페이지에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 설정 내용을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |



**참고:** 웹 변조 방지 기능은 html, txt 형식의 웹 페이지만을 지원합니다. html과 txt 이외의 형식으로 작성된 웹 페이지의 경우, 웹 변조 방지 기능이 정상적으로 동작하지 않을 수 있습니다.

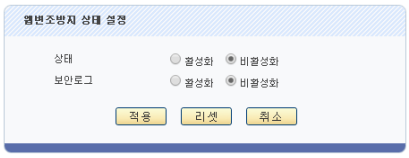
## 웹 페이지 체크 주기 설정

웹 페이지를 등록한 후에는 다음과 같은 방법으로 웹 변조 여부를 확인하는 웹 페이지 체크 주기를 설정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **웹변조방지** 메뉴를 클릭합니다. |
| 2 | <**웹변조방지 체크 주기**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**웹변조방지 체크 주기 설정**> 팝업 창에서 체크 주기 항목에 웹 체크 시간 간격을 입력한 후 [**적용**] 버튼을 클릭합니다.<br>(설정 범위: 5 ~ 1440, 기본값: 5분)<br>  |

### 관련 기능의 활성화 상태 설정

웹 페이지를 등록하고 웹 체크 시간 간격을 설정하고 나면, 다음과 같은 방법으로 웹 변조 방지 기능의 사용 여부와 로그 기능의 활성화 상태를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **웹변조방지** 메뉴를 클릭합니다. |
| 2 | <**웹변조방지**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**웹변조방지 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 웹 변조 방지 기능의 사용 여부를 지정합니다.<br>• **보안로그** 웹 변조 방지 기능에 의해 정보가 차단될 때 관련 정보를 로그로 기록할 것인지를 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

# 웹 페이지 확인 및 업데이트하기


웹 변조 방지 설정 화면의 <**웹 변조 방지 리스트**> 부분에는 웹 변조 기능을 적용하기 위해 등록된 웹 페이지의 목록이 출력됩니다. 그리고, 각 웹 페이지에 대한 다음과 같은 정보가 함께 표시됩니다.

- **변조 상태** 등록한 웹 페이지의 변조 여부. 다음과 같은 값으로 표시됩니다.
  - 변조: 검사 결과, 웹 페이지가 공격자에 의해 변조된 경우
  - 제거: 검사 결과, 웹 페이지가 공격자에 의해 제거된 경우.
  - 업데이트: 웹 페이지가 변조되거나 제거되지 않은 경우(정상적인 경우)
  - 응답 없음: 서버로부터 응답이 없는 경우
- **버츄얼 호스트** 사용자가 등록한 웹 페이지를 서비스하는 서버의 도메인 이름
- **웹페이지** 사용자가 등록한 웹 페이지.
- **LB 그룹** 웹 페이지를 서비스하는 서버가 속한 부하 분산 그룹 이름.
- **크기** 웹 페이지의 크기
- **업데이트 시간** 가장 마지막으로 웹 페이지가 업데이트된 시간
- **설명** 웹 페이지에 대한 설명

목록의 아래쪽에 있는 4개의 버튼 ([**페이지 보기**], [**페이지 검사**], [**업데이트**], [**전목록 업데이트**])을 사용하면 바로 목록에 등록된 웹 페이지의 내용을 확인하거나 변조 여부를 검사할 수 있습니다. 다음은 각 버튼의 기능입니다.

- **페이지 보기** WEBFRONT-K에 저장된 해당 웹 페이지의 내용을 보여줍니다. 웹 페이지를 선택한 후 이 버튼을 클릭하면 웹 페이지의 내용을 보여주는 화면이 나타납니다.
- **페이지 검사** 체크 주기가 경과되기 이전에 지정한 웹 페이지가 변경되었는지를 검사합니다. 웹 페이지를 선택한 후 이 버튼을 클릭하면 선택한 웹 페이지의 변조 여부를 바로 검사한 후 검사 결과를 '변조 상태' 항목에 표시합니다.
- **업데이트** 지정한 웹 페이지를 최신 웹 페이지로 업데이트합니다. 웹 페이지를 선택한 후 이 버튼을 클릭하면 현재 웹 페이지의 내용을 WEBFRONT-K에 저장합니다.
- **전목록업데이트** 등록되어 있는 모든 웹 페이지를 최신 웹 페이지로 업데이트합니다.

# 응답 형식 검사 기능 설정

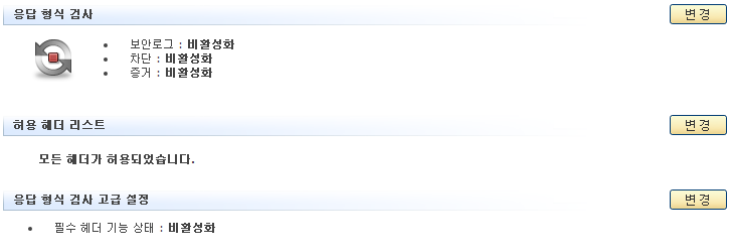
응답 형식 검사 기능은 웹 서버가 잘못된 형식의 응답 패킷을 클라이언트에게 전송하는 것을 방지하는 기능입니다. 응답 형식 검사 기능은 웹 서버의 응답 패킷을 검사하여 반드시 포함해야 하는 필수 헤더가 없는 등 응답 패킷이 지정한 형식과 맞지 않는 경우, 지정한 방식에 따라 해당 응답을 처리합니다.

이 절에서는 이러한 응답 형식 검사 기능의 설정 화면과 설정 과정에 대해 살펴본 후, 실제로 응답 형식 검사 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **컨텐트보호** - **응답형식검사** 메뉴를 클릭하면 응답 형식 검사 기능의 설정 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **응답 형식 검사** — 응답 형식 검사 기능의 활성화 상태와 보안 로그, 차단, 증거 기능의 활성화 상태가 표시됩니다.
- **허용 헤더 리스트** — 현재 설정된 허용 헤더의 목록이 표시됩니다. 등록된 허용 헤더가 없는 경우에는 '모든 헤더가 허용되었습니다.'라는 문구가 출력됩니다.
- **응답 형식 검사 고급 설정** — 필수 헤더 검사 여부가 표시됩니다.

### 설정 과정

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

❶ 허용 헤더 설정
웹 서버의 응답 패킷의 헤더에 포함되어야 하는 허용 헤더를 등록합니다. WEBFRONT-K는 응답 패킷의 헤더에 설정한 허용 헤더가 포함된 경우에는 응답을 클라이언트로 전달하고 포함하지 않은 경우에는 응답을 차단합니다. 기본적으로 권장 헤더가 등록되어 있고, 상태는 비활성화로 설정됩니다.

❷ 필수 헤더 설정
특정 메서드를 사용하는 응답 패킷에 반드시 포함되어야 하는 필수 헤더를 등록합니다. 웹 서버가 필수 헤더가 설정되어 있는 메서드를 통해 클라이언트로 응답 패킷을 보내면 WEBFRONT-K는 응답 패킷에 설정한 필수 헤더가 포함되었는지를 확인합니다. 필수 헤더 기능은 고급 기능으로 반드시 설정하지 않아도 됩니다. 기본적으로 필수 헤더 기능은 비활성화되어 있고, 등록된 필수 헤더는 없습니다.

❸ 관련 기능의 활성화 상태 설정
응답 형식 검사 기능의 사용 여부와 이 기능에 대한 보안 로그, 차단, 증거 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

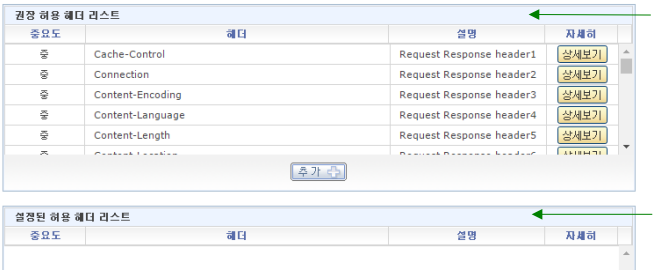
# 응답 형식 검사 설정하기

## 허용 헤더 설정

응답 형식 검사 수행 시 응답 패킷에 반드시 포함되어야 하는 허용 헤더를 설정하는 방법은 다음과 같습니다. 허용 헤더는 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **응답형식검사** 메뉴를 클릭합니다. |
| 2 | <**허용 헤더 리스트**>의 [**변경**] 버튼을 클릭합니다. |

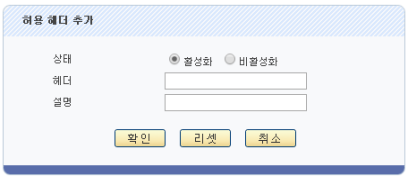
권장 허용 헤더 목록을 보여주는 <**허용 헤더 리스트 설정**> 화면이 나타납니다. 권장 목록의 허용 헤더를 추가하려면 3번 과정을, 사용자가 직접 허용 메서드를 입력하려면 4 ~ 5번 과정을 수행합니다.




WEBFRONT-K에서 제공하는 권장 허용 헤더 목록

응답 형식 검사 기능을 적용하기 위해 사용자가 등록한 허용 헤더 목록

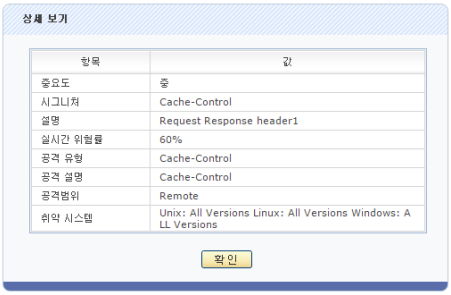
**참고:** 권장 허용 헤더 목록에 있는 정보는 실제 WEBFRONT-K 화면에서 출력되는 권장 정보와 다를 수 있습니다.

| | |
|---|---|
| 3 | 등록하고자 하는 허용 헤더가 권장 허용 헤더 목록에 있는 경우에는 목록에서 해당 허용 헤더를 선택한 후 [**추가**] 버튼을 클릭합니다. 여러 개의 허용 헤더를 선택할 때에는 [**Ctrl**] 키나 [**Shift**]키를 누른 상태에서 허용 헤더를 클릭하면 됩니다. 허용 헤더를 선택할 때에는 허용 헤더의 중요도와 상세 정보를 참고하는 것이 좋습니다. 권장 허용 헤더의 중요도와 상세 정보에 대한 설명은 다음 절인 [권**장 허용 헤더 정보 보기**]에 설명되어 있습니다. |
| 4 | 사용자가 직접 허용 헤더를 입력하려면 <**설정된 허용 헤더 리스트**>의 [**추가**] 버튼을 클릭합니다. |
| 5 | <**허용 헤더 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 등록하고 있는 허용 헤더에 대해 응답 형식 검사 기능을 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **헤더** 응답 패킷에 포함된 헤더와 비교할 허용 헤더를 입력합니다. 허용 헤더에는 알파벳, 숫자와 '-' 기호로 이루어진 최대 128자의 문자열을 입력할 수 있습니다.<br>• **설명** 허용 헤더에 대한 설명을 입력합니다. 알파벳과 한글, 숫자, 특수 문자로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정)<br>**참고:** 사용자가 직접 입력한 허용 헤더는 중요도 항목이 '사용자 정의'로 표시됩니다. |
| 6 | 허용 헤더를 모두 설정한 후에는 허용 헤더 설정 상태 항목에서 설정한 허용 헤더의 활성화 여부를 지정합니다. |
| 7 | 헤더를 모두 추가한 후에는 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

### 권장 허용 헤더 정보 보기

설정된 허용 헤더에 등록할 권장 허용 헤더를 선택할 때에는 허용 헤더의 중요도와 상세 정보를 참고하는 것이 좋습니다. 허용 헤더의 중요도는 상, 중, 하, 세 단계로 표시됩니다. 중요도가 '상'인 허용 헤더는 요청 형식 검사에 필요한 허용 헤더이므로 반드시 설정된 허용 헤더로 추가해야 합니다. 중요도가 '중'이나 '하'인 허용 헤더는 [**상세보기**] 버튼을 클릭하여 허용 헤더의 상세 정보를 확인한 후 추가 여부를 결정하도록 합니다.

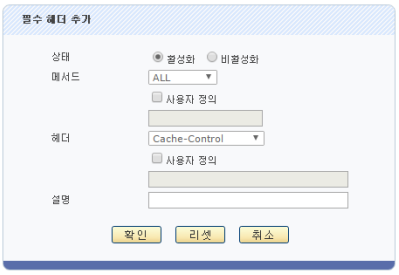
허용 헤더의 [**상세보기**] 버튼을 클릭하면 <**상세 보기**> 팝업 창이 나타납니다. <**상세 보기**> 팝업 창에서 보여주는 정보는 다음과 같습니다.




- 중요도
  허용 헤더의 중요도. 상, 중, 하로 표시됩니다.
- 시그니처
  허용 헤더. 비공개 허용 헤더인 경우에는 '시그니처 비공개'로 표시됩니다.
- 설명
  허용 헤더가 차단하는 공격에 대한 설명
- 실시간 위험률
  시그니처에 대한 실제 공격 사용빈도 위험률 (%)
- 공격 유형
  허용 헤더에 의해 차단할 공격의 유형
- 공격 설명
  허용 헤더에 의해 차단할 공격에 대한 설명
- 공격 범위
  공격 방식. remote인 경우에는 원격에서 서버를 공격하는 방식이고, local은 서버에서 직접 공격하는 방식입니다.
- 취약 시스템
  허용 헤더에 의해 차단할 공격에 대해 취약한 시스템

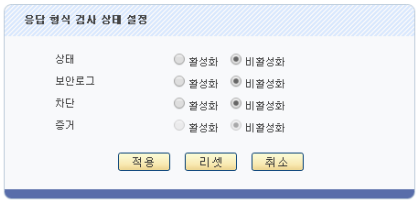
## 필수 헤더 설정

다음은 요청 패킷의 메서드 종류에 따라 응답 패킷에 반드시 포함되어야 하는 필수 헤더를 설정하는 방법입니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **응답형식검사** 메뉴를 클릭합니다. |
| 2 | <**응답 형식 검사 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**응답 형식 검사 고급 설정 보기**>의 [**변경**] – [**추가**] 버튼을 클릭합니다. |
| 4 | <**필수 헤더 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 등록하고 있는 필수 헤더를 응답 형식 검사 기능에 적용할지를 지정합니다. (기본값: 활성화)<br>• **메서드** 필수 헤더 검사를 수행할 메서드를 지정합니다. 메서드는 다음과 같은 2가지 방법 중의 한 가지 방법으로 지정할 수 있습니다. (기본값: ALL)<br>❶ 드롭다운 목록을 클릭한 후 목록에서 지정하려는 메서드를 선택합니다.<br>❷ 드롭다운 목록에 지정하려는 메서드가 없는 경우에는 사용자 정의 항목을 체크한 후 바로 아래의 텍스트 박스에 메서드를 직접 입력합니다. 메서드는 알파벳과 숫자로 이루어진 최대 16자의 문자열을 입력합니다.<br>• **헤더** 지정한 메서드를 사용하는 응답 패킷에 반드시 포함되어야 하는 필수 헤더를 지정합니다. 필수 헤더는 다음과 같은 2가지 중 한 가지 방법으로 지정할 수 있습니다. (기본값: Cache-Control)<br>❶ 드롭다운 목록을 클릭한 후 지정하려는 필수 헤더를 선택합니다.<br>❷ 드롭다운 목록에 지정하려는 헤더가 없는 경우에는 사용자 정의 항목을 체크한 후 바로 아래의 텍스트 박스에 헤더를 직접 입력합니다. 필수 헤더는 알파벳, 숫자와 '-' 기호로 이루어진 최대 128자의 문자열로 지정합니다.<br>• **설명** 필수 헤더에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 5 | 필수 헤더를 모두 추가하였으면 필수 헤더 기능 상태 항목에서 필수 헤더의 사용 여부를 지정합니다. |
| 6 | 설정 내용을 저장하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

허용 헤더와 필수 헤더(옵션)을 설정한 후에는 응답 형식 검사 기능의 사용 여부와 응답 형식 검사 기능과 관련된 보안 로그 기능 등의 활성화 여부를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **응답형식검사** 메뉴를 클릭합니다. |
| 2 | <**응답 형식 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**응답 형식 검사 상태 설정**> 팝업 창에서 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 응답 형식 검사 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 응답 형식 검사 기능의 정책에 부합되지 않는 클라이언트의 요청에 대한 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** 응답 형식 검사 기능에 의해 접근이 제한된 요청을 차단할 것인지 지정합니다. 이 항목을 활성화하면, 응답 형식 검사 기능의 정책에 부합되지 않는 응답 패킷은 모두 차단됩니다.<br>• **증거** 응답 형식 검사 기능의 정책에 부합되지 않는 응답 패킷에 대한 증거를 기록할 것인지 지정합니다. 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 판단의 근거가 되는 정보를 기록합니다. 로그의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

# 코드 노출 차단 기능 설정

코드 노출 차단 기능은 웹 서버가 HTML이나 스크립트 등의 코드를 클라이언트에게 전송하는 것을 방지하는 기능합니다. 코드 노출 차단 기능은 웹 서버의 응답 패킷에 코드가 포함되어 있는지를 검사하여 지정한 방식에 따라 패킷을 처리합니다. 이 절에서는 코드 노출 차단 기능의 설정 화면과 설정 과정에 대해 살펴본 후, 실제로 코드 노출 차단 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **컨텐트보호** - **코드노출차단** 메뉴를 클릭하면 코드 노출 차단 기능의 설정 화면이 나타납니다.


화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **코드 노출 차단** 코드 노출 차단 기능의 활성화 상태와 보안 로그 기능의 활성화 상태가 표시됩니다.
- **코드 노출 차단 기능** 코드 노출 차단 기능의 설정 정보가 표시됩니다.
- **검사 URL 리스트** 코드 노출 차단 기능을 적용할 검사 URL 목록이 표시됩니다.

### 설정 과정

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

❶ 코드 노출 차단 기능 설정
HTML과 스크립트 코드 노출 차단의 활성화 여부를 각각 지정합니다. 기본적으로는 이 기능들은 모두 비활성화되어 있습니다.

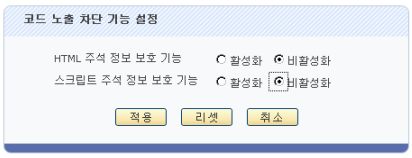
❷ 검사 URL 설정
코드 노출 차단 기능을 적용할 검사 URL을 등록합니다. 기본적으로 등록된 검사 URL은 없습니다.

❸ 관련 기능의 활성화 상태 설정
코드 노출 차단 기능의 사용 여부와 이 기능에 대한 보안 로그 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# 코드 노출 차단 설정하기

## 코드 노출 차단 기능 설정

HTML 코드 노출 차단 기능과 스크립트 주석 정보 노출 차단 기능의 사용 여부를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **코드노출차단** 메뉴를 클릭합니다. |
| 2 | <**코드 노출 차단 기능**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**코드 노출 차단 기능 설정**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 활성화되어 있습니다.<br>  <br><br>• **HTML 주석 정보 보호 기능**<br>HTML 코드 노출 차단 기능의 사용 여부를 지정합니다.<br>• **스크립트 주석 정보 보호 기능**<br>스크립트 코드 노출 차단 기능의 사용 여부를 지정합니다. |

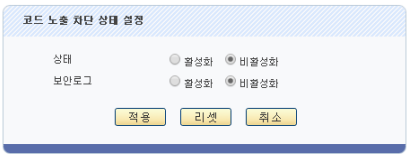
## 검사 URL 설정

코드 노출 차단 기능을 설정한 후에는 다음과 같은 방법으로 코드 노출 차단 기능을 적용할 검사 URL을 등록합니다. 검사 URL은 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **코드노출차단** 메뉴를 클릭합니다. |
| 2 | <**검사 URL 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**검사 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 현재 등록하고 있는 URL에 대해 코드 노출 차단 기능을 적용할지를 지정합니다. (기본값: 활성화)<br>• **URL** 코드 노출 차단 기능을 적용할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 됩니다.<br>• **설명** 검사 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 검사 URL 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

코드 노출 차단 기능을 설정하고 검사 URL을 모두 설정하고 나면 다음과 같은 방법으로 코드 노출 차단 기능의 사용 여부와 코드 노출 차단 기능과 관련된 로그 기능의 활성화 상태를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **코드노출차단** 메뉴를 클릭합니다. |
| 2 | <**코드 노출 차단**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**코드 노출 차단 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 코드 노출 차단 기능의 사용 여부를 지정합니다.<br>• **보안 로그** 코드 노출 차단 기능에 의해 정보가 차단될 때 관련 정보를 로그로 기록할 것인지를 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

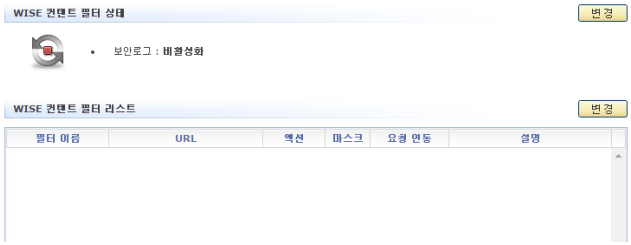
# WISE 컨텐트 필터 설정

WISE 컨텐트 필터는 웹 서버가 클라이언트로 보내는 응답 패킷에 대한 항목, 변수, 값, 조건 등 필터의 규칙을 세부적으로 설정하여 응답 패킷을 필터링하는 기능입니다. 앞에서 살펴본 컨텐트 보호 기능(신용카드 정보 유출 ~ 코드 노출 차단)으로는 원하는 사항을 검사해내기 어려울 경우, 컨텐트 필터를 사용하여 응답 패킷을 검사할 수 있는 보다 세밀한 조건을 지정할 수 있습니다. 이 절에서는 WISE 컨텐트 필터의 설정 화면과 설정 과정에 대해 살펴본 후, 실제로 WISE 컨텐트 필터를 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application** - **컨텐트보호** - **WISE 컨텐트필터** 메뉴를 클릭하면 WISE 컨텐트 필터의 설정 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **WISE 컨텐트 필터 상태** WISE 컨텐트 필터의 활성화 상태와 로그 등 관련 기능의 활성화 상태가 표시됩니다.
- **WISE 컨텐트 필터 리스트** 현재 설정된 WISE 컨텐트 필터의 목록이 표시됩니다. WISE 컨텐트 필터를 클릭하면, 설정한 필터링 조건이 바로 아래에 표시됩니다.

### 설정 과정

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

❶ WISE 컨텐트 필터 설정

먼저 WISE 컨텐트 필터를 정의합니다. 필터를 정의할 때는 필터의 이름, 활성화 상태, 필터링할 URL, 필터링된 응답 패킷의 처리 방법, 요청 연동 기능의 사용 여부 등을 설정합니다. 기본적으로 정의된 WISE 컨텐트 필터는 없습니다.

필터를 정의한 후에는 데이터 유형, 변수, 값, 비교 방법 등 필터링 조건을 설정합니다. 요청 패킷과 응답 패킷에 대한 필터링 조건은 각각 설정해야 됩니다. 응답 패킷의 필터링 조건은 반드시 설정해야 하고, 요청 패킷의 필터링 조건은 필터를 정의할 때 요청 연동 기능을 사용하도록 활성화한 경우에만 설정합니다. 기본적으로는 아무런 필터링 조건도 설정되어 있지 않습니다.

