AhnLab

V3 Net for Linux Server

관리자 설명서

AhnLab

목차

V3 Net for Linux Server

표기 규칙

본 문서에서 사용 중인 표기 규칙은 다음과 같습니다.

표기 규칙	표기 규칙 내용
<설치 확인>	창의 이름입니다.
굵은 글꼴	버튼 이름, 창에 나오는 메시지입니다.
참고	프로그램을 사용할 때 참고할 사항입니다.
주의	프로그램을 사용할 때 주의해야 할 사항입니다.
V3 Net for Linux Server	AhnLab V3 Net for Linux Server 의 줄임말로 도움말에서는 제품 명칭을 **V3 Net for Linux Server** 로 표기합니다.

오픈소스

본 제품에서 사용된 오픈소스 관련 정보는 https://opensource.ahnlab.com 에서 확인할 수 있습니다.

제품 등록

V3 Net for Linux Server 를 설치한 사용자는 반드시 제품 등록을 해야 합니다. 제품 등록을 하지 않으면 최신 엔진을 업데이트할 수 없으며 이외에도 다양한 고객지원 서비스를 이용할 수 없습니다. 제품 등록은 (주)안랩 홈페이지(https://www.ahnlab.com)의 **[고객지원 > 온라인 제품등록]**에서 할 수 있습니다.

재계약

- 고객지원 기간(1 년)이 만료되면 최신 엔진 업데이트 서비스 등의 고객지원 서비스를 받을 수 없으며 설치된 제품도 사용할 수 없습니다.
- 고객지원 기간(1 년)이 만료되어 고객지원 서비스를 계속 이용하려면 재계약을 해야 합니다. (주)안랩 온라인 쇼핑몰(https://shop.ahnlab.com)에서 재계약 제품을 구입할 수 있습니다.
- (주)안랩 홈페이지(https://www.ahnlab.com)의 **[고객지원 > 나의 등록제품]**에서 제품의 고객지원 서비스 만료일을 확인할 수 있습니다.
- 고객지원 서비스 및 재계약에 대한 궁금한 점은 고객만족센터로 연락하십시오.

고객지원

V3 Net for Linux Server 를 사용하는 도중 문제가 발생하였을 경우 (주)안랩으로 문의하십시오.

- 안랩 홈페이지: https://www.ahnlab.com
- 온라인 고객지원: 홈페이지 > 고객지원 > 온라인 고객지원 > 1:1 상담
- 구매문의: 1588-3096 (평일 오전 9 시~오후 6 시, 토/공휴일 제외)
- 기업고객 기술지원: 1577-9431 (평일 오전 9 시~오후 8 시, 토/공휴일 제외)
- 주소: 경기도 성남시 분당구 판교역로 220 (우)13493
- 팩스: 031-722-8901

제품 특징

V3 Net for Linux Server 는 악성코드의 위협으로부터 서버를 안전하게 보호하는 Linux 서버 전용 백신입니다. V3 Net for Linux Server 의 검사 기능을 이용하여 서버에 저장된 파일들을 빠르게 검사하고 치료하여 악성코드로부터 안전하게 서버를 보호할 수 있습니다.

악성코드 대응

- 20 년 동안 누적된 안랩의 자체 엔진으로 신속하고 정확한 진단 및 치료 기능을 제공합니다.
- 다양한 압축 파일에 대하여 검사가 가능하고 다중 압축 파일도 지원합니다.
- 자주 검사하는 디렉터리를 사용자 정의 검사 목록에 추가하여 언제든지 간편하게 검사할 수 있습니다.
- 예약 검사를 이용하여 원하는 시간에 주기적으로 검사할 수 있습니다.
- 자동 업데이트를 이용하여 항상 최신 버전으로 엔진을 유지할 수 있습니다.
- 예약 업데이트를 이용하여 원하는 시간에 주기적으로 엔진을 업데이트할 수 있습니다.

관리자 편의 기능

- 검사 예외 설정을 이용하여 검사하지 않을 확장자를 등록할 수 있습니다.
- 검사 예외 설정을 이용하여 검사하지 않을 디렉터리를 등록할 수 있습니다.
- 웹 기반의 편리한 관리 툴을 제공합니다.
- 바이러스 로그 및 이벤트 로그를 제공합니다.
- 기간 설정에 따른 바이러스 통계를 제공합니다.

시스템 사양

V3 Net for Linux Server 를 사용하기 위한 시스템 사양은 다음과 같습니다.

하드웨어 사양

구분	최소 사양	권장 사양
CPU	Intel Pentium 1.5GHz	Intel Pentium 3.0GHz
메모리	512MB	1GB
하드 디스크 드라이브	500MB	5GB
네트워크	10/100/1000 Ethernet Card	10/100/1000 Ethernet Card

운영체제

운영체제 이름	지원 버전
Red Hat	9
Red Hat Enterprise Linux	3.1~7.4
Fedora(Core)	1~29
CentOS	2.1~7.6
Ubuntu	8.1~18.04
Oracle Linux	5.0~7.6
Debian	9.5
SUSE Linux Enterprise Server	10~11
OpenSUSE	12.1~13.2 Leap-15.0

V3 Net for Linux Server 관리

V3 Net for Linux Server 는 웹 UI 를 통해 정책과 시스템 설정 사항을 관리합니다. 웹 UI 를 사용하기 위한 시스템 사양은 다음과 같습니다.

- 웹 브라우저: Microsoft Internet Explorer 10 이상
- 화면 해상도
  - 최소: 1024 x 768 픽셀
  - 권장: 1280 x 1024 픽셀

참고

웹 브라우저의 보안 설정에 따라 일부 팝업 창이 차단될 수 있습니다. V3 Net for Linux Server 웹 UI 에서는 항상 팝업 창을 허용하도록 설정하십시오.

설치 전 준비 사항

V3 Net for Linux Server 를 설치하기 전 다음과 같은 항목을 확인합니다.

- 제품 번호: 제품에 포함된 소프트웨어 사용권 증서에 표시되어 있는 제품 번호를 확인합니다.
- 서버 IP 주소: V3 Net for Linux Server 를 설치할 서버의 IP 주소를 확인합니다. 서버에서 **ifconfig** 명령을 입력하여 확인할 수 있습니다.
- AhnLab Policy Center IP 주소: AhnLab Policy Center 를 사용하여 V3 Net for Linux Server 를 관리하기를 원하는 경우 AhnLab Policy Center 관리자에게 AhnLab Policy Center 의 IP 주소를 미리 확인하십시오.
- AhnLab Policy Center 제품 번호: AhnLab Policy Center 를 사용하여 V3 Net for Linux Server 를 관리하기를 원하는 경우 AhnLab Policy Center 관리자에게 AhnLab Policy Center 의 제품 번호를 미리 확인하십시오.

