



사용자설명서

바이러스체이서 9.0 Enterprise 사용설명서의 내용과 소프트웨어는
(주)바이러스체이서의 저작권법에 의해 보호되고 있습니다.
(주)바이러스체이서의 사전 서명동의 없이 사용설명서 및 소프트웨어의 일부 또는 전체를 복사,
복제, 번역하거나 또는 전자매체나 기계가 읽을 수 있는 형태로 변경할 수 없습니다.

발행일 2015년 03월 03일(문서버전 1.3)





목 차

1. 개요.....	1
2. 주요 기능.....	1
3. 설치.....	2
3.1. 설치 전 확인 사항.....	2
3.2. 시스템 요구 사항.....	2
3.3. 설치 과정.....	3
4. 사용 설명.....	6
4.1. 프로그램 실행.....	6
4.2. 메인 프로그램.....	7
4.2.1. 메인 메뉴(Home).....	7
4.2.2. 검사하기.....	8
4.2.3. 업데이트.....	12
4.2.4. PC 보안.....	13
4.2.5. PC 관리.....	17
4.2.6. 기록관리.....	20
4.2.7. 환경 설정.....	22
4.2.8. 간편 메뉴 사용하기.....	26
5. 제거.....	28
6. 고객 지원.....	29



1. 개요

‘바이러스체이서 9.0 Enterprise’ 다양하고 지능적으로 변하는 사이버공격 및 악성코드 보안 위협에 대비하기 위해 개발된 강력한 시스템 보호 기능을 갖춘 통합 안티바이러스 솔루션입니다. 그리고 누구나 사용하기 간편한 UI로 보안 프로그램에 쉽게 접근 할 수 있습니다.

2. 주요 기능

직관성이 뛰어난 미니사이즈 UI 화면	<ul style="list-style-type: none"> - 사용자 편의성을 고려한 쉽고 편리한 간편모드 - 간편검사 및 업데이트 실행 중에도 기능이 중단 되지 않고 화면 전환 가능
나만의 원클릭 보안시스템	<ul style="list-style-type: none"> - 사용자의 검사 설정에 따라 한번의 클릭으로 검사 및 업데이트 할 수 있는 문제 해결하기 기능
실시간 바이러스 검출 그래프	<ul style="list-style-type: none"> - 유입되는 악성코드를 사전에 체크하여 실시간 감시 및 차단 - 감염된 PC에서 복제, 실행 등 위반 행위 시 바이러스 현황을 주간 별로 알려줌
네트워크 감시를 포함한 PC 보안	<ul style="list-style-type: none"> - 방화벽, 유해사이트 차단, 취약 계정 관리, 보안패치 제공
시스템 속도를 높이는 PC 성능 최적화	<ul style="list-style-type: none"> - 불필요한 임시파일 및 레지스트리를 삭제하여 PC 성능을 향상시키는 기능

Security Center ‘SC 2.1’ 통합보안관리 솔루션(중앙관리 시스템)

- ◇ 바이러스체이서의 중앙 관리뿐만 아니라 PC보안 상태의 모니터링, 에이전트 지원관리, 자산관리 등의 정보화 대응 서비스를 실시간으로 제공 합니다.



3. 설치

3.1. 설치 전 확인 사항

“바이러스체이서 9.0 Enterprise” 은 기업용, 개인용, 특화된 기업용 설치 파일로 구분되며 만약, 인터넷에 연결되지 않은 네트워크에 설치 할 경우 공급업체와 사전 협의가 필요합니다. 또한 설치하기 전에 다음 사항을 확인해야 합니다.

- 1) “바이러스체이서 9.0 Enterprise” 제품 설치를 위해서는 인터넷 연결이 필요 합니다. 인터넷이 연결되지 않았다면 먼저 인터넷을 연결 한 뒤 프로그램을 설치해야 합니다.
- 2) “바이러스체이서 9.0 Enterprise” 제품에는 바이러스 차단 프로그램이 포함되어 있습니다. 만약 다른 바이러스 차단 프로그램을 사용하는 경우 오류 방지를 위해 해당 프로그램을 제거하고, 설치해야 합니다.

3.2. 시스템 요구 사항

“바이러스체이서 9.0 Enterprise” 제품의 설치와 정상적인 사용을 위해서는 시스템은 다음 사양을 만족해야 합니다.

운영 체제

- Microsoft Windows XP Professional SP3 x86
- Microsoft Windows Vista Business SP1 x86, x64
- Microsoft Windows 7 Professional SP1 x86, x64
- Microsoft Windows 8 Pro x86/x64
- Microsoft Windows Server 2003 Standard SP2 x86, x64
- Microsoft Windows Server 2008 Standard SP2 x86, x64
- Microsoft Windows Server 2008 R2 Standard SP1 x64
- Microsoft Windows Server 2012 Standard x64

하드웨어

- CPU: Pentium4 16 GHz 이상 IBM-PC 호환 기종
- RAM: 2GB 이상
- HDD: 20GB 이상의 여유 공간
- NIC: 10/100/1000 Ethernet card 1 개 이상

지원 언어

- 한글, 영어

3.3. 설치 과정

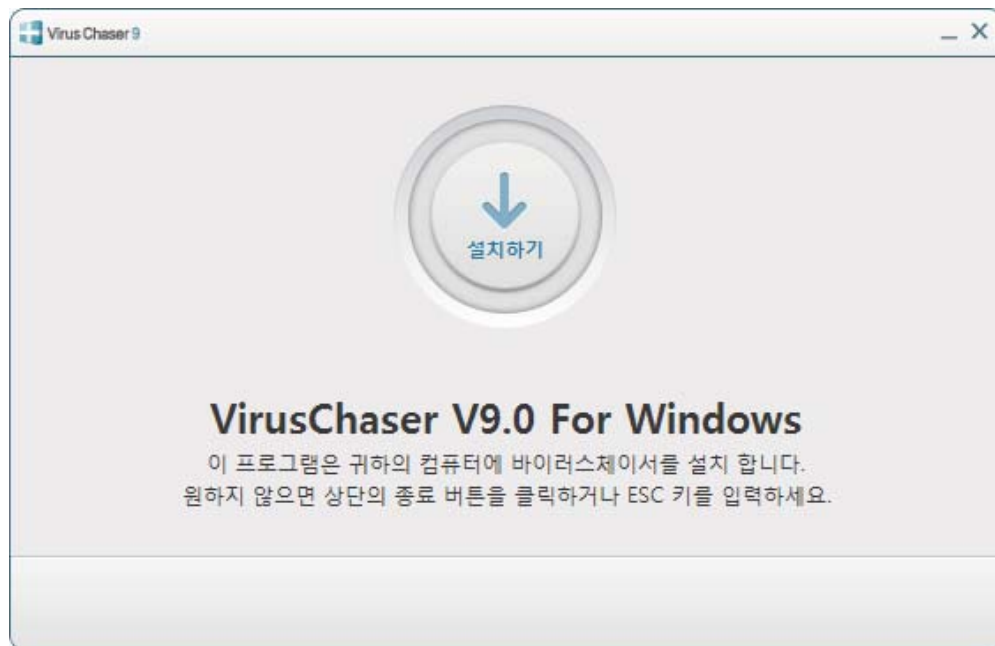
바이러스체이서 9.0 Enterprise의 설치 과정은 쉽고 간단합니다.

아래의 내용은 개인용 프로그램에 대한 것입니다.

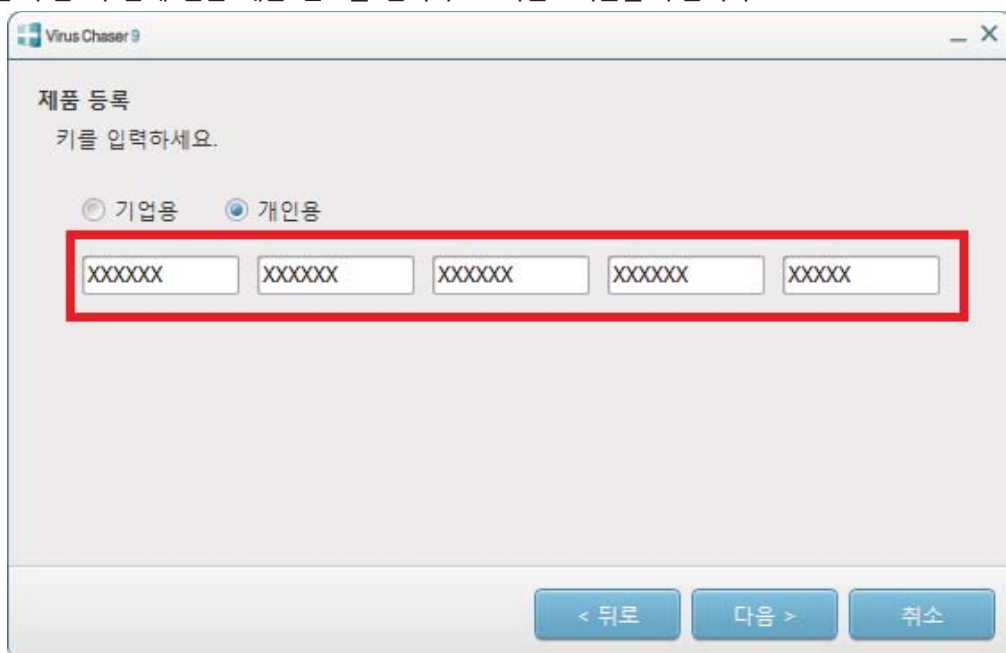
기업의 경우 이미 설치되어 있는 관리 툴 등을 이용하여 다양한 방법으로 설치가 가능하며 구체적인 내용은 공급업체와 상의 하는 것이 좋습니다.

1) 설치 시작

설치 파일 이름은 일반적으로 Setup.exe 라는 이름으로 되어 있고, 실행을 시키면 다음과 같이 나타납니다.

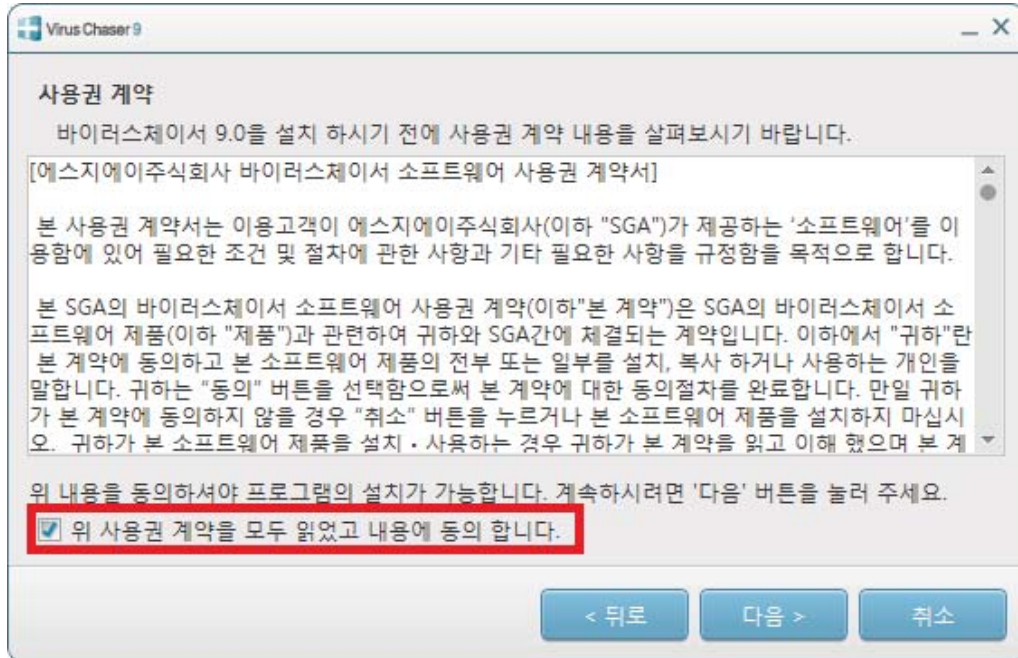


이때, 제품 구입 시 함께 받은 제품 번호를 입력하고 “다음” 버튼을 누릅니다.



