TREND MICRO

XG

OfficeScan™

관리자 안내서

엔터프라이즈 및 중소기업용

Endpoint Security

Protected Cloud

Web Security

TREND MICRO SMART Protection Network™

Trend Micro Incorporated는 사전 예고 없이 이 문서와 이 문서에서 설명된 제품을 변경할 수 있는 권한을 보유합니다. 제품을 설치 및 사용하기 전에 다음 Trend Micro 웹 사이트에서 제공하는 추가 정보 파일, 릴리스 정보 및 최신 버전의 해당 사용 설명서를 확인하십시오.

http://docs.trendmicro.com/ko-kr/enterprise/officescan.aspx

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Control Manager, Damage Cleanup Services, eManager, InterScan, Network VirusWall, ScanMail, ServerProtect, and TrendLabs는 Trend Micro Incorporated의 상표 또는 등록 상표입니다. 기타 모든 제품 또는 회사 이름은 해당 소유권자의 상표 또는 등록 상표일 수 있습니다.

Copyright © 2016. Trend Micro Incorporated. All rights reserved.

문서 항목 번호: OSKMXG7603/161028

릴리스 날짜: 2016년 10월

미국 특허 번호: 5,951,698

이 문서에서는 제품의 기본 기능을 소개하고 작업 환경에 대한 설치 지침을 제공합니다. 제품을 설치하거나 사용하기 전에 설명서 내용을 숙지하십시오.

제품의 특정 기능을 사용하는 방법에 대한 자세한 내용은 Trend Micro 온라인 도움말 센터나 Trend Micro 기술 자료를 참조하십시오.

Trend Micro에서는 설명서의 내용을 개선하기 위해 지속적인 노력을 기울이고 있습니다. 이 문서나 기타 Trend Micro 문서에 대한 질문, 의견 또는 제안이 있으면 docs@trendmicro.com으로 문의하십시오.

다음 사이트에서 이 문서를 평가해 주십시오.

http://www.trendmicro.com/download/documentation/rating.asp

목차

서문

서문 xi

OfficeScan 설명서 xii

대상 xii

문서 규칙 xiii

용어 xiv

부 I : 소개 및 시작하기

장 1 : OfficeScan 소개

OfficeScan 정보 1-2

OfficeScan XG의 새로운 기능 1-2

주요 기능 및 장점 1-5

OfficeScan 서버 1-7

OfficeScan 에이전트 1-9

Trend Micro 제품 및 서비스와의 통합 1-9

장 2 : OfficeScan 시작

웹 콘솔 2-2

대시보드 2-5

서버 마이그레이션 도구 2-36

Active Directory 통합 2-40

OfficeScan 에이전트 트리 2-44

OfficeScan 도메인 2-57

장 3 : 데이터 보호 시작

데이터 보호 설치 3-2
데이터 보호 라이선스 3-4
OfficeScan 에이전트에 데이터 보호 배포 3-6
Forensic 폴더 및 DLP 데이터베이스 3-8
데이터 보호 제거 3-14

부 II : OfficeScan 에이전트 보호

장 4 : Trend Micro 스마트 보호 사용

Trend Micro 스마트 보호 정보 4-2
스마트 보호 서비스 4-3
스마트 보호 소스 4-5
스마트 보호 패턴 파일 4-7
스마트 보호 서비스 설정 4-12
스마트 보호 서비스 사용 4-30

장 5 : OfficeScan 에이전트 설치

OfficeScan 에이전트 새로 설치 5-2
설치 고려 사항 5-2
배포 고려 사항 5-11
OfficeScan 에이전트로 마이그레이션 5-63
사후 설치 5-67
OfficeScan 에이전트 제거 5-70

장 6 : 보호 기능을 최신으로 유지

OfficeScan 구성 요소 및 프로그램 6-2
업데이트 개요 6-11

OfficeScan 서버 업데이트 6-14
통합 스마트 보호 서버 업데이트 6-26
OfficeScan 에이전트 업데이트 6-26
업데이트 에이전트 6-51
구성 요소 업데이트 요약 6-60

장 7 : 보안 위험 검색

보안 위험 정보 7-2
검색 방법 유형 7-8
검색 유형 7-14
모든 검색 유형에 대한 일반적인 설정 7-26
검색 권한 및 기타 설정 7-53
글로벌 검색 설정 7-69
보안 위험 알림 7-79
보안 위험 로그 7-88
보안 위험 비상 발생 7-103

장 8 : 알 수 없는 위협으로부터 보호

머신러닝 8-2
의심스러운 연결 서비스 8-5
샘플 제출 8-8
알 수 없는 위협 로그 8-10

장 9 : 동작 모니터링 사용

동작 모니터링 9-2
글로벌 동작 모니터링 설정 구성 9-12
동작 모니터링 권한 9-14
OfficeScan 에이전트 사용자에 대한 동작 모니터링 알림 9-15

동작 모니터링 로그 9-17

장 10 : 장치 제어 사용

장치 제어 10-2
저장 장치에 대한 권한 10-4
비저장 장치에 대한 권한 10-10
외부 장치에 대한 액세스 관리(데이터 보호가 활성화된 경우) 10-11
외부 장치에 대한 액세스 관리(데이터 보호가 활성화되지 않은 경우) 10-15
장치 제어 알림 수정 10-18
장치 제어 로그 10-18

장 11 : 데이터 손실 방지 사용

DLP(데이터 손실 방지) 정보 11-2
데이터 손실 방지 정책 11-3
데이터 식별자 유형 11-5
데이터 손실 방지 템플릿 11-19
DLP 채널 11-23
데이터 손실 방지 조치 11-38
데이터 손실 방지 예외 11-40
데이터 손실 방지 정책 구성 11-45
데이터 손실 방지 알림 11-51
데이터 손실 방지 로그 11-55

장 12 : 웹 검증 사용

웹 위협 정보 12-2
C&C(명령 및 제어) 연결 알림 서비스 12-2
웹 검증 12-4

웹 검증 정책 12-5
에이전트 사용자에 대한 웹 위협 알림 12-13
관리자에 대한 C&C 콜백 알림 12-14
에이전트 사용자에 대한 C&C 연결 알림 서비스 12-17
C&C 콜백 비상 발생 12-18
웹 위협 로그 12-20

장 13 : OfficeScan 방화벽 사용

OfficeScan 방화벽 정보 13-2
OfficeScan 방화벽 설정 또는 해제 13-6
방화벽 정책 및 프로필 13-8
방화벽 권한 13-22
글로벌 방화벽 설정 13-24
OfficeScan 에이전트 사용자에 대한 방화벽 위반 알림 13-26
방화벽 로그 13-28
방화벽 위반 비상 발생 13-29
OfficeScan 방화벽 테스트 13-31

부 III : OfficeScan 서버 및 에이전트 관리

장 14 : OfficeScan 서버 관리

역할 기반 관리 14-3
Trend Micro Control Manager 14-23
의심스러운 개체 목록 설정 14-31
참조 서버 14-33
관리자 알림 설정 14-35
시스템 이벤트 로그 14-37

로그 관리 14-39
라이선스 14-42
OfficeScan 데이터베이스 백업 14-45
SQL Server 마이그레이션 도구 14-47
OfficeScan Web Server/에이전트 연결 설정 14-52
서버-에이전트 통신 14-52
웹 콘솔 암호 14-58
웹 콘솔 설정 14-58
격리 보관 관리자 14-59
서버 튜너 14-60
Smart Feedback 14-63

장 15 : OfficeScan 에이전트 관리

엔드포인트 위치 15-2
OfficeScan 에이전트 프로그램 관리 15-6
에이전트-서버 연결 15-26
OfficeScan 에이전트 프록시 설정 15-47
OfficeScan 에이전트 정보 보기 15-52
에이전트 설정 가져오기 및 내보내기 15-53
보안 준수 15-55
Trend Micro 가상 데스크톱 지원 15-73
글로벌 에이전트 설정 15-86
에이전트 권한 및 기타 설정 구성 15-88

부 IV : 추가 보호 제공

장 16 : 외부 에이전트 보호

Edge 릴레이 서버 16-2

Edge 릴레이 서버 시스템 요구 사항 16-3
Edge 릴레이 서버 설치 16-4
Edge 릴레이 서버에 연결 16-13
Edge 릴레이 서버 연결 관리 16-14
Edge 릴레이 서버 인증서 관리 16-15

장 17 : Plug-in Manager 사용

Plug-in Manager 정보 17-2
Plug-in Manager 설치 17-3
기본 OfficeScan 기능 관리 17-4
Plug-in 프로그램 관리 17-4
Plug-in Manager 제거 17-12
Plug-in Manager 문제 해결 17-12

장 18 : 문제 해결 리소스

지원 정보 시스템 18-2
Case Diagnostic Tool 18-2
Trend Micro 성능 조정 도구 18-2
OfficeScan 서버 로그 18-2
OfficeScan 에이전트 로그 18-14

장 19 : 기술 지원

문제 해결 리소스 19-2
Trend Micro 연락처 19-3
의심스러운 콘텐츠를 Trend Micro로 보내기 19-4
기타 리소스 19-5

부록

부록 A: OfficeScan의 IPv6 지원

OfficeScan 서버 및 에이전트에 대한 IPv6 지원 A-2
IPv6 주소 구성 A-5
IP 주소가 표시되는 화면 A-6

부록 B: Windows Server Core 지원

Windows Server Core 지원 B-2
Windows Server Core 설치 방법 B-2
Windows Server Core의 OfficeScan 에이전트 기능 B-6
Windows Server Core 명령 B-7

부록 C: Windows 8/8.1/10 및 Windows Server 2012/2016 지원

Windows 8/8.1/10 및 Windows Server 2012/2016 정보 C-2
UI 모드의 OfficeScan 기능 지원 C-4
Internet Explorer 10/11 및 Microsoft Edge C-5

부록 D: OfficeScan 롤백

서버 백업 패키지를 사용하여 OfficeScan 서버 및 OfficeScan 에이전트 롤백 D-2

부록 E: 용어집

액티브업데이트 E-2
압축 파일 E-2
Cookie E-2
서비스 거부(DoS) 공격 E-2
DHCP E-2
DNS E-3
도메인 이름 E-3

동적 IP 주소 E-3
ESMTP E-4
최종 사용자 사용권 계약 E-4
잘못된 판정 E-4
FTP E-4
GeneriClean E-4
핫픽스 E-5
HTTP E-5
HTTPS E-5
ICMP E-6
IntelliScan E-6
IntelliTrap E-6
IP E-7
Java 파일 E-7
LDAP E-7
수신 포트 E-8
MCP 에이전트 E-8
혼합된 형태의 위협 공격 E-8
NAT E-8
NetBIOS E-9
단방향 통신 E-9
패치 E-9
피싱 공격 E-9
Ping E-10
POP3 ..... E-10
프록시 서버 E-10
RPC E-11

보안 패치 E-11
Service Pack E-11
SMTP E-11
SNMP E-11
SNMP 트랩 E-12
SSL E-12
SSL 인증서 E-12
TCP E-12
Telnet E-12
트로이 목마 포트 E-13
트러스트된 포트 E-14
양방향 통신 E-15
UDP E-15
치료할 수 없는 파일 E-15

색인

색인 IN-1

서문

서문

이 문서에서는 시작 정보, 에이전트 설치 절차 및 OfficeScan 서버 및 에이전트 관리에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- OfficeScan 설명서 페이지 xii
- 대상 페이지 xii
- 문서 규칙 페이지 xiii
- 용어 페이지 xiv

OfficeScan 설명서

OfficeScan 설명서는 다음을 포함합니다.

표 1. OfficeScan 설명서

설명서	설명
설치 및 업그레이드 안내서	OfficeScan 서버를 설치하고 서버 및 에이전트를 업그레이드하는 데 필요한 사항과 절차를 설명하는 PDF 문서입니다.
시스템 요구 사항	OfficeScan 서버를 설치하고 서버 및 에이전트를 업그레이드하기 위한 최소 및 권장 시스템 요구 사항을 간략하게 설명하는 PDF 문서입니다.
관리자 안내서	시작에 필요한 정보, OfficeScan 에이전트 설치 절차, OfficeScan 서버 및 에이전트 관리 방법에 대해 설명하는 PDF 문서입니다.
도움말	"방법", 권장 사용법 및 실제 사용 관련 정보를 제공하는 WebHelp 또는 CHM 포맷으로 컴파일된 HTML 파일입니다. 도움말은 OfficeScan 서버 및 에이전트 콘솔 그리고 OfficeScan 마스터 설치 프로그램에서 액세스할 수 있습니다.
추가 정보 파일	알려진 문제 목록과 기본 설치 단계에 대한 설명이 있습니다. 도움말이나 인쇄된 설명서에 없는 최신 제품 정보가 포함되어 있을 수도 있습니다.
기술 자료	문제 해결 정보의 온라인 데이터베이스입니다. 알려진 제품 문제에 대한 최신 정보를 제공합니다. 기술 자료에 액세스하려면 다음 웹 사이트로 이동합니다. http://esupport.trendmicro.com

최신 버전 PDF 문서 및 추가 정보를 다음 위치에서 다운로드합니다.

http://docs.trendmicro.com/ko-kr/enterprise/officescan.aspx

대상

OfficeScan 설명서는 다음과 같은 사용자를 위해 제작되었습니다.

- OfficeScan 관리자: OfficeScan 서버와 OfficeScan 에이전트의 설치 및 관리를 포함하여 OfficeScan 관리를 담당합니다. 이러한 사용자들은 고급 네트워킹 및 서버 관리 지식을 가지고 있는 것으로 간주됩니다.
- 최종 사용자: OfficeScan 에이전트를 엔드포인트에 설치한 사용자입니다. 이러한 사용자의 엔드포인트 사용 능력 수준은 초보자에서 고급 사용자까지 다양합니다.

문서 규칙

설명서에는 다음과 같은 규칙이 사용됩니다.

표 2. 문서 규칙

규칙	설명
대문자	머리글자어, 약어, 특정 명령 및 키보드의 키 이름
굵은꼴	메뉴 및 메뉴 명령, 명령 단추, 탭 및 옵션
기울임꼴	다른 문서에 대한 참조
고정 폭	샘플 명령줄, 프로그램 코드, 웹 URL, 파일 이름 및 프로그램 출력
이동 > **경로**	특정 화면으로 이동하기 위한 탐색 경로 예를 들어 **파일** > **저장**은 인터페이스에서 **파일**을 클릭한 다음 **저장**을 클릭함을 의미
참고	구성 참고 정보
팁	권장 사항 또는 의견
중요	필수 또는 기본 구성 설정 및 제품 제한 사항에 대한 정보

규칙	설명
경고!	중요한 조치 및 구성 옵션

용어

다음 표는 OfficeScan 설명서 전체에서 사용되는 공식적인 용어를 알려줍니다.

표 3. OfficeScan 용어

용어	설명
OfficeScan 에이전트	OfficeScan 에이전트 프로그램
에이전트 엔드포인트	OfficeScan 에이전트가 설치된 엔드포인트
에이전트 사용자(또는 사용자)	에이전트 엔드포인트에서 OfficeScan 에이전트를 관리하는 사람
서버	OfficeScan 서버 프로그램
서버 컴퓨터	OfficeScan 서버가 설치된 엔드포인트
관리자(또는 OfficeScan 관리자)	OfficeScan 서버를 관리하는 사람
콘솔	OfficeScan 서버 및 에이전트 설정을 구성 및 관리하는 사용자 인터페이스 OfficeScan 서버 프로그램의 콘솔은 "웹 콘솔"이라고 하고, OfficeScan 에이전트 프로그램의 콘솔은 "에이전트 콘솔"이라고 합니다.
보안 위험	바이러스/악성 프로그램, 스파이웨어/그레이웨어 및 웹 위협을 통칭하는 용어
라이선스 서비스	바이러스 백신, Damage Cleanup Services 및 웹 검증과 Anti-spyware 포함(모두 OfficeScan 서버 설치 중에 활성화됨)

용어	설명
OfficeScan 서비스	MMC(Microsoft Management Console)를 통해 호스팅되는 서비스입니다. 예: OfficeScan Master Service(ofcservice.exe)
프로그램	OfficeScan 에이전트 및 Plug-in Manager가 포함됩니다.
구성 요소	보안 위험을 검색, 발견하고 조치를 취합니다.
에이전트 설치 폴더	엔드포인트에서 OfficeScan 에이전트 파일이 포함된 폴더입니다. 설치 도중 기본 설정을 허용하면 설치 폴더 위치는 다음 중 하나가 됩니다. C:₩Program Files₩Trend Micro₩OfficeScan Client C:₩Program Files (x86)₩Trend Micro₩OfficeScan Client
서버 설치 폴더	엔드포인트에서 OfficeScan 서버 파일이 포함된 폴더입니다. 설치 도중 기본 설정을 허용하면 설치 폴더 위치는 다음 중 하나가 됩니다. C:₩Program Files₩Trend Micro₩OfficeScan C:₩Program Files (x86)₩Trend Micro₩OfficeScan 예를 들어, 특정 파일이 서버 설치 폴더의 ₩PCCSRV에 있는 경우 파일의 전체 경로는 다음과 같습니다. C:₩Program Files₩Trend Micro₩OfficeScan₩PCCSRV ₩<file_name>.
스마트 스캔 에이전트	스마트 스캔을 사용하도록 구성된 OfficeScan 에이전트
표준 스캔 에이전트	표준 스캔을 사용하도록 구성된 OfficeScan 에이전트
이중 스택	IPv4와 IPv6 주소를 모두 사용하는 엔터티 예: • IPv4와 IPv6 주소를 모두 사용하는 엔드포인트 • 이중 스택 OfficeScan 에이전트에 설치된 엔드포인트 • 에이전트에 업데이트를 배포하는 업데이트 에이전트 • 이중 스택 프록시 서버(예: DeleGate). IPv4 주소와 IPv6 주소 간에 변환할 수 있습니다.

용어	설명
순수 IPv4	IPv4 주소만 사용하는 엔터티
순수 IPv6	IPv6 주소만 사용하는 엔터티
플러그인 솔루션	원래 OfficeScan 기능 및 Plug-in Manager를 통해 제공되는 Plug-in 프로그램

부 I

소개 및 시작하기

장 1

OfficeScan 소개

이 장에서는 Trend Micro™ OfficeScan™을 소개하고 해당 특성 및 기능에 대해 간략하게 설명합니다.

다음과 같은 항목이 포함됩니다.

- OfficeScan 정보 페이지 1-2
- OfficeScan XG의 새로운 기능 페이지 1-2
- 주요 기능 및 장점 페이지 1-5
- OfficeScan 서버 페이지 1-7
- OfficeScan 에이전트 페이지 1-9
- Trend Micro 제품 및 서비스와의 통합 페이지 1-9

OfficeScan 정보

Trend Micro™ OfficeScan™은 악성 프로그램, 네트워크 바이러스, 웹 기반 위협, 스파이웨어 및 혼합된 위협 공격으로부터 회사 네트워크를 보호합니다. 통합된 솔루션인 OfficeScan은 엔드포인트에 있는 OfficeScan 에이전트 프로그램과 모든 에이전트를 관리하는 서버 프로그램으로 구성되어 있습니다. OfficeScan 에이전트는 엔드포인트를 보호하고 해당 보안 상태를 서버에 보고합니다. 서버는 웹 기반 관리 콘솔을 통해 손쉽게 조정된 보안 정책을 설정하고 모든 에이전트에 업데이트를 배포합니다.

OfficeScan은 기존의 방식보다 보안이 더욱 강화된 차세대 클라우드-클라이언트 인프라, Trend Micro 스마트 보호 네트워크(SPN)™를 통해 작동합니다. 독특한 in-the-cloud 기술과 더 가벼운 에이전트를 통해 기존 패턴 다운로드에 대한 의존성을 줄이고 데스크톱 업데이트 시 일반적으로 나타나는 지연 현상을 없앨 수 있습니다. 기업에서는 네트워크 대역폭이 증가하고, 이전에 비해 처리 능력이 조금만 필요하게 되어 이에 따라 비용 절감 효과를 얻을 수 있습니다. 사용자들은 회사 네트워크 내에서 또는 집에서 연결하건 이동 중에 연결하건 관계없이 연결할 때마다 최신 보호 기능에 즉시 액세스할 수 있습니다.

OfficeScan XG의 새로운 기능

이 OfficeScan 버전에 포함된 새로운 기능 및 개선 사항은 다음과 같습니다.

기능	설명
랜섬웨어 행위 차단 강화	랜섬웨어 공격에 대한 보호가 더욱 개선되어 이제 OfficeScan 에이전트가 랜섬웨어 위협에 의해 암호화된 파일을 복구하고, 랜섬웨어와 연관된 프로세스를 차단하고, 손상된 실행 파일이 네트워크를 감염시키지 않도록 방지합니다. 자세한 내용은 랜섬웨어 보호 페이지 9-3를 참조하십시오.

기능	설명
새로 발견된 프로그램 보호 개선 사항	개별 에이전트에 대한 랜섬웨어 보호 보안 정책을 보다 쉽게 극대화하기 위해 새로 발견된 프로그램 탐지 기능이 동작 모니터링 설정 화면으로 이동했습니다. 자세한 내용은 새로 발견된 프로그램 보호 페이지 9-5를 참조하십시오. 사용자가 새로 발견된 프로그램을 다운로드 및 실행한 후에 에이전트 엔드포인트에 표시되는 메시지를 사용자 정의할 수도 있습니다. 자세한 내용은 알림 메시지 내용 수정 페이지 9-16를 참조하십시오.
머신러닝	머신러닝 엔진은 고급 파일 특성 분석 및 휴리스틱 프로세스 모니터링을 통해 새로운 위협, 이전에 식별되지 않았던 위협 또는 알 수 없는 위협으로부터 네트워크를 보호할 수 있습니다. 머신러닝은 파일 또는 프로세스에 위협이 존재할 가능성 및 가능한 위협 유형을 확인할 수 있으므로 제로 데이 공격으로부터 보호할 수 있습니다.
OfficeScan Edge 릴레이 서버	OfficeScan Edge 릴레이 서버는 다음과 같은 기능을 제공하여 로컬 인트라넷에서 나가는 엔드포인트에 대한 더 높은 가시성과 개선된 보호를 제공합니다. • 의심스러운 개체 목록 동기화 • 샘플 제출 • 로그 제출 • 에이전트 상태 정보 제출(예: 현재 패턴 및 구성 요소 버전) 자세한 내용은 Edge 릴레이 서버 페이지 16-2를 참조하십시오.
의심스러운 파일 샘플 제출	이제 OfficeScan 에이전트는 Deep Discovery Virtual Analyzer와의 추가적인 통합 개선을 위해 이전에 알려지지 않은 위협이 포함되어 있을 수 있는 의심스러운 파일을 탐지하고 추가 분석을 위해 이를 Virtual Analyzer로 직접 보낼 수 있습니다. 위협이 존재함을 확인한 후에는 의심스러운 개체 목록이 즉시 업데이트되고 모든 에이전트에서 동기화되므로 이 위협이 네트워크에서 전파되는 것을 방지합니다. 자세한 내용은 샘플 제출 페이지 8-8를 참조하십시오.
대시보드 UI 개선 사항	네트워크 보호 상태에 대한 더 나은 가시성을 제공하도록 대시보드가 다시 설계되었습니다.

기능	설명
Control Manager 통합 개선 사항	Control Manager와 OfficeScan 서버 간의 무단 통신을 방지하기 위하여 Control Manager 서버 등록에는 인증서 인증이 필요하며 Control Manager 서버를 통한 정책 관리는 공개 키 암호화를 사용하여 관리됩니다. 자세한 내용은 Control Manager 인증서 권한 페이지 14-28를 참조하십시오.
위협 방지	실시간 검색은 CVE(공통 취약성 및 노출) 공격을 사용한 위협을 탐지하고 차단합니다. 자세한 내용은 검색 설정 페이지 7-27를 참조하십시오. 또한 동작 모니터링은 위협 공격에 공통적인 비정상적인 프로그램 동작을 탐지할 수 있습니다. 자세한 내용은 위협 방지 페이지 9-5를 참조하십시오.
의심스러운 연결 개선 사항	이제 의심스러운 연결 기능을 구성하여 글로벌 C&C IP 목록 및 악성 프로그램 네트워크 지문에 의해 탐지된 네트워크 연결을 기록하거나 차단할 수 있습니다. 자세한 내용은 의심스러운 연결 설정 구성 페이지 8-7를 참조하십시오.
방화벽 개선 사항	OfficeScan 방화벽의 응용 프로그램 필터는 이제 Windows 8 이상의 플랫폼을 지원합니다. OfficeScan 에이전트 사용자에게 방화벽 보안 수준 및 예외 목록 구성 권한을 부여할 수 있습니다. 자세한 내용은 방화벽 프로필 추가 페이지 13-20를 참조하십시오.
독립 모드	이전의 “로밍” 모드가 “독립” 모드로 이름이 변경되었습니다. 자세한 내용은 에이전트 연결 상태 페이지 2-44를 참조하십시오.
플랫폼 및 브라우저 지원	이 OfficeScan 버전은 다음에 대한 지원을 제공합니다. • Microsoft™ Windows™ Server 2016 **참고** 이 OfficeScan 버전은 Apache Web Server를 더 이상 지원하지 않습니다.

주요 기능 및 장점

OfficeScan은 다음과 같은 기능 및 장점을 제공합니다.

표 1-1. 주요 기능 및 장점

기능	장점
랜섬웨어 보호	향상된 검색 기능은 일반 동작을 식별하고 일반적으로 랜섬웨어 프로그램과 관련된 프로세스를 차단하여 엔드포인트에서 실행되는 대상 문서에서 랜섬웨어 프로그램을 식별 및 차단할 수 있습니다.
연결된 위협 방어	Control Manager 서버에서 의심스러운 개체 목록을 구독 신청하도록 OfficeScan을 구성합니다. Control Manager 콘솔을 사용하여 의심스러운 개체 목록에서 탐지된 개체에 대해 사용자 정의 조치를 만들어 사용자 환경과 관련된 Trend Micro 제품에 의해 보호되는 엔드포인트에서 식별된 위협에 대해 사용자 정의 방어를 제공할 수 있습니다. 이전에 식별되지 않은 위협이 포함되어 있을 수 있는 파일 개체를 향후 분석을 위해 Virtual Analyzer에 제출하도록 OfficeScan 에이전트를 구성할 수 있습니다. Virtual Analyzer는 개체를 평가한 후 알 수 없는 위협이 들어 있는 개체를 Virtual Analyzer의 의심스러운 개체 목록에 추가하고 이 목록을 네트워크 전체의 다른 OfficeScan 에이전트에 배포합니다.
Plug-in Manager 및 플러그인 솔루션	Plug-in Manager는 플러그인 솔루션의 설치, 배포 및 관리를 간편하게 해 줍니다. 관리자는 다음 두 종류의 플러그인 솔루션을 설치할 수 있습니다. • Plug-in 프로그램 • 원래 OfficeScan 기능
중앙 집중식 관리	웹 기반 관리 콘솔을 사용하면 관리자가 네트워크에 있는 모든 에이전트와 서버에 투명하게 액세스할 수 있습니다. 웹 콘솔은 모든 에이전트와 서버에서 보안 정책, 패턴 파일 및 소프트웨어 업데이트의 자동 배포를 조정합니다. 그리고 바이러스 사전 방역 서비스는 감염 벡터를 종료하고 공격 유형에 따른 보안 정책을 신속하게 배포하여 패턴 파일을 사용할 수 있게 되기 전에 바이러스 비상 발생을 예방 또는 억제합니다. 또한 OfficeScan에서는 실시간 모니터링을 수행하여 이벤트 알림을 제공하고 광범위한 보고를 전달합니다. 관리자는 원격 관리를 수행하고, 각 데스크톱이나 그룹에 사용자 정의 정책을 설정하고, 에이전트 보안 설정을 잠글 수 있습니다.

기능	장점
보안 위험 보호	OfficeScan은 파일을 검색한 후 검색된 각 보안 위험에 대해 특정 작업을 수행하여 보안 위험으로부터 컴퓨터를 보호합니다. 짧은 시간 동안 검색된 다수의 보안 위험은 비상의 조짐을 나타냅니다. 비상 발생을 억제하기 위해 OfficeScan은 바이러스 사전 방역 정책을 실행하고 위험이 완전히 없는 상태가 될 때까지 감염된 컴퓨터를 격리합니다. OfficeScan은 스마트 스캔을 사용하여 검색 프로세스를 보다 효율적으로 만듭니다. 이 기술은 로컬 엔드포인트에서 이전에 저장한 많은 수의 서명을 스마트 보호 소스에 오프로드하는 방식으로 작동합니다. 이러한 방식을 통해 점점 증가하는 시스템 및 네트워크의 서명 업데이트가 엔드포인트 시스템에 미치는 영향이 크게 감소합니다. 스마트 스캔에 대한 자세한 내용 및 스마트 스캔을 에이전트에 배포하는 방법은 검색 방법 유형 페이지 7-8을 참조하십시오.
DCS(Damage Cleanup Services)	DCS(Damage Cleanup Services)™에서는 컴퓨터에 남아 있는 파일 기반 및 네트워크 바이러스와 웜(트로이목마, 레지스트리 항목, 바이러스 파일)을 완전 자동 프로세스를 통해 제거합니다. 트로이목마로 인한 위협이나 불편함을 해결하기 위해 DCS(Damage Cleanup Services)는 다음과 같은 작업을 수행합니다. • 활동 중인 트로이 목마 검색 및 제거 • 트로이 목마가 만드는 프로세스 제거 • 트로이 목마가 수정한 시스템 파일 복구 • 트로이 목마가 남긴 파일 및 응용 프로그램 삭제 DCS(Damage Cleanup Services)는 백그라운드에서 자동으로 실행되기 때문에 구성할 필요가 없습니다. 사용자는 DCS가 실행되고 있다는 것조차 인식하지 못하지만 OfficeScan에서 트로이 목마를 제거하는 프로세스를 완료하려면 엔드포인트를 다시 시작하라고 사용자에게 알리는 경우도 있습니다.
웹 검증	웹 검증 기술은 기업 네트워크 내외부의 에이전트 컴퓨터에서 유해하고 잠재적으로 위험한 웹 사이트로 인한 피해를 사전에 방지합니다. 웹 검증은 연속적인 감염의 사슬을 끊어주고 악성 코드의 다운로드를 막아줍니다. OfficeScan을 스마트 보호 서버 또는 Trend Micro 스마트 보호 네트워크와 통합하여 웹 사이트와 페이지의 신뢰도를 확인하십시오.

기능	장점
OfficeScan 방화벽	OfficeScan 방화벽은 상태 기반 검사 및 고성능 네트워크 바이러스 검색을 통해 네트워크에서 에이전트와 서버를 보호합니다. 응용 프로그램, IP 주소, 포트 번호 또는 프로토콜에 따라 연결을 필터링할 규칙을 작성한 다음 여러 사용자 그룹에 적용합니다.
데이터 손실 방지	데이터 손실 방지는 우발적이거나 계획적인 유출로부터 조직의 디지털 자산을 보호합니다. 데이터 손실 방지를 통해 관리자는 다음을 수행할 수 있습니다. • 보호할 디지털 자산 식별 • 전자 메일 메시지 및 외부 장치와 같은 일반적인 전송 채널을 통한 디지털 자산의 전송을 제한하거나 방지하는 정책 생성 • 설정된 개인 정보 표준에 준수 적용
장치 제어	장치 제어는 컴퓨터에 연결된 외부 저장 장치 및 네트워크 리소스에 대한 액세스를 조정합니다. 장치 제어를 통해 데이터 손실 및 유출을 방지하고 파일 검색과 함께 보안 위험으로부터 보호할 수 있습니다.
동작 모니터링	동작 모니터링은 운영 체제 또는 설치된 소프트웨어에 대한 비정상적인 수정에 대해 에이전트를 지속적으로 모니터링합니다.

OfficeScan 서버

OfficeScan 서버는 모든 에이전트 구성, 보안 위험 로그, 업데이트를 보관하는 중앙 저장소입니다.

서버는 두 가지의 중요한 기능을 수행합니다.

- OfficeScan 에이전트 설치, 모니터링 및 관리
- 에이전트에 필요한 구성 요소를 대부분 다운로드합니다. OfficeScan 서버는 Trend Micro 액티브업데이트 서버에서 구성 요소를 다운로드한 후 에이전트에 배포합니다.

참고

일부 구성 요소는 스마트 보호 소스를 통해 다운로드됩니다. 자세한 내용은 스마트 보호 소스 페이지 4-5를 참조하십시오.

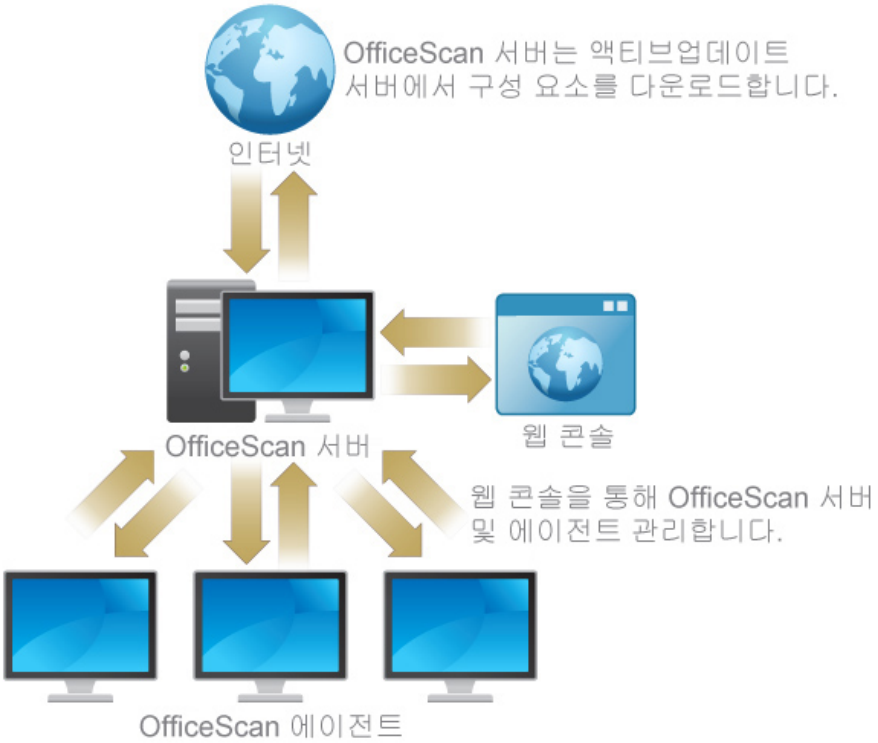


그림 1-1. OfficeScan 서버 작동 방식

OfficeScan 서버는 서버와 OfficeScan 에이전트 사이에서 실시간으로 양방향 통신을 제공할 수 있습니다. 에이전트는 브라우저 기반 웹 콘솔을 통해 관리하며, 관리자는 네트워크상의 어디에서나 이 콘솔에 액세스할 수 있습니다. 서버는 HTTP(HyperText Transfer Protocol)를 통해 에이전트와 통신합니다(에이전트가 서버와 통신할 때도 마찬가지임).

OfficeScan 에이전트

OfficeScan 에이전트를 각 엔드포인트에 설치하면 Windows 컴퓨터를 보안 위험으로부터 보호할 수 있습니다.

OfficeScan 에이전트는 설치된 서버의 상위 서버에 보고합니다. 에이전트가 다른 서버에 보고하도록 구성하려면 Agent Mover 도구를 사용하십시오. 에이전트는 이벤트 및 상태 정보를 서버에 실시간으로 보냅니다. 이벤트의 예로는 바이러스/악성 프로그램 탐지, 에이전트 시작, 에이전트 종료, 검색 시작, 업데이트 완료 등이 있습니다.

Trend Micro 제품 및 서비스와의 통합

OfficeScan은 다음 표에 나와 있는 Trend Micro 제품 및 서비스와 통합됩니다. 원활한 통합을 위해 제품에서 필요한 버전 또는 권장되는 버전을 실행하는지 확인하십시오.

표 1-2. OfficeScan과 통합되는 제품 및 서비스

제품/서비스	설명	버전
액티브업데이트 서버	OfficeScan 에이전트에서 보안 위협으로부터 엔드포인트를 보호하는 데 필요한 모든 구성 요소를 제공합니다.	해당 없음
스마트 보호 네트워크	에이전트에 파일 검증 서비스 및 웹 검증 서비스를 제공합니다. 스마트 보호 네트워크는 Trend Micro에서 호스팅합니다.	해당 없음

제품/서비스	설명	버전
독립 스마트 보호 서버	스마트 보호 네트워크와 동일한 파일 검증 서비스 및 웹 검증 서비스를 제공합니다. 독립 스마트 보호 서버는 기업 네트워크에 대한 서비스를 현지화하여 효율성을 최적화하는 용도로 설계되었습니다. **참고** 통합 스마트 보호 서버는 OfficeScan 서버와 함께 설치됩니다. 독립 스마트 보호 서버와 기능이 같지만 용량이 제한되어 있습니다.	• 3.0
Control Manager	플랫폼 또는 프로그램의 물리적 위치에 관계없이 중앙 위치에서 바이러스 백신 및 콘텐츠 보안 프로그램을 제어할 수 있는 기능을 제공하는 소프트웨어 관리 솔루션입니다.	• 6.0 SP3 Patch 2 (권장) • 6.0 SP3 • 6.0 SP2 • 6.0 SP1
Deep Discovery Analyzer	Deep Discovery는 조기 공격 탐지와 신속한 억제를 지원하고, 추가 공격 방지 기능을 즉시 개선하는 사용자 지정 보안 업데이트를 제공함으로써 사용자 지정 샌드박싱 및 해당하는 실시간 정보를 기반으로 네트워크 전체에 대한 모니터링 기능을 제공합니다.	5.1 이상

장 2

OfficeScan 시작

이 장에서는 OfficeScan을 시작하는 방법 및 초기 구성 설정을 설명합니다.

다음과 같은 항목이 포함됩니다.

- 웹 콘솔 페이지 2-2
- 대시보드 페이지 2-5
- 서버 마이그레이션 도구 페이지 2-36
- Active Directory 통합 페이지 2-40
- OfficeScan 에이전트 트리 페이지 2-44
- OfficeScan 도메인 페이지 2-57

웹 콘솔

웹 콘솔은 기업 네트워크 전체에 걸쳐 OfficeScan을 모니터링하는 중앙 지점입니다. 콘솔에는 보안 요구 사항 및 사양에 따라 구성할 수 있는 기본 설정과 값이 제공됩니다. 웹 콘솔에서는 JavaScript, CGI, HTML 및 HTTPS 등의 표준 인터넷 기술을 사용합니다.

참고

웹 콘솔에서 타임아웃 설정을 구성합니다. 웹 콘솔 설정 페이지 14-58를 참조하십시오.

웹 콘솔을 사용하여 다음을 수행합니다.

- 네트워크로 연결된 컴퓨터에 설치한 에이전트 관리
- 에이전트를 논리적 도메인으로 그룹화하여 동시에 구성 및 관리
- 네트워크로 연결된 단일 또는 여러 컴퓨터에서 검색 구성을 설정하고 수동 검색 시작
- 네트워크상의 보안 위험에 대한 알림을 구성하고 에이전트에서 보낸 로그 보기
- 비상 발생 기준 및 알림 구성
- 역할 및 사용자 계정을 구성하여 웹 콘솔 관리 작업을 다른 OfficeScan 관리자에게 위임
- 에이전트가 보안 지침을 준수하는지 확인

참고

웹 콘솔은 Windows UI 모드의 Windows 8, 8.1, 10 또는 Windows Server 2012를 지원하지 않습니다.

웹 콘솔을 열기 위한 요구 사항

다음 리소스가 있는 네트워크의 엔드포인트에서 웹 콘솔을 엽니다.

- 300MHz Intel™ Pentium™ 프로세서 또는 동급 프로세서
- 128MB RAM
- 30MB 이상의 빈 디스크 공간
- 256색 이상에서 1366 x 768 해상도를 지원하는 모니터
- 웹 브라우저 지원:
  - Microsoft Internet Explorer™ 10.0 이상
  - Microsoft Edge
  - Chrome

참고

OfficeScan에서는 웹 콘솔을 볼 때 HTTPS 트래픽만 지원합니다.

웹 브라우저에서 OfficeScan 서버 설치 유형에 따라 주소 표시줄에 다음 중 하나를 입력합니다.

표 2-1. OfficeScan 웹 콘솔 URL

설치 유형	URL
SSL을 사용하는 기본 사이트	https://<OfficeScan 서버 FQDN 또는 IP 주소>/OfficeScan
SSL을 사용하는 가상 사이트	https://<OfficeScan 서버 FQDN 또는 IP 주소>:<포트 번호>/OfficeScan

참고

OfficeScan의 이전 버전에서 업그레이드한 경우 웹 브라우저와 프록시 서버 캐시 파일로 인해 OfficeScan 웹 콘솔을 올바르게 로드하지 못할 수도 있습니다. 이러한 경우, 웹 콘솔에 액세스하는 데 사용하는 OfficeScan 서버와 엔드포인트 사이에 위치한 프록시 서버와 브라우저에서 캐시 메모리를 지우십시오.

로그온 계정

OfficeScan 서버 설치 도중, 설치 프로그램에서 루트 계정을 생성하고 이 계정에 대해 암호를 입력하라는 메시지를 표시합니다. 처음에 웹 콘솔을 열 때 사용자 이름으로 "root"를 입력하고 루트 계정 암호를 입력합니다. 암호를 잊어버린 경우에는 지원 센터에 연락하여 암호 초기화에 대한 도움을 얻으십시오.

다른 사용자들이 루트 계정을 사용하지 않고 웹 콘솔에 액세스할 수 있도록 하려면 사용자 역할을 정의하고 사용자 계정을 설정합니다. 사용자가 콘솔에 로그온하면, 해당 사용자용으로 설정된 사용자 계정을 사용할 수 있습니다. 자세한 내용은 역할 기반 관리 페이지 14-3를 참조하십시오.

웹 콘솔 배너

웹 콘솔의 배너 영역에서는 다음 옵션을 제공합니다.

그림 2-1. 웹 콘솔 배너 영역

- **<계정 이름>**: 계정에 대한 세부 정보(예: 암호)를 수정하려면 계정 이름(예: root)을 클릭합니다.
- **로그오프**: 웹 콘솔에서 로그오프합니다.

지원 받기

도움말 메뉴를 사용하면 다음 지원 정보에 액세스할 수 있습니다.

- **목차 및 색인**: 온라인 도움말을 엽니다.
- **새로운 기능**: 이번 릴리스에 새로 추가된 일부 주요 기능을 표시합니다.
- **지원**: 질문을 제출하고 Trend Micro 제품에 대한 일반적인 질문의 대답을 찾을 수 있는 Trend Micro 지원 센터 웹 페이지를 표시합니다.
- **위협 백과사전**: 악성 프로그램 관련 정보를 저장하는 Trend Micro의 저장소인 위협 백과사전 웹 사이트를 표시합니다. Trend Micro 위협 전문가가 탐

지된 악성 프로그램, 스팸, 유해 URL 및 취약점을 정기적으로 게시합니다. 또한 위협 백과사전에서는 주요 웹 공격에 대해 설명하고 관련 정보를 제공합니다.

- **Trend Micro 연락처**: 전 세계 사무소에 대한 정보가 포함된 Trend Micro **Contact Us** 웹 사이트를 표시합니다.
- **정보**: 제품 개요, 구성 요소 버전 정보를 확인하는 방법 및 지원 정보 시스템에 대한 링크를 제공합니다.

  자세한 내용은 지원 정보 시스템 페이지 18-2를 참조하십시오.

대시보드

대시보드은 OfficeScan 웹 콘솔을 열거나 주 메뉴에서 **대시보드**를 클릭할 때 표시됩니다.

각 웹 콘솔 사용자 계정에는 완전히 독립된 대시보드가 제공됩니다. 따라서 한 사용자 계정의 대시보드를 변경해도 다른 사용자 계정의 대시보드는 영향을 받지 않습니다.

대시보드에 OfficeScan 에이전트 데이터가 포함된 경우 사용자 계정의 에이전트 도메인 권한에 따라 표시되는 데이터가 달라집니다. 예를 들어 사용자 계정에 도메인 A와 B를 관리하는 권한을 부여한 경우 이 사용자 계정의 대시보드에는 도메인 A와 B에 속한 에이전트의 데이터만 표시됩니다.

사용자 계정에 대한 자세한 내용은 역할 기반 관리 페이지 14-3를 참조하십시오.

대시보드 화면에는 다음 항목이 포함됩니다.

- 제품 라이선스 상태 섹션
- 위젯
- 탭

제품 라이선스 상태 섹션

이 섹션은 대시보드의 맨 위에 있으며 OfficeScan 라이선스 상태를 표시합니다.

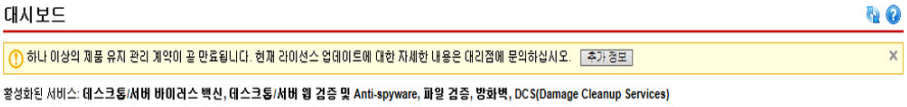


그림 2-2. 제품 라이선스 상태 섹션

다음과 같은 경우에 라이선스 상태에 대한 미리 알림이 표시됩니다.

- 정식 버전 라이선스를 소유한 경우:
  - 라이선스 만료 60일 전
  - 제품의 유예 기간 중. 유예 기간은 지역에 따라 다릅니다. Trend Micro 대리점에서 유예 기간을 확인하십시오.
  - 라이선스가 만료되고 유예 기간이 경과된 경우. 이 기간 중에는 기술 지원을 받거나 구성 요소 업데이트를 수행할 수 없습니다. 검색 엔진은 계속 이전 구성 요소를 사용하여 컴퓨터를 검색합니다. 이전 구성 요소로는 최신 보안 위협으로부터 시스템을 완벽하게 보호할 수 없습니다.
- 평가판 라이선스를 소유한 경우:
  - 라이선스 만료 14일 전
  - 라이선스가 만료된 경우. 이 기간 중에는 OfficeScan에서 구성 요소 업데이트, 검색 및 모든 에이전트 기능을 사용할 수 없습니다.

정품 인증 코드를 얻은 경우 **관리** > **설정** > **제품 라이선스**로 이동하여 라이선스를 갱신합니다.

제품 정보 표시줄

OfficeScan에서는 **대시보드** 화면 상단에 다양한 메시지를 표시하여 관리자에게 추가 정보를 제공합니다.

표시되는 정보는 다음과 같습니다.

- 사용 가능한 최신 OfficeScan Service Pack 또는 패치

참고

추가 정보를 클릭하여 Trend Micro 다운로드 센터(http://downloadcenter.trendmicro.com/?regs=KOR)에서 패치를 다운로드하십시오.

- 사용 가능한 새 위젯
- 계약의 만료 날짜가 가까운 경우 유지 관리 계약 알림
- 점검 모드 알림
- 정품 알림

참고

OfficeScan에 사용하는 라이선스가 정품이 아닌 경우 정보 메시지가 표시됩니다. 정품 라이선스를 구입하지 않은 경우 OfficeScan에서는 경고를 표시하고 업데이트 수행을 중지합니다.

탭 및 위젯

위젯은 대시보드의 핵심 구성 요소로서, 여러 보안 관련 이벤트에 대한 특정 정보를 제공합니다. 일부 위젯에서는 오래된 구성 요소 업데이트와 같은 특정 작업을 수행할 수 있습니다.

위젯에서 표시하는 정보는 다음에서 가져옵니다.

- OfficeScan 서버 및 에이전트
- 플러그인 솔루션 및 해당 에이전트
- Trend Micro 스마트 보호 네트워크

참고

Smart Feedback을 사용하도록 설정하여 스마트 보호 네트워크의 데이터를 표시할 수 있습니다. Smart Feedback에 대한 자세한 내용은 Smart Feedback 페이지 14-63을 참조하십시오.

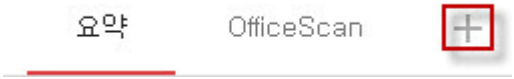
탭은 위젯에 대한 컨테이너를 제공합니다. **대시보드**은 최대 30개의 탭을 지원합니다.

탭 작업

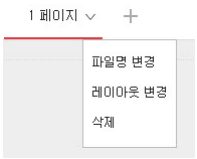
추가, 이름 변경, 레이아웃 변경, 삭제 및 탭 보기 간 자동 전환을 통해 탭을 관리합니다.

절차

1. **대시보드**로 이동합니다.
2. 새 탭을 추가하려면
   a. 추가 아이콘을 클릭합니다.



   b. 새 탭의 이름을 입력합니다.
3. 탭의 이름을 변경하려면
   a. 탭 이름을 마우스로 가리키고 아래쪽 화살표를 클릭합니다.



   b. **이름 변경**을 클릭하고 새 탭 이름을 입력합니다.
4. 탭의 위젯 레이아웃을 변경하려면
   a. 탭 이름을 마우스로 가리키고 아래쪽 화살표를 클릭합니다.
   b. **레이아웃 변경**을 클릭합니다.

c. 표시되는 화면에서 새 레이아웃을 선택합니다.

d. **저장**을 클릭합니다.

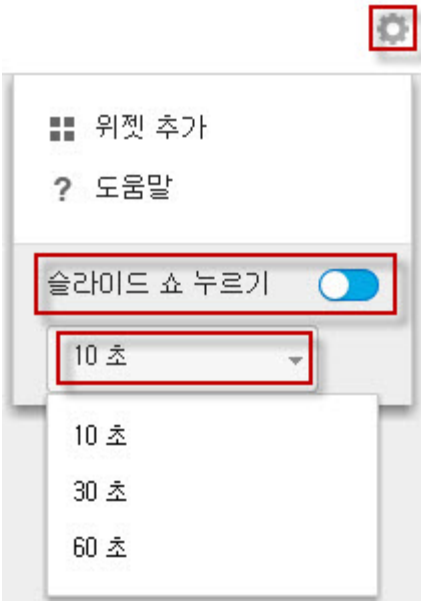
5. 탭을 삭제하려면

a. 탭 이름을 마우스로 가리키고 아래쪽 화살표를 클릭합니다.

b. **삭제**를 클릭하고 확인합니다.

6. 탭 슬라이드 쇼를 재생하려면

a. 탭 디스플레이 오른쪽에서 **설정** 단추를 클릭합니다.



b. **탭 슬라이드 쇼** 컨트롤을 사용하도록 설정합니다.

c. 다음 탭으로 전환되기 전 각 탭을 표시할 시간을 선택합니다.

위젯 작업

항목 추가, 이동, 크기 조정, 이름 변경 및 삭제를 통해 위젯을 관리합니다.

절차

1. **대시보드**로 이동합니다.
2. 탭을 클릭합니다.
3. 위젯을 추가하려면
   a. 탭 디스플레이 오른쪽에서 **설정** 단추를 클릭합니다.

   b. **위젯 추가**를 클릭합니다.
   c. 추가할 위젯을 선택합니다.
      - 위젯 맨 위의 드롭다운에서 범주를 선택하여 선택의 폭을 좁힙니다.
      - 화면 맨 위에 있는 검색 입력란을 사용하여 특정 위젯을 검색할 수 있습니다.
   d. **추가**를 클릭합니다.
4. 특정 위젯을 동일한 탭의 새 위치로 이동하려면 해당 위젯을 끌어 새 위치에 놓습니다.

5. 위젯 오른쪽 가장자리를 커서로 가리킨 다음 왼쪽이나 오른쪽으로 커서를 이동하여 여러 열 탭에서 위젯의 크기를 조정할 수 있습니다.

6. 위젯의 이름을 변경하려면

   a. 설정 아이콘(>)을 클릭합니다.

   b. 새 제목을 입력합니다.

   참고

   OfficeScan 및 Plug-ins Mashup과 같은 일부 위젯의 경우 위젯 관련 항목을 수정할 수 있습니다.

   c. **저장**을 클릭합니다.

7. 위젯을 삭제하려면 삭제 아이콘(>)을 클릭합니다.

요약 탭 위젯

요약 탭은 네트워크에 있는 모든 OfficeScan 에이전트의 보안 상태에 대한 개요를 제공합니다.

참고

요약 탭에 표시되는 위젯을 추가, 삭제 또는 수정할 수 없습니다.

사용 가능한 위젯:

- 전반적인 위협 탐지 및 정책 위반 위젯 페이지 2-12
- 엔드포인트 상태 위젯 페이지 2-13
- 기간별 보안 위험 탐지 위젯 페이지 2-18

전반적인 위협 탐지 및 정책 위반 위젯

이 위젯은 지난 24시간 동안 네트워크 전체의 모든 위협 탐지 및 정책 위반에 대한 개요를 제공합니다.

각 그룹에 대해 발생한 특정 탐지 유형에 대한 분석을 보려면 위협 또는 위반 수를 마우스로 가리킵니다. 특정 기능에 대한 로그를 보려면 오른쪽의 수를 클릭합니다.

표 2-2. 탐지 범주

범주	설명
알려진 위협	Trend Micro에서 확인한 보안 위협을 탐지하는 모든 기능을 표시합니다. • 바이러스/악성 프로그램 • 스파이웨어/그레이웨어 • 웹 검증
알 수 없는 위협	고급 휴리스틱, 분석 또는 기능 모델링을 사용하여 잠재적 위협을 탐지하는 모든 기능을 표시합니다. • 머신러닝 • 동작 모니터링 • 의심스러운 연결 • 의심스러운 파일 개체

범주	설명
정책 위반	기업의 보안 표준과 관련된 정책 위반을 포함하는 모든 기능을 표시합니다. • 방화벽 • 장치 제어 • 데이터 손실 방지

엔드포인트 상태 위젯

이 위젯은 네트워크에 있는 OfficeScan 에이전트의 연결 및 업데이트 상태에 대한 개요 그리고 OfficeScan 서버에 보고하지 않는 관리되지 않는 엔드포인트의 최신 보안 준수 수를 제공합니다.

서로 다른 상태에 대한 분석을 보려면 마우스로 수를 가리킵니다. 특정 상태에 대한 로그를 보려면 오른쪽의 수를 클릭합니다.

표 2-3. 에이전트/엔드포인트 그룹

그룹	설명
관리된 에이전트	네트워크에 있는 OfficeScan 에이전트의 마지막으로 보고된 연결 상태를 표시합니다. • 온라인 • 오프라인 • 독립
오래된 에이전트	구성 요소 범주 목록과 각 범주에서 오래된 에이전트가 있는 OfficeScan 에이전트의 수를 표시합니다.
관리되지 않는 엔드포인트	OfficeScan에서 탐지할 수 있지만 OfficeScan 에이전트 프로그램을 설치하지 않았거나 OfficeScan 서버에 보고하지 않는 모든 엔드포인트의 목록을 표시합니다. **참고** OfficeScan 서버에서 관리되지 않는 엔드포인트 수를 정기적으로 업데이트하도록 하려면 다음을 수행합니다. 1. 평가를 위해 Active Directory/IP 주소 범위를 정의합니다. 자세한 내용은 Active Directory 통합 페이지 2-40를 참조하십시오. 2. 예약 평가를 구성합니다. 자세한 내용은 관리되지 않는 엔드포인트에 대한 보안 준수 페이지 15-68를 참조하십시오.

랜섬웨어 요약 위젯

그림 2-3. 모든 랜섬웨어 데이터와 "랜섬웨어 시도 탐지됨" 막대형 차트의 확대 보기를 표시하는 기본 보기

이 위젯은 지정된 시간 범위 동안의 모든 랜섬웨어 공격 시도에 대한 개요를 제공합니다.

기본 보기는 모든 랜섬웨어 탐지의 요약을 표시하고 감염 채널을 기반으로 랜섬웨어 공격 시도를 추가로 분류합니다.

- 기본 보기의 랜섬웨어 탐지 수를 클릭하면 랜섬웨어 탐지 세부 정보를 나열하는 **보안 위험 - 랜섬웨어** 로그 화면이 열립니다.

위젯 오른쪽에서 아무 차트나 클릭하면 차트 데이터의 확대 보기가 표시됩니다.

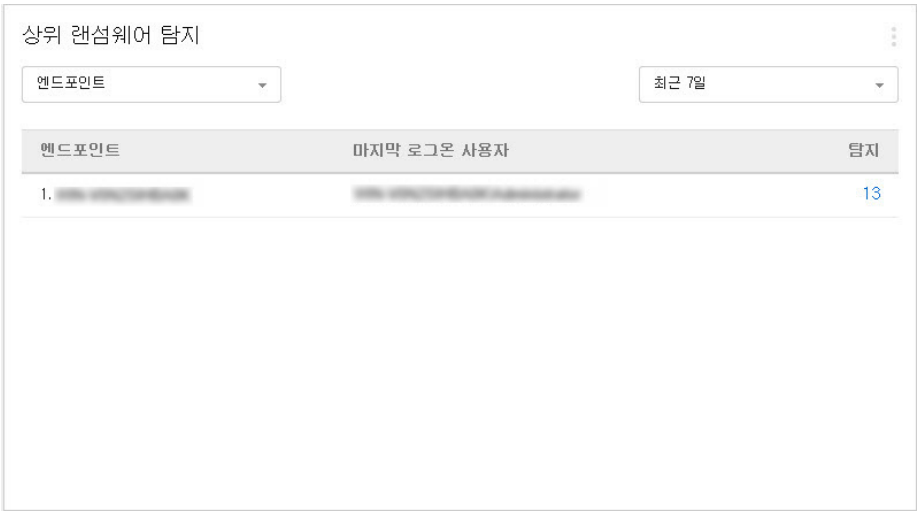
- 특정 날짜의 노드를 마우스로 가리키면 표시된 탐지 범주에 대한 총 탐지 수를 볼 수 있습니다. 특정 날짜의 랜섬웨어 탐지 세부 정보를 나열하는 **보안 위험 - 랜섬웨어** 로그 화면으로 리디렉션하려면 노드를 클릭합니다.

표 2-4. 랜섬웨어 탐지 채널

채널	설명	탐지 위치
Web	웹 클라이언트(예: 브라우저 또는 FTP 클라이언트)를 사용하여 다운로드한 파일	• 웹 검증 • 실시간 검색 • 동작 모니터링

채널	설명	탐지 위치
네트워크 트래픽	의심스러운 연결 기능에 의해 탐지된 랜섬웨어	• 의심스러운 연결
전자 메일	Microsoft Outlook 또는 Windows Live Mail을 사용하여 연 전자 메일 첨부 파일 **참고** OfficeScan은 **로컬 또는 네트워크 드라이브** 채널에서 기타 전자 메일 클라이언트 응용 프로그램을 사용하여 연 모든 첨부 파일을 분류합니다.	• 실시간 검색 • 동작 모니터링
자동 실행 파일	이동식 저장 장치에 위치하고 자동 실행 파일에 의해 실행되는 프로그램 **참고** OfficeScan은 **로컬 또는 네트워크 드라이브** 채널에서 이동식 저장 장치의 자동 실행 프로그램에 의해 실행되지 않는 기타 모든 파일/프로그램을 분류합니다.	• 실시간 검색 • 동작 모니터링
로컬 또는 네트워크 드라이브	다음을 포함한 로컬 또는 네트워크 드라이브에서 감지된 랜섬웨어 • Microsoft Outlook 또는 Windows Live Mail을 제외한 전자 메일 클라이언트를 사용하여 연 전자 메일 첨부 파일 • 자동 실행 프로그램에 의해 실행되지 않는 이동식 저장 장치의 파일	• 실시간 검색 • 수동 검색 • 예약 검색 • 지금 검색 • 동작 모니터링

상위 랜섬웨어 탐지 위젯



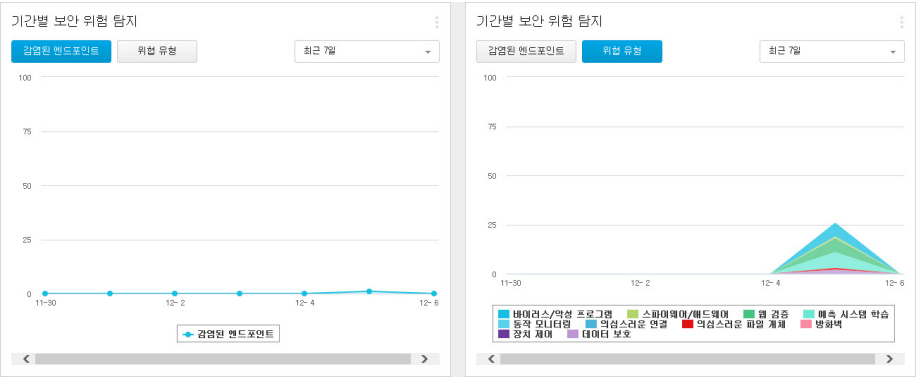
이 위젯은 지정된 시간 범위 동안의 상위 랜섬웨어 탐지에 대한 개요를 제공합니다.

드롭다운을 사용하여 표시할 랜섬웨어 데이터의 유형을 선택합니다.

보기	설명
엔드포인트	네트워크에서 가장 많은 수의 랜섬웨어가 탐지된 엔드포인트를 표시합니다. 랜섬웨어 탐지 수를 클릭하면 랜섬웨어 탐지 세부 정보를 나열하는 **보안 위험 - 랜섬웨어** 로그 화면이 열립니다.
랜섬웨어 유형	네트워크에서 가장 많은 수가 탐지된 랜섬웨어의 유형을 표시합니다. 특정 위협 유형에 대한 추가적인 정보를 얻기 위해 Trend Micro 위협 백과사전을 열려면 **위협 이름** 링크를 클릭합니다.

보기	설명
도메인	네트워크에서 가장 많은 수의 랜섬웨어가 탐지된 랜섬웨어 도메인을 표시합니다. 특정 도메인에 대한 추가적인 정보를 얻기 위해 Trend Micro 위협 백과사전을 열려면 **위협 이름** 링크를 클릭합니다.

기간별 보안 위험 탐지 위젯



이 위젯은 위협 탐지와 함께 네트워크의 엔드포인트에 대한 개요와 특정 시간 범위 동안 네트워크에 영향을 준 위협의 유형에 대한 개요를 제공합니다.

서로 다른 보기 간을 전환하려면 **영향받는 엔드포인트** 또는 **위협 유형** 단추를 클릭합니다.

보기	설명
감염된 엔드포인트	지정된 시간 범위 동안 위협이 탐지되었거나 정책 위반이 발생한 엔드포인트의 수를 표시합니다. 특정 날짜의 노드를 클릭하면 해당 날짜에 영향받은 모든 엔드포인트를 에이전트 트리에 표시하는 **에이전트 관리** 화면으로 리디렉션됩니다.

보기	설명
위협 유형	지정된 시간 범위 동안 기록된 위협 및 정책 위반의 수를 간략하게 보여주는 그래프를 표시합니다. • 그래프에서 탐지 정보를 표시하거나 숨기려면 그래프 맨 아래에서 위협 유형 이름을 클릭합니다. • 특정 날짜의 노드를 마우스로 가리키면 표시된 위협 유형에 대한 총 탐지 수를 볼 수 있습니다. 노드를 클릭하면 목록에서 강조 표시된 위협 유형에 대한 로그 화면으로 리디렉션됩니다.

팁

이 위젯을 여러 번 추가하여 두 가지 보기를 모두 표시할 수 있습니다. 위젯을 다른 탭에 추가할 때 **OfficeScan** 위젯 유형 아래에서 위젯을 찾습니다.

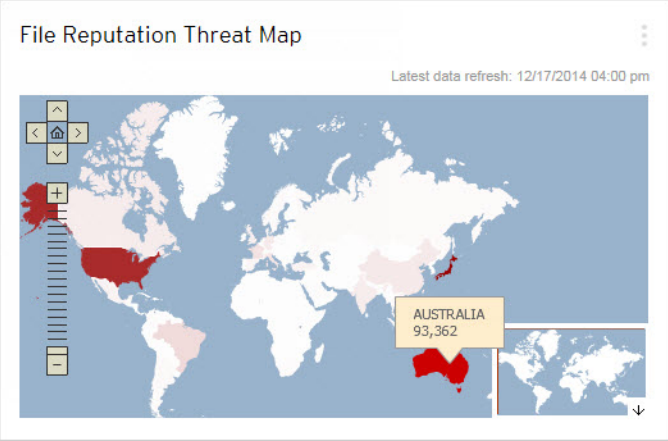
스마트 보호 네트워크 위젯

OfficeScan은 OfficeScan 에이전트에 파일 검증 서비스 및 웹 검증 서비스를 제공하는 Trend Micro 스마트 보호 네트워크의 정보가 들어 있는 기본 탭을 제공합니다.

사용 가능한 위젯:

- 웹 검증 상위 위협 소스 위젯 페이지 2-22
- 웹 검증 상위 위협 대상 사용자 위젯 페이지 2-21
- 파일 검증 위협 맵 위젯 페이지 2-20

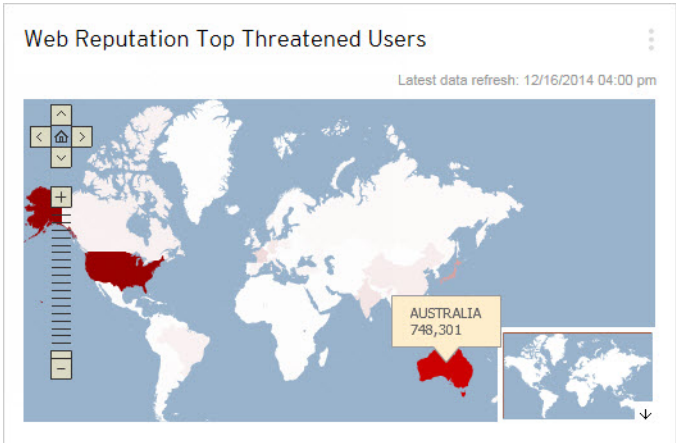
파일 검증 위협 맵 위젯



이 위젯에서는 파일 검증 서비스에서 탐지한 총 보안 위협 수를 보여 줍니다. 지리적 위치별 정보가 세계 지도에 표시됩니다.

지도의 다양한 지역을 마우스로 가리켜서 특정 지역에서 탐지된 총 보안 위협 수를 볼 수 있습니다.

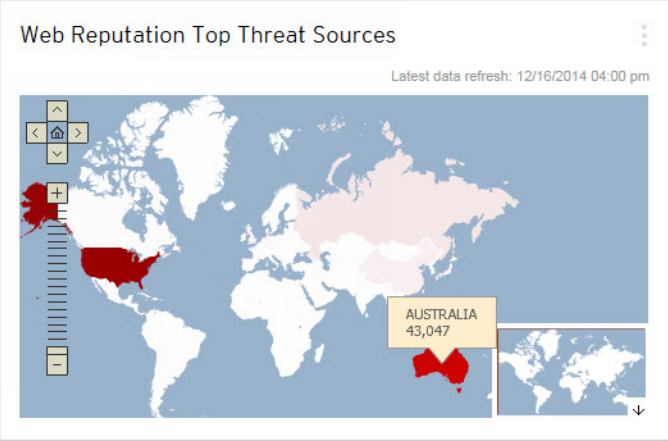
웹 검증 상위 위협 대상 사용자 위젯



이 위젯에서는 웹 검증 서비스에서 탐지한 유해 URL의 영향을 받는 사용자 수를 보여 줍니다. 지리적 위치별 정보가 세계 지도에 표시됩니다.

지도의 다양한 지역을 마우스로 가리켜서 특정 지역에서 영향받은 총 사용자 수를 볼 수 있습니다.

웹 검증 상위 위협 소스 위젯



이 위젯에서는 웹 검증 서비스에서 탐지한 총 보안 위협 수를 보여 줍니다. 지리적 위치별 정보가 세계 지도에 표시됩니다.

지도의 다양한 지역을 마우스로 가리켜서 특정 지역에서 탐지된 총 보안 위협 수를 볼 수 있습니다.

데이터 보호 위젯

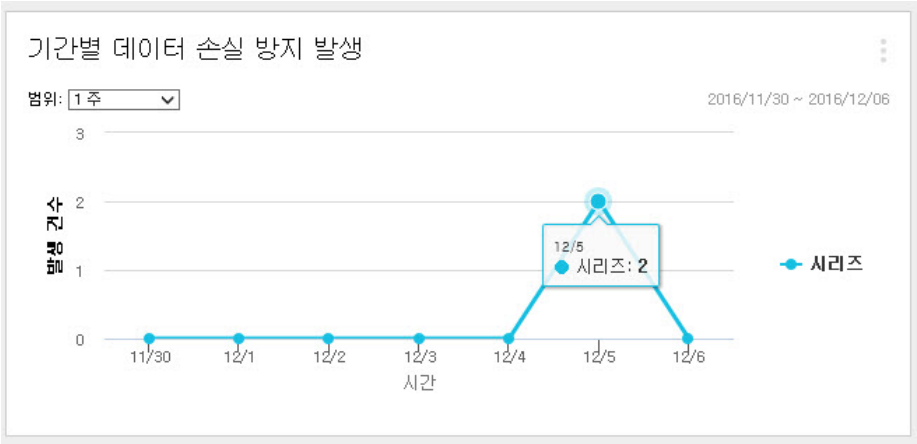
참고

데이터 보호 위젯은 OfficeScan 데이터 보호를 활성화한 후에 사용할 수 있습니다.

사용 가능한 위젯:

- 기간별 데이터 손실 방지 발생 위젯 페이지 2-23
- 상위 데이터 손실 방지 발생 위젯 페이지 2-24

기간별 데이터 손실 방지 발생 위젯

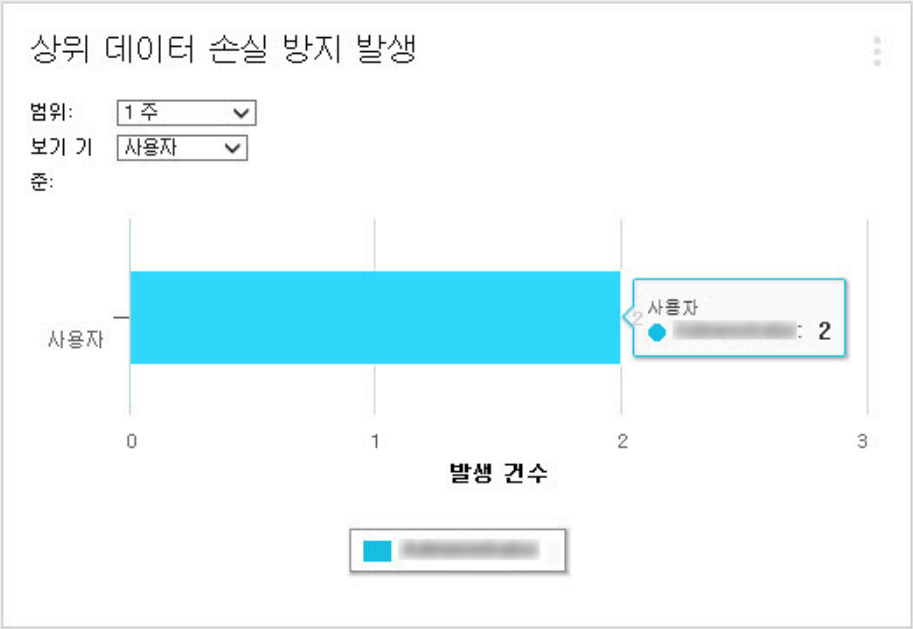


이 위젯은 특정 시간 범위 동안 데이터 손실 방지 발생의 전체 수를 표시합니다.

참고

여기에는 취해진 조치("차단" 또는 "그대로 두기")와 관계없이 모든 데이터 손실 방지 발생이 포함됩니다.

상위 데이터 손실 방지 발생 위젯



이 위젯은 지정된 시간 범위 동안 데이터 손실 방지 발생을 트리거한 상위 사용자, 채널, 템플릿 또는 엔드포인트를 표시합니다.

참고

- 이 위젯에는 최대 10개의 사용자, 채널, 템플릿 또는 엔드포인트가 표시됩니다.
- 여기에는 취해진 조치("차단" 또는 "그대로 두기")와 관계없이 모든 데이터 손실 방지 발생이 포함됩니다.

보기 기준 드롭다운을 사용하여 표시할 데이터 손실 방지 데이터의 유형을 선택합니다.

표 2-5. 데이터 손실 방지 보기

보기	설명
사용자	디지털 자산을 가장 많이 전송한 사용자 • 그래프에서 탐지 정보를 표시하거나 숨기려면 그래프 맨 아래에서 사용자 이름을 클릭합니다. • 사용자 이름과 해당 사용자에 대한 데이터 손실 방지 발생의 수를 보려면 마우스로 탐지 막대를 가리킵니다.
채널	디지털 자산을 전송하는 데 가장 자주 사용된 채널 • 그래프에서 탐지 정보를 표시하거나 숨기려면 그래프 맨 아래에서 채널 이름을 클릭합니다. • 채널 이름과 해당 채널에 대한 데이터 손실 방지 발생의 수를 보려면 마우스로 탐지 막대를 가리킵니다.
템플릿	가장 많은 탐지를 트리거한 디지털 자산 템플릿 • 그래프에서 탐지 정보를 표시하거나 숨기려면 그래프 맨 아래에서 템플릿 이름을 클릭합니다. • 템플릿 이름과 해당 템플릿에 대한 데이터 손실 방지 발생의 수를 보려면 마우스로 탐지 막대를 가리킵니다.
엔드포인트	디지털 자산을 가장 많이 전송한 엔드포인트 • 그래프에서 탐지 정보를 표시하거나 숨기려면 그래프 맨 아래에서 엔드포인트 이름을 클릭합니다. • 엔드포인트 이름과 해당 엔드포인트에 대한 데이터 손실 방지 발생의 수를 보려면 마우스로 탐지 막대를 가리킵니다.

OfficeScan 위젯

OfficeScan 위젯은 OfficeScan 에이전트 보안 상태 및 탐지, 플러그인 프로그램 정보 및 비상 발생에 대한 빠른 참조를 제공합니다.

사용 가능한 위젯:

- C&C 콜백 이벤트 위젯 페이지 2-26
- 보안 위험 탐지 위젯 페이지 2-28

- OfficeScan 및 Plug-ins Mashup 위젯 페이지 2-29
- 바이러스 에이전트 연결 위젯 페이지 2-30
- Edge 릴레이 서버 위젯에 연결된 에이전트 페이지 2-32
- 비상 발생 위젯 페이지 2-33
- 에이전트 업데이트 위젯 페이지 2-35

C&C 콜백 이벤트 위젯

이 위젯에는 공격 대상 및 소스 콜백 주소를 비롯한 C&C 콜백 이벤트 정보가 모두 표시됩니다.

특정 C&C 서버 목록의 C&C 콜백 정보를 보도록 선택할 수 있습니다. 목록 소스(글로벌 정보, Virtual Analyzer)를 선택하려면 편집 아이콘(>)을 클릭하고 **C&C 목록 소스** 드롭다운에서 목록을 선택합니다.

보기 기준 드롭다운을 사용하여 다음을 표시하는 C&C 콜백 데이터의 유형을 선택합니다.

- **손상된 호스트**: 대상 엔드포인트별로 최신 C&C 정보를 표시합니다.

  표 2-6. 손상된 호스트 정보

열	설명
손상된 호스트	C&C 공격의 대상으로 지정된 엔드포인트 이름
콜백 주소	엔드포인트가 연결하려고 한 콜백 주소의 수

열	설명
최신 콜백 주소	엔드포인트가 연결하려고 한 마지막 콜백 주소
콜백 시도 횟수	대상 엔드포인트가 콜백 주소에 연결하려고 시도한 횟수 **참고** 하이퍼링크를 클릭하여 **C&C 콜백 로그** 화면을 열고 자세한 정보를 볼 수 있습니다.

- **콜백 주소**: C&C 콜백 주소별로 최신 C&C 정보를 표시합니다.

표 2-7. C&C 주소 정보

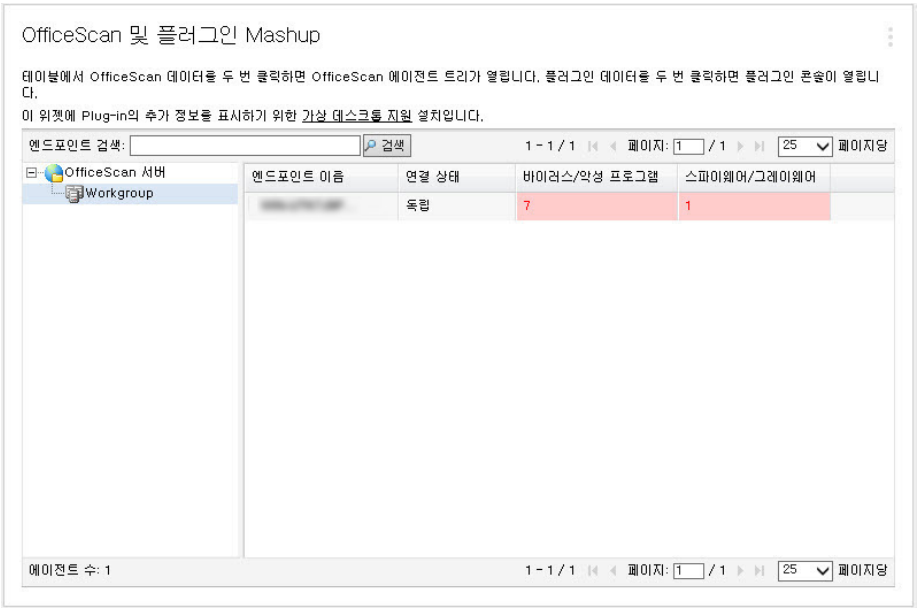
열	설명
콜백 주소	네트워크에서 시작된 C&C 콜백 주소
C&C 위험 수준	글로벌 정보 또는 Virtual Analyzer 목록에 따라 결정되는 콜백 주소의 위험 수준
손상된 호스트	콜백 주소가 대상으로 한 엔드포인트의 수
최신 손상된 호스트	C&C 콜백 주소에 마지막으로 연결하려고 한 엔드포인트의 이름
콜백 시도 횟수	네트워크의 주소에 대한 콜백 시도 횟수 **참고** 하이퍼링크를 클릭하여 **C&C 콜백 로그** 화면을 열고 자세한 정보를 볼 수 있습니다.

보안 위험 탐지 위젯

이 위젯은 탐지된 보안 위협의 수와 영향받는 엔드포인트의 수를 표시합니다.

에이전트 트리에 영향받는 OfficeScan 에이전트를 나열하는 **에이전트 관리** 화면을 열려면 엔드포인트 수를 클릭합니다.

OfficeScan 및 Plug-ins Mashup 위젯



이 위젯은 OfficeScan 에이전트의 데이터와 설치된 Plug-in 프로그램의 데이터를 조합한 후 이를 에이전트 트리에 표시합니다. 이 위젯을 사용하면 에이전트의 보호 범위를 신속하게 평가하고 개별 Plug-in 프로그램을 관리하는 데 필요한 오버헤드를 줄일 수 있습니다.

이 위젯은 다음 Plug-in 프로그램의 데이터를 표시합니다.

- Trend Micro 가상 데스크톱 지원

중요

Mashup 위젯에서 해당 데이터를 표시하려면 우선 지원되는 Plug-in 프로그램을 활성화해야 합니다. 새 버전을 사용할 수 있는 경우 Plug-in 프로그램을 업그레이드하십시오.

에이전트 트리에 표시할 열을 선택하려면 위젯의 오른쪽 위에서 **기타 옵션** 단추를 클릭하고 **설정** 단추를 클릭합니다.

열 아래의 데이터를 클릭하여 해당 Plug-in 프로그램 콘솔을 열거나 OfficeScan **에이전트 관리** 화면을 엽니다. 표시되는 화면은 클릭한 데이터 유형에 따라 달라집니다.

바이러스 에이전트 연결 위젯

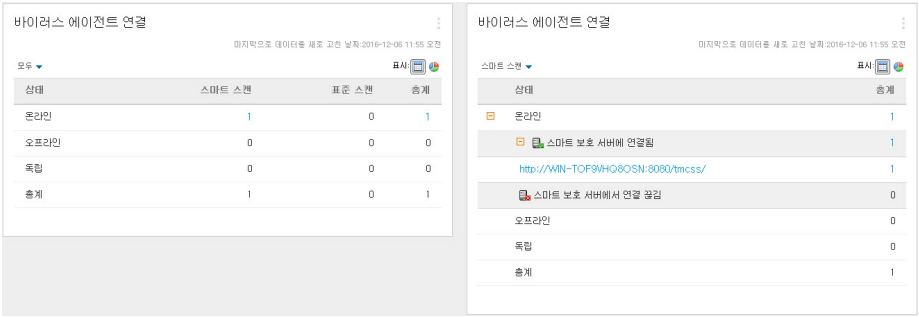


그림 2-4. 모든 스마트 스캔 및 표준 스캔 에이전트를 표시하는 기본 보기와 스마트 보호 서버가 포함된 확장된 스마트 스캔 에이전트 보기

이 위젯은 구성된 검색 방법(스마트 스캔 및 표준 스캔)과 관련하여 OfficeScan 에이전트와 OfficeScan 서버 간의 연결 상태를 표시합니다.

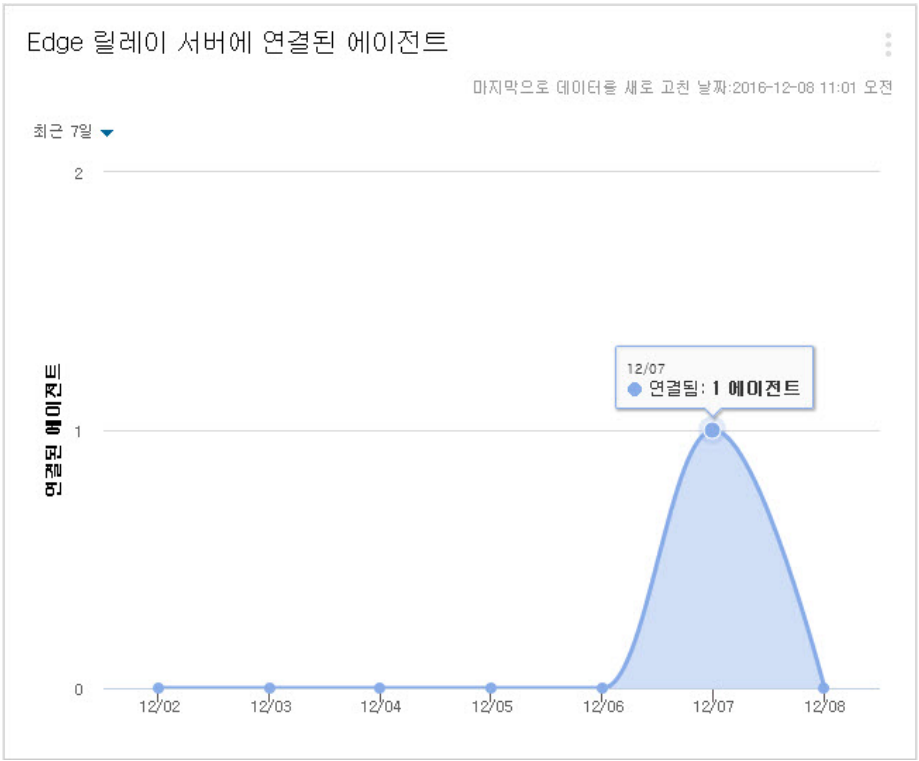
표시 아이콘( )을 클릭하여 데이터를 테이블에 표시할지 아니면 원형 차트에 표시할지 선택할 수 있습니다.

표시되는 데이터의 유형을 변경하려면 테이블/그래프 위의 드롭다운 목록을 사용합니다. 에이전트 트리에 관련된 OfficeScan 에이전트를 나열하는 **에이전트 관리** 화면을 열려면 상태에 대한 수를 클릭합니다.

보기	설명
모두	두 검색 방법에 대해 모든 OfficeScan 에이전트의 연결 상태를 표시합니다.

보기	설명
표준 스캔	표준 스캔 방법을 사용하는 모든 OfficeScan 에이전트의 연결 상태를 표시합니다.
스마트 스캔	스마트 스캔 방법을 사용하는 모든 OfficeScan 에이전트의 연결 상태를 표시합니다. 테이블에서 에이전트 연결 상태를 볼 때: • 스마트 보호 서버에 대한 에이전트의 연결 상태를 보려면 "온라인" 에이전트 정보를 확장합니다. • URL을 클릭하여 스마트 보호 서버 관리 콘솔을 엽니다. **참고** 온라인 에이전트(OfficeScan 서버에 보고)만 스마트 보호 서버와의 연결 상태를 보고할 수 있습니다. 스마트 보호 서버와의 오프라인 에이전트 연결을 복원하려면 OfficeScan 에이전트 아이콘에 표시된 문제 해결 페이지 15-38 항목을 참조하십시오.

Edge 릴레이 서버 위젯에 연결된 에이전트



이 위젯은 특정 시간 범위 동안 OfficeScan Edge 릴레이 서버에 연결된 OfficeScan 에이전트의 수를 표시합니다.

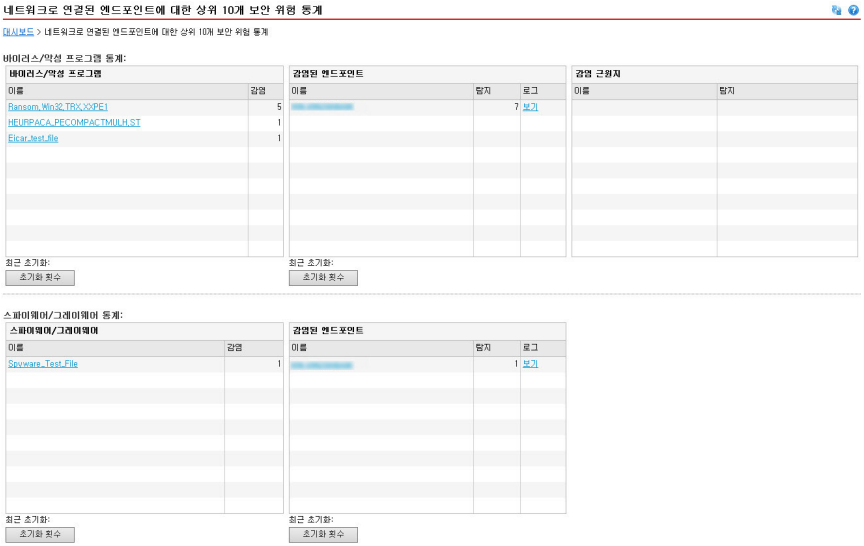
비상 발생 위젯

비상 발생 위젯에서는 모든 현재 보안 위험 비상 발생 및 최근 바이러스 비상 발생 경고의 상태를 제공합니다.

- 바이러스 비상 발생에 대한 자세한 내용을 보려면 경고의 날짜/시간 링크를 클릭합니다.
- 바이러스 비상 발생 경고 정보의 상태를 **초기화**하고 OfficeScan에서 바이러스 비상 발생을 탐지한 경우 즉시 바이러스 사전 방역 조치를 실행할 수 있습니다.

  바이러스 사전 방역 조치에 대한 자세한 내용은 바이러스 사전 방역 정책 페이지 7-108을 참조하십시오.

- **상위 10개 보안 위험 통계 보기**를 클릭하여 가장 일반적인 보안 위험, 보안 위험 수가 가장 많은 엔드포인트 및 상위 감염 소스를 확인할 수 있습니다.



상위 10개 보안 위험 통계 화면에서는 다음을 수행할 수 있습니다.

- 보안 위험 이름을 클릭하여 보안 위험에 대한 자세한 정보를 표시합니다.
- 엔드포인트 이름을 클릭하여 특정 엔드포인트의 전체 상태를 표시합니다.
- 엔드포인트 이름에 해당하는 **보기**를 클릭하여 해당 엔드포인트의 보안 위험 로그를 표시합니다.
- **초기화 횟수**를 클릭하여 각 테이블의 통계를 초기화합니다.

에이전트 업데이트 위젯

이 위젯은 보안 위험으로부터 OfficeScan 에이전트를 보호하는 구성 요소와 프로그램을 표시합니다.

업데이트가 필요한 OfficeScan 에이전트를 에이전트 트리에 나열하는 **에이전트 관리** 화면을 열려면 "오래됨" 수를 클릭합니다.

관리 위젯

관리 위젯은 OfficeScan 에이전트와 OfficeScan 서버의 연결 상태를 표시합니다.

사용 가능한 위젯:

- 에이전트-서버 연결 위젯 페이지 2-36

에이전트-서버 연결 위젯

이 위젯은 OfficeScan 서버와 모든 에이전트 간의 연결 상태를 보여 줍니다.

표시 아이콘( )을 클릭하여 테이블과 원형 차트 간에 전환할 수 있습니다.

에이전트 트리에 관련된 OfficeScan 에이전트를 나열하는 **에이전트 관리** 화면을 열려면 상태에 대한 수를 클릭합니다.

서버 마이그레이션 도구

OfficeScan에서 제공하는 서버 마이그레이션 도구를 사용하면 관리자가 이전 OfficeScan 버전에서 현재 버전으로 OfficeScan 설정을 복사할 수 있습니다. 서버 마이그레이션 도구는 다음 설정을 마이그레이션합니다.

기능	마이그레이션된 설정
에이전트 관리	• 수동 검색 설정* • 예약 검색 설정* • 실시간 검색 설정* • 지금 검색 설정* • 웹 검증 설정* • 동작 모니터링 설정* • 장치 제어 설정* • 데이터 손실 방지 설정* • 권한 및 기타 설정* • 추가 서비스 설정* • 스파이웨어/그레이웨어 승인된 목록* **참고** • 서버 마이그레이션 도구는 수동 검색, 예약 검색, 실시간 검색 및 지금 검색에 대해 백업 디렉터리를 마이그레이션하지 않습니다. • 설정은 루트 및 도메인 수준 모두에서 구성을 그대로 유지합니다.
에이전트 그룹화	모든 설정 **참고** Active Directory와 처음 동기화하고 나면 Active Directory 도메인 구조가 표시됩니다.
글로벌 에이전트 설정	모든 설정
엔드포인트 위치	• 위치 인식 설정 • 게이트웨이 IP 주소 및 MAC 목록

기능	마이그레이션된 설정
데이터 손실 방지	• 데이터 식별자 • 템플릿
방화벽	• 정책 • 프로필
로그 유지 관리	모든 설정
에이전트 업데이트 소스	• 에이전트 업데이트 소스 • 사용자 정의 업데이트 소스 목록
스마트 보호 소스	사용자 정의 스마트 보호 소스 목록
알림	• 일반 알림 설정 • 관리자 알림 설정 • 비상 발생 알림 설정 • 에이전트 알림 설정
프록시	모든 설정
비활성 에이전트	모든 설정
격리 보관 관리자	모든 설정
웹 콘솔	모든 설정
ofcscan.ini 설정	• [INI_CLIENT_INSTALLPATH_SECTION] WinNT_InstallPath • [INI_REESTABLISH_COMMUNICATION_SECTION]: 모든 설정
ofcserver.ini 설정	[INI_SERVER_DISK_THRESHOLD]: 모든 설정

참고

- 이 도구는 OfficeScan 서버의 OfficeScan 에이전트 목록을 백업하지 않고 도메인 구조만 백업합니다.
- OfficeScan 에이전트는 이전 버전의 OfficeScan 에이전트 서버에서 사용 가능한 기능만 마이그레이션합니다. 이전 서버에서 사용할 수 없는 기능의 경우 OfficeScan 에이전트는 기본 설정을 적용합니다.

서버 마이그레이션 도구 사용

참고

이 OfficeScan 버전은 OfficeScan 버전 10.6 SP3 이상에서의 마이그레이션을 지원합니다.

이전 OfficeScan 버전에는 최신 버전에서 제공되는 일부 설정이 포함되어 있지 않을 수 있습니다. OfficeScan에서는 이전 OfficeScan 서버 버전에서 마이그레이션되지 않은 기능에 자동으로 기본 설정을 적용합니다.

절차

1. OfficeScan XG 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin ₩Utility₩ServerMigrationTool로 이동합니다.
2. 서버 마이그레이션 도구를 소스 OfficeScan 서버 컴퓨터에 복사합니다.

   중요

   새 대상 서버에 맞게 모든 데이터의 포맷이 올바르게 지정되도록 하려면 소스 OfficeScan 서버 버전에서 OfficeScan XG 서버 마이그레이션 도구를 사용해야 합니다. OfficeScan XG은 이전 버전의 서버 마이그레이션 도구와는 호환되지 않습니다.

3. ServerMigrationTool.exe를 두 번 클릭하여 서버 마이그레이션 도구를 시작합니다.

   서버 마이그레이션 도구가 열립니다.

4. 소스 OfficeScan 서버의 설정을 내보내려면

a. **찾아보기** 단추를 사용하여 대상 폴더를 지정합니다.

참고
내보내기 패키지의 기본 이름은 OsceMigrate.zip입니다.

b. **내보내기**를 클릭합니다.

확인 메시지가 나타납니다.

c. 내보내기 패키지를 대상 OfficeScan 서버에 복사합니다.

5. 대상 OfficeScan 서버로 설정을 가져오려면

a. **찾아보기** 단추를 사용하여 내보내기 패키지를 찾습니다.

b. **가져오기**를 클릭합니다.

경고 메시지가 나타납니다.

c. **예**를 클릭하여 계속 진행합니다.

확인 메시지가 나타납니다.

6. 서버에 이전 OfficeScan 버전 설정이 모두 포함되었는지 확인합니다.

7. 이전 OfficeScan 에이전트를 새 서버로 이동합니다.

OfficeScan 에이전트 이동에 대한 자세한 내용은 다른 도메인 또는 OfficeScan 서버로 OfficeScan 에이전트 이동 페이지 2-66 또는 Agent Mover 페이지 15-22를 참조하십시오.

Active Directory 통합

OfficeScan을 Microsoft™ Active Directory™ 구조와 통합하면 OfficeScan 에이전트를 보다 효율적으로 관리하고, Active Directory 계정을 사용하여 웹 콘솔 권한을 할당하고, 보안 소프트웨어가 설치되지 않은 에이전트를 확인할 수 있습니다. 네트워크 도메인 내의 모든 사용자는 OfficeScan 콘솔에 대한 보안 액세스 권한을 가질 수 있습니다. 또한 다른 도메인의 사용자를 포함하여 특정 사용자에 대해 제한된 액세스를 구성할 수 있습니다. 인증 프로세스 및 암호화 키는 사용자에 대한 자격 증명 검증을 제공합니다.

Active Directory 통합을 통해 다음 기능을 완벽하게 이용할 수 있습니다.

- **사용자 정의 에이전트 그룹**: Active Directory 또는 IP 주소를 사용하여 수동으로 에이전트를 그룹화하고 OfficeScan 에이전트 트리의 도메인에 그룹화한 에이전트를 매핑합니다.

  자세한 내용은 자동 에이전트 그룹화 페이지 2-59를 참조하십시오.

- **관리되지 않는 엔드포인트**: OfficeScan 서버에 의해 관리되지 않는 네트워크의 엔드포인트가 회사의 보안 지침을 준수하는지 확인합니다.

  자세한 내용은 관리되지 않는 엔드포인트에 대한 보안 준수 페이지 15-68를 참조하십시오.

Active Directory 구조와 OfficeScan 서버를 수동으로 또는 주기적으로 동기화하여 데이터 일관성을 확보합니다.

자세한 내용은 Active Directory 도메인과 데이터 동기화 페이지 2-43를 참조하십시오.

Active Directory와 OfficeScan 통합

절차

1. **관리** > **Active Directory** > **Active Directory 통합**으로 이동합니다.
2. **Active Directory 도메인** 아래에서 Active Directory 도메인 이름을 지정합니다.
3. 지정된 Active Directory 도메인과 데이터를 동기화할 때 OfficeScan 서버에서 사용할 자격 증명을 지정합니다. 서버가 도메인의 일부가 아닌 경우 자격 증명은 필수 항목입니다. 그렇지 않으면 자격 증명은 선택 사항입니다. 이러한 자격 증명이 만료되지 않았는지 확인하십시오. 자격 증명이 만료되면 서버에서 데이터를 동기화할 수 없습니다.

   a. **도메인 자격 증명 지정**을 클릭합니다.

   b. 팝업 창이 열리면 사용자 이름과 암호를 입력합니다. 다음 형식 중 하나를 사용하여 사용자 이름을 지정할 수 있습니다.

- `도메인\사용자 이름:`
- `username@domain`

c. **저장**을 클릭합니다.

4. 도메인을 추가하려면 (+) 단추를 클릭합니다. 필요한 경우, 추가한 도메인에 대한 도메인 자격 증명을 지정합니다.

5. 도메인을 삭제하려면 (-) 단추를 클릭합니다.

6. 도메인 자격 증명을 지정한 경우 암호화 설정을 지정합니다. 하나의 보안 조치로서 OfficeScan은 지정한 도메인 자격 증명을 암호화한 후 데이터베이스에 저장합니다. OfficeScan에서는 데이터를 지정된 도메인과 동기화할 때 암호화 키를 사용하여 도메인 자격 증명의 암호를 해독합니다.

   a. **도메인 자격 증명에 대한 암호화 설정** 섹션으로 이동합니다.

   b. 128자 이내의 암호화 키를 입력합니다.

   c. 암호화 키를 저장할 파일을 지정합니다. .txt와 같은 일반적인 파일 포맷을 선택할 수 있습니다. 파일의 전체 경로와 이름(예: C:₩AD_Encryption₩EncryptionKey.txt)을 입력합니다.

경고!

파일이 제거되거나 파일 경로가 변경된 경우에는 OfficeScan에서 지정된 일부 도메인과 데이터를 동기화할 수 없습니다.

7. 다음 중 하나를 클릭합니다.

   - **저장**: 설정을 저장만 합니다. 데이터 동기화에는 네트워크 리소스가 소모될 수 있으므로 설정을 저장하기만 하고 나중에 한가한 시간에 동기화하도록 선택할 수 있습니다.
   - **저장 및 동기화**: 설정을 저장하고 Active Directory 도메인과 데이터를 동기화합니다.

8. 주기적인 동기화를 예약합니다. 자세한 내용은 Active Directory 도메인과 데이터 동기화 페이지 2-43를 참조하십시오.

Active Directory 도메인과 데이터 동기화

Active Directory 도메인과 데이터를 정기적으로 동기화하여 OfficeScan 에이전트 트리 구조를 최신 상태로 유지하고 관리되지 않는 에이전트를 쿼리합니다.

수동으로 Active Directory 도메인과 데이터 동기화

절차

1. **관리** > **Active Directory** > **Active Directory 통합**으로 이동합니다.
2. 도메인 자격 증명 및 암호화 설정이 변경되지 않았는지 확인합니다.
3. **저장 및 동기화**를 클릭합니다.

자동으로 Active Directory 도메인과 데이터 동기화

절차

1. **관리** > **Active Directory** > **예약 동기화**로 이동합니다.
2. **예약 Active Directory 동기화 사용**을 선택합니다.
3. 동기화 일정을 지정합니다.

   참고

   매일, 매주 및 매월 동기화할 경우 시간은 OfficeScan이 Active Directory와 OfficeScan 서버를 동기화하는 시간입니다.

4. **저장**을 클릭합니다.

OfficeScan 에이전트 트리

OfficeScan 에이전트 트리에서는 서버가 현재 관리하는 모든 에이전트를 도메인으로 그룹화하여 표시합니다. 에이전트를 도메인으로 그룹화하므로 동일한 구성을 동시에 구성 및 관리하고 도메인 구성원 모두에 적용할 수 있습니다.

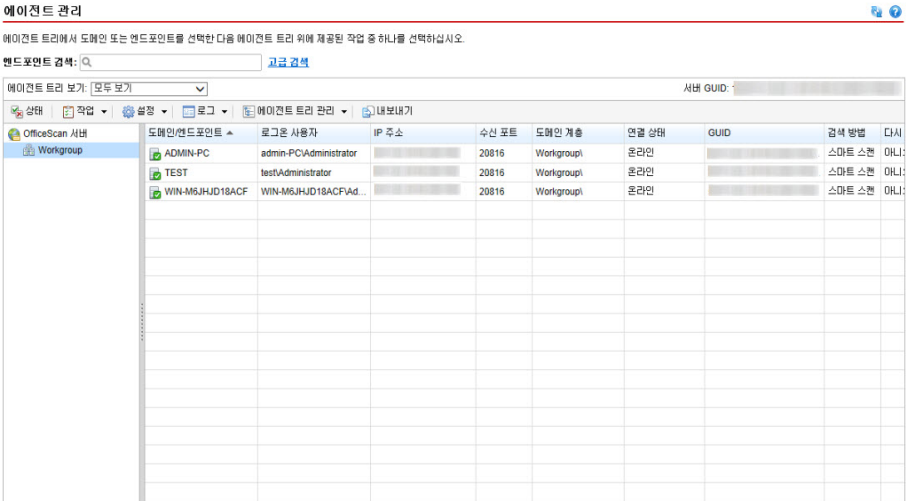


그림 2-5. OfficeScan 에이전트 트리

에이전트 연결 상태

OfficeScan 에이전트 연결 상태는 OfficeScan 서버가 OfficeScan 에이전트와 통신하는 방법에 따라 결정됩니다. 다음 표에서는 OfficeScan 에이전트에서 사용할 수 있는 서로 다른 연결 상태를 간략히 설명합니다.

표 2-8. OfficeScan 에이전트 연결 상태

상태	설명
온라인	OfficeScan 에이전트는 다음에 대한 양방향 통신을 위해 OfficeScan 서버에 연결할 수 있습니다. • 정책 설정 • 업데이트 • 검색 명령 • 의심스러운 개체 목록 동기화 • 샘플 제출 • 로그 제출
오프라인	OfficeScan 에이전트는 OfficeScan 서버 또는 Edge 릴레이 서버와 기능적으로 연결되어 있지 않습니다.
독립	OfficeScan 에이전트는 OfficeScan 서버에 연결할 수 있지만 통신은 제한적입니다. 독립 모드에 있는 동안: • OfficeScan 에이전트는 서버의 정책 설정을 적용하지 않습니다. • OfficeScan 에이전트는 서버의 검색 명령을 시작하지 않습니다. • OfficeScan 에이전트는 서버에 로그를 보내지 않습니다. OfficeScan 서버에 대한 기능적 연결을 사용할 수 있는 경우 구성 요소 업데이트 허용 또는 차단 권한을 가진 독립 에이전트를 구성할 수 있습니다. 최종 사용자는 독립 모드에서 에이전트에 대해 검색과 업데이트를 수동으로 시작할 수 있습니다.
오프 프레미스	OfficeScan 에이전트는 기업 네트워크 밖에 있으며 OfficeScan 서버에 직접 연결할 수 없습니다. 하지만 OfficeScan 에이전트는 다음을 위해 Edge 릴레이 서버에 연결할 수 있습니다. • 의심스러운 개체 목록 동기화 • 샘플 제출 • 로그 제출

에이전트 트리 아이콘

OfficeScan 에이전트 트리 아이콘은 OfficeScan에서 관리하는 엔드포인트의 유형 및 OfficeScan 에이전트의 상태를 나타내는 시각적 힌트를 제공합니다.

표 2-9. OfficeScan 에이전트 트리 아이콘

아이콘	설명
	도메인
	루트
	업데이트 에이전트
	표준 스캔 에이전트
	스마트 스캔을 사용할 수 있는 OfficeScan 에이전트
	스마트 스캔을 사용할 수 없는 OfficeScan 에이전트
	스마트 스캔을 사용할 수 있는 업데이트 에이전트
	스마트 스캔을 사용할 수 없는 업데이트 에이전트

에이전트 트리 일반 작업

다음은 에이전트 트리가 표시될 때 수행할 수 있는 일반 작업입니다.

절차

- 루트 도메인 아이콘( )을 클릭하여 도메인 및 에이전트를 모두 선택합니다. 루트 도메인 아이콘을 선택한 후 에이전트 트리 위의 작업을 선택하면

설정을 구성하는 화면이 표시됩니다. 화면에 표시되는 다음 일반 옵션에서 선택합니다:

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

- 여러 개의 인접한 도메인 또는 에이전트를 선택하려면
  - 오른쪽 패널에서 첫 번째 도메인을 선택하고 Shift 키를 누른 채 범위의 마지막 도메인 또는 에이전트를 클릭합니다.
- 떨어져 있는 도메인 또는 에이전트를 여럿 선택하려면 오른쪽 패널에서 Ctrl 키를 누른 채 선택하려는 도메인 또는 에이전트를 클릭합니다.
- **엔드포인트 검색** 텍스트 상자에서 에이전트 이름을 지정하여 관리할 에이전트를 검색합니다.

  에이전트 트리에 결과 목록이 나타납니다. 추가 검색 옵션을 보려면 **고급 검색**을 클릭합니다.

  참고

  특정 에이전트를 검색할 때는 IPv6 또는 IPv4 주소를 지정할 수 없습니다. IPv4 또는 IPv6 주소로 검색하려면 고급 검색을 사용하십시오. 자세한 내용은 고급 검색 옵션 페이지 2-48를 참조하십시오.

- 도메인을 선택하면 에이전트 트리 테이블이 확장되어 도메인에 속한 에이전트와 각 에이전트 관련 정보가 포함된 모든 열이 표시됩니다. 관련 열 집합만 보려면 에이전트 트리 보기에서 항목을 선택합니다.
  - **모두 보기**: 모든 열을 표시합니다.
  - **업데이트 보기**: 모든 구성 요소 및 프로그램을 표시합니다.
  - **바이러스 백신 기능 보기**: 바이러스 백신 구성 요소를 표시합니다.
  - **Anti-spyware 보기**: Anti-spyware 구성 요소를 표시합니다.

- **데이터 보호 기능 보기**: 에이전트에 설치된 데이터 보호 모듈의 상태를 표시합니다.
- **방화벽 보기**: 방화벽 구성 요소를 표시합니다.
- **스마트 보호 기능 보기**: 에이전트(표준 또는 스마트 스캔) 및 스마트 보호 구성 요소에서 사용하는 검색 방법을 표시합니다.
- **업데이트 에이전트 보기**: OfficeScan 서버에서 관리하는 모든 업데이트 에이전트에 대한 정보를 표시합니다.
- **외부 에이전트 보기**: Edge 릴레이 서버에 보고하는 모든 에이전트에 대한 정보를 표시합니다.

- 열 이름을 클릭하여 열 정보를 기준으로 에이전트를 정렬합니다.
- 새로 고침 아이콘( )을 클릭하여 에이전트 트리를 새로 고칩니다.
- 에이전트 트리 아래에서 총 에이전트 수, 스마트 스캔 에이전트 수 및 표준 스캔 에이전트 수와 같은 에이전트 통계를 봅니다.

고급 검색 옵션

다음 기준에 따라 에이전트을(를) 검색합니다.

절차

- **기본 기준**: IP 주소, 운영 체제, 도메인, MAC 주소, 검색 방법, 웹 검증 상태 등 엔드포인트에 대한 기본 정보를 포함합니다.
  - IPv4 세그먼트로 검색하려면 첫 번째 8진수로 시작하는 IP 주소 부분이 필요합니다. 이 항목으로 검색하면 해당 항목을 포함하는 IP 주소를 가진 엔드포인트가 모두 반환됩니다. 예를 들어, 10.5를 입력하면 IP 주소 범위 10.5.0.0~10.5.255.255에 해당하는 모든 컴퓨터를 반환합니다.
  - IPv6 주소 범위로 검색하려면 접두사와 길이가 필요합니다.
  - MAC 주소로 검색하려면 16진수로 표시된 MAC 주소 범위(예: 000A1B123C12)가 필요합니다.

- **구성 요소 버전**: 구성 요소 이름 옆에 있는 확인란을 선택하고 **다음보다 이전 버전** 또는 **다음을 포함한 이전 버전**을 선택하여 기준을 좁힌 후 버전 번호를 입력합니다. 현재 버전 번호가 기본적으로 표시됩니다.
- **상태**: 에이전트 설정 포함
- 검색 기준을 지정한 후 **검색**을 클릭합니다. 기준을 충족하는 엔드포인트 이름 목록이 에이전트 트리에 나타납니다.

에이전트 트리 특정 작업

웹 콘솔에서 특정 화면에 액세스할 때 에이전트 트리가 표시됩니다. 에이전트 트리 위에는 액세스한 화면과 관련된 메뉴 항목이 있습니다. 이러한 메뉴 항목을 통해 에이전트 설정을 구성하거나 에이전트 작업을 시작하는 것과 같은 특정 작업을 수행할 수 있습니다. 작업을 수행하려면 먼저 작업 대상을 선택한 후 메뉴 항목을 선택해야 합니다.

다음 화면에 에이전트 트리가 표시됩니다.

- 에이전트 관리 화면 페이지 2-49
- 바이러스 사전 방역 화면 페이지 2-53
- 에이전트 선택 화면 페이지 2-53
- 롤백 화면 페이지 2-54
- 보안 위험 로그 화면 페이지 2-55

에이전트 관리 화면

이 화면을 보려면 **에이전트** > **에이전트 관리**로 이동합니다.

에이전트 관리 화면에서는 일반 에이전트 설정을 관리하고 특정 에이전트에 대한 상태 정보(예: **로그온 사용자**, **IP 주소** 및 **연결 상태**)를 볼 수 있습니다.

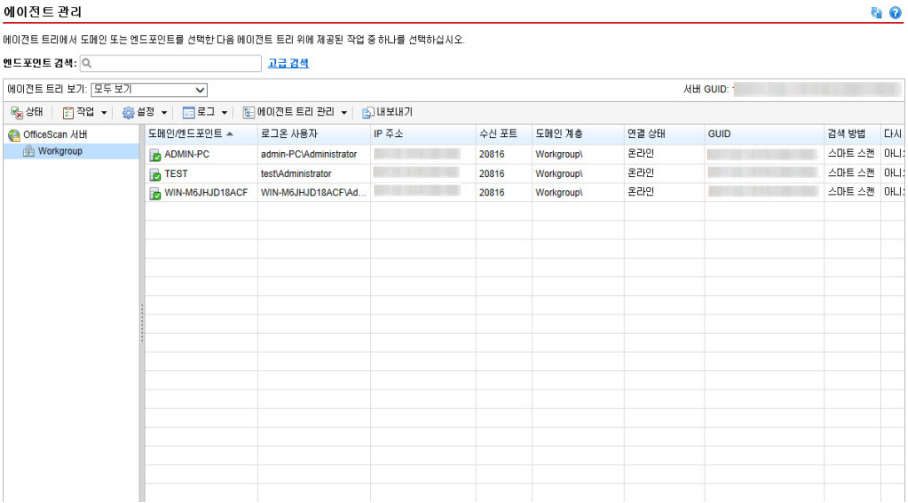


그림 2-6. 에이전트 관리 화면

다음 표에는 수행할 수 있는 작업이 나와 있습니다.

표 2-10. 에이전트 관리 작업

메뉴 단추	작업
상태	자세한 에이전트 정보를 봅니다. 자세한 내용은 OfficeScan 에이전트 정보 보기 페이지 15-52를 참조하십시오.
작업	• 에이전트 엔드포인트에서 지금 검색을 실행합니다. 자세한 내용은 지금 검색 시작 페이지 7-25를 참조하십시오. • 에이전트를 제거합니다. 자세한 내용은 웹 콘솔에서 OfficeScan 에이전트 제거 페이지 5-71를 참조하십시오. • 의심스러운 파일로 탐지된 항목을 복원합니다. 자세한 내용은 격리된 파일 복원 페이지 7-43을 참조하십시오. • 스파이웨어/그레이웨어 구성 요소를 복원합니다. 자세한 내용은 스파이웨어/그레이웨어 복원 페이지 7-50를 참조하십시오.

메뉴 단추	작업

설정	• 검색 설정을 구성합니다. 자세한 내용은 다음 항목을 참조하십시오.
	  • 검색 방법 유형 페이지 7-8
	  • 수동 검색 페이지 7-18
	  • 실시간 검색 페이지 7-15
	  • 예약 검색 페이지 7-20
	  • 지금 검색 페이지 7-22
	• 웹 검증 설정을 구성합니다. 자세한 내용은 웹 검증 정책 페이지 12-5를 참조하십시오.
	• 머신러닝 설정을 구성합니다. 자세한 내용은 머신러닝 설정 구성 페이지 8-3를 참조하십시오.
	• 의심스러운 연결 설정을 구성합니다. 자세한 내용은 의심스러운 연결 설정 구성 페이지 8-7를 참조하십시오.
	• 동작 모니터링 설정을 구성합니다. 자세한 내용은 동작 모니터링 페이지 9-2를 참조하십시오.
	• 장치 제어 설정을 구성합니다. 자세한 내용은 장치 제어 페이지 10-2를 참조하십시오.
	• 데이터 손실 방지 정책을 구성합니다. 자세한 내용은 데이터 손실 방지 정책 구성 페이지 11-45를 참조하십시오.
	• 에이전트를 업데이트 에이전트로 할당합니다. 자세한 내용은 업데이트 에이전트 구성 페이지 6-52를 참조하십시오.
	• 에이전트 권한 및 기타 설정을 구성합니다. 자세한 내용은 에이전트 권한 및 기타 설정 구성 페이지 15-88를 참조하십시오.
	• OfficeScan 에이전트 서비스를 사용하거나 사용하지 않도록 설정합니다. 자세한 내용은 OfficeScan 에이전트 서비스 페이지 15-7를 참조하십시오.
	• 스파이웨어/그레이웨어 승인된 목록을 구성합니다. 자세한 내용은 스파이웨어/그레이웨어 승인된 목록 페이지 7-48를 참조하십시오.
	• 신뢰할 수 있는 프로그램 목록을 구성합니다. 자세한 내용은 신뢰할 수 있는 프로그램 목록 구성 페이지 7-52를 참조하십시오.
	• 에이전트 설정을 가져오거나 내보냅니다. 자세한 내용은 에이전트 설정 가져오기 및 내보내기 페이지 15-53를 참조하십시오.

메뉴 단추	작업
로그	다음 로그를 봅니다. • 바이러스/악성 프로그램 로그(자세한 내용은 바이러스/악성 프로그램 로그 보기 페이지 7-89 참조). • 스파이웨어/그레이웨어 로그(자세한 내용은 스파이웨어/그레이웨어 로그 보기 페이지 7-96 참조) • 방화벽 로그(자세한 내용은 방화벽 로그 페이지 13-28 참조) • 웹 검증 로그(자세한 내용은 웹 위협 로그 페이지 12-20 참조) • 의심스러운 연결 로그(자세한 내용은 의심스러운 연결 로그 보기 페이지 8-13 참조) • 의심스러운 파일 로그(자세한 내용은 의심스러운 파일 로그 보기 페이지 7-100 참조) • C&C 콜백 로그(자세한 내용은 C&C 콜백 로그 보기 페이지 12-22 참조) • 동작 모니터링 로그(자세한 내용은 동작 모니터링 로그 페이지 9-17 참조) • 머신러닝 로그(자세한 내용은 머신러닝 로그 보기 페이지 8-10 참조) • 장치 제어 로그(자세한 내용은 장치 제어 로그 페이지 10-18 참조) • DLP 로그(자세한 내용은 데이터 손실 방지 로그 페이지 11-55 참조) • 검색 작업 로그(자세한 내용은 검색 작업 로그 보기 페이지 7-102 참조) 로그를 삭제합니다. 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.
에이전트 트리 관리	에이전트 트리를 관리합니다. 자세한 내용은 에이전트 그룹화 작업 페이지 2-63를 참조하십시오.
내보내기	에이전트 목록을 쉼표로 구분된 값(.csv) 파일로 내보냅니다.

바이러스 사전 방역 화면

이 화면을 표시하려면 **에이전트** > **바이러스 사전 방역**으로 이동합니다.

바이러스 사전 방역 화면에서는 바이러스 사전 방역 설정을 지정하고 활성화할 수 있습니다. 자세한 내용은 보안 위험 바이러스 사전 방역 구성 페이지 7-107를 참조하십시오.

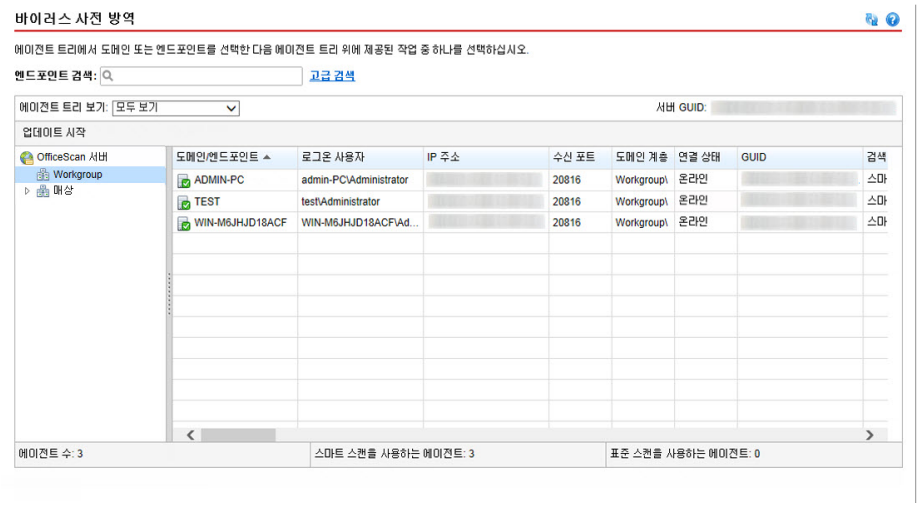


그림 2-7. 바이러스 사전 방역 화면

에이전트 선택 화면

이 화면을 보려면 **업데이트** > **에이전트** > **수동 업데이트**로 이동합니다. **수동으로 에이전트 선택**을 선택한 다음 **선택**을 클릭합니다.

에이전트 선택 화면에서 수동 업데이트를 시작할 수 있습니다. 자세한 내용은 OfficeScan 에이전트 수동 업데이트 페이지 6-42를 참조하십시오.

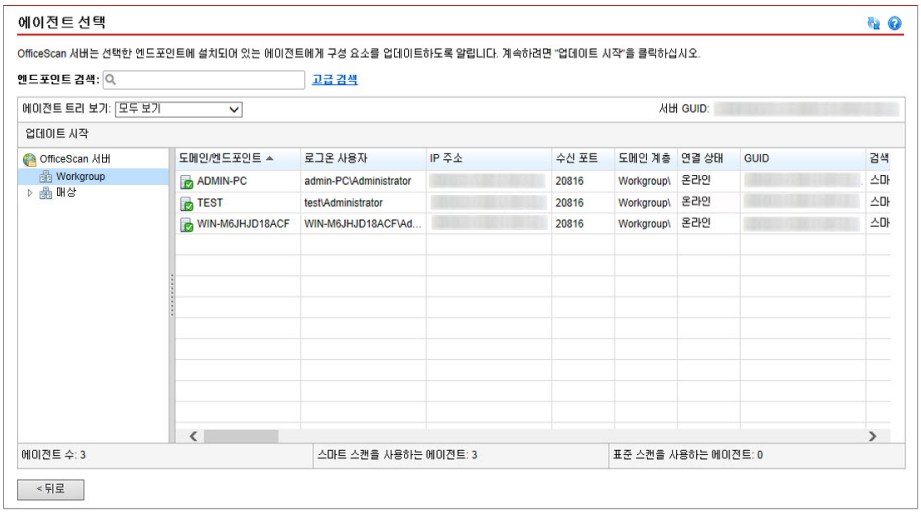


그림 2-8. 에이전트 선택 화면

롤백 화면

이 화면을 보려면 **업데이트** > **롤백**으로 이동합니다. **서버와 동기화**를 클릭합니다.

롤백 화면에서 에이전트 구성 요소를 롤백합니다. 자세한 내용은 OfficeScan 에이전트에 대한 구성 요소 롤백 페이지 6-49를 참조하십시오.

그림 2-9. 롤백 화면

보안 위험 로그 화면

이 화면을 보려면 **로그** > **에이전트** > **보안 위험**로 이동합니다.

보안 위험 로그 화면에서는 로그를 보고 관리할 수 있습니다.

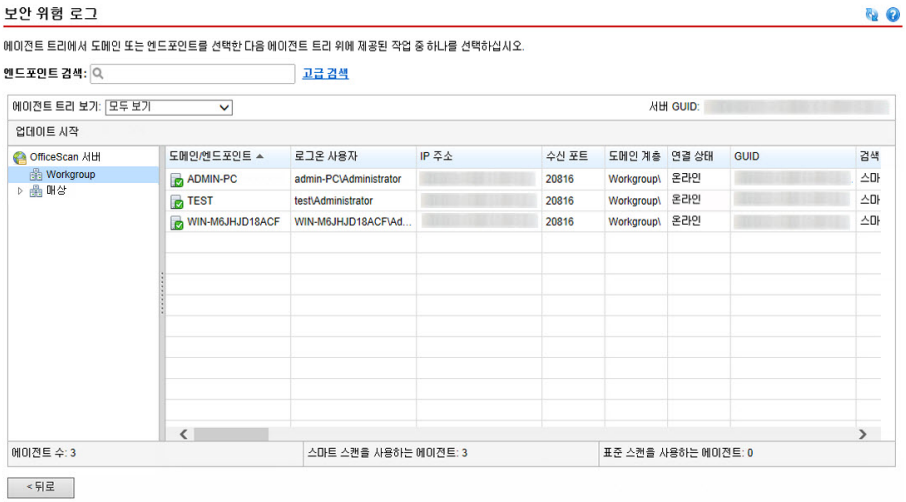


그림 2-10. 보안 위험 로그 화면

다음 작업을 수행합니다.

1. 에이전트에서 서버로 보내는 로그를 확인합니다. 자세한 내용은 다음을 참조하십시오.
   - 바이러스/악성 프로그램 로그 보기 페이지 7-89
   - 스파이웨어/그레이웨어 로그 보기 페이지 7-96
   - 방화벽 로그 보기 페이지 13-28
   - 웹 검증 로그 보기 페이지 12-21
   - 의심스러운 연결 로그 보기 페이지 8-13
   - 의심스러운 파일 로그 보기 페이지 7-100
   - C&C 콜백 로그 보기 페이지 12-22
   - 동작 모니터링 로그 보기 페이지 9-17

- 장치 제어 로그 보기 페이지 10-18
- 데이터 손실 방지 로그 보기 페이지 11-56

2. 로그를 삭제합니다. 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

OfficeScan 도메인

OfficeScan에서 도메인이란 동일한 구성을 공유하고 동일한 작업을 실행하는 에이전트 그룹을 말합니다. 에이전트를 도메인으로 그룹화하면 동일한 구성을 구성 및 관리하고 도메인 구성원 모두에 적용할 수 있습니다. 에이전트 그룹화에 대한 자세한 내용은 에이전트 그룹화 페이지 2-57를 참조하십시오.

에이전트 그룹화

에이전트 그룹화를 사용하여 OfficeScan 에이전트 트리에서 수동 또는 자동으로 도메인을 만들고 관리할 수 있습니다.

에이전트를 도메인으로 그룹화하는 방법은 두 가지입니다.

표 2-11. 에이전트 그룹화 방법

방법	에이전트 그룹화	설명
수동	• NetBIOS 도메인 • Active Directory 도메인 • DNS 도메인	수동 에이전트 그룹화의 경우에는 새로 설치한 에이전트가 속할 도메인을 정의합니다. 에이전트가 에이전트 트리에 표시되면 다른 도메인이나 OfficeScan 서버로 에이전트를 이동할 수 있습니다. 수동 에이전트 그룹화를 사용할 경우 에이전트 트리에서 도메인을 만들고 관리하고 제거할 수도 있습니다. 자세한 내용은 수동 에이전트 그룹화 페이지 2-58를 참조하십시오.

방법	에이전트 그룹화	설명
자동	사용자 정의 에이전트 그룹	자동 에이전트 그룹화의 경우에는 규칙을 사용하여 에이전트 트리에서 에이전트를 정렬합니다. 규칙을 정의한 후 에이전트 트리에 액세스하여 에이전트를 수동으로 정렬할 수도 있고, OfficeScan에서 특정 이벤트가 발생할 때나 예약한 간격에 자동으로 에이전트를 정렬하도록 할 수도 있습니다. 자세한 내용은 자동 에이전트 그룹화 페이지 2-59를 참조하십시오.

수동 에이전트 그룹화

OfficeScan은 에이전트를 새로 설치할 때만 이 설정을 사용합니다. 설치 프로그램은 대상 엔드포인트가 속한 네트워크 도메인을 확인합니다. 도메인 이름이 에이전트 트리에 이미 있는 경우, OfficeScan에서는 대상 엔드포인트의 에이전트를 해당 도메인 아래에 그룹화하고 도메인에 대해 구성된 설정을 적용합니다. 도메인 이름이 없는 경우, OfficeScan에서는 도메인을 에이전트 트리에 추가하고 에이전트를 해당 도메인 아래에 그룹화한 후 루트 설정을 도메인 및 에이전트에 적용합니다.

수동 에이전트 그룹화 구성

절차

1. **에이전트** > **에이전트 그룹화**로 이동합니다.
2. 에이전트 그룹화 방법을 지정합니다.
   - NetBIOS 도메인
   - Active Directory 도메인
   - DNS 도메인
3. **저장**을 클릭합니다.

다음 작업

다음 작업을 수행하여 도메인과 해당 도메인 아래에 그룹화된 에이전트를 관리합니다.

- 도메인 추가
- 도메인 또는 에이전트 삭제
- 도메인 이름 변경
- 단일 에이전트를 다른 도메인으로 이동

자세한 내용은 에이전트 그룹화 작업 페이지 2-63를 참조하십시오.

자동 에이전트 그룹화

자동 에이전트 그룹화에서는 IP 주소 또는 Active Directory 도메인으로 정의된 규칙을 사용합니다. 규칙에서 IP 주소 또는 IP 주소 범위를 정의하는 경우 OfficeScan 서버는 IP 주소가 일치하는 에이전트를 에이전트 트리의 특정 도메인으로 그룹화합니다. 마찬가지로, 규칙에서 Active Directory 도메인을 하나 이상 정의하는 경우 OfficeScan 서버는 특정 Active Directory 도메인에 속한 에이전트를 에이전트 트리의 특정 도메인으로 그룹화합니다.

에이전트에서는 규칙을 한 번에 하나만 적용합니다. 에이전트가 규칙을 두 개 이상 충족할 경우 우선 순위가 가장 높은 규칙이 적용되도록 규칙의 우선 순위를 지정하십시오.

자동 에이전트 그룹화 구성

절차

1. **에이전트** > **에이전트 그룹화**로 이동합니다.
2. **에이전트 그룹화** 섹션으로 이동하고 **기존 OfficeScan 에이전트에 대한 사용자 정의 에이전트 그룹 만들기**를 선택합니다.
3. **자동 에이전트 그룹화** 섹션으로 이동합니다.
4. 규칙 만들기를 시작하려면 **추가**를 클릭한 다음 **Active Directory** 또는 **IP 주소**를 선택합니다.

- **Active Directory**를 선택한 경우 Active Directory 도메인을 통해 에이전트 그룹화 규칙 정의 페이지 2-61에서 구성 지침을 참조하십시오.
- **IP 주소**를 선택한 경우 IP 주소를 통해 에이전트 그룹화 규칙 정의 페이지 2-62에서 구성 지침을 참조하십시오.

5. 둘 이상의 규칙을 만든 경우 다음 단계를 수행하여 규칙의 우선 순위를 지정합니다.
   a. 규칙을 선택합니다.
   b. **그룹 우선 순위** 열 아래의 화살표를 클릭하여 규칙을 목록에서 위 또는 아래로 이동합니다. 해당 규칙의 ID 번호가 새 위치를 반영하도록 변경됩니다.
6. 에이전트를 정렬하는 동안 규칙을 사용하려면
   a. 사용할 규칙의 확인란을 선택합니다.
   b. **상태** 컨트롤을 **설정**으로 전환하여 규칙을 사용하도록 설정합니다.

참고

규칙의 확인란을 선택하지 않거나 규칙을 사용하지 않도록 설정한 경우에는 에이전트 트리에서 클라이언트를 정렬할 때 규칙이 사용되지 않습니다. 예를 들어 규칙에서 에이전트를 새 도메인으로 이동하도록 지정한 경우 에이전트가 이동하지 않고 현재 도메인에 그대로 있습니다.

---

7. **예약된 도메인 만들기** 섹션에서 정렬 일정을 지정합니다.
   a. **예약된 도메인 만들기 사용**을 선택합니다.
   b. **예약된 도메인 만들기**에서 일정을 지정합니다.
8. 다음 옵션 중에서 선택합니다.
   - **지금 저장 및 도메인 만들기**: IP 주소를 통해 에이전트 그룹화 규칙 정의 페이지 2-62 7단계 또는 Active Directory 도메인을 통해 에이전트 그룹화 규칙 정의 페이지 2-61 7단계에서 새 도메인을 지정한 경우 이 옵션을 선택합니다.
   - **저장**: 새 도메인을 지정하지 않았거나 에이전트 정렬을 실행할 때만 새 도메인을 만들려는 경우 이 옵션을 선택합니다.

참고

이 단계를 완료한 후 에이전트 정렬이 시작되지 않습니다.

Active Directory 도메인을 통해 에이전트 그룹화 규칙 정의

아래 절차의 단계를 수행하기 전에 Active Directory 통합 설정을 구성했는지 확인하십시오. 자세한 내용은 Active Directory 통합 페이지 2-40를 참조하십시오.

절차

1. **에이전트** > **에이전트 그룹화**로 이동합니다.
2. **에이전트 그룹화** 섹션으로 이동하고 **기존 OfficeScan 에이전트에 대한 사용자 정의 에이전트 그룹 만들기**를 선택합니다.
3. **자동 에이전트 그룹화** 섹션으로 이동합니다.
4. **추가**를 클릭한 다음 **Active Directory**를 선택합니다.

   새 화면이 나타납니다.
5. **그룹화 사용**을 선택합니다.
6. 규칙 이름을 지정합니다.
7. **ctive Directory 소스**, 아래에서 Active Directory 도메인 또는 하위 도메인을 선택합니다.
8. **에이전트 트리** 아래에서 Active Directory 도메인을 매핑할 기존 OfficeScan 도메인을 선택합니다. 원하는 OfficeScan 도메인이 없는 경우 다음 단계를 수행합니다.

   a. 특정 OfficeScan 도메인 위에 마우스를 놓고 도메인 추가 아이콘(+)을 클릭합니다.

   b. 제공된 입력란에 도메인 이름을 입력합니다.

   c. 입력란 옆의 확인 표시를 클릭합니다. 새 도메인이 추가되고 자동으로 선택됩니다.

9. (선택 사항) **Active Directory 구조를 OfficeScan 에이전트 트리에 복제**를 선택합니다. 이 옵션은 선택한 Active Directory 도메인의 계층을 선택한 OfficeScan 도메인에 복제합니다.

10. **저장**을 클릭합니다.

IP 주소를 통해 에이전트 그룹화 규칙 정의

네트워크 IP 주소로 사용자 정의 에이전트 그룹을 만들어 에이전트을(를) OfficeScan 에이전트 트리에서 정렬합니다. 이 기능을 통해 관리자는 에이전트를 OfficeScan 서버에 등록하기 전에 OfficeScan 에이전트 트리 구조를 정렬할 수 있습니다.

절차

1. **에이전트** > **에이전트 그룹화**로 이동합니다.

2. **에이전트 그룹화** 섹션으로 이동하고 **기존 OfficeScan 에이전트에 대한 사용자 정의 에이전트 그룹 만들기**를 선택합니다.

3. **자동 에이전트 그룹화** 섹션으로 이동합니다.

4. **추가**를 클릭한 다음 **IP 주소**를 선택합니다.

   새 화면이 나타납니다.

5. **그룹화 사용**을 선택합니다.

6. 그룹화 이름을 지정합니다.

7. 다음 중 하나를 지정합니다.

   - 단일 IPv4 또는 IPv6 주소
   - IPv4 주소 범위
   - IPv6 접두사 및 길이

참고

이중 스택 에이전트의 IPv4 및 IPv6 주소가 별개의 두 에이전트 그룹에 속한 경우 이 에이전트는 IPv6 그룹에서 그룹화됩니다. 에이전트의 호스트 컴퓨터에서 IPv6을 사용할 수 없는 경우 이 에이전트는 IPv4 그룹으로 이동합니다.

8. IP 주소 또는 IP 주소 범위가 매핑될 OfficeScan 도메인을 선택합니다. 도메인이 존재하지 않은 경우 다음을 수행합니다.

   a. 에이전트 트리 위에 마우스를 놓고 도메인 추가 아이콘을 클릭합니다.

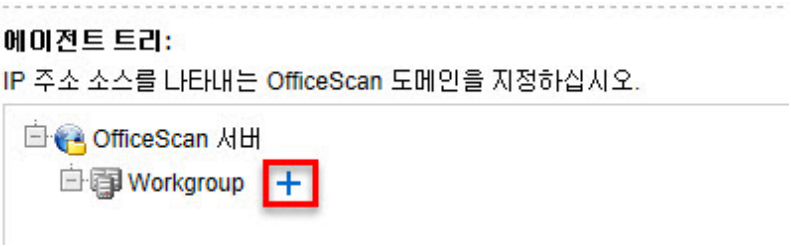


그림 2-11. 도메인 추가 아이콘

   b. 제공된 입력란에 도메인을 입력합니다.

   c. 입력란 옆의 확인 표시를 클릭합니다. 새 도메인이 추가되고 자동으로 선택됩니다.

9. **저장**을 클릭합니다.

에이전트 그룹화 작업

도메인에서 에이전트를 그룹화하는 경우 다음 작업을 수행할 수 있습니다.

- 도메인을 추가합니다. 자세한 내용은 도메인 추가 페이지 2-64를 참조하십시오.
- 도메인 또는 에이전트를 삭제합니다. 자세한 내용은 도메인 또는 에이전트 삭제 페이지 2-64를 참조하십시오.
- 도메인 이름을 변경합니다. 자세한 내용은 도메인 이름 변경 페이지 2-65를 참조하십시오.

- 단일 에이전트를 다른 도메인 또는 다른 OfficeScan 서버로 이동합니다. 자세한 내용은 다른 도메인 또는 OfficeScan 서버로 OfficeScan 에이전트 이동 페이지 2-66를 참조하십시오.

도메인 추가

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. **에이전트 트리 관리** > **도메인 추가**를 클릭합니다.
3. 추가할 도메인의 이름을 입력합니다.
4. **추가**를 클릭합니다.

   에이전트 트리에 새 도메인이 나타납니다.
5. (선택 사항) 하위 도메인을 만듭니다.
   a. 상위 도메인을 선택합니다.
   b. **에이전트 트리 관리** > **도메인 추가**를 클릭합니다.
   c. 하위 도메인 이름을 입력합니다.

도메인 또는 에이전트 삭제

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 다음을 선택합니다.
   - 하나 이상의 도메인
   - 도메인에 속한 에이전트 하나 이상 또는 모두
3. **에이전트 트리 관리** > **도메인/에이전트 제거**를 클릭합니다.

4. 비어 있는 도메인을 삭제하려면 **도메인/에이전트 제거**를 클릭합니다. 도메인에 에이전트가 있는 경우 **도메인/에이전트 제거**를 클릭하면 다음에 에이전트가 OfficeScan 서버에 연결할 때 OfficeScan 서버에서 도메인을 다시 만들어 해당 도메인 아래에 모든 에이전트를 그룹화합니다. 도메인을 삭제하기 전에 다음 작업을 수행할 수 있습니다.

   a. 에이전트를 다른 도메인으로 이동합니다. 에이전트를 다른 도메인으로 이동하려면 해당 에이전트를 대상 도메인으로 끌어 놓습니다.

   b. 모든 에이전트를 삭제합니다.

5. 단일 에이전트를 삭제하려면 **도메인/에이전트 제거**를 클릭합니다.

참고

에이전트 트리에서 에이전트를 삭제하더라도 에이전트 엔드포인트에서 OfficeScan 에이전트가 제거되지는 않습니다. OfficeScan 에이전트는 구성 요소 업데이트 등과 같이 서버와 상관없는 작업을 계속 수행할 수 있습니다. 그러나 서버에서 에이전트의 존재를 인식하지 못하므로 에이전트에 구성을 배포하거나 알림을 보낼 수 없습니다.

도메인 이름 변경

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 도메인을 선택합니다.
3. **에이전트 트리 관리** > **도메인 추가**를 클릭합니다.
4. 도메인의 새 이름을 입력합니다.
5. **파일명 변경**을 클릭합니다.

   에이전트 트리에 새 도메인 이름이 나타납니다.

다른 도메인 또는 OfficeScan 서버로 OfficeScan 에이전트 이동

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 에이전트를 하나 이상 또는 모두 선택합니다.
3. **에이전트 트리 관리** > **에이전트 이동**을 클릭합니다.
4. 에이전트를 다른 도메인으로 이동하려면
   - **선택한 에이전트를 다른 도메인으로 이동**을 선택합니다.
   - 도메인을 선택합니다.
   - (선택 사항) 새 도메인의 설정을 에이전트에 적용합니다.

   팁
   에이전트 트리에서 에이전트를 다른 도메인으로 끌어다 놓을 수도 있습니다.
5. 에이전트를 다른 OfficeScan 서버로 이동하려면
   - **선택한 에이전트를 다른 OfficeScan 서버로 이동**을 선택합니다.
   - 서버 이름 또는 IPv4/IPv6 주소와 HTTP 포트 번호를 입력합니다.
6. **이동**을 클릭합니다.

장 3

데이터 보호 시작

이 장에서는 데이터 보호 모듈을 설치하고 활성화 방법을 설명합니다.

다음과 같은 항목이 포함됩니다.

- 데이터 보호 설치 페이지 3-2
- 데이터 보호 라이선스 페이지 3-4
- OfficeScan 에이전트에 데이터 보호 배포 페이지 3-6
- Forensic 폴더 및 DLP 데이터베이스 페이지 3-8
- 데이터 보호 제거 페이지 3-14

데이터 보호 설치

데이터 보호 모듈에는 다음 기능이 포함되어 있습니다.

- **DLP(데이터 손실 방지)**: 디지털 자산의 무단 전송을 방지합니다.
- **장치 제어**: 외부 장치에 대한 액세스 규범화

참고

OfficeScan 정품에는 USB 저장 장치와 같은 일반적으로 사용되는 장치에 대한 액세스를 규범화하는 장치 제어 기능이 있습니다. 데이터 보호 모듈의 일부인 장치 제어는 모니터링되는 장치 범위를 확장합니다. 모니터링되는 장치 목록은 장치 제어 페이지 10-2를 참조하십시오.

데이터 손실 방지 및 장치 제어는 OfficeScan의 기본 기능이지만 별도로 라이선스가 부여됩니다. OfficeScan 서버를 설치하면 이러한 기능이 제공되지만 기능이 작동하지 않으며 에이전트에 배포할 수도 없습니다. 데이터 보호를 설치한다는 것은 액티브업데이트 서버 또는 사용자 지정 업데이트 소스(설정된 경우)에서 파일을 다운로드하는 것을 의미합니다. 이 파일이 OfficeScan 서버에 통합되면 데이터 보호 라이선스를 활성화하여 전체 기능을 사용할 수 있습니다. 설치 및 활성화는 **Plug-in Manager**에서 수행됩니다.

중요

독립 Trend Micro 데이터 손실 방지 소프트웨어를 이미 설치하고 엔드포인트에서 실행 중인 경우에는 데이터 보호 모듈을 설치할 필요가 없습니다.

데이터 보호 설치

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**를 클릭합니다.
2. **Plug-in Manager** 화면에서 **OfficeScan 데이터 보호** 섹션으로 이동하여 **다운로드**를 클릭합니다.

   다운로드할 파일의 크기가 **다운로드** 단추 옆에 표시됩니다.

Plug-in Manager는 다운로드한 파일을 <서버 설치 폴더>₩PCCSRV ₩Download₩Product에 저장합니다.

참고

Plug-in Manager에서 파일을 다운로드할 수 없는 경우 24시간 후에 자동으로 다시 다운로드됩니다. 파일을 다운로드하도록 Plug-in Manager를 수동으로 트리거하려면 Microsoft Management Console에서 OfficeScan Plug-in Manager 서비스를 다시 시작하십시오.

3. 다운로드 진행률을 확인합니다.

   다운로드하는 동안 다른 화면으로 이동할 수도 있습니다.

   파일을 다운로드하는 동안 문제가 발생한 경우 OfficeScan 웹 콘솔에서 서버 업데이트 로그를 확인합니다. 기본 메뉴에서 **로그** > **서버 업데이트**를 클릭합니다.

   Plug-in Manager가 파일을 다운로드한 후 OfficeScan 데이터 보호 기능이 새 화면에 표시됩니다.

참고

OfficeScan 데이터 보호 기능이 표시되지 않는 경우 Plug-in Manager 문제 해결 페이지 17-12에서 원인과 해결 방법을 확인하십시오.

4. OfficeScan 데이터 보호 기능을 즉시 설치하려면 **지금 설치**를 클릭하고, 나중에 설치하려면 다음을 수행합니다.

   a. **나중에 설치**를 클릭합니다.

   b. **Plug-in Manager** 화면을 엽니다.

   c. **OfficeScan 데이터 보호** 섹션으로 이동하여 **설치**를 클릭합니다.

5. 사용권 계약 내용을 읽고 **동의**를 클릭하여 조건에 동의합니다.

   설치가 시작됩니다.

6. 설치 진행률을 모니터링합니다. 설치 후 OfficeScan 데이터 보호 버전이 표시됩니다.

데이터 보호 라이선스

Plug-in Manager에서 데이터 보호 라이선스를 보고 활성화하고 갱신할 수 있습니다.

Trend Micro에서 정품 인증 코드를 받아 이 코드를 사용하여 라이선스를 활성화할 수 있습니다.

Plug-in 프로그램 라이선스 정품 인증

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **프로그램 관리**를 클릭합니다.

   제품 라이선스 새 정품 인증 코드 화면이 나타납니다.
3. 텍스트 필드에 정품 인증 코드를 입력하거나 복사하여 붙여 넣습니다.
4. **저장**을 클릭합니다.

   솔루션은 콘솔이 나타납니다.

라이선스 정보 보기 및 갱신

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **프로그램 관리**를 클릭합니다.
3. **라이선스 정보 보기**를 클릭하여 Trend Micro 웹 사이트에서 현재 라이선스에 대한 정보를 확인합니다.

4. 화면이 열리면 다음 라이선스 정보를 확인합니다.

옵션	설명
상태	"정품 인증됨", "정품 인증되지 않음" 또는 "만료됨"이 표시됩니다.
버전	"정식" 또는 "평가판" 버전이 표시됩니다. **참고** 정식 버전과 평가판이 둘 다 활성화된 경우에는 "정식"으로만 표시됩니다.
사용자 수	Plug-in 프로그램에서 관리할 수 있는 엔드포인트 수가 표시됩니다.
라이선스 만료 날짜	Plug-in 프로그램에 여러 개의 라이선스가 있는 경우 가장 늦은 만료일이 표시됩니다. 예를 들어, 라이선스 만료일이 2011/12/31 및 2011/06/30인 경우 2011/12/31이 표시됩니다.
정품 인증 코드	정품 인증 코드가 표시됩니다.
미리 알림	현재 라이선스 버전에 따라 플러그인에서는 유예 기간 중(정식 버전에만 해당) 또는 라이선스가 만료된 경우 라이선스 만료일에 대한 미리 알림을 표시합니다.