설치하기

V3 Net for Linux Server 를 설치하는 방법은 다음과 같습니다.

1. 설치 CD 를 CD 롬에 넣고 CD 롬 드라이브를 마운트합니다.

```
root@FileServer:/# mount -t iso9660 -r /dev/cdrom /mnt/cdrom
```

> **참고**
> 마운트 명령어는 운영 체제 또는 시스템에 따라 다를 수 있습니다. CD 롬이 마운트되지 않는 경우 운영 체제 또는 시스템에 맞는 마운트 명령을 확인하여 입력하십시오.

2. 설치 파일을 **/tmp** 에 복사합니다.

```
cp /mnt/cdrom/v3net-linux-3.x.x.x.x.tar.Z /tmp
```

> **참고**
> **/tmp** 에는 약 100M 정도의 여유 공간이 있어야 합니다.

3. 압축을 해제합니다.

```
uncompress v3net-linux-3.x.x.x.x.tar.Z 또는 gunzip v3net-linux-3.x.x.x.x.tar.Z
tar xvf v3net-linux-3.0.0.2.222.tar
```

> **참고**
> 해당 시스템에 **uncompress** 또는 **gunzip** 명령어가 없는 경우에는 Windows 에서 *.Z 압축을 해제 해야합니다.

4. 설치 경로로 이동합니다.

```
cd /tmp/v3net
```

5. 이동한 디렉터리에 설치 스크립트를 실행합니다.

```
root@FileServer:/tmp/v3net# ./install.sh
```

> **참고**
> **./install.sh** 를 root 계정이 아닌 다른 계정으로 실행하면 설치 스크립트가 실행되지 않습니다. 반드시 root 계정으로 **./install.sh** 를 실행하십시오.

> **참고**
> **su -** 명령을 입력하면 root 계정으로 로그인할 수 있습니다.

6. 설치 디렉터리를 묻는 메시지가 나타납니다. 기본 설치 디렉터리인 **/usr/local/v3net** 에 설치하려면 **Enter** 를 누르십시오. 다른 디렉터리에 설치하려면 설치할 디렉터리를 입력한 다음 **Enter** 를 누르십시오.

Installation Path (default: /usr/local/v3net):

7. 웹 보안 기능 사용 여부를 묻는 메시지가 나타납니다. 웹 보안을 사용하려면 **y** 를 입력하고 사용하지 않으려면 **n** 을 입력합니다.

Use Web Security?(y/n) (default: No):

8. 웹 UI 에 접속하기 위한 포트를 묻는 메시지가 나타납니다. 기본 HTTP 포트인 **80** 을 사용하려면 **Enter** 를 누르십시오. 다른 포트를 사용하려면 사용할 포트를 입력한 다음 **Enter** 를 누르십시오.

HTTP Port (default: 80):

9. 회사 이름을 묻는 메시지가 나타납니다. 회사 이름을 입력한 다음 **Enter** 를 누르십시오.(예: Company)

Company: Company

10. 사용자 이름을 묻는 메시지가 나타납니다. 사용자 이름을 입력한 다음 **Enter** 를 누르십시오.(예: User)

User Name: User

11. 제품에 적용할 언어를 선택합니다. 한국어, 영어, 중국어 간체를 선택할 수 있습니다. 적용할 언어의 번호를 입력한 다음 **Enter** 를 누르십시오.

Select Language (1: Korean, 2: English, 3: Simplified Chinese):

12. 제품 번호를 입력하라는 메시지가 나타나면 소프트웨어 사용권 증서에 있는 제품 번호를 입력한 다음 **Enter** 를 누르십시오.

Product No.(example: 12345678-12345678): 12345678-12345678

13. AhnLab Policy Center 와 연동할지를 묻는 메시지가 나타납니다. AhnLab Policy Center 를 사용한다면 **y** 를 입력하고 사용하지 않는다면 **n** 을 입력합니다.

Interoperate with AhnLab Policy Center? (y/n): y

14. **y** 를 입력하면 AhnLab Policy Center 의 IP 주소를 묻는 메시지가 나타납니다. AhnLab Policy Center 의 IP 주소를 입력한 다음 **Enter** 를 누르십시오.(예: 123.123.123.123)

AhnLab Policy Center IP Address: 123.123.123.123

15. AhnLab Policy Center 의 서버 타입을 선택하는 메시지가 나타납니다. **AhnLab Policy Center 4.6 / AhnLab Policy Center 4.6 for Windows** 를 서버로 설정하려면 **1** 을 입력하고, **AhnLab EPP Management** 를 서버로 설정하려면 **2** 를 입력한 다음 **Enter** 를 누르십시오.

AhnLab Policy Center Server Type
1. AhnLab Policy Center 4.6 / AhnLab Policy Center 4.6 for Windows
2. AhnLab EPP Management
AhnLab Policy Center Server Type ? (1/2) : 1

16. 서버 타입 선택 과정에서 **1** 을 입력하면, AhnLab Policy Center 제품 번호를 입력하라는 메시지가 나타납니다. 제품 번호를 입력한 다음 **Enter** 를 누르십시오.

```
AhnLab Policy Center Product No.(example: 12345678-12345678):
```

> **참고**
> 제품 번호 입력 과정은 서버 타입을 AhnLab Policy Center 4.6 / AhnLab Policy Center 4.6 for Windows 로 선택한 경우에만 진행됩니다. 서버 타입을 AhnLab EPP Management 로 선택한 경우에는 진행되지 않습니다.

17. 제품 설치를 진행하기 전, 이전 단계에서 입력한 내용이 맞는지 확인 후 설치 진행 여부를 선택하는 메시지가 나타납니다. 설치를 진행하려면 **y** 를 누릅니다.

```
[ Configured Information ]
---------------------------------------------------------------------
Installation Path: /usr/local/v3net
Use Web Security: No
AhnLab Policy Center IP Address: 123.123.123.123
HTTP Port: 9999
Company:
UserName:
Language : English
---------------------------------------------------------------------
Do you want to continue to install? (y/n): y
```

18. 제품 설치가 완료되면 다음과 같은 메시지가 나타납니다.

```
Installation completed.
```

19. 다음과 같은 명령을 입력하여 V3 Net for Linux Server 를 실행합니다.

```
root@FileServer:/usr/local/v3net/# ./v3net.sh start
Starting the process...
```

20. 다음과 같은 명령을 입력하여 V3 Net for Linux Server 제품 실행 상태를 확인합니다.

```
# ./v3net.sh status
--------------------------------------
V3 Net for Linux Server status
--------------------------------------
v3netd - running (5684)
v3netd watchdog - running (5830)
v3net-agentd - running (5695)
```

```
v3net-agentd watchdog - running (5839)
lighttpd - running (5690)
epp-agentd - not running
epp-agentd watchdog - not running
v3fbmond - running (5826)
v3fbmond watchdog - running (5965)
----------------------------------------
```

참고

제품 실행 상태는 **ps -ef | grep v3net** 명령으로도 확인할 수 있습니다.