2) 사용권 계약과 동의

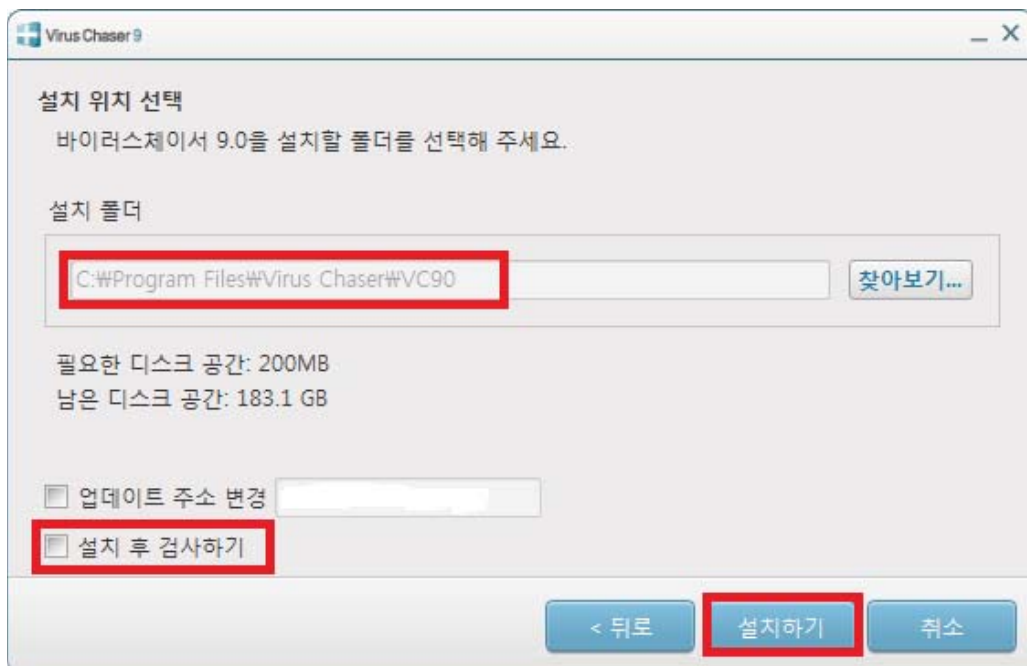
다음과 같이 사용권 계약에 동의를 해야 설치가 가능하며 계약의 내용을 잘 읽은 후 “위 사용권 계약을 모두 읽었고 내용에 동의 합니다.”를 선택하고 “다음” 버튼을 누릅니다. 단체사용자의 경우 별도의 사용권 계약이 이루어지고 이런 과정들이 모두 생략됩니다.



3) 설치 경로 선택

바이러스체이서 9.0 Enterprise 을 설치 할 폴더를 선택 할 수 있으며, 일반적으로는 운영체제가 설치된 드라이브의 “Program Files\Virus Chaser\VC90”에 설치 됩니다. 설치에 소요되는 시간은 환경에 따라 다소 차이가 있지만, 평균적으로 약 2-3분 정도 소요됩니다.

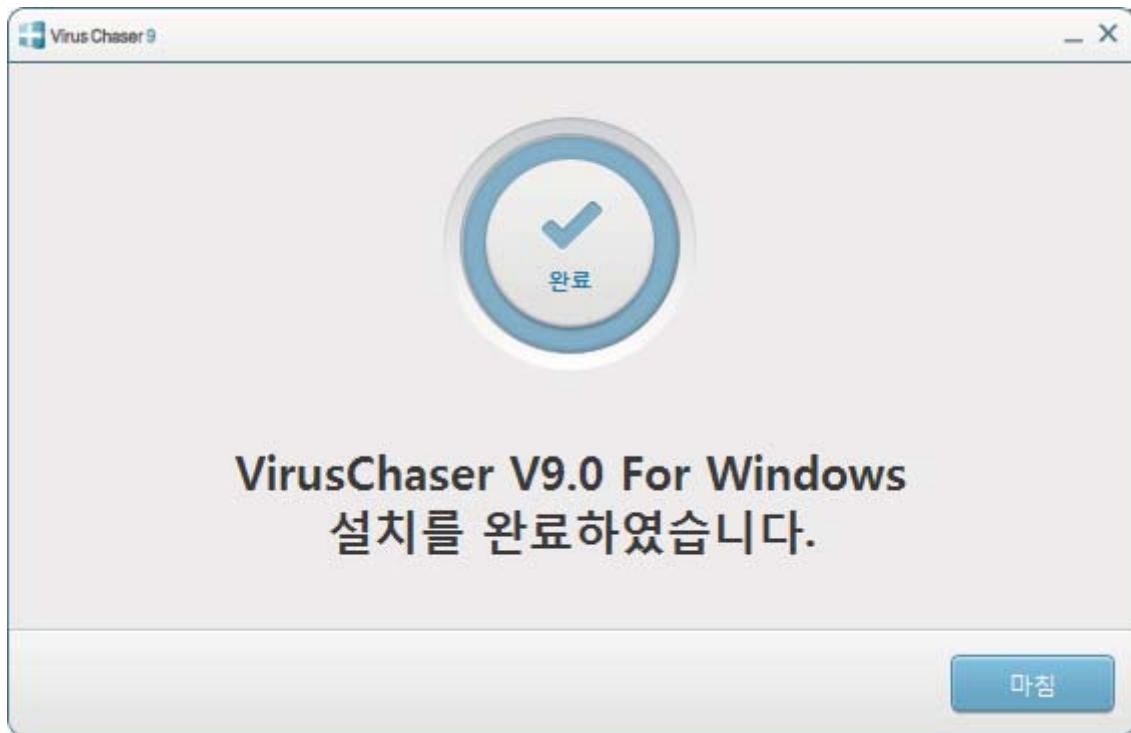
☆ “설치 후 검사하기”체크 후 설치하기를 누를 경우, 설치 후 트레이에서 간편검사가 진행됩니다.





4) 설치 완료

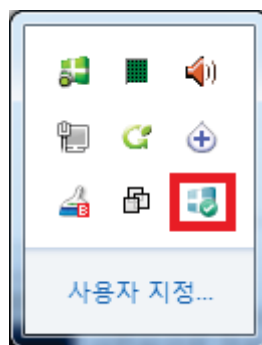
설치가 완료되면 다음과 같은 화면이 나타나고 “마침” 버튼을 누르면 모든 설치 과정이 종료됩니다.



5) 설치 확인

설치가 완료되면 다음과 같은 트레이 아이콘이 표시됩니다.

재시동 할 필요는 없지만 본 제품이 설치 되기 전에 이미 바이러스에 감염된 컴퓨터의 경우 설치 후 컴퓨터를 재 시작해야 안정적으로 사용 할 수 있습니다.

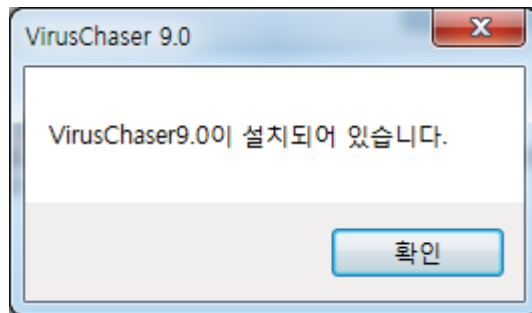


Windows 7 계열



6) 설치 실패

바이러스체이서 9.0 Enterprise 이 이미 설치되어 있는 경우 설치를 진행할 수 없습니다.



부득이 재 설치를 해야 한다면, 이미 설치 된 바이러스체이서 9.0을 제거 후 설치 해야 합니다. (“5. 제거” 항목 참조)

7) 설치 주의 사항

바이러스체이서 9.0 Enterprise 설치 시 바이러스체이서 9.0 이전 버전이 설치되어 있으면 자동으로 제거 합니다.

4. 사용 설명

4.1. 프로그램 실행

바이러스체이서 9.0 Enterprise이 설치되면 자동으로 프로그램이 실행되어 시스템을 보호하게 됩니다. 바이러스체이서 9.0 Enterprise 의 관리 콘솔을 실행시키기 위해서는 다음과 같이 트레이 아이콘에 마우스 오른쪽 버튼을 클릭하고 “관리자 열기”를 선택합니다.



- 관리자 열기 : 메인 프로그램을 실행 합니다.
- 보안 상태 : 현재의 보안 상태를 나타냅니다.
- 업데이트 : 업데이트 서버로부터 최신 업데이트를 실행 합니다.
- 간편 검사 : 간편검사를 시작/일시 중지 합니다.
- 무결성 검사 : 무결성 검사 기능을 실행 합니다.
- 간편모드 전환 : 모드를 간편하게 전환 합니다.

4.2. 메인 프로그램

메인 프로그램은 바이러스체이서 9.0 Enterprise 을 실행하면 가장 먼저 Home 메뉴가 표시되며, 검사하기, 업데이트, PC보안, PC관리, 기록관리로 구성되어 있습니다. 특정 메뉴로 이동을 원할 경우 상단에 나열된 탭을 선택하면 됩니다.

4.2.1. 메인 메뉴(Home)

메인 메뉴는 바이러스체이서 9.0 Enterprise 프로그램을 실행하면 표시되는 기본 화면으로 시스템 보안 상태 정보 및 업데이트 상태 정보를 확인할 수 있습니다. 메인 메뉴의 각 필드의 주요 기능은 다음과 같습니다.



- **보안 상태**

: 시스템의 보안 상태 정보가 표시 됩니다. 보안 상태에 따라 아이콘이 다르게 표시 됩니다. 상태에 따른 아이콘의 변화는 다음과 같습니다.