참고

유예 기간은 지역에 따라 다릅니다. Trend Micro 대리점에서 Plug-in 프로그램의 유예 기간을 확인하십시오.

5. 최신 라이선스 정보로 화면을 업데이트하려면 **정보 업데이트**를 클릭합니다.

6. **새 정품 인증 코드**를 클릭하여 **제품 라이선스 새 정품 인증 코드** 화면을 엽니다.

   자세한 내용은 Plug-in 프로그램 라이선스 정품 인증 페이지 3-4를 참조하십시오.

OfficeScan 에이전트에 데이터 보호 배포

데이터 보호 모듈은 해당 라이선스를 활성화한 후 OfficeScan 에이전트에 배포합니다. 배포하면 OfficeScan 에이전트에서 데이터 손실 방지 및 장치 제어를 사용할 수 있습니다.

중요

- Windows Server 2003, Windows Server 2008 및 Windows Server 2012에서는 호스트 컴퓨터의 성능 저하를 방지하기 위해 기본적으로 이 모듈이 사용하지 않도록 설정됩니다. 모듈을 사용하려면 시스템 성능을 지속적으로 모니터링하고 성능 저하를 발견한 경우 필요한 조치를 취하십시오.

  웹 콘솔에서 모듈을 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 OfficeScan 에이전트 서비스 페이지 15-7를 참조하십시오.

- Trend Micro 데이터 손실 방지 소프트웨어가 엔드포인트에 이미 있는 경우 OfficeScan에서는 이 소프트웨어를 데이터 보호 모듈로 대체하지 않습니다.
- 온라인 에이전트는 데이터 보호 모듈을 즉시 설치합니다. 오프라인 및 독립 에이전트는 OfficeScan 서버에 다시 연결한 후에 모듈을 설치합니다.
- 데이터 손실 방지 드라이버 설치를 마치려면 컴퓨터를 다시 시작해야 합니다. 사용자에게 다시 시작해야 함을 미리 알려 주십시오.
- Trend Micro에서는 배포 문제를 해결하는 데 도움이 되도록 디버그 로깅을 사용할 것을 권장합니다. 자세한 내용은 데이터 보호 모듈에 대한 디버그 로깅 사용 페이지 11-61를 참조하십시오.

OfficeScan 에이전트에 데이터 보호 모듈 배포

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 다음 작업을 수행할 수 있습니다.
   - 루트 도메인 아이콘( )을 클릭하여 기존 및 이후 에이전트 모두에 모듈을 배포합니다.

- 특정 도메인을 선택하여 해당 도메인에 속한 기존 및 이후 에이전트 모두에 모듈을 배포합니다.
- 특정 에이전트를 선택하여 해당 에이전트에만 모듈을 배포합니다.

3. 두 가지 방법 중 하나로 모듈을 배포합니다.
   - **설정** > **DLP 설정**을 클릭합니다.
   - **설정** > **장치 제어 설정**을 클릭합니다.

   참고

   설정 > **DLP 설정**을 통해 배포하는 경우 데이터 보호 모듈이 성공적으로 배포되면 데이터 손실 방지 드라이버가 설치됩니다. 드라이버가 설치되면 엔드포인트를 다시 시작하여 드라이버 설치를 완료하라는 메시지가 표시됩니다.

   메시지가 표시되지 않으면 드라이버를 설치하는 데 문제가 발생했을 수 있습니다. 디버그 로깅을 사용하도록 설정한 경우 디버그 로그에서 드라이브 설치 문제에 대한 자세한 내용을 확인합니다.

4. 모듈이 설치되지 않은 에이전트 수를 나타내는 메시지가 표시됩니다. **예**를 클릭하여 배포를 시작합니다.

   참고

   아니요를 클릭하거나 에이전트 하나 이상에 모듈이 배포되지 않은 경우 **설정** > **DLP 설정** 또는 **설정** > **장치 제어 설정**을 다시 클릭하면 같은 메시지가 표시됩니다.

   OfficeScan 에이전트가 서버에서 모듈을 다운로드하기 시작합니다.

5. 모듈이 에이전트에 배포되었는지 확인합니다.
   a. 에이전트 트리에서 도메인을 선택합니다.
   b. 에이전트 트리 보기에서 **데이터 보호 기능 보기** 또는 **모두 보기**를 선택합니다.
   c. **데이터 보호 상태** 열을 확인합니다. 배포 상태는 다음 중 하나일 수 있습니다.

- **실행**: 모듈이 성공적으로 배포되고 해당 기능이 사용하도록 설정되었습니다.
- **다시 시작해야 함**: 사용자가 컴퓨터를 다시 시작하지 않아 데이터 손실 방지 드라이버가 설치되지 않았습니다. 드라이버가 설치되지 않으면 데이터 손실 방지가 작동하지 않습니다.
- **중지됨**: 모듈에 대한 서비스가 시작되지 않았거나 대상 엔드포인트가 정상적으로 종료되었습니다. 데이터 보호 서비스를 시작하려면 **에이전트** > **에이전트 관리** > **설정** > **추가 서비스 설정**으로 이동하여 데이터 보호 서비스를 사용하도록 설정합니다.
- **설치할 수 없음**: 에이전트에 모듈을 배포하는 데 문제가 발생했습니다. 에이전트 트리에서 모듈을 다시 배포해야 합니다.
- **설치할 수 없음(데이터 손실 방지가 이미 있음)**: Trend Micro 데이터 손실 방지 소프트웨어가 엔드포인트에 이미 있는 경우 OfficeScan에서는 이 소프트웨어를 데이터 보호 모듈로 대체하지 않습니다.
- **설치되어 있지 않음**: 모듈이 에이전트에 배포되지 않았습니다. 이 상태는 에이전트에 모듈을 배포하지 않도록 선택했거나 배포하는 동안 에이전트의 상태가 오프라인 또는 독립 상태인 경우에 표시됩니다.

Forensic 폴더 및 DLP 데이터베이스

데이터 손실 방지 발생이 일어난 후 OfficeScan은 발생에 대한 정보를 특수 Forensic 데이터베이스에 기록합니다. 또한 OfficeScan은 발생을 트리거한 중요한 데이터의 복사본이 포함된 암호화된 파일을 생성하고 확인용 해시 값을 생성하며 해당 데이터의 무결성을 확인합니다. OfficeScan은 암호화된 Forensic 파일을 에이전트 컴퓨터에 생성한 다음 이 파일을 서버의 지정된 위치로 업로드합니다.

중요

- 암호화된 Forensic 파일에는 매우 중요한 데이터가 포함되므로 관리자는 이러한 파일에 대한 액세스 권한을 부여할 때 주의해야 합니다.
- OfficeScan은 Control Manager와 통합되어 DLP 발생 검토자 또는 DLP 준수 관리자 역할을 가진 Control Manager 사용자에게 암호화된 파일 내의 데이터에 액세스하는 기능을 제공합니다. DLP 역할 및 Control Manager에서 forensic 파일 데이터 액세스에 대한 자세한 내용은 *Control Manager 관리자 안내서 6.0 패치 2 이상*을 참조하십시오.

Forensic 폴더 및 데이터베이스 설정 수정

관리자는 OfficeScan의 INI 파일을 수정하여 Forensic 폴더의 위치 및 삭제 일정과 에이전트가 업로드하는 파일의 최대 크기를 변경할 수 있습니다.

경고!

데이터 손실 방지 발생을 기록한 후 Forensic 폴더 위치를 변경하면 데이터베이스 데이터와 기존 Forensic 파일 위치 사이의 연결이 끊어질 수 있습니다. Trend Micro에서는 Forensic 폴더 위치를 변경한 후에는 기존 Forensic 파일을 새 Forensic 폴더로 수동 마이그레이션할 것을 권장합니다.

다음 표에서는 OfficeScan 서버에 있는 <서버 설치 폴더>₩PCCSRV₩Private ₩ofcserver.ini 파일에서 사용 가능한 서버 설정을 간략히 설명합니다.

표 3-1. PCCSRV₩Private₩ofcserver.ini의 Forensic 폴더 서버 설정

목표	INI 설정	값
사용자 정의 Forensic 폴더 위치 사용	[INI_IDLP_SECTION] `EnableUserDefinedUploadFolder`	0: 사용 안 함(기본값) 1: 사용

목표	INI 설정	값
사용자 정의 Forensic 폴더 위치 구성	[INI_IDLP_SECTION] UserDefinedUploadFolder **참고** • 관리자가 EnableUserDefinedUploadFolder 설정을 사용하도록 설정해야 데이터 손실 방지 기능이 이 설정을 적용할 수 있습니다. • Forensic 폴더의 기본 위치는 다음과 같습니다. <서버 설치 폴더>₩PCCSRV₩Private ₩DLPForensicData • 사용자 정의 Forensic 폴더는 서버 컴퓨터의 물리적 드라이브(내부 또는 외부)에 위치해야 합니다. OfficeScan은 네트워크 드라이브 위치 매핑을 지원하지 않습니다.	기본값: <이 값을 고객 정의 폴더 경로로 대체하십시오 (예: C: ₩VolumeData ₩OfficeScanDlpForensicData).> 사용자 정의 값: 서버 컴퓨터에 장착된 드라이브의 물리적 위치여야 합니다.
Forensic 데이터 파일 삭제 사용	[INI_IDLP_SECTION] ForensicDataPurgeEnable	0: 사용 안 함 1: 사용(기본값)

목표	INI 설정	값
Forensic 데이터 파일 삭제 확인 빈도 구성	[INI_IDLP_SECTION] `ForensicDataPurgeCheckFrequency` **참고** • 관리자가 `ForensicDataPurgeEnable` 설정을 사용하도록 설정해야 OfficeScan에서 이 설정을 적용할 수 있습니다. • OfficeScan은 `ForensicDataExpiredPeriodInDays` 설정에 지정한 만료 날짜가 경과된 데이터 파일만 삭제합니다.	1: 매월, 매월 1일 00:00시 2: 매주(기본값), 매주 일요일 00:00시 3: 매일, 매일 00:00시 4: 매시간, 매시간 HH:00시
서버에서 Forensic 데이터 파일을 저장하는 시간 구성	[INI_IDLP_SECTION] `ForensicDataExpiredPeriodInDays`	기본값(일): 180 최소값: 1 최대값: 3650
Forensic 파일 디스크 공간 확인 빈도 구성	[INI_SERVER_DISK_THRESHOLD] `MonitorFrequencyInSecond` **참고** Forensic 데이터 폴더의 사용 가능한 디스크 공간이 `InformUploadOnDiskFreeSpaceInGb` 설정에 구성된 값보다 작으면 OfficeScan에서는 웹 콘솔에 이벤트 로그를 기록합니다.	기본값(초): 5

목표	INI 설정	값
Forensic 파일 디스크 공간 확인의 업로드 빈도 구성	[INI_SERVER_DISK_THRESHOLD] `IsapiCheckCountInRequest` **참고** Forensic 데이터 폴더의 사용 가능한 디스크 공간이 `InformUploadOnDiskFreeSpaceInGb` 설정에 구성된 값보다 작으면 OfficeScan에서는 웹 콘솔에 이벤트 로그를 기록합니다.	기본값(파일 수): 200
제한된 디스크 공간 알림을 트리거하는 최소 디스크 공간 값 구성	[INI_SERVER_DISK_THRESHOLD] `InformUploadOnDiskFreeSpaceInGb` **참고** Forensic 데이터 폴더의 사용 가능한 디스크 공간이 구성된 값보다 작으면 OfficeScan에서는 웹 콘솔에 이벤트 로그를 기록합니다.	기본값(GB): 10
에이전트에서 Forensic 데이터 파일을 업로드하는 데 사용할 수 있는 최소 공간 구성	[INI_SERVER_DISK_THRESHOLD] `RejectUploadOnDiskFreeSpaceInGb` **참고** Forensic 데이터 폴더의 사용 가능한 디스크 공간이 구성된 값보다 작으면 OfficeScan 에이전트가 Forensic 데이터 파일을 서버에 업로드하지 않으며 OfficeScan에서 웹 콘솔에 이벤트 로그를 기록합니다.	기본값(GB): 1

다음 표에서는 OfficeScan 서버에 있는 <서버 설치 폴더>₩PCCSRV₩ofcscan.ini 파일에서 사용 가능한 OfficeScan 에이전트 설정을 간략히 설명합니다.

표 3-2. PCCSRV₩ofcscan.ini의 **Forensic** 파일 에이전트 설정

목표	INI 설정	값
서버에 Forensic 데이터 파일 업로드 기능 사용	`UploadForensicDataEnable`	0: 사용 안 함 1: 사용(기본값)
OfficeScan 에이전트가 서버에 업로드하는 파일의 최대 크기 구성	`UploadForensicDataSizeLimitInMb` **참고** OfficeScan 에이전트는 이 크기보다 작은 파일만 서버로 보냅니다.	기본값(MB): 10 최소값: 1 최대값: 2048
OfficeScan 에이전트에서 Forensic 데이터 파일을 저장하는 시간 구성	`ForensicDataKeepDays` **참고** OfficeScan 에이전트에서는 매일 오전 11시에, 지정한 만료 날짜가 경과된 Forensic 데이터 파일을 삭제합니다.	기본값(일): 180 최소값: 1 최대값: 3650
OfficeScan 에이전트가 서버 연결을 확인하는 빈도 구성	`ForensicDataDelayUploadFrequenceInMinutes` **참고** OfficeScan 에이전트가 Forensic 파일을 서버에 업로드하지 못한 경우 자동으로 지정된 시간 간격으로 파일을 다시 보내려고 시도합니다.	기본값(분): 5 최소값: 5 최대값: 60

Forensic 데이터의 백업 만들기

Forensic 데이터 정보를 저장하는 데 필요한 시간은 회사의 보안 정책에 따라 크게 다를 수 있습니다. Trend Micro에서는 서버의 디스크 공간을 확보하려면 Forensic 폴더 데이터 및 Forensic 데이터베이스를 수동으로 백업할 것을 권장합니다.

절차

1. 서버에서 Forensic 데이터 폴더 위치로 이동합니다.
   - 기본 위치: <서버 설치 폴더>₩PCCSRV₩Private₩DLPForensicData
   - 사용자 정의 Forensic 폴더 위치를 찾으려면 사용자 정의 Forensic 폴더 위치 구성 페이지 3-10을 참조하십시오.
2. 폴더를 새 위치에 복사합니다.
3. Forensic 데이터 데이터베이스를 수동으로 백업하려면 <서버 설치 폴더>₩PCCSRV₩Private로 이동합니다.
4. DLPForensicDataTracker.db 파일을 새 위치에 복사합니다.

데이터 보호 제거

Plug-in Manager에서 데이터 보호 모듈을 제거한 경우

- 모든 데이터 손실 방지 구성, 설정 및 로그가 OfficeScan 서버에서 제거됩니다.
- 데이터 보호 모듈에서 제공한 모든 장치 제어 구성 및 설정이 서버에서 제거됩니다.
- 데이터 보호 모듈이 에이전트에서 제거됩니다. 에이전트 엔드포인트를 다시 시작해야 데이터 보호가 완전히 제거됩니다.
- 데이터 손실 방지 정책이 에이전트에 더 이상 적용되지 않습니다.
- 장치 제어에서 더 이상 다음 장치에 대한 액세스를 모니터링하지 않습니다.
  - Bluetooth 어댑터
  - COM 및 LPT 포트
  - IEEE 1394 인터페이스

- 이미징 장치
- 적외선 장치
- 모뎀
- PCMCIA 카드
- Print Screen 키
- 무선 NIC

데이터 보호 모듈을 언제든지 다시 설치할 수 있습니다. 설치 후 유효한 정품 인증 코드를 사용하여 라이선스를 활성화하십시오.

Plug-in Manager에서 데이터 보호 제거

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**를 클릭합니다.
2. **Plug-in Manager** 화면에서 **OfficeScan 데이터 보호** 섹션으로 이동하여 **제거**를 클릭합니다.
3. 제거 진행을 확인합니다. 제거하는 동안 다른 화면으로 이동할 수도 있습니다.
4. 제거 후 **Plug-in Manager** 화면을 새로 고칩니다. 언제든지 OfficeScan 데이터 보호 기능을 다시 설치할 수 있습니다.

부 II

OfficeScan 에이전트 보호

장 4

Trend Micro 스마트 보호 사용

이 장에서는 Trend Micro 스마트 보호 솔루션을 소개하고 솔루션을 사용하는 데 필요한 환경을 설정하는 방법에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- Trend Micro 스마트 보호 정보 페이지 4-2
- 스마트 보호 서비스 페이지 4-3
- 스마트 보호 소스 페이지 4-5
- 스마트 보호 패턴 파일 페이지 4-7
- 스마트 보호 서비스 설정 페이지 4-12
- 스마트 보호 서비스 사용 페이지 4-30

Trend Micro 스마트 보호 정보

Trend Micro™ 스마트 보호는 고객을 보안 위험 및 웹 위협으로부터 보호하기 위해 설계된 차세대 cloud-client 콘텐츠 보안 인프라입니다. 사용자가 네트워크에 있는지, 집에 있는지 또는 일하고 있는지에 관계없이 경량 에이전트를 사용하여 전자 메일, 웹 및 파일 검증 기술에 대해 고유한 in-the-cloud 상관 관계 및 위협 데이터베이스에 액세스하여 사용자를 보호하는 로컬 및 호스팅 솔루션을 모두 제공합니다. 고객의 보호 기능은 제품, 서비스 및 네트워크에 대한 사용자 액세스가 더 많아지면 자동으로 업데이트되고 강화되기 때문에 해당 사용자를 위한 실시간 환경 감시 보호 서비스를 만듭니다.

Trend Micro 스마트 보호 솔루션은 in-the-cloud 검증, 검색 및 상관 관계 기술을 통합하여 표준 패턴 파일 다운로드에 대한 의존성을 줄이고 데스크톱 업데이트와 관련하여 일반적으로 나타나는 지연 현상을 제거합니다.

새로운 솔루션의 필요성

파일 기반 위협 처리에 대한 현재 접근 방식에서는 엔드포인트를 보호하는 데 필요한 패턴(또는 정의)이 예약된 시간에 제공됩니다. 패턴은 Trend Micro에서 에이전트에 배치 파일로 제공합니다. 새 업데이트를 받으면 에이전트의 바이러스/악성 프로그램 방지 소프트웨어가 새로운 바이러스/악성 프로그램 위험에 대한 이 패턴 정의 배치 파일을 메모리에 다시 로드합니다. 새로운 바이러스/악성 프로그램 위험이 발견된 경우 지속적인 보호를 위해 패턴을 부분적으로 또는 전체적으로 다시 업데이트하고 에이전트에서 다시 로드해야 합니다.

시간이 흐르면서 독특한 신종 위협이 크게 증가했습니다. 이러한 위협은 앞으로 거의 기하급수적으로 증가할 것으로 예상됩니다. 또한 양적인 면에서 현재 알려진 보안 위험보다 훨씬 많을 것입니다. 앞으로 방대한 양의 보안 위험은 새로운 유형의 보안 위험을 나타냅니다. 방대한 양의 보안 위험은 서버 및 워크스테이션 성능, 네트워크 대역폭 사용량, 그리고 일반적으로 양질의 보호를 제공하는 데 걸리는 전체 시간 또는 "보호 시간"에 영향을 미칠 수 있습니다.

Trend Micro는 Trend Micro 고객이 바이러스/악성 프로그램 위협에 면역될 수 있도록 지원한다는 목표 아래 방대한 양의 위협을 처리하는 새로운 접근 방식을 개척했습니다. 이 선구적인 노력에 사용된 기술 및 아키텍처에서는 바이러스/악성 프로그램 서명 및 패턴 저장소를 클라우드로 오프로드하는 기술을 활용합니다. 이러한 바이러스/악성 프로그램 서명 저장소를 클라우드로 오프로드함

으로써 Trend Micro는 향후 새롭게 등장하는 방대한 양의 보안 위험으로부터 고객을 보다 안전하게 보호할 수 있습니다.

스마트 보호 서비스

스마트 보호에는 in-the-cloud에 저장된 악성 프로그램 방지 서명, 웹 검증 및 위협 데이터베이스를 제공하는 서비스가 포함됩니다.

스마트 보호 서비스에는 다음이 포함됩니다.

- **파일 검증 서비스**: 파일 검증 서비스는 이전에 에이전트 컴퓨터에 저장된 많은 악성 프로그램 방지 서명을 스마트 보호 소스에 오프로드합니다.

  자세한 내용은 파일 검증 서비스 페이지 4-3를 참조하십시오.

- **웹 검증 서비스**: 웹 검증 서비스는 이전에 Trend Micro에서만 호스팅하던 URL 검증 데이터를 로컬 스마트 보호 소스에서 호스팅할 수 있도록 해줍니다. 두 기술 모두 패턴 업데이트 또는 URL 유효성 확인 시 대역폭 사용량을 줄여 줍니다.

  자세한 내용은 웹 검증 서비스 페이지 4-4를 참조하십시오.

- **Smart Feedback**: Trend Micro는 전 세계 Trend Micro 제품에서 익명으로 보내는 정보를 지속적으로 수집하여 사전에 각각의 새로운 위협을 확인합니다.

  자세한 내용은 Smart Feedback 페이지 4-4를 참조하십시오.

파일 검증 서비스

파일 검증 서비스는 광범위한 in-the-cloud 데이터베이스를 기반으로 각 파일을 검증합니다. 악성 프로그램 정보가 클라우드에 저장되기 때문에 모든 사용자가 즉시 사용할 수 있습니다. 고성능 콘텐츠 전달 네트워크와 로컬 캐싱 서버는 확인 프로세스 동안 최소한의 대기 시간을 보장합니다. cloud-에이전트 아키텍처는 훨씬 신속한 보호를 제공하고 전체 에이전트 영역을 상당히 줄이는 것 외에 패턴 개발 부담을 제거합니다.

파일 검증 서비스를 사용하려면 에이전트가 스마트 스캔 모드에 있어야 합니다. 이 문서에서는 이러한 에이전트를 스마트 스캔 에이전트라고 합니다. 스마

트 스캔 모드에 있지 않아 파일 검증 서비스를 사용하지 않는 에이전트를 표준 스캔 에이전트라고 합니다. OfficeScan 관리자는 모든 또는 여러 에이전트를 스마트 스캔 모드에 있도록 구성할 수 있습니다.

웹 검증 서비스

세계 최대의 도메인 검증 데이터베이스 중 하나인 Trend Micro 웹 검증 기술은 웹 사이트 생성 시기, 악성 프로그램 동작 분석을 통해 발견된 의심스러운 활동의 이력 위치 변경 및 표시와 같은 요소를 기준으로 검증 점수를 할당하여 웹 도메인의 신뢰도를 추적합니다. 그런 다음 웹 검증에서는 계속해서 사이트를 검색하고 사용자가 감염된 사이트에 액세스하는 것을 차단합니다. 웹 검증 기능은 사용자가 액세스하는 페이지를 웹 위협(예: 악성 프로그램, 스파이웨어, 사용자를 유인하여 개인 정보를 제공하도록 설계된 피싱 메일 등)으로부터 안전하게 보호해 줍니다. 정확성을 높이고 잘못된 판정을 줄이기 위해 Trend Micro 웹 검증 기술은 합법적인 사이트의 일부분만 해킹 당하는 경우가 많고 검증이 시간에 따라 동적으로 변경될 수 있기 때문에 전체 사이트를 분류하거나 차단하는 대신 검증 점수를 사이트 내 특정 페이지 또는 링크에 할당합니다.

웹 검증 정책이 적용된 OfficeScan 에이전트에서는 웹 검증 서비스를 사용합니다. OfficeScan 관리자는 모든 또는 여러 에이전트에 웹 검증 정책을 적용할 수 있습니다.

Smart Feedback

Trend Micro Smart Feedback은 Trend Micro 제품 및 연중무휴로 운영되는 Trend Micro의 위협 연구 센터와 기술진 간에 지속적인 커뮤니케이션을 제공합니다. 모든 단일 고객의 루틴 검증 확인을 통해 식별된 각각의 새로운 위협은 모든 Trend Micro 위협 데이터베이스를 자동으로 업데이트하여 이후의 고객에게 해당 위협이 발생하지 않도록 차단합니다.

Trend Micro는 고객과 파트너의 광범위한 글로벌 네트워크를 통해 수집한 위협 정보를 지속적으로 처리하여 최신 위협에 대한 자동 실시간 보호 기능을 제공하고 "함께 공유하면 더 강력한" 보안 기능을 제공합니다. 이는 다른 사용자를 보호하는 커뮤니티가 포함된 자동 환경 감시와 매우 유사합니다. 수집되는 위협 정보가 특정 통신 내용이 아니라 통신 소스의 검증을 기반으로 하기 때문에 고객의 개인 정보 또는 비즈니스 정보가 항상 보호됩니다.

Trend Micro로 전송되는 정보의 샘플

- 파일 체크섬
- 액세스한 웹 사이트
- 크기 및 경로를 포함한 파일 정보
- 실행 파일 이름

웹 콘솔에서 언제든지 프로그램 참여를 종료할 수 있습니다.

팁

엔드포인트를 보호하기 위해 Smart Feedback에 참여할 필요는 없습니다. 참여 여부는 선택 사항이며 언제라도 참여를 취소할 수 있습니다. Trend Micro에서는 모든 Trend Micro 고객에게 더 나은 전체 보호를 제공하기 위해 Smart Feedback에 참여할 것을 권장합니다.

스마트 보호 네트워크에 대한 자세한 내용은 다음을 방문하십시오.

http://www.smartprotectionnetwork.com

스마트 보호 소스

Trend Micro에서는 OfficeScan 및 스마트 보호 소스에 파일 검증 서비스 및 웹 검증 서비스를 제공합니다.

스마트 보호 소스는 대부분의 바이러스/악성 프로그램 패턴 정의를 호스팅하여 파일 검증 서비스를 제공합니다. OfficeScan 에이전트는 나머지 정의를 호스팅합니다. 에이전트는 자체 패턴 정의에서 파일의 위험 여부를 확인할 수 없는 경우 스마트 보호 소스에 검색 쿼리를 보냅니다. 스마트 보호 소스는 식별 정보를 사용하여 위험 여부를 확인합니다.

스마트 보호 소스는 이전에 Trend Micro 호스팅 서버를 통해서만 사용할 수 있던 웹 검증 데이터를 호스팅하여 웹 검증 서비스를 제공합니다. 에이전트는 스마트 보호 소스에 웹 검증 쿼리를 보내 사용자가 액세스하려는 웹 사이트를 검증합니다. 에이전트는 웹 사이트의 검증 상태를 엔드포인트에 적용된 특정 웹 검증 정책과 비교하여 사이트에 대한 액세스를 허용할지 또는 차단할지 결정합니다.

에이전트가 연결되는 스마트 보호 소스는 에이전트의 위치에 따라 다릅니다. 에이전트는 Trend Micro 스마트 보호 네트워크 또는 스마트 보호 서버에 연결할 수 있습니다.

Trend Micro™ 스마트 보호 네트워크™

Trend Micro™ 스마트 보호 네트워크™는 고객을 보안 위험 및 웹 위협으로부터 보호하기 위해 설계된 차세대 클라우드 클라이언트 콘텐츠 보안 인프라입니다. 온-프레미스 및 Trend Micro 호스팅 솔루션을 구동하여 네트워크에서든 가정에서든 이동 중에든 항상 사용자를 보호합니다. 스마트 보호 네트워크에서는 더욱 가벼워진 경량 에이전트를 사용하여 위협 데이터베이스뿐 아니라 전자 메일, 웹 및 파일 검증 기술의 고유한 in-the-cloud 상관 관계에 액세스합니다. 고객의 보호 기능은 제품, 서비스 및 네트워크에 대한 사용자 액세스가 더 많아지면 자동으로 업데이트되고 강화되기 때문에 해당 사용자를 위한 실시간 환경 감시 보호 서비스를 만듭니다.

스마트 보호 네트워크에 대한 자세한 내용은 다음을 방문하십시오.

http://www.smartprotectionnetwork.com

스마트 보호 서버

스마트 보호 서버는 해당 로컬 기업 네트워크에 대한 액세스 권한을 가진 사용자를 위한 서버입니다. 로컬 서버는 기업 네트워크에 대한 스마트 보호 서비스를 현지화하여 효율성을 최적화합니다.

스마트 보호 서버에는 두 가지 유형이 있습니다.

- **통합 스마트 보호 서버**: OfficeScan 설치 프로그램에는 OfficeScan 서버가 설치된 동일한 엔드포인트에 설치되는 통합 스마트 보호 서버가 포함됩니다. 설치 후 OfficeScan 웹 콘솔에서 이 서버에 대한 설정을 관리합니다. 통합 서버는 소규모 OfficeScan 배포용으로 설계되었습니다. 대규모 배포에는 독립 스마트 보호 서버가 필요합니다.
- **독립 스마트 보호 서버**: 독립 스마트 보호 서버는 VMware 또는 Hyper-V 서버에 설치됩니다. 독립 서버에는 별도의 관리 콘솔이 있으며, OfficeScan 웹 콘솔에서 관리되지 않습니다.

스마트 보호 소스 비교

다음 표에는 스마트 보호 네트워크와 스마트 보호 서버 간의 차이점이 요약되어 있습니다.

표 4-1. 스마트 보호 소스 비교

비교 기준	스마트 보호 서버	TREND MICRO 스마트 보호 네트워크
사용 가능 여부	내부 에이전트에 사용할 수 있습니다. 이는 OfficeScan 웹 콘솔에서 지정된 위치 기준을 충족하는 에이전트입니다.	주로 외부 에이전트에 사용할 수 있습니다. 이는 OfficeScan 웹 콘솔에서 지정된 위치 기준을 충족하지 않는 에이전트입니다.
목적	기업 네트워크에 대한 스마트 보호 서비스를 현지화하여 효율성을 최적화하는 데 목적을 두고 설계되었습니다.	해당 기업 네트워크에 즉시 액세스할 수 없는 에이전트에 스마트 보호 서비스를 제공하는 글로벌 수준의 인터넷 기반 인프라입니다.
관리	OfficeScan 관리자가 이러한 스마트 보호 소스를 설치하고 관리합니다.	Trend Micro에서 이 소스를 유지 관리합니다.
패턴 업데이트 소스	Trend Micro 액티브업데이트 서버	Trend Micro 액티브업데이트 서버
에이전트 연결 프로토콜	HTTP 및 HTTPS	HTTPS

스마트 보호 패턴 파일

스마트 보호 패턴 파일은 파일 검증 서비스 및 웹 검증 서비스에 사용됩니다. Trend Micro는 Trend Micro 액티브업데이트 서버를 통해 이러한 패턴 파일을 릴리스합니다.

스마트 스캔 에이전트 패턴

스마트 스캔 에이전트 패턴은 매일 업데이트되며 OfficeScan 에이전트의 업데이트 소스(OfficeScan 서버 또는 사용자 정의 업데이트 소스)를 통해 다운로드됩니다. 그런 다음 업데이트 소스는 스마트 스캔 에이전트에 패턴을 배포합니다.

참고

스마트 스캔 에이전트는 관리자가 파일 검증 서비스를 사용하도록 구성한 OfficeScan 에이전트입니다. 파일 검증 서비스를 사용하지 않는 에이전트는 표준 스캔 에이전트라고 합니다.

스마트 스캔 에이전트는 보안 위험을 검색할 때 스마트 스캔 에이전트 패턴을 사용합니다. 이 패턴에서 파일의 위험 여부를 확인할 수 없는 경우 스마트 스캔 패턴이라는 또 다른 패턴이 사용됩니다.

스마트 스캔 패턴

스마트 스캔 패턴은 매시간 업데이트되며 스마트 보호 소스를 통해 다운로드됩니다. 스마트 스캔 에이전트는 스마트 스캔 패턴을 다운로드하지 않습니다. 에이전트는 스마트 보호 소스로 검색 쿼리를 보내 스마트 스캔 패턴을 기준으로 잠재적인 위협을 확인합니다.

웹 차단 목록

웹 차단 목록은 스마트 보호 소스를 통해 다운로드됩니다. 웹 검증 정책이 적용되는 OfficeScan 에이전트는 웹 차단 목록을 다운로드하지 않습니다.

참고

관리자는 모든 또는 여러 에이전트에 웹 검증 정책을 적용할 수 있습니다.

웹 검증 정책이 적용되는 에이전트는 스마트 보호 소스로 웹 검증 쿼리를 보내 웹 차단 목록을 기준으로 웹 사이트의 검증 상태를 확인합니다. 에이전트는 스마트 보호 소스로부터 받은 검증 데이터를 엔드포인트에 적용된 웹 검증 정책

과 비교합니다. 이 정책에 따라 에이전트는 사이트에 대한 액세스를 차단하거나 허용합니다.

스마트 보호 패턴 업데이트 프로세스

스마트 보호 패턴 업데이트는 Trend Micro 액티브업데이트 서버에서 가져옵니다.

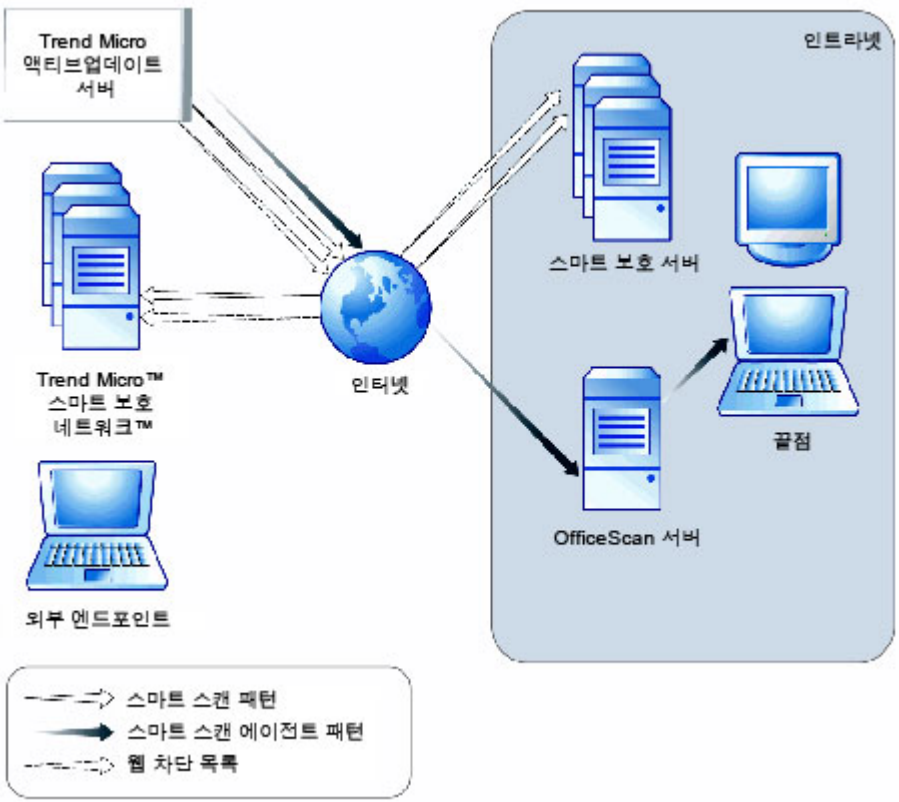


그림 4-1. 패턴 업데이트 프로세스

스마트 보호 패턴 사용

OfficeScan 에이전트는 스마트 스캔 에이전트 패턴을 사용하여 보안 위험을 검색하며, 스마트 스캔 에이전트 패턴에서 파일의 위험 여부를 확인할 수 없는 경우에만 스마트 스캔 패턴을 쿼리합니다. 사용자가 웹 사이트에 액세스하려고 하면 에이전트에서 웹 차단 목록을 쿼리합니다. 고급 필터링 기술을 통해 에이전트는 쿼리 결과를 "캐시"할 수 있습니다. 따라서 같은 쿼리를 두 번 이상 보낼 필요가 없습니다.

현재 인트라넷에 있는 에이전트는 스마트 보호 서버에 연결하여 스마트 스캔 패턴 또는 웹 차단 목록을 쿼리할 수 있습니다. 스마트 보호 서버에 연결하려면 네트워크 연결이 필요합니다. 둘 이상의 스마트 보호 서버가 설치된 경우 관리자는 연결 우선 순위를 결정할 수 있습니다.

팁

스마트 보호 서버에 연결할 수 없는 경우에 보호 지속성을 보장하기 위해 스마트 보호 서버를 여러 대 설치합니다.

현재 인트라넷에 없는 에이전트는 Trend Micro 스마트 보호 네트워크에 연결하여 쿼리할 수 있습니다. 스마트 보호 네트워크에 연결하려면 인터넷 연결이 필요합니다.

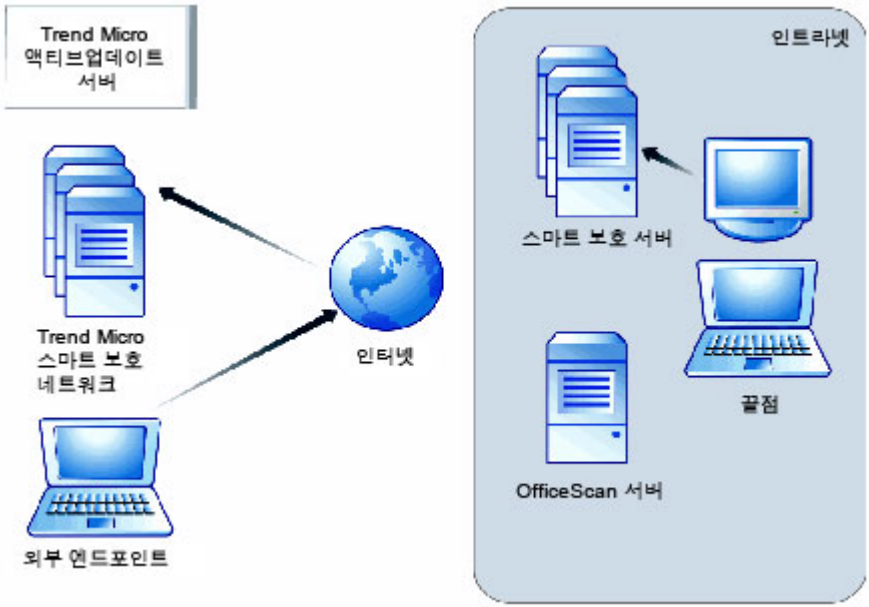


그림 4-2. 쿼리 프로세스

네트워크 또는 인터넷에 액세스할 수 없는 에이전트는 스마트 스캔 에이전트 패턴 및 이전 쿼리 결과가 포함된 캐시를 통해 보호받을 수 있습니다. 보호 기능은 새 쿼리가 필요한 경우에만 저하되며, 반복된 시도 후에는 에이전트에서 스마트 보호 소스에 연결할 수 없습니다. 이 경우 에이전트는 검증할 파일에 대한 플래그를 지정하고 일시적으로 파일에 대한 액세스를 허용합니다. 스마트 보호 소스에 대한 연결이 복원되면 플래그가 지정된 모든 파일이 다시 검색됩니다. 그런 다음 위협으로 확인된 파일에 대해 적절한 검색 작업이 수행됩니다.

다음 표에는 에이전트 위치에 따른 보호 범위가 요약되어 있습니다.

표 4-2. 위치에 따른 보호 동작

위치	패턴 파일 및 쿼리 동작
인트라넷에 액세스	• **패턴 파일**: 에이전트가 OfficeScan 서버 또는 사용자 정의 업데이트 소스에서 스마트 스캔 에이전트 패턴 파일을 다운로드합니다. • **파일 및 웹 검증 쿼리**: 에이전트가 쿼리를 위해 스마트 보호 서버에 연결합니다.
인트라넷에 액세스할 수 없지만 스마트 보호 네트워크에 연결됨	• **패턴 파일**: OfficeScan 서버 또는 사용자 정의 업데이트 소스에 연결할 수 없는 경우에는 에이전트에서 최신 스마트 스캔 에이전트 패턴 파일을 다운로드할 수 없습니다. • **파일 및 웹 검증 쿼리**: 에이전트가 쿼리를 위해 스마트 보호 네트워크에 연결합니다.
트라넷에 액세스할 수 없고 스마트 보호 네트워크에 연결되지 않음	• **패턴 파일**: OfficeScan 서버 또는 사용자 정의 업데이트 소스에 연결할 수 없는 경우에는 에이전트에서 최신 스마트 스캔 에이전트 패턴 파일을 다운로드할 수 없습니다. • **파일 및 웹 검증 쿼리**: 에이전트가 쿼리 결과를 받을 수 없으므로 스마트 스캔 에이전트 패턴 및 이전 쿼리 결과가 포함된 캐시에 의존해야 합니다.

스마트 보호 서비스 설정

에이전트에서 파일 검증 서비스 및 웹 검증 서비스를 활용하려면 먼저 스마트 보호 환경이 제대로 설정되어 있는지 확인하십시오. 다음과 같이 입력합니다.

- 스마트 보호 서버 설치 페이지 4-13
- 통합 스마트 보호 서버 관리 페이지 4-17
- 스마트 보호 소스 목록 페이지 4-21
- 에이전트 연결 프록시 설정 페이지 4-29
- Trend Micro Network VirusWall 설치 페이지 4-29

스마트 보호 서버 설치

에이전트 수가 1,000대 이하인 경우 통합 스마트 보호 서버 또는 독립 스마트 보호 서버를 설치할 수 있습니다. 1,000대가 넘는 에이전트가 있는 경우에는 독립 스마트 보호 서버를 설치합니다.

Trend Micro에서는 장애 조치를 위해 스마트 보호 서버를 여러 대 설치할 것을 권장합니다. 에이전트가 특정 서버에 연결할 수 없으면 사용자가 설정한 다른 서버에 연결을 시도합니다.

통합 서버와 OfficeScan 서버는 같은 엔드포인트에서 실행되므로 두 서버의 트래픽이 많은 시간에는 엔드포인트의 성능이 크게 저하될 수 있습니다. 따라서 독립 스마트 보호 서버는 에이전트의 기본 스마트 보호 소스로, 통합 서버는 백업으로 사용하는 것이 좋습니다.

독립 스마트 보호 서버 설치

독립 스마트 보호 서버 설치 및 관리에 대한 자세한 내용은 *스마트 보호 서버 설치 및 업그레이드 안내서*를 참조하십시오.

통합 스마트 보호 서버 설치

OfficeScan 서버 설치 중에 통합 서버를 설치한 경우

- 통합 서버를 사용하도록 설정하고 서버에 대한 설정을 구성합니다. 자세한 내용은 통합 스마트 보호 서버 관리 페이지 4-17를 참조하십시오.
- 통합 서버와 OfficeScan 에이전트가 같은 서버 컴퓨터에 있는 경우 OfficeScan 방화벽을 해제하는 것이 좋습니다. OfficeScan 방화벽은 에이전트 엔드포인트용이므로 서버에서 사용할 경우 성능에 영향을 미칠 수 있습니다. 방화벽 해제에 대한 자세한 내용은 OfficeScan 방화벽 설정 또는 해제 페이지 13-6를 참조하십시오.

참고

방화벽을 해제할 경우의 영향을 고려하고 이것이 보안 계획을 준수하는지 확인하십시오.

팁

통합 스마트 보호 서버 도구 페이지 4-14를 사용하여 OfficeScan 설치를 완료한 후 통합 스마트 보호 서버를 설치하십시오.

통합 스마트 보호 서버 도구

관리자는 Trend Micro 통합 스마트 보호 도구를 사용하여 OfficeScan 서버 설치가 완료된 후 통합 스마트 보호 서버를 간편하게 설치하거나 제거할 수 있습니다. 현재 버전의 OfficeScan에서는 OfficeScan 서버 설치가 완료된 후 관리자가 통합 스마트 보호 서버를 설치/제거할 수 없습니다. 이 도구는 이전 버전의 OfficeScan에서 설치 기능의 유연성을 향상시킵니다.

절차

1. 명령 프롬프트를 열고 ISPSInstaller.exe가 있는 <서버 설치 폴더>₩PCCSRV\Admin\Utility\ISPSInstaller 디렉터리로 이동합니다.
2. 다음 명령 중 하나를 사용하여 ISPSInstaller.exe를 실행합니다.

표 4-3. 설치 관리자 옵션

명령	설명
`ISPSInstaller.exe /i`	기본 포트 설정을 사용하여 통합 스마트 보호 서버를 설치합니다. 기본 포트 설정에 대한 자세한 내용은 아래 표를 참조하십시오.

명령	설명
`ISPSInstaller.exe /i /f:[port number] /s:[port number] /w:[port number]`	지정된 포트를 사용하여 통합 스마트 보호 서버를 설치합니다. **참고** Apache web server를 사용할 경우에는 포트를 구성해야 합니다. 여기서 각 항목은 다음과 같습니다. • `/f:[port number]`는 HTTP 파일 검증 포트를 나타냅니다. • `/s:[port number]`는 HTTPS 파일 검증 포트를 나타냅니다. • `/w:[port number]`는 웹 검증 포트를 나타냅니다. **참고** 지정되지 않은 포트에는 자동으로 기본값이 할당됩니다.
`ISPSInstaller.exe /u`	통합 스마트 보호 서버를 제거합니다.

표 4-4. 통합 스마트 보호 서버의 검증 서비스에 사용되는 포트

Web Server 및 설정	파일 검증 서비스에 사용되는 포트		웹 검증 서비스에 사용되는 HTTP 포트
	HTTP	HTTPS (SSL)	
SSL을 사용하는 IIS 기본 웹 사이트	80	443(구성할 수 없음)	80(구성할 수 없음)
SSL을 사용하지 않는 IIS 기본 웹 사이트	80	443(구성할 수 없음)	80(구성할 수 없음)
SSL을 사용하는 IIS 가상 웹 사이트	8080	4343(구성 가능)	8080(구성 가능)

WEB SERVER 및 설정	파일 검증 서비스에 사용되는 포트		웹 검증 서비스에 사용되는 HTTP 포트
	HTTP	HTTPS (SSL)	
SSL을 사용하지 않는 IIS 가상 웹 사이트	8080	4343(구성 가능)	8080(구성 가능)

3. 설치가 완료된 후 OfficeScan 웹 콘솔을 열고 다음을 확인합니다.
   - **시작** 메뉴에서 `services.msc`를 입력하여 **Microsoft Management Console**을 열고 Trend Micro Local Web Classification Server 및 Trend Micro Smart Scan Server가 "시작됨" 상태로 나열되어 있는지 확인합니다.
   - **Windows 작업 관리자**를 엽니다. **프로세스** 탭에서 iCRCService.exe 및 LWCSService.exe가 실행 중인지 확인합니다.
   - OfficeScan 웹 콘솔에 **관리** > **스마트 보호** > **통합 서버** 메뉴 항목이 나타나는지 확인합니다.

스마트 보호 서버 최선의 방법

다음 방법을 통해 스마트 보호 서버의 성능을 최적화할 수 있습니다.

- 수동 검색과 예약 검색을 동시에 수행하지 마십시오. 그룹별로 검색을 수행하십시오.
- 모든 에이전트에서 지금 검색을 동시에 수행하도록 구성하지 마십시오.
- 네트워크 연결 속도가 느린 경우(약 512Kbps) ptngrowth.ini 파일을 변경하여 스마트 보호 서버를 사용자 지정하십시오.

독립 서버에 대한 ptngrowth.ini 사용자 정의

절차

1. /var/tmcss/conf/ 의 ptngrowth.ini 파일 열기.

2. 아래의 권장 값을 사용하여 ptngrowth.ini 파일을 수정합니다.
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. ptngrowth.ini 파일을 저장합니다.
4. CLI(명령줄 인터페이스)에서 다음 명령을 입력하여 lighttpd 서비스를 다시 시작합니다.
   - `service lighttpd restart`

통합 서버에 대한 ptngrowth.ini 사용자 정의

절차

1. <서버 설치 폴더>₩PCCSRV₩WSSW의 ptngrowth.ini 파일 열기
2. 아래의 권장 값을 사용하여 ptngrowth.ini 파일을 수정합니다.
   - `[COOLDOWN]`
   - `ENABLE=1`
   - `MAX_UPDATE_CONNECTION=1`
   - `UPDATE_WAIT_SECOND=360`
3. ptngrowth.ini 파일을 저장합니다.
4. Trend Micro 스마트 보호 서버 서비스를 다시 시작합니다.

통합 스마트 보호 서버 관리

다음 작업을 수행하여 통합 스마트 보호 서버를 관리합니다.

- 통합 서버의 파일 검증 서비스 및 웹 검증 서비스 사용
- 통합 서버의 주소 기록
- 통합 서버의 구성 요소 업데이트
- 통합 서버의 승인/차단된 URL 목록 구성

자세한 내용은 통합 스마트 보호 서버 설정 구성 페이지 4-20를 참조하십시오.

통합 서버의 파일 검증 서비스 및 웹 검증 서비스 사용

에이전트에서 통합 서버로 검색 및 웹 검증 쿼리를 보내려면 파일 검증 서비스 및 웹 검증 서비스를 사용해야 합니다. 이러한 서비스를 사용하면 통합 서버가 액티브업데이트 서버에서 구성 요소를 업데이트할 수 있습니다.

이러한 서비스는 OfficeScan 서버 설치 중에 통합 서버를 설치하도록 선택한 경우 자동으로 설정됩니다.

서비스를 사용하지 않으려면 에이전트에서 쿼리를 보낼 수 있는 독립 스마트 보호 서버를 설치해야 합니다.

자세한 내용은 통합 스마트 보호 서버 설정 구성 페이지 4-20를 참조하십시오.

통합 서버의 주소 기록

내부 에이전트에 대한 스마트 보호 소스 목록을 구성할 때 통합 서버의 주소가 필요합니다. 목록에 대한 자세한 내용은 스마트 보호 소스 목록 페이지 4-21을 참조하십시오.

에이전트에서 통합 서버에 검색 쿼리를 보낼 때는 두 가지 파일 검증 서비스 주소 중 하나, 즉 HTTP 또는 HTTPS 주소로 서버를 식별합니다. HTTPS를 통해 연결하는 것이 보다 안전하지만 HTTP 연결은 대역폭을 더 적게 사용합니다.

에이전트에서 웹 검증 쿼리를 보낼 때는 해당 웹 검증 서비스 주소로 통합 서버를 식별합니다.

팁

다른 OfficeScan 서버에서 관리하는 에이전트에서도 이 통합 서버에 연결할 수 있습니다. 다른 OfficeScan 서버의 웹 콘솔에서 통합 서버의 주소를 스마트 보호 소스 목록에 추가하면 됩니다.

자세한 내용은 통합 스마트 보호 서버 설정 구성 페이지 4-20를 참조하십시오.

통합 서버의 구성 요소 업데이트

통합 서버는 다음 구성 요소를 업데이트합니다.

- **스마트 스캔 패턴**: OfficeScan 에이전트 에이전트는 통합 서버로 검색 쿼리를 보내 스마트 스캔 패턴을 기준으로 잠재적인 위협을 확인합니다.
- **웹 차단 목록**: 웹 검증 정책이 적용되는 OfficeScan 에이전트 에이전트는 통합 서버로 웹 검증 쿼리를 보내 웹 차단 목록을 기준으로 웹 사이트의 검증 상태를 확인합니다.

이러한 구성 요소를 수동으로 업데이트하거나 업데이트 일정을 구성할 수 있습니다. 통합 서버는 액티브업데이트 서버에서 구성 요소를 다운로드합니다.

참고

순수 IPv6 통합 서버는 Trend Micro 액티브업데이트 서버에서 직접 업데이트할 수 없습니다. 통합 서버에서 액티브업데이트 서버에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

자세한 내용은 통합 스마트 보호 서버 설정 구성 페이지 4-20를 참조하십시오.

통합 서버의 승인/차단된 URL 목록 구성

에이전트는 고유한 승인/차단된 URL 목록을 유지 관리합니다. 웹 검증 정책(자세한 내용은 웹 검증 정책 페이지 12-5 참조)을 설정할 때 에이전트 목록을 구성합니다. 에이전트 목록에 있는 모든 URL은 자동으로 허용되거나 차단됩니다.

통합 서버에는 고유한 승인/차단된 URL 목록이 있습니다. URL이 에이전트 목록에 없는 경우 에이전트는 통합 서버로 웹 검증 쿼리를 보냅니다(통합 서버가

스마트 보호 소스로 할당된 경우). 이 URL이 통합 서버의 승인/차단된 URL 목록에 있는 경우 통합 서버는 해당 URL을 허용하거나 차단하도록 에이전트에 알림을 보냅니다.

참고

차단된 URL 목록은 웹 차단 목록보다 우선 순위가 높습니다.

통합 서버의 승인/차단된 목록에 URL을 추가하려면 독립 스마트 보호 서버에서 목록을 가져와야 합니다. URL을 수동으로 추가할 수는 없습니다.

자세한 내용은 통합 스마트 보호 서버 설정 구성 페이지 4-20를 참조하십시오.

통합 스마트 보호 서버 설정 구성

절차

1. **관리** > **스마트 보호** > **통합 서버**로 이동합니다.
2. **파일 검증 서비스 사용**을 선택합니다.
3. 통합 서버에 검색 쿼리를 보낼 때 에이전트에서 사용할 프로토콜(HTTP 또는 HTTPS)을 선택합니다.
4. **웹 검증 서비스 사용**을 선택합니다.
5. **서버 주소** 열 아래에 있는 통합 서버의 주소를 기록합니다.
6. 통합 서버의 구성 요소를 업데이트하려면
   - 현재 버전의 스마트 스캔 패턴 및 웹 차단 목록을 확인합니다. 업데이트를 사용할 수 있는 경우 **지금 업데이트**를 클릭합니다. 화면의 맨 위에 업데이트 결과가 표시됩니다.
   - 패턴을 자동으로 업데이트하려면
     a. **예약 업데이트 사용**을 선택합니다.
     b. 매시간 업데이트할지 또는 15분마다 업데이트할지 선택합니다.

c. **파일 검증 서비스** 아래에서 업데이트 소스를 선택합니다. 스마트 스캔 패턴은 이 소스에서 업데이트됩니다.

d. **웹 검증 서비스** 아래에서 업데이트 소스를 선택합니다. 웹 차단 목록은 이 소스에서 업데이트됩니다.

참고

- 액티브업데이트 서버를 업데이트 소스로 선택할 경우 서버가 인터넷에 연결되어 있는지 확인하고, 프록시 서버를 사용하는 경우 프록시 설정을 사용하여 인터넷 연결을 설정할 수 있는지 테스트합니다. 자세한 내용은 OfficeScan 서버 업데이트용 프록시 페이지 6-18를 참조하십시오.
- 사용자 지정 업데이트 소스를 선택하는 경우 적합한 환경을 설정하고 이 업데이트 소스에 대한 리소스를 업데이트합니다. 또한 서버 컴퓨터와 이 업데이트 소스가 기능적으로 연결되어 있는지 확인합니다. 업데이트 소스를 설정하는 데 도움이 필요한 경우에는 지원 센터에 문의하십시오.

7. 통합 서버의 승인/차단된 목록을 구성하려면

   a. **가져오기**를 클릭하여 미리 서식이 지정된 .csv 파일의 URL로 목록을 채웁니다. 독립 스마트 보호 서버에서 .csv 파일을 가져올 수 있습니다.

   b. 기존 목록이 있는 경우 **내보내기**를 클릭하여 .csv 파일에 목록을 저장합니다.

8. **저장**을 클릭합니다.

스마트 보호 소스 목록

에이전트는 보안 위험을 검색하고 웹 사이트의 검증 상태를 확인할 때 스마트 보호 소스에 쿼리를 보냅니다.

스마트 보호 소스에 대한 IPv6 지원

순수 IPv6 에이전트는 다음과 같은 순수 IPv4 소스에 직접 쿼리를 보낼 수 없습니다.

- 스마트 보호 서버 2.0(통합 또는 독립)

  참고

  스마트 보호 서버에 대한 IPv6 지원은 버전 2.5부터 제공됩니다.

- Trend Micro 스마트 보호 네트워크

마찬가지로 순수 IPv4 에이전트는 순수 IPv6 스마트 보호 서버에 쿼리를 보낼 수 없습니다.

에이전트에서 소스에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

스마트 보호 소스와 엔드포인트 위치

에이전트가 연결되는 스마트 보호 소스는 에이전트 엔드포인트의 위치에 따라 다릅니다.

위치 설정 구성에 대한 자세한 내용은 엔드포인트 위치 페이지 15-2를 참조하십시오.

표 4-5. 위치별 스마트 보호 소스

위치	스마트 보호 소스
외부	외부 에이전트는 Trend Micro 스마트 보호 네트워크에 검색 및 웹 검증 쿼리를 보냅니다.

위치	스마트 보호 소스
내부	내부 에이전트는 스마트 보호 서버 또는 Trend Micro 스마트 보호 네트워크에 검색 및 웹 검증 쿼리를 보냅니다. 스마트 보호 서버를 설치한 경우 OfficeScan 웹 콘솔에서 스마트 보호 소스 목록을 구성합니다. 쿼리해야 하는 경우 내부 에이전트는 이 목록에서 서버를 선택합니다. 에이전트가 첫 번째 서버에 연결할 수 없는 경우 목록에서 다른 서버를 선택합니다. **팁** 독립 스마트 보호 서버는 기본 스캔 소스로, 통합 서버는 백업으로 할당합니다. 이렇게 하면 OfficeScan 서버 및 통합 서버를 호스팅하는 엔드포인트로 전달되는 트래픽이 감소합니다. 또한 독립 서버에서 더 많은 쿼리를 처리할 수 있습니다. 스마트 보호 소스에 대한 표준 또는 사용자 지정 목록을 구성할 수 있습니다. 표준 목록은 모든 내부 에이전트에서 사용됩니다. 사용자 지정 목록에서는 IP 주소 범위를 정의합니다. 내부 에이전트의 IP 주소가 이 범위 내에 있으면 에이전트에서 사용자 정의 목록을 사용합니다.

스마트 보호 소스의 표준 목록 구성

절차

1. **관리** > **스마트 보호** > **스마트 보호 소스**로 이동합니다.
2. **내부 에이전트** 탭을 클릭합니다.
3. **표준 목록 사용(모든 내부 에이전트에 대해)**을 선택합니다.
4. **표준 목록** 링크를 클릭합니다.

   새 화면이 열립니다.
5. **추가**를 클릭합니다.

   새 화면이 열립니다.
6. 스마트 보호 서버의 호스트 이름 또는 IPv4/IPv6 주소를 지정합니다. IPv6 주소를 지정할 경우 주소를 괄호로 묶습니다.

참고

스마트 보호 서버에 연결된 IPv4 및 IPv6 에이전트가 있는 경우 호스트 이름을 지정합니다.

7. **파일 검증 서비스**를 선택합니다. 에이전트에서 HTTP 또는 HTTPS 프로토콜을 사용하여 검색 쿼리를 보냅니다. HTTPS를 사용하면 보다 안전하게 연결할 수 있지만 HTTP가 대역폭을 더 적게 사용합니다.

   a. 에이전트에서 HTTP를 사용하도록 하려면 HTTP 요청에 대한 서버의 수신 포트를 입력합니다. 에이전트에서 HTTPS를 사용하도록 하려면 SSL을 선택하고 HTTPS 요청에 대한 서버의 수신 포트를 입력합니다.

   b. **연결 테스트**를 클릭하여 서버에 대한 연결을 설정할 수 있는지 확인합니다.

팁

수신 포트는 서버 주소의 일부를 구성합니다. 서버 주소를 확인하려면

통합 서버의 경우 OfficeScan 웹 콘솔을 열고 **관리** > **스마트 보호** > **통합 서버**로 이동합니다.

독립 서버의 경우 독립 서버의 콘솔을 열고 **요약** 화면으로 이동합니다.

8. **웹 검증 서비스**를 선택합니다. 에이전트에서 HTTP 프로토콜을 사용하여 웹 검증 쿼리를 보냅니다. HTTPS는 지원되지 않습니다.

   a. HTTP 요청에 대한 서버의 수신 포트를 입력합니다.

   b. **연결 테스트**를 클릭하여 서버에 대한 연결을 설정할 수 있는지 확인합니다.

9. **저장**을 클릭합니다.

   화면이 닫힙니다.

10. 이전 단계를 반복하여 서버를 추가합니다.

11. 화면 맨 위에서 **순서** 또는 **임의**를 선택합니다.

    - **순서**: 에이전트에서 목록에 표시된 순서대로 서버를 선택합니다. **순서**를 선택한 경우, **순서** 열 아래의 화살표를 사용하여 서버를 목록 위/아래로 이동합니다.

- **임의**: 에이전트에서 임의로 서버를 선택합니다.

팁

통합 스마트 보호 서버와 OfficeScan 서버가 같은 엔드포인트에서 실행되므로 두 서버의 트래픽이 많은 시간에는 엔드포인트의 성능이 심각하게 저하될 수 있습니다. OfficeScan 서버 컴퓨터로 전달되는 트래픽을 줄이려면 독립 스마트 보호 서버를 기본 스마트 보호 소스로 할당하고 통합 서버를 백업 소스로 할당합니다.

12. 화면의 기타 작업을 수행합니다.

- 다른 서버에서 목록을 내보낸 경우 이 목록을 이 화면으로 가져오려면 **가져오기**를 클릭한 다음 .dat 파일을 찾습니다. 목록이 화면에 로드됩니다.
- 목록을 .dat 파일로 내보내려면 **내보내기**를 클릭한 다음 **저장**을 클릭합니다.
- 서버의 서비스 상태를 새로 고치려면 **새로 고침**을 클릭합니다.
- 서버 이름을 클릭하여 다음 중 하나를 수행합니다.
  - 서버 정보를 보거나 편집합니다.
  - 웹 검증 서비스 또는 파일 검증 서비스에 대한 전체 서버 주소를 확인합니다.
- 스마트 보호 서버의 콘솔을 열려면 **콘솔 시작**을 클릭합니다.
  - 통합 스마트 보호 서버의 경우 서버의 구성 화면이 표시됩니다.
  - 독립 스마트 보호 서버 및 다른 OfficeScan 서버의 통합 스마트 보호 서버의 경우 콘솔 로그온 화면이 표시됩니다.
- 항목을 삭제하려면, 서버에 대한 확인란을 선택하고 **삭제**를 클릭합니다.

13. **저장**을 클릭합니다.

화면이 닫힙니다.

14. **모든 에이전트에 알림**을 클릭합니다.

스마트 보호 소스의 사용자 지정 목록 구성

절차

1. **관리** > **스마트 보호** > **스마트 보호 소스**로 이동합니다.
2. **내부 에이전트** 탭을 클릭합니다.
3. **에이전트 IP 주소에 기반한 사용자 정의 목록 사용**을 선택합니다.
4. (선택 사항) **사용자 지정 목록의 모든 서버를 사용할 수 없는 경우 표준 목록 사용**을 선택합니다.

   팁

   사용자 지정 소스를 사용할 수 없는 경우 에이전트가 스마트 보호 소스에 연결할 수 있도록 이 기능을 사용하도록 설정하는 것이 좋습니다.

5. **추가**를 클릭합니다.

   새 화면이 열립니다.

6. **IP 범위** 섹션에서 IPv4 주소 범위와 IPv6 주소 범위 중 하나 또는 둘 다를 지정합니다.

   참고

   IPv4 주소를 사용하는 에이전트는 순수 IPv4 또는 이중 스택 스마트 보호 서버에 연결할 수 있습니다. IPv6 주소를 사용하는 에이전트는 순수 IPv6 또는 이중 스택 스마트 보호 서버에 연결할 수 있습니다. IPv4 주소와 IPv6 주소를 둘 다 사용하는 에이전트는 모든 스마트 보호 서버에 연결할 수 있습니다.

7. **프록시 설정** 섹션에서 에이전트가 스마트 보호 서버에 연결하는 데 사용할 프록시 설정을 지정합니다.

   a. **에이전트와 스마트 보호 서버 간의 통신에 프록시 서버 사용**을 선택합니다.

b. 프록시 서버 이름 또는 IPv4/IPv6 주소와 포트 번호를 지정합니다.

c. 프록시 서버에 인증이 필요한 경우 사용자 이름 및 암호를 입력합니다.

8. **사용자 지정 스마트 보호 서버 목록**에서 스마트 보호 서버를 추가합니다.

a. 스마트 보호 서버의 호스트 이름 또는 IPv4/IPv6 주소를 지정합니다. IPv6 주소를 지정할 경우 주소를 괄호로 묶습니다.

참고

스마트 보호 서버에 연결된 IPv4 및 IPv6 에이전트가 있는 경우 호스트 이름을 지정합니다.

---

b. **파일 검증 서비스**를 선택합니다. 에이전트에서 HTTP 또는 HTTPS 프로토콜을 사용하여 검색 쿼리를 보냅니다. HTTPS를 사용하면 보다 안전하게 연결할 수 있지만 HTTP가 대역폭을 더 적게 사용합니다.

i. 에이전트에서 HTTP를 사용하도록 하려면 HTTP 요청에 대한 서버의 수신 포트를 입력합니다. 에이전트에서 HTTPS를 사용하도록 하려면 **SSL**을 선택하고 HTTPS 요청에 대한 서버의 수신 포트를 입력합니다.

ii. **연결 테스트**를 클릭하여 서버에 대한 연결을 설정할 수 있는지 확인합니다.

팁

수신 포트는 서버 주소의 일부를 구성합니다. 서버 주소를 확인하려면

통합 서버의 경우 OfficeScan 웹 콘솔을 열고 **관리** > **스마트 보호** > **통합 서버**로 이동합니다.

독립 서버의 경우 독립 서버의 콘솔을 열고 요약 화면으로 이동합니다.

---

c. **웹 검증 서비스**를 선택합니다. 에이전트에서 HTTP 프로토콜을 사용하여 웹 검증 쿼리를 보냅니다. HTTPS는 지원되지 않습니다.

i. HTTP 요청에 대한 서버의 수신 포트를 입력합니다.

ii. **연결 테스트**를 클릭하여 서버에 대한 연결을 설정할 수 있는지 확인합니다.

d. **목록에 추가**를 클릭합니다.

e. 이전 단계를 반복하여 서버를 추가합니다.

f. **순서** 또는 **임의**를 선택합니다.

- **순서**: 에이전트에서 목록에 표시된 순서대로 서버를 선택합니다. **순서**를 선택한 경우, **순서** 열 아래의 화살표를 사용하여 서버를 목록 위/아래로 이동합니다.
- **임의**: 에이전트에서 임의로 서버를 선택합니다.

팁

통합 스마트 보호 서버와 OfficeScan 서버가 같은 컴퓨터에서 실행되므로 두 서버의 트래픽이 많은 시간에는 컴퓨터의 성능이 심각하게 저하될 수 있습니다. OfficeScan 서버 컴퓨터로 전달되는 트래픽을 줄이려면 독립 스마트 보호 서버를 기본 스마트 보호 소스로 할당하고 통합 서버를 백업 소스로 할당합니다.

g. 화면의 기타 작업을 수행합니다.

- 서버의 서비스 상태를 새로 고치려면 **새로 고침**을 클릭합니다.
- 스마트 보호 서버의 콘솔을 열려면 **콘솔 시작**을 클릭합니다.
  - 통합 스마트 보호 서버의 경우 서버의 구성 화면이 표시됩니다.
  - 독립 스마트 보호 서버 및 다른 OfficeScan 서버의 통합 스마트 보호 서버의 경우 콘솔 로그온 화면이 표시됩니다.
- 항목을 삭제하려면 **삭제**( )를 클릭합니다.

9. **저장**을 클릭합니다.

화면이 닫힙니다. 방금 추가한 목록이 **IP 범위** 테이블 아래에 IP 범위 링크로 표시됩니다.

10. 사용자 지정 목록을 추가하려면 4~8단계를 반복합니다.
11. 화면의 기타 작업을 수행합니다.
    - 목록을 수정하려면 IP 범위 링크를 클릭한 다음 열리는 화면에서 설정을 수정합니다.
    - 목록을 .dat 파일로 내보내려면 **내보내기**를 클릭한 다음 **저장**을 클릭합니다.
    - 다른 서버에서 목록을 내보낸 경우 이 목록을 이 화면으로 가져오려면 **가져오기**를 클릭한 다음 .dat 파일을 찾습니다. 목록이 화면에 로드됩니다.
12. **모든 에이전트에 알림**을 클릭합니다.

에이전트 연결 프록시 설정

스마트 보호 네트워크에 연결하는 데 프록시 인증이 필요한 경우 인증 자격 증명을 지정합니다. 자세한 내용은 OfficeScan 에이전트용 외부 프록시 페이지 15-48를 참조하십시오.

스마트 보호 서버에 연결할 때 에이전트에서 사용할 내부 프록시 설정을 구성합니다. 자세한 내용은 OfficeScan 에이전트용 내부 프록시 페이지 15-47를 참조하십시오.

엔드포인트 위치 설정

OfficeScan에는 에이전트 컴퓨터의 위치를 식별하고 에이전트가 스마트 보호 네트워크에 연결되어 있는지 아니면 스마트 보호 서버에 연결되어 있는지를 확인하는 위치 인식 기능이 있습니다. 이 기능을 통해 에이전트를 위치와 상관없이 보호된 상태로 유지할 수 있습니다.

위치 설정을 구성하려면 엔드포인트 위치 페이지 15-2를 참조하십시오.

Trend Micro Network VirusWall 설치

Trend Micro™ Network VirusWall™ Enforcer를 설치한 경우

- 핫픽스(Network VirusWall Enforcer 2500인 경우 빌드 1047, Network VirusWall Enforcer 1200인 경우 빌드 1013 사용)를 설치합니다.
- 제품에서 에이전트의 검색 방법을 발견할 수 있게 하려면 OPSWAT 엔진을 버전 2.5.1017로 업데이트합니다.

스마트 보호 서비스 사용

이전에 스마트 보호 환경을 설정한 경우 에이전트에서 파일 검증 서비스 및 웹 검증 서비스를 사용할 수 있습니다. 또한 Smart Feedback 설정을 구성할 수 있습니다.

참고

스마트 보호 환경 설정에 대한 자세한 내용은 스마트 보호 서비스 설정 페이지 4-12을 참조하십시오.

파일 검증 서비스에서 제공하는 보호 기능을 활용하려면 에이전트에서 스마트 스캔이라는 검색 방법을 사용해야 합니다. 스마트 스캔에 대한 자세한 내용 및 에이전트에서 스마트 스캔을 사용하는 방법은 검색 방법 유형 페이지 7-8을 참조하십시오.

OfficeScan 에이전트에서 웹 검증 서비스를 사용할 수 있도록 하려면 웹 검증 정책을 구성해야 합니다. 자세한 내용은 웹 검증 정책 페이지 12-5를 참조하십시오.

참고

검색 방법 및 웹 검증 정책에 대한 설정은 세분화되어 있습니다. 요구 사항에 따라 모든 에이전트에 적용되는 설정을 구성하거나 개별 에이전트 또는 에이전트 그룹에 대한 별도의 설정을 구성할 수 있습니다.

Smart Feedback 구성에 대한 지침은 Smart Feedback 페이지 14-63을 참조하십시오.

장 5

OfficeScan 에이전트 설치

이 장에서는 OfficeScan 시스템 요구 사항 및 OfficeScan 에이전트 설치 절차에 대해 설명합니다.

OfficeScan 에이전트 업그레이드에 대한 자세한 내용은 *OfficeScan 설치 및 업그레이드 안내서*를 참조하십시오.

다음과 같은 항목이 포함됩니다.

- OfficeScan 에이전트 새로 설치 페이지 5-2
- 설치 고려 사항 페이지 5-2
- 배포 고려 사항 페이지 5-11
- OfficeScan 에이전트로 마이그레이션 페이지 5-63
- 사후 설치 페이지 5-67
- OfficeScan 에이전트 제거 페이지 5-70

OfficeScan 에이전트 새로 설치

OfficeScan 에이전트는 Microsoft Windows 플랫폼을 실행하는 컴퓨터에 설치할 수 있습니다. OfficeScan는 여러 타사 제품과도 호환됩니다.

시스템 요구 사항의 전체 목록 및 호환되는 타사 제품은 다음 웹 사이트에서 확인하십시오.

http://docs.trendmicro.com/ko-kr/enterprise/officescan.aspx

설치 고려 사항

에이전트를 설치하기 전에 다음 사항을 고려하십시오.

표 5-1. 에이전트 설치 고려 사항

고려 사항	설명
Windows 기능 지원	일부 OfficeScan 에이전트 기능은 특정 Windows 플랫폼에서 사용할 수 없습니다.
IPv6 지원	이중 스택 또는 순수 IPv6 에이전트에 OfficeScan 에이전트를 설치할 수 있습니다. 그러나 • OfficeScan 에이전트를 설치할 수 있는 일부 Windows 운영 체제에서 IPv6 주소 지정을 지원하지 않습니다. • 일부 설치 방법의 경우 OfficeScan 에이전트를 설치하기 위한 특정 요구 사항이 있습니다.
OfficeScan 에이전트 IP 주소	IPv4 주소와 IPv6 주소를 둘 다 사용하는 에이전트의 경우 에이전트가 서버에 등록할 때 사용할 IP 주소를 선택할 수 있습니다.

고려 사항	설명
예외 목록	다음 기능에 대한 예외 목록이 제대로 구성되었는지 확인합니다. • **동작 모니터링**: 중요한 엔드포인트 응용 프로그램을 승인된 프로그램 목록에 추가하여 OfficeScan 에이전트에서 이러한 응용 프로그램을 차단하지 않도록 합니다. 자세한 내용은 동작 모니터링 예외 목록 페이지 9-9를 참조하십시오. • **웹 검증**: 안전하다고 보는 웹 사이트를 승인된 URL 목록에 추가하여 OfficeScan 에이전트에서 이러한 웹 사이트에 대한 액세스를 차단하지 않도록 합니다. 자세한 내용은 웹 검증 정책 페이지 12-5를 참조하십시오.

OfficeScan 에이전트 기능

엔드포인트에서 사용할 수 있는 OfficeScan 에이전트 기능은 운영 체제에 따라 다릅니다.

표 5-2. 서버 플랫폼별 OfficeScan 에이전트 기능

기능	Windows 운영 체제			
	서버 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
수동 검색, 실시간 검색 및 예약 검색	예	예	예	예
구성 요소 업데이트(수동 및 예약 업데이트)	예	예	예	예
업데이트 에이전트	예	예	예	예
웹 검증	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨

기능	Windows 운영 체제			
	서버 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
DCS(Damage Cleanup Services)	예	예	예	예
OfficeScan 방화벽	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨	지원되지만 서버 설치 중에 기본적으로 사용하지 않도록 설정됨
동작 모니터링	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨
	지원 안 됨(64비트)	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨		
다음에 대한 에이전트 자기 보호: • 레지스트리 키 • 프로세스	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨
	지원 안 됨(64비트)	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨		
다음에 대한 에이전트 자기 보호: • 서비스 • 파일 보호	예	예	예	예

기능	Windows 운영 체제			
	서버 2003	Server 2008/ Server Core 2008	Server 2012/ Server Core 2012	Server 2016/ Server Core 2016
장치 제어 (무단 변경 방지 서비스)	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨
	지원 안 됨(64비트)	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨		
데이터 보호 (장치 제어에 대한 데이터 보호 포함)	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(32비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨
	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨	지원되지만(64비트) 기본적으로 사용하지 않도록 설정됨		
의심스러운 연결 설정	예	예	예	예
샘플 제출	예	예	예	예
POP3 메일 검색	예	예	예	예
에이전트 Plug-in Manager	예	예	예	예
독립 모드	예	지원됨(Server) 지원 안 됨(Server Core)	예	예
Smart Feedback	예	예	예	예

표 5-3. 데스크톱 플랫폼의 OfficeScan 에이전트 기능

기능	Windows 운영 체제				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
수동 검색, 실시간 검색 및 예약 검색	예	예	예	예	예
구성 요소 업데이트 (수동 및 예약 업데이트)	예	예	예	예	예
업데이트 에이전트	예	예	예	예	예
웹 검증	예	예	예	지원되지만 Windows UI 모드에 대한 지원이 제한됨	예
DCS(Damage Cleanup Services)	예	예	예	예	예
OfficeScan 방화벽	예	예	예	예	예
동작 모니터링	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)
	지원 안 됨(64비트)	지원됨(64비트) Vista 64비트 지원에는 SP1 또는 SP2가 필요함	지원됨(64비트)	지원됨(64비트)	지원됨(64비트)

기능	Windows 운영 체제				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
다음에 대한 에이전트 자기 보호: • 레지스트리 키 • 프로세스	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)
	지원 안 됨(64비트)	지원됨(64비트) Vista 64비트 지원에는 SP1 또는 SP2가 필요함	지원됨(64비트)	지원됨(64비트)	지원됨(64비트)
다음에 대한 에이전트 자기 보호: • 서비스 • 파일 보호	예	예	예	예	예
장치 제어 (무단 변경 방지 서비스)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)
	지원 안 됨(64비트)	지원됨(64비트) Vista 64비트 지원에는 SP1 또는 SP2가 필요함	지원됨(64비트)	지원됨(64비트)	지원됨(64비트)
데이터 보호 (장치 제어에 대한 데이터 보호 포함)	지원됨(32비트)	지원됨(32비트)	지원됨(32비트)	데스크톱 모드에서 지원됨(32비트)	지원됨(32비트)
	지원됨(64비트)	지원됨(64비트)	지원됨(64비트)	데스크톱 모드에서 지원됨(64비트)	지원됨(64비트)

기능	Windows 운영 체제				
	XP	Vista	Windows 7	Windows 8/8.1	Windows 10
의심스러운 연결 설정	예	예	예	예	예
샘플 제출	예	예	예	예	예
POP3 메일 검색	예	예	예	예	예
에이전트 Plug-in Manager	예	예	예	예	예
독립 모드	예	예	예	예	예
Smart Feedback	예	예	예	예	예

OfficeScan 에이전트 설치 및 IPv6 지원

이 항목에서는 OfficeScan 에이전트를 이중 스택 또는 순수 IPv6 에이전트에 설치할 때의 고려 사항에 대해 설명합니다.

운영 체제

OfficeScan 에이전트는 IPv6 주소 지정을 지원하는 다음 운영 체제에만 설치할 수 있습니다.

- Windows Vista™(모든 에디션)
- Windows Server 2008(모든 에디션)
- Windows 7(모든 에디션)
- Windows Server 2012(모든 에디션)
- Windows 8/8.1(모든 버전)
- Windows 10(Home, Pro, Education 및 Enterprise 버전)
- Windows Server 2016(모든 에디션)

시스템 요구 사항의 전체 목록은 다음 웹 사이트에서 확인하십시오.

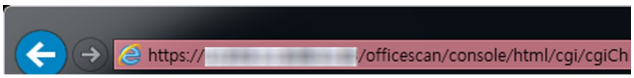
http://docs.trendmicro.com/ko-kr/enterprise/officescan.aspx

설치 방법

순수 IPv6 또는 이중 스택 에이전트에 OfficeScan 에이전트를 설치할 때는 모든 OfficeScan 에이전트 설치 방법을 사용할 수 있습니다. 그러나 일부 설치 방법의 경우 OfficeScan 에이전트를 설치하기 위한 특정 요구 사항이 있습니다.

ServerProtect 일반 서버 마이그레이션 도구는 IPv6 주소 지정을 지원하지 않으므로 이 도구를 사용하여 ServerProtect™를 OfficeScan 에이전트로 마이그레이션할 수 없습니다.

표 5-4. 설치 방법 및 IPv6 지원

설치 방법	요구 사항/고려 사항
웹 설치 페이지 및 브라우저 기반 설치	설치 페이지 URL에는 OfficeScan 서버의 호스트 이름 또는 해당 IP 주소가 포함됩니다.  순수 IPv6 에이전트를 설치하려면 서버가 이중 스택 또는 순수 IPv6이고 해당 호스트 이름 또는 IPv6 주소가 URL의 일부여야 합니다. 이중 스택 에이전트의 경우, 설치 상태 화면에 표시되는 IPv6 주소는 **네트워크** 탭, **에이전트** > **글로벌 에이전트 설정**의 **기본 IP 주소** 섹션에서 선택한 옵션에 따라 달라집니다.
에이전트 패키지 도구	패키지 도구를 실행할 때 에이전트에 업데이트 에이전트 권한을 할당할지 여부를 선택해야 합니다. 순수 IPv6 업데이트 에이전트는 순수 IPv6 또는 이중 스택 에이전트에만 업데이트를 배포할 수 있습니다.
보안 준수, Vulnerability Scanner 및 원격 설치	순수 IPv6 서버는 순수 IPv4 엔드포인트에 OfficeScan 에이전트를 설치할 수 없습니다. 마찬가지로 순수 IPv4 서버는 순수 IPv6 엔드포인트에 OfficeScan 에이전트를 설치할 수 없습니다.

에이전트 IP 주소

IPv6 주소 지정을 지원하는 환경에 설치된 OfficeScan 서버는 다음 OfficeScan 에이전트를 관리할 수 있습니다.

- 순수 IPv6 호스트 컴퓨터에 설치된 OfficeScan 서버는 순수 IPv6 에이전트를 관리할 수 있습니다.
- 이중 스택 호스트 컴퓨터에 설치되고 IPv4 주소와 IPv6 주소가 둘 다 할당된 OfficeScan 서버는 순수 IPv6, 이중 스택 및 순수 IPv4 에이전트를 관리할 수 있습니다.

에이전트를 설치하거나 업그레이드한 후 에이전트는 IP 주소를 사용하여 서버에 등록합니다.

- 순수 IPv6 에이전트는 해당 IPv6 주소를 사용하여 등록합니다.
- 순수 IPv4 에이전트는 해당 IPv4 주소를 사용하여 등록합니다.
- 이중 스택 에이전트는 해당 IPv4 또는 IPv6 주소를 사용하여 등록합니다. 이러한 에이전트에서 사용할 IP 주소를 선택할 수 있습니다.

서버에 등록할 때 이중 스택 에이전트에서 사용하는 IP 주소 구성

이 설정은 이중 스택 OfficeScan 서버에서만 사용할 수 있으며 이중 스택 에이전트에 의해서만 적용됩니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **네트워크** 탭을 클릭합니다.
3. **기본 IP 주소** 섹션으로 이동합니다.
4. 다음 옵션 중에서 선택합니다.
   - **IPv4만**: 에이전트에서 해당 IPv4 주소를 사용합니다.
   - **IPv4를 먼저 사용한 후 IPv6 사용**: 에이전트에서 해당 IPv4 주소를 먼저 사용합니다. 에이전트에서 IPv4 주소를 사용하여 등록할 수 없는 경우 해당 IPv6 주소를 사용합니다. 두 IP 주소를 사용하여 등록에 실패

한 경우 에이전트는 이 선택 사항의 IP 주소 우선 순위를 사용하여 다시 시도합니다.

- **IPv6을 먼저 사용한 후 IPv4 사용**: 에이전트에서 해당 IPv6 주소를 먼저 사용합니다. 에이전트에서 IPv6 주소를 사용하여 등록할 수 없는 경우 해당 IPv4 주소를 사용합니다. 두 IP 주소를 사용하여 등록에 실패한 경우 에이전트는 이 선택 사항의 IP 주소 우선 순위를 사용하여 다시 시도합니다.

5. **저장**을 클릭합니다.

배포 고려 사항

이 섹션에서는 OfficeScan 에이전트를 새로 설치하는 여러 OfficeScan 에이전트 설치 방법을 요약합니다. 모든 설치 방법에는 대상 컴퓨터의 로컬 관리자 권한이 필요합니다.

에이전트를 설치하고 IPv6 지원을 사용하려는 경우 OfficeScan 에이전트 설치 및 IPv6 지원 페이지 5-8의 지침을 참조하십시오.

표 5-5. 설치 배포 고려 사항

설치 방법/운영 체제 지원	배포 고려 사항					
	WAN 배포	중앙 관리 방식	사용자 개입 필요	IT 리소스 필요	대량 배포	대역폭 사용량
웹 설치 페이지 Windows Server Core 2008 및 Windows UI 모드의 Windows 8/8.1/ Server 2012/Server Core 2012를 제외한 모든 운영 체제에서 지원됨	아니요	아니요	예	아니요	아니요	높음

설치 방법/운영 체제 지원	배포 고려 사항					
	WAN 배포	**중앙 관리 방식**	**사용자 개입 필요**	**IT 리소스 필요**	**대량 배포**	**대역폭 사용량**
브라우저 기반 설치 모든 운영 체제에서 지원됨 **참고** Windows UI 모드로 작동하는 Windows 8, 8.1 또는 Windows Server 2012에서는 지원되지 않음	아니요	아니요	예	예	아니요	높음(설치가 동시에 시작되는 경우)
UNC 기반 설치 모든 운영 체제에서 지원됨	아니요	아니요	예	예	아니요	높음(설치가 동시에 시작되는 경우)

설치 방법/운영 체제 지원	배포 고려 사항					
	WAN 배포	**중앙 관리 방식**	**사용자 개입 필요**	**IT 리소스 필요**	**대량 배포**	**대역폭 사용량**
원격 설치 다음을 제외한 모든 운영 체제에서 지원됨: • Windows Vista Home Basic 및 Home Premium Edition • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1(기본 버전) • Windows 10 Home Edition	아니요	예	아니요	예	아니요	높음
로그인 스크립트 설정 모든 운영 체제에서 지원됨	아니요	아니요	예	예	아니요	높음(설치가 동시에 시작되는 경우)
에이전트 패키지 도구 모든 운영 체제에서 지원됨	아니요	아니요	예	예	아니요	낮음(예약된 경우)

설치 방법/운영 체제 지원	배포 고려 사항					
	WAN 배포	**중앙 관리 방식**	**사용자 개입 필요**	**IT 리소스 필요**	**대량 배포**	**대역폭 사용량**
에이전트 패키지 도구(Microsoft SMS를 통해 배포된 MSI 패키지) 모든 운영 체제에서 지원됨	예	예	예/아니요	예	예	낮음(예약된 경우)
에이전트 패키지 도구(Active Directory를 통해 배포되는 MSI 패키지) 모든 운영 체제에서 지원됨	예	예	예/아니요	예	예	높음(설치가 동시에 시작되는 경우)
에이전트 디스크 이미지 모든 운영 체제에서 지원됨	아니요	아니요	아니요	예	아니요	낮음

설치 방법/운영 체제 지원	배포 고려 사항					
	WAN 배포	**중앙 관리 방식**	**사용자 개입 필요**	**IT 리소스 필요**	**대량 배포**	**대역폭 사용량**
Trend Micro Vulnerability Scanner (TMVS) 다음을 제외한 모든 운영 체제에서 지원됨: • Windows Vista Home Basic 및 Home Premium Edition • Windows XP Home Edition • Windows 8/8.1(기본 버전) • Windows 10 Home Edition	아니요	예	아니요	예	아니요	높음

설치 방법/운영 체제 지원	배포 고려 사항					
	WAN 배포	중앙 관리 방식	사용자 개입 필요	IT 리소스 필요	대량 배포	대역폭 사용량
보안 준수 설치 다음을 제외한 모든 운영 체제에서 지원됨: • Windows Vista Home Basic 및 Home Premium Edition • Windows XP Home Edition • Windows 7 Home Basic/ Home Premium • Windows 8/8.1(기본 버전) • Windows 10 Home Edition	아니요	예	아니요	예	아니요	높음

웹 설치 페이지 설치

다음 플랫폼을 실행하는 엔드포인트에 OfficeScan 서버를 설치한 경우에는 웹 설치 페이지에서 OfficeScan 에이전트 프로그램을 설치할 수 있습니다.

- IIS(Internet Information Server) 7.0이 포함된 Windows Server 2008
- IIS(Internet Information Server) 7.5가 포함된 Windows Server 2008 R2
- IIS(Internet Information Server) 8.0이 포함된 Windows Server 2012
- IIS(Internet Information Server) 8.5가 포함된 Windows Server 2012 R2

- IIS(Internet Information Server) 10.0이 포함된 Windows Server 2016

웹 설치 페이지에서 설치하려면 다음이 필요합니다.

- ActiveX™ 컨트롤을 사용할 수 있도록 보안 수준이 설정된 Internet Explorer 필요한 버전은 다음과 같습니다.
  - Windows Vista 및 Windows Server 2008인 경우 7.0
  - Windows 7인 경우 8.0
  - Windows 8/8.1 및 Windows Server 2012인 경우 10.0
  - Windows 10 및 Windows Server 2016인 경우 11.0
- 엔드포인트에서 관리자 권한

웹 설치 페이지에서 OfficeScan 에이전트를 설치하도록 사용자에게 다음 지침을 보냅니다. 전자 메일을 통해 설치 알림을 보내려면 브라우저 기반 설치 시작 페이지 5-19을 참조하십시오.

웹 설치 페이지에서 설치

절차

1. 기본 제공되는 관리자 계정을 사용하여 엔드포인트에 로그온합니다.

   참고

   Windows 7, 8, 8.1, 10 플랫폼의 경우 먼저 기본 제공되는 관리자 계정을 사용하도록 설정해야 합니다. Windows 7, 8, 8.1 및 10에서는 내장 관리자 계정이 기본적으로 사용하지 않도록 설정되어 있습니다. 자세한 내용은 Microsoft 지원 사이트(http://technet.microsoft.com/en-us/library/dd744293%28WS.10%29.aspx)를 참조하십시오.

2. Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012, 2012R2 또는 2016을 실행하는 엔드포인트에 설치하려면 다음 단계를 수행합니다.

   a. Internet Explorer를 시작하고 OfficeScan 서버 URL(예: https://<OfficeScan 서버 이름>:4343/officescan)을 신뢰할 수 있는 사이트 목록에 추가합니다. Windows 7에서 **도구** > **인터넷 옵션** > **보안** 탭으로

이동하여 **신뢰할 수 있는 사이트** 아이콘을 선택한 다음 **사이트**를 클릭하여 목록에 액세스합니다.

b. **ActiveX 컨트롤을 자동으로 사용자에게 확인**을 사용하도록 Internet Explorer 보안 설정을 수정합니다. Windows 7에서 **도구** > **인터넷 옵션** > **보안** 탭으로 이동하여 **사용자 지정 수준...**을 클릭합니다.

3. Internet Explorer 창을 열고 다음을 입력합니다.

   https://<OfficeScan 서버 이름>:<포트>/officescan

4. 로그온 페이지에서 **설치 관리자** 링크를 클릭하여 다음 설치 옵션을 표시합니다.

   - **브라우저 기반 에이전트 설치**(Internet Explorer에만 해당): 운영 체제별로 화면의 지침을 따릅니다.
   - **MSI 에이전트 설치**: 운영 체제에 따라 32비트 또는 64비트 패키지를 다운로드하고 화면의 지침을 따릅니다.

   참고

   메시지가 표시되면 ActiveX 컨트롤 설치를 허용합니다.

5. 설치가 완료되면 Windows 시스템 트레이에 OfficeScan 에이전트 아이콘이 나타납니다.

   참고

   시스템 트레이에 표시되는 아이콘 목록에 대해서는 OfficeScan 에이전트 아이콘 페이지 15-26을 참조하십시오.

브라우저 기반 설치

네트워크의 사용자에게 OfficeScan 에이전트를 설치하도록 지시하는 전자 메일 메시지를 설정합니다. 사용자가 전자 메일에 제공된 OfficeScan 에이전트 설치 관리자 링크를 클릭하면 설치가 시작됩니다.

OfficeScan 에이전트를 설치하기 전에

- OfficeScan 에이전트 설치 요구 사항을 확인합니다.
- 네트워크에서 현재 보안 위험에 대해 보호되어 있지 않은 컴퓨터를 확인합니다. 다음 작업을 수행합니다.
  - Trend Micro Vulnerability Scanner를 실행합니다. 이 도구는 엔드포인트를 분석하여 지정된 IP 주소 범위에 따라 설치된 바이러스 백신 소프트웨어를 찾습니다. 자세한 내용은 Vulnerability Scanner 사용 페이지 5-38를 참조하십시오.
  - 보안 준수를 실행합니다. 자세한 내용은 관리되지 않는 엔드포인트에 대한 보안 준수 페이지 15-68를 참조하십시오.

브라우저 기반 설치 시작

절차

1. **에이전트** > **에이전트 설치** > **브라우저 기반**로 이동합니다.
2. 필요한 경우 전자 메일 메시지의 제목 행을 수정합니다.
3. **전자 메일 만들기**를 클릭합니다.

   기본 메일 프로그램이 열립니다.
4. 받는 사람에게 전자 메일을 보냅니다.

UNC 기반 설치 수행

AutoPcc.exe는 보호되지 않은 엔드포인트에 OfficeScan 에이전트를 설치하고 프로그램 파일과 구성 요소를 업데이트하는 독립 프로그램입니다. UNC(Uniform Naming Convention) 경로를 통해 AutoPcc를 사용하려면 엔드포인트가 도메인에 속해 있어야 합니다.

절차

1. **에이전트** > **에이전트 설치** > **UNC 기반**으로 이동합니다.

- AutoPcc.exe를 사용하여 보호되지 않은 엔드포인트에 OfficeScan 에이전트를 설치하려면

  a. 서버 컴퓨터에 연결합니다. UNC 경로로 이동합니다.

     ₩₩<서버 컴퓨터 이름>₩ofcscan

  b. AutoPcc.exe를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

- AutoPcc.exe를 사용하는 원격 데스크톱 설치의 경우

  a. 콘솔 모드로 원격 데스크톱 연결(Mstsc.exe)을 엽니다. 그러면 AutoPcc.exe 설치가 세션 0에서 강제 실행됩니다.

  b. ₩₩<서버 컴퓨터 이름>₩ofcscan 디렉터리로 이동하여 AutoPcc.exe를 실행합니다.

OfficeScan 웹 콘솔에서 원격으로 설치

OfficeScan 에이전트를 네트워크에 연결된 하나 이상의 엔드포인트에 원격으로 설치합니다. 원격 설치를 수행하려면 대상 엔드포인트에 대한 관리자 권한이 있어야 합니다. 원격 설치에서는 이미 OfficeScan 서버를 실행하는 엔드포인트에 OfficeScan 에이전트를 설치하지 않습니다.

참고

이 설치 방법은 Windows XP Home, Vista Home Basic 및 Home Premium Edition, Windows 7 Home Basic 및 Home Premium Edition(32비트 및 64비트 버전), Windows 8/8.1(32비트 및 64비트 기본 버전), Windows 10 Home Edition을 실행하는 엔드포인트에서 사용할 수 없습니다. 순수 IPv6 서버는 순수 IPv4 에이전트에 OfficeScan 에이전트를 설치할 수 없습니다. 마찬가지로 순수 IPv4 서버는 순수 IPv6 에이전트에 OfficeScan 에이전트를 설치할 수 없습니다.

절차

1. Windows 버전에 맞는 설치 전 작업을 수행하십시오.

   - Windows XP를 실행하는 경우

a. 기본 제공되는 도메인 관리자 계정을 사용 가능하도록 설정하고 계정 암호를 설정합니다.

b. 엔드포인트에서 **내 컴퓨터** > **도구** > **폴더 옵션** > **보기** 탭으로 이동한 후 **모든 사용자에게 동일한 폴더 공유 권한을 지정**을 사용하지 않도록 설정합니다.

c. **시작** > **프로그램** > **Windows 방화벽** > **예외** 탭으로 이동한 후 **파일 및 프린터 공유** 예외를 사용하도록 설정합니다.

d. **시작** > **실행**을 클릭하고 `services.msc`를 입력하여 Microsoft Management Console을 열고 **원격 레지스트리** 및 **원격 프로시저 호출** 서비스를 시작합니다. 를 설치할 때 기본 제공되는 관리자 계정 및 암호를 사용합니다.

- Windows Vista를 실행하는 경우

a. 기본 제공되는 도메인 관리자 계정을 사용 가능하도록 설정하고 계정 암호를 설정합니다.

b. **시작** > **제어판** > **보안** > **Windows 방화벽** > **설정 변경**을 클릭합니다.

c. **예외** 탭을 클릭하고 **파일 및 프린터 공유** 예외를 사용하도록 설정합니다.

d. **시작** > **실행**을 클릭하고 `services.msc`를 입력하여 Microsoft Management Console을 열고 **원격 레지스트리** 및 **원격 프로시저 호출** 서비스를 시작합니다. OfficeScan 에이전트를 설치할 때 기본 제공되는 관리자 계정 및 암호를 사용합니다.

- Windows 7, Windows 8(Pro, Enterprise), Windows 8.1, Windows 10(Pro, Education, Enterprise) 또는 Windows Server 2012/2016을 실행하는 경우:

a. 기본 제공되는 도메인 관리자 계정을 사용 가능하도록 설정하고 계정 암호를 설정합니다.

b. **시작** > **프로그램** > **관리 도구** > **고급 보안이 포함된 Windows 방화벽**으로 이동합니다.

c. 네트워크 환경에 따라 "도메인", "개인" 및/또는 "공용"에 대해 **파일 및 프린터 공유** 규칙을 사용하도록 설정합니다.

d. **시작** > **실행**을 클릭하고 `services.msc`를 입력하여 Microsoft Management Console을 열고 **원격 레지스트리** 및 **원격 프로시저 호출** 서비스를 시작합니다. OfficeScan 에이전트를 설치할 때 기본 제공되는 관리자 계정 및 암호를 사용합니다.

2. 웹 콘솔에서 **에이전트** > **에이전트 설치** > **원격**로 이동합니다.

3. 대상 엔드포인트를 선택합니다.

   - **도메인 및 엔드포인트** 목록에는 네트워크에 있는 모든 Windows 도메인이 표시됩니다. 도메인 아래의 엔드포인트를 표시하려면 도메인 이름을 두 번 클릭합니다. 엔드포인트를 선택한 다음 **추가**를 클릭합니다.
   - 생각해 둔 특정 엔드포인트 이름이 있는 경우에는 페이지 맨 위의 **엔드포인트 검색** 필드에 엔드포인트 이름을 입력하고 Enter 키를 누릅니다.

   OfficeScan에서 대상 엔드포인트의 사용자 이름과 암호를 입력하라는 메시지를 표시합니다. 계속하려면 관리자 계정의 사용자 이름과 암호를 사용합니다.

4. 사용자 이름과 암호를 입력한 다음 **로그인**을 클릭합니다.

   선택한 엔드포인트 테이블에 대상 엔드포인트가 나타납니다.

5. 엔드포인트를 더 추가하려면 3단계와 4단계를 반복합니다.

6. OfficeScan 에이전트를 대상 엔드포인트에 설치할 준비가 완료되면 **설치**를 클릭합니다.

   확인 상자가 나타납니다.

7. **예**를 클릭하여 대상 엔드포인트에 OfficeScan 에이전트를 설치할지 확인합니다.

   프로그램 파일이 각 대상 엔드포인트에 복사되는 동안 진행률 화면이 나타납니다.

OfficeScan에서 대상 엔드포인트에 대한 설치를 완료하면 엔드포인트 이름이 **선택한 엔드포인트** 목록에서 사라지고 **도메인 및 엔드포인트** 목록에 빨간색 확인 표시와 함께 나타납니다.

도메인 및 엔드포인트 목록에 모든 대상 엔드포인트가 빨간 확인 표시와 함께 나타나면 원격 설치가 완료된 것입니다.

참고

여러 엔드포인트에 설치할 경우 OfficeScan은 실패한 설치를 모두 로그(자세한 내용은 새 설치 로그 페이지 18-15 참조)에 기록하지만 그로 인해 다른 설치가 연기되지는 않습니다. **설치**를 클릭한 후에 설치를 감독할 필요는 없습니다. 설치 결과를 보려면 나중에 로그를 확인하십시오.

로그인 스크립트 설정을 사용한 설치

로그인 스크립트 설정을 사용하면 보호되지 않은 엔드포인트가 네트워크에 로그온할 때 해당 엔드포인트에 OfficeScan 에이전트를 자동으로 설치할 수 있습니다. 로그인 스크립트 설정에서는 서버 로그인 스크립트에 AutoPcc.exe라는 프로그램을 추가합니다.

AutoPcc.exe는 관리되지 않는 엔드포인트에 OfficeScan 에이전트를 설치하고 프로그램 파일과 구성 요소를 업데이트합니다. 로그인 스크립트를 통해 AutoPcc를 사용하려면 엔드포인트가 도메인에 속해 있어야 합니다.

OfficeScan 에이전트 설치

AutoPcc.exe는 보호되지 않는 Windows Server 2003 엔드포인트가 로그인 스크립트를 수정한 서버에 로그온하면 해당 엔드포인트에 OfficeScan 에이전트를 자동으로 설치합니다. 그러나 AutoPcc.exe는 Windows Vista, 7, 8, 8.1, 10, Server 2008, Server 2012 및 Server 2016 엔드포인트에는 OfficeScan 에이전트를 자동으로 설치하지 않습니다. 사용자가 서버 컴퓨터에 연결하여 ₩₩<서버 컴퓨터 이름>₩ofcscan으로 이동한 후 AutoPcc.exe를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택해야 합니다.

AutoPcc.exe를 사용하는 원격 데스크톱 설치의 경우

- 엔드포인트를 Mstsc.exe /console mode 모드로 실행해야 합니다. 그러면 AutoPcc.exe 설치가 세션 0에서 강제 실행됩니다.
- 드라이브를 "ofcscan" 폴더에 매핑하고 해당 위치에서 AutoPcc.exe를 실행합니다.

프로그램 및 구성 요소 업데이트

AutoPcc.exe는 프로그램 파일과 바이러스 백신, Anti-spyware 및 Damage Cleanup Services 구성 요소를 업데이트합니다.

Windows 서버 스크립트

기존 로그인 스크립트가 이미 있는 경우 로그인 스크립트 설정에서 AutoPcc.exe를 실행하는 명령을 추가합니다. 그렇지 않으면 OfficeScan에서 AutoPcc.exe를 실행할 명령이 포함된 ofcscan.bat라는 배치 파일을 만듭니다.

로그인 스크립트 설정 끝 부분에 다음 내용이 추가됩니다.

₩₩<Server_name>₩ofcscan₩autopcc

여기서 각 항목은 다음과 같습니다.

- <Server_name>은 OfficeScan 서버 컴퓨터의 엔드포인트 이름 또는 IP 주소입니다.
- "ofcscan"은 서버의 OfficeScan 공유 폴더 이름입니다.
- "autopcc"는 OfficeScan 에이전트를 설치하는 autopcc 실행 파일의 링크입니다.

네트워크 로그온 공유 디렉토리를 통한 로그인 스크립트 위치

- Windows Server 2003: ₩₩Windows 2003 server₩system drive₩windir ₩sysvol₩domain₩scripts₩ofcscan.bat
- Windows Server 2008: ₩₩Windows 2008 server₩system drive₩windir ₩sysvol₩domain₩scripts₩ofcscan.bat
- Windows Server 2012: ₩₩Windows 2012 server₩system drive₩windir ₩sysvol₩domain₩scripts₩ofcscan.bat
- Windows Server 2016: ₩₩Windows 2016 server₩system drive₩windir ₩sysvol₩domain₩scripts₩ofcscan.bat

로그인 스크립트 설정을 사용하여 로그인 스크립트에 Autopcc.exe 추가

절차

1. 서버 설치를 실행하는 데 사용한 엔드포인트의 Windows 시작 메뉴에서 **프로그램** > **Trend Micro OfficeScan 서버 <서버 이름>** > **로그인 스크립트 설정**을 클릭합니다.

   로그인 스크립트 설정 유틸리티가 로드됩니다. 네트워크의 모든 도메인이 표시된 트리가 콘솔에 표시됩니다.

2. 로그인 스크립트를 설정할 서버를 찾아 선택한 다음 **선택**을 클릭합니다. 서버가 주 도메인 컨트롤러인지 확인하고, 서버에 대한 관리자 액세스 권한이 있는지 확인합니다.

   로그인 스크립트 설정에서 사용자 이름과 암호를 입력하라는 프롬프트를 표시합니다.

3. 사용자 이름 및 암호를 입력합니다. **확인**을 클릭하여 계속합니다.

   사용자 선택 화면이 나타납니다. 서버에 로그온한 사용자의 프로필이 **사용자** 목록에 표시됩니다. **선택한 사용자** 목록에는 로그인 스크립트를 수정할 사용자의 프로필이 표시됩니다.

4. 사용자 프로필의 로그인 스크립트를 수정하려면 **사용자** 목록에서 사용자 프로필을 선택한 다음 **추가**를 클릭합니다.

5. 모든 사용자의 로그인 스크립트를 수정하려면 **모두 추가**를 클릭합니다.

6. 이전에 선택한 사용자 프로필을 제외하려면 **선택한 사용자** 목록에서 이름을 선택한 다음 **삭제**를 클릭합니다.

7. 선택을 초기화하려면 **모두 삭제**를 클릭합니다.

8. 모든 대상 사용자 프로필이 **선택한 사용자** 목록에 있으면 **적용**을 클릭합니다.

   서버 로그인 스크립트를 수정했다는 내용의 메시지가 표시됩니다.

9. **확인**을 클릭합니다.

로그인 스크립트 설정 초기 화면으로 돌아갑니다.

10. 다른 서버의 로그인 스크립트를 수정하려면 2-4단계를 반복합니다.

11. 로그인 스크립트 설정을 닫으려면 **종료**를 클릭합니다.

에이전트 패키지 도구를 사용한 설치

에이전트 패키지 도구는 CD-ROM과 같은 기존 미디어를 사용하여 사용자에게 보낼 수 있는 설치 패키지를 만듭니다. 사용자는 에이전트 엔드포인트에서 이 패키지를 실행하여 OfficeScan 에이전트를 설치하거나 업그레이드하고 구성 요소를 업데이트할 수 있습니다.

에이전트 패키지 도구는 OfficeScan 에이전트 또는 구성 요소를 낮은 대역폭의 원격 사무실에 있는 에이전트에 배포할 때 특히 유용합니다. 에이전트 패키지 도구를 사용하여 설치한 OfficeScan 에이전트는 패키지를 만든 위치를 서버에 보고합니다.

에이전트 패키지 도구를 사용하려면 다음 사항이 필요합니다.

- 350MB의 사용 가능한 디스크 공간
- Windows Installer 2.0(MSI 패키지 실행용)

패키지 배포 지침

1. 사용자에게 패키지를 보내고 EXE 또는 MSI 파일을 두 번 클릭하여 엔드포인트에서 OfficeScan 에이전트 패키지를 실행하도록 요청합니다.

   참고

   패키지가 생성된 서버에 보고하는 OfficeScan 에이전트를 사용하는 사용자에게만 패키지를 보냅니다.

2. Windows Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 또는 Server 2016을 실행하는 엔드포인트에서 EXE 패키지를 설치할 사용자가 있는 경우 사용자에게 EXE 파일을 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택하도록 지시합니다.

3. MSI 파일을 만든 경우 다음 작업을 수행하여 패키지를 배포합니다.

   - Active Directory 또는 Microsoft SMS를 사용합니다.

     자세한 내용은 Active Directory를 사용하여 MSI 패키지 배포 페이지 5-31 또는 Microsoft SMS를 사용하여 MSI 패키지 배포 페이지 5-32 항목을 참조하십시오.

4. 명령 프롬프트에서 MSI 패키지를 시작하여 Windows XP, Vista, Server 2008, 7, 8, 8.1, 10, Server 2012 또는 Server 2016을 실행하는 원격 엔드포인트에 OfficeScan 에이전트를 자동으로 설치합니다.

에이전트 패키지에 대한 검색 방법 지침

패키지에 대한 검색 방법을 선택합니다. 자세한 내용은 검색 방법 유형 페이지 7-8를 참조하십시오.

패키지에 포함된 구성 요소는 선택한 검색 방법에 따라 다릅니다. 각 검색 방법에 사용할 수 있는 구성 요소에 대한 자세한 내용은 OfficeScan 에이전트 업데이트 페이지 6-26를 참조하십시오.

검색 방법을 선택하기 전에 패키지를 효율적으로 배포할 수 있도록 다음 지침을 기록해 둡니다.

- 패키지를 사용하여 에이전트를 이 OfficeScan 버전으로 업그레이드하려면 웹 콘솔에서 도메인 수준 검색 방법을 확인합니다. 콘솔에서 **에이전트** > **에이전트 관리**로 이동하여 에이전트가 속한 에이전트 트리 도메인을 선택하고 **설정** > **검색 설정** > **검색 방법**을 클릭합니다. 도메인 수준 검색 방법은 패키지 검색 방법과 일치해야 합니다.
- 패키지를 사용하여 OfficeScan 에이전트를 새로 설치하는 경우 에이전트 그룹화 설정을 확인합니다. 웹 콘솔에서 **에이전트** > **에이전트 그룹화**로 이동합니다.
- 에이전트 그룹화 기준이 NetBIOS, Active Directory 또는 DNS 도메인인 경우 대상 엔드포인트가 속한 도메인을 확인합니다. 도메인이 있을 경우 도메인에 대해 구성된 검색 방법을 확인합니다. 도메인이 없는 경우 루트 수준 검색 방법을 확인합니다. 에이전트 트리에서 루트 도메인 아이콘( )을 선택하고 **설정** > **검색 설정** > **검색 방법**을 클릭하면 됩니다. 도메인 또는 루트 수준 검색 방법은 패키지 검색 방법과 일치해야 합니다.

- 에이전트 그룹화 기준이 사용자 정의 에이전트 그룹인 경우 **그룹화 우선 순위** 및 **소스**를 확인합니다.

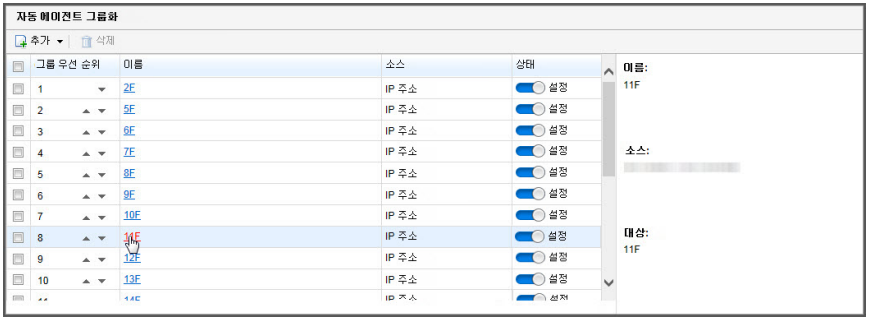


그림 5-1. 자동 에이전트 그룹화 미리 보기 창

대상 엔드포인트가 특정 소스에 속한 경우 해당 **대상**을 확인합니다. 대상은 에이전트 트리에 표시되는 도메인 이름입니다. 에이전트는 설치 후 해당 도메인에 대한 검색 방법을 적용합니다.

- 패키지를 사용하여 이 OfficeScan 버전을 사용하는 에이전트의 구성 요소를 업데이트하려면 에이전트가 속한 에이전트 트리 도메인에 대해 구성된 검색 방법을 확인합니다. 도메인 수준 검색 방법은 패키지 검색 방법과 일치해야 합니다.

에이전트 패키지 도구를 사용하여 설치 패키지 만들기

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩ClientPackager로 이동합니다.
2. ClnPack.exe를 두 번 클릭하여 도구를 실행합니다.

   에이전트 패키지 도구 콘솔이 열립니다.
3. 만들 패키지의 유형을 선택합니다.

표 5-6. 에이전트 패키지 유형

패키지 유형	설명
설정	**설치**를 선택하여 패키지를 실행 파일로 만듭니다. 패키지는 서버에서 현재 사용할 수 있는 구성 요소와 함께 OfficeScan 에이전트 프로그램을 설치합니다. 대상 엔드포인트에 이전 에이전트 버전이 설치된 경우, 실행 파일을 실행하면 에이전트가 업그레이드됩니다.
업데이트	서버에서 현재 사용할 수 있는 구성 요소가 들어 있는 패키지를 만들려면 **업데이트**를 선택합니다. 패키지가 실행 파일로 만들어집니다. 에이전트 엔드포인트에서 구성 요소를 업데이트하는 데 문제가 있을 경우 이 패키지를 사용합니다.
MSI	Microsoft Installer Package 포맷을 따르는 패키지를 만들려면 **MSI**를 선택합니다. 이 패키지도 서버에서 현재 사용할 수 있는 구성 요소와 함께 OfficeScan 에이전트 프로그램을 설치합니다. 대상 엔드포인트에 이전 에이전트 버전이 설치된 경우, MSI 파일을 실행하면 에이전트가 업그레이드됩니다.

4. 패키지를 만들 운영 체제를 선택합니다. 해당 운영 체제 유형을 실행하는 엔드포인트에만 패키지를 배포합니다. 다른 운영 체제 유형에 패키지를 배포하려면 또 다른 패키지를 만듭니다.

5. 에이전트 패키지가 배포되는 검색 방법을 선택합니다.

   검색 방법을 선택하는 방식에 대한 지침은 에이전트 패키지에 대한 검색 방법 지침 페이지 5-27을 참조하십시오.

6. **도메인** 아래에서 다음 중 하나를 선택합니다.

   - **에이전트가 도메인을 자동으로 보고할 수 있음**: OfficeScan 에이전트를 설치한 후 에이전트는 OfficeScan 서버 데이터베이스를 쿼리하고 도메인 설정을 서버에 보고합니다.
   - 목록의 모든 도메인: 에이전트 패키지 도구는 OfficeScan 서버와 동기화하고 현재 사용되는 도메인을 에이전트 트리에 나열합니다.

7. **옵션** 아래의 다음 항목 중에서 선택합니다.

옵션	설명
자동 모드	이 옵션은 백그라운드에서 실행되면서 설치 상태 창을 표시하지 않고 에이전트에서 보이지 않는 상태로 에이전트 엔드포인트에 설치되는 패키지를 만듭니다. 대상 엔드포인트에 원격으로 패키지를 배포하려는 경우에는 이 옵션을 사용하도록 설정합니다.
최신 버전으로 강제 덮어쓰기	이 옵션은 에이전트의 구성 요소 버전을 서버에서 현재 사용할 수 있는 버전으로 덮어씁니다. 서버 및 에이전트의 구성 요소가 동기화되도록 하려면 이 옵션을 사용하도록 설정합니다.
설치 전 검색 사용 안 함(처음 설치에만 해당)	대상 엔드포인트에 OfficeScan 에이전트가 설치되지 않은 경우 OfficeScan 에이전트를 설치하기 전에 먼저 패키지가 엔드포인트에서 보안 위험을 검색합니다. 대상 엔드포인트가 보안 위험에 감염되지 않은 경우에는 설치 전 검색을 사용하지 않도록 설정합니다. 설치 전 검색을 사용하도록 설정한 경우 다음과 같은 엔드포인트의 가장 취약한 영역에서 바이러스/악성 프로그램을 검색합니다. • 부트 영역 및 부트 디렉터리(부트 바이러스 대상) • Windows 폴더 • Program Files 폴더

8. **업데이트 에이전트 기능** 아래에서 업데이트 에이전트가 배포할 수 있는 기능을 선택합니다.

9. **구성 요소** 아래에서 패키지에 포함할 구성 요소 및 기능을 선택합니다.

   - 구성 요소에 대한 자세한 내용은 OfficeScan 구성 요소 및 프로그램 페이지 6-2을 참조하십시오.
   - 데이터 보호 모듈은 데이터 보호를 설치하고 활성화한 경우에만 사용할 수 있습니다. 데이터 보호에 대한 자세한 내용은 데이터 보호 시작 페이지 3-1을 참조하십시오.

10. **원본 파일** 옆에 표시된 ofcscan.ini 파일의 위치가 정확한지 확인합니다. 경로를 수정하려면 (...)를 클릭하여 ofcscan.ini 파일을 찾아봅니다.

    기본적으로 이 파일은 OfficeScan 서버의 <서버 설치 폴더>₩PCCSRV 폴더에 있습니다.

11. **출력 파일**에서 (...)을 클릭하여 OfficeScan 에이전트 패키지를 만들 위치를 지정하고 패키지 파일 이름(예: `AgentSetup.exe`)을 입력합니다.

12. **만들기**를 클릭합니다.

    에이전트 패키지 도구에서 패키지를 만들고 나면 "패키지를 만들었습니다"라는 메시지가 나타납니다. 이전 단계에서 지정한 디렉터리에서 패키지를 찾습니다.

13. 패키지를 배포합니다.

Active Directory를 사용하여 MSI 패키지 배포

Active Directory 기능을 활용하여 여러 에이전트 엔드포인트에 MSI 패키지를 동시에 배포합니다.

MSI 파일을 만드는 방법에 대한 자세한 내용은 에이전트 패키지 도구를 사용한 설치 페이지 5-26를 참조하십시오.

절차

1. 다음을 수행합니다.

   - Windows Server 2003 이하 버전의 경우

     a. Active Directory 콘솔을 엽니다.

     b. MSI 패키지를 배포할 조직 구성 단위(OU)를 마우스 오른쪽 단추로 클릭하고 **속성**을 클릭합니다.

     c. **그룹 정책** 탭에서 **새로 만들기**를 클릭합니다.

   - Windows Server 2008 및 Windows Server 2008 R2의 경우

     a. **그룹 정책 관리 콘솔**을 엽니다. **시작** > **제어판** > **관리 도구** > **그룹 정책 관리**를 클릭합니다.

     b. 콘솔 트리에서 편집할 GPO가 포함된 포리스트 및 도메인의 **그룹 정책 개체**를 확장합니다.

     c. 편집할 GPO를 마우스 오른쪽 단추로 클릭하고 **편집**을 클릭합니다. 그러면 **그룹 정책 개체 편집기**가 열립니다.

   - Windows Server 2012 및 Windows Server 2016의 경우:

a. **그룹 정책 관리 콘솔**을 엽니다. **서버 관리** > **도구** > **그룹 정책 관리**를 클릭합니다.

b. 콘솔 트리에서 편집할 GPO가 포함된 포리스트 및 도메인의 **그룹 정책 개체**를 확장합니다.

c. 편집할 GPO를 마우스 오른쪽 단추로 클릭하고 **편집**을 클릭합니다. 그러면 **그룹 정책 개체 편집기**가 열립니다.

2. **컴퓨터 구성** 또는 **사용자 구성**을 선택하고 여기에서 **소프트웨어 설정**을 엽니다.

팁

엔드포인트에 로그온한 사용자와 관계없이 MSI 패키지 설치를 성공적으로 완료하려면 **사용자 구성** 대신 **컴퓨터 구성**을 선택하는 것이 좋습니다.

---

3. **소프트웨어 설정** 아래에서 **소프트웨어 설치**를 마우스 오른쪽 단추로 클릭하고 **새로 만들기** 및 **패키지**를 선택합니다.

4. MSI 패키지를 찾아 선택합니다.

5. 배포 방법을 선택하고 **확인**을 클릭합니다.

   - **지정됨**: 사용자가 다음에 엔드포인트에 로그온하거나(사용자 구성을 선택한 경우) 엔드포인트가 다시 시작될 때(컴퓨터 구성을 선택한 경우) MSI 패키지가 자동으로 배포됩니다. 이 방법에서는 사용자가 작업을 수행하지 않아도 됩니다.

   - **게시됨**: MSI 패키지를 실행하려면 사용자에게 제어판으로 이동하여 프로그램 추가/제거 화면을 열고 네트워크에 프로그램을 추가/설치하는 옵션을 선택하도록 지시합니다. OfficeScan 에이전트 MSI 패키지가 표시되면 사용자가 OfficeScan 에이전트 설치를 계속할 수 있습니다.

Microsoft SMS를 사용하여 MSI 패키지 배포

서버에 Microsoft BackOffice SMS가 설치된 경우에는 Microsoft SMS(System Management Server)를 사용하여 MSI 패키지를 배포합니다.

MSI 파일을 만드는 방법에 대한 자세한 내용은 에이전트 패키지 도구를 사용한 설치 페이지 5-26를 참조하십시오.

SMS 서버가 대상 엔드포인트에 패키지를 배포하려면 OfficeScan 서버에서 MSI 파일을 가져와야 합니다.

- 로컬: SMS 서버와 OfficeScan 서버가 동일한 엔드포인트에 있습니다.
- 원격: SMS 서버와 OfficeScan 서버가 서로 다른 엔드포인트에 있습니다.

Microsoft SMS를 사용하여 설치할 때 알려진 문제점:

- SMS 콘솔의 **런타임** 열에 "알 수 없음"이 표시됩니다.
- 설치에 실패한 경우에도 SMS 프로그램 모니터에 설치가 완료되었음을 알리는 설치 상태가 표시될 수 있습니다.

  설치가 성공적으로 완료되었는지 확인하는 방법은 사후 설치 페이지 5-67를 참조하십시오.

다음은 Microsoft SMS 2.0 및 2003을 사용하는 경우에 적용할 수 있는 지침입니다.

로컬로 패키지 가져오기

절차

1. **SMS 관리자** 콘솔을 엽니다.
2. **트리** 탭에서 **패키지**를 클릭합니다.
3. **작업** 메뉴에서 **새로 만들기** > **정의로 패키지 만들기**를 클릭합니다.

   정의로 패키지 만들기 마법사의 **시작** 화면이 나타납니다.
4. **다음**을 클릭합니다.

   패키지 정의 화면이 나타납니다.
5. **찾아보기**를 클릭합니다.

   열기 화면이 나타납니다.

6. 에이전트 패키지 도구에서 만든 MSI 패키지 파일을 찾아 선택한 다음 **열기**를 클릭합니다.

   패키지 정의 화면에 MSI 패키지 이름이 나타납니다. 패키지에 "OfficeScan 에이전트" 및 프로그램 버전이 표시됩니다.

7. **다음**을 클릭합니다.

   원본 파일 화면이 나타납니다.

8. **항상 원본 디렉터리에서 파일 얻기**를 클릭하고 **다음**을 클릭합니다.

   만들려는 패키지 이름 및 원본 디렉터리가 표시된 **원본 디렉터리** 화면이 나타납니다.

9. **사이트 서버의 로컬 드라이브**를 클릭합니다.

10. **찾아보기**를 클릭하고 MSI 파일이 들어 있는 원본 디렉터리를 선택합니다.

11. **다음**을 클릭합니다.

    마법사가 패키지를 만듭니다. 프로세스가 완료되면 **SMS 관리자** 콘솔에 패키지 이름이 표시됩니다.

원격으로 패키지 가져오기

절차

1. OfficeScan 서버에서 에이전트 패키지 도구를 사용하여 확장자가 EXE인 설치 패키지를 만듭니다(MSI 패키지는 만들 수 없음). 자세한 내용은 에이전트 패키지 도구를 사용한 설치 페이지 5-26를 참조하십시오.

2. 원본을 저장할 엔드포인트에서 공유 폴더를 만듭니다.

3. SMS 관리자 콘솔을 엽니다.

4. **트리** 탭에서 **패키지**를 클릭합니다.

5. **작업** 메뉴에서 **새로 만들기** > **정의로 패키지 만들기**를 클릭합니다.

   정의로 패키지 만들기 마법사의 **시작** 화면이 나타납니다.

6. **다음**을 클릭합니다.

   패키지 정의 화면이 나타납니다.

7. **찾아보기**를 클릭합니다.

   열기 화면이 나타납니다.

8. MSI 패키지 파일을 찾습니다. 해당 파일은 사용자가 생성한 공유 폴더에 있습니다.

9. **다음**을 클릭합니다.

   원본 파일 화면이 나타납니다.

10. **항상 원본 디렉터리에서 파일 얻기**를 클릭하고 **다음**을 클릭합니다.

    원본 디렉터리 화면이 나타납니다.

11. **네트워크 경로(UNC 이름)**를 클릭합니다.

12. **찾아보기**를 클릭하고 MSI 파일이 있는 원본 디렉터리를 선택합니다(사용자가 생성한 공유 폴더).

13. **다음**을 클릭합니다.

    마법사가 패키지를 만듭니다. 프로세스가 완료되면 **SMS 관리자** 콘솔에 패키지 이름이 표시됩니다.

대상 엔드포인트에 패키지 배포

절차

1. **트리** 탭에서 **광고**를 클릭합니다.

2. **작업** 메뉴에서 **모든 작업** > **소프트웨어 배포**를 클릭합니다.

   소프트웨어 배포 마법사의 **시작** 화면이 나타납니다.

3. **다음**을 클릭합니다.

   패키지 화면이 나타납니다.

4. **기존 패키지 배포**를 클릭한 다음 생성한 설치 패키지 이름을 클릭합니다.
5. **다음**을 클릭합니다.

   배포 지점 화면이 나타납니다.
6. 패키지를 복사할 배포 지점을 선택하고 **다음**을 클릭합니다.

   프로그램 광고 화면이 나타납니다.
7. OfficeScan 에이전트 설치 패키지를 광고하려면 **예**를 클릭한 후 **다음**을 클릭합니다.

   광고 대상 화면이 나타납니다.
8. **찾아보기**를 클릭하여 대상 엔드포인트를 선택합니다.

   수집 찾아보기 화면이 나타납니다.
9. **모든 Windows NT 시스템**을 클릭합니다.
10. **확인**을 클릭합니다.

    광고 대상 화면이 다시 나타납니다.
11. **다음**을 클릭합니다.

    광고 이름 화면이 나타납니다.
12. 텍스트 상자에 광고의 이름 및 설명을 입력하고 **다음**을 클릭합니다.

    하위 수집에 광고 화면이 나타납니다.
13. 패키지를 하위 수집에 광고할 것인지 선택합니다. 지정한 수집의 구성원에만 프로그램을 광고할지 또는 하위 수집의 구성원에 광고할지 선택합니다.
14. **다음**을 클릭합니다.

    광고 예약 화면이 나타납니다.
15. 날짜 및 시간을 입력하거나 선택하여 OfficeScan 에이전트 설치 패키지를 광고할 시기를 지정합니다.

참고

특정 날짜에 Microsoft SMS에서 패키지 광고를 중지하도록 하려면 **예. 이 광고를 만료합니다**를 클릭한 다음 **만료 날짜 및 시간** 목록 상자에 날짜 및 시간을 지정합니다.

16. **다음**을 클릭합니다.

    프로그램 지정 화면이 나타납니다.

17. **예, 프로그램을 지정합니다**를 클릭하고 **다음**을 클릭합니다.

    Microsoft SMS가 광고를 생성하여 SMS 관리자 콘솔에 표시합니다.

18. Microsoft SMS가 광고된 프로그램(즉, OfficeScan 에이전트 프로그램)을 대상 엔드포인트에 배포하면 각 대상 엔드포인트에 화면이 표시됩니다. 사용자에게 **예**를 클릭하고 마법사가 제공하는 지침에 따라 엔드포인트에 OfficeScan 에이전트를 설치하도록 지시합니다.

에이전트 디스크 이미지를 사용하여 설치

디스크 이미징 기술을 통해 디스크 이미징 소프트웨어를 사용하여 OfficeScan 에이전트의 이미지를 만들고 네트워크상의 다른 컴퓨터에 이 이미지를 복제할 수 있습니다.

각 OfficeScan 에이전트 설치에는 서버에서 에이전트를 개별적으로 식별할 수 있게 해 주는 GUID(Globally Unique Identifier)가 필요합니다. ImgSetup.exe라는 OfficeScan 프로그램을 사용하여 복제본마다 다른 GUID를 만드십시오.

OfficeScan 에이전트의 디스크 이미지 만들기

절차

1. 엔드포인트에 OfficeScan 에이전트를 설치합니다.
2. <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩ImgSetup에서 ImgSetup.exe를 이 엔드포인트에 복사합니다.

3. 이 엔드포인트에서 ImgSetup.exe를 실행합니다.

   그러면 HKEY_LOCAL_MACHINE 아래에 RUN 레지스트리 키가 만들어집니다.

4. 디스크 이미징 소프트웨어를 사용하여 OfficeScan 에이전트의 디스크 이미지를 만듭니다.

5. 복제본을 다시 시작합니다.

   ImgSetup.exe가 자동으로 시작되어 새 GUID 값 하나를 만듭니다. OfficeScan 에이전트는 이 새 GUID를 서버에 보고하고, 서버는 새 OfficeScan 에이전트에 대한 새 레코드를 만듭니다.

경고!

OfficeScan 데이터베이스에 두 컴퓨터가 같은 이름으로 나타나지 않게 하려면 복제된 OfficeScan 에이전트의 엔드포인트 이름이나 도메인 이름을 수동으로 변경합니다.

Vulnerability Scanner 사용

Vulnerability Scanner를 사용하여 설치된 바이러스 백신 솔루션을 찾고, 네트워크에서 보호되지 않은 컴퓨터를 검색하고, OfficeScan 에이전트를 컴퓨터에 설치할 수 있습니다.

Vulnerability Scanner 사용 시 고려 사항

Vulnerability Scanner 사용 여부를 결정할 때 도움을 받으려면 다음을 고려합니다.

- 네트워크 관리 페이지 5-39
- 네트워크 토폴로지 및 아키텍처 페이지 5-39
- 소프트웨어/하드웨어 사양 페이지 5-40
- 도메인 구조 페이지 5-40
- 네트워크 트래픽 페이지 5-41

- 네트워크 크기 페이지 5-41

네트워크 관리

표 5-7. 네트워크 관리

설정	VULNERABILITY SCANNER의 효율성
엄격한 보안 정책으로 관리	높은 수준의 효율성. Vulnerability Scanner가 모든 컴퓨터에 바이러스 백신 소프트웨어가 설치되어 있는지 여부를 보고합니다.
관리 책임을 여러 사이트로 분산	중간 수준의 효율성
중앙 집중형 관리	중간 수준의 효율성
서비스 외주	중간 수준의 효율성
사용자가 자신의 컴퓨터 관리	효율적이지 않음. Vulnerability Scanner는 네트워크에서 바이러스 백신 설치를 검색하므로 사용자가 자신의 컴퓨터를 검색하는 용도로는 적합하지 않습니다.

네트워크 토폴로지 및 아키텍처

표 5-8. 네트워크 토폴로지 및 아키텍처

설정	VULNERABILITY SCANNER의 효율성
단일 위치	높은 수준의 효율성. Vulnerability Scanner를 사용하면 전체 IP 세그먼트를 검색하고 OfficeScan 에이전트를 LAN에 쉽게 설치할 수 있습니다.
고속 연결을 사용하는 여러 위치	중간 수준의 효율성
저속 연결을 사용하는 여러 위치	효율적이지 않음. 각 위치에서 Vulnerability Scanner를 실행해야 하며 OfficeScan 에이전트 설치를 로컬 OfficeScan 서버로 전송해야 합니다.
원격 컴퓨터 및 격리된 컴퓨터	중간 수준의 효율성

소프트웨어/하드웨어 사양

표 5-9. 소프트웨어/하드웨어 사양

설정	VULNERABILITY SCANNER의 효율성
Windows 일반 서버 기반 운영 체제	높은 수준의 효율성. Vulnerability Scanner는 NT 기반 운영 체제를 실행하는 컴퓨터에 원격으로 OfficeScan 에이전트를 쉽게 설치할 수 있습니다.
혼합된 운영 체제	중간 수준의 효율성 Vulnerability Scanner는 Windows 일반 서버 기반 운영 체제를 실행하는 컴퓨터에만 설치할 수 있습니다.
데스크톱 관리 소프트웨어	효율적이지 않음. Vulnerability Scanner는 데스크톱 관리 소프트웨어와 함께 사용할 수 없습니다. 그러나 이 소프트웨어는 OfficeScan 에이전트 설치의 진행률을 추적하는 데 도움이 됩니다.

도메인 구조

표 5-10. 도메인 구조

설정	VULNERABILITY SCANNER의 효율성
Microsoft Active Directory	높은 수준의 효율성. Vulnerability Scanner에서 도메인 관리자 계정을 지정하여 OfficeScan 에이전트를 원격 설치하도록 지정합니다.
작업 그룹	효율적이지 않음. Vulnerability Scanner는 다른 관리 계정 및 암호를 사용하는 컴퓨터에 설치하는 데 어려움이 있을 수 있습니다.
Novell™ 디렉터리 서비스	효율적이지 않음. OfficeScan 에이전트를 설치하려면 Vulnerability Scanner에 Windows 도메인 계정이 있어야 합니다.
피어 투 피어(P2P)	효율적이지 않음. Vulnerability Scanner는 다른 관리 계정 및 암호를 사용하는 컴퓨터에 설치하는 데 어려움이 있을 수 있습니다.

네트워크 트래픽

표 5-11. 네트워크 트래픽

설정	VULNERABILITY SCANNER의 효율성
LAN 연결	높은 수준의 효율성
512Kbps	중간 수준의 효율성
T1 연결 이상	중간 수준의 효율성
전화 접속	효율적이지 않음. OfficeScan 에이전트 설치를 완료하는 데 시간이 오래 걸립니다.

네트워크 크기

표 5-12. 네트워크 크기

설정	VULNERABILITY SCANNER의 효율성
대기업	높은 수준의 효율성. 네트워크가 커질수록 OfficeScan 에이전트 설치를 확인하기 위해 Vulnerability Scanner의 필요성이 더 커집니다.
중소기업	중간 수준의 효율성 소규모 네트워크에서는 OfficeScan 에이전트를 설치할 때 Vulnerability Scanner가 옵션이 될 수 있습니다. 다른 OfficeScan 에이전트 설치 방법이 구현하기 훨씬 쉬울 수 있습니다.

Vulnerability Scanner를 사용하여 OfficeScan 에이전트를 설치할 때의 지침

다음과 같은 경우 Vulnerability Scanner는 OfficeScan 에이전트를 설치하지 않습니다.

- OfficeScan 서버 또는 다른 보안 소프트웨어가 대상 호스트 컴퓨터에 설치되어 있는 경우
- 원격 엔드포인트에서 Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7 Home Basic, Windows 7 Home

Premium, Windows 8(기본 버전), Windows 8.1(기본 버전) 또는 Windows 10 Home을 실행하는 경우

참고

배포 고려 사항 페이지 5-11에 설명된 다른 설치 방법을 사용하여 대상 호스트 컴퓨터에 OfficeScan 에이전트를 설치할 수 있습니다.

Vulnerability Scanner를 사용하여 OfficeScan 에이전트를 설치하기 전에 다음 단계를 수행하십시오.

- Windows Vista(Business, Enterprise 또는 Ultimate Edition), Windows 7(Professional, Enterprise, Ultimate Edition), Windows 8(Pro, Enterprise), Windows 8.1(Pro, Enterprise), Windows 10(Pro, Education, Enterprise), Windows Server 2012(모든 에디션) 또는 Windows Server 2016(모든 에디션):

  1. 기본 제공되는 관리자 계정을 사용 가능하도록 설정하고 계정 암호를 설정합니다.
  2. **시작** > **프로그램** > **관리 도구** > **고급 보안이 포함된 Windows 방화벽**을 클릭합니다.
  3. 도메인 프로필, 개인 프로필 및 공개 프로필에 방화벽 상태를 "꺼짐"으로 설정합니다.
  4. **시작** > **실행**을 클릭하고 `services.msc`를 입력하여 Microsoft Management Console을 열고 **원격 레지스트리** 서비스를 시작합니다. OfficeScan 에이전트를 설치할 때 기본 제공되는 관리자 계정 및 암호를 사용합니다.

- Windows XP Professional(32비트 또는 64비트 버전)의 경우

  1. Windows 탐색기를 열고 **도구** > **폴더 옵션**을 클릭합니다.
  2. **보기** 탭을 클릭하고 **모든 사용자에게 동일한 폴더 공유 권한을 지정(권장)**을 사용하지 않도록 설정합니다.

취약점 검색 방법

취약점 검색에서는 대상 호스트 컴퓨터에 보안 소프트웨어가 설치되어 있는지 확인하고 보호되지 않는 호스트 컴퓨터에 OfficeScan 에이전트를 설치할 수 있습니다.

취약점 검색을 실행하는 방법에는 여러 가지가 있습니다.

표 5-13. 취약점 검색 방법

방법	세부 정보
수동 취약점 검색	요청 시 관리자가 취약점 검색을 실행할 수 있습니다.
DHCP 검색	관리자가 DHCP 서버로부터 IP 주소를 요청하는 호스트 컴퓨터에서 취약점 검색을 실행할 수 있습니다. Vulnerability Scanner는 포트 67(DHCP 요청에 대한 DHCP 서버의 수신 포트)을 수신합니다. 호스트 컴퓨터의 DHCP 요청을 탐지한 경우 해당 컴퓨터에서 취약점 검색이 실행됩니다. **참고** Vulnerability Scanner가 Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 또는 Windows Server 2012에서 시작된 경우에는 DHCP 요청을 탐지할 수 없습니다.
예약된 취약점 검색	관리자가 구성한 일정에 따라 취약점 검색이 자동으로 실행됩니다.

Vulnerability Scanner가 실행된 후 대상 호스트 컴퓨터에 OfficeScan 에이전트의 상태가 표시됩니다. 상태는 다음 중 하나일 수 있습니다.

- **일반**: OfficeScan 에이전트가 실행 중이고 제대로 작동합니다.
- **비정상**: OfficeScan 에이전트 서비스가 실행되지 않거나 에이전트에 실시간 보호 기능이 없습니다.
- **설치되어 있지 않음**: TMListen 서비스가 누락되었거나 OfficeScan 에이전트가 설치되지 않았습니다.

- **연결할 수 없음**: Vulnerability Scanner가 호스트 컴퓨터와 연결할 수 없고 OfficeScan 에이전트의 상태를 확인할 수 없습니다.

수동 취약점 검색 실행

절차

1. OfficeScan 서버 컴퓨터에서 취약점 검색을 실행하려면 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩TMVS로 이동하여 TMVS.exe를 두 번 클릭합니다. **Trend Micro Vulnerability Scanner** 콘솔이 나타납니다. Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 또는 Server 2012/2016을 실행하는 다른 엔드포인트에서 취약점 검색을 실행하려면

   a. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility로 이동합니다.

   b. TMVS 폴더를 다른 엔드포인트에 복사합니다.

   c. 다른 엔드포인트에서 TMVS 폴더를 열고 TMVS.exe를 두 번 클릭합니다.

      Trend Micro Vulnerability Scanner 콘솔이 나타납니다.

   참고

   터미널 서버에서는 이 도구를 시작할 수 없습니다.

2. **수동 검색** 섹션으로 이동합니다.

3. 확인할 엔드포인트의 IP 주소 범위를 입력합니다.

   a. IPv4 주소 범위를 입력합니다.

   참고

   Vulnerability Scanner는 순수 IPv4 또는 이중 스택 호스트 컴퓨터에서 실행되는 경우 IPv4 주소 범위만 쿼리할 수 있습니다. Vulnerability Scanner는 클래스 B IP 주소 범위(예: 168.212.1.1~168.212.254.254)만 지원합니다.

b. IPv6 주소 범위의 경우 IPv6 접두사와 길이를 입력합니다.

> **참고**
>
> Vulnerability Scanner는 순수 IPv6 또는 이중 스택 호스트 컴퓨터에서 실행되는 경우 IPv6 주소 범위만 쿼리할 수 있습니다.

4. **설정**을 클릭합니다.

   설정 화면이 나타납니다.

5. 다음 설정을 구성합니다.

옵션	설명
Ping 설정	취약점 검색에서 이전 단계에 지정된 IP 주소를 "ping"하여 해당 IP 주소가 현재 사용 중인지 확인할 수 있습니다. 대상 호스트 컴퓨터에서 IP 주소를 사용하는 경우 Vulnerability Scanner는 호스트 컴퓨터의 운영 체제를 확인할 수 있습니다. 자세한 내용은 Ping 설정 페이지 5-58를 참조하십시오.
컴퓨터 설명 검색 방법	"ping" 명령에 응답하는 호스트 컴퓨터에 대해 Vulnerability Scanner는 호스트 컴퓨터에 대한 추가 정보를 검색할 수 있습니다. 자세한 내용은 엔드포인트 설명 검색 방법 페이지 5-56를 참조하십시오.
제품 쿼리	Vulnerability Scanner는 대상 호스트 컴퓨터에 보안 소프트웨어가 설치되어 있는지 확인할 수 있습니다. 자세한 내용은 제품 쿼리 페이지 5-52를 참조하십시오.
OfficeScan 서버 설정	Vulnerability Scanner가 보호되지 않는 호스트 컴퓨터에 OfficeScan 에이전트를 자동으로 설치하도록 하려면 이러한 설정을 구성합니다. 이러한 설정은 OfficeScan 에이전트의 상위 서버와 호스트 컴퓨터에 로그온할 때 사용되는 관리 자격 증명을 식별합니다. 자세한 내용은 OfficeScan 서버 설정 페이지 5-60를 참조하십시오.

옵션	설명
	참고 특정 조건에서는 OfficeScan 에이전트를 대상 호스트 컴퓨터에 설치하지 못할 수도 있습니다. 자세한 내용은 Vulnerability Scanner를 사용하여 OfficeScan 에이전트를 설치할 때의 지침 페이지 5-41를 참조하십시오.
알림	Vulnerability Scanner는 OfficeScan 관리자에게 취약점 검색 결과를 보낼 수 있습니다. 또한 보호되지 않는 호스트 컴퓨터에 알림을 표시할 수 있습니다. 자세한 내용은 알림 페이지 5-56를 참조하십시오.
결과 저장	취약점 검색에서는 관리자에게 취약점 검색 결과를 보낼 뿐 아니라 결과를 .csv 파일에 저장할 수도 있습니다. 자세한 내용은 취약점 검색 결과 페이지 5-58를 참조하십시오.

6. **확인**을 클릭합니다.
7. **시작**을 클릭합니다.

   취약점 검색 결과가 **수동 검색** 탭 아래의 **결과** 테이블에 표시됩니다.

참고

엔드포인트에서 Windows 2008 또는 Windows Server 2012를 실행하는 경우에는 MAC 주소 정보가 **결과** 테이블에 표시되지 않습니다.

8. 결과를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **내보내기**를 클릭하고 파일을 저장할 폴더를 찾고 파일 이름을 입력한 다음 **저장**을 클릭합니다.

DHCP 검색 실행

절차

1. TMVS.ini 파일 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩TMVS에 있음)에서 DHCP 설정을 구성합니다.

표 5-14. TMVS.ini 파일의 **DHCP** 설정

설정	설명
DhcpThreadNum=x	DHCP 모드의 스레드 번호를 지정합니다. 최소값은 3이고, 최대값은 100입니다. 기본값은 8입니다.
DhcpDelayScan=x	요청하는 엔드포인트에 바이러스 방역 소프트웨어가 설치되어 있는지 확인하기 전에 대기하는 지연 시간(초)입니다. 최소값은 0(대기하지 않음)이고, 최대값은 600입니다. 기본값은 30입니다.
LogReport=x	0이면 기록이 사용되지 않고, 1이면 기록이 사용됩니다. Vulnerability Scanner에서 OfficeScan 서버에 검색 결과를 보냅니다. 웹 콘솔의 **시스템 이벤트 로그** 화면에 로그가 표시됩니다.
OsceServer=x	OfficeScan 서버의 IP 주소 또는 DNS 이름입니다.
OsceServerPort=x	OfficeScan 서버의 Web server 포트입니다.

2. OfficeScan 서버 컴퓨터에서 취약점 검색을 실행하려면 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩TMVS로 이동하여 TMVS.exe를 두 번 클릭합니다. **Trend Micro Vulnerability Scanner** 콘솔이 나타납니다. Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 또는 Server 2012/2016을 실행하는 다른 엔드포인트에서 취약점 검색을 실행하려면

   a. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility로 이동합니다.

   b. TMVS 폴더를 다른 엔드포인트에 복사합니다.

   c. 다른 엔드포인트에서 TMVS 폴더를 열고 TMVS.exe를 두 번 클릭합니다.