참고

AhnLab Policy Center 를 연동한 경우 apc-agentd, apc-agentd watcdog, AhnLab EPP Management 를 연동한 경우 epp-agentd, epp-agentd watchdog 이 출력됩니다.

제거하기

V3 Net for Linux Server 를 제거하는 방법은 다음과 같습니다.

1. 다음과 같은 명령을 입력하여 V3 Net for Linux Server 를 제거합니다.

```
root@FileServer:/# /usr/local/v3net/uninstall.sh
```

> **참고**
> 설치 디렉터리가 **/usr/local/v3net/**가 아닌 경우 V3 Net for Linux Server 를 설치한 디렉터리에 맞는 명령어를 입력하십시오.

2. 다음과 같이 제품 삭제를 확인하는 메시지가 나타나면 **y** 를 누릅니다.

```
Do you want to delete V3 Net for Linux Server(3.0.0.0 (Build 000))?(y/n) y
```

> **참고**
> 제품 제거 시 파일 검사나 업데이트가 실행 중인 경우, 현재 실행 중인 검사 및 업데이트를 중단해야 제품을 제거할 수 있습니다.

3. 제품 삭제가 완료되면 다음과 같은 메시지가 나타납니다.

```
Uninstallation completed.
```

보안 사항

V3 Net for Linux Server 를 설치하고 사용하기 전에 먼저 다음과 같은 보안 사항을 확인하십시오.

- 신뢰된 관리자: V3 Net for Linux Server 의 허가 받은 관리자는 악의가 없으며 V3 Net for Linux Server 관리 기능에 대하여 적절히 교육받고, 관리자 지침에 따라 정확하게 의무를 수행해야 합니다.
- 안전한 관리: 허가 받은 관리자는 V3 Net for Linux Server 를 안전한 방법으로 배포 및 설치해야 하며 안전한 방식으로 구성, 관리, 사용해야 합니다.
- 운영 체제 보강: V3 Net for Linux Server 를 사용할 때 필요 없는 서비스를 중지하고 운영 체제의 취약점을 보완하는 패치를 실행하여 운영 체제에 대한 신뢰성과 안정성을 보장할 수 있어야 합니다.
- V3 Net for Linux Server 의 최신 업데이트 유지: 관리자는 V3 Net for Linux Server 의 바이러스 차단 기능을 안전하게 관리해야 합니다. 또한 새로운 악의적인 공격으로부터 V3 Net for Linux Server 와 V3 Net for Linux Server 의 운영 환경을 보호하기 위해 엔진과 패치를 최신 버전으로 유지해야 합니다.
- V3 Net for Linux Server 의 관련 서버: 관리자는 V3 Net for Linux Server 와 관련된 AhnLab Policy Center 서버를 안전하게 관리하거나 안전성이 보장된 서버를 사용해야 합니다.
- 안전한 업데이트 서버: (주)안랩은 V3 Net for Linux Server 의 엔진, 패치의 업데이트에 사용되는 AST 서버 및 CDN 서버를 안전하게 관리하여 신뢰성과 안정성을 보장하고 있습니다.

로그인하기

V3 Net for Linux Server 를 사용하여 정책을 설정하거나 업데이트, 환경 설정 등을 하기 위해서는 웹 브라우저를 이용하여 V3 Net for Linux Server 에 접속해야 합니다. V3 Net for Linux Server 를 사용하기 위해 V3 Net for Linux Server 에 로그인, 로그아웃하는 방법은 다음과 같습니다.

> **참고**
> **웹 보안** 기능을 사용하려면 Internet Explorer 10.0 이상 버전의 웹 브라우저를 사용하여 접속해야 합니다.

로그인

V3 Net for Linux Server 를 설치하면 웹 브라우저를 통해서 다른 컴퓨터에서 접속할 수 있습니다. 다른 컴퓨터에서 V3 Net for Linux Server 에 로그인하는 방법은 다음과 같습니다.

1. 컴퓨터에서 웹 브라우저를 실행합니다.
2. 웹 브라우저의 주소 입력 창에 **http://V3 Net for Linux Server 의 IP 주소**를 입력하여 V3 Net for Linux Server 에 연결합니다.(예: http://123.123.123.123)

3. 로그인 화면이 나타나면 **아이디**에 관리자 아이디를 입력하고 비밀번호에 관리자의 비밀번호를 입력합니다. 관리자 아이디의 기본 값은 **v3net** 입니다. (관리자 비밀번호의 기본 값은 별도 전달)

4. **로그인**을 눌러 V3 Net for Linux Server 에 로그인합니다.

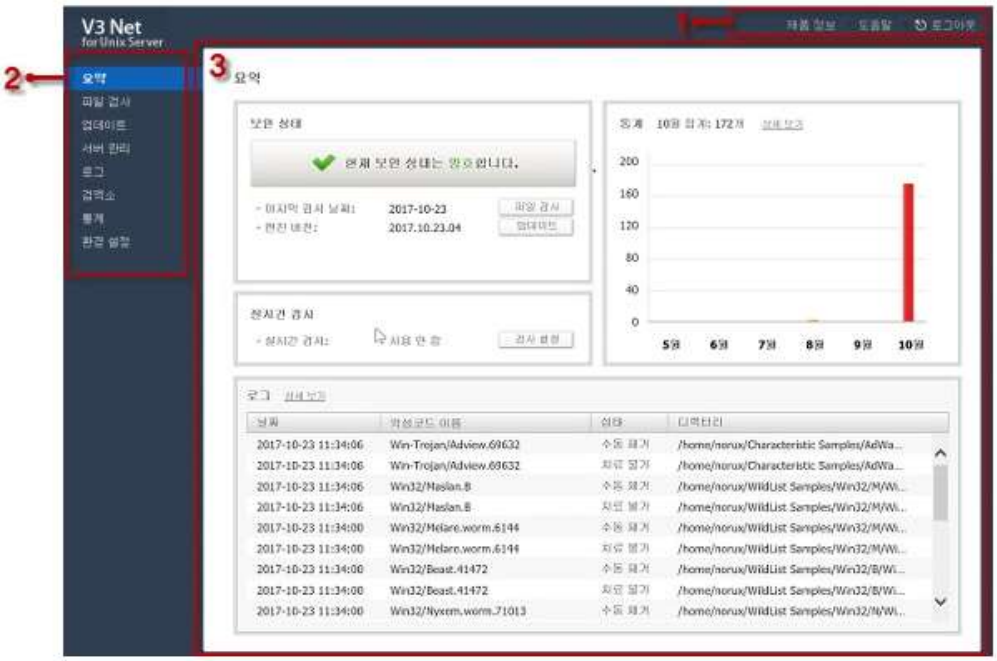
> ⚠**주의**
> 정상적으로 로그인한 다음에는 반드시 **서버 관리**에서 아이디 또는 비밀번호를 변경하십시오.