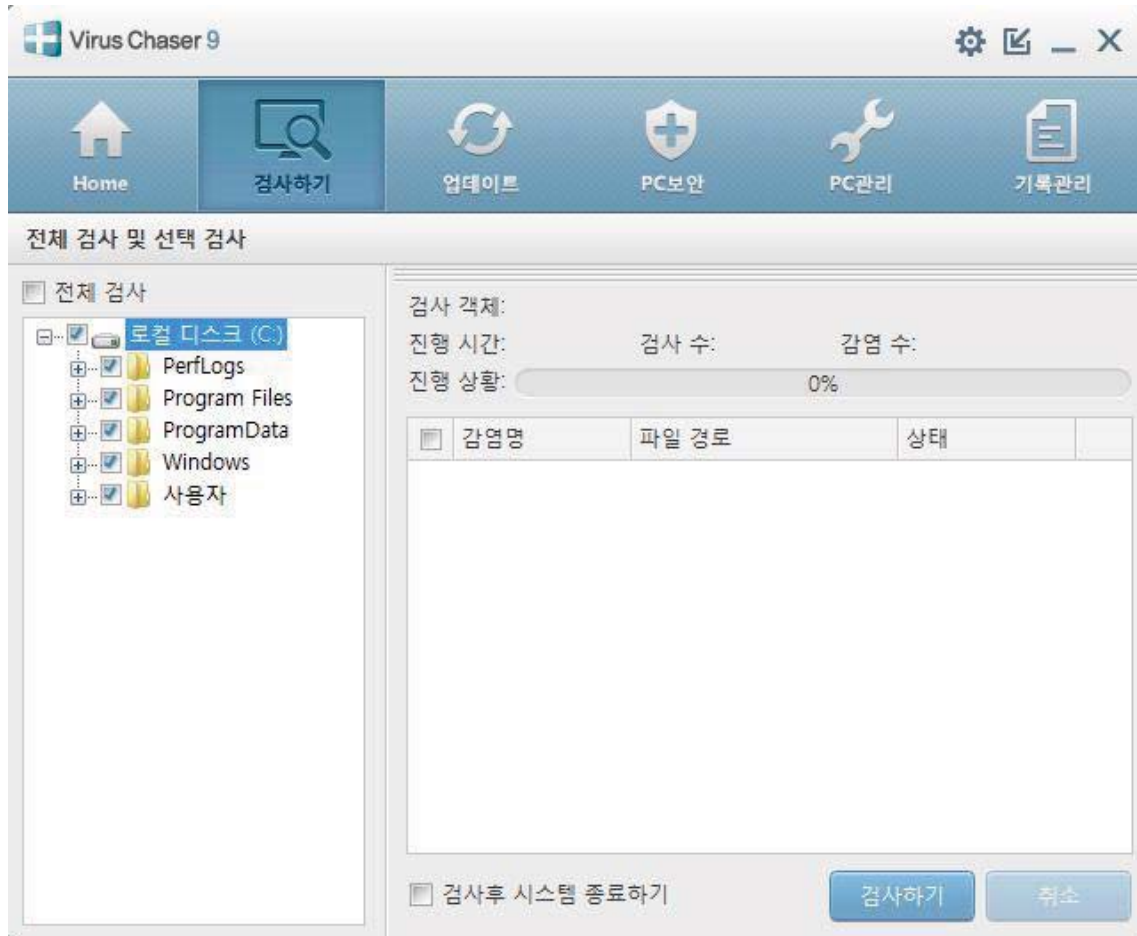
상태	아이콘	내용
안전		보안 상태 점검 항목 기준에 따라 안전 상태

경고		보안 상태 점검 항목 기준에 따라 경고 상태
위험		보안 상태 점검 항목 기준에 따라 위험 상태

- 실시간 바이러스 검출 그래프**
 : 실시간 감시로 인하여 바이러스 검출을 그래프로 확인할 수 있습니다.
- 간편검사**
 : 마지막 검사 날짜를 표시한다. 간편검사를 실행할 수 있으며 수동으로 시작/중지를 수행할 수 있습니다.
- 업데이트**
 : 업데이트 정보와 마지막 업데이트 날짜를 표시합니다. “업데이트 형식”에는 설정에 따라 수동/자동/지정 시간 업데이트가 표시되면 “업데이트 일시”에는 마지막으로 업데이트된 시각이 표시 됩니다. 또한 “업데이트” 버튼을 클릭하여 수동으로 최신 패턴 및 패치에 대한 업데이트를 수행할 수 있습니다.
- 최적화**
 : PC관리를 위해 시스템을 최적화 합니다. 마지막 최적화 날짜를 표시하며, 수동으로 최적화 목록을 선택하여 실행할 수 있습니다.

4.2.2. 검사하기

검사하기 메뉴는 전체 검사 및 선택 검사를 통해 검사할 대상을 선택하여 검사할 수 있도록 구성되어 있습니다.

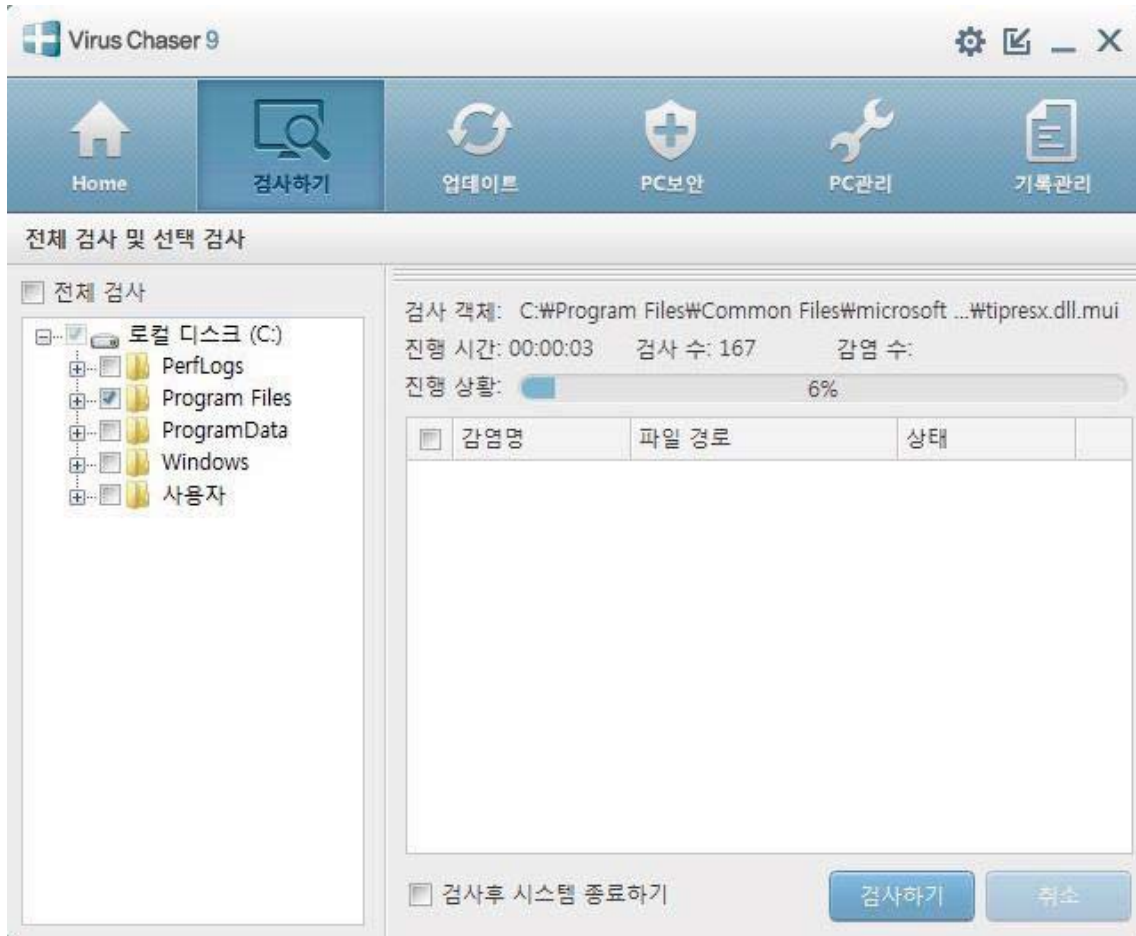


- **전체 검사**

: 검사할 대상을 전체로 선택하여 검사하기 위한 항목입니다. 전체 검사 항목에 체크표시하고 “검사하기” 버튼을 클릭하면 전체 항목의 검사를 시작 합니다.

- **선택 검사**

: 검사하고자 하는 대상을 사용자가 선택하여 검사하기 위한 항목입니다. 선택된 항목의 검사만 시작 합니다.