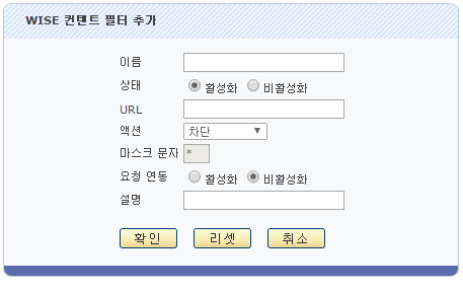
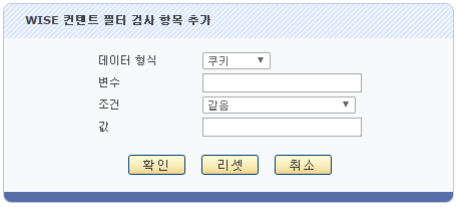
❷ 관련 기능의 활성화 상태 설정

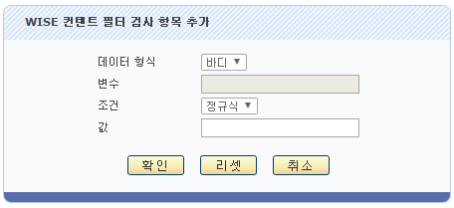
WISE 컨텐트 필터의 사용 여부와 이 기능에 대한 보안 로그 및 통계 기능의 사용 여부를 지정합니다. 기본적으로 이 기능들은 모두 비활성화되어 있습니다.

# WISE 컨텐트 필터 설정하기

## WISE 컨텐트 필터 추가

다음과 같은 방법으로 WISE 컨텐트 필터를 정의하고, 필터링 조건을 설정합니다. 하나의 애플리케이션에는 최대 1024개의 WISE 컨텐트 필터를 추가할 수 있습니다.

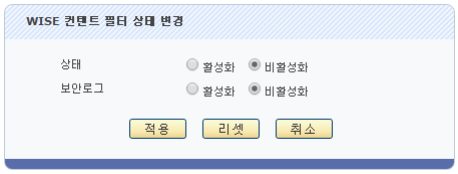
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **WISE 컨텐트필터** 메뉴를 클릭합니다. |
| 2 | <**WISE 컨텐트 필터 리스트**>의 [**변경**] - [**필터추가**] 버튼을 클릭합니다. |
| 3 | <**WISE 컨텐트 필터 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **이름** WISE 컨텐트 필터의 이름을 입력합니다. 이름은 알파벳과 숫자로 이루어진 최대 32 글자의 문자열로 지정할 수 있으며, 'filter'는 사용할 수 없습니다.<br>• **상태** 등록하고 있는 WISE 컨텐트 필터를 활성화할 것인지 지정합니다. (기본값: 활성화)<br>• **URL** WISE 컨텐트 필터를 통해 필터링을 수행할 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'이어야 됩니다.<br>• **액션** 드롭다운 목록을 클릭하여 현재 등록하고 있는 WISE 컨텐트 필터에 매치된 URL 응답 패킷의 처리 방법을 선택합니다.<br>– 차단: 해당 응답 패킷을 차단합니다. (기본값)<br>– 마스킹: 해당 응답 패킷을 마스크 문자로 마스킹합니다. 이 방법을 선택한 경우에는 아래에 있는 마스크 문자 항목을 설정해야 합니다.<br>• **마스크 문자** 액션 항목을 '마스킹'으로 선택한 경우, 이 항목에 응답 패킷의 정보를 마스킹할 문자를 입력합니다. 하나의 문자만 입력할 수 있으며, 알파벳, 숫자와 특수 문자를 모두 입력할 수 있습니다. (기본값: *)<br>• **요청 연동** 요청 연동 기능의 사용 여부를 지정합니다. 요청 연동을 활성화하면 요청 패킷과 응답 패킷에 대해 모두 필터링을 수행하며, 비활성화하면 응답 패킷에 대해서만 필터링합니다. (기본값: 비활성화)<br>• **설명** WISE 컨텐트 필터 또는 URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 추가한 요청 필터의 필터링 조건을 설정하기 위해 필터를 선택한 후 [**응답검사항목추가**] 버튼을 클릭합니다. 하나의 필터에 최대 16개의 필터링 조건을 추가할 수 있습니다. |
| 5 | <**WISE 컨텐트 필터 검사 항목 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **데이터 형식** WISE 컨텐트 필터 기능을 통해 패킷의 어떤 부분을 검사할 것인지를 지정합니다. 앞의 3번 과정에서 액션 항목을 '차단'으로 설정한 경우에는 쿠키, 헤더, 바디를 검사할 수 있고, '마스킹'으로 설정한 경우에는 바디만 검사할 수 있습니다.<br>• **변수** 데이터 형식을 쿠키나 헤더로 선택한 경우 해당되는 변수를 입력합니다. 변수는 알파벳, 숫자와 '-' 기호로 이루어진 최대 256자의 문자열로 지정할 수 있습니다. 바디를 선택한 경우에는 이 항목을 입력하지 않습니다.<br>• **조건** 드롭다운 목록을 클릭하여 설정한 데이터 형식의 값과 응답 패킷의 해당 데이터 형식의 값을 비교할 조건을 선택합니다.<br>– 같음: 해당 데이터 형식의 값이 값 항목에 설정한 값과 일치하는지 검사합니다.<br>– 포함: 해당 데이터 형식의 값이 값 항목에 설정한 값을 포함하는지 검사합니다. |

| | |
|---|---|
| | – 포함하지 않음: 해당 데이터 형식의 값이 값 항목에 설정한 값을 포함하지 않았는지 검사합니다.<br>– 정규식: 해당 데이터 형식의 값이 값 항목에 설정한 정규식과 일치하는지 검사합니다.<br>– 매개변수가 존재함: 해당 데이터 형식의 변수가 존재하는지 검사합니다.<br>– 매개변수가 존재하지 않음: 해당 데이터 형식의 변수가 존재하지 않는지 검사합니다.<br>– 값이 존재하지 않음: 해당 데이터 유형의 값이 존재하지 않는지 검사합니다.<br>데이터 형식 항목에서 선택한 항목에 따라 드롭다운 목록에 나타나는 조건은 다릅니다. 쿠키와 헤더를 선택한 경우에는 위의 모든 조건 중 하나를 선택할 수 있고, 바디를 선택한 경우에는 포함과 정규식 중 하나를 선택할 수 있습니다. 기본적으로는 '같음'이 지정됩니다.<br>• **값** 데이터 형식의 값을 입력합니다. 변수가 존재하는 데이터 형식의 경우에는 변수에 해당하는 값을 입력합니다. '조건' 항목에서 선택한 조건에 따라 입력하는 값의 형식이 다릅니다. 각 조건에 대한 설명은 다음과 같습니다.<br>– '정규식'을 선택한 경우에는 최대 256자의 정규식을 입력합니다.<br>– '값이 존재하지 않음', '매개변수가 존재함', '매개변수가 존재하지 않음' 이외의 조건을 선택한 경우에는 알파벳, 숫자와 특수 기호로 이루어진 최대 256자의 문자열을 입력합니다. |
| 6 | 3번 과정에서 요청 연동을 활성화한 경우에는 요청 패킷에 대한 필터링 조건을 설정합니다. <**WISE 컨텐트 필터 리스트**>에서 필터를 선택한 후 [**요청검사항목추가**] 버튼을 클릭합니다. |
| 7 | <**WISE 컨텐트 필터 검사 항목 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 입력한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **데이터 형식** WISE 컨텐트 필터가 요청 패킷의 어떤 부분을 검사할 것인지를 지정합니다. 검사할 수 있는 패킷의 부분에는 쿠키, 메서드, 헤더, 매개변수, IP 주소의 5가지가 있습니다. (기본값: 쿠키)<br>• **변수** 선택한 데이터 형식에 해당되는 변수를 입력합니다. 변수는 알파벳, 숫자와 '-' 기호로 이루어진 최대 256자의 문자열로 지정할 수 있습니다. 메서드나 IP 주소를 선택한 경우에는 이 항목을 입력하지 않습니다. 매개변수를 선택한 경우 '*'를 사용하여 해당 URL의 모든 매개변수를 설정할 수 있습니다.<br>• **조건** 드롭다운 목록을 클릭하여 설정한 데이터 형식의 값과 응답 패킷의 해당 데이터 형식의 값을 비교할 조건을 선택합니다. (기본값: 같음)<br>– 같음: 해당 데이터 형식의 값이 값 항목에 설정한 값과 일치하는지 검사합니다.<br>– 포함: 해당 데이터 형식의 값이 값 항목에 설정한 값을 포함하는지 검사합니다.<br>– 포함하지 않음: 해당 데이터 형식의 값이 값 항목에 설정한 값을 포함하지 않았는지 검사합니다.<br>– 정규식: 해당 데이터 형식의 값이 값 항목에 설정한 정규식과 일치하는지 검사합니다.<br>– 매개변수가 존재함: 해당 데이터 형식의 변수가 존재하는지 검사합니다.<br>– 매개변수가 존재하지 않음: 해당 데이터 형식의 변수가 존재하지 않는지 검사합니다.<br>– 값이 존재하지 않음: 해당 데이터 유형의 값이 존재하지 않는지 검사합니다.<br>데이터 형식 항목에서 선택한 유형에 따라 드롭다운 목록에 나타나는 조건이 달라집니다. 쿠키나 헤더, 매개변수를 선택한 경우에는 위의 모든 비교 조건 중에서 선택할 수 있고, 메서드를 선택하면 같음, 포함, 포함하지 않음, 정규식 중에서 선택할 수 있습니다. IP 주소를 선택한 경우에는 포함과 포함하지 않음 중에서만 선택할 수 있습니다.<br>• **값** 데이터 형식의 값을 입력합니다. 변수가 존재하는 데이터 형식의 경우에는 변수에 해당하는 값을 입력합니다. 값은 알파벳, 숫자와 특수 기호로 이루어진 최대 256자의 문자열로 지정할 수 있습니다. |
| 6 | WISE 컨텐트 필터를 모두 추가하였으면 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

**참고:** 하나의 애플리케이션에는 WISE 컨텐트 필터의 응답 검사 항목과 요청 검사 항목을 합하여 최대 2048개까지 추가할 수 있습니다.

## 관련 기능의 활성화 상태 설정

WISE 컨텐트 필터를 설정하고 나면 다음과 같은 방법으로 WISE 컨텐트 필터 기능의 사용 여부와 WISE 컨텐트 필터 기능과 관련된 로그 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **컨텐트보호** - **WISE 컨텐트필터** 메뉴를 클릭합니다. |
| 2 | <**WISE 컨텐트 필터 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**WISE 컨텐트 필터 상태 변경**> 팝업 창에서 다음 설명을 참고하여 각 기능의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** WISE 컨텐트 필터 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** WISE 컨텐트 필터 기능의 조건에 부합되지 않는 클라이언트의 요청에 대한 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

# 제5장 학습 기능

학습 기능은 WEBFRONT-K의 정책 설정을 보조하기 위한 기능으로 클라이언트가 접속을 요청한 URL과 매개변수를 전달하는 URL, 매개변수의 형식과 길이 정보를 기록합니다. 관리자는 학습을 통해 얻은 정보를 이용하여 접근 제어(허용 URL) 기능과 폼필드 검사(액션 URL) 기능에 대한 정책을 설정할 수 있습니다. WEBFRONT-K는 애플리케이션 접근 제어 학습, 폼 필드 학습 2가지 종류의 학습 기능을 제공합니다. 이와 같은 학습 기능을 사용하는 방법은 모두 동일합니다. 그러므로, 이 장에서는 각각의 학습 기능 사용 방법을 설명하지 않고, 접근 제어 학습 기능을 사용하는 방법을 예를 들어 학습 기능을 설정하는 방법과 학습 기능을 통해 얻은 정보를 사용하는 방법을 소개합니다.

이 장의 마지막에는 일반적인 학습 기능과 별도로 접근 로그를 바탕으로 각 사이트의 URL의 구조를 보여주는 URL 구조 분석 기능에 대해 살펴봅니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 설정하기 전에
- 학습 기능 설정하기
- 학습 내용 적용하기
- URL 구조 분석 기능 사용하기

# 설정하기 전에

## 설정 과정

WEBFRONT-K를 통해 전송되는 요청 패킷에 대해 학습하기 위해서는 다음과 같은 과정을 통해 학습 기능을 설정하고 사용해야 합니다.

❶ 학습 기능 상태 설정

학습 기능을 통해 정보를 수집하려면, 학습 기능을 먼저 활성화해야 합니다. 각 학습 기능의 활성화 상태는 접근제어 기능과 폼필드 검사 기능을 설정할 때 지정할 수 있습니다. 기본적으로 모든 학습 기능은 비활성화되어 있습니다.

❷ 임계값 설정

WEBFRONT-K는 최소 세션 임계값을 사용하여 학습을 제한할 수 있습니다. 최소 세션 임계값을 설정하면, 학습을 통하여 기록된 모든 정보를 학습 결과 화면에 출력하지 않고, 동일한 요청 패킷이 기록된 횟수가 설정한 최소 세션 임계값을 초과하는 경우에만 출력합니다. 기본값은 1입니다.

❸ 학습 내용 적용

학습 기능을 활성화하고, 임계값을 설정하면 요청 패킷이 학습되어 학습 기능의 결과 화면에 출력됩니다. 관리자는 학습된 내용을 보고, 이 내용을 규칙으로 적용할 것인지, 잠시 보류할 것인지, 삭제할 것인지를 지정할 수 있습니다.

## 학습 기능 사용 방법

WEBFRONT-K를 처음 설치하면, 모든 요청 검사 기능은 비활성화되어 있고, 설정된 정책도 없습니다. 그러므로, WEBFRONT-K는 요청 검사 기능을 수행하지 않고 모든 요청을 웹 서버로 통과시키게 됩니다. 다시 말해서, WEBFRONT-K를 설치한 후, 아무런 요청 검사 정책도 설정하지 않으면, 웹 서비스는 WEBFRONT-K를 설치하기 전과 동일하게 이루어집니다. 요청 검사 기능을 사용하기 위해서는 WEBFRONT-K에 정책을 설정해야 합니다. 관리자가 웹 애플리케이션에 대한 정보를 잘 알고 있는 경우에는 직접 정책을 설정하면 됩니다. 그러나, 일반적으로 충분한 정보를 갖추기가 힘들고 또 모든 상황을 고려하여 정책을 설정하기는 어렵습니다. 이런 경우에, 먼저 학습 기능을 이용하여 웹 애플리케이션에 대한 정보들을 학습할 수 있습니다.

정책을 설정하기 전에 학습을 위해 권장하는 설정 방법은 다음과 같습니다.

1. 학습 기능을 사용할 요청 검사 기능(접근 제어, 폼필드 검사)을 활성화합니다.
   요청 검사 기능이 비활성화되어 있으면 모든 패킷은 허용 패킷으로 간주됩니다. 학습 기능은 허용되지 않는 패킷을 기록하기 때문에 허용되지 않는 패킷이 없으면 학습 기능이 수행되지 않습니다. 그러므로 요청 검사 기능을 활성화해야만 허용되지 않는 요청 패킷이 존재할 수 있으므로 학습 기능도 수행될 수 있습니다.

2. 요청 검사 기능(접근 제어, 폼필드 검사)에서 허용되지 않는 요청 패킷도 웹 서버로 전달되도록 설정합니다.
   접근 제어 학습은 접근 제어 기능의 허용 URL을 설정하기 위한 학습 기능입니다. 기본적으로 모든 URL을 의미하는 '/*/'이 등록되어 있지만 학습 기능을 통해 허용 URL을 상세히 설정하기 위해서는 해당 설정을 삭제해야 합니다. 허용 URL 설정이 없는 경우에는 모든 URL에 대해 접근이 차단되기 때문에 학습을 하는 동안 접근 제어 기능을 탐지 상태(차단 기능 비활성화)로 운영해야 합니다.
   폼필드 학습은 폼필드 검사 기능의 액션 URL(액션 URL, 매개변수 형식/최소 길이/최대 길이)을 설정하기 위한 학습 기능입니다. 기본적으로 등록된 액션 URL은 없습니다. 그러나 폼필드 검사의 다른 보안 기능을 사용하는 경우 학습이 정상적으로 수행되지 않을 수 있으므로 폼필드 검사 기능을 탐지 상태(차단 기능 비활성화)로 운영해야 합니다.

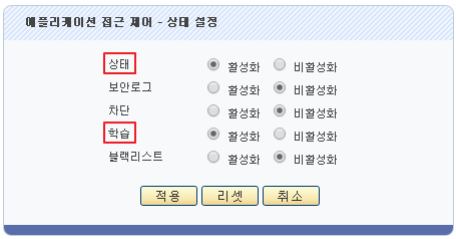
3. 최소 세션 임계값을 '1' 정도로 작게 설정합니다.
   처음에는 정책을 설정하기 위한 정보가 부족하므로, 허용되지 않는 대부분의 요청 패킷을 학습할 필요가 있습니다. 그러므로, 최소 세션 임계값을 작게 설정하여 거의 모든 요청 패킷의 정보가 기록되도록 합니다. 최소 세션 임계값이 '1'인 경우에는 허용되지 않는 모든 요청 패킷을 학습하게 됩니다.

# 학습 기능 설정하기

학습 기능의 상태와 임계값, 보충 학습을 설정하는 방법에 대해 살펴봅니다.

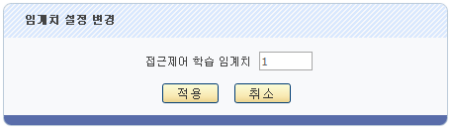
## 학습 기능 상태 설정

다음은 접근 제어 학습 기능을 활성화하는 과정입니다. 학습 기능을 활성화하는 방법은 설정하는 메뉴만 다르고 모두 동일합니다. 폼 필드 검사 학습 기능을 활성화하려면 이 부분의 설명을 참고하여 폼 필드 검사 기능의 설정 부분에서 설정하면 됩니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **요청검사** - **접근제어** 메뉴를 클릭합니다. |
| 2 | <**애플리케이션 접근제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**애플리케이션 접근 제어 – 상태 설정**> 팝업 창에서 상태, 학습 항목을 활성화로 변경하고 [**적용**] 버튼을 클릭합니다.<br>  |

## 임계값 설정

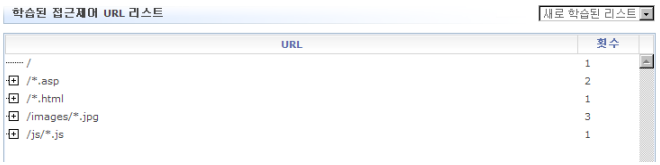
학습 결과 화면에 출력되는 요청 패킷의 수를 제한하기 위해 임계값을 설정하는 과정은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **학습** - **접근제어학습** 메뉴를 클릭합니다. |
| 2 | <**접근제어 학습 임계치**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**임계치 설정 변경**> 팝업 창에서 접근제어 학습 임계치 항목을 입력한 후 [**적용**] 버튼을 클릭합니다. (설정 범위: 1 ~ 65535, 기본값: 1)<br>  |

**참고:** WEBFRONT-K를 처음 설치하여 정책을 설정한 경우에는 학습할 내용이 많기 때문에, 임계값을 상대적으로 작게 1 정도로 설정하도록 합니다. 학습을 통하여 웹 사이트가 정상적으로 서비스를 할 수 있도록 정책을 설정한 후에는 임계값을 웹 애플리케이션의 상황에 따라 상대적으로 크게 설정하도록 합니다. 그러면, 공격과 같이 일시적으로 수신되는 비정상적인 요청이 정상적인 요청으로 학습되는 것을 방지하여 반복적으로 들어오는 정상적인 요청만 학습할 수 있습니다.

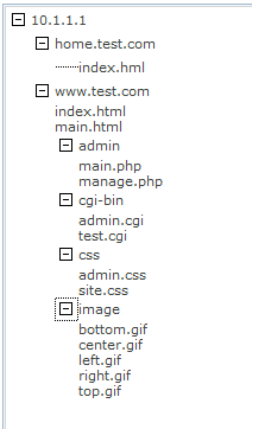
# 학습 내용 적용하기

앞에서 설정한 학습 기능을 통해 요청 패킷이 학습되면 다음과 같은 방법으로 학습된 결과를 애플리케이션 접근 제어 기능에 적용할 수 있습니다. 다른 기능에도 동일한 방법으로 학습 결과를 적용하면 됩니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **학습** - **접근제어학습** 메뉴를 클릭합니다. |
| 2 | 접근제어 학습 기능의 설정 화면이 나타납니다. 화면의 학습된 접근제어 URL 리스트에는 애플리케이션 접근 제어에 대해 새롭게 학습한 내용이 표시됩니다. 아래의 설명을 참고하여 학습된 내용을 처리하도록 합니다.<br>  <br><br>• **학습한 내용을 정책으로 설정하기**<br>학습된 내용을 정책에 적용하려면 해당 내용을 선택한 후 화면 아래에 있는 [**적용**] 버튼을 클릭합니다. 그러면, 학습 내용이 직접 애플리케이션 접근 제어 기능 설정에 추가되고 이 화면에서는 삭제됩니다. 학습된 내용은 각 학습 기능 별로 다음과 같이 적용됩니다.<br>– 접근 제어 학습: 허용 URL<br>– 폼필드 학습: 액션 URL<br>• **학습 내용 삭제하기**<br>학습된 내용을 목록에서 삭제하려는 경우에는 해당 내용을 선택한 후 [**건너뛰기**] 버튼을 클릭합니다. 그러면, 선택된 내용은 이 화면에서 삭제됩니다. 삭제한 내용이 다시 학습되면 학습 화면에 나타납니다.<br>• **학습 내용 무시하기**<br>학습된 내용을 영구적으로 목록에서 삭제하고 다시는 이러한 내용을 학습하지 않도록 하려면 해당 내용을 선택한 후 [**무시**] 버튼을 클릭합니다. 그러면, 선택된 내용은 이 화면에서 삭제되고, 이 내용에 대해서는 다시 학습하지 않습니다. 이 내용은 3번 과정을 참고하여 다시 볼 수 있습니다. |
| 3 | <**학습된 접근제어 URL 리스트**>의 오른쪽에 있는 드롭다운 목록을 클릭하여 '무시된 리스트'를 선택하면 학습된 내용 목록에서 영구적으로 삭제한 내용들을 볼 수 있습니다. 영구적으로 삭제된 내용들은 다시 학습되지 않으므로, 이 목록에 있는 내용을 주기적으로 확인하여 정책에 반영할지를 결정하도록 합니다.<br>무시된 리스트에 있는 내용을 다시 학습되도록 하려면 해당 내용을 클릭한 후 아래에 있는 [**무시 취소**] 버튼을 클릭합니다. |

# URL 구조 분석 기능 사용하기

URL 구조 분석 기능은 사이트의 URL 구조를 다음과 같은 트리 형태로 보여주는 기능입니다. 트리의 맨 위에 있는 IP 주소는 애플리케이션의 IP 주소이고 그 아래에는 도메인 이름이, 그 아래에는 도메인 이름 뒤에 이어지는 URL과 파일 이름 등이 차례로 표시됩니다.

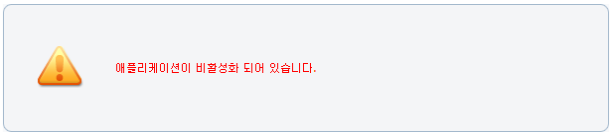



URL 구조 분석 기능은 WEBFRONT-K에 저장된 접근 로그를 사용합니다. 접근 로그에는 사용자가 요청한 URL에 대한 정보와 사용자가 요청한 URL에 포함되어 함께 로딩되는 URL이나 파일에 대한 정보가 저장됩니다. URL 구조 분석 기능은 이러한 접근 로그를 사용하여 현재까지 사용자에 의해 요청된 모든 URL에 대한 구조 정보를 보여줍니다.