      Trend Micro Vulnerability Scanner 콘솔이 나타납니다.

> **참고**
>
> 터미널 서버에서는 이 도구를 시작할 수 없습니다.

3. **수동 검색** 섹션에서 **설정**을 클릭합니다.

설정 화면이 나타납니다.

4. 다음 설정을 구성합니다.

옵션	설명
제품 쿼리	Vulnerability Scanner는 대상 호스트 컴퓨터에 보안 소프트웨어가 설치되어 있는지 확인할 수 있습니다. 자세한 내용은 제품 쿼리 페이지 5-52를 참조하십시오.
OfficeScan 서버 설정	Vulnerability Scanner가 보호되지 않는 호스트 컴퓨터에 OfficeScan 에이전트를 자동으로 설치하도록 하려면 이러한 설정을 구성합니다. 이러한 설정은 OfficeScan 에이전트의 상위 서버와 호스트 컴퓨터에 로그온할 때 사용되는 관리 자격 증명을 식별합니다. 자세한 내용은 OfficeScan 서버 설정 페이지 5-60를 참조하십시오. **참고** 특정 조건에서는 OfficeScan 에이전트를 대상 호스트 컴퓨터에 설치하지 못할 수도 있습니다. 자세한 내용은 Vulnerability Scanner를 사용하여 OfficeScan 에이전트를 설치할 때의 지침 페이지 5-41를 참조하십시오.
알림	Vulnerability Scanner는 OfficeScan 관리자에게 취약점 검색 결과를 보낼 수 있습니다. 또한 보호되지 않는 호스트 컴퓨터에 알림을 표시할 수 있습니다. 자세한 내용은 알림 페이지 5-56를 참조하십시오.
결과 저장	취약점 검색에서는 관리자에게 취약점 검색 결과를 보낼 뿐 아니라 결과를 .csv 파일에 저장할 수도 있습니다. 자세한 내용은 취약점 검색 결과 페이지 5-58를 참조하십시오.

5. **확인**을 클릭합니다.

6. **결과** 테이블에서 **DHCP 검색** 탭을 클릭합니다.

참고

DHCP 검색 탭은 Windows Server 2008, Windows 7, Windows 8, Windows 8.1, Windows 10 및 Windows Server 2012를 실행하는 컴퓨터에서 사용할 수 없습니다.

7. **시작**을 클릭합니다.

   Vulnerability Scanner가 DHCP 요청을 수신하고, 네트워크에 로그온하는 컴퓨터에 대해 취약점을 확인하기 시작합니다.

8. 결과를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **내보내기**를 클릭하고 파일을 저장할 폴더를 찾고 파일 이름을 입력한 다음 **저장**을 클릭합니다.

예약된 취약점 검색 구성

절차

1. OfficeScan 서버 컴퓨터에서 취약점 검색을 실행하려면 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩TMVS로 이동하여 TMVS.exe를 두 번 클릭합니다. **Trend Micro Vulnerability Scanner** 콘솔이 나타납니다. Windows Server 2003, Server 2008, Vista, 7, 8, 8.1, 10 또는 Server 2012/2016을 실행하는 다른 엔드포인트에서 취약점 검색을 실행하려면

   a. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility로 이동합니다.

   b. TMVS 폴더를 다른 엔드포인트에 복사합니다.

   c. 다른 엔드포인트에서 TMVS 폴더를 열고 TMVS.exe를 두 번 클릭합니다.

      Trend Micro Vulnerability Scanner 콘솔이 나타납니다.

참고

터미널 서버에서는 이 도구를 시작할 수 없습니다.

2. **예약 검색** 섹션으로 이동합니다.

3. **추가/편집**을 클릭합니다.

   예약 검색 화면이 표시됩니다.

4. 예약된 취약점 검색의 이름을 입력합니다.

5. 확인할 엔드포인트의 IP 주소 범위를 입력합니다.

   a. IPv4 주소 범위를 입력합니다.

   참고

   Vulnerability Scanner는 순수 IPv4 또는 이중 스택 호스트 컴퓨터에서 실행되는 경우 IPv4 주소 범위만 쿼리할 수 있습니다. Vulnerability Scanner는 클래스 B IP 주소 범위(예: 168.212.1.1~168.212.254.254)만 지원합니다.

   b. IPv6 주소 범위의 경우 IPv6 접두사와 길이를 입력합니다.

   참고

   Vulnerability Scanner는 순수 IPv6 또는 이중 스택 호스트 컴퓨터에서 실행되는 경우 IPv6 주소 범위만 쿼리할 수 있습니다.

6. 24시간 포맷을 사용하여 **예약**에 대해 시작 시간을 지정한 다음 검색을 실행할 빈도를 선택합니다. 매일, 매주 또는 매달 중에서 선택합니다.

7. 사용할 취약점 검색 설정 집합을 선택합니다.

   a. 수동 취약점 검색 설정을 구성한 경우 이 설정을 사용하려면 **현재 설정 사용**을 선택합니다.

      수동 취약점 검색 설정에 대한 자세한 내용은 수동 취약점 검색 실행 페이지 5-44을 참조하십시오.

   b. 수동 취약점 검색 설정을 지정하지 않았거나 다른 설정 집합을 사용하려면 **설정 수정**을 선택하고 **설정**을 클릭합니다.

      설정 화면이 나타납니다.

   c. 다음 설정을 구성합니다.

Ping 설정	취약점 검색에서 이전 단계에 지정된 IP 주소를 "ping"하여 해당 IP 주소가 현재 사용 중인지 확인할 수 있습니다. 대상 호스트 컴퓨터에서 IP 주소를 사용하는 경우 Vulnerability Scanner는 호스트 컴퓨터의 운영 체제를 확인할 수 있습니다. 자세한 내용은 Ping 설정 페이지 5-58를 참조하십시오.
컴퓨터 설명 검색 방법	"ping" 명령에 응답하는 호스트 컴퓨터에 대해 Vulnerability Scanner는 호스트 컴퓨터에 대한 추가 정보를 검색할 수 있습니다. 자세한 내용은 엔드포인트 설명 검색 방법 페이지 5-56를 참조하십시오.
제품 쿼리	Vulnerability Scanner는 대상 호스트 컴퓨터에 보안 소프트웨어가 설치되어 있는지 확인할 수 있습니다. 자세한 내용은 제품 쿼리 페이지 5-52를 참조하십시오.
OfficeScan 서버 설정	Vulnerability Scanner가 보호되지 않는 호스트 컴퓨터에 OfficeScan 에이전트를 자동으로 설치하도록 하려면 이러한 설정을 구성합니다. 이러한 설정은 OfficeScan 에이전트의 상위 서버와 호스트 컴퓨터에 로그온할 때 사용되는 관리 자격 증명을 식별합니다. 자세한 내용은 OfficeScan 서버 설정 페이지 5-60를 참조하십시오. **참고** 특정 조건에서는 OfficeScan 에이전트를 대상 호스트 컴퓨터에 설치하지 못할 수도 있습니다. 자세한 내용은 Vulnerability Scanner를 사용하여 OfficeScan 에이전트를 설치할 때의 지침 페이지 5-41를 참조하십시오.
알림	Vulnerability Scanner는 OfficeScan 관리자에게 취약점 검색 결과를 보낼 수 있습니다. 또한 보호되지 않는 호스트 컴퓨터에 알림을 표시할 수 있습니다. 자세한 내용은 알림 페이지 5-56를 참조하십시오.

결과 저장	취약점 검색에서는 관리자에게 취약점 검색 결과를 보낼 뿐 아니라 결과를 .csv 파일에 저장할 수도 있습니다. 자세한 내용은 취약점 검색 결과 페이지 5-58를 참조하십시오.

8. **확인**을 클릭합니다.

   예약 검색 화면이 닫힙니다. 만든 예약된 취약점 검색은 **예약 검색** 섹션에 표시됩니다. 알림을 사용하도록 설정한 경우 Vulnerability Scanner에서 예약된 취약점 검색 결과를 보냅니다.

9. 예약된 취약점 검색을 즉시 실행하려면 **지금 실행**을 클릭합니다.

   취약점 검색 결과가 **예약 검색** 탭 아래의 **결과** 테이블에 표시됩니다.

참고

엔드포인트에서 Windows 2008 또는 Windows Server 2012를 실행하는 경우에는 MAC 주소 정보가 **결과** 테이블에 표시되지 않습니다.

10. 결과를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **내보내기**를 클릭하고 파일을 저장할 폴더를 찾고 파일 이름을 입력한 다음 **저장**을 클릭합니다.

취약점 검색 설정

Trend Micro Vulnerability Scanner(TMVS.exe) 또는 TMVS.ini 파일에서 취약점 검색 설정을 구성할 수 있습니다.

참고

Vulnerability Scanner에 대한 디버그 로그를 수집하는 방법에 대한 자세한 내용은 LogServer.exe를 사용하는 서버 디버그 로그 페이지 18-3를 참조하십시오.

제품 쿼리

Vulnerability Scanner는 에이전트에 보안 소프트웨어가 설치되어 있는지 확인할 수 있습니다. 다음 표에는 Vulnerability Scanner에서 보안 제품을 확인하는 방법이 나와 있습니다.

표 5-15. Vulnerability Scanner에서 확인하는 보안 제품

제품	설명
ServerProtect for Windows	Vulnerability Scanner가 RPC 엔드포인트를 사용하여 SPNTSVC.exe가 실행 중인지 확인합니다. 운영 체제, 바이러스 검색 엔진, 바이러스 패턴 및 제품 버전을 비롯한 정보를 반환합니다. Vulnerability Scanner가 ServerProtect 정보 서버 또는 ServerProtect 관리 콘솔을 검색할 수 없습니다.
ServerProtect for Linux	대상 엔드포인트가 Windows를 실행하지 않는 경우 Vulnerability Scanner는 포트 14942에 연결을 시도하여 엔드포인트에 ServerProtect for Linux가 설치되어 있는지 확인합니다.
OfficeScan 에이전트	Vulnerability Scanner가 OfficeScan 에이전트 포트를 사용하여 OfficeScan 에이전트가 설치되어 있는지 확인합니다. 또한 TmListen.exe 프로세스가 실행 중인지 확인합니다. 해당 기본 위치에서 실행된 경우 포트 번호를 자동으로 검색합니다. OfficeScan 서버 이외의 엔드포인트에서 Vulnerability Scanner를 시작한 경우에는 다른 엔드포인트의 통신 포트를 확인한 다음 사용합니다.
PortalProtect™	Vulnerability Scanner가 http://localhost:port/PortalProtect/index.html 웹 페이지를 로드하여 제품 설치를 확인합니다.
ScanMail™ for Microsoft Exchange™	Vulnerability Scanner가 http://ipaddress:port/scanmail.html 웹 페이지를 로드하여 ScanMail 설치를 확인합니다. 기본적으로 ScanMail은 포트 16372를 사용합니다. ScanMail이 다른 포트 번호를 사용하는 경우 포트 번호를 지정합니다. 그렇지 않으면 Vulnerability Scanner가 ScanMail을 찾을 수 없습니다.
InterScan™ 제품군	Vulnerability Scanner가 여러 제품의 각 웹 페이지를 로드하여 제품 설치를 확인합니다. • InterScan Messaging Security Suite 5.x: http://localhost:port/eManager/cgi-bin/eManager.htm • InterScan eManager 3.x: http://localhost:port/eManager/cgi-bin/eManager.htm • InterScan VirusWall™ 3.x: http://localhost:port/InterScan/cgi-bin/interscan.dll

제품	설명
Trend Micro Internet Security™ (PC-cillin)	Vulnerability Scanner는 포트 40116을 사용하여 Trend Micro Internet Security가 설치되어 있는지 확인합니다.
McAfee VirusScan ePolicy Orchestrator	Vulnerability Scanner에서 TCP 포트 8081에 특수 토큰을 보냅니다. 이 포트는 ePolicy Orchestrator가 서버와 에이전트 간을 연결하기 위해 사용하는 기본 포트입니다. 이 바이러스 백신 제품이 있는 엔드포인트는 특수 토큰 유형을 사용하여 응답합니다. Vulnerability Scanner에서는 독립 실행형 McAfee VirusScan을 찾을 수 없습니다.
Norton Antivirus™ Corporate Edition	Vulnerability Scanner에서 Norton Antivirus Corporate Edition RTVScan의 기본 포트인 UDP 포트 2967에 특수 토큰을 보냅니다. 이 바이러스 백신 제품이 있는 엔드포인트는 특수 토큰 유형을 사용하여 응답합니다. Norton Antivirus Corporate Edition은 UDP를 사용하여 통신하므로 정확도를 보장할 수 없습니다. 또한 네트워크 트래픽에 따라 UDP 대기 시간이 달라질 수 있습니다.

Vulnerability Scanner에서는 다음 프로토콜을 사용하여 제품과 컴퓨터를 검색합니다.

- **RPC**: ServerProtect for NT 검색
- **UDP**: Norton AntiVirus Corporate Edition 클라이언트 검색
- **TCP**: McAfee VirusScan ePolicy Orchestrator 검색
- **ICMP**: ICMP 패킷을 전송하여 컴퓨터 검색
- **HTTP**: OfficeScan 에이전트 검색
- **DHCP**: DHCP 요청을 발견하는 경우 Vulnerability Scanner에서는 요청하는 엔드포인트에 바이러스 백신 소프트웨어가 이미 설치되어 있는지 확인합니다.

제품 쿼리 설정 구성

제품 쿼리 설정은 취약점 검색 설정의 하위 집합입니다. 취약점 검색 설정에 대한 자세한 내용은 취약점 검색 방법 페이지 5-43을 참조하십시오.

절차

1. Vulnerability Scanner(TMVS.exe)에서 제품 쿼리 설정을 지정하려면

   a. TMVS.exe를 시작합니다.

   b. **설정**을 클릭합니다.

      설정 화면이 나타납니다.

   c. **제품 쿼리** 섹션으로 이동합니다.

   d. 확인할 제품을 선택합니다.

   e. 제품 이름 옆의 **설정**을 클릭한 다음 Vulnerability Scanner에서 확인할 포트 번호를 지정합니다.

   f. **확인**을 클릭합니다.

      설정 화면이 닫힙니다.

2. Vulnerability Scanner에서 보안 소프트웨어를 동시에 확인할 컴퓨터 수를 설정하려면

   a. <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩TMVS로 이동하여 메모장과 같은 텍스트 편집기를 사용하여 TMVS.ini를 엽니다.

   b. 수동 취약점 검색 중에 확인할 컴퓨터 수를 설정하려면 `ThreadNumManual` 값을 변경합니다. 8에서 64 사이의 값을 지정합니다.

      예를 들어 Vulnerability Scanner에서 동시에 60대의 컴퓨터를 확인하도록 하려면 `ThreadNumManual=60`을 입력합니다.

   c. 예약된 취약점 검색 중에 확인할 컴퓨터 수를 설정하려면 `ThreadNumSchedule` 값을 변경합니다. 8에서 64 사이의 값을 지정합니다.

      예를 들어 Vulnerability Scanner에서 동시에 50대의 컴퓨터를 확인하도록 하려면 `ThreadNumSchedule=50`을 입력합니다.

   d. TMVS.ini를 저장합니다.

엔드포인트 설명 검색 방법

Vulnerability Scanner는 호스트 컴퓨터를 "ping"할 수 있는 경우 호스트 컴퓨터에 대한 추가 정보를 검색할 수 있습니다. 정보를 검색하는 방법에는 다음 두 가지가 있습니다.

- **빠른 검색**: 엔드포인트 이름만 검색합니다.
- **일반 검색**: 도메인 정보와 엔드포인트 정보를 모두 검색합니다.

검색 설정 구성

검색 설정은 취약점 검색 설정의 하위 집합입니다. 취약점 검색 설정에 대한 자세한 내용은 취약점 검색 방법 페이지 5-43을 참조하십시오.

절차

1. TMVS.exe를 시작합니다.
2. **설정**을 클릭합니다.

   설정 화면이 나타납니다.
3. **컴퓨터 설명 검색 방법** 섹션으로 이동합니다.
4. **일반** 또는 **빠른**을 선택합니다.
5. **일반**을 선택한 경우 **컴퓨터 설명(사용 가능한 경우) 검색**을 선택합니다.
6. **확인**을 클릭합니다.

   설정 화면이 닫힙니다.

알림

Vulnerability Scanner는 OfficeScan 관리자에게 취약점 검색 결과를 보낼 수 있습니다. 또한 보호되지 않는 호스트 컴퓨터에 알림을 표시할 수 있습니다.

알림 설정 구성

알림 설정은 취약점 검색 설정의 하위 집합입니다. 취약점 검색 설정에 대한 자세한 내용은 취약점 검색 방법 페이지 5-43을 참조하십시오.

절차

1. TMVS.exe를 시작합니다.
2. **설정**을 클릭합니다.

   설정 화면이 나타납니다.
3. **알림** 섹션으로 이동합니다.
4. 취약점 검색 결과를 자동으로 받거나 조직의 다른 관리자에게 자동으로 보내려면
   a. **시스템 관리자에게 결과를 전자 메일로 보내기**를 선택합니다.
   b. **구성**을 클릭하여 전자 메일 설정을 지정합니다.
   c. **받는 사람**에 수신자의 전자 메일 주소를 입력합니다.
   d. **보낸 사람**에 발신자의 전자 메일 주소를 입력합니다.
   e. **SMTP 서버**에 SMTP 서버 주소를 입력합니다.

      예를 들어 `smtp.company.com`을 입력합니다. SMTP 서버 정보가 필요합니다.
   f. **제목**에 새 메시지 제목을 입력하거나 기본 제목을 사용합니다.
   g. **확인**을 클릭합니다.
5. 컴퓨터에 보안 소프트웨어가 설치되어 있지 않음을 사용자에게 알리려면
   a. **보호되지 않은 컴퓨터에 알림 표시**를 선택합니다.
   b. **사용자 정의**를 클릭하여 알림 메시지를 구성합니다.
   c. **알림 메시지** 화면에서 새 메시지 이름을 입력하거나 기본 메시지를 사용합니다.
   d. **확인**을 클릭합니다.
6. **확인**을 클릭합니다.

   설정 화면이 닫힙니다.

취약점 검색 결과

취약점 검색 결과를 쉼표로 구분된 값(CSV) 파일에 저장하도록 Vulnerability Scanner를 구성할 수 있습니다.

검색 결과 구성

취약점 검색 결과 설정은 취약점 검색 설정의 하위 집합입니다. 취약점 검색 설정에 대한 자세한 내용은 취약점 검색 방법 페이지 5-43을 참조하십시오.

절차

1. TMVS.exe를 시작합니다.
2. **설정**을 클릭합니다.

   설정 화면이 나타납니다.
3. **결과 저장** 섹션으로 이동합니다.
4. **결과를 CSV 파일에 자동 저장합니다**를 선택합니다.
5. CSV 파일을 저장할 기본 폴더를 변경하려면
   a. **찾아보기**를 클릭합니다.
   b. 엔드포인트 또는 네트워크에서 대상 폴더를 선택합니다.
   c. **확인**을 클릭합니다.
6. **확인**을 클릭합니다.

   설정 화면이 닫힙니다.

Ping 설정

"ping" 설정을 사용하여 대상 컴퓨터의 존재를 검증하고 해당 운영 체제를 확인할 수 있습니다. 이러한 설정을 사용하지 않도록 설정하면 Vulnerability Scanner에서 지정된 IP 주소 범위의 모든 IP 주소를 검색합니다. 따라서 호스트 컴퓨터에서 사용되지 않는 IP 주소도 검색하므로 검색 시간이 오래 걸립니다.

Ping 설정 구성

Ping 설정은 취약점 검색 설정의 하위 집합입니다. 취약점 검색 설정에 대한 자세한 내용은 취약점 검색 방법 페이지 5-43을 참조하십시오.

절차

1. Vulnerability Scanner(TMVS.exe)에서 Ping 설정을 지정하려면

   a. TMVS.exe를 시작합니다.

   b. **설정**을 클릭합니다.

      설정 화면이 나타납니다.

   c. **Ping** 설정 섹션으로 이동합니다.

   d. **Vulnerability Scanner가 네트워크의 컴퓨터를 ping하여 상태를 확인할 수 있도록 허용**을 선택합니다.

   e. **패킷 크기** 및 **타임아웃** 필드에서 기본값을 적용하거나 수정합니다.

   f. **ICMP OS 지문을 사용하여 운영 체제 유형을 검색합니다**를 선택합니다.

      이 옵션을 선택한 경우 Vulnerability Scanner가 호스트 컴퓨터에서 Windows 운영 체제를 실행하는지 아니면 다른 운영 체제를 실행하는지 확인합니다. Windows를 실행하는 호스트 컴퓨터의 경우 Vulnerability Scanner는 Windows 버전을 식별할 수 있습니다.

   g. **확인**을 클릭합니다.

      설정 화면이 닫힙니다.

2. Vulnerability Scanner가 동시에 ping하는 컴퓨터 수를 설정하려면

   a. <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩TMVS로 이동하여 메모장과 같은 텍스트 편집기를 사용하여 TMVS.ini를 엽니다.

   b. `EchoNum` 값을 변경합니다. 1에서 64 사이의 값을 지정합니다.

      예를 들어 Vulnerability Scanner가 동시에 60대의 컴퓨터를 ping하게 하려면 `EchoNum=60`을 입력합니다.

c. TMVS.ini를 저장합니다.

OfficeScan 서버 설정

OfficeScan 서버 설정은 다음과 같은 경우에 사용됩니다.

- Vulnerability Scanner에서 보호되지 않는 대상 컴퓨터에 OfficeScan 에이전트를 설치하는 경우. 서버 설정을 통해 Vulnerability Scanner는 OfficeScan 에이전트의 상위 서버와 대상 컴퓨터에 로그온할 때 사용할 관리 자격 증명을 식별할 수 있습니다.

  참고

  특정 조건에서는 OfficeScan 에이전트를 대상 호스트 컴퓨터에 설치하지 못할 수도 있습니다.

  자세한 내용은 Vulnerability Scanner를 사용하여 OfficeScan 에이전트를 설치할 때의 지침 페이지 5-41를 참조하십시오.

- Vulnerability Scanner에서 OfficeScan 서버에 에이전트 설치 로그를 보내는 경우

OfficeScan 서버 설정 구성

OfficeScan 서버 설정은 취약점 검색 설정의 하위 집합입니다. 취약점 검색 설정에 대한 자세한 내용은 취약점 검색 방법 페이지 5-43을 참조하십시오.

절차

1. TMVS.exe를 시작합니다.
2. **설정**을 클릭합니다.

   설정 화면이 나타납니다.
3. **OfficeScan 서버 설정** 섹션으로 이동합니다.
4. OfficeScan 서버 이름과 포트 번호를 입력합니다.
5. **보호되지 않은 컴퓨터에 OfficeScan 에이전트 자동 설치**를 선택합니다.

6. 관리 자격 증명을 구성하려면
   a. **계정에 설치**를 클릭합니다.
   b. **계정 정보** 화면에서 사용자 이름과 암호를 입력합니다.
   c. **확인**을 클릭합니다.
7. **OfficeScan 서버로 로그 보내기**를 선택합니다.
8. **확인**을 클릭합니다.

   설정 화면이 닫힙니다.

보안 준수를 사용한 설치

네트워크 도메인 내에 있는 컴퓨터에 OfficeScan 에이전트를 설치하거나 해당 IP 주소를 사용하여 OfficeScan 에이전트를 대상 엔드포인트에 설치합니다.

OfficeScan 에이전트를 설치하기 전에 다음 사항에 유의하십시오.

절차

1. 각 엔드포인트의 로그온 자격 증명을 기록합니다. OfficeScan이 설치 도중 로그온 자격 증명을 지정하라는 메시지를 표시합니다.
2. 다음의 경우 OfficeScan 에이전트가 엔드포인트에 설치되지 않습니다.
   - OfficeScan 서버가 엔드포인트에 설치되어 있습니다.
   - 엔드포인트에서 Windows XP Home, Windows Vista Home Basic, Windows Vista Home Premium, Windows 7™ Starter, Windows 7 Home Basic, Windows 7 Home Premium, Windows 8(기본 버전), Windows 8.1(기본 버전) 및 Windows 10 Home을 실행합니다. 이러한 플랫폼을 실행하는 컴퓨터가 있는 경우, 다른 설치 방법을 선택합니다. 자세한 내용은 배포 고려 사항 페이지 5-11를 참조하십시오.
3. 대상 엔드포인트에서 Windows Vista(Business, Enterprise 또는 Ultimate Edition), Windows 7(Professional, Enterprise 또는 Ultimate Edition), Windows 8(Pro, Enterprise), Windows 8.1(Pro, Enterprise), Windows 10(Pro, Education,

Enterprise) 또는 Windows Server 2012(Standard)를 실행하는 경우 엔드포인트에서 다음 단계를 수행합니다.

a. 기본 제공되는 관리자 계정을 사용 가능하도록 설정하고 계정 암호를 설정합니다.

b. Windows 방화벽을 사용 안 함으로 설정합니다.

c. **시작** > **프로그램** > **관리 도구** > **고급 보안이 포함된 Windows 방화벽**을 클릭합니다.

d. 도메인 프로필, 개인 프로필 및 공개 프로필에 방화벽 상태를 "꺼짐"으로 설정합니다.

e. Microsoft Management Console을 열고(**시작** > **실행**을 클릭하고 `services.msc` 입력) **원격 레지스트리** 서비스를 시작합니다. OfficeScan 에이전트를 설치할 때 기본 제공되는 관리자 계정 및 암호를 사용합니다.

4. 엔드포인트에 설치된 Trend Micro 또는 타사 엔드포인트 보안 프로그램이 있는 경우, OfficeScan이 자동으로 소프트웨어를 제거하고 OfficeScan 에이전트와 바꿀 수 있는지 확인합니다. OfficeScan에서 자동으로 제거하는 에이전트 보안 소프트웨어 목록을 보려면 <서버 설치 폴더>₩PCCSRV ₩Admin에서 다음 파일을 엽니다. 메모장과 같은 텍스트 편집기를 사용하여 이러한 파일을 열 수 있습니다.

   - tmuninst.ptn
   - tmuninst_as.ptn

   대상 엔드포인트에 있는 소프트웨어가 목록에 포함되지 않은 경우에는 먼저 수동으로 제거합니다. 소프트웨어 제거 과정에 따라 제거 후에 엔드포인트를 다시 시작하거나 다시 시작하지 않아도 됩니다.

OfficeScan 에이전트 설치

절차

1. **점검** > **관리되지 않는 엔드포인트**로 이동합니다.

2. 에이전트 트리 맨 위에서 **설치**를 클릭합니다.

   - 이전 OfficeScan 에이전트 버전이 엔드포인트에 이미 설치되어 있고 **설치**를 클릭하는 경우, 설치를 건너뛰고 에이전트가 이 버전으로 업그레이드되지 않습니다. 에이전트를 업그레이드하려면 설정을 사용하지 않도록 설정해야 합니다.

     a. **에이전트** > **에이전트 관리**로 이동합니다.

     b. **설정** > **권한 및 기타 설정** > **기타 설정** 탭을 클릭합니다.

     c. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음** 옵션을 사용하지 않도록 설정합니다.

3. 각 엔드포인트에 대해 관리자 로그온 계정을 지정하고 **로그온**을 클릭합니다. OfficeScan이 대상 엔드포인트에서 에이전트를 설치하기 시작합니다.

4. 설치 상태를 봅니다.

OfficeScan 에이전트로 마이그레이션

대상 엔드포인트에 설치된 에이전트 보안 소프트웨어를 OfficeScan 에이전트로 바꿉니다.

다른 Endpoint Security 소프트웨어에서 마이그레이션

설치 프로그램은 OfficeScan 에이전트를 설치할 때 대상 엔드포인트에 Trend Micro 또는 타사 엔드포인트 보안 소프트웨어가 설치되어 있는지 확인합니다. 설치 프로그램은 소프트웨어를 자동으로 제거하고 OfficeScan 에이전트로 바꿀 수 있습니다.

OfficeScan에서 자동으로 제거하는 Endpoint Security 소프트웨어 목록을 보려면 <서버 설치 폴더>₩PCCSRV₩Admin에서 다음 파일을 엽니다. 메모장과 같은 텍스트 편집기를 사용하여 이러한 파일을 엽니다.

- tmuninst.ptn

- tmuninst_as.ptn

대상 엔드포인트에 있는 소프트웨어가 목록에 포함되지 않은 경우에는 먼저 수동으로 제거합니다. 소프트웨어 제거 과정에 따라 제거 후에 엔드포인트를 다시 시작하거나 다시 시작하지 않아도 됩니다.

OfficeScan 에이전트 마이그레이션 문제

- 자동 에이전트 마이그레이션이 완료되었지만 설치 직후 OfficeScan 에이전트에 문제가 발생한 경우 엔드포인트를 다시 시작합니다.
- OfficeScan 설치 프로그램이 OfficeScan 에이전트를 계속 설치했지만 다른 보안 소프트웨어를 제거할 수 없는 경우에는 두 소프트웨어 간에 충돌이 있는 것입니다. 두 소프트웨어를 제거한 다음 배포 고려 사항 페이지 5-11에 설명된 설치 방법 중 하나를 사용하여 OfficeScan 에이전트를 설치합니다.

ServerProtect 일반 서버에서 마이그레이션

ServerProtect™ 일반 서버 마이그레이션 도구는 Trend Micro ServerProtect 일반 서버를 실행하는 컴퓨터를 OfficeScan 에이전트로 마이그레이션하도록 도와주는 도구입니다.

ServerProtect 일반 서버 마이그레이션 도구는 OfficeScan 서버와 동일한 하드웨어 및 소프트웨어 사양을 공유합니다. Windows Server 2003 또는 Windows Server 2008을 실행하는 컴퓨터에서 이 도구를 실행하십시오.

ServerProtect 일반 서버가 제거되면 이 도구는 OfficeScan 에이전트를 설치합니다. 또한 검색 제외 목록 설정(모든 검색 유형에 대해)을 OfficeScan 에이전트로 마이그레이션합니다.

OfficeScan 에이전트를 설치하는 동안 마이그레이션 도구 에이전트 설치 관리자가 시간이 초과되어 설치에 실패했음을 알리는 메시지를 표시할 수 있습니다. 그러나 OfficeScan 에이전트가 제대로 설치되었을 수도 있습니다. 따라서 OfficeScan 웹 콘솔에서 에이전트 엔드포인트에 에이전트가 설치되었는지 확인하십시오.

다음과 같은 경우에는 마이그레이션을 수행할 수 없습니다.

- 원격 에이전트에서 IPv6 주소만 사용하는 경우 마이그레이션 도구가 IPv6 주소 지정을 지원하지 않는 경우
- 원격 에이전트에서 NetBIOS 프로토콜을 사용할 수 없는 경우
- 455, 337 및 339 포트가 차단된 경우
- 원격 에이전트에서 RPC 프로토콜을 사용할 수 없는 경우
- 원격 레지스트리 서비스가 중지된 경우

참고

ServerProtect 일반 서버 마이그레이션 도구는 ServerProtect용 Control Manager™ 에이전트를 제거하지 않습니다. 에이전트 제거 방법에 대한 자세한 내용은 ServerProtect 및/또는 Control Manager 설명서를 참조하십시오.

ServerProtect 일반 서버 마이그레이션 도구 사용

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩SPNSXfr을 열고 SPNSXfr.exe 및 SPNSX.ini 파일을 <서버 설치 폴더>₩PCCSRV₩Admin에 복사합니다.
2. SPNSXfr.exe를 두 번 클릭하여 도구를 엽니다.

   Server Protect 일반 서버 마이그레이션 도구 콘솔이 열립니다.
3. OfficeScan 서버를 선택합니다. OfficeScan 서버의 경로가 OfficeScan 서버 경로 아래에 나타납니다. 이 경로가 올바르지 않으면 **찾아보기**를 클릭하여 OfficeScan을 설치한 디렉터리에서 PCCSRV 폴더를 선택합니다. 다음에 도구를 열 때 도구에서 OfficeScan 서버를 자동으로 다시 찾을 수 있도록 하려면 **자동 서버 경로 찾기** 확인란(기본적으로 선택됨)을 선택합니다.
4. **대상 엔드포인트**에서 다음 중 하나를 클릭하여 마이그레이션을 수행할 ServerProtect 일반 서버를 실행 중인 컴퓨터를 선택합니다.
   - **Windows 네트워크 트리**: 네트워크의 도메인 트리를 표시합니다. 이 방법으로 컴퓨터를 선택하려면 에이전트 컴퓨터를 검색할 도메인을 클릭합니다.

- **정보 서버 이름**: 정보 서버 이름을 기준으로 검색합니다. 이 방법으로 컴퓨터를 선택하려면 텍스트 상자에 네트워크의 정보 서버 이름을 입력합니다. 여러 정보 서버를 검색하려면 서버 이름 사이에 세미콜론(;)을 삽입합니다.
- **일반 서버 이름**: 일반 서버 이름을 기준으로 검색합니다. 이 방법으로 컴퓨터를 선택하려면 텍스트 상자에 네트워크의 일반 서버 이름을 입력합니다. 여러 일반 서버를 검색하려면 서버 이름 사이에 세미콜론(;)을 입력합니다.
- **IP 범위 검색**: IP 주소 범위를 기준으로 검색합니다. 이 방법으로 컴퓨터를 선택하려면 IP 범위 아래에 클래스 B IP 주소 범위를 입력합니다.

참고

에이전트를 검색할 때 네트워크의 DNS Server가 응답하지 않으면 검색에 대한 응답이 중지됩니다. 검색 시간이 초과될 때까지 기다리십시오.

5. **설치 후 다시 시작**을 선택하여 마이그레이션 후 대상 컴퓨터를 자동으로 다시 시작합니다.

   마이그레이션을 완료하려면 다시 시작해야 합니다. 이 옵션을 선택하지 않은 경우 마이그레이션 후 컴퓨터를 수동으로 다시 시작하십시오.

6. **검색**을 클릭합니다.

   ServerProtect 일반 서버 아래에 검색 결과가 표시됩니다.

7. 마이그레이션을 수행할 컴퓨터를 클릭합니다.

   a. 모든 컴퓨터를 선택하려면 **모두 선택**을 클릭합니다.

   b. 모든 컴퓨터의 선택을 취소하려면 **모두 취소**를 클릭합니다.

   c. 목록을 쉼표로 구분된 값(CSV) 파일로 내보내려면 **CSV로 내보내기**를 클릭합니다.

8. 대상 컴퓨터에 로그온할 때 사용자 이름 및 암호가 필요한 경우 다음을 수행합니다.

   a. **그룹 계정/암호 사용** 확인란을 선택합니다.

b. **로그온 계정 설정**을 클릭합니다.

관리자 정보 입력 창이 나타납니다.

c. 사용자 이름 및 암호를 입력합니다.

참고

로컬/도메인 관리자 계정을 사용하여 대상 엔드포인트에 로그온합니다. "Guest" 또는 "Normal user" 등 적절하지 않은 권한으로 로그온할 경우 설치를 수행할 수 없습니다.

d. **확인**을 클릭합니다.

e. 로그온할 수 없는 경우 마이그레이션이 진행되는 동안 사용자 이름과 암호를 다시 입력할 수 있도록 하려면 **로그온 실패 시 다시 묻기**를 클릭합니다.

9. **마이그레이션**을 클릭합니다.

10. **설치 후 다시 시작** 옵션을 선택하지 않은 경우 대상 컴퓨터를 다시 시작하여 마이그레이션을 완료합니다.

사후 설치

설치를 완료한 후 다음을 확인하십시오.

- OfficeScan 에이전트 바로 가기 페이지 5-68
- 프로그램 목록 페이지 5-68
- OfficeScan 에이전트 서비스 페이지 5-68
- OfficeScan 에이전트 설치 로그 페이지 5-69

OfficeScan 에이전트 바로 가기

OfficeScan 에이전트 바로가기는 에이전트 엔드포인트의 Windows 시작 메뉴에 표시됩니다.

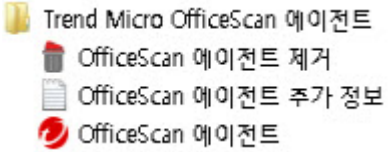


그림 5-2. OfficeScan 에이전트 바로 가기

참고

Windows 8/8.1/10 또는 Windows Server 2012/2012 R2/2016 플랫폼에서 제공되지 않습니다.

프로그램 목록

Trend Micro OfficeScan 에이전트는 에이전트 엔드포인트의 제어판에 있는 **프로그램 추가/제거** 목록에 나열됩니다.

OfficeScan 에이전트 서비스

다음 OfficeScan 에이전트 서비스가 **Microsoft Management Console**에 표시됩니다.

- OfficeScan NT Listener (TmListen.exe)
- OfficeScan NT RealTime Scan(NTRtScan.exe)
- OfficeScan NT 프록시 서비스(TmProxy.exe)

참고

Windows 7/8/8.1/10 또는 Windows Server 2008 R2/2012/2016 플랫폼에는 OfficeScan NT 프록시 서비스가 없습니다.

- OfficeScan NT 방화벽(TmPfw.exe)(설치 중에 방화벽을 사용하도록 설정한 경우)
- Trend Micro 무단 변경 방지 서비스(TMBMSRV.exe)
- Trend Micro 일반 클라이언트 솔루션 프레임워크(TmCCSF.exe)

OfficeScan 에이전트 설치 로그

OfficeScan 에이전트 설치 로그인 OFCNT.LOG는 다음 위치에 있습니다.

- MSI 패키지 설치를 제외한 모든 설치 방법의 경우 %windir%
- MSI 패키지 설치 방법의 경우 %temp%

권장 설치 후 작업

Trend Micro에서는 다음과 같은 설치 후 작업을 수행할 것을 권장합니다.

구성 요소 업데이트

OfficeScan 에이전트 구성 요소를 업데이트하여 에이전트에서 보안 위험을 방지하는 보호 기능을 최신 상태로 유지합니다. 웹 콘솔에서 수동 에이전트 업데이트를 실행하거나 사용자에게 컴퓨터에서 "지금 업데이트"를 실행하도록 지시할 수 있습니다.

EICAR 테스트 스크립트를 사용하여 검색 테스트

EICAR(European Institute for Computer Antivirus Research)에서는 바이러스 백신 소프트웨어가 적절하게 설치 및 구성되었는지 안전하게 확인할 수 있는 EICAR 테스트 스크립트를 개발했습니다. 자세한 내용은 다음 EICAR 웹 사이트를 참조하십시오.

http://www.eicar.org

EICAR 테스트 스크립트는 확장자가 .com인 비활성 텍스트 파일입니다. 이 스크립트는 바이러스가 아니며 바이러스 코드가 전혀 포함되어 있지 않지만 대부분의 바이러스 백신 소프트웨어에서는 이 스크립트가 바이러스인 것처럼 반응

합니다. 이 파일을 사용하면 바이러스 발생을 시뮬레이트하고 전자 메일 알림 및 바이러스 로그가 제대로 작동하는지 확인할 수 있습니다.

경고!

바이러스 백신 제품을 테스트하기 위해 실제 바이러스를 사용하지 마십시오.

테스트 검색 수행

절차

1. 에이전트에서 실시간 검색을 사용하도록 설정합니다.
2. 다음 문자열을 복사하여 메모장이나 일반 텍스트 편집기에 붙여 넣습니다.
   `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`
3. 파일을 임시 디렉터리에 EICAR.com으로 저장합니다. OfficeScan에서 즉시 이 파일을 발견합니다.
4. 네트워크의 다른 컴퓨터를 테스트하려면 EICAR.com 파일을 전자 메일 메시지에 첨부하여 다른 컴퓨터로 보냅니다.

팁

Trend Micro에서는 압축 소프트웨어(예: WinZip)를 사용하여 EICAR 파일을 패키지로 만든 다음 다른 테스트 검색을 수행할 것을 권장합니다.

OfficeScan 에이전트 제거

컴퓨터에서 OfficeScan 에이전트를 제거하는 방법에는 다음 두 가지가 있습니다.

- 웹 콘솔에서 OfficeScan 에이전트 제거 페이지 5-71
- OfficeScan 에이전트 제거 프로그램 실행 페이지 5-73

위 방법을 사용하여 OfficeScan 에이전트를 제거할 수 없는 경우에는 OfficeScan 에이전트를 수동으로 제거합니다. 자세한 내용은 수동으로 OfficeScan 에이전트 제거 페이지 5-73를 참조하십시오.

웹 콘솔에서 OfficeScan 에이전트 제거

웹 콘솔에서 OfficeScan 에이전트 프로그램을 제거합니다. 프로그램에 문제가 발생한 경우에만 제거를 수행하고, 즉시 다시 설치하여 보안 위험으로부터 엔드포인트를 보호합니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **작업** > **에이전트 제거**를 클릭합니다.
4. **에이전트 제거** 화면에서 **제거 시작**을 클릭합니다. 서버가 에이전트에 알림을 보냅니다.
5. 알림 상태를 확인하고 알림을 받지 않은 에이전트가 있는지 확인합니다.
   a. **알림을 받지 못한 엔드포인트 선택**, **제거 시작**을 차례로 클릭하여 알림을 받지 못한 에이전트에 즉시 알림을 재전송합니다.
   b. OfficeScan에서 현재 알림을 보내고 있는 에이전트에 대한 알림을 중지하도록 하려면 **제거 중지**를 클릭합니다. 이미 알림이 전송되어 제거를 수행하고 있는 에이전트는 이 명령을 무시합니다.

OfficeScan 에이전트 제거 프로그램

사용자에게 OfficeScan 에이전트 프로그램을 제거할 권한을 부여한 다음 컴퓨터에서 에이전트 제거 프로그램을 실행하도록 지시합니다.

구성에 따라 제거하는 데 암호가 필요할 수도 있고 필요하지 않을 수도 있습니다. 암호가 필요한 경우 제거 프로그램을 실행할 사용자에게만 암호를 공유하고 다른 사용자에게 누설된 경우 암호를 즉시 변경해야 합니다.

OfficeScan 에이전트 제거 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **제거** 섹션으로 이동합니다.
5. 암호 없이 제거할 수 있도록 허용하려면 **사용자가 OfficeScan 에이전트를 제거할 수 있음**을 선택합니다. 암호가 필요한 경우 **사용자가 OfficeScan 에이전트를 제거할 수 있음(암호 필요)**을 선택하고 암호를 입력한 후 확인합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트 제거 프로그램 실행

절차

1. Windows **시작** 메뉴에서 **프로그램** > **Trend Micro OfficeScan 에이전트** > **OfficeScan 에이전트 제거**를 클릭합니다.

   다음 단계를 수행할 수도 있습니다.

   a. **제어판** > **프로그램 추가/제거**를 클릭합니다.

   b. **Trend Micro OfficeScan 에이전트**를 찾은 다음 **변경**을 클릭합니다.

   c. 화면의 지침을 따릅니다.

2. 메시지가 표시되면 제거 암호를 입력합니다. OfficeScan은 제거 진행률 및 완료를 사용자에게 알립니다. 제거를 완료하기 위해 사용자가 에이전트 엔드포인트를 다시 시작할 필요는 없습니다.

수동으로 OfficeScan 에이전트 제거

웹 콘솔에서 OfficeScan 에이전트를 제거할 때 문제가 발생하거나 제거 프로그램을 실행한 후에 문제가 발생하는 경우에만 수동 제거를 수행합니다.

절차

1. 관리자 권한이 있는 계정을 사용하여 에이전트 엔드포인트에 로그온합니다.

2. 시스템 트레이에서 OfficeScan 에이전트 아이콘을 마우스 오른쪽 단추로 클릭하고 **OfficeScan 종료**를 선택합니다. 암호를 묻는 메시지가 표시되면 종료 암호를 지정한 다음 **확인**을 클릭합니다.

참고

- Windows 8, 8.1, 10, Windows Server 2012 및 Windows Server 2016의 경우 데스크톱 모드로 전환하여 OfficeScan 에이전트를 종료합니다.
- OfficeScan 에이전트를 종료할 컴퓨터에서 암호를 사용하지 않도록 설정합니다. 자세한 내용은 에이전트 권한 및 기타 설정 구성 페이지 15-88를 참조하십시오.

3. 종료 암호를 지정하지 않은 경우에는 Microsoft Management Console에서 다음 서비스를 중지합니다.
   - OfficeScan NT Listener
   - OfficeScan NT Firewall
   - OfficeScan NT 실시간 검색
   - OfficeScan NT 프록시 서비스

   참고

   Windows 7, 8, 8.1, 10 또는 Windows Server 2008R2, 2012, 2016 플랫폼에는 OfficeScan NT Proxy Service가 없습니다.

   - Trend Micro 무단 변경 방지 서비스
   - Trend Micro 일반 클라이언트 솔루션 프레임워크
4. 시작 메뉴에서 OfficeScan 에이전트 바로 가기를 제거합니다.
   - Windows 8, 8.1, 10, Windows Server 2012 및 Windows Server 2016의 경우
     a. 데스크톱 모드로 전환합니다.
     b. 마우스 커서를 화면 오른쪽 아래로 이동하면 표시되는 메뉴에서 **시작**을 클릭합니다.

        홈 화면이 나타납니다.
     c. **Trend Micro OfficeScan**을 마우스 오른쪽 단추로 클릭합니다.
     d. **시작 화면에서 제거**를 클릭합니다.

- 다른 모든 Windows 플랫폼의 경우

  시작 > **프로그램**을 클릭하고 **Trend Micro OfficeScan 에이전트**를 마우스 오른쪽 단추로 클릭한 다음 **삭제**를 클릭합니다.

5. 레지스트리 편집기(regedit.exe)를 엽니다.

경고!

다음 단계에서 레지스트리 키를 삭제해야 합니다. 레지스트리를 잘못 변경하면 시스템에 심각한 문제가 발생할 수 있습니다. 레지스트리를 변경하기 전에 항상 백업 복사본을 만드십시오. 자세한 내용은 레지스트리 편집기 도움말을 참조하십시오.

6. 다음 레지스트리 키를 삭제합니다.

- 다른 Trend Micro 제품이 엔드포인트에 설치되지 않은 경우:
  - 32비트 컴퓨터인 경우:

    `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`
  - 64비트 컴퓨터인 경우:

    `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro`

    `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro`
- 다른 Trend Micro 제품이 엔드포인트에 설치된 경우 다음 키만 삭제합니다.
  - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfcWatchDog`

    64비트 컴퓨터인 경우:

    `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfcWatchDog`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp`

    64비트 컴퓨터인 경우:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\PC-cillinNTCorp

7. 다음 레지스트리 키/값을 삭제합니다.
   - 32비트 시스템의 경우
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 아래에 있는 OfficeScanNT 모니터 (REG_SZ)
   - 64비트 시스템의 경우
     - HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\OfficeScanNT
     - HKEY_LOCAL_MACHINE\SOFTWARE\ Wow6432Node\Microsoft\Windows\CurrentVersion\Run 아래에 있는 OfficeScanNT 모니터(REG_SZ)
8. 다음 위치에서 다음 레지스트리 키의 인스턴스를 모두 삭제합니다.
   - 위치:
     - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
     - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
     - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services
     - HKEY_LOCAL_MACHINE\SYSTEM\ControlSet003\Services
   - 키:
     - NTRtScan
     - tmccsf
     - tmcfw

- tmcomm
- TmFilter
- TmListen
- tmpfw
- TmPreFilter
- TmProxy

참고

Windows 7/8/8.1/10 또는 Windows Server 2008 R2/2012/2016 플랫폼에는 TmProxy가 없습니다.

- tmtdi

참고

Windows 7/8/8.1/10 또는 Windows Server 2012/2016 플랫폼에는 tmtdi가 없습니다.

- VSApiNt
- tmlwf(Windows Vista/Server 2008/7/8/8.1/10/Server 2012/2016 컴퓨터의 경우)
- tmwfp(Windows Vista/Server 2008/7/8/8.1/10/Server 2012/2016 컴퓨터의 경우)
- tmactmon
- TMBMServer
- TMebc
- tmevtmgr
- tmeevw(Windows 7/8/8.1/10/Server 2008 R2/Server 2012 컴퓨터의 경우)

- tmusa(Windows 7/8/8.1/10/Server 2008 R2/Server 2012/2016 컴퓨터의 경우)
- tmnciesc
- tmeext(Windows XP/2003용)
- tmel(Windows 8/8.1/10/Server 2012/2016 컴퓨터의 경우)
- tmumh

9. 레지스트리 편집기를 닫습니다.
10. **시작** > **설정** > **제어판**을 클릭하고 **시스템**을 두 번 클릭합니다.

참고

Windows 8/8.1/10, Windows Server 2012 및 Windows Server 2016 시스템의 경우 이 단계를 건너뜁니다.

11. **하드웨어** 탭을 클릭한 다음 **장치 관리자**를 클릭합니다.

참고

Windows 8/8.1/10, Windows Server 2012 및 Windows Server 2016 시스템의 경우 이 단계를 건너뜁니다.

12. **보기** > **숨김 장치 표시**를 클릭합니다.

참고

Windows 8/8.1/10, Windows Server 2012 및 Windows Server 2016 시스템의 경우 이 단계를 건너뜁니다.

13. **비 플러그 앤 플레이 드라이버**를 확장하고 다음 장치를 제거합니다 (Windows XP/Vista/7/Server 2003/Server 2008의 경우).
    - tmactmon
    - tmcomm
    - TMEBC

- tmevtmgr
- TMUMH
- Trend Micro 필터
- Trend Micro PreFilter
- Trend Micro TDI 드라이버
- Trend Micro VSAPI NT
- Trend Micro 무단 변경 방지 서비스
- Trend Micro WFP 호출 드라이버(Windows Vista/Server 2008/7 컴퓨터의 경우)

14. 명령줄 편집기(Windows 8/8.1/10/Server 2012에만 해당)에서 다음 명령을 사용하여 Trend Micro 드라이버를 수동으로 삭제합니다.

- `sc delete tmcomm`
- `sc delete tmactmon`
- `sc delete tmevtmgr`
- `sc delete tmfilter`
- `sc delete tmprefilter`
- `sc delete tmwfp`
- `sc delete vsapint`
- `sc delete tmeevw`
- `sc delete tmusa`
- `sc delete tmebc`
- `sc delete tmumh`
- `sc delete tmccsf`
- `sc delete Tmnciesc`

- `sc delete tmlwf`

참고

관리자 권한으로 명령줄 편집기를 실행(예: cmd.exe를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행** 클릭)하여 명령을 실행해야 합니다.

15. 방화벽 드라이버를 제거합니다.

    a. **내 네트워크 환경**을 마우스 오른쪽 단추로 클릭한 후 **속성**을 클릭합니다.

    b. **로컬 영역 연결**을 마우스 오른쪽 단추로 클릭한 후 **속성**을 클릭합니다.

    c. **일반** 탭에서 **Trend Micro 방화벽 드라이버**를 선택하고 **제거**를 클릭합니다.

    참고

    다음 단계는 Windows Vista/Server 2008/7/8/8.1/10/Server 2012 운영 체제에만 적용됩니다. 그 밖의 운영 체제를 사용하는 에이전트에서는 15단계를 건너뜁니다.

    d. **네트워크**를 마우스 오른쪽 단추로 클릭한 후 **속성**을 클릭합니다.

    e. **네트워크 연결 관리**를 클릭합니다.

    f. **로컬 영역 연결**을 마우스 오른쪽 단추로 클릭한 후 **속성**을 클릭합니다.

    g. **네트워킹** 탭에서 **Trend Micro NDIS 6.0 필터 드라이버**를 선택하고 **제거**를 클릭합니다.

16. 에이전트 엔드포인트를 다시 시작합니다.

17. 다른 Trend Micro 제품이 엔드포인트에 설치되지 않은 경우에는 Trend Micro 설치 폴더(일반적으로 C:₩Program Files₩Trend Micro)를 삭제합니다. 64비트 컴퓨터의 경우 C:₩Program Files (x86)₩Trend Micro에서 설치 폴더를 찾을 수 있습니다.

18. 다른 Trend Micro 제품이 설치된 경우에는 다음 폴더를 삭제합니다.

- <에이전트 설치 폴더>
- Trend Micro 설치 폴더 아래의 BM 폴더(일반적으로 32비트 시스템의 경우 C:₩Program Files₩Trend Micro₩BM, 64비트 시스템의 경우 C:₩Program Files (x86)₩Trend Micro₩BM)

장 6

보호 기능을 최신으로 유지

이 장에서는 OfficeScan 구성 요소 및 업데이트 절차에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- OfficeScan 구성 요소 및 프로그램 페이지 6-2
- 업데이트 개요 페이지 6-11
- OfficeScan 서버 업데이트 페이지 6-14
- 통합 스마트 보호 서버 업데이트 페이지 6-26
- OfficeScan 에이전트 업데이트 페이지 6-26
- 업데이트 에이전트 페이지 6-51
- 구성 요소 업데이트 요약 페이지 6-60

OfficeScan 구성 요소 및 프로그램

OfficeScan은 구성 요소와 프로그램을 사용하여 최신 보안 위험으로부터 에이전트 컴퓨터를 보호합니다. 수동 또는 예약 업데이트를 실행하여 이러한 구성 요소와 프로그램을 최신으로 유지합니다.

이러한 구성 요소 외에도, OfficeScan 에이전트는 OfficeScan 서버로부터 업데이트된 구성 파일을 받습니다. 에이전트에 새 설정을 적용하려면 구성 파일이 필요합니다. 웹 콘솔을 통해 OfficeScan 설정을 수정할 때마다 구성 파일이 변경됩니다.

구성 요소는 다음과 같이 그룹화됩니다.

- 바이러스 백신 구성 요소 페이지 6-3
- Anti-spyware 구성 요소 페이지 6-6
- DCS(Damage Cleanup Services) 구성 요소 페이지 6-7
- 방화벽 구성 요소 페이지 6-7
- 동작 모니터링 구성 요소 페이지 6-7
- 의심스러운 연결 구성 요소 페이지 6-9
- 브라우저 악용 방지 솔루션 페이지 6-9
- 프로그램 페이지 6-9
- 웹 검증 구성 요소 페이지 6-11

바이러스 백신 구성 요소

구성 요소	설명
바이러스 검색 엔진 32/64비트	모든 Trend Micro 제품의 중심에는 초기의 파일 기반 바이러스에 대비해 개발된 검색 엔진이 있습니다. 오늘날의 검색 엔진은 매우 정교하며 다양한 유형의 바이러스 및 악성 프로그램을 검색할 수 있습니다. 또한 검색 엔진은 연구를 위해 개발 및 사용되는 대조 바이러스도 검색합니다. 이 엔진 및 패턴 파일은 모든 파일의 모든 바이트를 검색하지는 않으며 함께 작동하여 다음을 식별합니다. • 바이러스 코드의 경고 징후 • 파일 내에서 바이러스가 있는 정확한 위치
바이러스 패턴	바이러스 패턴에는 OfficeScan 에이전트에서 최신 바이러스/악성 프로그램 및 혼합된 형태의 위협 공격을 식별하는 데 도움이 되는 정보가 포함되어 있습니다. Trend Micro는 매주 여러 차례, 그리고 매우 위험한 바이러스/악성 프로그램이 발견될 때마다 새로운 버전의 바이러스 패턴을 만들어 릴리스합니다.
바이러스 검색 드라이버	바이러스 검색 드라이버는 파일에 대한 사용자 작업을 모니터링합니다. 작업에는 파일 열기 또는 닫기, 응용 프로그램 실행이 포함됩니다. 이 드라이버는 TmXPFlt.sys 및 TmPreFlt.sys의 두 가지 버전으로 제공됩니다. TmXPFlt.sys는 바이러스 검색 엔진의 실시간 구성에 사용되고 TmPreFlt.sys는 사용자 작업을 모니터링하는 데 사용됩니다. **참고** 이 구성 요소는 콘솔에 표시되지 않습니다. 해당 버전을 확인하려면 <서버 설치 폴더>₩PCCSRV₩Pccnt₩Drv로 이동합니다. .sys 파일을 마우스 오른쪽 단추로 클릭하고 **속성**을 선택한 후 **버전** 탭으로 이동합니다.

구성 요소	설명
스마트 스캔 패턴 스마트 스캔 에이전트 패턴	OfficeScan 에이전트는 스마트 스캔 모드에 있을 때 기존 악성 프로그램 및 Anti-spyware 패턴에서 제공하는 보호 기능을 동일하게 제공하고 함께 작동하는 간단한 패턴 두 가지를 사용합니다. **스마트 스캔 패턴**은 대부분의 패턴 정의를 포함합니다. **스마트 스캔 에이전트 패턴**은 스마트 스캔 패턴에 없는 다른 모든 패턴 정의를 포함합니다. OfficeScan 에이전트는 **스마트 스캔 에이전트 패턴**을 사용하여 보안 위협을 검색합니다. 검색 중에 파일에 대한 위험을 알 수 없는 OfficeScan 에이전트는 OfficeScan 서버에서 호스팅되는 서비스인 스캔 서버로 검색 쿼리를 보내 위험을 확인합니다. 스캔 서버는 **스마트 스캔 패턴**을 사용하여 위험을 확인합니다. OfficeScan 에이전트는 스캔 성능을 향상시키기 위해 스캔 서버에서 제공하는 검색 쿼리 결과를 "캐시"합니다.
IntelliTrap 패턴	IntelliTrap 패턴은 실행 파일로 압축된 실시간 압축 파일을 검색합니다. 자세한 내용은 IntelliTrap 페이지 E-6를 참조하십시오.
IntelliTrap 예외 패턴	IntelliTrap 예외 패턴에는 "승인된" 압축 파일 목록이 포함되어 있습니다.

구성 요소	설명
메모리 검사 패턴	실시간 검색 기능은 동작 모니터링을 통해 식별된 압축된 실행 파일을 메모리 검사 패턴을 사용하여 평가합니다. 실시간 검색 기능은 압축된 실행 파일에 대해 다음과 같은 조치를 취합니다. 1. 프로세스 이미지 경로를 확인한 후 메모리에 매핑 파일을 만듭니다. **참고** 검색 제외 목록은 파일 검색보다 우선합니다. 2. 프로세스 ID를 고급 보호 서비스에 전송하며, 이 서비스는 다음을 수행합니다. a. 바이러스 검색 엔진을 사용하여 메모리 검색을 수행합니다. b. Windows 시스템 파일, 신뢰할 수 있는 소스에서 가져온 디지털 서명된 파일 및 Trend Micro에서 테스트한 파일에 대한 글로벌 승인된 목록을 통해 프로세스를 필터링합니다. 안전한 파일로 확인된 후에는 OfficeScan에서 해당 파일에 대해 아무 조치도 취하지 않습니다. 3. 메모리 검색을 처리한 후 고급 보호 서비스는 결과를 실시간 검색 기능에 전송합니다. 4. 그러면 실시간 검색 기능은 검색된 악성 프로그램을 격리 보관하고 프로세스를 종료합니다.
상황별 정보 엔진 32/64비트	상황별 정보 엔진은 일반적이지 않은 파일에 의해 실행되는 프로세스를 모니터링하고 상황별 정보 쿼리 처리기가 분석을 위해 머신러닝 엔진으로 보내는 동작 특성을 추출합니다.
상황별 정보 패턴	상황별 정보 패턴에는 알려진 위협과는 관련이 없는 "승인된" 동작 목록이 들어 있습니다.
상황별 정보 쿼리 처리기 32/64비트	상황별 정보 쿼리 처리기는 상황별 정보 엔진에서 식별된 동작을 처리하고 머신러닝 엔진으로 보고서를 보냅니다.
고급 위협 검색 엔진 32/64비트	고급 위협 검색 엔진은 일반적이지 않은 파일에서 파일 특성을 추출하고 해당 정보를 머신러닝 엔진으로 보냅니다.
고급 위협 상관 관계 패턴	고급 위협 상관 관계 패턴에는 알려진 위협과는 관련이 없는 파일 특성 목록이 들어 있습니다.

검색 엔진 업데이트

Trend Micro는 최신 바이러스/악성 프로그램 정보를 바이러스 패턴 파일에 저장하여 보호 기능을 최신으로 유지하면서 검색 엔진 업데이트 횟수를 최소화합니다. 또한 Trend Micro는 정기적으로 새로운 검색 엔진 버전을 제공합니다. Trend Micro는 다음과 같은 경우 새로운 엔진을 릴리스합니다.

- 새로운 검색 및 탐지 기술이 소프트웨어에 통합된 경우
- 기존 검색 엔진으로 처리할 수 없는 새로운 유해 가능성이 있는 바이러스/악성 프로그램이 발견된 경우
- 검색 성능이 향상된 경우
- 파일 포맷, 스크립팅 언어, 인코딩 및/또는 압축 포맷이 추가된 경우

Anti-spyware 구성 요소

구성 요소	설명
스파이웨어/그레이웨어 패턴	스파이웨어/그레이웨어 패턴은 파일 및 프로그램, 메모리 모듈, Windows 레지스트리 및 URL 바로 가기에서 스파이웨어/그레이웨어를 식별합니다.
스파이웨어/그레이웨어 검색 엔진 32/64비트	스파이웨어/그레이웨어 검색 엔진은 스파이웨어/그레이웨어를 검색하고 적절한 검색 조치를 수행합니다.
스파이웨어 활성 모니터링 패턴	스파이웨어 활성 모니터링 패턴은 실시간 스파이웨어/그레이웨어 검색에 사용됩니다. 표준 스캔 에이전트만 이 패턴을 사용합니다. 스마트 스캔 에이전트는 스마트 스캔 에이전트 패턴을 사용하여 스파이웨어/그레이웨어를 실시간으로 검색합니다. 검색 중에 검색 대상의 위험을 확인할 수 없는 경우 에이전트는 스마트 보호 소스로 검색 쿼리를 보냅니다.

DCS(Damage Cleanup Services) 구성 요소

구성 요소	설명
DCE(Damage Cleanup Engine) 32/64비트	DCE(Damage Cleanup Engine)는 트로이 목마 바이러스 및 트로이 목마 프로세스를 검색하고 제거합니다.
Damage Cleanup 템플릿	Damage Cleanup 템플릿은 DCE(Damage Cleanup Engine)를 사용하여 트로이 목마 파일 및 프로세스를 식별한 후 제거할 수 있습니다.
Early Boot Cleanup 드라이버 32/64비트	Trend Micro Early Boot Cleanup 드라이버는 운영 체제 드라이버 전에 로드되어 부트 유형 루트키트를 탐지하고 차단할 수 있습니다. OfficeScan 에이전트 로드 후 Trend Micro Early Boot Cleanup 드라이버는 Damage Cleanup Services를 호출하여 루트키트를 치료합니다.

방화벽 구성 요소

구성 요소	설명
방화벽 드라이버 32/64비트	방화벽 드라이버는 에이전트 엔드포인트에서 네트워크 바이러스를 검색하기 위해 방화벽 패턴과 함께 사용됩니다. 이 드라이버는 32비트 및 64비트 플랫폼을 지원합니다.
방화벽 패턴	바이러스 패턴과 마찬가지로 에이전트는 방화벽 패턴을 통해 네트워크 바이러스의 존재 여부를 나타내는 비트 및 바이트의 고유한 패턴인 바이러스 서명을 식별할 수 있습니다.

동작 모니터링 구성 요소

구성 요소	설명
동작 모니터링 탐지 패턴 32/64비트	이 패턴에는 의심스러운 위협 동작을 탐지하기 위한 규칙이 포함되어 있습니다.
동작 모니터링 핵심 드라이버 32/64비트	이 커널 모드 드라이버는 시스템 이벤트를 모니터링한 후 동작 모니터링 핵심 서비스로 전달하여 정책이 적용되도록 합니다.

구성 요소	설명
동작 모니터링 핵심 서비스 32/64비트	이 사용자 모드 서비스는 다음과 같은 기능을 제공합니다. • 루트키트 탐지 제공 • 외부 장치에 대한 액세스 규범화 • 파일, 레지스트리 키 및 서비스 보호
동작 모니터링 구성 패턴	동작 모니터링 드라이버는 이 패턴을 사용하여 정상적인 시스템 이벤트를 식별하고 정책이 적용되지 않도록 제외시킵니다.
스마트 검색 패턴	이 패턴에는 동작 모니터링 핵심 서비스에서 시스템 이벤트를 담당하는 프로그램이 안전한지 여부를 확인하는 데 사용하는 유효한 디지털 서명 목록이 포함되어 있습니다.
정책 적용 패턴	동작 모니터링 핵심 서비스는 이 패턴의 정책을 기준으로 시스템 이벤트를 확인합니다.
메모리 검색 트리거 패턴(32/64비트)	동작 모니터링 기능이 다음 작업을 감지하면 메모리 검색 트리거 패턴을 사용하여 가능한 위협을 식별합니다. • 파일 쓰기 작업 • 레지스트리 쓰기 작업 • 새 프로세스 생성 동작 모니터링 기능이 이러한 작업 중 하나를 식별하면 실시간 검색의 메모리 검사 패턴을 호출하여 보안 위험을 확인합니다. 실시간 검색 작업에 대한 자세한 내용은 메모리 검사 패턴 페이지 6-5을 참조하십시오.
손상 복구 패턴	손상 복구 패턴에는 의심스러운 위협 동작의 모니터링에 사용되는 정책이 포함되어 있습니다.
프로그램 검사 모니터링 패턴	프로그램 검사 모니터링 패턴은 동작 모니터링에 사용되는 검사 지점을 모니터하고 저장합니다.

의심스러운 연결 구성 요소

구성 요소	설명
글로벌 C&C IP 목록	글로벌 C&C IP 목록은 NCIE(네트워크 콘텐츠 검사 엔진)와 함께 작동하여 알려진 C&C 서버와의 네트워크 연결을 탐지합니다. NCIE는 네트워크 채널을 통한 C&C 서버 연결을 탐지합니다. OfficeScan은 평가를 위해 서버에 대한 연결 정보를 모두 글로벌 C&C IP 목록에 기록합니다.
관련 규칙 패턴	이 의심스러운 연결 서비스에서는 관련 규칙 패턴을 사용하여 네트워크 패킷 헤더에 있는 고유한 악성 프로그램 패밀리 서명을 탐지합니다.

브라우저 악용 방지 솔루션

구성 요소	설명
브라우저 위협 방지 패턴	이 패턴은 최신 웹 브라우저 위협을 식별하고 이 위협이 웹 브라우저를 손상시키는 데 사용되지 못하게 합니다.
스크립트 분석자 통합 패턴	이 패턴은 웹 페이지에서 스크립트를 분석하고 유해 스크립트를 식별합니다.

프로그램

구성 요소	설명
OfficeScan 에이전트	OfficeScan 에이전트 프로그램은 보안 위험으로부터 실제적인 보호를 제공합니다.

구성 요소	설명
핫픽스, 패치 및 Service Pack	Trend Micro에서는 공식적인 제품 릴리스 후에도 문제점을 해결하고 제품 성능을 향상시키고 새로운 기능을 추가하기 위해 다음을 개발하는 경우가 종종 있습니다. • 핫픽스 페이지 E-5 • 패치 페이지 E-9 • 보안 패치 페이지 E-11 • Service Pack 페이지 E-11 이러한 항목이 제공되는 경우 공급업체 또는 지원 센터에서 사용자에게 연락할 수도 있습니다. 새 핫픽스, 패치 및 Service Pack 릴리스에 대한 자세한 내용은 다음 Trend Micro 웹 사이트를 참조하십시오. http://www.trendmicro.com/download 모든 릴리스 항목에는 설치, 배포 및 구성 정보를 포함하는 추가 정보 파일이 포함됩니다. 설치를 수행하기 전에 추가 정보 파일을 자세히 읽어 보십시오.

핫픽스 및 패치 기록

OfficeScan 서버가 핫픽스나 패치 파일을 OfficeScan 에이전트에 배포하면, OfficeScan 에이전트 프로그램은 레지스트리 편집기에 핫픽스나 패치에 대한 정보를 기록합니다. Microsoft SMS, LANDesk™ 또는 BigFix™와 같은 논리 소프트웨어를 사용하여 여러 에이전트에 대해 이 정보를 쿼리할 수 있습니다.

참고

이 기능은 서버에만 배포된 핫픽스 및 패치를 기록하지 않습니다.

이 기능은 OfficeScan 8.0 Service Pack 1 Patch 3.1 이상에서 제공됩니다.

- 8.0 Service Pack 1(Patch 3.1) 이상 버전에서 업그레이드된 에이전트는 버전 8.0 이상에 대해 설치된 핫픽스와 패치를 기록합니다.
- 8.0 Service Pack 1(Patch 3.1) 이전 버전에서 업그레이드된 에이전트는 버전 10.0 이상에 대해 설치된 핫픽스와 패치를 기록합니다.

정보는 다음 키에 저장됩니다.

- `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`
- x64 유형의 플랫폼을 실행하는 컴퓨터의 경우

  `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\ PC-cillinNTCorp\CurrentVersion\HotfixHistory\<Product version>`

다음 키를 확인합니다.

- **키**: `HotFix_installed`

  종류: `REG_SZ`

  값: `<핫픽스 또는 패치 이름>`
- **키**: `HotfixInstalledNum`

  종류: `DWORD`

  값: `<핫픽스 또는 패치 번호>`

웹 검증 구성 요소

구성 요소	설명
URL 필터링 엔진	URL 필터링 엔진은 OfficeScan과 Trend Micro URL 필터링 서비스 간의 통신을 간편하게 해줍니다. URL Filtering Service는 URL 등급을 지정하여 OfficeScan에 이 정보를 제공하는 시스템입니다.

업데이트 개요

모든 구성 요소 업데이트는 Trend Micro 액티브업데이트 서버에서 가져옵니다. 업데이트를 사용할 수 있으면 OfficeScan 서버와 스마트 보호 소스(스마트 보호 서버 또는 스마트 보호 네트워크)에서 업데이트된 구성 요소를 다운로드합니다. OfficeScan 서버와 스마트 보호 소스는 각각 특정 구성 요소 집합을 다운로드하므로 둘 간에 겹치는 구성 요소 다운로드가 없습니다.

참고

Trend Micro 액티브업데이트 서버 이외의 소스에서 업데이트를 가져오도록 OfficeScan 서버와 스마트 보호 서버를 모두 구성할 수 있습니다. 이렇게 하려면 사용자 지정 업데이트 소스를 설정해야 합니다. 이 업데이트 소스를 설정하는 데 도움이 필요한 경우에는 지원 센터에 문의하십시오.

OfficeScan 서버 및 OfficeScan 에이전트 업데이트

OfficeScan 서버는 에이전트가 필요로 하는 대부분의 구성 요소를 다운로드하며, 스마트 보호 소스에서 다운로드하는 스마트 스캔 패턴만 다운로드하지 않습니다.

OfficeScan 서버가 수많은 에이전트를 관리하는 경우, 업데이트 시 막대한 양의 서버 컴퓨터 리소스가 사용되므로 서버 안정성과 성능에 영향을 줄 수 있습니다. 이 문제를 해결하기 위해 OfficeScan에는 업데이트 에이전트 기능이 있으며 이 기능을 통해 다른 에이전트에 업데이트를 배포하는 작업을 특정 에이전트 간에 공유할 수 있습니다.

다음 표에서는 OfficeScan 서버와 에이전트에 대한 다양한 구성 요소 업데이트 옵션과 각 옵션을 사용할 적절한 상황에 대해 설명합니다.

표 6-1. 서버-에이전트 업데이트 옵션

업데이트 옵션	설명	권장 사항
액티브업데이트 서버 > 서버 > 에이전트	OfficeScan 서버는 Trend Micro 액티브업데이트 서버 또는 기타 업데이트 소스에서 업데이트된 구성 요소를 받고, 에이전트에서 구성 요소 업데이트를 시작합니다.	OfficeScan 서버와 에이전트 간에 낮은 대역폭 섹션이 없는 경우에 이 방법을 사용합니다.

업데이트 옵션	설명	권장 사항
액티브업데이트 서버 > 서버 > 업데이트 에이전트 > 에이전트	OfficeScan 서버는 액티브업데이트 서버 또는 기타 업데이트 소스에서 업데이트된 구성 요소를 받고, 에이전트에서 구성 요소 업데이트를 시작합니다. 그러면 업데이트 에이전트로 사용되는 에이전트가 에이전트에 구성 요소를 업데이트하도록 알립니다.	OfficeScan 서버와 에이전트 간에 낮은 대역폭 섹션이 있는 경우, 이 방법을 사용하여 네트워크에서 트래픽 부하의 균형을 조정합니다.
액티브업데이트 서버 > 업데이트 에이전트 > 에이전트	업데이트 에이전트는 액티브업데이트 서버 또는 기타 업데이트 소스에서 직접 업데이트된 구성 요소를 받고 에이전트에 구성 요소를 업데이트하도록 알립니다.	이 방법은 OfficeScan 서버 또는 다른 업데이트 에이전트에서 업데이트 에이전트를 업데이트하는 데 문제가 있는 경우에만 사용합니다. 대부분의 경우 업데이트 에이전트는 외부 업데이트 소스보다 OfficeScan 서버 또는 다른 업데이트 에이전트에서 업데이트를 받는 속도가 더 빠릅니다.
액티브업데이트 서버 > 에이전트	OfficeScan 에이전트는 액티브업데이트 서버 또는 기타 업데이트 소스에서 직접 업데이트된 구성 요소를 받습니다.	이 방법은 OfficeScan 서버 또는 업데이트 에이전트에서 에이전트를 업데이트하는 데 문제가 있는 경우에만 사용합니다. 대부분의 경우, 에이전트는 외부 업데이트 소스보다 OfficeScan 서버 또는 업데이트 에이전트에서 업데이트를 더 빠르게 받습니다.

스마트 보호 소스 업데이트

스마트 보호 소스(스마트 보호 서버 또는 스마트 보호 네트워크)는 스마트 스캔 패턴을 다운로드합니다. 스마트 스캔 에이전트는 이 패턴을 다운로드하지 않습니다. 에이전트는 스마트 보호 소스로 검색 쿼리를 보내 이 패턴을 기준으로 잠재적 위협을 확인합니다.

참고

스마트 보호 소스에 대한 자세한 내용은 스마트 보호 소스 페이지 4-5를 참조하십시오.

다음 표에서는 스마트 보호 소스에 대한 업데이트 프로세스를 설명합니다.

표 6-2. 스마트 보호 소스 업데이트 프로세스

업데이트 프로세스	설명
액티브업데이트 서버 > 스마트 보호 네트워크	Trend Micro 스마트 보호 네트워크는 Trend Micro 액티브업데이트 서버에서 업데이트를 받습니다. 기업 네트워크에 연결되지 않은 스마트 스캔 에이전트는 Trend Micro 스마트 보호 네트워크로 쿼리를 보냅니다.
액티브업데이트 서버 > 스마트 보호 서버	스마트 보호 서버(통합 또는 독립)는 Trend Micro 액티브업데이트 서버에서 업데이트를 받습니다. 기업 네트워크에 연결된 스마트 보호 에이전트는 스마트 보호 서버로 쿼리를 보냅니다.
스마트 보호 네트워크 > 스마트 보호 서버	스마트 보호 서버(통합 또는 독립)는 Trend Micro 스마트 보호 네트워크에서 업데이트를 받습니다. 기업 네트워크에 연결된 스마트 보호 에이전트는 스마트 보호 서버로 쿼리를 보냅니다.

OfficeScan 서버 업데이트

OfficeScan 서버는 다음 구성 요소를 다운로드하고 에이전트에 배포합니다.

표 6-3. OfficeScan 서버에서 다운로드한 구성 요소

구성 요소	배포	
	표준 스캔 에이전트	스마트 스캔 에이전트
바이러스 백신		
스마트 스캔 에이전트 패턴	아니요	예
바이러스 패턴	예	아니요
IntelliTrap 패턴	예	예

구성 요소	배포	
	표준 스캔 에이전트	스마트 스캔 에이전트
IntelliTrap 예외 패턴	예	예
바이러스 검색 엔진 32/64비트	예	예
메모리 검사 패턴	예	예
안티-멀웨어 패턴 조기 실행 32/64비트	예	예
상황별 정보 엔진 32/64비트	예	예
상황별 정보 패턴	예	예
상황별 정보 쿼리 처리기 32/64비트	예	예
고급 위협 검색 엔진 32/64비트	예	예
고급 위협 상관 관계 패턴	예	예
Anti-spyware		
스파이웨어/그레이웨어 패턴	예	예
스파이웨어 활성 모니터링 패턴	예	아니요
스파이웨어/그레이웨어 검색 엔진 32/64비트	예	예
DCS(Damage Cleanup Services)		
Damage Cleanup 템플릿	예	예
DCE(Damage Cleanup Engine) 32/64비트	예	예
Early Boot Cleanup 드라이버 32/64비트	예	예
방화벽		
방화벽 패턴	예	예
동작 모니터링 구성 요소		

구성 요소	배포	
	표준 스캔 에이전트	스마트 스캔 에이전트
동작 모니터링 탐지 패턴 32/64비트	예	예
동작 모니터링 핵심 드라이버 32/64비트	예	예
동작 모니터링 핵심 서비스 32/64비트	예	예
동작 모니터링 구성 패턴	예	예
정책 적용 패턴	예	예
스마트 검색 패턴	예	예
메모리 검색 트리거 패턴(32/64비트)	예	예
프로그램 검사 모니터링 패턴	예	예
손상 복구 패턴	예	예
의심스러운 연결		
글로벌 C&C IP 목록	예	예
관련 규칙 패턴	예	예
브라우저 악용 방지 솔루션		
브라우저 위협 방지 패턴	예	예
스크립트 분석자 통합 패턴	예	예

업데이트 미리 알림 및 팁:

- 서버에서 업데이트된 구성 요소를 에이전트에 배포할 수 있도록 하려면 자동 에이전트 업데이트를 사용하도록 설정하십시오. 자세한 내용은 OfficeScan 에이전트 자동 업데이트 페이지 6-36를 참조하십시오. 자동 에이전트 업데이트를 사용하지 않도록 설정한 경우에는 서버에서 업데이트를 다운로드하지만 에이전트에 배포하지는 않습니다.
- 순수 IPv6 OfficeScan 서버는 순수 IPv4 에이전트에 직접 업데이트를 배포할 수 없습니다. 마찬가지로 순수 IPv4 OfficeScan 서버는 순수 IPv6 에이전트

에 직접 업데이트를 배포할 수 없습니다. OfficeScan 서버가 에이전트에 업데이트를 배포할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

- Trend Micro는 정기적으로 패턴 파일을 릴리스하여 에이전트 보호를 최신 상태로 유지합니다. 패턴 파일 업데이트를 정기적으로 사용할 수 있기 때문에 OfficeScan은 패턴 파일을 더 빠르게 다운로드할 수 있는 "구성 요소 복제"라는 메커니즘을 사용합니다. 자세한 내용은 OfficeScan 서버 구성 요소 복제 페이지 6-19를 참조하십시오.
- 프록시 서버를 사용하여 인터넷에 연결한 경우, 업데이트를 성공적으로 다운로드할 수 있도록 올바른 프록시 설정을 사용합니다.
- 웹 콘솔의 대시보드에서 **에이전트 업데이트** 위젯을 추가하여 구성 요소의 현재 버전을 보고, 업데이트된 구성 요소 및 오래된 구성 요소가 있는 에이전트 수를 확인할 수 있습니다.

OfficeScan 서버 업데이트 소스

Trend Micro 액티브업데이트 서버 또는 다른 소스로부터 구성 요소를 다운로드하도록 OfficeScan 서버를 구성합니다. OfficeScan 서버에서 액티브업데이트 서버에 직접 연결할 수 없는 경우 다른 소스를 지정할 수 있습니다. 샘플 시나리오는 격리된 OfficeScan 서버 업데이트 페이지 6-22를 참조하십시오.

서버에서는 사용 가능한 업데이트를 다운로드한 후 **업데이트** > **에이전트** > **자동 업데이트**에 지정된 설정에 따라 구성 요소를 업데이트하도록 에이전트에 자동으로 알릴 수 있습니다. 구성 요소 업데이트가 중요한 경우 서버에서 **업데이트** > **에이전트** > **수동 업데이트**로 이동하여 에이전트에 한 번에 알릴 수 있습니다.

참고

업데이트 > **에이전트** > **자동 업데이트**에서 배포 일정 또는 이벤트에 따른 업데이트 설정을 지정하지 않은 경우 서버는 업데이트를 다운로드하지만 에이전트에 업데이트하도록 알리지는 않습니다.

OfficeScan 서버 업데이트에 대한 IPv6 지원

순수 IPv6 OfficeScan 서버는 다음과 같은 순수 IPv4 업데이트 소스에서 직접 업데이트할 수 없습니다.

- Trend Micro 액티브업데이트 서버
- 모든 순수 IPv4 사용자 정의 업데이트 소스

마찬가지로 순수 IPv4 OfficeScan 서버는 순수 IPv6 사용자 정의 업데이트 소스에서 직접 업데이트할 수 없습니다.

서버에서 업데이트 소스에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

OfficeScan 서버 업데이트용 프록시

Trend Micro 액티브업데이트 서버에서 업데이트를 다운로드할 때 프록시 설정을 사용하도록 서버 컴퓨터에서 호스트된 서버 프로그램을 구성합니다. 서버 프로그램에 OfficeScan 서버와 통합 스마트 보호 서버가 포함되어 있습니다.

프록시 설정 구성

절차

1. **관리** > **설정** > **프록시**으로 이동합니다.
2. **외부 프록시** 탭을 클릭합니다.
3. **OfficeScan 서버 업데이트** 섹션으로 이동합니다.
4. **패턴, 엔진 및 라이선스 업데이트에 프록시 서버 사용**을 선택합니다.
5. 프록시 프로토콜, 서버 이름 또는 IPv4/IPv6 주소와 포트 번호를 지정합니다.
6. 프록시 서버에 인증이 필요한 경우 사용자 이름 및 암호를 입력합니다.
7. **저장**을 클릭합니다.

서버 업데이트 소스 구성

절차

1. **업데이트** > **서버** > **업데이트 소스**로 이동합니다.
2. 구성 요소 업데이트를 다운로드할 위치를 선택합니다.

   액티브업데이트 서버를 선택하는 경우 서버가 인터넷에 연결되어 있는지 확인하고, 프록시 서버를 사용하는 경우 프록시 설정을 사용하여 인터넷 연결을 설정할 수 있는지 테스트합니다. 자세한 내용은 OfficeScan 서버 업데이트용 프록시 페이지 6-18를 참조하십시오.

   사용자 지정 업데이트 소스를 선택하는 경우 적합한 환경을 설정하고 이 업데이트 소스에 대한 리소스를 업데이트합니다. 또한 서버 컴퓨터와 이 업데이트 소스가 기능적으로 연결되어 있는지 확인합니다. 업데이트 소스를 설정하는 데 도움이 필요한 경우에는 지원 센터에 문의하십시오.

   참고

   OfficeScan 서버는 업데이트 소스에서 구성 요소를 다운로드할 때 구성 요소 복제를 사용합니다. 자세한 내용은 OfficeScan 서버 구성 요소 복제 페이지 6-19를 참조하십시오.
3. **저장**을 클릭합니다.

OfficeScan 서버 구성 요소 복제

Trend Micro 액티브업데이트 서버에서 최신 버전의 전체 패턴 파일을 다운로드할 수 있게 되면 14개의 "인크리멘탈 패턴"도 사용할 수 있게 됩니다. 인크리멘탈 패턴은 전체 패턴 파일의 최신 버전과 이전 버전의 차이를 바탕으로 만든 전체 패턴의 작은 버전입니다. 예를 들어, 최신 버전이 175인 경우, 인크리멘탈 패턴 v_173.175에는 버전 175에 있지만 버전 173에는 없는 서명이 포함됩니다(패턴 번호는 2씩 증가하여 릴리즈되므로 173은 이전 버전의 전체 패턴임). 인크리멘탈 패턴 v_171.175에는 버전 175에 있지만 버전 171에는 없는 서명이 포함됩니다.

최신 패턴을 다운로드할 때 발생하는 네트워크 트래픽을 줄이기 위해 OfficeScan에서는 OfficeScan 서버 또는 업데이트 에이전트에 인크리멘탈 패턴

만 다운로드하여 구성 요소를 업데이트하는 구성 요소 복제를 수행합니다. 업데이트 에이전트가 구성 요소 복제를 수행하는 방법에 대한 자세한 내용은 업데이트 에이전트 구성 요소 복제 페이지 6-57를 참조하십시오.

구성 요소 복제는 다음 구성 요소에 적용할 수 있습니다.

- 바이러스 패턴
- 스마트 스캔 에이전트 패턴
- Damage Cleanup 템플릿
- IntelliTrap 예외 패턴
- 스파이웨어/그레이웨어 패턴
- 스파이웨어 활성 모니터링 패턴

구성 요소 복제 시나리오

서버의 구성 요소 복제에 대한 자세한 내용은 다음 시나리오를 참조하십시오.

표 6-4. 서버 구성 요소 복제 시나리오

OfficeScan 서버에 있는 전체 패턴	현재 버전: 171 사용 가능한 다른 버전: 169	167	165	161	159	
액티브업데이트 서버에 있는 최신 버전	173.175	171.175	169.175	167.175	165.175	163.175
	161.175	159.175	157.175	155.175	153.175	151.175
	149.175	147.175				

1. OfficeScan 서버는 현재 전체 패턴 버전을 액티브업데이트 서버에 있는 최신 버전과 비교합니다. 두 버전 사이의 차이가 14 이하인 경우, 서버는 두 버전 사이의 차이를 바탕으로 만든 인크리멘탈 패턴만 다운로드합니다.

참고

차이가 14보다 큰 경우에는 서버가 패턴 파일의 전체 버전과 14개의 인크리멘탈 패턴을 자동으로 다운로드합니다.

예를 들면 다음과 같습니다.

- 버전 171과 175 사이의 차이는 2입니다. 즉, 서버에 버전 173과 175가 없습니다.
- 서버에서 인크리멘탈 패턴 171.175를 다운로드합니다. 이 인크리멘탈 패턴은 버전 171과 175 사이의 차이에 해당됩니다.

2. 서버는 인크리멘탈 패턴을 현재 전체 패턴과 병합하여 최신 전체 패턴을 생성합니다.

   예를 들면 다음과 같습니다.

   - 서버에서 OfficeScan이 버전 171을 인크리멘탈 패턴 171.175와 병합하여 버전 175를 생성합니다.
   - 서버에는 1개의 인크리멘탈 패턴(171.175)과 최신 전체 패턴(버전 175)이 있습니다.

3. 서버는 서버에서 사용할 수 있는 다른 전체 패턴에 따라 인크리멘탈 패턴을 생성합니다. 서버에서 이 인크리멘탈 패턴을 생성하지 않으면, 이전의 인크리멘탈 패턴을 다운로드하지 못한 에이전트에서 전체 패턴 파일을 자동으로 다운로드하기 때문에 네트워크 트래픽이 늘어납니다.

   예를 들면 다음과 같습니다.

   - 서버에 패턴 버전 169, 167, 165, 163, 161, 159가 있기 때문에 다음과 같은 인크리멘탈 패턴을 생성할 수 있습니다.

     169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - 서버에 이미 인크리멘탈 패턴 171.175가 있기 때문에 버전 171을 사용할 필요가 없습니다.
   - 이제 서버에는 다음과 같은 일곱 개의 인크리멘탈 패턴이 있습니다.

     171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

   - 서버는 최신 7개의 전체 버전(버전 175, 171, 169, 167, 165, 163, 161)을 유지합니다. 이전 버전(버전 159)은 제거됩니다.

4. 서버는 현재 인크리멘탈 패턴을 액티브업데이트 서버에서 사용할 수 있는 인크리멘탈 패턴과 비교하고 서버에 없는 인크리멘탈 패턴을 다운로드합니다.

예를 들면 다음과 같습니다.

- 액티브업데이트 서버에 다음과 같은 14개의 인크리멘탈 패턴이 있습니다.

  173.175, 171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- OfficeScan 서버에 다음과 같은 7개의 인크리멘탈 패턴이 있습니다.

  171.175, 169.175, 167.175, 165.175, 163.175, 161.175, 159.175

- OfficeScan 서버에서 다음과 같은 7개의 인크리멘탈 패턴을 추가로 다운로드합니다.

  173.175, 157.175, 155.175, 153.175, 151.175, 149.175, 147.175

- 이제 서버에는 액티브업데이트 서버에서 사용할 수 있는 인크리멘탈 패턴이 모두 있습니다.

5. 최신 전체 패턴과 14개의 인크리멘탈 패턴을 에이전트에서 사용할 수 있습니다.

격리된 OfficeScan 서버 업데이트

OfficeScan 서버가 모든 외부 소스로부터 완전히 격리된 네트워크에 속해 있는 경우 최신 구성 요소가 포함된 내부 소스에서 업데이트하도록 허용하여 서버의 구성 요소를 최신 상태로 유지할 수 있습니다.

이 항목에서는 격리된 OfficeScan 서버를 업데이트하는 데 필요한 작업에 대해 설명합니다.

격리된 OfficeScan 서버 업데이트

이 절차는 참조용으로 제공됩니다. 이 절차의 모든 작업을 수행할 수 있는 경우 각 작업의 자세한 단계는 지원 센터에 문의하십시오.

절차

1. Trend Micro Control Manager 또는 임의 호스트 컴퓨터와 같은 업데이트 소스를 식별합니다. 업데이트 소스는 다음 조건을 충족해야 합니다.

   - Trend Micro 액티브업데이트 서버에서 최신 구성 요소를 다운로드할 수 있도록 안정적인 인터넷 연결이 설정되어 있어야 합니다. 인터넷에 연결할 수 없는 경우 업데이트 소스에서 최신 구성 요소를 받을 수 있는 방법은 Trend Micro에서 직접 구성 요소를 받아 업데이트 소스에 복사하는 방법뿐입니다.
   - OfficeScan 서버와 기능적으로 연결되어 있어야 합니다. OfficeScan 서버와 업데이트 소스 간에 프록시 서버가 있는 경우 프록시 설정을 구성합니다. 자세한 내용은 OfficeScan 서버 업데이트용 프록시 페이지 6-18를 참조하십시오.
   - 구성 요소를 다운로드할 수 있는 충분한 디스크 공간이 있어야 합니다.

2. OfficeScan 서버에서 새 업데이트 소스를 가리킵니다. 자세한 내용은 OfficeScan 서버 업데이트 소스 페이지 6-17를 참조하십시오.

3. 서버에서 에이전트에 배포할 구성 요소를 식별합니다. 배포 가능한 구성 요소 목록은 OfficeScan 에이전트 업데이트 페이지 6-26를 참조하십시오.

   팁

   구성 요소가 에이전트에 배포되고 있는지 확인하는 방법 중 하나는 웹 콘솔에서 **업데이트 요약** 화면(**업데이트** > **요약**)으로 이동하는 것입니다. 이 화면에서 배포 중인 구성 요소의 업데이트 비율은 항상 0%보다 큰 값으로 표시됩니다.

4. 구성 요소를 다운로드할 빈도를 결정합니다. 패턴 파일은 자주(경우에 따라 매일) 업데이트되므로 정기적으로 업데이트하는 것이 좋습니다. 엔진 및 드라이버의 경우 지원 센터에 요청하여 중요한 업데이트에 대한 알림을 받을 수 있습니다.

5. 업데이트 소스에서 다음을 수행합니다.

   a. 액티브업데이트 서버에 연결합니다. 서버의 URL은 OfficeScan 버전에 따라 다릅니다.

b. 다음 항목을 다운로드합니다.

- server.ini 파일. 이 파일에는 최신 구성 요소에 대한 정보가 포함되어 있습니다.
- 3단계에서 식별한 구성 요소.

c. 다운로드한 항목을 업데이트 소스의 디렉터리에 저장합니다.

6. OfficeScan 서버의 수동 업데이트를 실행합니다. 자세한 내용은 수동으로 OfficeScan 서버 업데이트 페이지 6-24를 참조하십시오.

7. 구성 요소를 업데이트해야 할 때마다 5~6단계를 반복합니다.

OfficeScan 서버 업데이트 방법

OfficeScan 서버 구성 요소를 수동으로 업데이트하거나, 업데이트 일정을 구성하여 업데이트합니다.

서버에서 업데이트된 구성 요소를 에이전트에 배포할 수 있도록 하려면 자동 에이전트 업데이트를 사용하도록 설정하십시오. 자세한 내용은 OfficeScan 에이전트 자동 업데이트 페이지 6-36를 참조하십시오. 자동 에이전트 업데이트를 사용하지 않도록 설정한 경우에는 서버에서 업데이트를 다운로드하지만 에이전트에 배포하지는 않습니다.

업데이트 방법은 다음과 같습니다.

- **수동 서버 업데이트**: 업데이트가 중요한 경우, 서버가 직접 업데이트를 가져올 수 있도록 수동 업데이트를 수행합니다. 자세한 내용은 수동으로 OfficeScan 서버 업데이트 페이지 6-24를 참조하십시오.
- **서버 예약 업데이트**: OfficeScan 서버는 최신 구성 요소를 가져오도록 예약된 기간 동안 업데이트 소스에 연결됩니다. 자세한 내용은 OfficeScan 서버 업데이트 예약 페이지 6-25를 참조하십시오.

수동으로 OfficeScan 서버 업데이트

서버를 설치하거나 업그레이드한 후 그리고 바이러스 발생이 나타날 때마다 OfficeScan 서버에서 구성 요소를 수동으로 업데이트합니다.

절차

1. **업데이트** > **서버** > **수동 업데이트**로 이동합니다.
2. 업데이트할 구성 요소를 선택합니다.
3. **업데이트**를 클릭합니다.

   서버가 업데이트된 구성 요소를 다운로드합니다.

OfficeScan 서버 업데이트 예약

업데이트 소스를 주기적으로 확인하여 사용 가능한 업데이트를 자동으로 다운로드하도록 OfficeScan 서버를 구성합니다. 에이전트는 일반적으로 서버에서 업데이트 파일을 받기 때문에, 예약 업데이트를 사용하면 쉽고 효과적으로 보안 위험에 대한 보호 기능을 항상 최신으로 유지할 수 있습니다.

절차

1. **업데이트** > **서버** > **예약 업데이트**로 이동합니다.
2. **OfficeScan 서버의 예약 업데이트 사용**을 선택합니다.
3. 업데이트할 구성 요소를 선택합니다.
4. 업데이트 일정을 지정합니다.

   매일, 매주 및 매달 업데이트할 경우 기간은 OfficeScan에서 업데이트를 수행하는 기간(시간)입니다. OfficeScan에서는 이 기간 동안 지정된 시간에 업데이트합니다.
5. **저장**을 클릭합니다.

OfficeScan 서버 업데이트 로그

서버 업데이트 로그에서 특정 구성 요소를 업데이트하는 데 문제가 있는지 확인합니다. 로그에 OfficeScan 서버에 대한 구성 요소 업데이트가 포함되어 있습니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

업데이트 로그 보기

절차

1. **로그** > **서버 업데이트**로 이동합니다.
2. **결과** 열에서 업데이트되지 않은 구성 요소가 있는지 확인합니다.
3. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

통합 스마트 보호 서버 업데이트

통합 스마트 보호 서버는 두 가지 구성 요소, 즉 스마트 스캔 패턴과 웹 차단 목록을 다운로드합니다. 이러한 구성 요소에 대한 자세한 내용과 업데이트 방법은 통합 스마트 보호 서버 관리 페이지 4-17를 참조하십시오.

OfficeScan 에이전트 업데이트

최신 보안 위험으로부터 에이전트를 보호하려면 에이전트 구성 요소를 정기적으로 업데이트해야 합니다.

에이전트를 업데이트하기 전에 해당 업데이트 소스(OfficeScan 서버 또는 사용자 정의 업데이트 소스)에 최신 구성 요소가 있는지 확인합니다. OfficeScan 서버를 업데이트하는 방법에 대한 자세한 내용은 OfficeScan 서버 업데이트 페이지 6-14를 참조하십시오.

다음 표에는 업데이트 소스를 통해 에이전트에 배포되는 모든 구성 요소와 특정 검색 방법을 사용할 때 사용되는 구성 요소가 나와 있습니다.

표 6-5. 에이전트에 배포되는 OfficeScan 구성 요소

구성 요소	배포	
	표준 스캔 에이전트	스마트 스캔 에이전트
바이러스 백신		
스마트 스캔 에이전트 패턴	아니요	예
바이러스 패턴	예	아니요
IntelliTrap 패턴	예	예
IntelliTrap 예외 패턴	예	예
바이러스 검색 엔진 32/64비트	예	예
메모리 검사 패턴	예	예
안티-멀웨어 패턴 조기 실행 32/64비트	예	예
상황별 정보 엔진 32/64비트	예	예
상황별 정보 패턴	예	예
상황별 정보 쿼리 처리기 32/64비트	예	예
고급 위협 검색 엔진 32/64비트	예	예
고급 위협 상관 관계 패턴	예	예
Anti-spyware		
스파이웨어/그레이웨어 패턴	예	예
스파이웨어 활성 모니터링 패턴	예	아니요
스파이웨어/그레이웨어 검색 엔진 32/64비트	예	예
DCS(Damage Cleanup Services)		
Damage Cleanup 템플릿	예	예
DCE(Damage Cleanup Engine) 32/64비트	예	예

구성 요소	배포	
	표준 스캔 에이전트	스마트 스캔 에이전트
Early Boot Cleanup 드라이버 32/64비트	예	예
웹 검증 서비스		
URL 필터링 엔진	예	예
방화벽		
방화벽 패턴	예	예
방화벽 드라이버 32/64비트	예	예
동작 모니터링 구성 요소		
동작 모니터링 탐지 패턴 32/64비트	예	예
동작 모니터링 핵심 드라이버 32/64비트	예	예
동작 모니터링 핵심 서비스 32/64비트	예	예
동작 모니터링 구성 패턴	예	예
정책 적용 패턴	예	예
스마트 검색 패턴	예	예
메모리 검색 트리거 패턴(32/64비트)	예	예
프로그램 검사 모니터링 패턴	예	예
손상 복구 패턴	예	예
의심스러운 연결		
글로벌 C&C IP 목록	예	예
관련 규칙 패턴	예	예
브라우저 악용 방지 솔루션		
브라우저 위협 방지 패턴	예	예

구성 요소	배포	
	표준 스캔 에이전트	스마트 스캔 에이전트
스크립트 분석자 통합 패턴	예	예

OfficeScan 에이전트 업데이트 소스

에이전트는 표준 업데이트 소스(OfficeScan 서버)에서 업데이트를 가져오거나 Trend Micro 액티브업데이트 서버와 같은 사용자 정의 업데이트 소스에서 특정 구성 요소를 가져올 수 있습니다. 자세한 내용은 OfficeScan 에이전트의 표준 업데이트 소스 페이지 6-29 및 OfficeScan 에이전트의 사용자 정의 업데이트 소스 페이지 6-31를 참조하십시오.

OfficeScan 에이전트 업데이트에 대한 IPv6 지원

순수 IPv6 에이전트는 다음과 같은 순수 IPv4 업데이트 소스에서 직접 업데이트할 수 없습니다.

- 순수 IPv4 OfficeScan 서버
- 순수 IPv4 업데이트 에이전트
- 모든 순수 IPv4 사용자 정의 업데이트 소스
- Trend Micro 액티브업데이트 서버

마찬가지로 순수 IPv4 에이전트는 순수 IPv6 OfficeScan 서버 또는 업데이트 에이전트와 같은 순수 IPv6 업데이트 소스에서 직접 업데이트할 수 없습니다.

에이전트에서 업데이트 소스에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

OfficeScan 에이전트의 표준 업데이트 소스

OfficeScan 서버는 에이전트의 표준 업데이트 소스입니다.

OfficeScan 서버에 연결할 수 없는 경우 에이전트는 백업 소스가 없으므로 오래된 상태로 유지됩니다. OfficeScan 서버에 연결할 수 없는 에이전트를 업데이트

하려면 Trend Micro에서는 에이전트 패키지 도구를 사용할 것을 권장합니다. 이 도구를 사용하여 서버에서 제공되는 최신 구성 요소가 포함된 패키지를 만들어 에이전트에서 실행할 수 있습니다.

참고

에이전트의 IP 주소(IPv4 또는 IPv6)에 따라 OfficeScan 서버에 대한 연결을 설정할 수 있는지 여부가 결정됩니다. 에이전트 업데이트의 IPv6 지원에 대한 자세한 내용은 OfficeScan 에이전트 업데이트에 대한 IPv6 지원 페이지 6-29을 참조하십시오.

OfficeScan 에이전트의 표준 업데이트 소스 구성

절차

1. **업데이트** > **에이전트** > **업데이트 소스**로 이동합니다.
2. **기본 업데이트 소스(OfficeScan 서버에서 업데이트)**에서 선택합니다.
3. **모든 에이전트에 알림**을 클릭합니다.

OfficeScan 에이전트 업데이트 프로세스

참고

이 항목에서는 OfficeScan 에이전트의 업데이트 프로세스에 대해 설명합니다. 업데이트 에이전트의 업데이트 프로세스는 OfficeScan 에이전트의 표준 업데이트 소스 페이지 6-29에 설명되어 있습니다.

OfficeScan 서버에서 직접 업데이트하도록 OfficeScan 에이전트를 구성한 경우 다음과 같이 업데이트 프로세스가 진행됩니다.

1. OfficeScan 에이전트가 OfficeScan 서버에서 업데이트를 가져옵니다.
2. OfficeScan 서버에서 업데이트할 수 없는 경우 OfficeScan 에이전트는 Trend Micro 액티브업데이트 서버에 직접 연결하려고 시도합니다(**에이전트** > **에이전트 관리**에서 **설정** > **권한 및 기타 설정** > **기타 설정(탭)** > **업데이트 설정**을 클릭하여 **OfficeScan 에이전트가 Trend Micro 액티브업데이트 서버에서 업데이트 다운로드** 옵션을 사용하도록 설정한 경우).

참고

구성 요소만 액티브업데이트 서버에서 업데이트할 수 있습니다. 도메인 설정, 프로그램 및 핫픽스는 OfficeScan 서버 또는 업데이트 에이전트에서 다운로드할 수만 있습니다. 액티브업데이트 서버에서 패턴 파일만 다운로드하도록 OfficeScan 에이전트를 구성하여 업데이트 프로세스 속도를 높일 수 있습니다. 자세한 내용은 액티브업데이트 서버를 OfficeScan 에이전트 업데이트 소스로 사용 페이지 6-35를 참조하십시오.

OfficeScan 에이전트의 사용자 정의 업데이트 소스

OfficeScan 에이전트는 OfficeScan 서버와 별도로 사용자 정의 업데이트 소스에서 업데이트할 수 있습니다. 사용자 정의 업데이트 소스를 사용하면 OfficeScan 서버로 전달되는 OfficeScan 에이전트 업데이트 트래픽을 줄일 수 있으며, OfficeScan 서버에 연결할 수 없는 OfficeScan 에이전트가 적시에 업데이트를 받을 수 있습니다. 사용자 정의 업데이트 소스 목록에 사용자 지정 업데이트 소스를 지정합니다. 이 목록에는 최대 1024개의 업데이트 소스를 나열할 수 있습니다.

팁

Trend Micro에서는 일부 OfficeScan 에이전트를 업데이트 에이전트로 할당한 다음 목록에 추가할 것을 권장합니다.

OfficeScan 에이전트의 사용자 정의 업데이트 소스 구성

절차

1. **업데이트** > **에이전트** > **업데이트 소스**로 이동합니다.
2. **사용자 정의 업데이트 소스**를 선택하고 **추가**를 클릭합니다.
3. 표시되는 화면에서 에이전트의 IP 주소를 지정합니다. IPv4 범위 및/또는 IPv6 접두사와 길이를 입력할 수 있습니다.
4. 업데이트 소스를 지정합니다. 업데이트 에이전트를 선택(하나를 할당한 경우)하거나, 특정 소스의 URL을 입력할 수 있습니다.

참고

OfficeScan 에이전트가 해당 IP 주소를 사용하여 업데이트 소스에 연결할 수 있는지 확인합니다. 예를 들어 IPv4 주소 범위를 지정한 경우 업데이트 소스에 IPv4 주소가 있어야 합니다. IPv6 접두사와 길이를 지정한 경우 업데이트 소스에 IPv6 주소가 있어야 합니다. 에이전트 업데이트의 IPv6 지원에 대한 자세한 내용은 OfficeScan 에이전트 업데이트 소스 페이지 6-29을 참조하십시오.

5. **저장**을 클릭합니다.
6. 화면의 기타 작업을 수행합니다.
   a. 다음 설정 중 하나를 선택합니다. 이러한 설정의 작동 방식에 대한 자세한 내용은 OfficeScan 에이전트 업데이트 프로세스 페이지 6-30를 참조하십시오.
      - **업데이트 에이전트가 OfficeScan 서버에서만 구성 요소, 도메인 설정 및 에이전트 프로그램과 핫픽스 업데이트**
      - 모든 사용자 정의 소스를 사용할 수 없거나 찾을 수 없는 경우 OfficeScan 에이전트는 OfficeScan 서버에서 다음 항목을 업데이트합니다.
        - **구성 요소**
        - **도메인 설정**
        - **OfficeScan 에이전트 프로그램 및 핫픽스**
   b. 하나 이상의 업데이트 에이전트를 소스로 지정한 경우 **업데이트 에이전트 분석 보고서**를 클릭하여 에이전트의 업데이트 상태를 집중 분석하는 보고서를 생성합니다. 보고서에 대한 자세한 내용은 업데이트 에이전트 분석 보고서 페이지 6-59를 참조하십시오.
   c. IP 주소 범위 링크를 클릭하여 업데이트 소스를 편집합니다. 표시되는 화면에서 설정을 수정하고 **저장**을 클릭합니다.
   d. 확인란을 선택하고 **삭제**를 클릭하여 업데이트 소스를 목록에서 제거합니다.
   e. 업데이트 소스를 이동하려면 위쪽 또는 아래쪽 화살표를 클릭합니다. 한 번에 한 소스만 이동할 수 있습니다.

7. **모든 에이전트에 알림**을 클릭합니다.

OfficeScan 에이전트 업데이트 프로세스

참고

이 항목에서는 OfficeScan 에이전트의 업데이트 프로세스에 대해 설명합니다. 업데이트 에이전트의 업데이트 프로세스는 업데이트 에이전트의 사용자 정의 업데이트 소스 페이지 6-55에 설명되어 있습니다.

사용자 정의 업데이트 소스 목록을 설정하고 저장하면 다음과 같이 업데이트 프로세스가 진행됩니다.

1. OfficeScan 에이전트가 목록에 있는 첫 번째 소스에서 업데이트합니다.
2. 첫 번째 소스에서 업데이트할 수 없는 경우 OfficeScan 에이전트는 두 번째 소스에서 업데이트합니다.
3. 모든 소스에서 업데이트할 수 없는 경우 OfficeScan 에이전트는 **업데이트 소스** 화면에서 다음 설정을 확인합니다.

표 6-6. 사용자 정의 업데이트 소스에 대한 추가 설정

설정	설명
업데이트 에이전트가 OfficeScan 서버에서만 구성 요소, 도메인 설정 및 에이전트 프로그램과 핫픽스 업데이트	이 설정을 사용하도록 설정한 경우 업데이트 에이전트는 OfficeScan 서버에서 직접 업데이트하고 사용자 정의 업데이트 소스 목록을 무시합니다. 이 설정을 사용하지 않도록 설정한 경우 업데이트 에이전트는 일반 에이전트에 대해 구성된 사용자 정의 업데이트 소스 설정을 적용합니다.
모든 사용자 정의 소스를 사용할 수 없거나 찾을 수 없는 경우 OfficeScan 에이전트는 OfficeScan 서버에서 다음 항목을 업데이트합니다.	

설정	설명
구성 요소	이 설정을 사용하도록 설정한 경우 에이전트는 OfficeScan 서버에서 구성 요소를 업데이트합니다. 이 옵션을 사용하지 않도록 설정한 경우 에이전트는 다음 조건을 만족하면 Trend Micro 액티브업데이트 서버에 직접 연결을 시도합니다. • **에이전트** > **에이전트 관리**에서 **설정** > **권한 및 기타 설정** > **기타 설정(탭)** > **업데이트 설정**을 클릭하고 **OfficeScan 에이전트가 Trend Micro 액티브업데이트 서버에서 업데이트 다운로드** 옵션을 사용하도록 설정한 경우 • 액티브업데이트 서버가 사용자 정의 업데이트 소스 목록에 포함되어 있지 않은 경우 **참고** 구성 요소만 액티브업데이트 서버에서 업데이트할 수 있습니다. 도메인 설정, 프로그램 및 핫픽스는 OfficeScan 서버 또는 업데이트 에이전트에서 다운로드할 수만 있습니다. 액티브업데이트 서버에서 패턴 파일만 다운로드하도록 에이전트를 구성하여 업데이트 프로세스 속도를 높일 수 있습니다. 자세한 내용은 액티브업데이트 서버를 OfficeScan 에이전트 업데이트 소스로 사용 페이지 6-35를 참조하십시오.
도메인 설정	이 설정을 사용하도록 설정한 경우 에이전트는 OfficeScan 서버에서 도메인 수준 설정을 업데이트합니다.
OfficeScan 에이전트 프로그램 및 핫픽스	이 설정을 사용하도록 설정한 경우 에이전트는 OfficeScan 서버에서 프로그램 및 핫픽스를 업데이트합니다.

4. 사용 가능한 모든 소스에서 업데이트할 수 없는 경우, 에이전트는 업데이트 프로세스를 종료합니다.

액티브업데이트 서버를 OfficeScan 에이전트 업데이트 소스로 사용

OfficeScan 에이전트가 Trend Micro 액티브업데이트 서버에서 직접 업데이트를 다운로드하는 경우 패턴 파일로만 다운로드를 제한하여 업데이트 중에 사용되는 대역폭을 줄이고 업데이트 프로세스 속도를 높일 수 있습니다.

스캔 엔진 및 기타 구성 요소는 패턴 파일만큼 자주 업데이트되지 않으며 이는 다운로드를 패턴 파일로만 제한하는 또 다른 이유입니다.

순수 IPv6 에이전트 컴퓨터는 Trend Micro 액티브업데이트 서버에서 직접 업데이트할 수 없습니다. OfficeScan 에이전트에서 액티브업데이트 서버에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

액티브업데이트 서버에서의 다운로드 제한

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **시스템** 탭을 클릭합니다.
3. **업데이트** 섹션으로 이동합니다.
4. **업데이트를 수행할 때 액티브업데이트 서버에서 패턴 파일만 다운로드합니다**를 선택합니다.

OfficeScan 에이전트 업데이트 방법

OfficeScan 서버 또는 사용자 정의 업데이트 소스에서 구성 요소를 업데이트하는 OfficeScan 에이전트는 다음 업데이트 방법을 사용할 수 있습니다.

- **자동 업데이트**: 에이전트 업데이트가 특정 이벤트 발생 시 자동으로 실행되거나 일정을 기준으로 실행됩니다. 자세한 내용은 OfficeScan 에이전트 자동 업데이트 페이지 6-36를 참조하십시오.

- **수동 업데이트**: 업데이트가 중요한 경우, 수동 업데이트를 사용하여 에이전트에 구성 요소 업데이트를 수행하도록 즉시 알립니다. 자세한 내용은 OfficeScan 에이전트 수동 업데이트 페이지 6-42를 참조하십시오.
- **권한에 따른 업데이트**: 사용자에게 업데이트 권한이 있으면 컴퓨터의 OfficeScan 에이전트를 업데이트하는 방법을 더 잘 제어할 수 있습니다. 자세한 내용은 업데이트 권한 및 기타 설정 구성 페이지 6-43를 참조하십시오.

OfficeScan 에이전트 자동 업데이트

자동 업데이트를 사용하면 모든 에이전트에 업데이트하도록 알리는 부담을 없애고, 에이전트 컴퓨터의 구성 요소를 최신 상태로 유지하지 못할 위험을 없앨 수 있습니다.

이러한 구성 요소 외에도, OfficeScan 에이전트는 자동 업데이트 동안 업데이트된 구성 파일을 받습니다. 에이전트에 새 설정을 적용하려면 구성 파일이 필요합니다. 웹 콘솔을 통해 OfficeScan 설정을 수정할 때마다 구성 파일이 변경됩니다. 에이전트에 구성 파일을 적용하는 빈도를 지정하려면 3단계, OfficeScan 에이전트 자동 업데이트 구성 페이지 6-38을 참조하십시오.

참고

자동 업데이트 중에 프록시 설정을 사용하도록 에이전트를 구성할 수 있습니다. 자세한 내용은 OfficeScan 에이전트 구성 요소 업데이트용 프록시 페이지 6-46를 참조하십시오.

자동 업데이트에는 두 가지 유형이 있습니다.

- 이벤트에 따른 업데이트 페이지 6-36
- 일정에 따른 업데이트 페이지 6-37

이벤트에 따른 업데이트

서버는 온라인 에이전트에 최신 구성 요소를 다운로드한 후 구성 요소를 업데이트하도록 알리고 오프라인 에이전트에는 에이전트가 다시 시작된 다음 서버에 연결할 때 알릴 수 있습니다. 필요한 경우 업데이트 후에 OfficeScan 에이전트 엔드포인트에서 지금 검색(수동 검색)을 시작합니다.

표 6-7. 이벤트에 따른 업데이트 옵션

옵션	설명
OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 에이전트에서 구성 요소 업데이트 시작	서버는 업데이트를 완료하자마자 에이전트에 업데이트하도록 알립니다. 자주 업데이트되는 에이전트는 인크리멘탈 패턴만 다운로드해야 하므로 업데이트를 완료하는 데 걸리는 시간을 줄일 수 있습니다(인크리멘탈 패턴에 대한 자세한 내용은 OfficeScan 서버 구성 요소 복제 페이지 6-19 참조). 그러나 자주 업데이트하면 특히 동시에 업데이트하는 에이전트 수가 많은 경우 서버 성능이 저하될 수 있습니다. 에이전트가 독립 모드이고 이러한 에이전트도 업데이트하도록 하려면 **독립 및 오프라인 에이전트 포함**을 선택합니다. 독립 모드에 대한 자세한 내용은 OfficeScan 에이전트 독립 모드 권한 페이지 15-19 항목을 참조하십시오.
에이전트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(독립 에이전트 제외)	업데이트하지 못한 에이전트가 서버와의 연결을 설정하면 구성 요소를 즉시 다운로드합니다. 에이전트가 오프라인 상태이거나, 에이전트가 설치된 엔드포인트가 가동 중이 아니면 에이전트가 업데이트하지 못할 수 있습니다.
업데이트 후 지금 검색 수행(독립 에이전트 제외)	서버가 이벤트에 따른 업데이트 후에 검색하도록 에이전트에 알립니다. 네트워크 내에 이미 확산된 보안 위험에 대한 대응으로 특정 업데이트를 수행하는 경우 이 옵션을 사용할 수 있도록 설정하십시오.

참고

OfficeScan 서버가 구성 요소를 다운로드한 후 에이전트에 업데이트 알림을 제대로 전송하지 못한 경우에는 15분 후에 알림이 자동으로 재전송됩니다. 서버는 에이전트 응답을 받을 때까지 최대 5번에 걸쳐 업데이트 알림을 계속 보냅니다. 5번째 시도에서도 클라이언트 응답을 받지 못한 경우 서버는 알림 전송을 중지합니다. 에이전트가 다시 시작된 다음 서버에 연결할 때 구성 요소를 업데이트하는 옵션을 선택할 경우에는 구성 요소 업데이트가 계속됩니다.

일정에 따른 업데이트

예약 업데이트를 실행하는 것은 권한입니다. 먼저 권한을 부여할 OfficeScan 에이전트를 선택해야 이러한 OfficeScan 에이전트에서 일정에 따라 업데이트를 실행합니다.

참고

NAT(Network Address Translation)를 통해 일정에 따른 업데이트를 사용하려면 NAT를 사용하여 예약된 OfficeScan 에이전트 업데이트 구성 페이지 6-40를 참조하십시오.

OfficeScan 에이전트 자동 업데이트 구성

절차

1. **업데이트** > **에이전트** > **자동 업데이트**로 이동합니다.
2. **이벤트에 따른 업데이트**를 위한 이벤트를 선택합니다.
   - **OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 에이전트에서 구성 요소 업데이트 시작**
     - **독립 및 오프라인 에이전트 포함**
   - **에이전트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(독립 에이전트 제외)**
   - **업데이트 후 지금 검색 수행(독립 에이전트 제외)**

   사용 가능한 옵션에 대한 자세한 내용은 이벤트에 따른 업데이트 페이지 6-36를 참조하십시오.
3. **일정에 따른 업데이트**의 일정을 구성합니다.
   - **분** 또는 **시간**

     시간 또는 분 단위로 업데이트 빈도를 예약하는 경우 **에이전트 구성을 하루에 한 번만 업데이트** 옵션을 사용할 수 있습니다. 구성 파일에는 웹 콘솔을 사용하여 구성한 OfficeScan 에이전트 설정이 모두 포함됩니다.

팁

Trend Micro에서는 구성 요소를 자주 업데이트하지만 OfficeScan 구성 설정은 거의 변경되지 않습니다. 구성 요소와 구성 파일을 함께 업데이트할 경우 OfficeScan에서 업데이트를 완료하는 데 필요한 시간이 길어지고 대역폭 소비량이 커집니다. 따라서 Trend Micro에서는 OfficeScan 에이전트 구성을 하루에 한 번만 업데이트할 것을 권장합니다.

- **매일** 또는 **매주**

  업데이트 시간 및 OfficeScan 서버가 구성 요소를 업데이트하도록 에이전트에 알리는 기간을 지정합니다.

팁

이 설정을 구성하면 지정한 시작 시간에 모든 온라인 에이전트가 서버에 동시에 연결하지 못하므로 서버에 전달되는 트래픽 양이 크게 감소합니다. 예를 들어, 시작 시간이 오후 12시이고 기간이 2시간이면 OfficeScan은 모든 온라인 에이전트에 오후 12시부터 오후 2시까지 구성 요소를 업데이트하도록 임의로 알립니다.

참고

업데이트 일정을 구성한 후 선택한 에이전트에서 해당 일정을 사용하도록 설정합니다.

일정에 따른 업데이트가 사용되도록 설정하는 방법에 대한 자세한 내용은 업데이트 권한 및 기타 설정 구성 페이지 6-43의 4단계를 참조하십시오.

4. **저장**을 클릭합니다.

   OfficeScan에서 오프라인 에이전트에는 즉시 알리지 못합니다. **에이전트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(독립 에이전트 제외)**을 선택하면 기간이 만료된 후 온라인 상태가 되는 오프라인 에이전트를 업데이트할 수 있습니다. 이 설정을 사용하도록 설정하지 않은 오프라인 에이전트는 다음 일정 때나 수동 업데이트 동안에 구성 요소를 업데이트합니다.

NAT를 사용하여 예약된 OfficeScan 에이전트 업데이트 구성

로컬 네트워크에서 NAT를 사용하는 경우 다음과 같은 문제가 발생할 수 있습니다.

- 웹 콘솔에서 OfficeScan 에이전트가 오프라인 상태로 표시됩니다.
- OfficeScan 서버에서 에이전트에 업데이트와 구성 변경 사항을 알릴 수 없습니다.

아래 설명된 대로 예약 업데이트를 통해 서버의 업데이트된 구성 요소와 구성 파일을 OfficeScan 에이전트로 배포하여 이러한 문제를 해결합니다.

절차

- 에이전트 컴퓨터에 OfficeScan 에이전트를 설치하기 전에
  a. **업데이트** > **에이전트** > **자동 업데이트**의 **일정에 따른 업데이트** 섹션에서 에이전트 업데이트 일정을 구성합니다.
  b. **에이전트** > **에이전트 관리**에서 **설정** > **권한 및 기타 설정** > **권한(탭)** > **구성 요소 업데이트**를 클릭하여 에이전트에 예약 업데이트를 사용할 권한을 부여합니다.
- 에이전트 컴퓨터에 이미 OfficeScan 에이전트가 있는 경우
  a. **에이전트** > **에이전트 관리**에서 **설정** > **권한 및 기타 설정** > **권한(탭)** > **구성 요소 업데이트**를 클릭하여 에이전트에 "지금 업데이트"를 수행할 권한을 부여합니다.
  b. 사용자에게 에이전트 엔드포인트에서 구성 요소를 수동으로 업데이트(시스템 트레이에서 OfficeScan 에이전트 아이콘을 마우스 오른쪽 단추로 클릭하고 "지금 업데이트" 클릭)하여 업데이트된 구성 설정을 가져오도록 합니다.

OfficeScan 에이전트에서 업데이트를 수행하면 업데이트된 구성 요소와 구성 파일을 모두 받게 됩니다.

도메인 예약 업데이트 도구 사용

자동 에이전트 업데이트에서 구성된 업데이트 일정은 예약 업데이트 권한이 있는 에이전트에만 적용됩니다. 다른 에이전트의 경우 별도의 업데이트 일정을 설정할 수 있습니다. 이렇게 하려면 에이전트 트리 도메인별로 일정을 구성해야 합니다. 도메인에 속한 모든 에이전트에 일정이 적용됩니다.

참고

특정 에이전트 또는 특정 하위 도메인에 대한 업데이트 일정을 설정할 수는 없습니다. 모든 하위 도메인에 해당 상위 도메인에 대해 구성된 일정이 적용됩니다.

절차

1. 에이전트 트리 도메인 이름과 업데이트 일정을 기록합니다.
2. <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩DomainScheduledUpdate로 이동합니다.
3. 다음 파일을 <서버 설치 폴더>₩PCCSRV에 복사합니다.
   - DomainSetting.ini
   - dsu_convert.exe
4. 메모장과 같은 텍스트 편집기를 사용하여 DomainSetting.ini를 엽니다.
5. 에이전트 트리 도메인을 지정한 다음 해당 도메인에 대한 업데이트 일정을 구성합니다. 이 단계를 반복하여 도메인을 더 추가합니다.

   참고

   자세한 구성 지침은 .ini 파일에서 확인할 수 있습니다.

6. DomainSetting.ini를 저장합니다.
7. 명령 프롬프트를 열고 PCCSRV 폴더의 디렉터리로 변경합니다.
8. 다음 명령을 입력하고 `Enter` 키를 누릅니다.

   ```
   dsuconvert.exe DomainSetting.ini
   ```

9. 웹 콘솔에서 **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
10. **저장**을 클릭합니다.

OfficeScan 에이전트 수동 업데이트

OfficeScan 에이전트 구성 요소가 최신 버전이 아닌 경우 또는 비상 발생 시마다 OfficeScan 에이전트 구성 요소를 수동으로 업데이트합니다. OfficeScan 에이전트가 장기간 업데이트 소스를 통해 구성 요소를 업데이트하지 못하면 OfficeScan 에이전트 구성 요소를 최신 상태로 유지할 수 없습니다.

OfficeScan 에이전트에서는 구성 요소 외에 수동 업데이트 중에 업데이트된 구성 파일도 자동으로 받습니다. OfficeScan 에이전트에 새 설정을 적용하려면 구성 파일이 필요합니다. 웹 콘솔을 통해 OfficeScan 설정을 수정할 때마다 구성 파일이 변경됩니다.

참고

수동 업데이트를 시작하는 것 외에 사용자에게 수동 업데이트를 실행할 권한을 부여(OfficeScan 에이전트 엔드포인트의 경우 **지금 업데이트**라고도 함)할 수 있습니다. 자세한 내용은 업데이트 권한 및 기타 설정 구성 페이지 6-43를 참조하십시오.

수동으로 OfficeScan 에이전트 업데이트

절차

1. **업데이트** > **에이전트** > **수동 업데이트**로 이동합니다.
2. OfficeScan 서버에서 현재 사용할 수 있는 구성 요소와 이러한 구성 요소를 마지막으로 업데이트한 날짜가 화면의 맨 위에 표시됩니다. 에이전트에 업데이트하도록 알리기 전에 구성 요소가 최신 상태인지 확인합니다.

참고

서버에서 오래된 구성 요소를 수동으로 업데이트합니다.

자세한 내용은 OfficeScan 에이전트 수동 업데이트 페이지 6-42를 참조하십시오.

3. 오래된 구성 요소가 있는 에이전트만 업데이트하려면

   a. **오래된 구성 요소가 있는 에이전트 선택**을 클릭합니다.

   b. (선택 사항) **독립 및 오프라인 에이전트 포함**을 선택합니다.

      - 서버에 기능적으로 연결된 독립 에이전트를 업데이트하려는 경우
      - 오프라인 에이전트가 온라인 상태가 되면 업데이트하려는 경우

   c. **업데이트 시작**을 클릭합니다.

   참고

   서버에서 서버에 있는 버전보다 이전 버전의 구성 요소가 있는 에이전트를 검색한 다음 이러한 에이전트에 업데이트하도록 알립니다. 알림 상태를 확인하려면 **업데이트** > **요약** 화면으로 이동합니다.

4. 선택한 에이전트를 업데이트하려면

   a. **수동으로 에이전트 선택**을 선택합니다.

   b. **선택**을 클릭합니다.

   c. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.

   d. **업데이트 시작**을 클릭합니다.

   참고

   서버에서 각 에이전트에 업데이트 구성 요소를 다운로드하도록 알립니다. 알림 상태를 확인하려면 **업데이트** > **요약** 화면으로 이동합니다.

업데이트 권한 및 기타 설정 구성

업데이트 설정을 구성하고 에이전트 사용자에게 "지금 업데이트" 수행 및 예약 업데이트 사용과 같은 특정 권한을 부여합니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭하고 **업데이트 설정** 섹션에서 다음 옵션을 구성합니다.

옵션	설명
OfficeScan 에이전트가 Trend Micro 액티브업데이트 서버에서 업데이트 다운로드	업데이트를 시작할 때 OfficeScan 에이전트는 먼저 **업데이트** > **에이전트** > **업데이트 소스** 화면에 지정된 업데이트 소스에서 업데이트를 가져옵니다. 업데이트가 실패하는 경우, 에이전트는 OfficeScan 서버에서 업데이트하도록 시도합니다. 이 옵션을 선택하면 에이전트는 OfficeScan 서버를 통한 업데이트에 실패하는 경우 Trend Micro 액티브업데이트 서버에서 업데이트를 시도할 수 있습니다. **참고** 순수 IPv6 에이전트는 Trend Micro 액티브업데이트 서버에서 직접 업데이트할 수 없습니다. 에이전트에서 액티브업데이트 서버에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.
OfficeScan 에이전트에서 일정에 따른 업데이트 사용	이 옵션을 선택하면 모든 OfficeScan 에이전트가 기본적으로 일정에 따른 업데이트를 사용하도록 구성됩니다. **일정에 따른 업데이트 사용/사용 안 함** 권한이 있는 사용자는 이 설정을 무시할 수 있습니다. 업데이트 일정을 구성하는 방법에 대한 자세한 내용은 OfficeScan 에이전트 자동 업데이트 구성 페이지 6-38을 참조하십시오.
OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫	이 옵션을 선택하면 구성 요소 업데이트는 진행되지만 핫픽스 배포 및 OfficeScan 에이전트 업그레이드는 제한됩니다.

옵션	설명
픽스를 배포할 수 없음	**참고** 이 옵션을 사용하지 않도록 설정하면 모든 에이전트가 동시에 서버에 연결하여 업그레이드하거나 핫픽스를 설치하므로 서버 성능에 상당한 영향을 줄 수 있습니다.

5. **권한** 탭을 클릭하고 **구성 요소 업데이트** 섹션에서 다음 옵션을 구성합니다.

옵션	설명
"지금 업데이트" 수행	이 권한이 있는 사용자는 시스템 트레이에서 OfficeScan 에이전트 아이콘을 마우스 오른쪽 단추로 클릭하고 **지금 업데이트**를 선택하여 필요에 따라 구성 요소를 업데이트할 수 있습니다. **참고** OfficeScan 에이전트 사용자는 "지금 업데이트" 작업 중에 프록시 설정을 사용할 수 있습니다. 자세한 내용은 에이전트에 대한 프록시 구성 권한 페이지 15-50를 참조하십시오.
일정에 따른 업데이트 사용/사용 안 함	이 옵션을 선택하면 OfficeScan 에이전트 사용자가 OfficeScan 에이전트 마우스 오른쪽 단추 메뉴를 사용하여 예약 업데이트를 사용하거나 사용하지 않도록 설정하여 **일정에 따른 업데이트 사용** 설정을 재지정할 수 있습니다. **참고** 관리자가 먼저 **기타 설정** 탭에서 **OfficeScan 에이전트에서 일정에 따른 업데이트 사용** 설정을 선택해야 OfficeScan 에이전트 메뉴에 이 메뉴 항목이 표시됩니다.

6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트 업데이트를 위한 예약된 디스크 공간 구성

OfficeScan은 에이전트 디스크 공간의 일정 부분을 핫픽스, 패턴 파일, 검색 엔진, 프로그램 업데이트용으로 할당할 수 있습니다. OfficeScan에서는 기본적으로 60MB의 디스크 공간을 이 용도로 예약합니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **시스템** 탭을 클릭합니다.
3. **업데이트** 섹션으로 이동합니다.
4. **업데이트용으로 __MB의 디스크 공간 예약**을 선택합니다.
5. 디스크 공간의 양을 선택합니다.
6. **저장**을 클릭합니다.

OfficeScan 에이전트 구성 요소 업데이트용 프록시

OfficeScan 에이전트는 자동 업데이트 중에 또는 "지금 업데이트"를 수행할 권한이 있는 경우 프록시 설정을 사용할 수 있습니다.

표 6-8. OfficeScan 에이전트 구성 요소 업데이트 중에 사용되는 프록시 설정

업데이트 방법	사용되는 프록시 설정	사용
액티브업데이트	• 자동 프록시 설정. 자세한 내용은 OfficeScan 에이전트에 대한 자동 프록시 설정 페이지 15-51를 참조하십시오. • 내부 프록시 설정. 자세한 내용은 OfficeScan 에이전트용 내부 프록시 페이지 15-47를 참조하십시오.	1. OfficeScan 에이전트는 먼저 자동 프록시 설정을 사용하여 구성 요소를 업데이트합니다. 2. 자동 프록시 설정을 사용할 수 없는 경우 내부 프록시 설정이 사용됩니다. 3. 두 설정을 모두 사용할 수 없는 경우에는 에이전트가 프록시 설정을 사용하지 않습니다.
지금 업데이트	• 자동 프록시 설정. 자세한 내용은 OfficeScan 에이전트에 대한 자동 프록시 설정 페이지 15-51를 참조하십시오. • 사용자 구성 프록시 설정. 에이전트 사용자에게 프록시 설정을 구성할 권한을 부여할 수 있습니다. 자세한 내용은 에이전트에 대한 프록시 구성 권한 페이지 15-50를 참조하십시오.	1. OfficeScan 에이전트는 먼저 자동 프록시 설정을 사용하여 구성 요소를 업데이트합니다. 2. 자동 프록시 설정을 사용할 수 없는 경우 사용자 구성 프록시 설정이 사용됩니다. 3. 두 설정을 모두 사용할 수 없거나, 자동 프록시 설정을 사용할 수 없고 에이전트 사용자에게 필요한 권한이 없는 경우에는 에이전트에서 구성 요소를 업데이트할 때 프록시를 사용하지 않습니다.

OfficeScan 에이전트 업데이트 알림 구성

OfficeScan은 에이전트 사용자에게 업데이트 관련 이벤트의 발생 시기를 알려 줍니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **에이전트 제어** 탭을 클릭합니다.

3. **경고 설정** 섹션으로 이동합니다.
4. 다음 옵션을 선택합니다.
   - **__일 후에 바이러스 패턴 파일이 업데이트되지 않으면 Windows 작업 표시줄에 경고 아이콘 표시**: 지정된 일 수 이내에 업데이트하지 않은 바이러스 패턴을 업데이트하도록 사용자에게 알리기 위해 Windows 작업 표시줄에 경고 아이콘이 표시됩니다. 패턴을 업데이트하려면 OfficeScan 에이전트 업데이트 방법 페이지 6-35에 설명된 업데이트 방법 중 하나를 사용합니다.

     서버에서 관리하는 모든 에이전트가 이 설정을 적용합니다.
   - **엔드포인트를 다시 시작하여 커널 모드 드라이버를 로드해야 하는 경우 알림 메시지 표시**: 커널 모드 드라이버의 새 버전이 포함된 업그레이드 패키지나 핫픽스를 설치한 후에도 드라이버의 이전 버전은 엔드포인트에 그대로 있을 수 있습니다. 이전 버전을 종료하고 새 버전을 로드하려면 엔드포인트를 다시 시작해야 합니다. 엔드포인트를 다시 시작하면 새 버전이 자동으로 설치되므로 더 이상 다시 시작할 필요가 없습니다.

     에이전트 엔드포인트가 핫픽스나 업그레이드 패키지를 설치하고 나면 즉시 알림 메시지가 표시됩니다.
5. **저장**을 클릭합니다.

OfficeScan 에이전트 업데이트 로그 보기

에이전트 업데이트 로그에서 에이전트의 바이러스 패턴을 업데이트하는 데 문제가 있는지 확인합니다.

참고

이 제품 버전에서는 웹 콘솔에서 바이러스 패턴 업데이트에 대한 로그만 쿼리할 수 있습니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

절차

1. **로그** > **에이전트** > **에이전트 구성 요소 업데이트**로 이동합니다.
2. 에이전트 업데이트 수를 보려면 **진행률** 열에서 **보기**를 클릭합니다. 표시되는 **구성 요소 업데이트 진행률** 화면에서 15분마다 업데이트되는 에이전트 수와 업데이트된 총 에이전트 수를 확인합니다.
3. 바이러스 패턴을 업데이트한 에이전트를 보려면 **세부 정보** 열에서 **보기**를 클릭합니다.
4. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

OfficeScan 에이전트 업데이트 적용

보안 준수를 사용하여 에이전트에 최신 구성 요소가 있는지 확인합니다. 보안 준수는 OfficeScan 서버와 에이전트 간의 구성 요소 불일치를 확인합니다. 불일치는 일반적으로 에이전트가 구성 요소 업데이트를 위해 서버에 연결할 수 없는 경우 발생합니다. 에이전트가 다른 소스(예를 들어 액티브업데이트 서버)에서 업데이트를 가져올 경우 에이전트의 구성 요소가 서버의 구성 요소보다 최신 버전일 수 있습니다.

자세한 내용은 관리되는 에이전트에 대한 보안 준수 페이지 15-55를 참조하십시오.

OfficeScan 에이전트에 대한 구성 요소 롤백

롤백은 이전 버전의 바이러스 패턴, 스마트 스캔 에이전트 패턴 및 바이러스 검색 엔진으로 되돌리는 것을 말합니다. 이러한 구성 요소가 제대로 작동하지 않으면 이전 버전으로 롤백합니다. OfficeScan은 현재 및 이전 버전의 바이러스 검색 엔진과 최근 5개 버전의 바이러스 패턴 및 스마트 스캔 에이전트 패턴을 유지합니다.

참고

위에서 언급한 구성 요소만 롤백할 수 있습니다.

OfficeScan에서는 32비트 플랫폼과 64비트 플랫폼을 실행하는 에이전트에 대해 서로 다른 검색 엔진을 사용합니다. 이러한 검색 엔진은 개별적으로 롤백해야 합니다. 모든 유형의 검색 엔진에 대한 롤백 절차는 동일합니다.

절차

1. **업데이트** > **롤백**으로 이동합니다.
2. 해당 섹션에서 **서버와 동기화**를 클릭합니다.
   a. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
   b. **롤백**을 클릭합니다.
   c. **업데이트 로그 보기**를 클릭하여 결과를 확인하거나 **뒤로**를 클릭하여 롤백 화면으로 돌아갑니다.
3. 서버에 이전 버전의 패턴 파일이 있는 경우 **서버 및 에이전트 버전 롤백**을 클릭하여 에이전트의 패턴 파일과 서버의 패턴 파일을 모두 롤백합니다.

OfficeScan 에이전트 핫픽스에 대한 터치 도구 실행

터치 도구를 사용하면 한 파일의 타임스탬프가 다른 파일의 타임스탬프 또는 엔드포인트의 시스템 시간과 동기화됩니다. OfficeScan 서버에 핫픽스를 배포하려 했지만 제대로 배포되지 않은 경우, 터치 도구를 사용하여 핫픽스의 타임스탬프를 변경하십시오. 그러면 OfficeScan이 핫픽스 파일을 새 파일로 해석하여 서버가 자동으로 핫픽스를 다시 배포합니다.

절차

1. OfficeScan 서버에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩Touch로 이동합니다.
2. TMTouch.exe를 변경할 파일이 포함된 폴더에 복사합니다. 파일의 타임스탬프를 다른 파일의 타임스탬프와 동기화하려면 두 파일을 터치 도구와 같은 위치에 둡니다.

3. 명령 프롬프트를 열고 터치 도구 위치로 이동합니다.
4. 다음과 같이 입력합니다.

   `TmTouch.exe <대상 파일 이름> <원본 파일 이름>`

   여기서 각 항목은 다음과 같습니다.

   - `<대상 파일 이름>`은 변경할 타임스탬프의 핫픽스 파일의 이름입니다.
   - `<원본 파일 이름>`은 타임스탬프를 복제할 파일의 이름입니다.

   참고

   원본 파일 이름을 지정하지 않으면 대상 파일의 타임스탬프가 엔드포인트의 시스템 시간으로 설정됩니다. 와일드카드 문자(*)는 대상 파일 이름에만 사용하고 원본 파일 이름에는 사용하지 마십시오.

5. 타임스탬프가 변경되었는지 확인하려면 명령 프롬프트에 `dir`을 입력하거나 Windows 탐색기에서 파일의 등록정보를 확인합니다.

업데이트 에이전트

OfficeScan 에이전트에 구성 요소, 도메인 설정 또는 에이전트 프로그램 및 핫픽스를 배포하는 작업을 분산하려면 업데이트 에이전트 역할을 할 일부 OfficeScan 에이전트를 할당하거나 다른 에이전트에 대한 소스를 업데이트합니다. 이렇게 하면 상당한 양의 네트워크 트래픽을 OfficeScan 서버로 전달하지 않고도 에이전트가 업데이트를 적시에 받을 수 있습니다.

네트워크가 위치별로 세그먼트화되고 세그먼트 사이의 네트워크 링크에 트래픽 부하가 높을 경우, 각 위치에서 하나 이상의 업데이트 에이전트를 할당합니다.

참고

업데이트 에이전트에서 구성 요소를 업데이트하도록 할당한 OfficeScan 에이전트만 업데이트 에이전트에서 업데이트된 구성 요소와 설정을 받습니다. 하지만 모든 OfficeScan 에이전트가 계속 OfficeScan 서버에 상태를 보고합니다.

업데이트 에이전트 시스템 요구 사항

시스템 요구 사항의 전체 목록은 다음 웹 사이트에서 확인하십시오.

http://docs.trendmicro.com/ko-kr/enterprise/officescan.aspx

업데이트 에이전트 구성

업데이트 에이전트 구성은 다음과 같이 2단계로 된 프로세스입니다.

1. OfficeScan 에이전트를 특정 구성 요소의 업데이트 에이전트로 할당합니다.
2. 이 업데이트 에이전트에서 업데이트할 에이전트를 지정합니다.

참고

하나의 업데이트 에이전트에서 처리할 수 있는 동시 에이전트 연결 수는 엔드포인트의 하드웨어 사양에 따라 다릅니다.

업데이트 에이전트로 OfficeScan 에이전트 지정

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 업데이트 에이전트로 지정할 에이전트를 선택합니다.

참고

루트 도메인 아이콘은 모든 에이전트를 업데이트 에이전트로 지정하므로 루트 도메인 아이콘을 선택할 수 없습니다. 순수 IPv6 업데이트 에이전트는 순수 IPv4 에이전트에 직접 업데이트를 배포할 수 없습니다. 마찬가지로 순수 IPv4 업데이트 에이전트는 순수 IPv6 에이전트에 직접 업데이트를 배포할 수 없습니다. 업데이트 에이전트가 에이전트에 업데이트를 배포할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

3. **설정** > **업데이트 에이전트 설정**을 클릭합니다.

4. 업데이트 에이전트가 공유할 수 있는 항목을 선택합니다.
   - 구성 요소 업데이트
   - 도메인 설정
   - OfficeScan 에이전트 프로그램 및 핫픽스
5. **저장**을 클릭합니다.

업데이트 에이전트에서 업데이트하는 OfficeScan 에이전트 지정

절차

1. **업데이트** > **에이전트** > **업데이트 소스**로 이동합니다.
2. **사용자 정의 업데이트 소스 목록**에서 **추가**를 클릭합니다.
3. 표시되는 화면에서 에이전트의 IP 주소를 지정합니다. IPv4 범위 및/또는 IPv6 접두사와 길이를 입력할 수 있습니다.
4. **업데이트 에이전트** 필드에서 에이전트에 할당할 업데이트 에이전트를 선택합니다.

   참고

   에이전트가 해당 IP 주소를 사용하여 업데이트 에이전트에 연결할 수 있는지 확인합니다. 예를 들어 IPv4 주소 범위를 지정한 경우 업데이트 에이전트에 IPv4 주소가 있어야 합니다. IPv6 접두사와 길이를 지정한 경우 업데이트 에이전트에 IPv6 주소가 있어야 합니다.
5. **저장**을 클릭합니다.

업데이트 에이전트의 업데이트 소스

업데이트 에이전트는 OfficeScan 서버와 같은 여러 소스나 사용자 정의 업데이트 소스에서 업데이트를 가져올 수 있습니다. 웹 콘솔의 업데이트 소스 화면에서 업데이트 소스를 구성합니다.

업데이트 에이전트에 대한 IPv6 지원

순수 IPv6 업데이트 에이전트는 다음과 같은 순수 IPv4 업데이트 소스에서 직접 업데이트할 수 없습니다.

- 순수 IPv4 OfficeScan 서버
- 모든 순수 IPv4 사용자 정의 업데이트 소스
- Trend Micro 액티브업데이트 서버

마찬가지로 순수 IPv4 업데이트 에이전트는 순수 IPv6 OfficeScan 서버와 같은 순수 IPv6 업데이트 소스에서 직접 업데이트할 수 없습니다.

업데이트 에이전트에서 업데이트 소스에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

업데이트 에이전트의 표준 업데이트 소스

OfficeScan 서버는 업데이트 에이전트의 표준 업데이트 소스입니다. OfficeScan 서버에서 직접 업데이트하도록 에이전트를 구성하는 경우, 다음과 같이 업데이트 프로세스가 진행됩니다.

1. 업데이트 에이전트가 OfficeScan 서버에서 업데이트를 가져옵니다.
2. OfficeScan 서버에서 업데이트할 수 없는 경우 다음 조건을 만족하면 에이전트가 Trend Micro 액티브업데이트 서버에 직접 연결을 시도합니다.
   - **에이전트** > **에이전트 관리**에서 **설정** > **권한 및 기타 설정** > **기타 설정** > **업데이트 설정**을 클릭하고 **OfficeScan 에이전트가 Trend Micro 액티브업데이트 서버에서 업데이트 다운로드** 옵션을 사용하도록 설정한 경우
   - 액티브업데이트 서버는 사용자 정의 업데이트 소스 목록의 첫 번째 항목입니다.