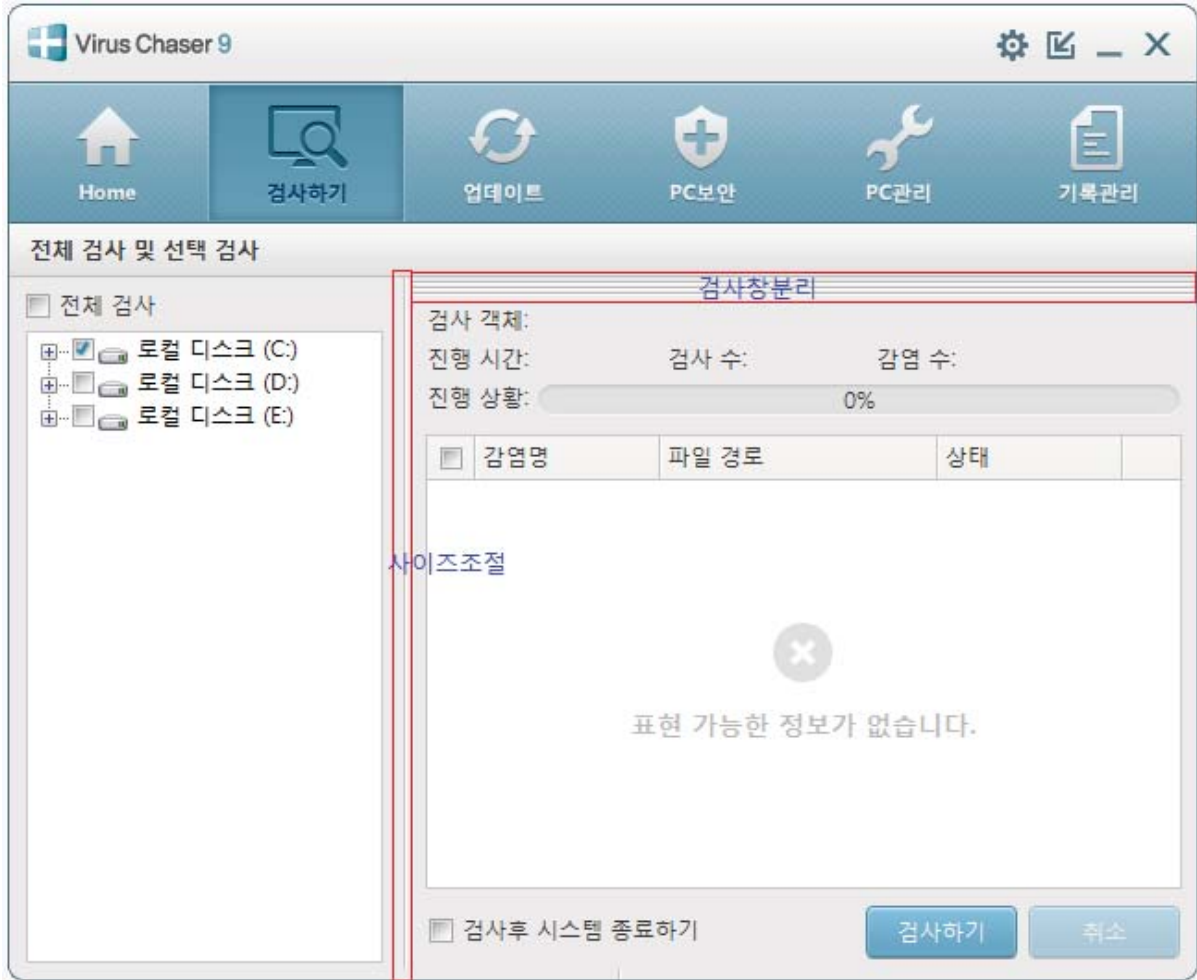


- **검사 후 시스템 종료하기**

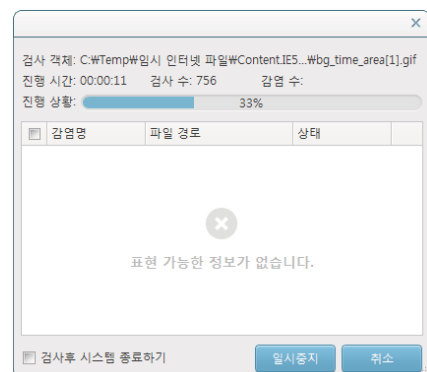
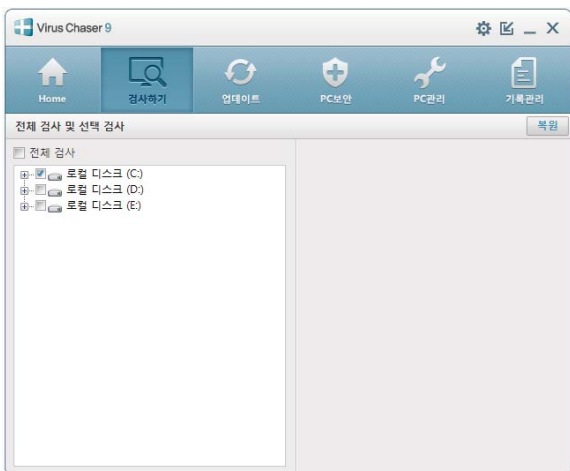
: 검사 후 시스템 종료하기 항목을 체크표시하고 “검사하기” 버튼을 클릭하면 검사를 마친 후에 시스템을 자동으로 종료합니다.

- **검사 창 분리하기**

: 검사화면의 상위 검사 창 분리영역을 클릭 후 마우스를 이동시키면 검사 창만 분리시킬 수 있습니다. 복원버튼 또는 검사창의 닫기 버튼을 클릭하면 원래 자리로 복원 됩니다. 분리된 상태에서는 가운데 사이즈 조절영역 클릭으로 폴더 선택창 크기를 조절 할 수 있습니다.

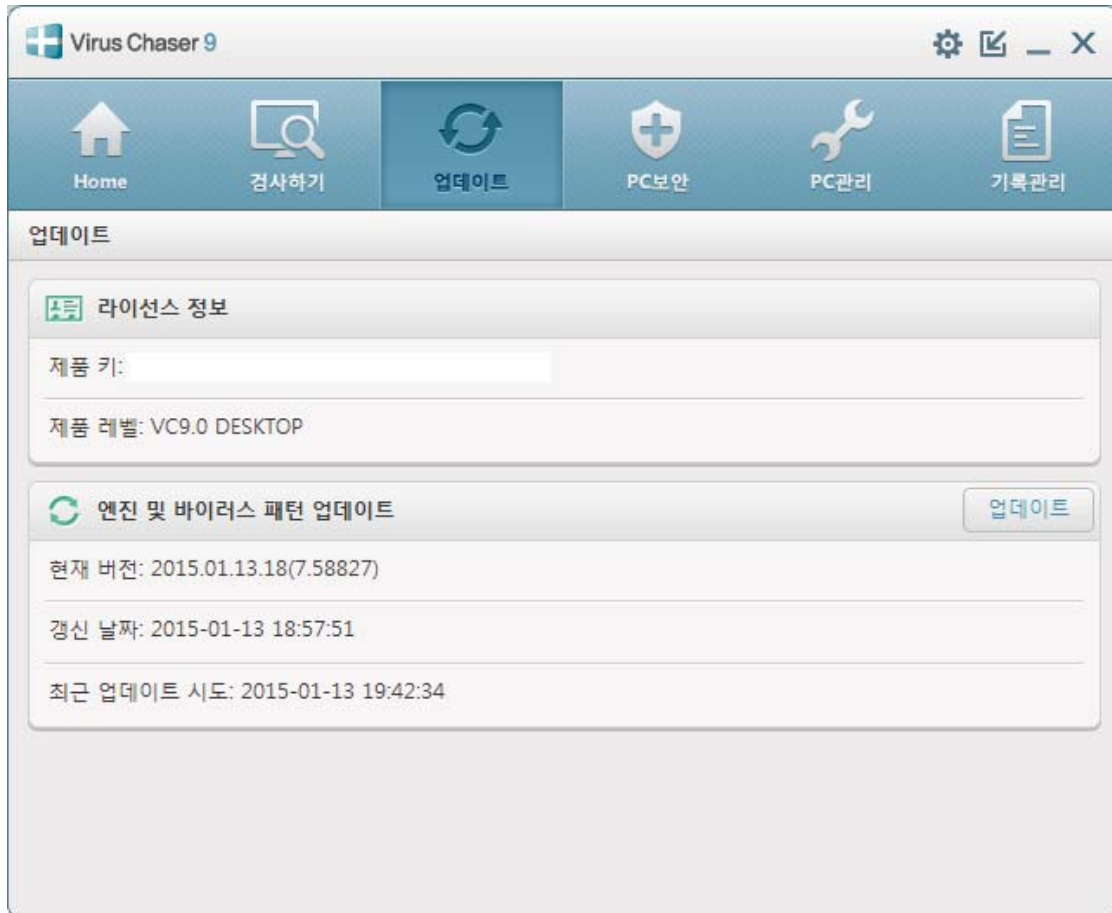


사이즈조절

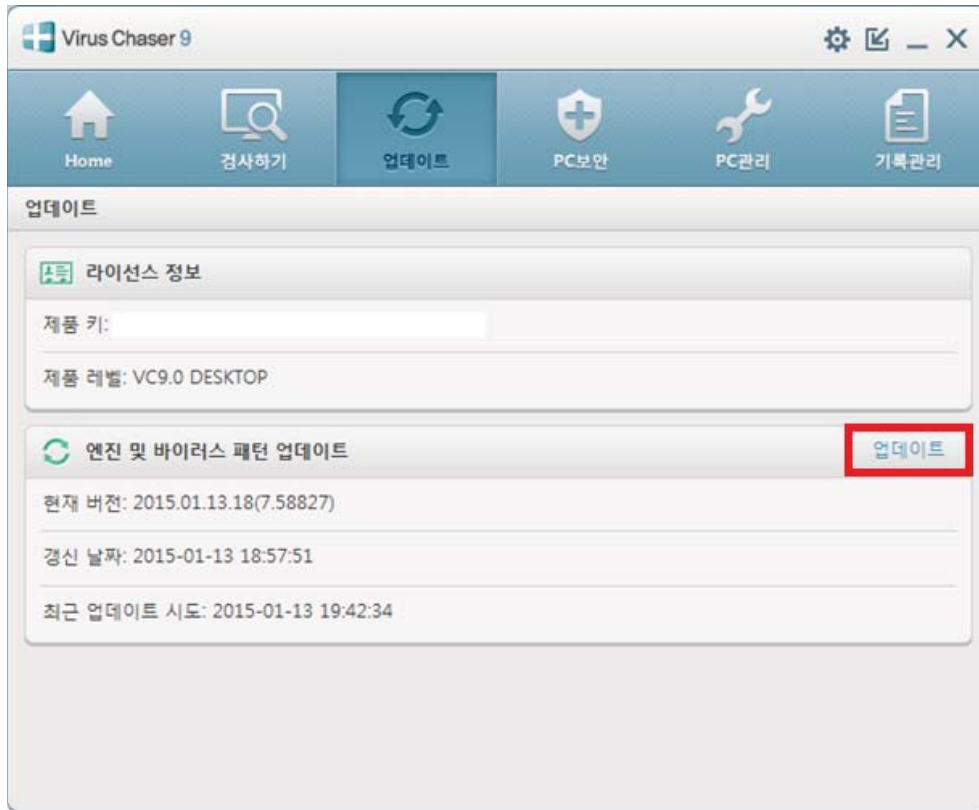


4.2.3. 업데이트

업데이트 메뉴는 라이선스 정보와 엔진 및 바이러스 패턴 업데이트를 할 수 있도록 구성되어 있습니다.

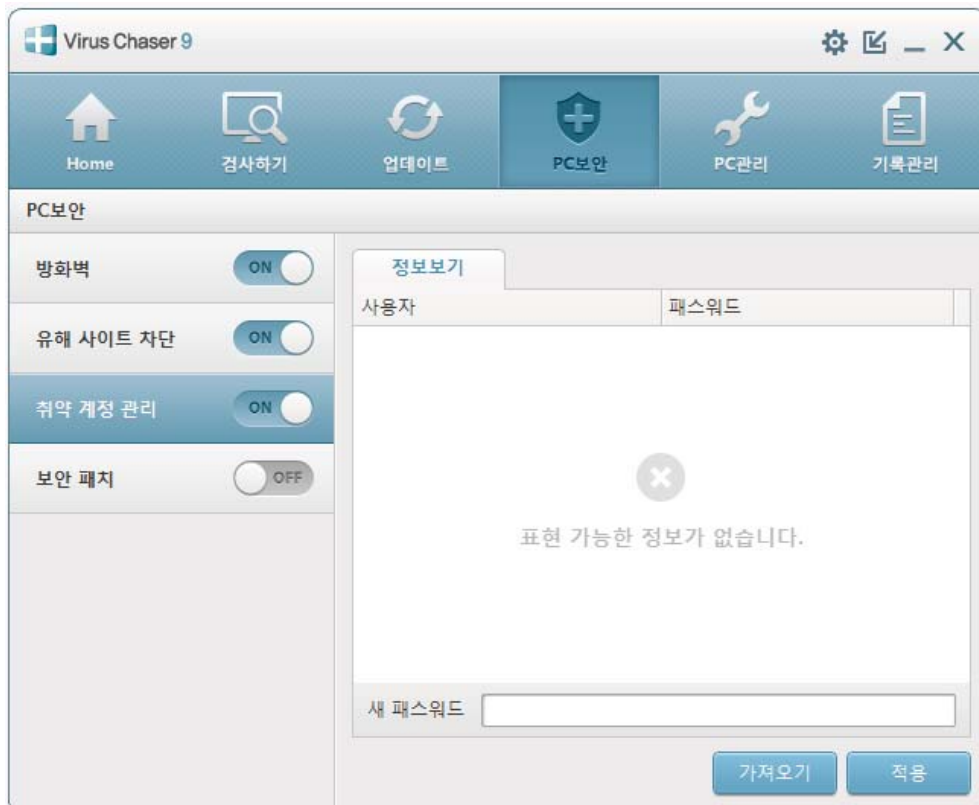


- 라이선스 정보**
 : 라이선스 정보는 설치를 실행할 때 입력한 제품 키와 제품 레벨을 나타냅니다.
- 엔진 및 바이러스 패턴 업데이트**
 : 엔진 및 바이러스 패턴 업데이트는 업데이트 서버로부터 최신 버전을 업데이트 할 수 있는 기능입니다. “업데이트” 버튼을 클릭하면 업데이트가 진행된 후 업데이트가 완료되면 현재 버전 및 최신 업데이트 날짜를 확인할 수 있습니다.