**주의:** 많은 자원을 사용하는 학습 기능을 WEBFRONT-K를 설정하기 전에 필요한 정보를 수집하는 동안에만 활성화하는 것과 마찬가지로, URL 분석 기능도 가능하면 사이트의 구성을 파악하는 초기 단계에만 사용하는 것이 좋습니다. 왜냐하면, URL 구조 분석 기능에서 사용하는 접근 로그는 사용자가 요청한 URL 외에도 관련된 URL과 도메인을 구성하는 파일 등에 대한 정보가 포함되므로 다른 로그에 비해 저장되는 데이터 양이 매우 많습니다. 따라서, 접근 로그를 활성화하면 저장되어 있던 중요한 보안 로그들이 삭제될 가능성이 높기 때문입니다. 그러므로, 가급적 반드시 필요한 경우에만 접근 로그를 활성화할 것을 권장하고 있습니다.

# 사용하기 전에

URL 구조 분석 기능을 사용하려면 '애플리케이션 접근 제어 기능'을 활성화해야 하고, '접근 로그'를 활성화해야 합니다. URL 구조 분석 기능을 사용하기 위해 **Application** 메뉴에서 **학습 – URL 구조 분석** 메뉴를 클릭했을 때 다음과 같은 화면이 나타나면 이 두가지 기능(애플리케이션 접근 제어, 접근 로그)이 모두 활성화되어 있지 않은 상태입니다.




이런 경우에는 **Application** 메뉴에서 **요청 검사 – 접근 제어** 메뉴를 클릭한 후 다음 그림에 표시된 세 부분이 모두 '활성화' 상태(아이콘은 초록색)인지를 확인합니다.


세 항목 중 하나라도 활성화되어 있지 않으면 이 설명서의 [**제3장 요청 검사 기능 설정**]을 참고하여 해당 항목을 활성화하도록 합니다.

# URL 구조 출력하기

URL 구조 분석 기능을 사용하려면 **Application** – **학습** – **URL 구조 분석** 메뉴를 클릭합니다. 그러면, 현재 저장된 접근 로그를 분석하여 URL의 구조를 보여주는 다음과 같은 <**애플리케이션 URL 구조 분석**> 화면이 나타납니다.


## URL 구조 트리

처음에는 URL 구조를 보여주는 트리가 접혀 있어 애플리케이션의 IP 주소만 표시됩니다. IP 주소의 왼쪽에 있는 ⊞를 클릭하면 도메인 이름이 나타납니다. 그리고, 다시 도메인 이름 왼쪽의 ⊞를 클릭하면 도메인을 구성하는 하위 URL과 파일 이름이 출력됩니다. 하위 URL에도 ⊞ 표시가 있으면 아래에 있는 내용을 펼쳐볼 수 있습니다. 펼쳐진 내용을 접으려면 ⊟를 클릭합니다.

# 제6장 위장 기능 설정

위장은 클라이언트와의 연결에 사용되는 URL을 웹 서버의 실제 URL과 다르게 변환하거나 중요한 웹 서버의 정보를 숨김 또는 변환하는 기능입니다. 이 장에서는 WEBFRONT에서 지원하는 URL 정보 위장 기능과 서버 정보 위장 기능을 설정하는 방법에 대해 상세하게 소개합니다.

이 장은 다음 내용으로 구성되어 있습니다.

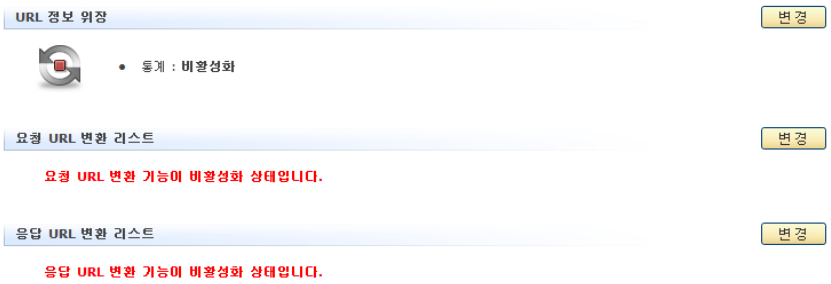
# URL 정보 위장 기능 설정

URL 변환은 클라이언트가 웹 서버로 요청하는 URL이나 웹 서버가 클라이언트로 응답하는 URL을 변환하여 내부의 웹 서버에서 사용되는 URL 정보가 외부에 유출되지 않도록 하는 기능입니다. 이 절에서는 URL 정보 위장 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후 URL 정보 위장 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application - 위장 - URL정보위장** 메뉴를 클릭하면, URL 정보 위장 기능의 현재 설정 정보를 보여주는 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **URL 정보 위장** URL 정보 위장 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. URL 정보 위장 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고 는 비활성화 상태를 나타냅니다.
- **요청 URL 변환 리스트** 요청 URL 위장의 사용 여부가 표시됩니다.
- **응답 URL 변환 리스트** 응답 URL 위장의 사용 여부가 표시됩니다.

### 설정 과정

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

❶ 요청 URL 정보 위장 설정
요청 URL에 대해 URL 정보 위장 기능을 적용하려는 경우에 이 세부 기능을 설정합니다. 이 부분에서는 요청 URL 정보 위장의 사용 여부를 지정하고 URL 위장 기능을 적용할 요청 URL과 이 요청 URL을 변환할 변환 URL을 등록합니다. 기본적으로는 요청 URL 정보 위장 기능이 비활성화되어 있고 등록된 요청 URL은 없습니다.

❷ 응답 URL 정보 위장 설정
응답 URL에 대해 URL 정보 위장 기능을 적용하려는 경우에 이 세부 기능을 설정합니다. 이 부분에서는 응답 URL 정보 위장의 사용 여부를 지정하고 URL 위장 기능을 적용할 응답 URL과 이 응답 URL을 변환할 변환 URL을 등록합니다. 기본적으로는 응답 URL 정보 위장 기능이 비활성화되어 있고 등록된 응답 URL은 없습니다.

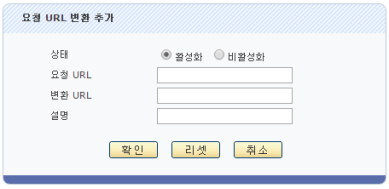
❸ 관련 기능의 활성화 상태 설정
URL 정보 위장 기능의 사용 여부와 이 기능에 대한 통계 기능의 사용 여부를 지정합니다. 기본적으로 모두 비활성화되어 있습니다.

# URL 정보 위장 설정하기

이 절에서는 요청 URL의 정보를 위장하기 위한 설정 과정과 클라이언트에게 전송하는 응답 URL의 정보를 위장하기 위한 설정 과정을 차례로 살펴봅니다.

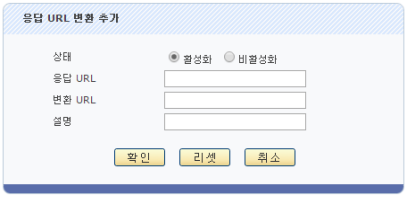
## 요청 URL 정보 위장 설정하기

위장 기능 중에서 요청 URL 정보 위장 기능을 설정하는 방법은 다음과 같습니다. 위장할 요청 URL은 최대 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **위장** - **URL정보위장** 메뉴를 클릭합니다. |
| 2 | <**요청 URL 변환 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**요청 URL 변환 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 등록하고 있는 요청 URL에 대해 위장 기능을 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **요청 URL** 위장하려는 요청 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. URL은 반드시 'http://'또는 'https://'로 시작되어야 합니다.<br>• **변환 URL** 요청 URL을 위장할 매스커레이딩 URL 을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. URL은 반드시 'http://'또는 'https://'로 시작되어야 합니다.<br>• **설명** 요청 URL 정보 위장에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 위장하려는 요청 URL을 모두 설정하였으면 요청 URL 변환 상태 항목에서 요청 URL 위장 기능의 사용 여부를 지정합니다. (기본값: 비활성화) |
| 5 | 설정한 요청 URL 변환 기능을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

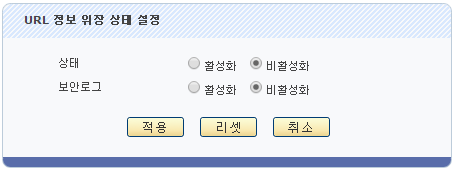
## 응답 URL 정보 위장 설정하기

위장 기능 중에서 응답 URL 정보 위장 기능을 설정하는 방법은 다음과 같습니다. 위장할 응답 URL은 최대 256개까지 등록할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **위장** - **URL정보위장** 메뉴를 클릭합니다. |
| 2 | <**응답 URL 변환 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**응답 URL 변환 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 등록하고 있는 응답 URL에 대해 위장 기능을 적용할 것인지를 지정합니다. (기본값: 활성화)<br>• **응답 URL** 위장하려는 응답 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. URL은 반드시 'http://'또는 'https://'로 시작되어야 합니다.<br>• **변환 URL** 응답 URL을 위장할 매스커레이딩 URL 을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등 기호로 구성될 수 있습니다. URL은 반드시 'http://'또는 'https://'로 시작되어야 합니다.<br>• **설명** 응답 URL 정보 위장에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 위장하려는 응답 URL을 모두 설정하였으면 응답 URL 변환 상태 항목에서 응답 URL 위장 기능의 사용 여부를 지정합니다.<br>(기본값: 비활성화) |
| 5 | 설정한 응답 URL 변환 기능을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

## 관련 기능의 활성화 상태 설정

위장하려는 요청 URL이나 응답 URL을 모두 설정하고 나면 다음과 같은 방법으로 URL 정보 위장 기능의 사용 여부와 URL 정보 위장 기능과 관련된 보안 로그 기능의 활성화 상태를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **위장** - **URL정보위장** 메뉴를 클릭합니다. |
| 2 | <**URL 정보 위장**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**URL 정보 위장 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** URL 정보 위장 기능을 활성화할 것인지 지정합니다.<br>• **보안 로그** 요청 또는 응답에 대해 URL 정보 위장 기능이 동작한 경우, 해당 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application - 로그**] 메뉴 또는 [**System - 통합로그**] 메뉴에서 확인할 수 있습니다. |

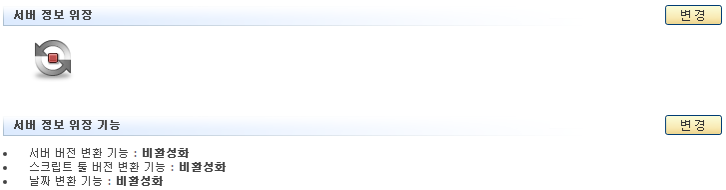
# 서버 정보 위장 기능 설정

서버 정보 위장 기능은 클라이언트에게 전송되는 웹 서버의 주요 정보들을 변환하거나 숨기거나 삭제하여 외부에 유출되는 것을 방지하는 기능입니다. 이 절에서는 서버 정보 위장 기능을 설정하는 화면과 설정하는 과정에 대해 살펴본 후 서버 정보 위장 기능을 설정하는 방법을 살펴봅니다.

## 설정 개요

### 설정 화면

**Application - 위장 - Server정보위장** 메뉴를 클릭하면 서버 정보 위장 기능의 현재 설정 정보를 보여주는 화면이 나타납니다.




화면의 각 부분에서 보여주는 설정 정보는 다음과 같습니다.

- **서버 정보 위장** 서버 정보 위장 기능의 활성화 상태와 관련 기능의 활성화 상태가 표시됩니다. 서버 정보 위장 기능의 사용 여부는 아이콘으로 표시됩니다. 은 활성화 상태를 나타내고 는 비활성화 상태를 나타냅니다.
- **서버 정보 위장 기능** 서버의 버전, 스크립트 툴 버전과 날짜 정보를 각각 삭제하거나 위장할 것인지의 여부가 표시됩니다.

### 설정 과정

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

❶ 서버 정보 위장 설정
서버의 버전, 스크립트 툴 버전과 삭제된 날짜 정보를 각각 위장할 것인지의 여부와 변환하거나 삭제하는 등 위장 방법을 지정합니다. 기본적으로 이 항목들은 모두 비활성화되어 있습니다.

❷ 관련 기능의 활성화 상태 설정
서버 정보 위장 기능의 사용 여부와 이 기능에 대한 통계 기능의 사용 여부를 지정합니다. 기본적으로 모두 비활성화되어 있습니다.

# 서버 정보 위장 기능 설정하기

이 절에서는 위장 기능을 통해 서버의 정보를 보호하기 위한 설정 방법에 대해 살펴봅니다.

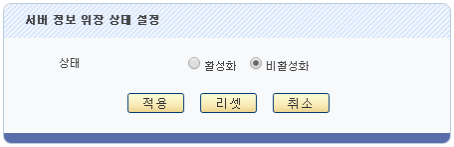
## 서버 정보 위장 설정

위장 기능 중에서 서버 정보 위장 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **위장** - **Server정보위장** 메뉴를 클릭합니다. |
| 2 | <**서버 정보 위장 기능**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**서버 정보 위장 기능 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목의 값을 설정하고 [**확인**] 버튼을 클릭합니다.<br>  <br>• **서버 버전 변환**<br>서버의 버전 정보를 변환할지를 지정합니다. 활성화를 선택하면 서버의 버전 정보 변환 설정 항목들이 설정할 수 있도록 활성화됩니다. (기본값: 비활성화)<br>서버의 버전 정보를 변환하는 방법은 다음과 같은 2가지가 있습니다.<br>– 변환 서버 버전 정보를 다른 정보로 대체하려면 이 항목을 선택하고 오른쪽에 있는 텍스트 박스에 대체할 정보를 입력합니다.<br>– 삭제 서버 버전 정보를 삭제하려면 이 항목을 선택합니다.<br>• **스크립트 툴 버전 변환**<br>서버의 스크립트 툴 정보를 변환할지를 지정합니다. 활성화를 선택하면 서버의 버전 정보 변환 설정 항목들이 설정할 수 있도록 활성화됩니다. (기본값: 비활성화)<br>서버의 스크립트 툴 정보를 변환하는 방법은 다음과 같은 2가지가 있습니다.<br>– 변환 서버 스크립트 툴 정보를 다른 정보로 대체하려면 이 항목을 선택하고 오른쪽에 있는 텍스트 박스에 대체할 정보를 입력합니다.<br>– 삭제 서버 스크립트 툴 정보를 삭제하려면 이 항목을 선택합니다.<br>• **날짜 변환**<br>서버의 날짜 정보를 삭제할지를 지정합니다. (기본값: 비활성화) |

### 관련 기능의 활성화 상태 설정

서버 정보 위장 기능을 설정하고 나면 다음과 같은 방법으로 서버 정보 위장 기능의 사용 여부를 지정합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **위장** - **Server정보위장** 메뉴를 클릭합니다. |
| 2 | <**서버 정보 위장**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**서버 정보 위장 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목의 활성화 상태를 지정한 후 [**적용**] 버튼을 클릭합니다. 기본적으로 모든 항목은 비활성화되어 있습니다.<br>  <br><br>• **상태** 서버 정보 위장 기능의 사용 여부를 지정합니다. |

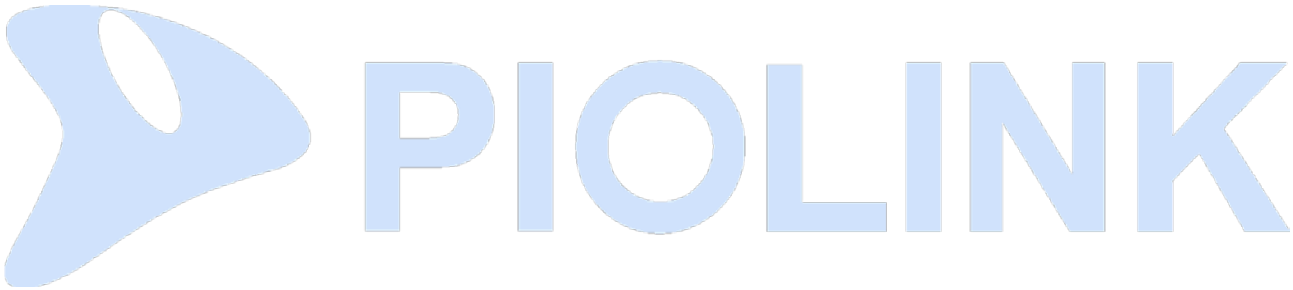
# 제7장 부하 분산 설정

부하 분산은 자신을 통해 전송되는 인터넷 트래픽을 IP 패킷 데이터의 영역까지 검사하여 트래픽을 가장 적절한 웹 서버로 보내고, 서비스를 제공하지 않을 트래픽은 차단시켜주는 L7 부하 분산 기능입니다. 이 장에서는 WEBFRONT-K가 제공하는 부하 분산 기능을 설정하는 방법을 상세하게 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

- 설정 과정
- 패턴 설정
- 실제 서버 설정
- 그룹 설정
- 규칙 설정
- 장애 감시 설정
- 소스 NAT 설정

**참고:** 부하 분산 기능에 대한 상세한 설명은 이 설명서와 함께 제공되는 **WEBFRONT-K 소개서**의 [**제6장 WEBFRONT-K 고가용성 기능 - 서버 부하 분산**] 부분을 참고합니다.



# 설정 과정

부하 분산 기능은 부하 분산 규칙에 근거하여 요청 패킷을 전송할 실제 서버 또는 그룹을 선택합니다. 부하 분산 규칙은 우선 순위, 패턴과 그룹으로 구성되는데, 특정 패턴을 가진 요청 패킷은 특정 실제 서버 그룹 또는 실제 서버로 전송되도록 합니다. WEBFRONT-K가 클라이언트로부터 요청을 받으면 우선 순위가 높은 부하 분산 규칙부터 적용됩니다.

WEBFRONT-K의 부하 분산 기능은 다음과 같은 과정에 따라 설정합니다.

❶ 패턴 설정

먼저 부하 분산 서비스를 적용할 요청 패킷을 선택할 때 사용할 패턴을 정의합니다. 패턴은 다음과 같은 매치 종류(type), 매치 방법(match method), 문자열(string)로 구성됩니다.

- **문자열** 패턴의 문자열은 요청 헤더의 필드와 비교할 문자열입니다. 문자열은 정규식으로 정의할 수 있습니다. 정규식에 대한 설명은 이 설명서와 함께 제공되는 WEBFRONT-K 시스템 구성 설명서의 [**제4장 애플리케이션 - 정규식 설정**] 부분을 참고합니다.

- **매치 종류** 매치 종류는 패턴의 문자열과 비교할 요청 헤더의 필드입니다. 매치 종류에는 다음과 같은 5가지가 있습니다.
  - URI HTTP 요청의 URI 필드
  - 호스트 HTTP 요청의 호스트 필드
  - 쿠키 HTTP 요청의 쿠키 필드
  - 사용자-에이전트 필드 HTTP 요청의 사용자-에이전트 필드
  - Accept-Language HTTP 요청의 Accept-Language 필드

- **매치 방법** 매치 방법은 선택한 매치 종류에 해당되는 요청 헤더의 필드와 패턴의 문자열을 비교하는 방법입니다. 매치 방법에는 다음과 같은 4가지가 있습니다.
  - 시작 헤더 필드가 패턴의 문자열로 시작되는지 비교
  - 끝 헤더 필드가 패턴의 문자열로 끝나는지 비교
  - 정규식 헤더 필드가 패턴의 정규식과 일치하는지 비교
  - Any 헤더 필드에 패턴의 문자열을 포함되어 있는지 비교

❷ 실제 서버 설정

실제 서버는 부하 분산 서비스의 대상이 되는 서버를 의미합니다. 실제 서버의 속성에는 IP 주소, TCP 포트 번호와 가중치가 있습니다.

❸ 그룹 설정

❷번 과정에서 등록한 실제 서버로 구성되는 실제 서버 그룹을 설정합니다. 그룹은 컨텐츠 관점에서 동일한 실제 서버들의 집합입니다. 그룹의 속성에는 실제 서버와 부하 분산 알고리즘이 있습니다. 특정 컨텐츠에 대한 클라이언트의 요청이 들어오면 먼저 해당 컨텐츠를 가진 그룹이 선택됩니다. 그런 후에 그룹 설정 시 지정한 부하 분산 알고리즘에 따라 실제 서버가 선택됩니다.

❹ 규칙 설정

서버 그룹을 선택하는데 사용되는 규칙을 설정합니다. 규칙은 이전에 설정해둔 패턴을 사용하여 정의합니다. 규칙을 정의할 때에는 특정 패턴과 일치하는 클라이언트의 요청을 특정한 서버 그룹으로 전송하도록 합니다.

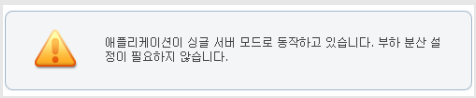
❺ 장애 감시 설정

실제 서버의 동작 상태를 감시하는 장애 감시 기능을 설정합니다. 장애 감시 기능은 부하 분산 서비스가 적용되고 있는 서버의 상태를 주기적으로 검사하여 부하 분산 서비스에 반영합니다. 장애 감시 결과, 서버가 정상적으로 동작하지 않는다고 판단되면, 해당 서버를 실제 서버에서 제외하여 부하 분산이 되지 않도록 합니다. 따라서, 서비스가 이루어지지 않는 서버로 클라이언트의 요청이 전달되는 것을 방지할 수 있습니다.

❻ 소스 NAT 설정 (선택 설정)

WEBFRONT-K 를 One-Armed 구성으로 사용하는 경우에는 소스 NAT 기능의 상태와 소스 NAT IP 주소를 설정합니다. 소스 NAT 기능은 요청 패킷의 출발지 IP 주소를 WEBFRONT-K 에 설정된 소스 NAT IP 주소로 변환하여 웹 서버로 전송 하고, 그에 대한 응답 패킷의 목적지 IP 주소를 클라이언트의 IP 주소로 변환하여 전송합니다.

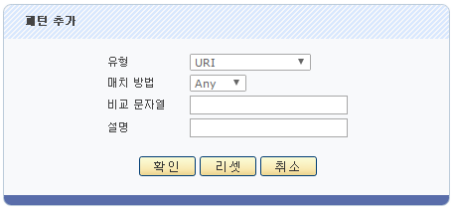
**참고:** 부하 분산 기능은 애플리케이션이 **부하 분산** 모드인 경우에만 설정할 수 있습니다. 애플리케이션이 **일반** 모드로 설정되어 있을 때 부하 분산 메뉴를 클릭하면 다음과 같은 알림 메시지가 나타납니다.




애플리케이션을 부하 분산 모드로 설정하려면 **애플리케이션 - 일반 설정** 메뉴를 클릭한 후 <**애플리케이션 일반 설정 정보**>의 **모드** 항목을 변경하면 됩니다.