로그아웃

V3 Net for Linux Server 사용을 마치고 로그아웃하려면 웹 브라우저를 닫거나 오른쪽 위에 있는 **로그아웃**을 누르십시오.

둘러보기

V3 Net for Linux Server 의 웹 UI 는 다음과 같이 구성되어 있습니다.



1. 공통 메뉴

V3 Net for Linux Server 를 사용할 때 어느 화면에서나 사용할 수 있는 메뉴입니다.

- 제품 정보: V3 Net for Linux Server 의 제품 이름, 버전 정보, 설치 날짜, 설치 디렉터리, 언어, 관리자 아이디, 엔진 버전, 커널 패키지 버전, 저작권, 오픈소스 라이선스 정보 등을 확인할 수 있습니다.
- 도움말: V3 Net for Linux Server 의 도움말을 볼 수 있습니다.
- 로그아웃: V3 Net for Linux Server 에서 로그아웃합니다.

2. 메뉴

V3 Net for Linux Server 의 정책을 설정하거나 환경을 설정하는데 필요한 주 메뉴입니다.

3. 작업 영역

V3 Net for Linux Server 의 정책을 설정하고 정보를 확인할 수 있는 영역입니다. 선택한 메뉴에 따라 목록으로 된 화면이 나타나거나 항목을 추가할 수 있는 화면, 정보를 확인할 수 있는 화면이 나타납니다.

주요 기능

V3 Net for Linux Server 의 각 메뉴별 주요 기능은 다음과 같습니다.

- 요약: V3 Net for Linux Server 의 보안 상태와 실시간 검사, 바이러스 통계 및 로그에 대한 요약 정보를 확인할 수 있습니다.
- 파일 검사: 서버의 파일을 검사할 수 있습니다.
- 업데이트: V3 Net for Linux Server 를 업데이트하거나 업데이트와 관련된 설정을 설정할 수 있습니다.
- 서버 관리: V3 Net for Linux Server 의 정보를 확인할 수 있으며, 웹 보안 사용 설정과 관리자 정보를 설정할 수 있습니다.
- 로그: V3 Net for Linux Server 의 검사 로그와 이벤트 로그를 확인할 수 있습니다.
- 검역소: 치료된 파일을 확인하고 복원하거나 신고할 수 있습니다.
- 통계: 월별, 기간별 바이러스 통계를 확인할 수 있습니다.
- 환경 설정: 검사 설정과 검사 예외 설정, 일반 환경 설정을 설정할 수 있습니다.

요약

요약에서는 V3 Net for Linux Server 의 보안 상태와 바이러스 통계 및 로그에 대한 요약 정보를 확인할 수 있습니다.

보안 상태

V3 Net for Linux Server 의 엔진이 최신 버전이 아닐 경우 웜 또는 바이러스를 진단하지 못할 수 있습니다. 또한, 엔진이 최신 버전이라 하더라도 파일을 검사한지 오래되었다면 보안 상태가 위험할 수 있습니다.

- 마지막 검사 날짜: 마지막으로 검사한 날짜를 확인할 수 있습니다. **마지막 검사 날짜**가 오래되었다면 **파일 검사**를 눌러 파일을 검사할 수 있습니다.
- 엔진 버전: V3 Net for Linux Server 의 엔진 버전을 확인할 수 있습니다. 엔진 버전이 최신 버전이 아닐 경우에는 **업데이트**를 눌러 업데이트를 진행할 수 있습니다.
- 관리 서버 연결 상태: 관리 서버와 연동하도록 설치한 경우 나타나는 항목입니다. 관리 서버와의 연결 상태를 확인할 수 있습니다.

실시간 검사

실시간 검사에서는 실시감 검사 사용 여부를 확인할 수 있습니다. **검사 설정**을 누르면 실시감 검사를 설정할 수 있습니다.

통계

통계에서는 월별 통계를 그래프로 확인할 수 있습니다. **상세 보기**를 누르면 월별, 기간별 통계를 확인할 수 있습니다.

로그

로그에서는 검사 관련 로그를 확인할 수 있습니다. **상세 보기**를 누르면 검사 로그와 이벤트 로그를 자세하게 확인할 수 있습니다.

파일 검사

파일 검사는 V3 Net for Linux Server 의 가장 중요한 기능입니다. 파일 검사에서는 V3 Net for Linux Server 가 설치된 파일 서버에 대해서 검사를 실행하여 악성코드를 진단, 치료할 수 있습니다.

검사 대상을 선택하여 파일 검사하기

검사 대상을 선택하여 파일을 검사하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. <파일 검사>의 **검사 대상**에서 검사할 디렉터리를 선택합니다.
3. **검사 시작**을 누릅니다.
4. <검사하기>가 나타나며 자동으로 검사가 시작됩니다.
5. 발견된 악성코드가 있을 경우 **치료하기**를 누르면 악성코드를 치료할 수 있습니다.
6. **닫기**를 눌러 <검사하기>를 닫습니다.

사용자 정의 검사 목록으로 검사하기

사용자 정의 검사를 이용하면 자주 검사하는 디렉터리를 간편하게 검사할 수 있습니다.

사용자 정의 검사 추가

사용자 정의 검사를 하려면 우선 사용자 정의 검사를 추가해야 합니다. 사용자 정의 검사를 추가하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. <파일 검사>의 **사용자 정의 검사 목록**을 누릅니다.
3. ✚**추가**를 누른 다음 **검사 이름**을 입력합니다.
4. **검사 대상 선택**에서 검사할 디렉터리를 선택합니다.
5. **확인**을 누릅니다.
6. **적용**을 눌러 설정을 적용합니다.

사용자 정의 검사 수정

사용자 정의 검사를 수정하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. <파일 검사>의 **사용자 정의 검사 목록**을 누릅니다.
3. 수정할 항목을 하나만 선택한 다음 **수정**을 누릅니다.
4. 원하는 항목을 수정한 다음 **확인**을 누릅니다.
5. **적용**을 눌러 설정을 적용합니다.