4.2.4. PC 보안

PC보안 메뉴는 PC보안에 해당하는 세부 항목인 취약 계정 관리, 보안 패치를 사용 또는 중지로 설정하여 사용자가 원하지 않는 보안 설정을 차단할 수 있도록 구성되어 있습니다.



• **방화벽**

: 네트워크 제어를 통해 방화벽 기능을 제공 합니다.

방화벽을 설정하려면 우측의 프로그램, IP주소 , 포트 항목을 클릭 합니다

프로그램은 등록 시 전체경로가 표시되며, IP주소 및 포트는 개별, 범위 등록이 가능합니다.

대상을 추가한 후 적용 버튼을 눌러 설정을 적용합니다. 정보보기 탭을 통해 전체 등록된 상태를 확인 합니다.

정보보기	프로그램	IP 주소	포트
차단 리스트			
C:\Util\ProcessMonitor\Procmon.exe			
C:\Util\depends22_x64\depends.exe			
211.211.211.1 ~ 211.211.211.5			
5550 ~ 5555			
211.39.138.113			

• **유해사이트 차단**

: URL을 등록하여 대상 URL의 접근을 차단 합니다.

유해사이트 차단 설정하려면 우측의 입력 창을 통하여 입력 후 ‘+’ 버튼을 클릭하여 추가 합니다. 이

미 등록된 URL을 삭제 하려면 ‘-’버튼을 클릭하여 제거 합니다. 대상을 추가한 후 적용 버튼을 눌러 설정을 적용합니다. 전체 등록된 상태를 확인합니다.

정보보기	
URL	상태
www.koreasex.com	유해사이트
www.XXXkorea.net	유해사이트

• **취약 계정 관리**

: “취약 계정 관리”에서는 사용자 계정의 취약성을 점검하여 사용자가 패스워드를 변경할 수 있도록 관리해주며 취약 계정 관리를 사용 또는 중지할 수 있도록 설정할 수 있는 기능입니다. 취약한 계정을 “가져오기” 버튼을 선택한 후 정보보기 목록에서 확인합니다.



취약한 패스워드를 가지고 있는 계정은 새 패스워드를 입력하여 패스워드를 변경한 후 “적용” 버튼을 클릭합니다.

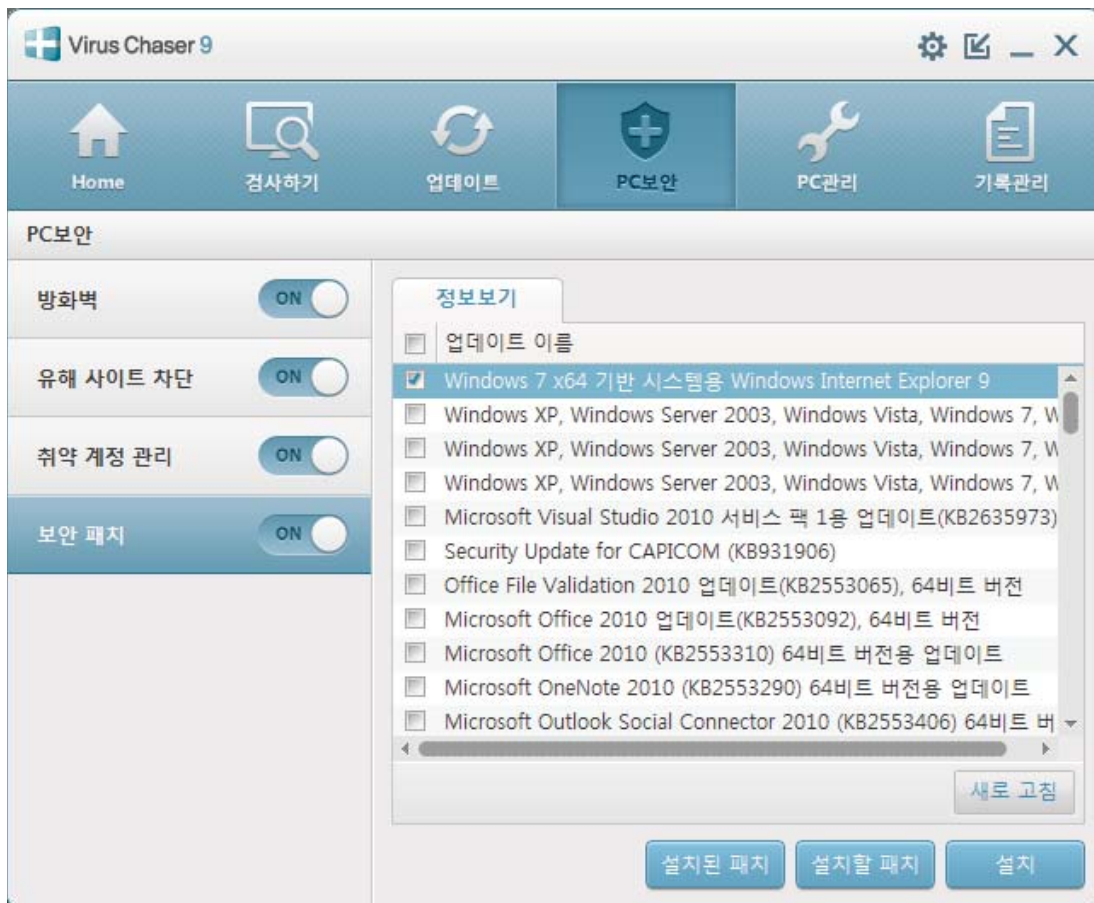


패스워드 변경이 완료 되었다면 패스워드 변경 완료 팝업 창이 나타나면 “확인” 버튼을 클릭 합니다.



• 보안 패치

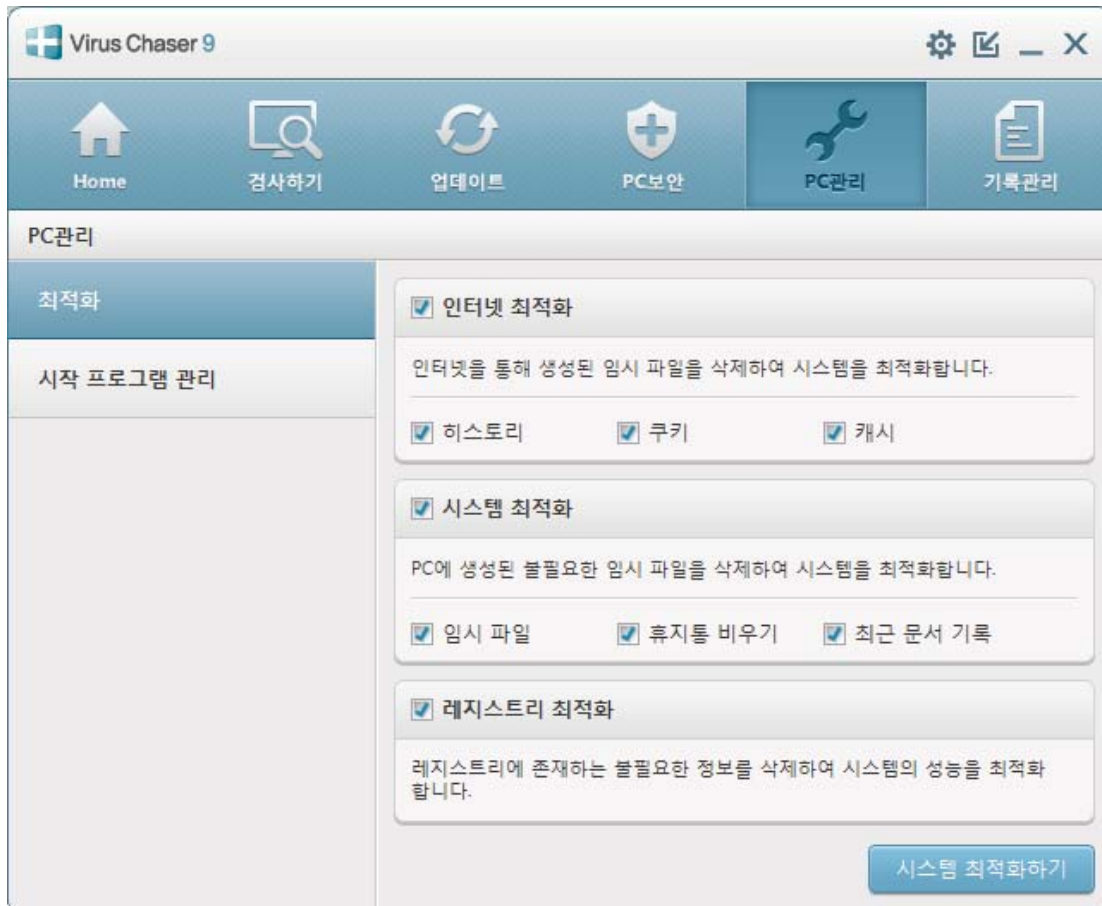
: 시스템 보안에 필요한 정보 업데이트를 통해 현재 시스템에 설치되어 있는 패치와 설치해야 할 패치를 조회하고 설치해야 할 패치를 사용자가 선택하여 바로 설치 할 수 있도록 하는 기능입니다.



- ① 설치된 패치
 - 설치된 패치 정보를 보기 위해서는 “설치된 패치를 클릭합니다.
- ② 설치할 패치
 - 설치할 패치 정보를 보기 위해서는 “설치할 패치를 클릭합니다.
 - “업데이트 목록을 불러오는 중입니다” 라는 메시지가 나오면서 설치할 패치 목록이 나타납니다.
 - 설치할 패치를 선택 후 “설치”버튼을 클릭하면 선택된 패치가 설치됩니다.

4.2.5. PC 관리

“PC관리” 메뉴는 최적화, 시작 프로그램 관리로 나누어져 있습니다. “최적화”는 시스템에 불필요한 임시 파일 및 인터넷을 통해 생성된 임시 파일과 레지스트리에 존재하는 불필요한 정보를 삭제하여 시스템을 최적화 시키는 기능을 제공합니다. “시작 프로그램 관리”는 시스템 시작 시 실행되는 프로그램들을 관리하여 보다 효율적으로 PC를 관리할 수 있는 기능을 가지고 있습니다.



- **최적화**

: “최적화”는 인터넷 최적화, 시스템 최적화, 레지스트리 최적화 3가지로 구분 됩니다.