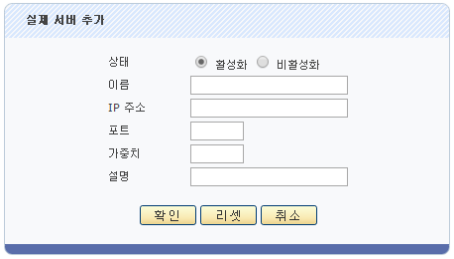
# 패턴 설정

먼저 다음과 같은 방법으로 L7 부하 분산 서비스를 적용할 HTTP 요청을 선택하기 위해 사용할 패턴을 정의합니다. 하나의 애플리케이션에는 최대 256개의 패턴을 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **부하분산** - **패턴** 메뉴를 클릭합니다. |
| 2 | <**패턴 설정**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**패턴 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **유형** 패턴 문자열 항목에서 지정한 문자열을 HTTP 요청 패킷의 어떤 헤더 필드와 비교할 것인지를 선택합니다. 선택할 수 있는 필드는 다음 5가지입니다.<br>– URI URI 필드(기본값)<br>– 호스트 호스트 필드<br>– 쿠키 쿠키 필드<br>– 사용자-에이전트 사용자 에이전트 필드<br>– Accept-Language 수용 언어 필드<br>• **매치 방법** 패턴 문자열 항목에서 지정한 문자열과 위에 있는 유형 항목에서 선택한 필드의 값을 비교할 방법을 선택합니다. 선택할 수 있는 비교 방법은 다음 4가지입니다.<br>– Any 필드에 해당 문자열이 포함되어 있는지 검사합니다(기본).<br>– 시작 필드가 해당 문자열로 시작하는지 검사합니다.<br>– 끝 필드가 해당 문자열로 끝나는지 검사합니다.<br>– 정규식 필드가 지정된 정규식과 일치하는지 검사합니다.<br>• **비교 문자열** 패킷을 분류할 때 비교 대상으로 사용될 문자열을 입력합니다. 문자열은 127자까지 지정할 수 있고, "를 제외한 모든 문자가 포함될 수 있습니다.<br>• **설명** 패턴에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 4 | 패턴 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

# 실제 서버 설정

패턴을 등록한 후에는 다음과 같은 방법을 통해 애플리케이션 서비스를 제공하는 실제 서버를 등록합니다. 하나의 애플리케이션에는 실제 서버를 최대 256개까지 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **부하분산** - **실제서버** 메뉴를 클릭합니다. |
| 2 | <**실제 서버 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**실제 서버 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 등록하고 있는 실제 서버를 실제로 부하 분산 서비스에 적용할 것인지를 지정합니다. 기본적으로는 활성화로 선택되어 있습니다.<br>• **이름** 실제 서버의 이름을 입력합니다. 실제 서버의 이름은 알파벳과 숫자, '-', '_' 문자로 이루어진 최대 16 글자의 문자열을 사용할 수 있습니다. 첫 글자는 반드시 알파벳이어야 합니다.<br>**주의:** 실제 서버의 이름은 한번 지정하면 변경할 수 없으므로 잘못된 이름을 입력하지 않도록 주의합니다.<br>• **IP 주소** 실제 서버의 IP 주소를 입력합니다.<br>• **포트** 실제 서버에서 사용하는 포트를 설정합니다. 지정할 수 있는 범위는 0-65535입니다.<br>• **가중치** 실제 서버에 할당할 가중치를 지정합니다. 가중치는 L7 서버 부하 분산 서비스가 부하 분산 방식으로 가중치 라운드 로빈, 가중치 최소 연결, 최대 가중치를 사용하는 경우에 필요한 값입니다. 사용자가 지정하지 않는 경우에는 기본으로 가중치 '1'이 사용됩니다. 지정할 수 있는 값의 범위는 0~65535입니다.<br>• **설명** 실제 서버에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 4 | 실제 서버 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

# 그룹 설정

실제 서버를 등록한 후에는 다음과 같은 방법으로 동일한 웹 서비스를 제공하는 실제 서버들을 묶어 그룹으로 지정합니다. 하나의 애플리케이션에는 최대 256개의 그룹을 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **부하분산** – **그룹** 메뉴를 클릭합니다. |
| 2 | <**그룹 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**그룹 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 설정하고 있는 실제 서버 그룹을 실제로 부하 분산 서비스에 적용할 것인지를 지정합니다. 기본적으로는 활성화로 선택되어 있습니다.<br>• **이름** 그룹의 이름을 입력합니다. 그룹의 이름은 알파벳과 숫자, '-', '_' 문자로 이루어진 최대 16 글자의 문자열을 사용할 수 있습니다. 첫 글자는 반드시 알파벳이어야 합니다.<br>• **부하 분산 알고리즘** 드롭다운 목록을 클릭한 후, 그룹에 속한 서버로 부하를 분산시킬 때 사용할 부하 분산 방식을 선택합니다. 선택할 수 있는 부하 분산 방식에는 라운드 로빈, 가중치 라운드 로빈, 최소 연결, 가중치 최소 연결, 해싱, URL 해싱, 최대 가중치, 목적지 IP 유지가 있습니다. 사용자가 지정하지 않는 경우 기본으로 설정되는 부하 분산 방식은 '라운드 로빈'입니다.<br>• **설명** 그룹에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다.<br>• **실제 서버 리스트** [**선택**] 버튼을 클릭하면 현재 등록된 실제 서버 리스트를 보여주는 <**실제 서버 선택**> 팝업 창이 나타납니다. 그룹에 포함시킬 실제 서버를 리스트에서 선택한 후 [**확인**]을 클릭합니다. 그룹을 설정하기 전에 반드시 실제 서버를 추가해야 합니다. |
| 4 | 그룹 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

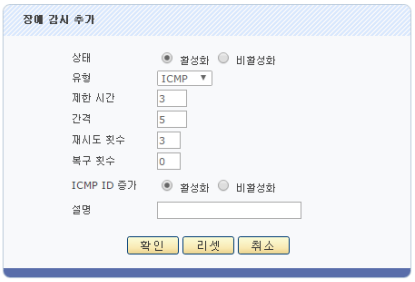
# 규칙 설정

그룹을 선택하는 데 사용할 규칙을 정의하는 방법은 다음과 같습니다. 하나의 애플리케이션에는 최대 256개의 규칙을 추가할 수 있습니다.

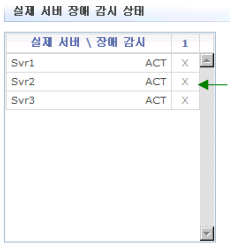
| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **부하분산** – **규칙** 메뉴를 클릭합니다. |
| 2 | <**규칙 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**규칙 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 설정하고 있는 규칙을 실제로 부하 분산 서비스에 적용할 것인지를 지정합니다. 기본적으로는 활성화로 선택되어 있습니다.<br>• **우선 순위** 규칙의 우선 순위를 지정합니다. 규칙의 우선 순위는 그룹에 여러 개의 규칙이 정의되어 있는 경우, 우선적으로 적용할 규칙을 결정할 때 사용됩니다. 지정할 수 있는 값의 범위는 0-255이고, 기본으로 설정되는 값은 '1'입니다.<br>• **설명** 규칙에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다.<br>• **패턴 리스트** 규칙에서 사용할 패턴을 선택합니다. 하나의 규칙에는 최대 2개의 패턴을 사용할 수 있습니다. [**선택**] 버튼을 클릭하면 현재 정의된 패턴 리스트를 보여주는 <**패턴 선택**> 팝업 창이 나타납니다. 리스트에서 원하는 패턴을 선택한 후 [**확인**]을 클릭합니다. 설정된 패턴이 없는 경우에는 '패턴 설정' 절의 내용을 참고하여 먼저 패턴을 정의해야 합니다.<br>• **그룹** 현재 설정 중인 규칙을 적용할 그룹을 선택합니다. [**선택**] 버튼을 클릭하면 현재 정의된 그룹리스트를 보여주는 <**그룹 선택**> 팝업 창이 나타납니다. 리스트에서 원하는 그룹을 선택한 후 [**확인**]을 클릭합니다. 설정된 그룹이 없는 경우에는 '그룹 설정' 절의 내용을 참고하여 먼저 그룹을 정의해야 합니다. |
| 4 | 그룹 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

# 장애 감시 설정

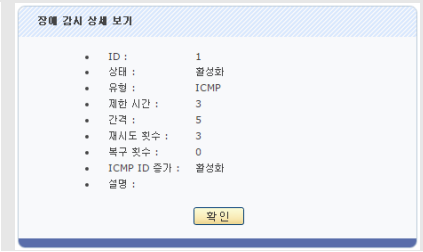
장애 감시 기능을 설정하는 방법은 다음과 같습니다. 하나의 애플리케이션에는 최대 256개의 장애 감시를 추가할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **부하분산** – **장애감시** 메뉴를 클릭합니다. |
| 2 | <**장애 감시 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**장애 감시 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br>• **상태** 현재 설정 중인 장애 감시 설정을 부하 분산 서비스에 바로 적용할 것인지 여부를 선택합니다. 바로 적용하는 경우에는 '활성화'를, 바로 적용하지 않는 경우에는 '비활성화'를 선택합니다. 사용자가 지정하지 않으면 기본으로 '활성화'가 선택됩니다.<br>• **유형** 드롭다운 목록을 클릭한 후, 서버의 장애 감시 방식을 선택합니다. 장애 감시 방식은 사용하는 프로토콜의 종류에 따라 ICMP, TCP, HTTP 장애 감시가 있습니다. 선택한 장애 감시 유형에 따라 나머지 설정 항목이 달라집니다.<br>**ICMP**<br>– **ICMP ID 증가**<br>'ICMP ID 증가' 기능의 활성화 여부를 선택합니다. ICMP ID 증가는 ICMP 프로토콜로 서버의 장애를 감시할 때 전송하는 ICMP 패킷의 ID를 증가시키는 기능입니다. 기본적으로는 ICMP 패킷의 ID가 증가되지 않도록 ICMP ID 증가 기능이 비활성화되어 있습니다.<br>**TCP**<br>– **포트**<br>장애 감시 패킷을 전송할 포트 번호를 0~65535 사이의 값으로 지정합니다. 기본으로 설정된 값은 '0'입니다.<br>**HTTP**<br>– **포트**<br>장애 감시 패킷을 전송할 포트 번호를 0~65535 사이의 값으로 지정합니다. 기본으로 설정된 값은 0입니다.<br>– **URL**<br>HTTP 프로토콜로 서버의 장애를 감시할 때 데이터를 가져올URL을 설정합니다.<br>– **Domain**<br>HTTP 프로토콜로 서버의 장애를 감시할 때 사용할 도메인을 설정합니다. 도메인을 지정하면 지정한 도메인의 URL로부터 데이터를 가져옵니다. URL은 반드시 지정해야 하지만 도메인은 반드시 설정하지 않아도 됩니다.<br>• **제한 시간** 서버의 장애 여부를 판단하는 타임아웃 값을 0~10초 사이의 값으로 지정합니다. 서버로 장애 감시 패킷을 전송한 후 지정된 타임아웃이 경과할 때까지 서버로부터 응답이 없는 경우에는 서버에 장애가 발생한 것으로 판단합니다. 기본 값은 '3'초입니다.<br>• **간격** 서버의 장애를 판단하기 위해 장애 감시 패킷을 서버로 전송하는 주기를 1~60초 사이의 값으로 설정합니다. 장애 감시 패킷을 수신한 서버는 즉시 그에 대한 응답 패킷을 전송하게 됩니다. 전송 주기가 짧을수록 서버의 장애 여부를 정확하게 파악할 수 있지만, 장애 감시 패킷과 응답 패킷이 네트워크의 부하가 될 수 있으므로 네트워크 상태에 따라 적절한 값으로 설정하도록 합니다. 기본으로 설정된 값은 '5'초입니다.<br>• **재시도 횟수** 장애 감시 패킷의 재전송 횟수를 0~5 범위의 값으로 지정합니다. 이 값은 아래에 있는 복구 횟수 항목의 값과는 반대되는 값으로, 장애 감시 패킷에 대한 응답을 보내지 못한 서버의 장애 여부를 보다 확실하게 확인하기 위해 추가로 장애 감시 패킷을 몇 번 더 보낼 것인지를 나타냅니다. 기본으로 설정된 값은 '3'입니다.<br>• **복구 횟수** 서버가 다시 복구되었는지 판단하기 위해 추가로 장애 감시 패킷을 전송할 횟수를 0~5 범위의 값으로 지정합니다. 장애가 발생했던 서버에게 이 명령으로 설정한 횟수만큼 장애 감시 패킷을 보낸 후 응답이 계속 수신되면 해당 서버가 정상적으로 복구되었다고 판단하게 됩니다. 기본으로 설정된 값은 '0'입니다.<br>• **설명** 장애 감시에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. |
| 4 | 장애 감시 설정을 시스템에 적용하기 위해 [**적용**] 버튼을 클릭합니다. |

**참고:** <**실제 서버 장애 감시 상태**> 부분에 장애 감시를 통해 파악된 각 실제 서버의 상태가 표시됩니다. <**장애 감시 리스트**>의 [**상세보기**] 버튼을 클릭하면 해당 장애 감시의 상세한 설정 정보를 볼 수 있습니다.




장애 감시 결과.
정상적인 실제 서버는 O로, 비정상적인 실제 서버는 'X'로 표시됩니다. 장애 감시가 수행되기 전에는 이와 같이 X로 표시됩니다.

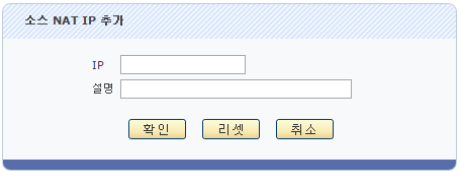


# 소스 NAT 설정

소스 NAT 기능을 사용하기 위해서는 소스 NAT IP 주소를 설정하고, 소스 NAT 상태를 활성화해야 합니다.

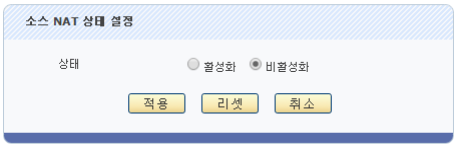
## 소스 NAT IP 주소 설정

소스 NAT IP 주소를 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** – **부하분산** – **소스NAT설정** 메뉴를 클릭합니다. |
| 2 | <**소스 NAT IP 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**소스 NAT IP 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **IP** 요청 패킷의 출발지 주소로 변환할 IP 주소를 입력합니다.<br>• **설명** 소스 NAT IP 주소에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |

## 소스 NAT 상태 활성화

소스 NAT 상태를 활성화하는 방법은 다음과 같습니다. 기본적으로는 비활성화되어 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** – **부하분산** – **소스NAT설정** 메뉴를 클릭합니다. |
| 2 | <**소스 NAT 상태**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**소스 NAT 상태 설정**> 팝업 창에서 상태를 활성화로 변경하고 [**적용**] 버튼을 클릭합니다.<br>  <br> |

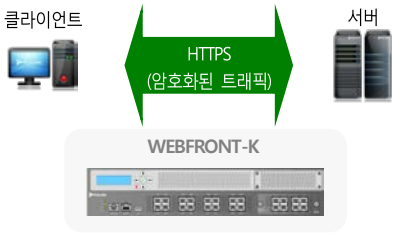
# 제8장 SSL 기능 설정

SSL(Secure Sockets Layer) 기능은 WEBFRONT-K를 통해 전송되는 패킷을 암호화(encryption)하거나 복호화(decryption)하여 패킷의 안전성과 신뢰성을 보장할 수 있는 기능입니다. 이 장에서는 WEBFRONT-K가 제공하는 SSL 기능을 설정하는 방법에 대해 상세히 살펴봅니다.

이 장은 다음 내용으로 구성되어 있습니다.

# 개요

SSL은 각종 해킹으로부터 트래픽을 보호하기 위해 클라이언트와 서버가 암호화된 트래픽(HTTPS)을 주고 받을 수 있게 해주는 프로토콜입니다. WEBFRONT-K는 이러한 SSL 프로토콜을 지원하기 위해 하드웨어 SSL 가속기를 제공합니다.




WEBFRONT-K의 SSL 가속기는 클라이언트로부터 수신된 HTTPS 트래픽을 HTTP로 변환(복호화)하여 서버로 전송하고, 서버에서 수신한 트래픽을 HTTPS로 변환(암호화)하여 클라이언트로 전송합니다. 이러한 트래픽 변환 작업들은 SSL 가속기에서 전담하여 처리하기 때문에 SSL로 인해 가중되는 CPU의 부하가 없어 기존 기능들의 성능에 전혀 영향을 주지 않습니다.

## 백엔드 기능

백엔드 기능은 다음과 같이 서버와 WEBFRONT-K 간에도 암호화된 HTTPS 트래픽을 전송하는 기능입니다.


SSL 기능은 일반적으로 클라이언트와 통신시에만 트래픽을 HTTPS로 암호화하고, 서버와는 HTTP 트래픽을 송수신합니다. 대개의 경우, 클라이언트의 트래픽이 공격의 대상이 되는데다 서버와의 통신에도 HTTPS로 암호화하면 성능이 매우 낮아지기 때문입니다. 하지만, 이미 SSL 기능을 사용 중인 클라이언트-서버 환경에서 WEBFRONT-K의 SSL 기능으로 대체하고자 하는 경우에는 백엔드 기능을 활성화하면 서버의 설정을 변경할 필요가 없으므로 설치가 간편해집니다.

백엔드 기능을 사용하지 않는 경우에는 클라이언트와 WEBFRONT-K간에는 HTTPS 트래픽이, WEBFRONT-K와 서버 간에는 HTTP 트래픽이 송수신됩니다.

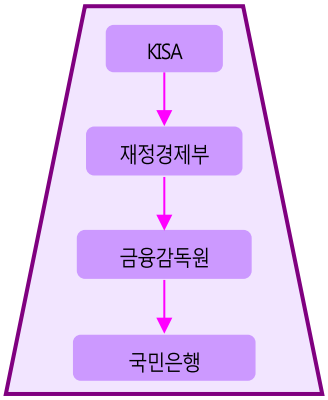
## 키(key)와 인증서(certificate)

WEBFRONT-K의 SSL 기능을 사용하려면 키와 인증서를 WEBFRONT-K에 등록해야 합니다. 키와 인증서는 WEBFRONT-K가 클라이언트/서버와 SSL 접속 준비 과정(SSL handshaking)을 수행할 때 사용됩니다. 키는 SSL 접속 준비 과정 중에 주고 받는 데이터를 암호화할 때, 인증서는 서버가 믿을 수 있는지 검증할 때 사용합니다.

키는 사용자가 생성하지만, 인증서는 인증 기관으로부터 발급 받아야 합니다. 인증 기관으로부터 인증서를 발급 받기 위해서는 CSR(Certificate Signing Request)이라는 인증 요청서를 인증 기관에 접수해야 합니다. 인증 요청서는 WEBFRONT-K에서 생성할 수 있습니다. 인증 기관으로부터 발급 받은 인증서는 SSL 기능을 사용하기 전에 WEBFRONT-K에 등록해야 합니다.

### 인증서 체인

WEBFRONT-K에는 단일 인증서나 인증서 모음인 인증서 체인(chain)을 등록할 수 있습니다. 인증서 체인은 연속적인 인증 기관이 서명한 일련의 인증서로 계층적인 구조를 가집니다. 계층 구조의 상위에 있는 인증서가 하위에 있는 기관을 인증해줍니다. 예를 들어, 클라이언트의 PC에 재정경제부를 신뢰할 수 있는 인증서가 있고, 클라이언트가 국민은행을 통해 인터넷 뱅킹을 수행하는 경우를 가정해봅니다. 클라이언트가 국민은행 서버에 접속했을 때 국민은행 서버는 다음과 같은 인증서 체인을 클라이언트에게 보냅니다.




이 인증서 체인을 통해 국민은행의 인증서는 금융 감독원의 인증서에 의해 인증되고, 다시 금융감독원의 인증서는 클라이언트가 신뢰하는 재정경제부의 인증서에 의해 인증됩니다. 따라서, 클라이언트는 접속한 서버가 믿을 수 있는 국민은행 서버라는 것을 확신하고 인터넷 뱅킹을 수행하게 됩니다.

인증 기관에서 발급하는 대부분의 인증서는 서버의 인증서와 인증 기관을 인증해주는 인증서가 포함되어 있는 인증서 체인입니다. 만약, 인증 기관에서 서버의 인증서만 보내주면 인증 기관에 연락하여 인증 기관의 인증서를 받아야 합니다. 그리고, 서버의 인증서와 인증 기관의 인증서를 합쳐서 하나의 인증서 체인으로 만든 후에 WEBFRONT-K에 등록해야 합니다.

**참고:** 이후 이 설명서에서는 단일 인증서와 인증서 체인을 모두 '인증서'로 지칭합니다.

**참고:** 이미 SSL 기능을 사용 중인 서버에 WEBFRONT-K의 SSL 기능을 적용하는 경우에는 새로 인증서를 발급 받을 필요 없이 서버에 등록된 키와 인증서를 다운로드하여 WEBFRONT-K에 등록하면 됩니다. WEBFRONT-K는 현재 PEM 형식의 인증서만 지원하므로 WEBFRONT-K에 등록하기 전에 인증서의 형식을 확인하도록 합니다. PEM 형식 이외의 인증서를 사용하는 경우에는 파이오링크의 기술 지원 센터(support@piolink.com)로 인증서를 보내시면 PEM 형식으로 변환하여 보내드립니다. PEM 형식 이외의 인증서는 차후에 지원될 예정입니다.

### 임시 인증서

임시 인증서는 WEBFRONT-K가 생성하는 인증서로, 인증 기관에서 발급 받은 공인 인증서 대신 내부에서 사용할 수 있는 자체 서명 인증서(Self-Signed Certificate)입니다. 임시 인증서는 테스트용이나 인증 요청서로만 사용해야 합니다.

### 인증서 관리

WEBFRONT-K에 등록된 키와 인증서, 인증 요청서는 별도의 파일로 사용자 PC에 다운로드할 수 있습니다. 키와 인증서는 하나의 파일로 합쳐져서 다운로드됩니다. 그리고, 키, 인증서, 인증 요청서는 각각의 내용을 다음과 같이 텍스트 형태로 볼 수 있습니다.

# SSL 기능 설정

## 설정 과정

WEBFRONT-K에 SSL 기능을 설정하는 과정은 다음과 같습니다.

1. 애플리케이션 유형 설정
2. 키와 인증서 등록
    2.1. 키와 임시 인증서(인증 요청서) 생성
    2.2. 인증서 발급
    2.3. 비밀 키와 인증서 등록
3. 부가 기능 설정
4. SSL 고급설정
5. Request Buffering 예외 URL 리스트
6. SSL 기능 활성화

### 애플리케이션 설정

WEBFRONT-K의 SSL 기능은 애플리케이션별로 설정합니다. 애플리케이션에 SSL 기능이 활성화되면, 애플리케이션의 트래픽 중에서 HTTPS 유형의 트래픽에만 SSL 기능이 적용됩니다. 예를 들어, 아래 그림과 같이 애플리케이션이 설정되어 있는 경우, 10.1.1.1로 수신된 트래픽 중에서도 443 포트로 수신된 트래픽에만 SSL 기능이 적용되고 80 포트로 수신된 트래픽에는 적용되지 않습니다. 애플리케이션 유형을 설정하는 방법은 [**제2장 애플리케이션 기본 설정 – 일반 설정 – 일반 애플리케이션 설정하기 - 애플리케이션 IP 주소와 포트 설정**] 부분을 참고합니다.

## 키와 인증서 등록

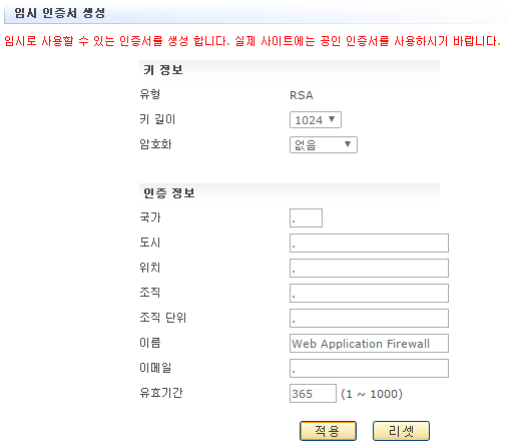
WEBFRONT-K의 SSL 기능이 동작하려면 키와 인증서가 WEBFRONT-K에 등록되어 있어야 합니다. 키는 인증 요청서를 만들 때 생성됩니다. 인증서는 베리사인(www.verisign.com)이나 한국 전자 인증(www.crosscert.com), 코모도(www.comodo.com)와 같은 인증 기관을 통해 발급 받아야 합니다.