사용자 정의 검사 삭제

사용자 정의 검사를 삭제하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. <파일 검사>의 **사용자 정의 검사 목록**을 누릅니다.
3. 삭제할 항목을 모두 선택한 다음 **삭제**를 누릅니다.
4. 삭제를 확인하는 메시지가 나타나면 **확인**을 누릅니다.
5. **적용**을 눌러 설정을 적용합니다.

사용자 정의 검사

추가한 사용자 정의 검사로 검사하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. <파일 검사>의 **사용자 정의 검사 목록**을 누릅니다.
3. 검사할 사용자 정의 검사를 하나만 선택합니다.
4. **검사 시작**을 누르면 <검사하기>가 나타나며 자동으로 검사가 시작됩니다.
5. 발견된 악성코드가 있을 경우 **치료하기**를 누르면 악성코드를 치료할 수 있습니다.
6. **닫기**를 눌러 <검사하기>를 닫습니다.

예약 검사

예약 검사에서는 원하는 시간에 자동으로 검사를 실행하도록 설정할 수 있습니다.

예약 검사 추가

예약 검사를 추가하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. **예약 검사**의 ✚**추가**를 누릅니다.
3. 설정 창이 나타나면 **예약 검사 사용**을 선택한 후, 다음과 같은 항목을 설정합니다.
    - 예약 검사 이름: 예약 검사의 이름을 입력합니다.
    - 예약 기간 선택: 검사를 실행할 주기를 선택합니다.
        - 매일: 매일 설정한 시간에 검사를 실행합니다.
        - 매주: 매주 설정한 요일의 설정한 시간에 검사를 실행합니다.
        - 매월: 매월 설정한 날의 설정한 시간에 검사를 실행합니다.
        - 한 번만: 설정한 날의 설정한 시간에 한 번만 검사를 실행합니다.
    - 검사 대상 선택: 검사할 디렉터리를 선택합니다.
    - 검사 설정: 검사에 대한 설정을 할 수 있습니다.
    - 검사 파일 선택: 검사할 파일을 선택할 수 있습니다.
        - 모든 파일 검사: 검사할 디렉터리에 있는 모든 파일을 검사합니다.
        - 감염되기 쉬운 파일 검사: 악성코드에 감염되기 쉬운 파일만 검사합니다. 모든 파일 검사에 비해 검사 시간이 짧지만 모든 파일을 검사하지 않으므로 진단하지 못하는 악성코드가 있을 수 있습니다.
        - 추가로 검사할 확장자: 사용자가 확장자를 입력하여 추가로 파일을 검사합니다. 확장자를 여러 개 입력할 경우 /로 구분하여 입력합니다.
        - 압축 파일 검사: 압축 파일을 검사합니다. 압축 파일안에 포함된 파일이 악성코드에 감염되어 있을 경우 위험하지 않지만 예방을 위해 검사할 수 있습니다. 압축 파일을 검사하도록 설정하면 압축 파일의 크기, 개수, 다중 압축 여부에 따라 검사 시간이 길어질 수 있습니다.
    - 치료 방법 선택: 악성코드 또는 감염된 압축 파일의 치료 방법을 선택할 수 있습니다.
        - 그대로 두기: 악성코드 또는 감염된 압축 파일이 진단되어도 그대로 둡니다.

  - 치료하기: 악성코드가 진단되면 치료합니다.
  - 삭제하기: 악성코드 또는 감염된 압축 파일이 진단되면 삭제합니다.
  - 자동 치료: 진단된 항목을 자동으로 치료합니다.
  - 치료 또는 삭제 전 감염된 파일을 검역소로 보내기: 치료 또는 삭제하기 전에 감염된 파일을 검역소에 백업합니다. 정상 파일을 잘못 진단하거나 중요한 파일이어서 복구가 필요한 경우에 복원할 수 있으므로 선택하는 것이 좋습니다.
- CPU 점유율 선택: 예약 검사 실행 시 CPU 점유율을 선택합니다.

4. **확인**을 누릅니다.
5. **적용**을 눌러 설정을 적용합니다.

> **참고**
> 예약 검사를 추가하는 방법에 대한 예는 새벽에 예약 검사하기를 참고하십시오.

예약 검사 수정

예약 검사를 수정하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. **예약 검사 목록**에서 수정할 항목을 하나만 선택한 다음 **수정**을 누릅니다.
3. 원하는 항목을 수정한 다음 **확인**을 누릅니다.
4. **적용**을 눌러 설정을 적용합니다.

예약 검사 삭제

예약 검사를 삭제하는 방법은 다음과 같습니다.

1. 메뉴에서 **파일 검사**를 선택합니다.
2. **예약 검사 목록**에서 삭제할 항목을 모두 선택한 다음 **삭제**를 누릅니다.
3. 삭제를 확인하는 메시지가 나타나면 **확인**을 누릅니다.
4. **적용**을 눌러 설정을 적용합니다.

업데이트

(주)안랩은 악성코드에 대응하기 위해 정기적으로 새로운 엔진을 제공합니다. 이전 버전의 엔진으로는 새로운 유형의 악성코드를 탐지하지 못하거나 치료하지 못할 수 있습니다. V3 Net for Linux Server 를 사용할 때에는 엔진, 제품 패치를 최신 버전으로 유지하는 것이 매우 중요합니다. 업데이트에서는 V3 Net for Linux Server 를 업데이트하거나 업데이트와 관련된 설정을 설정할 수 있습니다.

업데이트 설정

업데이트에서는 업데이트와 관련된 항목을 설정할 수 있습니다. **업데이트 주기 설정**에 설정한 주기마다 **업데이트 서버 설정**에 설정한 서버를 통해 업데이트를 받아옵니다. 업데이트를 설정하는 방법은 다음과 같습니다.