- ① 인터넷 최적화
 - 인터넷에 생성된 임시 파일을 삭제하여 시스템을 최적화 합니다.
- ② 시스템 최적화
 - PC에 생성된 불필요한 임시 파일을 삭제하여 시스템을 최적화 합니다.
- ③ 레지스트리 최적화
 - 레지스트리에 존재하는 불필요한 정보를 삭제하여 시스템의 성능을 최적화 합니다.



• 시작 프로그램 관리

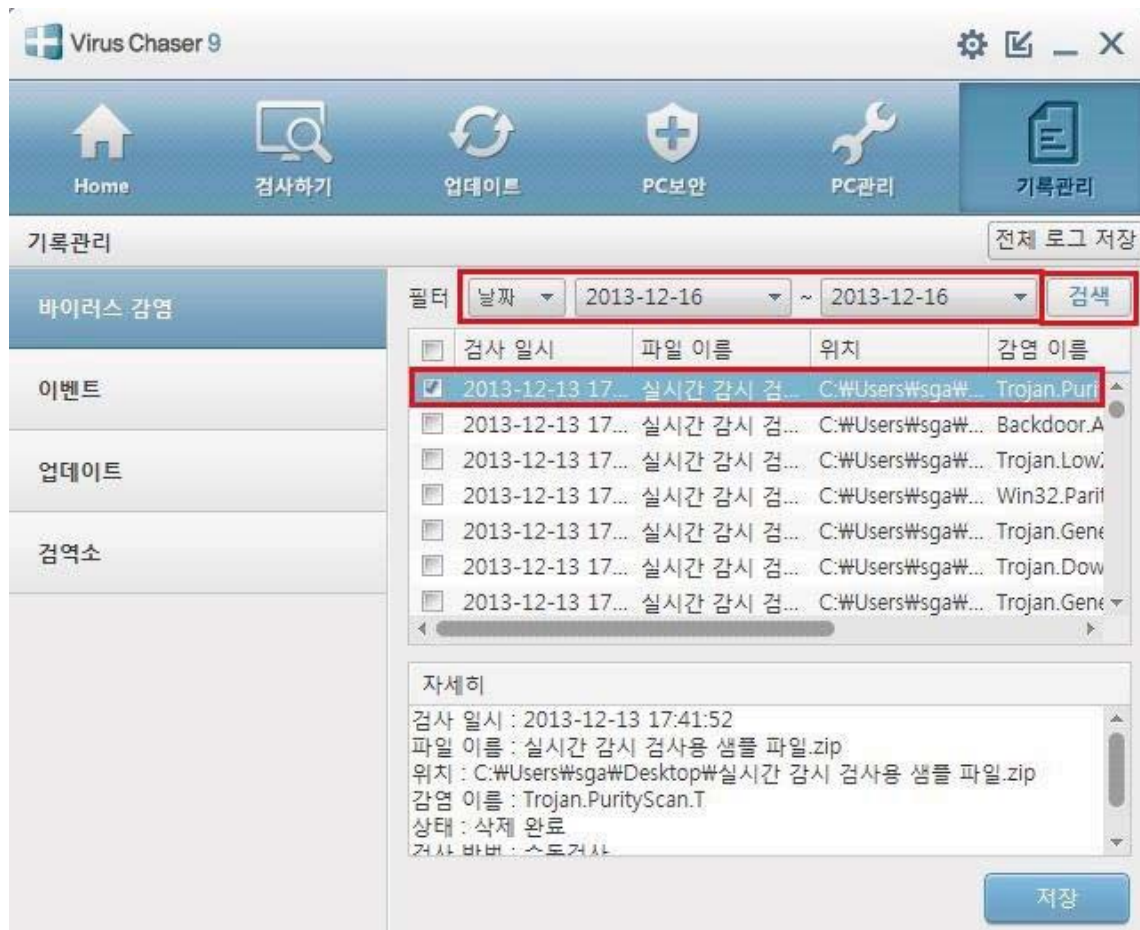
: “시작 프로그램 관리”는 시스템이 시작과 동시에 실행되는 프로그램들을 관리하는 항목으로 시스템 부팅 속도와 직접적인 영향을 미치므로 사용자가 사용할 시작 프로그램과 사용하지 않는 시작 프로그램들을 설정하여 효율적인 PC관리를 도와주는 기능을 가지고 있습니다.

- ① 모두 사용
 - 사용할 시작 프로그램이 전체라면 전체 항목을 선택하거나 “모두 사용”버튼을 클릭하고 “적용”버튼을 클릭합니다.
- ② 모두 사용 안함
 - 시작 프로그램을 모두 사용 안 할 경우는 전체 항목을 선택하거나 “모두 사용 안함”버튼을 클릭하고 “적용”버튼을 클릭합니다.
- ③ 새로 고침
 - 현재 적용된 시작 프로그램 관리 항목을 보기 위해서는 “새로 고침”버튼을 클릭하여 확인합니다.

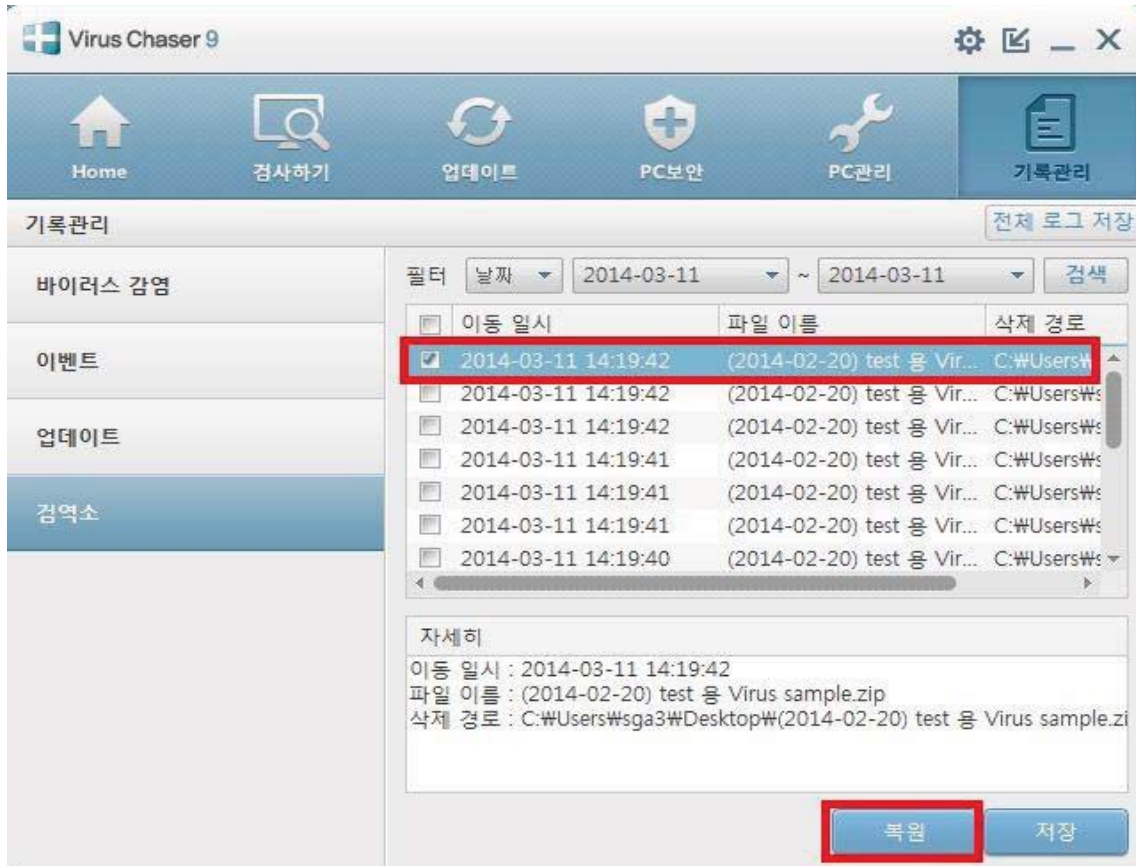


4.2.6. 기록관리

“기록관리” 메뉴는 바이러스 감염, 이벤트, 업데이트, 검역소 기록을 관리합니다.



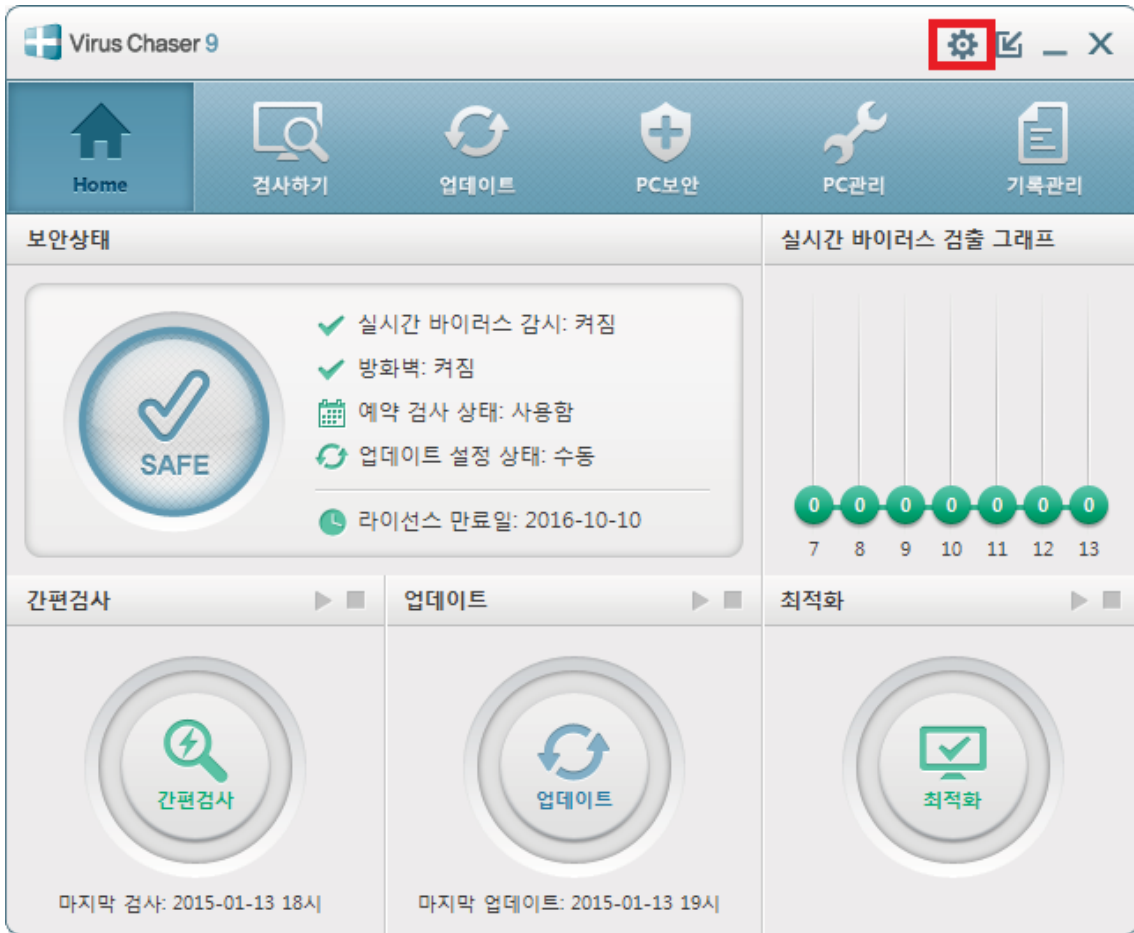
- ① 바이러스 감염
 - “바이러스 감염 날짜 검색”와 같이 조회할 날짜를 선택하거나, “바이러스 키워드 검색”과 같이 키워드를 선택하여 키워드를 입력한 후 “검색” 버튼을 클릭하여 자세히 보고 싶은 기록을 목록에서 선택합니다.
- ② 이벤트
 - 업데이트 실행, 바이러스 검사 시작/중지 등의 이벤트 발생에 대한 감사 기록을 조회하는 기능입니다.
- ③ 업데이트
 - “업데이트 날짜 검색 메뉴”와 같이 조회할 날짜를 선택하거나, “업데이트 키워드 검색 메뉴”와 같이 조회할 키워드를 입력한 후 “검색” 버튼을 클릭하여 자세히 보고 싶은 기록을 목록에서 선택합니다.
- ④ 검역소
 - “검역소 날짜 검색 메뉴”와 같이 조회할 날짜를 선택하거나 “검역소 키워드 검색 메뉴”와 같이 키워드를 입력한 후 “검색” 버튼을 클릭하여 자세히 보고 싶은 기록을 목록에서 선택합니다.
 - 검역소의 기록된 로그 기록을 복원하려면 해당 로그를 선택한 후 “복원” 버튼을 누릅니다.