### 키와 임시 인증서(인증 요청서) 생성하기

내부적인 SSL 기능 테스트용 인증서나 인증 요청서로 사용할 수 있는 임시 인증서를 생성하는 방법은 다음과 같습니다.

**참고:** 임시 인증서는 WEBFRONT-K에 인증서가 등록되어 있지 않은 경우에만 생성할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **임시인증서생성** 메뉴를 클릭합니다. |
| 2 | <**임시 인증서 생성**> 화면에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다. |




- **키 길이** 드롭다운 목록에서 키의 크기를 지정합니다. 지정할 수 있는 키의 크기는 1024bits, 2048bits가 있습니다. 키의 크기가 클수록 보안성이 뛰어나지만 그만큼 성능이 낮아지게 되므로, 네트워크와 클라이언트, 서버의 특성 등으로 고려하여 적절한 크기로 지정하도록 합니다. 기본 값은 1024bits입니다.
- **암호화** 드롭다운 목록에서 키를 암호화할 알고리즘을 지정합니다. 지정할 수 있는 알고리즘에는 'DES', '3DES', 'AES128', 'AES192', 'AES256'이 있습니다. 각각'DES 알고리즘', 'Triple DES 알고리즘', '128비트 AES 알고리즘', '192비트 AES 알고리즘', '256비트 AES 알고리즘'을 나타냅니다. 암호화하지 않는 경우에는 '없음'을 선택합니다. 암호화 알고리즘을 선택하면 인증 암호 항목에 암호화 시 사용할 암호를 입력해야 합니다. (기본값: 없음)

  **주의:** 암호화되지 않은 키가 유출되면 인증서가 위조될 가능성이 있으므로 암호화 알고리즘을 지정하기를 권장합니다.

- **인증 암호** 키를 암호화할 때 사용할 암호를 입력합니다. 암호는 특수 문자나 공백이 모두 허용되는데, 다른 사람이 짐작하기 힘들도록 가급적 긴 문장을 사용하는 것이 좋습니다. 이 암호는 인증서를 발급 받은 후 WEBFRONT-K에 인증서를 등록할 때 입력해야 하므로 반드시 따로 기록을 해두어야 합니다. 암호를 분실하면 알아내거나 수정할 수 없기 때문에 다시 인증서를 발급 받아야 합니다.
- **국가** 인증서에 입력할 국가 이름을 지정합니다. 해당 국가의 두 자리(2-bit) 문자 코드를 입력합니다.
- **도시** 인증서에 입력할 도나 시 이름을 지정합니다(예: Seoul). 공백이나 특수 문자가 포함된 지역 이름도 입력할 수 있습니다. 지역 ~ 이메일 주소 항목들도 마찬가지로 공백이나 특수 문자를 입력할 수 있습니다.
- **위치** 인증서에 입력할 도시(구/군) 이름을 지정합니다. (예: Geumchon-Gu)
- **조직** 인증서에 입력할 조직이나 회사 이름을 지정합니다. (예: PIOLINK, Inc.)
- **조직 단위** 인증서에 입력할 조직이나 회사의 부서 이름을 지정합니다. (예: Smart Development team).
- **이름** 인증서에 입력할 사용자의 이름 또는 도메인 주소를 지정합니다. 일반적으로 www.piolink.com나 *.piolink.com과 같은 도메인 이름을 인증서의 이름으로 지정합니다. 접속하려는 도메인 이름이 인증서의 이름과 다르면 웹 브라우저에서 피싱(Phishing)으로 의심하여 경고 메시지를 출력하므로 정확한 도메인 이름을 입력하도록 합니다.

  **참고**: 와일드 카드(*)가 포함된 도메인에 대한 인증서의 발급 여부는 인증 기관마다 다르므로 먼저 인증 기관에 문의하도록 합니다.

- **이메일** 인증서를 수신할 웹 마스터나 시스템 관리자의 이메일 주소를 입력합니다.
- **유효기간** 인증서의 유효 기간을 지정합니다. (설정 범위: 1 ~ 1,000일, 기본값: 365일)

## 인증서 발급받기

인증 기관 홈페이지에 접속하여 인증서를 신청합니다.

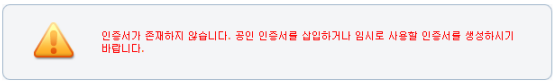
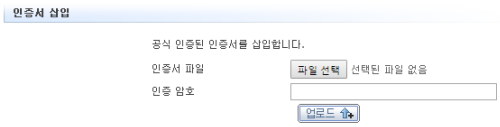
**참고:** WEBFRONT-K에서 CSR을 생성한 경우 CSR을 복사하는 방법은 다음과 같습니다.

1. **Application** - **SSL** - **인증서 관리** 메뉴를 선택합니다.
2. <**인증서 정보**> 화면에서 인증 요청서를 다운로드합니다.


3. 다운로드한 인증 요청서(ssl_cgi 파일로 저장)를 메모장과 같은 ASCII 텍스트 편집기에서 연 후, 전체 내용을 선택하여 **CSR 정보 입력** 항목에 복사합니다.

## 인증서 등록하기

인증 기관에서 발급 받은 인증서를 사용자 PC에 저장한 후 키와 인증서를 하나의 인증서 파일로 합칩니다. 키와 인증서는 텍스트 파일이므로 메모장과 같은 텍스트 편집기에서 쉽게 하나의 파일로 합칠 수 있습니다. 그런 후에 다음과 같은 방법으로 이 인증서를 WEBFRONT-K에 등록합니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **인증서관리** 메뉴를 클릭합니다. |
| 2 | 키나 인증서가 등록되어 있지 않은 경우에는 <**인증서 삽입**> 화면이 나타납니다. 인증서 파일 항목에 있는 [**파일 선택**] 버튼을 클릭합니다.<br>  <br><br>  <br><br>**참고:** 키나 인증서가 등록되어 있는 경우에는 <**인증서 정보**> 화면이 나타납니다. [**변경**] 버튼을 클릭하면 <**인증서 삽입**> 화면이 나타납니다. |
| 3 | <**파일 선택**> 팝업 창에서 인증서 파일(키와 인증서가 합쳐진 파일)이 저장된 폴더에서 인증서 파일을 선택한 후 [**열기**] 버튼을 클릭합니다. |
| 4 | <**인증서 삽입**> 화면에서 [**업로드**] 버튼을 클릭합니다. |

**참고:** SSL 하드웨어 가속기가 장착되어있지 않으면 다음과 같은 메시지가 출력되며 SSL 기능을 설정할 수 없습니다.

## 부가 기능 설정

다음과 같은 SSL 부가 기능들을 설정할 수 있습니다.

- **세션 재사용**
  세션 재사용은 클라이언트가 동일한 서버로 다시 접속하는 경우, 이전 접속 시 사용했던 세션(클라이언트와 WEBFRONT-K간에 맺어졌던) 정보를 활용하여 클라이언트와의 접속 준비 과정을 간소화 해주는 기능입니다. 세션 재사용 기능을 사용하면 클라이언트와 SSL 접속을 준비하는 과정에서 송수신되는 데이터의 양이 줄어들기 때문에 WEBFRONT-K의 성능에 도움을 줄 수 있습니다. 세션 재사용 기능은 반복적인 SSL 접속 준비 과정을 생략하여 WEBFRONT-K의 부하를 줄일 수 있지만, 보안성이 떨어지고 성능에 별다른 영향을 주지 않는 1024bit의 키를 사용하는 경우에는 큰 효과가 없습니다. 세션 재사용 기능에 의해 재사용될 SSL 세션의 정보는 SSL 세션 정보 풀(pool)에 저장됩니다. SSL 세션 정보 풀에는 최대 30,000개의 SSL 세션에 대한 정보가 저장될 수 있고 저장된 정보는 60초까지 유효합니다.
- **최대 세션 개수**
  최대 세션 개수는 SSL 세션의 개수가 지정한 최대 세션 수에 도달하면 이 후 만들어지는 새로운 세션에는 SSL 기능을 적용하지 않도록 하는 기능입니다.
- **웹서버 응답 대기 시간**
  웹서버 응답 대기 시간은 클라이언트의 요청에 대한 웹서버의 응답 시간을 설정하는 기능입니다. 설정한 대기 시간을 초과할 때까지 응답하지 못할 경우, 클라이언트로 504 Gateway Timeout 페이지를 반환합니다.
- **Connection Pooling**
  Connection Pooling은 클라이언트와 WEBFRONT-K, 그리고 웹서버 간 TCP 커넥션을 연결할 때, 매번 새로운 커넥션을 연결하는 것이 아니라 생성된 커넥션을 풀에 저장해 두었다가 클라이언트로부터 요청이 있을 경우 저장해두었던 커넥션을 재사용하는 기능입니다.
- **Request Buffer Size**
  Request Buffer Size는 클라이언트의 요청을 처리할 때 할당되는 메모리 크기를 조절하는 기능입니다.
- **에러시 RESET 종료**
  에러시 RESET 종료는 HTTPS 서비스 중 세션이 비정상적으로 종료될 경우, TCP Reset으로 세션을 종료하는 기능입니다.
- **서버 HTTP Keepalive 제한 시간**
  서버 HTTP Keepalive 제한 시간은 서버측 세션에 대해 일정 시간이 지나면 연결을 종료하는 기능입니다.
- **서버 TCP Keepalive**
  서버 TCP Keepalive는 WEBFRONT-K와 서버측 사이의 세션을 유지하는 기능입니다.

세션 재사용 기능이나 최대 접속 수, 통과 기능과 같은 SSL 기능의 부가 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **일반 설정** 메뉴를 클릭합니다. |
| 2 | <**SSL 설정정보**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**SSL 설정정보 변경**> 화면에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **세션 재사용** 세션 재사용 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **최대 세션 개수** 최대 세션 개수를 지정합니다. (설정 범위: 1 ~ 65,535, 기본값: 30,000)<br>• **웹서버 응답 대기시간** 웹서버 응답 대기 시간을 지정합니다. (설정 범위: 30 ~ 600(초), 기본값: 600)<br>• **Connection Pooling** Connection Pooling 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **Request Buffer Size** Request Buffer Size를 지정합니다. (설정 범위: 1Byte ~ 100Mbyte, 기본값: 1MB):<br>• **에러시 RESET 종료** 에러시 RESET 종료 기능의 사용 여부를 지정합니다. (기본값: 비활성화) |

| | | |
|---|---|---|
| | • **서버 HTTP Keepalive 제한 시간**<br>• **서버 TCP Keepalive** | 서버 HTTP Keepalive 제한 시간을 지정합니다. (설정 범위: 0 ~ 86,400(초), 기본값: 60)<br>서버 TCP Keepalive 시간을 지정합니다. '0'으로 지정하면 기능이 비활성화된 것과 같습니다. (설정 범위: 1 ~ 32,767(초), 기본값: 0) |

## SSL 고급설정

다음과 같은 SSL 고급 기능을 설정할 수 있습니다.

- **서버 구간**
  WEBFRONT-K와 웹 서버간의 SSL 연결 시에 사용하는 프로토콜과 SSL 암호 알고리즘을 지정합니다. SSL 프로토콜은 SSLv3, TLSv1, TLSv1.1, TLSv1.2를 지원합니다.

- **클라이언트 구간**
  WEBFRONT-K와 클라이언트간의 SSL 연결 시에 사용하는 프로토콜과 SSL 암호 알고리즘을 지정합니다. 지원하는 SSL 프로토콜의 종류는 서버 구간과 동일합니다.

- **SSL 버전별 차단**
  SSL 버전별 차단은 특정 SSL 프로토콜 버전에 대한 연결을 차단하는 기능입니다. 차단 방식에는 일반, 리다이렉트, 사용자 정의가 있으며, 차단 시 보안 로그를 남길 수 있습니다.

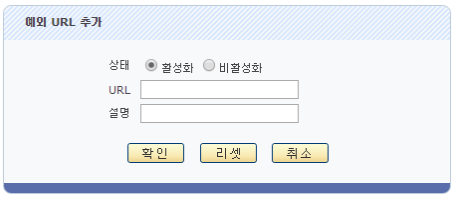
- **DH 파라미터**
  DH 파라미터는 서버 구간 또는 클라이언트 구간의 SSL 암호 알고리즘에 사용하는 디피헬만(Diffie-Hellman) 키를 관리자가 직접 지정하는 기능입니다. SSL 암호 알고리즘에 디피헬만 방식이 포함되어 있지 않을 경우, DH 파라미터는 설정할 필요가 없습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **일반 설정** 메뉴를 클릭합니다. |
| 2 | <**SSL 고급설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **서버 구간**<br>- SSL 프로토콜 서버 구간에서 사용하는 SSL 프로토콜을 지정합니다. 기본적으로 모든 지원 프로토콜이 활성화되어 있습니다.<br>- SSL 암호 알고리즘 서버 구간에서 사용하는 SSL 암호알고리즘을 지정합니다.<br>• **클라이언트 구간**<br>- SSL 프로토콜 클라이언트 구간에서 사용하는 SSL 프로토콜을 지정합니다. 기본적으로 모든 지원 프로토콜이 활성화되어 있습니다.<br>- SSL 암호알고리즘 클라이언트 구간에서 사용하는 SSL 암호알고리즘을 지정합니다.<br>• **SSL 버전별 차단**<br>- 보안로그 SSL 버전별 차단 기능에 의해 연결이 차단된 경우, 보안로그를 기록할 것인지 지정합니다.<br>- 차단 SSL 프로토콜 연결을 차단할 SSL 프로토콜을 지정합니다.<br>- 유형 연결이 차단된 클라이언트에게 전송할 응답 형식을 지정합니다. (일반/리다이렉트/사용자 정의) |

| | |
|---|---|
| | 각 응답 형식에 대한 설명은 **[제2장 애플리케이션 기본 설정 > 응답 설정 > 차단 응답 설정]**을 참고합니다.<br>• **DH 파라미터**<br>- 유형 아래의 DH 키 옵션 중 하나를 선택합니다.<br>- 비활성화 DH 키 유형을 별도로 지정하지 않습니다. (기본값)<br>- 사용자 정의 PEM 형식의 DH 키를 직접 입력합니다.<br>- 1024 1024bit의 DH 키를 사용합니다.<br>- 2048 2048bit의 DH 키를 사용합니다.<br>- 4096 4096bit의 DH 키를 사용합니다. |

### Request Buffering 예외 URL 리스트

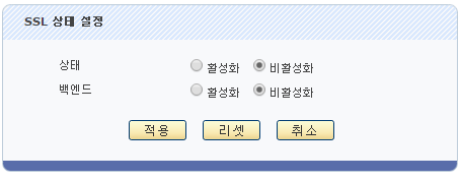
Request Buffering 기능에서 제외할 예외 URL을 설정하는 방법은 다음과 같습니다. 예외 URL은 256개까지 설정할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **일반 설정** 메뉴를 클릭합니다. |
| 2 | <**Request Buffering 예외 URL 리스트**>의 [**변경**] - [**추가**] 버튼을 클릭합니다. |
| 3 | <**예외 URL 추가**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**확인**] 버튼을 클릭합니다.<br>  <br><br>• **상태** 예외 URL의 사용 여부를 지정합니다. (기본값: 활성화)<br>• **URL** Request Buffering 기능에서 제외할 예외 URL을 입력합니다. URL은 최대 1024 글자의 영문자와 숫자, 그리고 '/', '.', '-', '*' 등의 기호로 구성될 수 있습니다. 첫 문자는 반드시 '/'여야 합니다.<br>• **설명** URL에 대한 설명을 입력합니다. 알파벳과 한글로 이루어진 최대 128 글자의 문자열을 입력할 수 있습니다. (선택 설정) |
| 4 | 상태 항목에서 예외 URL의 활성화 여부를 지정합니다. (기본값: 비활성화) |
| 5 | 예외 URL 설정을 시스템에 적용하기 위해 **[적용]** 버튼을 클릭합니다. |

## SSL 기능 활성화

SSL 인증서를 등록하고 부가 기능을 설정한 후에는 SSL 기능을 활성화합니다. 서버와도 HTTPS 트래픽을 송수신하려면 백엔드 기능을 활성화합니다.

**참고:** 인증서가 등록되어 있지 않으면 SSL 기능을 활성화할 수 없습니다. 인증 기관에서 발급 받은 인증서를 등록하거나 WEBFRONT-K에서 임시 인증서를 생성한 후, SSL 기능을 활성화해야 합니다. 임시 인증서를 생성하는 방법은 다음 절인 [**임시 인증서 생성하기**] 절에 설명되어 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **일반 설정** 메뉴를 클릭합니다. |
| 2 | <**SSL**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**SSL 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **상태** SSL 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **백엔드** WEBFRONT-K와 서버 간에도 SSL 기능을 적용하여 HTTPS 트래픽을 송수신하는 백엔드 기능의 사용 여부를 지정합니다. 백엔드 기능을 활성화하면 SSL 성능이 낮아지게 되므로 사용자 네트워크의 트래픽 양과 특성을 잘 고려하여 백엔드 기능의 사용 여부를 결정하도록 합니다. |

**참고:** SSL 하드웨어 가속기가 장착되어있지 않으면 다음과 같은 메시지가 출력되며 SSL 기능을 설정할 수 없습니다.

# 인증서 관리

## 인증서 정보 보기

WEBFRONT-K에 등록된 인증서에 대한 정보를 보려면 **Application** - **SSL** - **인증서관리** 메뉴를 클릭합니다. 그러면, 인증서의 상세 정보를 보여주는 <**인증서 정보**> 화면이 나타납니다.


각 항목은 다음과 같은 정보를 나타냅니다.

- **키 형식** 키의 종류
- **키 길이** 키의 길이(bits)
- **암호화 방법** 키를 암호화한 알고리즘의 종류
- **MD5 지문** MD5 알고리즘을 사용하여 생성된 128bit의 MD5 지문
- **SHA1 지문** SHA-1 알고리즘을 사용하여 생성된 160bit의 SHA-1 지문
- **이름** 인증서를 사용할 대상 도메인 주소
- **발급 대상** 인증서 발급을 요청한 사람 혹은 기관에 대한 정보
- **인증서 발급** 인증서를 발급한 기관
- **발급일** 인증서를 발급한 날짜
- **만료일** 인증서의 효력이 종료되는 날짜
- **X509** [상세보기] 버튼을 클릭하면 인증서를 X509 표준 형식으로 보여줍니다.

키와 인증서, 인증 요청서의 [**상세보기**] 버튼을 클릭하면 비밀 키와 인증서, 인증 요청서 파일의 내용을 보여주는 화면이 나타납니다. 키는 암호화되어 있는 경우에만 [**상세보기**] 버튼이 표시됩니다.

## 인증서와 키 다운로드하기

다음과 같은 방법으로 WEBFRONT-K에 등록된 키와 인증서를 사용자 PC로 다운로드할 수 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **인증서관리** 메뉴를 클릭합니다. |
| 2 | <**인증서 정보**> 화면의 아래 부분에 있는 [**다운로드**] 버튼을 클릭합니다.<br>  |
| 3 | <**파일 다운로드**> 팝업 창의 [**저장**] 버튼을 클릭합니다. |
| 4 | <**다른 이름으로 저장**> 팝업 창에서 파일 이름과 폴더를 지정한 후 [**저장**] 버튼을 클릭합니다. |

## 인증서 삭제하기

WEBFRONT-K에 등록된 인증서를 삭제하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **인증서관리** 메뉴를 클릭합니다. |
| 2 | <**인증서 정보**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**현재 인증서 삭제**>의 [**삭제**] 버튼을 클릭합니다. |

**참고:** 인증서는 SSL 기능이 비활성화되어 있을 때에만 삭제할 수 있습니다. SSL 기능을 비활성화하는 방법은 [**SSL 기능 활성화**] 절을 참고합니다.

# SSL 프로토콜 검사

SSL 프로토콜 검사는 SSL 프로토콜의 대표적인 취약점을 검사하고, SSL 접속 준비 과정(SSL handshaking)에서의 과다 요청을 제어하는 기능입니다.

## SSL 프로토콜 검사 고급 설정

SSL 프로토콜 검사는 다음과 같이 3종류로 나눌 수 있습니다.

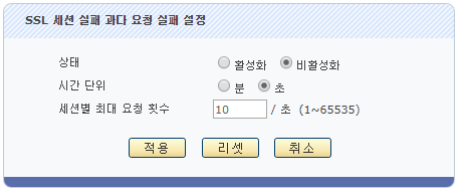
- **대표적인 SSL 취약점 검사**
  Heartbleed 취약점, Poodle 취약점, Freak 취약점, Logjam 취약점, CCS Injection 취약점
- **SSL 에러 탐지 기능**
  프로토콜 위반 취약점, 잘못된 길이 취약점, 버퍼 오버플로 취약점
- **SSL 레코드 프로토콜 및 핸드쉐이크 프로토콜 취약점**
  취약한 레코드 버전 SSLv2, 취약한 레코드 버전 SSLv2, 취약한 Handshake 버전 SSLv2, 취약한 Handshake 버전 SSLv2

SSL 프로토콜 검사 고급 설정 방법은 다음과 같습니다. SSL 프로토콜 검사 고급 설정은 기본적으로 비활성화되어 있습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **SSL 프로토콜 검사** 메뉴를 클릭합니다. |
| 2 | <**SSL 프로토콜 검사 고급 설정**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**SSL 상태 설정**> 팝업 창에서 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  |

## SSL 세션 실패 과다 요청 제어

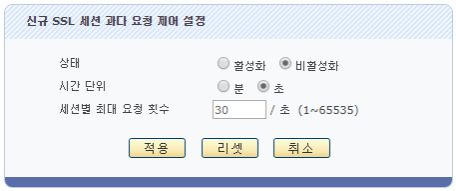
SSL 세션 실패 과다 요청 제어는 SSL 세션 실패 횟수가 최대 허용 횟수를 초과할 경우, 이를 제어하는 기능입니다. SSL 프로토콜 검사 기능 중에서 SSL 세션 실패 과다 요청 제어 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **SSL 프로토콜 검사** 메뉴를 클릭합니다. |
| 2 | <**SSL 세션 실패 과다 요청 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**SSL 세션 실패 과다 요청 실패 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **상태** SSL 세션 실패 과다 요청 제어 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **시간 단위** 세션별 최대 요청 횟수에 적용할 시간 단위를 지정합니다. (기본값: 초)<br>• **세션별 최대 요청 횟수** 세션별로 서비스가 되도록 허용하는 최대 요청 수를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 10) |



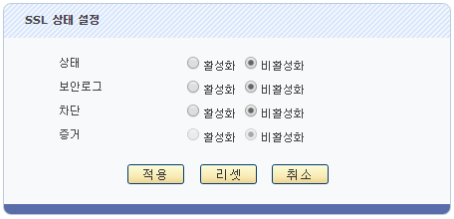
## 신규 SSL 세션 과다 요청 제어

신규 SSL 세션 과다 요청 제어는 SSL 세션 요청 횟수가 최대 허용 횟수를 초과할 경우, 이를 제어하는 기능입니다. SSL 프로토콜 검사 기능 중에서 신규 SSL 세션 과다 요청 제어 기능을 설정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **SSL 프로토콜 검사** 메뉴를 클릭합니다. |
| 2 | <**신규 SSL 세션 과다 요청 제어**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**신규 SSL 세션 과다 요청 제어 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br>• **상태** 신규 SSL 세션 과다 요청 제어 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **시간 단위** 세션별 최대 요청 횟수에 적용할 시간 단위를 지정합니다. (기본값: 초)<br>• **세션별 최대 요청 횟수** 세션별로 서비스가 되도록 허용하는 최대 요청 수를 입력합니다. (설정 범위: 1 ~ 65535, 기본값: 30) |

### 관련 기능의 활성화 상태 설정

SSL 프로토콜 검사 기능의 사용 여부와 보안 로그, 차단, 증거 기능의 활성화 상태를 지정하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **SSL** – **SSL 프로토콜 검사** 메뉴를 클릭합니다. |
| 2 | <**SSL 프로토콜 검사**>의 [**변경**] 버튼을 클릭합니다. |
| 3 | <**SSL 상태 설정**> 팝업 창에서 다음 설명을 참고하여 각 항목을 설정한 후 [**적용**] 버튼을 클릭합니다.<br>  <br><br>• **상태** SSL 프로토콜 검사 기능의 사용 여부를 지정합니다. (기본값: 비활성화)<br>• **보안 로그** SSL 프로토콜 검사 정책을 위반한 요청 패킷에 대해 로그를 기록할 것인지 지정합니다. 기록된 로그는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다.<br>• **차단** SSL 프로토콜 검사 기능에 의해 접근이 제한된 요청 패킷을 차단할 것인지 지정합니다.<br>• **증거** SSL 프로토콜 검사 정책을 위반한 요청 패킷에 대한 증거를 기록할 것인지 지정합니다. 보안 로그는 요청에 대한 주요 정보만 기록하지만, 증거는 패킷의 데이터 내용 등 오탐 여부를 판단하기 위한 근거가 되는 정보를 기록합니다. **보안 로그**의 상태를 활성화한 경우에만 증거의 상태를 지정할 수 있습니다. 기록된 증거는 [**Application** - **로그**] 메뉴 또는 [**System** - **통합로그**] 메뉴에서 확인할 수 있습니다. |

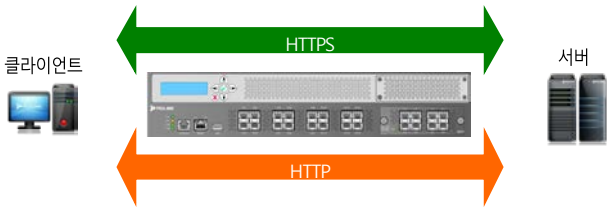
# 설정 시 주의 사항

다음은 SSL 기능 설정 시 주의해야 하는 사항입니다. SSL 기능을 설정하기 전에 반드시 다음 내용을 참고하여 관련된 사항이 있는지 확인하도록 합니다.