1. 메뉴에서 **업데이트**를 선택합니다.
2. **업데이트 주기 설정**에서 다음과 같은 항목을 설정합니다.
   - 자동 업데이트 사용: 자동 업데이트의 사용 여부를 선택합니다. **자동 업데이트 사용**을 선택하면 **자동 업데이트 주기**마다 업데이트를 실행합니다.
     - 자동 업데이트 주기: 자동 업데이트의 주기를 설정합니다.
   - 예약 업데이트 사용: 업데이트를 원하는 시간에 실행하도록 설정할 수 있습니다.
     - 매일: 매일 설정한 시간에 업데이트를 실행합니다.
     - 매주: 매주 설정한 요일의 설정한 시간에 업데이트를 실행합니다.
     - 매월: 매월 설정한 날의 설정한 시간에 업데이트를 실행합니다.
     - 한 번만: 설정한 날의 설정한 시간에 한 번만 업데이트를 실행합니다.
3. **업데이트 서버 설정**에서 다음과 같은 항목을 설정합니다.
   - 인터넷을 통한 업데이트: 일반적으로 사용하는 업데이트 방법입니다. (주)안랩의 업데이트 서버에 연결하여 업데이트 파일을 받아 옵니다.
   - 사용자 정의 서버를 통한 업데이트: 인터넷을 사용할 수 없는 환경에서 사용하는 업데이트 방법입니다. 업데이트 서버에 업데이트 파일을 두고 FTP 로 접속하여 업데이트 파일을 받아오는 방법입니다. FTP 서버의 경로를 입력한 다음 FTP 서버에 접속할 수 있는 아이디와 비밀번호를 입력합니다.
   - 로컬 디렉터리를 통한 업데이트: 네트워크를 완전히 사용할 수 없는 환경에서 사용하는 업데이트 방법입니다. 업데이트 파일을 로컬 서버에 복사해 두고 경로를 설정하여 업데이트하는 방법입니다. **변경**을 눌러 업데이트 파일이 있는 디렉터리를 설정할 수 있습니다.
4. **프록시 서버 설정**에서 다음과 같은 항목을 설정합니다.

- 프록시 서버 사용: 업데이트를 위해 인터넷에 연결할 때 프록시 서버를 사용합니다.
  - 서버 주소: 프록시 서버의 주소를 입력합니다.
  - 포트 번호(1~65534): 프록시 서버에서 사용하는 포트 번호를 입력합니다. 포트 번호는 1~65534 사이에서 입력할 수 있습니다.

5. **기타 설정**에서 다음과 같은 항목을 설정합니다.

- 업데이트 시 제품 패치하기: 업데이트 파일을 받아올 때 제품의 패치도 함께 받아옵니다.
- 업데이트 정보 보기: 업데이트가 완료되면 업데이트된 내역을 확인할 수 있습니다.
- 무결성 검사하기: 받아온 업데이트 파일에 대해 무결성을 검사하여 정상적으로 받았는지 확인합니다.

6. 설정을 완료한 다음 **적용**을 누릅니다.

업데이트하기

V3 Net for Linux Server 를 즉시 업데이트하는 방법은 다음과 같습니다.

1. 메뉴에서 **업데이트**를 선택합니다.
2. **업데이트 시작**을 누릅니다.
3. 업데이트 창이 나타나며 업데이트가 진행됩니다.
4. 업데이트가 완료되면 창이 자동으로 닫힙니다.
5. 메뉴에서 **요약**을 눌러 **보안 상태**의 **엔진 버전**을 확인하여 최신 버전으로 엔진이 올바르게 업데이트되었는지 확인합니다.

> **참고**
> 업데이트 설정에 대한 예는 사용자 정의 서버를 통해 업데이트하기, 로컬 디렉터리를 통해 업데이트하기를 참고하십시오.

서버 관리

서버 관리에서는 V3 Net for Linux Server 의 정보를 확인할 수 있으며, 웹 보안 기능 사용 설정 및 관리자 정보를 변경할 수 있습니다.

웹 보안 사용 설정하기

웹 보안 기능을 사용하면, https 보안 연결을 통한 안전한 연결을 할 수 있습니다. 웹 보안 기능을 사용하기 위한 방법은 다음과 같습니다.

1. 메뉴에서 **서버 관리**를 선택합니다.
2. **서버 관리**에서 다음과 같은 정보를 확인합니다.
   - 호스트 이름: 접속한 V3 Net for Linux Server 의 호스트 이름을 확인할 수 있습니다.
3. **웹 보안 사용** 설정을 선택합니다. 웹 보안 기능을 사용하려면 다음 설정을 반드시 완료해야 합니다.
   - 접속 허용 IP 주소를 최소 1 개 이상 입력하십시오.
   - 설정되어 있는 기본 관리자 정보를 변경하십시오.
   - Internet Explorer 10.0 이상 버전을 사용하고, TLS 1.2 사용을 설정하십시오.

   참고
   TLS 1.2 사용은 **Internet Explorer > 도구 > 인터넷 옵션 > 고급**에서 설정할 수 있습니다.
4. **서버 관리 포트**와 **접속 허용 IP 주소**를 입력합니다.
   - 서버 관리 포트: 서버에 접속할 때 사용할 TCP 포트를 입력합니다. 기본 값은 HTTP 의 기본 포트인 **80** 입니다. TCP **80** 포트를 다른 웹 서비스로 사용해야 할 경우나 보안을 강화하기 위해서 서버 관리 포트를 변경할 수 있습니다. **서버 관리 포트**를 변경하면 현재 보고 있는 웹 UI 가 자동으로 새로 고침되며, 변경된 서버 관리 포트를 이용하여 웹 UI 에 다시 접속됩니다.
   - 접속 허용 IP 주소 1: 서버 접속을 허용할 관리자의 IP 주소 1 을 입력합니다.
   - 접속 허용 IP 주소 2: 서버 접속을 허용할 관리자의 IP 주소 2 을 입력합니다.
5. **관리자 정보**에서 다음과 같은 항목을 설정합니다. 웹 보안 기능을 사용하려면, 반드시 기본 관리자 정보를 변경해야 합니다.
   - 아이디: 관리자의 아이디를 확인하고 변경할 수 있습니다. 아이디는 영문 대/소문자와 숫자를 사용하여 최소 5 자 이상으로 입력하십시오. 공백은 입력할 수 없습니다.
   - 비밀번호: **비밀번호 변경**을 누르면 관리자의 비밀번호를 변경할 수 있습니다.

6. 설정을 완료한 다음 **적용**을 누릅니다.

참고

웹 보안 사용 설정을 변경하면 서버가 다시 시작됩니다.

로그

로그에서는 V3 Net for Linux Server 의 검사 로그와 이벤트 로그를 확인할 수 있습니다.

검사 로그 목록

로그에서 **검사 로그**를 선택하면 V3 Net for Linux Server 의 검사와 관련된 로그를 확인할 수 있습니다. **검사 로그**에서 확인할 수 있는 항목은 다음과 같습니다.

- 날짜: 로그가 발생한 날짜입니다.
- 악성코드 이름: 진단된 악성코드의 이름입니다.
- 상태: 현재 악성코드의 상태입니다.
- 검사 방법: 악성코드를 진단한 검사 이름을 표시합니다
- 디렉터리: 진단된 파일이 있는 디렉터리입니다.