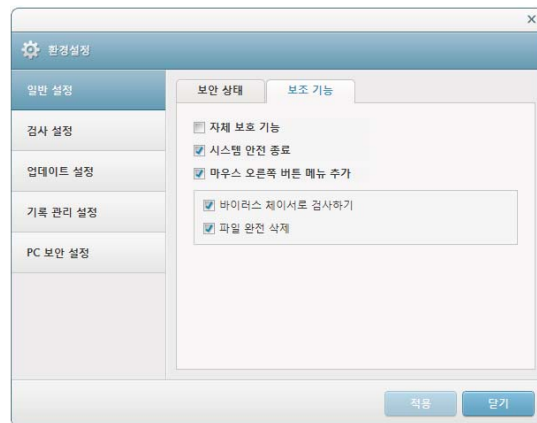
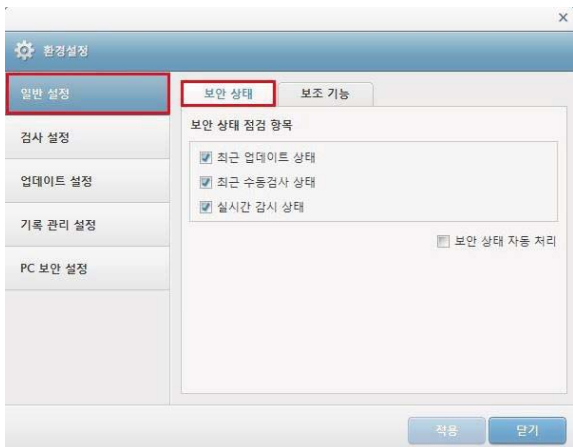
4.2.7. 환경 설정

“환경설정” 메뉴는 각 항목에 대한 세부 환경설정을 확인 및 설정할 수 있습니다.



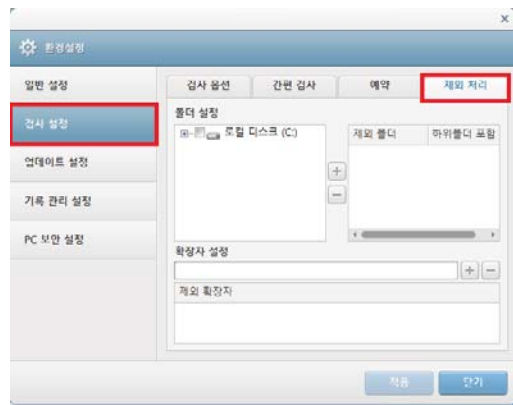
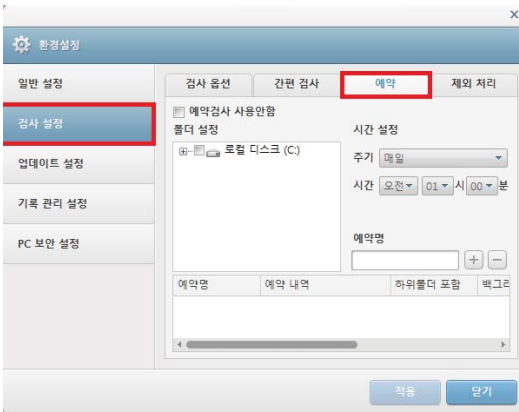
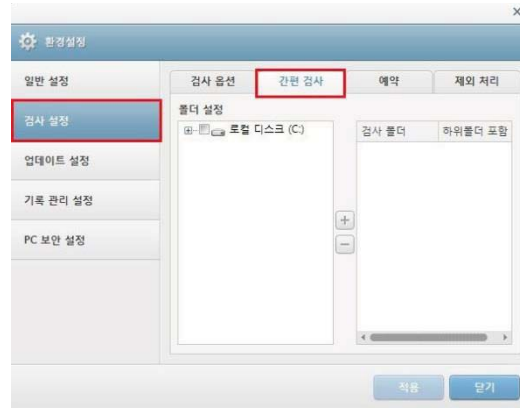
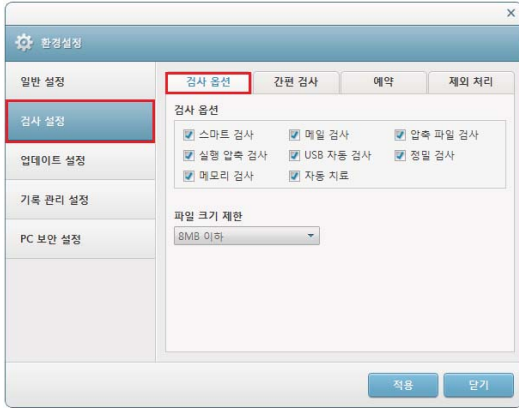
- **일반 설정**

: 일반 설정 항목은 점검할 항목 별 상태를 나타내주며 보안 상태와 자체 보호 기능 및 시스템 안전 종료 등의 설정을 다루는 보조 기능을 확인할 수 있습니다.



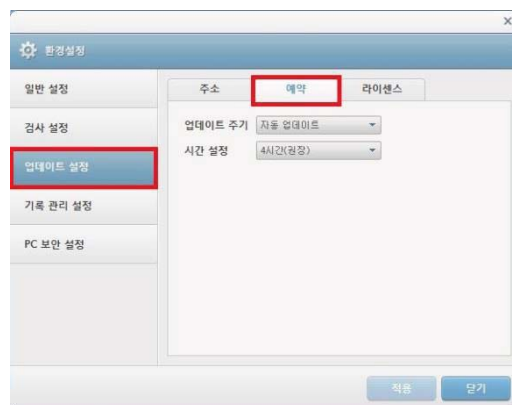
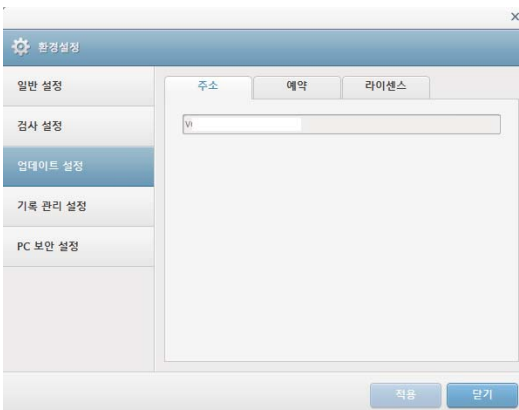
• 검사 설정

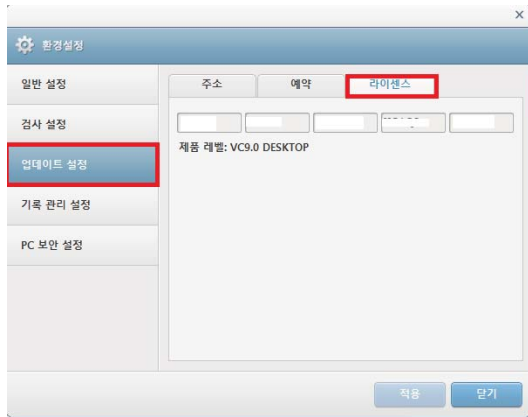
: 검사 설정은 검사할 대상을 확인하고, 날짜와 시간을 지정하여 예약 검사를 진행할 수 있는 설정과 제외하고자 하는 검사 대상을 확인할 수 있습니다.



• 업데이트 설정

: 업데이트 설정은 업데이트 서버 주소 설정과 업그레이드 주기 예약 설정, 프록시 설정 등 VC 모듈을 최신의 상태로 유지하기 위한 업데이트 환경을 설정을 확인할 수 있습니다.





• 기록 관리 설정

: 기록 관리 세부 항목 환경을 확인할 수 있고 기록 관리 목록에 나타나는 표시 정보들의 컬럼 설정을 확인할 수 있습니다.