팁

OfficeScan 서버를 업데이트하는 데 문제가 발생하는 경우에만 액티브업데이트 서버를 목록의 맨 위에 배치합니다. 업데이트 에이전트가 액티브업데이트 서버에서 직접 업데이트하는 경우, 네트워크와 인터넷 간에 많은 대역폭이 사용됩니다.

3. 사용 가능한 모든 소스에서 업데이트할 수 없는 경우, 업데이트 에이전트가 업데이트 프로세스를 종료합니다.

업데이트 에이전트의 사용자 정의 업데이트 소스

OfficeScan 서버 외에 업데이트 에이전트가 사용자 지정 업데이트 소스에서 업데이트할 수 있습니다. 사용자 정의 업데이트 소스를 사용하면 OfficeScan 서버로 전달되는 에이전트 업데이트 트래픽을 줄일 수 있습니다. 사용자 정의 업데이트 소스 목록에 사용자 지정 업데이트 소스를 지정합니다. 이 목록에는 최대 1024개의 업데이트 소스를 나열할 수 있습니다. 목록을 구성하는 단계에 대해서는 OfficeScan 에이전트의 사용자 정의 업데이트 소스 페이지 6-31를 참조하십시오.

참고

업데이트 에이전트가 사용자 정의 업데이트 소스에 연결할 수 있도록 하려면 **에이전트의 업데이트 소스** 화면(**업데이트** > **에이전트** > **업데이트 소스**) 화면에서 **업데이트 에이전트가 OfficeScan 서버에서만 구성 요소, 도메인 설정 및 에이전트 프로그램과 핫픽스 업데이트** 옵션을 사용하지 않도록 설정했는지 확인합니다.

목록을 설정하고 저장하면 다음과 같이 업데이트 프로세스가 진행됩니다.

1. 업데이트 에이전트가 목록에 있는 첫 번째 항목부터 업데이트합니다.
2. 첫 번째 항목부터 업데이트할 수 없는 경우에는 에이전트가 두 번째 항목부터 업데이트합니다.
3. 모든 항목에서 업데이트할 수 없는 경우 에이전트는 **모든 사용자 정의 소스를 사용할 수 없거나 찾을 수 없는 경우 OfficeScan 에이전트는 OfficeScan 서버에서 다음 항목을 업데이트합니다**라는 제목 아래에서 다음 옵션을 확인합니다.

    - **구성 요소**: 이 옵션을 사용하도록 설정한 경우, 에이전트가 OfficeScan 서버에서 업데이트합니다.

      이 옵션을 사용하지 않도록 설정한 경우 다음 조건을 만족하면 에이전트가 Trend Micro 액티브업데이트 서버에 직접 연결을 시도합니다.

참고

구성 요소만 액티브업데이트 서버에서 업데이트할 수 있습니다. 도메인 설정, 프로그램 및 핫픽스는 서버 또는 업데이트 에이전트에서 다운로드할 수만 있습니다.

- **에이전트 > 에이전트 관리**에서 **설정 > 권한 및 기타 설정 > 기타 설정 > 업데이트 설정**을 클릭하고 **에이전트가 Trend Micro 액티브업데이트 서버에서 업데이트 다운로드** 옵션을 사용하도록 설정한 경우
- 액티브업데이트 서버가 사용자 정의 업데이트 소스 목록에 포함되어 있지 않은 경우

- **도메인 설정**: 이 옵션을 사용하도록 설정한 경우, 에이전트가 OfficeScan 서버에서 업데이트합니다.
- **OfficeScan 에이전트 프로그램 및 핫픽스**: 이 옵션을 사용하도록 설정한 경우, 에이전트가 OfficeScan 서버에서 업데이트합니다.

4. 사용 가능한 모든 소스에서 업데이트할 수 없는 경우, 업데이트 에이전트가 업데이트 프로세스를 종료합니다.

표준 업데이트 소스(OfficeScan 서버에서 업데이트) 옵션을 사용하도록 설정하고 OfficeScan 서버가 에이전트에 구성 요소를 업데이트하도록 알리는 경우 업데이트 프로세스가 달라집니다. 해당 프로세스는 다음과 같습니다.

1. 에이전트가 OfficeScan 서버에서 직접 업데이트하고 업데이트 소스 목록을 삭제합니다.
2. 서버에서 업데이트할 수 없는 경우 다음 조건을 만족하면 에이전트가 Trend Micro 액티브업데이트 서버에 직접 연결을 시도합니다.
   - **에이전트 > 에이전트 관리**에서 **설정 > 권한 및 기타 설정 > 기타 설정 > 업데이트 설정**을 클릭하고 **OfficeScan 에이전트가 Trend Micro 액티브업데이트 서버에서 업데이트 다운로드** 옵션을 사용하도록 설정한 경우
   - 액티브업데이트 서버는 사용자 정의 업데이트 소스 목록의 첫 번째 항목입니다.

팁

OfficeScan 서버를 업데이트하는 데 문제가 발생하는 경우에만 액티브업데이트 서버를 목록의 맨 위에 배치합니다. OfficeScan 에이전트가 액티브업데이트 서버에서 직접 업데이트하는 경우 네트워크와 인터넷 간에 많은 대역폭이 사용됩니다.

3. 사용 가능한 모든 소스에서 업데이트할 수 없는 경우, 업데이트 에이전트가 업데이트 프로세스를 종료합니다.

업데이트 에이전트의 업데이트 소스 구성

절차

1. **업데이트** > **에이전트** > **업데이트 소스**로 이동합니다.
2. 업데이트 에이전트의 표준 업데이트 소스(OfficeScan 서버)에서 업데이트할지, 업데이트 에이전트의 사용자 정의 업데이트 소스에서 업데이트할지 선택합니다.
3. **모든 에이전트에 알림**을 클릭합니다.

업데이트 에이전트 구성 요소 복제

OfficeScan 서버와 마찬가지로 업데이트 에이전트도 구성 요소를 다운로드할 때 구성 요소 복제를 사용합니다. 서버에서 구성 요소 복제를 수행하는 방법에 대한 자세한 내용은 OfficeScan 서버 구성 요소 복제 페이지 6-19를 참조하십시오.

업데이트 에이전트의 구성 요소 복제 프로세스는 다음과 같습니다.

1. 업데이트 에이전트는 현재 전체 패턴 버전을 업데이트 소스에 있는 최신 버전과 비교합니다. 두 버전 사이의 차이가 14 이하인 경우, 업데이트 에이전트는 두 버전 사이의 차이를 바탕으로 만든 인크리멘탈 패턴만 다운로드합니다.

참고

차이가 14보다 큰 경우에는 업데이트 에이전트가 패턴 파일의 전체 버전을 자동으로 다운로드합니다.

2. 업데이트 에이전트는 다운로드한 인크리멘탈 패턴을 현재 전체 패턴과 병합하여 최신 전체 패턴을 생성합니다.
3. 업데이트 에이전트에서 업데이트 소스에 있는 나머지 인크리멘탈 패턴을 모두 다운로드합니다.
4. 최신 전체 패턴과 모든 인크리멘탈 패턴을 에이전트에서 사용할 수 있습니다.

업데이트 에이전트용 업데이트 방법

업데이트 에이전트는 일반 에이전트에서 사용할 수 있는 동일한 업데이트 방법을 사용합니다. 자세한 내용은 OfficeScan 에이전트 업데이트 방법 페이지 6-35를 참조하십시오.

예약 업데이트 구성 도구를 사용하여 에이전트 패키지 도구를 통해 설치한 업데이트 에이전트의 예약 업데이트를 활성화하고 구성할 수도 있습니다.

참고

다른 설치 방법을 사용하여 업데이트 에이전트를 설치한 경우에는 이 도구를 사용할 수 없습니다. 자세한 내용은 배포 고려 사항 페이지 5-11를 참조하십시오.

예약 업데이트 구성 도구 사용

절차

1. 업데이트 에이전트 엔드포인트에서 <에이전트 설치 폴더>로 이동합니다.
2. SUCTool.exe를 두 번 클릭하여 도구를 실행합니다. 예약 업데이트 구성 도구 콘솔이 열립니다.
3. **예약 업데이트 사용**을 선택합니다.
4. 업데이트 빈도와 시간을 지정합니다.
5. **적용**을 클릭합니다.

업데이트 에이전트 분석 보고서

업데이트 에이전트 분석 보고서를 생성하여 업데이트 인프라를 분석하고 업데이트 에이전트 및 기타 업데이트 소스에서 일부 업데이트를 다운로드할 에이전트를 결정합니다.

참고

이 보고서에는 업데이트 에이전트에서 일부 업데이트를 받도록 구성된 모든 OfficeScan 에이전트가 포함됩니다. 하나 이상의 도메인 관리 작업을 다른 관리자에게 위임한 경우 다른 관리자도 관리하지 않는 도메인에 속한 업데이트 에이전트에서 일부 업데이트를 받도록 구성된 모든 OfficeScan 에이전트를 볼 수 있습니다.

OfficeScan은 업데이트 에이전트 분석 보고서를 쉼표로 구분된 값(.csv) 파일로 내보냅니다.

이 보고서에는 다음 정보가 포함됩니다.

- OfficeScan 에이전트 엔드포인트
- IP 주소
- 에이전트 트리 경로
- 업데이트 소스
- 에이전트가 업데이트 에이전트에서 다음을 다운로드하는 경우
  - 구성 요소
  - 도메인 설정
  - OfficeScan 에이전트 프로그램 및 핫픽스

중요

업데이트 에이전트 분석 보고서에는 업데이트 에이전트에서 일부 업데이트를 받도록 구성된 OfficeScan 에이전트만 나열됩니다. 업데이트 에이전트에서 전체 업데이트(구성 요소, 도메인 설정 및 OfficeScan 에이전트 프로그램과 핫픽스 포함)를 수행하도록 구성된 OfficeScan 에이전트는 보고서에 표시되지 않습니다.

보고서 생성에 대한 자세한 내용은 OfficeScan 에이전트의 사용자 정의 업데이트 소스 페이지 6-31를 참조하십시오.

구성 요소 업데이트 요약

웹 콘솔은 사용자에게 전체 구성 요소 업데이트 상태를 알리고 만료된 구성 요소를 업데이트할 수 있도록 하는 **업데이트 요약** 화면(**업데이트** > **요약**으로 이동)을 제공합니다. 서버 예약 업데이트를 사용하도록 설정하면 화면에 다음 업데이트 일정도 표시됩니다.

최신 구성 요소 업데이트 상태를 보려면 화면을 정기적으로 새로 고칩니다.

참고

통합 스마트 보호 서버에서 구성 요소 업데이트를 보려면 **관리** > **스마트 보호** > **통합 서버**로 이동합니다.

OfficeScan 에이전트의 업데이트 상태

에이전트에 대해 구성 요소 업데이트를 시작한 경우, 이 섹션에서 다음과 같은 정보를 볼 수 있습니다.

- 구성 요소 업데이트 알림을 받은 에이전트 수
- 아직 알림을 받지 못했지만 이미 알림 대기열에 있는 에이전트 수 대기열에 있는 에이전트에 대한 알림을 취소하려면 **알림 취소**를 클릭합니다.

구성 요소

업데이트 상태 테이블에서 OfficeScan 서버가 다운로드하고 배포한 각 구성 요소의 업데이트 상태를 확인할 수 있습니다.

각 구성 요소에 대한 현재 버전 및 최신 업데이트 날짜를 확인합니다. 오래된 구성 요소가 있는 에이전트를 보려면 해당 번호 링크를 클릭합니다. 오래된 구성 요소가 있는 에이전트를 수동으로 업데이트합니다.

장 7

보안 위험 검색

이 장에서는 파일 기반 검색을 사용하여 보안 위험으로부터 엔드포인트를 보호하는 방법에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- 보안 위험 정보 페이지 7-2
- 검색 방법 유형 페이지 7-8
- 검색 유형 페이지 7-14
- 모든 검색 유형에 대한 일반적인 설정 페이지 7-26
- 검색 권한 및 기타 설정 페이지 7-53
- 글로벌 검색 설정 페이지 7-69
- 보안 위험 알림 페이지 7-79
- 보안 위험 로그 페이지 7-88
- 보안 위험 비상 발생 페이지 7-103

보안 위험 정보

보안 위험은 바이러스/악성 프로그램 및 스파이웨어/그레이웨어를 통칭하는 용어입니다. OfficeScan은 파일을 검색한 후 검색된 각 보안 위험에 대해 특정 작업을 수행하여 보안 위험으로부터 엔드포인트를 보호합니다. 짧은 시간 동안 검색된 다수의 보안 위험은 비상의 조짐을 나타냅니다. OfficeScan은 바이러스 사전 방역 정책을 적용하고 위험이 완전히 없는 상태가 될 때까지 감염된 엔드포인트를 격리하여 비상 발생을 억제하도록 도와줍니다. 알림 및 로그를 사용하여 보안 위험을 추적할 수 있으며 즉시 조치를 취해야 하는 경우에는 경고가 발생합니다.

바이러스 및 악성 프로그램

바이러스/악성 프로그램 종류는 수만 가지에 달하며 매일 새로운 바이러스가 만들어지고 있습니다. 한때 DOS나 Windows에 한정된 것으로 여겨졌던 엔드포인트 바이러스가 요즘은 기업의 네트워크, 전자 메일 시스템 및 웹 사이트의 취약점을 이용하여 막대한 손상을 일으킬 수 있습니다.

표 7-1. 바이러스/악성 프로그램 유형

바이러스/악성 프로그램 유형	설명
조크 프로그램	조크 프로그램은 바이러스와 유사한 프로그램으로, 주로 엔드포인트 모니터에서 화면 표시 동작을 조작합니다.
기타	"기타"에는 다른 어떠한 유형의 바이러스/악성 프로그램으로도 분류되지 않는 바이러스/악성 프로그램이 포함됩니다.
패커	패커는 압축 및/또는 암호화된 Windows 또는 Linux™ 실행 프로그램으로, 흔히 트로이 목마 프로그램이라고 합니다. 실행 프로그램을 압축하면 바이러스 백신 제품에서 패커를 찾아내기가 더욱 어려워집니다.

바이러스/악성 프로그램 유형	설명
루트키트	루트키트는 사용자의 동의 없이 또는 사용자 모르게 시스템에 코드를 설치하고 실행하는 프로그램(또는 프로그램 모음)입니다. 루트키트는 은폐 모드를 사용하여 컴퓨터에서 탐지할 수 없는 영구적인 상태를 유지합니다. 루트키트는 컴퓨터를 감염시키는 대신 악성 코드를 실행하기 위한 탐지할 수 없는 환경을 제공합니다. 루트키트는 소셜 엔지니어링을 통해 시스템에 설치되거나, 악성 프로그램 실행 시 시스템에 설치될 수 있으며, 단순히 유해 웹 사이트를 검색하는 것만으로도 시스템에 설치될 수 있습니다. 설치된 후 공격자는 프로세스, 파일, 레지스트리 키 및 통신 채널 숨기기를 비롯해 원격 액세스, 도청 등 거의 모든 기능을 시스템에서 수행할 수 있습니다.
테스트 바이러스	테스트 바이러스는 실제 바이러스처럼 동작하며 바이러스 검색 소프트웨어에서 발견될 수 있는 비활성 파일입니다. EICAR 테스트 스크립트와 같은 테스트 바이러스를 사용하여 설치되어 있는 바이러스 백신 프로그램에서 검색을 제대로 수행하는지 확인할 수 있습니다.
트로이 목마	트로이 목마 프로그램은 포트를 사용하여 컴퓨터 또는 실행 프로그램에 대한 액세스 권한을 얻는 경우가 많습니다. 트로이목마 프로그램은 복제되지는 않지만 시스템에 상주하여 해커가 침입할 수 있도록 포트를 여는 등 유해한 동작을 수행합니다. 기존의 바이러스 백신 솔루션의 경우 바이러스는 발견 및 제거할 수 있지만 트로이 목마 특히, 시스템에서 이미 실행 중인 트로이 목마는 제거할 수 없습니다.

바이러스/악성 프로그램 유형	설명
바이러스	바이러스는 복제되는 프로그램입니다. 바이러스가 복제되려면 다음을 포함하여 바이러스 자체가 다른 프로그램 파일에 첨부되어 호스트 프로그램이 실행될 때마다 실행되어야 합니다. • **ActiveX 악성 코드**: 웹 페이지에 상주하면서 ActiveX™ 컨트롤을 실행하는 코드입니다. • **부트 섹터 바이러스**: 파티션 또는 디스크의 부트 섹터를 감염시키는 바이러스입니다. • **COM 및 EXE 파일 감염자**: 확장자가 .com 또는 .exe인 실행 프로그램입니다. • **Java 악성 코드**: 운영 체제와 상관없이 Java™로 작성되었거나 Java에 포함된 바이러스 코드입니다. • **매크로 바이러스**: 응용 프로그램 매크로로 인코딩되며, 주로 문서에 포함되는 바이러스입니다. • **VBScript**, **JavaScript** 또는 **HTML 바이러스**: 웹 페이지에 상주하며 브라우저를 통해 다운로드되는 바이러스입니다. • **웜**: 주로 전자 메일을 통해 자체 복사본이나 해당 세그먼트를 다른 엔드포인트 시스템으로 전파할 수 있는 독립형 프로그램 또는 일련의 프로그램입니다.
네트워크 바이러스	엄밀히 말하면, 네트워크에서 확산되는 바이러스가 모두 네트워크 바이러스인 것은 아닙니다. 웜과 같은 일부 바이러스/악성 프로그램 유형만 네트워크 바이러스라고 할 수 있습니다. 특히, 네트워크 바이러스는 TCP, FTP, UDP, HTTP 및 전자 메일 프로토콜과 같은 네트워크 프로토콜을 사용하여 복제됩니다. 일반적으로 네트워크 바이러스로 인해 시스템 파일이 변경되거나 하드 디스크의 부트 섹터가 수정되지는 않습니다. 대신, 네트워크 바이러스는 에이전트 엔드포인트의 메모리를 감염시켜 네트워크 트래픽이 초과되게 하므로 네트워크의 속도 저하 및 오류를 발생시킬 수 있습니다. 네트워크 바이러스는 메모리에 남아 있기 때문에 기존의 파일 I/O 기반 검색 방법으로는 발견할 수 없는 경우가 많습니다.

바이러스/악성 프로그램 유형	설명
가능성이 있는 바이러스/악성 프로그램	가능성이 있는 바이러스/악성 프로그램은 바이러스/악성 프로그램의 특징을 일부 지닌 의심스러운 파일입니다. 자세한 내용은 Trend Micro 위협 백과사전을 참조하십시오. http://about-threats.trendmicro.com/apac/threatencyclopedia#malware **참고** 가능성이 있는 바이러스/악성 프로그램은 치료할 수 없지만 검색 조치를 구성할 수는 있습니다.

스파이웨어 및 그레이웨어

엔드포인트는 바이러스/악성 프로그램이 아닌 다른 잠재적 위협 요소에도 노출될 수 있습니다. 스파이웨어/그레이웨어란 바이러스나 트로이 목마로 분류되지는 않지만 네트워크에서 엔드포인트의 성능을 떨어뜨리고 조직에 심각한 보안, 기밀성 및 법적 위험을 초래할 수 있는 응용 프로그램이나 파일을 말합니다. 스파이웨어/그레이웨어는 여러 팝업 창을 표시하거나 사용자 키 입력을 기록하며 엔드포인트를 취약한 공격에 노출시키는 등 원치 않는 여러 가지 위협적인 동작을 수행합니다.

OfficeScan에서 스파이웨어로 인식하지 않는 응용 프로그램이나 파일이 그레이웨어 유형으로 생각될 경우 Trend Micro에서 분석할 수 있도록 다음으로 보내주십시오.

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

유형	설명
스파이웨어	계정 사용자 이름 및 암호와 같은 데이터를 수집한 후 이 데이터를 제3자에게 전송합니다.
애드웨어	광고를 표시하고 사용자 웹 서핑 기본 설정과 같은 데이터를 수집하여 해당 사용자를 웹 브라우저를 통한 광고 대상으로 설정합니다.

유형	설명
전화 걸기 프로그램	엔드포인트 인터넷 설정을 변경하여 엔드포인트에서 모뎀을 통해 미리 구성된 전화 번호로 강제로 전화를 걸게 할 수 있습니다. 이러한 전화 번호는 흔히 회사에 많은 요금을 부과할 수 있는 국제 전화 번호 또는 PPC(Pay-Per-Call)입니다.
조크 프로그램	CD-ROM 트레이를 열고 닫거나 수많은 메시지 상자를 표시하는 등 비정상적인 엔드포인트 동작을 일으킵니다.
해킹 도구	해커가 컴퓨터에 침입할 수 있도록 도와줍니다.
원격 액세스 도구	해커가 원격으로 컴퓨터에 액세스하여 제어할 수 있도록 도와줍니다.
암호 해독 응용 프로그램	해커가 계정 사용자 이름 및 암호를 해독할 수 있도록 도와줍니다.
기타	유해 가능성이 있는 기타 프로그램 유형입니다.

스파이웨어/그레이웨어의 네트워크 침투 방식

스파이웨어/그레이웨어는 주로 사용자가 설치 패키지에 그레이웨어 응용 프로그램이 포함된 정품 소프트웨어를 다운로드할 때 기업 네트워크로 들어옵니다. 대부분의 소프트웨어 프로그램에는 최종 사용자 사용권 계약(EULA)이 포함되어 있으며, 사용자는 다운로드하기 전에 해당 계약 내용에 동의해야 합니다. 일반적으로 EULA에는 응용 프로그램에 대한 정보와 해당 프로그램이 개인 데이터 수집을 목적으로 한다는 내용이 명시되어 있습니다. 그러나 대체로 사용자는 이러한 정보를 간과하거나 해당 법률 용어를 이해하지 못합니다.

잠재적 위험 및 위협

네트워크에 스파이웨어 및 기타 유형의 그레이웨어가 있는 경우 다음과 같은 상황을 초래할 수 있습니다.

표 7-2. 잠재적 위험 및 위협

위험 또는 위협	설명
엔드포인트 성능 저하	스파이웨어/그레이웨어 응용 프로그램이 작업을 수행하는 데에는 대체로 상당한 CPU 및 시스템 메모리 리소스가 필요합니다.
웹 브라우저 관련 충돌 증가	애드웨어와 같은 유형의 그레이웨어는 대개 브라우저 프레임이나 창에 정보를 표시합니다. 이러한 응용 프로그램의 코드가 시스템 프로세스와 상호 작용하는 방식에 따라, 그레이웨어로 인하여 브라우저가 충돌하거나 정지될 수 있으며 엔드포인트를 다시 시작해야 할 수도 있습니다.
사용자 작업의 효율성 저하	빈번하게 표시되는 팝업 광고를 닫거나 조크 프로그램에 대응하다 보면 작업에 방해를 받을 수 있습니다.
네트워크 대역폭 저하	스파이웨어/그레이웨어 응용 프로그램은 수집한 데이터를 네트워크에서 또는 네트워크 외부에서 실행 중인 다른 응용 프로그램에 정기적으로 전송합니다.
개인 및 기업 정보 손실	스파이웨어/그레이웨어 응용 프로그램이 수집하는 데이터는 사용자가 방문하는 웹 사이트 목록과 같은 단순한 데이터가 아닙니다. 스파이웨어/그레이웨어는 온라인 은행 계좌 및 회사 네트워크에 액세스하는 데 사용되는 것과 같은 사용자 자격 증명을 수집할 수도 있습니다.
법적 책임 위험 증가	사용자 네트워크상의 엔드포인트 리소스가 외부로 유출될 경우, 해커는 에이전트 컴퓨터를 이용하여 공격을 실행하거나 네트워크 외부에 있는 컴퓨터에 스파이웨어/그레이웨어를 설치할 수 있습니다. 이러한 작업에 사용자의 네트워크 리소스가 사용될 경우 타인으로 인해 발생한 손상에 대해 사용자의 회사에 법적인 책임이 부과될 수 있습니다.

스파이웨어/그레이웨어 및 기타 위협으로부터 보호

스파이웨어/그레이웨어가 엔드포인트에 설치되지 않도록 하기 위해 수행할 수 있는 여러 단계가 있습니다. Trend Micro에서는 다음과 같이 할 것을 권장합니다.

- 스파이웨어/그레이웨어 파일 및 응용 프로그램을 검색하여 제거하도록 모든 유형의 검색(수동 검색, 실시간 검색, 예약 검색 및 지금 검색)을 구성합니다. 자세한 내용은 검색 유형 페이지 7-14를 참조하십시오.

- 에이전트 사용자에게 다음을 수행하도록 안내합니다.
  - 다운로드하여 컴퓨터에 설치하는 응용 프로그램에 포함된 설명서와 최종 사용자 사용권 계약(EULA)을 읽어 봅니다.
  - 에이전트 사용자가 소프트웨어 작성자와 보고 있는 웹 사이트를 모두 신뢰할 수 있다고 확신하는 경우가 아니면, 소프트웨어를 다운로드하여 설치할지 묻는 모든 메시지에 대해 **아니요**를 클릭합니다.
  - 원치 않는 상업용 전자 메일(스팸)을 삭제합니다(특히 스팸에서 단추나 하이퍼링크를 클릭할 것을 요청하는 경우).
- 엄격한 보안 수준이 유지되도록 웹 브라우저 설정을 구성합니다. Trend Micro에서는 웹 브라우저에서 ActiveX 컨트롤을 설치하기 전에 사용자에게 설치 여부를 묻도록 구성할 것을 권장합니다.
- Microsoft Outlook을 사용하는 경우에는 Outlook에서 스팸 메시지에 전송된 그림과 같은 HTML 항목을 자동으로 다운로드하지 않도록 보안 설정을 구성합니다.
- 피어 투 피어(P2P) 파일 공유 서비스 사용을 허용하지 마십시오. 스파이웨어 및 기타 그레이웨어 응용 프로그램은 MP3 음악 파일과 같이 사용자가 다운로드하려는 다른 파일 포맷으로 표시될 수 있습니다.
- 에이전트 컴퓨터에 설치된 소프트웨어를 정기적으로 검사하며 스파이웨어나 기타 그레이웨어일 수 있는 응용 프로그램을 찾아냅니다.
- Windows 운영 체제를 Microsoft의 최신 패치로 업데이트하여 최신 상태로 유지합니다. 자세한 내용은 Microsoft 웹 사이트를 참조하십시오.

검색 방법 유형

OfficeScan 에이전트는 보안 위험 검색 시 두 가지 검색 방법 중 하나를 사용할 수 있습니다. 검색 방법은 스마트 스캔과 표준 스캔입니다.

- **스마트 스캔**

  이 문서에서는 스마트 스캔을 사용하는 에이전트를 **스마트 스캔 에이전트**라고 합니다. 스마트 스캔 에이전트는 파일 검증 서비스에서 제공하는 로컬 검색 및 in-the-cloud 쿼리를 활용합니다.

- **표준 스캔**

  스마트 스캔을 사용하지 않는 에이전트를 **표준 스캔 에이전트**라고 합니다. 표준 스캔 에이전트는 모든 OfficeScan 구성 요소를 에이전트 엔드포인트에 저장하고 모든 파일을 로컬로 검색합니다.

기본 검색 방법

이 OfficeScan 버전에서는 새로 설치에 대한 기본 검색 방법으로 스마트 스캔을 사용합니다. 즉, OfficeScan 서버를 새로 설치하는 경우 웹 콘솔에서 검색 방법을 변경하지 않으면 서버에서 관리하는 모든 에이전트에 스마트 스캔이 사용됩니다.

자동 에이전트 업그레이드를 사용하는 경우 이전 버전에서 OfficeScan 서버를 업그레이드하면 해당 서버가 관리하는 모든 에이전트에서 업그레이드 이전에 구성된 검색 방법을 계속 사용합니다. 예를 들어 스마트 스캔과 표준 스캔을 둘 다 지원하는 OfficeScan 11.0에서 업그레이드하는 경우에는 업그레이드된 에이전트 중 스마트 스캔을 사용하던 에이전트는 모두 스마트 스캔을 계속 사용하고 표준 스캔을 사용하던 에이전트는 모두 표준 스캔을 계속 사용합니다.

검색 방법 비교

다음 표에서는 두 가지 검색 방법을 비교 설명합니다.

표 7-3. 표준 스캔과 스마트 스캔 비교

비교 기준	표준 스캔	스마트 스캔
사용 가능 여부	이 OfficeScan 버전과 모든 이전 OfficeScan 버전에서 사용 가능	OfficeScan 10부터 사용 가능

비교 기준	표준 스캔	스마트 스캔
검색 동작	표준 스캔 에이전트는 로컬 엔드포인트에서 검색을 수행합니다.	• 스마트 스캔 에이전트는 로컬 엔드포인트에서 검색을 수행합니다. • 에이전트가 검색 중에 파일에 대한 위험을 알 수 없는 경우 에이전트는 스마트 보호 소스로 검색 쿼리를 보내 위험을 확인합니다. • 에이전트는 검색 성능을 향상시키기 위해 검색 쿼리 결과를 "캐시"합니다.
사용 중인 구성 요소 및 업데이트된 구성 요소	업데이트 소스에서 사용할 수 있는 모든 구성 요소(스마트 스캔 에이전트 패턴 제외)	업데이트 소스에서 사용할 수 있는 모든 구성 요소(바이러스 패턴 및 스파이웨어 활성 모니터링 패턴 제외)
일반적인 업데이트 소스	OfficeScan 서버	OfficeScan 서버

검색 방법 변경

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **검색 설정** > **검색 방법**을 클릭합니다.
4. **표준 스캔** 또는 **스마트 스캔**을 선택합니다.
5. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

스마트 스캔에서 표준 스캔으로 전환

에이전트를 표준 스캔으로 전환할 때는 다음을 고려합니다.

1. 전환할 에이전트 수

   비교적 적은 수의 에이전트를 동시에 전환하면 OfficeScan 서버 및 스마트 보호 서버 리소스를 효율적으로 사용할 수 있습니다. 이러한 서버는 에이전트가 검색 방법을 변경하는 동안 다른 중요한 작업을 수행할 수 있습니다.

2. 타이밍

   표준 스캔으로 다시 전환할 때 에이전트는 OfficeScan 서버에서 정식 버전의 바이러스 패턴 및 스파이웨어 활성 모니터링 패턴을 다운로드합니다. 이러한 패턴 파일은 표준 스캔 에이전트에서만 사용합니다.

   다운로드 프로세스를 짧은 시간 내에 완료하려면 컴퓨터 사용량이 적은 시간대에 전환하십시오. 또한, 에이전트가 서버에서 업데이트하도록 예약되지 않은 시간에 전환하십시오. 그리고 에이전트의 "지금 업데이트" 기능이 임시로 사용되지 않도록 설정한 다음, 에이전트가 스마트 스캔으로 전환되고 나면 다시 사용되도록 설정하십시오.

3. 에이전트 트리 설정

   검색 방법은 루트, 도메인 또는 개별 에이전트 수준에서 설정할 수 있는 개별 설정입니다. 표준 스캔으로 전환 시, 다음을 수행할 수 있습니다.

   - 새로운 에이전트 트리 도메인을 생성하고 검색 방법으로 표준 스캔을 할당합니다. 이 도메인으로 이동하는 에이전트는 표준 스캔을 사용합니다. 에이전트 이동 시, **선택한 에이전트에 새 도메인의 설정 적용** 설정을 사용하도록 설정합니다.
   - 도메인을 선택하고 표준 스캔을 사용하도록 구성합니다. 도메인에 속하는 스마트 스캔 에이전트는 표준 스캔으로 전환됩니다.

- 도메인에서 하나 이상의 스마트 스캔 에이전트를 선택한 후 표준 스캔으로 전환합니다.

참고

도메인의 검색 방법에 대한 변경 사항은 개별 에이전트에 대해 구성한 검색 방법보다 우선합니다.

표준 스캔에서 스마트 스캔으로 전환

표준 스캔에서 스마트 스캔으로 에이전트를 전환하는 경우 스마트 보호 서비스를 설정해야 합니다.

자세한 내용은 스마트 보호 서비스 설정 페이지 4-12를 참조하십시오.

다음 표에는 스마트 스캔으로 전환할 때의 기타 고려 사항이 나와 있습니다.

표 7-4. 스마트 스캔으로 전환 시 고려 사항

고려 사항	세부 정보
제품 라이선스	스마트 스캔을 사용하려면 다음 서비스에 대한 라이선스를 활성화하고 라이선스가 만료되지 않아야 합니다. • 바이러스 백신 • 웹 검증 및 Anti-spyware
OfficeScan 서버	에이전트가 OfficeScan 서버에 연결할 수 있는지 확인합니다. 온라인 에이전트만 스마트 스캔으로 전환하도록 알림을 받습니다. 오프라인 에이전트는 온라인 상태가 될 때 알림을 받습니다. 독립 에이전트도 온라인 상태가 될 때 알림을 받거나, 에이전트에 예약 업데이트 권한이 있는 경우에는 예약 업데이트가 실행될 때 알림을 받습니다. 또한 스마트 스캔 에이전트가 서버에서 스마트 스캔 에이전트 패턴을 다운로드해야 하기 때문에 OfficeScan 서버에 최신 구성 요소가 있는지 확인합니다. 구성 요소를 업데이트하려면 OfficeScan 서버 업데이트 페이지 6-14를 참조하십시오.

고려 사항	세부 정보
전환할 에이전트 수	비교적 적은 수의 에이전트를 동시에 전환하면 OfficeScan 서버 리소스를 효율적으로 사용할 수 있습니다. OfficeScan 서버는 에이전트가 검색 방법을 변경하는 동안 다른 중요한 작업을 수행할 수 있습니다.
타이밍	처음 스마트 스캔으로 전환 시, 에이전트는 OfficeScan 서버에서 정식 버전의 스마트 스캔 에이전트 패턴을 다운로드해야 합니다. 스마트 스캔 패턴은 스마트 스캔 에이전트에서만 사용됩니다. 다운로드 프로세스를 짧은 시간 내에 완료하려면 컴퓨터 사용량이 적은 시간대에 전환하십시오. 또한, 에이전트가 서버에서 업데이트하도록 예약되지 않은 시간에 전환하십시오. 그리고 에이전트의 "지금 업데이트" 기능이 임시로 사용되지 않도록 설정한 다음, 에이전트가 스마트 스캔으로 전환되고 나면 다시 사용되도록 설정하십시오.
에이전트 트리 설정	검색 방법은 루트, 도메인 또는 개별 에이전트 수준에서 설정할 수 있는 개별 설정입니다. 스마트 스캔으로 전환 시, 다음을 수행할 수 있습니다. • 새로운 에이전트 트리 도메인을 생성하고 검색 방법으로 스마트 스캔을 할당합니다. 이 도메인으로 이동하는 에이전트는 스마트 스캔을 사용합니다. 에이전트 이동 시, **선택한 에이전트에 새 도메인의 설정 적용** 설정을 사용하도록 설정합니다. • 도메인을 선택하고 스마트 스캔을 사용하도록 구성합니다. 도메인에 속하는 표준 스캔 에이전트는 스마트 스캔으로 전환됩니다. • 도메인에서 하나 이상의 표준 스캔 에이전트를 선택한 후 스마트 스캔으로 전환합니다. **참고** 도메인의 검색 방법에 대한 변경 사항은 개별 에이전트에 대해 구성한 검색 방법보다 우선합니다.

고려 사항	세부 정보
IPv6 지원	스마트 스캔 에이전트는 스마트 보호 소스에 검색 쿼리를 보냅니다. 그러나 순수 IPv6 스마트 스캔 에이전트는 다음과 같은 순수 IPv4 소스에 직접 쿼리를 보낼 수 없습니다. • 스마트 보호 서버 2.0(통합 또는 독립) **참고** 스마트 보호 서버에 대한 IPv6 지원은 버전 2.5부터 제공됩니다. • Trend Micro 스마트 보호 네트워크 마찬가지로 순수 IPv4 스마트 스캔 에이전트는 순수 IPv6 스마트 보호 서버에 쿼리를 보낼 수 없습니다. 스마트 스캔 에이전트에서 소스에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

검색 유형

OfficeScan에서는 보안 위험으로부터 OfficeScan 에이전트 컴퓨터를 보호하기 위해 다음 유형의 검색을 제공합니다.

표 7-5. 검색 유형

검색 유형	설명
실시간 검색	파일이 수신, 다운로드, 복사, 수정 또는 열릴 때 엔드포인트에 있는 해당 파일을 자동으로 검색합니다. 자세한 내용은 실시간 검색 페이지 7-15를 참조하십시오.
수동 검색	사용자가 요청한 파일 또는 파일 집합을 검색하는 사용자 시작 검색입니다. 자세한 내용은 수동 검색 페이지 7-18를 참조하십시오.

검색 유형	설명
예약 검색	관리자 또는 최종 사용자가 구성한 일정을 기반으로 엔드포인트에 있는 파일을 자동으로 검색합니다. 자세한 내용은 예약 검색 페이지 7-20를 참조하십시오.
지금 검색	하나 이상의 대상 컴퓨터에서 파일을 검색하는 관리자 시작 검색입니다. 자세한 내용은 지금 검색 페이지 7-22를 참조하십시오.

실시간 검색

실시간 검색은 지속적이며 진행하는 검색입니다. 파일이 수신, 다운로드, 복사, 수정 또는 열릴 때마다 실시간 검색은 파일에 보안 위험이 있는지 검색합니다. OfficeScan이 보안 위험을 발견하지 못한 경우, 파일은 해당 위치에 유지되고 사용자는 파일에 액세스하도록 진행할 수 있습니다. OfficeScan에서 보안 위험 또는 가능성이 있는 바이러스/악성 프로그램을 발견하면 감염된 파일의 이름과 특정 보안 위험을 보여 주는 알림 메시지를 표시합니다.

실시간 검색 기능은 OfficeScan 에이전트가 시작될 때마다 다시 로드되는 영구 검색 캐시를 유지 관리합니다. OfficeScan 에이전트는 OfficeScan 에이전트가 종료된 이후 발생한 파일 또는 폴더의 변경 사항을 추적하고 캐시에서 이러한 파일을 제거합니다.

참고

알림 메시지를 수정하려면 웹 콘솔을 열고 **관리** > **알림** > **에이전트**으로 이동합니다.

실시간 검색 설정을 구성하고 하나 이상의 에이전트 및 도메인에 적용하거나 서버가 관리하는 모든 에이전트에 적용합니다.

실시간 검색 설정 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **검색 설정** > **실시간 검색 설정**을 클릭합니다.
4. 다음 옵션을 선택합니다.
   - **바이러스/악성 프로그램 검색 사용**
   - **스파이웨어/그레이웨어 검색 사용**

   참고

   바이러스/악성 프로그램 검색을 비활성화하면 스파이웨어/그레이웨어 검색도 비활성화됩니다. 바이러스 발생 시, 바이러스가 에이전트 컴퓨터의 파일 및 폴더를 수정 또는 삭제하지 못하도록 방지하기 위해 실시간 검색을 사용하지 않도록 설정할 수 없습니다(처음에 사용하지 않도록 설정한 경우 자동으로 사용하도록 설정됨).
5. **대상** 탭에서 다음을 구성합니다.
   - 파일에 대한 사용자 작업 페이지 7-26
   - 검색할 파일 페이지 7-27
   - 검색 설정 페이지 7-27
6. **조치** 탭을 클릭하고 다음을 구성합니다.

표 7-6. 검색 조치

조치	참조
바이러스/악성 프로그램 조치	기본 조치(하나 선택: • ActiveAction 사용 페이지 7-37 • 모든 바이러스/악성 프로그램 유형에 동일한 처리 방법 사용 페이지 7-38 • 각 바이러스/악성 프로그램 유형에 특정 처리 방법 사용 페이지 7-39 **참고** 다른 조치에 대한 자세한 내용은 바이러스/악성 프로그램 검색 조치 페이지 7-35를 참조하십시오. 추가 바이러스/악성 프로그램 조치: • 격리 보관 디렉터리 페이지 7-39 • 치료 이전에 파일 백업 페이지 7-41 • DCS(Damage Cleanup Services) 페이지 7-41 • 바이러스/악성 프로그램이 탐지되면 알림 메시지 표시 페이지 7-42 • 가능성이 있는 바이러스/악성 프로그램이 탐지되면 알림 메시지 표시 페이지 7-42
스파이웨어/그레이웨어 조치	기본 조치: • 스파이웨어/그레이웨어 검색 조치 페이지 7-47 추가 스파이웨어/그레이웨어 조치: • 스파이웨어/그레이웨어가 탐지되면 알림 메시지 표시 페이지 7-48

7. **검색 제외** 탭에서 검색에서 제외할 디렉터리, 파일 및 확장자를 구성합니다.

   자세한 내용은 검색 제외 페이지 7-31를 참조하십시오.

8. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

수동 검색

수동 검색은 주문형 검색이고 사용자가 OfficeScan 에이전트 콘솔에서 검색을 실행한 이후 즉시 시작됩니다. 검색을 완료하는 데 걸리는 시간은 검색할 파일의 수와 OfficeScan 에이전트 엔드포인트의 하드웨어 리소스에 따라 달라집니다.

수동 검색 설정을 구성하고 하나 이상의 에이전트 및 도메인에 적용하거나 서버가 관리하는 모든 에이전트에 적용합니다.

수동 검색 설정 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **검색 설정** > **수동 검색 설정**을 클릭합니다.
4. **대상** 탭에서 다음을 구성합니다.
   - 검색할 파일 페이지 7-27
   - 검색 설정 페이지 7-27

- CPU 사용량 페이지 7-29

5. **조치** 탭을 클릭하고 다음을 구성합니다.

표 7-7. 검색 조치

조치	참조
바이러스/악성 프로그램 조치	기본 조치(하나 선택: • ActiveAction 사용 페이지 7-37 • 모든 바이러스/악성 프로그램 유형에 동일한 처리 방법 사용 페이지 7-38 • 각 바이러스/악성 프로그램 유형에 특정 처리 방법 사용 페이지 7-39 **참고** 다른 조치에 대한 자세한 내용은 바이러스/악성 프로그램 검색 조치 페이지 7-35를 참조하십시오. 추가 바이러스/악성 프로그램 조치: • 격리 보관 디렉터리 페이지 7-39 • 치료 이전에 파일 백업 페이지 7-41 • DCS(Damage Cleanup Services) 페이지 7-41
스파이웨어/그레이웨어 조치	기본 조치: • 스파이웨어/그레이웨어 검색 조치 페이지 7-47

6. **검색 제외** 탭에서 검색에서 제외할 디렉터리, 파일 및 확장자를 구성합니다.

   자세한 내용은 검색 제외 페이지 7-31를 참조하십시오.

7. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

예약 검색

예약 검색은 지정된 날짜 및 시간에 자동으로 실행됩니다. 예약 검색을 사용하면 에이전트에 대한 정기 검색을 자동화하여 검색 관리의 효율성을 개선할 수 있습니다.

예약 검색 설정을 구성하고 하나 이상의 에이전트 및 도메인에 적용하거나 서버가 관리하는 모든 에이전트에 적용합니다.

예약 검색 설정 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **검색 설정** > **예약 검색 설정**을 클릭합니다.
4. 다음 옵션을 선택합니다.
   - **바이러스/악성 프로그램 검색 사용**
   - **스파이웨어/그레이웨어 검색 사용**

   참고

   바이러스/악성 프로그램 검색을 비활성화하면 스파이웨어/그레이웨어 검색도 비활성화됩니다.
5. **대상** 탭에서 다음을 구성합니다.
   - 예약 페이지 7-30

- 검색할 파일 페이지 7-27
- 검색 설정 페이지 7-27
- CPU 사용량 페이지 7-29

6. **조치** 탭을 클릭하고 다음을 구성합니다.

표 7-8. 검색 조치

조치	참조
바이러스/악성 프로그램 조치	기본 조치(하나 선택: • ActiveAction 사용 페이지 7-37 • 모든 바이러스/악성 프로그램 유형에 동일한 처리 방법 사용 페이지 7-38 • 각 바이러스/악성 프로그램 유형에 특정 처리 방법 사용 페이지 7-39 **참고** 다른 조치에 대한 자세한 내용은 바이러스/악성 프로그램 검색 조치 페이지 7-35를 참조하십시오. 추가 바이러스/악성 프로그램 조치: • 격리 보관 디렉터리 페이지 7-39 • 치료 이전에 파일 백업 페이지 7-41 • DCS(Damage Cleanup Services) 페이지 7-41 • 바이러스/악성 프로그램이 탐지되면 알림 메시지 표시 페이지 7-42 • 가능성이 있는 바이러스/악성 프로그램이 탐지되면 알림 메시지 표시 페이지 7-42

조치	참조
스파이웨어/그레이웨어 조치	기본 조치: • 스파이웨어/그레이웨어 검색 조치 페이지 7-47 추가 스파이웨어/그레이웨어 조치: • 스파이웨어/그레이웨어가 탐지되면 알림 메시지 표시 페이지 7-48

7. **검색 제외** 탭에서 검색에서 제외할 디렉터리, 파일 및 확장자를 구성합니다.

   자세한 내용은 검색 제외 페이지 7-31를 참조하십시오.

8. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

지금 검색

지금 검색은 웹 콘솔을 사용하여 OfficeScan 관리자에 의해 원격으로 시작되고, 하나 이상의 에이전트 컴퓨터를 대상으로 실행될 수 있습니다.

지금 검색 설정을 구성하고 하나 이상의 에이전트 및 도메인에 적용하거나 서버가 관리하는 모든 에이전트에 적용합니다.

지금 검색 설정 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **검색 설정** > **지금 검색 설정**을 클릭합니다.
4. 다음 옵션을 선택합니다.
   - **바이러스/악성 프로그램 검색 사용**
   - **스파이웨어/그레이웨어 검색 사용**

   참고

   바이러스/악성 프로그램 검색을 비활성화하면 스파이웨어/그레이웨어 검색도 비활성화됩니다.
5. **대상** 탭에서 다음을 구성합니다.
   - 검색할 파일 페이지 7-27
   - 검색 설정 페이지 7-27
   - CPU 사용량 페이지 7-29
6. **조치** 탭을 클릭하고 다음을 구성합니다.

표 7-9. 검색 조치

조치	참조
바이러스/악성 프로그램 조치	기본 조치(하나 선택: • ActiveAction 사용 페이지 7-37 • 모든 바이러스/악성 프로그램 유형에 동일한 처리 방법 사용 페이지 7-38 • 각 바이러스/악성 프로그램 유형에 특정 처리 방법 사용 페이지 7-39 **참고** 다른 조치에 대한 자세한 내용은 바이러스/악성 프로그램 검색 조치 페이지 7-35를 참조하십시오. 추가 바이러스/악성 프로그램 조치: • 격리 보관 디렉터리 페이지 7-39 • 치료 이전에 파일 백업 페이지 7-41 • DCS(Damage Cleanup Services) 페이지 7-41
스파이웨어/그레이웨어 조치	기본 조치: • 스파이웨어/그레이웨어 검색 조치 페이지 7-47

7. **검색 제외** 탭에서 검색에서 제외할 디렉터리, 파일 및 확장자를 구성합니다.

   자세한 내용은 검색 제외 페이지 7-31를 참조하십시오.

8. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

지금 검색 시작

감염된 것으로 의심되는 컴퓨터에서 지금 검색을 시작합니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **작업** > **지금 검색**을 클릭합니다.
4. 검색을 시작하기 전에 미리 구성된 **지금 검색** 설정을 변경하려면 **설정**을 클릭합니다.

   지금 검색 설정 화면이 열립니다. 자세한 내용은 지금 검색 페이지 7-22를 참조하십시오.
5. 검색을 수행할 에이전트를 에이전트 트리에서 선택하고 **지금 검색 시작**을 클릭합니다.

   서버가 에이전트에 알림을 보냅니다.
6. 알림 상태를 확인하고 알림을 받지 않은 에이전트가 있는지 확인합니다.
7. **알림을 받지 못한 엔드포인트 선택**, **지금 검색 시작**을 차례로 클릭하여 알림을 받지 못한 에이전트에 즉시 알림을 재전송합니다.

   예: 전체 에이전트 수: 50

표 7-10. 알림을 받지 못한 에이전트 시나리오

에이전트 트리 선택	알림을 받은 에이전트 ("지금 검색 시작" 클릭 후)	알림을 받지 않은 에이전트
없음(50개 에이전트가 모두 자동으로 선택됨)	50개 중 35개 에이전트	15 에이전트
수동 선택(50개 중 45개 에이전트 선택됨)	45개 중 40개 에이전트	5개 에이전트 + 수동 선택에 포함되지 않은 다른 5개 에이전트

8. OfficeScan에서 현재 알림을 보내고 있는 에이전트에 대한 알림을 중지하도록 하려면 **알림 중지**를 클릭합니다. 이미 알림을 받아 검색을 진행 중인 에이전트는 이 명령을 무시합니다.
9. 이미 검색을 진행 중인 에이전트의 경우에는 **지금 검색 중지**를 클릭하여 검색을 중지하도록 알리십시오.

모든 검색 유형에 대한 일반적인 설정

각 검색 유형에 대해 세 가지 설정 집합 즉, 검색 기준, 검색 제외 및 검색 조치를 구성합니다. 이러한 설정을 하나 이상의 에이전트 및 도메인이나 서버에서 관리하는 모든 에이전트에 배포합니다.

검색 기준

파일 형식 및 확장자와 같은 파일 특성을 사용하여 특정 검색 유형에서 검색해야 하는 파일을 지정합니다. 또한, 검색을 트리거할 조건을 지정합니다. 예를 들어 파일이 엔드포인트에 다운로드된 후 실시간 검색에서 각 파일을 검색하도록 구성합니다.

파일에 대한 사용자 작업

실시간 검색을 트리거하는 파일에 대한 작업을 선택합니다. 다음 옵션에서 선택합니다.

- **생성/수정된 파일 검색**: 엔드포인트에 배포된 새 파일(예: 파일 다운로드 이후) 또는 수정 중인 파일을 검색합니다.
- **회수된 파일 검색**: 파일이 열릴 때 검색합니다.
- **생성/수정 및 회수된 파일 검색**

예를 들어 세 번째 옵션을 선택하면 엔드포인트에 다운로드된 새 파일이 검색되고, 보안 위험이 발견되지 않는 경우, 현재 위치에 유지됩니다. 사용자가 동일한 파일을 여는 경우 사용자가 해당 파일을 수정했으면 이 수정 사항이 저장되기 전에 해당 파일이 검색됩니다.

검색할 파일

다음 옵션에서 선택합니다.

- **검색 가능한 모든 파일**: 모든 파일을 검색합니다.
- **IntelliScan에 의해 검색된 파일 형식**: 유해하지 않은 확장자 이름으로 숨겨져 있는 파일을 포함하여 유해 가능성이 있는 악성 코드로 알려진 파일만 검색합니다.

  자세한 내용은 IntelliScan 페이지 E-6를 참조하십시오.
- **다음 확장자를 가진 파일**: 확장자가 파일 확장자 목록에 포함되어 있는 파일만 검색합니다. 새 확장자를 추가하거나 기존 확장자를 제거합니다.

검색 설정

다음 옵션 중 하나 이상을 선택합니다.

- **시스템 종료 시 플로피 디스크 검색**: 실시간 검색 기능은 엔드포인트를 종료하기 전에 플로피 디스크에 부트 바이러스가 있는지 검색합니다. 이 옵션은 사용자가 디스크에서 엔드포인트를 다시 부팅할 때 바이러스/악성 프로그램이 실행되지 못하도록 방지합니다.
- **숨김 폴더 검색**: 수동 검색 도중 OfficeScan이 엔드포인트에서 숨김 폴더를 발견한 후 검색할 수 있습니다.
- **네트워크 드라이브 검색**: 수동 검색 또는 실시간 검색 도중 OfficeScan 에이전트 엔드포인트에 매핑되는 네트워크 드라이브 또는 폴더를 검색합니다

- **Plug-in 후 USB 저장 장치의 부트 섹터 검색**: 사용자가 USB 저장 장치를 연결할 때마다 장치의 부트 섹터만 자동으로 검색합니다(실시간 검색).
- **플러그인 후 이동식 저장 장치의 모든 파일 검색**: 사용자가 USB 저장 장치를 연결할 때마다 장치의 모든 파일을 자동으로 검색합니다(실시간 검색).
- **메모리에서 탐지된 악성 프로그램 변종 격리 보관**: 동작 모니터링 기능이 시스템 메모리에서 의심스러운 프로세스를 검색하면 실시간 검색이 이 프로세스를 매핑하고 악성 프로그램 위협을 검색합니다. 악성 프로그램 위협이 있는 경우 실시간 검색 기능은 프로세스 및/또는 파일을 격리 보관합니다.

참고

이 기능을 사용하려면 관리자가 무단 변경 방지 서비스 및 고급 보호 서비스를 사용하도록 설정해야 합니다.

- **압축 파일 검색**: 이 설정을 사용하는 경우 OfficeScan은 지정한 수의 압축 레이어까지 검색하고 이를 초과하는 레이어는 검색을 건너뜁니다. 또한 OfficeScan은 압축 파일 내에서 감염된 파일을 치료하거나 삭제합니다. 예를 들어, 최대값이 2개 레이어이고 검색할 압축 파일에 레이어가 6개 있는 경우 OfficeScan은 2개 레이어를 검색하고 나머지 4개는 건너뜁니다. 압축 파일에 보안 위협이 있는 경우 OfficeScan은 파일을 치료하거나 삭제합니다.

참고

OfficeScan은 Office Open XML 포맷의 Microsoft Office 2007 파일을 압축 파일로 간주합니다. Office 2007 응용 프로그램의 파일 포맷인 Office Open XML은 ZIP 압축 기술을 사용합니다. 이러한 응용 프로그램을 사용하여 만든 파일에서 바이러스/악성 프로그램을 검색하려면 압축 파일 검색을 사용해야 합니다.

- **OLE 개체 검색**: 파일에 여러 OLE(개체 연결 및 삽입) 레이어가 포함된 경우 OfficeScan은 지정한 개수의 레이어까지 검색하고 나머지 레이어는 건너뜁니다.

  서버에서 관리하는 모든 에이전트는 수동 검색, 실시간 검색, 예약 검색 및 지금 검색 중에 이 설정을 확인합니다. 각 레이어는 바이러스/악성 프로그램 및 스파이웨어/그레이웨어가 있는지 검색됩니다.

예:

지정한 레이어 수는 2입니다. 파일 내에 포함된 것이 Microsoft Word 문서(첫 번째 레이어)이고, Word 문서 내에 Microsoft Excel 스프레드시트(두 번째 레이어)가 있으며, 스프레드시트 내에 .exe 파일(세 번째 레이어)이 있는 경우, OfficeScan은 Word 문서 및 Excel 스프레드시트를 검색하고 .exe 파일은 건너뜁니다.

- **OLE 파일에서 공격 코드 탐지**: OLE 위협 탐지는 Microsoft Office 파일에서 공격 코드를 확인하여 악성 프로그램을 스스로 식별합니다.

  참고

  지정한 개수의 레이어가 **OLE 개체 검색** 및 **공격 코드 감지** 옵션 둘 다에 적용될 수 있습니다.

- **IntelliTrap 사용**: 압축된 실행 파일에서 바이러스/악성 프로그램을 발견하고 제거합니다. 이 옵션은 실시간 검색에서만 사용할 수 있습니다.

  자세한 내용은 IntelliTrap 페이지 E-6를 참조하십시오.

- **웹 및 전자 메일 채널을 통해 다운로드한 파일에 대해 CVE 위협 검색 사용**: CVE(공통 취약성 및 노출) 시스템을 기반으로 상용 제품의 알려진 취약점에 대해 공격을 시도하는 프로세스를 차단합니다. 이 옵션은 실시간 검색에서만 사용할 수 있습니다.

- **부트 영역 검색**: 수동 검색, 예약 검색 및 지금 검색 동안 하드 디스크 부트 섹터에 바이러스/악성 프로그램이 있는지 검색합니다.

CPU 사용량

한 파일을 검색한 후 다음 파일을 검색하기 전에 OfficeScan을 일시 중지할 수 있습니다. 이 설정은 수동 검색, 예약 검색 및 지금 검색 도중에 사용됩니다.

다음 옵션에서 선택합니다.

- **높음**: 검색 간 일시 중지 없음
- **보통**: CPU 사용량이 50%보다 높으면 파일 검색을 일시 중지하고 50% 이하이면 일시 중지하지 않습니다.

- **낮음**: CPU 사용량이 20%보다 높으면 파일 검색을 일시 중지하고 20% 이하이면 일시 중지하지 않습니다.

보통 또는 낮음을 선택한 경우, 검색이 시작되고 CPU 사용량이 임계값(50% 또는 20%) 이내에 있으면, OfficeScan이 검색 간에 일시 중지하지 않으며 검색 시간이 더 빨라집니다. OfficeScan이 프로세스에서 더 많은 CPU 리소스를 사용하지만 CPU 사용량이 최적이기 때문에 엔드포인트 성능은 크게 영향을 받지 않습니다. CPU 사용량이 임계값을 초과하기 시작하면 OfficeScan이 일시 중지하여 CPU 사용량을 줄이고, 소비량이 다시 임계값 이내가 되면 일시 중지를 해제합니다.

높음을 선택하는 경우, OfficeScan은 실제 CPU 사용량을 확인하지 않고 일시 중지 없이 파일을 검색합니다.

예약

예약 검색을 실행할 빈도(매일, 매주 또는 매월) 및 시간을 구성합니다.

매월 실행되는 예약 검색의 경우 특정 날짜 또는 요일 및 해당 주를 선택할 수 있습니다.

- **특정 날짜**: 1일과 31일 사이에서 선택합니다. 29일, 30일 또는 31일을 선택한 경우 특정 월에 이 날짜가 없으면 OfficeScan에서는 그 달의 말일에 예약 검색을 실행합니다. 따라서
  - 29를 선택한 경우 다른 모든 달에는 29일에 예약 검색이 실행되고 2월에는 28일(윤년 제외)에 예약 검색이 실행됩니다.
  - 30을 선택한 경우 다른 모든 달에는 30일에 예약 검색이 실행되고 2월에는 28일 또는 29일에 예약 검색이 실행됩니다.
  - 31을 선택한 경우 다른 모든 달에는 31일에 예약 검색이 실행되고 2월에는 28일 또는 29일, 4월, 6월, 9월, 11월에는 30일에 예약 검색이 실행됩니다.
- **요일 및 해당 주**: 요일은 한 달에 네 번 또는 다섯 번 돌아옵니다. 예를 들어 월요일은 보통 한 달에 네 번 있습니다. 요일과 해당 요일이 달의 몇 번째 주에 해당하는지 지정합니다. 예를 들어 매월 둘째 주 월요일에 예약 검색을 실행할 수 있습니다. 다섯째 주를 선택하고 특정 월에 다섯째 주가 없는 경우에는 넷째 주에 검색이 실행됩니다.

검색 제외

검색 성능을 높이고 잘못된 경보를 유발하는 검색 파일을 건너뛰려면 검색 제외를 구성합니다. 특정 검색 유형이 실행될 때, OfficeScan이 검색 제외 목록을 확인하여 바이러스/악성 프로그램 및 스파이웨어/그레이웨어 검색 모두에서 제외될 엔드포인트의 파일을 결정합니다.

검색 제외를 사용하면 OfficeScan이 다음 조건인 경우 파일을 검색하지 않습니다.

- 파일이 특정 디렉터리(또는 그 하위 디렉터리 중 하나)에 있습니다.
- 파일 이름이 검색 제외 목록의 이름과 일치합니다.
- 파일 확장자가 검색 제외 목록의 확장자와 일치합니다.

팁

Trend Micro가 실시간 검색에서 제외하도록 권장하는 제품 목록을 보려면 다음 사이트를 방문하십시오.

http://esupport.trendmicro.com/solution/en-US/1059770.aspx

와일드카드 예외

파일 및 디렉터리에 대한 검색 제외 목록에는 와일드카드 문자를 사용할 수 있습니다. 하나의 문자를 대체하려면 "?" 문자를 사용하고 여러 문자를 대체하려면 "*" 문자를 사용합니다.

와일드카드 문자를 사용할 때는 주의해야 합니다. 잘못된 문자를 사용하면 잘못된 파일이나 디렉터리가 제외될 수 있습니다. 예를 들어 C:₩*를 스캔 제외 목록(파일)에 추가하면 전체 C:₩ 드라이브가 제외됩니다.

표 7-11. 와일드카드 문자를 사용한 검색 제외

값	제외되는 항목	제외되지 않는 항목
`c:\director*\fil\*.txt`	c:₩directory₩fil₩doc.txt c:₩directories₩fil₩files₩document.txt	c:₩directory₩file₩ c:₩directories₩files₩ c:₩directory₩file₩doc.txt c:₩directories₩files₩document.txt
`c:\director?\file\*.txt`	c:₩directory₩file₩doc.txt	c:₩directories₩file₩document.txt
`c:\director?\file\?.txt`	c:₩directory₩file₩1.txt	c:₩directory₩file₩doc.txt c:₩directories₩file₩document.txt
`c:\*.txt`	C:₩ 디렉터리의 모든 .txt 파일	C:₩ 디렉터리의 기타 파일 형식 모두
`[]`	지원되지 않음	지원되지 않음

검색 제외 목록(디렉터리)

OfficeScan은 컴퓨터의 특정 디렉터리에 있는 모든 파일을 검색하지 않습니다. 최대 256개의 디렉터리를 지정할 수 있습니다.

참고

디렉터리를 검색에서 제외하면 OfficeScan에서 해당 디렉터리의 모든 하위 디렉터리도 검색에서 자동으로 제외합니다.

Trend Micro 제품이 설치된 디렉터리를 제외합니다.를 선택할 수도 있습니다. 이 옵션을 선택하는 경우, OfficeScan이 다음 Trend Micro 제품의 디렉터리를 검색에서 자동으로 제외합니다.

- <서버 설치 폴더>

참고

수동 검색 중에 OfficeScan은 계속 서버 설치 폴더를 검색합니다.

- IM Security
- InterScan eManager 3.5x
- InterScan Web Security Suite
- InterScan Web Protect
- InterScan FTP VirusWall
- InterScan Web VirusWall
- InterScan NSAPI Plug-in
- InterScan E-mail VirusWall
- ScanMail eManager™ 3.11, 5.1, 5.11, 5.12
- ScanMail for Lotus Notes™ eManager NT
- ScanMail™ for Microsoft Exchange

목록에 포함된 Trend Micro 제품이 없는 경우, 검색 제외 목록에 제품 디렉터리를 추가하십시오.

또한 **보안 설정** 탭, **에이전트** > **글로벌 에이전트 설정**의 **검색 설정** 섹션으로 이동하여 Microsoft Exchange 2000/2003 디렉터리를 제외하도록 OfficeScan을 구성합니다. Microsoft Exchange 2007 이상을 사용하는 경우 검색 제외 목록에 디렉터리를 수동으로 추가합니다. 검색 제외 세부 정보는 다음 사이트를 참조하십시오.

http://technet.microsoft.com/en-us/library/bb332342.aspx

파일 목록을 구성할 때 다음 옵션 중에서 선택합니다.

- **현재 목록 유지**(기본값): OfficeScan에서는 에이전트의 기존 검색 제외 목록을 실수로 덮어쓰지 않도록 방지하기 위해 이 옵션을 제공합니다. 검색 검색 제외 목록의 변경 사항을 저장하고 배포하려면 다른 옵션을 선택하십시오.
- **덮어쓰기**: 이 옵션은 에이전트에서 전체 제외 목록을 제거하고 현재 목록으로 대체합니다. **모든 에이전트에 적용**을 클릭하면 OfficeScan에 확인 경고 메시지가 표시됩니다.

- **다음 위치에 경로 추가**: 이 옵션은 에이전트의 기존 검색 제외 목록에 현재 목록의 항목을 추가합니다. 특정 항목이 에이전트의 기존 검색 제외 목록에 이미 있는 경우 에이전트에서는 해당 항목을 무시합니다.
- **다음 위치에서 경로 제거**: 이 옵션은 에이전트의 기존 검색 제외 목록에서 현재 목록의 항목(있는 경우)을 제거합니다.

검색 제외 목록(파일)

OfficeScan에서는 파일 이름이 이 검색 제외 목록에 포함된 이름과 일치하는 경우 해당 파일을 검색하지 않습니다. 엔드포인트의 특정 위치에 있는 파일을 제외하려는 경우 C:₩Temp₩sample.jpg와 같은 파일 경로를 포함합니다.

최대 256개의 파일을 지정할 수 있습니다.

파일 목록을 구성할 때 다음 옵션 중에서 선택합니다.

- **현재 목록 유지**(기본값): OfficeScan에서는 에이전트의 기존 검색 제외 목록을 실수로 덮어쓰지 않도록 방지하기 위해 이 옵션을 제공합니다. 검색 검색 제외 목록의 변경 사항을 저장하고 배포하려면 다른 옵션을 선택하십시오.
- **덮어쓰기**: 이 옵션은 에이전트에서 전체 제외 목록을 제거하고 현재 목록으로 대체합니다. **모든 에이전트에 적용**을 클릭하면 OfficeScan에 확인 경고 메시지가 표시됩니다.
- **다음 위치에 경로 추가**: 이 옵션은 에이전트의 기존 검색 제외 목록에 현재 목록의 항목을 추가합니다. 특정 항목이 에이전트의 기존 검색 제외 목록에 이미 있는 경우 에이전트에서는 해당 항목을 무시합니다.
- **다음 위치에서 경로 제거**: 이 옵션은 에이전트의 기존 검색 제외 목록에서 현재 목록의 항목(있는 경우)을 제거합니다.

검색 제외 목록(파일 확장자)

파일 확장자가 이 검색 제외 목록에 포함된 확장자와 일치하는 경우 OfficeScan이 해당 파일을 검색하지 않습니다. 최대 256개의 파일 확장자를 지정할 수 있습니다. 확장자 앞에 마침표(.)는 필요하지 않습니다.

수동 검색, 예약 검색 및 지금 검색의 경우, 와일드카드 문자로 물음표(?) 또는 별표(*)를 사용합니다. 예를 들어 확장자가 D로 시작하는 모든 파일(예: DOC, DOT 또는 DAT)을 검색하지 않으려면 `D*` 또는 `D?`를 입력합니다.

참고

실시간 검색은 확장자를 지정할 때 와일드카드 문자의 사용을 지원하지 않습니다.

모든 검색 유형에 검색 제외 설정 적용

OfficeScan에서 특정 검색 유형에 대해 검색 제외 설정을 구성한 후 다른 모든 검색 유형에 동일한 설정을 적용할 수 있습니다. 예:

1월 1일, OfficeScan 관리자 Chris는 에이전트 컴퓨터에 JPG 파일이 여러 개 있음을 발견하고 이 파일에는 보안 위협이 없음을 알았습니다. Chris는 수동 검색의 파일 검색 제외 목록에 JPG를 추가한 후 모든 검색 유형에 이 설정을 적용했습니다. 실시간 검색, 지금 검색 및 예약 검색이 .jpg 파일 검색을 건너뛰도록 설정되었습니다.

일주일 후, Chris가 실시간 검색의 검색 제외 목록에서 JPG를 제거했지만 검색 제외 설정을 모든 검색 유형에 적용하지는 않았습니다. 이제 JPG 파일은 실시간 검색 도중에만 검색됩니다.

검색 조치

특정 검색 유형이 보안 위험을 발견할 때 OfficeScan이 수행하는 조치를 지정합니다. OfficeScan은 바이러스/악성 프로그램 및 스파이웨어/그레이웨어에 대해 서로 다른 일련의 검색 조치를 적용합니다.

바이러스/악성 프로그램 검색 조치

OfficeScan이 수행하는 검색 조치는 바이러스/악성 프로그램 유형에 따라 다르고 바이러스/악성 프로그램을 탐지한 검색 유형에 따라 다릅니다. 예를 들어 OfficeScan이 수동 검색(검색 유형) 동안 트로이 목마 프로그램(바이러스/악성 프로그램 유형)을 발견하면 감염된 파일을 치료(조치)합니다.

다른 바이러스/악성 프로그램 유형에 대한 자세한 내용은 바이러스 및 악성 프로그램 페이지 7-2을 참조하십시오.

다음은 바이러스/악성 프로그램에 대해 OfficeScan이 수행할 수 있는 조치입니다.

표 7-12. 바이러스/악성 프로그램 검색 조치

조치	설명
삭제	OfficeScan이 감염된 파일을 삭제합니다.
격리 보관	OfficeScan은 감염된 파일의 이름을 변경하고 암호화한 후 <에이전트 설치 폴더>₩Suspect에 있는 에이전트 엔드포인트로 이 파일을 이동시킵니다. 그런 다음 OfficeScan 에이전트는 격리된 파일을 지정된 격리 보관 디렉터리로 보냅니다. 자세한 내용은 격리 보관 디렉터리 페이지 7-39를 참조하십시오. 기본 격리 보관 디렉터리는 OfficeScan 서버의 <서버 설치 폴더>₩PCCSRV₩Virus에 있습니다. 격리된 파일을 복원해야 하는 경우 중앙 격리 보관 복원을 사용하십시오. 자세한 내용은 격리된 파일 복원 페이지 7-43를 참조하십시오.
치료	OfficeScan은 파일에 대한 전체 액세스를 허용하기 전에 감염된 파일을 치료합니다. 치료할 수 없는 파일인 경우 OfficeScan은 두 번째 조치인 격리 보관, 삭제, 파일명 변경, 그대로 두기 중 하나를 수행합니다. 두 번째 조치를 구성하려면 **에이전트** > **에이전트 관리**로 이동합니다. **설정** > **검색 설정** > **{검색 유형}** > **조치** 탭을 클릭합니다. 가능성이 있는 바이러스/악성 프로그램을 제외하고 모든 유형의 악성 프로그램에 대해 이 조치를 수행할 수 있습니다.
파일명 변경	OfficeScan은 감염된 파일의 확장자를 "vir"로 변경합니다. 파일명이 변경된 파일을 처음에는 열 수 없지만 파일을 특정 응용 프로그램에 연결하는 경우 열 수 있습니다. 파일명이 변경된 감염된 파일을 열면 바이러스/악성 프로그램이 실행될 수 있습니다.

조치	설명
그대로 두기	OfficeScan은 수동 검색, 예약 검색 및 지금 검색 동안에만 유형에 관계없이 바이러스를 탐지한 경우 이 검색 조치를 사용할 수 있습니다. 감염된 파일을 열거나 실행하기 위한 시도가 탐지될 때 어떠한 조치도 수행하지 않으면 바이러스/악성 프로그램이 실행되도록 허용할 수 있기 때문에 실시간 검색 동안에는 OfficeScan이 이 검색 조치를 사용할 수 없습니다. 다른 모든 검색 조치는 실시간 검색 동안 사용할 수 있습니다.
액세스 거부	이 검색 조치는 실시간 검색 동안에만 수행할 수 있습니다. OfficeScan이 감염된 파일을 열거나 실행하려는 시도를 탐지하면 즉시 해당 동작을 차단합니다. 사용자는 탐지된 파일을 수동으로 삭제할 수 있습니다.

ActiveAction 사용

바이러스/악성 프로그램의 유형에 따라 서로 다른 검색 조치가 필요합니다. 검색 조치를 사용자 정의하려면 바이러스/악성 프로그램에 대해 알아야 하며 이 작업은 지루한 작업일 수 있습니다. OfficeScan에서는 ActiveAction을 사용하여 이러한 문제를 해결합니다.

ActiveAction은 바이러스/악성 프로그램에 대해 미리 구성된 검색 조치 모음입니다. 검색 조치를 잘 모르거나 특정 유형의 바이러스/악성 프로그램에 적절한 검색 조치를 확신할 수 없는 경우 Trend Micro에서는 ActiveAction을 사용할 것을 권장합니다.

ActiveAction을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- ActiveAction에서는 Trend Micro에서 권장하는 검색 조치를 사용합니다. 따라서 검색 조치를 구성할 필요가 없습니다.
- 바이러스 제작자는 바이러스/악성 프로그램이 컴퓨터를 공격하는 방식을 지속적으로 변경합니다. ActiveAction 설정은 최신 위협 및 최신 바이러스/악성 프로그램 공격 방법으로부터 보호하기 위해 업데이트됩니다.

참고

스파이웨어/그레이웨어 검색에는 ActiveAction을 사용할 수 없습니다.

다음 표에서는 ActiveAction에서 각 바이러스/악성 프로그램 유형을 처리하는 방법에 대해 설명합니다.

표 7-13. 바이러스 및 악성 프로그램에 대한 Trend Micro 권장 검색 조치

바이러스/악성 프로그램 유형	실시간 검색		수동 검색/예약 검색/지금 검색	
	첫 번째 조치	두 번째 조치	첫 번째 조치	두 번째 조치
CVE 위협	액세스 거부	해당 없음	해당 없음	해당 없음
조크	격리 보관	해당 없음	격리 보관	해당 없음
트로이 목마	격리 보관	해당 없음	격리 보관	해당 없음
바이러스	치료	격리 보관	치료	격리 보관
테스트 바이러스	액세스 거부	해당 없음	그대로 두기	해당 없음
패커	격리 보관	해당 없음	격리 보관	해당 없음
가능성이 있는 악성 프로그램	액세스 거부 또는 사용자가 구성한 조치	해당 없음	그대로 두기 또는 사용자가 구성한 조치	해당 없음
기타 악성 프로그램	치료	격리 보관	치료	격리 보관

가능성이 있는 악성 프로그램에 대한 기본 조치는 실시간 검색 중에는 "액세스 거부"이고, 수동 검색, 예약 검색 및 지금 검색 중에는 "그대로 두기"입니다. 이러한 조치가 선호가 조치가 아닌 경우 격리 보관, 삭제 또는 파일명 변경으로 변경할 수 있습니다.

모든 바이러스/악성 프로그램 유형에 동일한 처리 방법 사용

가능성이 있는 바이러스/악성 프로그램을 제외하고 모든 유형의 바이러스/악성 프로그램에 대해 동일한 조치를 수행하려는 경우, 이 옵션을 선택합니다. 첫 번째 조치로 "치료"를 선택한 경우, 치료가 성공하지 않으면 OfficeScan이 수행하는 두 번째 조치를 선택합니다. 첫 번째 조치가 "치료"가 아니면 두 번째 조치를 구성할 수 없습니다.

"치료"를 첫 번째 조치로 선택하면 OfficeScan에서 가능성이 있는 바이러스/악성 프로그램을 탐지한 경우 두 번째 조치를 수행합니다.

각 바이러스/악성 프로그램 유형에 특정 처리 방법 사용

각 바이러스/악성 프로그램 유형에 대한 검색 조치를 수동으로 선택합니다.

가능성이 있는 바이러스/악성 프로그램을 제외하고 모든 바이러스/악성 프로그램 유형에 대해 모든 검색 조치를 사용할 수 있습니다. 첫 번째 조치로 "치료"를 선택한 경우, 치료가 성공하지 않으면 OfficeScan이 수행하는 두 번째 조치를 선택합니다. 첫 번째 조치가 "치료"가 아니면 두 번째 조치를 구성할 수 없습니다.

가능성이 있는 바이러스/악성 프로그램의 경우 "치료"를 제외하고 모든 검색 조치를 사용할 수 있습니다.

격리 보관 디렉터리

감염된 파일에 대한 조치가 "격리 보관"인 경우 OfficeScan 에이전트는 파일을 암호화하고 <에이전트 설치 폴더>₩SUSPECT에 있는 임시 격리 보관 폴더로 이동한 다음 지정된 격리 보관 디렉터리로 해당 파일을 보냅니다.

참고

나중에 암호화된 격리된 파일에 액세스해야 하는 경우 이 파일을 복원할 수 있습니다.

자세한 내용은 암호화된 파일 복원 페이지 7-44를 참조하십시오.

OfficeScan 서버 컴퓨터에 있는 기본 격리 보관 디렉터리를 적용합니다. 이 디렉터리는 URL 포맷이며 서버의 호스트 이름 또는 IP 주소를 포함합니다.

- 서버에서 IPv4 및 IPv6 에이전트를 모두 관리하는 경우 모든 에이전트에서 격리된 파일을 서버에 보낼 수 있도록 호스트 이름을 사용합니다.
- 서버가 IPv4 주소만 사용하거나 해당 IPv4 주소로 식별되는 경우 순수 IPv4 및 이중 스택 에이전트만 격리된 파일을 서버에 보낼 수 있습니다.
- 서버가 IPv6 주소만 사용하거나 해당 IPv6 주소로 식별되는 경우 순수 IPv6 및 이중 스택 에이전트만 격리된 파일을 서버에 보낼 수 있습니다.

URL, UNC 경로 또는 절대 파일 경로 포맷으로 위치를 입력하여 대체 격리 보관 디렉터리를 지정할 수도 있습니다. 이 경우 에이전트에서 이 대체 디렉터리에 연결할 수 있어야 합니다. 예를 들어 이중 스택 및 순수 IPv6 에이전트에서 격리된 파일을 받는 경우 대체 디렉터리에 IPv6 주소가 있어야 합니다. Trend Micro에서는 디렉터리를 입력할 때 이중 스택 대체 디렉터리를 지정하고 해당 호스트 이름으로 디렉터리를 식별하고 UNC 경로를 사용할 것을 권장합니다.

URL, UNC 경로 또는 절대 파일 경로를 사용할 시기에 대한 지침은 다음 표를 참조하십시오.

표 7-14. 격리 보관 디렉터리

격리 보관 디렉터리	허용되는 포맷	예	참고
해당 OfficeScan 서버 컴퓨터의 디렉터리	URL	http:// <osceserver>	이것은 기본 디렉터리입니다. 격리 보관 폴더의 크기와 같이 이 디렉터리에 대해 설정을 구성합니다. 자세한 내용은 격리 보관 관리자 페이지 14-59를 참조하십시오.
	UNC 경로	₩₩<osceserver>₩ofcscan₩Virus	
다른 OfficeScan 서버 컴퓨터의 디렉터리(네트워크에 다른 OfficeScan 서버가 있는 경우)	URL	http:// <osceserver2>	에이전트가 이 디렉터리에 연결될 수 있는지 확인합니다. 잘못된 디렉터리를 지정한 경우 OfficeScan 에이전트에서는 올바른 격리 보관 디렉터리를 지정할 때까지 격리된 파일을 SUSPECT 폴더에 보관합니다. 서버의 바이러스/악성 프로그램 로그에서 검색 결과는 "격리 보관 파일을 지정된 격리 보관 폴더로 보낼 수 없습니다."입니다. UNC 경로를 사용하는 경우, 격리 보관 디렉터리 폴더가 "Everyone" 그룹에 공유되어 있고 이 그룹에 읽기 및 쓰기 권한을 할당했는지 확인합니다.
	UNC 경로	₩₩<osceserver2>₩ ofcscan₩Virus	
네트워크의 다른 엔드포인트	UNC 경로	₩₩<computer_name>₩temp	
OfficeScan 에이전트의 다른 디렉터리	절대 경로	C:₩temp	

치료 이전에 파일 백업

OfficeScan이 감염된 파일을 치료하도록 설정되어 있는 경우, 먼저 파일을 백업할 수 있습니다. 이를 통해 나중에 파일이 필요한 경우, 해당 파일을 복원할 수 있습니다. OfficeScan은 백업 파일이 열리지 않도록 하기 위해 해당 파일을 암호화한 다음 <에이전트 설치 폴더>₩Backup 폴더에 저장합니다.

암호화된 백업 파일을 복원하려면 암호화된 파일 복원 페이지 7-44을 참조하십시오.

DCS(Damage Cleanup Services)

DCS(Damage Cleanup Services)는 파일 기반 및 네트워크 바이러스와 컴퓨터에 남아 있는 바이러스 및 웜(트로이목마, 레지스트리 항목 및 바이러스 파일)을 제거합니다.

에이전트는 검색 유형에 따라 바이러스/악성 프로그램을 검색하기 이전 또는 이후에 DCS(Damage Cleanup Services)를 트리거합니다.

- 수동 검색, 예약 검색 또는 지금 검색 시 OfficeScan 에이전트는 먼저 DCS(Damage Cleanup Services)를 트리거한 다음 바이러스/악성 프로그램 검색을 진행합니다. 바이러스/악성 프로그램을 검색하는 동안 클린업이 필요한 경우 에이전트는 DCS(Damage Cleanup Services)를 다시 트리거할 수 있습니다.
- 실시간 검색 중에는 OfficeScan 에이전트에서 먼저 바이러스/악성 프로그램 검색을 수행한 다음 클린업이 필요한 경우 DCS(Damage Cleanup Services)를 트리거합니다.

DCS(Damage Cleanup Services)에서 실행할 클린업 유형을 선택할 수 있습니다.

- **표준 클린업**: OfficeScan 에이전트는 표준 클린업 중에 다음 작업을 수행합니다.
  - 활동 중인 트로이 목마 검색 및 제거
  - 트로이 목마가 만드는 프로세스 제거
  - 트로이 목마가 수정한 시스템 파일 복구
  - 트로이 목마가 남긴 파일 및 응용 프로그램 삭제

- **고급 클린업**: 표준 클린업 작업 외에 OfficeScan 에이전트는 FakeAV라고도 하는 악성 보안 소프트웨어와 특정 루트키트 변종의 활동을 중지합니다. 또한 OfficeScan 에이전트에서는 고급 클린업 규칙을 사용하여 FakeAV 및 루트키트 동작을 보이는 응용 프로그램을 사전에 탐지하여 중지합니다.

참고

고급 클린업에서는 예방 보호를 제공하지만 잘못된 판정(false-positive)도 많이 발생합니다.

가능한 바이러스/악성 프로그램이 발견될 경우 클린업 실행 옵션을 선택하지 않으면 DCS(Damage Cleanup Services)에서 가능성이 있는 바이러스/악성 프로그램에 대해 클린업을 실행하지 않습니다. 이 옵션은 가능성이 있는 바이러스/악성 프로그램에 대한 조치가 **그대로 두기** 또는 **액세스 거부**가 아닌 경우에만 선택할 수 있습니다. 예를 들어 조치가 격리 보관일 때 실시간 검색 중에 OfficeScan 에이전트에서 가능성이 있는 바이러스/악성 프로그램을 발견한 경우 OfficeScan 에이전트는 먼저 감염된 파일을 격리 보관한 후 필요에 따라 클린업을 실행합니다. 클린업 유형(표준 또는 고급)은 선택할 수 있습니다.

바이러스/악성 프로그램이 탐지되면 알림 메시지 표시

실시간 검색 및 예약 검색 도중 OfficeScan이 바이러스/악성 프로그램을 발견하면, 사용자에게 탐지 정보를 알리도록 알림 메시지를 표시할 수 있습니다.

알림 메시지를 수정하려면 **관리** > **알림** > **에이전트**의 **유형** 드롭다운에서 **바이러스/악성 프로그램**을 선택합니다.

가능성이 있는 바이러스/악성 프로그램이 탐지되면 알림 메시지 표시

실시간 검색 및 예약 검색 도중 OfficeScan에서 가능성이 있는 바이러스/악성 프로그램을 발견한 경우 사용자에게 이를 알리는 알림 메시지를 표시할 수 있습니다.

알림 메시지를 수정하려면 **관리** > **알림** > **에이전트**의 **유형** 드롭다운에서 **바이러스/악성 프로그램**을 선택합니다.

격리된 파일 복원

탐지가 정확하지 않다고 생각되는 경우 OfficeScan에서 격리 보관한 파일을 복원할 수 있습니다. 중앙 격리 보관 복원 기능을 사용하여 격리 보관 디렉터리에서 파일을 검색하고 SHA1 확인 검사를 사용하여 복원할 파일이 수정되지 않았는지 확인할 수 있습니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 도메인을 선택하거나 에이전트를 선택합니다.
3. **작업** > **중앙 격리 보관 복원**을 클릭합니다.

   중앙 격리 보관 복원 기준 화면이 열립니다.
4. **감염된 파일/개체** 필드에 복원할 데이터의 이름을 입력합니다.
5. 필요에 따라 기간, 보안 위협 이름 및 데이터의 파일 경로를 지정합니다.
6. **검색**을 클릭합니다.

   중앙 격리 보관 복원 화면이 나타나고 검색 결과가 표시됩니다.
7. **도메인 수준 제외 목록에 복원된 파일 추가**를 선택하여 파일이 복원되는 도메인의 모든 OfficeScan 에이전트에서 검색 제외 목록에 파일을 추가하게 합니다.

   이렇게 하면 OfficeScan에서 이후에 검색할 때 이 파일을 위협으로 탐지하지 않습니다.
8. 필요에 따라 확인에 사용할 파일의 SHA1 값을 입력합니다.
9. 목록에서 복원할 파일을 선택하고 **복원**을 클릭합니다.

   팁

   파일을 복원하는 개별 OfficeScan 에이전트를 보려면 **엔드포인트** 열의 링크를 클릭합니다.
10. 확인 대화 상자에서 **닫기**를 클릭합니다.

OfficeScan에서 격리된 파일을 복원했는지 확인하려면 중앙 격리 보관 복원 로그 보기 페이지 7-96를 참조하십시오.

암호화된 파일 복원

감염된 파일이 열리지 않도록 방지하기 위해 OfficeScan은 다음 인스턴스 도중 파일을 암호화합니다.

- 파일을 격리 보관하기 전
- 파일을 치료하기 전에 백업할 때

파일에서 정보를 검색해야 하는 경우, OfficeScan에서는 해당 파일을 해독한 후 복원하는 도구를 제공합니다. OfficeScan은 다음 파일을 해독하고 복원할 수 있습니다.

표 7-15. OfficeScan에서 해독 및 복원할 수 있는 파일

파일	설명
에이전트 엔드포인트에 있는 격리된 파일	이러한 파일은 <에이전트 설치 폴더>₩SUSPECT₩Backup 폴더에 있으며 7일 후 자동으로 지워집니다. 또한, 이러한 파일은 OfficeScan 서버의 지정된 격리 보관 디렉터리에 업로드됩니다.
지정된 격리 보관 디렉터리에 있는 격리된 파일	기본적으로 이 디렉터리는 OfficeScan 서버 컴퓨터에 있습니다. 자세한 내용은 격리 보관 디렉터리 페이지 7-39를 참조하십시오.
암호화된 백업 파일	이는 OfficeScan이 치료할 수 있었던 감염된 파일의 백업입니다. 이러한 파일은 <에이전트 설치 폴더>₩Backup 폴더에 있습니다. 이러한 파일을 복원하려면 해당 파일을 <에이전트 설치 폴더>₩SUSPECT₩Backup 폴더로 이동해야 합니다. OfficeScan에서는 **에이전트** > **에이전트 관리**로 이동하여 **설정** > **검색 설정** > **{검색 유형}** > **조치** 탭을 클릭하여 **치료 이전에 파일 백업**을 선택한 경우에만 치료 전에 파일을 백업하고 암호화합니다.

경고!

감염된 파일을 복원하면 바이러스/악성 프로그램이 다른 파일 및 컴퓨터로 확산될 수 있습니다. 파일을 복원하기 전에, 감염된 엔드포인트를 격리하고 이 엔드포인트의 중요 파일을 백업 위치로 이동합니다.

파일 해독 및 복원

절차

- 파일이 OfficeScan 에이전트 엔드포인트에 있는 경우
  a. 명령 프롬프트를 열고 <에이전트 설치 폴더>로 이동합니다.
  b. VSEncode.exe 파일을 두 번 클릭하거나 명령 프롬프트에 다음을 입력하여 이 파일을 실행합니다.

     ```
     VSEncode.exe /u
     ```

     이 매개 변수를 실행하면 <에이전트 설치 폴더>₩SUSPECT₩Backup 아래에 있는 파일 목록을 표시하는 화면이 열립니다.
  c. 복원할 파일 선택하고 **복원**을 클릭합니다. 도구는 한 번에 하나의 파일만 복원할 수 있습니다.
  d. 열린 화면에서 파일을 복원할 폴더를 지정합니다.
  e. **확인**을 클릭합니다. 파일이 지정된 폴더로 복원됩니다.

     참고

     OfficeScan에서 파일을 다시 검색하고 해당 파일이 복원되자마자 이를 감염된 것으로 간주할 수 있습니다. 파일이 검색되지 않도록 방지하려면 검색 제외 목록에 추가합니다. 자세한 내용은 검색 제외 페이지 7-31를 참조하십시오.
  f. 파일 복원이 완료되면 **닫기**를 클릭합니다.
- 파일이 OfficeScan 서버 또는 사용자 지정 격리 보관 디렉터리에 있는 경우
  a. 파일이 OfficeScan 서버 컴퓨터에 있으면 명령 프롬프트를 열고 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩VSEncrypt로 이동합니다.

파일이 사용자 정의 격리 보관 디렉터리에 있으면 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility로 이동하여 사용자 정의 격리 보관 디렉터리가 있는 엔드포인트에 VSEncrypt 폴더를 복사합니다.

b. 텍스트 파일을 만든 다음 암호화하거나 해독할 파일의 전체 경로를 입력합니다.

예를 들어 C:₩My Documents₩Reports에 있는 파일을 복원하려면 텍스트 파일에 C:\My Documents\Reports*.*를 입력합니다.

OfficeScan 서버 컴퓨터의 격리된 파일은 <서버 설치 폴더>₩PCCSRV₩Virus에 있습니다.

c. INI 또는 TXT 확장자로 텍스트 파일을 저장합니다. 예를 들어 C: 드라이브에 ForEncryption.ini로

d. 명령 프롬프트를 열고 VSEncrypt 폴더가 있는 디렉터리로 이동합니다.

e. 다음을 입력하여 VSEncode.exe를 실행합니다.

```
VSEncode.exe /d /i <INI 또는 TXT 파일의 위치>
```

여기서 각 항목은 다음과 같습니다.

<INI 또는 TXT 파일의 위치>는 생성한 INI 또는 TXT 파일의 경로입니다 (예: C:₩ForEncryption.ini).

f. 다양한 명령을 실행하려면 다른 매개 변수를 사용하십시오.

표 7-16. 복원 매개 변수

매개 변수	설명
없음(매개 변수 없음)	파일 암호화
/d	파일 해독
/debug	디버그 로그를 생성하고 엔드포인트에 저장합니다. OfficeScan 에이전트 엔드포인트에서 디버그 로그 VSEncrypt.log는 <에이전트 설치 폴더>에 만들어집니다.
/o	암호화된 파일이나 해독된 파일이 이미 있으면 해당 파일을 덮어씁니다.

매개 변수	설명
/f <파일 이름>	단일 파일을 암호화 또는 해독합니다.
/nr	원본 파일 이름을 복원하지 않습니다.
/v	도구에 대한 정보를 표시합니다.
/u	도구의 사용자 인터페이스를 시작합니다.
/r <대상 폴더>	파일이 복원될 폴더입니다.
/s <원본 파일 이름>	암호화된 원본 파일의 이름입니다.

예를 들어 Suspect 폴더에 있는 파일을 해독하고 디버그 로그를 만들려면 VSEncode [/d] [/debug]를 입력합니다. 파일을 해독하거나 암호화하면 OfficeScan에서는 동일한 폴더에 해독되거나 암호화된 파일을 만듭니다. 파일을 해독 또는 암호화하기 전에 파일이 잠겨 있지 않은지 확인하십시오.

스파이웨어/그레이웨어 검색 조치

OfficeScan이 수행하는 검색 조치는 스파이웨어/그레이웨어를 탐지한 검색 유형에 따라 다릅니다. 각 바이러스/악성 프로그램 유형에 대해 특정 조치를 구성할 수 있으나, 모든 유형의 스파이웨어/그레이웨어에 대해 한 가지 조치만 구성할 수 있습니다. 예를 들어 OfficeScan이 수동 검색(스캔 유형) 동안 스파이웨어/그레이웨어 유형을 발견하면 영향 받는 시스템 리소스를 치료(조치)합니다.

다양한 유형의 스파이웨어/그레이웨어에 대한 자세한 내용은 스파이웨어 및 그레이웨어 페이지 7-5를 참조하십시오.

참고

스파이웨어/그레이웨어 검색 조치는 웹 콘솔을 통해서만 구성할 수 있습니다. OfficeScan 에이전트 콘솔에서는 이러한 설정에 액세스할 수 없습니다.

다음 표에는 스파이웨어/그레이웨어에 대해 OfficeScan이 수행할 수 있는 조치가 나와 있습니다.

표 7-17. 스파이웨어/그레이웨어 검색 조치

조치	설명
치료	OfficeScan은 프로세스를 종료하거나 레지스트리, 파일, 쿠키 및 바로 가기를 삭제합니다. 스파이웨어/그레이웨어를 치료한 후 OfficeScan 에이전트에서는 스파이웨어/그레이웨어 데이터를 백업합니다. 이 데이터는 스파이웨어/그레이웨어가 액세스하기에 안전하다고 판단한 경우 복원할 수 있습니다. 자세한 내용은 스파이웨어/그레이웨어 복원 페이지 7-50를 참조하십시오.
그대로 두기	OfficeScan은 발견된 스파이웨어/그레이웨어에 대해 어떠한 조치도 수행하지 않으며 스파이웨어/그레이웨어 탐지만 로그에 기록합니다. 이 조치는 수동 검색, 예약 검색 및 지금 검색 도중에만 수행할 수 있습니다. 실시간 검색 도중 조치는 "액세스 거부"입니다. 발견된 스파이웨어/그레이웨어가 승인된 목록에 포함된 경우, OfficeScan은 어떠한 조치도 수행하지 않습니다. 자세한 내용은 스파이웨어/그레이웨어 승인된 목록 페이지 7-48를 참조하십시오.
액세스 거부	OfficeScan은 발견된 스파이웨어/그레이웨어 구성 요소에 대한 액세스(복사, 열기)를 거부합니다. 이 조치는 실시간 검색 동안에만 수행할 수 있습니다. 수동 검색, 예약 검색 및 지금 검색 도중 조치는 "그대로 두기"입니다.

스파이웨어/그레이웨어가 탐지되면 알림 메시지 표시

실시간 검색 및 예약 검색 도중 OfficeScan이 스파이웨어/그레이웨어를 발견하면, 사용자에게 탐지 정보를 알리도록 알림 메시지를 표시할 수 있습니다.

알림 메시지를 수정하려면 **관리** > **알림** > **에이전트**의 **유형** 드롭다운에서 **스파이웨어/그레이웨어**를 선택합니다.

스파이웨어/그레이웨어 승인된 목록

OfficeScan에서는 스파이웨어 또는 그레이웨어로 간주하지 않으려는 파일 또는 응용 프로그램을 포함하는 "승인된" 스파이웨어/그레이웨어의 목록을 제공합니다. 검색 도중에 특정 스파이웨어/그레이웨어가 발견되면, OfficeScan이 승인된 목록을 확인하고 승인된 목록에서 일치 항목을 찾은 경우 조치를 수행하지 않습니다.

승인된 목록을 하나 이상의 에이전트 및 도메인에 적용하거나, 서버가 관리하는 모든 에이전트에 적용합니다. 승인된 목록은 모든 검색 유형에 적용됩니다. 즉, 수동 검색, 실시간 검색, 예약 검색 및 지금 검색 중에 동일한 승인된 목록이 사용됩니다.

승인된 목록에 이미 발견된 스파이웨어/그레이웨어 추가

절차

1. 다음 중 하나로 이동합니다.
   - **에이전트** > **에이전트 관리**
   - **로그** > **에이전트** > **보안 위험**
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **스파이웨어/그레이웨어 로그** 또는 **로그 보기** > **스파이웨어/그레이웨어 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 선택하고 **승인된 목록에 추가**를 클릭합니다.
6. 승인된 스파이웨어/그레이웨어를 선택한 에이전트 컴퓨터 또는 특정 도메인에만 적용합니다.
7. **저장**을 클릭합니다. 선택한 에이전트에서 설정을 적용하고 OfficeScan 서버에서 **에이전트** > **에이전트 관리** > **설정** > **스파이웨어/그레이웨어 승인된 목록**에 있는 승인된 목록에 스파이웨어/그레이웨어를 추가합니다.

참고

OfficeScan은 승인된 목록에 최대 1024개의 스파이웨어/그레이웨어를 수용할 수 있습니다.

스파이웨어/그레이웨어 승인된 목록 관리

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **스파이웨어/그레이웨어 승인된 목록**을 클릭합니다.
4. **스파이웨어/그레이웨어 이름** 표에서 스파이웨어/그레이웨어 이름을 선택합니다. 여러 이름을 선택하려면 Ctrl 키를 누른 채로 하나씩 선택합니다.
   - **검색** 필드에 키워드를 입력하고 **검색**을 클릭할 수도 있습니다. OfficeScan이 키워드와 일치하는 이름으로 표를 새로 고칩니다.
5. **추가**를 클릭합니다.

   이름이 **승인된 목록** 표로 이동합니다.
6. 승인된 목록에서 이름을 제거하려면 이름을 선택하고 **제거**를 클릭합니다. 여러 이름을 선택하려면 Ctrl 키를 누른 채로 하나씩 선택합니다.
7. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

스파이웨어/그레이웨어 복원

스파이웨어/그레이웨어를 치료한 후 OfficeScan 에이전트는 스파이웨어/그레이웨어 데이터를 백업합니다. 데이터가 유해하지 않다고 생각되는 경우 백업

데이터를 복원하도록 온라인 에이전트에 알리십시오. 백업 시간에 따라 복원할 스파이웨어/그레이웨어 데이터를 선택합니다.

참고

OfficeScan 에이전트 사용자는 스파이웨어/그레이웨어 복원을 시작할 수 없고, 해당 에이전트가 복원할 수 있는 백업 데이터에 대한 알림을 받지도 않습니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 도메인을 열고 에이전트를 선택합니다.

   참고

   한 번에 하나의 에이전트에서만 스파이웨어/그레이웨어 복원을 수행할 수 있습니다.

3. **작업** > **스파이웨어/그레이웨어 복원**을 클릭합니다.
4. 각 데이터 세그먼트에 대해 복원할 항목을 보려면 **보기**를 클릭합니다.

   새 화면이 표시됩니다. **뒤로**를 클릭하여 이전 화면으로 돌아갑니다.
5. 복원할 데이터 세그먼트를 선택합니다.
6. **복원**을 클릭합니다.

   OfficeScan에서 복원 상태를 알립니다. 전체 보고서를 보려면 스파이웨어/그레이웨어 복원 로그를 확인합니다. 자세한 내용은 스파이웨어/그레이웨어 복원 로그 보기 페이지 7-100를 참조하십시오.

신뢰할 수 있는 프로그램 목록

실시간 및 동작 모니터링 검색 동안 OfficeScan이 신뢰할 수 있는 프로세스 검색을 건너뛰도록 구성할 수 있습니다. 신뢰할 수 있는 프로그램 목록에 프로그램을 추가하면 OfficeScan에서는 실시간 검색 시 프로그램 또는 프로그램에서 시작된 프로세스를 검색하지 않습니다. 신뢰할 수 있는 프로그램을 신뢰할 수 있

는 프로그램 목록에 추가하면 엔드포인트에서의 검색 성능을 향상시킬 수 있습니다.

참고

다음 요구 사항을 만족하면 신뢰할 수 있는 프로그램 목록에 파일을 추가할 수 있습니다.

- 파일이 Windows 시스템 디렉터리에 있지 않습니다.
- 파일에 유효한 디지털 서명이 있습니다.

프로그램을 신뢰할 수 있는 프로그램 목록에 추가하면 OfficeScan에서는 이 프로그램을 다음 검색에서 자동으로 제외합니다.

- 실시간 검색 파일 검사
- 동작 모니터링
- 실시간 검색 프로세스 검사

신뢰할 수 있는 프로그램 목록 구성

신뢰할 수 있는 프로그램 목록에는 실시간 검색 및 동작 모니터링 검색의 프로그램에서 호출된 프로그램과 모든 하위 프로세스가 제외됩니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **신뢰할 수 있는 프로그램 목록**을 클릭합니다.
4. 목록에서 제외할 프로그램의 전체 프로그램 경로를 입력합니다.
5. **신뢰할 수 있는 프로그램 목록에 추가**를 클릭합니다.
6. 목록에서 프로그램을 제거하려면 **삭제** 아이콘을 클릭합니다.

7. 신뢰할 수 있는 프로그램 목록을 내보내려면 **내보내기**를 클릭한 후 파일의 위치를 선택합니다.

참고

OfficeScan에서 목록을 DAT 형식으로 저장합니다.

8. 신뢰할 수 있는 프로그램 목록을 가져오려면 **가져오기**를 클릭한 후 파일의 위치를 선택합니다.

   a. **찾아보기...**를 클릭하고 DAT 파일의 위치를 선택합니다.

   b. **가져오기**를 클릭합니다.

9. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

검색 권한 및 기타 설정

검색 권한이 있는 사용자는 컴퓨터의 파일이 검색되는 방법에 대해 더 많은 제어 권한을 가집니다. 검색 권한을 통해 사용자 또는 OfficeScan 에이전트는 다음 작업을 수행할 수 있습니다.

- 사용자는 수동 검색, 예약 검색 및 실시간 검색 설정을 구성할 수 있습니다. 자세한 내용은 검색 유형 권한 페이지 7-54를 참조하십시오.
- 사용자는 예약 검색을 연기하거나 중지하거나 건너뛸 수 있습니다. 자세한 내용은 예약 검색 권한 및 기타 설정 페이지 7-57를 참조하십시오.

- 사용자는 POP3 전자 메일 메시지에서 바이러스/악성 프로그램을 검색할 수 있습니다. 자세한 내용은 메일 검색 권한 및 기타 설정 페이지 7-62를 참조하십시오.
- OfficeScan 에이전트는 캐시 설정을 사용하여 검색 성능을 개선할 수 있습니다. 자세한 내용은 검색을 위한 캐시 설정 페이지 7-64를 참조하십시오.
- 사용자는 개별 신뢰할 수 있는 프로그램 목록을 사용자 정의할 수 있습니다. 자세한 내용은 신뢰할 수 있는 프로그램 목록 권한 페이지 7-68를 참조하십시오.

검색 유형 권한

사용자가 자체 수동 검색, 실시간 검색 및 예약 검색 설정을 구성하도록 허용합니다.

검색 유형 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **검색** 섹션으로 이동합니다.
5. 사용자가 구성할 수 있는 검색 유형을 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트에 대한 검색 설정 구성

절차

1. 시스템 트레이에서 OfficeScan 에이전트 아이콘을 마우스 오른쪽 단추로 클릭하고 **OfficeScan 에이전트 콘솔 열기**를 선택합니다.
2. **설정** > **{검색 유형}**을 클릭합니다.

그림 7-1. OfficeScan 에이전트 콘솔의 검색 설정

3. 다음 설정을 구성합니다.

   - 실시간 검색 설정: 파일에 대한 사용자 작업, 검색할 파일, 검색 설정, 검색 제외, 검색 조치
   - 수동 검색 설정: 검색할 파일, 검색 설정, CPU 사용량, 검색 제외, 검색 조치
   - 예약 검색 설정: 예약, 검색할 파일, 검색 설정, CPU 사용량, 검색 제외, 검색 조치

4. **확인**을 클릭합니다.

예약 검색 권한 및 기타 설정

에이전트에서 예약 검색이 실행되도록 설정된 경우 사용자는 예약 검색을 연기하거나 건너뛰거나 중지할 수 있습니다.

예약 검색 연기

"예약 검색 연기" 권한이 있는 사용자는 다음 작업을 수행할 수 있습니다.

- 예약 검색이 실행되기 전에 예약 검색을 연기한 후 연기 기간을 지정할 수 있습니다. 예약 검색은 한 번만 연기할 수 있습니다.
- 예약 검색이 진행 중인 경우, 사용자는 검색을 중지하고 나중에 다시 시작할 수 있습니다. 그런 다음 사용자는 검색이 다시 시작되기 전까지의 경과 시간을 지정할 수 있습니다. 검색이 다시 시작될 때는 이전에 검색된 모든 파일이 다시 검색됩니다. 예약 검색을 중지한 후 한 번만 다시 시작할 수 있습니다.

참고

사용자가 지정할 수 있는 최소 연기 기간/경과 시간은 15분입니다. 최대값은 12시간 45분입니다.

보안 설정 탭의 **에이전트** > **글로벌 에이전트 설정**으로 이동하여 연기 시간을 수정할 수 있습니다. **예약 검색 설정** 섹션에서 **최대 __시간 __분 예약 검색 연기** 설정을 수정합니다.

예약 검색 건너뛰기 및 중지

이 권한을 통해 사용자는 다음 작업을 수행할 수 있습니다.

- 예약 검색 실행 전에 건너뛰기
- 예약 검색이 진행 중일 때 중지

참고

사용자는 두 번 이상 예약 검색을 건너뛰거나 중지할 수 있습니다. 시스템이 다시 시작된 후에도 예약 검색에서는 다음 예약 시간에 검색을 다시 시작합니다.

예약 검색 권한 알림

사용자에게 예약 검색 권한을 활용하도록 허용하려면 OfficeScan에서 예약 검색을 실행하기 전에 알림 메시지를 표시하도록 구성하여 해당 사용자에게 부여한 권한에 대해 알립니다.

예약 검색 권한 부여 및 권한 알림 표시

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **예약 검색** 섹션으로 이동합니다.
5. 다음 옵션을 선택합니다.
   - **예약 검색 연기**
   - **예약 검색 건너뛰기 및 중지**
6. **기타 설정** 탭을 클릭하고 **예약 검색 설정** 섹션으로 이동합니다.
7. **예약 검색 실행 전 알림 표시**를 선택합니다.

   이 옵션을 사용하는 경우 예약 검색이 실행되기 몇 분 전에 알림 메시지가 에이전트 엔드포인트에 표시됩니다. 검색 일정(날짜 및 시간)과 예약 검색 연기, 건너뛰기 또는 중지와 같은 예약 검색 권한을 사용자에게 알립니다.

   참고

   시간(분)을 구성할 수 있습니다. 시간(분)을 구성하려면 **보안 설정** 탭의 **에이전트** > **글로벌 에이전트 설정**으로 이동합니다. **예약 검색 설정** 섹션에서 **예약 검색 실행 __분 전에 사용자에게 알림** 설정을 수정합니다.

8. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

에이전트에서 예약 검색 연기/건너뛰기 및 중지

절차

- 예약 검색이 시작되지 않는 경우
  a. 시스템 트레이에서 OfficeScan 에이전트 아이콘을 마우스 오른쪽 단추로 클릭하고 **고급 예약 검색 설정**을 선택합니다.

그림 7-2. 예약 검색 고급 설정 옵션

참고

알림 메시지가 사용 가능하도록 설정되어 있고 예약 검색이 실행되기 몇 분 전에 표시되도록 설정된 경우, 사용자는 이 단계를 수행할 필요가 없습니다. 알림 메시지에 대한 자세한 내용은 예약 검색 권한 알림 페이지 7-58을 참조하십시오.

b. 표시되는 알림 창의 다음 옵션 중 선택합니다.

- **검색 연기 시간 __시간 __분.**
- **이 예약 검색을 건너뜁니다. 다음 예약 검색은 <date> <time>에 실행됩니다.**

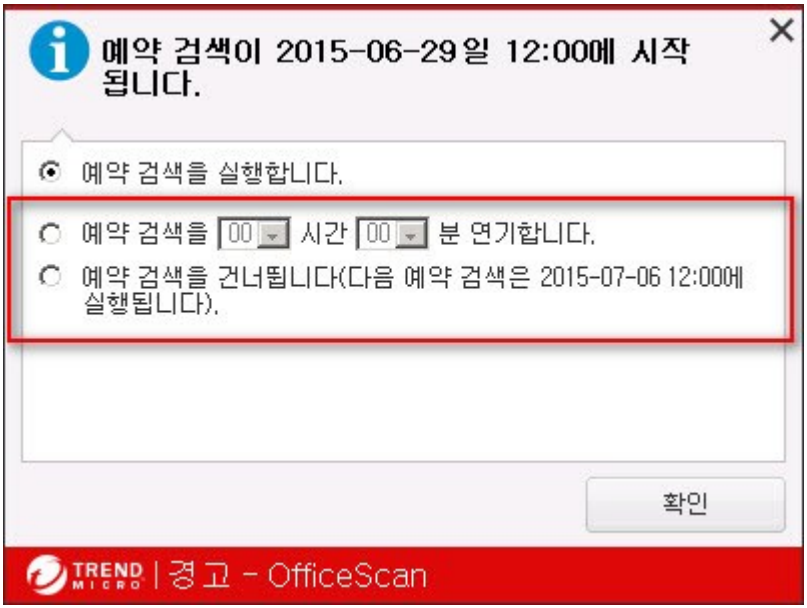


그림 7-3. OfficeScan 에이전트 엔드포인트에 대한 예약 검색 권한

- 예약 검색이 진행 중인 경우

a. 시스템 트레이에서 OfficeScan 에이전트 아이콘을 마우스 오른쪽 단추로 클릭하고 **예약 검색 고급 설정**을 선택합니다.

b. 표시되는 알림 창의 다음 옵션 중 선택합니다.

- **검색을 중지합니다. 다음 시간 후에 검색을 다시 시작합니다. __시간 __분**
- **검색을 중지합니다. 다음 예약 검색은 <date> <time>에 실행됩니다.**

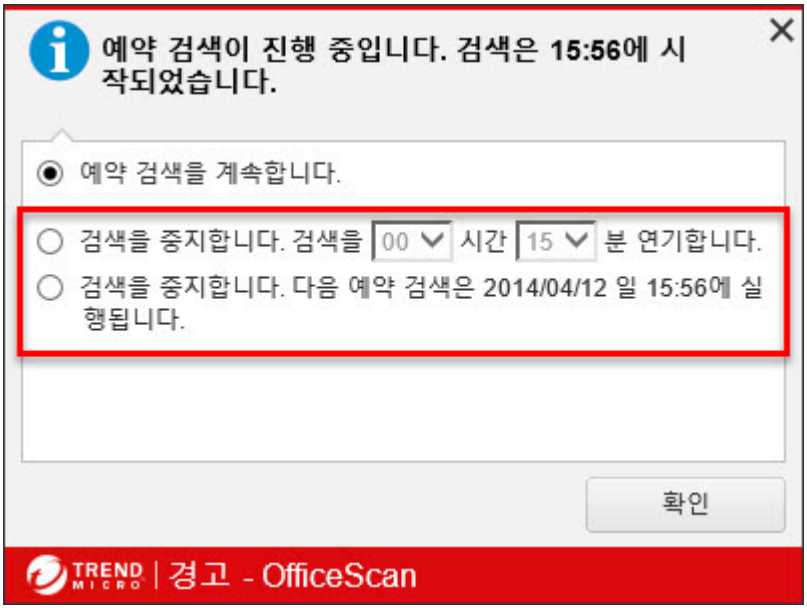


그림 7-4. OfficeScan 에이전트 엔드포인트에 대한 예약 검색 권한

메일 검색 권한 및 기타 설정

에이전트에 메일 검색 권한이 있는 경우 OfficeScan 에이전트 콘솔에 **메일 검색** 옵션이 표시됩니다. **메일 검색** 옵션에는 POP3 메일 검색이 표시됩니다.

그림 7-5. OfficeScan 에이전트 콘솔의 메일 검색 설정

다음 표에서는 POP3 메일 검색 프로그램에 대해 설명합니다.

표 7-18. 메일 검색 프로그램

세부 정보	설명
목적	POP3 전자 메일 메시지에서 바이러스/악성 프로그램을 검색합니다.
필수 구성 요소	• 웹 콘솔에서 관리자가 사용하도록 설정해야 사용할 수 있습니다. **참고** POP3 메일 검색을 사용하려면 메일 검색 권한 부여 및 POP3 메일 검색 사용 페이지 7-63을 참조하십시오. • 바이러스/악성 프로그램에 대한 조치는 OfficeScan 에이전트 콘솔에서 구성할 수 있지만 웹 콘솔에서는 구성할 수 없습니다.
지원되는 검색 유형	실시간 검색 POP3 Mail Server에서 전자 메일 메시지가 검색되면 검색이 실행됩니다.
검색 결과	• 검색이 완료된 후에 제공되는 발견된 보안 위험에 대한 정보 • 검색 결과는 OfficeScan 에이전트 콘솔의 **로그** 화면에 기록되지 않음 • 검색 결과는 서버로 전송되지 않음
기타 세부 정보	웹 검증 기능과 OfficeScan NT 프록시 서비스(TMProxy.exe) 공유

메일 검색 권한 부여 및 POP3 메일 검색 사용

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.

3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **메일 검색** 섹션으로 이동합니다.
5. **OfficeScan 에이전트 콘솔에 메일 검색 설정 표시**를 선택합니다.
6. **기타 설정** 탭을 클릭하고 **POP3 전자 메일 검색 설정** 섹션으로 이동합니다.
7. **POP3 전자 메일 검색**을 선택합니다.
8. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

검색을 위한 캐시 설정

OfficeScan 에이전트는 디지털 서명 및 주문형 검색 캐시 파일을 생성하여 검색 성능을 향상시킬 수 있습니다. 주문형 검색이 실행되는 경우 OfficeScan 에이전트는 먼저 디지털 서명 캐시 파일을 검사한 다음 주문형 검색 캐시 파일을 검사하여 검색에서 제외할 파일을 확인합니다. 검색에서 제외되는 파일 수가 많을수록 검색 시간이 단축됩니다.

디지털 서명 캐시

디지털 서명 캐시 파일은 수동 검색, 예약 검색 및 지금 검색 중에 사용됩니다. 에이전트는 디지털 서명 캐시 파일에 서명이 추가된 파일을 검색하지 않습니다.

OfficeScan 에이전트는 동작 모니터링에 사용된 것과 동일한 스마트 검색 패턴을 사용하여 디지털 서명 캐시 파일을 생성합니다. 스마트 검색 패턴에는 Trend

Micro에서 신뢰할 수 있는 것으로 간주하므로 검색에서 제외할 수 있는 파일 목록이 포함되어 있습니다.

참고

Windows Server 플랫폼(Windows XP, 2003 및 SP1이 포함되지 않은 Vista는 64비트 버전이 지원되지 않음)에서는 동작 모니터링이 자동으로 해제됩니다. 이러한 플랫폼에서 디지털 서명 캐시를 사용하도록 설정한 경우 OfficeScan 에이전트는 캐시에서 사용할 스마트 검색 패턴을 다운로드하지만 다른 동작 모니터링 구성 요소는 다운로드하지 않습니다.

에이전트는 웹 콘솔에서 구성 가능한 일정에 따라 디지털 서명 캐시 파일을 생성합니다. 이를 통해 에이전트는 다음을 수행할 수 있습니다.

- 마지막 캐시 파일이 생성된 이후에 시스템에 도입된 새 파일의 서명 추가
- 시스템에서 수정되거나 삭제된 파일의 서명 제거

캐시 생성 프로세스 중에 에이전트는 다음 폴더에서 신뢰할 수 있는 파일을 확인한 후 이러한 파일의 서명을 디지털 서명 캐시 파일에 추가합니다.

- %PROGRAMFILES%
- %WINDIR%

캐시 생성 프로세스 중에는 에이전트에서 최소한의 시스템 리소스를 사용하므로 이 프로세스는 엔드포인트의 성능에 영향을 주지 않습니다. 또한 에이전트는 특정한 이유(예: 호스트 컴퓨터의 전원이 꺼지거나 무선 엔드포인트의 AC 어댑터가 연결되지 않은 경우)로 중단된 캐시 생성 작업을 다시 시작할 수 있습니다.

주문형 검색 캐시

주문형 검색 캐시 파일은 수동 검색, 예약 검색 및 지금 검색 중에 사용됩니다. OfficeScan 에이전트는 주문형 검색 캐시 파일에 캐시가 추가된 파일을 검색하지 않습니다.

검색을 실행할 때마다 OfficeScan 에이전트는 위협이 없는 파일의 등록정보를 확인합니다. 위협이 없는 파일이 일정 기간(기간은 구성 가능함) 동안 수정되지 않은 경우 OfficeScan 에이전트는 주문형 검색 캐시 파일에 해당 파일의 캐시를

추가합니다. 캐시가 만료되지 않은 경우 다음 검색 시 파일이 검색되지 않습니다.

위협이 없는 파일의 캐시는 일정 기간(일)(이 기간도 구성 가능함) 내에 만료됩니다. 캐시가 만료될 때 또는 만료된 후 검색이 발생한 경우 OfficeScan 에이전트는 만료된 캐시를 제거하고 이 파일에서 위협을 검색합니다. 파일이 위협이 없고 수정되지 않은 경우 파일의 캐시가 주문형 검색 캐시 파일에 다시 추가됩니다. 파일이 위협이 없지만 최근에 수정된 경우에는 캐시가 추가되지 않고 다음 검색 시 파일이 다시 검색됩니다.

위협이 없는 파일의 캐시는 다음 예와 같이 감염된 파일이 검색에서 제외되는 것을 방지하기 위해 만료됩니다.

- 아주 오래된 패턴 파일은 수정되지 않은 감염된 파일을 위협이 없는 것으로 간주할 수 있습니다. 캐시가 만료되지 않으면 실시간 검색에 의해 발견되고 수정될 때까지 감염된 파일이 시스템에 그대로 유지됩니다.
- 캐시된 파일이 수정되고 파일 수정 중에 실시간 검색이 작동하지 않은 경우 수정된 파일에서 위협을 검색할 수 있도록 캐시를 만료해야 합니다.

주문형 검색 캐시 파일에 추가되는 캐시 수는 검색 유형 및 해당 검색 대상에 따라 다릅니다. 예를 들어 OfficeScan 에이전트가 수동 검색 중에 엔드포인트에 있는 1,000개의 파일 중 200개만 검색한 경우 캐시 수가 적을 수 있습니다.

주문형 검색을 자주 실행하면 주문형 검색 캐시 파일로 인해 검색 시간이 크게 단축됩니다. 예를 들어 일부 캐시가 만료되지 않은 검색 작업에서 일반적으로 12분 정도 걸리는 검색이 1분으로 단축될 수 있습니다. 파일을 수정되지 않은 상태로 유지해야 하는 기간(일)을 줄이고 캐시 만료일을 연장하면 일반적으로 성능이 향상됩니다. 파일이 수정되지 않은 상태로 유지되는 기간이 비교적 짧기 때문에 더 많은 캐시가 캐시 파일에 추가될 수 있습니다. 또한 캐시 만료일이 늘어나면 검색에서 더 많은 파일을 건너뛰게 됩니다.

주문형 검색을 자주 실행하지 않는 경우 다음 검색이 실행되기 전에 캐시가 만료될 수 있으므로 주문형 검색 캐시를 사용하지 않도록 설정할 수 있습니다.

검색을 위한 캐시 설정 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭하고 **검색을 위한 캐시 설정** 섹션으로 이동합니다.
5. 디지털 서명 캐시에 대한 설정을 구성합니다.
   a. **디지털 서명 캐시 사용**을 선택합니다.
   b. **다음 간격으로 캐시 생성: __일**에서 에이전트가 캐시를 생성하는 주기를 지정합니다.
6. 주문형 검색 캐시에 대한 설정을 구성합니다.
   a. **주문형 검색 캐시 사용**을 선택합니다.
   b. **다음 기간 동안 변경되지 않은 안전한 파일에 대한 캐시 추가: __일**에서 파일이 캐시되기 전에 변경되지 않은 상태로 유지되는 일 수를 지정합니다.
   c. **안전한 각 파일의 캐시는 다음 기간 이내에 만료됨: __일**에서 캐시가 캐시 파일에서 그대로 유지되는 최대 일 수를 지정합니다.

   참고

   검색 중에 추가된 모든 캐시가 같은 날 만료되는 것을 방지하기 위해 캐시는 지정한 최대 일 수 이내에 임의로 만료됩니다. 예를 들어 500개의 캐시가 오늘 추가되고 지정한 최대 일 수가 10일인 경우 캐시의 일부는 다음 날 만료되고 대부분은 연속된 이후의 날짜에 만료됩니다. 그리고 10일째 되는 날에는 남아 있는 모든 캐시가 만료됩니다.
7. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

신뢰할 수 있는 프로그램 목록 권한

실시간 및 동작 모니터링 검색 동안 OfficeScan이 신뢰할 수 있는 프로세스 검색을 건너뛰도록 구성할 권한을 최종 사용자에게 부여할 수 있습니다. 신뢰할 수 있는 프로그램 목록에 프로그램을 추가하면 OfficeScan에서는 실시간 검색 시 프로그램 또는 프로그램에서 시작된 프로세스를 검색하지 않습니다. 신뢰할 수 있는 프로그램을 신뢰할 수 있는 프로그램 목록에 추가하면 엔드포인트에서의 검색 성능을 향상시킬 수 있습니다.

신뢰할 수 있는 프로그램 목록 설정 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **신뢰할 수 있는 프로그램 목록** 섹션으로 이동합니다.
5. **OfficeScan 에이전트 콘솔에 신뢰할 수 있는 프로그램 목록 표시**를 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

글로벌 검색 설정

에이전트에 적용되는 글로벌 검색 설정에는 여러 가지 방법이 있습니다.

- 특정 검색 설정은 서버가 관리하는 모든 에이전트 또는 특정 검색 권한이 있는 에이전트에만 적용될 수 있습니다. 예를 들어 예약 검색 연기 기간을 구성하는 경우, 예약 검색을 연기할 권한이 있는 에이전트만 해당 설정을 사용합니다.
- 특정 검색 설정은 모든 검색 유형 또는 특정 검색 유형에만 적용될 수 있습니다. 예를 들어 OfficeScan 서버와 OfficeScan 에이전트가 모두 설치된 엔드포인트에서 검색하는 데 OfficeScan 서버 데이터베이스를 제외할 수 있습니다. 단, 이 설정은 실시간 검색 중에만 적용됩니다.
- 바이러스/악성 프로그램이나 스파이웨어/그레이웨어 또는 둘 다에 대해 검색 시 특정 검색 설정을 적용할 수 있습니다. 예를 들어, 스파이웨어/그레이웨어 검색 중에는 점검 모드만 적용됩니다.

글로벌 검색 설정 구성

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **보안 설정** 탭을 클릭하고 사용 가능한 각 섹션에서 글로벌 검색 설정을 구성합니다.
   - 검색 설정 섹션 페이지 7-71

- 예약 검색 설정 섹션 페이지 7-76

3. **시스템** 탭을 클릭합니다.

4. **인증된 안전한 소프트웨어 서비스 설정** 섹션에서 **동작 모니터링, 방화벽 및 바이러스 방역 검색에 대해 인증된 안전한 소프트웨어 서비스 사용** 설정을 구성합니다.

   인증된 안전한 소프트웨어 서비스에서는 Trend Micro 데이터 센터를 쿼리하여 악성 프로그램 동작 차단, 이벤트 모니터링, 방화벽 또는 바이러스 백신 검색을 통해 탐지된 프로그램의 안전성을 확인합니다. 인증된 안전한 소프트웨어 서비스를 사용하도록 설정하면 잘못된 판정이 탐지될 가능성이 줄어듭니다.

   참고

   인증된 안전한 소프트웨어 서비스를 사용도록 설정하기 전에 OfficeScan 에이전트 프록시 설정이 올바른지 확인해야 합니다(자세한 내용은 OfficeScan 에이전트 프록시 설정 페이지 15-47 참조). 잘못된 프록시 설정은 일시적인 인터넷 연결 끊김과 함께 Trend Micro 데이터 센터의 응답을 지연시키거나 수신되지 않도록 하여 모니터링 대상 프로그램이 응답하지 않는 것처럼 보이게 합니다.

   또한 순수 IPv6 OfficeScan 에이전트는 Trend Micro 데이터 센터에서 직접 쿼리할 수 없습니다. OfficeScan 에이전트에서 Trend Micro 데이터 센터에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

5. **네트워크** 탭을 클릭합니다.

6. **바이러스/악성 프로그램 로그 대역폭 설정** 섹션에서 **1시간 이내에 동일한 바이러스/악성 프로그램이 재검출될 경우 OfficeScan 에이전트에서 단일 바이러스/악성 프로그램 로그 항목을 작성하도록 설정** 설정을 구성합니다.

   OfficeScan에서는 짧은 기간 동안 동일한 바이러스/악성 프로그램으로부터 여러 건의 감염을 발견하는 경우 바이러스 로그 항목을 통합합니다. OfficeScan에서 하나의 바이러스/악성 프로그램을 여러 번 발견하면 바이러스/악성 프로그램 로그가 빨리 채워지고 OfficeScan 에이전트에서 서버로 로그 정보를 보내는 동안 네트워크 대역폭을 많이 소비할 수 있습니다. 이 기능을 사용하면 바이러스/악성 프로그램 로그 항목 수도 줄이고 바이

러스 로그 정보를 서버에 보고할 때 OfficeScan 에이전트에서 소비하는 네트워크 대역폭도 줄일 수 있습니다.

7. **에이전트 제어** 탭을 클릭합니다.

8. **일반 설정** 섹션에서 **엔드포인트의 Windows 바로 가기 메뉴에 수동 검색 추가** 설정을 구성합니다.

   이 설정을 사용하면 서버에서 관리되는 모든 OfficeScan 에이전트의 Windows 탐색기 마우스 오른쪽 단추 메뉴에 **OfficeScan으로 검색** 옵션이 추가됩니다. 사용자가 Windows 데스크톱 또는 Windows Explorer에서 파일 또는 폴더를 마우스 오른쪽 단추로 클릭하고 해당 옵션을 선택하면, 수동 검색이 파일 또는 폴더에 바이러스/악성 프로그램 및 스파이웨어/그레이웨어가 있는지 검색합니다.

그림 7-6. OfficeScan으로 검색 옵션

9. **저장**을 클릭합니다.

검색 설정 섹션

글로벌 에이전트 설정 화면의 **보안 설정** 탭에 있는 **검색 설정** 섹션에서 관리자는 다음을 구성할 수 있습니다.

- OfficeScan 서버 데이터베이스 폴더를 실시간 검색에서 제외 페이지 7-72
- 검색에서 Microsoft Exchange Server 폴더 및 파일 제외 페이지 7-72

- 파일 작업에 대한 연기된 검색 사용 페이지 7-73
- 엔드포인트에서 악성 프로그램 방지 조기 실행 보호 사용 페이지 7-73
- 압축 파일 내에서 감염된 파일 치료/삭제 페이지 7-73
- 점검 모드 사용 페이지 7-75
- 쿠키 검색 페이지 7-76

OfficeScan 서버 데이터베이스 폴더를 실시간 검색에서 제외

OfficeScan 에이전트 및 OfficeScan 서버가 동일한 엔드포인트에 있는 경우, OfficeScan 에이전트는 실시간 검색 도중 서버 데이터베이스에 바이러스/악성 프로그램 및 스파이웨어/그레이웨어가 있는지 검색하지 않습니다.

팁

검색 도중 발생할 수 있는 데이터베이스 손상을 방지하기 위해 이 설정을 사용합니다.

검색에서 Microsoft Exchange Server 폴더 및 파일 제외

OfficeScan 에이전트 및 Microsoft Exchange 2000/2003 서버가 동일한 엔드포인트에 있는 경우, 수동 검색, 실시간 검색, 예약 검색 및 지금 검색 도중 OfficeScan이 다음 Microsoft Exchange 폴더 및 파일에 바이러스/악성 프로그램 및 스파이웨어/그레이웨어가 있는지 검색하지 않습니다.

- ₩Exchsrvr₩Mailroot₩vsi 1의 다음 폴더: Queue, PickUp 및 BadMail
- .₩Exchsrvr₩mdbdata(priv1.stm, priv1.edb, pub1.stm 및 pub1.edb 파일 포함)
- .₩Exchsrvr₩Storage Group

Microsoft Exchange 2007 이상 폴더의 경우 검색 제외 목록에 해당 폴더를 수동으로 추가해야 합니다. 검색 제외 정보는 다음 웹 사이트를 참조하십시오.

http://technet.microsoft.com/en-us/library/bb332342.aspx

검색 제외 목록을 구성하는 단계는 검색 제외 페이지 7-31를 참조하십시오.

파일 작업에 대한 연기된 검색 사용

관리자는 OfficeScan에서 파일 검색을 연기하도록 구성할 수 있습니다. OfficeScan은 사용자가 파일을 복사한 다음 복사 프로세스가 완료된 후 파일을 검색할 수 있습니다. 이 연기된 검색 기능을 사용하면 복사와 검색 프로세스의 성능이 향상됩니다.

참고

연기된 검색 기능을 사용하려면 VSAPI(바이러스 검색 엔진) 버전이 9.713 이상이어야 합니다. 서버 업그레이드에 대한 자세한 내용은 수동으로 OfficeScan 서버 업데이트 페이지 6-24를 참조하십시오.

엔드포인트에서 악성 프로그램 방지 조기 실행 보호 사용

OfficeScan은 엔드포인트에서 부트 시간 보호를 제공하기 위한 보안 부트(Secure Boot) 표준의 일부로 ELAM(악성 프로그램 방지 조기 실행) 기능을 지원합니다. 관리자가 이 기능을 사용하도록 설정하면 엔트포인트가 시작될 때 OfficeScan 에이전트를 다른 타사 소프트웨어보다 먼저 시작할 수 있습니다. 이 기능을 통해 OfficeScan 에이전트는 운영 체제 부트 프로세스 중에 악성 프로그램을 탐지할 수 있습니다.

OfficeScan 에이전트는 타사 소프트웨어 드라이버를 모두 검색한 후 드라이버 분류 정보를 시스템 커널에 보고합니다. 관리자는 Windows의 그룹 정책에서 드라이버 분류를 기반으로 조치를 정의하고 엔드포인트의 이벤트 뷰어를 사용하여 검색 결과를 볼 수 있습니다.

참고

ELAM은 Windows 8, Windows Server 2012 이상 버전에서만 지원됩니다.

압축 파일 내에서 감염된 파일 치료/삭제

수동 검색, 실시간 검색, 예약 검색 및 지금 검색 도중, 서버에 의해 관리되는 모든 에이전트가 압축 파일에서 바이러스/악성 프로그램을 탐지할 때 그리고 다음 조건이 충족되는 경우, 에이전트가 감염된 파일을 치료하거나 삭제합니다.

- "치료" 또는 "삭제"는 OfficeScan이 수행하도록 설정된 조치입니다. **에이전트 > 에이전트 관리 > 설정 > 검색 설정 > {검색 유형} > 조치** 탭으로 이동하여 OfficeScan에서 감염된 파일에 대해 수행할 조치를 확인합니다.
- 이 설정을 사용하도록 설정하십시오. 이 설정을 사용하면 검색 도중 엔드포인트 리소스 사용이 증가할 수 있으며, 검색 완료 시간이 더 오래 걸릴 수 있습니다. 이것은 OfficeScan이 압축 파일의 압축을 해제하고, 압축 파일 내의 감염된 파일을 치료/삭제한 후, 파일을 다시 압축해야 하기 때문입니다.
- 압축 파일 포맷이 지원됩니다. OfficeScan은 ZIP 압축 기술을 사용하는 ZIP이나 Office Open XML 등과 같은 특정 압축 파일 포맷만 지원합니다. Office Open XML은 Excel, PowerPoint 및 Word와 같은 Microsoft Office 2007 응용 프로그램의 기본 포맷입니다.

참고

지원되는 압축 파일 포맷의 전체 목록에 대해서는 지원 센터에 문의하십시오.

예를 들어, 실시간 검색은 바이러스에 감염된 파일을 삭제하도록 설정됩니다. 실시간 검색에서 abc.zip이라는 압축 파일의 압축을 해제하고 압축 파일 내의 감염된 파일 123.doc를 탐지하면 OfficeScan이 123.doc를 삭제한 후 액세스하는 데 안전해진 abc.zip을 다시 압축합니다.

다음 표에서는 조건이 충족되지 않을 경우 어떤 일이 발생하는지 설명합니다.

표 7-19. 압축 파일 시나리오 및 결과

"압축 파일 내에서 감염된 파일 치료/삭제" 상태	OFFICESCAN이 수행하도록 설정한 조치	압축 파일 포맷	결과
사용	치료 또는 삭제	지원되지 않음 예: def.rar에는 감염된 123.doc 파일이 포함되어 있습니다.	OfficeScan은 def.rar 파일을 암호화하지만 123.doc 파일에 대해서는 치료, 삭제를 비롯한 어떠한 조치도 수행하지 않습니다.

"압축 파일 내에서 감염된 파일 치료/삭제" 상태	OFFICESCAN이 수행하도록 설정한 조치	압축 파일 포맷	결과
사용 안 함	치료 또는 삭제	지원됨/지원되지 않음 예: abc.zip에는 감염된 123.doc 파일이 있습니다.	OfficeScan은 abc.zip 및 123.doc 파일을 치료, 삭제하거나 이에 대한 어떠한 조치도 수행하지 않습니다.
사용/사용 안 함	치료 또는 삭제 안 함(즉, 파일명 변경, 격리 보관, 액세스 거부 또는 그대로 두기 중 하나)	지원됨/지원되지 않음 예: abc.zip에는 감염된 123.doc 파일이 있습니다.	OfficeScan은 123.doc 파일이 아닌 abc.zip 파일에 대해 구성된 조치(파일명 변경, 격리 보관, 거부/허용 또는 그대로 두기)을 수행합니다. 조치가 다음과 같은 경우 **파일명 변경**: OfficeScan에서 abc.zip 파일명을 abc.vir로 변경하되, 123.doc 파일명은 변경하지 않습니다. **격리 보관**: OfficeScan에서 abc.zip 파일을 격리 보관합니다(123.doc 및 감염되지 않은 모든 파일이 격리 보관됨). **그대로 두기**: OfficeScan에서 바이러스 탐지를 기록하기만 하고 abc.zip 및 123.doc 파일에 대해 어떠한 작업도 수행하지 않습니다. **액세스 거부**: OfficeScan에서 abc.zip 파일이 열릴 때 이에 대한 액세스를 거부합니다(123.doc 및 감염되지 않은 모든 파일은 열 수 없음).

점검 모드 사용

점검 모드에서는 서버에서 관리하는 모든 에이전트가 수동 검색, 예약 검색, 실시간 검색 및 지금 검색을 통해 탐지된 스파이웨어/그레이웨어를 기록하지만

스파이웨어/그레이웨어 구성 요소를 치료하지는 않습니다. OfficeScan은 프로세스를 종료하거나 레지스트리, 파일, 쿠키 및 바로 가기를 삭제합니다.

Trend Micro는 Trend Micro에서 자체적으로 스파이웨어/그레이웨어로 감지한 항목을 평가한 다음 평가에 따라 적절한 조치를 취하도록 하는 점검 모드를 제공합니다. 예를 들어 발견된 것 중 보안 위험이 없다고 판단되는 스파이웨어/그레이웨어는 스파이웨어/그레이웨어 승인된 목록에 추가할 수 있습니다.

점검 모드인 경우 OfficeScan은 다음과 같은 검색 조치를 수행합니다.

- **그대로 두기**: 수동 검색, 예약 검색 및 지금 검색 도중
- **액세스 거부**: 실시간 검색 도중

참고

점검 모드는 사용자가 구성한 검색 조치를 무시합니다. 예를 들어, 수동 검색 도중의 검색 조치로 "치료"를 선택하더라도 에이전트가 점검 모드이면 "그대로 두기"가 검색 조치로 유지됩니다.

쿠키 검색

쿠키를 잠재적인 보안 위험으로 고려하는 경우, 이 옵션을 선택합니다. 선택하는 경우 서버에서 관리하는 모든 에이전트가 수동 검색, 예약 검색, 실시간 검색 및 지금 검색 도중 쿠키에 스파이웨어/그레이웨어가 있는지 검색합니다.

예약 검색 설정 섹션

예약 검색을 실행하도록 설정된 에이전트만 다음 설정을 사용합니다. 예약 검색은 바이러스/악성 프로그램 및 스파이웨어/그레이웨어를 검색할 수 있습니다.

글로벌 검색 설정의 예약 검색 설정 섹션에서 관리자는 다음을 구성할 수 있습니다.

- 실행하기 다음 시간 전 __분 전에 예약 검색 사용자에게 알림 페이지 7-77
- 최대 __시간 __분 예약 검색 연기 페이지 7-77
- 검색이 __시간 __분을 초과하여 지속되는 경우 자동으로 예약 검색 중지 페이지 7-77

- 무선 엔드포인트의 배터리 수명이 __%가 안 되고 해당 AC 어댑터가 전원에 연결되어 있지 않은 경우 예약 검색 건너뛰기 페이지 7-78
- 예약되지 않은 검색 다시 시작 페이지 7-78

실행하기 다음 시간 전 __분 전에 예약 검색 사용자에게 알림

OfficeScan은 검색이 실행되기 몇 분 전에 알림 메시지를 표시하여 검색 일정(날짜 및 시간)과 사용자에게 부여한 예약 검색 권한을 해당 사용자에게 알립니다.

에이전트 > **에이전트 관리** > **설정** > **권한 및 기타 설정** > **기타 설정(탭)** > **예약 검색 설정**에서 알림 메시지를 사용하거나 사용하지 않도록 설정할 수 있습니다. 사용하지 않는 경우, 미리 알림이 표시되지 않습니다.

최대 __시간 __분 예약 검색 연기

"예약 검색 연기" 권한이 있는 사용자만 다음 작업을 수행할 수 있습니다.

- 예약 검색이 실행되기 전에 예약 검색을 연기한 후 연기 기간을 지정할 수 있습니다.
- 예약 검색이 진행 중인 경우, 사용자는 검색을 중지하고 나중에 다시 시작할 수 있습니다. 그런 다음 사용자는 검색이 다시 시작되기 전까지의 경과 시간을 지정할 수 있습니다. 검색이 다시 시작될 때는 이전에 검색된 모든 파일이 다시 검색됩니다.

  사용자가 지정할 수 있는 최대 연기 기간/경과 시간은 12시간 45분이며, 제공된 필드에서 시간 및/또는 분을 지정하여 이 값을 줄일 수 있습니다.

검색이 __시간 __분을 초과하여 지속되는 경우 자동으로 예약 검색 중지

지정된 시간이 초과되고 검색이 아직 완료되지 않은 경우 OfficeScan이 검색을 중지합니다. 그런 다음 OfficeScan은 즉시 검색 도중 탐지된 보안 위험에 대해 사용자에게 알립니다.

무선 엔드포인트의 배터리 수명이 __ %가 안 되고 해당 AC 어댑터가 전원에 연결되어 있지 않은 경우 예약 검색 건너뛰기

무선 엔드포인트의 배터리 수명이 거의 소진되었고 AC 어댑터가 전원에 연결되어 있지 않은 것으로 탐지되면 예약 검색이 실행될 때 OfficeScan은 즉시 검색을 건너뜁니다. 배터리 수명이 거의 소진되었지만 AC 어댑터가 전원에 연결되어 있으면 검색은 진행됩니다.

예약되지 않은 검색 다시 시작

OfficeScan이 예약된 검색 지정일 및 시간에 실행되지 않아 예약 검색이 시작되지 않은 경우 또는 사용자가 예약 검색을 중단한 경우(검색 시작 후 엔드포인트 종료 등) OfficeScan이 검색을 다시 시작할 시점을 지정할 수 있습니다.

다시 시작할 예약 검색 지정:

- **중단된 예약 검색 다시 시작**: 사용자가 엔드포인트를 종료하여 중단한 예약 검색을 다시 시작합니다.
- **누락된 예약 검색 다시 시작**: 엔드포인트가 실행되지 않아 누락된 예약 검색을 다시 시작합니다.

검색을 다시 시작할 시기 지정:

- **내일 같은 시간**: OfficeScan이 다음 날 정확히 같은 시간에 실행되는 경우 검색이 다시 시작됩니다.
- **__분 경과: 엔드포인트 시작**: OfficeScan은 사용자가 엔드포인트를 켜고 몇 분 후 검색을 다시 시작합니다. 시간(분)은 10 및 120 사이입니다.

참고

관리자가 이 권한을 사용하면 사용자는 다시 시작된 예약 검색을 연기 또는 건너뛸 수 있습니다. 자세한 내용은 예약 검색 권한 및 기타 설정 페이지 7-57를 참조하십시오.

보안 위험 알림

OfficeScan에서는 사용자 자신, 다른 OfficeScan 관리자 및 OfficeScan 에이전트 사용자에게 발견된 보안 위험을 알리는 일련의 기본 알림 메시지를 제공합니다.

관리자에게 전송되는 알림에 대한 자세한 내용은 관리자를 위한 보안 위험 알림 페이지 7-79을 참조하십시오.

OfficeScan 에이전트 사용자에게 전송되는 알림에 대한 자세한 내용은 OfficeScan 에이전트 사용자를 위한 보안 위험 알림 페이지 7-85을 참조하십시오.

관리자를 위한 보안 위험 알림

보안 위험을 감지한 경우 또는 보안 위험에 대한 조치가 실패하여 사용자의 작업이 필요한 경우 사용자 자신과 다른 OfficeScan 관리자에게 알림을 보내도록 OfficeScan을 구성합니다.

OfficeScan에서는 사용자 자신과 다른 OfficeScan 관리자에게 보안 위험 탐지를 알리는 일련의 기본 알림 메시지를 제공합니다. 요구 사항에 맞게 알림을 수정하고 추가 알림 설정을 구성할 수 있습니다.

표 7-20. 보안 위험 알림 유형

유형	참조
바이러스/악성 프로그램	관리자를 위한 보안 위험 알림 구성 페이지 7-80
스파이웨어/그레이웨어	관리자를 위한 보안 위험 알림 구성 페이지 7-80
디지털 자산 전송	관리자에 대한 데이터 손실 방지 알림 구성 페이지 11-52
C&C 콜백	관리자에 대한 C&C 콜백 알림 구성 페이지 12-14

참고

OfficeScan에서는 전자 메일, SNMP 트랩 및 Windows NT 이벤트 로그를 통해 알림을 보낼 수 있습니다. OfficeScan에서 이러한 채널을 통해 알림을 보내는 경우에 대한 설정을 구성하십시오. 자세한 내용은 관리자 알림 설정 페이지 14-35를 참조하십시오.

관리자를 위한 보안 위험 알림 구성

절차

1. **관리** > **알림** > **관리자**으로 이동합니다.
2. **기준** 탭에서 다음을 수행합니다.
   a. **바이러스/악성 프로그램** 및 **스파이웨어/그레이웨어** 섹션으로 이동합니다.
   b. OfficeScan에서 바이러스/악성 프로그램 및 스파이웨어/그레이웨어가 발견된 경우에 알림을 보낼 것인지, 아니면 이러한 보안 위험에 대한 조치가 실패한 경우에만 알림을 보낼 것인지 지정합니다.
3. **전자 메일** 탭에서 다음을 수행합니다.
   a. **바이러스/악성 프로그램 탐지** 및 **스파이웨어/그레이웨어 탐지** 섹션으로 이동합니다.
   b. **전자 메일을 통한 알림 사용**을 선택합니다.
   c. **에이전트 트리 도메인 권한이 있는 사용자에게 알림 보내기**를 선택합니다.

      역할 기반 관리를 사용하여 사용자에게 에이전트 트리 도메인 권한을 부여할 수 있습니다. 특정 도메인에 속한 OfficeScan 에이전트에서 검색이 수행된 경우 도메인 권한이 있는 사용자의 전자 메일 주소로 전자 메일이 전송됩니다. 다음 표의 예를 참조하십시오.

표 7-21. 에이전트 트리 도메인 및 권한

에이전트 트리 도메인	도메인 권한이 있는 역할	역할이 있는 사용자 계정	사용자 계정의 전자 메일 주소
도메인 A	관리자(기본 제공)	루트	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
도메인 B	관리자(기본 제공)	루트	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

도메인 A에 속한 OfficeScan 에이전트에서 바이러스를 발견한 경우 mary@xyz.com, john@xyz.com 및 chris@xyz.com으로 전자 메일이 전송됩니다.