이벤트 로그 목록

로그에서 **이벤트 로그**를 선택하면 V3 Net for Linux Server 와 관련된 일반적인 로그를 확인할 수 있습니다. **이벤트 로그**에서 확인할 수 있는 항목은 다음과 같습니다.

- 날짜: 로그가 발생한 날짜입니다.
- 분류: 이벤트 로그의 분류입니다.
- 내용: 이벤트 로그의 내용입니다.

참고

로그 목록에서 **내보내기**를 누르면 로그를 CSV 파일 형식으로 내보낼 수 있습니다.

검역소

검역소에서는 치료된 파일을 확인하고 복원하거나 신고할 수 있습니다. 확인할 수 있는 항목은 다음과 같습니다.

- 날짜: 파일이 검역소로 옮겨진 날짜입니다.
- 파일 이름: 검역소로 옮겨진 파일의 이름입니다.
- 디렉터리: 파일의 원래 위치입니다.
- 악성코드 이름: 진단된 악성코드의 이름입니다.
- 파일 종류: 진단된 파일의 종류입니다. 압축 파일인지 일반파일인지 확인할 수 있습니다.

참고

파일 이름의 오른쪽에 있는 를 누르면 검사 대상에 대한 상세한 정보를 확인할 수 있습니다.

참고

검역소에서 **신고하기**를 누르면 진단된 파일을 신고할 수 있는 웹사이트를 열 수 있습니다.

참고

항목을 선택하고 **복원하기**를 누르면 파일을 원래 디렉터리 또는 원하는 다른 디렉터리로 복원할 수 있습니다.

통계

통계에서는 월별, 기간별 바이러스 통계를 확인할 수 있습니다.

월별 통계 보기

통계 보기를 **월별**로 선택하면 치료 건수를 월별로 확인할 수 있으며 월별 그래프도 확인할 수 있습니다.

기간별 통계 보기

통계 보기를 **기간별**로 선택하면 원하는 기간을 선택하여 치료 건수를 일별로 확인할 수 있습니다.

검사 설정

검사 설정에서는 검사와 관련된 설정을 할 수 있습니다. 검사 설정을 하는 방법은 다음과 같습니다.

실시간 검사

- 실시간 검사 사용: 실시간 검사 사용 여부를 선택합니다.
- 실시간 검사 종료 후 자동으로 다시 시작: 실시간 검사를 종료했을 경우 자동으로 다시 시작할 시간을 설정합니다. 자동으로 다시 시작할 주기는 **사용 안 함, 10 분 후, 30 분 후, 60 분 후**를 선택할 수 있으며, 선택한 시간이 지난 후에 실시간 검사를 다시 시작합니다. **사용 안 함**을 선택하면, 실시간 검사를 종료한 후 자동으로 다시 시작하지 않습니다.
- 검사 대상: 검사할 파일을 선택할 수 있습니다.
  - 모든 파일 검사: 검사할 디렉터리에 있는 모든 파일을 검사합니다.
- 치료 방법: 악성코드에 감염된 대상을 치료하는 방법을 선택할 수 있습니다.
  - 악성코드 감염 파일: 악성코드에 감염된 파일에 대한 치료 방법을 설정합니다.
    - 그대로 두기: 악성코드 또는 감염된 압축 파일이 진단되어도 그대로 둡니다.
    - 치료하기: 악성코드가 진단되면 치료합니다.
    - 치료 또는 삭제 전 감염된 파일을 검역소로 보내기: 치료 또는 삭제하기 전에 감염된 파일을 검역소에 백업합니다. 정상 파일을 잘못 진단하거나 중요한 파일이어서 복구가 필요한 경우에 복원할 수 있으므로 선택하는 것이 좋습니다.
  - 실행 중인 악성코드: 실행 중인 악성코드의 치료 방법을 선택할 수 있습니다.
    - 강제로 멈추고 치료하기: 실행 중인 악성코드를 강제로 멈추고 치료합니다.
    - 실행 중인 상태로 치료하기: 실행 중인 악성코드를 멈추지 않고 실행 중인 상태로 치료합니다.
  - 치료 또는 삭제 전 감염된 파일을 검역소로 보내기: 치료 또는 삭제하기 전에 감염된 파일을 검역소에 백업합니다. 정상 파일을 잘못 진단하거나 중요한 파일이어서 복구가 필요한 경우에 복원할 수 있으므로 선택하는 것이 좋습니다.

파일 검사

- 검사 대상: 검사할 파일을 선택할 수 있습니다.
  - 모든 파일 검사: 검사할 디렉터리에 있는 모든 파일을 검사합니다.

- 감염되기 쉬운 파일 검사: 악성코드에 감염되기 쉬운 파일만 검사합니다. 모든 파일 검사에 비해 검사 시간이 짧지만 모든 파일을 검사하지 않으므로 진단하지 못하는 악성코드가 있을 수 있습니다.
- 추가로 검사할 확장자: 사용자가 확장자를 입력하여 추가로 파일을 검사합니다. 확장자를 여러 개 입력할 경우 /로 구분하여 입력합니다.

▪ 추가 기능

- 압축 파일 검사: 압축 파일을 검사합니다. 압축 파일안에 포함된 파일이 악성코드에 감염되어 있을 경우 위험하지 않지만 예방을 위해 검사할 수 있습니다. 압축 파일을 검사하도록 설정하면 압축 파일의 크기, 개수, 다중 압축 여부에 따라 검사 시간이 길어질 수 있습니다.

▪ 치료 방법: 악성코드 또는 감염된 압축 파일의 치료 방법을 선택할 수 있습니다.

- 그대로 두기: 악성코드 또는 감염된 압축 파일이 진단되어도 그대로 둡니다.
- 치료하기: 악성코드가 진단되면 치료합니다.
- 삭제하기: 악성코드 또는 감염된 압축 파일이 진단되면 삭제합니다.
- 자동 치료: 진단된 항목을 자동으로 치료합니다.
- 치료 또는 삭제 전 감염된 파일을 검역소로 보내기: 치료 또는 삭제하기 전에 감염된 파일을 검역소에 백업합니다. 정상 파일을 잘못 진단하거나 중요한 파일이어서 복구가 필요한 경우에 복원할 수 있으므로 선택하는 것이 좋습니다.

검사 예외 설정

검사 예외 설정에서는 검사 시 검사하지 않을 대상이나 검사 예외 악성코드를 설정할 수 있습니다.

검사 예외 사용

검사 예외 대상이나 검사 예외 악성코드를 설정하려면 **검사 예외 사용**을 선택해야 합니다.

참고

검사 예외 사용을 선택하지 않으면, 검사 예외 대상이나 검사 예외 악성코드를 설정할 수 없습니다.