### 하나의 도메인에서 HTTP와 HTTPS를 모두 지원하는 경우

하나의 도메인에서 HTTP와 HTTPS를 모두 지원하는 경우, 의도한 방식대로 SSL 기능이 동작하도록 하기 위해서는 설정 시 주의를 기울여야 합니다.

다음 그림과 같이 동일한 도메인으로 클라이언트가 전송한 트래픽을 변환하지 않고 그대로 서버에게 전달하도록 하는 경우(HTTP는 HTTP로, HTTPS는 HTTPS로)에는 **2**개의 애플리케이션을 등록해야 합니다. 각 애플리케이션은 도메인 이름과 목적지 주소가 동일하지만 **포트**는 서로 달라야 합니다. HTTPS 트래픽이 전송될 애플리케이션은 **HTTPS** 유형으로 설정해야 하고 SSL 기능을 사용하기 위해 인증서를 등록해야 합니다. 그리고, 서버와도 HTTPS 트래픽이 송수신되어야 하므로 백엔드 기능을 활성화해야 합니다.



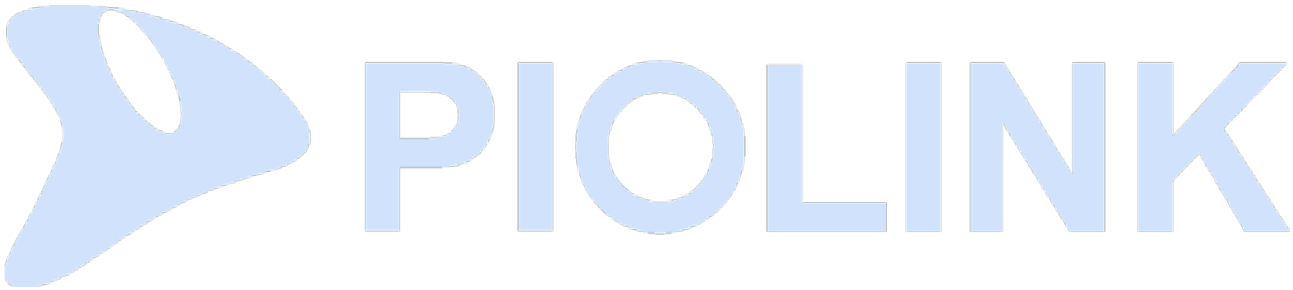

다음 그림과 같이 클라이언트와의 통신에는 HTTP와 HTTPS를 지원하지만 서버와는 HTTP 트래픽을 주고 받는 경우에는 하나의 애플리케이션만 등록하면 됩니다. 대신, 애플리케이션에는 2개의 IP 주소를 포트만 다르게(80, 443)하여 등록해야 하고, SSL 기능을 사용하기 위해 인증서를 등록해야 합니다. 서버와는 HTTP 트래픽이 송수신되므로 백엔드 기능은 비활성화해야 합니다.

# 제9장 애플리케이션 로그

이 장에서는 WEBFRONT-K의 애플리케이션 로그 기능에 대해 살펴본 후, 로그를 설정하는 방법과 사용자가 원하는 로그만을 보여주는 로그 필터를 정의하고 사용하는 방법, 그리고 로그를 화면에 출력하고 출력된 내용을 텍스트 파일로 저장하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.





# 로그 개요

애플리케이션 로그(log)는 WEBFRONT-K의 애플리케이션 보안 기능에 의해 발생하는 각종 이벤트들을 기록한 것입니다. WEBFRONT-K는 애플리케이션 보안 기능이 동작 중에 어떤 이벤트들이 일어났는지 사용자가 알 수 있도록 이벤트에 대한 정보를 모두 로그로 저장할 수 있습니다. 어떤 기능이 언제 수행되었는지 문제가 발생하지는 않았는지, 어떤 보안 기능에 의해 어떤 클라이언트가 보낸 요청이 차단되었는지 등의 이벤트에 대한 정보를 저장된 로그를 통해서 확인할 수 있습니다. 로그는 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.

**참고:** 로그 레벨은 **System** - **통합 로그 설정** 메뉴를 사용하여 설정할 수 있습니다. 로그 레벨을 설정하는 방법은 이 설명서와 함께 제공되는 시스템 구성 설명서의 [**제8장 통합 로그**] 장을 참고합니다.

## 로그 종류

WEBFRONT-K는 이벤트의 종류에 따라 애플리케이션 로그 메시지를 다음 3가지 종류로 구분합니다.

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

### 로그 필터

로그 버퍼에 저장된 로그를 출력해보면 가장 최근에 기록된 로그부터 순차적으로 표시됩니다. 출력된 로그가 많은 경우에는 순차적으로 출력된 로그 중에서 사용자가 원하는 로그를 찾아내기가 쉽지 않습니다. WEBFRONT-K는 사용자가 보고자 하는 로그를 쉽게 찾을 수 있도록 도와주는 로그 필터를 제공합니다. 로그 필터는 다음과 같은 3가지 검색 조건으로 구성되는데, 이 조건들을 잘 설정하여 검색하면 원하는 로그만 볼 수 있습니다.

- 로그 종류
  보안 로그, 감사 로그, 접근 로그 중에서 사용자가 지정한 종류의 로그만 보여줍니다. 모든 종류의 로그가 출력되도록 설정할 수도 있습니다.
- 이벤트 레벨
  Emergency, Alert, Critical, Error, Warning, Notice, Information 레벨 중에서 사용자가 지정한 레벨 이상의 이벤트에 대한 로그만 보여줍니다.
- 이벤트의 발생 시간
  어제, 오늘, 혹은 지난 몇 시간 동안 발생한 로그만 볼 수 있습니다. 이 기간 외에 사용자가 직접 원하는 날짜를 지정할 수도 있습니다.

WEBFRONT-K에는 최대 256개의 로그 필터를 추가하고 저장할 수 있습니다. 로그 필터를 저장해두면 필요할 때마다 로그 필터를 다시 설정할 필요 없이 원하는 로그를 편리하게 검색할 수 있습니다. 잠시 로그를 검색하려는 경우에는 굳이 로그 필터를 저장하지 않아도 됩니다.

# 로그 보기

이 절에서는 각 종류의 로그를 출력하는 방법과 로그 필터를 사용하여 필터링된 로그를 출력하는 방법에 대해 살펴봅니다.

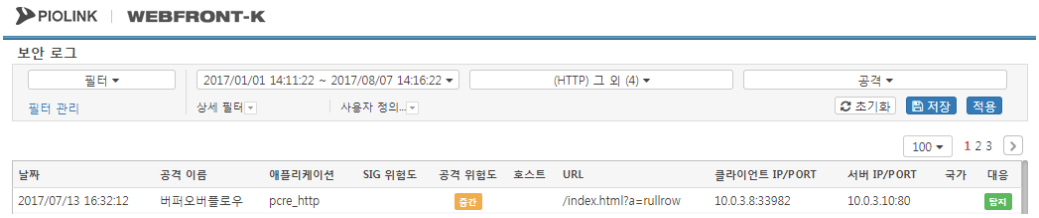
## 보안/감사/접근 로그 보기

**Application** 메뉴 중에서 **로그 – 보안로그 / 감사로그 / 접근로그** 메뉴를 클릭하면 다음과 같은 메시지가 출력되고, 웹 브라우저에 로그 뷰어 창이 열립니다.

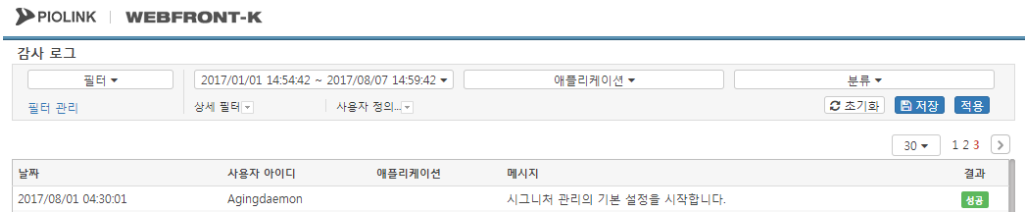

### 로그 메시지의 내용

다음은 WEBFRONT-K에 저장된 각 로그 메시지의 예입니다.

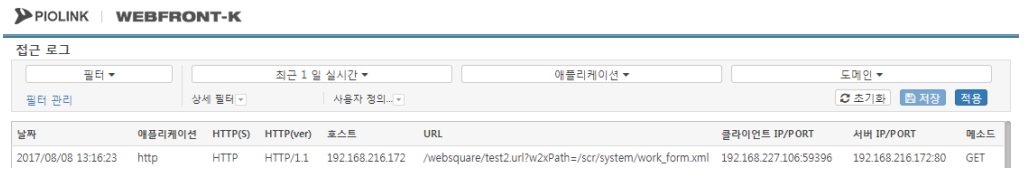
#### 보안 로그




#### 감사 로그

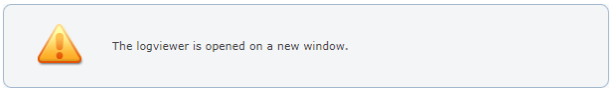
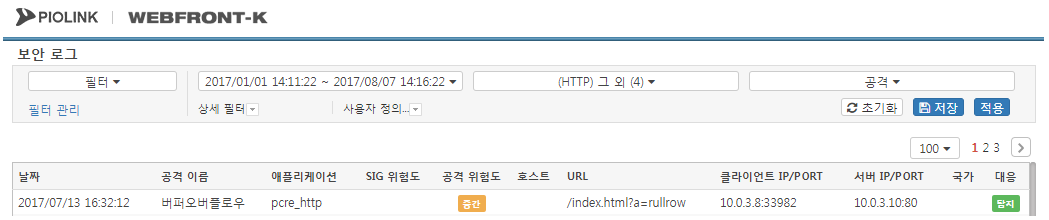
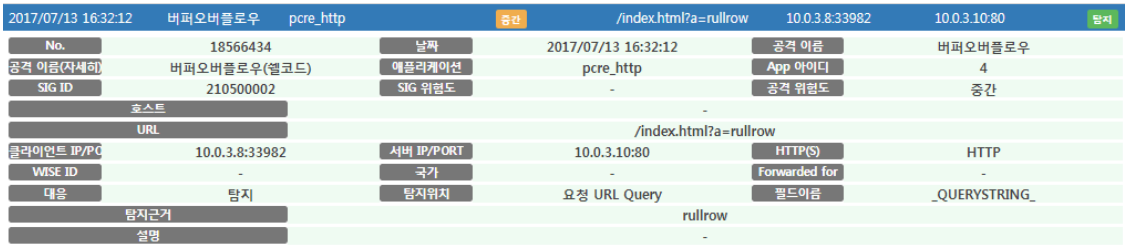



#### 접근 로그



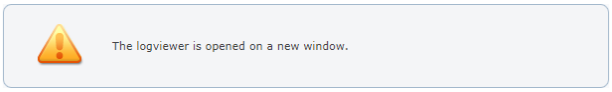
# 보안 로그

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

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **로그** – **보안 로그** 메뉴를 클릭합니다. |
| 2 | Web Manager에 "The logviewer is opened on a new window." 메시지가 출력되고, 웹 브라우저에 로그 뷰어창이 열립니다.<br>  |
| 3 | 보안 로그 화면에서 필터, 기간, 애플리케이션, 공격 종류를 선택한 후, **[적용]** 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.<br>  <br>• **날짜** 로그가 발생한 날짜<br>• **공격 이름** 클라이언트의 공격 이름 또는 공격 종류<br>• **애플리케이션** 대상 애플리케이션의 이름<br>• **SIG 위험도** 시그니처 위험도<br>• **공격 위험도** 공격 위험도<br>• **호스트** HTTP 요청 헤더의 호스트 헤더 정보<br>• **URL** 클라이언트가 접근을 시도한 URL<br>• **클라이언트 IP/PORT** 클라이언트의 IP 주소와 포트 번호<br>• **서버 IP/PORT** 서버의 IP 주소와 포트 번호<br>• **국가** 클라이언트의 IP 주소에 근거한 국가 정보<br>• **대응** 해당 로그를 처리하였을 때의 대응 방법 (탐지/차단/마스킹/통과(WISE)/검사(WISE)) |
| 4 | 특정 로그에 대한 상세 정보를 확인하려면 해당 로그를 클릭합니다.<br>  |

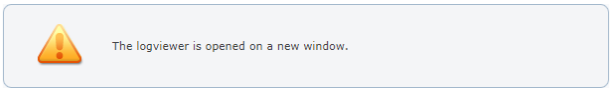
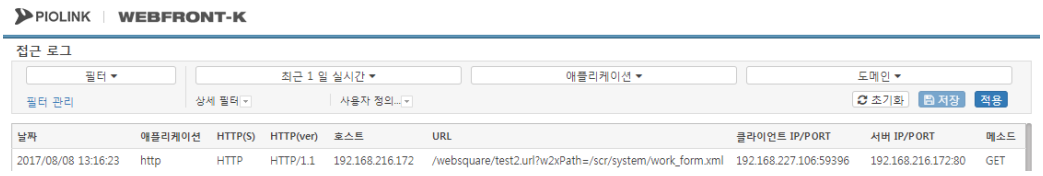
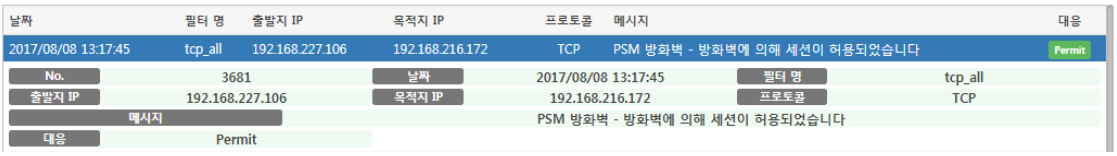
# 감사 로그

애플리케이션 감사 로그는 애플리케이션 관리자가 WEBFRONT-K에서 조회한 애플리케이션 보안 설정 정보와 변경한 애플리케이션 보안 설정 정보를 기록하는 로그입니다. WEBFRONT-K의 애플리케이션 감사 로그를 조회하는 방법은 다음과 같습니다

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **로그** – **감사 로그** 메뉴를 클릭합니다. |
| 2 | Web Manager에 “The logviewer is opened on a new window.” 메시지가 출력되고, 웹 브라우저에 로그 뷰어창이 열립니다.<br>  |
| 3 | 감사 로그 화면에서 필터, 기간, 애플리케이션, 분류를 선택한 후, **[적용]** 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.<br>  <br>• **날짜** 로그가 발생한 날짜<br>• **사용자 아이디** 클라이언트의 공격 이름 또는 공격 종류<br>• **애플리케이션** 대상 애플리케이션의 이름<br>• **메시지** 처리 결과에 대한 설명<br>• **결과** 해당 로그를 처리하였을 때의 설정 결과 |
| 4 | 특정 로그에 대한 상세 정보를 확인하려면 확인할 로그를 클릭합니다.<br>  |

# 접근 로그

애플리케이션 접근 로그는 WEBFRONT-K로 웹 요청 패킷이 수신될 때마다 발생하는 로그로, 웹 요청 패킷에 대한 정보가 기록되는 로그입니다. WEBFRONT-K의 애플리케이션 접근 로그를 조회하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **System** - **통합 로그** – **접근 로그** 메뉴를 클릭합니다. |
| 2 | Web Manager에 “The logviewer is opened on a new window.” 메시지가 출력되고, 웹 브라우저에 로그 뷰어창이 열립니다.<br>  |
| 3 | 접근 로그 화면에서 필터, 기간, 애플리케이션, 도메인을 선택한 후, **[적용]** 버튼을 클릭하면 조건에 부합하는 로그가 출력됩니다.<br>  <br>• **날짜** 로그가 발생한 날짜<br>• **애플리케이션** 대상 애플리케이션의 이름<br>• **HTTP(S)** 전송 프로토콜<br>• **HTTP(ver)** HTTP 버전<br>• **호스트** 클라이언트 헤더의 host 필드값<br>• **URL** 클라이언트가 접근을 시도한 URL<br>• **클라이언트 IP/PORT** 클라이언트의 IP 주소와 포트 번호<br>• **서버 IP/PORT** 서버의 IP 주소와 포트 번호<br>• **메소드** 클라이언트가 사용한 HTTP 메소드 |
| 4 | 특정 로그에 대한 상세 정보를 확인하려면 확인할 로그를 클릭합니다.<br>  |

# 제10장 애플리케이션 모니터링

WEBFRONT-K는 애플리케이션 보안 기능에 대한 다음과 같은 모니터링 기능을 제공합니다.

- 모니터링
  일정 기간 동안 모니터링한 WEBFRONT-K의 트래픽 양과 보안 기능에 의해 차단되거나 학습된 정보에 대한 통계 정보를 보여주는 기능

이 장에서는 이러한 WEBFRONT-K의 애플리케이션 모니터링 기능을 통해 WEBFRONT-K의 애플리케이션 보안 기능의 상태와 통계 정보 등을 파악하는 방법에 대해 설명합니다.

이 장은 다음 내용으로 구성되어 있습니다.

# 애플리케이션 모니터링

모니터링은 일정 기간 동안 모니터링한 WEBFRONT-K의 보안 기능에 의해 차단되거나 학습된 웹 공격에 대한 정보를 보여줍니다. 모니터링을 통해 볼 수 있는 정보는 다음과 같습니다.

- 요청 검사 기능을 통해 차단된 웹 공격 횟수
- 컨텐트 보호 기능을 통해 차단된 웹 공격 횟수
- 학습 기능을 통해 학습된 정보 개수
- 위장 기능을 통해 변경된 정보 개수
- 각 실제 서버가 처리한 트래픽의 양

WEBFRONT-K는 위 정보들을 한꺼번에 보여주는 애플리케이션 통합 모니터링 기능과 각 보안 기능별로 모니터링 정보를 보다 상세하게 조회할 수 있는 상세 모니터링 기능을 제공합니다. 애플리케이션 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.

다음 절에서는 먼저 애플리케이션 통합 모니터링 화면에 출력되는 정보들을 살펴본 후, 각 보안 기능의 상세 모니터링 기능을 사용하여 사용자가 원하는 정보만을 검색하는 방법을 살펴보도록 합니다.

## 애플리케이션 통합 모니터링

최근 25분 동안 WEBFRONT-K를 통해 송수신된 트래픽의 양과 각 웹 보안 기능에 의해 차단된 웹 공격에 대한 정보, 그리고 요청 검사 기능에 설정된 학습 기능을 통해 학습된 정보를 출력하려면 **Application** 메뉴에서 **모니터링** – **애플리케이션통합** 메뉴를 클릭합니다.

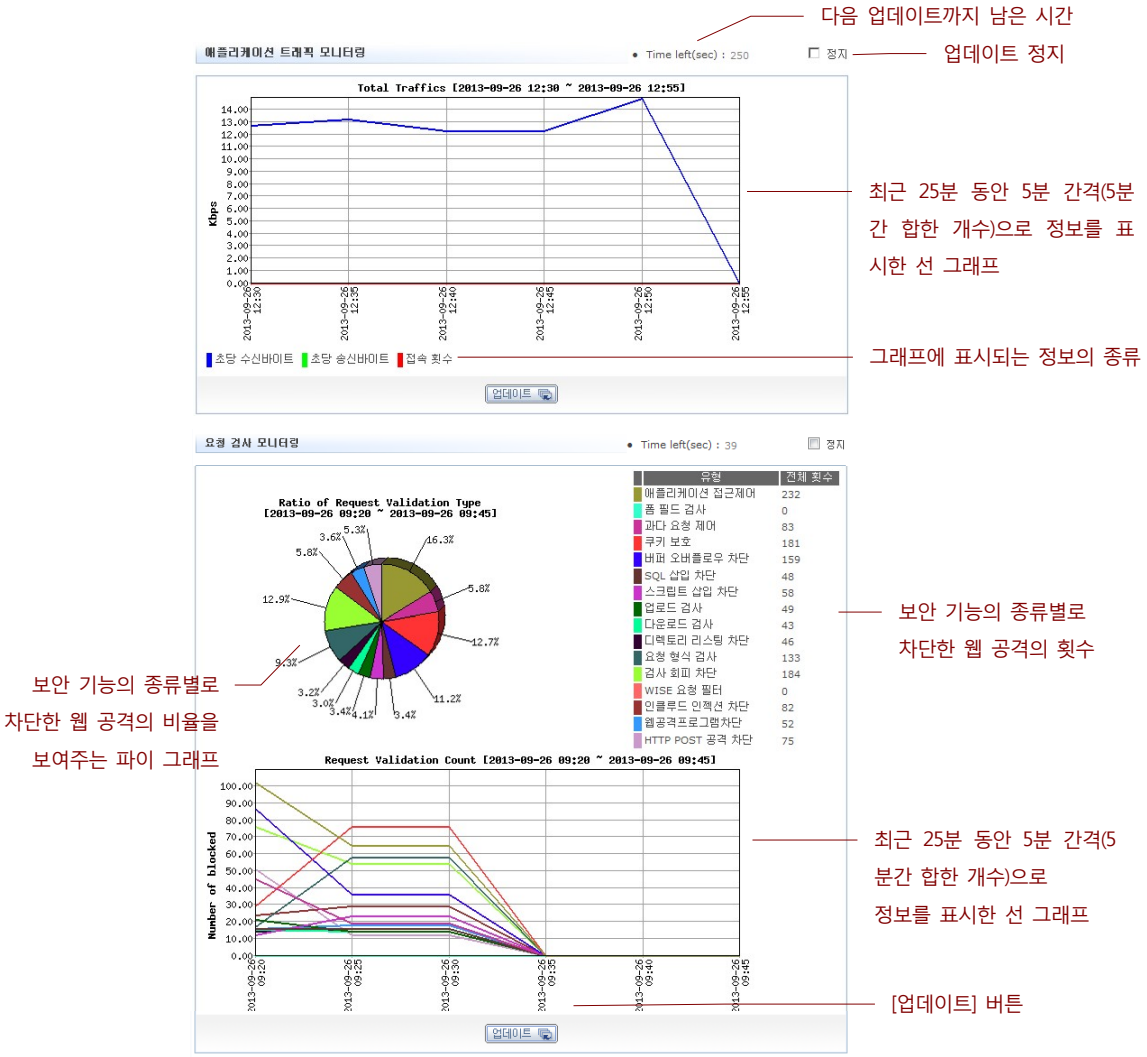
애플리케이션 트래픽 정보와 웹 공격에 대한 정보(일부)를 보여주는 화면이 나타납니다.