도메인 B에 속한 OfficeScan 에이전트에서 스파이웨어를 발견한 경우 mary@xyz.com 및 jane@xyz.com으로 전자 메일이 전송됩니다.

참고

이 옵션을 사용하도록 설정한 경우 도메인 권한이 있는 모든 사용자에게 해당 전자 메일 주소가 있어야 합니다. 전자 메일 주소가 없는 사용자에게는 전자 메일 알림이 전송되지 않습니다. 사용자 및 전자 메일 주소는 **관리** > **계정 관리** > **사용자 계정**에서 구성합니다.

d. **다음 전자 메일 주소로 알림 보내기**를 선택하고 전자 메일 주소를 입력합니다.

e. 기본 제목 및 메시지를 적용하거나 수정합니다. **제목** 및 **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다.

표 7-22. 보안 위험 알림용 토큰 변수

변수	설명
바이러스/악성 프로그램 탐지	

변수	설명
%v	바이러스/악성 프로그램 이름
%s	바이러스/악성 프로그램에 감염된 엔드포인트
%i	엔드포인트의 IP 주소
%c	엔드포인트의 MAC 주소
%m	엔드포인트의 도메인
%p	바이러스/악성 프로그램의 위치
%y	바이러스/악성 프로그램 발견 날짜 및 시간
%e	바이러스 검색 엔진 버전
%r	바이러스 패턴 버전
%a	보안 위험에 대해 수행한 조치
%n	감염된 엔드포인트에 로그온한 사용자 이름
스파이웨어/그레이웨어 탐지	
%s	스파이웨어/그레이웨어가 탐지된 엔드포인트
%i	엔드포인트의 IP 주소
%m	엔드포인트의 도메인
%y	스파이웨어/그레이웨어 발견 날짜 및 시간
%n	발견 당시 엔드포인트에 로그온한 사용자 이름
%T	스파이웨어/그레이웨어 및 검색 결과

4. **SNMP 트랩** 탭에서 다음을 수행합니다.

   a. **바이러스/악성 프로그램 탐지** 및 **스파이웨어/그레이웨어 탐지** 섹션으로 이동합니다.

   b. **SNMP 트랩을 통한 알림 사용**을 선택합니다.

   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 다음 표의 토큰 변수를 사용하여 데이터를 표시할 수 있습니다.

표 7-23. 보안 위험 알림용 토큰 변수

변수	설명
바이러스/악성 프로그램 탐지	
%v	바이러스/악성 프로그램 이름
%s	바이러스/악성 프로그램에 감염된 엔드포인트
%i	엔드포인트의 IP 주소
%c	엔드포인트의 MAC 주소
%m	엔드포인트의 도메인
%p	바이러스/악성 프로그램의 위치
%y	바이러스/악성 프로그램 발견 날짜 및 시간
%e	바이러스 검색 엔진 버전
%r	바이러스 패턴 버전
%a	보안 위험에 대해 수행한 조치
%n	감염된 엔드포인트에 로그온한 사용자 이름
스파이웨어/그레이웨어 탐지	
%s	스파이웨어/그레이웨어가 탐지된 엔드포인트
%i	엔드포인트의 IP 주소
%m	엔드포인트의 도메인
%y	스파이웨어/그레이웨어 발견 날짜 및 시간
%n	발견 당시 엔드포인트에 로그온한 사용자 이름
%T	스파이웨어/그레이웨어 및 검색 결과
%v	스파이웨어/그레이웨어 이름
%a	보안 위험에 대해 수행한 조치

5. **NT 이벤트 로그** 탭에서 다음을 수행합니다.

a. **바이러스/악성 프로그램 탐지** 및 **스파이웨어/그레이웨어 탐지** 섹션으로 이동합니다.

b. **NT 이벤트 로그를 통한 알림 사용**을 선택합니다.

c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 다음 표의 토큰 변수를 사용하여 데이터를 표시할 수 있습니다.

표 7-24. 보안 위험 알림용 토큰 변수

변수	설명
바이러스/악성 프로그램 탐지	
%v	바이러스/악성 프로그램 이름
%s	바이러스/악성 프로그램에 감염된 엔드포인트
%i	엔드포인트의 IP 주소
%c	엔드포인트의 MAC 주소
%m	엔드포인트의 도메인
%p	바이러스/악성 프로그램의 위치
%y	바이러스/악성 프로그램 발견 날짜 및 시간
%e	바이러스 검색 엔진 버전
%r	바이러스 패턴 버전
%a	보안 위험에 대해 수행한 조치
%n	감염된 엔드포인트에 로그온한 사용자 이름
스파이웨어/그레이웨어 탐지	
%s	스파이웨어/그레이웨어가 탐지된 엔드포인트
%i	엔드포인트의 IP 주소
%m	엔드포인트의 도메인
%y	스파이웨어/그레이웨어 발견 날짜 및 시간
%n	발견 당시 엔드포인트에 로그온한 사용자 이름

변수	설명
%T	스파이웨어/그레이웨어 및 검색 결과
%v	스파이웨어/그레이웨어 이름
%a	보안 위험에 대해 수행한 조치

6. **저장**을 클릭합니다.

OfficeScan 에이전트 사용자를 위한 보안 위험 알림

OfficeScan에서는 다음과 같은 경우 OfficeScan 에이전트 엔드포인트에 알림 메시지를 표시할 수 있습니다.

- 실시간 검색 및 예약 검색에서 바이러스/악성 프로그램 및 스파이웨어/그레이웨어가 발견된 후 즉시. 알림 메시지를 사용하고 선택적으로 해당 내용을 수정합니다.
- 감염된 파일 치료를 마치려면 에이전트 엔드포인트를 다시 시작해야 하는 경우. 실시간 검색의 경우, 특정 보안 위험이 검색된 후에 메시지가 표시됩니다. 수동 검색, 예약 검색 및 지금 검색의 경우에는 OfficeScan에서 모든 검색 대상의 검색을 완료한 후 해당 메시지가 단 한 번 표시됩니다.

표 7-25. 보안 위험 에이전트 알림 유형

유형	참조
바이러스/악성 프로그램	바이러스/악성 프로그램 알림 구성 페이지 7-87
스파이웨어/그레이웨어	스파이웨어/그레이웨어 알림 구성 페이지 7-87
방화벽 위반	방화벽 알림 메시지 내용 수정 페이지 13-27
웹 검증 위반	웹 위협 알림 수정 페이지 12-14
장치 제어 위반	장치 제어 알림 수정 페이지 10-18
동작 모니터링 정책 위반	알림 메시지 내용 수정 페이지 9-16

유형	참조
디지털 자산 전송	에이전트에 대한 데이터 손실 방지 알림 구성 페이지 11-55
C&C 콜백	웹 위협 알림 수정 페이지 12-14

사용자에게 발견된 바이러스/악성 프로그램 및 스파이웨어/그레이웨어 알림

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **검색 설정** > **실시간 검색 설정** 또는 **설정** > **검색 설정** > **예약 검색 설정**을 클릭합니다.
4. **조치** 탭을 클릭합니다.
5. 다음 옵션을 선택합니다.
   - **바이러스/악성 프로그램이 발견될 경우 에이전트 엔드포인트에 알림 메시지 표시**
   - **가능한 바이러스/악성 프로그램이 발견될 경우 에이전트 엔드포인트에 알림 메시지 표시**
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

바이러스/악성 프로그램 알림 구성

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 **바이러스/악성 프로그램**을 선택합니다.
3. 탐지 설정을 구성합니다.
   a. 모든 바이러스/악성 프로그램 관련 이벤트에 대한 하나의 알림을 표시하거나 다음 심각도 수준에 따라 별도의 알림을 표시하도록 선택합니다.
      - **높음**: OfficeScan 에이전트가 치명적인 악성 프로그램을 처리할 수 없습니다.
      - **보통**: OfficeScan 에이전트가 악성 프로그램을 처리할 수 없습니다.
      - **낮음**: OfficeScan 에이전트가 모든 위협을 해결할 수 있습니다.
   b. 기본 메시지를 적용하거나 수정합니다.
4. **저장**을 클릭합니다.

스파이웨어/그레이웨어 알림 구성

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 **스파이웨어/그레이웨어**를 선택합니다.
3. 기본 메시지를 적용하거나 수정합니다.
4. **저장**을 클릭합니다.

감염된 파일 치료를 마치려면 다시 시작해야 한다고 에이전트에 알리기

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭하고 **다시 시작 알림** 섹션으로 이동합니다.
5. **감염된 파일 치료를 마치기 위해 엔드포인트를 다시 시작해야 하는 경우 알림 메시지 표시**를 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

보안 위험 로그

OfficeScan이 바이러스/악성 프로그램 또는 스파이웨어/그레이웨어를 발견한 경우 및 스파이웨어/그레이웨어를 복원한 경우 로그를 생성합니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

바이러스/악성 프로그램 로그 보기

OfficeScan 에이전트에서 바이러스 및 악성 프로그램을 발견한 경우 로그를 생성하여 서버에 전송합니다.

절차

1. 다음 중 하나로 이동합니다.
   - **로그** > **에이전트** > **보안 위험**
   - **에이전트** > **에이전트 관리**
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **바이러스/악성 프로그램 로그** 또는 **로그 보기** > **바이러스/악성 프로그램 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.
   - 바이러스/악성 프로그램 발견 날짜 및 시간
   - 엔드포인트
   - 보안 위협
   - 감염 근원지
   - 감염된 파일/개체
   - 파일 경로
   - 감염 채널
   - 바이러스/악성 프로그램을 탐지한 검색 유형
   - 검색 결과

참고

검색 결과에 대한 자세한 내용은 바이러스/악성 프로그램 검색 결과 페이지 7-90를 참조하십시오.

- IP 주소
- MAC 주소
- 로그 세부 정보(세부 정보를 보려면 **보기**를 클릭합니다.)

6. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

   CSV 파일에는 다음 정보가 포함됩니다.

   - 로그의 모든 정보
   - 발견 당시 엔드포인트에 로그온된 사용자 이름

바이러스/악성 프로그램 검색 결과

다음 검색 결과가 바이러스/악성 프로그램 로그에 표시됩니다.

표 7-26. 검색 결과

결과	설명
삭제됨	• 첫 번째 조치는 "삭제"이며 감염된 파일이 삭제되었습니다. • 첫 번째 조치는 "치료"이지만 치료에 실패했습니다. 두 번째 조치는 "삭제"이며 감염된 파일이 삭제되었습니다.
격리 보관됨	• 첫 번째 조치는 "격리 보관"이며 감염된 파일이 격리 보관되었습니다. • 첫 번째 조치는 "치료"이지만 치료에 실패했습니다. 두 번째 조치는 "격리 보관"이며 감염된 파일이 격리 보관되었습니다.
치료됨	감염된 파일이 치료되었습니다.
파일명 변경됨	• 첫 번째 조치는 "파일명 변경"이며 감염된 파일의 이름이 변경되었습니다.

결과	설명
	• 첫 번째 조치는 “치료”이지만 치료에 실패했습니다. 두 번째 조치는 “파일명 변경”이며 감염된 파일의 이름이 변경되었습니다.
액세스가 거부됨	• 첫 번째 조치는 “액세스 거부”이며 사용자가 감염된 파일을 열려고 액세스할 때 액세스가 거부되었습니다. • 첫 번째 조치는 “치료”이지만 치료에 실패했습니다. 두 번째 조치는 “액세스 거부”이며 사용자가 감염된 파일을 열려고 액세스할 때 액세스가 거부되었습니다. • 실시간 검색 도중 가능성이 있는 바이러스/악성 프로그램이 탐지되었습니다. • 실시간 검색에서는 검색 조치가 “치료”(첫 번째 조치) 및 “격리 보관”(두 번째 조치)인 경우에도 부트 바이러스에 감염된 파일에 대한 액세스를 거부할 수 있습니다. 이는 부트 바이러스를 치료하려고 하면 감염된 엔드포인트의 MBR(Master Boot Record)이 손상될 수 있기 때문입니다. OfficeScan에서 파일을 치료하거나 격리 보관하도록 수동 검색을 실행합니다.
그대로 둠	• 첫 번째 조치는 “그대로 두기”이므로 OfficeScan은 감염된 파일에 대해 어떠한 조치도 취하지 않습니다. • 첫 번째 조치는 “치료”이지만 치료에 실패했습니다. 두 번째 조치는 “그대로 두기”이므로 OfficeScan은 감염된 파일에 대해 어떠한 조치도 취하지 않습니다.
잠재적인 보안 위험 통과	수동 검색, 예약 검색 및 지금 검색 도중 OfficeScan이 "가능성이 있는 바이러스/악성 프로그램"을 발견하면 이 검색 결과만 표시됩니다. 가능성이 있는 바이러스/악성 프로그램에 대한 자세한 내용을 알아보거나 분석을 위해 의심스러운 파일을 Trend Micro에 제출하는 방법에 대해서는 Trend Micro 온라인 바이러스 백과사전에서 다음 페이지를 참조하십시오. http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=POSSIBLE_VIRUS&VSect=Sn
파일을 치료하거나 격리 보관할 수 없습니다	“치료”가 첫 번째 조치입니다. “격리 보관”이 두 번째 조치이지만 두 조치가 모두 실패했습니다. 솔루션: 파일을 격리 보관할 수 없습니다/파일명을 변경할 수 없습니다 페이지 7-92를 참조하십시오.

결과	설명
파일을 치료하거나 삭제할 수 없습니다	"치료"가 첫 번째 조치입니다. "삭제"가 두 번째 조치이지만 두 조치가 모두 실패했습니다. 솔루션: 파일을 삭제할 수 없습니다 페이지 7-92를 참조하십시오.
파일을 치료하거나 파일의 이름을 변경할 수 없습니다	"치료"가 첫 번째 조치입니다. "파일명 변경"이 두 번째 조치이지만 두 조치가 모두 실패했습니다. 솔루션: 파일을 격리 보관할 수 없습니다/파일명을 변경할 수 없습니다 페이지 7-92를 참조하십시오.
파일을 격리 보관할 수 없습니다./파일명을 변경할 수 없습니다	설명 1 다른 응용 프로그램에서 감염된 파일을 잠갔거나, 감염된 파일이 실행 중이거나, CD에 있을 수 있습니다. OfficeScan에서는 응용 프로그램에서 파일을 잠금 해제하거나 파일이 실행된 후에 파일을 격리 보관하고 파일명을 변경합니다. 솔루션 감염된 파일이 CD에 있는 경우, 네트워크의 다른 엔드포인트가 바이러스에 감염될 수 있으므로 CD를 사용하지 않도록 합니다.
	설명 2 감염된 파일이 에이전트 엔드포인트의 임시 인터넷 파일 폴더에 있습니다. 사용자가 검색하는 동안 엔드포인트에서 파일을 다운로드하므로 웹 브라우저가 감염된 파일을 잠갔을 수 있습니다. 웹 브라우저가 파일을 잠금 해제하면 OfficeScan에서 파일을 격리 보관/파일명을 변경합니다. 솔루션: 없음
파일을 삭제할 수 없습니다	설명 1 감염된 파일이 압축 파일에 포함되어 있을 수 있으며, **보안 설정** 탭의 **에이전트** > **글로벌 에이전트 설정**에서 **압축 파일 내에서 감염된 파일 치료/삭제** 설정을 사용하지 않도록 설정했을 수 있습니다. 솔루션 **압축 파일 내에서 감염된 파일 치료/삭제** 옵션을 사용하도록 설정합니다. 이 옵션을 선택하면 OfficeScan은 압축 파일의 압축을 풀고, 압축 파일 내의 감염된 파일을 치료/삭제한 후 파일을 다시 압축합니다.

결과	설명
	참고 이 설정을 사용하면 검색 도중 엔드포인트 리소스 사용이 증가할 수 있으며, 검색 완료 시간이 더 오래 걸릴 수 있습니다.
	설명 2 다른 응용 프로그램에서 감염된 파일을 잠갔거나, 감염된 파일이 실행 중이거나, CD에 있을 수 있습니다. OfficeScan에서는 응용 프로그램에서 파일을 잠금 해제하거나 파일이 실행된 후에 파일을 삭제합니다. 솔루션 감염된 파일이 CD에 있는 경우, 네트워크의 다른 엔드포인트가 바이러스에 감염될 수 있으므로 CD를 사용하지 않도록 합니다.
	설명 3 감염된 파일이 OfficeScan 에이전트 엔드포인트의 임시 인터넷 파일 폴더에 있습니다. 사용자가 검색하는 동안 엔드포인트에서 파일을 다운로드하므로 웹 브라우저가 감염된 파일을 잠갔을 수 있습니다. 웹 브라우저가 파일을 잠금 해제하면 OfficeScan에서 파일을 삭제합니다. 솔루션: 없음
격리된 파일을 지정된 격리 보관 폴더로 보낼 수 없습니다	OfficeScan이 OfficeScan 에이전트 엔드포인트의 ₩Suspect 폴더에 파일을 격리 보관하는 데 성공했지만 지정된 격리 보관 디렉터리로 파일을 보낼 수 없습니다. 솔루션 어떤 검색 유형(수동 검색, 실시간 검색, 예약 검색 또는 지금 검색)에서 바이러스/악성 프로그램을 발견했는지 확인한 후 **에이전트** > **에이전트 관리 > 설정** > **{검색 유형}** > **조치** 탭에 지정된 격리 보관 디렉터리를 확인합니다. 격리 보관 디렉터리가 OfficeScan 서버 컴퓨터에 있거나 다른 OfficeScan 서버 컴퓨터에 있는 경우 1. 에이전트에서 서버에 연결할 수 있는지 확인합니다. 2. 격리 보관 디렉터리 포맷으로 URL을 사용하는 경우

결과	설명
	a. http:// 뒤에 지정한 엔드포인트 이름이 정확한지 확인합니다. b. 감염된 파일 크기를 확인합니다. **관리** > **설정** > **격리 보관 관리자**에 지정된 최대 파일 크기를 초과하는 경우, 파일에 맞게 설정을 조정합니다. 또한 파일 삭제 등의 다른 조치를 수행할 수 있습니다. c. 격리 보관 디렉터리 폴더의 크기를 확인한 후 **관리** > **설정** > **격리 보관 관리자**에 지정된 폴더 용량을 초과했는지 여부를 확인합니다. 폴더 용량을 조정하거나 격리 보관 디렉터리에서 파일을 수동으로 삭제합니다. 3. UNC 경로를 사용하는 경우, 격리 보관 디렉터리 폴더가 "Everyone" 그룹에 공유되어 있고 이 그룹에 읽기 및 쓰기 권한을 할당했는지 확인합니다. 또한, 격리 보관 디렉터리 폴더가 존재하는지 여부와 UNC 경로가 정확한지 여부를 확인합니다. 격리 보관 디렉터리가 네트워크의 다른 엔드포인트에 있는 경우(이 시나리오의 경우, UNC 경로만 사용할 수 있음) 1. OfficeScan 에이전트가 엔드포인트에 연결할 수 있는지 확인합니다. 2. 격리 보관 디렉터리 폴더가 "Everyone" 그룹에 공유되어 있고, 이 그룹에 읽기 및 쓰기 권한을 할당했는지 확인합니다. 3. 격리 보관 디렉터리 폴더가 존재하는지 여부를 확인합니다. 4. UNC 경로가 정확한지 확인합니다. 격리 보관 디렉터리가 OfficeScan 에이전트 엔드포인트의 다른 디렉터리에 있는 경우(이 시나리오의 경우, 절대 경로만 사용할 수 있음), 격리 보관 디렉터리 폴더가 있는지 확인합니다.
파일을 치료할 수 없습니다	설명 1 감염된 파일이 압축 파일에 포함되어 있을 수 있으며, **보안 설정** 탭의 **에이전트** > **글로벌 에이전트 설정**에서 압축 파일 내에서 감염된 파일 "치료/삭제" 설정을 사용하지 않도록 설정했을 수 있습니다. 솔루션 **압축 파일 내에서 감염된 파일 치료/삭제** 옵션을 사용하도록 설정합니다. 이 옵션을 선택하면 OfficeScan은 압축 파일의 압축을 풀

결과	설명
	고, 압축 파일 내의 감염된 파일을 치료/삭제한 후 파일을 다시 압축합니다. **참고** 이 설정을 사용하면 검색 도중 엔드포인트 리소스 사용이 증가할 수 있으며, 검색 완료 시간이 더 오래 걸릴 수 있습니다.
	설명 2 감염된 파일이 OfficeScan 에이전트 엔드포인트의 임시 인터넷 파일 폴더에 있습니다. 사용자가 검색하는 동안 엔드포인트에서 파일을 다운로드하므로 웹 브라우저가 감염된 파일을 잠갔을 수 있습니다. 웹 브라우저가 파일을 잠금 해제하면 OfficeScan에서 파일을 치료합니다. 솔루션: 없음
	설명 3 파일이 치료 불가능할 수 있습니다. 자세한 내용 및 해결 방법은 치료할 수 없는 파일 페이지 E-15을 참조하십시오.
처리 방법 필요	OfficeScan에서 사용자 개입 없이는 감염된 파일에 대해 구성된 조치를 완료할 수 없습니다. **처리 방법 필요** 열을 마우스로 가리켜 다음 세부 정보를 표시합니다. • "처리 방법 필요 - OfficeScan 도구 상자에 있는 위협 방지 툴킷의 "부트 치료" 도구를 사용하여 이 위협을 제거하는 방법에 대한 세부 정보를 확인하려면 지원 센터에 문의하십시오." • "처리 방법 필요 - OfficeScan 도구 상자에 있는 위협 방지 툴킷 "복구 디스크" 도구를 사용하여 이 위협을 제거하는 방법에 대한 세부 정보를 확인하려면 지원 센터에 문의하십시오." • "처리 방법 필요 - OfficeScan 도구 상자에 있는 위협 방지 툴킷 "루트키트 버스터" 도구를 사용하여 이 위협을 제거하는 방법에 대한 세부 정보를 확인하려면 지원 센터에 문의하십시오." • "처리 방법 필요 - 감염된 에이전트에서 위협이 발견되었습니다. 보안 위협 치료를 완료하려면 엔드포인트를 다시 시작하십시오."

결과	설명
	• "처리 방법 필요 - 엔드포인트에서 탐지된 루트키트 위협 제거를 완료하려면 전체 시스템 검색이 필요합니다."

중앙 격리 보관 복원 로그 보기

악성 프로그램을 치료한 후 OfficeScan 에이전트는 악성 프로그램 데이터를 백업합니다. 데이터가 유해하지 않다고 생각되는 경우 백업 데이터를 복원하도록 온라인 에이전트에 알리십시오. 복원된 악성 프로그램 백업 데이터, 영향받는 엔드포인트 및 복원 결과에 대한 정보를 로그에서 확인할 수 있습니다.

절차

1. **로그** > **에이전트** > **중앙 격리 보관 복원**로 이동합니다.
2. **성공**, **실패** 및 **보류 중** 열에서 OfficeScan이 격리된 데이터를 복원했는지 확인합니다.
3. 각 열의 항목 수 링크를 클릭하여 영향받는 각 엔드포인트에 대한 자세한 내용을 봅니다.

   참고

   실패한 복원의 경우 **중앙 격리 보관 복원 세부 정보** 화면에서 **모두 복원**을 클릭하여 파일 복원을 다시 시도할 수 있습니다.

4. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

스파이웨어/그레이웨어 로그 보기

OfficeScan 에이전트에서 스파이웨어 및 그레이웨어를 발견한 경우 로그를 생성하여 서버에 전송합니다.

절차

1. 다음 중 하나로 이동합니다.
   - **로그** > **에이전트** > **보안 위험**
   - **에이전트** > **에이전트 관리**
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **스파이웨어/그레이웨어 로그** 또는 **로그 보기** > **스파이웨어/그레이웨어 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.
   - 스파이웨어/그레이웨어 발견 날짜 및 시간
   - 영향받는 엔드포인트
   - 스파이웨어/그레이웨어 이름
   - 감염 채널
   - 스파이웨어/그레이웨어를 발견한 검색 유형
   - 스파이웨어/그레이웨어 검색 결과에 대한 세부 정보(검색 조치가 성공적으로 수행되었거나 그렇지 않은 경우).

     자세한 내용은 스파이웨어/그레이웨어 검색 결과 페이지 7-98를 참조하십시오.
   - IP 주소
   - MAC 주소
   - 로그 세부 정보(세부 정보를 보려면 **보기**를 클릭합니다.)
6. 스파이웨어/그레이웨어 승인된 목록에 유해하지 않은 것으로 간주하는 스파이웨어/그레이웨어를 추가합니다.
7. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

CSV 파일에는 다음 정보가 포함됩니다.

- 로그의 모든 정보
- 발견 당시 엔드포인트에 기록된 사용자 이름

스파이웨어/그레이웨어 검색 결과

다음 검색 결과가 스파이웨어/그레이웨어 로그에 표시됩니다.

표 7-27. 첫 번째 수준 스파이웨어/그레이웨어 검색 결과

결과	설명
성공, 조치 필요 없음	검색 조치에 성공한 경우의 첫 번째 수준 결과입니다. 두 번째 수준 결과는 다음과 같을 수 있습니다. • 치료됨 • 액세스가 거부됨
추가 조치 필요	검색 조치에 실패한 경우의 첫 번째 수준 결과입니다. 두 번째 수준의 결과에 다음과 같은 메시지가 하나 이상 포함됩니다. • 그대로 둠 • 치료하기에 스파이웨어/그레이웨어가 안전하지 않습니다. • 스파이웨어/그레이웨어 검색을 수동으로 중지했습니다. 전체 검색을 수행하십시오. • 스파이웨어/그레이웨어가 치료되었습니다. 컴퓨터를 다시 시작해야 합니다. 컴퓨터를 다시 시작하십시오. • 스파이웨어/그레이웨어를 치료할 수 없습니다. • 스파이웨어/그레이웨어 검색 결과를 확인할 수 없습니다. Trend Micro 기술 지원 센터에 문의하십시오.

표 7-28. 두 번째 수준 스파이웨어/그레이웨어 검색 결과

결과	설명	솔루션
치료됨	OfficeScan은 프로세스를 종료하거나 레지스트리, 파일, 쿠키 및 바로 가기를 삭제합니다.	해당 없음
액세스가 거부됨	OfficeScan이 발견된 스파이웨어/그레이웨어 구성 요소에 대한 액세스(복사, 열기)를 거부했습니다.	해당 없음
그대로 둠	OfficeScan은 아무 조치도 취하지 않지만 점검을 위해 스파이웨어/그레이웨어 발견이 기록됩니다.	스파이웨어/그레이웨어 승인된 목록에 안전한 것으로 간주하는 스파이웨어/그레이웨어를 추가합니다.
치료하기에 스파이웨어/그레이웨어가 안전하지 않습니다.	: 이 메시지는 스파이웨어 검색 엔진이 단일 폴더를 치료하려고 하고 다음 기준을 만족하면 표시됩니다. • 치료할 항목이 250MB를 초과합니다. • 운영 체제에서 해당 폴더의 파일을 사용합니다. 정상적인 시스템 작업에 필요한 폴더일 수 있습니다. • 폴더가 루트 디렉터리입니다(예: C: 또는 F:)	지원 센터에 문의하여 도움을 받으십시오.
스파이웨어/그레이웨어 검색을 수동으로 중지했습니다. 전체 검색을 수행하십시오.	사용자가 검색 완료 이전에 검색을 중지했습니다.	수동 검색을 실행하고 검색이 완료될 때까지 기다립니다.
스파이웨어/그레이웨어가 치료되었습니다. 컴퓨터를 다시 시작해야 합니다. 컴퓨터를 다시 시작하십시오.	OfficeScan이 스파이웨어/그레이웨어 구성 요소를 치료했지만 작업을 완료하려면 엔드포인트를 다시 시작해야 합니다.	엔드포인트를 즉시 다시 시작합니다.

결과	설명	솔루션
스파이웨어/그레이웨어를 치료할 수 없습니다.	스파이웨어/그레이웨어가 CD-ROM 또는 네트워크 드라이브에서 발견되었습니다. OfficeScan은 이러한 위치에서 발견된 스파이웨어/그레이웨어를 치료할 수 없습니다.	감염된 파일을 수동으로 제거하십시오.
스파이웨어/그레이웨어 검색 결과를 확인할 수 없습니다. Trend Micro 기술 지원 센터에 문의하십시오.	새 버전의 스파이웨어 검색 엔진에서 OfficeScan이 처리하도록 구성되지 않은 새 검색 결과를 제공합니다.	새 검색 결과를 확인하는 데 도움을 얻으려면 지원 센터에 문의하십시오.

스파이웨어/그레이웨어 복원 로그 보기

스파이웨어/그레이웨어를 치료한 후 OfficeScan 에이전트는 스파이웨어/그레이웨어 데이터를 백업합니다. 데이터가 유해하지 않다고 생각되는 경우 백업 데이터를 복원하도록 온라인 에이전트에 알리십시오. 복원된 스파이웨어/그레이웨어 백업 데이터, 영향받는 엔드포인트 및 복원 결과에 대한 정보는 로그에서 확인할 수 있습니다.

절차

1. **로그** > **에이전트** > **스파이웨어/그레이웨어 복원**로 이동합니다.
2. **결과** 열에서 OfficeScan이 스파이웨어/그레이웨어 데이터를 복원했는지 확인합니다.
3. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

의심스러운 파일 로그 보기

OfficeScan 에이전트에서 의심스러운 파일 목록에 있는 파일을 발견한 경우 로그를 생성하여 서버에 전송합니다.

절차

1. 다음 중 하나로 이동합니다.
   - **로그** > **에이전트** > **보안 위험**
   - **에이전트** > **에이전트 관리**
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **의심스러운 파일 로그** 또는 **로그 보기** > **의심스러운 파일 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.
   - 의심스러운 파일 발견 날짜 및 시간
   - 엔드포인트
   - 도메인
   - 파일의 감염 근원지 SHA-1 해시 값
   - 파일 경로
   - 의심스러운 파일을 탐지한 검색 유형
   - 검색 결과

     참고

     검색 결과에 대한 자세한 내용은 바이러스/악성 프로그램 검색 결과 페이지 7-90를 참조하십시오.
   - IP 주소

검색 작업 로그 보기

수동 검색, 예약 검색 또는 지금 검색 시 OfficeScan 에이전트는 검색에 대한 정보가 포함된 검색 로그를 만듭니다. OfficeScan 서버나 OfficeScan 에이전트 콘솔에 액세스하여 검색 로그를 볼 수 있습니다.

OfficeScan 서버에서 검색 작업 로그를 보려면 다음 위치 중 하나로 이동합니다.

- **로그** > **에이전트** > **보안 위험**로 이동한 후 **로그 보기** > **검색 작업 로그**를 클릭합니다.
- **에이전트** > **에이전트 관리**로 이동한 후 **로그** > **검색 작업 로그**를 클릭합니다.

검색 작업 로그에는 다음 정보가 표시됩니다.

- OfficeScan에서 검색을 시작한 날짜 및 시간
- OfficeScan에서 검색을 중지한 날짜 및 시간
- 검색 상태
  - **완료**: 검색이 정상적으로 완료되었습니다.
  - **중단**: 검색이 완료되기 전에 사용자가 검색을 중지했습니다.
  - **예기치 않게 중지됨**: 사용자, 시스템 또는 예기치 않은 이벤트로 인해 검색이 중단되었습니다. 예를 들어 OfficeScan 실시간 검색 서비스가 예기치 않게 종료되거나 사용자가 에이전트를 강제로 다시 시작했을 수 있습니다.
- 검색 유형
- 검색한 개체 수
- 바이러스/악성 프로그램 감염 탐지 수
- 스파이웨어/그레이웨어 탐지 수
- 스마트 스캔 에이전트 패턴 버전
- 바이러스 패턴 버전

- 스파이웨어/그레이웨어 패턴 버전

보안 위험 비상 발생

보안 위험 비상 발생은 특정 기간 동안 바이러스/악성 프로그램, 스파이웨어/그레이웨어 및 공유 폴더 세션이 특정 임계값을 초과한 경우에 발생합니다. 네트워크에서 비상 발생에 대응하고 이를 저지하는 데에는 다음을 비롯한 몇 가지 방법이 있습니다.

- 네트워크에서 의심스러운 활동을 모니터링하도록 OfficeScan 사용
- 중요한 에이전트 엔드포인트 포트 및 폴더 차단
- 비상 발생 경고 메시지를 에이전트에 보내기
- 감염된 엔드포인트 치료

보안 위험 비상 발생 기준 및 알림

다음 이벤트가 발생한 경우 자신과 다른 OfficeScan 관리자에게 알림을 보내도록 OfficeScan을 구성합니다.

표 7-29. 보안 위험 비상 발생 알림 유형

유형	참조
• 바이러스/악성 프로그램 • 스파이웨어/그레이웨어 • 공유 폴더 세션	보안 위험 비상 발생 기준 및 알림 구성 페이지 7-104
방화벽 위반	방화벽 위반 비상 발생 기준 및 알림 구성 페이지 13-29
C&C 콜백	C&C 콜백 비상 발생 기준 및 알림 구성 페이지 12-19

- 바이러스/악성 프로그램 발생
- 스파이웨어/그레이웨어 발생

- 방화벽 위반 발생
- 공유 폴더 세션 발생

발견 수 및 탐지 기간에 따라 비상 발생을 정의합니다. 탐지 기간 내에 탐지 수가 초과되면 비상 발생이 트리거됩니다.

OfficeScan에서는 사용자 자신과 다른 OfficeScan 관리자에게 비상 발생을 알리는 일련의 기본 알림 메시지를 제공합니다. 요구 사항에 맞게 알림을 수정하고 추가 알림 설정을 구성할 수 있습니다.

참고

OfficeScan에서는 전자 메일, SNMP 트랩 및 Windows NT 이벤트 로그를 통해 보안 위험 비상 발생 알림을 보낼 수 있습니다. 공유 폴더 세션 발생의 경우 OfficeScan에서는 전자 메일을 통해 알림을 보냅니다. OfficeScan에서 이러한 채널을 통해 알림을 보내는 경우에 대한 설정을 구성하십시오. 자세한 내용은 관리자 알림 설정 페이지 14-35를 참조하십시오.

보안 위험 비상 발생 기준 및 알림 구성

절차

1. **관리** > **알림** > **비상 발생**으로 이동합니다.
2. **기준** 탭에서 다음을 수행합니다.
   a. **바이러스/악성 프로그램** 및 **스파이웨어/그레이웨어** 섹션으로 이동합니다.
   b. 고유한 탐지 소스 수를 지정합니다.
   c. 각 보안 위험의 발견 수와 탐지 기간을 지정합니다.

팁

Trend Micro에서는 이 화면에서 기본값을 적용할 것을 권장합니다.

OfficeScan은 10개의 서로 다른 유형의 바이러스/악성 프로그램 탐지 유형이 5시간 내 총 101개의 보안 위험을 보고하면 알림을 보냅니다. 유형과 관

계없이 하나의 에이전트에서 5시간 내 101개의 바이러스/악성 프로그램이 탐지된 경우에도 OfficeScan은 비상 발생 알림을 보냅니다.

3. **기준** 탭에서 다음을 수행합니다.

   a. **공유 폴더 세션** 섹션으로 이동합니다.

   b. **네트워크에서 공유 폴더 세션 모니터링**을 선택합니다.

   c. **기록된 공유 폴더 세션**에서 번호 링크를 클릭하여 공유 폴더가 있는 엔드포인트와 공유 폴더에 액세스하는 엔드포인트를 확인합니다.

   d. 공유 폴더 세션 수와 탐지 기간을 지정합니다.

   공유 폴더 세션 수가 초과되면 OfficeScan에서 알림 메시지를 보냅니다.

4. **전자 메일** 탭에서 다음을 수행합니다.

   a. **바이러스/악성 프로그램 발생**, **스파이웨어/그레이웨어 발생** 및 **공유 폴더 세션 발생** 섹션으로 이동합니다.

   b. **전자 메일을 통한 알림 사용**을 선택합니다.

   c. 전자 메일 받는 사람을 지정합니다.

   d. 기본 전자 메일 제목 및 메시지를 적용하거나 수정합니다. **제목** 및 **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다.

표 7-30. 보안 위험 비상 발생 알림용 토큰 변수

변수	설명
바이러스/악성 프로그램 발생	
%CV	발견된 전체 바이러스/악성 프로그램 수
%CC	바이러스/악성 프로그램이 있는 전체 엔드포인트 수
스파이웨어/그레이웨어 발생	
%CV	발견된 전체 스파이웨어/그레이웨어 수
%CC	스파이웨어/그레이웨어가 있는 전체 엔드포인트 수
공유 폴더 세션 발생	

변수	설명
%S	공유 폴더 세션 수
%T	공유 폴더 세션이 누적된 시간
%M	시간(분)

e. 전자 메일에 포함할 추가 바이러스/악성 프로그램 및 스파이웨어/그레이웨어 정보를 선택합니다. 에이전트/도메인 이름, 보안 위험 이름, 발견 날짜 및 시간, 경로 및 감염된 파일과 검색 결과를 포함할 수 있습니다.

f. 기본 알림 메시지를 그대로 사용하거나 수정하여 사용합니다.

5. **SNMP 트랩** 탭에서 다음을 수행합니다.

   a. **바이러스/악성 프로그램 발생** 및 **스파이웨어/그레이웨어 발생** 섹션으로 이동합니다.

   b. **SNMP 트랩을 통한 알림 사용**을 선택합니다.

   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 7-30 : 보안 위험 비상 발생 알림용 토큰 변수 페이지 7-105를 참조하십시오.

6. **NT 이벤트 로그** 탭에서 다음을 수행합니다.

   a. **바이러스/악성 프로그램 발생** 및 **스파이웨어/그레이웨어 발생** 섹션으로 이동합니다.

   b. **NT 이벤트 로그를 통한 알림 사용**을 선택합니다.

   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 7-30 : 보안 위험 비상 발생 알림용 토큰 변수 페이지 7-105를 참조하십시오.

7. **저장**을 클릭합니다.

보안 위험 바이러스 사전 방역 구성

비상이 발생하면, 비상 발생에 대응하고 저지하기 위해 바이러스 사전 방역 조치를 실행합니다. 구성이 올바르지 않으면 예상치 않은 네트워크 문제가 야기될 수 있기 때문에 주의해서 예방 설정을 구성합니다.

절차

1. **에이전트** > **바이러스 사전 방역**으로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **바이러스 사전 방역 시작**을 클릭합니다.
4. 다음 바이러스 사전 방역 정책 중 하나를 클릭한 다음 정책에 대한 설정을 구성합니다.
   - 공유 폴더에 대한 액세스 제한/금지 페이지 7-109
   - 취약한 포트 차단 페이지 7-110
   - 파일 및 폴더 쓰기 금지 페이지 7-111
   - 압축된 실행 파일에 대한 액세스 거부 페이지 7-114
   - 악성 프로그램 프로세스/파일에 대한 상호 배제 처리 만들기 페이지 7-112
5. 적용할 정책을 선택합니다.
6. 바이러스 사전 방역이 적용되는 기간(시간)을 선택합니다. 기본값은 48시간입니다. 바이러스 사전 방역 기간이 만료되기 전에 네트워크 설정을 수동으로 복원할 수 있습니다.

경고!

바이러스 사전 방역을 무기한으로 적용할 수 없습니다. 특정 파일, 폴더 또는 포트에 대한 액세스를 무기한 차단 또는 거부하려면, OfficeScan을 사용하는 대신 엔드포인트 및 네트워크 설정을 직접 수정합니다.

7. 기본 에이전트 알림 메시지를 그대로 사용하거나 수정하여 사용합니다.

> **참고**
>
> 비상 발생 시 알림을 보내도록 OfficeScan을 구성하려면 **관리** > **알림** > **비상 발생**으로 이동합니다.

8. **바이러스 사전 방역 시작**을 클릭합니다.

   선택한 바이러스 사전 방역 조치가 새로운 창에 표시됩니다.

9. 바이러스 사전 방역 에이전트 트리로 돌아와서 **바이러스 사전 방역** 열을 선택합니다.

   바이러스 사전 방역 조치를 적용 중인 엔드포인트에 확인 표시가 나타납니다.

OfficeScan은 시스템 이벤트 로그에 다음 이벤트를 기록합니다.

- 서버 이벤트(바이러스 사전 방역 시작 및 바이러스 사전 방역을 사용하도록 에이전트에 알림)
- OfficeScan 에이전트 이벤트(바이러스 사전 방역 사용)

바이러스 사전 방역 정책

바이러스 발생이 나타나면 다음과 같은 정책을 적용합니다.

- 공유 폴더에 대한 액세스 제한/금지 페이지 7-109
- 취약한 포트 차단 페이지 7-110
- 파일 및 폴더 쓰기 금지 페이지 7-111
- 압축된 실행 파일에 대한 액세스 거부 페이지 7-114
- 악성 프로그램 프로세스/파일에 대한 상호 배제 처리 만들기 페이지 7-112

공유 폴더에 대한 액세스 제한/금지

비상 발생 시 네트워크의 공유 폴더에 대한 액세스를 제한 또는 거부하여 보안 위험이 공유 폴더를 통해 확산되는 것을 방지합니다.

이 정책이 적용되면, 사용자가 폴더를 공유할 수 있지만 해당 정책이 새로 공유된 폴더에 적용되지는 않습니다. 그러므로 비상 발생 시 폴더를 공유하지 않거나 새로 공유된 폴더에 정책을 적용하기 위해 다시 정책을 배포하도록 사용자에게 알립니다.

절차

1. **에이전트** > **바이러스 사전 방역**으로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **바이러스 사전 방역 시작**을 클릭합니다.
4. **공유 폴더에 대한 액세스 거부/금지**를 클릭합니다.
5. 다음 옵션에서 선택합니다.
   - **읽기 전용 액세스 허용**: 공유 폴더에 대한 액세스 제한
   - **액세스 거부**

   참고

   읽기 액세스 전용 설정은 이미 전체 액세스 거부로 구성된 공유 폴더에는 적용되지 않습니다.
6. **저장**을 클릭합니다.

   바이러스 사전 방역 설정 화면이 다시 표시됩니다.
7. **바이러스 사전 방역 시작**을 클릭합니다.

   선택한 바이러스 사전 방역 조치가 새로운 창에 표시됩니다.

취약한 포트 차단

비상 발생 시, 바이러스/악성 프로그램이 OfficeScan 에이전트 엔드포인트에 액세스하는 데 사용할 수 있는 취약한 포트를 차단합니다.

경고!

바이러스 사전 방역 설정은 신중하게 구성하십시오. 사용 중인 포트를 차단하면 해당 포트를 사용하는 네트워크 서비스를 사용할 수 없게 됩니다. 예를 들어 트러스트된 포트를 차단하면 OfficeScan이 바이러스 비상 발생 기간 동안 에이전트와 통신할 수 없습니다.

절차

1. **에이전트** > **바이러스 사전 방역**으로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **바이러스 사전 방역 시작**을 클릭합니다.
4. **포트 차단**을 클릭합니다.
5. **트러스트된 포트 차단**. 여부를 선택합니다.
6. **차단된 포트** 열 아래에서 차단할 포트를 선택합니다.
   a. 테이블에 포트가 없는 경우 **추가**를 클릭합니다. 열리는 화면에서 차단할 포트를 선택하고 **저장**을 클릭합니다.
      - **모든 포트(ICMP 포함)**: 트러스트된 포트를 제외한 모든 포트를 차단합니다. 트러스트된 포트도 차단하려면 이전 화면에서 트러스트된 포트 차단 확인란을 선택합니다.
      - **지정된 포트**
        - **공통으로 사용하는 포트**: OfficeScan에서 포트 차단 설정을 저장할 하나 이상의 포트 번호를 선택합니다.
        - **트로이 목마 프로그램에 일반적으로 사용되는 포트**: 트로이 목마 프로그램에 의해 일반적으로 사용되는 포트를 차단합

니다. 자세한 내용은 트로이 목마 포트 페이지 E-13를 참조하십시오.

- **1에서 65535 사이의 포트 또는 포트 범위**: 차단할 트래픽 방향과 지정한 포트를 차단하는 이유와 같은 설명을 선택적으로 지정합니다.
- **Ping 프로토콜(ICMP 거부)**: Ping 요청과 같은 ICMP 패킷을 차단하려는 경우에만 클릭합니다.

b. 차단된 포트에 대한 설정을 편집하려면 포트 번호를 클릭합니다.

c. 열리는 화면에서 설정을 수정하고 **저장**을 클릭합니다.

d. 목록에서 포트를 제거하려면 포트 번호 옆의 확인란을 선택하고 **삭제**를 클릭합니다.

7. **저장**을 클릭합니다.

   바이러스 사전 방역 설정 화면이 다시 표시됩니다.

8. **바이러스 사전 방역 시작**을 클릭합니다.

   선택한 바이러스 사전 방역 조치가 새로운 창에 표시됩니다.

파일 및 폴더 쓰기 금지

바이러스/악성 프로그램은 호스트 엔드포인트에 있는 파일과 폴더를 수정 또는 삭제할 수 있습니다. 비상 발생 시에 바이러스/악성 프로그램이 OfficeScan 에이전트 엔드포인트에 있는 파일 및 폴더를 수정하거나 삭제하지 못하도록 OfficeScan을 구성합니다.

경고!

OfficeScan에서는 매핑된 네트워크 드라이브에 대한 쓰기 액세스 거부를 지원하지 않습니다.

절차

1. **에이전트** > **바이러스 사전 방역**으로 이동합니다.

2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **바이러스 사전 방역 시작**을 클릭합니다.
4. **파일 및 폴더 쓰기 금지**를 클릭합니다.
5. 디렉터리 경로를 입력합니다. 보호할 디렉터리 경로를 입력하고 나면 **추가**를 클릭합니다.

   참고

   디렉터리에 대해 가상 경로가 아닌 절대 경로를 입력합니다.

6. 보호된 디렉터리에서 보호할 파일을 지정합니다. 모든 파일을 선택하거나 특정 파일 확장자를 기반으로 파일을 선택합니다. 파일 확장자의 경우, 목록에 없는 확장자를 지정하려면 텍스트 상자에 입력한 다음 **추가**를 클릭합니다.
7. 특정 파일을 보호하려면 **보호할 파일**에서 파일의 전체 이름을 입력하고 **추가**를 클릭합니다.
8. **저장**을 클릭합니다.

   바이러스 사전 방역 설정 화면이 다시 표시됩니다.
9. **바이러스 사전 방역 시작**을 클릭합니다.

   선택한 바이러스 사전 방역 조치가 새로운 창에 표시됩니다.

악성 프로그램 프로세스/파일에 대한 상호 배제 처리 만들기

위협이 시스템을 감염시키고 시스템 전체에 전파되기 위해 필요로 하는 리소스를 재정의하여 상호 배제(Mutex) 프로세스를 활용하는 보안 위협을 차단하도록 바이러스 사전 방역을 구성할 수 있습니다. 바이러스 사전 방역에서는 알려진 악성 프로그램과 관련이 있는 파일 및 프로세스에 대해 상호 배제를 만들어 악성 프로그램이 이러한 리소스에 액세스하지 못하도록 차단합니다.

팁

악성 프로그램 위협에 대한 해결 방법을 구현할 수 있을 때까지 이러한 배제를 유지하는 것이 좋습니다. 비상 발생 중에 차단해야 하는 올바른 Mutex 이름을 확인하려면 지원 센터에 문의하십시오.

참고

상호 배제 처리는 32비트 플랫폼에서만 지원되며, 무단 변경 방지 서비스가 있어야 사용할 수 있습니다.

절차

1. **에이전트** > **바이러스 사전 방역**으로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **바이러스 사전 방역 시작**을 클릭합니다.
4. **악성 프로그램 프로세스/파일에 대한 상호 배제(Mutex) 처리 만들기**를 클릭합니다.
5. 제공된 입력란에 보호할 상호 배제(Mutex) 이름을 입력합니다.

   + 및 - 단추를 사용하여 목록에서 상호 배제(Mutex) 이름을 추가하거나 제거합니다.

   참고

   바이러스 사전 방역에서는 최대 6개의 상호 배제(Mutex) 위협에 대한 상호 배제 처리를 지원합니다.
6. **저장**을 클릭합니다.

   바이러스 사전 방역 설정 화면이 다시 표시됩니다.
7. **바이러스 사전 방역 시작**을 클릭합니다.

   선택한 바이러스 사전 방역 조치가 새로운 창에 표시됩니다.

압축된 실행 파일에 대한 액세스 거부

비상 발생 시 압축된 실행 파일에 대한 액세스를 거부하면 이러한 파일에 포함될 수 있는 보안 위험이 네트워크를 통해 확산되지 않도록 방지할 수 있습니다. 지원되는 패커 실행 프로그램에서 생성된 신뢰할 수 있는 파일에 대한 액세스는 허용할 수 있습니다.

절차

1. **에이전트** > **바이러스 사전 방역**으로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **바이러스 사전 방역 시작**을 클릭합니다.
4. **압축된 실행 파일에 대한 액세스 거부**를 클릭합니다.
5. 지원되는 패커 실행 프로그램 목록에서 선택하고 **추가**를 클릭하여 이러한 패커 프로그램에서 만들어진 압축된 실행 파일에 대한 액세스를 허용합니다.

   참고

   실행 가능한 패커 목록에 있는 패커 프로그램으로 만든 압축된 파일의 사용만 허용할 수 있습니다. 바이러스 사전 방역 기능은 다른 압축 실행 파일 형식에 대한 액세스는 모두 거부합니다.

6. **저장**을 클릭합니다.

   바이러스 사전 방역 설정 화면이 다시 표시됩니다.

7. **바이러스 사전 방역 시작**을 클릭합니다.

   선택한 바이러스 사전 방역 조치가 새로운 창에 표시됩니다.

바이러스 사전 방역 사용 안 함

비상 발생이 저지되었고 감염된 모든 파일이 이미 치료되었거나 격리 보관되었다는 확신이 들면, OfficeScan은 바이러스 사전 방역을 사용하지 않도록 설정하여 네트워크 설정을 정상으로 복원합니다.

절차

1. **에이전트** > **바이러스 사전 방역**으로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정 복원**을 클릭합니다.
4. 사용자에게 비상 발생 상황이 종료되었음을 알리려면 **원래 설정을 복원한 후 사용자에게 알림**을 선택합니다.
5. 기본 에이전트 알림 메시지를 그대로 사용하거나 수정하여 사용합니다.
6. **설정 복원**을 클릭합니다.

참고

네트워크 설정을 수동으로 복원하지 않을 경우 OfficeScan에서는 **바이러스 사전 방역 설정** 화면의 **네트워크 설정을 __시간 후 자동으로 정상 복원**에 지정된 시간이 경과하면 이러한 설정을 자동으로 복원합니다. 기본 설정은 48시간입니다.

OfficeScan은 시스템 이벤트 로그에 다음 이벤트를 기록합니다.

- 서버 이벤트(바이러스 사전 방역 시작 및 바이러스 사전 방역을 사용하도록 OfficeScan 에이전트에 알림)
- OfficeScan 에이전트 이벤트(바이러스 사전 방역 사용)

7. 바이러스 사전 방역을 사용하지 않도록 설정한 후 네트워크로 연결된 엔드포인트에서 보안 위험을 검사하여 비상 발생이 저지되었는지 확인합니다.

장 8

알 수 없는 위협으로부터 보호

이 장에서는 네트워크 침투를 시도하는 알 수 없는 위협으로부터 엔드포인트를 보호하는 방법에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- 머신러닝 페이지 8-2
- 의심스러운 연결 서비스 페이지 8-5
- 샘플 제출 페이지 8-8
- 알 수 없는 위협 로그 페이지 8-10

머신러닝

Trend Micro 머신러닝은 위협 정보를 상호 연결하고 세부적인 파일 분석을 수행하는 고급 시스템 학습 기술을 사용하여 디지털 DNA 지문, API 매핑 및 기타 파일 기능을 통해 새로 등장하는 알 수 없는 보안 위험을 탐지합니다. 또한 머신러닝은 알 수 없거나 일반적이지 않은 프로세스에 대한 동작 분석을 수행하여 새로운 위협 또는 알 수 없는 위협이 네트워크 감염을 시도하는지 여부를 확인합니다.

머신러닝은 식별되지 않은 위협이나 제로 데이 공격으로부터 환경을 보호할 수 있는 강력한 도구입니다.

탐지 유형	설명
파일	OfficeScan이 알 수 없는 또는 일반적이지 않은 파일을 탐지하면 ATSE(고급 위협 검색 엔진)로 파일을 검색하여 파일의 특성을 추출한 다음 해당 보고서를 Trend Micro 스마트 보호 네트워크에서 호스팅되는 머신러닝 엔진으로 보냅니다. 머신러닝에서는 악성 프로그램 모델링을 사용하여 해당 샘플을 악성 프로그램 모델과 비교하고, 가능성 점수를 할당하고, 파일에 포함되어 있는 악성 프로그램 유형을 판별합니다. 머신러닝 구성 방법에 따라 OfficeScan은 감염된 파일에 대한 "격리 보관"을 시도하여 위협이 네트워크 전반에 계속 확산되지 않도록 차단합니다.
프로세스	OfficeScan이 알 수 없는 또는 일반적이지 않은 프로세스를 탐지하면 상황별 정보 엔진을 사용하여 프로세스를 모니터링한 다음 동작 보고서를 머신러닝 엔진으로 보냅니다. 머신러닝에서는 악성 프로그램의 동작 모델링을 사용하여 해당 프로세스의 동작을 모델과 비교하고, 가능성 점수를 할당하고, 프로세스에 의해 실행되고 있는 악성 프로그램 유형을 판별합니다. 예측 학습 시스템 구성 방법에 따라 OfficeScan은 감염된 프로세스를 "종료"하고 프로세스를 실행한 파일에 대한 치료를 시도할 수 있습니다.

머신러닝 설정 구성

참고

머신러닝을 사용하려면 다음 서비스를 사용하도록 설정해야 합니다.

- 무단 변경 방지
- 고급 보호 서비스

자세한 내용은 웹 콘솔에서 에이전트 서비스 사용 또는 사용 안 함 페이지 15-8를 참조하십시오.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **머신러닝 설정**을 클릭합니다.

   머신러닝 설정 화면이 나타납니다.
4. **머신러닝 사용**을 선택합니다.
5. **탐지 설정**에서 탐지의 유형 그리고 머신러닝에서 수행할 관련 조치를 선택합니다.

탐지 유형	처리 방법
파일	• **격리 보관**: 머신러닝 분석을 기반으로 악성 프로그램 관련 특성을 보이는 파일을 자동으로 격리 보관하려면 선택합니다. • **기록만**: 위협에 대한 추가적인 내부 조사를 위해 알 수 없는 파일을 검색하고 머신러닝 분석을 기록하려면 선택합니다.

탐지 유형	처리 방법
프로세스	• **종료**: 머신러닝 분석을 기반으로 악성 프로그램 관련 동작을 보이는 프로세스를 자동으로 종료하려면 선택합니다. **중요** 머신러닝에서 악성 프로세스를 실행한 파일에 대한 치료를 시도합니다. 치료 조치가 성공하지 못하는 경우 OfficeScan은 감염된 파일을 격리 보관합니다. • **기록만**: 위협에 대한 추가적인 내부 조사를 위해 알 수 없는 프로세스를 검색하고 머신러닝 분석을 기록하려면 선택합니다.

6. **예외**에서, 글로벌 머신러닝 파일 예외를 구성하여 모든 에이전트가 파일을 악성으로 탐지하는 것을 방지합니다.

   a. **파일 해시 추가**를 클릭합니다.

      예외 목록에 파일 추가 화면이 나타납니다.

   b. 검색에서 제외하려면 파일에 SHA-1 해시 값을 지정합니다.

   c. 필요한 경우 예외 이유와 관련된 메모를 제공하거나 해시 값과 연관된 파일 이름을 설명합니다.

   d. **추가**를 클릭합니다.

      OfficeScan이 파일 해시를 예외 목록에 추가합니다.

7. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   • **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

   • **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

의심스러운 연결 서비스

의심스러운 연결 서비스에서는 사용자 정의 및 글로벌 IP C&C 목록을 관리하고 엔드포인트와 잠재적인 C&C 서버의 연결 동작을 모니터링합니다.

- 사용자 정의된, 승인된 IP 목록과 차단된 IP 목록을 사용하면 엔드포인트에서 특정 IP 주소에 대한 액세스 여부를 추가로 제어할 수 있습니다. 글로벌 C&C IP 목록으로 차단되는 주소에 대한 액세스를 허용하려는 경우나 보안 위험을 야기할 수 있는 주소에 대한 액세스를 차단하려는 경우에 이 목록을 구성하십시오.

  자세한 내용은 글로벌 사용자 정의 IP 목록 설정 구성 페이지 8-6를 참조하십시오.

- 글로벌 C&C IP 목록은 NCIE(네트워크 콘텐츠 검사 엔진)와 함께 작동하여 Trend Micro에서 확인한 C&C 서버와의 네트워크 연결을 탐지합니다. NCIE는 네트워크 채널을 통한 C&C 서버 연결을 탐지합니다. 의심스러운 연결 서비스는 글로벌 C&C IP 목록에 있는 서버에 대한 연결 정보를 모두 기록하여 평가합니다.

  글로벌 C&C IP 목록을 사용하도록 설정하는 방법에 대한 자세한 내용은 의심스러운 연결 설정 구성 페이지 8-7을 참조하십시오.

- 네트워크 패킷에 대한 관련 규칙 패턴 일치를 통해 엔드포인트에서 악성 프로그램을 탐지한 경우 의심스러운 연결 서비스는 연결 동작을 추가로 조사하여 C&C 콜백이 발생했는지 확인합니다. C&C 콜백을 탐지한 후에 의심스러운 연결 서비스는 GeneriClean 기술을 사용하여 연결 소스를 차단하고 치료할 수 있습니다.

  의심스러운 연결 서비스 구성에 대한 자세한 내용은 의심스러운 연결 설정 구성 페이지 8-7을 참조하십시오.

  GeneriClean에 대한 자세한 내용은 GeneriClean 페이지 E-4를 참조하십시오.

추가 서비스 설정 화면에서 의심스러운 연결 서비스를 사용하도록 설정하여 에이전트에서 C&C 서버 콜백을 방지합니다. 자세한 내용은 웹 콘솔에서 에이전트 서비스 사용 또는 사용 안 함 페이지 15-8를 참조하십시오.

글로벌 사용자 정의 IP 목록 설정 구성

관리자는 OfficeScan에서 에이전트와 사용자 정의 C&C IP 주소 간의 모든 연결을 허용, 차단 또는 기록하도록 구성할 수 있습니다.

참고

사용자 정의 IP 목록에서는 IPv4 주소만 지원합니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **보안 설정** 탭을 클릭합니다.
3. **의심스러운 연결 설정** 섹션으로 이동합니다.
4. **사용자 정의 IP 목록 편집**을 클릭합니다.
5. **승인된 목록** 또는 **차단된 목록** 탭에서 모니터링할 IP 주소를 추가합니다.

   팁

   사용자 정의 차단된 IP 목록에 있는 주소와의 연결만 기록하도록 OfficeScan을 구성할 수 있습니다. 사용자 정의 차단된 IP 목록에 있는 주소와의 연결만 기록하려면 의심스러운 연결 설정 구성 페이지 8-7을 참조하십시오.

   a. **추가**를 클릭합니다.

   b. 새 화면이 나타나면 OfficeScan에서 모니터링할 IP 주소, IP 주소 범위 또는 IPv4 주소와 서브넷 마스크를 입력합니다.

   c. **저장**을 클릭합니다.

6. 목록에서 IP 주소를 제거하려면 주소 옆의 확인란을 선택하고 **삭제**를 클릭합니다.
7. 목록을 구성한 후 **닫기**를 클릭하여 **글로벌 에이전트 설정** 화면으로 돌아갑니다.

8. **저장**을 클릭하여 에이전트에 업데이트된 목록을 배포합니다.

의심스러운 연결 설정 구성

OfficeScan에서는 글로벌 C&C IP 목록에 있는 에이전트와 주소 간의 모든 연결을 기록하고 차단할 수 있습니다. **의심스러운 연결 설정** 화면에서는 사용자 정의 차단된 IP 목록에 구성된 IP 주소에 대한 액세스를 기록하면서 계속 허용할 수도 있습니다.

또한 OfficeScan은 봇넷이나 다른 악성 프로그램 위협의 결과일 수 있는 연결도 모니터링할 수 있습니다. OfficeScan에서는 악성 프로그램 위협을 탐지하면 감염을 치료하려고 시도할 수 있습니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **의심스러운 연결 설정**을 클릭합니다.

   의심스러운 연결 설정 화면이 나타납니다.
4. **글로벌 C&C IP 목록의 주소에 대한 네트워크 연결 탐지** 설정을 사용하도록 설정하여 Trend Micro에서 확인한 C&C 서버에 대한 연결을 모니터링하고 **기록만**을 선택하거나 연결 **차단**을 선택합니다.
   - 에이전트가 사용자 정의 차단된 IP 목록에 구성된 주소에 연결할 수 있도록 하려면 **사용자 정의 차단 IP 목록 주소에 대한 액세스 로깅 및 허용** 설정을 사용하도록 설정합니다.

참고

네트워크 연결 기록을 사용하도록 설정해야 OfficeScan에서 사용자 정의 차단된 IP 목록에 있는 주소에 대한 액세스를 허용할 수 있습니다.

글로벌 C&C IP 목록에 대한 자세한 내용은 의심스러운 연결 서비스 페이지 8-5를 참조하십시오.

5. **악성 프로그램 네트워크 지문을 사용하여 연결 탐지** 설정을 사용하도록 설정하고 **기록만**을 선택하거나 연결 **차단**을 선택합니다.

   악성 프로그램 네트워크 지문은 패킷 헤더에 대한 패턴 일치를 수행합니다. OfficeScan에서는 알려진 악성 프로그램 위협과 헤더가 일치하는 패킷의 모든 연결을 관련 규칙 패턴을 사용하여 기록합니다.

   - OfficeScan에서 C&C 서버에 대한 연결을 치료할 수 있도록 하려면 **C&C 콜백이 발견되면 의심스러운 연결 치료** 설정을 사용하도록 설정합니다. OfficeScan에서는 GeneriClean을 사용하여 악성 프로그램 위협을 치료하고 C&C 서버에 대한 연결을 종료합니다.

   참고

   악성 프로그램 네트워크 지문을 사용하여 로그 연결을 사용하도록 설정해야 OfficeScan에서 패킷 구조 일치를 통해 발견한 C&C 서버와의 연결을 치료할 수 있습니다.

6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

샘플 제출

이전에 식별되지 않은 위협이 포함되어 있을 수 있는 파일 개체를 향후 분석을 위해 Virtual Analyzer에 제출하도록 OfficeScan 에이전트를 구성할 수 있습니다. Virtual Analyzer는 개체를 평가한 후 알 수 없는 위협이 들어 있는 개체를 Virtual Analyzer의 의심스러운 개체 목록에 추가하고 이 목록을 네트워크 전체의 다른 OfficeScan 에이전트에 배포합니다.

자세한 내용은 의심스러운 개체 목록 설정 페이지 14-31를 참조하십시오.

샘플을 제출하려면 다음이 필요합니다.

- OfficeScan 서버를 Trend Micro Control Manager 서버(6.0 SP3 패치 2 이상)에 등록해야 합니다.
- Trend Micro Control Manager 서버가 Trend Micro Deep Discovery Analyzer 서버(5.1 이상)에 연결되어 있어야 합니다.

의심스러운 파일에는 다음과 같은 것들이 있습니다.

- Trend Micro에서 알지 못하는 프로그램(지원되는 웹 브라우저 또는 전자 메일 채널을 통해 다운로드됨)
- 프로세스의 휴리스틱 탐지(지원되는 웹 브라우저 또는 전자 메일 채널을 통해 다운로드됨)
- 이동식 저장소의 일반적이지 않은 자동 실행 프로그램

중요

OfficeScan 에이전트는 최대 50MB의 샘플 파일을 분석을 위해 Virtual Analyzer에 제출할 수 있습니다.

샘플 제출 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **샘플 제출 설정**을 클릭합니다.

   샘플 제출 설정 화면이 나타납니다.
4. **Virtual Analyzer로 의심스러운 파일 제출 사용**을 선택합니다.
5. **저장**을 클릭합니다.

알 수 없는 위협 로그

OfficeScan 에이전트는 알 수 없는 위협 활동을 기록하고 로그를 서버로 전송합니다. 지속적으로 실행되는 OfficeScan 에이전트는 로그를 집계하고 집계한 로그를 지정된 간격(기본적으로 60분)으로 전송합니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

머신러닝 로그 보기

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그 보기** > **머신러닝 로그** 또는 **로그** > **머신러닝 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.

항목	설명
날짜/시간	탐지가 발생한 시간
엔드포인트	탐지가 발생한 엔드포인트
IP 주소	소스 엔드포인트의 IP 주소 및 포트 번호
보안 위협	머신러닝 엔진에서 확인한 보안 위협의 이름
결과	수행한 조치의 결과
파일 이름	프로세스를 실행한 프로그램 또는 파일 개체의 이름

항목	설명
유형	탐지를 트리거한 개체의 유형(“파일” 또는 “프로세스”)
파일 경로	프로세스를 실행한 프로그램의 경로 또는 파일 개체의 경로
감염 채널	위협이 시작된 채널
세부 정보	특정 탐지에 대한 세부적인 분석을 표시하는 링크 자세한 내용은 머신러닝 로그 세부 정보 페이지 8-11를 참조하십시오.

6. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **모두 CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

머신러닝 로그 세부 정보

세부 정보 열 아래에서 **보기** 링크를 클릭하여 각 머신러닝 로그 탐지에 대한 포괄적인 보고서를 볼 수 있습니다.

로그 세부 정보 화면은 다음 두 가지 섹션으로 구성되어 있습니다.

- 상단 배너: 이 로그 탐지와 관련된 특정 세부 정보
- 하단 탭 컨트롤: 위협 가능성 점수, 파일 정보 및 동일하게 탐지한 네트워크의 다른 엔드포인트를 포함하는 머신러닝 위협과 관련한 세부 정보

다음 표에서는 상단 배너에 제공되는 정보에 대해 설명합니다.

표 8-1. 로그 세부 정보 - 상단 배너

섹션	설명
탐지 시간/조치	이 특정 로그 탐지가 발생한 시간 그리고 에이전트가 위협에 대해 수행한 조치를 나타냅니다.

섹션	설명
파일 이름	지정된 엔드포인트에 대해 탐지를 트리거한 파일의 이름을 나타냅니다. **팁** 영향받는 파일의 파일 해시 값을 글로벌 머신러닝 예외 목록에 신속하게 추가하려면 **예외 목록에 추가**를 클릭합니다. **머신러닝 설정** 화면에서 전체 예외 목록을 봅니다. 자세한 내용은 머신러닝 설정 구성 페이지 8-3를 참조하십시오. **중요** 이 탐지를 통해 탐지된 파일 이름이 다른 에이전트에서 탐지된 파일 이름과 같지 않을 수 있습니다. 머신러닝은 특정 파일 이름이 아닌 파일 해시 값에 따라 탐지를 연결합니다. 다른 엔드포인트의 파일 이름을 확인하려면 **감염된 엔드포인트** 탭을 봅니다.
엔드포인트 정보	탐지 시점에 로그온한 사용자, 엔드포인트 이름 및 엔드포인트의 IP 주소를 표시합니다.
채널 정보	위협이 시작된 채널과 위협이 전송된 엔드포인트의 폴더 위치를 표시합니다.

다음 표에서는 하단 탭에 제공되는 정보에 대해 설명합니다.

표 8-2. 로그 세부 정보 - 탭 정보

탭	설명
위협 지표	머신러닝 분석의 결과를 제공합니다. • **위협 가능성**: 파일/프로세스가 악성 프로그램 모델에 얼마나 일치하는지 나타냅니다. • **가능한 위협 유형**: 머신러닝이 분석 결과를 알려진 다른 위협과 비교한 후 파일에 포함된 위협과 가장 일치하는 유형을 나타냅니다. • **위협 식별자**: 탐지된 위협 유형을 나타낼 수 있는 파일/프로세스에서 사용하는 API 함수의 목록을 제공합니다. **중요** API 함수 식별은 위협 유형 판별에서 하나의 요소에 지나지 않습니다. 머신러닝은 기타 여러 가지 파일 특성과 분석 방법을 사용하여 위협 가능성과 가능한 위협 유형을 계산합니다. • **유사한 알려진 위협**: 탐지 항목과 유사한 파일/프로세스 특성을 보이는 알려진 위협 유형의 목록을 제공합니다.
파일 세부 정보	파일 등록정보와 관련된 일반적인 세부 정보 그리고 이 특정 탐지 로그에 대한 인증서 정보를 제공합니다.
감염된 엔드포인트	네트워크에서 동일한 머신러닝 탐지가 있는 다른 에이전트의 목록을 표시하고 다른 에이전트의 탐지에 대한 관련 세부 정보를 제공합니다.

의심스러운 연결 로그 보기

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.

3. **로그 보기** > **의심스러운 연결 로그** 또는 **로그** > **의심스러운 연결 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.

항목	설명
날짜/시간	탐지가 발생한 시간
엔드포인트	탐지가 발생한 엔드포인트
도메인	탐지가 발생한 엔드포인트의 도메인
프로세스	전송을 시작한 프로세스(path\application_name)
로컬 IP 및 포트	소스 엔드포인트의 IP 주소 및 포트 번호
원격 IP 및 포트	대상 엔드포인트의 IP 주소 및 포트 번호
결과	수행한 조치의 결과
탐지 위치	C&C 서버를 식별한 C&C 목록 소스
트래픽 방향	전송 방향

6. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **모두 CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

샘플 제출 로그 보기

OfficeScan은 샘플 제출 데이터를 시스템 이벤트 로그에 저장합니다. 샘플 제출 데이터를 보다 종합적으로 요약하려면 Control Manager 콘솔을 사용하여 로그를 보는 것이 좋습니다. Control Manager는 의심스러운 개체 파일 처리 프로세스에 대한 세부적인 분석을 제공하므로 의심스러운 개체가 네트워크에 어떻게 영향을 줄 수 있는지 더 명확하게 알 수 있습니다.

절차

1. **로그** > **시스템 이벤트**로 이동합니다.

2. **이벤트**에서 다음 로그 유형을 확인합니다.

   - "Virtual Analyzer로 샘플 제출됨[파일[<file_name], SHA1[<file_SHA1_value>]"
   - "Virtual Analyzer 샘플 분석 완료[<date_time_analysis_completed>, 파일[<file_name], SHA1[<file_SHA1_value>], 바이러스[<detection_type], 규칙[<virtual_analyzer_rule_type]]"

장 9

동작 모니터링 사용

이 장에서는 동작 모니터링 기능을 사용하여 보안 위험으로부터 컴퓨터를 보호하는 방법에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- 동작 모니터링 페이지 9-2
- 글로벌 동작 모니터링 설정 구성 페이지 9-12
- 동작 모니터링 권한 페이지 9-14
- OfficeScan 에이전트 사용자에 대한 동작 모니터링 알림 페이지 9-15
- 동작 모니터링 로그 페이지 9-17

동작 모니터링

동작 모니터링은 운영 체제 또는 설치된 소프트웨어에 대한 비정상적인 수정에 대해 엔드포인트를 지속적으로 모니터링합니다. 동작 모니터링은 **악성 프로그램 동작 차단** 및 **이벤트 모니터링**을 통해 엔드포인트를 보호합니다. 이 두 기능에 대한 보완은 사용자가 구성한 **예외 목록**과 **인증된 안전한 소프트웨어 서비스**를 기반으로 합니다.

중요

- 동작 모니터링은 Windows XP 또는 Windows 2003 64비트 플랫폼을 지원하지 않습니다.
- 동작 모니터링은 Windows Vista 64비트 플랫폼 SP1 이상을 지원합니다.
- 기본적으로 동작 모니터링은 Windows Server 플랫폼의 모든 버전에서 사용되지 않도록 설정되어 있습니다. 이러한 서버 플랫폼에서 동작 모니터링을 사용하도록 설정하기 전에 OfficeScan 에이전트 서비스 페이지 15-7에 설명된 지침과 모범 사례를 읽어 보십시오.

악성 프로그램 동작 차단

악성 프로그램 동작 차단에서는 유해한 동작을 보이는 프로그램의 추가 위협으로부터 보호하는 데 필요한 레이어를 제공합니다. 일정 기간 동안 시스템 이벤트를 관찰하는 악성 프로그램 동작 차단에서는 프로그램이 여러 조합 또는 시퀀스의 작업을 실행할 때 알려진 유해한 동작을 탐지하여 연관된 프로그램을 차단합니다. 이 기능을 사용하여 알려지지 않은 새로운 위협으로부터 보호를 강화할 수 있습니다.

악성 프로그램 동작 모니터링에서는 다음과 같은 위협 수준 검색 옵션을 제공합니다.

- **알려진 위협**: 알려진 악성 프로그램 위협과 관련된 동작을 차단합니다.
- **알려진 위협 및 잠재적 위협**: 알려진 위협과 연관된 동작을 차단하고 유해할 수 있는 동작에 대한 조치를 취합니다.

알림을 사용하도록 설정한 경우 프로그램이 차단되면 OfficeScan에서 OfficeScan 에이전트 엔드포인트에 알림을 표시합니다. 알림에 대한 자세한 내

용은 OfficeScan 에이전트 사용자에 대한 동작 모니터링 알림 페이지 9-15을 참조하십시오.

랜섬웨어 보호

랜섬웨어 보호는 "랜섬웨어 위협"으로부터 에이전트의 파일이 무단 수정되거나 암호화되지 않도록 해줍니다. 랜섬웨어는 파일에 대한 액세스를 제한하고 영향받은 파일의 복원을 위해 돈을 요구하는 일종의 악성 프로그램입니다.

OfficeScan은 다음과 같은 방법을 제공하여 랜섬웨어 위협으로부터 환경을 보호합니다.

참고

OfficeScan에서 안전한 프로세스를 유해한 프로세스로 탐지하는 횟수를 줄이기 위해 에이전트에는 Trend Micro 서버를 사용하여 추가 확인 프로세스를 수행하는 인터넷 액세스 기능이 포함됩니다.

옵션	설명
무단 암호화 또는 수정으로부터 문서 보호	랜섬웨어 공격을 나타낼 수 있는 일련의 특정 이벤트를 탐지하도록 동작 모니터링을 구성할 수 있습니다. 동작 모니터링이 다음 기준과 모두 일치하면 OfficeScan에서는 유해 프로그램을 종료하고 격리 보관을 시도합니다. 1. 프로세스가 특정 시간 간격 내 세 개의 파일을 수정, 삭제 또는 파일의 이름을 변경하려는 안전한 시도로 인식되지 않은 경우 2. 프로세스가 보호된 파일 확장자 유형을 수정하려고 할 경우 또한 **의심스러운 프로그램에 의해 변경된 파일 자동 백업**을 사용하도록 설정하여 엔드포인트에서 암호화된 파일의 사본을 생성합니다. 암호화 프로세스가 완료된 후 OfficeScan에서 랜섬웨어 위협을 탐지하면 OfficeScan이 최종 사용자에게 영향받은 파일을 데이터 손실 없이 복원하라는 메시지를 표시합니다. **참고** 자동 파일 백업을 사용하려면 에이전트 엔드포인트에 최소 100MB의 디스크 공간이 필요합니다. 자동 파일 백업에서는 크기가 10MB 미만인 파일만 백업합니다. 00 에이전트 엔드포인트의 백업 폴더 위치는 <에이전트 설치 폴더>₩CCSF₩module₩DRE₩data입니다. **경고!** **의심스러운 프로그램에 의해 변경된 파일 자동 백업**을 사용하도록 설정하지 않은 경우 OfficeScan은 랜섬웨어 위협에 의해 영향을 받은 첫 번째 파일들을 복구할 수 없습니다.
일반적으로 랜섬웨어와 관련된 프로세스 차단	랜섬웨어는 보통 파일 공격을 시도하기 전에 엔드포인트의 특정 위치에 실행 파일을 배포합니다. 이러한 위치에서 시작되는 프로세스를 차단하면 랜섬웨어가 파일을 공격하지 못하도록 차단할 수 있습니다.

옵션	설명
프로그램 검사를 사용하여 손상된 실행 파일을 탐지하고 차단	프로그램 검사는 프로세스를 모니터링하고 API 후크를 수행하여 프로그램이 예상치 않은 방식으로 동작하고 있지는 않은지 확인합니다. 이 절차로 손상된 실행 파일의 전반적인 탐지율이 증가하지만 시스템 성능이 저하될 수 있습니다. **팁** 프로그램 검사는 **차단할 위협** 드롭다운에서 **알려진 위협 및 잠재적 위협**을 선택할 때 더욱 강화된 보안을 제공합니다. **중요** SP2(또는 그 이상)가 포함되지 않은 Windows Server 2003 및 Windows XP 64비트 플랫폼에서는 지원되지 않습니다.

위협 방지

위협 방지는 프로그램 검사와 함께 작동하여 프로그램의 동작을 모니터링하고 공격자가 프로그램 취약점을 악용했음을 나타낼 수 있는 비정상적인 동작을 탐지합니다. 일단 탐지되면 동작 모니터링에서 프로그램 프로세스를 종료합니다.

중요

위협 방지를 사용하려면 **프로그램 검사를 사용하여 손상된 실행 파일을 탐지하고 차단**을 선택해야 합니다.

새로 발견된 프로그램 보호

동작 모니터링 기능은 웹 검증 서비스 및 실시간 검색과 함께 작동하여 HTTP 채널, 전자 메일 응용 프로그램 또는 Microsoft Office 매크로 스크립트를 통해 다운로드된 파일의 출현을 확인합니다. "새로 발견된" 파일을 탐지하면 관리자는 파일을 실행하기 전에 사용자에게 확인하도록 할 수 있습니다. Trend Micro에서는 스마트 보호 네트워크에서 확인한 파일 사용 기간 또는 탐지된 파일 수를 기준으로 하여 프로그램을 새로 발견된 것으로 분류합니다.

동작 모니터링에서는 각 채널에서 다음 파일 유형을 검색합니다.

- HTTP/HTTPS: .exe 파일을 검색합니다.
- 전자 메일 응용 프로그램: .exe 파일과 암호화되지 않은 .zip 및 .rar 파일로 압축된 .exe 파일을 검색합니다.

참고

- 먼저 관리자가 에이전트에서 웹 검증 서비스를 사용할 수 있게 설정해야 OfficeScan에서 HTTP 또는 HTTPS 트래픽을 검색하여 이 프롬프트를 표시할 수 있습니다.
- OfficeScan은 실행 프로세스 동안 전자 메일 응용 프로그램을 통해 다운로드된 파일 이름이 일치하는지 확인합니다. 파일 이름이 변경된 경우 사용자에게 프롬프트가 표시되지 않습니다.

이벤트 모니터링

이벤트 모니터링은 무단 소프트웨어 및 악성 프로그램 공격으로부터 보호하는 보다 일반적인 접근 방법을 제공합니다. 시스템 영역에서 특정 이벤트를 모니터링하므로 관리자는 이를 통해 해당 이벤트를 트리거하는 프로그램을 조정할 수 있습니다. 악성 프로그램 동작 차단에서 제공하는 수준 이상의 특정 시스템 보호 요구 사항이 있는 경우 이벤트 모니터링을 사용합니다.

다음 표에 모니터링되는 시스템 이벤트 목록이 나와 있습니다.

표 9-1. 모니터링되는 시스템 이벤트

이벤트	설명
중복 시스템 파일	Windows 시스템 파일에서 사용된 파일 이름을 사용하여 자체 프로그램 또는 다른 유해 프로그램의 복사본을 만드는 유해 프로그램이 많이 있습니다. 이 이벤트를 통해 일반적으로 시스템 파일을 재정의하거나 교체하거나, 탐지를 방지하거나, 사용자가 유해 프로그램 파일을 삭제하지 않도록 합니다.
호스트 파일 수정	호스트 파일은 도메인 이름을 IP 주소와 일치시킵니다. 웹 브라우저가 감염되거나 존재하지 않거나 위조된 웹 사이트로 리디렉션되도록 호스트 파일을 수정하는 유해 프로그램이 많이 있습니다.

이벤트	설명
의심스러운 동작	의심스러운 동작은 합법적인 프로그램에서 거의 수행하지 않는 특정 동작 또는 일련의 동작일 수 있습니다. 의심스러운 동작을 보이는 프로그램은 주의해서 사용해야 합니다.
새 Internet Explorer 플러그인	스파이웨어/그레이웨어 프로그램은 도구 모음 및 브라우저 도우미 개체를 포함하여 원치 않는 Internet Explorer Plug-in을 설치하는 경우가 많습니다.
Internet Explorer 설정 수정	홈 페이지, 신뢰할 수 있는 웹 사이트, 프록시 서버 설정 및 메뉴 확장을 포함하여 Internet Explorer 설정을 변경하는 바이러스/악성 프로그램이 많이 있습니다.
보안 정책 수정	Windows 보안 정책을 수정하면 원치 않는 응용 프로그램이 시스템 설정을 실행하고 변경할 수 있습니다.
프로그램 라이브러리 주입	모든 응용 프로그램이 프로그램 라이브러리(DLL)를 자동으로 로드하도록 Windows를 구성하는 유해 프로그램이 많이 있습니다. 이렇게 하면 응용 프로그램이 시작될 때마다 DLL에서 유해 루틴이 실행될 수 있습니다.
셸 수정	특정 파일 유형에 연결되도록 Windows 셸 설정을 수정하는 유해 프로그램이 많이 있습니다. 이 루틴은 Windows Explorer에서 관련된 파일을 열 경우 유해 프로그램을 자동으로 시작할 수 있습니다. 또한 Windows 셸 설정을 변경하면 유해 프로그램이 합법적인 응용 프로그램과 함께 시작되어 사용하는 프로그램을 추적할 수 있습니다.
새 서비스	Windows 서비스는 전체 관리 액세스를 통해 일반적으로 백그라운드에서 계속 실행되면서 특별한 기능을 지원하는 프로세스입니다. 유해 프로그램이 자체를 서비스로 설치하여 숨김 상태로 유지하는 경우도 있습니다.
시스템 파일 수정	특정 Windows 시스템 파일은 시작 프로그램 및 화면 보호기 설정과 같은 시스템 동작을 결정합니다. 시작할 때 자동으로 시작하여 시스템 동작을 제어하도록 시스템 파일을 수정하는 유해 프로그램이 많이 있습니다.
방화벽 정책 수정	Windows 방화벽 정책은 네트워크, 통신용 포트 및 컴퓨터와 통신할 수 있는 IP 주소에 액세스할 수 있는 응용 프로그램을 확인합니다. 네트워크 및 인터넷에 액세스할 수 있도록 정책을 수정하는 유해 프로그램이 많이 있습니다.

이벤트	설명
시스템 프로세스 수정	다수의 유해 프로그램은 기본 제공되는 Windows 프로세스에서 여러 동작을 수행합니다. 이러한 동작에는 실행 중인 프로세스의 종료 또는 수정이 포함될 수 있습니다.
새 시작 프로그램	유해 응용 프로그램은 일반적으로 Windows 레지스트리에 자동 시작 항목을 추가하거나 수정하여 컴퓨터가 시작할 때마다 자동으로 시작합니다.

이벤트 모니터링에서는 모니터링되는 시스템 이벤트를 탐지한 경우 이벤트에 대해 구성된 조치를 수행합니다.

다음 표에는 관리자가 모니터링되는 시스템 이벤트에 대해 수행할 수 있는 가능한 조치가 나와 있습니다.

표 9-2. 모니터링되는 시스템 이벤트에 대한 조치

조치	설명
점검	OfficeScan에서 이벤트와 관련된 프로그램을 항상 허용하지만 평가를 위해 로그에 이 조치를 기록합니다. 이는 모든 모니터링되는 시스템 이벤트에 대한 기본 조치입니다. **참고** 64비트 시스템의 프로그램 라이브러리 주입에는 이 옵션이 지원되지 않습니다.
허용	OfficeScan에서 이벤트와 관련된 프로그램을 항상 허용합니다.

조치	설명
필요 시 묻기	OfficeScan에서 이벤트와 관련된 프로그램을 허용할지 또는 거부할지 그리고 예외 목록에 프로그램을 추가할지를 묻는 메시지를 사용자에게 표시합니다. 사용자가 일정 기간 동안 응답하지 않으면 OfficeScan에서 프로그램 실행을 자동으로 허용합니다. 기본 기간은 30초입니다. 기간을 수정하려면 글로벌 동작 모니터링 설정 구성 페이지 9-12을 참조하십시오. **참고** 64비트 시스템의 프로그램 라이브러리 주입에는 이 옵션이 지원되지 않습니다.
거부	OfficeScan 에서 이벤트와 관련된 프로그램을 항상 차단하고 이 조치를 로그에 기록합니다. 알림을 사용하도록 설정한 경우 프로그램이 차단되면 OfficeScan에서 OfficeScan 컴퓨터에 알림을 표시합니다. 알림에 대한 자세한 내용은 OfficeScan 에이전트 사용자에 대한 동작 모니터링 알림 페이지 9-15을 참조하십시오.

동작 모니터링 예외 목록

동작 모니터링 예외 목록에는 동작 모니터링에 의해 모니터링되지 않는 프로그램이 포함됩니다.

- **승인된 프로그램**: 이 목록의 프로그램은 실행될 수 있습니다. 승인된 프로그램은 최종적으로 실행이 허용되기 전에 다른 OfficeScan 기능(예: 파일 기반 검색)에 의해 확인됩니다.
- **차단된 프로그램**: 이 목록의 프로그램은 시작할 수 없습니다. 이 목록을 구성하려면 이벤트 모니터링을 사용하도록 설정해야 합니다.

웹 콘솔에서 예외 목록을 구성합니다. 또한 OfficeScan 에이전트 콘솔에서 예외 목록을 구성할 수 있는 권한을 사용자에게 부여할 수 있습니다. 자세한 내용은 동작 모니터링 권한 페이지 9-14를 참조하십시오.

악성 프로그램 동작 차단, 이벤트 모니터링 및 예외 목록 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **동작 모니터링 설정**을 클릭합니다.
4. **규칙** 탭을 클릭합니다.
5. 악성 프로그램 동작 차단을 사용하려면
   a. **악성 프로그램 동작 차단 사용**을 선택하고 차단할 위협 유형을 지정합니다.
      - **알려진 위협**: 알려진 악성 프로그램 위협과 관련된 동작을 차단합니다.
      - **알려진 위협 및 잠재적 위협**: 알려진 위협과 연관된 동작을 차단하고 유해할 수 있는 동작에 대한 조치를 취합니다.

   b. 랜섬웨어 위협으로부터 보호하기 위해 사용할 랜섬웨어 보호 기능을 선택합니다.
      - **무단 암호화 또는 수정으로부터 문서 보호**: 잠재적인 랜섬웨어 위협이 문서 내용을 암호화하거나 수정하는 것을 중지합니다.
        - **의심스러운 프로그램에 의해 변경된 파일 자동 백업 및 복원**: OfficeScan이 랜섬웨어 위협을 탐지하는 경우 데이터 손실을 방지하기 위해 엔드포인트에 암호화되는 파일의 백업 사본을 만듭니다.

참고

자동 파일 백업을 사용하려면 에이전트 엔드포인트에 최소 100MB의 디스크 공간이 필요합니다. 자동 파일 백업에서는 크기가 10MB 미만인 파일만 백업합니다.

- **일반적으로 랜섬웨어와 관련된 프로세스 차단**: 알려진 랜섬웨어 위협과 관련된 프로세스를 문서의 암호화 또는 수정이 발생하기 전에 차단합니다.
- **프로그램 검사를 사용하여 손상된 실행 파일을 탐지하고 차단**: 프로그램 검사는 프로세스를 모니터링하고 API 후크를 수행하여 프로그램이 예상치 않은 방식으로 동작하고 있지는 않은지 확인합니다. 이 절차로 손상된 실행 파일의 전반적인 탐지율이 증가하지만 시스템 성능이 저하될 수 있습니다.

팁

프로그램 검사는 **차단할 위협** 드롭다운에서 **알려진 위협 및 잠재적 위협**을 선택할 때 더욱 강화된 보안을 제공합니다.

자세한 내용은 랜섬웨어 보호 페이지 9-3를 참조하십시오.

c. **위협 방지**에서, **위협 공격과 관련된 비정상적인 동작을 보인 프로그램 종료**를 사용하도록 설정하여 잠재적 위협이 되는 프로그램을 차단합니다.

참고

위협 방지를 사용하려면 **프로그램 검사를 사용하여 손상된 실행 파일을 탐지하고 차단**을 선택해야 합니다.

자세한 내용은 위협 방지 페이지 9-5를 참조하십시오.

6. **새로 발견된 프로그램** 섹션에서 **HTTP 또는 전자 메일 응용 프로그램을 통해 다운로드한 새로 발견된 프로그램 모니터링**을 사용하도록 설정하고 다운로드한 프로그램을 실행하기 전에 **사용자에게 확인**할지 아니면 OfficeScan에서 탐지를 기록하게만 할지 선택합니다.
7. 이벤트 모니터링 설정을 구성합니다.
   a. **이벤트 모니터링 사용**을 선택합니다.
   b. 모니터링할 시스템 이벤트를 선택한 다음 선택한 각 이벤트에 대한 조치를 선택합니다.

      모니터링되는 시스템 이벤트와 조치에 대한 자세한 내용은 이벤트 모니터링 페이지 9-6을 참조하십시오.

8. **예외** 탭을 클릭하고 예외 목록을 구성합니다.

   a. **전체 프로그램 경로를 입력하십시오.** 아래에 승인하거나 차단할 프로그램의 전체 경로를 입력합니다. 여러 항목을 세미콜론(;)으로 구분하십시오.

   b. **승인된 목록에 추가** 또는 **차단된 목록에 추가**를 클릭합니다.

   c. 차단되거나 승인된 프로그램을 목록에서 제거하려면 해당 프로그램 옆의 휴지통 아이콘( )을 클릭합니다.

   참고

   OfficeScan에서는 최대 1024개의 승인된 프로그램 및 1024개의 차단된 프로그램이 허용됩니다.

9. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

글로벌 동작 모니터링 설정 구성

OfficeScan은 글로벌 에이전트 설정을 모든 에이전트에 적용하거나 특정 권한이 있는 에이전트에만 적용합니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **보안 설정** 탭을 클릭합니다.

3. **동작 모니터링 설정** 섹션으로 이동합니다.

4. **사용자가 다음 시간 내에 응답하지 않는 경우 자동으로 조치 수행: __ 초** 설정을 필요에 맞게 구성합니다.

   이 설정은 이벤트 모니터링을 사용하고 모니터링되는 시스템 이벤트에 대한 조치가 "필요 시 묻기"인 경우에만 작동합니다. 이 조치는 사용자에게 이벤트와 관련된 프로그램을 허용할지 아니면 거부할지 묻는 메시지를 표시합니다. 사용자가 일정 기간 동안 응답하지 않으면 OfficeScan에서 프로그램 실행을 자동으로 허용합니다.

   자세한 내용은 이벤트 모니터링 페이지 9-6를 참조하십시오.

5. **시스템** 탭을 클릭합니다.

6. **인증된 안전한 소프트웨어 서비스 설정** 섹션으로 이동하고 필요한 경우 인증된 안전한 소프트웨어 서비스를 사용하도록 설정합니다.

   인증된 안전한 소프트웨어 서비스에서는 Trend Micro 데이터 센터를 쿼리하여 악성 프로그램 동작 차단, 이벤트 모니터링, 방화벽 또는 바이러스 백신 검색을 통해 탐지된 프로그램의 안전성을 확인합니다. 인증된 안전한 소프트웨어 서비스를 사용하도록 설정하면 잘못된 판정이 탐지될 가능성이 줄어듭니다.

   참고

   인증된 안전한 소프트웨어 서비스를 사용도록 설정하기 전에 OfficeScan 에이전트 프록시 설정이 올바른지 확인해야 합니다(자세한 내용은 OfficeScan 에이전트 프록시 설정 페이지 15-47 참조). 잘못된 프록시 설정은 일시적인 인터넷 연결 끊김과 함께 Trend Micro 데이터 센터의 응답을 지연시키거나 수신되지 않도록 하여 모니터링 대상 프로그램이 응답하지 않는 것처럼 보이게 합니다.

   또한 순수 IPv6 OfficeScan 에이전트는 Trend Micro 데이터 센터에서 직접 쿼리할 수 없습니다. OfficeScan 에이전트에서 Trend Micro 데이터 센터에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

7. **저장**을 클릭합니다.

동작 모니터링 권한

에이전트에 동작 모니터링 권한이 있으면 동작 모니터링 옵션이 OfficeScan 에이전트 콘솔의 **설정** 화면에 표시됩니다. 이 경우 사용자는 고유한 예외 목록을 관리할 수 있습니다.

그림 9-1. OfficeScan 에이전트 콘솔의 동작 모니터링 옵션

동작 모니터링 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **동작 모니터링 권한** 섹션으로 이동합니다.
5. **OfficeScan 에이전트 콘솔에 동작 모니터링 설정 표시**를 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트 사용자에 대한 동작 모니터링 알림

OfficeScan에서는 동작 모니터링에 의해 프로그램이 차단된 후 즉시 OfficeScan 에이전트 컴퓨터에 알림 메시지를 표시할 수 있습니다. 알림 메시지 보내기를 사용하도록 설정하고 필요한 경우 메시지 내용을 수정합니다.

알림 메시지 보내기 사용

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭하고 **동작 모니터링 설정** 섹션으로 이동합니다.
5. **프로그램이 차단되면 알림 표시**를 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

알림 메시지 내용 수정

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 **동작 모니터링 정책 위반**을 선택합니다.
3. 제공된 텍스트 상자에서 기본 메시지를 수정합니다.
   - 동작 모니터링 정책 위반: 악성 프로그램 동작 차단에서 정책 위반을 탐지했을 때 최종 사용자가 수신하는 메시지를 지정합니다.

- 새로 발견된 프로그램: 동작 차단에서 HTTP/HTTPS 또는 전자 메일 응용 프로그램 채널을 통해 다운로드된 인식할 수 없는 프로그램을 탐지했을 때 최종 사용자가 수신하는 메시지를 지정합니다.

4. **저장**을 클릭합니다.

동작 모니터링 로그

OfficeScan 에이전트는 무단 프로그램 액세스 인스턴스를 기록하고 해당 로그를 서버에 보냅니다. 지속적으로 실행되는 OfficeScan 에이전트는 로그를 집계하고 집계한 로그를 지정된 간격(기본적으로 60분)으로 전송합니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

동작 모니터링 로그 보기

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **동작 모니터링 로그** 또는 **로그 보기** > **동작 모니터링 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.
   - 무단 프로세스가 탐지된 날짜/시간
   - 무단 프로세스가 탐지된 엔드포인트

- 엔드포인트 도메인
- 위반(프로세스에서 위반한 이벤트 모니터링 규칙)
- 위반이 탐지되었을 때 수행된 조치
- 이벤트(프로그램에서 액세스한 개체 유형)
- 무단 프로그램의 위험 수준
- 무단 프로그램
- 작업(무단 프로그램에 의해 수행된 작업)
- 액세스된 프로세스 대상
- 위협이 시작된 감염 채널

6. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

동작 모니터링 로그 보내기 일정 구성

절차

1. <서버 설치 폴더>₩PCCSRV에 액세스합니다.
2. 메모장과 같은 텍스트 편집기를 사용하여 ofcscan.ini 파일을 엽니다.
3. 문자열 "`SendBMLogPeriod`"를 검색한 다음 그 옆의 값을 확인합니다.

   기본값은 3600초이고 문자열은 `SendBMLogPeriod=3600`으로 나타납니다.
4. 값을 초 단위로 지정합니다.

   예를 들어 로그 기간을 2시간으로 변경하고, 값을 7200으로 변경합니다.
5. 파일을 저장합니다.
6. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
7. 설정 변경 없이 **저장**을 클릭합니다.

8. 에이전트를 다시 시작합니다.

장 10

장치 제어 사용

이 장에서는 장치 제어 기능을 사용하여 보안 위험으로부터 컴퓨터를 보호하는 방법에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- 장치 제어 페이지 10-2
- 저장 장치에 대한 권한 페이지 10-4
- 비저장 장치에 대한 권한 페이지 10-10
- 장치 제어 알림 수정 페이지 10-18
- 장치 제어 로그 페이지 10-18

장치 제어

장치 제어는 컴퓨터에 연결된 외부 저장 장치 및 네트워크 리소스에 대한 액세스를 조정합니다. 장치 제어를 통해 데이터 손실 및 유출을 방지하고 파일 검색과 함께 보안 위험으로부터 보호할 수 있습니다.

내부 및 외부 에이전트에 대한 장치 제어 정책을 구성할 수 있습니다. OfficeScan 관리자는 일반적으로 외부 에이전트에 대해 더 엄격한 정책을 구성합니다.

정책은 OfficeScan 에이전트 트리의 개별 설정입니다. 에이전트 그룹 또는 개별 에이전트에 특정 정책을 적용할 수 있습니다. 또한 모든 에이전트에 단일 정책을 적용할 수도 있습니다.

정책을 배포하면 에이전트에서 **엔드포인트 위치 화면**(엔드포인트 위치 페이지 15-2 참조)에 설정된 위치 기준을 사용하여 해당 위치 및 적용할 정책을 확인합니다. 에이전트는 위치가 변경될 때마다 정책을 전환합니다.

중요

- 모든 버전의 Windows Server 2003, Windows Server 2008, Windows Server 2012 및 Windows Server 2016에서는 기본적으로 장치 제어가 사용하지 않도록 설정됩니다. 이러한 서버 플랫폼에서 장치 제어를 사용하려면 먼저 OfficeScan 에이전트 서비스 페이지 15-7에 설명된 지침과 모범 사례를 읽어 보십시오.
- 지원되는 장치 모델의 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

  http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

---

OfficeScan에서 모니터링할 수 있는 장치 유형은 데이터 보호 라이선스가 활성화되어 있는지 여부에 따라 다릅니다. 데이터 보호는 별도의 라이선스 모듈이므로 사용하려면 별도로 활성화해야 합니다. 데이터 보호 라이선스에 대한 자세한 내용은 데이터 보호 라이선스 페이지 3-4를 참조하십시오.

표 10-1. 무단 변경 방지 서비스에 의해 모니터링되는 장치

장치 유형	장치 설명
저장 장치	CD/DVD **중요** 장치 제어는 라이브 파일 시스템 형식을 사용하는 CD/DVD 기록 장치에 대한 액세스만 제한할 수 있습니다. 마스터 형식을 사용하는 일부 타사 응용 프로그램은 장치 제어를 사용할 때도 여전히 읽기/쓰기 작업을 수행할 수 있습니다. 데이터 손실 방지를 사용하여 모든 포맷 유형을 사용하는 CD/DVD 기록 장치에 대한 액세스를 제한합니다. 자세한 내용은 데이터 레코더(CD/DVD)에 대한 액세스 차단 페이지 11-33를 참조하십시오.
	플로피 디스크
	네트워크 드라이브
	USB 저장 장치

표 10-2. 데이터 손실 방지에 의해 모니터링되는 장치

장치 유형	장치 설명
모바일 장치	모바일 장치
저장 장치	CD/DVD
	플로피 디스크
	네트워크 드라이브
	USB 저장 장치

장치 유형	장치 설명
비저장 장치	Bluetooth 어댑터
	COM 및 LPT 포트
	IEEE 1394 인터페이스
	이미징 장치
	적외선 장치
	모뎀
	PCMCIA 카드
	Print Screen 키
	무선 NIC

저장 장치에 대한 권한

저장 장치에 대한 장치 제어 권한은 다음과 같은 경우에 사용됩니다.

- USB 저장 장치, CD/DVD, 플로피 디스크 및 네트워크 드라이브에 대한 액세스를 허용하는 경우. 이러한 장치에 대한 전체 액세스 권한을 부여하거나 액세스 수준을 제한할 수 있습니다.
- 승인된 USB 저장 장치 목록을 구성하는 경우. 장치 제어를 통해 승인된 장치 목록에 추가된 장치를 제외한 모든 USB 저장 장치에 대한 액세스를 차단할 수 있습니다. 승인된 장치에 대한 전체 액세스 권한을 부여하거나 액세스 수준을 제한할 수 있습니다.

다음 표에는 저장 장치에 대한 권한이 설명되어 있습니다.

표 10-3. 저장 장치에 대한 장치 제어 권한

권한	장치의 파일	들어오는 파일
전체 액세스	허용된 작업: 복사, 이동, 열기, 저장, 삭제, 실행	허용된 작업: 저장, 이동, 복사 이것은 파일을 장치에 저장, 이동 및 복사할 수 있음을 의미합니다.
수정	허용된 작업: 복사, 이동, 열기, 저장, 삭제 금지된 작업: 실행	허용된 작업: 저장, 이동, 복사
읽기 및 실행	허용된 작업: 복사, 열기, 실행 금지된 작업: 저장, 이동, 삭제	금지된 작업: 저장, 이동, 복사
읽기	허용된 작업: 복사, 열기 금지된 작업: 저장, 이동, 삭제, 실행	금지된 작업: 저장, 이동, 복사
장치 콘텐츠만 나열	금지된 작업: 모든 작업 장치와 장치에 포함된 파일을 사용자가 볼 수 있음(예: Windows 탐색기에서)	금지된 작업: 저장, 이동, 복사
차단 (데이터 보호를 설치한 후 사용 가능)	금지된 작업: 모든 작업 장치와 장치에 포함된 파일을 사용자가 볼 수 없음(예: Windows 탐색기에서)	금지된 작업: 저장, 이동, 복사

OfficeScan의 파일 기반 검색 기능은 장치 권한을 보완하고 무시할 수 있습니다. 예를 들어, 권한을 통해 파일을 열 수 있지만 OfficeScan에서 파일이 악성 프로그램에 감염되었음을 발견하는 경우, 악성 프로그램을 제거하도록 파일에 특정 검색 조치가 수행됩니다. 검색 조치가 치료인 경우 파일이 치료된 후에 열리며, 검색 조치가 삭제인 경우에는 파일이 삭제됩니다.

팁

데이터 보호에 대한 장치 제어는 모든 64비트 플랫폼을 지원합니다. OfficeScan에서 지원하지 않는 시스템에 대한 무단 변경 방지 모니터링의 경우 장치 권한을 **차단**으로 설정하여 이러한 장치에 대한 액세스를 제한하십시오.

저장 장치에 대한 고급 권한

고급 권한은 대부분의 저장 장치에 제한된 권한을 부여한 경우에 적용됩니다. 권한은 다음 중 하나일 수 있습니다.

- **수정**
- **읽기 및 실행**
- **읽기**
- **장치 콘텐츠만 나열**

권한은 제한된 상태로 유지하면서 저장 장치 및 로컬 엔드포인트의 특정 프로그램에 대한 고급 권한을 부여할 수 있습니다.

프로그램을 정의하려면 다음 프로그램 목록을 구성합니다.

표 10-4. 프로그램 목록

프로그램 목록	설명	유효한 입력
장치에 대한 읽기 및 쓰기 권한이 있는 프로그램	이 목록에는 장치에 대한 읽기 및 쓰기 권한이 있는 저장 장치의 프로그램 및 로컬 프로그램이 포함됩니다. 로컬 프로그램에는 주로 C:₩Program Files ₩Microsoft Office₩Office에 있는 Microsoft Word(winword.exe) 등이 있습니다. USB 저장 장치에 대한 권한이 "장치 콘텐츠만 나열"이지만 "C:₩Program Files₩Microsoft Office₩Office₩winword.exe"가 이 목록에 포함된 경우: • 사용자는 Microsoft Word에서 액세스한 USB 저장 장치의 모든 파일에 대한 읽기 및 쓰기 권한을 가집니다. • 사용자는 Microsoft Word 파일을 USB 저장 장치에 저장, 이동 또는 복사할 수 있습니다.	프로그램 경로 및 이름 자세한 내용은 프로그램 경로 및 이름 지정 페이지 10-9를 참조하십시오.
장치에서 실행할 수 있는 프로그램	이 목록에는 사용자 또는 시스템에서 실행할 수 있는 저장 장치의 프로그램이 포함됩니다. 예를 들어 사용자가 CD에서 소프트웨어를 설치할 수 있도록 허용하려면 설치 프로그램 경로 및 이름(예: "E:₩Installer₩Setup.exe")을 이 목록에 추가합니다.	프로그램 경로 및 이름 또는 디지털 서명 공급자 자세한 내용은 프로그램 경로 및 이름 지정 페이지 10-9 또는 디지털 서명 공급자 지정 페이지 10-8을 참조하십시오.

프로그램을 두 목록 모두에 추가해야 하는 경우가 있을 수 있습니다. 예를 들어 USB 저장 장치의 데이터 잠금 기능이 설정된 경우 장치의 잠금을 해제하려고 하면 사용자에게 유효한 사용자 이름과 암호를 묻는 메시지가 표시됩니다. 데이터 잠금 기능은 장치에서 "Password.exe"라는 프로그램을 사용합니다. 사용자가 장치의 잠금을 해제하려면 이 프로그램을 실행해야 합니다. 또한 사용자가 사용자 이름 또는 암호를 변경하려면 "Password.exe"의 장치에 대한 읽기 및 쓰기 권한이 있어야 합니다.

사용자 인터페이스의 각 프로그램 목록은 최대 100개의 프로그램을 포함할 수 있습니다.

프로그램 목록에 프로그램을 더 추가하려면 최대 1,000개의 프로그램을 수용할 수 있는 ofcscan.ini 파일에 프로그램을 추가해야 합니다. ofcscan.ini 파일에 프로그램을 추가하는 방법에 대한 자세한 내용은 ofcscan.ini를 사용하여 장치 제어 목록에 프로그램 추가 페이지 10-16를 참조하십시오.

경고!

ofcscan.ini 파일에 추가된 프로그램은 루트 도메인에 배포되며 개별 도메인 및 에이전트에 있는 프로그램을 덮어씁니다.

디지털 서명 공급자 지정

공급자가 발급한 프로그램을 신뢰하는 경우 디지털 서명 공급자를 지정합니다. 예를 들어 Microsoft Corporation 또는 Trend Micro, Inc를 입력합니다. 디지털 서

명 공급자를 가져오려면 프로그램 등록정보를 확인하면 됩니다(예: 프로그램을 마우스 오른쪽 단추로 클릭하고 **속성** 선택).

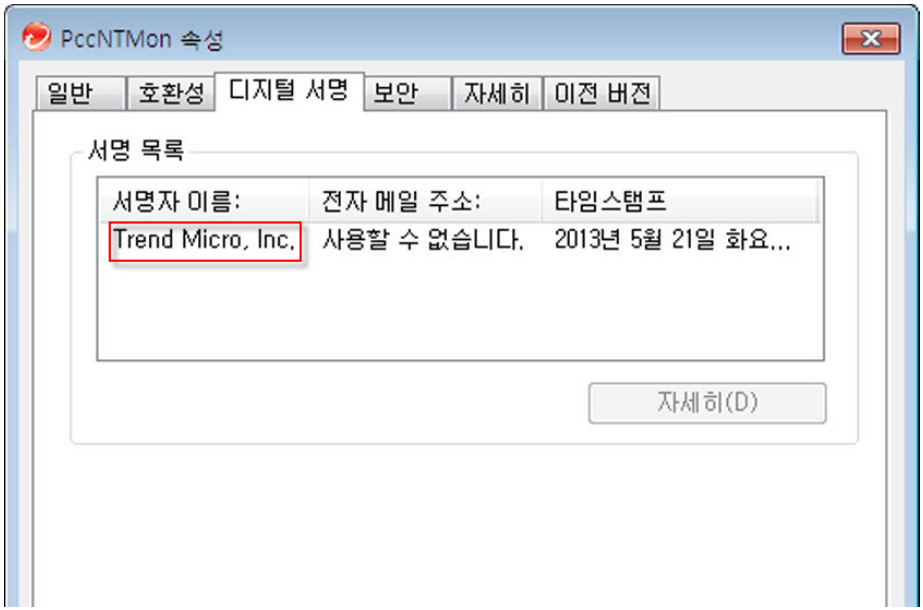


그림 10-1. OfficeScan 에이전트 프로그램의 디지털 서명 공급자(PccNTMon.exe)

프로그램 경로 및 이름 지정

프로그램 경로 및 이름은 259자 이내여야 하며 영숫자 문자(A~Z, a~z, 0~9)만 포함해야 합니다. 프로그램 이름만 지정할 수는 없습니다.

드라이브 문자 및 프로그램 이름 자리에 와일드카드를 사용할 수 있습니다. 드라이브 문자와 같은 단일 문자 데이터를 나타내려면 물음표(?)를 사용하고, 프로그램 이름과 같은 다중 문자 데이터를 나타내려면 별표(*)를 사용합니다.

참고

와일드카드를 사용하여 폴더 이름을 나타낼 수는 없습니다. 폴더 이름은 정확하게 지정해야 합니다.

와일드카드가 올바르게 사용된 경우의 예는 다음과 같습니다.

표 10-5. 와일드카드의 올바른 사용법

예	일치하는 데이터
?:\Password.exe	모든 드라이브 바로 아래에 있는 "Password.exe" 파일
C:\Program Files\Microsoft *.exe	파일 확장자가 있는 C:\Program Files의 모든 파일
C:\Program Files*.*	파일 확장자가 있는 C:\Program Files의 모든 파일
C:\Program Files\a**?**c.exe	문자 "a"로 시작하고 문자 "c"로 끝나는 3자로 된 C:\Program Files의 모든 .exe 파일
C:*	파일 확장자 여부에 관계없이 C:\ 드라이브 바로 아래에 있는 모든 파일

와일드카드가 잘못 사용된 경우의 예는 다음과 같습니다.

표 10-6. 와일드카드의 잘못된 사용법

예	이유
??:\Buffalo\Password.exe	?? 는 2자를 나타내는데, 드라이브 문자는 1자로 된 영숫자 문자입니다.
***:\Buffalo\Password.exe	*는 다중 문자 데이터를 나타내는데, 드라이브 문자는 단일 영숫자 문자로만 되어 있습니다.
C:*\Password.exe	와일드카드를 사용하여 폴더 이름을 나타낼 수는 없습니다. 폴더 이름은 정확하게 지정해야 합니다.
C:**?**\Password.exe	

비저장 장치에 대한 권한

비저장 장치에 대한 액세스를 허용하거나 차단할 수 있습니다. 이러한 장치에 대한 개별 권한 또는 고급 권한은 없습니다.

외부 장치에 대한 액세스 관리(데이터 보호가 활성화된 경우)

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **장치 제어 설정**을 클릭합니다.
4. **외부 에이전트** 탭을 클릭하여 외부 에이전트에 대한 설정을 구성하거나 **내부 에이전트** 탭을 클릭하여 내부 에이전트에 대한 설정을 구성합니다.
5. **장치 제어 사용**을 선택합니다.
6. 다음과 같이 설정을 적용합니다.
   - **외부 에이전트** 탭을 클릭한 경우 **내부 에이전트에 모든 설정 적용**을 선택하여 내부 에이전트에 설정을 적용할 수 있습니다.
   - **내부 에이전트** 탭을 클릭한 경우 **외부 에이전트에 모든 설정 적용**을 선택하여 외부 에이전트에 설정을 적용할 수 있습니다.

   확인 메시지가 나타납니다. 배포 명령이 모든 에이전트에 전파될 때까지 어느 정도의 시간이 소요될 수 있습니다.
7. USB 저장 장치에서 자동 실행 기능(autorun.inf)을 허용할지 또는 차단할지 선택합니다.
8. 저장 장치에 대한 설정을 구성합니다.
   a. 각 저장 장치에 대한 권한을 선택합니다.

      권한에 대한 자세한 내용은 저장 장치에 대한 권한 페이지 10-4을 참조하십시오.

   b. USB 저장 장치에 대한 권한이 **차단**인 경우 승인된 장치 목록을 구성합니다. 권한을 사용하여 액세스 수준을 제어할 수 있으며 사용자가 이러한 장치에 액세스할 수 있습니다.

승인된 USB 장치 목록 구성 페이지 10-13를 참조하십시오.

9. 각 비저장 장치에 대해 **허용** 또는 **차단**을 선택합니다.

10. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

    - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
    - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

고급 권한 구성

사용자 인터페이스에서 특정 저장 장치에 대한 고급 권한 및 알림을 구성할 수 있지만 실제로 권한 및 알림은 모든 저장 장치에 적용됩니다. 즉, CD/DVD에 대해 **고급 권한 및 알림**을 클릭한 경우 실제로는 모든 저장 장치에 대한 권한 및 알림을 정의하게 됩니다.

참고

고급 권한에 대한 자세한 내용 및 고급 권한이 있는 프로그램을 올바르게 정의하는 방법은 저장 장치에 대한 고급 권한 페이지 10-6을 참조하십시오.

절차

1. **고급 권한 및 알림**을 클릭합니다.

   새 화면이 열립니다.

2. **저장 장치에 대한 읽기 및 쓰기 권한이 있는 프로그램** 아래에 프로그램 경로 및 파일 이름을 입력하고 **추가**를 클릭합니다.

   디지털 서명 공급자는 사용할 수 없습니다.

3. **저장 장치에서 실행할 수 있는 프로그램** 아래에 프로그램 경로 및 이름 또는 디지털 서명 공급자를 입력하고 **추가**를 클릭합니다.

4. **OfficeScan에서 장치에 대한 무단 액세스를 탐지한 경우 엔드포인트에 알림 메시지 표시**를 선택합니다.

   - 장치에 대한 무단 액세스는 금지된 장치 작업을 의미합니다. 예를 들어 장치 권한이 "읽기"인 경우 사용자는 장치에서 파일을 저장, 이동, 삭제 또는 실행할 수 없습니다.
   - 알림 메시지를 수정할 수 있습니다. 자세한 내용은 장치 제어 알림 수정 페이지 10-18를 참조하십시오.

5. **뒤로**를 클릭합니다.

승인된 USB 장치 목록 구성

승인된 USB 장치 목록에는 별표(*) 와일드카드를 사용할 수 있습니다. 필드를 별표(*)로 바꾸면 다른 필드를 충족하는 장치를 모두 포함할 수 있습니다. 예를 들어 [vendor]-[model]-*로 지정하면 일련 ID에 관계없이 지정된 공급업체 및 지정된 모델 유형의 USB 장치가 모두 승인된 목록에 포함됩니다.

절차

1. **승인된 장치**를 클릭합니다.
2. 장치 공급업체를 입력합니다.
3. 장치 모델 및 일련 ID를 입력합니다.

   팁

   장치 목록 도구를 사용하여 엔드포인트에 연결된 장치를 쿼리합니다. 이 도구는 각 장치의 장치 공급업체, 모델 및 일련 ID 를 제공합니다.

4. 장치에 대한 권한을 선택합니다.

   권한에 대한 자세한 내용은 저장 장치에 대한 권한 페이지 10-4을 참조하십시오.

5. 장치를 더 추가하려면 더하기(+) 아이콘을 클릭합니다.

6. **< 뒤로**를 클릭합니다.

장치 목록 도구

각 엔드포인트에서 장치 목록 도구를 로컬로 실행하여 해당 엔드포인트에 연결된 외부 장치를 쿼리할 수 있습니다. 이 도구는 엔드포인트에서 외부 장치를 검색하여 브라우저 창에 장치 정보를 표시합니다. 이 정보를 사용하여 데이터 손실 방지 및 장치 제어에 대한 장치 설정을 구성할 수 있습니다.

장치 목록 도구 실행

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더 페이지 xv>₩PCCSRV ₩Admin₩Utility₩ListDeviceInfo로 이동합니다.
2. listDeviceInfo.exe를 대상 엔드포인트에 복사합니다.
3. 해당 엔드포인트에서 listDeviceInfo.exe를 실행합니다.
4. 표시되는 브라우저 창에서 장치 정보를 확인합니다. 데이터 손실 방지 및 장치 제어에서 사용하는 정보는 다음과 같습니다.
   - 공급업체(필수)
   - 모델(선택)
   - 일련 ID(선택)

외부 장치에 대한 액세스 관리(데이터 보호가 활성화되지 않은 경우)

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **장치 제어 설정**을 클릭합니다.
4. **외부 에이전트** 탭을 클릭하여 외부 에이전트에 대한 설정을 구성하거나 **내부 에이전트** 탭을 클릭하여 내부 에이전트에 대한 설정을 구성합니다.
5. **장치 제어 사용**을 선택합니다.
6. 다음과 같이 설정을 적용합니다.
   - **외부 에이전트** 탭을 클릭한 경우 **내부 에이전트에 모든 설정 적용**을 선택하여 내부 에이전트에 설정을 적용할 수 있습니다.
   - **내부 에이전트** 탭을 클릭한 경우 **외부 에이전트에 모든 설정 적용**을 선택하여 외부 에이전트에 설정을 적용할 수 있습니다.

   확인 메시지가 나타납니다. 배포 명령이 모든 에이전트에 전파될 때까지 어느 정도의 시간이 소요될 수 있습니다.
7. USB 저장 장치에서 자동 실행 기능(autorun.inf)을 허용할지 또는 차단할지 선택합니다.
8. 각 저장 장치에 대한 권한을 선택합니다.
9. 저장 장치에 대한 권한이 **수정**, **읽기 및 실행**, **읽기** 또는 **장치 콘텐츠만 나열**인 경우 고급 권한 및 알림을 구성합니다.

   고급 권한 구성 페이지 10-12를 참조하십시오.
10. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

ofcscan.ini를 사용하여 장치 제어 목록에 프로그램 추가

참고

목록에 대한 자세한 내용 및 목록에 추가할 수 있는 프로그램을 올바르게 정의하는 방법은 저장 장치에 대한 고급 권한 페이지 10-6을 참조하십시오.

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV로 이동합니다.
2. 텍스트 편집기를 사용하여 ofcscan.ini를 엽니다.
3. 저장 장치에 대한 읽기 및 쓰기 권한이 있는 프로그램을 추가하려면
   a. 다음 줄로 이동합니다.

      ```
      [DAC_APPROVED_LIST]
      Count=x
      ```

   b. "x"를 프로그램 목록에 있는 프로그램 수로 바꿉니다.
   c. "Count=x" 아래에 다음을 입력하여 프로그램을 추가합니다.

      ```
      항목<번호>=<프로그램 경로 및 이름 또는 디지털 서명 공급자>
      ```

      예:

      ```
      [DAC_APPROVED_LIST]
      Count=3
      ```

```
Item0=C:₩Program Files₩program.exe

Item1=?:₩password.exe

Item2=Microsoft Corporation
```

4. 저장 장치에서 실행할 수 있는 프로그램을 추가하려면

   a. 다음 줄로 이동합니다.

   ```
   [DAC_EXECUTABLE_LIST]

   Count=x
   ```

   b. "x"를 프로그램 목록에 있는 프로그램 수로 바꿉니다.

   c. "Count=x" 아래에 다음을 입력하여 프로그램을 추가합니다.

   항목<번호>=<프로그램 경로 및 이름 또는 디지털 서명 공급자>

   예:

   ```
   [DAC_EXECUTABLE_LIST]

   Count=3

   Item0=?:\Installer\Setup.exe

   Item1=E:\*.exe

   Item2=Trend Micro, Inc.
   ```

5. ofcscan.ini 파일을 저장하고 닫습니다.

6. OfficeScan 웹 콘솔을 열고 **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.

7. **저장**을 클릭하여 모든 에이전트에 프로그램 목록을 배포합니다.

장치 제어 알림 수정

장치 제어 위반이 발생하면 엔드포인트에 알림 메시지가 표시됩니다. 필요한 경우 관리자는 기본 알림 메시지를 수정할 수 있습니다.

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 **장치 제어 위반**을 선택합니다.
3. 제공된 텍스트 상자에서 기본 메시지를 수정합니다.
4. **저장**을 클릭합니다.

장치 제어 로그

OfficeScan 에이전트는 무단 장치 액세스 인스턴스를 기록하고 해당 로그를 서버에 보냅니다. 계속 실행하는 에이전트는 로그를 집계하고 1시간 후에 전송합니다. 다시 시작된 에이전트는 마지막으로 로그가 서버로 전송된 시간을 확인합니다. 경과된 시간이 1시간을 초과한 경우, 에이전트가 즉시 로그를 전송합니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

장치 제어 로그 보기

참고

저장 장치에 액세스하려고 할 때만 로그 데이터가 생성됩니다. OfficeScan 에이전트는 **비저장 장치**에 대한 액세스는 구성된 대로 차단하거나 허용하지만 조치를 기록하지는 않습니다.

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **장치 제어 로그** 또는 **로그 보기** > **장치 제어 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.
   - 권한 없는 액세스가 발견된 날짜/시간
   - 외부 장치가 연결되어 있거나 네트워크 리소스가 매핑된 엔드포인트
   - 외부 장치가 연결되어 있거나 네트워크 리소스가 매핑된 엔드포인트 도메인
   - 액세스된 장치 유형 또는 네트워크 리소스
   - 대상, 즉 액세스된 장치 또는 네트워크 리소스에 있는 항목
   - 액세스가 시작된 위치를 지정하는 액세스한 사용자
   - 대상에 설정된 권한
6. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

장 11

데이터 손실 방지 사용

이 장에서는 데이터 손실 방지 기능을 사용하는 방법을 설명합니다.

다음과 같은 항목이 포함됩니다.

- DLP(데이터 손실 방지) 정보 페이지 11-2
- 데이터 손실 방지 정책 페이지 11-3
- 데이터 식별자 유형 페이지 11-5
- 데이터 손실 방지 템플릿 페이지 11-19
- DLP 채널 페이지 11-23
- 데이터 손실 방지 조치 페이지 11-38
- 데이터 손실 방지 예외 페이지 11-40
- 데이터 손실 방지 정책 구성 페이지 11-45
- 데이터 손실 방지 알림 페이지 11-51
- 데이터 손실 방지 로그 페이지 11-55

DLP(데이터 손실 방지) 정보

기존 보안 솔루션은 외부 보안 위협이 네트워크에 침투하는 것을 방지하는 데 중점을 둡니다. 오늘날의 보안 환경에서 이러한 방식은 반쪽짜리 해결책에 불과합니다. 조직의 기밀 데이터와 중요한 데이터(이하 "디지털 자산")가 외부의 권한 없는 당사자에게 노출되는 데이터 위반이 공공연하게 발생하고 있습니다. 이러한 데이터 위반은 내부 직원의 실수나 부주의, 데이터 아웃소싱, 컴퓨팅 장치의 도난 또는 분실, 악의적인 공격 등에 의해 발생할 수 있습니다.

데이터 위반은 다음과 같은 결과를 초래할 수 있습니다.

- 브랜드 평판 저해
- 고객 신뢰도 실추
- 불필요한 개선 비용 및 규정 위반에 따른 벌금
- 비즈니스 기회 및 매출 상실(지적 재산권 도난 시)

데이터 위반이 만연하는 현실과 그 결과의 심각성을 인식한 조직에서는 이제 디지털 자산 보호를 보안 인프라의 매우 중요한 구성 요소로 간주하고 있습니다.

데이터 손실 방지는 우발적이거나 계획적인 유출로부터 조직의 중요한 데이터를 보호합니다. 데이터 손실 방지를 통해 다음을 수행할 수 있습니다.

- 데이터 식별자를 사용하여 보호해야 하는 중요한 정보 식별
- 전자 메일 및 외부 장치와 같은 일반적인 전송 채널을 통한 디지털 자산의 전송을 제한하거나 방지하는 정책 생성
- 설정된 개인 정보 표준에 준수 적용

중요한 정보를 모니터링하여 잠재적인 손실을 예방하려면 먼저 다음과 같은 질문에 대답할 수 있어야 합니다.

- 권한 없는 사용자로부터 보호해야 하는 데이터는 무엇입니까?
- 중요한 데이터가 어디에 있습니까?
- 중요한 데이터가 어떤 방식으로 전송됩니까?

- 중요한 데이터에 액세스하거나 전송할 권한이 있는 사용자는 누구입니까?
- 보안 위반이 발생한 경우 어떤 조치를 취해야 합니까?

이 중요한 감사에는 일반적으로 조직의 중요한 정보에 대해 잘 알고 있는 여러 부서와 담당자가 참여합니다.

중요한 정보와 보안 정책을 이미 정의한 경우 데이터 식별자와 회사 정책을 정의할 수 있습니다.

데이터 손실 방지 정책

OfficeScan에서는 DLP 정책에 정의된 규칙 집합을 기준으로 파일 또는 데이터를 평가합니다. 정책은 무단 전송을 방지해야 하는 파일 또는 데이터와, 전송을 탐지한 경우 OfficeScan에서 수행할 조치를 결정합니다.

참고

OfficeScan에서는 서버와 OfficeScan 에이전트 간의 데이터 전송을 모니터링하지 않습니다.

OfficeScan을 통해 관리자는 내부 및 외부 OfficeScan 에이전트에 대한 정책을 구성할 수 있습니다. 관리자는 일반적으로 외부 에이전트에 대해 더 엄격한 정책을 구성합니다.

관리자는 특정 정책을 에이전트 그룹이나 개별 에이전트에 적용할 수 있습니다.

정책을 배포하면 에이전트에서 **엔드포인트 위치** 화면(엔드포인트 위치 페이지 15-2 참조)에 설정된 위치 기준을 사용하여 정확한 위치 설정 및 적용할 정책을 확인합니다. 에이전트는 위치가 변경될 때마다 정책을 전환합니다.

정책 구성

다음 설정을 구성하고 선택한 에이전트에 배포하여 DLP 정책을 정의합니다.

표 11-1. DLP 정책을 정의하는 설정

설정	설명
규칙	DLP 규칙은 여러 템플릿, 채널 및 조치로 구성될 수 있습니다. 각 규칙은 포괄하는 DLP 정책의 하위 집합입니다. **참고** 데이터 손실 방지 기능은 규칙과 템플릿을 우선 순위에 따라 처리합니다. 규칙을 "그대로 두기"로 설정하는 경우 데이터 손실 방지 기능은 목록에 있는 다음 규칙을 처리합니다. 규칙을 "차단" 또는 "사용자 정당성"으로 설정하는 경우 데이터 손실 방지 기능은 사용자 조치를 차단하거나 허용하고 해당 규칙/템플릿을 추가로 처리하지 않습니다.
템플릿	DLP 템플릿은 데이터 식별자와 논리 연산자(And, Or, Except)를 조합하여 조건문을 구성합니다. 특정 조건문을 충족하는 파일 또는 데이터에만 DLP 규칙이 적용됩니다. 데이터 손실 방지 기능은 미리 정의된 템플릿 집합을 함께 제공하며 관리자가 사용자 정의 템플릿을 만들 수도 있습니다. DLP 규칙은 템플릿을 하나 이상 포함할 수 있습니다. 데이터 손실 방지 기능은 템플릿을 확인할 때 첫 번째 일치 규칙을 사용합니다. 즉, 파일 또는 데이터가 템플릿의 데이터 식별자와 일치하는 경우 데이터 손실 방지 기능은 다른 템플릿을 더 이상 확인하지 않습니다.
채널	채널은 중요한 정보를 전송하는 엔터티입니다. 데이터 손실 방지 기능은 전자 메일, 이동식 저장 장치 및 인스턴트 메시징 응용 프로그램과 같은 널리 사용되는 전송 채널을 지원합니다.
조치	데이터 손실 방지 기능은 채널을 통해 중요한 정보를 전송하려는 시도를 탐지한 경우 하나 이상의 조치를 수행합니다.
예외	예외는 구성된 DLP 규칙을 재정의하는 데 사용됩니다. 예외를 구성하여 모니터링되지 않는 대상, 모니터링되는 대상 및 압축 파일 검색을 관리할 수 있습니다.
데이터 식별자	데이터 손실 방지 기능은 데이터 식별자를 사용하여 중요한 정보를 식별합니다. 데이터 식별자는 식, 파일 특성 및 키워드를 포함하여 DLP 템플릿의 구성 요소로 사용됩니다.

데이터 식별자 유형

디지털 자산은 조직에서 무단 전송으로부터 보호해야 하는 파일 및 데이터입니다. 관리자는 다음과 같은 데이터 식별자를 사용하여 디지털 자산을 정의할 수 있습니다.

- **식:** 특정 구조를 가진 데이터

  자세한 내용은 식 페이지 11-5를 참조하십시오.

- **파일 특성:** 파일 형식 및 파일 크기와 같은 파일 등록정보

  자세한 내용은 파일 특성 페이지 11-10를 참조하십시오.

- **키워드 목록:** 특정 단어나 구의 목록

  자세한 내용은 키워드 페이지 11-13를 참조하십시오.

참고

관리자는 DLP 템플릿에서 사용 중인 데이터 식별자는 삭제할 수 없습니다. 데이터 식별자를 삭제하려면 먼저 템플릿을 삭제하십시오.

식

식은 특정 구조를 가진 데이터입니다. 예를 들어 신용 카드 번호는 일반적으로 16자리 숫자이며 식 기반 탐지에 적합하도록 "nnnn-nnnn-nnnn-nnnn" 포맷으로 표시됩니다.

관리자는 미리 정의된 식과 사용자 정의 식을 사용할 수 있습니다.

자세한 내용은 미리 정의된 식 페이지 11-5 및 사용자 정의 식 페이지 11-6를 참조하십시오.

미리 정의된 식

데이터 손실 방지 기능은 미리 정의된 식의 집합을 제공합니다. 이러한 식은 수정하거나 삭제할 수 없습니다.

데이터 손실 방지 기능은 패턴 일치 및 수학 방정식을 사용하여 이러한 식을 확인합니다. 데이터 손실 방지에서 잠재적으로 중요한 데이터를 식과 일치시킨 후 데이터에 대해 추가 확인 과정이 진행될 수도 있습니다.

미리 정의된 식의 전체 목록은 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx에서 *데이터 보호 목록* 문서를 참조하십시오.

미리 정의된 식에 대한 설정 보기

참고

미리 정의된 식은 수정하거나 삭제할 수 없습니다.

절차

1. **에이전트** > **데이터 손실 방지** > **데이터 식별자**로 이동합니다.
2. **식** 탭을 클릭합니다.
3. 식 이름을 클릭합니다.
4. 화면이 열리면 설정을 확인합니다.

사용자 정의 식

미리 정의된 식이 회사의 요구 사항에 적합하지 않은 경우 사용자 정의 식을 만듭니다.

식은 강력한 문자열 일치 도구입니다. 식을 만들기 전에 식 구문을 잘 알고 있어야 합니다. 잘못 작성된 식은 성능을 크게 저하시킬 수 있습니다.

식을 만들 때

- 미리 정의된 식을 참조하여 올바른 식을 정의합니다. 예를 들어 날짜가 포함된 식을 만드는 경우 "Date" 접두사가 있는 식을 참조할 수 있습니다.
- 데이터 손실 방지에서는 PCRE(Perl Compatible Regular Expressions)에 정의된 식 포맷을 따릅니다. PCRE에 대한 자세한 내용은 다음 웹 사이트를 참조하십시오.

http://www.pcre.org/

- 간단한 식으로 시작합니다. 잘못된 경보가 발생하는 경우 식을 수정하거나 식을 미세 조정하여 탐지 기능을 개선합니다.

식을 만들 때 관리자는 여러 기준 중에서 선택할 수 있습니다. 데이터 손실 방지 기능에서 DLP 정책에 적용하려면 식이 선택한 기준을 충족해야 합니다. 여러 기준 옵션에 대한 자세한 내용은 사용자 정의 식에 대한 기준 페이지 11-7을 참조하십시오.

사용자 정의 식에 대한 기준

표 11-2. 사용자 정의 식에 대한 기준 옵션

기준	규칙	예
없음	없음	모두 - 미국 인구 조사국(US Census Bureau)의 이름 • 식: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]
특정 문자	식이 지정한 문자를 포함해야 합니다. 또한 식의 문자 수가 최소값 및 최대값 제한 내에 있어야 합니다.	미국 - 은행 고유 번호 • 식: [^\d]([0123678]\d{8})[^\d] • 문자: 0123456789 • 최소 문자 수: 9 • 최대 문자 수: 9

기준	규칙	예
접미사	접미사는 식의 마지막 세그먼트를 나타냅니다. 접미사는 지정한 문자를 포함하고 특정 개수의 문자가 있어야 합니다. 또한 식의 문자 수가 최소값 및 최대값 제한 내에 있어야 합니다.	모두 - 집 주소 • 식: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2}(lane|ln|street|st|avenue|ave|road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\ s\d{5}(-\d{4})?)[^\d-] • 접미사 문자: 0123456789- • 문자 수: 5 • 식의 최소 문자 수: 25 • 식의 최대 문자 수: 80
단일 문자 구분 기호	식이 하나의 문자로 구분된 두 개의 세그먼트로 구성되어야 합니다. 문자 길이는 1바이트여야 합니다. 또한 구분 기호 왼쪽의 문자 수가 최소값 및 최대값 제한 내에 있어야 합니다. 구분 기호 오른쪽의 문자 수가 최대값 제한을 초과하지 않아야 합니다.	모두 - 전자 메일 주소 • 식: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • 구분 기호: @ • 왼쪽의 최소 문자 수: 3 • 왼쪽의 최대 문자 수: 15 • 오른쪽의 최대 문자 수: 30

사용자 정의 식 만들기

절차

1. **에이전트** > **데이터 손실 방지** > **데이터 식별자**로 이동합니다.
2. **식** 탭을 클릭합니다.
3. **추가**를 클릭합니다.

   새 화면이 표시됩니다.
4. 식 이름을 입력합니다. 이름은 길이가 100바이트 이내여야 하고 다음 문자를 포함할 수 없습니다.

- > < * ^ | & ? \ /

5. 256바이트 이내의 설명을 입력하십시오.
6. 표시되는 데이터를 입력합니다.

   예를 들어 ID 번호에 대한 식을 만들려면 샘플 ID 번호를 입력합니다. 이 데이터는 참조용으로만 사용되며 제품 내에 표시되지 않습니다.
7. 다음 기준 중 하나를 선택하고 해당 기준에 대한 추가 설정을 구성합니다 (사용자 정의 식에 대한 기준 페이지 11-7 참조).

   - 없음
   - 특정 문자
   - 접미사
   - 단일 문자 구분 기호
8. 실제 데이터에 대해 식을 테스트합니다.

   예를 들어 국가 ID에 대한 식이 있는 경우 **테스트 데이터** 텍스트 상자에 유효한 ID 번호를 입력하고 **테스트**를 클릭한 다음 결과를 확인합니다.
9. 결과에 만족하는 경우 **저장**을 클릭합니다.

참고

테스트에 성공한 경우에만 설정을 저장하십시오. 데이터를 탐지할 수 없는 식은 시스템 리소스를 낭비하고 성능에 영향을 줄 수 있습니다.

10. 에이전트에 설정을 배포하도록 알리는 메시지가 나타납니다. **닫기**를 클릭합니다.
11. **DLP 데이터 식별자** 화면으로 돌아와서 **모든 에이전트에 적용**을 클릭합니다.

사용자 정의 식 가져오기

식이 포함된 올바른 포맷의 .dat 파일이 있는 경우 이 옵션을 사용합니다. 현재 액세스 중인 서버 또는 다른 서버에서 식을 내보내 파일을 생성할 수 있습니다.

참고

이 데이터 손실 방지 버전에서 생성한 .dat 식 파일은 이전 버전과 호환되지 않습니다.

절차

1. **에이전트** > **데이터 손실 방지** > **데이터 식별자**로 이동합니다.
2. **식** 탭을 클릭합니다.
3. **가져오기**를 클릭한 다음 식이 포함된 .dat 파일을 찾습니다.
4. **열기**를 클릭합니다.

   가져오기 성공 여부를 알리는 메시지가 표시됩니다. 가져오려는 식이 이미 있는 경우에는 메시지가 생략됩니다.
5. **모든 에이전트에 적용**을 클릭합니다.

파일 특성

파일 특성은 파일의 특정 등록정보입니다. 데이터 식별자를 정의할 때 두 가지 파일 특성, 즉 파일 형식과 파일 크기를 사용할 수 있습니다. 예를 들어 소프트웨어 개발 회사에서는 회사 소프트웨어 설치 관리자의 공유를 소프트웨어 개발 및 테스트를 담당하는 R&D 부서로 제한할 수 있습니다. 이 경우 OfficeScan 관리자는 R&D를 제외한 모든 부서에 대해 크기가 10~40MB인 실행 파일의 전송을 차단하는 정책을 만들 수 있습니다.

파일 특성 자체는 중요한 파일의 식별자로 적절하지 않습니다. 이 항목의 예를 계속 들자면, 다른 부서에서 공유한 타사 소프트웨어 설치 관리자는 차단될 가능성이 높습니다. 따라서 보다 명확한 대상을 지정하여 중요한 파일을 탐지하려면 Trend Micro에서는 파일 특성과 다른 DLP 데이터 식별자를 함께 사용할 것을 권장합니다.

지원되는 파일 형식의 전체 목록은 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx에서 *데이터 보호 목록* 문서를 참조하십시오.

미리 정의된 파일 특성 목록

데이터 손실 방지 기능은 미리 정의된 파일 특성 목록을 제공합니다. 이러한 목록은 수정하거나 삭제할 수 없습니다. 목록에는 템플릿에서 정책 위반을 트리거해야 하는지를 결정하는 고유한 조건이 기본 제공됩니다.

미리 정의된 파일 특성 목록을 사용하여 데이터 레코더(CD/DVD)에 대한 액세스를 제한할 수 있습니다.

자세한 내용은 데이터 레코더(CD/DVD)에 대한 액세스 차단 페이지 11-33를 참조하십시오.

파일 특성 목록 만들기

절차

1. **에이전트** > **데이터 손실 방지** > **데이터 식별자**로 이동합니다.
2. **파일 특성** 탭을 클릭합니다.
3. **추가**를 클릭합니다.

   새 화면이 표시됩니다.
4. 파일 특성 목록의 이름을 입력합니다. 이름은 길이가 100바이트 이내여야 하고 다음 문자를 포함할 수 없습니다.

   - > < * ^ | & ? \ /
5. 256바이트 이내의 설명을 입력하십시오.
6. 원하는 실제 파일 형식을 선택합니다.
7. 포함하려는 파일 형식이 목록에 없는 경우 **파일 확장자**를 선택하고 해당 파일 형식의 확장자를 입력합니다. 데이터 손실 방지 기능은 지정된 확장자를 가진 파일을 확인하지만 실제 파일 형식을 확인하지는 않습니다. 파일 확장자를 지정할 때의 지침은 다음과 같습니다.

   - 각 확장자는 별표(*)로 시작하고 그 뒤에 마침표(.)와 확장자가 차례로 와야 합니다. 별표는 파일의 실제 이름을 나타내는 와일드카드입니다. 예를 들어 *.pol은 12345.pol, test.pol 등과 일치합니다.

- 확장자에 와일드카드를 포함할 수 있습니다. 단일 문자를 나타내려면 물음표(?)를 사용하고 두 자 이상의 문자를 나타내려면 별표(*)를 사용합니다. 다음 예를 참조하십시오.

  - *.*m은 ABC.dem, ABC.prm, ABC.sdcm 파일과 일치합니다.

  - *.m*r은 ABC.mgdr, ABC.mtp2r, ABC.mdmr 파일과 일치합니다.

  - *.fm?은 ABC.fme, ABC.fml, ABC.fmp 파일과 일치합니다.

- 확장자 끝에 별표를 추가할 때는 주의해야 합니다. 파일 이름 및 관련 없는 확장자의 일부와 일치할 수도 있기 때문입니다. 예를 들어 *.do*는 abc.doctor_john.jpg, abc.donor12.pdf 등과 일치합니다.

- 세미콜론(;)을 사용하여 파일 확장자를 구분합니다. 세미콜론 뒤에 공백을 추가할 필요는 없습니다.

8. 최소 및 최대 파일 크기를 바이트 단위로 입력합니다. 두 파일 크기 모두 0보다 큰 정수여야 합니다.

9. **저장**을 클릭합니다.

10. 에이전트에 설정을 배포하도록 알리는 메시지가 나타납니다. **닫기**를 클릭합니다.

11. **DLP 데이터 식별자** 화면으로 돌아와서 **모든 에이전트에 적용**을 클릭합니다.

파일 특성 목록 가져오기

이 옵션은 특성 목록이 포함된 올바른 포맷의 .dat 파일이 있는 경우에 사용합니다. 현재 액세스 중인 서버 또는 다른 서버에서 파일 특성 목록을 내보내 파일을 생성할 수 있습니다.

참고

이 데이터 손실 방지 버전에서 생성한 .dat 파일 특성 파일은 이전 버전과 호환되지 않습니다.

절차

1. **에이전트** > **데이터 손실 방지** > **데이터 식별자**로 이동합니다.
2. **파일 특성** 탭을 클릭합니다.
3. **가져오기**를 클릭한 다음 파일 특성 목록이 포함된 .dat 파일을 찾습니다.
4. **열기**를 클릭합니다.

   가져오기 성공 여부를 알리는 메시지가 표시됩니다. 가져오려는 파일 특성 목록이 이미 있는 경우에는 메시지가 생략됩니다.
5. **모든 에이전트에 적용**을 클릭합니다.

키워드

키워드는 특정 단어나 구입니다. 키워드 목록에 관련 키워드를 추가하여 데이터의 특정 유형을 식별할 수 있습니다. 예를 들어 "prognosis", "blood type", "vaccination" 및 "physician"은 의료 진단서에 표시될 수 있는 키워드입니다. 의료 진단서 파일의 전송을 방지하려면 DLP 정책에 이러한 키워드를 사용한 다음, 이러한 키워드가 포함된 파일을 차단하도록 데이터 손실 방지 기능을 구성하면 됩니다.

일반적으로 사용되는 단어를 조합하여 의미 있는 키워드를 구성할 수 있습니다. 예를 들어 "end", "read", "if" 및 "at"을 조합하여 "END-IF", "END-READ", "AT END" 등의 소스 코드에 사용되는 키워드를 구성할 수 있습니다.

미리 정의된 키워드 목록과 사용자 정의 키워드 목록을 사용할 수 있습니다. 자세한 내용은 미리 정의된 키워드 목록 페이지 11-13 및 사용자 정의 키워드 목록 페이지 11-15를 참조하십시오.

미리 정의된 키워드 목록

데이터 손실 방지에서는 미리 정의된 키워드 목록 집합을 제공합니다. 이러한 키워드 목록은 수정하거나 삭제할 수 없습니다. 각 목록에는 템플릿에서 정책 위반을 트리거해야 하는지를 결정하는 고유한 조건이 기본 제공됩니다.

데이터 손실 방지 기능의 미리 정의된 키워드 목록에 대한 자세한 내용은 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx에서 *데이터 보호 목록* 문서를 참조하십시오.

키워드 목록 작동 방식

키워드 수 조건

각 키워드 목록에는 문서에 특정 개수의 키워드를 요구하는 조건이 포함되어 있습니다. 이 조건을 충족하지 않으면 목록에서 위반을 트리거합니다.

키워드 수 조건은 다음 값을 포함합니다.