검사 예외 대상 설정

검사하지 않을 디렉터리나 확장자를 추가하는 기능입니다.

주의

검사 예외로 추가한 대상은 악성코드에 감염된 경우에도 검사하지 않으므로 반드시 필요한 경우에만 사용하십시오.

검사 예외 디렉터리 추가

검사 예외 디렉터리를 추가하면 시스템의 중요한 디렉터리를 설정하여 시스템을 보호할 수 있습니다. 검사를 하지 않을 디렉터리를 추가하는 방법은 다음과 같습니다.

1. 메뉴에서 **환경 설정**을 선택합니다.
2. **검사 예외 설정**을 누릅니다.
3. **검사 예외 사용**을 선택합니다. **검사 예외 사용**을 선택하면 검사 예외로 추가한 디렉터리는 어떠한 경우에도 검사하지 않습니다. 파일 검사 또는 예약 검사에서 **검사 대상**을 설정하여 검사해도 검사 예외 디렉터리는 검사하지 않습니다.
4. **디렉터리 추가**를 누릅니다.
5. <디렉터리 선택>이 나타나면 검사를 하지 않을 디렉터리를 선택한 다음 **확인**을 누릅니다.
6. 디렉터리가 검사 예외 목록에 추가되면 **적용**을 누릅니다.

검사 예외 확장자 추가

검사 예외 확장자를 추가하면 악성코드에 감염될 확률이 적은 확장자를 등록하여 검사 시간을 줄일 수 있습니다. 검사를 하지 않을 확장자를 추가하는 방법은 다음과 같습니다.

1. 메뉴에서 **환경 설정**을 선택합니다.
2. **검사 예외 설정**을 누릅니다.
3. **검사 예외 사용**을 선택합니다. **검사 예외 사용**을 선택하면 검사 예외로 추가한 확장자는 어떠한 경우에도 검사하지 않습니다. 예약 검사에서 **추가로 검사할 확장자**를 설정하여 검사해도 검사 예외 확장자는 검사하지 않습니다.
4. **확장자 추가**를 누릅니다.
5. <확장자 추가>가 나타나면 검사를 하지 않을 확장자를 입력한 다음 **확인**을 누릅니다.

> **참고**
> 확장자를 여러 개 입력할 경우 /로 구분하여 입력할 수 있으며 악성코드에 감염될 확률이 높은 exe, dll, ocx 와 같은 확장자는 입력할 수 없습니다.

6. 확장자가 검사 예외 목록에 추가되면 **적용**을 누릅니다.

검사 예외 삭제

검사 예외로 추가한 디렉터리 또는 확장자를 삭제하는 방법은 다음과 같습니다.

1. 메뉴에서 **환경 설정**을 선택합니다.
2. **검사 예외 설정**을 누릅니다.
3. 검사 예외 목록에서 삭제할 디렉터리 또는 확장자를 선택한 다음 **삭제**를 누릅니다.
4. 삭제했다는 메시지가 나타나면 **확인**을 누릅니다.

> **참고**
> **기본 값**을 누르면 **검사 예외 대상 사용**의 사용 여부가 기본 값으로 설정됩니다.

검사 예외 악성코드 설정

검사하지 않을 악성코드를 설정하는 기능입니다.

> **주의**
> 검사 예외로 추가한 악성코드는 악성코드로 알려져 있지만 검사에서 제외하므로 반드시 필요한 경우에만 사용하십시오.

검사 예외 악성코드 추가

검사에서 제외할 악성코드를 추가합니다. 검사 예외 악성코드를 추가하는 방법은 다음과 같습니다.

1. 메뉴에서 **환경 설정**을 선택합니다.
2. **검사 예외 설정**을 누릅니다
3. 검사 예외 악성코드 설정에서 **추가**를 눌러 <검사 예외 악성코드 추가/수정>에서 악성코드 이름을 입력합니다. 악성코드 이름은 반드시 진단명과 동일하게 입력해야 합니다.
4. **확인**을 누른 후 입력한 악성코드 이름이 예외 목록에 등록되었는지 확인합니다.

참고

검사 예외 악성코드는 최대 50 개까지 추가할 수 있습니다.

검사 예외 악성코드 수정

검사 예외 악성코드를 수정하는 방법은 다음과 같습니다.

1. 메뉴에서 **환경 설정**을 선택합니다.
2. **검사 예외 설정**을 누릅니다
3. 검사 예외 악성코드 설정에서 **수정**을 눌러 <검사 예외 악성코드 추가/수정>에서 악성코드 이름을 수정합니다.
4. **확인**을 누른 후 수정한 악성코드 이름이 목록에 반영되었는지 확인합니다.

검사 예외 악성코드 삭제

검사 예외 악성코드를 삭제하는 방법은 다음과 같습니다.

1. 메뉴에서 **환경 설정**을 선택합니다.
2. **검사 예외 설정**을 누릅니다
3. 검사 예외 악성코드 목록에서 삭제할 대상을 선택한 후 **삭제**를 누릅니다.
4. 선택한 검사 예외 악성코드가 목록에서 삭제되었는지 확인합니다.

참고

관리 제품을 통해 관리자가 설정한 검사 예외 악성코드는 사용자 임의로 수정하거나 삭제할 수 없습니다.

일반 환경 설정

일반 환경 설정에서는 일반적인 환경을 설정할 수 있습니다. 일반 환경 설정을 설정하는 방법은 다음과 같습니다.

1. 메뉴에서 **환경 설정**을 선택합니다.
2. **일반 환경 설정**을 누릅니다.
3. **검역소 설정**에서 설정되어 있는 검역소의 디렉터리를 확인할 수 있습니다. **변경**을 누르면 검역소의 디렉터리를 변경할 수 있습니다.
4. **보관 공간 설정**에서 다음과 같은 항목을 설정합니다.
   - 검역소 크기: 검역소의 크기를 설정합니다. 설정한 검역소 크기보다 검역소 디렉터리의 크기가 커지면 오래된 파일부터 자동으로 삭제됩니다.
   - 검사 로그 크기: 검사 로그의 크기를 설정합니다. 설정한 **검사 로그 크기**보다 검사 로그의 크기가 커지면 오래된 로그부터 자동으로 삭제됩니다.
   - 이벤트 로그 크기: 이벤트 로그의 크기를 설정합니다. 설정한 **이벤트 로그 크기**보다 이벤트 로그의 크기가 커지면 오래된 로그부터 자동으로 삭제됩니다.
5. 설정이 완료되면 **적용**을 누릅니다.

참고

기본 값을 누르면 모든 설정이 기본 값으로 설정됩니다.