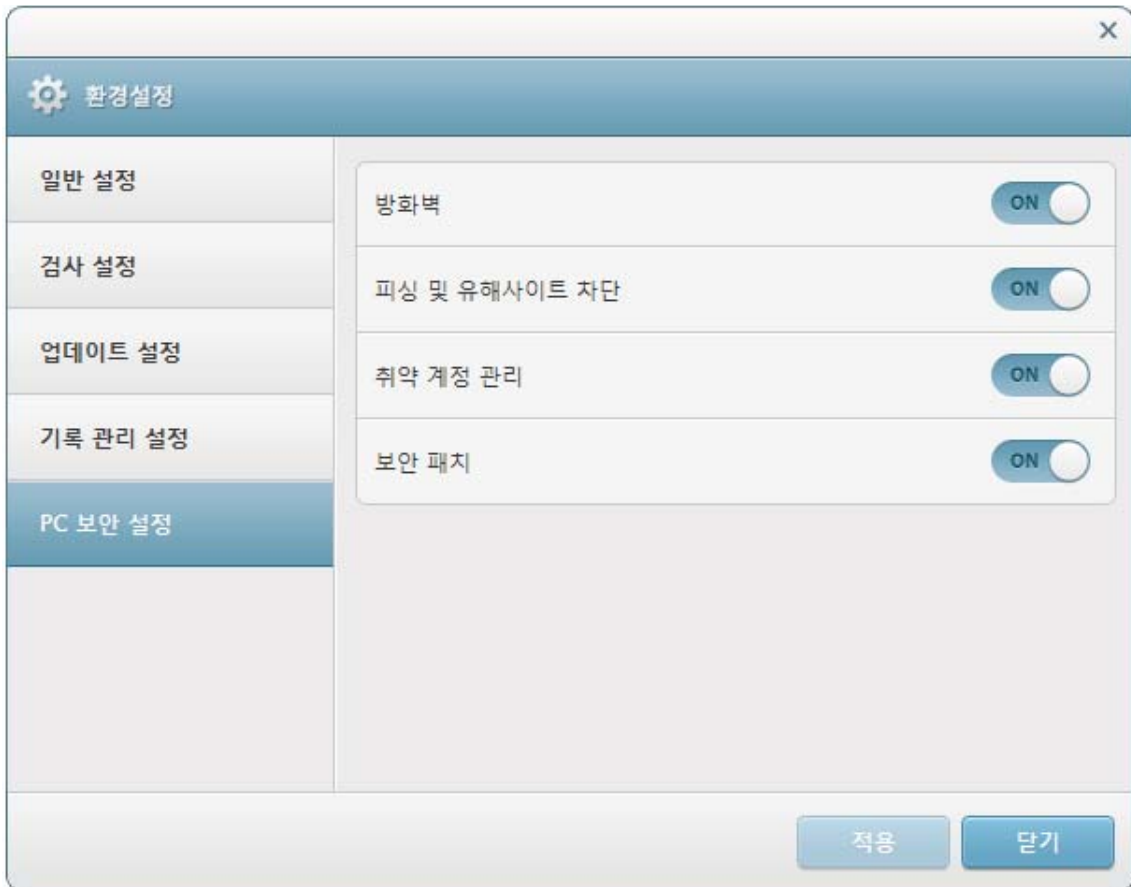


항목		내용
바이러스 감염 컬럼 설정	검사 일시	바이러스 검사를 실행한 일시
	파일 이름	바이러스로 진단된 파일의 이름.
	위치	바이러스로 진단된 파일의 경로
	감염 이름	감염된 파일의 이름
	상태	검사한 후 처리 상태를 의미. (삭제완료, 치료완료로 구분)
	검사 방법	수동검사, 자동검사, 예약검사 등의 바이러스 탐지 방법

이벤트 기록 컬럼 설정	기록 일시	이벤트 기록의 일시
	항목	이벤트 발생에 대한 감사 기록 항목을 의미
	내용	이벤트 발생 항목에 대한 처리 내용
업데이트 컬럼 설정	일시	업데이트가 실행된 일시
	내용	업데이트가 실행된 파일들의 내용을 의미
파일 저장소 컬럼 설정	이동 일시	검역소로 이동한 일시
	파일 이름	검역소로 이동한 파일의 명칭
	삭제 경로	검역소로 이동하기 전 파일의 경로를 의미

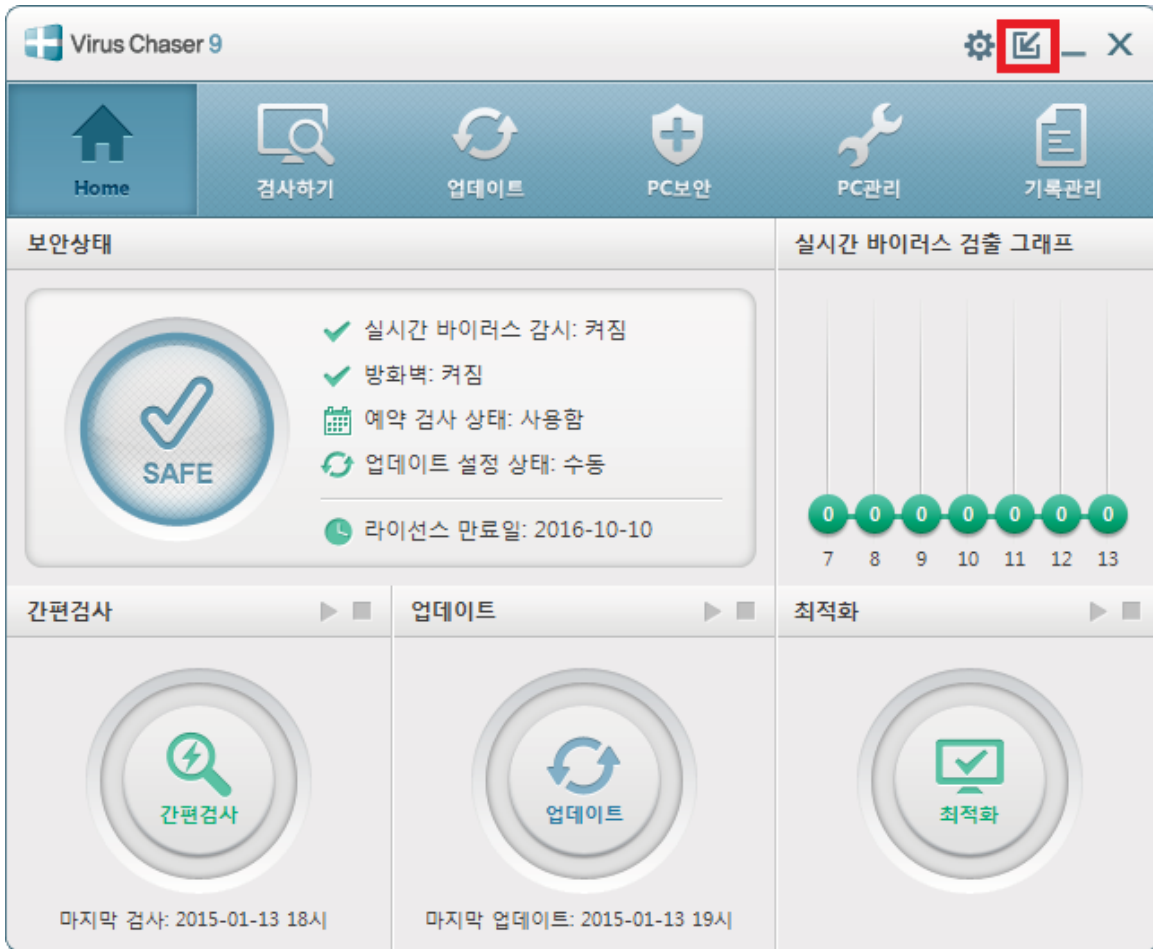
• PC 보안 설정

: 시스템의 보안을 설정하는 항목으로 취약 계정 관리, 보안패치의 작동 설정을 확인 할 수 있습니다.



4.2.8. 간편 메뉴 사용하기

“간편 메뉴” 설정을 통해 사용자가 사용하기 쉽게 구성 되었습니다.



- PC 보안 설정 : 메인 메뉴의 보안상태와 동일하게 동작합니다.
- 실시간 감시 : 메인 메뉴의 실시간 감시 ON/OFF와 동일하게 동작합니다.



- 업데이트 : 업데이트를 진행합니다.

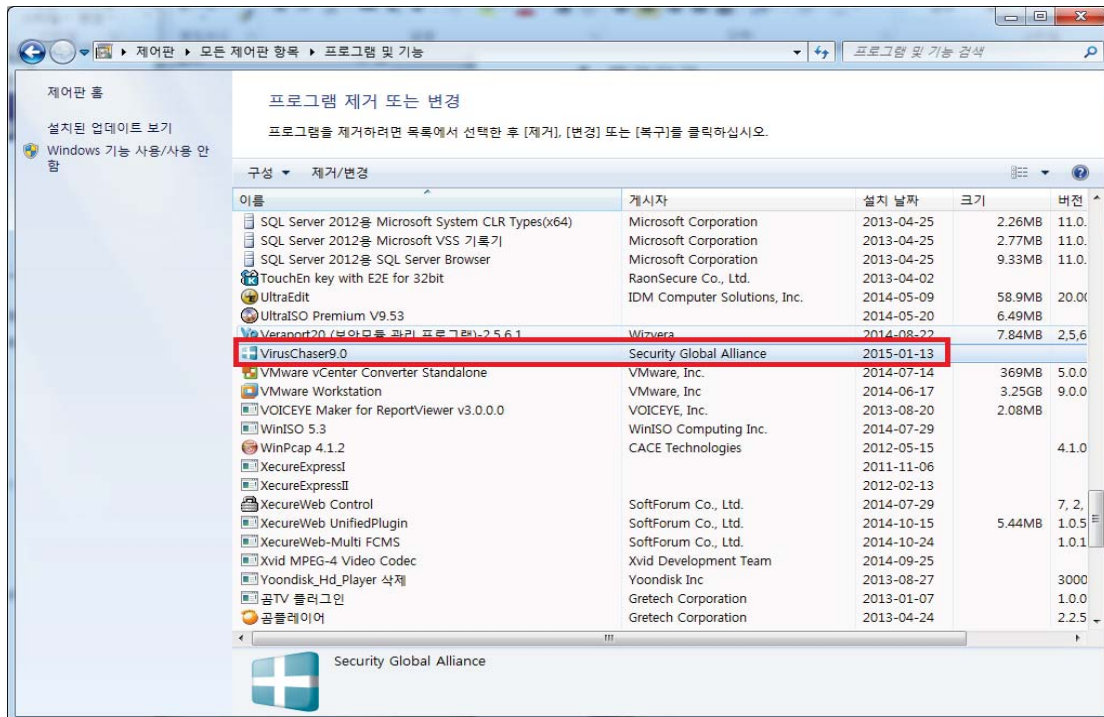


- 간편검사 : 간편검사를 진행합니다.

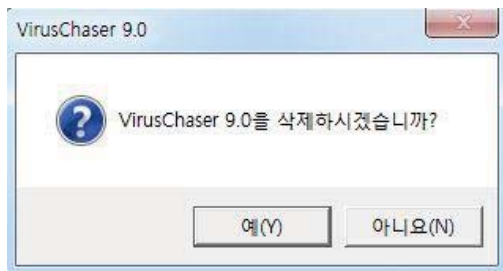


5. 제거

[제어판] → [프로그램 추가/제거]에서 VirusChaser 9.0 “제거/변경” 버튼을 클릭 합니다.



- **제거 패스워드 확인**
: 제거 확인 메시지가 나오면 “예”를 클릭한다.



6. 고객 지원

바이러스체이서 9.0 제품을 구매한 고객이 제품을 사용하는 도중 발생하는 프로그램 문제 및 제품에 대한 문의를 하실 수 있습니다.

문의하시기 전, 사용설명서와 홈페이지 고객센터에 있는FAQ/고객상담실을 이용하여 문의사항에 대한 내용이 있는지 확인하시기 바랍니다.

문의사항에 대한 내용을 찾지 못한 경우 고객 지원 센터에 연락하시기 바랍니다.

〈 고객 지원 센터 연락처 〉

- ◆ 홈페이지 : <http://www.viruschaser.com>
- ◆ 고객센터 : <http://www.viruschaser.com> 고객센터) FAQ (자주하는 질문)
<http://www.viruschaser.com> 고객센터)고객상담실 (1:1 메일상담)
- ◆ 이메일 : 영 업 문 의 - sales@sgacorp.kr
기 술 문 의 - cs@sgacorp.kr
바이러스문의 - cert@viruschaser.com
- ◆ 트위터 : @virus_chaser
- ◆ 주소 : 137-896 서울특별시 서초구 양재동 마방로 2 길 44(양재동 315-1)
2층 바이러스체이서 보안기술센터 담당자 앞.
- ◆ 대표전화 : 070-7308-9200