- **모두**: 목록의 모든 키워드가 문서에 있어야 합니다.
- **임의**: 목록의 키워드 중 하나가 문서에 있어야 합니다.
- **특정 개수**: 지정된 개수 이상의 키워드가 문서에 있어야 합니다. 문서의 키워드가 지정된 수보다 많으면 데이터 손실 방지 기능이 위반을 트리거합니다.

거리 조건

일부 목록에는 위반 여부를 결정하는 "거리" 조건이 포함되어 있습니다. "거리"는 한 키워드의 첫 번째 문자와 다른 키워드의 첫 번째 문자 사이에 있는 문자 수를 의미합니다. 다음 항목을 고려합니다.

F**irst Name:_John_ L**ast Name:_Smith_

Forms - 이름, 성 목록에는 50이라는 "거리" 조건이 지정되어 있고 "이름"과 "성"이라는 일반적으로 사용되는 양식 필드가 있습니다. 위 예의 경우 "First Name"의 "F"와 "Last Name"의 "L" 사이에 있는 문자 수가 18이므로 데이터 손실 방지 기능은 위반을 트리거합니다.

위반을 트리거하지 않는 항목의 예는 다음과 같습니다.

The f**irst name of our new employee from Switzerland is John. His l**ast name is Smith.

이 예에서는 "first name"의 "f"와 "last name"의 "l" 사이에 있는 문자 수가 61입니다. 이는 거리 임계값을 초과하므로 위반이 트리거되지 않습니다.

사용자 정의 키워드 목록

미리 정의된 키워드 목록이 요구 사항에 적합하지 않은 경우 사용자 정의 키워드 목록을 만듭니다.

키워드 목록을 구성할 때 선택할 수 있는 여러 기준이 있습니다. 키워드 목록이 선택한 기준을 충족해야 데이터 손실 방지 기능이 정책에 적용할 수 있습니다. 각 키워드 목록에 대해 다음 기준 중 하나를 선택합니다.

- **임의의 키워드**
- **모든 키워드**
- **<x>자 이내의 모든 키워드**
- **임계값을 초과하는 키워드 점수 합계**

기준 규칙에 대한 자세한 내용은 사용자 정의 키워드 목록 기준 페이지 11-15을 참조하십시오.

사용자 정의 키워드 목록 기준

표 11-3. 키워드 목록에 대한 기준

기준	규칙
임의의 키워드	키워드 목록에 있는 키워드 중 하나 이상이 파일에 포함되어야 합니다.
모든 키워드	키워드 목록에 있는 모든 키워드가 파일에 포함되어야 합니다.

기준	규칙
<x>자 이내의 모든 키워드	키워드 목록에 있는 모든 키워드가 파일에 포함되어야 합니다. 또한, 각 키워드 쌍은 서로 <x>자 이내여야 합니다. 예를 들어, 3개 키워드가 WEB, DISK 및 USB이고, 지정한 문자 수가 20이라고 가정해 보겠습니다. 데이터 손실 방지에서 DISK, WEB 및 USB의 순서로 모든 키워드가 발견되는 경우 "D"(DISK)에서 "W"(WEB), 그리고 "W"에서 "U"(USB)까지의 문자 수는 20자 또는 이하여야 합니다. 기준과 일치하는 데이터: DISK####WEB############USB 기준과 일치하지 않는 데이터: DISK******************WEB****USB("D"와 "W" 사이에 23자) 문자 수를 결정할 때는 작은 수(예: 10)를 사용하면 검색 시간이 단축되지만 상대적으로 작은 영역만 포함하게 된다는 점에 주의하십시오. 이 경우 특히 큰 파일에서 중요한 데이터를 발견할 가능성이 줄어들 수 있습니다. 숫자가 클수록 포함되는 영역도 증가하지만 검색 시간이 느려질 수 있습니다.
임계값을 초과하는 키워드 점수 합계	키워드 목록에 있는 키워드 중 하나 이상이 파일에 포함되어야 합니다. 하나의 키워드만 발견된 경우 해당 점수가 임계값보다 높아야 합니다. 여러 키워드가 발견된 경우 해당 점수 합계가 임계값보다 높아야 합니다. 각 키워드에 1에서 10 사이의 점수를 할당합니다. 매우 기밀한 단어나 구(예: HR 부서의 경우 "급여 인상")는 상대적으로 점수가 높아야 합니다. 자체로는 가중치가 크지 않은 단어나 구는 점수가 낮을 수 있습니다. 임계값을 구성할 때 키워드에 할당한 점수를 고려하십시오. 예를 들어 5개의 키워드가 있고 그 중 3개의 우선 순위가 높은 경우 임계값은 이 세 키워드의 점수 합계보다 낮거나 같을 수 있습니다. 이는 이 세 키워드가 발견된 것만으로도 파일을 중요한 파일로 간주할 수 있음을 의미합니다.

키워드 목록 만들기

절차

1. **에이전트** > **데이터 손실 방지** > **데이터 식별자**로 이동합니다.
2. **키워드** 탭을 클릭합니다.

3. **추가**를 클릭합니다.

   새 화면이 표시됩니다.

4. 키워드 목록의 이름을 입력합니다. 이름은 길이가 100바이트 이내여야 하고 다음 문자를 포함할 수 없습니다.

   - > < * ^ | & ? \ /

5. 256바이트 이내의 설명을 입력하십시오.

6. 다음 기준 중 하나를 선택하고 해당 기준에 대한 추가 설정을 구성합니다.

   - **임의의 키워드**
   - **모든 키워드**
   - **<x>자 이내의 모든 키워드**
   - **임계값을 초과하는 키워드 점수 합계**

7. 목록에 키워드를 수동으로 추가하려면

   a. 길이가 3~40바이트인 키워드를 입력하고 대/소문자를 구분하는지 지정합니다.

   b. **추가**를 클릭합니다.

8. "가져오기" 옵션을 사용하여 키워드를 추가하려면

   참고

   키워드가 포함된 올바른 포맷의 .csv 파일이 있는 경우 이 옵션을 사용합니다. 현재 액세스 중인 서버 또는 다른 서버에서 키워드를 내보내 파일을 생성할 수 있습니다.

   a. **가져오기**를 클릭한 다음 키워드가 포함된 .csv 파일을 찾습니다.

   b. **열기**를 클릭합니다.

   가져오기 성공 여부를 알리는 메시지가 표시됩니다. 가져오려는 키워드가 목록에 이미 있는 경우에는 메시지가 생략됩니다.

9. 키워드를 삭제하려면 키워드를 선택하고 **삭제**를 클릭합니다.
10. 키워드를 내보내려면

> **참고**
> "내보내기" 기능을 사용하여 키워드를 백업하거나 다른 서버로 가져올 수 있습니다. 키워드 목록의 모든 키워드를 내보냅니다. 개별 키워드를 내보낼 수는 없습니다.

    a. **내보내기**를 클릭합니다.
    b. 결과 .csv 파일을 원하는 위치에 저장합니다.
11. **저장**을 클릭합니다.
12. 에이전트에 설정을 배포하도록 알리는 메시지가 나타납니다. **닫기**를 클릭합니다.
13. **DLP 데이터 식별자** 화면으로 돌아와서 **모든 에이전트에 적용**을 클릭합니다.

키워드 목록 가져오기

이 옵션은 키워드 목록이 포함된 올바른 포맷의 .dat 파일이 있는 경우에 사용합니다. 현재 액세스 중인 서버 또는 다른 서버에서 키워드 목록을 내보내 파일을 생성할 수 있습니다.

> **참고**
> 이 데이터 손실 방지 버전에서 생성한 .dat 키워드 목록 파일은 이전 버전과 호환되지 않습니다.

절차

1. **에이전트** > **데이터 손실 방지** > **데이터 식별자**로 이동합니다.
2. **키워드** 탭을 클릭합니다.

3. **가져오기**를 클릭한 다음 키워드 목록이 포함된 .dat 파일을 찾습니다.
4. **열기**를 클릭합니다.

   가져오기 성공 여부를 알리는 메시지가 표시됩니다. 가져오려는 키워드 목록이 이미 있는 경우에는 메시지가 생략됩니다.
5. **모든 에이전트에 적용**을 클릭합니다.

데이터 손실 방지 템플릿

DLP 템플릿은 DLP 데이터 식별자와 논리 연산자(And, Or, Except)를 조합하여 조건문을 구성합니다. 특정 조건문을 충족하는 파일 또는 데이터에만 DLP 정책이 적용됩니다.

예를 들어 "고용 계약" 정책을 적용하려면 파일이 Microsoft Word 파일(파일 특성)이어야 하고 특정 법률 용어(키워드)를 포함해야 하며 ID 번호(식)를 포함해야 합니다. 이 정책을 통해 HR 담당자는 직원이 인쇄된 사본에 서명할 수 있도록 인쇄를 통해 파일을 전송할 수 있습니다. 전자 메일과 같은 다른 모든 가능한 채널을 통한 전송은 차단됩니다.

DLP 데이터 식별자를 구성한 경우 사용자 고유의 템플릿을 만들 수 있습니다. 또한 미리 정의된 템플릿을 사용할 수 있습니다. 자세한 내용은 사용자 정의 DLP 템플릿 페이지 11-20 및 미리 정의된 DLP 템플릿 페이지 11-19를 참조하십시오.

참고

DLP 정책에서 사용 중인 템플릿은 삭제할 수 없습니다. 템플릿을 삭제하려면 먼저 정책에서 제거하십시오.

미리 정의된 DLP 템플릿

데이터 손실 방지 기능은 여러 규정 표준을 준수하는 데 사용할 수 있는 다음과 같은 미리 정의된 템플릿 집합을 제공합니다. 이러한 템플릿은 수정하거나 삭제할 수 없습니다.

- **GLBA**: Gramm-Leach-Billey Act(금융서비스 현대화법)
- **HIPAA**: Health Insurance Portability and Accountability Act(건강보험 양도 및 책임에 관한 법)
- **PCI-DSS**: PCI-DSS(신용 카드 데이터 보안 표준)
- **SB-1386**: US Senate Bill 1386(미국 상원 법안 1386)
- **US PII**: United States Personally Identifiable Information(미국 개인 식별 정보)

미리 정의된 모든 템플릿의 용도가 상세하게 정리된 목록과 보호되는 데이터 예는 http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx에서 *데이터 보호 목록* 문서를 참조하십시오.

사용자 정의 DLP 템플릿

데이터 식별자를 구성한 경우 사용자 고유의 템플릿을 만듭니다. 템플릿은 데이터 식별자와 논리 연산자(And, Or, Except)를 조합하여 조건문을 구성합니다.

조건문과 논리 연산자의 작동 방식에 대한 자세한 내용 및 예는 조건문 및 논리 연산자 페이지 11-20를 참조하십시오.

조건문 및 논리 연산자

데이터 손실 방지 기능은 왼쪽에서 오른쪽으로 조건문을 평가합니다. 조건문을 구성할 때 논리 연산자를 신중하게 사용해야 합니다. 잘못 사용할 경우 조건문 오류로 인해 예기치 않은 결과가 발생할 수 있습니다.

다음 표의 예를 참조하십시오.

표 11-4. 샘플 조건문

조건문	해석 및 예
[데이터 식별자 1] **And** [데이터 식별자 2] **Except** [데이터 식별자 3]	파일이 [데이터 식별자 1]과 [데이터 식별자 2]를 충족하고 [데이터 식별자 3]을 충족하지 않아야 합니다. 예: 파일이 [Adobe PDF 문서]이고 [전자 메일 주소]를 포함해야 하지만 [키워드 목록의 모든 키워드]를 포함해서는 안 됩니다.
[데이터 식별자 1] **Or** [데이터 식별자 2]	파일이 [데이터 식별자 1] 또는 [데이터 식별자 2]를 충족해야 합니다. 예: 파일이 [Adobe PDF 문서] 또는 [a Microsoft Word 문서]여야 합니다.
Except [데이터 식별자 1]	파일이 [데이터 식별자 1]을 충족해서는 안 됩니다. 예: 파일이 [멀티미디어 파일]이 아니어야 합니다.

위 표의 마지막 예와 같이, 파일이 조건문의 모든 데이터 식별자를 충족해서는 안 되는 경우 조건문의 첫 번째 데이터 식별자에 "Except" 연산자를 포함할 수 있습니다. 그러나 대부분의 경우 첫 번째 데이터 식별자에는 연산자가 포함되지 않습니다.

템플릿 만들기

절차

1. **에이전트** > **데이터 손실 방지** > **DLP 템플릿**으로 이동합니다.
2. **추가**를 클릭합니다.

   새 화면이 표시됩니다.
3. 템플릿 이름을 입력합니다. 이름은 길이가 100바이트 이내여야 하고 다음 문자를 포함할 수 없습니다.

- > < * ^ | & ? \ /

4. 256바이트 이내의 설명을 입력하십시오.
5. 데이터 식별자를 선택하고 "추가" 아이콘을 클릭합니다.

   정의를 선택할 때 다음과 같이 할 수 있습니다.

   - Ctrl 키를 누른 채 데이터 식별자를 선택하여 여러 항목을 선택합니다.
   - 특정 정의를 찾으려는 경우 검색 기능을 사용합니다. 데이터 식별자의 전체 이름 또는 일부 이름을 입력할 수 있습니다.
   - 각 템플릿은 최대 30개의 데이터 식별자를 포함할 수 있습니다.
6. 새 식을 만들려면 **식**을 클릭한 다음 **새 식 추가**를 클릭합니다. 표시되는 화면에서 식에 대한 설정을 구성합니다.
7. 새 파일 특성 목록을 만들려면 **파일 특성**을 클릭한 다음 **새 파일 특성 추가**를 클릭합니다. 표시되는 화면에서 파일 특성 목록에 대한 설정을 구성합니다.
8. 새 키워드 목록을 만들려면 **키워드**를 클릭한 다음 **새 키워드 추가**를 클릭합니다. 표시되는 화면에서 키워드 목록에 대한 설정을 구성합니다.
9. 식을 선택한 경우 발생 횟수를 입력합니다. 이 횟수만큼 식이 발생해야 데이터 손실 방지 기능이 해당 식에 정책을 적용합니다.
10. 각 정의에 대한 논리 연산자를 선택합니다.

참고

조건문을 구성할 때 논리 연산자를 신중하게 사용해야 합니다. 잘못 사용할 경우 조건문 오류로 인해 예기치 않은 결과가 발생할 수 있습니다. 올바른 사용 예는 조건문 및 논리 연산자 페이지 11-20를 참조하십시오.

11. 선택한 식별자 목록에서 데이터 식별자를 제거하려면 휴지통 아이콘을 클릭합니다.
12. **미리 보기** 아래에서 조건문을 확인하고 의도한 문이 아닌 경우 변경합니다.
13. **저장**을 클릭합니다.

14. 에이전트에 설정을 배포하도록 알리는 메시지가 나타납니다. **닫기**를 클릭합니다.
15. **DLP 템플릿** 화면으로 돌아가서 **모든 에이전트에 적용**을 클릭합니다.

템플릿 가져오기

템플릿이 포함된 올바른 포맷의 .dat 파일이 있는 경우 이 옵션을 사용합니다. 현재 액세스 중인 서버 또는 다른 서버에서 템플릿을 내보내 파일을 생성할 수 있습니다.

참고

OfficeScan 10.6에서 DLP 템플릿을 가져오려면 먼저 연관된 데이터 식별자(이전에는 정의라고 함)를 가져와야 합니다. 데이터 손실 방지 기능은 연관된 데이터 식별자가 없는 템플릿을 가져올 수 없습니다.

절차

1. **에이전트** > **데이터 손실 방지** > **DLP 템플릿**으로 이동합니다.
2. **가져오기**를 클릭한 다음 템플릿이 포함된 .dat 파일을 찾습니다.
3. **열기**를 클릭합니다.

   가져오기 성공 여부를 알리는 메시지가 표시됩니다. 가져오려는 템플릿이 이미 있는 경우에는 메시지가 생략됩니다.
4. **모든 에이전트에 적용**을 클릭합니다.

DLP 채널

사용자는 여러 채널을 통해 중요한 정보를 전송할 수 있습니다. OfficeScan에서는 다음 채널을 모니터링할 수 있습니다.

- **네트워크 채널**: 중요한 정보가 HTTP 및 FTP와 같은 네트워크 프로토콜을 통해 전송됩니다.

- **시스템 및 응용 프로그램 채널**: 중요한 정보가 엔드포인트의 로컬 응용 프로그램 및 주변 기기를 통해 전송됩니다.

네트워크 채널

OfficeScan에서는 다음 네트워크 채널을 통한 데이터 전송을 모니터링할 수 있습니다.

- 전자 메일 클라이언트
- FTP
- HTTP 및 HTTPS
- IM 응용 프로그램
- SMB 프로토콜
- 웹 메일

모니터링할 데이터 전송을 결정하기 위해 OfficeScan에서는 전송 범위(사용자가 구성해야 함)를 확인합니다. 선택한 범위에 따라 OfficeScan에서는 모든 데이터 전송을 모니터링하거나 LAN(Local Area Network) 외부 전송만 모니터링합니다.

전송 범위에 대한 자세한 내용은 네트워크 채널의 전송 범위 및 대상 페이지 11-28을 참조하십시오.

전자 메일 클라이언트

OfficeScan에서는 여러 전자 메일 에이전트를 통해 전송되는 전자 메일을 모니터링합니다. 이 때 OfficeScan은 전자 메일의 제목, 본문 및 첨부 파일에 대한 데이터 식별자를 확인합니다. 지원되는 전자 메일 에이전트 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

사용자가 전자 메일을 보내려고 할 때 모니터링이 발생합니다. 전자 메일에 데이터 식별자가 포함된 경우 OfficeScan에서 전자 메일을 허용하거나 차단합니다.

모니터링되지 않는 내부 전자 메일 도메인 및 모니터링되는 하위 도메인을 정의할 수 있습니다.

- **모니터링되지 않는 전자 메일 도메인**: OfficeScan에서는 모니터링되지 않는 도메인으로 전송되는 전자 메일의 전송을 즉시 허용합니다.

  참고

  모니터링되지 않는 전자 메일 도메인과 모니터링되는 전자 메일 하위 도메인으로의 데이터 전송(여기서 "모니터링"은 조치)은 전송이 허용된다는 점에서 서로 유사합니다. 유일한 차이점은 모니터링되지 않는 전자 메일 도메인의 경우 OfficeScan에서 전송을 기록하지 않는 반면, 모니터링되는 전자 메일 하위 도메인의 경우 전송이 항상 기록된다는 점입니다.

- **모니터링되는 전자 메일 하위 도메인**: OfficeScan에서 모니터링되는 하위 도메인으로 전송되는 전자 메일을 탐지한 경우 정책에 따른 조치를 확인합니다. 조치에 따라 전송이 허용되거나 차단됩니다.

  참고

  전자 메일 에이전트를 모니터링되는 채널로 선택한 경우 전자 메일이 정책과 일치해야 모니터링됩니다. 반면, 모니터링되는 전자 메일 하위 도메인으로 전송되는 전자 메일은 정책과 일치하지 않는 경우에도 자동으로 모니터링됩니다.

다음 포맷 중 하나를 사용하여 도메인을 지정하십시오(여러 도메인의 경우 쉼표로 구분).

- X400 포맷(예: /O=Trend/OU=USA, /O=Trend/OU=China)
- 전자 메일 도메인(예: example.com)

SMTP 프로토콜을 통해 전송되는 전자 메일 메시지의 경우 OfficeScan은 대상 SMTP 서버가 다음 목록에 있는지 확인합니다.

1. 모니터링되는 대상
2. 모니터링되지 않는 대상

참고

모니터링되는 대상과 모니터링되지 않는 대상에 대한 자세한 내용은 모니터링되지 않는 대상 및 모니터링되는 대상 정의 페이지 11-40를 참조하십시오.

3. 모니터링되지 않는 전자 메일 도메인
4. 모니터링되는 전자 메일 하위 도메인

즉, 전자 메일이 모니터링되는 대상 목록에 있는 SMTP 서버로 전송되는 경우에는 전자 메일이 모니터링됩니다. SMTP 서버가 모니터링되는 대상 목록에 없는 경우에는 OfficeScan에서 다른 목록을 확인합니다.

다른 프로토콜을 통해 전송되는 전자 메일의 경우 OfficeScan에서는 다음 목록만 확인합니다.

1. 모니터링되지 않는 전자 메일 도메인
2. 모니터링되는 전자 메일 하위 도메인

FTP

OfficeScan에서는 FTP 클라이언트가 FTP 서버에 파일을 업로드하려는 것을 탐지한 경우 파일에 데이터 식별자가 있는지 확인합니다. 파일은 아직 업로드되지 않습니다. DLP 정책에 따라 OfficeScan에서 업로드를 허용하거나 차단합니다.

파일 업로드를 차단하는 정책을 구성할 때 다음 사항을 고려해야 합니다.

- OfficeScan에서 업로드를 차단한 경우 일부 FTP 클라이언트는 파일을 다시 업로드하려고 시도합니다. 이 경우 OfficeScan은 다시 업로드하지 못하도록 FTP 클라이언트를 종료합니다. FTP 클라이언트가 종료된 후 사용자에게 알림이 제공되지는 않습니다. DLP 정책을 적용할 때 이 상황을 사용자에게 알려 주십시오.
- 업로드하려는 파일이 FTP 서버에 있는 파일을 덮어쓰는 경우 FTP 서버의 파일이 삭제될 수 있습니다.

지원되는 FTP 클라이언트 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

HTTP 및 HTTPS

OfficeScan에서는 HTTP 및 HTTPS를 통해 전송되는 데이터를 모니터링합니다. HTTPS의 경우 OfficeScan은 암호화 및 전송되기 전에 데이터를 확인합니다.

지원되는 웹 브라우저 및 응용 프로그램 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

IM 응용 프로그램

OfficeScan에서는 사용자가 IM(인스턴트 메시징) 응용 프로그램을 통해 보내는 메시지 및 파일을 모니터링합니다. 사용자가 받는 메시지 및 파일은 모니터링되지 않습니다.

지원되는 IM 응용 프로그램 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

OfficeScan에서 AOL Instant Messenger, MSN, Windows Messenger 또는 Windows Live Messenger를 통해 전송되는 메시지 또는 파일을 차단하는 경우 해당 응용 프로그램도 종료합니다. OfficeScan에서 응용 프로그램을 종료하지 못한 경우에는 응용 프로그램이 응답하지 않으므로 사용자가 응용 프로그램을 강제 종료해야 합니다. 응용 프로그램이 종료된 후 사용자에게 알림이 제공되지는 않습니다. DLP 정책을 적용할 때 이 상황을 사용자에게 알려 주십시오.

SMB 프로토콜

OfficeScan에서는 공유 파일 액세스를 지원하는 SMB(서버 메시지 블록) 프로토콜을 통한 데이터 전송을 모니터링합니다. 다른 사용자가 사용자의 공유 파일을 복사하거나 읽으려고 하면 OfficeScan에서 파일이 데이터 식별자이거나 데이터 식별자를 포함하는지 확인한 후 작업을 허용하거나 차단합니다.

참고

장치 제어 조치가 DLP 조치보다 우선 순위가 높습니다. 예를 들어 장치 제어에서 매핑된 네트워크 드라이브의 파일 이동을 허용하지 않는 경우 DLP에서 이를 허용해도 중요한 데이터의 전송이 진행되지 않습니다.

장치 제어 조치에 대한 자세한 내용은 저장 장치에 대한 권한 페이지 10-4을 참조하십시오.

OfficeScan에서 공유 파일 액세스를 모니터링하는 응용 프로그램 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

웹 메일

웹 기반 전자 메일 서비스는 HTTP를 통해 데이터를 전송합니다. OfficeScan에서는 지원되는 서비스에서 나가는 데이터를 탐지한 경우 데이터에 데이터 식별자가 있는지 확인합니다.

지원되는 웹 기반 전자 메일 서비스 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

네트워크 채널의 전송 범위 및 대상

전송 범위 및 대상은 OfficeScan에서 모니터링해야 하는 네트워크 채널의 데이터 전송을 정의합니다. 모니터링해야 하는 전송의 경우 OfficeScan에서는 전송을 허용하거나 차단하기 전에 데이터 식별자가 있는지 확인합니다. 모니터링하지 않는 전송의 경우 OfficeScan에서는 데이터 식별자가 있는지 확인하지 않고 전송을 즉시 허용합니다.

전송 범위: 모든 전송

OfficeScan에서는 호스트 컴퓨터 외부로 전송되는 데이터를 모니터링합니다.

참고

Trend Micro에서는 외부 에이전트에 대해 이 범위를 선택할 것을 권장합니다.

호스트 컴퓨터 외부의 특정 대상에 대한 데이터 전송을 모니터링하지 않으려면 다음을 정의하십시오.

- **모니터링되지 않는 대상**: OfficeScan에서는 이러한 대상으로 전송되는 데이터는 모니터링하지 않습니다.

  참고

  모니터링되지 않는 대상과 모니터링되는 대상으로의 데이터 전송(여기서 "모니터링"은 조치)은 전송이 허용된다는 점에서 서로 유사합니다. 유일한 차이점은 모니터링되지 않는 대상의 경우 OfficeScan에서 전송을 기록하지 않는 반면, 모니터링되는 대상의 경우 전송이 항상 기록된다는 점입니다.

- **모니터링되는 대상**: 모니터링되지 않는 대상 중에서 모니터링해야 하는 특정 대상입니다. 모니터링되는 대상은
  - 모니터링되지 않는 대상을 정의한 경우 선택 사항입니다.
  - 모니터링되지 않는 대상을 정의하지 않은 경우 구성할 수 없습니다.

예:

회사의 법률 부서에 다음 IP 주소가 할당되어 있습니다.

- 10.201.168.1~10.201.168.25

법률 부서의 정규직 직원을 제외한 모든 직원에게 전송되는 재직 증명서를 모니터링하는 정책을 만들려고 합니다. 이를 위해 **모든 전송**을 전송 범위로 선택하고 다음을 수행합니다.

옵션	단계
옵션 1	1. 10.201.168.1~10.201.168.25를 모니터링되지 않는 대상에 추가합니다. 2. 법률 부서 계약직 직원의 IP 주소를 모니터링되는 대상에 추가합니다. 세 개의 IP 주소(10.201.168.21~10.201.168.23)가 있다고 가정해 보겠습니다.

옵션	단계
옵션 2	법률 부서 정규직 직원의 IP 주소를 모니터링되지 않는 대상에 추가합니다. • 10.201.168.1-10.201.168.20 • 10.201.168.24-10.201.168.25

모니터링되는 대상 및 모니터링되지 않는 대상에 대한 지침은 모니터링되지 않는 대상 및 모니터링되는 대상 정의 페이지 11-40를 참조하십시오.

전송 범위: LAN(Local Area Network) 외부 전송만

OfficeScan에서는 LAN(Local Area Network) 외부 대상으로 전송되는 데이터를 모니터링합니다.

참고

Trend Micro에서는 내부 에이전트에 대해 이 범위를 선택할 것을 권장합니다.

"네트워크"는 회사 또는 로컬 네트워크를 의미합니다. 여기에는 현재 네트워크(엔드포인트의 IP 주소 및 넷마스크)와 다음과 같은 표준 개인 IP 주소가 포함됩니다.

- 클래스 A: 10.0.0.0 ~ 10.255.255.255
- 클래스 B: 172.16.0.0 ~ 172.31.255.255
- 클래스 C: 192.168.0.0 ~ 192.168.255.255

이 전송 범위를 선택한 경우 다음을 정의할 수 있습니다.

- **모니터링되지 않는 대상**: 안전한 것으로 간주하여 모니터링하지 않으려는 LAN 외부 대상을 정의합니다.

  참고

  모니터링되지 않는 대상과 모니터링되는 대상으로의 데이터 전송(여기서 "모니터링"은 조치)은 전송이 허용된다는 점에서 서로 유사합니다. 유일한 차이점은 모니터링되지 않는 대상의 경우 OfficeScan에서 전송을 기록하지 않는 반면, 모니터링되는 대상의 경우 전송이 항상 기록된다는 점입니다.

- **모니터링되는 대상**: 모니터링하려는 LAN 내부 대상을 정의합니다.

모니터링되는 대상 및 모니터링되지 않는 대상에 대한 지침은 모니터링되지 않는 대상 및 모니터링되는 대상 정의 페이지 11-40를 참조하십시오.

충돌 해결

전송 범위, 모니터링되는 대상 및 모니터링되지 않는 대상에 대한 설정이 서로 충돌하는 경우 OfficeScan에서는 다음 우선 순위(내림차순)를 차례대로 인식합니다.

- 모니터링되는 대상
- 모니터링되지 않는 대상
- 전송 범위

시스템 및 응용 프로그램 채널

OfficeScan에서는 다음과 같은 시스템 및 응용 프로그램 채널을 모니터링할 수 있습니다.

- 클라우드 저장소 서비스
- 데이터 레코더(CD/DVD)
- P2P(피어 투 피어) 응용 프로그램
- PGP 암호화
- 프린터
- 이동식 저장소
- 동기화 소프트웨어(ActiveSync)
- Windows 클립보드

클라우드 저장소 서비스

OfficeScan에서는 사용자가 클라우드 저장소 서비스를 사용하여 액세스하는 파일을 모니터링합니다. 지원되는 클라우드 저장소 서비스 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

참고

에이전트 엔드포인트에 엔드포인트 암호화가 설치된 경우 데이터 손실 방지 기능을 통해 클라우드 저장소 서비스에서 암호화가 지원됩니다.

데이터 레코더(CD/DVD)

OfficeScan에서는 CD 또는 DVD에 기록된 데이터를 모니터링합니다. 지원되는 데이터 기록 장치 및 소프트웨어 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

OfficeScan에서 지원되는 장치나 소프트웨어에서 시작된 "burn" 명령을 탐지한 경우 조치가 "그대로 두기"이면 데이터 기록이 진행됩니다. 조치가 "차단"이면 OfficeScan에서 기록할 파일이 데이터 식별자이거나 데이터 식별자를 포함하는지 확인합니다. OfficeScan에서 데이터 식별자를 하나 이상 탐지한 경우 아무 파일(데이터 식별자가 아닌 파일 또는 데이터 식별자를 포함하지 않는 파일 포함)도 기록되지 않습니다. OfficeScan에서는 CD 또는 DVD 꺼내기를 방지할 수도 있습니다. 이 문제가 발생한 경우 사용자에게 소프트웨어 프로세스를 다시 시작하거나 장치를 다시 설정하도록 지시하십시오.

OfficeScan에서는 추가 CD/DVD 기록 규칙을 구현합니다.

- 잘못된 판정을 줄이기 위해 다음 파일은 OfficeScan에서 모니터링하지 않습니다.

.bud	.dll	.gif	.gpd	.htm	.ico	.ini

.jpg	.lnk	.sys	.ttf	.url	.xml

- Roxio 데이터 레코드에서 사용하는 두 가지 파일 형식(*.png 및 *.skn)은 성능 향상을 위해 모니터링되지 않습니다.
- 다음 디렉터리의 파일은 OfficeScan에서 모니터링하지 않습니다.

*:₩autoexec.bat	*:₩Windows
..₩Application Data	..₩Cookies
..₩Local Settings	..₩ProgramData
..₩Program Files	..₩Users₩*₩AppData
..₩WINNT	

- 장치 및 소프트웨어에 의해 생성된 ISO 이미지는 모니터링되지 않습니다.

데이터 레코더(CD/DVD)에 대한 액세스 차단

장치 제어는 라이브 파일 시스템 형식을 사용하는 CD/DVD 기록 장치에 대한 액세스만 제한할 수 있습니다. 마스터 형식을 사용하는 일부 타사 응용 프로그램은 장치 제어를 사용할 때도 여전히 읽기/쓰기 작업을 수행할 수 있습니다. 데이터 손실 방지를 사용하여 모든 포맷 유형을 사용하는 CD/DVD 기록 장치에 대한 액세스를 제한합니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **DLP 설정**을 클릭합니다.
4. **외부 에이전트** 탭을 클릭하여 외부 에이전트에 대한 정책을 구성하거나 **내부 에이전트** 탭을 클릭하여 내부 에이전트에 대한 정책을 구성합니다.

참고

에이전트 위치 설정을 아직 구성하지 않은 경우 구성합니다. 에이전트는 이러한 위치 설정을 사용하여 적용할 올바른 데이터 손실 방지 정책을 결정합니다. 자세한 내용은 엔드포인트 위치 페이지 15-2를 참조하십시오.

5. 다음 중 하나를 선택합니다.
   - **외부 에이전트** 탭을 클릭한 경우 **내부 에이전트에 모든 설정 적용**을 선택하여 내부 에이전트에 모든 데이터 손실 방지 설정을 적용할 수 있습니다.
   - **내부 에이전트** 탭을 클릭한 경우 **외부 에이전트에 모든 설정 적용**을 선택하여 외부 에이전트에 모든 데이터 손실 방지 설정을 적용할 수 있습니다.
6. **규칙** 탭에서 **추가**를 클릭합니다.
7. **이 규칙 사용**을 선택합니다.
8. 규칙 이름을 지정합니다.
9. **템플릿** 탭을 클릭합니다.
10. 목록에서 **모든 파일 확장자** 템플릿을 선택하고 **추가**를 클릭합니다.
11. **채널** 탭을 클릭합니다.
12. **시스템 및 응용 프로그램 채널** 섹션에서 **데이터 레코더(CD/DVD)**를 선택합니다.
13. **조치** 탭을 클릭합니다.
14. **차단** 조치를 선택합니다.
15. **저장**을 클릭합니다.
16. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
    - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

P2P(피어 투 피어) 응용 프로그램

OfficeScan에서는 사용자가 P2P(피어 투 피어) 응용 프로그램을 통해 공유하는 파일을 모니터링합니다.

지원되는 P2P(피어 투 피어) 응용 프로그램 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

PGP 암호화

OfficeScan에서는 PGP 암호화 소프트웨어를 통해 암호화할 데이터를 모니터링합니다. OfficeScan은 암호화가 진행되기 전에 데이터를 확인합니다.

지원되는 PGP 암호화 소프트웨어 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

프린터

OfficeScan에서는 여러 응용 프로그램에서 시작된 프린터 작업을 모니터링합니다.

저장되지 않은 새 파일에 대한 프린터 작업은 인쇄 정보가 메모리에 저장되지 않은 상태이므로 OfficeScan에서 이 작업을 차단하지 않습니다.

프린터 작업을 시작할 수 있는 지원되는 응용 프로그램 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

이동식 저장소

OfficeScan는 이동식 저장 장치로의 데이터 전송 또는 이동식 저장 장치 내의 데이터 전송을 모니터링합니다. 데이터 전송과 관련된 작업에는 다음이 포함됩니다.

- 장치 내 파일 만들기
- 호스트 컴퓨터에서 장치로 파일 복사
- 장치 내 수정된 파일 닫기
- 장치 내 파일 정보(예: 파일 확장자) 수정

전송할 파일에 데이터 식별자가 포함된 경우 OfficeScan은 전송을 차단하거나 허용합니다.

참고

- 장치 제어 조치가 DLP 조치보다 우선 순위가 높습니다. 예를 들어 장치 제어에서 이동식 저장 장치로의 파일 복사를 허용하지 않는 경우 DLP에서 이를 허용해도 중요한 정보의 전송이 진행되지 않습니다.
- 에이전트 엔드포인트에 엔드포인트 암호화가 설치된 경우 데이터 손실 방지 기능을 통해 이동식 저장 장치에서 암호화가 지원됩니다.

데이터 전송 작업에 유용한, 지원되는 이동식 저장 장치 및 응용 프로그램 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

이동식 저장 장치로의 파일 전송 처리는 간단한 프로세스입니다. 예를 들어 사용자가 Microsoft Word에서 파일을 만들어 SD 카드에 파일을 저장할 수 있습니다(파일을 저장한 파일 형식에 상관없음). 그러나 파일에 전송할 수 없는 데이터 식별자가 포함된 경우 OfficeScan에서는 파일의 저장을 방지합니다.

장치 내 파일 전송의 경우 OfficeScan은 파일을 처리하기 전에 먼저 %WINDIR%₩system32₩dgagent₩temp에 파일을 백업합니다(파일 크기가 75MB 이하인

경우). 그런 다음 파일 전송을 허용한 경우 OfficeScan은 백업 파일을 제거합니다. OfficeScan에서 전송을 차단한 경우에는 파일이 프로세스 중에 삭제될 수 있습니다. 이 경우 OfficeScan은 원본 파일이 있는 폴더에 백업 파일을 복사합니다.

OfficeScan을 통해 예외를 정의할 수 있습니다. OfficeScan은 이러한 장치로의 데이터 전송이나 이러한 장치 내의 데이터 전송을 항상 허용합니다. 공급업체별로 장치를 식별하고 필요한 경우 장치 모델과 일련 ID를 제공합니다.

팁

장치 목록 도구를 사용하여 엔드포인트에 연결된 장치를 쿼리합니다. 이 도구는 각 장치의 장치 공급업체, 모델 및 일련 ID 를 제공합니다. 자세한 내용은 장치 목록 도구 페이지 10-14를 참조하십시오.

동기화 소프트웨어(ActiveSync)

OfficeScan에서는 동기화 소프트웨어를 통해 모바일 장치로 전송되는 데이터를 모니터링합니다.

지원되는 동기화 소프트웨어 목록은 다음 위치에서 *데이터 보호 목록* 문서를 참조하십시오.

http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx

데이터의 소스 IP 주소가 127.0.0.1이고 포트 990 또는 5678(동기화에 사용되는 포트)을 통해 데이터가 전송되는 경우 OfficeScan은 전송을 허용하거나 차단하기 전에 해당 데이터가 데이터 식별자인지 확인합니다.

OfficeScan에서 포트 990을 통해 전송되는 파일을 차단한 경우 잘못된 형식의 문자가 포함된 같은 이름의 파일은 모바일 장치의 대상 폴더에 생성될 수 있습니다. 이는 OfficeScan에서 전송을 차단하기 전에 파일의 일부가 장치에 복사되었기 때문입니다.

Windows 클립보드

OfficeScan에서는 전송을 허용하거나 차단하기 전에 Windows 클립보드로 전송되는 데이터를 모니터링합니다.

또한 OfficeScan에서는 호스트 컴퓨터와 VMWare 또는 원격 데스크톱 간의 클립보드 작업을 모니터링할 수 있습니다. 모니터링은 OfficeScan 에이전트가 있는 엔터티에서 수행됩니다. 예를 들어 VMware 가상 컴퓨터의 OfficeScan 에이전트는 가상 컴퓨터의 클립보드 데이터가 호스트 컴퓨터에 전송되지 않도록 방지할 수 있습니다. 마찬가지로 OfficeScan 에이전트가 있는 호스트 컴퓨터는 원격 데스크톱을 통해 액세스한 엔드포인트에 클립보드 데이터를 복사하지 못할 수 있습니다.

데이터 손실 방지 조치

데이터 손실 방지 기능은 데이터 식별자 전송을 탐지한 경우 탐지한 데이터 식별자에 대한 DLP 정책을 확인하고 정책에 대해 구성된 조치를 수행합니다.

다음 표에는 데이터 손실 방지 조치가 나와 있습니다.

표 11-5. 데이터 손실 방지 조치

조치	설명
조치	
그대로 두기	데이터 손실 방지 기능이 전송을 허용하고 기록합니다.
차단	데이터 손실 방지 기능이 전송을 차단하고 기록합니다.
추가 조치	
에이전트 사용자에게 알림	데이터 손실 방지 기능이 사용자에게 데이터 전송 발생 사실과 이 전송을 그대로 두었는지, 차단했는지를 알리는 알림 메시지를 표시합니다.
데이터 기록	기본 조치에 상관없이 데이터 손실 방지 기능은 <클라이언트 설치 폴더>₩DLPLite₩Forensic에 중요한 정보를 기록합니다. 데이터 손실 방지에 의해 플래그가 지정된 중요한 정보를 평가하려면 이 조치를 선택합니다. 기록된 중요한 정보는 과도한 하드 디스크 공간을 사용할 수 있습니다. 따라서 Trend Micro에서는 매우 중요한 정보에 대해서만 이 옵션을 선택할 것을 권장합니다.

조치	설명
지정된 키/암호를 사용하는 암호화 지원 채널(엔드포인트 암호화가 설치된 경우에만 사용) **참고** 이 옵션은 **그대로 두기** 조치를 선택한 상태에서 이동식 저장소 및 클라우드 저장소 서비스 채널에서만 사용할 수 있습니다.	OfficeScan 에이전트와 함께 Trend Micro 엔드포인트 암호화가 설치된 경우 데이터 손실 방지 기능에서는 사용자가 파일을 다른 위치로 전달하기 전에 파일을 자동으로 암호화합니다. 엔드포인트 암호화가 설치되지 않은 경우에는 데이터 손실 방지 기능에서 파일에 대해 차단 조치를 수행합니다. 다음과 같은 암호화 키나 고정된 암호 중 하나를 선택합니다. • **사용자 키**: **로컬 키**라고도 하며, 이 키는 각 사용자에 대해 고유하며, 암호화된 파일에 대한 액세스 권한을 파일을 만든 사용자로 제한합니다. • **공유 키**: 이 키는 **그룹 키** 또는 **엔터프라이즈 키**라고도 하며, 엔드포인트 암호화 관리자가 PolicyServer MMC를 사용하여 유형을 구성합니다. • **고정 암호**: 사용자가 화면의 프롬프트를 사용하여 수동으로 고정된 암호를 제공합니다. 엔드포인트 암호화에서 암호 해독 암호를 제공한 후 사용자가 모든 엔드포인트에서 액세스할 수 있는 자동 압축 풀기 패키지를 만듭니다. **중요** • 대상 엔드포인트에는 엔드포인트 암호화가 설치되어야 하며, 사용자는 데이터를 암호화하기 위해 엔드포인트 암호화에 로그인해야 합니다. • USB 장치에 있는 암호화된 파일의 경우 사용자가 파일 암호를 해독할 때 데이터 손실 방지 검색이 수행될 수 있습니다. USB 장치에서 중요한 데이터가 포함된 파일의 암호를 해독하면 USB 암호화 프로토콜이 트리거되어 시스템에서 중요한 데이터를 다시 암호화해야 한다는 메시지가 표시됩니다. OfficeScan에서 데이터를 "다시 암호화"하지 않도록 하려면 데이터에 액세스하기 전에 암호화된 파일을 로컬 드라이브로 이동하십시오. • 웹 클라이언트 사용 시 데이터 손실 방지 기능은 파일을 클라우드 저장소에 업로드하려는 시도를 차단합니다. 웹 클라이언트를 사용하여 업로드하기 전에 파일을 수동으로 암호화하십시오.

조치	설명
사용자 정당성 **참고** 이 옵션은 **차단** 조치를 선택한 경우에만 사용할 수 있습니다.	데이터 손실 방지 기능은 "차단" 조치를 수행하기 전에 사용자에게 확인합니다. 사용자는 중요 데이터를 전송해도 안전에 문제가 없는 이유에 대한 설명을 제공하여 "차단" 조치를 무시할 수 있습니다. 사용 가능한 정당성 이유는 다음과 같습니다. • **이 작업은 설정된 비즈니스 프로세스의 일부분입니다.** • **관리자가 데이터 전송을 승인했습니다.** • **이 파일의 데이터는 기밀 정보가 아닙니다.** • **기타**: 사용자가 제공된 텍스트 필드에 다른 설명을 제공합니다.

데이터 손실 방지 예외

DLP 예외는 정책 내에 정의한 모든 규칙을 포함하여 전체 정책에 적용됩니다. 데이터 손실 방지 기능은 모든 전송에 예외 설정을 적용한 이후에 디지털 자산을 검색합니다. 전송이 예외 규칙 중 하나와 일치하는 경우 데이터 손실 방지 기능은 예외 유형에 따라 전송을 즉시 허용하거나 검색합니다.

모니터링되지 않는 대상 및 모니터링되는 대상 정의

채널 탭에서 구성한 전송 범위를 기반으로 모니터링되지 않는 대상과 모니터링되는 대상을 정의합니다. **모든 전송**의 모니터링되지 않는 대상과 모니터링되는 대상을 정의하는 방법에 대한 자세한 내용은 전송 범위: 모든 전송 페이지 11-28을 참조하십시오. **LAN(Local Area Network) 외부 전송만**의 모니터링되지 않는 대상과 모니터링되는 대상을 정의하는 방법에 대한 자세한 내용은 전송 범위: LAN(Local Area Network) 외부 전송만 페이지 11-30을 참조하십시오.

모니터링되는 대상 및 모니터링되지 않는 대상을 정의할 때 다음 지침을 따르십시오.

1. 다음을 사용하여 각 대상을 정의합니다.
    - IP 주소

- 호스트 이름
- FQDN
- 네트워크 주소 및 서브넷 마스크(예: 10.1.1.1/32)

참고

서브넷 마스크의 경우 데이터 손실 방지에서는 CIDR(Classless Inter-Domain Routing) 형식의 포트만 지원합니다. 따라서 255.255.255.0 대신 32와 같은 숫자만 입력할 수 있습니다.

2. 특정 채널을 대상으로 지정하려면 해당 채널의 기본 포트 번호 또는 회사에서 정의한 포트 번호를 포함합니다. 예를 들어 포트 21은 일반적으로 FTP 트래픽에 사용되고 포트 80은 HTTP에 사용되며 포트 443은 HTTPS에 사용됩니다. 포트 번호에서 콜론을 사용하여 대상을 구분하십시오.
3. 포트 범위를 포함할 수도 있습니다. 모든 포트를 포함하려면 포트 범위를 무시하면 됩니다.

   아래는 대상에 포트 번호와 포트 범위가 포함된 몇 가지 예입니다.

   - 10.1.1.1:80
   - host:5-20
   - host.domain.com:20
   - 10.1.1.1/32:20
4. 대상을 쉼표로 구분하십시오.

압축 해제 규칙

압축 파일에 포함된 파일에서 디지털 자산을 검색할 수 있습니다. 검색할 파일을 결정하기 위해 데이터 손실 방지 기능은 압축 파일에 다음 규칙을 적용합니다.

- **압축 해제된 파일의 크기가 다음을 초과하는 경우: __MB(1-512MB)**
- **압축 레이어가 다음을 초과하는 경우: __(1-20)**

- **검색할 파일 수가 다음을 초과하는 경우: __(1-2000)**

규칙 1: 압축 해제된 파일의 최대 크기

압축 파일은 압축 해제 시 지정된 제한을 충족해야 합니다.

예: 제한을 20MB로 설정했습니다.

시나리오 1: 압축 해제 시 archive.zip의 크기가 30MB인 경우 archive.zip에 포함된 파일이 검색되지 않습니다. 나머지 두 규칙을 더 이상 확인하지 않습니다.

시나리오 2: 압축 해제 시 my_archive.zip의 크기가 10MB인 경우

- my_archive.zip에 압축 파일이 포함되어 있지 않은 경우 OfficeScan에서는 규칙 2를 건너뛰고 규칙 3을 진행합니다.
- my_archive.zip에 압축 파일이 포함된 경우 모든 압축 해제된 파일의 크기가 제한 내에 있어야 합니다. 예를 들어 my_archive.zip에 AAA.rar, BBB.zip 및 EEE.zip이 포함되고 EEE.zip에 222.zip이 포함된 경우

my_archive.zip	= 압축 해제 시 10MB
₩AAA.rar	= 압축 해제 시 25MB
₩BBB.zip	= 압축 해제 시 3MB
₩EEE.zip	= 압축 해제 시 1MB
₩222.zip	= 압축 해제 시 2MB

my_archive.zip, BBB.zip, EEE.zip 및 222.zip 파일의 전체 크기가 20MB 제한 이내이므로 규칙 2가 확인됩니다. AAA.rar은 건너뜁니다.

규칙 2: 최대 압축 레이어 수

지정된 레이어 수 내의 파일에 검색 플래그가 지정됩니다.

예:

my_archive.zip

₩BBB.zip	₩CCC.xls	
₩DDD.txt		
₩EEE.zip	₩111.pdf	
	₩222.zip	₩333.txt

제한을 2개 레이어로 설정한 경우

- OfficeScan에서 세 번째 레이어에 있는 333.txt를 무시합니다.
- OfficeScan에서 다음 파일에 검색 플래그를 지정한 후 규칙 3을 확인합니다.
  - DDD.txt(첫 번째 레이어에 있음)
  - CCC.xls(두 번째 레이어에 있음)
  - 111.pdf(두 번째 레이어에 있음)

규칙 3: 검색할 최대 파일 수

OfficeScan에서 지정된 제한까지 파일을 검색합니다. OfficeScan에서는 파일 및 폴더를 번호 순으로 검색한 다음 영문자 순으로 검색합니다.

규칙 2의 예에 이어 OfficeScan에서 강조 표시된 파일에 검색 플래그를 지정했습니다.

my_archive.zip		
₩BBB.zip	**₩CCC.xls**	
₩DDD.txt		
₩EEE.zip	**₩111.pdf**	
	₩222.zip	₩333.txt

또한 my_archive.zip에 규칙2가 확인되지 않은 7Folder라는 폴더가 포함되어 있습니다. 이 폴더에는 FFF.doc 및 GGG.ppt가 들어 있습니다. 따라서 아래 강조 표시된 것처럼 검색할 총 파일 수는 5개입니다.

my_archive.zip			
	₩7Folder	**₩FFF.doc**	
	₩7Folder	**₩GGG.ppt**	
	₩BBB.zip	**₩CCC.xls**	
	₩DDD.txt		
	₩EEE.zip	**₩111.pdf**	
		₩222.zip	₩333.txt

제한을 4개 파일로 설정한 경우 다음 파일이 검색됩니다.

- FFF.doc
- GGG.ppt
- CCC.xls
- DDD.txt

참고

포함된 파일이 있는 파일의 경우 OfficeScan에서는 포함된 파일의 내용을 추출합니다.

추출된 내용이 텍스트인 경우 호스트 파일(예: 123.doc)과 포함된 파일(예: abc.txt 및 xyz.xls)이 1개로 간주됩니다.

추출된 내용이 텍스트가 아닌 경우 호스트 파일(예: 123.doc)과 포함된 파일(예: abc.exe)이 별개로 간주됩니다.

압축 해제 규칙을 트리거하는 이벤트

다음 이벤트는 압축 해제 규칙을 트리거합니다.

표 11-6. 압축 해제 규칙을 트리거하는 이벤트

전송할 압축 파일이 정책과 일치하고 압축 파일에 대한 조치가 그대로 두기(파일 전송)입니다.	예를 들어 사용자가 전송하는 .ZIP 파일을 모니터링하기 위해 파일 특성(.ZIP)을 정의하여 템플릿에 추가하고 정책에서 이 템플릿을 사용한 다음 조치를 **그대로 두기**로 설정했습니다. **참고** 조치가 차단인 경우 전체 압축 파일이 전송되지 않으므로 포함된 파일을 검색할 필요가 없습니다.
전송할 압축 파일이 정책과 일치하지 않습니다.	이 경우에도 OfficeScan에서는 압축 파일에 압축 해제 규칙을 적용하여 디지털 자산을 검색해야 하는 포함된 파일 및 전체 압축 파일의 전송 여부를 결정합니다.

두 이벤트는 결과가 같습니다. OfficeScan에서 압축 파일을 발견한 경우

- 규칙 1이 충족되지 않으면 OfficeScan에서 전체 압축 파일의 전송을 허용합니다.
- 규칙 1이 충족되면 다른 두 규칙을 확인합니다. 다음의 경우 OfficeScan에서는 전체 압축 파일의 전송을 허용합니다.
  - 검색한 일부 파일이 정책과 일치하지 않는 경우
  - 검색한 모든 파일이 정책과 일치하고 조치가 **그대로 두기**인 경우

    검색한 파일 중 하나 이상이 정책과 일치하고 조치가 **차단**인 경우에는 전체 압축 파일의 전송이 차단됩니다.

데이터 손실 방지 정책 구성

데이터 식별자를 구성하고 템플릿에 정리한 후에는 데이터 손실 방지 정책을 만들 수 있습니다.

정책을 만들 때 데이터 식별자 및 템플릿 외에 채널 및 조치도 구성해야 합니다. 정책에 대한 자세한 내용은 데이터 손실 방지 정책 페이지 11-3을 참조하십시오.

데이터 손실 방지 정책 만들기

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **DLP 설정**을 클릭합니다.
4. **외부 에이전트** 탭을 클릭하여 외부 에이전트에 대한 정책을 구성하거나 **내부 에이전트** 탭을 클릭하여 내부 에이전트에 대한 정책을 구성합니다.

   참고

   에이전트 위치 설정을 아직 구성하지 않은 경우 구성합니다. 에이전트는 이러한 위치 설정을 사용하여 적용할 올바른 데이터 손실 방지 정책을 결정합니다. 자세한 내용은 엔드포인트 위치 페이지 15-2를 참조하십시오.

5. **데이터 손실 방지 사용**을 선택합니다.
6. 다음 중 하나를 선택합니다.
   - **외부 에이전트** 탭을 클릭한 경우 **내부 에이전트에 모든 설정 적용**을 선택하여 내부 에이전트에 모든 데이터 손실 방지 설정을 적용할 수 있습니다.
   - **내부 에이전트** 탭을 클릭한 경우 **외부 에이전트에 모든 설정 적용**을 선택하여 외부 에이전트에 모든 데이터 손실 방지 설정을 적용할 수 있습니다.
7. **규칙** 탭에서 **추가**를 클릭합니다.

   정책에는 규칙을 최대 40개까지 포함할 수 있습니다.

8. 규칙 설정을 구성합니다.

   DLP 규칙 만들기에 대한 자세한 내용은 데이터 손실 방지 규칙 만들기 페이지 11-47를 참조하십시오.

9. **예외** 탭을 클릭하고 필요한 예외 설정을 구성합니다.

   사용 가능한 예외 설정에 대한 자세한 내용은 데이터 손실 방지 예외 페이지 11-40를 참조하십시오.

10. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

    - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
    - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

데이터 손실 방지 규칙 만들기

참고

데이터 손실 방지 기능은 규칙과 템플릿을 우선 순위에 따라 처리합니다. 규칙을 "그대로 두기"로 설정하는 경우 데이터 손실 방지 기능은 목록에 있는 다음 규칙을 처리합니다. 규칙을 "차단" 또는 "사용자 정당성"으로 설정하는 경우 데이터 손실 방지 기능은 사용자 조치를 차단하거나 허용하고 해당 규칙/템플릿을 추가로 처리하지 않습니다.

절차

1. **이 규칙 사용**을 선택합니다.
2. 규칙 이름을 지정합니다.

   템플릿 설정을 구성합니다.

3. **템플릿** 탭을 클릭합니다.
4. **사용 가능한 템플릿** 목록에서 템플릿을 선택하고 **추가**를 클릭합니다.

   템플릿을 선택할 때 다음과 같이 할 수 있습니다.

   - 선택할 템플릿 이름을 클릭합니다. 그러면 선택된 템플릿이 이름이 강조 표시됩니다.
   - 특정 템플릿을 찾으려는 경우 검색 기능을 사용합니다. 템플릿의 전체 이름 또는 일부 이름을 입력할 수 있습니다.

   참고

   정책에는 템플릿을 최대 200개까지 포함할 수 있습니다.

5. **사용 가능한 템플릿** 목록에서 원하는 템플릿을 찾을 수 없는 경우 다음을 수행합니다.

   a. **새 템플릿 추가**를 클릭합니다.

      데이터 손실 방지 템플릿 화면이 표시됩니다.

      데이터 손실 방지 템플릿 화면에서 템플릿을 추가하는 방법에 대한 자세한 내용은 데이터 손실 방지 템플릿 페이지 11-19을 참조하십시오.

   b. 템플릿을 만든 후 해당 템플릿을 선택하고 **추가**를 클릭합니다.

   참고

   OfficeScan에서는 템플릿을 확인할 때 첫 번째 일치 규칙을 사용합니다. 즉, 파일 또는 데이터가 템플릿의 정의와 일치하는 경우 OfficeScan에서 다른 템플릿을 더 이상 확인하지 않습니다. 우선 순위는 목록에 있는 템플릿의 순서를 기반으로 합니다.

채널 설정을 구성합니다.

6. **채널** 탭을 클릭합니다.
7. 규칙에 대한 채널을 선택합니다.

   채널에 대한 자세한 내용은 네트워크 채널 페이지 11-24 및 시스템 및 응용 프로그램 채널 페이지 11-31을 참조하십시오.

8. 네트워크 채널을 선택한 경우 전송 범위를 선택합니다.

   - **모든 전송**
   - **LAN(Local Area Network) 외부 전송만**

   전송 범위, 전송 범위에 따른 대상의 작동 방식 및 대상을 올바르게 정의하는 방법은 네트워크 채널의 전송 범위 및 대상 페이지 11-28을 참조하십시오.

9. **전자 메일 클라이언트**를 선택한 경우 다음을 수행합니다.

   a. **예외**를 클릭합니다.

   b. 모니터링되는 내부 전자 메일 도메인과 모니터링되지 않는 내부 전자 메일 도메인을 지정합니다.

      모니터링되는 대상 및 모니터링되지 않는 대상에 대한 자세한 내용은 전자 메일 클라이언트 페이지 11-24를 참조하십시오.

10. **이동식 저장소**를 선택한 경우 다음을 수행합니다.

    a. **예외**를 클릭합니다.

    b. 모니터링되지 않는 이동식 저장 장치를 공급업체별로 식별하여 추가합니다. 장치 모델 및 일련 ID는 선택 사항입니다.

       승인된 USB 장치 목록에는 별표(*) 와일드카드를 사용할 수 있습니다. 필드를 별표(*)로 바꾸면 다른 필드를 충족하는 장치를 모두 포함할 수 있습니다.

       예를 들어 [vendor]-[model]-*로 지정하면 일련 ID에 관계없이 지정된 공급업체 및 지정된 모델 유형의 USB 장치가 모두 승인된 목록에 포함됩니다.

    c. 장치를 더 추가하려면 더하기(+) 아이콘을 클릭합니다.

팁

장치 목록 도구를 사용하여 엔드포인트에 연결된 장치를 쿼리합니다. 이 도구는 각 장치의 장치 공급업체, 모델 및 일련 ID 를 제공합니다. 자세한 내용은 장치 목록 도구 페이지 10-14를 참조하십시오.

조치 설정을 구성합니다.

11. **조치** 탭을 클릭합니다.

12. 기본 조치와 추가 조치를 선택합니다.

    조치에 대한 자세한 내용은 데이터 손실 방지 조치 페이지 11-38를 참조하십시오.

    참고

    데이터 손실 방지는 이동식 장치 및 클라우드 저장소 서비스에서만 중요한 데이터 암호화를 지원합니다. 암호화가 지원되지 않는 모든 채널에서는 암호화 없이 "그대로 두기" 조치를 수행합니다. 대상 엔드포인트에는 엔드포인트 암호화가 설치되어야 하며, 사용자는 데이터를 암호화하기 위해 엔드포인트 암호화에 로그인해야 합니다.

13. **템플릿**, **채널** 및 **조치** 설정을 구성한 후 **저장**을 클릭합니다.

DLP 규칙 가져오기, 내보내기 및 복사

관리자는 이전에 정의한 규칙(올바른 포맷의 .dat 파일 포함)을 가져오거나 구성한 DLP 규칙 목록을 내보낼 수 있습니다. 관리자는 DLP 규칙을 복사하는 방법으로 이전에 정의한 규칙의 내용을 수정하여 시간을 절약할 수 있습니다.

다음 표에서는 각 기능이 어떻게 동작하는지 설명합니다.

표 11-7. DLP 규칙 가져오기, 내보내기 및 복사

기능	설명
가져오기	규칙 목록을 가져오면 기존 DLP 규칙 목록에 없던 규칙이 추가됩니다. 데이터 손실 방지 기능은 대상 목록에 이미 있는 규칙은 건너뜁니다. 데이터 손실 방지 기능은 각 규칙에 대한 사용 또는 사용 안 함 상태를 비롯해 미리 구성된 설정을 모두 유지합니다.

기능	설명
내보내기	규칙 목록을 내보내면 내보낸 전체 목록이 포함된 .dat 파일이 생성되며, 관리자는 이 파일을 다른 도메인이나 에이전트로 가져와 배포할 수 있습니다. 데이터 손실 방지 기능은 현재 구성에 따라 모든 규칙 설정을 저장합니다. **참고** • 관리자는 목록을 내보내기 전에 새 규칙이나 수정된 규칙을 저장 또는 적용해야 합니다. • 데이터 손실 방지 기능은 정책에 구성된 예외는 내보내지 않으며 각 규칙에 구성된 설정만 내보냅니다.
복사	규칙을 복사하면 규칙의 현재 구성 설정이 똑같이 복제됩니다. 관리자는 규칙의 새 이름을 입력해야 하며 새 규칙에 필요한 구성을 수정할 수 있습니다.

데이터 손실 방지 알림

OfficeScan에서는 OfficeScan 관리자 및 에이전트 사용자에게 디지털 자산 전송을 알리는 일련의 기본 알림 메시지를 제공합니다.

관리자에게 전송되는 알림에 대한 자세한 내용은 관리자에 대한 데이터 손실 방지 알림 페이지 11-51을 참조하십시오.

에이전트 사용자에게 전송되는 알림에 대한 자세한 내용은 에이전트 사용자에 대한 데이터 손실 방지 알림 페이지 11-55을 참조하십시오.

관리자에 대한 데이터 손실 방지 알림

디지털 자산 전송이 탐지된 경우 관리자에게 알림을 보내거나 전송이 차단된 경우에만 관리자에게 알림을 보내도록 OfficeScan을 구성할 수 있습니다.

OfficeScan에서는 관리자에게 디지털 자산 전송을 알리는 일련의 기본 알림 메시지를 제공합니다. 회사의 요구 사항에 맞게 알림을 수정하고 추가 알림 설정을 구성할 수 있습니다.

참고

OfficeScan에서는 전자 메일, SNMP 트랩 및 Windows NT 이벤트 로그를 통해 알림을 보낼 수 있습니다. OfficeScan에서 이러한 채널을 통해 알림을 보내는 경우에 대한 설정을 구성하십시오. 자세한 내용은 관리자 알림 설정 페이지 14-35를 참조하십시오.

관리자에 대한 데이터 손실 방지 알림 구성

절차

1. **관리** > **알림** > **관리자**으로 이동합니다.
2. **기준** 탭에서 다음을 수행합니다.
   a. **디지털 자산 전송** 섹션으로 이동합니다.
   b. 디지털 자산 전송이 탐지된 경우(조치는 차단 또는 그대로 두기일 수 있음)에 알림을 보낼지 아니면 전송이 차단된 경우에만 알림을 보낼지 지정합니다.
3. **전자 메일** 탭에서 다음을 수행합니다.
   a. **디지털 자산 전송** 섹션으로 이동합니다.
   b. **전자 메일을 통한 알림 사용**을 선택합니다.
   c. **에이전트 트리 도메인 권한이 있는 사용자에게 알림 보내기**를 선택합니다.

      역할 기반 관리를 사용하여 사용자에게 에이전트 트리 도메인 권한을 부여할 수 있습니다. 특정 도메인에 속한 에이전트에서 전송이 수행되는 경우 도메인 권한이 있는 사용자의 전자 메일 주소로 전자 메일이 전송됩니다. 다음 표의 예를 참조하십시오.

표 11-8. 에이전트 트리 도메인 및 권한

에이전트 트리 도메인	도메인 권한이 있는 역할	역할이 있는 사용자 계정	사용자 계정의 전자 메일 주소
도메인 A	관리자(기본 제공)	루트	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
도메인 B	관리자(기본 제공)	루트	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

도메인 A에 속한 OfficeScan 에이전트에서 디지털 자산 전송을 탐지한 경우 mary@xyz.com, john@xyz.com 및 chris@xyz.com으로 전자 메일이 전송됩니다.

도메인 B에 속한 OfficeScan 에이전트에서 전송을 탐지한 경우 mary@xyz.com 및 jane@xyz.com으로 전자 메일이 전송됩니다.

참고

이 옵션을 사용할 때는 도메인 권한이 있는 모든 사용자에게 해당 전자 메일 주소가 있어야 합니다. 전자 메일 주소가 없는 사용자에게는 전자 메일 알림이 전송되지 않습니다. 사용자 및 전자 메일 주소는 **관리** > **계정 관리** > **사용자 계정**에서 구성합니다.

d. **다음 전자 메일 주소로 알림 보내기**를 선택하고 전자 메일 주소를 입력합니다.

e. 기본 제목 및 메시지를 적용하거나 수정합니다. **제목** 및 **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시합니다.

표 11-9. 데이터 손실 방지 알림용 토큰 변수

변수	설명
%USER%	전송이 탐지된 당시 엔드포인트에 로그온한 사용자

변수	설명
%COMPUTER%	전송이 탐지된 엔드포인트
%DOMAIN%	엔드포인트의 도메인
%DATETIME%	전송이 탐지된 날짜 및 시간
%CHANNEL%	전송이 탐지된 채널
%TEMPLATE%	탐지를 트리거한 디지털 자산 템플릿
%RULE%	탐지를 트리거한 규칙 이름 **참고** 메시지에 규칙 이름을 표시하려면 **메시지** 필드에 이 변수를 추가합니다.

4. **SNMP 트랩** 탭에서 다음을 수행합니다.
   a. **디지털 자산 전송** 섹션으로 이동합니다.
   b. **SNMP 트랩을 통한 알림 사용**을 선택합니다.
   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 11-9 : 데이터 손실 방지 알림용 토큰 변수 페이지 11-53를 참조하십시오.
5. **NT 이벤트 로그** 탭에서 다음을 수행합니다.
   a. **디지털 자산 전송** 섹션으로 이동합니다.
   b. **NT 이벤트 로그를 통한 알림 사용**을 선택합니다.
   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 11-9 : 데이터 손실 방지 알림용 토큰 변수 페이지 11-53를 참조하십시오.
6. **저장**을 클릭합니다.

에이전트 사용자에 대한 데이터 손실 방지 알림

OfficeScan에서는 디지털 자산의 전송을 허용하거나 차단한 후 에이전트 컴퓨터에 알림 메시지를 즉시 표시할 수 있습니다.

디지털 자산 전송이 차단되거나 허용되었음을 사용자에게 알리려면 데이터 손실 방지 정책을 만들 때 **에이전트 사용자에게 알림** 옵션을 선택합니다. 정책 만들기에 대한 자세한 내용은 데이터 손실 방지 정책 구성 페이지 11-45을 참조하십시오.

에이전트에 대한 데이터 손실 방지 알림 구성

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 **디지털 자산 전송**을 선택합니다.
3. 기본 메시지를 적용하거나 수정합니다.
4. **저장**을 클릭합니다.

데이터 손실 방지 로그

에이전트는 디지털 자산 전송(차단 및 허용된 전송)을 기록하여 해당 로그를 서버에 즉시 전송합니다. 에이전트에서 로그를 보낼 수 없는 경우 5분 후에 다시 시도합니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

데이터 손실 방지 로그 보기

절차

1. **에이전트** > **에이전트 관리** 또는 **로그** > **에이전트** > **보안 위험**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **데이터 손실 방지 로그** 또는 **로그 보기** > **DLP 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다.

   로그에는 다음 정보가 포함됩니다.

표 11-10. 데이터 손실 방지 로그 정보

열	설명
날짜/시간	데이터 손실 방지에서 발생을 기록한 날짜 및 시간
사용자	엔드포인트에 로그온한 사용자 이름
엔드포인트	데이터 손실 방지 기능이 전송을 탐지한 엔드포인트 이름
도메인	엔드포인트의 도메인
IP	엔드포인트의 IP 주소
규칙 이름	발생을 트리거한 규칙 이름입니다. **참고** 이전 버전의 OfficeScan에서 생성된 정책에서는 기본 이름 LEGACY_DLP_Policy를 표시합니다.
채널	전송이 발생한 채널

열	설명
프로세스	디지털 자산 전송을 지원한 프로세스(프로세스는 채널에 따라 다름) 자세한 내용은 채널별 프로세스 페이지 11-57를 참조하십시오.
소스	디지털 자산을 포함하는 파일의 소스 또는 채널(소스를 사용할 수 없는 경우)
대상	디지털 자산을 포함하는 파일의 대상 또는 채널(소스를 사용할 수 없는 경우)
조치	전송에 대해 취한 조치
세부 정보	전송에 대한 추가 세부 정보를 포함하는 링크 자세한 내용은 데이터 손실 방지 로그 세부 정보 페이지 11-60를 참조하십시오.

6. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

채널별 프로세스

다음 표에는 데이터 손실 방지 로그의 **프로세스** 열에 표시되는 프로세스가 나와 있습니다.

표 11-11. 채널별 프로세스

채널	프로세스
동기화 소프트웨어(ActiveSync)	동기화 소프트웨어의 전체 경로 및 프로세스 이름 예: C:₩Windows₩system32₩WUDFHost.exe
데이터 레코더(CD/DVD)	데이터 레코더의 전체 경로 및 프로세스 이름 예: C:₩Windows₩Explorer.exe

채널	프로세스
Windows 클립보드	해당 없음
전자 메일 클라이언트 - Lotus Notes	Lotus Notes의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩IBM₩Lotus₩Notes₩nlnotes.exe
전자 메일 클라이언트 - Microsoft Outlook	Microsoft Outlook의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩Microsoft Office₩Office12₩OUTLOOK.EXE
전자 메일 클라이언트 - SMTP 프로토콜을 사용하는 모든 클라이언트	전자 메일 클라이언트의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩Mozilla Thunderbird₩thunderbird.exe
이동식 저장소	저장 장치로 전송되거나 저장 장치 내에서 전송되는 응용 프로그램의 프로세스 이름 예: explorer.exe
FTP	FTP 클라이언트의 전체 경로 및 프로세스 이름 예: D:₩Program Files₩FileZilla FTP Client₩filezilla.exe
HTTP	"HTTP 응용 프로그램"
HTTPS	브라우저 또는 응용 프로그램의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩Internet Explorer₩iexplore.exe
IM 응용 프로그램	IM 응용 프로그램의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩Skype₩Phone₩Skype.exe

채널	프로세스
IM 응용 프로그램 - MSN	• MSN의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩Windows Live₩Messenger₩ msnmsgr.exe • "HTTP 응용 프로그램"(데이터가 채팅 창에서 전송되는 경우)
P2P(피어 투 피어) 응용 프로그램	P2P(피어 투 피어) 응용 프로그램의 전체 경로 및 프로세스 이름 예: D:₩Program Files₩BitTorrent₩bittorrent.exe
PGP 암호화	PGP 암호화 소프트웨어의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩PGP Corporation₩PGP Desktop₩ PGPmnApp.exe
프린터	프린터 작업을 시작한 응용 프로그램의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩Microsoft Office₩Office12₩ WINWORD.EXE
SMB 프로토콜	공유 파일 액세스(파일 복사 또는 새 파일 만들기)가 수행된 응용 프로그램의 전체 경로 및 프로세스 이름 예: C:₩Windows₩Explorer.exe
웹 메일(HTTP 모드)	"HTTP 응용 프로그램"
웹 메일(HTTPS 모드)	브라우저 또는 응용 프로그램의 전체 경로 및 프로세스 이름 예: C:₩Program Files₩Mozilla Firefox₩firefox.exe

데이터 손실 방지 로그 세부 정보

데이터 손실 방지 로그 세부 정보 화면에는 디지털 자산 전송에 대한 추가 세부 정보가 표시됩니다. 전송에 대한 세부 정보는 OfficeScan에서 발생을 탐지한 채널 및 프로세스에 따라 다릅니다.

다음 표에는 표시되는 세부 정보가 나와 있습니다.

표 11-12. 데이터 손실 방지 로그 세부 정보

세부 정보	설명
날짜/시간	데이터 손실 방지에서 발생을 기록한 날짜 및 시간
위반 ID	발생의 고유 ID
사용자	엔드포인트에 로그온한 사용자 이름
엔드포인트	데이터 손실 방지 기능이 전송을 탐지한 엔드포인트 이름
도메인	엔드포인트의 도메인
IP	엔드포인트의 IP 주소
채널	전송이 발생한 채널
프로세스	디지털 자산 전송을 지원한 프로세스(프로세스는 채널에 따라 다름) 자세한 내용은 채널별 프로세스 페이지 11-57를 참조하십시오.
소스	디지털 자산을 포함하는 파일의 소스 또는 채널(소스를 사용할 수 없는 경우)
전자 메일 보낸 사람	전송이 시작된 전자 메일 주소
전자 메일 제목	디지털 자산이 포함된 전자 메일 메시지의 제목 행
전자 메일 받는 사람	전자 메일 메시지의 대상 전자 메일 주소
URL	웹 사이트 또는 웹 페이지의 URL
FTP 사용자	FTP 서버에 로그인하는 데 사용된 사용자 이름
파일 클래스	데이터 손실 방지 기능이 디지털 자산을 탐지한 파일의 형식

세부 정보	설명
규칙/템플릿	탐지를 트리거한 정확한 규칙 이름 및 템플릿의 목록 **참고** 각 규칙에는 발생을 트리거한 템플릿이 여럿 포함될 수 있습니다. 템플릿 이름이 여럿일 때는 쉼표로 구분합니다.
조치	전송에 대해 취한 조치
사용자 정당성 이유	사용자가 중요한 데이터를 계속 전송하기 위해 제공한 이유

데이터 보호 모듈에 대한 디버그 로깅 사용

절차

1. 지원 센터에서 logger.cfg 파일을 받습니다.
2. 다음 데이터를 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`(32 비트 시스템의 경우)에 또는 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\PC-cillinNTCorp\DlpLite`(64 비트 시스템의 경우)에 추가:
   - **종류**: `String`
   - **이름**: `debugcfg`
   - **값**: C:₩Log₩logger.cfg
3. C:₩ directory에 "Log" 폴더를 만듭니다.
4. logger.cfg를 "Log" 폴더에 복사합니다.
5. 웹 콘솔에서 데이터 손실 방지 및 장치 제어 설정을 배포하여 로그 수집을 시작합니다.

참고

레지스트리 키에서 `debugcfg`를 삭제하고 엔드포인트를 다시 시작하여 데이터 보호 모듈에 대한 디버그 로깅을 사용하지 않도록 설정할 수 있습니다.

장 12

웹 검증 사용

이 장에서는 웹 기반 위협에 대해 알아보고 OfficeScan을 사용하여 웹 기반 위협으로부터 네트워크와 컴퓨터를 보호하는 방법을 설명합니다.

다음과 같은 항목이 포함됩니다.

- 웹 위협 정보 페이지 12-2
- C&C(명령 및 제어) 연결 알림 서비스 페이지 12-2
- 웹 검증 페이지 12-4
- 웹 검증 정책 페이지 12-5
- 에이전트 사용자에 대한 웹 위협 알림 페이지 12-13
- 관리자에 대한 C&C 콜백 알림 페이지 12-14
- C&C 콜백 비상 발생 페이지 12-18
- 웹 위협 로그 페이지 12-20

웹 위협 정보

웹 위협에는 인터넷에서 발생하는 광범위한 위협이 포함됩니다. 웹 위협은 하나의 파일이나 방법이 아니라 다양한 파일과 방법을 조합하여 사용해 그 방법이 매우 복잡합니다. 예를 들어, 웹 위협 작성자는 사용되는 버전과 변종을 계속 변경합니다. 웹 위협은 감염된 엔드포인트가 아니라 웹 사이트의 고정된 위치에 있으므로 웹 위협 작성자는 탐지되지 않도록 해당 코드를 계속 수정합니다.

최근에는 해커, 바이러스 제작자, 스패머 및 스파이웨어 제작자로 알려진 사람을 사이버 범죄자라고 합니다. 이러한 사람은 웹 위협을 통해 다음과 같은 두 가지 목표 중 하나를 추구합니다. 첫 번째 목표는 후속 판매를 위해 정보를 훔치는 것입니다. 이로 인해 ID 손실의 형태로 기밀 정보가 노출됩니다. 감염된 엔드포인트는 피싱 공격 또는 다른 정보 캡처 활동을 전달하는 매개체가 될 수도 있습니다. 다른 여러 영향 중에서도 이 위협은 웹 상거래의 신뢰를 떨어뜨려 인터넷 거래에 필요한 신용을 손상시킬 수 있습니다. 두 번째 목표는 사용자의 CPU 전원을 하이재킹하여 이를 유익한 작업을 수행하는 장치로 사용하는 것입니다. 이러한 활동에는 스팸을 보내거나 배포된 서비스 거부(DoS) 공격 또는 PPC(Pay-Per-Click) 활동 형태로 강탈하는 것이 있습니다.

C&C(명령 및 제어) 연결 알림 서비스

Trend Micro C&C(명령 및 제어) 연결 알림 서비스는 향상된 탐지 및 알림 기능을 제공하여 지속적인 고급 위협과 대상 지정 공격으로 인한 손상을 완화합니다. C&C 연결 알림 서비스는 웹 검증 서비스와 통합하여 웹 검증 보안 수준에 따라 탐지한 콜백 주소에 대해 수행되는 조치를 결정합니다.

C&C IP 목록을 사용하면 네트워크 콘텐츠 검사 엔진으로 모든 네트워크 채널을 통한 C&C 연결을 식별하여 C&C 콜백 탐지를 더욱 개선할 수 있습니다.

웹 검증 서비스 보안 수준을 구성하는 방법에 대한 자세한 내용은 웹 검증 정책 구성 페이지 12-5을 참조하십시오.

표 12-1. C&C 연결 알림 서비스 기능

기능	설명
글로벌 정보 목록	Trend Micro 스마트 보호 네트워크에서는 전 세계의 소스를 통해 글로벌 정보 목록을 작성하고 각 C&C 콜백 주소의 위험 수준을 테스트 및 평가합니다. 웹 검증 서비스는 글로벌 정보 목록과 함께 유해 웹 사이트에 대한 검증 점수를 사용하여 고급 위협으로부터의 보호를 개선합니다. 웹 검증 보안 수준에 따라 할당된 위험 수준을 기준으로 유해 웹 사이트나 C&C 서버에 대해 수행하는 조치가 결정됩니다.
Virtual Analyzer 목록	스마트 보호 서버를 Virtual Analyzer와 통합하여 Virtual Analyzer C&C 서버 목록을 가져올 수 있습니다. Virtual Analyzer는 보안 환경에서 잠재적 위험을 평가하고 고급 휴리스틱 및 동작 테스트 방법을 통해 분석된 위협에 위험 수준을 할당합니다. Virtual Analyzer는 가능한 C&C 서버에 연결하려고 시도하는 위협을 Virtual Analyzer 목록에 기록합니다. Virtual Analyzer 목록은 회사별로 달라지며 대상 지정 공격에 대한 맞춤형 보호 기능을 제공합니다. OfficeScan는 Virtual Analyzer에서 목록을 검색하고 글로벌 정보 및 로컬 Virtual Analyzer 목록 모두를 기준으로, 가능한 C&C 위협을 모두 평가합니다. Virtual Analyzer의 의심스러운 개체 목록을 연결하는 방법에 대한 자세한 내용은 의심스러운 개체 목록 설정 구성 페이지 14-32을 참조하십시오.
의심스러운 연결 서비스	의심스러운 연결 서비스에서는 사용자 정의 및 글로벌 IP C&C 목록을 관리하고 엔드포인트와 잠재적인 C&C 서버의 연결 동작을 모니터링합니다. 자세한 내용은 의심스러운 연결 서비스 페이지 8-5를 참조하십시오.
관리자 알림	관리자는 C&C 콜백 탐지 후 자세하고 사용자 정의 가능한 알림을 받도록 선택할 수 있습니다. 자세한 내용은 관리자에 대한 C&C 콜백 알림 구성 페이지 12-14를 참조하십시오.
에이전트 알림	관리자는 엔드포인트에서 C&C 콜백 탐지 후 자세하고 사용자 정의 가능한 알림을 최종 사용자에게 보내도록 선택할 수 있습니다. 자세한 내용은 에이전트 사용자에 대한 C&C 연결 알림 서비스 페이지 12-17를 참조하십시오.

기능	설명
비상 발생 알림	관리자는 C&C 콜백 이벤트 관련 비상 발생 알림을 사용자 정의하고 비상 발생이 단일 엔드포인트에서 발생하는지, 아니면 전체 네트워크에서 발생하는지를 지정할 수 있습니다. 자세한 내용은 C&C 콜백 비상 발생 페이지 12-18를 참조하십시오.
C&C 콜백 로그	로그에서는 모든 C&C 콜백 이벤트와 관련된 자세한 정보를 제공합니다. 자세한 내용은 C&C 콜백 로그 보기 페이지 12-22를 참조하십시오.

웹 검증

웹 검증 기술은 웹 사이트 생성 시기, 악성 프로그램 동작 분석을 통해 발견된 의심스러운 활동의 이력 위치 변경 및 표시와 같은 요소를 기준으로 검증을 할당하여 웹 도메인의 신뢰도를 추적합니다. 그런 다음 계속해서 사이트를 검색하고 사용자가 감염된 사이트에 액세스하지 않도록 차단합니다.

OfficeScan 에이전트는 스마트 보호 소스에 쿼리를 보내 사용자가 액세스하려는 웹 사이트의 검증 상태를 확인합니다. 웹 사이트의 검증은 엔드포인트에 적용된 특정 웹 검증 정책과 상호 관련됩니다. 사용하는 정책에 따라 OfficeScan 에이전트는 웹 사이트에 대한 액세스를 차단하거나 허용합니다.

참고

스마트 보호 소스에 대한 자세한 내용은 스마트 보호 소스 목록 페이지 4-21을 참조하십시오.

안전한 것으로 간주하는 웹 사이트를 승인된 목록에 추가하고 위험한 것으로 간주하는 웹 사이트를 차단된 목록에 추가할 수 있습니다. 그러면 OfficeScan 에이전트에서 이러한 웹 사이트에 대한 액세스를 탐지한 경우 액세스를 자동으로 허용하거나 차단하고 스마트 보호 소스에 더 이상 쿼리를 보내지 않습니다.

웹 검증 정책

웹 검증 정책은 OfficeScan이 웹 사이트에 대한 액세스를 차단할지 허용할지를 지시합니다.

내부 및 외부 에이전트에 대한 정책을 구성할 수 있습니다. OfficeScan 관리자는 일반적으로 외부 에이전트에 대해 더 엄격한 정책을 구성합니다.

정책은 OfficeScan 에이전트 트리의 개별 설정입니다. 에이전트 그룹 또는 개별 에이전트에 특정 정책을 적용할 수 있습니다. 또한 모든 에이전트에 단일 정책을 적용할 수도 있습니다.

정책을 배포하면 에이전트에서 **엔드포인트 위치** 화면(엔드포인트 위치 페이지 15-2 참조)에 설정된 위치 기준을 사용하여 해당 위치 및 적용할 정책을 확인합니다. 에이전트는 위치가 변경될 때마다 정책을 전환합니다.

웹 검증 정책 구성

조직 내에서 HTTP 통신을 처리하도록 프록시 서버를 설정한 상태에서 웹 액세스 허용을 위해 인증이 필요한 경우 프록시 서버 인증 자격 증명을 지정합니다.

프록시 설정 구성에 대한 지침은 OfficeScan 에이전트용 외부 프록시 페이지 15-48를 참조하십시오.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 대상을 선택합니다.
   - Windows 데스크톱 플랫폼을 실행하는 에이전트에 대한 정책을 구성하려면 루트 도메인 아이콘( ), 특정 도메인 또는 에이전트를 선택합니다.

참고

루트 도메인이나 특정 도메인을 선택하는 경우 Windows 데스크톱 플랫폼을 실행하는 에이전트에만 설정이 적용됩니다. Windows Server 플랫폼을 실행하는 에이전트는 해당 도메인에 속한 경우에도 설정이 적용되지 않습니다.

- Windows Server 플랫폼을 실행하는 에이전트에 대한 정책을 구성하려면 특정 에이전트를 선택합니다.

3. **설정** > **웹 검증 설정**을 클릭합니다.
4. **외부 에이전트** 탭을 클릭하여 외부 에이전트에 대한 정책을 구성하거나 **내부 에이전트** 탭을 클릭하여 내부 에이전트에 대한 정책을 구성합니다.

팁

에이전트 위치 설정을 아직 구성하지 않은 경우 구성합니다. 에이전트는 이러한 설정을 사용하여 해당 위치를 확인하고 올바른 웹 검증 정책을 적용합니다. 자세한 내용은 엔드포인트 위치 페이지 15-2를 참조하십시오.

5. **다음 운영 체제에서 웹 검증 정책 사용**을 선택합니다.

1단계에서 선택한 대상에 따라 화면에 나열되는 운영 체제가 달라집니다.

팁

웹 검증 기능이 있는 Trend Micro 제품(예: InterScan Web Security Virtual Appliance)을 이미 사용 중인 경우 내부 에이전트에 대한 웹 검증은 사용하지 않는 것이 좋습니다.

웹 검증 정책을 사용하도록 설정하면

- 외부 에이전트는 스마트 보호 네트워크에 웹 검증 쿼리를 보냅니다.
- 내부 에이전트는 다음 위치에 웹 검증 쿼리를 보냅니다.
  - 스마트 보호 서버 - **스마트 보호 서버에 쿼리 보내기** 옵션을 선택한 경우. 이 옵션에 대한 자세한 내용은 7단계를 참조하십시오.
  - 스마트 보호 네트워크 - **스마트 보호 서버에 쿼리 보내기** 옵션을 선택하지 않은 경우.

6. **점검 모드 사용**을 선택합니다.

참고

점검 모드에서는 에이전트가 모든 웹 사이트에 대한 액세스를 허용하지만 점검을 사용하지 않을 경우 차단되는 것으로 간주되는 웹 사이트에 대한 액세스를 기록합니다. Trend Micro는 웹 사이트를 평가한 다음 평가에 따라 적절한 조치를 취할 수 있도록 점검 모드를 제공합니다. 예를 들어 안전한 것으로 간주하는 웹 사이트를 승인된 목록에 추가할 수 있습니다.

7. **HTTPS URL 확인**을 선택합니다.

HTTPS 통신에서는 인증서를 사용하여 Web server를 식별합니다. 또한 데이터를 암호화하여 도난과 도청을 방지합니다. HTTPS를 사용하여 웹 사이트에 액세스하는 것은 좀 더 안전하기는 하지만 여전히 위험합니다. 손상된 사이트는 유효한 인증서가 있는 경우에도 악성 프로그램을 호스팅하고 개인 정보를 도용할 수 있습니다. 또한 인증서는 비교적 얻기 쉬우므로 이를 통해 HTTPS를 사용하는 악의적인 Web server를 쉽게 설정할 수 있습니다.

HTTPS를 사용하는 손상된 사이트 및 유해 사이트에 노출되는 것을 방지하려면 HTTPS URL 확인을 사용하십시오. OfficeScan에서는 다음 브라우저의 HTTPS 트래픽을 모니터링할 수 있습니다.

표 12-2. HTTPS 트래픽 모니터링에 지원되는 브라우저

브라우저	버전
Microsoft Internet Explorer	• 8.x • 9.x • 10.x • 11.x
Mozilla Firefox	3.5 이상

중요

- HTTPS 검색은 데스크톱 모드로 작동하는 Windows 8, Windows 8.1, Windows 10 또는 Windows 2012 플랫폼만 지원합니다.
- OfficeScan 에이전트에서 처음 HTTPS 검색을 사용하도록 설정한 후에는 HTTPS 검색이 작동하려면 브라우저에서 필요한 Add-on을 사용하도록 설정해야 합니다.
  - Firefox

    Windows 7, 8, 8.1, 10, Server 2008 R2 또는 Server 2012를 실행하는 OfficeScan 에이전트의 경우 사용자는 브라우저 팝업 창 또는 **Add-ons** > **Extensions** 화면에서 Trend Micro Osprey Firefox Extension 2.0.0.1077 Add-on을 사용하도록 설정해야 합니다.

    Windows XP, Vista, Server 2003 또는 Server 2008을 실행하는 OfficeScan 에이전트의 경우 사용자는 브라우저 팝업 창 또는 **Add-ons** > **Extensions** 화면에서 Trend Micro NSC Firefox Extension 5.82.0.1092 추가 기능을 사용하도록 설정해야 합니다.
  - Internet Explorer 9, 10 및 11

    Windows 7, 8, 8.1, 10, Server 2008 R2 또는 Server 2012를 실행하는 OfficeScan 에이전트의 경우 사용자는 브라우저 팝업 창에서 Trend Micro Osprey Plugin Class 추가 기능을 사용하도록 설정해야 합니다.

    Windows XP, Vista, Server 2003 또는 Server 2008을 실행하는 OfficeScan 에이전트의 경우 사용자는 브라우저 팝업 창에서 TmIEPlugInBHO Class 추가 기능을 사용하도록 설정해야 합니다.

  웹 검증을 위한 Internet Explorer 설정 구성에 대한 자세한 내용은 다음 기술 자료 문서를 참조하십시오.

  - http://esupport.trendmicro.com/solution/en-us/1060643.aspx
  - http://esupport.trendmicro.com/solution/en-us/1095350.aspx

8. **일반 HTTP 포트만 검색**을 선택하여 포트 80, 81 및 8080을 통한 트래픽으로 웹 검증 검색을 제한합니다. 기본적으로 OfficeScan에서는 모든 포트의 모든 트래픽을 검색합니다.

참고

Windows 7, 8, 8.1, 10 또는 Windows Server 2008 R2, 2012 이상 플랫폼에서는 지원되지 않습니다.

9. 내부 에이전트가 스마트 보호 서버에 웹 검증 쿼리를 보내도록 하려면 **스마트 보호 서버에 쿼리 보내기**를 선택합니다.

- 이 옵션을 사용하는 경우
  - 에이전트는 스마트 보호 소스 목록을 참조하여 쿼리를 보낼 스마트 보호 서버를 확인합니다.

    스마트 보호 소스 목록에 대한 자세한 내용은 스마트 보호 소스 목록 페이지 4-21을 참조하십시오.
  - 스마트 보호 서버를 사용할 수 있는지 확인합니다. 사용 가능한 스마트 보호 서버가 없는 경우 에이전트는 스마트 보호 네트워크에 쿼리를 보내지 않습니다. 에이전트가 사용할 수 있는 웹 검증 데이터 소스는 승인된 URL 목록과 차단된 URL 목록(10단계에서 구성)뿐입니다.
  - 에이전트를 프록시 서버를 통해 스마트 보호 서버에 연결하려면 **관리** > **설정** > **프록시** > **내부 프록시** 탭에서 프록시 설정을 지정합니다.
  - 스마트 보호 서버를 정기적으로 업데이트하여 보호 상태를 최신 상태로 유지해야 합니다.
  - 테스트되지 않은 웹 사이트는 에이전트에서 차단되지 않습니다. 이러한 웹 사이트에 대한 웹 검증 데이터는 스마트 보호 서버에 저장되지 않습니다.
- 이 옵션을 사용하지 않는 경우
  - 에이전트는 스마트 보호 네트워크에 웹 검증 쿼리를 보냅니다. 쿼리를 성공적으로 보내려면 에이전트 엔드포인트가 인터넷에 연결되어 있어야 합니다.
  - 스마트 보호 네트워크에 연결하는 데 프록시 서버 인증이 필요한 경우 **관리** > **설정** > **프록시** > **외부 프록시(탭)** > **Trend Micro 서버와 OfficeScan 에이전트 연결**에서 인증 자격 증명을 지정합니다.

- 11단계에서 **Trend Micro에서 테스트하지 않은 페이지 차단** 옵션을 선택하면 테스트되지 않은 웹 사이트를 에이전트에서 차단합니다.

10. 웹 검증 보안 수준을 **높음**, **보통**, **낮음** 중에서 선택합니다.

참고

보안 수준에 따라 OfficeScan에서 URL에 대한 액세스를 허용할지 또는 차단할지가 결정됩니다. 예를 들어 보안 수준을 낮음으로 설정하면 OfficeScan에서는 웹 위협으로 알려진 URL만 차단합니다. 보안 수준을 더 높게 설정하면 웹 위협 탐지 비율은 향상되지만 잘못 판정될 가능성도 높아집니다.

---

11. 9단계에서 **스마트 보호 서버에 쿼리 보내기**를 사용하지 않도록 설정한 경우 **Trend Micro에서 테스트하지 않은 페이지 차단**을 선택할 수 있습니다.

참고

Trend Micro에서 웹 페이지의 안전성을 철저히 테스트하지만 새롭거나 잘 알려지지 않은 웹 사이트를 방문할 때 테스트되지 않은 페이지가 나타날 수 있습니다. 테스트되지 않은 페이지에 대한 액세스를 차단하면 안전성이 향상되지만 안전한 페이지에 대한 액세스가 차단될 수도 있습니다.

---

12. **유해 스크립트가 포함된 페이지 차단**을 선택하여 웹 브라우저 위협과 유해 스크립트를 식별하고 이러한 위협으로 인한 웹 브라우저 손상을 방지합니다.

    OfficeScan은 브라우저 위협 방지 패턴과 스크립트 분석 패턴을 모두 활용하여 웹 페이지를 식별 및 차단함으로써 시스템이 위협에 노출되지 않도록 합니다

표 12-3. 브라우저 위협 방지를 지원하는 브라우저

브라우저	버전
Microsoft Internet Explorer	• 7.x • 8.x • 9.x • 10.x • 11.x

중요

브라우저 위협 방지 기능을 사용하려면 고급 보호 서비스를 사용하도록 설정해야 합니다.

고급 보호 서비스를 사용하도록 설정하려면 **에이전트** > **에이전트 관리**로 이동한 후 **설정** > **추가 서비스 설정**을 클릭합니다.

OfficeScan 에이전트에서 브라우저 위협 방지 기능을 사용하도록 처음 설정한 후 사용자는 브라우저에서 필수 추가 기능을 사용하도록 설정해야 브라우저 위협 방지 기능이 작동합니다. Internet Explorer 9, 10 또는 11을 실행하는 OfficeScan 에이전트의 경우 사용자는 브라우저 팝업 창에서 Trend Micro IE Protection 추가 기능을 사용하도록 설정해야 합니다.

13. 승인된 목록과 차단된 목록을 구성합니다.

참고

승인된 목록이 차단된 목록보다 우선합니다. URL이 승인된 목록에 있는 항목과 일치하는 경우 에이전트는 URL이 차단된 목록에 있더라도 해당 URL에 대한 액세스를 항상 허용합니다.

a. **승인/차단된 목록 사용**을 선택합니다.

b. URL을 입력합니다.

URL의 아무 곳에나 와일드카드 문자(*)를 추가할 수 있습니다.

예:

- www.trendmicro.com/*를 입력하면 Trend Micro 웹 사이트의 모든 페이지가 승인됩니다.
- *.trendmicro.com/*를 입력하면 trendmicro.com의 모든 하위 도메인에 있는 모든 페이지가 승인됩니다.

IP 주소가 포함된 URL을 입력할 수 있습니다. URL에 IPv6 주소가 포함된 경우 주소를 괄호로 묶습니다.

c. **승인된 목록에 추가** 또는 **차단된 목록에 추가**를 클릭합니다.

d. 목록을 .dat 파일로 내보내려면 **내보내기**를 클릭한 다음 **저장**을 클릭합니다.

e. 다른 서버에서 목록을 내보낸 경우 이 목록을 이 화면으로 가져오려면 **가져오기**를 클릭한 다음 .dat 파일을 찾습니다. 목록이 화면에 로드됩니다.

중요

웹 검증에서는 승인된 목록과 차단된 목록에 있는 주소는 검색하지 않습니다.

---

14. 웹 검증 피드백을 제출하려면 **URL 다시 점검** 아래에 제공된 URL을 클릭합니다. Trend Micro 웹 검증 쿼리 시스템이 브라우저 창에 열립니다.

15. OfficeScan 에이전트가 서버에 웹 검증 로그를 보내도록 허용할지 여부를 선택합니다. OfficeScan에서 차단하는 URL을 분석하고 액세스해도 안전하다고 판단되는 URL을 적절히 처리하려는 경우 에이전트에서 로그를 보내도록 허용합니다.

16. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

에이전트 사용자에 대한 웹 위협 알림

OfficeScan에서 웹 검증 정책을 위반하는 URL을 차단한 이후 즉시 OfficeScan 에이전트 엔드포인트에 알림 메시지를 표시할 수 있습니다. 알림 메시지를 사용하도록 설정하고 선택적으로 알림 메시지의 내용을 수정해야 합니다.

웹 위협 알림 메시지 사용

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭합니다.
5. **웹 검증 설정** 섹션에서 **웹 사이트가 차단되면 알림 표시**를 선택합니다.
6. **C&C 콜백 설정** 섹션에서 **C&C 콜백이 발견되면 알림 표시**를 선택합니다.
7. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

웹 위협 알림 수정

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 수정할 웹 위협 알림 유형을 선택합니다.
   - **웹 검증 위반**
   - **C&C 콜백**
3. 제공된 텍스트 상자에서 기본 메시지를 수정합니다.
4. **저장**을 클릭합니다.

관리자에 대한 C&C 콜백 알림

OfficeScan에서는 사용자 자신과 다른 OfficeScan 관리자에게 C&C 콜백 탐지를 알리는 일련의 기본 알림 메시지를 제공합니다. 요구 사항에 맞게 알림을 수정하고 추가 알림 설정을 구성할 수 있습니다.

관리자에 대한 C&C 콜백 알림 구성

절차

1. **관리** > **알림** > **관리자**으로 이동합니다.
2. **기준** 탭에서 다음을 수행합니다.
   a. **C&C 콜백** 섹션으로 이동합니다.

b. OfficeScan에서 C&C 콜백을 탐지한 경우(조치는 차단 또는 기록일 수 있음) 알림을 보낼지 아니면 콜백 주소의 위험 수준이 높음인 경우에만 알림을 보낼지를 지정합니다.

3. **전자 메일** 탭에서 다음을 수행합니다.

a. **C&C 콜백** 섹션으로 이동합니다.

b. **전자 메일을 통한 알림 사용**을 선택합니다.

c. **에이전트 트리 도메인 권한이 있는 사용자에게 알림 보내기**를 선택합니다.

역할 기반 관리를 사용하여 사용자에게 에이전트 트리 도메인 권한을 부여할 수 있습니다. 특정 도메인에 속한 에이전트에서 전송이 수행되는 경우 도메인 권한이 있는 사용자의 전자 메일 주소로 전자 메일이 전송됩니다. 다음 표의 예를 참조하십시오.

표 12-4. 에이전트 트리 도메인 및 권한

에이전트 트리 도메인	도메인 권한이 있는 역할	역할이 있는 사용자 계정	사용자 계정의 전자 메일 주소
도메인 A	관리자(기본 제공)	루트	mary@xyz.com
	Role_01	admin_john	john@xyz.com
		admin_chris	chris@xyz.com
도메인 B	관리자(기본 제공)	루트	mary@xyz.com
	Role_02	admin_jane	jane@xyz.com

도메인 A에 속한 OfficeScan 에이전트에서 C&C 콜백을 발견한 경우 mary@xyz.com, john@xyz.com 및 chris@xyz.com으로 전자 메일이 전송됩니다.

도메인 B에 속한 OfficeScan 에이전트에서 C&C 콜백을 탐지한 경우 mary@xyz.com 및 jane@xyz.com으로 전자 메일이 전송됩니다.

참고

이 옵션을 사용할 때는 도메인 권한이 있는 모든 사용자에게 해당 전자 메일 주소가 있어야 합니다. 전자 메일 주소가 없는 사용자에게는 전자 메일 알림이 전송되지 않습니다. 사용자 및 전자 메일 주소는 **관리** > **계정 관리** > **사용자 계정**에서 구성합니다.

d. **다음 전자 메일 주소로 알림 보내기**를 선택하고 전자 메일 주소를 입력합니다.

e. 기본 제목 및 메시지를 적용하거나 수정합니다. **제목** 및 **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다.

표 12-5. C&C 콜백 알림용 토큰 변수

변수	설명
%CLIENTCOMPUTER%	콜백을 전송한 대상 엔드포인트
%IP%	대상 엔드포인트의 IP 주소
%DOMAIN%	컴퓨터의 도메인
%DATETIME%	전송이 탐지된 날짜 및 시간
%CALLBACKADDRESS%	C&C 서버의 콜백 주소
%CNCRISKLEVEL%	C&C 서버의 위험 수준
%CNCLISTSOURCE%	C&C 소스 목록을 나타냄
%ACTION%	수행한 조치

4. **SNMP 트랩** 탭에서 다음을 수행합니다.

   a. **C&C 콜백** 섹션으로 이동합니다.

   b. **SNMP 트랩을 통한 알림 사용**을 선택합니다.

   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 12-5 : C&C 콜백 알림용 토큰 변수 페이지 12-16를 참조하십시오.

5. **NT 이벤트 로그** 탭에서 다음을 수행합니다.

   a. **C&C 콜백** 섹션으로 이동합니다.

   b. **NT 이벤트 로그를 통한 알림 사용**을 선택합니다.

   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 12-5 : C&C 콜백 알림용 토큰 변수 페이지 12-16를 참조하십시오.

6. **저장**을 클릭합니다.

에이전트 사용자에 대한 C&C 연결 알림 서비스

OfficeScan에서는 C&C 서버 URL을 차단한 후 즉시 OfficeScan 에이전트 컴퓨터에 알림 메시지를 표시할 수 있습니다. 알림 메시지를 사용하도록 설정해야 하며 필요한 경우 알림 메시지의 내용을 수정할 수도 있습니다.

C&C 콜백 알림 메시지 사용

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭합니다.
5. **C&C 콜백 설정** 섹션에서 **C&C 콜백이 발견되면 알림 표시**를 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

C&C 콜백 알림 수정

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 **C&C 콜백**을 선택합니다.
3. 제공된 텍스트 상자에서 기본 메시지를 수정합니다.
4. **저장**을 클릭합니다.

C&C 콜백 비상 발생

콜백 수, 소스 및 위험 수준으로 C&C 콜백 비상 발생을 정의합니다.

OfficeScan에서는 사용자 자신과 다른 OfficeScan 관리자에게 비상 발생을 알리는 기본 알림 메시지를 제공합니다. 요구 사항에 맞게 알림 메시지를 수정할 수 있습니다.

참고

OfficeScan에서는 전자 메일을 통해 C&C 콜백 비상 발생 알림을 보낼 수 있습니다. OfficeScan에서 전자 메일을 보낼 수 있도록 전자 메일 설정을 구성하십시오. 자세한 내용은 관리자 알림 설정 페이지 14-35를 참조하십시오.

C&C 콜백 비상 발생 기준 및 알림 구성

절차

1. **관리** > **알림** > **비상 발생**으로 이동합니다.
2. **기준** 탭에서 다음 옵션을 구성합니다.

옵션	설명
같은 손상된 호스트	엔드포인트별 콜백 탐지를 기준으로 비상 발생을 정의하려면 선택합니다.
C&C 위험 수준	비상 발생을 모든 C&C 콜백에서 트리거할지, 아니면 위험 수준이 높은 소스에서만 트리거할지를 지정합니다.
조치	**모든 조치**, **기록됨** 또는 **차단됨** 중에서 선택합니다.
탐지	비상 발생을 정의하는 데 필요한 탐지 수를 나타냅니다.
시간	이러한 수의 탐지가 어느 정도 시간 이내에 발생해야 하는지를 나타냅니다.

팁

Trend Micro에서는 이 화면에서 기본값을 적용할 것을 권장합니다.

3. **전자 메일** 탭에서 다음을 수행합니다.
   a. **C&C 콜백** 섹션으로 이동합니다.
   b. **전자 메일을 통한 알림 사용**을 선택합니다.
   c. 전자 메일 받는 사람을 지정합니다.
   d. 기본 전자 메일 제목 및 메시지를 적용하거나 수정합니다. **제목** 및 **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다.

표 12-6. C&C 콜백 비상 발생 알림용 토큰 변수

변수	설명
%C	C&C 콜백 로그 수

변수	설명
%T	C&C 콜백 로그가 누적된 기간

e. 사용 가능한 추가 C&C 정보에서 전자 메일에 포함할 정보를 선택합니다.

4. **SNMP 트랩** 탭에서 다음을 수행합니다.

   a. **C&C 콜백** 섹션으로 이동합니다.

   b. **SNMP 트랩을 통한 알림 사용**을 선택합니다.

   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 12-6 : C&C 콜백 비상 발생 알림용 토큰 변수 페이지 12-19를 참조하십시오.

5. **NT 이벤트 로그** 탭에서 다음을 수행합니다.

   a. **C&C 콜백** 섹션으로 이동합니다.

   b. **NT 이벤트 로그를 통한 알림 사용**을 선택합니다.

   c. 기본 메시지를 적용하거나 수정합니다. **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다. 자세한 내용은 표 12-6 : C&C 콜백 비상 발생 알림용 토큰 변수 페이지 12-19를 참조하십시오.

6. **저장**을 클릭합니다.

웹 위협 로그

웹 검증 로그를 서버로 보내도록 내부 및 외부 에이전트를 모두 구성합니다. OfficeScan에서 차단되는 URL을 분석하여 액세스하기에 안전하다고 생각되는 URL에 대해 적절한 조치를 취하려는 경우에 이 방법을 사용합니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

웹 검증 로그 보기

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그 보기** > **웹 검증 로그** 또는 **로그** > **웹 검증 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.

항목	설명
날짜/시간	탐지가 발생한 시간
엔드포인트	탐지가 발생한 엔드포인트
도메인	탐지가 발생한 엔드포인트의 도메인
URL	웹 검증 서비스에서 차단하는 URL
위험 수준	URL의 위험 수준
설명	보안 위협에 대한 설명
프로세스	연결을 시도한 프로세스(path\application_name)
조치	탐지에 대해 수행한 조치

6. 차단하지 않아야 할 URL이 있는 경우 **승인된 목록에 추가** 단추를 클릭하여 승인된 URL 목록에 웹 사이트를 추가합니다.
7. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **모두 CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

C&C 콜백 로그 보기

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그 보기** > **C&C 콜백 로그** 또는 **로그** > **C&C 콜백 로그**를 클릭합니다.
4. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
5. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.

항목	설명
날짜/시간	탐지가 발생한 시간
사용자	탐지 당시 로그온한 사용자
손상된 호스트	콜백이 시작된 엔드포인트
IP 주소	손상된 호스트의 IP 주소
도메인	탐지가 발생한 엔드포인트의 도메인
콜백 주소	엔드포인트가 콜백을 보낸 주소
C&C 목록 소스	C&C 서버를 식별한 C&C 목록 소스
C&C 위험 수준	C&C 서버의 위험 수준
프로토콜	전송에 사용된 인터넷 프로토콜
프로세스	전송을 시작한 프로세스(path\application_name)
조치	콜백에 대해 수행한 조치

6. 차단하지 않아야 할 URL을 웹 검증에서 차단한 경우 **웹 검증 승인된 목록에 추가** 단추를 클릭하여 웹 검증 승인된 목록에 주소를 추가합니다.

참고

OfficeScan에서는 웹 검증 승인된 목록에 URL만 추가할 수 있습니다. 글로벌 C&C IP 목록 또는 Virtual Analyzer(IP) C&C 목록에 따른 탐지의 경우 사용자 정의 승인된 C&C IP 목록에 이러한 IP 주소를 수동으로 추가하십시오.

자세한 내용은 글로벌 사용자 정의 IP 목록 설정 구성 페이지 8-6를 참조하십시오.

7. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **모두 CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

장 13

OfficeScan 방화벽 사용

이 장에서는 OfficeScan 방화벽의 기능 및 구성에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- OfficeScan 방화벽 정보 페이지 13-2
- OfficeScan 방화벽 설정 또는 해제 페이지 13-6
- 방화벽 정책 및 프로필 페이지 13-8
- 방화벽 권한 페이지 13-22
- 글로벌 방화벽 설정 페이지 13-24
- OfficeScan 에이전트 사용자에 대한 방화벽 위반 알림 페이지 13-26
- 방화벽 로그 페이지 13-28
- 방화벽 위반 비상 발생 페이지 13-29
- OfficeScan 방화벽 테스트 페이지 13-31

OfficeScan 방화벽 정보

OfficeScan 방화벽은 상태 기반 검사 및 고성능 네트워크 바이러스 검색을 통해 네트워크에서 에이전트와 서버를 보호합니다. 중앙 관리 콘솔을 통해서는 규칙을 작성하여 응용 프로그램, IP 주소, 포트 번호 또는 프로토콜에 따라 연결을 필터링한 다음 다른 사용자 그룹에 규칙을 적용할 수 있습니다.

참고

Windows 방화벽을 사용 중인 Windows XP 엔드포인트에서도 OfficeScan 방화벽을 설정, 구성 및 사용할 수 있습니다. 그러나 방화벽 정책이 충돌하거나 예상치 못한 결과가 일어나지 않도록 정책을 주의해서 관리하십시오. Windows 방화벽에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

OfficeScan 방화벽에는 다음과 같은 주요 기능과 장점이 있습니다.

- 트래픽 필터링 페이지 13-2
- 응용 프로그램 필터링 페이지 13-3
- 인증된 안전한 소프트웨어 목록 페이지 13-3
- 네트워크 바이러스 검색 페이지 13-3
- 사용자 정의 가능한 프로필 및 정책 페이지 13-3
- 상태 기반 검사 페이지 13-4
- 침입 탐지 시스템(IDS) 페이지 13-4
- 방화벽 위반 비상 발생 모니터 페이지 13-5
- OfficeScan 에이전트 방화벽 권한 페이지 13-6

트래픽 필터링

OfficeScan 방화벽에서는 들어오고 나가는 모든 트래픽을 필터링하여 다음 기준에 따라 특정 유형의 트래픽을 차단할 수 있습니다.

- 방향(인바운드/아웃바운드)

- 프로토콜(TCP/UDP/ICMP/ICMPv6)
- 대상 포트
- 소스 및 대상 엔드포인트

응용 프로그램 필터링

OfficeScan 방화벽은 특정 응용 프로그램에 대한 들어오는 트래픽과 나가는 트래픽을 필터링하여 이러한 응용 프로그램에서 네트워크에 액세스할 수 있도록 합니다. 그러나 네트워크 연결은 관리자가 설정한 정책에 따라 다릅니다.

인증된 안전한 소프트웨어 목록

인증된 안전한 소프트웨어 목록에서는 방화벽 정책 보안 수준을 우회할 수 있는 응용 프로그램 목록을 제공합니다. 이러한 응용 프로그램에 대해서는 보안 수준이 보통 또는 높음으로 설정된 경우에도 OfficeScan에서 실행 및 네트워크 액세스를 허용합니다.

전체 목록을 확인하려면 글로벌 인증된 안전한 소프트웨어 목록 쿼리를 사용하면 됩니다. 이 목록은 Trend Micro에 의해 동적으로 업데이트됩니다.

참고

이 기능은 동작 모니터링과 연동됩니다. 글로벌 인증된 안전한 소프트웨어 목록을 사용하기 전에 무단 변경 방지 서비스 및 인증된 안전한 소프트웨어 서비스를 사용하도록 설정해야 합니다.

네트워크 바이러스 검색

또한 OfficeScan 방화벽은 각 패킷에 네트워크 바이러스가 있는지 검사합니다. 자세한 내용은 바이러스 및 악성 프로그램 페이지 7-2를 참조하십시오.

사용자 정의 가능한 프로필 및 정책

OfficeScan 방화벽을 사용하면 지정한 유형의 네트워크 트래픽을 차단하거나 허용하도록 정책을 구성할 수 있습니다. 하나 이상의 프로필에 정책을 할당한 다

음 지정한 OfficeScan 에이전트에 배포할 수 있습니다. 이렇게 하면 고도로 사용자 정의된 방법을 통해 에이전트에 대한 방화벽 설정을 조직 및 구성할 수 있습니다.

상태 기반 검사

OfficeScan 방화벽은 상태 기반 검사(Stateful Inspection) 방화벽으로, OfficeScan 에이전트에 대한 모든 연결을 모니터링하고 모든 연결 상태를 기억합니다. 이 방화벽은 연결 시 특정 상태를 식별하고 수행해야 할 조치를 예측하며 정상적으로 연결되어 있을 때 중단을 검색할 수 있습니다. 따라서 방화벽을 효율적으로 사용하려면 프로필과 정책을 만드는 것 뿐만 아니라 방화벽을 통과하는 패킷을 필터링하고 연결도 분석해야 합니다.

침입 탐지 시스템(IDS)

OfficeScan 방화벽에는 침입 탐지 시스템(IDS)도 포함됩니다. IDS를 사용하면 OfficeScan 에이전트에 대한 공격을 나타낼 수 있는 네트워크 패킷의 패턴을 식별하는 데 도움이 됩니다. OfficeScan 방화벽은 다음과 같은 잘 알려진 침입을 막습니다.

침입	설명
Too Big Fragment	해커가 대상 엔드포인트에 과도한 크기의 TCP/UDP 패킷을 지정하는 서비스 거부(DoS) 공격입니다. 이로 인해 엔드포인트 버퍼에 오버플로가 발생하여 엔드포인트가 정지되거나 다시 부팅될 수 있습니다.
Ping of Death	해커가 대상 엔드포인트에 과도한 크기의 ICMP/ICMPv6 패킷을 지정하는 서비스 거부(DoS) 공격입니다. 이로 인해 엔드포인트 버퍼에 오버플로가 발생하여 엔드포인트가 정지되거나 다시 부팅될 수 있습니다.
Conflicted ARP	해커가 동일한 소스 및 대상 IP 주소를 사용하여 ARP(Address Resolution Protocol) 요청을 대상 엔드포인트로 보내는 공격 유형입니다. 대상 엔드포인트가 ARP 응답(해당 MAC 주소)을 자신에게 계속 보내게 되므로 엔드포인트가 정지하거나 충돌이 발생합니다.

침입	설명
SYN Flood	하나의 프로그램이 다수의 TCP 동기화(SYN) 패킷을 엔드포인트로 전송하여 엔드포인트에서 동기화 인식(SYN/ACK) 응답을 계속 전송하게 하는 서비스 거부(DoS) 공격입니다. 이로 인해 엔드포인트 메모리 소모량이 많아져 결국에는 엔드포인트가 중지될 수 있습니다.
Overlapping Fragment	Teardrop 공격과 마찬가지로, 이 서비스 거부(DoS) 공격은 오버래핑 TCP 단편을 엔드포인트로 전송합니다. 이로 인해 첫 번째 TCP 단편의 헤더 정보를 덮어쓰고 방화벽을 통과할 수 있게 됩니다. 그러면 악성 코드가 들어 있는 나머지 단편이 방화벽을 통과하여 대상 엔드포인트로 전달될 수 있습니다.
Teardrop	Overlapping fragment 공격과 마찬가지로, 이 서비스 거부(DoS) 공격도 IP 단편을 처리합니다. 두 번째 또는 나머지 IP 단편에서 오프셋 값이 혼동되기 때문에 단편 재결합을 시도할 때 수신 엔드포인트 운영 체제에서 충돌이 발생할 수 있습니다.
Tiny Fragment Attack	작은 TCP 단편 크기가 첫 번째 TCP 패킷 헤더 정보를 다음 단편에 강제로 적용하는 공격 유형입니다. 이로 인해 트래픽을 필터링하는 라우터에서 악의적인 데이터가 포함되어 있을 수 있는 이후의 단편을 무시할 수 있습니다.
Fragmented IGMP	Fragmented IGMP 패킷을 대상 엔드포인트로 전송하여 IGMP 패킷을 올바르게 처리할 수 없게 하는 서비스 거부(DoS) 공격입니다. 이로 인해 엔드포인트가 정지하거나 속도가 느려질 수 있습니다.
LAND Attack	소스 및 대상 주소가 동일한 IP 동기화(SYN) 패킷을 엔드포인트로 전송하여 엔드포인트에서 동기화 인식(SYN/ACK) 응답을 자신에게 전송하게 하는 공격 유형입니다. 이로 인해 엔드포인트가 정지하거나 속도가 느려질 수 있습니다.

방화벽 위반 비상 발생 모니터

OfficeScan 방화벽에서는 방화벽 위반이 특정 임계값을 초과하는 경우(공격을 알리는 신호일 수 있음) 지정된 수신자에게 사용자 정의 알림 메시지를 보냅니다.

OfficeScan 에이전트 방화벽 권한

OfficeScan 에이전트 콘솔에서 방화벽 설정을 볼 수 있는 권한을 OfficeScan 에이전트 사용자에게 부여합니다. 또한 방화벽, 침입 탐지 시스템 및 방화벽 위반 알림 메시지를 사용하거나 사용하지 않도록 설정하는 권한도 사용자에게 부여합니다.

OfficeScan 방화벽 설정 또는 해제

OfficeScan 서버를 설치하는 동안 OfficeScan 방화벽을 설정 또는 해제할지 묻는 메시지가 표시됩니다.

설치하는 동안 방화벽을 설정한 경우 성능이 저하되면(특히 Windows Server 2003, Windows Server 2008, Windows Server 2012 등의 서버 플랫폼) 방화벽을 해제하는 것이 좋습니다.

설치하는 동안 방화벽을 사용하지 않도록 설정했지만 에이전트 침입을 방지하기 위해 방화벽을 사용하도록 설정하려면 먼저 OfficeScan 에이전트 서비스 페이지 15-7에서 지침을 읽어 보십시오.

전체 또는 선택한 OfficeScan 에이전트 엔드포인트에서 방화벽을 사용하거나 사용하지 않도록 설정할 수 있습니다.

선택한 엔드포인트에서 OfficeScan 방화벽 사용 또는 사용 안 함

웹 콘솔에서 다음 방법 중 하나를 사용하여 방화벽을 사용하거나 사용하지 않도록 설정합니다.

방법	절차
새 정책을 만들어 OfficeScan 에이전트에 적용합니다.	1. 방화벽을 설정/해제하는 새 정책을 만듭니다. 새 정책을 만드는 단계에 대해서는 방화벽 정책 추가 페이지 13-10을 참조하십시오. 2. 정책을 OfficeScan 에이전트에 적용합니다.

방법	절차
웹 콘솔에서 방화벽 서비스를 설정/해제합니다.	자세한 단계는 OfficeScan 에이전트 서비스 페이지 15-7를 참조하십시오. **참고** 방화벽 서비스를 사용하지 않도록 설정하면 선택한 에이전트에서 모든 방화벽 정책이 자동으로 사용하지 않도록 설정됩니다.

선택된 엔드포인트에서 다음 방법 중 하나를 사용하여 방화벽을 사용하거나 사용하지 않도록 설정합니다.

방법	절차
방화벽 드라이버를 사용하거나 사용하지 않도록 설정합니다.	1. **Windows 네트워크 연결 속성**을 엽니다. 2. 네트워크 카드에서 **Trend Micro 방화벽 드라이버** 확인란을 선택하거나 선택을 취소합니다.
방화벽 서비스를 사용하거나 사용하지 않도록 설정합니다.	1. 명령 프롬프트를 열고 `services.msc`를 입력합니다. 2. MMC(Microsoft Management Console)에서 **OfficeScan NT 방화벽**을 시작하거나 중지합니다.

모든 엔드포인트에서 OfficeScan 방화벽 사용 또는 사용 안 함

절차

1. **관리** > **설정** > **제품 라이선스**로 이동합니다.
2. **추가 서비스** 섹션으로 이동합니다.
3. **추가 서비스** 섹션의 **엔드포인트용 방화벽** 행 옆에서 **사용** 또는 **사용 안 함**을 클릭합니다.

방화벽 정책 및 프로필

OfficeScan 방화벽은 정책 및 프로필을 사용하여 네트워크로 연결된 엔드포인트를 보호하기 위한 방법을 구성하고 사용자 정의합니다.

Active Directory 통합 및 역할 기반 관리를 통해 각 사용자는 권한에 따라 특정 도메인에 대한 정책 및 프로필을 만들거나 구성하거나 삭제할 수 있습니다.

팁

동일한 엔드포인트에 여러 방화벽을 설치하면 예상치 못한 결과가 발생할 수 있습니다. OfficeScan 방화벽을 배포하고 사용하기 전에 OfficeScan 에이전트에서 다른 소프트웨어 기반 방화벽 응용 프로그램을 제거하십시오.

다음은 OfficeScan 방화벽을 성공적으로 사용하기 위해 필요한 단계입니다.

1. 정책을 만듭니다. 정책을 사용하면 네트워크로 연결된 엔드포인트에서 트래픽을 차단 또는 허용하고 방화벽 기능을 사용하도록 설정하는 보안 수준을 선택할 수 있습니다.
2. 정책에 예외를 추가합니다. 예외를 사용하면 OfficeScan 에이전트를 정책에서 제외할 수 있습니다. 예외를 사용하면 에이전트를 지정하고, 정책의 보안 수준 설정과 관계없이 특정 유형의 트래픽을 허용하거나 차단할 수 있습니다. 예를 들어 정책에서는 일련의 에이전트에 대해 모든 트래픽을 차단하지만, 에이전트가 Web server에 액세스할 수 있도록 HTTP 트래픽을 허용하는 예외를 만듭니다.
3. 프로필을 만들고 OfficeScan 에이전트에 프로필을 할당합니다. 방화벽 프로필은 일련의 에이전트 특성을 포함하며 정책과 연결됩니다. 에이전트가 프로필에 지정된 특성과 일치하면 연관된 정책이 트리거됩니다.

방화벽 정책

방화벽 정책을 사용하면 정책 예외에 지정되지 않은 특정 유형의 네트워크 트래픽을 차단하거나 허용할 수 있습니다. 또한 정책은 사용하거나 사용하지 않도록 설정된 방화벽 기능을 정의합니다. 정책을 하나 이상의 방화벽 정책에 할당합니다.

Active Directory 통합 및 역할 기반 관리를 통해 각 사용자는 권한에 따라 특정 도메인에 대한 정책을 만들거나 구성하거나 삭제할 수 있습니다.

다음 표에서는 방화벽 정책을 구성할 때 사용할 수 있는 설정을 간략히 설명합니다.

설정	설명
보안 수준	OfficeScan 에이전트 엔드포인트에서 모든 인바운드 및/또는 아웃바운드 트래픽을 차단하거나 허용하는 일반 설정입니다.
방화벽 기능	OfficeScan 방화벽, 침입 탐지 시스템(IDS) 및 방화벽 위반 알림 메시지의 사용 여부를 지정합니다. 자세한 내용은 침입 탐지 시스템(IDS) 페이지 13-4를 참조하십시오.
인증된 안전한 소프트웨어 목록	인증된 안전한 응용 프로그램을 네트워크에 연결하도록 허용할지 여부를 지정합니다. 자세한 내용은 인증된 안전한 소프트웨어 목록 페이지 13-3를 참조하십시오.
정책 예외 목록	다양한 유형의 네트워크 트래픽을 차단하거나 허용하도록 구성할 수 있는 예외 목록입니다.

참고

방화벽 프로필을 만들 때 최종 사용자에게 보안 수준 및 정책 예외 목록을 수정할 수 있는 권한을 부여할 수 있습니다.

자세한 내용은 방화벽 프로필 추가 페이지 13-20를 참조하십시오.

기본 방화벽 정책

OfficeScan에는 사용자가 수정하거나 삭제할 수 있는 기본 정책 집합이 제공됩니다.

정책 이름	보안 수준	에이전트 설정	예외	사용 권장 시기
모든 액세스	낮음	방화벽 사용	없음	에이전트에 네트워크에 대한 무제한 액세스 권한을 부여하려는 경우 사용합니다.
Trend Micro Control Manager용 통신 포트	낮음	방화벽 사용	포트 80 및 10319를 통해 들어오고 나가는 모든 TCP/UDP 트래픽 허용	에이전트에 MCP 에이전트가 설치되어 있는 경우에 사용합니다.
ScanMail for Microsoft Exchange 콘솔	낮음	방화벽 사용	포트 16372를 통해 들어오고 나가는 모든 TCP 트래픽 허용	에이전트가 ScanMail 콘솔에 액세스해야 하는 경우 사용합니다.
IMSS(InterScan Messaging Security Suite) 콘솔	낮음	방화벽 사용	포트 80를 통해 들어오고 나가는 모든 TCP 트래픽 허용	에이전트가 IMSS 콘솔에 액세스해야 하는 경우 사용합니다.

방화벽 정책 추가

절차

1. **에이전트** > **방화벽** > **정책**으로 이동합니다.
2. 새 정책을 추가하려면 **추가**를 클릭합니다.

   만들려는 새 정책에 기존 정책과 비슷한 설정이 있을 경우에는 기존 정책을 선택하고 **복사**를 클릭합니다.
3. 정책의 이름을 입력합니다.
4. 보안 수준을 선택합니다.

   선택한 보안 수준은 방화벽 정책 예외 기준에 맞는 트래픽에는 적용되지 않습니다.
5. 정책에 사용할 방화벽 기능을 선택합니다.

- 방화벽에서 나가는 패킷을 차단하면 방화벽 위반 알림 메시지가 표시됩니다. 메시지를 수정하려면 방화벽 알림 메시지 내용 수정 페이지 13-27을 참조하십시오.
- 관리자가 방화벽 기능을 모두 사용하도록 설정하고 OfficeScan 에이전트 사용자에게 방화벽 설정을 구성할 수 있는 권한을 부여한 경우, 해당 사용자들은 OfficeScan 에이전트 콘솔에서 방화벽 기능을 사용하거나 사용하지 않도록 설정하고 방화벽 설정을 수정할 수 있게 됩니다.

경고!

OfficeScan 웹 콘솔을 사용하여 사용자가 구성하는 OfficeScan 에이전트 콘솔 설정을 재정의할 수 없습니다.

- 기능을 사용하도록 설정하지 않은 경우에는 OfficeScan 웹 콘솔에서 구성하는 방화벽 설정이 OfficeScan 에이전트 콘솔의 **네트워크 카드 목록**에 표시됩니다.
- OfficeScan 에이전트 콘솔의 **방화벽** 탭에 있는 **설정**의 정보는 항상 OfficeScan 에이전트 콘솔에 구성된 설정을 반영하지, 서버 웹 콘솔의 설정을 반영하지 않습니다.

6. 로컬 또는 전역 인증된 안전한 소프트웨어 목록을 사용합니다.

참고

이 서비스를 사용하기 전에 무단 변경 방지 서비스 및 인증된 안전한 소프트웨어 서비스를 사용하고 있는지 확인해야 합니다.

7. 예외에서 방화벽 정책 예외를 선택합니다. 여기 표시되는 정책 예외는 방화벽 예외 템플릿에 따라 결정됩니다. 자세한 내용은 방화벽 예외 템플릿 편집 페이지 13-13를 참조하십시오.
   - 기존 정책 예외 이름을 클릭하고 열리는 페이지에서 설정을 변경하여 해당 정책 예외를 수정합니다.

참고

수정된 정책 예외는 만들 정책에만 적용됩니다. 정책 예외 수정 사항을 영구적으로 적용하려면 방화벽 예외 템플릿의 정책 예외를 동일하게 수정해야 합니다.

- **추가**를 클릭하여 새 정책 예외를 만듭니다. 열리는 페이지에서 설정을 지정합니다.

참고

또한 정책 예외는 만들 정책에만 적용됩니다. 이 정책 예외를 다른 정책에 적용하려면 먼저 방화벽 예외 템플릿의 정책 예외 목록에 추가해야 합니다.

8. **저장**을 클릭합니다.

기존 방화벽 정책 수정

절차

1. **에이전트** > **방화벽** > **정책**으로 이동합니다.
2. 정책을 클릭합니다.
3. 다음을 수정합니다.
   - 정책 이름
   - 보안 수준
   - 정책에 사용할 방화벽 기능
   - 인증된 안전한 소프트웨어 서비스 목록 상태
   - 정책에 포함할 방화벽 정책 예외
     - 기존 정책 예외 편집(정책 예외 이름을 클릭하고 열리는 페이지에서 설정 변경)
     - **추가**를 클릭하여 새 정책 예외를 만듭니다. 열리는 페이지에서 설정을 지정합니다.
4. **저장**을 클릭하여 기존 정책에 수정 사항을 적용합니다.

방화벽 예외 템플릿 편집

방화벽 예외 템플릿에는 OfficeScan 에이전트 엔드포인트의 포트 번호 및 IP 주소에 따라 다양한 종류의 네트워크 트래픽을 허용하거나 차단하도록 구성할 수 있는 정책 예외가 포함되어 있습니다. 정책 예외를 만든 후 정책 예외가 적용되는 정책을 편집합니다.

사용하려는 정책 예외 유형을 결정합니다. 다음과 같은 두 가지 유형이 있습니다.

- **제한**

  지정된 네트워크 트래픽 유형만 차단하고 모든 네트워크 트래픽을 허용하는 정책에 적용됩니다. 예를 들어 제한 정책 예외는 트로이 목마에 자주 사용되는 포트와 같이 공격에 취약한 OfficeScan 에이전트 포트를 차단하는 데 사용합니다.

- **허가**

  지정된 네트워크 트래픽 유형만 허용하고 모든 네트워크 트래픽을 차단하는 정책에 적용합니다. 예를 들어 OfficeScan 에이전트가 OfficeScan 서버 및 Web server에만 액세스하도록 허용하려면 트러스트된 포트(OfficeScan 서버와 통신하는 데 사용되는 포트) 및 OfficeScan 에이전트에서 HTTP 통신에 사용하는 포트에서 들어오는 트래픽을 허용합니다.

  OfficeScan 에이전트 수신 포트: **에이전트** > **에이전트 관리** > **상태**. 포트 번호는 **기본 정보**에 있습니다.

  서버 수신 포트: **관리** > **설정** > **에이전트 연결**. 포트 번호는 **에이전트 연결 설정**에 있습니다.

  OfficeScan에는 사용자가 수정하거나 삭제할 수 있는 기본 방화벽 정책 예외 집합이 제공됩니다.

표 13-1. 기본 방화벽 정책 예외

예외 이름	조치	프로토콜	포트	방향
DNS	허용	TCP/UDP	53	수신 및 송신
NetBIOS	허용	TCP/UDP	137, 138, 139, 445	수신 및 송신

예외 이름	조치	프로토콜	포트	방향
HTTPS	허용	TCP	443	수신 및 송신
HTTP	허용	TCP	80	수신 및 송신
Telnet	허용	TCP	23	수신 및 송신
SMTP	허용	TCP	25	수신 및 송신
FTP	허용	TCP	21	수신 및 송신
POP3	허용	TCP	110	수신 및 송신
LDAP	허용	TCP/UDP	389	수신 및 송신

참고

기본 예외는 모든 에이전트에 적용됩니다. 기본 예외가 특정 에이전트에만 적용되도록 하려면 예외를 편집하고 에이전트의 IP 주소를 지정합니다.

이전 버전의 OfficeScan에서 업그레이드하는 경우 LDAP 예외를 사용할 수 없습니다. 이 예외가 예외 목록에 표시되지 않으면 수동으로 추가합니다.

방화벽 정책 예외 추가

절차

1. **에이전트** > **방화벽** > **정책**으로 이동합니다.
2. **예외 템플릿 편집**을 클릭합니다.
3. **추가**를 클릭합니다.
4. 정책 예외의 이름을 입력합니다.
5. 응용 프로그램 유형을 선택합니다. 모든 응용 프로그램을 선택하거나 응용 프로그램 경로 또는 레지스트리 키를 지정할 수 있습니다.

참고

입력된 이름과 전체 경로를 확인합니다. 응용 프로그램 예외에는 와일드카드를 사용할 수 없습니다.

6. OfficeScan에서 네트워크 트래픽(예외 기준에 맞는 트래픽 차단 또는 허용) 및 트래픽 방향(OfficeScan 에이전트 엔드포인트의 인바운드 또는 아웃바운드 네트워크 트래픽)에 대해 수행할 조치를 선택합니다.

7. TCP, UDP, ICMP 또는 ICMPv6 중 해당 네트워크 프로토콜 유형을 선택합니다.

8. 조치를 수행할 OfficeScan 에이전트 엔드포인트의 포트를 지정합니다.

9. 예외에 포함할 OfficeScan 에이전트 엔드포인트 IP 주소를 선택합니다. 예를 들어 모든 네트워크 트래픽(인바운드 및 아웃바운드)을 거부하도록 선택하고 네트워크에 있는 단일 엔드포인트의 IP 주소를 입력하면 정책에 이 예외가 포함된 모든 OfficeScan 에이전트에서 해당 IP 주소로 데이터를 보내거나 해당 IP 주소에서 데이터를 받을 수 없게 됩니다.

    - **모든 IP 주소**: 모든 IP 주소를 포함합니다.
    - **단일 IP 주소**: IPv4 또는 IPv6 주소나 호스트 이름을 입력합니다.
    - **범위(IPv4 또는 IPv6)**: IPv4 또는 IPv6 주소 범위를 입력합니다.
    - **범위(IPv6)**: IPv6 주소 접두사 및 길이를 입력합니다.
    - **서브넷 마스크**: IPv4 주소와 해당 서브넷 마스크를 입력합니다.

10. **저장**을 클릭합니다.

방화벽 정책 예외 수정

절차

1. **에이전트** > **방화벽** > **정책**으로 이동합니다.
2. **예외 템플릿 편집**을 클릭합니다.
3. 정책 예외를 클릭합니다.
4. 다음을 수정합니다.
    - 정책 예외 이름

- 응용 프로그램 유형, 이름 또는 경로
- OfficeScan에서 네트워크 트래픽 및 트래픽 방향에 대해 수행할 조치
- 네트워크 프로토콜 유형
- 정책 예외의 포트 번호
- OfficeScan 에이전트 엔드포인트 IP 주소

5. **저장**을 클릭합니다.

정책 예외 목록 설정 저장

절차

1. **에이전트** > **방화벽** > **정책**으로 이동합니다.
2. **예외 템플릿 편집**을 클릭합니다.
3. 다음 저장 옵션 중 하나를 클릭합니다.
   - **템플릿 변경 내용 저장**: 현재 정책 예외 및 설정과 함께 예외 템플릿을 저장합니다. 이 옵션은 기존 정책을 제외하고 이후 만들어지는 정책에만 템플릿을 적용합니다.
   - **저장 후 기존 정책에 적용**: 현재 정책 예외 및 설정과 함께 예외 템플릿을 저장합니다. 이 옵션은 템플릿을 기존 정책 및 이후 정책에 적용합니다.

방화벽 프로필

방화벽 프로필을 사용하면 정책을 적용하기 전에 단일 에이전트 또는 에이전트 그룹이 갖추어야 하는 특성을 선택하는 유연성을 발휘할 수 있습니다. 특정 도메인에 대한 프로필을 만들거나 구성하거나 삭제할 수 있는 사용자 역할을 만듭니다.

기본 제공 관리자 계정을 사용하거나 모든 관리 권한이 있는 사용자는 **에이전트 보안 수준/예외 목록 덮어쓰기** 옵션을 사용하도록 설정하여 OfficeScan 에이전트 프로필 설정을 서버 설정으로 바꿀 수 있습니다.

프로필에 포함되는 내용은 다음과 같습니다.

- **관련 정책**: 각 프로필은 단일 정책을 사용합니다.
- **에이전트 특성**: 다음과 같은 특성이 하나 이상 있는 OfficeScan 에이전트에서 관련 정책을 적용합니다.
    - **IP 주소**: 특정 IP 주소, 특정 범위 이내의 IP 주소 또는 지정된 서브넷에 속하는 IP 주소를 사용하는 OfficeScan 에이전트
    - **도메인**: 특정 OfficeScan 도메인에 속하는 OfficeScan 에이전트
    - **엔드포인트**: 특정 엔드포인트 이름을 가진 OfficeScan 에이전트
    - **플랫폼**: 특정 플랫폼을 실행하는 OfficeScan 에이전트
    - **로그온 이름**: 지정된 사용자가 로그온한 OfficeScan 에이전트 엔드포인트
    - **NIC 설명**: NIC 설명이 일치하는 OfficeScan 에이전트 엔드포인트
    - **에이전트 연결 상태**: OfficeScan 에이전트가 온라인인지 오프라인인지 여부

참고

OfficeScan 에이전트가 OfficeScan 서버 또는 참조 서버에 연결할 수 있으면 온라인 상태이고, 서버에 연결할 수 없으면 오프라인 상태입니다.

OfficeScan에는 "모든 액세스" 정책을 사용하는 "모든 에이전트 프로필"이라는 기본 프로필이 제공됩니다. 이 기본 프로필을 수정하거나 삭제할 수 있습니다. 또한 새 프로필을 만들 수도 있습니다. 각 프로필과 연관된 정책 및 현재 프로필 상태를 비롯하여 모든 기본 방화벽 프로필과 사용자가 만든 방화벽 프로필은 웹 콘솔의 방화벽 프로필 목록에 표시됩니다. 프로필 목록을 관리하고 모든 프로필을 OfficeScan 에이전트에 배포합니다. OfficeScan 에이전트는 모든 방화벽 프로필을 에이전트 엔드포인트에 저장합니다.

방화벽 프로필 목록 구성

절차

1. **에이전트** > **방화벽** > **프로필**로 이동합니다.
2. 기본 제공 관리자 계정을 사용하거나 모든 관리 권한이 있는 사용자는 필요한 경우 **에이전트 보안 수준/예외 목록 덮어쓰기** 옵션을 선택하여 OfficeScan 에이전트 프로필 설정을 서버 설정으로 바꿀 수 있습니다.
3. 새 프로필을 추가하려면 **추가**를 클릭합니다. 기존 프로필을 편집하려면 프로필 이름을 선택합니다.

   프로필 구성 화면이 나타납니다. 자세한 내용은 방화벽 프로필 추가 및 편집 페이지 13-19를 참조하십시오.
4. 기존 프로필을 삭제하려면 정책 옆에 있는 확인란을 선택하고 **삭제**를 클릭합니다.
5. 목록에서 프로필 순서를 변경하려면 이동할 프로필 옆에 있는 확인란을 선택한 후 **위로 이동** 또는 **아래로 이동**을 클릭합니다.

   OfficeScan에서는 프로필 목록에 표시된 순서대로 방화벽 프로필을 OfficeScan 에이전트에 적용합니다. 예를 들어 에이전트가 첫 번째 프로필과 일치하는 경우 OfficeScan은 해당 프로필에 대해 구성된 조치를 에이전트에 적용합니다. OfficeScan에서는 해당 에이전트에 대해 구성된 다른 프로필은 무시합니다.

   팁

   정책이 배타적일수록 목록 위쪽에 배치하는 것이 좋습니다. 예를 들어 단일 에이전트에 대해 만든 정책을 맨 위로 이동하고 그 다음으로 에이전트 범위에 대한 정책, 네트워크 도메인에 대한 정책, 모든 에이전트에 대한 정책순으로 배치할 수 있습니다.
6. 참조 서버를 관리하려면 **참조 서버 목록 편집**을 클릭합니다. 참조 서버는 방화벽 프로필을 적용할 때 OfficeScan 서버를 대체하는 역할을 하는 엔드포인트입니다. 네트워크에 있는 모든 엔드포인트를 참조 서버로 사용할 수 있습니다(자세한 내용은 참조 서버 페이지 14-33 참조). 참조 서버를 사용하도록 설정하는 경우 OfficeScan에서는 다음과 같이 가정합니다.

- 참조 서버에 연결된 OfficeScan 에이전트는 에이전트가 OfficeScan 서버와 통신할 수 없는 경우에도 온라인 상태입니다.
- 온라인 OfficeScan 에이전트에 적용되는 방화벽 프로필은 참조 서버에 연결된 OfficeScan 에이전트에도 적용됩니다.

참고

기본 제공 관리자 계정을 사용하거나 모든 관리 권한이 있는 사용자만 참조 서버 목록을 보고 구성할 수 있습니다.

7. 다음과 같이 현재 설정을 저장하고 프로필을 OfficeScan 에이전트에 할당합니다.
   a. **에이전트 보안 수준/예외 목록 덮어쓰기**를 설정할지 여부를 선택합니다. 이 옵션은 사용자가 구성한 모든 방화벽 설정을 덮어씁니다.
   b. **에이전트에 프로필 할당**을 클릭합니다. OfficeScan에서는 프로필 목록의 모든 프로필을 모든 OfficeScan 에이전트에 할당합니다.
8. 다음과 같이 프로필이 OfficeScan 에이전트에 할당되었는지 확인합니다.
   a. **에이전트** > **에이전트 관리**로 이동합니다. 에이전트 트리 보기 드롭다운 상자에서 **방화벽 보기**를 선택합니다.
   b. 에이전트 트리의 **방화벽** 열에 녹색 확인 표시가 있는지 확인합니다. 프로필과 관련된 정책에서 침입 탐지 시스템을 사용하면 **IDS** 열 아래에도 녹색 확인 표시가 나타납니다.
   c. 에이전트에서 올바른 방화벽 정책을 적용했는지 확인합니다. 정책은 에이전트 트리의 **방화벽 정책** 열에 나타납니다.

방화벽 프로필 추가 및 편집

OfficeScan 에이전트 엔드포인트에는 다양한 보호 수준이 필요할 수 있습니다. 방화벽 프로필을 사용하면 관련 정책이 적용되는 에이전트 엔드포인트를 지정할 수 있습니다. 일반적으로 사용 중인 정책마다 하나의 프로필이 필요합니다.

방화벽 프로필 추가

절차

1. **에이전트** > **방화벽** > **프로필**로 이동합니다.
2. **추가**를 클릭합니다.
3. **이 프로필 사용**을 클릭하여 OfficeScan에서 프로필을 OfficeScan 에이전트에 배포할 수 있도록 합니다.
4. 프로필을 식별하는 이름과 선택적 설명을 입력합니다.
5. 이 프로필에 대한 정책을 선택합니다.
6. OfficeScan에서 정책을 적용할 에이전트 엔드포인트를 지정합니다. 다음 기준에 따라 엔드포인트를 선택합니다.
   - IP 주소
   - 도메인: 단추를 클릭하여 에이전트 트리를 열고 도메인을 선택합니다.

     참고

     모든 도메인 권한을 가진 사용자만 도메인을 선택할 수 있습니다.
   - 엔드포인트 이름: 단추를 클릭하여 에이전트 트리를 열고 OfficeScan 에이전트 엔드포인트를 선택합니다.
   - 플랫폼
   - 로그온 이름
   - NIC 설명: 와일드카드 없이 전체 또는 일부 설명을 입력합니다.

     팁

     NIC 설명은 일반적으로 제조업체 이름으로 시작하므로 Trend Micro에서는 NIC 카드 제조업체를 입력할 것을 권장합니다. 예를 들어 "Intel"을 입력한 경우 Intel에서 제조한 모든 NIC가 기준을 충족합니다. 그러나 "Intel(R) Pro/100"과 같은 특정 NIC 모델을 입력한 경우 "Intel(R) Pro/100"으로 시작하는 NIC 설명만 기준을 충족합니다.

- 에이전트 연결 상태

7. 지정된 트래픽 유형을 허용하도록 구성 가능한 예외 목록을 편집하거나 방화벽 보안 수준을 변경할 수 있는 권한을 사용자에게 부여할지 선택합니다.

   자세한 내용은 방화벽 정책 페이지 13-8를 참조하십시오.

8. **저장**을 클릭합니다.

방화벽 프로필 수정

절차

1. **에이전트** > **방화벽** > **프로필**로 이동합니다.
2. 프로필을 클릭합니다.
3. **이 프로필 사용**을 클릭하여 OfficeScan에서 이 프로필을 OfficeScan 에이전트에 배포할 수 있도록 합니다. 다음을 수정합니다.
   - 프로필 이름 및 설명
   - 프로필에 할당된 정책
   - OfficeScan 에이전트 다음 기준에 따른 엔드포인트
     - IP 주소
     - 도메인: 단추를 클릭하여 에이전트 트리를 열고 도메인을 선택합니다.
     - 엔드포인트 이름: 단추를 클릭하여 에이전트 트리를 열고 에이전트 엔드포인트를 선택합니다.
     - 플랫폼
     - 로그온 이름
     - NIC 설명: 와일드카드 없이 전체 또는 일부 설명을 입력합니다.