스크롤 바를 사용하여 화면을 아래쪽으로 내리면 웹 공격(나머지)과 요청 검사, 컨텐트 보호, 서버 트래픽에 대한 모니터링 결과를 볼 수 있습니다.

## 모니터링 화면 구조

애플리케이션 통합 모니터링에서는 6종류의 모니터링 화면을 볼 수 있습니다. 가장 위에 트래픽 양에 대한 정보를 보여주는 모니터링 화면이 있고, 아래 쪽에 차례로 웹 공격과 요청 검사, 컨텐트 보호에 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 <**애플리케이션 트래픽 모니터링**> 화면과 <**요청 검사 모니터링**> 화면입니다.




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 24시간이 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 24시간 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

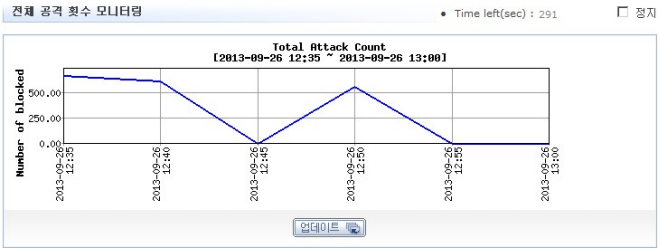
<**애플리케이션 트래픽 모니터링**> 부분에는 WEBFRONT-K의 인터페이스를 통해 송수신된 트래픽 양에 대한 정보가 출력됩니다.


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

- 초당 수신 패킷 양(Rx bytes per second, 파란색)
  1초 동안 WEBFRONT-K의 모든 인터페이스로 수신된 패킷의 총 byte 수
- 초당 송신 패킷 양(Tx bytes per second, 초록색)
  1초 동안 WEBFRONT-K의 모든 인터페이스를 통해 전송된 패킷의 총 byte 수
- 초당 수신 패킷 수(Rx packets per second, 빨간색)
  1초 동안 WEBFRONT-K의 모든 인터페이스로 수신된 패킷의 총 개수

## 웹 공격 횟수에 대한 모니터링 정보

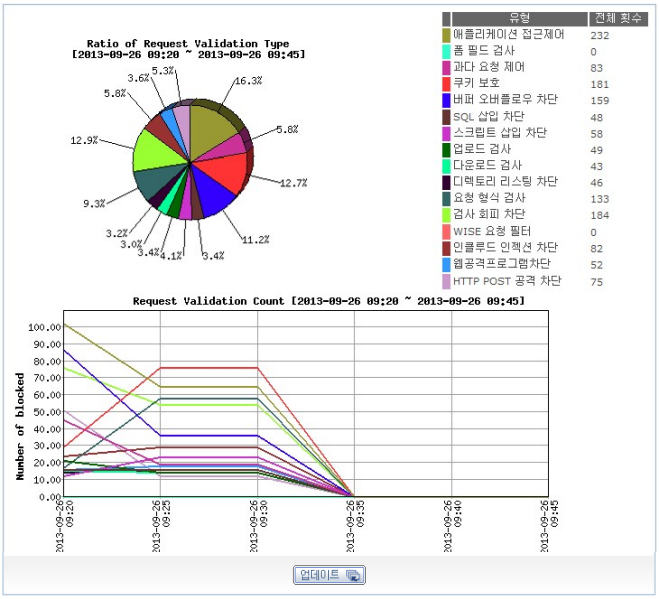
<**전체 공격 횟수 모니터링**> 부분에서는 WEBFRONT-K에 등록된 애플리케이션으로 행해진 웹 공격의 횟수에 대한 정보를 볼 수 있습니다. 애플리케이션에 설정된 모든 웹 보안 기능에 의해 최근 25분 동안 차단된 웹 공격의 횟수가 이 화면에 출력됩니다.




화면의 꺾은 선 그래프는 WEBFRONT-K의 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

<**요청 검사 모니터링**> 부분에는 WEBFRONT-K에 설정된 요청 검사 기능을 통해 최근 25분 동안 차단된 웹 공격에 대한 정보가 출력됩니다.

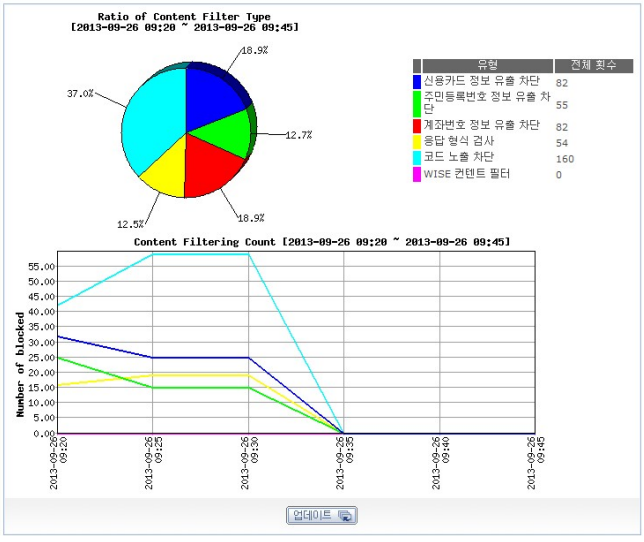



화면의 오른쪽에 있는 표는 요청 검사 기능의 종류와 각 종류의 요청 검사 기능이 차단한 웹 공격의 횟수입니다.

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.

## 컨텐트 보호에 대한 모니터링 정보

<**컨텐트 보호 모니터링**> 부분에는 WEBFRONT-K에 설정된 컨텐트 보호 기능을 통해 최근 25분동안 차단된 웹 공격에 대한 정보가 출력됩니다.

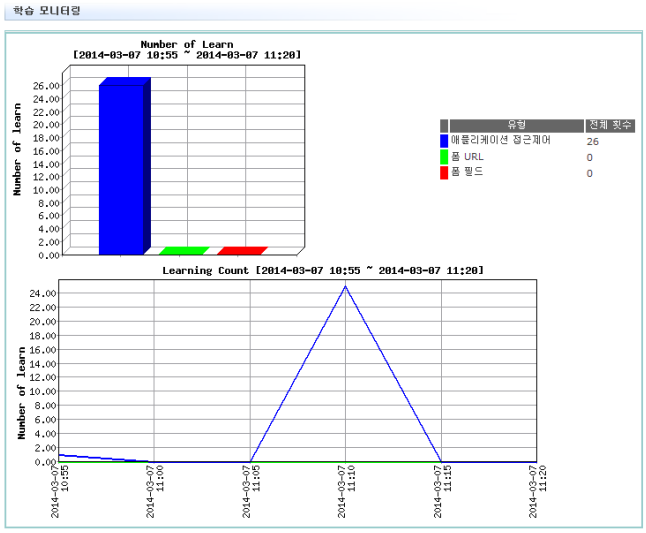



화면의 오른쪽에 있는 표는 컨텐트 보호 기능의 종류와 각 종류의 컨텐트 보호 기능이 차단한 웹 공격의 횟수입니다.

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

## 학습 기능에 대한 모니터링 정보

<**학습 모니터링**> 부분에는 WEBFRONT-K에 설정된 학습 기능에 의해 최근 25분 동안 학습한 정보의 개수가 출력됩니다.

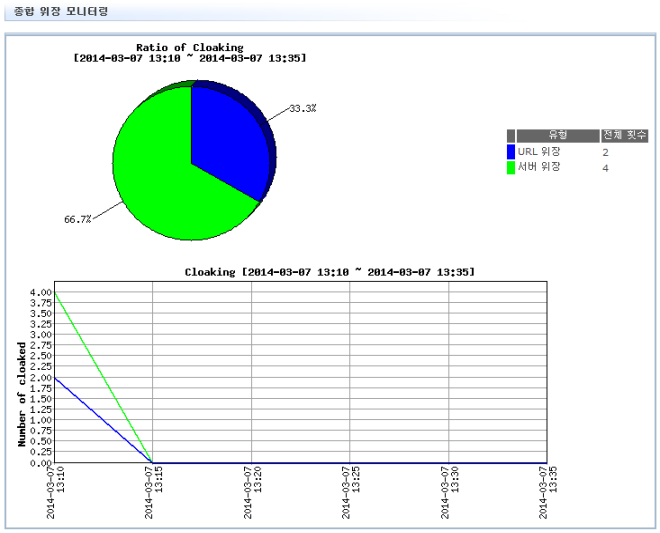



화면의 오른쪽에 있는 표는 요청 검사 기능의 종류와 각 요청 검사 기능에 설정된 학습 기능에 의해 학습된 정보의 개수입니다.

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.

## 위장 기능에 대한 모니터링 정보

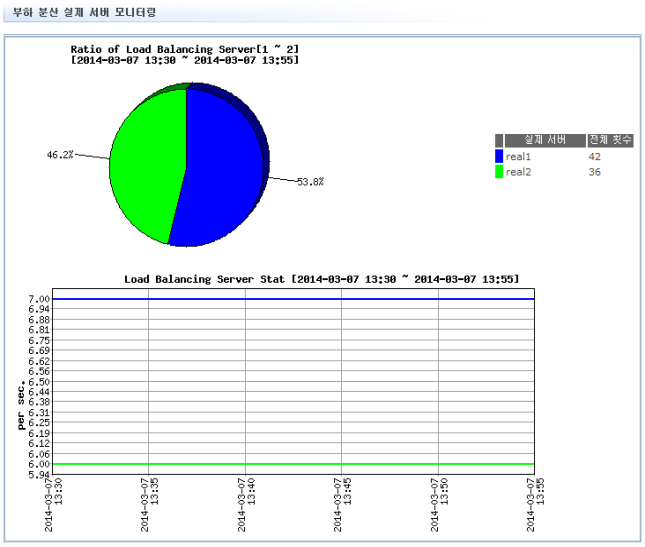
<**종합 위장 모니터링**> 부분에는 WEBFRONT-K에 설정된 위장 기능에 의해 최근 25분 동안 변경된 정보의 개수가 출력됩니다.




화면의 오른쪽에 있는 표는 위장 기능의 종류와 각 종류의 위장 기능이 동작한 횟수입니다. 아래에 있는 꺾은 선 그래프는 모든 위장 기능이 동작한 횟수를 5분 간격으로 보여줍니다.

## 부하 분산 실제 서버 모니터링 정보

<**부하 분산 실제 서버 모니터링**> 부분에는 최근 25분 동안 WEBFRONT-K와 연결된 각 실제 서버가 처리한 트래픽의 정보가 출력됩니다.




화면의 오른쪽에 있는 표는 실제 서버의 이름과 각 서버가 처리한 트래픽의 횟수입니다. 왼쪽의 파이 그래프는 실제 서버별로 처리한 트래픽의 상대적인 비율을 보여줍니다. 아래에 있는 꺾은 선 그래프는 각 서버가 처리한 트래픽의 횟수를 5분 간격으로 보여줍니다.

# 애플리케이션 상세 모니터링

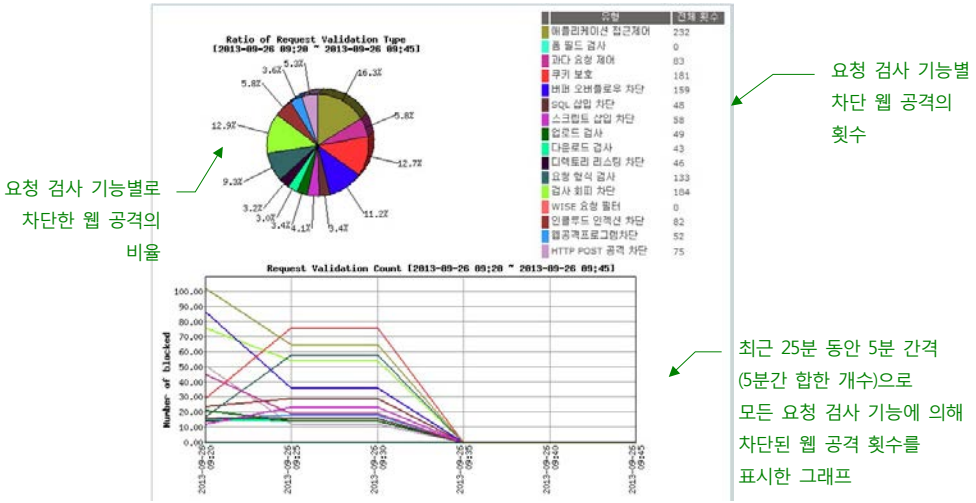
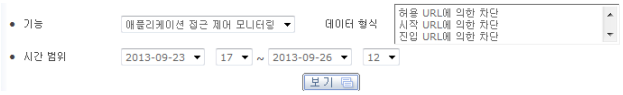
## 요청 검사 상세 모니터링 정보 보기

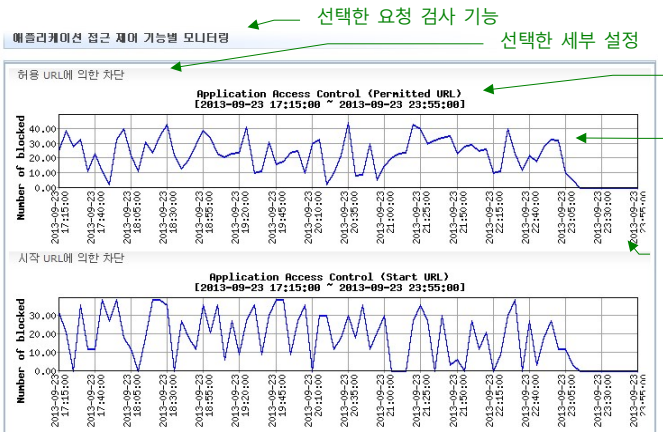
애플리케이션 모니터링 화면에서는 요청 검사 기능별 차단 웹 공격 횟수나 애플리케이션의 요청 검사 기능에 의해 차단된 총 웹 공격 횟수를 볼 수 있습니다. 볼 수 있는 정보는 최근 25분 동안 수집된 정보로 한정됩니다.

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

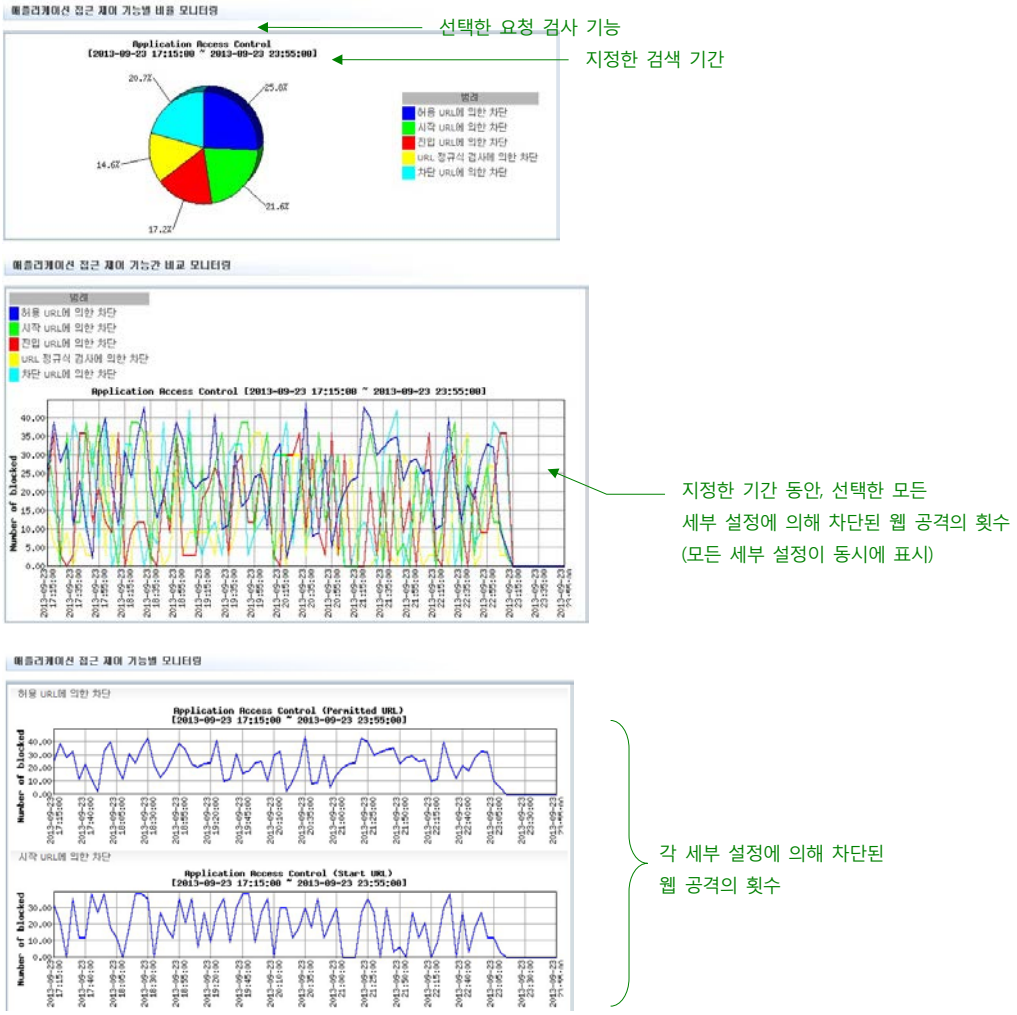
- 특정 요청 검사 기능에 대한 정보만 조회(예: 접근 제어 기능에 대한 정보만 출력)
- 요청 검사의 종류에 따라 원하는 정보만 조회(예: 접근 제어 기능의 시작 URL에 의해 차단된 웹 공격에 대한 정보만 출력)
- 특정 시간 동안 모니터링한 정보만 출력

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

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **모니터링** – **요청검사 모니터링** 메뉴를 클릭합니다. |
| 2 | 요청 검사 상세 모니터링 화면이 나타납니다. 화면의 윗 부분에는 애플리케이션에 설정된 요청 검사 기능에 의해 최근 24 시간 동안 차단된 웹 공격에 대한 정보가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 정보를 검색할 때 지정하는 조건들입니다.<br>  <br> |
| 3 | 다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 [**보기**] 버튼을 클릭합니다.<br>  <br><br>• **기능** 특정 요청 검사 기능에 대한 정보만 출력하려면 이 항목에서 드롭다운 목록을 클릭한 후 원하는 요청 검사 기능을 선택합니다.<br>• **데이터 형식** 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. [**Shift**] 키나 [**Ctrl**] 키를 사용하여 여러 개의 항목을 지정할 수도 있습니다.<br>• **시간 범위** 특정 기간에 수집된 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다. |
| 4 | 지정한 검색 조건에 따라 다음 두가지 형태 중 하나의 그래프가 나타납니다.<br>• 검색 조건으로 하나의 데이터 형식을 선택하면 다음과 같이 하나의 그래프만 출력됩니다. |




• 검색 조건으로 여러 개의 데이터 형식을 선택한 경우에는 다음과 같이 맨 위에 파이 그래프가 출력되고 아래에는 선택한 세부 설정의 개수만큼 꺾은 선 그래프가 출력됩니다.