팁

NIC 설명은 일반적으로 제조업체 이름으로 시작하므로 Trend Micro에서는 NIC 카드 제조업체를 입력할 것을 권장합니다. 예를 들어 "Intel"을 입력한 경우 Intel에서 제조한 모든 NIC가 기준을 충족합니다. 그러나 "Intel(R) Pro/100"과 같은 특정 NIC 모델을 입력한 경우 "Intel(R) Pro/100"으로 시작하는 NIC 설명만 기준을 충족합니다.

- 에이전트 연결 상태

4. **저장**을 클릭합니다.

방화벽 권한

방화벽 권한을 통해 사용자는 방화벽 설정을 구성할 수 있습니다. 모든 사용자가 구성한 설정은 OfficeScan 서버에서 배포된 설정에 의해 무시될 수 없습니다. 예를 들어 사용자가 침입 탐지 시스템(IDS)을 사용하지 않고 OfficeScan 서버에서 IDS를 사용하는 경우 IDS는 OfficeScan 에이전트 엔드포인트에서 사용되지 않는 상태로 유지됩니다.

다음 설정을 사용하여 사용자가 방화벽을 구성하도록 허용할 수 있습니다.

표 13-2. 방화벽 권한

권한	설명
OfficeScan 에이전트 콘솔에 방화벽 설정 표시	**방화벽** 옵션은 OfficeScan 에이전트에 모든 방화벽 설정을 표시합니다.

권한	설명
사용자가 방화벽, 침입 탐지 시스템 및 방화벽 위반 알림 메시지를 사용하거나 사용하지 않도록 설정할 수 있음	OfficeScan 방화벽은 상태 기반 검사, 고성능 네트워크 바이러스 검색 및 제거를 통해 네트워크의 에이전트와 서버를 보호합니다. 사용자에게 방화벽 및 해당 기능을 사용하거나 사용하지 않도록 설정할 수 있는 권한을 부여하는 경우, 침입 및 해커 공격에 엔드포인트를 노출시키지 않으려면 장시간 방화벽을 사용하지 않도록 설정하지 말라고 경고합니다. 사용자에게 이 권한을 부여하지 않은 경우에는 OfficeScan 서버 웹 콘솔에서 구성한 방화벽 설정이 OfficeScan 에이전트 콘솔의 네트워크 카드 목록에 표시됩니다.
에이전트에서 OfficeScan 서버에 방화벽 로그를 보낼 수 있음	OfficeScan 방화벽 차단 및 허용에 대한 트래픽을 분석하려면 이 옵션을 선택합니다. 방화벽 로그에 대한 자세한 내용은 방화벽 로그 페이지 13-28를 참조하십시오. 이 옵션을 선택한 경우 **보안 설정** 탭의 **에이전트** > **글로벌 에이전트 설정**에서 로그 전송 일정을 구성합니다. **방화벽 설정** 섹션으로 이동합니다. 일정은 방화벽 로그 전송 권한이 있는 에이전트에만 적용됩니다. 자세한 내용은 글로벌 방화벽 설정 페이지 13-24을 참조하십시오.

방화벽 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **방화벽 권한** 섹션으로 이동합니다.
5. 다음 옵션을 선택합니다.
   - OfficeScan 에이전트 콘솔에 방화벽 탭 표시 페이지 13-22

- 사용자가 방화벽, 침입 탐지 시스템 및 방화벽 위반 알림 메시지를 사용하거나 사용하지 않도록 설정할 수 있음 페이지 13-23
- OfficeScan 에이전트에서 OfficeScan 서버에 방화벽 로그를 보낼 수 있음 페이지 13-23

6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

글로벌 방화벽 설정

글로벌 방화벽 설정을 OfficeScan 에이전트에 적용하는 여러 가지 방법이 있습니다.

- 특정 방화벽 설정을 서버에서 관리하는 모든 에이전트에 적용할 수 있습니다.
- 특정 방화벽 권한이 있는 OfficeScan 에이전트에만 설정을 적용할 수 있습니다. 예를 들어 방화벽 로그 전송 일정은 서버에 로그를 보낼 권한이 있는 OfficeScan 에이전트에만 적용됩니다.

필요에 따라 다음 글로벌 설정을 사용합니다.

- **서버에 방화벽 로그 보내기**

  OfficeScan 서버에 방화벽 로그를 보낼 수 있는 권한을 특정 OfficeScan 에이전트에 부여할 수 있습니다. 이 섹션에서 로그 보내기 일정을 구성합니다. 방화벽 로그를 보낼 권한이 있는 에이전트만 일정을 사용합니다.

  선택한 에이전트에 사용할 수 있는 방화벽 권한에 대한 자세한 내용은 방화벽 권한 페이지 13-22을 참조하십시오.

- **시스템 재부팅 후 OfficeScan 방화벽 드라이버만 업데이트**

  OfficeScan 에이전트 엔드포인트를 다시 시작한 후에만 OfficeScan 에이전트가 방화벽 드라이버를 업데이트할 수 있습니다. 에이전트 업그레이드 중 방화벽 드라이버를 업데이트할 때 에이전트 엔드포인트가 중단(예: 일시적으로 네트워크 연결이 끊김)될 수 있는 문제를 방지하려면 이 옵션을 사용하도록 설정합니다.

- **방화벽 비상 발생 가능성을 확인하기 위해 OfficeScan 서버에 방화벽 로그 정보를 매시간 보냅니다.**

  이 옵션을 사용하도록 설정하면 OfficeScan 에이전트가 방화벽 로그 수를 한 시간에 한 번씩 OfficeScan 서버에 보냅니다. 방화벽 로그에 대한 자세한 내용은 방화벽 로그 페이지 13-28를 참조하십시오.

  OfficeScan에서는 로그 수 및 방화벽 위반 비상 발생 기준을 사용하여 방화벽 위반 비상 발생 가능성을 확인합니다. 비상 발생 시 OfficeScan에서는 OfficeScan 관리자에게 전자 메일 알림을 보냅니다.

- **인증된 안전한 소프트웨어 서비스 설정** 섹션으로 이동하고 필요한 경우 인증된 안전한 소프트웨어 서비스를 사용하도록 설정합니다.

  인증된 안전한 소프트웨어 서비스에서는 Trend Micro 데이터 센터를 쿼리하여 악성 프로그램 동작 차단, 이벤트 모니터링, 방화벽 또는 바이러스 백신 검색을 통해 탐지된 프로그램의 안전성을 확인합니다. 인증된 안전한 소프트웨어 서비스를 사용하도록 설정하면 잘못된 판정이 탐지될 가능성이 줄어듭니다.

참고

인증된 안전한 소프트웨어 서비스를 사용도록 설정하기 전에 OfficeScan 에이전트 프록시 설정이 올바른지 확인해야 합니다(자세한 내용은 OfficeScan 에이전트 프록시 설정 페이지 15-47 참조). 잘못된 프록시 설정은 일시적인 인터넷 연결 끊김과 함께 Trend Micro 데이터 센터의 응답을 지연시키거나 수신되지 않도록 하여 모니터링 대상 프로그램이 응답하지 않는 것처럼 보이게 합니다.

또한 순수 IPv6 OfficeScan 에이전트는 Trend Micro 데이터 센터에서 직접 쿼리할 수 없습니다. OfficeScan 에이전트에서 Trend Micro 데이터 센터에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

글로벌 방화벽 설정 구성

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **보안 설정** 탭에서 **방화벽 설정** 섹션으로 이동하고 다음을 구성합니다.
   - 서버에 방화벽 로그 보내기 페이지 13-24
   - 시스템 재부팅 후 OfficeScan 방화벽 드라이버만 업데이트 페이지 13-25
   - 방화벽 비상 발생 가능성을 확인하기 위해 OfficeScan 서버에 방화벽 로그 정보를 매시간 보냅니다. 페이지 13-25
3. **시스템** 탭에서 **인증된 안전한 소프트웨어 설정** 섹션으로 이동하고 다음을 구성합니다.
   - 동작 모니터링, 방화벽 및 바이러스 백신 검색에 대해 인증된 안전한 소프트웨어 서비스 사용 페이지 13-25
4. **저장**을 클릭합니다.

OfficeScan 에이전트 사용자에 대한 방화벽 위반 알림

OfficeScan은 OfficeScan 방화벽에서 방화벽 정책을 위반한 아웃바운드 트래픽을 차단한 후에 바로 엔드포인트에 알림 메시지를 표시할 수 있습니다. 사용자에게 알림 메시지 사용 여부를 설정할 권한을 부여합니다.

참고

특정 방화벽 정책을 구성할 때 알림을 사용하도록 설정할 수도 있습니다. 방화벽 정책을 구성하려면 방화벽 정책 추가 페이지 13-10을 참조하십시오.

사용자에게 알림 메시지 사용 여부를 설정할 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **방화벽 권한** 섹션으로 이동합니다.
5. **사용자가 방화벽, 침입 탐지 시스템 및 방화벽 위반 알림 메시지를 사용하거나 사용하지 않도록 설정할 수 있음**을 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

방화벽 알림 메시지 내용 수정

절차

1. **관리** > **알림** > **에이전트**으로 이동합니다.
2. **유형** 드롭다운에서 **방화벽 위반**을 선택합니다.
3. 제공된 텍스트 상자에서 기본 메시지를 수정합니다.
4. **저장**을 클릭합니다.

방화벽 로그

서버에서 사용 가능한 방화벽 로그는 방화벽 로그를 보낼 권한이 있는 OfficeScan 에이전트가 보냅니다. OfficeScan 방화벽에서 차단하는 엔드포인트의 트래픽을 모니터링하고 분석하려면 특정 에이전트에 이 권한을 부여합니다.

방화벽 권한에 대한 자세한 내용은 방화벽 권한 페이지 13-22을 참조하십시오.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

방화벽 로그 보기

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **로그** > **방화벽 로그** 또는 **로그 보기** > **방화벽 로그**를 클릭합니다.
4. 가장 최신 로그를 사용할 수 있는지 확인하려면 **에이전트에 알림**을 클릭합니다. 일정 시간 동안 에이전트가 방화벽 로그를 전송하도록 한 이후에 다음 단계로 진행합니다.
5. 로그 기준을 지정하고 **로그 표시**를 클릭합니다.
6. 로그를 표시합니다. 로그에는 다음 정보가 포함됩니다.
   - 방화벽 위반 발견 날짜 및 시간
   - 방화벽 위반이 발생한 엔드포인트
   - 방화벽 위반이 발생한 엔드포인트 도메인
   - 원격 호스트 IP 주소

- 로컬 호스트 IP 주소
- 프로토콜
- 포트 번호
- 방향: 인바운드(수신) 또는 아웃바운드(송신) 트래픽이 방화벽 정책을 위반한 경우
- 프로세스: 방화벽 위반을 발생시킨 엔드포인트에서 실행 중인 실행 프로그램 또는 서비스
- 설명: 실제 보안 위험(네트워크 바이러스 또는 IDS 공격 등) 또는 방화벽 정책 위반을 지정합니다.

7. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

방화벽 위반 비상 발생

방화벽 위반 횟수 및 탐지 기간에 따라 방화벽 위반 비상 발생을 정의합니다.

OfficeScan에서는 사용자 자신과 다른 OfficeScan 관리자에게 비상 발생을 알리는 기본 알림 메시지를 제공합니다. 요구 사항에 맞게 알림 메시지를 수정할 수 있습니다.

참고

OfficeScan에서는 전자 메일을 통해 방화벽 비상 발생 알림을 보낼 수 있습니다. OfficeScan에서 전자 메일을 보낼 수 있도록 전자 메일 설정을 구성하십시오. 자세한 내용은 관리자 알림 설정 페이지 14-35를 참조하십시오.

방화벽 위반 비상 발생 기준 및 알림 구성

절차

1. **관리** > **알림** > **비상 발생**으로 이동합니다.

2. **기준** 탭에서 다음을 수행합니다.

   a. **방화벽 위반** 섹션으로 이동합니다.

   b. **OfficeScan 에이전트에서 방화벽 위반 모니터링**을 선택합니다.

   c. IDS 로그, 방화벽 로그 및 네트워크 바이러스 로그 수를 지정합니다.

   d. 탐지 기간을 지정합니다.

팁

Trend Micro에서는 이 화면에서 기본값을 적용할 것을 권장합니다.

로그 수가 초과되면 OfficeScan에서 알림 메시지를 보냅니다. 예를 들어 IDS 로그, 방화벽 로그 및 네트워크 바이러스 로그 수를 각각 100개로 지정하고 기간을 3시간으로 지정한 경우 서버에서 3시간 이내에 301개의 로그를 받으면 OfficeScan에서 알림을 보냅니다.

3. **전자 메일** 탭에서 다음을 수행합니다.

   a. **방화벽 위반 비상 발생** 섹션으로 이동합니다.

   b. **전자 메일을 통한 알림 사용**을 선택합니다.

   c. 전자 메일 받는 사람을 지정합니다.

   d. 기본 전자 메일 제목 및 메시지를 적용하거나 수정합니다. **제목** 및 **메시지** 필드에서 토큰 변수를 사용하여 데이터를 표시할 수 있습니다.

표 13-3. 방화벽 위반 비상 발생 알림용 토큰 변수

변수	설명
%A	초과한 로그 형식
%C	방화벽 위반 로그 수
%T	방화벽 위반 로그가 누적된 시간

4. **저장**을 클릭합니다.

OfficeScan 방화벽 테스트

OfficeScan 방화벽이 제대로 작동하는지 확인하려면 단일 OfficeScan 에이전트 또는 OfficeScan 에이전트 그룹에 대해 테스트를 수행합니다.

경고!

통제된 환경에서만 OfficeScan 에이전트 프로그램 설정을 테스트하십시오. 네트워크 또는 인터넷에 연결되어 있는 엔드포인트에서는 테스트를 수행하지 마십시오. 그럴 경우 OfficeScan 에이전트 엔드포인트가 바이러스, 해커 공격 및 기타 위험에 노출될 수 있습니다.

절차

1. 테스트 정책을 만들어 저장합니다. 테스트할 트래픽 유형을 차단하도록 설정을 구성합니다. 예를 들어 OfficeScan 에이전트가 인터넷에 액세스하지 않도록 하려면 다음을 수행합니다.
   a. 보안 수준을 **낮음**으로 설정합니다(모든 인바운드/아웃바운드 트래픽 허용).
   b. **방화벽 사용 및 방화벽 위반이 발생하면 사용자에게 알림**을 선택합니다.
   c. HTTP(또는 HTTPS) 트래픽을 차단하는 예외를 만듭니다.
2. 테스트 프로필을 만들어 저장하고 방화벽 기능을 테스트할 에이전트를 선택합니다. 테스트 프로필을 테스트 정책에 연결합니다.
3. **에이전트에 프로필 할당**을 클릭합니다.
4. 배포를 확인합니다.
   a. **에이전트** > **에이전트 관리**를 클릭합니다.
   b. 에이전트가 속한 도메인을 선택합니다.
   c. 에이전트 트리 보기에서 **방화벽 보기**를 선택합니다.
   d. 에이전트 트리의 **방화벽** 열에 녹색 확인 표시가 있는지 확인합니다. 해당 에이전트에 대해 침입 탐지 시스템을 사용하도록 설정한 경우 **IDS** 열에도 녹색 확인 표시가 있는지 확인합니다.

e. 에이전트에서 올바른 방화벽 정책을 적용했는지 확인합니다. 정책은 에이전트 트리의 **방화벽 정책** 열에 나타납니다.

5. 정책에서 구성한 트래픽 유형 보내기/받기를 시도하여 에이전트 엔드포인트에서 방화벽을 테스트합니다.

6. 에이전트의 인터넷 액세스를 금지하도록 구성된 정책을 테스트하려면 에이전트 엔드포인트에서 웹 브라우저를 엽니다. 방화벽 위반에 대한 알림 메시지를 표시하도록 OfficeScan을 구성한 경우, 아웃바운드 트래픽 위반이 발생하면 에이전트 엔드포인트에 메시지가 표시됩니다.

부 III

OfficeScan 서버 및 에이전트 관리

장 14

OfficeScan 서버 관리

이 장에서는 OfficeScan 서버 관리 및 구성에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- 역할 기반 관리 페이지 14-3
- Trend Micro Control Manager 페이지 14-23
- 의심스러운 개체 목록 설정 페이지 14-31
- 참조 서버 페이지 14-33
- 관리자 알림 설정 페이지 14-35
- 시스템 이벤트 로그 페이지 14-37
- 로그 관리 페이지 14-39
- 라이선스 페이지 14-42
- OfficeScan 데이터베이스 백업 페이지 14-45
- SQL Server 마이그레이션 도구 페이지 14-47
- OfficeScan Web Server/에이전트 연결 설정 페이지 14-52
- 서버-에이전트 통신 페이지 14-52

- 웹 콘솔 암호 페이지 14-58
- 웹 콘솔 설정 페이지 14-58
- 격리 보관 관리자 페이지 14-59
- 서버 튜너 페이지 14-60
- Smart Feedback 페이지 14-63

역할 기반 관리

역할 기반 관리를 사용하여 OfficeScan 웹 콘솔에 대한 액세스 권한을 부여하고 제어할 수 있습니다. 조직의 OfficeScan 관리자가 여러 명인 경우 이 기능을 사용하여 관리자에게 특정 웹 콘솔 권한을 할당하고 특정 작업을 수행하는 데 필요한 도구 및 권한만 제공할 수 있습니다. 또한 관리할 도메인을 하나 이상 할당하여 에이전트 트리에 대한 액세스를 제어할 수 있습니다. 관리자가 아닌 사용자에게 웹 콘솔에 대한 "보기 전용" 권한을 부여할 수도 있습니다.

각 사용자(관리자 또는 관리자가 아닌 사용자)에게는 특정 역할이 할당됩니다. 역할은 웹 콘솔에 대한 액세스 수준을 정의합니다. 사용자는 사용자 지정 사용자 계정 또는 Active Directory 계정을 사용하여 웹 콘솔에 로그온합니다.

역할 기반 관리 작업은 다음과 같습니다.

1. 사용자 역할을 정의합니다. 자세한 내용은 사용자 역할 페이지 14-3을 참조하십시오.
2. 사용자 계정을 구성하고 특정 역할을 각 사용자 계정에 할당합니다. 자세한 내용은 사용자 계정 페이지 14-13을 참조하십시오.

시스템 이벤트 로그에서 모든 사용자에 대한 웹 콘솔 작업을 확인합니다. 다음 작업이 기록됩니다.

- 콘솔에 로그온
- 암호 수정
- 콘솔에서 로그오프
- 세션 타임아웃(사용자가 자동으로 로그오프됨)

사용자 역할

사용자 역할에 따라 사용자가 액세스할 수 있는 웹 콘솔 메뉴 항목이 결정됩니다. 역할마다 각 메뉴 항목에 대한 권한이 할당됩니다.

다음에 대한 권한이 할당됩니다.

- 메뉴 항목 권한 페이지 14-4

- 메뉴 항목 유형 페이지 14-4
- 서버 및 에이전트에 대한 메뉴 항목 페이지 14-4
- 관리되는 도메인의 메뉴 항목 페이지 14-7

메뉴 항목 권한

권한에 따라 각 메뉴 항목에 대한 액세스 수준이 결정됩니다. 메뉴 항목에 대한 권한은 다음 중 하나일 수 있습니다.

- **구성**: 메뉴 항목에 대한 전체 액세스가 허용됩니다. 사용자는 메뉴 항목의 데이터를 보고, 모든 설정을 구성하고, 모든 작업을 수행할 수 있습니다.
- **보기**: 사용자는 메뉴 항목의 설정, 작업 및 데이터를 볼 수만 있습니다.
- **액세스 권한 없음**: 메뉴 항목이 보기에서 숨겨집니다.

메뉴 항목 유형

OfficeScan 사용자 역할에는 구성할 수 있는 두 가지 유형의 메뉴 항목이 있습니다.

표 14-1. 메뉴 항목 유형

유형	범위
서버/에이전트의 메뉴 항목	• 서버 설정, 작업 및 데이터 • 글로벌 에이전트 설정, 작업 및 데이터 사용 가능한 메뉴 항목의 전체 목록은 서버 및 에이전트에 대한 메뉴 항목 페이지 14-4을 참조하십시오.
관리되는 도메인의 메뉴 항목	에이전트 트리 외부에서 사용할 수 있는 개별 에이전트 설정, 작업 및 데이터 사용 가능한 메뉴 항목의 전체 목록은 관리되는 도메인의 메뉴 항목 페이지 14-7을 참조하십시오.

서버 및 에이전트에 대한 메뉴 항목

다음 표에는 서버/에이전트에 사용 가능한 메뉴 항목이 나와 있습니다.

참고

메뉴 항목은 관련 플러그인 프로그램을 활성화한 후에만 표시됩니다. 예를 들어 데이터 손실 방지 모듈을 활성화하지 않은 경우 데이터 손실 방지 메뉴 항목이 목록에 표시되지 않습니다. 추가 Plug-in 프로그램은 항목은 플러그인 메뉴 항목 아래에 표시됩니다.

"관리자(기본 제공)" 역할이 할당된 사용자만 플러그인 메뉴 항목에 액세스할 수 있습니다.

표 14-2. 에이전트 메뉴 항목

최상위 메뉴 항목	메뉴 항목
에이전트	• 에이전트 관리 • 에이전트 그룹화 • 글로벌 에이전트 설정 • 엔드포인트 위치 • 데이터 손실 방지 • 연결 확인 • 바이러스 사전 방역

표 14-3. 로그 메뉴 항목

최상위 메뉴 항목	메뉴 항목

로그	• 에이전트
	  • 보안 위험
	  • 에이전트 구성 요소 업데이트
	• 서버 업데이트
	• 시스템 이벤트
	• 로그 유지 관리

표 14-4. 업데이트 메뉴 항목

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
업데이트	서버	• 예약 업데이트 • 수동 업데이트 • 업데이트 소스
	에이전트	• 자동 업데이트 • 업데이트 소스
	롤백	해당 없음

표 14-5. 관리 메뉴 항목

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
관리	계정 관리	• 사용자 계정 • 사용자 역할 **참고** 기본 제공 관리자 계정을 사용하는 사용자만 사용자 계정 및 사용자 역할에 액세스할 수 있습니다.
	스마트 보호	• 스마트 보호 소스 • 통합 서버 • Smart Feedback
	Active Directory	• Active Directory 통합 • 예약 동기화
	알림	• 일반 설정 • 비상 발생 • 에이전트

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
	설정	• 프록시 • 에이전트 연결 • 비활성 에이전트 • 격리 보관 관리자 • 제품 라이선스 • Control Manager • 웹 콘솔 • 데이터베이스 백업 • 의심스러운 개체 목록 • Edge 릴레이

관리되는 도메인의 메뉴 항목

다음 표에는 관리되는 도메인에 대해 사용 가능한 메뉴 항목이 나와 있습니다.

표 14-6. 대시보드 메뉴 항목

기본 메뉴 항목	메뉴 항목
대시보드 **참고** 모든 사용자가 권한에 관계없이 이 페이지에 액세스할 수 있습니다.	해당 없음

표 14-7. 점검 메뉴 항목

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
점검	보안 준수	• 수동 보고서 • 예약 보고서
	관리되지 않는 엔드포인트	해당 없음

표 14-8. 에이전트 메뉴 항목

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
에이전트	방화벽	• 정책 • 프로필
	에이전트 설치	• 브라우저 기반 • 원격

표 14-9. 로그 메뉴 항목

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
로그	에이전트	• 연결 확인 • 중앙 격리 보관 복원 • 스파이웨어/그레이웨어 복원

표 14-10. 업데이트 메뉴 항목

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
업데이트	요약	해당 없음
	에이전트	수동 업데이트

표 14-11. 관리 메뉴 항목

최상위 메뉴 항목	메뉴 항목	하위 메뉴 항목
관리	알림	관리자

기본 제공 사용자 역할

OfficeScan에는 사용자가 수정하거나 삭제할 수 없는 기본 제공 사용자 역할 집합이 제공됩니다. 기본 제공 역할은 다음과 같습니다.

표 14-12. 기본 제공 사용자 역할

역할 이름	설명
관리자	다른 OfficeScan 관리자나 OfficeScan을 잘 알고 있는 사용자에게 이 역할을 위임합니다. 이 역할의 사용자에게는 모든 메뉴 항목에 대한 "구성" 권한이 부여됩니다. **참고** "관리자(기본 제공)" 역할이 할당된 사용자만 플러그인 메뉴 항목에 액세스할 수 있습니다.

게스트 사용자	참조하기 위해 웹 콘솔을 보려는 사용자에게 이 역할을 위임합니다.
	• 이 역할의 사용자는 다음 메뉴 항목에 대한 액세스 권한이 없습니다.
	  • 플러그인
	  • **관리** > **계정 관리** > **사용자 역할**
	  • **관리** > **계정 관리** > **사용자 계정**
	• 사용자에게 다른 모든 메뉴 항목에 대한 "보기" 권한이 부여됩니다.

역할 이름	설명
Trend 고급 사용자 (업그레이드 전용 역할)	이 역할은 OfficeScan 10에서 업그레이드한 경우에만 제공됩니다. 이 역할은 OfficeScan 10의 "고급 사용자" 역할의 권한을 상속합니다. 이 역할의 사용자에게는 모든 에이전트 트리 도메인에 대한 "구성" 권한이 부여되지만 이 릴리스의 새로운 기능에 대한 액세스 권한은 부여되지 않습니다.

사용자 지정 역할

기본 제공 역할이 요구 사항을 충족하지 않는 경우 사용자 지정 역할을 만들 수 있습니다.

기본 제공 관리자 역할이 있는 사용자와 OfficeScan 설치 중에 만든 루트 계정을 사용하는 사용자만 사용자 지정 사용자 역할을 만들고 이러한 역할을 사용자 계정에 할당할 수 있습니다.

사용자 지정 역할 추가

절차

1. **관리** > **계정 관리** > **사용자 역할**로 이동합니다.
2. **추가**를 클릭합니다. 만들려는 역할에 기존 역할과 유사한 설정이 있는 경우 기존 역할을 선택하고 **복사**를 클릭합니다.

   새 화면이 나타납니다.
3. 역할 이름을 입력하고, 선택적으로 설명을 입력합니다.
4. **서버/에이전트의 메뉴 항목**을 클릭하고 사용 가능한 각 메뉴 항목에 대한 권한을 지정합니다. 사용 가능한 메뉴 항목 목록은 서버 및 에이전트에 대한 메뉴 항목 페이지 14-4을 참조하십시오.
5. **관리되는 도메인의 메뉴 항목**을 클릭하고 사용 가능한 각 메뉴 항목에 대한 권한을 지정합니다. 사용 가능한 메뉴 항목 목록은 관리되는 도메인의 메뉴 항목 페이지 14-7을 참조하십시오.

6. **저장**을 클릭합니다.

   새 역할은 사용자 역할 목록에 표시됩니다.

사용자 지정 역할 수정

절차

1. **관리** > **계정 관리** > **사용자 역할**로 이동합니다.
2. 역할 이름을 클릭합니다.

   새 화면이 나타납니다.
3. 다음을 수정합니다.
   - 설명
   - 역할 권한
     - **서버/에이전트의 메뉴 항목**
     - **관리되는 도메인의 메뉴 항목**
4. **저장**을 클릭합니다.

사용자 지정 역할 삭제

절차

1. **관리** > **계정 관리** > **사용자 역할**로 이동합니다.
2. 역할 옆에 있는 확인란을 선택합니다.
3. **삭제**를 클릭합니다.

참고

하나 이상의 사용자 계정에 할당된 역할은 삭제할 수 없습니다.

사용자 지정 역할 가져오기 또는 내보내기

절차

1. **관리** > **계정 관리** > **사용자 역할**로 이동합니다.
2. 사용자 지정 역할을 .dat 파일로 내보내려면
   a. 역할을 선택하고 **내보내기**를 클릭합니다.
   b. .dat 파일을 저장합니다. 다른 OfficeScan 서버를 관리하는 경우 .dat 파일을 사용하여 사용자 지정 역할을 해당 서버로 가져옵니다.

   참고

   버전이 같은 서버 간에만 역할을 내보낼 수 있습니다.
3. 사용자 지정 역할을 .csv 파일로 내보내려면
   a. 역할을 선택하고 **역할 설정 내보내기**를 클릭합니다.
   b. .csv 파일을 저장합니다. 이 파일을 사용하여 선택한 역할에 대한 정보 및 권한을 확인합니다.
4. 다른 OfficeScan 서버에서 저장한 사용자 지정 역할을 현재 OfficeScan 서버로 가져오려면 **가져오기**를 클릭하고 사용자 지정 역할이 들어 있는 .dat 파일을 찾습니다.
   - 이름이 같은 역할을 가져오는 경우 사용자 역할 화면의 역할을 덮어쓰게 됩니다.
   - 버전이 같은 서버 간에만 역할을 가져올 수 있습니다.
   - 다른 OfficeScan 서버에서 가져온 역할:
     - 서버/에이전트의 메뉴 항목 및 관리되는 도메인의 메뉴 항목에 대한 권한을 그대로 유지합니다.

- 에이전트 관리 메뉴 항목에 대한 기본 권한을 적용합니다. 다른 서버에서 해당 역할의 에이전트 관리 메뉴 항목에 대한 권한을 기록한 다음 가져온 역할에 다시 적용합니다.

사용자 계정

사용자 계정을 설정하고 특정 역할을 각 사용자에게 할당합니다. 사용자 역할에 따라 사용자가 보거나 구성할 수 있는 웹 콘솔 메뉴 항목이 결정됩니다.

OfficeScan 서버 설치 중에 설치 프로그램이 "root"라고 하는 기본 계정을 자동으로 만듭니다. 루트 계정을 사용하여 로그온한 사용자는 모든 메뉴 항목에 액세스할 수 있습니다. 루트 계정은 삭제할 수 없지만, 암호 및 전체 이름 또는 계정 설명과 같은 계정 세부 정보를 수정할 수는 있습니다. 루트 계정 암호를 잊어버린 경우에는 지원 센터에 연락하여 암호 초기화에 대한 도움을 얻으십시오.

사용자 지정 계정 또는 Active Directory 계정을 추가합니다. 모든 사용자 계정은 웹 콘솔의 사용자 계정 목록에 표시됩니다.

에이전트 트리에서 사용할 수 있는 개별 에이전트 설정, 작업 및 데이터를 보거나 구성할 수 있는 권한을 사용자 계정에 할당합니다. 사용 가능한 에이전트 트리 메뉴 항목의 전체 목록은 에이전트 관리 메뉴 항목 페이지 14-13을 참조하십시오.

참고

OfficeScan 서버를 업그레이드한 후에는 사용자 정의 계정을 편집하여 이전에 추가된 사용자 정의 계정에 대한 **3단계 에이전트 트리 메뉴 정의** 화면에서 모든 새 기능을 사용하도록 설정해야 합니다. 권한에 대한 자세한 내용은 도메인에 대한 권한 정의 페이지 14-18을 참조하십시오.

OfficeScan 사용자 계정을 사용하여 "Single Sign-On"을 수행할 수 있습니다. Single Sign-On을 통해 사용자는 Trend Micro Control Manager 콘솔에서 OfficeScan 웹 콘솔에 액세스할 수 있습니다. 자세한 내용은 다음 절차를 참조하십시오.

에이전트 관리 메뉴 항목

다음 표에는 사용 가능한 에이전트 관리 메뉴 항목이 나와 있습니다.

참고

메뉴 항목은 관련 플러그인 프로그램을 활성화한 후에만 표시됩니다. 예를 들어 데이터 손실 방지 모듈을 활성화하지 않은 경우 데이터 손실 방지 메뉴 항목이 목록에 표시되지 않습니다.

표 14-13. 에이전트 관리 메뉴 항목

기본 메뉴 항목	하위 메뉴
상태	해당 없음
작업	• 지금 검색 • 에이전트 제거 • 중앙 격리 보관 복원 • 스파이웨어/그레이웨어 복원

기본 메뉴 항목	하위 메뉴

설정	• 검색 설정
	  • 검색 방법
	  • 수동 검색 설정
	  • 실시간 검색 설정
	  • 예약 검색 설정
	  • 지금 검색 설정
	• 웹 검증 설정
	• 의심스러운 연결 설정
	• 동작 모니터링 설정
	• 장치 제어 설정
	• DLP 설정
	• 샘플 제출
	• 업데이트 에이전트 설정
	• 권한 및 기타 설정
	• 추가 서비스 설정
	• 스파이웨어/그레이웨어 승인된 목록
	• 신뢰할 수 있는 프로그램 목록
	• 머신러닝 설정
	• 설정 내보내기
	• 설정 가져오기

기본 메뉴 항목	하위 메뉴
로그	• 바이러스/악성 프로그램 로그 • 스파이웨어/그레이웨어 로그 • 방화벽 로그 • 웹 검증 로그 • 의심스러운 연결 로그 • 의심스러운 파일 로그 • C&C 콜백 로그 • 동작 모니터링 로그 • 머신러닝 로그 • 장치 제어 로그 • 데이터 손실 방지 로그 • 검색 작업 로그 • 로그 삭제
에이전트 트리 관리	• 도메인 추가 • 도메인 이름 변경 • 에이전트 이동 • 도메인/에이전트 제거
내보내기	해당 없음

사용자 지정 계정 추가

절차

1. **관리** > **계정 관리** > **사용자 계정**으로 이동합니다.
2. **추가**를 클릭합니다.

   1단계 사용자 정보 화면이 나타납니다.

3. **이 계정 사용**을 선택합니다.
4. **역할 선택** 드롭다운에서 이전에 구성한 역할을 선택합니다.

   사용자 역할을 만드는 방법에 대한 자세한 내용은 사용자 지정 역할 페이지 14-10을 참조하십시오.
5. 사용자 이름, 설명 및 암호를 입력한 다음 암호를 확인합니다.

   중요

   사용자 이름을 계정 암호로 사용할 수 없습니다. 사용자 이름이 아닌 암호를 입력하십시오.
6. 계정에 대한 전자 메일 주소를 입력합니다.

   참고

   OfficeScan에서는 이 전자 메일 주소로 알림을 보냅니다. 보안 위험 탐지 및 디지털 자산 전송에 대한 알림에 제공됩니다. 알림에 대한 자세한 내용은 관리자를 위한 보안 위험 알림 페이지 7-79을 참조하십시오.
7. **다음**을 클릭합니다.

   2단계 에이전트 도메인 제어 화면이 나타납니다.
8. 에이전트 트리에서 루트 도메인이나 도메인 하나 이상을 선택하여 에이전트 트리 범위를 정의합니다.

   지금은 도메인만 정의되었습니다. 선택한 도메인에 대한 액세스 수준은 10단계에서 정의합니다.
9. **다음**을 클릭합니다.

   3단계 에이전트 트리 메뉴 정의 화면이 나타납니다.
10. **사용 가능한 메뉴 항목** 컨트롤을 클릭하고 사용 가능한 각 메뉴 항목에 대한 권한을 지정합니다. 사용 가능한 메뉴 항목 목록은 에이전트 관리 메뉴 항목 페이지 14-13을 참조하십시오.

    8단계에서 구성한 에이전트 트리 범위에 따라 메뉴 항목에 대한 권한 수준이 결정되고 권한의 대상이 정의됩니다. 에이전트 트리 범위는 루트 도메인(모든 에이전트) 또는 특정 에이전트 트리 도메인일 수 있습니다.

표 14-14. 에이전트 관리 메뉴 항목 및 에이전트 트리 범위

기준	에이전트 트리 범위	
	루트 도메인	특정 도메인
메뉴 항목 권한	구성, 보기 또는 액세스 권한 없음	구성, 보기 또는 액세스 권한 없음
대상	루트 도메인(모든 에이전트) 또는 특정 도메인 예를 들어 역할에 에이전트 트리의 "작업" 메뉴 항목에 대한 "구성" 권한을 부여할 수 있습니다. 대상이 루트 도메인인 경우 사용자는 모든 에이전트에서 작업을 시작할 수 있습니다. 대상이 도메인 A 및 B인 경우 도메인 A 및 B의 에이전트에서만 작업을 시작할 수 있습니다.	선택한 도메인만 예를 들어 역할에 에이전트 트리의 "설정" 메뉴 항목에 대한 "구성" 권한을 부여할 수 있습니다. 이 경우 사용자는 선택한 도메인의 에이전트에만 설정을 배포할 수 있습니다.
	에이전트 트리는 "서버/에이전트의 메뉴 항목"에서 에이전트 관리 메뉴 항목에 대한 권한이 "보기"인 경우에만 표시됩니다.	

- **구성** 아래에 있는 확인란을 선택하면 **보기** 아래에 있는 확인란이 자동으로 선택됩니다.
- 아무 확인란도 선택하지 않으면 "액세스 권한 없음" 권한이 부여됩니다.
- 특정 도메인에 대한 권한을 구성하는 중에 **선택한 도메인 설정을 다른 도메인에 복사**를 클릭하여 다른 도메인에 권한을 복사할 수 있습니다.

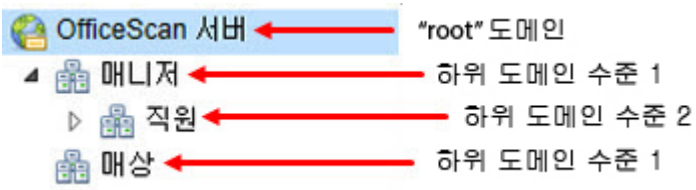
11. **마침**을 클릭합니다.
12. 사용자에게 계정 세부 정보를 보냅니다.

도메인에 대한 권한 정의

도메인에 대한 권한을 정의하는 경우 OfficeScan에서는 상위 도메인에 대한 권한을 해당 상위 도메인이 관리하는 모든 하위 도메인에 자동으로 적용합니다. 해당 상위 도메인보다 낮은 권한을 하위 도메인에 부여할 수는 없습니다. 예를

들어 OfficeScan이 관리하는 모든 에이전트("OfficeScan 서버" 도메인)를 보고 구성할 수 있는 권한을 가진 시스템 관리자는 하위 도메인에 대한 권한을 사용하여 이러한 구성 기능에 액세스할 수 있어야 합니다. 하위 도메인에서 권한을 제거하면 시스템 관리자는 모든 에이전트에 대한 전체 구성 권한을 잃어버리게 됩니다.

다음 절차의 경우 도메인 트리는 아래와 같습니다.



예를 들어 사용자 계정 "Chris"에게 하위 도메인 "직원"에 대한 특정 메뉴 항목을 보고 구성할 수 있는 권한을 부여하되 상위 도메인 "관리자"에서는 로그를 볼 수만 있는 권한을 부여하려면 다음 절차를 수행하십시오.

표 14-15. 사용자 계정 "Chris"에 대한 권한

도메인	필요한 권한
OfficeScan 서버	특별 권한 없음
관리자	**로그** 보기
직원	**작업** 보기 및 구성 **로그** 보기 및 구성 **설정** 보기
제품 구매	특별 권한 없음

절차

1. **사용자 계정: 3단계 에이전트 트리 메뉴 정의** 화면으로 이동합니다.
2. "OfficeScan 서버" 도메인을 클릭합니다.

3. 모든 **보기** 및 **구성** 확인란의 선택을 취소합니다.

   참고

   사용자 계정: 2단계 에이전트 도메인 제어 화면에서 모든 해당 하위 도메인을 선택한 경우에만 "OfficeScan 서버"도메인을 구성할 수 있습니다.

4. "구매" 도메인을 클릭합니다.

5. 모든 **보기** 및 **구성** 확인란의 선택을 취소합니다.

   참고

   "구매" 도메인은 **사용자 계정: 2단계 에이전트 도메인 제어**화면에서 선택한 경우에만 표시됩니다.

6. "관리자" 도메인을 클릭합니다.

7. "로그 보기"를 선택하여 로그를 확인하고 다른 모든 **보기** 및 **구성** 확인란의 선택을 취소합니다.

8. "직원" 도메인을 클릭합니다.

9. Chris에 대해 다음 메뉴 항목을 선택합니다.

   - **작업**: 보기 및 구성
   - **로그**: 보기 및 구성
   - **설정**: 보기

   Chris는 이제 "직원" 도메인에 대해 선택한 메뉴 항목을 보고 구성할 수 있고 "관리자" 도메인에 대한 **로그**를 볼 수만 있습니다.

Chris에게 "관리자" 도메인을 보고 구성할 수 있는 권한이 있는 경우 OfficeScan에서는 "직원" 하위 도메인에도 동일한 권한을 자동으로 부여합니다. 이는 "관리자" 도메인이 모든 해당 하위 도메인을 관리하기 때문입니다.

사용자 지정 계정 수정

참고

OfficeScan 서버를 업그레이드한 후에는 사용자 정의 계정을 편집하여 이전에 추가된 사용자 정의 계정에 대한 **3단계 에이전트 트리 메뉴 정의** 화면에서 모든 새 기능을 사용하도록 설정해야 합니다. 권한에 대한 자세한 내용은 도메인에 대한 권한 정의 페이지 14-18을 참조하십시오.

절차

1. **관리** > **계정 관리** > **사용자 계정**으로 이동합니다.
2. 사용자 계정을 클릭합니다.
3. 제공된 확인란을 사용하여 계정을 사용하거나 사용하지 않도록 설정합니다.
4. 다음을 수정합니다.
   - 역할
   - 설명
   - 암호

     참고

     계정을 편집할 때 이전에 구성된 암호를 다시 입력할 수 없습니다. 이전에 구성한 암호를 사용하여 계속하려면 **암호** 필드를 수정하지 마십시오.

   - 전자 메일 주소
5. **다음**을 클릭합니다.
6. 에이전트 트리 범위를 정의합니다.
7. **다음**을 클릭합니다.
8. **사용 가능한 메뉴 항목** 컨트롤을 클릭하고 사용 가능한 각 메뉴 항목에 대한 권한을 지정합니다.

사용 가능한 메뉴 항목 목록은 에이전트 관리 메뉴 항목 페이지 14-13을 참조하십시오.

9. **마침**을 클릭합니다.
10. 사용자에게 새 계정 세부 정보를 보냅니다.

Active Directory 계정 또는 그룹 추가

절차

1. **관리** > **계정 관리** > **사용자 계정**으로 이동합니다.
2. **추가**를 클릭합니다.

   1단계 사용자 정보 화면이 나타납니다.
3. **이 계정 사용**을 선택합니다.
4. **역할 선택** 드롭다운에서 이전에 구성한 역할을 선택합니다.

   사용자 역할을 만드는 방법에 대한 자세한 내용은 사용자 지정 역할 페이지 14-10을 참조하십시오.
5. **Active Directory 사용자 또는 그룹**을 선택합니다.

   중요

   사용자 계정을 관리하려면 OfficeScan 서버가 Active Directory 도메인에 가입해야 합니다.
6. 사용자 이름 및 계정이 속한 도메인을 지정하여 계정(사용자 이름 또는 그룹)을 검색합니다.

   참고

   여러 계정을 검색하려면 (*) 문자를 사용합니다. 와일드카드 문자를 지정하지 않은 경우 전체 계정 이름을 포함합니다. 계정 이름이 완전하지 않거나 기본 그룹 "도메인 사용자"를 사용하는 경우에는 OfficeScan에서 결과를 반환하지 않습니다.

7. OfficeScan이 유효한 계정을 발견하면 계정 이름을 **사용자 및 그룹** 아래에 표시합니다. 앞으로 아이콘(>)을 클릭하여 계정을 **선택한 사용자 및 그룹**으로 이동합니다.

   Active Directory 그룹을 지정하는 경우에는 그룹에 속한 모든 구성원이 같은 역할을 갖게 됩니다. 특정 계정이 적어도 두 개 이상의 그룹에 속하지만 두 그룹의 역할이 다른 경우

   - 두 역할에 대한 권한이 병합됩니다. 사용자가 특정 설정을 구성하고 설정에 대한 권한이 충돌하는 경우, 더 높은 권한이 적용됩니다.
   - 모든 사용자 역할은 시스템 이벤트 로그에 표시됩니다. 예: "사용자 홍길동이 고급 사용자에 해당하는 권한으로 로그온했습니다".

8. **다음**을 클릭합니다.

   2단계 에이전트 도메인 제어 화면이 나타납니다.

9. 에이전트 트리 범위를 정의합니다.

10. **다음**을 클릭합니다.

    3단계 에이전트 트리 메뉴 정의 화면이 나타납니다.

11. **사용 가능한 메뉴 항목** 컨트롤을 클릭하고 사용 가능한 각 메뉴 항목에 대한 권한을 지정합니다.

    사용 가능한 메뉴 항목 목록은 에이전트 관리 메뉴 항목 페이지 14-13을 참조하십시오.

12. **마침**을 클릭합니다.

13. 사용자에게 자신의 도메인 계정과 암호를 사용하여 웹 콘솔에 로그온하도록 알립니다.

Trend Micro Control Manager

Trend Micro™ Control Manager™는 Trend Micro 제품 및 서비스를 게이트웨이, Mail Server, 파일 서버 및 기업 데스크톱 수준에서 관리하는 중앙 관리 콘솔입니다. Control Manager 웹 기반 관리 콘솔은 네트워크 전체에 걸쳐 관리되는 제품과 서비스를 중앙에서 모니터링할 수 있습니다.

Control Manager를 사용하면 시스템 관리자는 감염, 보안 위반, 바이러스 진입점 등의 활동에 대해 모니터링 및 보고할 수 있습니다. 시스템 관리자는 네트워크 전체에 걸쳐 업데이트 구성 요소를 다운로드 및 배포하여 최신 바이러스에 대해 네트워크를 일관성 있게 보호할 수 있습니다. Control Manager를 사용하면 수동 업데이트와 예약 업데이트가 가능하며, 제품을 그룹으로 또는 개별적으로 구성 및 관리하여 유연성을 높일 수 있습니다.

이 OfficeScan 릴리스에서 Control Manager 통합

이 OfficeScan 릴리스에는 Control Manager에서 OfficeScan 서버를 관리할 때 사용하는 다음 기능이 포함됩니다.

- OfficeScan 바이러스 백신, 데이터 손실 방지 및 장치 제어에 대한 정책을 생성, 관리 및 배포하고 Control Manager 콘솔에서 OfficeScan 에이전트에 직접 권한을 할당할 수 있습니다.

  다음 표에는 Control Manager 6.0 SP3 Patch 2에서 제공되는 정책 구성이 나와 있습니다.

표 14-16. OfficeScan의 Control Manager 정책 관리 유형

정책 유형	기능
OfficeScan 바이러스 백신 및 에이전트 설정	• 추가 서비스 설정 • 동작 모니터링 설정 • 장치 제어 설정 • 수동 검색 설정 • 권한 및 기타 설정 • 실시간 검색 설정 • 스파이웨어/그레이웨어 승인된 목록 • 검색 방법 • 지금 검색 설정 • 예약 검색 설정 • 의심스러운 연결 설정 • 신뢰할 수 있는 프로그램 목록 • 업데이트 에이전트 설정 • 웹 검증 설정
데이터 보호	데이터 손실 방지 정책 설정 **참고** OfficeScan 에이전트 정책에서 데이터 보호에 대한 장치 제어 권한을 관리할 수 있습니다.

- Control Manager 콘솔에서 OfficeScan 서버 간에 다음 설정을 복제할 수 있습니다.
  - 데이터 식별자 유형 페이지 11-5
  - 데이터 손실 방지 템플릿 페이지 11-19

참고

데이터 보호 라이선스가 정품 인증을 받지 않은 OfficeScan 서버에 이러한 설정을 복제하는 경우 라이선스의 정품 인증을 받아야 이 설정이 적용됩니다.

지원되는 Control Manager 버전

이 OfficeScan 버전에서는 다음과 같은 Control Manager 버전을 지원합니다.

- Control Manager 6.0 이상

OfficeScan 서버 및 OfficeScan 에이전트가 Control Manager에 보고하는 IP 주소에 대한 자세한 내용은 IP 주소가 표시되는 화면 페이지 A-6을 참조하십시오.

Control Manager 버전에 대한 최신 패치와 핵심 핫픽스를 적용하여 Control Manager가 OfficeScan을 관리할 수 있도록 합니다. 최신 패치와 핫픽스를 구하려면 지원 센터에 문의하거나 다음 Trend Micro 업데이트 센터를 방문하십시오.

http://www.trendmicro.com/download

OfficeScan을 설치한 후에 Control Manager에 등록한 다음 Control Manager 관리 콘솔에서 OfficeScan의 설정을 구성합니다. OfficeScan 서버 관리에 대한 자세한 내용은 *Control Manager 설명서*를 참조하십시오.

OfficeScan을 Control Manager에 등록

중요

OfficeScan 10.6 SP3 이전에서 OfficeScan XG 이상으로 업그레이드한 후 인증서 권한을 사용하려면 Control Manager 서버에 대한 연결을 등록 취소한 다음 연결을 다시 등록해야 합니다.

절차

1. **관리** > **설정** > **Control Manager**으로 이동합니다.
2. Control Manager에 표시되는 OfficeScan 서버의 이름인 엔터티 표시 이름을 지정합니다.

기본적으로, 엔터티 표시 이름에 서버 컴퓨터의 호스트 이름과 이 제품의 이름(예: Server01_OSCE)이 포함됩니다.

참고

Control Manager에서는 Control Manager에서 관리하는 OfficeScan 서버와 기타 제품을 "엔터티"라고 합니다.

3. 이 서버에 연결할 때 사용할 Control Manager 서버 FQDN 또는 IP 주소와 포트 번호를 지정합니다. 선택적으로 HTTPS를 사용하여 연결 보안을 강화할 수도 있습니다.
   - 이중 스택 OfficeScan 서버의 경우 Control Manager FQDN 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
   - 순수 IPv4 OfficeScan 서버의 경우 Control Manager FQDN 또는 IPv4 주소를 입력합니다.
   - 순수 IPv6 OfficeScan 서버의 경우 Control Manager FQDN 또는 IPv6 주소를 입력합니다.
4. **Control Manager 인증서** 옆에서 **찾아보기...**를 클릭하고 대상 Control Manager 서버에서 다운로드한 인증서 파일을 선택합니다.

   Control Manager 인증서 파일을 가져오려면 Control Manager 서버로 이동하고 다음 위치의 OfficeScan 서버에 인증서 파일을 복사합니다.

   <Control Manager 설치 폴더>₩Certificate₩CA₩TMCM_CA_Cert.pem

중요

회사가 Control Manager 서버에서 사용자 정의 인증서를 사용하는 경우 Control Manager 등록 중에 루트 CA 인증서를 업로드해야 합니다.

   자세한 내용은 Control Manager 인증서 권한 페이지 14-28를 참조하십시오.

5. Control Manager의 IIS Web server에 인증이 필요한 경우에는 사용자 이름과 암호를 입력합니다.
6. 프록시 서버를 사용하여 Control Manager 서버에 연결하는 경우에는 다음 프록시 설정을 지정합니다.

- 프록시 프로토콜
- 서버 FQDN 또는 IPv4/IPv6 주소와 포트
- 프록시 서버 인증 사용자 ID 및 암호

7. 통신 포트 전달에 단방향 또는 양방향 중 어느 것을 사용할지 결정한 다음 IPv4/IPv6 주소와 포트를 지정합니다.

8. OfficeScan에서 지정한 설정에 따라 Control Manager 서버에 연결할 수 있는지 확인하려면 **연결 테스트**을 클릭합니다.

   연결이 설정되면 **등록**을 클릭합니다.

9. Control Manager 서버가 버전 6.0 SP1 이상인 경우 OfficeScan 통합 스마트 보호 서버의 업데이트 소스로 Control Manager 서버를 사용할지 묻는 메시지가 나타납니다. **확인**을 클릭하여 Control Manager 서버를 통합 스마트 보호 서버 업데이트 소스로 사용하거나 **취소**를 클릭하여 현재 업데이트 소스(기본적으로 액티브업데이트 서버)를 계속 사용합니다.

10. 등록 후에 이 화면의 설정을 변경한 경우에는 설정을 변경한 후 **업데이트 설정**을 클릭하여 Control Manager 서버에 변경 사항에 대해 알립니다.

참고

Control Manager 서버가 Deep Discovery에 연결되어 있는 경우에는 등록이 완료된 후 자동 가입 프로세스가 시작됩니다. 자세한 내용은 의심스러운 개체 목록 설정 페이지 14-31를 참조하십시오.

11. Control Manager 서버로 더 이상 OfficeScan을 관리하지 않으려면 **등록 취소**를 클릭합니다.

Control Manager 인증서 권한

OfficeScan을 Control Manager 서버에 등록하기 전에 우선 다음 위치의 Control Manager 서버에서 Control Manager 인증서 파일을 가져와야 합니다.

<Control Manager 설치 폴더>₩Certificate₩CA₩TMCM_CA_Cert.pem

OfficeScan과 Control Manager는 서버 간에 허가된 등록 및 정책 관리 통신만 이루어질 수 있도록 인증서 및 공개 키 암호화를 사용합니다. 한 서버에서 무단 통신을 탐지하는 경우 서버는 수신되는 정책 설정 또는 등록을 거부합니다.

중요

회사가 Control Manager 서버에서 사용자 정의 인증서를 사용하는 경우 Control Manager 등록 중에 루트 CA 인증서를 업로드해야 합니다.

Control Manager 관리 콘솔에서 OfficeScan 상태 확인

절차

1. Control Manager 관리 콘솔을 엽니다.

   Control Manager 콘솔을 열려면 네트워크에 연결된 엔드포인트에서 웹 브라우저를 열고 다음을 입력합니다.

   https://<Control Manager 서버 이름>/Webapp/login.aspx

   여기서 <Control Manager 서버 이름>은 Control Manager 서버의 IP 주소 또는 호스트 이름입니다.

2. 기본 메뉴에서 **디렉터리** > **제품**을 클릭합니다.

3. 표시되는 트리에서 **[Control Manager 서버]** > **로컬 폴더** > **새 엔터티** 폴더로 이동합니다.

4. OfficeScan 서버 아이콘이 표시되는지 확인합니다.

정책 내보내기 도구

Trend Micro OfficeScan 서버 정책 내보내기 도구를 사용하면 관리자가 Control Manager 6.0 이상에서 지원하는 OfficeScan 정책 설정을 내보낼 수 있습니다. 또한 정책을 가져오려면 Control Manager 가져오기 도구도 필요합니다. 정책 내보내기 도구는 OfficeScan 10.6 Service Pack 1 이상을 지원합니다.

- 실시간 검색 설정
- 예약 검색 설정
- 수동 검색 설정
- 지금 검색 설정
- 업데이트 에이전트 설정
- 웹 검증 설정
- 검색 방법
- 동작 모니터링 설정
- 장치 제어 설정
- 데이터 손실 방지 설정
- 권한 및 기타 설정
- 추가 서비스 설정
- 스파이웨어/그레이웨어 승인된 목록
- 의심스러운 연결 설정

정책 내보내기 도구 사용

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩PolicyExportTool로 이동합니다.
2. PolicyExportTool.exe를 두 번 클릭하여 정책 내보내기 도구를 시작합니다.

   명령줄 인터페이스 화면이 열리고 정책 내보내기 도구에서 설정 내보내기를 시작합니다. 이 도구는 내보낸 설정이 포함된 폴더 2개(PolicyClient 및 PolicyDLP)를 PolicyExportTool 폴더에 생성합니다.
3. 두 폴더를 Control Manager 설치 폴더에 복사합니다.
4. Control Manager 서버에서 정책 가져오기 도구를 실행합니다.

   정책 가져오기 도구에 대한 자세한 내용은 Control Manager 서버의 *정책 가져오기 도구 추가 정보*(TMCM_installation folder₩WebUI₩WebApp₩widget ₩common₩tool₩PolicyImport₩)를 참조하십시오.

참고

정책 내보내기 도구에서는 사용자 정의된 데이터 식별자나 사용자 정의된 DLP 템플릿을 내보내지 않습니다. 사용자 정의된 데이터 식별자 및 DLP 템플릿을 내보내야 하는 관리자는 OfficeScan 콘솔에서 수동 내보내기를 수행한 다음 Control Manager 콘솔을 사용하여 파일을 수동으로 가져와야 합니다.

의심스러운 개체 목록 설정

의심스러운 개체는 Trend Micro Deep Discovery 제품 또는 다른 소스에 의해 완료한 분석에서 생성된 디지털 산출물입니다. OfficeScan은 의심스러운 개체를 동기화하고 Deep Discovery에 연결되어 있는 Control Manager 6.0 SP3 이상 서버에서 이러한 개체에 대한 조치를 검색할 수 있습니다.

Control Manager에 가입한 후 C&C 콜백 또는 네트워크 상의 에이전트로 식별되는 가능한 지정 공격을 모니터링하기 위해 의심스러운 개체의 유형을 선택합니다. 의심스러운 개체에는 다음이 포함됩니다.

- 의심스러운 URL 목록
- 의심스러운 IP 목록
- 의심스러운 파일 목록

참고

OfficeScan 10.6~11.0에서 의심스러운 주요 개체 소스는 Deep Discovery Analyzer입니다. OfficeScan 11.0 SP1부터는 주 소스가 Control Manager 6.0 SP3이며, 이는 더욱 강력한 의심스러운 개체 관리 및 처리 프로세스를 제공합니다.

OfficeScan이(가) Deep Discovery Analyzer에 가입되어 있다면 의심스러운 URL 목록만 사용할 수 있습니다. OfficeScan을(를) Deep Discovery Analyzer에서 탈퇴한 후 다시 가입할 수 없습니다. OfficeScan은(는) 의심스러운 개체를 동기화하기 위해 Deep Discovery에 연결되어 있는 Control Manager에 가입해야 합니다.

Control Manager가 의심스러운 개체를 관리하는 방법에 대한 자세한 내용은 *Control Manager 관리자 안내서*를 참조하십시오.

의심스러운 개체 목록 설정 구성

Control Manager에 OfficeScan을 등록하는 동안 Control Manager는 OfficeScan에 API 키를 배포하여 가입 프로세스를 시작합니다. 이 자동 가입 프로세스를 활성화하려면 Control Manager 관리자에게 문의하여 Control Manager가 Deep Discovery에 연결되어 있고 필요한 설정 사항이 구성되어 있는지 확인합니다.

Control Manager 서버를 등록하는 방법에 대한 자세한 내용은 OfficeScan을 Control Manager에 등록 페이지 14-26을 참조하십시오.

절차

1. **관리** > **설정** > **의심스러운 개체 목록**으로 이동합니다.
2. 에이전트에서 사용하도록 설정할 목록을 선택합니다.
   - 의심스러운 URL 목록
   - 의심스러운 IP 목록(등록된 Control Manager 서버 구독을 신청한 경우에만 사용 가능)
   - 의심스러운 파일 목록(등록된 Control Manager 서버 구독을 신청한 경우에만 사용 가능)

   관리자는 언제든 **지금 동기화** 단추를 클릭하여 의심스러운 개체 목록과 수동으로 동기화할 수 있습니다.
3. **OfficeScan 에이전트에서 의심스러운 개체 목록 업데이트** 아래에서 에이전트가 의심스러운 개체 목록을 업데이트할 시기를 지정합니다.
   - **OfficeScan 에이전트 구성 요소 업데이트 일정에 따라**: OfficeScan 에이전트에서 현재 업데이트 일정에 따라 의심스러운 개체 목록을 업데이트합니다.
   - **서버의 의심스러운 개체 목록 업데이트 후 자동으로**: OfficeScan 서버가 업데이트된 목록을 수신한 후 OfficeScan 에이전트에서 자동으로 의심스러운 개체 목록을 업데이트합니다.

참고

업데이트 에이전트에서 업데이트를 수신하도록 구성되지 않은 OfficeScan 에이전트는 동기화 중에 가입된 의심스러운 개체 목록에 대한 인크리멘탈 업데이트를 수행합니다.

4. **저장**을 클릭합니다.

참조 서버

OfficeScan 에이전트에서 사용할 정책 또는 프로필을 결정하는 방법 중 하나는 OfficeScan 서버와의 연결 상태를 확인하는 것입니다. 내부 OfficeScan 에이전트(또는 회사 네트워크 내의 에이전트)에서 서버에 연결할 수 없는 경우, 에이전트는 오프라인 상태가 됩니다. 그러면 에이전트는 외부 에이전트용 정책 또는 프로필을 적용합니다. 참조 서버가 이 문제를 해결해 줍니다.

OfficeScan 서버와의 연결이 끊긴 OfficeScan 에이전트는 참조 서버에 연결하려고 합니다. 에이전트가 참조 서버와 연결되면 내부 에이전트용 정책 또는 프로필을 적용합니다.

참조 서버에서 관리하는 정책 및 프로필은 다음과 같습니다.

- 방화벽 프로필
- 웹 검증 정책
- 데이터 보호 정책
- 장치 제어 정책

다음 사항에 유의하십시오.

- Web server, SQL 서버 또는 FTP 서버와 같이 서버 기능이 있는 컴퓨터를 참조 서버로 할당합니다. 최대 320대의 참조 서버를 지정할 수 있습니다.
- OfficeScan 에이전트는 참조 서버 목록의 첫 번째 참조 서버에 연결합니다. 연결을 설정할 수 없는 경우 에이전트는 목록에 있는 다음 서버에 연결하려고 합니다.

- OfficeScan 에이전트는 사용할 바이러스 백신(동작 모니터링, 장치 제어, 방화벽 프로필, 웹 검증 정책) 또는 데이터 보호 설정을 결정할 때 참조 서버를 사용합니다. 참조 서버는 에이전트를 관리하거나 업데이트 및 에이전트 설정을 배포하지 않습니다. OfficeScan 서버가 이러한 작업을 수행합니다.
- OfficeScan 에이전트는 참조 서버에 로그를 전송하거나 참조 서버를 업데이트 소스로 사용할 수 없습니다.

참조 서버 목록 관리

절차

1. **에이전트** > **방화벽** > **프로필** 또는 **에이전트** > **엔드포인트 위치**로 이동합니다.
2. 표시되는 화면에 따라 다음을 수행합니다.
   - **에이전트에 대한 방화벽 프로필** 화면이 표시된 경우 **참조 서버 목록 편집**을 클릭합니다.
   - **엔드포인트 위치** 화면이 표시된 경우 **참조 서버 목록**을 클릭합니다.
3. **참조 서버 목록 사용**을 선택합니다.
4. 목록에 엔드포인트를 추가하려면 **추가**를 클릭합니다.
   a. 다음과 같이 엔드포인트의 IPv4/IPv6 주소, 이름 또는 정규화된 도메인 이름(FQDN)을 지정합니다.
      - computer.networkname
      - 12.10.10.10
      - mycomputer.domain.com
   b. 에이전트가 이 엔드포인트와 통신할 포트를 입력합니다. 참조 서버에서 개방형 연락처 포트(예: 포트 20, 23 또는 80)를 지정합니다.

참고

동일한 참조 서버에 대해 다른 포트 번호를 지정하려면 2a단계와 2b단계를 반복합니다. OfficeScan 에이전트는 목록의 첫 번째 포트 번호를 사용하고, 연결에 실패할 경우 다음 포트 번호를 사용합니다.

c. **저장**을 클릭합니다.

5. 목록의 엔드포인트 설정을 편집하려면 엔드포인트 이름을 클릭합니다. 엔드포인트 이름이나 포트를 수정한 다음 **저장**을 클릭합니다.
6. 목록에서 엔드포인트를 제거하려면 엔드포인트 이름을 선택한 다음 **삭제**를 클릭합니다.
7. 엔드포인트가 참조 서버 역할을 할 수 있게 하려면 **에이전트에 할당**을 클릭합니다.

관리자 알림 설정

OfficeScan에서 전자 메일 및 SNMP 트랩을 통해 알림을 보낼 수 있도록 관리자 알림 설정을 구성합니다. OfficeScan에서는 이 알림 채널에 대해 별도의 설정을 구성하지 않고 Windows NT 이벤트 로그를 통해 알림을 보낼 수도 있습니다.

OfficeScan에서는 다음 사항이 탐지된 경우 여러 OfficeScan 관리자에게 알림을 보낼 수 있습니다.

표 14-17. 관리자 알림을 트리거하는 탐지

탐지	알림 채널		
	전자 메일	SNMP 트랩	Windows NT 이벤트 로그
바이러스 및 악성 프로그램	예	예	예
스파이웨어 및 그레이웨어	예	예	예
디지털 자산 전송	예	예	예
C&C 콜백	예	예	예

탐지	알림 채널		
	전자 메일	SNMP 트랩	Windows NT 이벤트 로그
바이러스 및 악성 프로그램 비상 발생	예	예	예
스파이웨어 및 그레이웨어 비상 발생	예	예	예
방화벽 위반 비상 발생	예	아니요	아니요
공유 폴더 세션 발생	예	아니요	아니요
C&C 콜백 비상 발생	예	예	예

일반 알림 설정 구성

절차

1. **관리** > **알림** > **일반 설정**으로 이동합니다.
2. 전자 메일 알림 설정을 구성합니다.
   a. **SMTP 서버** 필드에서 IPv4/IPv6 주소 또는 엔드포인트 이름을 지정합니다.
   b. 1에서 65535까지의 포트 번호를 지정합니다.
   c. 전자 메일 주소를 지정합니다.

      다음 단계에서 ESMTP를 사용하도록 설정하려면 유효한 전자 메일 주소를 지정합니다.
   d. 필요한 경우 **ESMTP**를 사용하도록 설정합니다.
   e. **보낸 사람** 필드에서 지정한 전자 메일 주소의 사용자 이름 및 암호를 지정합니다.
   f. 에이전트를 서버에 인증하는 방법을 선택합니다.

- **로그인**: 로그인은 이전 버전의 메일 사용자 에이전트입니다. 서버 및 에이전트 모두 BASE64를 사용하여 사용자 이름과 암호를 인증합니다.
- **일반 텍스트**: 일반 텍스트는 사용하기 가장 쉽지만 사용자 이름과 암호가 인터넷을 통해 보내지기 전에 하나의 문자열 및 BASE64 인코딩으로 보내져 안전하지 않을 수 있습니다.
- **CRAM-MD5**: CRAM-MD5는 시도/응답 인증 메커니즘 조합과 암호 메시지 요약 5 알고리즘을 사용하여 정보를 교환하고 인증합니다.

3. SNMP 트랩 알림 설정을 구성합니다.
   a. **서버 IP 주소** 필드에서 IPv4/IPv6 주소 또는 엔드포인트 이름을 지정합니다.
   b. 추측하기 어려운 커뮤니티 이름을 지정합니다.

참고

커뮤니티 이름은 보안상의 이유로 별표(*)를 사용하여 마스크 처리된 값으로 표시됩니다. 할당된 기본값은 "public"입니다.

4. **저장**을 클릭합니다.

시스템 이벤트 로그

OfficeScan에서는 종료, 시작과 같이 서버 프로그램과 관련된 이벤트를 기록합니다. 이러한 로그를 사용하여 OfficeScan 서버 및 서비스가 제대로 작동되는지를 확인할 수 있습니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

시스템 이벤트 로그 보기

절차

1. **로그** > **시스템 이벤트**로 이동합니다.
2. **이벤트**에서 추가 조치가 필요한 로그를 확인합니다. OfficeScan에서는 다음 이벤트를 기록합니다.

표 14-18. 시스템 이벤트 로그

로그 형식	이벤트
OfficeScan Master Service 및 데이터베이스 서버	• Master Service가 시작되었습니다. • Master Service가 중지되었습니다. • Master Service를 중지하지 못했습니다.
바이러스 사전 방역	• 바이러스 사전 방역 사용 • 바이러스 사전 방역 사용 안 함 • 마지막 시간<분>의 공유 폴더 세션 수
데이터베이스 백업	• 데이터베이스를 백업했습니다. • 데이터베이스를 백업하지 못했습니다.
역할 기반 웹 콘솔 액세스	• 콘솔에 로그온 • 암호 수정 • 콘솔에서 로그오프 • 세션 타임아웃(사용자가 자동으로 로그오프됨)
서버 인증	• OfficeScan 에이전트가 서버에서 잘못된 명령을 받음 • 인증 인증서가 잘못되었거나 만료됨

3. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

로그 관리

OfficeScan에서는 보안 위험 탐지, 이벤트 및 업데이트에 대한 포괄적인 로그를 보관합니다. 이러한 로그를 사용하여 회사의 보호 정책을 평가하고 감염 또는 공격 위험이 높은 OfficeScan 에이전트를 식별할 수 있습니다. 또한 에이전트-서버 연결을 확인하고 구성 요소가 성공적으로 업데이트되었는지 확인할 수도 있습니다.

OfficeScan에서는 특정 시간 확인 메커니즘을 사용하여 OfficeScan 서버와 에이전트 간의 시간 일관성을 확인합니다. 따라서 로그 분석 중 혼동을 일으킬 수 있는 표준 시간대, 일광 절약 시간 및 시차로 인한 로그 불일치가 방지됩니다.

참고

OfficeScan에서는 서버 업데이트 및 시스템 이벤트 로그를 제외한 모든 로그에 대해 시간 확인을 수행합니다.

OfficeScan 서버가 OfficeScan 에이전트에서 받는 로그는 다음과 같습니다.

- 바이러스/악성 프로그램 로그 보기 페이지 7-89
- 스파이웨어/그레이웨어 로그 보기 페이지 7-96
- 스파이웨어/그레이웨어 복원 로그 보기 페이지 7-100
- 방화벽 로그 보기 페이지 13-28
- 웹 검증 로그 보기 페이지 12-21
- 의심스러운 연결 로그 보기 페이지 8-13
- 의심스러운 파일 로그 보기 페이지 7-100
- C&C 콜백 로그 보기 페이지 12-22
- 동작 모니터링 로그 보기 페이지 9-17
- 장치 제어 로그 보기 페이지 10-18
- 검색 작업 로그 보기 페이지 7-102
- 데이터 손실 방지 로그 보기 페이지 11-56

- OfficeScan 에이전트 업데이트 로그 보기 페이지 6-48
- 연결 확인 로그 보기 페이지 15-42

OfficeScan 서버에서 생성하는 로그는 다음과 같습니다.

- OfficeScan 서버 업데이트 로그 페이지 6-25
- 시스템 이벤트 로그 페이지 14-37

다음 로그도 OfficeScan 서버 및 OfficeScan 에이전트에서 사용할 수 있습니다.

- Windows 이벤트 로그 페이지 18-25
- OfficeScan 서버 로그 페이지 18-2
- OfficeScan 에이전트 로그 페이지 18-14

로그 유지 관리

로그 크기가 하드 디스크의 공간을 너무 많이 차지하지 않도록 방지하려면 웹 콘솔에서 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다.

일정에 따라 로그 삭제

절차

1. **로그** > **로그 유지 관리**로 이동합니다.
2. **로그의 예약 삭제 기능 사용**을 선택합니다.
3. 삭제할 로그 형식을 선택합니다. 디버그 로그를 제외하고 OfficeScan에서 생성된 모든 로그를 일정에 따라 삭제할 수 있습니다. 디버그 로그에 대해 로그 수집을 중지하려면 디버그 로깅을 비활성화합니다.

참고

바이러스/악성 프로그램 로그의 경우 특정 검색 유형 및 Damage Cleanup Services에서 생성된 로그를 삭제할 수 있습니다. 스파이웨어/그레이웨어 로그의 경우 특정 검색 유형의 로그를 삭제할 수 있습니다. 검색 유형에 대한 자세한 내용은 검색 유형 페이지 7-14을 참조하십시오.

4. 선택한 모든 로그 형식의 로그를 모두 삭제할 것인지, 아니면 특정 일 수보다 오래된 로그만 삭제할 것인지 선택합니다.
5. 로그 삭제 빈도와 시간을 지정합니다.
6. **저장**을 클릭합니다.

수동으로 로그 삭제

절차

1. **로그** > **에이전트** > **보안 위험** 또는 **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. 다음 단계 중 하나를 수행합니다.
   - **보안 위험 로그** 화면에 액세스한 경우 **로그 삭제**를 클릭합니다.
   - **에이전트 관리** 화면에 액세스한 경우 **로그** > **로그 삭제**를 클릭합니다.
4. 삭제할 로그 형식을 선택합니다. 다음 로그 중 하나를 수동으로 삭제할 수 있습니다.
   - 동작 모니터링 로그
   - C&C 콜백 로그
   - 데이터 손실 방지 로그
   - 장치 제어 로그
   - 방화벽 로그
   - 머신러닝 로그
   - 스파이웨어/그레이웨어 로그
   - 검색 작업 로그

- 의심스러운 연결 로그
- 의심스러운 파일 로그
- 바이러스/악성 프로그램 로그
- 웹 검증 로그

참고

바이러스/악성 프로그램 로그의 경우 특정 검색 유형 및 Damage Cleanup Services에서 생성된 로그를 삭제할 수 있습니다. 스파이웨어/그레이웨어 로그의 경우 특정 검색 유형의 로그를 삭제할 수 있습니다.

검색 유형에 대한 자세한 내용은 검색 유형 페이지 7-14을 참조하십시오.

5. 선택한 모든 로그 형식의 로그를 모두 삭제할 것인지, 아니면 특정 일 수보다 오래된 로그만 삭제할 것인지 선택합니다.
6. **삭제**를 클릭합니다.

라이선스

웹 콘솔에서 OfficeScan 라이선스 서비스를 보고, 정품을 인증하고, 갱신하고 OfficeScan 방화벽을 사용하거나 사용하지 않도록 설정합니다. OfficeScan 방화벽은 바이러스 백신 서비스의 일부이며, 바이러스 사전 방역에 대한 지원도 포함합니다.

참고

데이터 보호 및 가상 데스크톱 지원과 같은 일부 기본 OfficeScan 기능에는 고유한 라이선스가 있습니다. 이러한 기능에 대한 라이선스는 Plug-in Manager에서 활성화되고 관리됩니다. 이러한 기능의 라이선스에 대한 자세한 내용은 데이터 보호 라이선스 페이지 3-4 및 가상 데스크톱 지원 라이선스 페이지 15-75를 참조하십시오.

순수 IPv6 OfficeScan 서버에서는 Trend Micro Online Registration Server에 연결하여 라이선스를 활성화/갱신할 수 없습니다. OfficeScan 서버에서 Registration Server에 연결할 수 있도록 하려면 IP 주소를 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)가 필요합니다.

제품 라이선스 정보 보기

절차

1. **관리** > **설정** > **제품 라이선스**로 이동합니다.
2. 화면 맨 위에 표시되는 라이선스의 상태 요약 정보를 확인합니다. 다음과 같은 경우에 라이선스에 대한 미리 알림이 표시됩니다.

표 14-19. 라이선스 미리 알림

라이선스 유형	미리 알림
정식 버전	• 제품의 유예 기간 중. 유예 기간은 지역에 따라 다릅니다. Trend Micro 대리점에서 유예 기간을 확인하십시오. • 라이선스가 만료되고 유예 기간이 경과된 경우. 이 기간 중에는 기술 지원을 받거나 구성 요소 업데이트를 수행할 수 없습니다. 검색 엔진은 계속 엔드포인트를 검색하지만 이전 구성 요소를 사용하게 됩니다. 이전 구성 요소로는 최신 보안 위협으로부터 시스템을 완벽하게 보호할 수 없습니다.
평가판	라이선스가 만료된 경우. 이 기간 중에는 OfficeScan에서 구성 요소 업데이트를 사용할 수 없습니다. 검색 엔진은 계속 엔드포인트를 검색하지만 이전 구성 요소를 사용하게 됩니다. 이전 구성 요소로는 최신 보안 위협으로부터 시스템을 완벽하게 보호할 수 없습니다.

3. 라이선스 정보를 확인합니다. **라이선스 정보** 섹션에서는 다음 정보를 제공합니다.

   - **서비스**: 모든 OfficeScan 라이선스 서비스를 포함합니다.
   - **상태**: "정품 인증됨", "정품 인증되지 않음", "만료됨" 또는 "유예 기간 중"이 표시됩니다. 서비스에 여러 개의 라이선스가 있고 하나 이상의 라이선스가 계속 유효한 경우 상태는 "정품 인증됨"으로 표시됩니다.
   - **버전**: "정식" 또는 "평가판" 버전이 표시됩니다. 정식 버전과 평가판이 모두 있는 경우에는 버전이 "정식"으로 표시됩니다.
   - **만료일**: 서비스에 여러 개의 라이선스가 있는 경우 가장 늦은 만료일이 표시됩니다. 예를 들어, 라이선스 만료일이 2007/12/31 및 2008/06/30인 경우에는 2008/06/30이 표시됩니다.

   참고

   정품 인증되지 않은 라이선스 서비스의 버전 및 만료일은 "해당 없음"입니다.

4. OfficeScan을 사용하면 라이선스 서비스에 대한 여러 개의 라이선스를 정품 인증할 수 있습니다. 서비스 이름을 클릭하여 해당 서비스에 대한 모든 라이선스(유효 및 만료된 라이선스)를 표시합니다.

라이선스 활성화 또는 갱신

절차

1. **관리** > **설정** > **제품 라이선스**로 이동합니다.
2. 라이선스 서비스의 이름을 클릭합니다.
3. **제품 라이선스 세부 정보** 화면이 열리면 **새 정품 인증 코드**를 클릭합니다.
4. 열려 있는 화면에서 정품 인증 코드를 입력하고 **저장**을 클릭합니다.

참고

서비스를 정품 인증하기 전에 등록합니다. 등록 키와 정품 인증 코드에 대한 자세한 내용은 Trend Micro 대리점에 문의하십시오.

5. 다시 **제품 라이선스 세부 정보** 화면에서 **정보 업데이트**를 클릭하여 새 라이선스 세부 정보 및 서비스 상태로 화면을 새로 고칩니다. 이 화면에는 라이선스에 대한 세부 정보를 볼 수 있는 Trend Micro 웹 사이트에 대한 링크도 제공됩니다.

OfficeScan 데이터베이스 백업

OfficeScan 서버 데이터베이스에는 검색 설정과 권한을 비롯한 모든 OfficeScan 설정이 포함되어 있습니다. 서버 데이터베이스가 손상된 경우에도 백업이 있으면 복원할 수 있습니다. 데이터베이스는 언제든지 수동으로 백업할 수 있으며 백업 일정을 구성할 수 있습니다.

데이터베이스를 백업할 때 OfficeScan은 자동으로 데이터베이스의 조각 모음을 돕고 손상된 것으로 보이는 색인 파일을 모두 복구합니다.

시스템 이벤트 로그에서 백업 상태를 확인합니다. 자세한 내용은 시스템 이벤트 로그 페이지 14-37를 참조하십시오.

팁

Trend Micro에서는 자동 백업 일정을 구성할 것을 권장합니다. 데이터베이스는 서버 트래픽이 낮은 한가한 시간에 백업하십시오.

경고!

다른 도구나 소프트웨어로 백업을 수행하지 마십시오. 데이터베이스 백업은 OfficeScan 웹 콘솔에서만 구성해야 합니다.

OfficeScan 데이터베이스 백업

절차

1. **관리** > **설정** > **데이터베이스 백업**으로 이동합니다.
2. 데이터베이스를 저장할 위치를 입력합니다. 아직 폴더가 없는 경우에는 **폴더가 없으면 새로 만들기**를 선택합니다. C:₩OfficeScan₩DatabaseBackup과 같이 드라이브와 전체 디렉터리 경로를 포함합니다.

   기본적으로 OfficeScan은 <서버 설치 폴더>₩DBBackup 디렉터리에 백업을 저장합니다.

   참고

   OfficeScan에서는 백업 경로 아래에 하위 폴더를 만듭니다. 폴더 이름은 백업 시간을 나타내며, 시간 형식으로 YYYYMMDD_HHMMSS가 사용됩니다. OfficeScan은 최근 7개의 백업 폴더를 보존하고, 오래된 폴더는 자동으로 삭제합니다.

3. 백업 경로가 원격 컴퓨터에 있는 경우에는(UNC 경로 사용) 적절한 계정 이름과 해당 암호를 입력합니다. 해당 계정에 컴퓨터에 대한 쓰기 권한이 있는지 확인합니다.
4. 백업 일정을 구성하려면
   a. **예약 데이터베이스 백업 사용**을 선택합니다.
   b. 백업 빈도와 시간을 지정합니다.
   c. 데이터베이스를 백업하고 변경 사항을 저장하려면 **지금 백업**을 클릭합니다. 데이터베이스는 백업하지 않고 변경 사항만 저장하려면 **저장**을 클릭합니다.

데이터베이스 백업 파일 복원

절차

1. OfficeScan Master Service를 중지합니다.
2. <서버 설치 폴더>₩PCCSRV₩HTTPDB의 데이터베이스 파일을 백업 파일로 덮어씁니다.
3. OfficeScan Master Service를 다시 시작합니다.

SQL Server 마이그레이션 도구

관리자는 SQL Server 마이그레이션 도구를 사용하여 기존 OfficeScan 데이터베이스를 기본 CodeBase 스타일에서 SQL Server 데이터베이스로 마이그레이션할 수 있습니다. SQL Server 마이그레이션 도구는 다음과 같은 데이터베이스 마이그레이션을 지원합니다.

- OfficeScan CodeBase 데이터베이스에서 새 SQL Server Express 데이터베이스로
- OfficeScan CodeBase 데이터베이스에서 기존 SQL Server 데이터베이스로
- 다른 위치로 이동한 OfficeScan SQL 데이터베이스(이전에 마이그레이션함)

SQL Server 마이그레이션 도구 사용

SQL Server 마이그레이션 도구는 SQL Server 2014 SP2 Express를 사용하여 기존 CodeBase 데이터베이스를 SQL 데이터베이스로 마이그레이션합니다.

팁

OfficeScan 데이터베이스를 마이그레이션한 후에는 새로 마이그레이션한 SQL 데이터베이스를 다른 SQL Server로 이동할 수 있습니다. SQL Server 마이그레이션 도구를 다시 실행하고 **기존 OfficeScan SQL 데이터베이스로 전환**을 선택하여 다른 SQL Server를 사용합니다.

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩SQL로 이동합니다.
2. SQLTxfr.exe를 두 번 클릭하여 도구를 실행합니다.

   SQL Server 마이그레이션 도구 콘솔이 열립니다.
3. 마이그레이션 유형을 선택합니다.

옵션	설명
새 SQL Server 2014 SP2 Express를 설치하고 OfficeScan 데이터베이스 마이그레이션	SQL Server 2014 SP2 Express를 자동으로 설치하고 기존 OfficeScan 데이터베이스를 새 SQL 데이터베이스로 마이그레이션합니다. **참고** OfficeScan은 SQL Server에 포트 1433을 자동으로 할당합니다.
기존 SQL Server로 OfficeScan 데이터베이스 마이그레이션	기존 SQL Server의 새 SQL 데이터베이스로 기존 OfficeScan 데이터베이스 마이그레이션합니다.
기존 OfficeScan SQL 데이터베이스로 전환	기존 SQL Server의 기존 OfficeScan SQL 데이터베이스를 가리키도록 OfficeScan 구성 설정을 변경합니다.

4. 다음과 같이 **서버 이름**을 지정합니다.
   - SQL을 새로 설치하는 경우: <SQL 서버의 호스트 이름 또는 IP 주소>\<인스턴스 이름>
   - SQL Server를 마이그레이션하는 경우: <SQL 서버의 호스트 이름 또는 IP 주소>,<포트 번호>\<인스턴스 이름>
   - 기존 OfficeScan SQL 데이터베이스로 전환하는 경우: <SQL 서버의 호스트 이름 또는 IP 주소>,<포트 번호>\<인스턴스 이름>

중요

OfficeScan에서는 SQL Server가 설치될 때 OfficeScan 데이터베이스의 인스턴스를 자동으로 만듭니다. 기존 SQL Server 또는 데이터베이스로 마이그레이션할 경우 SQL Server에 있는 OfficeScan 인스턴스의 기존 인스턴스 이름을 입력합니다.

5. SQL Server 데이터베이스에 대한 인증 자격 증명을 제공합니다.

   - **Windows 계정**을 사용하여 서버에 로그인하는 경우 **사용자 이름**은 다음 형식을 사용해야 합니다.

     domain_name\user_name 또는 user_name

     중요

     사용자 계정은 로컬 관리자 그룹 또는 AD(Active Directory) 기본 제공 관리자에 속해야 하며 Windows **로컬 보안 정책** 또는 **그룹 정책 관리** 콘솔을 사용하여 다음의 사용자 권한 할당 정책을 구성해야 합니다.

     - 서비스로 로그온
     - 배치 작업으로 로그온
     - 로컬 로그온

     사용자 계정에는 다음과 같은 데이터베이스 역할이 있어야 합니다.

     - dbcreator
     - bulkadmin
     - db_owner

6. SQL Server를 새로 설치하는 경우 새 암호를 입력하고 확인합니다.

참고

암호는 다음과 같은 최소 강도 요구 사항을 충족해야 합니다.

a. 최소 길이: 8자

b. 다음 중 3가지 이상을 포함해야 합니다.

- 대문자: A~Z
- 소문자: a~z
- 숫자: 0~9 0 - 9
- 특수 문자: !@#$^*?_~-();.+: !@#$^*?_~-();.+:

7. SQL Server의 OfficeScan **데이터베이스 이름**을 지정합니다.

   OfficeScan CodeBase 데이터베이스를 새 SQL 데이터베이스로 마이그레이션할 경우 OfficeScan에서는 자동으로 새 데이터베이스를 제공한 이름으로 만듭니다.

8. 필요한 경우 다음 작업을 수행합니다.

   - **연결 테스트**를 클릭하여 기존 SQL Server 또는 데이터베이스의 인증 자격 증명을 확인합니다.
   - **SQL 데이터베이스 사용할 수 없는 경고...**를 클릭하여 SQL 데이터베이스 알림 설정을 구성합니다.

     자세한 내용은 SQL 데이터베이스를 사용할 수 없음 경고 구성 페이지 14-50를 참조하십시오.

9. **시작**을 클릭하여 구성 변경 사항을 적용합니다.

SQL 데이터베이스를 사용할 수 없음 경고 구성

OfficeScan에서는 SQL 데이터베이스를 사용할 수 없는 경우 항상 이 알림을 자동으로 보냅니다.

경고!

OfficeScan에서는 데이터베이스를 사용할 수 없는 경우 서비스를 모두 자동으로 중지합니다. 데이터베이스를 사용할 수 없으면 OfficeScan에서 에이전트 또는 이벤트 정보를 기록하거나, 업데이트를 수행하거나, 에이전트를 구성할 수 없습니다.

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩SQL로 이동합니다.
2. SQLTxfr.exe를 두 번 클릭하여 도구를 실행합니다.

   SQL Server 마이그레이션 도구 콘솔이 열립니다.
3. **SQL 데이터베이스를 사용할 수 없음 경고…**를 클릭합니다.

   SQL Server를 사용할 수 없음 경고 화면이 열립니다.
4. 알림을 받는 사람의 전자 메일 주소를 입력합니다.

   항목이 여럿이면 세미콜론(;)으로 구분합니다.
5. 필요한 경우 **제목** 및 **메시지**를 수정합니다.

   OfficeScan에서는 다음과 같은 토큰 변수를 제공합니다.

   표 14-20. SQL 데이터베이스를 사용할 수 없음 경고 토큰

변수	설명
%x	OfficeScan SQL 서버 인스턴스의 이름
%s	영향받는 OfficeScan 서버의 이름

6. **확인**을 클릭합니다.

OfficeScan Web Server/에이전트 연결 설정

OfficeScan 서버를 설치할 때 설치 프로그램은 네트워크로 연결된 컴퓨터에서 OfficeScan 서버에 연결할 수 있게 해주는 Web Server를 자동으로 설치합니다. 네트워크로 연결된 엔드포인트 에이전트가 연결할 Web Server를 구성합니다.

Web server 설정을 외부(예: IIS 관리 콘솔)에서 수정한 경우 OfficeScan에서 변경 사항을 복제합니다. 예를 들어, 네트워크로 연결된 컴퓨터의 서버 IP 주소를 수동으로 변경하거나 동적 IP를 지정한 경우에는 OfficeScan의 서버 설정을 다시 구성해야 합니다.

경고!

연결 설정을 변경하면 서버와 에이전트 간의 연결이 영구적으로 손실되어 OfficeScan 에이전트를 다시 배포해야 할 수 있습니다.

연결 설정 구성

절차

1. **관리** > **설정** > **에이전트 연결**으로 이동합니다.
2. Web server의 도메인 이름 또는 IPv4/IPv6 주소와 포트 번호를 입력합니다.

   참고

   포트 번호는 OfficeScan 서버가 OfficeScan 에이전트와의 통신에 사용하는 트러스트된 포트입니다.

3. **저장**을 클릭합니다.

서버-에이전트 통신

서버와 에이전트 간 모든 통신이 유효하도록 OfficeScan을 구성할 수 있습니다. OfficeScan은 공개 키 암호화 및 향상된 암호화 기능을 제공하여 서버와 에이전트 간 모든 통신을 보호합니다.

통신 보호 기능에 대한 자세한 내용은 다음을 참조하십시오.

- 서버에서 시작된 통신에 대한 인증 페이지 14-53
- 서버-에이전트 통신에 대해 향상된 암호화 페이지 14-57

서버에서 시작된 통신에 대한 인증

OfficeScan에서는 OfficeScan 서버가 에이전트에 대해 시작하는 통신을 공개 키 암호화를 사용하여 인증합니다. 서버는 공개 키 암호화를 사용하여 개인 키를 유지하고 공개 키를 모든 에이전트에 배포합니다. 에이전트는 들어오는 통신이 서버에서 시작되었고 유효한지를 공개 키를 사용하여 확인합니다. 에이전트는 확인에 성공하는 경우 응답합니다.

참고

OfficeScan은 에이전트가 서버에 대해 시작하는 통신은 인증하지 않습니다.

공개 및 개인 키는 Trend Micro 인증서와 연결되어 있습니다. OfficeScan 서버 설치 중에 설치 프로그램에서는 인증서를 호스트의 인증서 저장소에 저장합니다. 인증 인증서 관리자 도구를 사용하여 Trend Micro 인증서와 키를 관리할 수 있습니다.

OfficeScan 서버 전반에 걸쳐 단일 인증 키를 사용할지 여부를 결정할 때는 다음 사항에 유의하십시오.

- 단일 인증서 키를 구현하는 것이 표준 보안 수준을 얻기 위한 일반적인 방법입니다. 이 접근 방식을 활용하면 조직 보안 수준의 균형이 유지되고 여러 개의 키를 유지 관리하는 데 따르는 오버헤드가 줄어듭니다.
- OfficeScan 서버 전반에 걸쳐 여러 인증서 키를 구현하면 보안 수준이 극대화됩니다. 이 접근 방식을 활용하면 인증서 키가 만료되어 서버 전체에 다시 배포해야 할 때 요구되는 유지 관리 노력이 늘어나게 됩니다.

중요

OfficeScan 서버를 다시 설치하려면 먼저 기존 인증서를 백업했는지 확인하십시오. 새 설치가 완료된 후에는 백업한 인증서를 가져와서 OfficeScan 서버와 OfficeScan 에이전트 간의 통신 인증이 중단 없이 계속되도록 하십시오. 서버 설치 중에 새 인증서를 만들면 OfficeScan 에이전트가 더 이상 존재하지 않는 이전 인증서를 계속 사용하게 되기 때문에 서버 통신을 인증할 수 있습니다.

인증서 백업, 복원, 내보내기 및 가져오기에 대한 자세한 내용은 인증 인증서 관리자 사용 페이지 14-54을 참조하십시오.

서버에서 시작된 통신에 대한 인증 구성

절차

1. OfficeScan 서버에서 <서버_설치_폴더>₩PCCSRV로 이동한 후 텍스트 편집기를 사용하여 ofcscan.ini를 엽니다.
2. `[Global Settings]` 섹션에서 텍스트 문자열 `SGNF`를 추가하거나 수정합니다.

   인증을 사용하려면: `SGNF=1`

   인증을 사용하지 않으려면: `SGNF=0`

   참고

   OfficeScan에서는 기본적으로 인증을 사용합니다. 이 기능을 사용하지 않으려는 경우에만 ofcscan.ini 파일에 `SGNF` 키를 추가하십시오.

3. 웹 콘솔에서 **에이전트** > **글로벌 에이전트 설정**으로 이동한 후 **저장**을 클릭하여 설정을 에이전트에 배포합니다.

인증 인증서 관리자 사용

OfficeScan 서버는 에이전트의 만료된 인증서를 만료된 공개 키와 함께 유지 관리합니다. 예를 들어 서버에 장기간 연결하지 않은 에이전트에 만료된 공개 키가 있다고 가정해 보겠습니다. 이 에이전트가 다시 연결할 때는 만료된 공개 키

와 만료된 인증서를 연결하여 서버에서 시작한 통신을 인식할 수 있습니다. 그러면 서버에서 최신 공개 키를 에이전트에 배포합니다.

인증서를 구성할 때는 다음 사항에 유의하십시오.

- 매핑된 드라이브와 UNC 경로를 인증서 경로로 사용할 수 있습니다.
- 강력한 암호를 선택한 다음 나중에 참조할 수 있도록 기록하십시오.

중요

인증 인증서 관리자 도구를 사용할 때는 다음 요구 사항에 유의하십시오.

- 사용자에게 관리자 권한이 있어야 합니다.
- 도구에서는 로컬 엔드포인트에 있는 인증서만 관리할 수 있습니다.

절차

1. OfficeScan 서버에서 명령 프롬프트를 열고 디렉터리를 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩CertificateManager로 변경합니다.
2. 다음 명령을 실행합니다.

명령	예	설명
CertificateManager.exe -c [백업_암호]	`CertificateManager.exe -c strongpassword`	새 Trend Micro 인증서를 생성하고 기존 인증서를 대체합니다. 기존 인증서가 만료되었거나 권한 없는 당사자에게 노출된 경우 이렇게 합니다.

명령	예	설명
CertificateManager.exe -b [암호] [인증서 경로] **참고** 인증서는 ZIP 포맷입니다.	`CertificateManager.exe -b strongpassword D:\Test\TrendMicro.zip`	현재 OfficeScan 서버에서 발급한 모든 Trend Micro 인증서를 백업합니다. OfficeScan 서버에서 인증서를 백업하려면 이렇게 합니다. **참고** OfficeScan 서버 인증서를 백업하면 OfficeScan 서버를 다시 설치해야 할 때 이러한 인증서를 사용할 수 있습니다.
CertificateManager.exe -r [암호] [인증서 경로] **참고** 인증서는 ZIP 포맷입니다.	`CertificateManager.exe -r strongpassword D:\Test\TrendMicro.zip`	서버에서 모든 Trend Micro 인증서를 복원합니다. 다시 설치한 OfficeScan 서버에서 인증서를 복원하려면 이렇게 합니다.
CertificateManager.exe -e [인증서 경로]	`CertificateManager.exe -e <에이전트_설치_폴더>\OfcNTCer.dat`	현재 사용되는 인증서와 연결된 OfficeScan 에이전트 공개 키를 내보냅니다. 에이전트에서 사용하는 공개 키가 손상되는 경우 이렇게 합니다. .dat 파일을 에이전트의 루트 폴더로 복사하여 기존 파일을 덮어씁니다. **중요** OfficeScan 에이전트의 인증서 파일 경로는 다음과 같아야 합니다. <에이전트_설치_폴더>₩OfcNTCer.dat

명령	예	설명
CertificateManager.exe -i [암호] [인증서 경로] **참고** 인증서의 기본 파일 이름은 다음과 같습니다. OfcNTCer.pfx	CertificateManager.exe -i strongpassword D:\Test\OfcNTCer.pfx	Trend Micro 인증서를 인증서 저장소로 가져옵니다.
CertificateManager.exe -l [CSV 경로]	CertificateManager.exe -l D:\Test\MismatchedAgentList.csv	현재 일치하지 않는 인증서를 사용하는 에이전트를 CSV 포맷으로 나열합니다.

서버-에이전트 통신에 대해 향상된 암호화

OfficeScan은 정부의 보안 준수 표준을 충족하기 위해 고급 암호화 표준(AES) 256을 사용하여 서버와 에이전트 간 향상된 통신 암호화를 제공합니다.

중요

OfficeScan에서는 OfficeScan 11.0 SP1 이상 버전 및 Plug-in Manager 2.2 이상 버전을 실행하는 서버 및 에이전트에서만 AES-256 암호화를 지원합니다.

경고!

AES-256 암호화를 사용하도록 설정하기 전에 서버가 관리하는 모든 OfficeScan 에이전트를 11.0 SP1 버전으로 업그레이드해야 합니다. 그 이전 버전의 OfficeScan 에이전트에서는 AES-256으로 암호화된 통신의 암호를 해독할 수 없습니다. 이러한 OfficeScan 에이전트 버전에서 AES-256 암호화를 사용하도록 설정하면 프록시 서버 사용 시 OfficeScan 서버와의 통신이 완전히 손실될 수 있습니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **네트워크** 탭을 클릭합니다.
3. **서버-에이전트 통신** 섹션으로 이동합니다.
4. **OfficeScan 서버와 OfficeScan 에이전트 간 통신용 AES-256 암호화** 옆의 **변경** 단추를 클릭합니다.

   메시지가 나타납니다.
5. **버전 확인**을 클릭하여 모든 에이전트가 OfficeScan 11.0 SP1 이상으로 업데이트되었는지 확인합니다.
6. **확인**을 클릭합니다.

웹 콘솔 암호

서버 컴퓨터에 역할 기반 관리를 사용하는 데 필요한 리소스가 없는 경우 웹 콘솔 암호(또는 OfficeScan 서버 설치 중에 만든 루트 계정에 대한 암호)를 관리하는 화면에 액세스만 할 수 있습니다. 예를 들어, 서버 컴퓨터에서 Windows Server 2003을 실행하고 권한 부여 관리자 런타임이 설치되지 않은 경우 이 화면에 액세스할 수 있습니다. 리소스가 적절한 경우에는 이 화면이 표시되지 않으며 **사용자 계정** 화면에서 루트 계정을 수정하여 암호를 관리할 수 있습니다.

OfficeScan이 Control Manager에 등록되지 않은 경우에는 웹 콘솔에 액세스할 수 있는 권한을 얻는 방법에 대해 지원 센터에 문의합니다.

웹 콘솔 설정

웹 콘솔 설정 화면을 사용하여 다음 작업을 수행할 수 있습니다.

- 요약 대시보드를 주기적으로 새로 고치도록 OfficeScan 서버를 구성할 수 있습니다. 기본적으로 서버는 30초마다 대시보드를 새로 고칩니다. 초는 10에서 300 사이가 될 수 있습니다.

- 웹 콘솔 타임아웃 설정을 지정할 수 있습니다. 기본적으로 비활성 상태로 30분이 지나면 웹 콘솔에서 자동으로 로그오프됩니다. 분은 10에서 60 사이가 될 수 있습니다.

웹 콘솔 설정 구성

절차

1. **관리** > **설정** > **웹 콘솔**으로 이동합니다.
2. **자동 새로 고침 사용**을 선택한 다음 새로 고침 간격을 선택합니다.
3. **웹 콘솔에서 자동 로그아웃 사용**을 선택한 다음 타임아웃 간격을 선택합니다.
4. **저장**을 클릭합니다.

격리 보관 관리자

OfficeScan 에이전트에서 보안 위험이 탐지되어 검색 조치로 격리 보관이 적용될 때마다 감염된 파일을 암호화한 다음 <에이전트 설치 폴더>₩SUSPECT ₩Backup에 있는 로컬 격리 보관 폴더로 이동합니다.

파일을 로컬 격리 보관 디렉터리로 이동한 후에 OfficeScan 에이전트는 지정된 격리 보관 디렉터리로 보냅니다. **에이전트** > **에이전트 관리** > **설정** > **{검색 유형} 설정** > **조치** 탭에서 디렉터리를 지정합니다. 지정된 격리 보관 디렉터리의 파일이 다른 파일을 감염시키지 않도록 암호화됩니다. 자세한 내용은 격리 보관 디렉터리 페이지 7-39를 참조하십시오.

지정된 격리 보관 디렉터리가 OfficeScan 서버 컴퓨터에 있을 경우, 웹 콘솔에서 서버의 격리 보관 디렉터리 설정을 수정합니다. 서버는 <서버 설치 폴더>₩PCCSRV₩Virus에 격리된 파일을 저장합니다.

참고

네트워크 연결 문제 등 어떤 이유로든 OfficeScan 에이전트에서 암호화된 파일을 OfficeScan 서버로 보낼 수 없는 경우 암호화된 파일은 OfficeScan 에이전트 격리 보관 폴더에 남습니다. OfficeScan 에이전트는 OfficeScan 서버에 연결할 때 파일을 다시 보내려 합니다.

격리 보관 디렉터리 설정 구성

절차

1. **관리** > **설정** > **격리 보관 관리자**로 이동합니다.
2. 격리 보관 폴더의 기본 용량 및 OfficeScan에서 격리 보관 폴더에 저장할 수 있는 감염된 파일의 최대 크기를 그대로 사용하거나 수정하여 사용합니다.

   기본값이 화면에 표시됩니다.
3. **격리 보관 설정 저장**을 클릭합니다.
4. 격리 보관 폴더에서 기존 파일을 모두 제거하려면 **격리된 파일 모두 삭제**를 클릭합니다.

서버 튜너

서버 튜너를 사용하면 다음의 서버 관련 성능 문제에 대해 매개 변수를 사용하여 OfficeScan 서버의 성능을 최적화할 수 있습니다.

- **다운로드**

  OfficeScan 서버로부터 업데이트를 요청하는 OfficeScan 에이전트(업데이트 에이전트 포함)의 수가 서버의 사용 가능한 리소스를 초과하는 경우, 서버는 에이전트 업데이트 요청을 대기열로 옮기고 리소스를 사용할 수 있게 되면 요청을 처리합니다. OfficeScan 서버의 구성 요소를 성공적으로 업데이트한 에이전트는 서버에 업데이트가 완료되었음을 알립니다. 에이전트로부터 업데이트 알림을 받을 때까지 OfficeScan 서버에서 대기하는 최대 시간(분)을 설정합니다. 또한 업데이트를 수행하고 새 구성 설정을 적용하

도록 에이전트에 알리려고 서버가 시도하는 최대 횟수를 설정합니다. 서버는 에이전트 알림을 받지 않은 경우에만 계속 시도합니다.

- **버퍼**

  OfficeScan 서버가 OfficeScan 에이전트에서 업데이트 수행 요청과 같은 여러 요청을 받는 경우 서버는 최대한 요청을 많이 처리하고 나머지 요청을 버퍼에 저장합니다. 그런 다음 서버는 리소스를 사용할 수 있게 되면 버퍼에 저장된 요청을 한 번에 하나씩 처리합니다. 에이전트 업데이트 요청 및 에이전트 로그 보고와 같은 이벤트의 버퍼 크기를 지정합니다.

- **네트워크 트래픽**

  하루 중 네트워크 트래픽의 양은 계속해서 달라집니다. OfficeScan 서버와 다른 업데이트 소스로 전달되는 네트워크 트래픽의 흐름을 제어하려면 하루 중 지정한 시간에 동시에 업데이트할 수 있는 OfficeScan 에이전트 수를 지정합니다.

서버 튜너를 사용하려면 SvrTune.exe 파일이 필요합니다.

서버 튜너 실행

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩SvrTune으로 이동합니다.
2. SvrTune.exe를 두 번 클릭하여 서버 튜너를 시작합니다.

   서버 튜너 콘솔이 열립니다.
3. **다운로드**에서 다음 설정을 수정합니다.

   - **클라이언트 타임아웃**: 에이전트로부터 업데이트 응답을 받을 때까지 OfficeScan 서버가 대기하는 시간(분)을 입력합니다. 에이전트가 이 시간 동안 응답하지 않을 경우 OfficeScan 서버에서는 에이전트에 현재 구성 요소가 있다고 간주하지 않습니다. 알림을 받은 에이전트가 제한 시간을 초과하면 알림을 기다리는 다른 에이전트의 슬롯을 사용할 수 있습니다.

- **업데이트 에이전트 타임아웃**:업데이트 에이전트로부터 업데이트 응답을 받을 때까지 OfficeScan 서버에서 대기하는 시간(분)을 입력합니다. 알림을 받은 에이전트가 제한 시간을 초과하면 알림을 기다리는 다른 에이전트의 슬롯을 사용할 수 있습니다.
- **다시 시도 횟수**: 업데이트를 수행하고 새 구성 설정을 적용하도록 에이전트에 알리려고 OfficeScan 서버가 시도하는 최대 횟수를 입력합니다.
- **다시 시도 간격**: 알림 시도 간에 OfficeScan 서버에서 대기하는 시간(분)을 입력합니다.

4. **네트워크 트래픽**에서 다음 설정을 수정합니다.
   - **사용량이 보통인 시간대**: 네트워크 트래픽이 보통인 시간대를 나타내는 라디오 단추를 클릭합니다.
   - **사용량이 많지 않은 시간대**: 네트워크 트래픽이 가장 낮은 시간대를 나타내는 라디오 단추를 클릭합니다.
   - **사용량이 많은 시간대**: 네트워크 트래픽이 가장 높은 시간대를 나타내는 라디오 단추를 클릭합니다.
   - **최대 클라이언트 연결**: "기타 업데이트 소스" 및 OfficeScan 서버 모두에서 구성 요소를 동시에 업데이트할 수 있는 최대 클라이언트 수를 입력합니다. 각 시간에 대해 최대 클라이언트 수를 입력합니다. 최대 연결 수에 도달할 경우 OfficeScan 에이전트에서는 업데이트가 완료되거나 에이전트 응답이 **클라이언트 타임아웃** 또는 **업데이트 에이전트 타임아웃** 필드에 지정한 타임아웃 값에 도달하여 현재 에이전트 연결이 닫힌 후에만 구성 요소를 업데이트할 수 있습니다.
5. **확인**을 클릭합니다. OfficeScan Master Service를 다시 시작하라는 메시지가 나타납니다.

참고

컴퓨터가 아니라 서비스만 다시 시작합니다.

---

6. 다음 다시 시작 옵션에서 선택합니다.
   - 서버 튜너 설정을 저장하고 서비스를 다시 시작하려면 **예**를 클릭합니다. 설정은 다시 시작하는 즉시 적용됩니다.

- 서버 튜너 설정을 저장하지만 서비스를 다시 시작하지 않으려면 **아니요**를 클릭합니다. OfficeScan Master Service를 다시 시작하거나 설정을 적용할 OfficeScan 서버 컴퓨터를 다시 시작합니다.

Smart Feedback

Trend Micro Smart Feedback은 익명의 위협 정보를 스마트 보호 네트워크에서 공유하여 Trend Micro가 새로운 위협을 신속하게 식별하고 처리할 수 있습니다. 이 콘솔을 통해 언제든지 Smart Feedback을 사용하지 않도록 설정할 수 있습니다.

Smart Feedback 프로그램 참여

절차

1. **관리** > **스마트 보호** > **Smart Feedback**으로 이동합니다.
2. **Trend Micro Smart Feedback 사용**을 클릭합니다.
3. Trend Micro가 사용자의 조직을 이해할 수 있도록 **업계** 유형을 선택합니다.
4. OfficeScan 에이전트에서 파일의 잠재적인 보안 위협에 대한 정보를 보내려면 **의심스러운 프로그램 파일의 피드백 사용** 확인란을 선택합니다.

   참고

   Smart Feedback으로 보낸 파일에는 사용자 데이터가 포함되지 않으며 위협 분석용으로만 제출됩니다.

5. 피드백을 보내기 위한 기준을 구성하기 위해 피드백을 트리거하는 특정 시간 동안의 탐지 수를 선택합니다.
6. 네트워크 중단을 최소화하기 위해 피드백을 보낼 때 OfficeScan이 사용할 수 있는 최대 대역폭을 지정합니다.
7. **저장**을 클릭합니다.

장 15

OfficeScan 에이전트 관리

이 장에서는 OfficeScan 에이전트 관리 및 구성에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- 엔드포인트 위치 페이지 15-2
- OfficeScan 에이전트 프로그램 관리 페이지 15-6
- 에이전트-서버 연결 페이지 15-26
- OfficeScan 에이전트 프록시 설정 페이지 15-47
- OfficeScan 에이전트 정보 보기 페이지 15-52
- 에이전트 설정 가져오기 및 내보내기 페이지 15-53
- 보안 준수 페이지 15-55
- Trend Micro 가상 데스크톱 지원 페이지 15-73
- 글로벌 에이전트 설정 페이지 15-86
- 에이전트 권한 및 기타 설정 구성 페이지 15-88

엔드포인트 위치

OfficeScan에서는 OfficeScan 에이전트의 위치가 내부인지 또는 외부인지 확인하는 위치 인식 기능을 제공합니다. 위치 인식은 다음과 같은 OfficeScan 기능 및 서비스에서 활용됩니다.

표 15-1. 위치 인식을 활용하는 기능 및 서비스

FEATURE/ SERVICE	설명
웹 검증 서비스	OfficeScan 에이전트의 위치에 따라 OfficeScan 에이전트에서 적용할 웹 검증 정책이 결정됩니다. 관리자는 일반적으로 외부 에이전트에 대해 더 엄격한 정책을 적용합니다. 웹 검증 정책에 대한 자세한 내용은 웹 검증 정책 페이지 12-5을 참조하십시오.
파일 검증 서비스	스마트 스캔을 사용하는 에이전트의 경우 OfficeScan 에이전트의 위치에 따라 에이전트에서 검색 쿼리를 보낼 스마트 보호 소스가 결정됩니다. 외부 OfficeScan 에이전트는 스마트 보호 네트워크에 검색 쿼리를 보내는 반면, 내부 에이전트는 스마트 보호 소스 목록에 정의된 소스에 쿼리를 보냅니다. 스마트 보호 소스에 대한 자세한 내용은 스마트 보호 소스 페이지 4-5을 참조하십시오.
데이터 손실 방지	OfficeScan 에이전트의 위치에 따라 에이전트에서 적용할 데이터 손실 방지 정책이 결정됩니다. 관리자는 일반적으로 외부 에이전트에 대해 더 엄격한 정책을 적용합니다. 데이터 손실 방지 정책에 대한 자세한 내용은 데이터 손실 방지 정책 페이지 11-3을 참조하십시오.
장치 제어	OfficeScan 에이전트의 위치에 따라 에이전트에서 적용할 장치 제어 정책이 결정됩니다. 관리자는 일반적으로 외부 에이전트에 대해 더 엄격한 정책을 적용합니다. 장치 제어 정책에 대한 자세한 내용은 장치 제어 페이지 10-2를 참조하십시오.

위치 기준

위치가 OfficeScan 에이전트 엔드포인트의 게이트웨이 IP 주소를 기반으로 하는지, 아니면 OfficeScan 서버 또는 다른 참조 서버와의 OfficeScan 에이전트 연결 상태를 기반으로 하는지를 지정합니다.

- **에이전트 연결 상태**: OfficeScan 에이전트를 OfficeScan 서버 또는 인트라넷의 할당된 참조 서버와 연결할 수 있는 경우 엔드포인트의 위치는 내부가 됩니다. 또한, 기업 네트워크 외부의 엔드포인트가 OfficeScan 서버/참조 서버와 연결을 설정할 수 있는 경우, 이 엔드포인트의 위치 또한 내부입니다. 이러한 조건 중 아무 것도 적용되지 않으면 해당 엔드포인트 위치는 외부가 됩니다.
- **게이트웨이 IP 및 MAC 주소**: OfficeScan 에이전트 엔드포인트의 게이트웨이 IP 주소가 **엔드포인트 위치** 화면에서 지정한 게이트웨이 IP 주소와 일치하는 경우, 엔드포인트의 위치는 내부입니다. 그렇지 않으면 엔드포인트의 위치는 외부입니다.

위치 설정 구성

절차

1. **에이전트** > **엔드포인트 위치**로 이동합니다.
2. 위치가 **에이전트 연결 상태**를 기반으로 하는지 아니면 **게이트웨이 IP 및 MAC 주소**를 기반으로 하는지를 선택합니다.
3. **에이전트 연결 상태**를 선택하는 경우, 참조 서버를 사용할지를 결정합니다.

   자세한 내용은 참조 서버 페이지 14-33를 참조하십시오.

   a. 참조 서버를 지정하지 않을 경우 OfficeScan 에이전트는 다음 이벤트가 발생할 때 OfficeScan 서버와의 연결 상태를 확인합니다.

      - OfficeScan 에이전트가 독립 모드에서 일반(온라인/오프라인) 모드로 전환될 때
      - OfficeScan 에이전트의 검색 방법이 전환될 때.

자세한 내용은 검색 방법 유형 페이지 7-8를 참조하십시오.

- OfficeScan 에이전트가 엔드포인트에 대해 IP 주소 변경을 감지할 때.
- OfficeScan 에이전트가 다시 시작됩니다.
- 서버가 연결 확인을 시작할 때

  자세한 내용은 OfficeScan 에이전트 아이콘 페이지 15-26를 참조하십시오.
- 웹 검증 위치 기준이 글로벌 설정을 적용하는 동안 변경될 때
- 바이러스 사전 방역 정책이 더 이상 적용되지 않고 사전 방역 설정이 복원될 때

b. 참조 서버를 지정한 경우 OfficeScan 에이전트는 OfficeScan 서버와의 연결 상태를 먼저 확인한 다음, OfficeScan 서버에 대한 연결이 실패할 경우 참조 서버와의 연결 상태를 확인합니다. OfficeScan 에이전트는 매시간 그리고 위에서 언급한 이벤트가 발생할 경우 연결 상태를 확인합니다.

4. **게이트웨이 IP 및 MAC 주소**를 선택하는 경우

a. 제공된 텍스트 상자에 게이트웨이 IPv4/IPv6 주소를 입력합니다.

b. MAC 주소를 입력합니다.

c. **추가**를 클릭합니다.

MAC 주소를 입력하지 않으면 OfficeScan은 지정된 IP 주소에 속한 모든 MAC 주소를 포함합니다.

d. 추가할 모든 게이트웨이 IP 주소가 포함될 때까지 a~c단계를 반복합니다.

e. 게이트웨이 설정 가져오기 도구를 사용하여 게이트웨이 설정 목록을 가져옵니다.

자세한 내용은 게이트웨이 설정 가져오기 페이지 15-5를 참조하십시오.

5. **저장**을 클릭합니다.

게이트웨이 설정 가져오기

OfficeScan은 사용할 웹 검증 정책 및 연결할 스마트 보호 소스를 결정하기 위해 엔드포인트의 위치를 확인합니다. OfficeScan에서 위치를 식별하는 방법 중 하나는 엔드포인트의 게이트웨이 IP 주소와 MAC 주소를 확인하는 것입니다.

엔드포인트 위치 화면에서 게이트웨이 설정을 구성하거나, 게이트웨이 설정 가져오기 도구를 사용하여 게이트웨이 설정 목록을 **엔드포인트 위치** 화면으로 가져옵니다.

게이트웨이 설정 가져오기 사용

절차

1. 게이트웨이 설정 목록이 포함된 텍스트 파일(.txt)을 준비합니다. 각 줄에 IPv4 또는 IPv6 주소를 입력하고 선택적으로 MAC 주소를 입력합니다.

   IP 주소와 MAC 주소는 쉼표로 구분합니다. 최대 항목 수는 4096입니다.

   예:

   ```
   10.1.111.222,00:17:31:06:e6:e7

   2001:0db7:85a3:0000:0000:8a2e:0370:7334

   10.1.111.224,00:17:31:06:e6:e7
   ```

2. 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩GatewaySettingsImporter로 이동합니다.

3. GSImporter.exe를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

   참고

   터미널 서비스에서는 게이트웨이 설정 가져오기 도구를 실행할 수 없습니다.

4. **게이트웨이 설정 가져오기** 화면에서 1단계에서 만든 파일을 찾아 **가져오기**를 클릭합니다.

5. **확인**을 클릭합니다.

   게이트웨이 설정이 **엔드포인트 위치** 화면에 표시되고 OfficeScan 서버가 해당 설정을 OfficeScan 에이전트에 배포합니다.

6. 모든 항목을 삭제하려면 **모두 지우기**를 클릭합니다.

   특정 항목만 삭제해야 하는 경우 **엔드포인트 위치** 화면에서 해당 항목을 제거합니다.

7. 설정을 파일로 내보내려면 **모두 내보내기**를 클릭한 후 파일 이름과 형식을 지정합니다.

OfficeScan 에이전트 프로그램 관리

다음 항목에서는 OfficeScan 에이전트 프로그램을 관리 및 보호하는 방법에 대해 설명합니다.

- OfficeScan 에이전트 서비스 페이지 15-7
- OfficeScan 에이전트 서비스 다시 시작 페이지 15-11
- OfficeScan 에이전트 자기 보호 페이지 15-12
- OfficeScan 에이전트 콘솔 액세스 제한 페이지 15-17
- OfficeScan 에이전트 종료 및 잠금 해제 페이지 15-18
- OfficeScan 에이전트 독립 모드 권한 페이지 15-19
- Agent Mover 페이지 15-22
- 비활성 OfficeScan 에이전트 페이지 15-25

OfficeScan 에이전트 서비스

OfficeScan 에이전트는 다음 표에 나열된 서비스를 실행합니다. 이러한 서비스의 상태는 Microsoft Management Console에서 확인할 수 있습니다.

표 15-2. OfficeScan 에이전트 서비스

서비스	제어되는 기능
Trend Micro 무단 변경 방지 서비스(TMBMSRV.exe)	• 동작 모니터링 • 장치 제어 • 인증된 안전한 소프트웨어 서비스
OfficeScan NT 방화벽 (TmPfw.exe)	OfficeScan 방화벽
OfficeScan 데이터 보호 서비스(dsagent.exe)	• 데이터 손실 방지 • 장치 제어
OfficeScan NT Listener(tmlisten.exe)	OfficeScan 에이전트와 OfficeScan 서버 간의 통신
OfficeScan NT 프록시 서비스(TmProxy.exe)	• 웹 검증 • POP3 메일 검색
OfficeScan NT RealTime Scan(ntrtscan.exe)	• 실시간 검색 • 예약 검색 • 수동 검색/지금 검색
OfficeScan Common Client Solution Framework(TmCCSF.exe)	고급 보호 서비스 • 브라우저 위협 방지 • 메모리 검색

다음 서비스는 강력한 보호 기능을 제공하지만 특히 시스템 집약적인 응용 프로그램을 실행하는 서버에서 모니터링 메커니즘이 시스템 리소스를 소모할 수 있습니다.

- Trend Micro 무단 변경 방지 서비스(TMBMSRV.exe)

- OfficeScan NT 방화벽(TmPfw.exe)
- OfficeScan 데이터 보호 서비스(dsagent.exe)

따라서 이러한 서비스는 서버 플랫폼(Windows Server 2003, Windows Server 2008 및 Windows Server 2012)에서 기본적으로 비활성화됩니다. 이러한 서비스를 사용하려는 경우 다음 사항에 주의합니다.

- 시스템 성능을 지속적으로 모니터링하고 성능 저하를 발견한 경우 필요한 조치를 취합니다.
- TMBMSRV.exe의 경우 시스템 집약적인 응용 프로그램을 동작 모니터링 정책에서 제외하면 서비스를 활성화할 수 있습니다. 시스템 집약적인 응용 프로그램은 성능 조정 도구를 사용하여 식별할 수 있습니다. 자세한 내용은 Trend Micro 성능 조정 도구 사용 페이지 15-10를 참조하십시오.

데스크톱 플랫폼의 경우 성능이 크게 저하되는 경우에만 서비스를 비활성화합니다.

웹 콘솔에서 에이전트 서비스 사용 또는 사용 안 함

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. Windows XP, Vista, 7, 8, 8.1 또는 10을 실행하는 OfficeScan 에이전트의 경우:
   a. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.

   참고

   루트 도메인이나 특정 도메인을 선택하는 경우 Windows 데스크톱 플랫폼을 실행하는 에이전트에만 설정이 적용됩니다. Windows Server 플랫폼을 실행하는 에이전트는 해당 도메인에 속한 경우에도 설정이 적용되지 않습니다.

   b. **설정** > **추가 서비스 설정**을 클릭합니다.
   c. 다음 섹션 아래의 확인란을 선택하거나 선택을 취소합니다.

- **무단 변경 방지 서비스**
- **방화벽 서비스**
- **의심스러운 연결 서비스**
- **데이터 보호 서비스**
- **고급 보호 서비스**

d. **저장**을 클릭하여 설정을 도메인에 적용합니다. 루트 도메인 아이콘을 선택한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 Windows 데스크톱 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 Windows 데스크톱 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

3. Windows Server 플랫폼을 실행하는 OfficeScan 에이전트의 경우:

a. 에이전트 트리에서 단일 도메인을 선택합니다.

b. **설정** > **추가 서비스 설정**을 클릭합니다.

c. 다음 섹션 아래의 확인란을 선택하거나 선택을 취소합니다.

- **무단 변경 방지 서비스**
- **방화벽 서비스**
- **의심스러운 연결 서비스**
- **데이터 보호 서비스**
- **고급 보호 서비스**

d. **저장**을 클릭합니다.

Trend Micro 성능 조정 도구 사용

절차

1. 다음 위치에서 Trend Micro 성능 조정 도구를 다운로드합니다.

   http://esupport.trendmicro.com/solution/en-us/1056425.aspx

2. TMPerfTool.zip의 압축을 풀어 TMPerfTool.exe를 추출합니다.

3. TMPerfTool.exe를 <에이전트 설치 폴더> 또는 TMBMCLI.dll과 같은 폴더에 둡니다.

4. TMPerfTool.exe를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

5. 사용권 계약을 읽고 동의한 후 **확인**을 클릭합니다.

6. **분석**을 클릭합니다.

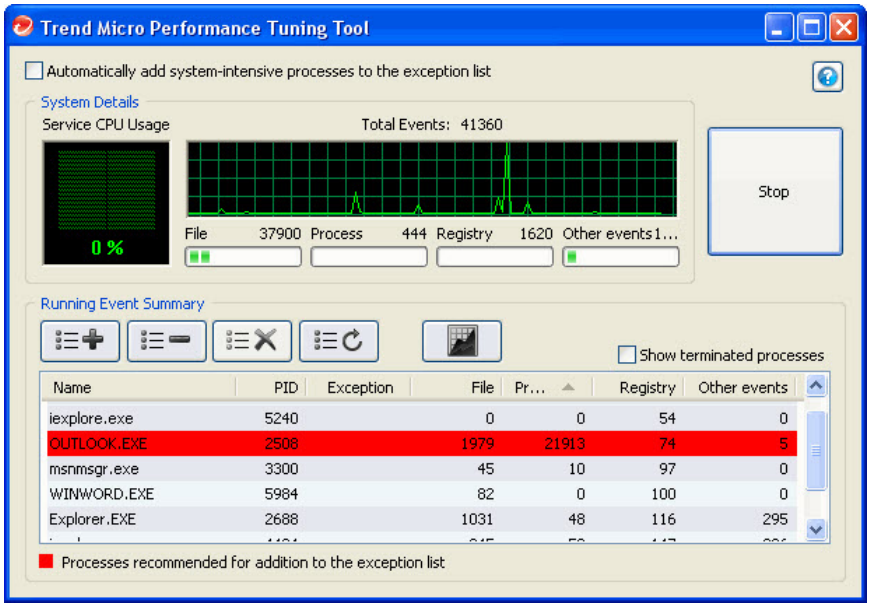


그림 15-1. 강조 표시된 시스템 집약적인 프로세스

도구가 CPU 사용량 및 이벤트 로드를 모니터링하기 시작합니다. 시스템 집약적인 프로세스는 빨간색으로 강조 표시됩니다.

7. 시스템 집약적인 프로세스를 선택하고 **예외 목록에 추가(허용)** 단추( )를 클릭합니다.
8. 시스템 또는 응용 프로그램 성능이 향상되는지 확인합니다.
9. 성능이 향상된 경우 프로세스를 다시 선택하고 **예외 목록에서 제거** 단추( )를 클릭합니다.
10. 성능이 다시 저하되면 다음 단계를 수행합니다.
    a. 응용 프로그램의 이름을 확인합니다.
    b. **중지**를 클릭합니다.
    c. **보고서 생성** 단추( )를 클릭하고 .xml 파일을 저장합니다.
    d. 충돌하는 것으로 식별된 응용 프로그램을 검토하여 동작 모니터링 예외 목록에 추가합니다.

    자세한 내용은 동작 모니터링 예외 목록 페이지 9-9를 참조하십시오.

OfficeScan 에이전트 서비스 다시 시작

OfficeScan은 정상적인 시스템 프로세스에 의해 중지되지 않고 예기치 않게 응답이 중지된 OfficeScan 에이전트 서비스를 다시 시작합니다. 에이전트 서비스에 대한 자세한 내용은 OfficeScan 에이전트 서비스 페이지 15-7를 참조하십시오.

OfficeScan 에이전트 서비스를 다시 시작하는 데 필요한 설정을 구성합니다.

서비스 다시 시작 설정 구성

절차

1. **에이전트 > 글로벌 에이전트 설정**으로 이동합니다.

2. **시스템** 탭을 클릭합니다.
3. **서비스 다시 시작** 섹션으로 이동합니다.
4. **서비스가 예기치 않게 종료된 경우 OfficeScan 에이전트 서비스를 자동으로 다시 시작**을 선택합니다.
5. 다음을 구성합니다.
   - **다음 시간 이후에 서비스 다시 시작 __분**: OfficeScan에서 서비스를 다시 시작하기 전에 경과해야 하는 시간(분)을 지정합니다.
   - **서비스를 다시 시작하는 첫 번째 시도가 실패하는 경우, 재시도 __번**: 서비스를 다시 시작하기 위한 최대 재시도 횟수를 지정합니다. 최대 재시도 횟수 이후 계속 중지된 상태인 경우, 수동으로 서비스를 다시 시작합니다.
   - **_시간 후 다시 시작 실패 수 초기화**: 최대 재시도 횟수 수행 이후 서비스가 계속 중지된 상태인 경우, OfficeScan은 실패 횟수를 초기화하기 위해 특정 시간(시간) 동안 기다립니다. 해당 시간이 경과한 이후 서비스가 계속 중지된 상태인 경우, OfficeScan이 서비스를 다시 시작합니다.

OfficeScan 에이전트 자기 보호

OfficeScan 에이전트 자기 보호를 통해 OfficeScan 에이전트는 올바로 작동하는 데 필요한 프로세스 및 기타 리소스를 보호할 수 있습니다. OfficeScan 에이전트 자기 보호 기능은 프로그램 또는 실제 사용자가 악성 프로그램 방지 기능을 해제하려고 시도하는 경우 이를 차단합니다.

OfficeScan 에이전트 자기 보호 기능은 다음 옵션을 제공합니다.

- OfficeScan 에이전트 서비스 보호 페이지 15-13
- OfficeScan 에이전트 설치 폴더의 파일 보호 페이지 15-14
- OfficeScan 에이전트 레지스트리 키 보호 페이지 15-15
- OfficeScan 에이전트 프로세스 보호 페이지 15-16

OfficeScan 에이전트 자기 보호 설정 구성

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭하고 **OfficeScan 에이전트 자기 보호** 섹션으로 이동합니다.
5. 다음 옵션을 사용하도록 설정합니다.
   - OfficeScan 에이전트 서비스 보호 페이지 15-13
   - OfficeScan 에이전트 설치 폴더의 파일 보호 페이지 15-14
   - OfficeScan 에이전트 레지스트리 키 보호 페이지 15-15
   - OfficeScan 에이전트 프로세스 보호 페이지 15-16
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트 서비스 보호

OfficeScan은 다음 OfficeScan 에이전트 서비스를 종료하려는 시도를 모두 차단합니다.

- OfficeScan NT Listener (TmListen.exe)
- OfficeScan NT RealTime Scan (NTRtScan.exe)
- OfficeScan NT Proxy Service (TmProxy.exe)
- OfficeScan NT Firewall (TmPfw.exe)
- OfficeScan Data Protection Service (dsagent.exe)
- Trend Micro Unauthorized Change Prevention Service (TMBMSRV.exe)

참고

이 옵션을 사용하면 OfficeScan에서 타사 제품이 엔드포인트에 설치되는 것을 차단할 수 있습니다. 이 문제가 발생한 경우 일시적으로 옵션을 해제한 다음 타사 제품을 설치한 후 다시 설정하십시오.

- Trend Micro 일반 클라이언트 솔루션 프레임워크(TmCCSF.exe)

OfficeScan 에이전트 설치 폴더의 파일 보호

다른 프로그램 및 사용자가 OfficeScan 에이전트 파일을 수정하거나 삭제하지 못하도록 OfficeScan에서는 향상된 여러 보호 기능을 제공합니다.

OfficeScan 에이전트 설치 폴더의 파일 보호를 사용하도록 설정하면 OfficeScan이 루트 <에이전트 설치 폴더>에서 다음 파일을 잠급니다.

- 확장자가 .exe, .dll 및 .sys인 디지털 서명된 모든 파일
- 다음을 비롯한 디지털 서명이 없는 일부 파일

- bspatch.exe
- bzip2.exe
- INETWH32.dll
- libcurl.dll
- libeay32.dll
- libMsgUtilExt.mt.dll
- msvcm80.dll
- MSVCP60.DLL
- msvcp80.dll
- msvcr80.dll
- OfceSCV.dll
- OFCESCVPack.exe
- patchbld.dll
- patchw32.dll
- patchw64.dll
- PiReg.exe
- ssleay32.dll
- Tmeng.dll
- TMNotify.dll
- zlibwapi.dll

OfficeScan 에이전트 설치 폴더의 파일 보호 및 바이러스/악성 프로그램 위협 실시간 검색을 사용하도록 설정하면 OfficeScan에서 다음 작업을 수행합니다.

- 설치 폴더에서 .exe 파일을 시작하기 전에 파일 무결성 검사

  액티브업데이트 업데이트 동안 OfficeScan은 업데이트를 트리거하는 파일 발급자가 Trend Micro인지 확인합니다. 발급자가 Trend Micro로 인식되지 않고 액티브업데이트가 잘못된 파일을 대체할 수 없는 경우 OfficeScan에서는 Windows 이벤트 로그에 발생을 기록하고 업데이트를 차단합니다.

- DLL 공격 차단

  일부 악성 프로그램 작성자는 에이전트가 동적 링크 라이브러리 파일을 로드하기 전에 이 파일을 로드할 목적으로 동적 링크 라이브러리 파일을 OfficeScan 에이전트 설치 폴더나 동작 모니터링 폴더에 복사합니다. 이러한 파일은 OfficeScan에서 제공하는 보호 기능을 중단하려고 합니다. 공격 파일이 OfficeScan 에이전트 폴더에 복사되지 않도록 OfficeScan에서는 설치 폴더 및 동작 모니터링 폴더에 파일이 복사되지 않도록 차단합니다.

- Windows의 "SHARE:NONE" 설정을 사용하여 파일 잠금 차단

OfficeScan 에이전트 레지스트리 키 보호

OfficeScan은 다음 레지스트리 키 및 하위 키 아래의 새로운 항목을 수정, 삭제 또는 추가하기 위한 모든 시도를 차단합니다.

- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\NSC
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Osprey
- HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\AMSP

OfficeScan 에이전트 프로세스 보호

OfficeScan에서는 다음 표의 프로세스를 종료하려는 모든 시도를 차단합니다.

프로세스	설명
TmListen.exe	OfficeScan 서버에서 명령과 알림을 수신하고 OfficeScan 에이전트와 서버 간의 통신을 용이하게 합니다.
NTRtScan.exe	OfficeScan 에이전트에서 실시간, 예약 및 수동 검색을 수행합니다.
TmProxy.exe	대상 응용 프로그램에 전달하기 전에 네트워크 트래픽을 검색합니다.
TmPfw.exe	패킷 수준 방화벽, 네트워크 바이러스 검색 및 침입 탐지 기능을 제공합니다.
TMBMSRV.exe	외부 저장소 장치에 대한 액세스를 조정하고 레지스트리 키 및 프로세스에 대한 무단 변경을 방지합니다.
DSAgent.exe	중요한 데이터의 전송을 모니터링하고 장치에 대한 액세스를 제어합니다.
PccNTMon.exe	이 프로세스는 OfficeScan 에이전트 콘솔을 시작합니다.
TmCCSF.exe	브라우저 위협 방지 및 메모리 검색을 수행합니다.

OfficeScan은 Microsoft 소프트웨어 제한 정책(SRP)의 프로세스 추가로부터 보호할 수도 있습니다. 소프트웨어 제한 정책은 나열된 응용 프로그램을 엔드포인트에서 실행하지 못하도록 합니다. 소프트웨어 제한 정책 목록의 OfficeScan 프로세스 추가를 제한하려면

1. **OfficeScan 에이전트 프로세스 보호**를 사용하도록 설정합니다.

2. **무단 변경 방지 서비스**를 사용하도록 설정합니다.

   자세한 내용은 웹 콘솔에서 에이전트 서비스 사용 또는 사용 안 함 페이지 15-8를 참조하십시오.

OfficeScan 에이전트 콘솔 액세스 제한

이 설정을 지정하면 시스템 트레이 또는 Windows 시작 메뉴에서 OfficeScan 에이전트 콘솔에 액세스할 수 없습니다. 사용자는 <에이전트 설치 폴더>에서 PccNTMon.exe를 두 번 클릭하는 방법으로만 OfficeScan 에이전트 콘솔에 액세스할 수 있습니다. 이 설정을 구성한 후 OfficeScan 에이전트를 다시 로드해야 설정이 적용됩니다.

이 설정으로 OfficeScan 에이전트를 사용할 수 없게 되지는 않습니다. OfficeScan 에이전트는 백그라운드에서 실행되면서 보안 위험으로부터 계속 보호해줍니다.

OfficeScan 에이전트 콘솔에 대한 액세스 제한

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘()을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **기타 설정** 탭을 클릭하고 **OfficeScan 에이전트 액세스 제한** 섹션으로 이동합니다.
5. **사용자가 시스템 트레이 또는 Windows 시작 메뉴에서 OfficeScan 에이전트 콘솔에 액세스할 수 없음**을 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

- **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트 종료 및 잠금 해제

OfficeScan 에이전트 종료 및 잠금 해제 권한을 통해 사용자는 암호 사용 여부에 관계없이 OfficeScan 에이전트를 일시적으로 중지하거나 고급 웹 콘솔 기능에 액세스할 수 있습니다.

에이전트 종료 및 잠금 해제 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **종료 및 잠금 해제** 섹션으로 이동합니다.
5. 암호 없이 OfficeScan 에이전트를 종료할 수 있도록 허용하려면 **암호 필요 없음**을 선택합니다.
   - 암호가 필요한 경우 **암호 필요**를 선택하고 암호를 입력한 후 확인합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.

- **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트 독립 모드 권한

에이전트-서버 이벤트가 특정 사용자의 작업에 방해가 되는 경우 이 사용자에게 OfficeScan 에이전트 독립 모드 권한을 부여합니다. 예를 들어 프레젠테이션을 자주 진행하는 사용자는 프레젠테이션을 시작하기 전에 독립 모드를 설정하여 OfficeScan 서버에서 OfficeScan 에이전트 설정 배포 및 OfficeScan 에이전트 검색을 시작하지 않도록 합니다.

OfficeScan 에이전트가 독립 모드인 경우:

- OfficeScan 에이전트는 서버와 에이전트가 기능적으로 연결되어 있는 경우에도 OfficeScan 서버에 로그를 보내지 않습니다.
- OfficeScan 서버는 서버와 에이전트가 기능적으로 연결되어 있는 경우에도 작업을 시작하지 않고 OfficeScan 에이전트 설정을 에이전트에 배포하지 않습니다.
- OfficeScan 에이전트는 업데이트 소스에 연결할 수 있는 경우 구성 요소를 업데이트합니다. 소스에는 OfficeScan 서버, 업데이트 에이전트 또는 사용자 지정 업데이트 소스가 포함됩니다.

  독립 에이전트에서 업데이트를 트리거하는 이벤트는 다음과 같습니다.

  - 사용자가 수동 업데이트를 수행하는 경우
  - 자동 에이전트 업데이트가 실행되는 경우. 독립 에이전트에서 자동 에이전트 업데이트를 사용하지 않도록 설정할 수 있습니다.

    자세한 내용은 독립 에이전트에서 자동 에이전트 업데이트 사용 안 함 페이지 15-20를 참조하십시오.

  - 예약 업데이트가 실행되는 경우. 필요한 권한이 있는 에이전트만 예약 업데이트를 실행할 수 있습니다. 이 권한은 언제든지 취소할 수 있습니다.

자세한 내용은 독립 에이전트에서 예약 업데이트 권한 취소 페이지 15-21를 참조하십시오.

에이전트 독립 모드 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **독립 모드** 섹션으로 이동합니다.
5. **독립 모드 사용**을 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

독립 에이전트에서 자동 에이전트 업데이트 사용 안 함

절차

1. **업데이트** > **에이전트** > **자동 업데이트**로 이동합니다.
2. **이벤트에 따른 업데이트** 섹션으로 이동합니다.
3. **독립 및 오프라인 에이전트 포함**을 사용하지 않도록 설정합니다.

참고

이 옵션은 **OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 에이전트에서 구성 요소 업데이트 시작**을 사용하지 않도록 설정한 경우 자동으로 해제됩니다.

독립 에이전트에서 예약 업데이트 권한 취소

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하거나 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **구성 요소 업데이트** 섹션으로 이동합니다.
5. **일정에 따른 업데이트 사용/사용 안 함** 옵션의 선택을 취소합니다.
6. **저장**을 클릭합니다.

OfficeScan 에이전트 언어 구성

OfficeScan 서버 언어 설정이나 로컬로 로그온된 사용자 언어 설정을 사용하여 표시하도록 모든 OfficeScan 에이전트를 구성할 수 있습니다. OfficeScan 에이전트 프로그램을 설치하거나 업그레이드하면 에이전트는 **글로벌 설정** 화면에서 구성된 언어 설정을 적용합니다.

기본적으로, OfficeScan 에이전트에서 로그온된 사용자 언어 설정을 지원하지 않는 경우 언어 설정은 OfficeScan 서버 언어로 기본 설정되며, 이 서버 언어도 지원하지 않는 경우에는 영어로 설정됩니다.

OfficeScan 에이전트 언어 설정 구성

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **에이전트 제어** 탭을 클릭합니다.
3. **에이전트 언어 구성** 섹션으로 이동합니다.
4. OfficeScan 에이전트에서 언어 설정을 적용하는 방식을 지정합니다.
   - **엔드포인트에서 로컬 언어 설정**: OfficeScan 에이전트가 로그온된 사용자의 언어 설정을 사용하여 표시됩니다.

     참고

     OfficeScan 에이전트에서 로그온된 사용자 언어 설정을 지원하지 않는 경우 에이전트가 OfficeScan 서버 언어를 적용합니다. 엔드포인트에서 OfficeScan 서버 언어를 지원하지 않는 경우에는 영어로 표시됩니다.
   - **OfficeScan 서버 언어**: OfficeScan 에이전트가 OfficeScan 서버 언어를 사용하여 표시됩니다.

     참고

     엔드포인트에서 OfficeScan 서버 언어를 지원하지 않는 경우에는 영어로 표시됩니다.
5. **저장**을 클릭합니다.

Agent Mover

네트워크에 OfficeScan 서버가 둘 이상인 경우 Agent Mover 도구를 사용하여 OfficeScan 서버 간에 OfficeScan 에이전트를 전송할 수 있습니다. 이 도구는 네트워크에 새 OfficeScan 서버를 추가한 후 기존 OfficeScan 에이전트를 새 서버로 전송하려는 경우에 특히 유용합니다.

참고

두 서버는 언어 버전이 같아야 합니다. Agent Mover를 사용하여 이전 버전을 실행하는 OfficeScan 에이전트를 현재 버전의 서버로 이동한 경우 해당 OfficeScan 에이전트가 자동으로 업그레이드됩니다.

이 도구를 사용하려면 사용하는 계정에 관리자 권한이 있어야 합니다.

Agent Mover 실행

절차

1. OfficeScan 서버에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩IpXfer로 이동합니다.
2. IpXfer.exe를 OfficeScan 에이전트 엔드포인트에 복사합니다. OfficeScan 에이전트 엔드포인트가 x64 유형 플랫폼을 실행하는 경우에는 대신 IpXfer_x64.exe를 복사합니다.
3. OfficeScan 에이전트 엔드포인트에서 명령 프롬프트를 연 다음 실행 파일을 복사한 폴더로 이동합니다.
4. 다음 구문을 사용하여 Agent Mover를 실행합니다.

   ```
   <실행 파일 이름> -s <서버 이름> -p <서버 수신 포트> -c <에이전트 수신 포트> -d <도메인 또는 도메인 계층> -e <인증서 위치 및 파일 이름> -pwd <에이전트 종료 및 잠금 해제 권한 암호>
   ```

표 15-3. Agent Mover 매개 변수

매개 변수	설명
`<실행 파일 이름>`	IpXfer.exe 또는 IpXfer_x64.exe
`-s <서버 이름>`	대상 OfficeScan 서버(OfficeScan 에이전트가 전송되는 서버)의 이름입니다.
`-p <서버 수신 포트>`	대상 OfficeScan 서버의 수신 포트(또는 트러스트된 포트) OfficeScan 웹 콘솔에서 수신 포트를 확인하려면 기본 메뉴에서 **관리** > **설정** > **에이전트 연결**을 클릭합니다.

매개 변수	설명
-c <에이전트 수신 포트>	OfficeScan 에이전트 엔드포인트에서 서버와 통신하는 데 사용하는 포트 번호
-d <도메인 또는 도메인 계층>	에이전트를 그룹화할 에이전트 트리 도메인 또는 하위 도메인 도메인 계층은 하위 도메인을 나타냅니다.
-e <인증서 위치 및 파일 이름>	이동하는 동안 OfficeScan 에이전트에 대한 새 인증 인증서를 가져옵니다. 이 매개 변수를 사용하지 않는 경우 OfficeScan 에이전트에서는 해당 새 관리 서버에서 현재 인증 인증서를 자동으로 검색합니다. **참고** OfficeScan 서버의 기본 인증서 위치는 다음과 같습니다. <서버 설치 폴더>₩PCCSRV₩Pccnt₩Common ₩OfcNTCer.dat. OfficeScan이 아닌 소스의 인증서를 사용하는 경우 인증서가 DER(Distinguished Encoding Rules) 포맷인지 확인합니다.
-pwd <에이전트 종료 및 잠금 해제 권한 암호>	권한 및 기타 설정에 구성된 종료 및 잠금 해제 권한 암호 **참고** 종료 및 잠금 해제 암호가 필요하지만 암호를 제공하지 않은 경우 Agent Mover가 에이전트 이동을 시도하기 전에 암호를 입력하라는 메시지를 표시합니다.

예:

```
ipXfer.exe -s Server01 -p 8080 -c 21112 -d Workgroup -pwd
unlock
```

```
ipXfer_x64.exe -s Server02 -p 8080 -c 21112 -d Workgroup
\Group01 -pwd unlock
```

5. OfficeScan 에이전트가 이제 다른 서버에 보고하는지 확인하려면 다음을 수행합니다.

   a. OfficeScan 에이전트 엔드포인트의 시스템 트레이에서 OfficeScan 에이전트 프로그램 아이콘을 마우스 오른쪽 단추로 클릭합니다.

   b. **구성 요소 버전**을 선택합니다.

   c. **서버 이름/포트** 필드에서 OfficeScan 에이전트가 보고하는 OfficeScan 서버를 확인합니다.