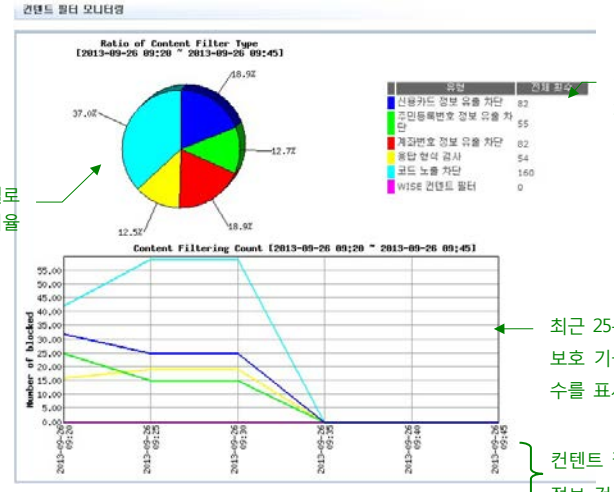
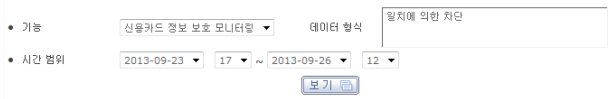
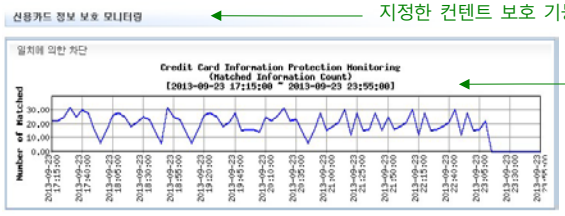
## 컨텐트 보호 상세 모니터링 정보 보기

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

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

- 특정 컨텐트 보호 기능에 대한 정보만 조회(예: 신용 카드 정보 차단 기능에 대한 정보만 출력)
- 컨텐트 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

컨텐트 보호 상세 모니터링 화면에서 컨텐트 보호 정보를 조회하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **모니터링** – **컨텐트 필터 모니터링** 메뉴를 클릭합니다. |
| 2 | 컨텐트 필터 상세 모니터링 화면이 나타납니다.<br>  <br><br>컨텐트 보호 기능별 차단한 웹 공격의 비율<br>컨텐트 보호 기능별 차단 웹 공격의 횟수<br>최근 25분 동안 모든 컨텐트 보호 기능에 의해 차단된 웹 공격 횟수를 표시한 그래프<br>컨텐트 필터 기능의 정보 검색 조건<br>화면의 윗 부분에는 애플리케이션에 설정된 컨텐트 보호 기능에 의해 최근 25분 동안 차단된 웹 공격에 대한 정보가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 정보를 검색할 때 지정하는 조건들입니다. |
| 3 | 다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 [**보기**] 버튼을 클릭 합니다.<br>  <br><br>• **기능** 특정 컨텐트 보호 기능에 대한 정보만 출력하려면 이 항목에서 드롭다운 목록을 클릭한 후 원하는 컨텐트 보호 기능을 선택합니다.<br>• **데이터 형식** 기능 항목에서 컨텐트 보호 기능의 종류를 선택하면 이 항목에는 선택한 컨텐트 보호 기능의 세부 설정이 표시됩니다. 응답 형식 검사를 제외하고는 모두 '일치에 의한 차단' 만 출력되므로 이 항목을 선택하면 됩니다. 기능 항목을 응답 형식 검사로 지정한 경우에는 세부 설정을 선택합니다. [**Shift**] 키나 [**Ctrl**] 키를 사용하여 두 항목을 동시에 선택할 수도 있습니다.<br>• **시간 범위** 특정 기간에 수집된 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다. |
| 4 | 지정한 검색 조건에 따라 다음 형태 중 하나의 그래프가 나타납니다.<br>• 검색 조건으로 하나의 데이터 형식을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.<br>  <br><br>지정한 컨텐트 보호 기능(데이터 형식)<br>사용자가 지정한 검색 기간<br>지정한 기간 동안 선택한 컨텐트 보호 기능에 의해 차단된 웹 공격의 횟수를 보여주는 그래프<br>• 검색 조건으로 여러 개의 데이터 형식을 선택한 경우에는 맨 위에 파이 그래프가 출력되고 아래에는 선택한 세부 종류 개수만큼 꺾은 선 그래프가 출력됩니다. |

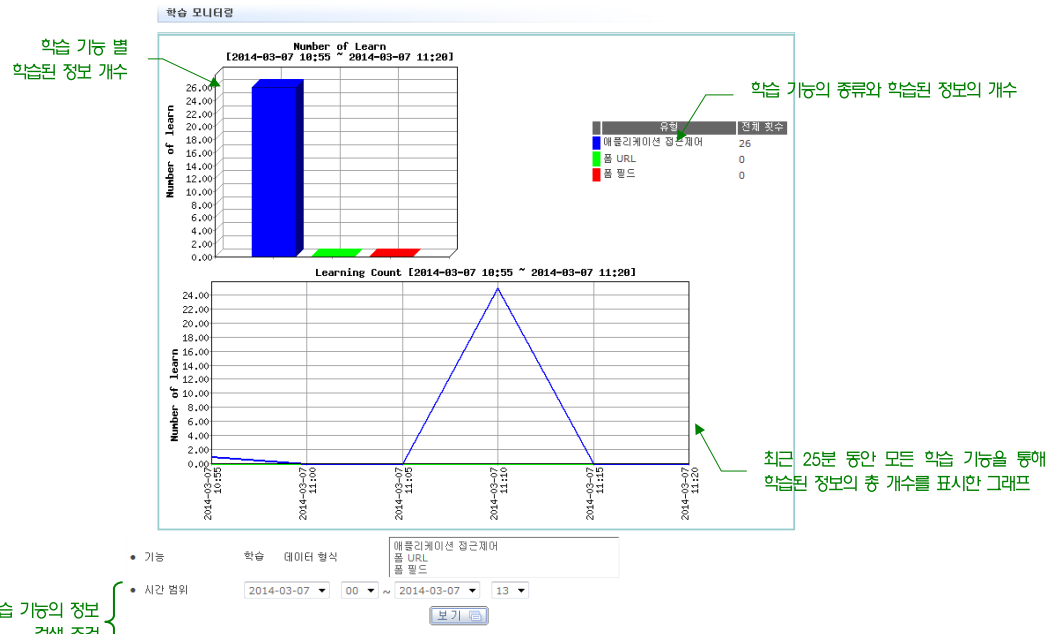
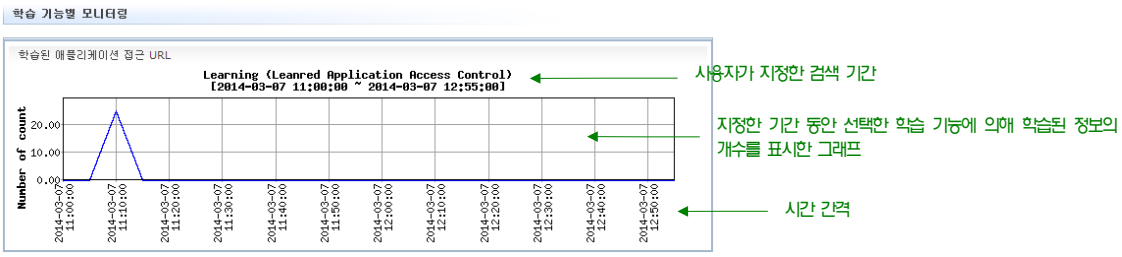
## 학습 모니터링 상세 정보 보기

애플리케이션 모니터링 화면에서는 각 요청 검사 기능별로 학습된 정보의 개수나 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 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 | **Application** - **모니터링** – **학습 모니터링** 메뉴를 클릭합니다. |
| 2 | 학습 기능 상세 모니터링 화면이 나타납니다.<br>  <br><br>화면의 윗 부분에는 애플리케이션의 요청 검사 기능에 설정된 학습 기능에 의해 최근 24 시간 동안 학습한 정보의 개수가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 학습에 관한 정보를 검색할 때 지정하는 조건들입니다. |
| 3 | 다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 [**보기**] 버튼을 클릭합니다.<br>  <br><br>• **데이터 형식** 특정한 학습 기능에 대한 정보만 출력하려는 경우에는 여기에서 원하는 요청 기능을 선택합니다. [**Shift**] 키나 [**Ctrl**] 키를 사용하여 여러 개의 항목을 지정할 수도 있습니다.<br>• **시간 범위** 특정 기간에 수집된 학습 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다. |
| 4 | 지정한 검색 조건에 따라 다음 형태 중 하나의 그래프가 나타납니다.<br>• 검색 조건으로 하나의 데이터 형식을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.<br>  <br><br>• 검색 조건으로 여러 개의 데이터 형식을 선택한 경우에는 다음과 같이 맨 위에 파이 그래프가 출력되고 아래에는 선택한 요청 검사 기능의 개수만큼 꺾은 선 그래프가 출력됩니다. |


학습 기능별 비율 모니터링
선택한 학습 기능별로 학습된 정보의 개수를 보여주는 막대 그래프
Learning
Number of count
범례
학습된 애플리케이션 접근 URL
학습된 폼 URL
막대 그래프에 정보가 표시되는 학습 기능들
학습 기능간 비교 모니터링
지정한 기간 동안 선택한 모든 학습 기능에 의해 학습된 정보의 개수
Learning [2014-03-07 11:00:00 ~ 2014-03-07 12:55:00]
Number of blocked
학습 기능별 모니터링
학습된 애플리케이션 접근 URL
Learning (Leanred Application Access Control)
[2014-03-07 11:00:00 ~ 2014-03-07 12:55:00]
학습된 폼 URL
Learning (Learned Form URL)
[2014-03-07 11:00:00 ~ 2014-03-07 12:55:00]
각 학습 기능에 의해 학습된 정보의 개수

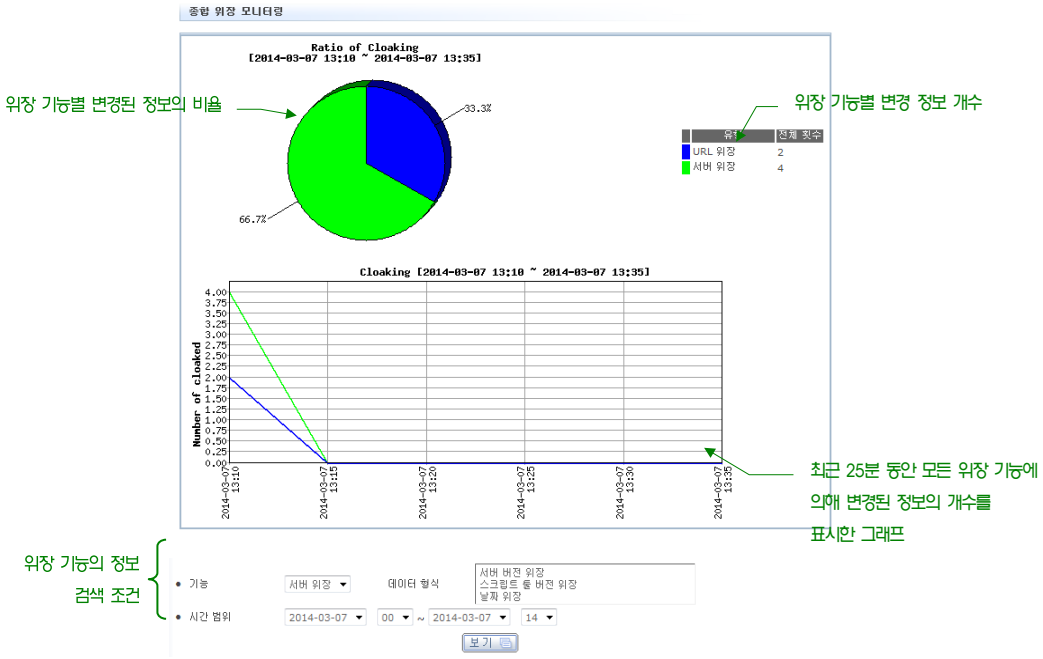
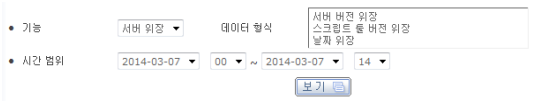
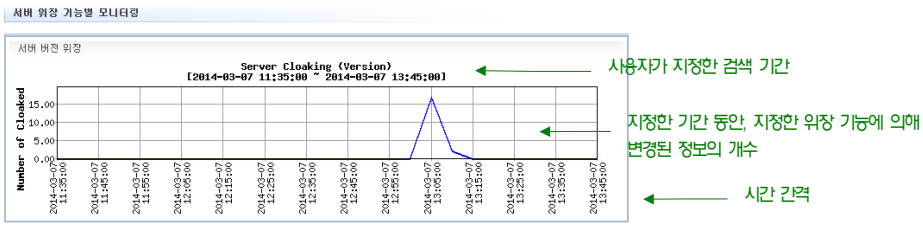
## 위장 모니터링 상세 정보 보기

애플리케이션 모니터링 화면에서는 위장 기능별 변경된 정보 개수나 애플리케이션의 위장 기능에 의해 변경된 총 정보 개수를 볼 수 있습니다. 볼 수 있는 정보는 최근 25분 동안 수집된 정보로 한정됩니다.

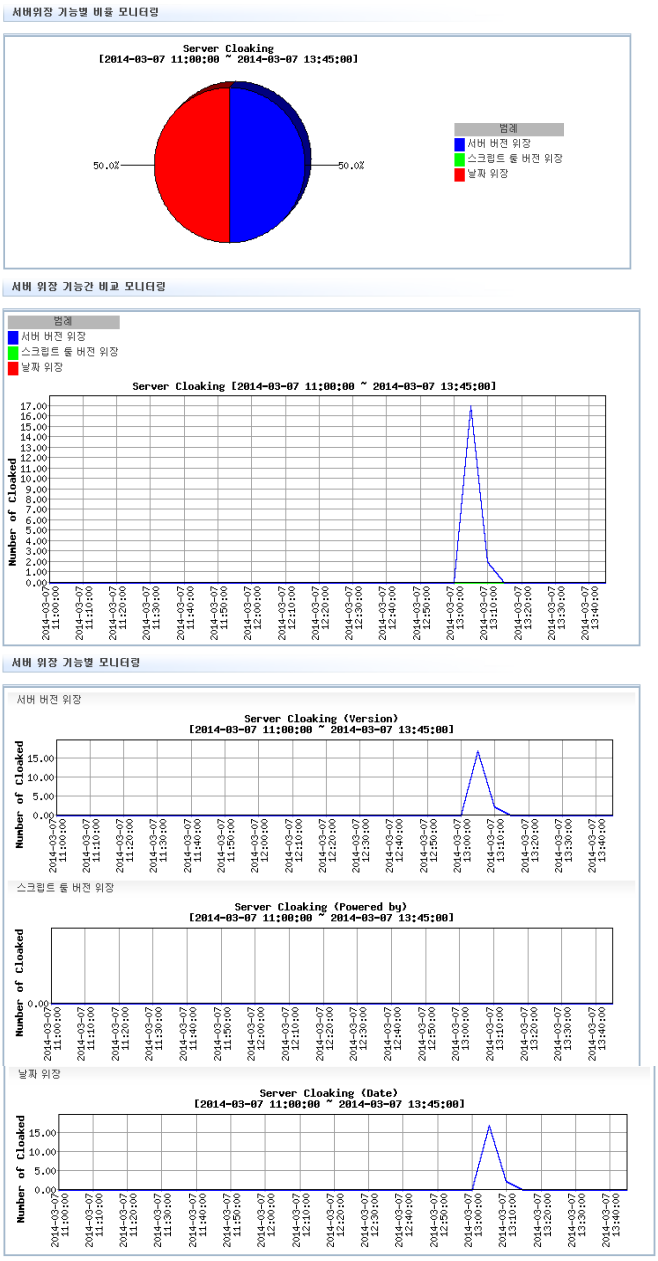
이와 달리 위장 상세 모니터링 화면에서는 일주일간 수집된 정보를 볼 수 있고, 다음과 같이 사용자가 여러 옵션을 선택하여 원하는 정보만 조회할 수 있습니다.

- 특정 위장 기능에 대한 정보만 조회(예: 서버 위장 기능이나 URL 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 | **Application** - **모니터링** – **위장 모니터링** 메뉴를 클릭합니다. |
| 2 | 위장 상세 모니터링 화면이 나타납니다. 화면의 윗 부분에는 최근 24 시간 동안 애플리케이션에 설정된 위장 기능에 의해 차단된 웹 공격에 대한 정보가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 정보를 검색할 때 지정하는 조건들입니다.<br>  <br> |
| 3 | 다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 [**보기**] 버튼을 클릭합니다.<br>  <br>• **기능** 특정 위장 기능에 대한 정보만 출력하려면 이 항목에서 드롭다운 목록을 클릭한 후 원하는 위장 기능을 선택합니다.<br>• **데이터 형식** 기능 항목에서 위장 기능의 종류를 선택하면 이 항목에는 선택한 위장 기능의 세부 설정이 표시됩니다. 특정 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.<br>• **시간 범위** 특정 기간에 수집된 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다. |
| 4 | 지정한 검색 조건에 따라 다음 두가지 형태 중 하나의 그래프가 나타납니다.<br>• 검색 조건으로 하나의 데이터 형식을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.<br>  <br> |

• 검색 조건으로 여러 개의 데이터 형식을 선택한 경우에는 다음과 같이 맨 위에 파이 그래프가 출력되고 아래에는 선택한 세부 종류 개수만큼 꺾은 선 그래프가 출력됩니다.

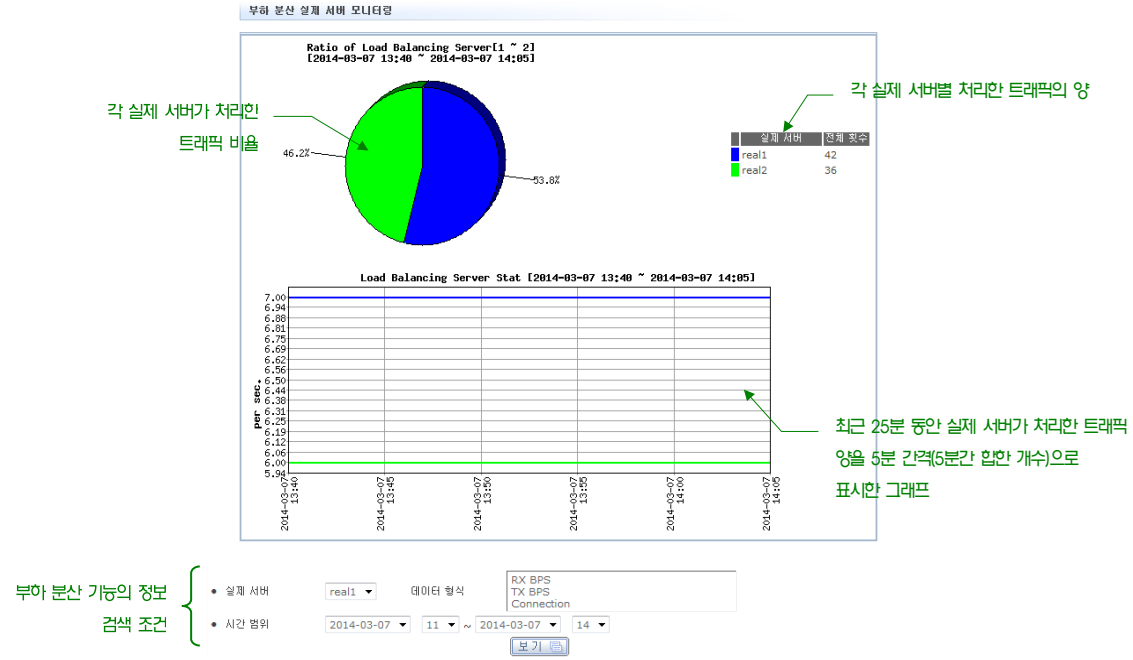
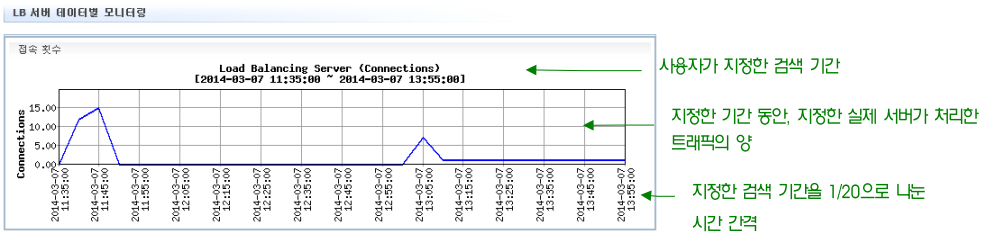


## 부하 분산 실제 서버 모니터링 상세 정보 보기

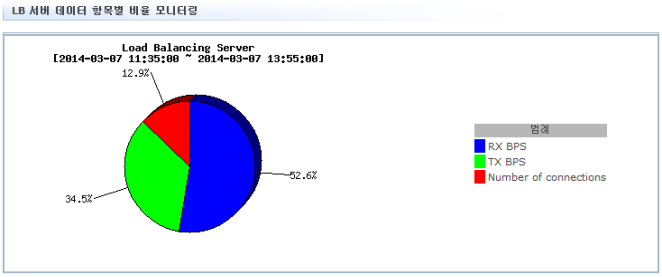
애플리케이션 모니터링 화면에서는 부하 분산을 수행하는 각 실제 서버가 처리한 트래픽의 횟수를 볼 수 있습니다. 볼 수 있는 정보는 최근 24 시간 동안 수집된 정보로 한정됩니다. 이와 달리 부하 분산 실제 서버 상세 모니터링 화면에서는 일주일간 수집된 정보를 볼 수 있고, 다음과 같이 사용자가 여러 옵션을 선택하여 원하는 정보만 조회할 수 있습니다.

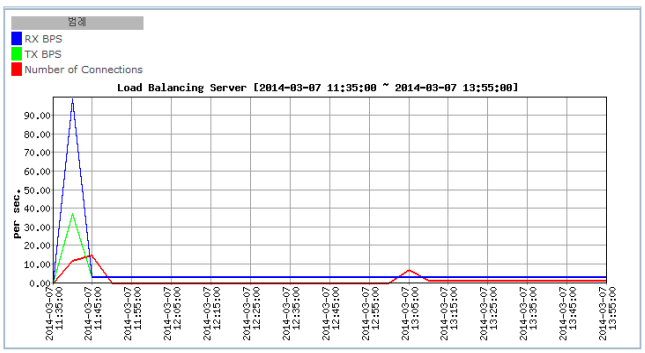
- 특정 실제 서버에 대한 정보만 조회
- 특정 실제 서버의 특정 트래픽 종류에 대한 정보만 조회(예: 수신 트래픽 정보만 출력)
- 특정 시간 동안 모니터링한 정보만 출력

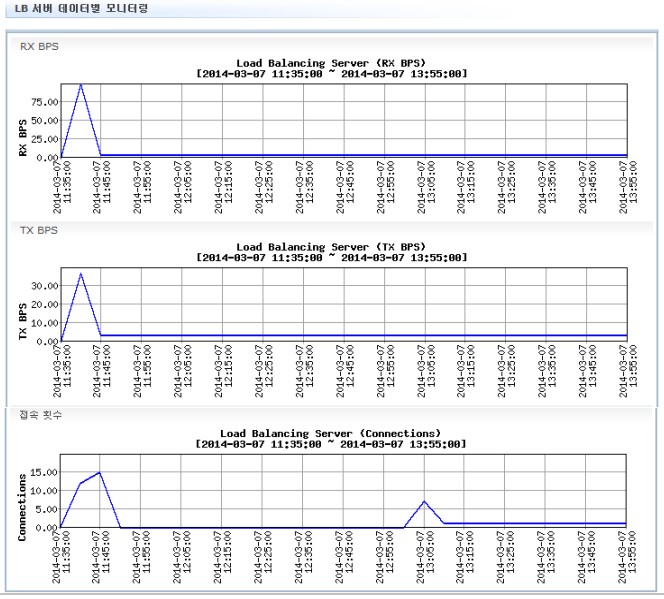
부하 분산 상세 모니터링 화면에서 정보를 조회하는 방법은 다음과 같습니다.

| 순서 | 설정 과정 |
|---|---|
| 1 | **Application** - **모니터링** – **부하분산 모니터링** 메뉴를 클릭합니다. |
| 2 | 부하 분산 실제 서버 상세 모니터링 화면이 나타납니다. 화면의 윗 부분에는 최근 24 시간 동안 애플리케이션에 설정된 실제 서버의 트래픽에 대한 정보가 표시됩니다. 화면의 아래쪽에 있는 항목들은 사용자가 정보를 검색할 때 지정하는 조건들입니다.<br>  |
| 3 | 다음 설명을 참고하여 사용자가 출력하고자 하는 정보에 대한 검색 조건을 지정하고 [**보기**] 버튼을 클릭합니다.<br>  <br>• **기능** 특정 실제 서버에 대한 정보만 출력하려면 이 항목에서 드롭다운 목록을 클릭한 후 원하는 실제 서버를 선택합니다.<br>• **데이터 형식** 기능 항목에서 선택한 실제 서버의 세부 모니터링 항목이 표시됩니다. 수신한 트래픽 정보, 송신한 트래픽 정보, 연결 횟수 정보 중에서 원하는 항목을 선택합니다. [**Shift**] 키나 [**Ctrl**] 키를 사용하여 여러 개의 항목을 지정할 수도 있습니다.<br>• **시간 범위** 특정 기간에 수집된 정보만을 출력하려면 이 항목에서 각각 모니터링 시작 시간과 끝 시간을 지정합니다. |
| 4 | 지정한 검색 조건에 따라 다음 두 가지 형태 중 하나의 그래프가 나타납니다.<br>• 검색 조건으로 하나의 데이터 형식을 선택하면 다음과 같이 하나의 그래프만 출력됩니다.<br>  |

• 검색 조건으로 여러 개의 데이터 형식을 선택한 경우에는 다음과 같이 맨 위에 파이 그래프가 출력되고 아래에는 선택한 세부 종류 개수만큼 꺾은 선 그래프가 출력됩니다.




PIOLINK