참고

OfficeScan 에이전트를 관리하는 새 OfficeScan 서버의 에이전트 트리에 해당 에이전트가 표시되지 않는 경우에는 새 서버의 Master Service(ofservice.exe)를 다시 시작합니다.

비활성 OfficeScan 에이전트

OfficeScan 에이전트 제거 프로그램을 사용하여 엔드포인트에서 OfficeScan 에이전트 프로그램을 제거하면 프로그램에서 서버에 자동으로 알립니다. 서버는 이 알림을 수신하면 에이전트 트리에서 OfficeScan 에이전트 아이콘을 제거하여 에이전트가 더 이상 없다고 표시합니다.

그러나 엔드포인트 하드 드라이브를 다시 포맷하거나 OfficeScan 에이전트 파일을 수동으로 삭제하는 등 다른 방법을 사용하여 OfficeScan 에이전트를 제거한 경우에는 OfficeScan에서 이 내용을 인식하지 못하므로 OfficeScan 에이전트가 비활성 상태로 표시됩니다. 사용자가 장시간 OfficeScan 에이전트를 종료하거나 사용하지 않도록 설정한 경우에도 서버에서는 OfficeScan 에이전트를 비활성 상태로 표시합니다.

에이전트 트리에 활성 에이전트만 표시하려면 에이전트 트리에서 비활성 에이전트를 자동으로 제거하도록 OfficeScan을 구성합니다.

비활성 에이전트 자동 제거

절차

1. **관리** > **설정** > **비활성 에이전트**로 이동합니다.
2. **비활성 에이전트 자동 제거 사용**을 선택합니다.
3. 며칠이 지나면 OfficeScan이 OfficeScan 에이전트를 비활성으로 간주할지를 선택합니다.
4. **저장**을 클릭합니다.

에이전트-서버 연결

OfficeScan 에이전트는 구성 요소를 업데이트하고, 알림을 받고, 구성 변경 사항을 적시에 적용할 수 있도록 해당 상위 서버와의 지속적인 연결을 유지해야 합니다. 다음 항목에서는 OfficeScan 에이전트의 연결 상태를 확인하고 연결 문제를 해결하는 방법에 대해 알아봅니다.

- 에이전트 IP 주소 페이지 5-10
- OfficeScan 에이전트 아이콘 페이지 15-26
- 에이전트-서버 연결 확인 페이지 15-41
- 연결 확인 로그 페이지 15-42
- 연결할 수 없는 에이전트 페이지 15-42

OfficeScan 에이전트 아이콘

시스템 트레이의 OfficeScan 에이전트 아이콘은 OfficeScan 에이전트의 현재 상태를 나타내고 사용자에게 특정 작업을 수행하도록 알려 주는 시각적 힌트를 제공합니다. 지정된 시간에 다음과 같은 시각적 힌트 조합이 아이콘에 표시됩니다.

표 15-4. OfficeScan 에이전트 아이콘으로 표시되는 OfficeScan 에이전트 상태

에이전트 상태	설명	시각적 힌트
에이전트와 OfficeScan 서버의 연결	온라인 에이전트가 OfficeScan 서버에 연결되었습니다. 서버에서 이러한 에이전트에 대해 작업을 시작하고 설정을 배포할 수 있습니다.	아이콘에 하트비트와 유사한 기호가 포함됩니다. 배경색은 실시간 검색 서비스의 상태에 따라 파란색 또는 빨간색 음영입니다.
	오프라인 에이전트와 OfficeScan 서버의 연결이 끊어졌습니다. 이러한 에이전트는 서버에서 관리할 수 없습니다.	아이콘에 끊어진 하트비트와 유사한 기호가 포함됩니다. 배경색은 실시간 검색 서비스의 상태에 따라 파란색 또는 빨간색 음영입니다. 에이전트는 네트워크에 연결된 경우에도 오프라인 상태가 될 수 있습니다. 이 문제에 대한 자세한 내용은 OfficeScan 에이전트 아이콘에 표시된 문제 해결 페이지 15-38을 참조하십시오.
	독립 에이전트가 OfficeScan 서버와 통신할 수도 있고 그렇지 않을 수도 있습니다.	아이콘에 데스크톱 및 신호 기호가 포함됩니다. 배경색은 실시간 검색 서비스의 상태에 따라 파란색 또는 빨간색 음영입니다. 독립 모드 에이전트에 대한 자세한 내용은 OfficeScan 에이전트 독립 모드 권한 페이지 15-19 항목을 참조하십시오.

에이전트 상태	설명	시각적 힌트
스마트 보호 소스의 가용성	스마트 보호 소스에 스마트 보호 서버 및 Trend Micro 스마트 보호 네트워크가 포함되어 있습니다. 표준 스캔 에이전트는 웹 검증 쿼리를 위해 스마트 보호 소스에 연결합니다. 스마트 스캔 에이전트는 검색 및 웹 검증 쿼리를 위해 스마트 보호 소스에 연결합니다.	스마트 보호 소스를 사용할 수 있는 경우 아이콘에 확인 표시가 포함됩니다.
		사용 가능한 스마트 보호 소스가 없는 경우 에이전트에서 소스와의 연결을 설정하려고 하면 아이콘에 진행률 표시줄이 포함됩니다. 이 문제에 대한 자세한 내용은 OfficeScan 에이전트 아이콘에 표시된 문제 해결 페이지 15-38을 참조하십시오.
		표준 스캔 에이전트의 경우 에이전트에서 웹 검증을 사용하지 않으면 확인 표시 또는 진행률 표시줄이 나타나지 않습니다.

에이전트 상태	설명	시각적 힌트
실시간 검색 서비스 상태	OfficeScan에서는 실시간 검색뿐 아니라 수동 검색 및 예약 검색에도 실시간 검색 서비스를 사용합니다. 이 서비스가 작동해야 합니다. 그렇지 않으면 에이전트가 보안 위험에 취약해집니다.	실시간 검색 서비스가 작동하는 경우에는 전체 아이콘이 파란색으로 음영 처리됩니다. 에이전트의 검색 방법을 나타내는 데 두 가지 파란색 음영이 사용됩니다. • 표준 스캔의 경우 • 스마트 스캔의 경우
		실시간 검색 서비스가 비활성화되거나 작동하는 경우에는 전체 아이콘이 빨간색으로 음영 처리됩니다. 에이전트의 검색 방법을 나타내는 데 두 가지 빨간색 음영이 사용됩니다. • 표준 스캔의 경우 • 스마트 스캔의 경우 이 문제에 대한 자세한 내용은 OfficeScan 에이전트 아이콘에 표시된 문제 해결 페이지 15-38을 참조하십시오.

에이전트 상태	설명	시각적 힌트
실시간 검색 상태	실시간 검색에서는 파일이 만들어지거나 수정되거나 검색될 때 보안 위험을 검색하여 예방 보호를 제공합니다.	실시간 검색을 사용하는 경우에는 시각적 힌트가 없습니다.
		실시간 검색을 사용하지 않는 경우에는 전체 아이콘이 빨간색 원으로 둘러싸이고 내부에 빨간색 대각선이 포함됩니다. 이 문제에 대한 자세한 내용은 OfficeScan 에이전트 아이콘에 표시된 문제 해결 페이지 15-38을 참조하십시오.
패턴 업데이트 상태	에이전트는 패턴을 정기적으로 업데이트하여 최신 위협을 방지해야 합니다.	패턴이 최신 상태이거나 약간 오래된 경우에는 시각적 힌트가 없습니다.
		패턴이 아주 오래된 경우에는 아이콘 안에 느낌표가 포함됩니다. 이는 패턴이 오랫동안 업데이트되지 않았음을 의미합니다. 에이전트를 업데이트하는 방법에 대한 자세한 내용은 OfficeScan 에이전트 업데이트 페이지 6-26를 참조하십시오.
OfficeScan 서버 평가판 라이센스 상태	온라인 에이전트가 만료된 평가판 라이센스를 사용 중인 OfficeScan 서버에 연결되었습니다.	이 아이콘은 OfficeScan 서버의 평가판 라이센스가 만료되었음을 나타냅니다.

스마트 스캔 아이콘

OfficeScan 에이전트에서 스마트 스캔을 사용하는 경우 다음 아이콘 중 하나가 표시됩니다.

표 15-5. 스마트 스캔 아이콘

아이콘	OfficeScan 서버와 연결	스마트 보호 소스의 가용성	실시간 검색 서비스	실시간 검색
	온라인	사용 가능	작동 중	사용
	온라인	사용 가능	작동 중	사용 안 함
	온라인	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음
	온라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용
	온라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함
	온라인	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음
	오프라인	사용 가능	작동 중	사용
	오프라인	사용 가능	작동 중	사용 안 함
	오프라인	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음
	오프라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용
	오프라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함
	오프라인	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음
	독립	사용 가능	작동 중	사용

아이콘	OfficeScan 서버와 연결	스마트 보호 소스의 가용성	실시간 검색 서비스	실시간 검색
	독립	사용 가능	작동 중	사용 안 함
	독립	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음
	독립	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용
	독립	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함
	독립	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음

표준 스캔 아이콘

OfficeScan 에이전트에서 표준 스캔을 사용하는 경우 다음 아이콘 중 하나가 표시됩니다.

표 15-6. 표준 스캔 아이콘

아이콘	OfficeScan 서버와 연결	스마트 보호 소스에서 제공하는 웹 검증 서비스	실시간 검색 서비스	실시간 검색	바이러스 패턴
	온라인	사용 가능	작동 중	사용	최신 또는 약간 오래됨
	온라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용	최신 또는 약간 오래됨
	온라인	사용 가능	작동 중	사용	매우 오래됨
	온라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용	매우 오래됨

아이콘	OfficeScan 서버와 연결	스마트 보호 소스에서 제공하는 웹 검증 서비스	실시간 검색 서비스	실시간 검색	바이러스 패턴
	온라인	사용 가능	작동 중	사용 안 함	최신 또는 약간 오래됨
	온라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함	최신 또는 약간 오래됨
	온라인	사용 가능	작동 중	사용 안 함	매우 오래됨
	온라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함	매우 오래됨
	온라인	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	온라인	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	온라인	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	온라인	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	오프라인	사용 가능	작동 중	사용	최신 또는 약간 오래됨
	오프라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용	최신 또는 약간 오래됨
	오프라인	사용 가능	작동 중	사용	매우 오래됨

아이콘	OfficeScan 서버와 연결	스마트 보호 소스에서 제공하는 웹 검증 서비스	실시간 검색 서비스	실시간 검색	바이러스 패턴
	오프라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용	매우 오래됨
	오프라인	사용 가능	작동 중	사용 안 함	최신 또는 약간 오래됨
	오프라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함	최신 또는 약간 오래됨
	오프라인	사용 가능	작동 중	사용 안 함	매우 오래됨
	오프라인	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함	매우 오래됨
	오프라인	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	오프라인	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	오프라인	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	오프라인	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	독립	사용 가능	작동 중	사용	최신 또는 약간 오래됨
	독립	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용	최신 또는 약간 오래됨

아이콘	OfficeScan 서버와 연결	스마트 보호 소스에서 제공하는 웹 검증 서비스	실시간 검색 서비스	실시간 검색	바이러스 패턴
	독립	사용 가능	작동 중	사용	매우 오래됨
	독립	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용	매우 오래됨
	독립	사용 가능	작동 중	사용 안 함	최신 또는 약간 오래됨
	독립	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함	최신 또는 약간 오래됨
	독립	사용 가능	작동 중	사용 안 함	매우 오래됨
	독립	사용할 수 없음, 소스에 다시 연결 중	작동 중	사용 안 함	매우 오래됨
	독립	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	독립	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	독립	사용 가능	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	독립	사용할 수 없음, 소스에 다시 연결 중	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	온라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용	최신 또는 약간 오래됨

아이콘	OfficeScan 서버와 연결	스마트 보호 소스에서 제공하는 웹 검증 서비스	실시간 검색 서비스	실시간 검색	바이러스 패턴
	온라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용	매우 오래됨
	온라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용 안 함	최신 또는 약간 오래됨
	온라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용 안 함	매우 오래됨
	온라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	온라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	오프라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용	최신 또는 약간 오래됨
	오프라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용	매우 오래됨
	오프라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용 안 함	최신 또는 약간 오래됨

아이콘	OfficeScan 서버와 연결	스마트 보호 소스에서 제공하는 웹 검증 서비스	실시간 검색 서비스	실시간 검색	바이러스 패턴
	오프라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용 안 함	매우 오래됨
	오프라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨
	오프라인	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨
	독립	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용	최신 또는 약간 오래됨
	독립	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용	매우 오래됨
	독립	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용 안 함	최신 또는 약간 오래됨
	독립	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	작동 중	사용 안 함	매우 오래됨
	독립	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	최신 또는 약간 오래됨

아이콘	OFFICESCAN 서버와 연결	스마트 보호 소스에서 제공하는 웹 검증 서비스	실시간 검색 서비스	실시간 검색	바이러스 패턴
	독립	해당 없음(에이전트에서 웹 검증 기능을 사용하지 않음)	사용 안 함 또는 작동하지 않음	사용 안 함 또는 작동하지 않음	매우 오래됨

OfficeScan 에이전트 아이콘에 표시된 문제 해결

OfficeScan 에이전트 아이콘이 다음과 같은 상태를 나타낼 경우 필요한 조치를 수행하십시오.

상태	설명
패턴 파일이 오랫동안 업데이트되지 않음	OfficeScan 에이전트 사용자가 구성 요소를 업데이트해야 합니다. 웹 콘솔에서 **업데이트** > **에이전트** > **자동 업데이트**를 통해 구성 요소 업데이트 설정을 구성하거나, **에이전트** > **에이전트 관리 > 설정** > **권한 및 기타 설정** > **권한(탭)** > **구성 요소 업데이트**를 통해 사용자에게 업데이트 권한을 부여합니다.
실시간 검색 서비스가 해제되었거나 작동하지 않음	실시간 검색 서비스(OfficeScan NT RealTime Scan)가 해제되었거나 작동하지 않는 경우 사용자는 Microsoft Management Console에서 서비스를 수동으로 시작해야 합니다.
실시간 검색 사용 안 함	웹 콘솔에서 실시간 검색을 사용하도록 설정합니다(**에이전트** > **에이전트 관리 > 설정** > **검색 설정** > **실시간 검색 설정**).
실시간 검색을 사용하지 않으며 OfficeScan 에이전트가 독립 모드임	먼저 독립 모드를 사용하지 않도록 설정해야 합니다. 독립 모드를 사용하지 않도록 설정한 후 웹 콘솔에서 실시간 검색을 사용하도록 설정합니다.
OfficeScan 에이전트가 네트워크에 연결되어 있지만 오프라인으로 표시됨	웹 콘솔에서 연결을 확인한 다음(**에이전트** > **연결 확인**) 연결 확인 로그(**로그** > **에이전트** > **연결 확인 로그**)를 검사합니다. 확인한 후에도 OfficeScan 에이전트가 여전히 오프라인 상태인 경우 다음을 수행합니다. 1. 서버와 OfficeScan 에이전트의 연결 상태가 모두 오프라인인 경우에는 네트워크 연결을 확인합니다.

상태	설명
	2. OfficeScan 에이전트의 연결 상태는 오프라인이지만 서버는 온라인 상태인 경우, 서버의 도메인 이름이 변경된 후에 OfficeScan 에이전트에서 이전 도메인 이름을 사용하여 서버에 연결하려고 했을 수 있습니다(서버 설치 중에 도메인 이름을 선택한 경우). OfficeScan 서버의 도메인 이름을 DNS 또는 WINS 서버에 등록하거나 도메인 이름과 IP 정보를 에이전트 엔드포인트의 다음 폴더에 있는 "hosts" 파일에 추가합니다. <Windows 폴더>₩system32₩drivers₩etc 3. OfficeScan 에이전트의 연결 상태가 온라인이지만 서버가 오프라인 상태인 경우에는 OfficeScan 방화벽 설정을 확인합니다. 방화벽이 서버에서 에이전트로 가는 통신을 차단하고 에이전트에서 서버로 가는 통신을 허용하는 경우일 수 있습니다. 4. OfficeScan 에이전트의 연결 상태는 온라인이지만 서버가 오프라인 상태인 경우에는 OfficeScan 에이전트의 IP 주소가 변경되었지만 해당 상태가 서버에 반영되지 않았을 수 있습니다(예: 에이전트가 다시 로드된 경우). OfficeScan 에이전트를 다시 배포해 봅니다.
스마트 보호 소스를 사용할 수 없음	에이전트와 스마트 보호 소스의 연결이 끊어진 경우 다음 작업을 수행합니다. 1. 웹 콘솔에서 **엔드포인트 위치** 화면(**에이전트** > **엔드포인트 위치**)으로 이동하여 다음 엔드포인트 위치 설정이 제대로 구성되었는지 확인합니다. • 참조 서버 및 포트 번호 • 게이트웨이 IP 주소 2. 웹 콘솔에서 스마트 보호 소스 화면(**관리** > **스마트 보호** > **스마트 보호 소스**)으로 이동하여 다음 작업을 수행합니다. a. 표준 또는 사용자 지정 목록의 스마트 보호 서버 설정이 올바른지 확인합니다. b. 서버에 대한 연결을 설정할 수 있는지 테스트합니다. c. 소스 목록을 구성한 후 **모든 에이전트에 알림**을 클릭합니다. 3. 스마트 보호 서버 및 OfficeScan 에이전트의 다음 구성 파일이 동기화되었는지 확인합니다. • sscfg.ini

상태	설명
	• ssnotify.ini 4. 레지스트리 편집기를 열고 에이전트가 기업 네트워크에 연결되었는지 확인합니다. 키: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\iCRC Scan\Scan Server` • LocationProfile=1인 경우 OfficeScan 에이전트가 네트워크에 연결되어 있으며 스마트 보호 서버에 연결할 수 있어야 합니다. • LocationProfile=2인 경우 OfficeScan 에이전트가 네트워크에 연결되어 있지 않으며 스마트 보호 네트워크에 연결해야 합니다. Internet Explorer에서 OfficeScan 에이전트 엔드포인트가 인터넷 웹 페이지를 검색할 수 있는지 확인합니다. 5. 스마트 보호 네트워크 및 스마트 보호 서버에 연결하는 데 사용된 내부 및 외부 프록시 설정을 확인합니다. 자세한 내용은 OfficeScan 에이전트용 내부 프록시 페이지 15-47 및 OfficeScan 에이전트용 외부 프록시 페이지 15-48를 참조하십시오. 6. Windows XP, Vista, Server 2003 및 Server 2008을 실행하는 표준 스캔 에이전트의 경우 OfficeScan NT Proxy Service(TmProxy.exe)가 실행되고 있는지 확인합니다. 이 서비스가 중지된 경우 에이전트에서 웹 검증을 위해 스마트 보호 소스에 연결할 수 없습니다. Windows 7, Server 2012 및 그 이상의 버전을 실행하는 표준 스캔 에이전트의 경우 tmusa 드라이버가 실행되고 있는지 확인합니다. 이 드라이버가 중지된 경우 에이전트에서 웹 검증을 위해 스마트 보호 소스에 연결할 수 없습니다.

에이전트-서버 연결 확인

OfficeScan 서버와 에이전트 연결 상태는 OfficeScan 웹 콘솔의 에이전트 트리에 표시됩니다.

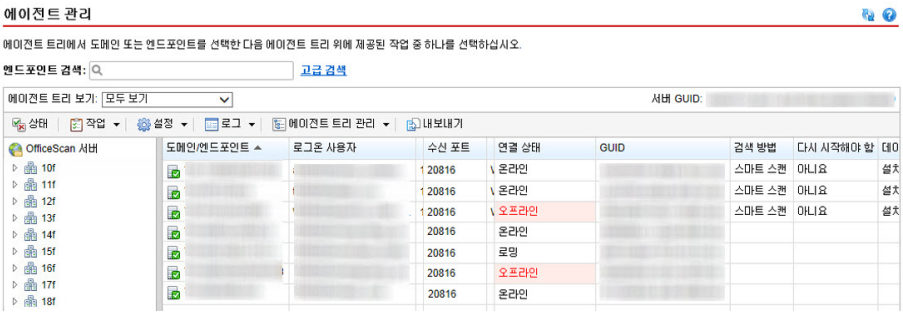


그림 15-2. OfficeScan 서버와 에이전트 연결 상태를 표시하는 에이전트 트리

특정 조건으로 인해 에이전트 트리에 에이전트 연결 상태가 올바로 표시되지 않을 수 있습니다. 예를 들어 에이전트 엔드포인트의 네트워크 케이블이 갑자기 끊어지면 에이전트가 오프라인 상태임을 서버에 알릴 수 없습니다. 이 에이전트는 에이전트 트리에서 계속 온라인 상태로 표시됩니다.

수동으로 에이전트-서버 연결을 확인하거나 OfficeScan이 예약 확인을 수행하도록 합니다. 특정 도메인이나 에이전트를 선택한 후 해당 연결 상태를 확인할 수는 없습니다. OfficeScan은 등록된 모든 에이전트의 연결 상태를 확인합니다.

에이전트-서버 연결 확인

절차

1. **에이전트** > **연결 확인**으로 이동합니다.
2. 에이전트-서버 연결을 수동으로 확인하려면 **수동 확인** 탭으로 이동하여 **지금 확인**을 클릭합니다.
3. 에이전트-서버 연결을 자동으로 확인하려면 **예약 확인** 탭으로 이동합니다.

a. **예약 확인 사용**을 선택합니다.

b. 확인 빈도와 시작 시간을 선택합니다.

c. **저장**을 클릭하여 확인 일정을 저장합니다.

4. 에이전트 트리에서 상태를 확인하거나 연결 확인 로그를 확인합니다.

연결 확인 로그

OfficeScan은 OfficeScan 서버가 등록된 모든 에이전트와 통신할 수 있는지 여부를 확인할 수 있도록 연결 확인 로그를 유지합니다. OfficeScan은 웹 콘솔에서 에이전트-서버 연결을 확인할 때마다 로그 항목을 만듭니다.

로그의 크기가 하드 디스크의 너무 많은 공간을 차지하지 않도록 방지하려면 수동으로 로그를 삭제하거나 로그 삭제 일정을 구성합니다. 로그 관리에 대한 자세한 내용은 로그 관리 페이지 14-39를 참조하십시오.

연결 확인 로그 보기

절차

1. **로그** > **에이전트** > **연결 확인 로그**로 이동합니다.
2. **상태** 열을 확인하여 연결 확인 결과를 표시합니다.
3. 로그를 쉼표로 구분된 값(CSV) 파일로 저장하려면 **CSV로 내보내기**를 클릭합니다. 파일을 열거나 특정 위치에 저장합니다.

연결할 수 없는 에이전트

연결할 수 없는 네트워크의 OfficeScan 에이전트(예: NAT 게이트웨이 뒤의 네트워크 세그먼트에 있는 에이전트)는 서버에서 에이전트에 직접 연결할 수 없으므로 거의 항상 오프라인 상태입니다. 따라서 서버가 에이전트에 다음 작업을 알릴 수 없습니다.

- 최신 구성 요소 다운로드
- 웹 콘솔에서 구성된 에이전트 설정 적용. 예를 들어 웹 콘솔에서 예약 검색 빈도를 변경한 경우 서버는 새 설정을 적용하도록 에이전트에 즉시 알립니다.

따라서 연결할 수 없는 에이전트는 이러한 작업을 적시에 수행할 수 없습니다. 서버와의 연결을 시작할 때만 작업을 수행합니다. 서버와의 연결은 다음과 같은 경우에 시작됩니다.

- 설치 후 서버에 등록할 때
- 다시 시작하거나 다시 로드할 때. 이 이벤트는 자주 발생하지 않으며 일반적으로 사용자의 개입이 필요합니다.
- 에이전트에서 수동 또는 예약 업데이트가 트리거될 때. 이 이벤트 역시 자주 발생하지 않습니다.

등록, 다시 시작 또는 다시 로드 중에만 서버에서 에이전트의 연결을 "인식"하고 에이전트를 온라인 상태로 간주합니다. 그러나 서버는 여전히 에이전트와의 연결을 설정할 수 없으므로 상태를 즉시 오프라인으로 변경합니다.

OfficeScan에서는 연결할 수 없는 에이전트와 관련된 문제를 해결하는 "하트비트" 및 서버 폴링 기능을 제공합니다. 이러한 기능을 통해 서버는 구성 요소 업데이트 및 설정 변경을 에이전트에 알리는 일을 중지합니다. 대신 서버는 수동적인 역할을 취하여 에이전트가 하트비트를 보내거나 폴링을 시작할 때까지 항상 기다립니다. 서버가 이러한 이벤트를 탐지하면 에이전트를 온라인 상태로 간주합니다.

참고

에이전트에서 시작한 이벤트가 하트비트 및 서버 폴링과 관련이 없는 경우(예: 수동 에이전트 업데이트 및 로그 전송)에는 연결할 수 없는 에이전트 상태를 업데이트하도록 서버를 트리거하지 않습니다.

하트비트

OfficeScan 에이전트는 에이전트의 연결이 작동하고 있음을 서버에 알리는 하트비트 메시지를 보냅니다. 하트비트 메시지를 받은 경우 서버는 에이전트를 온라인 상태로 간주합니다. 에이전트 트리에 표시되는 에이전트 상태는 다음 중 하나일 수 있습니다.

- **온라인**: 정상적인 온라인 에이전트
- **연결할 수 없음/온라인**: 연결할 수 없는 네트워크의 온라인 에이전트

참고

OfficeScan 에이전트는 하트비트 메시지를 보낼 때 구성 요소를 업데이트하거나 새 설정을 적용하지 않습니다. 정상적인 에이전트는 이러한 작업을 일상적인 업데이트 중에 수행합니다(OfficeScan 에이전트 업데이트 페이지 6-26 참조). 연결할 수 없는 네트워크의 에이전트는 이러한 작업을 서버 폴링 중에 수행합니다.

하트비트 기능은 연결할 수 없는 네트워크의 OfficeScan 에이전트가 서버에 연결할 수 있을 때에도 항상 오프라인 상태로 표시되는 문제를 해결합니다.

웹 콘솔의 설정은 에이전트에서 하트비트 메시지를 보내는 빈도를 제어합니다. 서버에서 하트비트를 받지 않은 경우 에이전트를 즉시 오프라인으로 간주하지는 않습니다. 에이전트의 상태를 다음으로 변경하기 전에 하트비트 없이 경과해야 하는 시간을 제어하는 또 다른 설정이 있습니다.

- **오프라인**: 정상적인 오프라인 OfficeScan 에이전트
- **연결할 수 없음/오프라인**: 연결할 수 없는 네트워크의 오프라인 OfficeScan 에이전트

하트비트 설정을 선택할 때 최신 에이전트 상태 정보 표시에 대한 요구 사항과 시스템 리소스 관리에 대한 요구 사항 간에 균형을 유지할 수 있습니다. 대부분의 경우 기본 설정을 그대로 적용하면 됩니다. 그러나 하트비트 설정을 사용자 정의할 때 다음 사항을 고려해야 합니다.

표 15-7. 하트비트 권장 사항

하트비트 빈도	권장 사항
긴 간격 하트비트(60분 이상)	하트비트 사이의 간격이 길수록 서버에서 웹 콘솔에 에이전트의 상태를 나타내기 전에 발생할 수 있는 이벤트 수가 많아집니다.
짧은 간격 하트비트(60분 이하)	간격이 짧으면 더 최신 에이전트 상태가 제공되지만 대역폭 사용량이 많아질 수 있습니다.

서버 폴링

서버 폴링 기능은 구성 요소 업데이트 및 에이전트 설정 변경에 대한 알림을 적시에 받지 못하는, 연결할 수 없는 OfficeScan 에이전트 문제를 해결합니다. 이 기능은 하트비트 기능과 독립적으로 작동합니다.

서버 폴링 기능을 사용하면 다음과 같은 작업이 실행됩니다.

- OfficeScan 에이전트에서 OfficeScan 서버와의 연결을 자동으로 주기적으로 시작합니다. 서버에서 폴링이 발생했다고 탐지한 경우 에이전트를 "연결할 수 없음/온라인"으로 간주합니다.
- OfficeScan 에이전트가 해당 업데이트 소스 중 하나 이상에 연결하여 업데이트된 구성 요소를 다운로드하고 새로운 에이전트 설정을 적용합니다. OfficeScan 서버 또는 업데이트 에이전트가 기본 업데이트 소스인 경우 에이전트는 구성 요소와 새로운 설정을 모두 가져옵니다. 소스가 OfficeScan 서버 또는 업데이트 에이전트가 아닌 경우 에이전트는 업데이트된 구성 요소만 가져온 다음 OfficeScan 서버 또는 업데이트 에이전트에 연결하여 새로운 설정을 가져옵니다.

하트비트 및 서버 폴링 기능 구성

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **네트워크** 탭을 클릭합니다.
3. **연결할 수 없는 네트워크** 섹션으로 이동합니다.
4. 서버 폴링 설정을 구성합니다.

   서버 폴링에 대한 자세한 내용은 서버 폴링 페이지 15-45을 참조하십시오.

   a. OfficeScan 서버에서 IPv4 주소와 IPv6 주소를 둘 다 사용하는 경우 IPv4 주소 범위와 IPv6 접두사 및 길이를 입력할 수 있습니다.

      서버가 순수 IPv4이면 IPv4 주소 범위를 입력하고, 서버가 순수 IPv6이면 IPv6 접두사와 길이를 입력합니다.

에이전트의 IP 주소가 범위 내의 IP 주소와 일치하는 경우 에이전트는 하트비트 및 서버 폴링 설정을 적용하고 서버는 에이전트를 연결할 수 없는 네트워크의 일부로 간주합니다.

참고

IPv4 주소를 사용하는 에이전트는 순수 IPv4 또는 이중 스택 OfficeScan 서버에 연결할 수 있습니다.

IPv6 주소를 사용하는 에이전트는 순수 IPv6 또는 이중 스택 OfficeScan 서버에 연결할 수 있습니다.

이중 스택 에이전트는 이중 스택, 순수 IPv4 또는 순수 IPv6 OfficeScan 서버에 연결할 수 있습니다.

b. **에이전트에서 업데이트된 구성 요소 및 설정에 대해 서버를 폴링하는 간격: __분**에서 서버 폴링 빈도를 지정합니다. 1분에서 129600분 사이의 값을 입력합니다.

팁

Trend Micro에서는 서버 폴링 빈도를 하트비트 설정 빈도의 세 배 이상으로 설정할 것을 권장합니다.

5. 하트비트 설정을 구성합니다.

하트비트 기능에 대한 자세한 내용은 하트비트 페이지 15-43를 참조하십시오.

a. **에이전트에서 서버에 하트비트를 보낼 수 있음**을 선택합니다.

b. **모든 에이전트** 또는 **연결할 수 없는 네트워크의 에이전트만**을 선택합니다.

c. **에이전트에서 하트비트를 보내는 간격: __분**에서 에이전트가 하트비트를 보내는 빈도를 지정합니다. 1분에서 129600분 사이의 값을 입력합니다.

d. **하트비트가 없는 경우 다음 시간 후 에이전트가 오프라인 상태로 전환됨: __분**에서 OfficeScan 서버가 에이전트를 오프라인 상태로 간주하기 전에 하트비트 없이 경과해야 하는 시간을 지정합니다. 1분에서 129600분 사이의 값을 입력합니다.

6. **저장**을 클릭합니다.

OfficeScan 에이전트 프록시 설정

내부 및 외부 서버에 연결할 때 프록시 설정을 사용하도록 OfficeScan 에이전트를 구성합니다.

OfficeScan 에이전트용 내부 프록시

OfficeScan 에이전트는 내부 프록시 설정을 사용하여 네트워크의 다음 서버에 연결할 수 있습니다.

- OfficeScan 서버

  서버 컴퓨터는 OfficeScan 서버 및 통합 스마트 보호 서버를 호스팅합니다. OfficeScan 에이전트는 OfficeScan 서버에 연결하여 구성 요소를 업데이트하고, 구성 설정을 획득하고, 로그를 보낼 수 있습니다. 또한 OfficeScan 에이전트는 통합 스마트 보호 서버에 연결하여 검색 쿼리를 보낼 수 있습니다.

- 스마트 보호 서버

  스마트 보호 서버는 모든 독립 스마트 보호 서버 및 다른 OfficeScan 서버의 통합 스마트 보호 서버를 포함합니다. OfficeScan 에이전트는 이러한 서버에 연결하여 검색 및 웹 검증 쿼리를 보낼 수 있습니다.

내부 프록시 설정 구성

절차

1. **관리** > **설정** > **프록시**으로 이동합니다.
2. **내부 프록시** 탭을 클릭합니다.
3. **OfficeScan 서버와 에이전트의 연결** 섹션으로 이동합니다.

a. **에이전트가 OfficeScan 서버에 연결할 때 다음 프록시 설정을 사용합니다**를 선택합니다.

b. 프록시 서버 이름 또는 IPv4/IPv6 주소와 포트 번호를 지정합니다.

> **참고**
>
> IPv4 및 IPv6 에이전트가 둘 다 있는 경우 해당 호스트 이름으로 식별되는 이중 스택 프록시 서버를 지정합니다. 이는 내부 프록시 설정이 글로벌 설정이기 때문입니다. IPv4 주소를 지정한 경우 IPv6 에이전트에서 프록시 서버에 연결할 수 없습니다. IPv4 에이전트의 경우에도 마찬가지입니다.

c. 프록시 서버에 인증이 필요한 경우 사용자 이름과 암호를 입력한 다음 암호를 확인합니다.

4. **독립 스마트 보호 서버와 에이전트 연결** 섹션으로 이동합니다.

a. **에이전트가 독립 스마트 보호 서버에 연결할 때 다음 프록시 설정을 사용합니다**를 선택합니다.

b. 프록시 서버 이름 또는 IPv4/IPv6 주소와 포트 번호를 지정합니다.

c. 프록시 서버에 인증이 필요한 경우 사용자 이름과 암호를 입력한 다음 암호를 확인합니다.

5. **저장**을 클릭합니다.

OfficeScan 에이전트용 외부 프록시

OfficeScan 서버 및 OfficeScan 에이전트는 Trend Micro에서 호스팅하는 서버에 연결할 때 외부 프록시 설정을 사용할 수 있습니다. 이 항목에서는 에이전트에 대한 외부 프록시 설정을 설명합니다. 서버에 대한 외부 프록시 설정은 OfficeScan 서버 업데이트용 프록시 페이지 6-18를 참조하십시오.

OfficeScan 에이전트는 Internet Explorer 또는 Chrome에서 구성된 프록시 설정을 사용하여 Trend Micro 스마트 보호 네트워크에 연결합니다. 프록시 서버 인증이 필요한 경우 에이전트는 프록시 서버 인증 자격 증명(사용자 ID 및 암호)을 사용합니다.

프록시 서버 인증 자격 증명 구성

절차

1. **관리** > **설정** > **프록시**으로 이동합니다.
2. **외부 프록시** 탭을 클릭합니다.
3. **Trend Micro 서버와 OfficeScan 에이전트 연결** 섹션으로 이동합니다.
4. 프록시 서버 인증에 필요한 사용자 ID 및 암호를 입력합니다. 다음 프록시 인증 프로토콜이 지원됩니다.
   - 기본 액세스 인증
   - 요약 액세스 인증
   - 통합된 Windows 인증
5. **저장**을 클릭합니다.

글로벌 스마트 보호 서비스 프록시 설정 구성

OfficeScan 에이전트는 다음 기능에 대해 스마트 보호 소스를 쿼리할 때 구성된 스마트 보호 서비스 프록시 설정을 사용합니다.

- 머신러닝
- 동작 모니터링

참고

통합 스마트 보호 서버를 사용할 수 없는 경우 OfficeScan 에이전트는 쿼리를 수행할 때 Trend Micro 스마트 보호 네트워크에 연결합니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.

2. **시스템** 탭을 클릭합니다.
3. **스마트 보호 서비스 프록시** 섹션으로 이동합니다.
4. **서비스 쿼리에 대해 구성된 스마트 보호 소스 사용**을 사용하도록 설정합니다.

중요

스마트 보호 서비스 프록시는 파일 검증 쿼리에 대해 HTTPS 프로토콜만 지원합니다. 파일 검증 서비스를 제공하는 모든 구성된 스마트 보호 서버가 HTTPS 프로토콜을 사용하는지 확인해야 합니다.

기본적으로 통합된 스마트 보호 서버는 HTTPS 통신을 사용하지 않습니다. 통신 방법을 변경하려면 통합 스마트 보호 서버 설정 구성 페이지 4-20을(를) 참조하십시오.

독립 스마트 보호 서버가 사용하는 통신 방법을 확인하려면 스마트 보호 소스의 사용자 지정 목록 구성 페이지 4-26을(를) 참조하십시오.

5. **저장**을 클릭합니다.

에이전트에 대한 프록시 구성 권한

에이전트 사용자에게 프록시 설정을 구성할 권한을 부여할 수 있습니다. OfficeScan 에이전트는 다음과 같은 경우에만 사용자가 구성한 프록시 설정을 사용합니다.

- OfficeScan 에이전트에서 "지금 업데이트"를 수행할 때
- 사용자가 자동 프록시 설정을 사용하지 않거나 OfficeScan 에이전트에서 자동 프록시 설정을 찾을 수 없을 때

  자세한 내용은 OfficeScan 에이전트에 대한 자동 프록시 설정 페이지 15-51를 참조하십시오.

경고!

사용자가 구성한 프록시 설정이 잘못되면 업데이트 문제가 발생할 수 있습니다. 사용자가 고유한 프록시 설정을 구성하도록 허용할 때 주의하십시오.

프록시 구성 권한 부여

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 **프록시 설정** 섹션으로 이동합니다.
5. **사용자가 프록시 설정을 구성할 수 있음**을 선택합니다.
6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.
   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

OfficeScan 에이전트에 대한 자동 프록시 설정

대부분의 최종 사용자에게 프록시 설정을 수동으로 구성하는 작업은 너무 복잡할 수 있습니다. 자동 프록시 설정을 사용하면 사용자가 작업하지 않고도 정확한 프록시 설정을 적용할 수 있습니다.

자동 프록시 설정을 사용하도록 설정하면 OfficeScan 에이전트에서 자동 업데이트 또는 지금 업데이트를 통해 구성 요소를 업데이트할 때 이 설정이 기본 프록시 설정으로 사용됩니다. 자동 업데이트 및 지금 업데이트에 대한 자세한 내용은 OfficeScan 에이전트 업데이트 방법 페이지 6-35을 참조하십시오.

OfficeScan 에이전트가 자동 프록시 설정을 사용하여 연결할 수 없는 경우에 프록시 설정 구성 권한이 있는 에이전트 사용자는 사용자 구성 프록시 설정을 사

용할 수 있습니다. 그렇지 않으면 자동 프록시 설정을 사용하여 연결할 수 없습니다.

참고

프록시 인증은 지원되지 않습니다.

자동 프록시 설정 구성

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. **네트워크** 탭을 클릭합니다.
3. **프록시 구성** 섹션으로 이동합니다.
4. OfficeScan에서 관리자가 구성한 DHCP 또는 DNS별 프록시 설정을 자동으로 검색하도록 하려면 **설정 자동 검색**을 선택합니다.
5. OfficeScan에서 네트워크 관리자가 설정한 PAC(프록시 자동 구성) 스크립트를 사용하여 적절한 프록시 서버를 검색하도록 하려면 다음을 수행합니다.
   a. **자동 구성 스크립트 사용**을 선택합니다.
   b. PAC 스크립트 주소를 입력합니다.
6. **저장**을 클릭합니다.

OfficeScan 에이전트 정보 보기

상태 보기 화면에는 OfficeScan 에이전트에 대한 권한, 에이전트 소프트웨어 세부 정보 및 시스템 이벤트 등 중요한 정보가 표시됩니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **상태**를 클릭합니다.
4. 에이전트 엔드포인트의 이름을 확장하여 상태 정보를 확인합니다. 에이전트를 여럿 선택한 경우 **모두 확장**을 클릭하여 선택한 모든 에이전트의 상태 정보를 표시합니다.
5. (선택 사항) **초기화** 단추를 사용하여 보안 위험 개수를 0으로 다시 설정합니다.

에이전트 설정 가져오기 및 내보내기

OfficeScan에서는 특정 OfficeScan 에이전트 또는 도메인에 의해 적용된 에이전트 트리 설정을 파일에 내보낼 수 있습니다. 그런 다음 이 파일을 가져와 다른 에이전트와 도메인 또는 같은 버전의 다른 OfficeScan 서버에 설정을 적용할 수 있습니다.

업데이트 에이전트 설정을 제외한 모든 에이전트 트리 설정을 내보냅니다.

에이전트 설정 내보내기

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **설정 내보내기**를 클릭합니다.
4. 선택한 OfficeScan 에이전트 또는 도메인에 대한 설정을 보려면 링크를 클릭합니다.

5. **내보내기**를 클릭하여 설정을 저장합니다.

   설정은 .dat 파일에 저장됩니다.

6. **저장**을 클릭한 다음 .dat 파일을 저장할 위치를 지정합니다.

7. **저장**을 클릭합니다.

에이전트 설정 가져오기

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.

2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.

3. **설정** > **설정 가져오기**를 클릭합니다.

4. **찾아보기**를 클릭하여 엔드포인트에서 .dat 파일을 찾은 후 **가져오기**를 클릭합니다.

   설정 요약이 표시된 **설정 가져오기** 화면이 표시됩니다.

5. 가져올 권한 또는 검색 설정에 관한 자세한 내용을 보려면 링크를 클릭합니다.

6. 설정을 가져옵니다.

   - 루트 도메인 아이콘을 클릭한 경우 **모든 도메인에 적용**을 선택한 다음 **대상에 적용**을 클릭합니다.
   - 도메인을 선택한 경우 **선택된 도메인에 속하는 모든 컴퓨터에 적용**을 선택한 후 **대상에 적용**을 클릭합니다.
   - 여러 에이전트를 선택한 경우 **대상에 적용**을 클릭합니다.

보안 준수

보안 준수를 사용하여 결함 확인, 솔루션 배포 및 보안 인프라를 유지합니다. 이 기능을 통해 네트워크 환경의 보안을 유지하고 보안과 기능에 대한 조직의 요구 사항 간에 균형을 유지하는 데 필요한 시간을 줄일 수 있습니다.

다음 두 가지 유형의 엔드포인트에 대해 보안 준수를 적용합니다.

- **관리됨**: OfficeScan 서버에서 관리하는 OfficeScan 에이전트를 포함하는 엔드포인트. 자세한 내용은 관리되는 에이전트에 대한 보안 준수 페이지 15-55를 참조하십시오.
- **관리되지 않음**: 다음을 포함합니다.
  - OfficeScan 서버에서 관리하지 않는 OfficeScan 에이전트
  - OfficeScan 에이전트가 설치되지 않은 엔드포인트
  - OfficeScan 서버가 연결할 수 없는 엔드포인트
  - 보안 상태를 확인할 수 없는 엔드포인트

  자세한 내용은 관리되지 않는 엔드포인트에 대한 보안 준수 페이지 15-68를 참조하십시오.

관리되는 에이전트에 대한 보안 준수

보안 준수 기능은 OfficeScan 서버에서 관리하는 OfficeScan 에이전트의 보안 상태를 점검하는 데 도움이 되는 준수 보고서를 생성합니다. 이러한 보고서는 필요에 따라 또는 일정에 따라 생성됩니다.

수동 점검 화면에는 다음 탭이 표시됩니다.

- **서비스**: 에이전트 서비스가 작동 중인지 확인하려면 이 탭을 사용합니다.

  자세한 내용은 서비스 페이지 15-56를 참조하십시오.
- **구성 요소**: OfficeScan 에이전트의 구성 요소가 최신인지 확인하려면 이 탭을 사용합니다.

  자세한 내용은 구성 요소 페이지 15-58를 참조하십시오.

- **검색 준수**: OfficeScan 에이전트에서 검색을 주기적으로 실행하는지 확인하려면 이 탭을 사용합니다.

  자세한 내용은 검색 준수 페이지 15-60를 참조하십시오.

- **설정**: 에이전트 설정이 서버의 설정과 일치하는지 확인하려면 이 탭을 사용합니다.

  자세한 내용은 설정 페이지 15-62를 참조하십시오.

참고

구성 요소 탭에서는 현재 버전 및 이전 버전의 제품을 실행하는 OfficeScan 에이전트를 표시할 수 있습니다. 그 밖의 탭에는 버전 10.5 또는 10.6을 실행하는 OfficeScan 에이전트나 OfficeScan 에이전트만 표시됩니다.

중요

- 보안 준수 기능은 준수 보고서를 생성하기 전에 OfficeScan 에이전트의 연결 상태를 쿼리합니다. 여기에 보고서의 온라인 및 오프라인 에이전트는 포함되지만 독립 모드의 에이전트는 포함되지 않습니다.
- 역할 기반 사용자 계정의 경우
  - 각 웹 콘솔 사용자 계정에는 완전히 독립된 준수 보고서 설정 집합이 제공됩니다. 따라서 한 사용자 계정의 준수 보고서 설정을 변경해도 다른 사용자 계정의 설정은 영향을 받지 않습니다.
  - 보고서 범위는 사용자 계정에 대한 에이전트 도메인 권한에 따라 달라집니다. 예를 들어 사용자 계정에 도메인 A와 B를 관리하는 권한을 부여한 경우 이 사용자 계정의 보고서에는 도메인 A와 B에 속한 에이전트의 데이터만 표시됩니다.

    사용자 계정에 대한 자세한 내용은 역할 기반 관리 페이지 14-3를 참조하십시오.

서비스

보안 준수에서는 다음 OfficeScan 에이전트 서비스가 작동 중인지 확인합니다.

- 바이러스 백신

- Anti-spyware
- 방화벽
- 웹 검증
- 동작 모니터링/장치 제어(Trend Micro 무단 변경 방지 서비스라고도 함)
- 데이터 보호
- 의심스러운 연결

비호환 에이전트는 준수 보고서에서 두 번 이상 계산됩니다.

그림 15-3. 준수 보고서 - 서비스 탭

- **비호환 서비스를 사용하는 엔드포인트** 범주에서
- OfficeScan 에이전트가 비호환으로 처리되는 범주에서. 예를 들어 OfficeScan 에이전트의 바이러스 백신 서비스가 작동하지 않는 경우 에이전트는 **바이러스 백신** 범주에 포함됩니다. 둘 이상의 설정 집합이 일치하지 않는 경우 에이전트는 각각의 비호환 범주에 포함됩니다.

웹 콘솔 또는 OfficeScan 에이전트에서 작동하지 않는 서비스를 다시 시작합니다. 다시 시작한 후 서비스가 작동하면 다음 점검 중에 에이전트가 더 이상 비호환으로 표시되지 않습니다.

구성 요소

보안 준수 기능은 OfficeScan 서버와 OfficeScan 에이전트 간의 구성 요소 버전 불일치를 확인합니다. 불일치는 일반적으로 에이전트가 구성 요소 업데이트를 위해 서버에 연결할 수 없는 경우 발생합니다. 에이전트가 다른 소스(예: Trend Micro 액티브업데이트 서버)에서 업데이트를 가져올 경우 에이전트의 구성 요소가 서버의 구성 요소보다 최신 버전일 수 있습니다.

보안 준수에서 확인하는 구성 요소는 다음과 같습니다.

- 스마트 스캔 에이전트 패턴
- 바이러스 패턴
- IntelliTrap 패턴
- IntelliTrap 예외 패턴
- 바이러스 검색 엔진 32/64비트
- 스파이웨어/그레이웨어 패턴
- 스파이웨어 활성 모니터링 패턴
- 스파이웨어/그레이웨어 검색 엔진 32/64비트
- Damage Cleanup 템플릿
- DCE(Damage Cleanup Engine) 32/64비트
- 방화벽 패턴
- 방화벽 드라이버 32/64비트
- 동작 모니터링 핵심 드라이버 32/64비트
- 동작 모니터링 핵심 서비스 32/64비트
- 동작 모니터링 구성 패턴
- 스마트 검색 패턴
- 정책 적용 패턴
- 동작 모니터링 탐지 패턴 32/64비트
- 글로벌 C&C IP 목록
- 관련 규칙 패턴
- Early Boot Cleanup 드라이버 32/64비트
- 메모리 검색 트리거 패턴(32/64비트)
- 메모리 검사 패턴
- 브라우저 위협 방지 패턴
- 스크립트 분석자 통합 패턴
- 프로그램 검사 모니터링 패턴
- 손상 복구 패턴
- 안티-멀웨어 패턴 조기 실행 32/64비트
- 상황별 정보 엔진 32/64비트
- 상황별 정보 패턴
- 상황별 정보 쿼리 처리기 32/64비트
- 고급 위협 검색 엔진 32/64비트
- 고급 위협 상관 관계 패턴
- 프로그램 버전

비호환 에이전트는 준수 보고서에서 두 번 이상 계산됩니다.

그림 15-4. 준수 보고서 - 준수 탭

- **불일치 구성 요소 버전을 사용하는 엔드포인트** 범주에서
- 에이전트가 비호환으로 처리되는 범주에서. 예를 들어 에이전트의 스마트 스캔 에이전트 패턴 버전이 서버의 버전과 일치하지 않는 경우 에이전트는 **스마트 스캔 에이전트 패턴** 범주에 포함됩니다. 둘 이상의 구성 요소 버전이 불일치하는 경우 에이전트는 각각의 비호환 범주에 포함됩니다.

구성 요소 버전 불일치를 해결하려면 에이전트 또는 서버에서 오래된 구성 요소를 업데이트합니다.

검색 준수

보안 준수에서는 지금 검색 또는 예약 검색이 정기적으로 실행되는지, 이러한 검색이 적절한 시간 내에 완료되는지 여부를 확인합니다.

참고

보안 준수 기능은 에이전트에서 예약 검색을 사용하는 경우에만 예약 검색 상태를 보고할 수 있습니다.

보안 준수에서는 다음과 같은 검색 준수 기준을 사용합니다.

- **마지막 (x)일 동안 수행된 지금 검색 또는 예약 검색이 없습니다.**: OfficeScan 에이전트에서 지정된 기간 이내에 지금 검색 또는 예약 검색을 실행하지 않은 경우 비호환으로 처리됩니다.
- **지금 검색 또는 예약 검색이 (x)시간을 초과했습니다.**: OfficeScan 에이전트에서 지금 검색 또는 예약 검색을 마지막으로 실행한 시간이 지정된 시간을 초과하는 경우 비호환으로 처리됩니다.

비호환 에이전트는 준수 보고서에서 두 번 이상 계산됩니다.

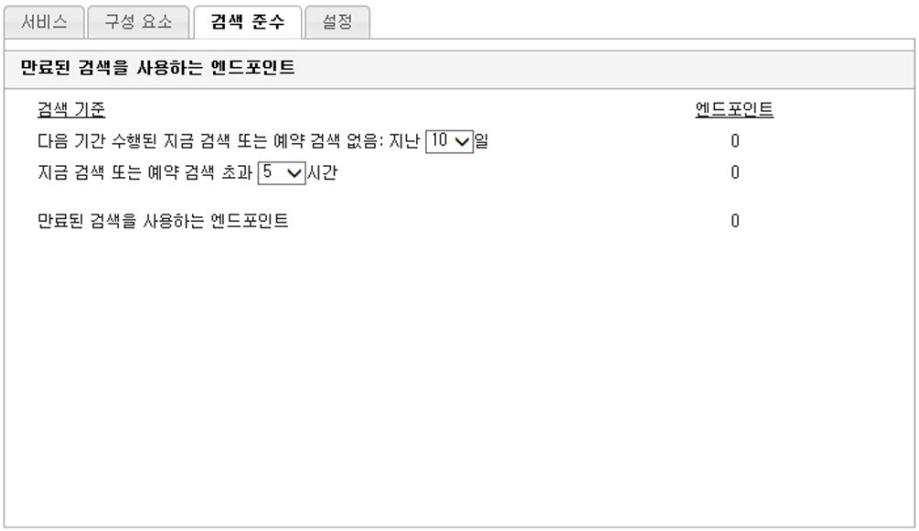


그림 15-5. 준수 보고서 - 검색 준수 탭

- **만료된 검색을 사용하는 엔드포인트** 범주에서

- 에이전트가 비호환으로 처리되는 범주에서. 예를 들어 예약 검색을 마지막으로 실행한 시간이 지정된 시간을 초과한 경우 에이전트는 **지금 검색 또는 예약 검색이 <x> 시간을 초과했습니다.** 범주에 포함됩니다. 둘 이상의 검색 준수 기준을 충족하는 에이전트는 각각의 비호환 범주에 포함됩니다.

검색 작업을 수행하지 않았거나 검색을 완료할 수 없는 에이전트에서 지금 검색 또는 예약 검색을 실행합니다.

설정

보안 준수 기능은 에이전트 트리에서 에이전트와 해당 상위 도메인의 설정이 같은지 확인합니다. 에이전트를 다른 설정 집합이 적용된 다른 도메인으로 이동하거나 특정 권한을 가진 에이전트 사용자가 OfficeScan 에이전트 콘솔에서 설정을 수동으로 구성한 경우 설정이 일치하지 않을 수 있습니다.

OfficeScan은 다음 설정을 확인합니다.

- 검색 방법
- 수동 검색 설정
- 실시간 검색 설정
- 예약 검색 설정
- 지금 검색 설정
- 권한 및 기타 설정
- 추가 서비스 설정
- 웹 검증
- 동작 모니터링
- 장치 제어
- 스파이웨어/그레이웨어 승인된 목록
- 데이터 손실 방지 설정
- 의심스러운 연결
- 신뢰할 수 있는 프로그램 목록
- 샘플 제출
- 머신러닝

비호환 에이전트는 준수 보고서에서 두 번 이상 계산됩니다.

그림 15-6. 준수 보고서 - 설정 탭

- **불일치 구성 설정을 사용하는 엔드포인트** 범주에서
- 에이전트가 비호환으로 처리되는 범주에서. 예를 들어 에이전트와 해당 상위 도메인의 검색 방법 설정이 일치하지 않는 경우 에이전트는 **검색 방법** 범주에 포함됩니다. 둘 이상의 설정 집합이 불일치하는 경우 에이전트는 각각의 비호환 범주에 포함됩니다.

설정 불일치를 해결하려면 도메인 설정을 에이전트에 적용합니다.

주문형 준수 보고서

보안 준수에서는 주문형 준수 보고서를 생성할 수 있습니다. 이 보고서를 통해 OfficeScan 서버에서 관리하는 OfficeScan 에이전트의 보안 상태를 점검할 수 있습니다.

준수 보고서에 대한 자세한 내용은 관리되는 에이전트에 대한 보안 준수 페이지 15-55를 참조하십시오.

주문형 준수 보고서 생성

절차

1. **점검** > **보안 준수** > **수동 보고서**으로 이동합니다.
2. **에이전트 트리 범위** 섹션으로 이동합니다.
3. 루트 도메인 또는 도메인을 선택하고 **평가**를 클릭합니다.
4. 에이전트 서비스에 대한 준수 보고서를 확인합니다.

   에이전트 서비스에 대한 자세한 내용은 서비스 페이지 15-56를 참조하십시오.

   a. **서비스** 탭을 클릭합니다.

   b. **비호환 서비스를 사용하는 엔드포인트**에서 비호환 서비스를 사용하는 에이전트 수를 확인합니다.

   c. 숫자 링크를 클릭하여 에이전트 트리에 영향을 받는 모든 에이전트를 표시합니다.

   d. 쿼리 결과에서 에이전트를 선택합니다.

   e. **OfficeScan 에이전트 다시 시작**을 클릭하여 서비스를 다시 시작합니다.

   참고

   다른 점검을 수행한 후에도 에이전트가 계속 비호환으로 나타나면 에이전트 엔드포인트에서 서비스를 수동으로 다시 시작합니다.

   f. 에이전트의 목록을 파일에 저장하려면 **내보내기**를 클릭합니다.

5. 에이전트 구성 요소에 대한 준수 보고서를 확인합니다.

   에이전트 구성 요소에 대한 자세한 내용은 구성 요소 페이지 15-58을 참조하십시오.

   a. **구성 요소** 탭을 클릭합니다.

b. **불일치 구성 요소 버전을 사용하는 엔드포인트**에서 서버의 버전과 일치하지 않는 구성 요소 버전을 사용하는 에이전트 수를 확인합니다.

c. 숫자 링크를 클릭하여 에이전트 트리에 영향을 받는 모든 에이전트를 표시합니다.

참고

하나 이상의 에이전트에 OfficeScan 서버보다 최신 구성 요소가 포함된 경우 OfficeScan 서버를 수동으로 업데이트합니다.

d. 쿼리 결과에서 에이전트를 선택합니다.

e. **지금 업데이트**를 클릭하여 에이전트가 구성 요소를 다운로드하도록 합니다.

참고

- 에이전트에서 에이전트 프로그램을 업그레이드할 수 있도록 하려면 **에이전트 > 에이전트 관리 > 설정 > 권한 및 기타 설정**에서 **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음** 옵션을 사용하지 않도록 설정합니다.
- 방화벽 드라이버를 업데이트하려면 **지금 업데이트**를 클릭하는 대신 엔드포인트를 다시 시작합니다.

f. 에이전트의 목록을 파일에 저장하려면 **내보내기**를 클릭합니다.

6. 검색에 대한 준수 보고서를 확인합니다.

검색에 대한 자세한 내용은 검색 준수 페이지 15-60를 참조하십시오.

a. **검색 준수** 탭을 클릭합니다.

b. **만료된 검색을 사용하는 엔드포인트**에서 다음을 구성합니다.

- 에이전트가 지금 검색 또는 예약 검색을 수행하지 않은 일수
- 지금 검색 또는 예약 검색의 실행 시간

참고

일수 또는 시간을 초과한 경우 에이전트는 비호환으로 처리됩니다.

c. **에이전트 트리 범위** 섹션 옆의 **점검**을 클릭합니다.

d. **만료된 검색을 사용하는 엔드포인트**에서 검색 기준을 충족하는 에이전트 수를 확인합니다.

e. 숫자 링크를 클릭하여 에이전트 트리에 영향을 받는 모든 에이전트를 표시합니다.

f. 쿼리 결과에서 에이전트를 선택합니다.

g. **지금 검색**을 클릭하여 에이전트에서 지금 검색을 시작합니다.

참고

검색이 반복 실행되지 않도록 하기 위해 지금 검색이 마지막으로 실행된 시간이 지정된 시간을 초과하는 경우에는 **지금 검색** 옵션이 비활성화됩니다.

h. 에이전트의 목록을 파일에 저장하려면 **내보내기**를 클릭합니다.

7. 설정에 대한 준수 보고서를 확인합니다.

설정에 대한 자세한 내용은 설정 페이지 15-62을 참조하십시오.

a. **설정** 탭을 클릭합니다.

b. **불일치 구성 설정을 사용하는 컴퓨터**에서 에이전트 트리 도메인 설정과 일치하지 않는 설정을 사용하는 에이전트 수를 확인합니다.

c. 숫자 링크를 클릭하여 에이전트 트리에 영향을 받는 모든 에이전트를 표시합니다.

d. 쿼리 결과에서 에이전트를 선택합니다.

e. **도메인 설정 적용**을 클릭합니다.

f. 에이전트의 목록을 파일에 저장하려면 **내보내기**를 클릭합니다.

예약 준수 보고서

보안 준수에서 일정에 따라 준수 보고서를 생성할 수 있습니다. 이 보고서를 통해 OfficeScan 서버에서 관리하는 OfficeScan 에이전트의 보안 상태를 점검할 수 있습니다.

준수 보고서에 대한 자세한 내용은 관리되는 에이전트에 대한 보안 준수 페이지 15-55를 참조하십시오.

예약 준수 보고서에 대한 설정 구성

절차

1. **점검** > **보안 준수** > **예약 보고서**로 이동합니다.
2. **예약 보고 사용**을 선택합니다.
3. 보고서 제목을 지정합니다.
4. 다음 중 하나 또는 모두를 선택합니다.
   - 서비스 페이지 15-56
   - 구성 요소 페이지 15-58
   - 검색 준수 페이지 15-60
   - 설정 페이지 15-62
5. 예약 준수 보고서에 대한 알림을 받을 전자 메일 주소를 지정합니다.

   참고

   전자 메일 알림이 성공적으로 전송될 수 있도록 전자 메일 알림 설정을 구성합니다. 자세한 내용은 관리자 알림 설정 페이지 14-35를 참조하십시오.

6. 일정을 지정합니다.
7. **저장**을 클릭합니다.

관리되지 않는 엔드포인트에 대한 보안 준수

보안 준수에서는 OfficeScan 서버가 속한 네트워크의 관리되지 않는 엔드포인트를 쿼리할 수 있습니다. Active Directory 및 IP 주소를 사용하여 엔드포인트를 쿼리합니다.

관리되지 않는 엔드포인트의 보안 상태는 다음과 같을 수 있습니다.

표 15-8. 관리되지 않는 엔드포인트의 보안 상태

상태	설명
다른 OfficeScan 서버에서 관리	컴퓨터에 설치된 OfficeScan 에이전트를 다른 OfficeScan 서버에서 관리합니다. OfficeScan 에이전트는 온라인 상태이고 이 OfficeScan 버전 또는 이전 버전을 실행합니다.
OfficeScan 에이전트가 설치되지 않음	OfficeScan 에이전트가 엔드포인트에 설치되지 않았습니다.
연결할 수 없음	OfficeScan 서버가 엔드포인트에 연결할 수 없고 해당 보안 상태를 확인할 수 없습니다.
해결되지 않은 Active Directory 점검	엔드포인트가 Active Directory 도메인에 속해 있지만 OfficeScan 서버에서 해당 보안 상태를 확인할 수 없습니다. **참고** OfficeScan 서버 데이터베이스에는 서버가 관리하는 에이전트의 목록이 포함됩니다. 서버가 컴퓨터의 GUID에 대해 Active Directory를 쿼리한 다음 데이터베이스에 저장된 GUID와 비교합니다. GUID가 데이터베이스에 없는 경우 엔드포인트는 해결되지 않은 Active Directory 평가 범주 아래에 속합니다.

보안 점검을 실행하려면 다음 작업을 수행합니다.

1. 쿼리 범위를 정의합니다. 자세한 내용은 Active Directory/IP 주소 범위 및 쿼리 정의 페이지 15-69를 참조하십시오.
2. 쿼리 결과에서 보호되지 않은 컴퓨터를 확인합니다. 자세한 내용은 쿼리 결과 보기 페이지 15-71를 참조하십시오.
3. OfficeScan 에이전트를 설치합니다. 자세한 내용은 보안 준수를 사용한 설치 페이지 5-61를 참조하십시오.

4. 예약 쿼리를 구성합니다. 자세한 내용은 예약 쿼리 점검 구성 페이지 15-72를 참조하십시오.

Active Directory/IP 주소 범위 및 쿼리 정의

처음으로 쿼리할 때 OfficeScan 서버가 요청 시 또는 정기적으로 쿼리할 Active Directory 개체 및 IP 주소를 포함하는 Active Directory/IP 주소 범위를 정의합니다. 범위를 정의한 후, 쿼리 프로세스를 시작합니다.

참고

Active Directory 범위를 정의하려면 먼저 OfficeScan을 Active Directory와 통합해야 합니다. 통합에 대한 자세한 내용은 Active Directory 통합 페이지 2-40을 참조하십시오.

절차

1. **점검** > **관리되지 않는 엔드포인트**로 이동합니다.
2. **Active Directory/IP 주소 범위** 섹션에서 **범위 정의**를 클릭합니다.

   새 화면이 열립니다.
3. Active Directory 범위를 정의하려면 다음을 수행합니다.
   a. **Active Directory 범위** 섹션으로 이동합니다.
   b. 실시간 쿼리를 수행하여 보다 정확한 결과를 얻기 위해 **주문형 점검 사용**을 선택합니다. 이 옵션을 사용하지 않으면 OfficeScan에서 각 OfficeScan 에이전트 대신 데이터베이스를 쿼리합니다. 데이터베이스만 쿼리하면 속도는 더 빠르지만 정확성이 떨어집니다.
   c. 쿼리할 개체를 선택합니다. 처음에 쿼리하는 경우, 계정이 1,000개 미만인 개체를 선택한 후 쿼리를 완료하는 데 소요된 시간을 기록합니다. 이 데이터를 성능 벤치마크로 사용합니다.
4. IP 주소 범위를 정의하려면 다음을 수행합니다.
   a. **IP 주소 범위** 섹션으로 이동합니다.

b. **IP 주소 범위 사용**을 선택합니다.

c. IP 주소 범위를 지정합니다. 더하기 또는 빼기 단추를 클릭하여 IP 주소 범위를 추가하거나 삭제합니다.

- 순수 IPv4 OfficeScan 서버의 경우 IPv4 주소 범위를 입력합니다.
- 순수 IPv6 OfficeScan 서버의 경우 IPv6 접두사와 길이를 입력합니다.
- 이중 스택 OfficeScan 서버의 경우 IPv4 주소 범위 및/또는 IPv6 접두사와 길이를 입력합니다.

  IPv6 주소 범위는 16비트로 제한되며, 이는 IPv4 주소 범위에 대한 제한과 유사합니다. 따라서 접두사 길이는 112자에서 128자 사이여야 합니다.

표 15-9. IPv6 주소의 접두사 길이 및 개수

길이	IPv6 주소 개수
128	2
124	16
120	256
116	4,096
112	65,536

5. 고급 설정에서 OfficeScan 서버가 에이전트와 통신하는 데 사용하는 포트를 지정합니다. OfficeScan 서버 설치 도중, 설치 프로그램이 임의로 포트 번호를 생성합니다.

   OfficeScan 서버에서 사용하는 통신 포트를 확인하려면 **에이전트** > **에이전트 관리**로 이동하여 도메인을 선택합니다. IP 주소 열 옆에 포트가 표시됩니다. Trend Micro는 참조를 위해 포트 번호 기록을 보관할 것을 권장합니다.

   a. **포트 지정**을 클릭합니다.

   b. 포트 번호를 입력하고 **추가**를 클릭합니다. 추가할 모든 포트 번호를 가질 때까지 이 단계를 반복합니다.

c. **저장**을 클릭합니다.

6. 특정 포트 번호를 사용하여 엔드포인트의 연결 상태를 확인하려면 **<x> 포트를 확인하여 엔드포인트를 연결할 수 없는 것으로 선언하십시오.**를 선택합니다. 연결이 설정되지 않은 경우 OfficeScan에서는 즉시 엔드포인트를 연결할 수 없는 상태로 간주합니다. 기본 포트 번호는 135입니다.

   이 설정을 사용하면 쿼리 속도가 빨라집니다. 엔드포인트와의 연결을 설정할 수 없는 경우, OfficeScan 서버는 더 이상 다른 모든 연결 확인 작업을 수행할 필요도 없이 엔드포인트를 연결할 수 없다고 간주합니다.

7. 범위를 저장하고 쿼리를 시작하려면 **저장 및 다시 평가**를 클릭합니다. 설정만 저장하려면 **저장만**을 클릭합니다.

   외부 서버 관리 화면에 쿼리의 결과가 표시됩니다.

참고

특히 쿼리 범위가 넓은 경우, 쿼리를 완료하는 데 시간이 오래 걸릴 수 있습니다. 외부 서버 관리 화면이 결과를 표시할 때까지 다른 쿼리를 수행하지 마십시오. 그렇지 않으면 현재 쿼리 세션이 종료되고 쿼리 프로세스가 다시 시작됩니다.

쿼리 결과 보기

쿼리 결과는 **보안 상태** 섹션 아래에 표시됩니다. 관리되지 않는 엔드포인트의 상태는 다음 중 하나로 표시됩니다.

- 다른 OfficeScan 서버에서 관리
- OfficeScan 에이전트가 설치되지 않음
- 연결할 수 없음
- 해결되지 않은 Active Directory 점검

절차

1. **보안 상태** 섹션에서 숫자 링크를 클릭하여 영향을 받는 모든 컴퓨터를 표시합니다.

2. 검색 기준을 충족하는 컴퓨터만 검색 및 표시하려면 검색 및 고급 검색 기능을 사용합니다.

   고급 검색 기능을 사용하는 경우, 다음 항목을 지정합니다.

   - IPv4 주소 범위
   - IPv6 접두사 및 길이(접두사는 112자에서 128자 사이여야 함)
   - 엔드포인트 이름
   - OfficeScan 서버 이름
   - Active Directory 트리
   - 보안 상태

   이름이 완전하지 않은 경우에는 OfficeScan이 결과를 반환하지 않습니다. 전체 이름이 확실하지 않은 경우 와일드카드 문자(*)를 사용합니다.

3. 컴퓨터의 목록을 파일에 저장하려면 **내보내기**를 클릭합니다.

4. 다른 OfficeScan 서버에서 관리하는 OfficeScan 에이전트의 경우 Agent Mover 도구를 사용하여 현재 OfficeScan 서버에서 이러한 OfficeScan 에이전트를 관리하도록 설정합니다. 이 도구에 대한 자세한 내용은 Agent Mover 페이지 15-22를 참조하십시오.

예약 쿼리 점검 구성

보안 지침을 준수하는지 확인하기 위해 Active Directory 및 IP 주소를 주기적으로 쿼리하도록 OfficeScan 서버를 구성합니다.

절차

1. **점검** > **관리되지 않는 엔드포인트**로 이동합니다.
2. 에이전트 트리의 맨 위에서 **예약 정의**를 클릭합니다.
3. 예약 쿼리를 사용하도록 설정합니다.
4. 일정을 지정합니다.

5. **저장**을 클릭합니다.

Trend Micro 가상 데스크톱 지원

Trend Micro 가상 데스크톱 지원을 사용하여 가상 데스크톱 보호를 최적화합니다. 이 기능은 단일 가상 서버에 있는 OfficeScan 에이전트의 작업을 조정합니다.

단일 서버에서 여러 데스크톱을 실행하고 주문형 검색 또는 구성 요소 업데이트를 수행하면 상당한 시스템 리소스가 소모됩니다. 이 기능을 사용하면 에이전트가 검색 실행이나 구성 요소 업데이트를 동시에 수행하지 못하게 할 수 있습니다.

예를 들어 VMware vCenter 서버에 OfficeScan 에이전트를 실행하는 가상 데스크톱이 세 개인 경우 OfficeScan에서는 지금 검색을 시작하고 세 개 에이전트 모두에 업데이트를 동시에 배포할 수 있습니다. 가상 데스크톱 지원에서는 이러한 에이전트가 동일한 물리적 서버에 있다고 인식합니다. 가상 데스크톱 지원에서는 작업을 첫 번째 에이전트에서 실행하고 첫 번째 에이전트의 작업이 완료될 때까지 다른 두 개 에이전트에서 동일한 작업을 연기할 수 있습니다.

가상 데스크톱 지원은 다음 플랫폼에서 사용할 수 있습니다.

- VMware vCenter™ (VMware View™)
- Citrix™ XenServer™ (Citrix XenDesktop™)
- Microsoft Hyper-V™ Server

다른 가상화 응용 프로그램을 사용하는 관리자의 경우 OfficeScan 서버가 가상 에이전트를 관리하는 에뮬레이트된 하이퍼바이저로 작동할 수도 있습니다.

이러한 플랫폼에 대한 자세한 내용은 VMware View, Citrix XenDesktop 또는 Microsoft Hyper-V 웹 사이트를 참조하십시오.

OfficeScan VDI 설치 전 검색 템플릿 생성 도구를 사용하여 주문형 검색을 최적화하거나 기본 또는 골든 이미지에서 GUID를 제거합니다.

가상 데스크톱 지원 설치

가상 데스크톱 지원은 기본 OfficeScan 기능이지만 별도의 라이선스가 부여됩니다. OfficeScan 서버를 설치하면 이 기능이 제공되지만 기능이 작동하지는 않습

니다. 이 기능을 설치한다는 것은 액티브업데이트 서버 또는 사용자 지정 업데이트 소스(설정된 경우)에서 파일을 다운로드하는 것을 의미합니다. 이 파일이 OfficeScan 서버에 통합되면 가상 데스크톱 지원을 활성화하여 전체 기능을 사용할 수 있습니다. 설치 및 활성화는 Plug-in Manager에서 수행됩니다.

참고

순수 IPv6 환경에서는 가상 데스크톱 지원이 제대로 지원되지 않습니다. 자세한 내용은 순수 IPv6 서버 제한 사항 페이지 A-3를 참조하십시오.

가상 데스크톱 지원 설치

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**를 클릭합니다.
2. **Plug-in Manager** 화면에서 **Trend Micro 가상 데스크톱 지원** 섹션으로 이동하여 **다운로드**를 클릭합니다.

   다운로드 단추 옆에 패키지 크기가 표시됩니다.

   Plug-in Manager는 다운로드한 패키지를 <서버 설치 폴더>₩PCCSRV₩Download₩Product에 저장합니다.

   참고

   Plug-in Manager에서 파일을 다운로드할 수 없는 경우 24시간 후에 자동으로 다시 다운로드됩니다. 패키지를 다운로드하도록 Plug-in Manager를 수동으로 트리거하려면 Microsoft Management Console에서 OfficeScan Plug-in Manager 서비스를 다시 시작하십시오.
3. 다운로드 진행률을 확인합니다. 다운로드하는 동안 다른 화면으로 이동할 수도 있습니다.

   패키지를 다운로드하는 동안 문제가 발생하면 OfficeScan 제품 콘솔에서 서버 업데이트 로그를 확인하십시오. 기본 메뉴에서 **로그** > **서버 업데이트**를 클릭합니다.

   Plug-in Manager가 파일을 다운로드한 후 가상 데스크톱 지원이 새 화면에 표시됩니다.

참고

가상 데스크톱 지원이 표시되지 않는 경우 Plug-in Manager 문제 해결 페이지 17-12에서 원인과 해결 방법을 확인하십시오.

4. 가상 데스크톱 지원을 즉시 설치하려면 **지금 설치**를 클릭합니다. 나중에 설치하려면 다음을 수행합니다.
   a. **나중에 설치**를 클릭합니다.
   b. **Plug-in Manager** 화면을 엽니다.
   c. **Trend Micro 가상 데스크톱 지원** 섹션으로 이동하여 **설치**를 클릭합니다.
5. 사용권 계약 내용을 읽고 **동의**를 클릭하여 조건에 동의합니다.

   설치가 시작됩니다.
6. 설치 진행률을 모니터링합니다. 설치 후 가상 데스크톱 지원 버전이 표시됩니다.

가상 데스크톱 지원 라이선스

Plug-in Manager에서 가상 데스크톱 지원 라이선스를 보고 활성화하고 갱신할 수 있습니다.

Trend Micro에서 정품 인증 코드를 받아 이 코드를 사용하여 가상 데스크톱 지원의 전체 기능을 활성화할 수 있습니다.

가상 데스크톱 지원 활성화 또는 갱신

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**를 클릭합니다.
2. **Plug-in Manager** 화면에서 **Trend Micro 가상 데스크톱 지원** 섹션으로 이동하여 **프로그램 관리**를 클릭합니다.

3. **라이선스 정보 보기**를 클릭합니다.
4. **제품 라이선스 세부 정보** 화면이 열리면 **새 정품 인증 코드**를 클릭합니다.
5. 열려 있는 화면에서 정품 인증 코드를 입력하고 **저장**을 클릭합니다.
6. 다시 제품 라이선스 세부 정보 화면에서 **정보 업데이트**를 클릭하여 화면에서 새 라이선스 세부 정보 및 기능 상태를 새로 고칩니다. 이 화면에는 라이선스에 대한 세부 정보를 볼 수 있는 Trend Micro 웹 사이트에 대한 링크도 제공됩니다.

가상 데스크톱 지원에 대한 라이선스 정보 보기

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인** > **[Trend Micro 가상 데스크톱 지원] 프로그램 관리**을 클릭합니다.
2. **라이선스 정보 보기**를 클릭합니다.
3. 화면이 열리면 라이선스 세부 정보를 확인합니다.

   가상 데스크톱 지원 라이선스 세부 정보 섹션에서는 다음 정보를 제공합니다.

   - **상태**: "정품 인증됨", "정품 인증되지 않음" 또는 "만료됨"이 표시됩니다.
   - **버전**: "정식" 또는 "평가판" 버전이 표시됩니다. 정식 버전과 평가판이 모두 있는 경우에는 버전이 "정식"으로 표시됩니다.
   - **만료일**: 가상 데스크톱 지원에 여러 개의 라이선스가 있는 경우 가장 늦은 만료일이 표시됩니다. 예를 들어, 라이선스 만료일이 2010/12/31 및 2010/06/30인 경우에는 2010/12/31 표시됩니다.
   - **사용자 수**: 가상 데스크톱 지원을 사용할 수 있는 OfficeScan 에이전트 에이전트 수를 표시합니다.
   - **정품 인증 코드**: 정품 인증 코드가 표시됩니다.

   다음과 같은 경우에 라이선스에 대한 미리 알림이 표시됩니다.

정식 버전 라이선스를 소유한 경우:

- 기능의 유예 기간 중. 유예 기간은 지역에 따라 다릅니다. Trend Micro 대리점에서 유예 기간을 확인하십시오.
- 라이선스가 만료되고 유예 기간이 경과된 경우. 이 기간 중에는 기술 지원을 받을 수 없습니다.

평가판 라이선스를 소유한 경우:

- 라이선스가 만료된 경우. 이 기간 중에는 기술 지원을 받을 수 없습니다.

4. **온라인으로 자세한 라이선스 보기**를 클릭하여 Trend Micro 웹 사이트에서 라이선스에 대한 정보를 확인합니다.
5. 최신 라이선스 정보로 화면을 업데이트하려면 **정보 업데이트**를 클릭합니다.

가상 서버 연결

VMware vCenter 4(VMware View 4), Citrix XenServer 5.5(Citrix XenDesktop 4) 또는 Microsoft Hyper-V Server를 추가하여 주문형 검색 또는 구성 요소 업데이트를 최적화합니다. OfficeScan 서버는 지정된 가상 서버와 통신하여 동일한 물리적 서버에 있는 OfficeScan 에이전트를 확인합니다.

다른 VDI 서버의 경우 OfficeScan 서버는 에뮬레이트된 가상 하이퍼바이저를 제공하여 다른 플랫폼의 가상 에이전트를 관리합니다. OfficeScan 하이퍼바이저는 가상 에이전트 요청을 서버에서 수신하는 순서대로 처리합니다. OfficeScan 서버는 요청을 한 번에 하나씩 처리하고 다른 요청은 대기열에 넣습니다.

서버 연결 추가

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인** > **[Trend Micro 가상 데스크톱 지원] 프로그램 관리**을 클릭합니다.

2. **VMware vCenter Server**, **Citrix XenServer**, **Microsoft Hyper-V** 또는 **기타 가상화 응용 프로그램**을 선택합니다.

   참고

   기타 가상화 응용 프로그램을 선택할 경우 추가 정보가 필요하지 않습니다. OfficeScan 서버는 요청을 수신하는 순서대로 가상 에이전트 요청에 응답합니다.

3. 서버에 대한 연결을 사용합니다.
4. 다음 정보를 지정합니다.
   - VMware vCenter 및 Citrix XenServer 서버의 경우
     - IP 주소
     - 포트
     - 연결 프로토콜(HTTP 또는 HTTPS)
     - 사용자 이름:
     - 암호
   - Microsoft Hyper-V Server의 경우
     - 호스트 이름 또는 IP 주소
     - 도메인\사용자 이름:

       참고

       로그온 계정은 관리자 그룹의 도메인 계정이어야 합니다.

     - 암호
5. 필요에 따라 VMware vCenter 또는 Citrix XenServer에 대한 프록시 연결을 사용하도록 설정합니다.
   a. 프록시 서버 이름 또는 IP 주소 및 포트를 지정합니다.
   b. 프록시 서버에 인증이 필요한 경우 사용자 이름 및 암호를 지정합니다.

6. **연결 테스트**를 클릭하여 OfficeScan 서버가 서버에 제대로 연결될 수 있는지 확인합니다.

   참고

   Microsoft Hyper-V 연결 문제 해결에 대한 자세한 내용은 Microsoft Hyper-V 연결 문제 해결 페이지 15-81을 참조하십시오.

7. **저장**을 클릭합니다.

추가 서버 연결 추가

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인** > **[Trend Micro 가상 데스크톱 지원] 프로그램 관리**을 클릭합니다.
2. **새 vCenter 연결 추가**, **새 XenServer 연결 추가** 또는 **새 Hyper-V 연결 추가**를 클릭합니다.
3. 단계를 반복하여 적절한 서버 정보를 제공합니다.
4. **저장**을 클릭합니다.

연결 설정 삭제

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인** > **[Trend Micro 가상 데스크톱 지원] 프로그램 관리**으로 이동합니다.
2. **이 연결 삭제**를 클릭합니다.
3. **확인**을 클릭하여 이 설정을 삭제할지 확인합니다.
4. **저장**을 클릭합니다.

VDI 검색 용량 변경

관리자는 vdi.ini 파일을 수정하여, 동시 검색을 실행하는 VDI 엔드포인트 수를 늘릴 수 있습니다. Trend Micro에서는 VDI 용량 변경에 따른 영향을 엄격히 모니터링하여 시스템 리소스에서 증가된 검색을 처리할 수 있는지 확인할 것을 권장합니다.

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>PCCSRV₩Private₩vdi.ini로 이동합니다.

2. `[TaskController]` 설정을 찾습니다.

   기본 TaskController 설정은 다음과 같습니다.

   - OfficeScan 10.5 클라이언트의 경우

     ```
     [TaskController]

     Controller_00_MaxConcurrentGuests=1

     Controller_01_MaxConcurrentGuests=3
     ```

     여기서 각 항목은 다음과 같습니다.

     - `Controller_00_MaxConcurrentGuests=1`은 검색을 동시에 수행할 수 있는 최대 클라이언트 수와 동일합니다.
     - `Controller_01_MaxConcurrentGuests=3`은 업데이트를 동시에 수행할 수 있는 최대 클라이언트 수와 동일합니다.

   - OfficeScan 10.6 클라이언트 및 OfficeScan 11.0(이상) 에이전트의 경우:

     ```
     [TaskController]

     Controller_02_MaxConcurrentGuests=1

     Controller_03_MaxConcurrentGuests=3
     ```

     여기서 각 항목은 다음과 같습니다.

- `Controller_02_MaxConcurrentGuests=1`은 검색을 동시에 수행할 수 있는 최대 클라이언트 수와 동일합니다.
- `Controller_03_MaxConcurrentGuests=3`은 업데이트를 동시에 수행할 수 있는 최대 클라이언트 수와 동일합니다.

3. 필요한 경우 각 컨트롤러의 수를 늘리거나 줄입니다.

   모든 설정의 최소값은 1입니다.

   모든 설정의 최대값은 65536입니다.

4. vdi.ini 파일을 저장하고 닫습니다.
5. OfficeScan Master Service를 다시 시작합니다.
6. VDI 엔드포인트의 CPU, 메모리 및 디스크 사용 리소스를 모니터링합니다. 1~5단계 반복을 통해 컨트롤러 설정을 추가로 수정하여 VDI 환경에 가장 잘 맞게 동시 검색 수를 늘리거나 줄입니다.

Microsoft Hyper-V 연결 문제 해결

Microsoft Hyper-V 연결에서는 에이전트-서버 통신에 WMI(Windows Management Instrumentation) 및 DCOM을 사용합니다. 방화벽 정책이 이 통신을 차단하여 Hyper-V Server에 연결하지 못할 수 있습니다.

Hyper-V Server 수신 포트는 기본적으로 포트 135를 사용한 후 추가 통신을 위해 임의로 구성된 포트를 선택합니다. 이 두 포트 중 하나 또는 WMI 트래픽이 방화벽에 의해 차단된 경우 서버와의 통신에 실패합니다. 관리자는 Hyper-V Server와의 통신을 허용하도록 방화벽 정책을 수정할 수 있습니다.

다음 방화벽 알림을 수행하기 전에 IP 주소, 도메인\사용자 이름 및 암호를 비롯한 모든 연결 설정이 올바른지 확인합니다.

Windows 방화벽을 통해 WMI 통신 허용

절차

1. Hyper-V Server에서 **Windows 방화벽 허용되는 프로그램** 화면을 엽니다.

   Windows 2008 R2 시스템에서 **제어판** > **시스템 및 보안** > **Windows 방화벽** > **Windows 방화벽을 통해 프로그램 또는 기능 허용**으로 이동합니다.

2. **WMI(Windows Management Instrumentation)**를 선택합니다.

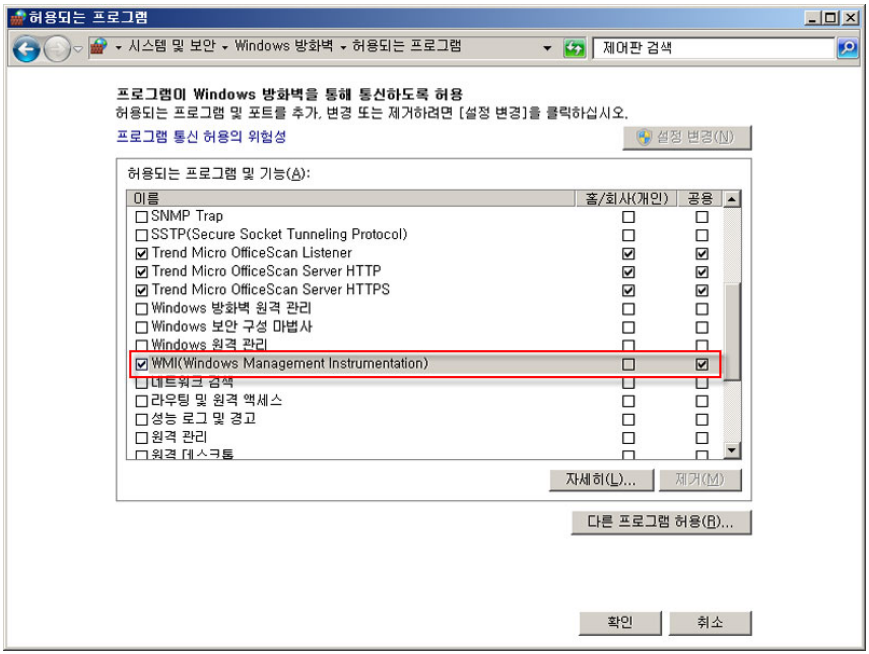


그림 15-7. Windows 방화벽 허용되는 프로그램 화면

3. **저장**을 클릭합니다.
4. Hyper-V 연결을 다시 테스트합니다.

Windows 방화벽 또는 타사 방화벽을 통해 포트 통신 열기

절차

1. Hyper-V Server에서 방화벽이 포트 135를 통한 통신을 허용하는지 확인하고 Hyper-V 연결을 다시 테스트합니다.

   포트를 여는 방법에 대한 자세한 내용은 해당 방화벽 설명서를 참조하십시오.

2. Hyper-V Server에 연결하지 못한 경우 고정 포트를 사용하도록 WMI를 구성합니다.

   *WMI용 고정 포트 설정*에 대한 자세한 내용은 다음을 참조하십시오.

   http://msdn.microsoft.com/en-us/library/windows/desktop/bb219447(v=vs.85).aspx

3. 방화벽을 통한 통신을 위해 포트 135와 새로 만든 고정 포트(24158)를 엽니다.

4. Hyper-V 연결을 다시 테스트합니다.

VDI 설치 전 검색 템플릿 생성 도구

OfficeScan VDI 설치 전 검색 템플릿 생성 도구를 사용하여 주문형 검색을 최적화하거나 기본 또는 골든 이미지에서 GUID를 제거합니다. 이 도구는 기본 또는 골든 이미지를 검색하고 이미지를 인증합니다. 이 이미지 복제를 검색하는 경우 OfficeScan은 변경된 부분만 확인합니다. 이를 통해 검색 시간을 단축합니다.

팁

Trend Micro는 Windows Update 적용 후 또는 새 응용 프로그램 설치 후 설치 전 검색 템플릿 생성을 권장합니다.

설치 전 검색 템플릿 생성

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩TCacheGen으로 이동합니다.
2. VDI 설치 전 검색 템플릿 생성 도구를 선택합니다. 다음 버전을 사용할 수 있습니다.

   표 15-10. VDI 설치 전 검색 템플릿 생성 도구 버전

파일 이름	지침
TCacheGen.exe	32비트 플랫폼에서 직접 도구를 실행하려면 이 파일을 선택합니다.
TCacheGen_x64.exe	64비트 플랫폼에서 직접 도구를 실행하려면 이 파일을 선택합니다.
TCacheGenCli.exe	32비트 플랫폼의 명령줄 인터페이스에서 도구를 실행하려면 이 파일을 선택합니다.
TCacheGenCli_x64.exe	64비트 플랫폼의 명령줄 인터페이스에서 도구를 실행하려면 이 파일을 선택합니다.

3. 이전 단계에서 선택한 도구 버전을 엔드포인트에 복사합니다.
4. 도구를 실행합니다.
   - 도구를 직접 실행하려면
     a. TCacheGen.exe 또는 TCacheGen_x64.exe를 두 번 클릭합니다.
     b. **설치 전 검색 템플릿 생성**을 선택하고 **다음**을 클릭합니다.
   - 명령줄 인터페이스에서 도구를 실행하려면
     a. 명령 프롬프트를 열고 디렉터리를 <에이전트 설치 폴더>로 변경합니다.
     b. 다음 명령을 입력합니다.

```
TCacheGenCli Generate_Template
```

또는

```
TcacheGenCli_x64 Generate_Template
```

참고

설치 전 검색 템플릿을 생성하고 GUID를 제거하기 전에 도구가 보안 위협이 있는 이미지를 검색합니다.

설치 전 검색 템플릿을 생성한 후 도구에서 OfficeScan 에이전트를 종료합니다. OfficeScan 에이전트를 다시 로드하지 마십시오. OfficeScan 에이전트를 다시 로드할 경우 설치 전 검색 템플릿을 다시 만들어야 합니다.

템플릿에서 GUID 제거

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩TCacheGen으로 이동합니다.
2. VDI 설치 전 검색 템플릿 생성 도구를 선택합니다. 다음 버전을 사용할 수 있습니다.

표 15-11. VDI 설치 전 검색 템플릿 생성 도구 버전

파일 이름	지침
TCacheGen.exe	32비트 플랫폼에서 직접 도구를 실행하려면 이 파일을 선택합니다.
TCacheGen_x64.exe	64비트 플랫폼에서 직접 도구를 실행하려면 이 파일을 선택합니다.
TCacheGenCli.exe	32비트 플랫폼의 명령줄 인터페이스에서 도구를 실행하려면 이 파일을 선택합니다.
TCacheGenCli_x64.exe	64비트 플랫폼의 명령줄 인터페이스에서 도구를 실행하려면 이 파일을 선택합니다.

3. 이전 단계에서 선택한 도구 버전을 엔드포인트에 복사합니다.

4. 도구를 실행합니다.
   - 도구를 직접 실행하려면
     a. TCacheGen.exe 또는 TCacheGen_x64.exe를 두 번 클릭합니다.
     b. **템플릿에서 GUID 제거**를 선택하고 **다음**을 클릭합니다.
   - 명령줄 인터페이스에서 도구를 실행하려면
     a. 명령 프롬프트를 열고 디렉터리를 <에이전트 설치 폴더>로 변경합니다.
     b. 다음 명령을 입력합니다.

        ```
        TCacheGenCli Remove GUID
        ```

        또는

        ```
        TcacheGenCli_x64 Remove GUID
        ```

글로벌 에이전트 설정

OfficeScan은 글로벌 에이전트 설정을 모든 에이전트에 적용하거나 특정 권한이 있는 에이전트에만 적용합니다.

절차

1. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.
2. 다음 설정을 구성합니다.

표 15-12. 글로벌 에이전트 설정

탭	설정	참조
보안 설정	검색 설정	검색 설정 섹션 페이지 7-71
	예약 검색 설정	예약 검색 설정 섹션 페이지 7-76
	방화벽 설정	글로벌 방화벽 설정 페이지 13-24
	의심스러운 연결 설정	글로벌 사용자 정의 IP 목록 설정 구성 페이지 8-6
	동작 모니터링 설정	글로벌 동작 모니터링 설정 구성 페이지 9-12
시스템	인증된 안전한 소프트웨어 서비스 설정	글로벌 검색 설정 구성 페이지 7-69
	스마트 보호 서비스 프록시	글로벌 스마트 보호 서비스 프록시 설정 구성 페이지 15-49
	업데이트	• 액티브업데이트 서버를 OfficeScan 에이전트 업데이트 소스로 사용 페이지 6-35 • OfficeScan 에이전트 업데이트를 위한 예약된 디스크 공간 구성 페이지 6-46
	서비스 다시 시작	OfficeScan 에이전트 서비스 다시 시작 페이지 15-11
네트워크	프록시 구성	OfficeScan 에이전트에 대한 자동 프록시 설정 페이지 15-51
	기본 IP 주소	에이전트 IP 주소 페이지 5-10
	서버-에이전트 통신	서버-에이전트 통신에 대해 향상된 암호화 페이지 14-57
	바이러스/악성 프로그램 로그 대역폭 설정	글로벌 검색 설정 구성 페이지 7-69
	연결할 수 없는 네트워크	연결할 수 없는 에이전트 페이지 15-42

탭	설정	참조
에이전트 제어	일반 설정	글로벌 검색 설정 구성 페이지 7-69
	경고 설정	OfficeScan 에이전트 업데이트 알림 구성 페이지 6-47
	에이전트 언어 구성	OfficeScan 에이전트 언어 구성 페이지 15-21

3. **저장**을 클릭합니다.

에이전트 권한 및 기타 설정 구성

사용자에게 OfficeScan 에이전트에서 특정 설정을 수정하고 높은 수준의 작업을 수행하는 권한을 부여합니다.

참고

바이러스 백신 설정은 OfficeScan 바이러스 백신 기능을 활성화한 후에만 표시됩니다.

팁

조직 전체에 동일한 설정 및 정책을 실행하려면 사용자에게 제한된 권한을 부여합니다.

절차

1. **에이전트** > **에이전트 관리**로 이동합니다.
2. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 포함하거나 아니면 특정 도메인 또는 에이전트를 선택합니다.
3. **설정** > **권한 및 기타 설정**을 클릭합니다.
4. **권한** 탭에서 다음 사용자 권한을 구성합니다.

표 15-13. 에이전트 권한

에이전트 권한	참조
독립 모드 권한	OfficeScan 에이전트 독립 모드 권한 페이지 15-19
검색 권한	검색 유형 권한 페이지 7-54
예약 검색 권한	예약 검색 권한 및 기타 설정 페이지 7-57
방화벽 권한	방화벽 권한 페이지 13-22
동작 모니터링 권한	동작 모니터링 권한 페이지 9-14
신뢰할 수 있는 프로그램 목록	신뢰할 수 있는 프로그램 목록 권한 페이지 7-68
메일 검색 권한	메일 검색 권한 및 기타 설정 페이지 7-62
프록시 설정 권한	에이전트에 대한 프록시 구성 권한 페이지 15-50
구성 요소 업데이트 권한	업데이트 권한 및 기타 설정 구성 페이지 6-43
종료 및 잠금 해제	에이전트 종료 및 잠금 해제 권한 부여 페이지 15-18
제거	OfficeScan 에이전트 제거 권한 부여 페이지 5-72

5. **기타 설정** 탭을 클릭하고 다음 설정을 구성합니다.

표 15-14. 기타 에이전트 설정

설정	참조
업데이트 설정	업데이트 권한 및 기타 설정 구성 페이지 6-43
웹 검증 설정	에이전트 사용자에 대한 웹 위협 알림 페이지 12-13
동작 모니터링 설정	동작 모니터링 권한 페이지 9-14
C&C 연결 알림 설정	에이전트 사용자에 대한 C&C 연결 알림 서비스 페이지 12-17

설정	참조
중앙 격리 보관 복원 경고 설정	격리된 파일을 복원한 후 엔드포인트에 알림 메시지를 표시합니다.
머신러닝 설정	알 수 없는 위협을 탐지한 후 엔드포인트에 알림 메시지를 표시합니다.
OfficeScan 에이전트 자기 보호	OfficeScan 에이전트 자기 보호 페이지 15-12
예약 검색 설정	예약 검색 권한 부여 및 권한 알림 표시 페이지 7-58
검색을 위한 캐시 설정	검색을 위한 캐시 설정 페이지 7-64
POP3 전자 메일 검색 설정	메일 검색 권한 부여 및 POP3 메일 검색 사용 페이지 7-63
OfficeScan 에이전트 액세스 제한	OfficeScan 에이전트 콘솔 액세스 제한 페이지 15-17
다시 시작 알림	OfficeScan 에이전트 사용자를 위한 보안 위험 알림 페이지 7-85

6. 에이전트 트리에서 도메인 또는 에이전트를 선택한 경우 **저장**을 클릭합니다. 루트 도메인 아이콘을 클릭한 경우 다음 옵션 중에서 선택합니다.

   - **모든 에이전트에 적용**: 모든 기존 에이전트와 기존/이후 도메인에 추가되는 모든 새 에이전트에 설정을 적용합니다. 이후 도메인은 설정을 구성할 때 아직 만들어지지 않은 도메인입니다.
   - **이후 도메인에만 적용**: 이후 도메인에 추가되는 에이전트에만 설정을 적용합니다. 이 옵션은 기존 도메인에 추가된 새 에이전트에는 설정을 적용하지 않습니다.

부 IV

추가 보호 제공

장 16

외부 에이전트 보호

이 장에서는 기업 인트라넷에서 나가는 OfficeScan 에이전트를 보호하는 데 필요한 Edge 릴레이 서버 설치 및 구성 단계에 대해 설명합니다.

다음과 같은 항목이 포함됩니다.

- Edge 릴레이 서버 페이지 16-2
- Edge 릴레이 서버 시스템 요구 사항 페이지 16-3
- Edge 릴레이 서버 설치 페이지 16-4
- Edge 릴레이 서버에 연결 페이지 16-13
- Edge 릴레이 서버 연결 관리 페이지 16-14
- Edge 릴레이 서버 인증서 관리 페이지 16-15

Edge 릴레이 서버

OfficeScan Edge 릴레이 서버는 사용자가 회사 인트라넷 외부에서 사용하는 엔드포인트에 대한 향상된 보호와 관리자 가시성을 제공합니다.
DMZ(Demilitarized Zone)에 Edge 릴레이 서버를 설치함으로써, OfficeScan 서버에 대해 기능적 연결을 설정할 수 없는 오프 프레미스 OfficeScan 에이전트는 계속 다음 표의 작업을 수행할 수 있습니다.

중요

Edge 릴레이 서버는 IPv6 통신을 지원하지 않습니다.

작업	설명
의심스러운 개체 목록 동기화	Edge 릴레이 서버는 구성된 일정을 기반으로 OfficeScan 서버에서 업데이트된 의심스러운 개체 목록을 수신하고 해당 목록을 외부 에이전트에 배포합니다. 자세한 내용은 의심스러운 개체 목록 설정 페이지 14-31를 참조하십시오.
샘플 제출	외부 에이전트가 알 수 없는 위협을 탐지하는 경우 의심스러운 개체를 구성된 Virtual Analyzer에 보낼 수 있습니다. 의심스러운 개체가 외부 에이전트에서 Virtual Analyzer로 제출되는 과정은 다음과 같습니다. 1. 외부 에이전트가 Edge 릴레이 서버로 개체를 전송합니다. 2. Edge 릴레이 서버는 구성된 다음 동기화 중에 개체를 OfficeScan 서버로 전달합니다. 3. OfficeScan 서버는 분석을 위해 개체를 Virtual Analyzer로 전달합니다. 자세한 내용은 샘플 제출 페이지 8-8를 참조하십시오.
로그 제출	Edge 릴레이 서버는 외부 에이전트 로그를 수집하고 구성된 일정을 기반으로 로그 데이터를 OfficeScan 서버에 정기적으로 보냅니다.
상태 보고서	외부 에이전트는 현재 패턴 또는 구성 요소 버전과 같은 상태 업데이트를 Edge 릴레이 서버로 보냅니다.

Edge 릴레이 서버가 구성되면 OfficeScan 에이전트에서 해당 설정을 수신하고 OfficeScan 서버에 대한 연결을 사용할 수 없게 되면 자동으로 Edge 릴레이 서버에 보고합니다.

Edge 릴레이 서버, OfficeScan 서버 및 OfficeScan 에이전트 간의 통신은 인증서 인증을 사용하여 암호화됩니다.

자세한 내용은 Edge 릴레이 서버 인증서 관리 페이지 16-15를 참조하십시오.

Edge 릴레이 서버 시스템 요구 사항

Edge 릴레이 서버를 설치하기 전에 대상 서버 컴퓨터가 최소 시스템 요구 사항을 충족하는지 확인하십시오.

리소스	요구 사항
프로세서	2GHz 듀얼 코어
메모리	4 GB
디스크 공간	50 GB
운영 체제	Windows Server 2012 R2

네트워크 카드	• 네트워크 카드 2개
	  • 하나는 OfficeScan 서버에 대한 인트라넷 연결용
	  • 다른 하나는 오프 프레미스 OfficeScan 에이전트에 대한 외부 연결용
	• 인트라넷 및 인터넷 연결에 서로 다른 포트를 사용하도록 구성된 네트워크 카드 1개

리소스	요구 사항
데이터베이스	• SQL Server™ 2008 R2 Express(이상) • SQL Server™ 2008 R2(이상) **참고** OfficeScan Edge 릴레이 서버 설치 프로그램은 설치 중에 SQL Server 2014 SP2 Express를 설치할 수 있는 옵션을 제공합니다.

Edge 릴레이 서버 설치

Edge 릴레이 서버를 설치하기 전에 대상 서버 컴퓨터가 최소 시스템 요구 사항을 충족하는지 확인하십시오.

자세한 내용은 Edge 릴레이 서버 시스템 요구 사항 페이지 16-3를 참조하십시오.

중요

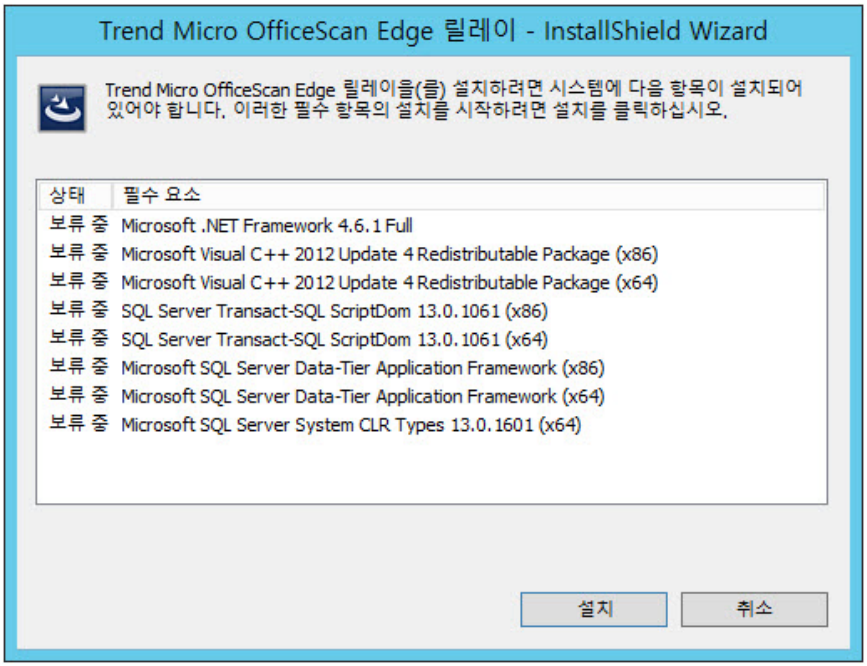
Edge 릴레이 서버는 IPv6 통신을 지원하지 않습니다.

절차

1. OfficeScan 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV₩Admin₩Utility ₩EdgeServer 폴더를 찾은 다음 해당 폴더를 대상 Edge 릴레이 서버 컴퓨터에 복사합니다.
2. 대상 Edge 릴레이 서버에서 EdgeServer 폴더를 열고 setup.exe 파일을 실행하여 설치 프로세스를 시작합니다.

   설치 패키지가 서버에서 필수 구성 요소를 확인합니다.
3. 서버에 다음과 같은 구성 요소가 없는 경우 **설치**를 클릭하여 설치 프로그램이 Edge 릴레이 서버 설치 프로세스 중에 누락된 구성 요소를 설치하도록 허용합니다.

- Microsoft .NET Framework 4.5 전체
- Microsoft Visual C++ 2012 Update 4 재배포 가능 패키지(x64)
- Microsoft SQL Server 시스템 CLR 유형 10.00.2531(x64)
- SQL Server Transact-SQL ScriptDom (x64)
- Microsoft SQL Server 데이터 계층 응용 프로그램 프레임워크(x64)

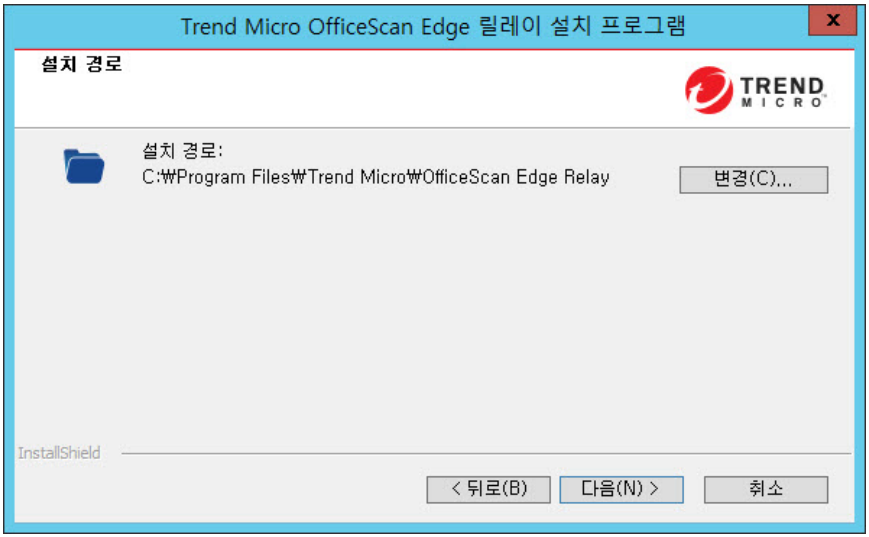


시작 화면이 나타납니다.

4. **다음**을 클릭합니다.

설치 경로 화면이 나타납니다.

5. 기본 설치 디렉터리를 적용하거나 **변경...**을 클릭하여 다른 위치를 선택합니다.



6. **다음>**을 클릭합니다.

   Edge 릴레이 서버 - OfficeScan 에이전트 연결 화면이 나타납니다.

7. Edge 릴레이 서버 연결을 위해 오프 프레미스 OfficeScan 에이전트에서 사용하는 다음 설정을 지정합니다.

   - **FQDN(정규화된 도메인 이름)**: Edge 릴레이 서버의 FQDN을 입력합니다.
   - **IP 주소**: IP 주소 형식을 선택합니다.

     중요

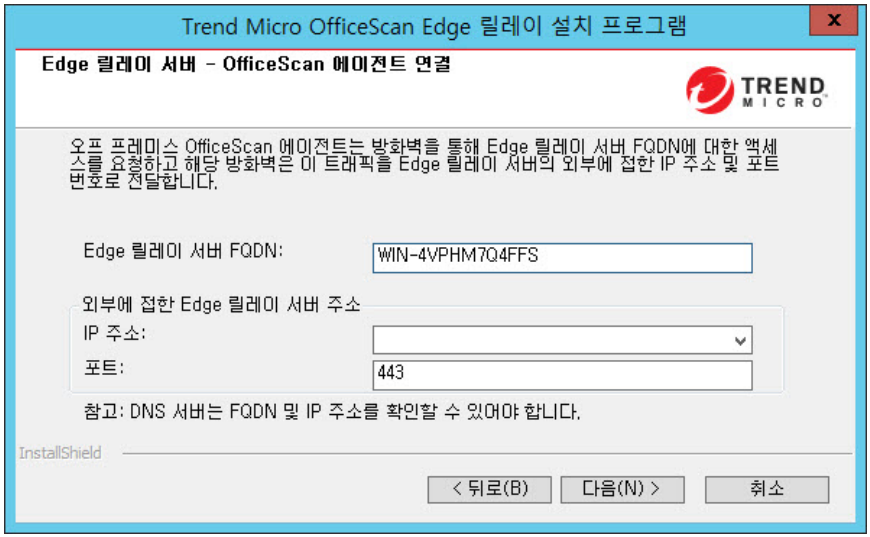
     Edge 릴레이 서버는 IPv6 통신을 지원하지 않습니다.

   - **포트**: 기본 포트를 적용하거나 포트를 지정합니다.

중요

다음을 허용하려면 방화벽 및 게이트웨이를 구성해야 합니다.

- 인터넷에서 Edge 릴레이 서버로 OfficeScan 에이전트 통신의 리디렉션
- 지정된 포트를 통한 통신



8. **다음>**을 클릭합니다.

   Edge 릴레이 서버 - OfficeScan 서버 연결 화면이 나타납니다.

9. Edge 릴레이 서버 연결을 위해 OfficeScan 서버에서 사용하는 다음 설정을 지정합니다.

   - **IP 주소**: IP 주소 형식을 선택합니다.

     중요

     Edge 릴레이 서버는 IPv6 통신을 지원하지 않습니다.

   - **포트**: 기본 포트를 적용하거나 포트를 지정합니다.

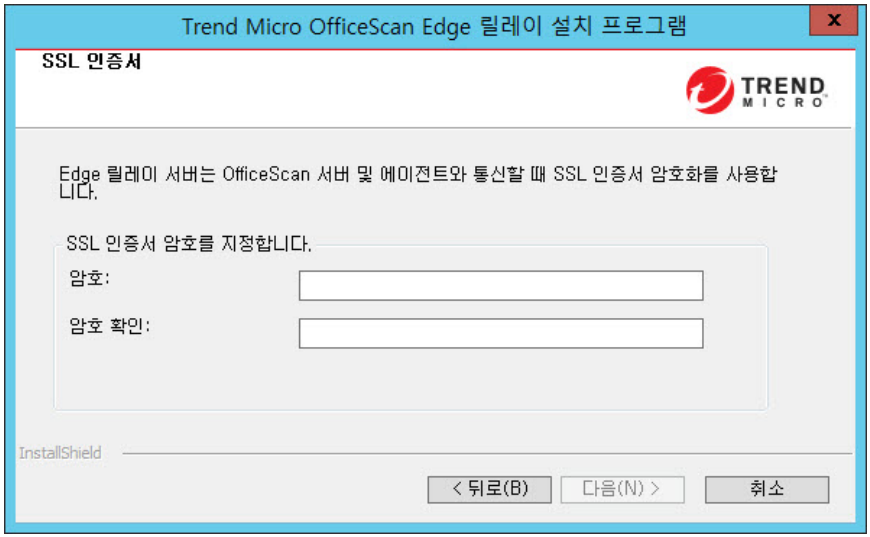
중요

- OfficeScan 서버의 포트는 오프 프레미스 OfficeScan 에이전트에 대해 구성된 포트와 같을 수 없습니다.
- 방화벽이 지정된 포트를 통한 통신을 허용하는지 확인합니다.

10. **다음>**을 클릭합니다.

    SSL 인증서 화면이 나타납니다.

11. Edge 릴레이 서버 인증서에 사용할 암호를 지정하고 확인합니다.

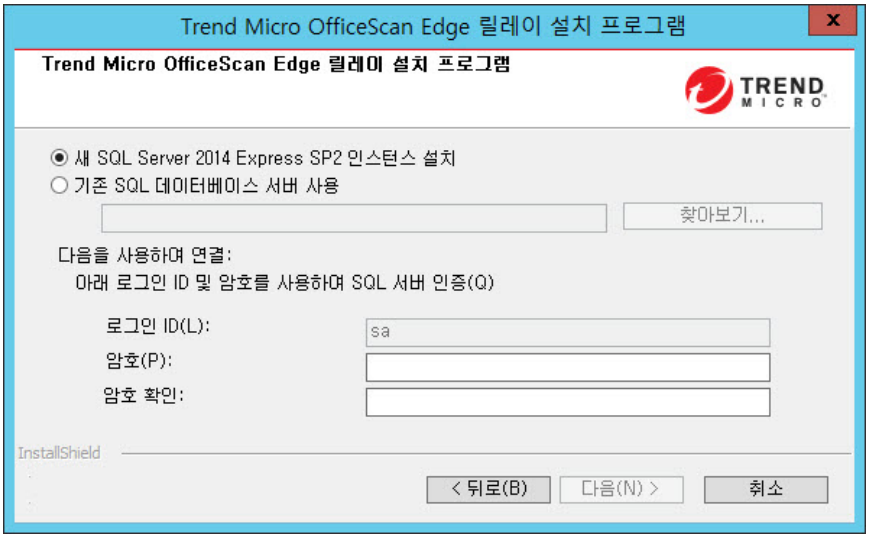


12. **다음>**을 클릭합니다.

    데이터베이스 서버 화면이 나타납니다.

13. Edge 릴레이 서버에서 사용하는 SQL Server 데이터베이스를 지정합니다.

    - **새 SQL Server 2008 R2 SP2 Express 인스턴스 설치**
    - **기존 SQL 데이터베이스 서버 사용**: **찾아보기...**를 클릭하고 목록의 사용 가능한 서버에서 선택합니다.

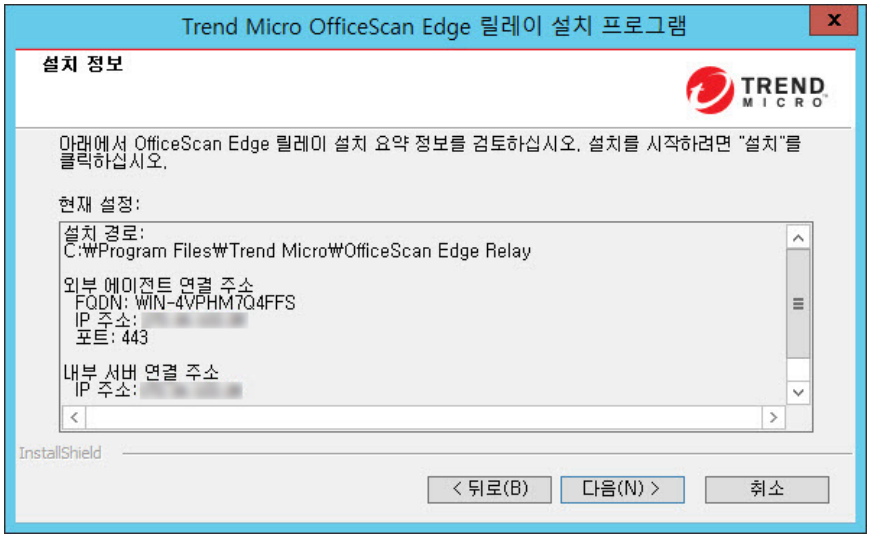


14. SQL Server 데이터베이스에 연결하는 데 사용할 암호를 지정합니다. 새로운 SQL Server Express 데이터베이스를 설치 중인 경우 암호를 확인합니다.

15. **다음>**을 클릭합니다.

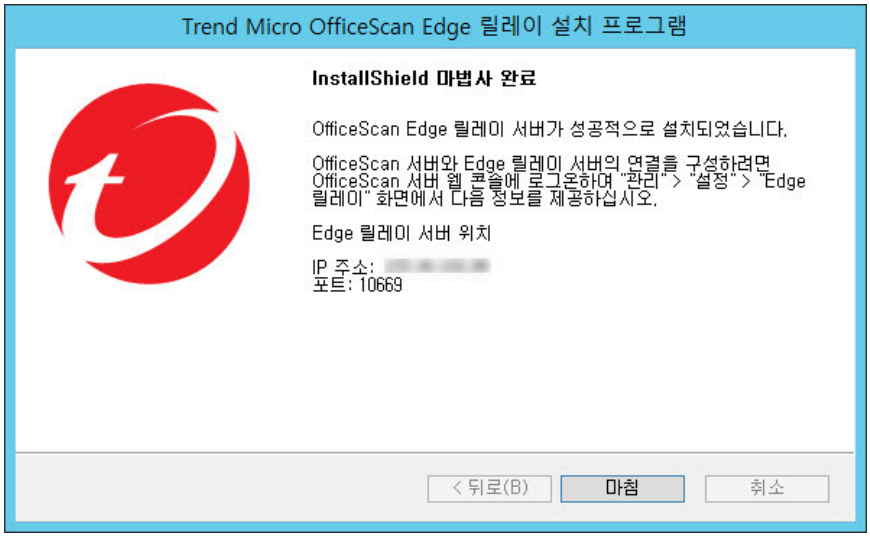
    설치 정보 화면이 나타납니다.

16. 설치를 시작하려면 **다음 >**을 클릭합니다.



설치가 완료되고 나면 **InstallShield 마법사 완료** 화면이 나타납니다.

17. **마침**을 클릭합니다.



Edge 릴레이 서버를 사용할 준비가 되었습니다. Edge 릴레이 서버와 연결하도록 OfficeScan 서버를 구성할 수 있습니다.

자세한 내용은 Edge 릴레이 서버에 연결 페이지 16-13를 참조하십시오.

Edge 릴레이 서버에 연결

Edge 릴레이 서버를 설치한 후에는 OfficeScan 서버에서 Edge 릴레이 서버 연결 설정을 구성해야 합니다. Edge 릴레이 서버에 연결한 후, OfficeScan 서버에 보고하는 OfficeScan 에이전트는 연결 설정을 수신하고 기업 인트라넷을 벗어난 후에 자동으로 Edge 릴레이 서버와 통신할 수 있습니다.

절차

1. OfficeScan 웹 콘솔에서 **관리** > **설정** > **Edge 릴레이**로 이동합니다.

   Edge 릴레이 설정 화면이 나타납니다.

2. Edge 릴레이 서버의 **IP 주소**와 **포트**를 입력합니다.

   참고

   Edge 릴레이 서버와의 인트라넷 통신을 위해 구성한 IP 주소 및 포트를 입력해야 합니다.

3. 프록시 서버가 있어야 DMZ에서 Edge 릴레이 서버와 통신할 수 있는 환경인 경우에는 **외부 프록시 서버 설정을 사용한 연결**을 사용합니다.

   외부 프록시 설정을 구성하려면 **외부 프록시 서버 설정**을 클릭하여 **프록시 설정** 화면으로 리디렉션합니다. **OfficeScan 서버 업데이트** 섹션에서 필요한 프록시 정보를 구성합니다.

   자세한 내용은 프록시 설정 구성 페이지 6-18를 참조하십시오.

4. **연결**을 클릭합니다.

   Edge 릴레이 서버에 대한 연결이 성공하면 화면이 연결 정보로 새로 고쳐집니다.

자세한 내용은 Edge 릴레이 서버 연결 관리 페이지 16-14를 참조하십시오.

Edge 릴레이 서버 연결 관리

Edge 릴레이 서버에 연결한 후, OfficeScan 서버에 보고하는 OfficeScan 에이전트는 연결 설정을 수신하고 기업 인트라넷을 벗어난 후에 자동으로 Edge 릴레이 서버와 통신할 수 있습니다. 그런 다음 **Edge 릴레이 설정** 화면에서 Edge 릴레이 서버 연결 상태를 모니터링하고, 동기화 일정을 구성하고, 즉시 동기화를 수행할 수 있습니다.

절차

1. OfficeScan 웹 콘솔에서 **관리** > **설정** > **Edge 릴레이**로 이동합니다.

   Edge 릴레이 설정 화면이 나타납니다.

2. Edge 릴레이 서버 설정을 모니터링하거나 구성합니다.

설정	설명
IP 주소	Edge 릴레이 서버의 현재 IP 주소 새로운 Edge 릴레이 서버 연결 설정을 구성하려면 **연결 해제**를 클릭하고 연결 설정을 다시 구성합니다. 자세한 내용은 Edge 릴레이 서버에 연결 페이지 16-13를 참조하십시오.
상태	OfficeScan 서버와 Edge 릴레이 서버 간의 "온라인" 또는 "오프라인" 연결 상태
동기화됨	Edge 릴레이 서버가 OfficeScan 서버와 마지막으로 동기화된 시간 OfficeScan 서버와 Edge 릴레이 서버 간에 즉시 동기화를 수행하려면 **지금 동기화**를 클릭합니다.
예약 동기화	OfficeScan 서버와 Edge 릴레이 서버가 동기화되는 빈도 대역폭에 따라 동기화 빈도를 **매시간** 또는 **15분마다**로 구성합니다.

3. **저장**을 클릭합니다.

Edge 릴레이 서버 인증서 관리

OfficeScan은 에이전트가 통신에 사용하는 Edge 릴레이 서버 인증서를 만들거나 갱신할 수 있는 명령줄 도구를 제공합니다. Edge 릴레이 서버는 새 인증서를 만든 후 이 인증서를 OfficeScan 서버에 전송합니다. 이 인증서는 에이전트가 다음에 OfficeScan 서버에 연결할 때 에이전트에 배포됩니다.

중요

새 Edge 릴레이 서버 인증서를 가져오려면 오프 프레미스 OfficeScan 에이전트가 OfficeScan 서버에 연결해야 합니다. 업데이트된 인증서를 수신하지 않은 모든 외부 에이전트는 OfficeScan 서버와 연결이 설정될 때까지 Edge 릴레이 서버와 더 이상 통신할 수 없습니다.

절차

1. Edge 릴레이 서버에서 명령줄 편집기를 열고 다음 디렉터리로 이동합니다.

   C:₩Program Files₩Trend Micro₩OfficeScan Edge₩OfcEdgeSvc₩web₩service

2. 다음 명령을 실행하여 인증서 도구를 실행합니다.

   ```
   OfcEdgeCfg.exe --renewcert -certpwd <암호>
   ```

   여기서 각 항목은 다음과 같습니다.

   - **`--renewcert`**: 새 인증서를 만듭니다.
   - **`-certpwd <암호>`**: 인증서 패키지에 대한 암호를 지정합니다.

   Edge 릴레이 서버는 새 인증서 패키지를 만들고 자동으로 인증서를 OfficeScan 서버로 보냅니다. OfficeScan 서버는 OfficeScan 에이전트가 다음에 OfficeScan 서버에 보고할 때 OfficeScan 에이전트에 새 인증서를 배포합니다.

장 17

Plug-in Manager 사용

이 장에서는 Plug-in Manager 설정 방법 및 Plug-in Manager를 통해 제공되는 플러그인 솔루션에 대해 알아봅니다.

다음과 같은 항목이 포함됩니다.

- Plug-in Manager 정보 페이지 17-2
- Plug-in Manager 설치 페이지 17-3
- 기본 OfficeScan 기능 관리 페이지 17-4
- Plug-in 프로그램 관리 페이지 17-4
- Plug-in Manager 제거 페이지 17-12
- Plug-in Manager 문제 해결 페이지 17-12

Plug-in Manager 정보

OfficeScan에는 새로운 솔루션을 기존 OfficeScan 환경에 통합하는 Plug-in Manager라는 프레임워크가 포함되어 있습니다. 이러한 솔루션의 간편한 관리를 지원하기 위해 Plug-in Manager에서는 솔루션 데이터를 한 눈에 볼 수 있도록 위젯 형태로 제공합니다.

참고

현재 IPv6을 지원하는 플러그인 솔루션은 없습니다. 서버에서 이러한 솔루션을 다운로드할 수 있지만 순수 IPv6 OfficeScan 에이전트 또는 순수 IPv6 호스트에 배포할 수는 없습니다.

Plug-in Manager는 다음과 같은 기능을 제공합니다.

- **기본 제품 기능**

  몇 가지 기본 OfficeScan 기능은 별도로 라이선스가 부여되고 Plug-in Manager를 통해 활성화됩니다. 이 릴리스에서는 **Trend Micro 가상 데스크톱 지원**과 **OfficeScan 데이터 보호** 기능이 이 범주에 속합니다.

- **Plug-in 프로그램**

  Plug-in 프로그램은 OfficeScan 프로그램의 일부가 아닙니다. Plug-in 프로그램은 라이선스가 별도로 부여되고 관리 콘솔도 별도입니다. 관리 콘솔은 OfficeScan 웹 콘솔 내에서 액세스합니다. Plug-in 프로그램의 예에는 **Trend Micro OfficeScan 도구 상자** 및 **Trend Micro Security (for Mac)**이 있습니다.

- **대시보드 탭 및 위젯**

  OfficeScan **대시보드** 화면에서 OfficeScan 서버 및 에이전트 보호 상태를 모니터링하는 데 사용되는 탭과 위젯을 표시하려면 Plug-in Manager가 필요합니다.

이 문서에서는 Plug-in 프로그램 설치 및 관리에 대한 일반적인 개요를 제공하고 위젯에서 사용 가능한 Plug-in 프로그램 데이터에 대해 설명합니다. 프로그램 구성 및 관리에 대한 자세한 내용은 특정 Plug-in 프로그램 설명서를 참조하십시오.

엔드포인트의 Plug-in 프로그램 에이전트

일부 Plug-in 프로그램(예: Trend Micro Security (for Mac))의 에이전트는 엔드포인트의 Windows 운영 체제에 설치됩니다. CNTAoSMgr.exe라는 프로세스 이름으로 실행되는 OfficeScan 에이전트 Plug-in Manager에서 이러한 에이전트를 관리합니다.

OfficeScan에서는 OfficeScan 에이전트와 함께 CNTAoSMgr.exe를 설치합니다. CNTAoSMgr.exe에 대한 유일한 추가 시스템 요구 사항은 Microsoft XML 파서(MSXML) 버전 3.0 이상입니다.

참고

다른 Plug-in 프로그램의 에이전트는 Windows 운영 체제에 설치되지 않으므로 OfficeScan 에이전트 Plug-in Manager에서 관리되지 않습니다. 이러한 에이전트의 한 가지 예가 Trend Micro Security (for Mac)입니다.

위젯

위젯을 사용하면 배포한 플러그인 솔루션에 대한 데이터를 한 눈에 볼 수 있습니다. 위젯은 OfficeScan 서버의 **대시보드** 화면에서 사용할 수 있습니다. **OfficeScan 및 Plug-ins Mashup**이라는 특수한 위젯에서는 OfficeScan 에이전트의 데이터와 플러그인 솔루션의 데이터를 조합한 후 에이전트 트리에 표시합니다.

이 관리자 안내서에서는 위젯 및 위젯을 지원하는 솔루션에 대해 간략하게 설명합니다.

Plug-in Manager 설치

이전 Plug-in Manager 버전에서는 Trend Micro 액티브업데이트 서버에서 Plug-in Manager 설치 패키지를 다운로드하여 OfficeScan 서버를 호스팅하는 컴퓨터에 설치했습니다. 이 버전에서는 다음 위치의 OfficeScan 서버 설치 패키지에 설치 패키지가 포함되어 있습니다.

<서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩PLM₩PLMSetup.exe

PLMSetup.exe 파일을 실행하여 Plug-in Manager를 설치합니다.

OfficeScan을 처음 사용하는 경우 OfficeScan 설치를 완료한 후 OfficeScan 서버와 Plug-in Manager를 둘 다 설치합니다. 기존에 Plug-in Manager를 사용하던 사용자가 이 OfficeScan 버전으로 업그레이드하는 경우에는 설치 패키지를 실행하기 전에 Plug-in Manager 서비스를 중지해야 합니다.

설치 후 작업 수행

Plug-in Manager를 설치한 후 다음을 수행합니다.

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. 플러그인 솔루션을 관리합니다.
3. OfficeScan 웹 콘솔의 **대시보드**에 액세스하여 플러그인 솔루션의 위젯을 관리합니다.

기본 OfficeScan 기능 관리

기본 OfficeScan 기능은 OfficeScan과 함께 설치되며 관리자가 Plug-in Manager를 통해 활성화합니다. Trend Micro 가상 데스크톱 지원과 같은 일부 기능은 Plug-in Manager에서 관리되고, OfficeScan 데이터 보호와 같은 다른 기능은 OfficeScan 웹 콘솔에서 관리됩니다.

Plug-in 프로그램 관리

Plug-in 프로그램은 OfficeScan과 독립적으로 설치 및 활성화합니다. 각 플러그인에서는 제품 관리를 위한 콘솔을 별도로 제공합니다. 관리 콘솔은 OfficeScan 웹 콘솔을 통해 액세스할 수 있습니다.

Plug-in 프로그램 설치

Plug-in 프로그램은 **Plug-in Manager** 콘솔에 표시됩니다. 이 콘솔에서 프로그램을 다운로드, 설치 및 관리할 수 있습니다. Plug-in Manager는 Trend Micro 액티브업데이트 서버 또는 사용자 지정 업데이트 소스(제대로 설정된 경우)에서 Plug-in 프로그램의 설치 패키지를 다운로드합니다. 액티브업데이트 서버에서 패키지를 다운로드하려면 인터넷에 연결되어 있어야 합니다.

Plug-in Manager는 설치 패키지를 다운로드하거나 설치를 시작할 때 다운로드, 설치 및 업그레이드와 같은 다른 Plug-in 프로그램 기능을 일시적으로 사용하지 않도록 설정합니다.

Plug-in Manager는 Trend Micro Control Manager의 Single Sign-On 기능을 통한 Plug-in 프로그램 설치 또는 관리를 지원하지 않습니다.

Plug-in 프로그램 설치

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **다운로드**를 클릭합니다.

   다운로드 단추 옆에 Plug-in 프로그램 패키지 크기가 표시됩니다. Plug-in Manager는 다운로드한 패키지를 <서버 설치 폴더>₩PCCSRV₩Download₩Product에 저장합니다.

   Plug-in Manager는 다운로드한 패키지를 <서버 설치 폴더>₩PCCSRV₩Download₩Product에 저장합니다.

   다운로드하는 동안 진행률을 모니터링하거나 다른 화면으로 이동할 수 있습니다.

   참고

   OfficeScan에서 패키지를 다운로드하거나 설치하는 동안 문제가 발생한 경우 OfficeScan 웹 콘솔에서 서버 업데이트 로그를 확인하십시오. 기본 메뉴에서 **로그** > **서버 업데이트**를 클릭합니다.

3. **지금 설치** 또는 **나중에 설치**를 클릭합니다.

   - **지금 설치**를 클릭하면 설치가 시작되고 설치 진행률 화면이 나타납니다.
   - **나중에 설치**를 클릭하면 **Plug-in Manager** 화면이 나타납니다.

     Plug-in Manager 화면의 Plug-in 프로그램 섹션에 있는 **설치** 단추를 클릭하여 Plug-in 프로그램을 설치합니다.

   Trend Micro 최종 사용자 사용권 계약 화면이 나타납니다.

   참고

   일부 Plug-in 프로그램에는 이 화면이 필요하지 않습니다. 이 화면이 나타나지 않는 경우 Plug-in 프로그램 설치가 시작됩니다.

4. **동의함**를 클릭하여 Plug-in 프로그램을 설치합니다.

   설치하는 동안 진행률을 모니터링하거나 다른 화면으로 이동할 수 있습니다.

   참고

   OfficeScan에서 패키지를 다운로드하거나 설치하는 동안 문제가 발생한 경우 OfficeScan 웹 콘솔에서 서버 업데이트 로그를 확인하십시오. 기본 메뉴에서 **로그** > **서버 업데이트**를 클릭합니다.

설치를 마치면 **Plug-in Manager** 화면에 현재 Plug-in 프로그램 버전이 표시됩니다.

Plug-in 프로그램 라이선스 정품 인증

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **프로그램 관리**를 클릭합니다.

제품 라이선스 새 정품 인증 코드 화면이 나타납니다.

3. 텍스트 필드에 정품 인증 코드를 입력하거나 복사하여 붙여 넣습니다.
4. **저장**을 클릭합니다.

   솔루션은 콘솔이 나타납니다.

라이선스 정보 보기 및 갱신

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **프로그램 관리**를 클릭합니다.
3. 플러그인 콘솔에서 **라이선스 정보 보기** 하이퍼링크를 탐색합니다.

   Plug-in 프로그램에 따라서는 **라이선스 정보 보기** 하이퍼링크가 다른 위치에 표시되기도 합니다. 자세한 내용은 Plug-in 프로그램 사용자 설명서를 참조하십시오.
4. 화면이 열리면 다음 라이선스 정보를 확인합니다.

옵션	설명
상태	"정품 인증됨", "정품 인증되지 않음" 또는 "만료됨"이 표시됩니다.
버전	"정식" 또는 "평가판" 버전이 표시됩니다. **참고** 정식 버전과 평가판이 둘 다 활성화된 경우에는 "정식"으로만 표시됩니다.
사용자 수	Plug-in 프로그램에서 관리할 수 있는 엔드포인트 수가 표시됩니다.
라이선스 만료 날짜	Plug-in 프로그램에 여러 개의 라이선스가 있는 경우 가장 늦은 만료일이 표시됩니다.

옵션	설명
	예를 들어, 라이선스 만료일이 2011/12/31 및 2011/06/30인 경우 2011/12/31이 표시됩니다.
정품 인증 코드	정품 인증 코드가 표시됩니다.
미리 알림	현재 라이선스 버전에 따라 플러그인에서는 유예 기간 중(정식 버전에만 해당) 또는 라이선스가 만료된 경우 라이선스 만료일에 대한 미리 알림을 표시합니다.

참고

유예 기간은 지역에 따라 다릅니다. Trend Micro 대리점에서 Plug-in 프로그램의 유예 기간을 확인하십시오.

Plug-in 프로그램 라이선스가 만료된 후에는 플러그인이 계속 작동하지만 업데이트와 지원을 더 이상 받을 수 없습니다.

5. **온라인으로 자세한 라이선스 보기**를 클릭하여 Trend Micro 웹 사이트에서 현재 라이선스에 대한 정보를 확인합니다.
6. 최신 라이선스 정보로 화면을 업데이트하려면 **정보 업데이트**를 클릭합니다.
7. **새 정품 인증 코드**를 클릭하여 **제품 라이선스 새 정품 인증 코드** 화면을 엽니다.

   자세한 내용은 Plug-in 프로그램 라이선스 정품 인증 페이지 3-4를 참조하십시오.

Plug-in 프로그램 관리

OfficeScan 웹 콘솔에서 액세스할 수 있는 Plug-in 프로그램의 관리 콘솔에서 설정을 구성하고 프로그램 관련 작업을 수행할 수 있습니다. 작업에는 프로그램 활성화를 비롯해 엔드포인트로의 Plug-in 프로그램 에이전트 배포도 포함될 수 있습니다. 프로그램 구성 및 관리에 대한 자세한 내용은 특정 Plug-in 프로그램에 대한 설명서를 참조하십시오.

Plug-in 프로그램 관리

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **프로그램 관리**를 클릭합니다.

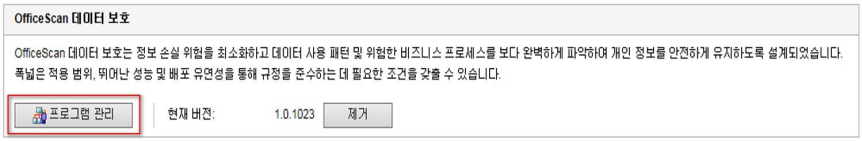


그림 17-1. 프로그램 관리 단추

Plug-in 프로그램을 처음으로 관리하는 경우 Plug-in 프로그램을 활성화해야 할 수 있습니다. 자세한 내용은 Plug-in 프로그램 라이선스 정품 인증 페이지 3-4를 참조하십시오.

Plug-in 프로그램 업그레이드

설치된 새 버전의 Plug-in 프로그램은 Plug-in Manager 콘솔에 표시됩니다. 콘솔에서 패키지를 다운로드하고 Plug-in 프로그램을 업그레이드합니다. Plug-in Manager는 Trend Micro 액티브업데이트 서버 또는 사용자 지정 업데이트 소스(제대로 설정된 경우)에서 패키지를 다운로드합니다. 액티브업데이트 서버에서 패키지를 다운로드하려면 인터넷에 연결되어 있어야 합니다.

Plug-in Manager는 설치 패키지를 다운로드하거나 업그레이드를 시작할 때 다운로드, 설치 및 업그레이드와 같은 다른 Plug-in 프로그램 기능을 일시적으로 사용하지 않도록 설정합니다.

Plug-in Manager는 Trend Micro Control Manager의 Single Sign-On 기능을 통한 Plug-in 프로그램 업그레이드를 지원하지 않습니다.

Plug-in 프로그램 업그레이드

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **다운로드**를 클릭합니다.

   다운로드 단추 옆에 업그레이드 패키지 크기가 표시됩니다.

   다운로드하는 동안 진행률을 모니터링하거나 다른 화면으로 이동할 수 있습니다.

   참고

   OfficeScan에서 패키지를 다운로드하거나 설치하는 동안 문제가 발생한 경우 OfficeScan 웹 콘솔에서 서버 업데이트 로그를 확인하십시오. 기본 메뉴에서 **로그** > **서버 업데이트**를 클릭합니다.
3. Plug-in Manager에서 패키지를 다운로드한 후 새 화면이 표시됩니다.
4. **지금 업그레이드** 또는 **나중에 업그레이드**를 클릭합니다.
   - **지금 업그레이드**를 클릭하면 업그레이드가 시작되고 업그레이드 진행률 화면이 나타납니다.
   - **나중에 업그레이드**를 클릭하면 **Plug-in Manager** 화면이 표시됩니다.

     Plug-in Manager 화면의 Plug-in 프로그램 섹션에 있는 **업그레이드** 단추를 클릭하여 Plug-in 프로그램을 업그레이드합니다.

업그레이드 후 Plug-In Manager 서비스를 다시 시작해야 할 수도 있습니다. 이 경우 **Plug-in Manager** 화면을 일시적으로 사용할 수 없습니다. 화면을 다시 사용할 수 있게 되면 현재 Plug-in 프로그램 버전이 표시됩니다.

Plug-in 프로그램 제거

Plug-in 프로그램을 제거하는 방법은 다음과 같습니다.

- Plug-in Manager 콘솔에서 Plug-in 프로그램을 제거합니다.
- OfficeScan 서버를 제거하면 Plug-in Manager와 설치된 모든 서버 Plug-in 프로그램도 제거됩니다. OfficeScan 서버를 제거하는 방법에 대한 자세한 내용은 *OfficeScan 설치 및 업그레이드 안내서*를 참조하십시오.

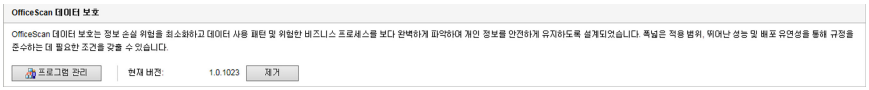
엔드포인트의 에이전트를 사용하는 Plug-in 프로그램의 경우

- Plug-in 프로그램을 제거하면 플러그인 에이전트도 제거되는지 알아보려면 Plug-in 프로그램에 대한 설명서를 참조하십시오.
- OfficeScan 에이전트와 같은 엔드포인트에 설치된 플러그인 에이전트의 경우 OfficeScan 에이전트를 제거하면 플러그인 에이전트와 OfficeScan 에이전트 Plug-in Manager(CNTAoSMgr.exe)도 제거됩니다.

Plug-in Manager 콘솔에서 Plug-in 프로그램 제거

절차

1. OfficeScan 웹 콘솔을 열고 기본 메뉴에서 **플러그인**을 클릭합니다.
2. **Plug-in Manager** 화면에서 Plug-in 프로그램 섹션으로 이동하여 **제거**를 클릭합니다.



3. 제거하는 동안 제거 진행률을 모니터링하거나 다른 화면으로 이동합니다.
4. 제거 후 **Plug-in Manager** 화면을 새로 고칩니다.

   이 Plug-in 프로그램을 다시 설치할 수 있습니다.

Plug-in Manager 제거

OfficeScan 서버를 제거하면 Plug-in Manager와 설치된 모든 서버 Plug-in 프로그램도 제거됩니다. OfficeScan 서버를 제거하는 방법에 대한 자세한 내용은 *OfficeScan 설치 및 업그레이드 안내서*를 참조하십시오.

Plug-in Manager 문제 해결

OfficeScan 서버와 OfficeScan 에이전트의 디버그 로그에서 Plug-in Manager 및 Plug-in 프로그램 디버그 정보를 확인합니다.

Plug-in 프로그램이 Plug-In Manager 콘솔에 표시되지 않음

다음과 같은 경우 다운로드하여 설치할 수 있는 Plug-in 프로그램이 Plug-in Manager 콘솔에 표시되지 않을 수 있습니다.

절차

1. Plug-in Manager가 Plug-in 프로그램을 여전히 다운로드하는 중이어서 프로그램 패키지 크기가 큰 경우 시간이 걸릴 수 있습니다. 때때로 화면에 Plug-in 프로그램이 표시되는지 확인하십시오.

   참고

   Plug-in Manager에서 Plug-in 프로그램을 다운로드할 수 없는 경우 24시간 후에 자동으로 다시 다운로드합니다. Plug-in 프로그램을 다운로드하도록 Plug-in Manager를 수동으로 트리거하려면 OfficeScan Plug-in Manager 서비스를 다시 시작합니다.

2. 서버 컴퓨터가 인터넷에 연결되지 않습니다. 서버가 프록시 서버를 통해 인터넷에 연결되는 경우 프록시 설정을 사용하여 인터넷 연결을 설정할 수 있는지 확인하십시오.

3. OfficeScan 업데이트 소스가 액티브업데이트 서버가 아닙니다. OfficeScan 웹 콘솔에서 **업데이트** > **서버** > **업데이트 소스**로 이동하여 업데이트 소스

를 확인합니다. 업데이트 소스가 액티브업데이트 서버가 아닌 경우 다음 옵션이 있습니다.

- 액티브업데이트 서버를 업데이트 소스로 선택합니다.
- **기타 업데이트 소스**를 선택한 경우 **기타 업데이트 소스** 목록의 첫 번째 항목을 업데이트 소스로 선택하고 액티브업데이트 서버에 연결할 수 있는지 확인하십시오. Plug-in Manager는 목록의 첫 번째 항목만 지원합니다.
- **현재 파일 복사본을 포함하는 인트라넷 위치**를 선택한 경우 인트라넷의 엔드포인트가 액티브업데이트 서버에도 연결할 수 있는지 확인하십시오.

엔드포인트의 플러그인 에이전트 설치 및 표시 문제

다음과 같은 경우 엔드포인트의 Plug-in 프로그램 에이전트 설치가 실패하거나 OfficeScan 에이전트 콘솔에 에이전트가 표시되지 않을 수 있습니다.

절차

1. 엔드포인트에서 Plug-in Manager(CNTAosMgr.exe)가 실행 중이지 않은 경우. OfficeScan 에이전트 엔드포인트에서 Windows 작업 관리자를 열고 CNTAosMgr.exe 프로세스를 실행합니다.
2. 플러그인 에이전트의 설치 패키지가 <에이전트 설치 폴더>₩AU_Data₩AU_Temp₩{xxx}AU_Down₩Product에 있는 OfficeScan 에이전트 엔드포인트 폴더에 다운로드되지 않은 경우. ₩AU_Data₩AU_Log₩에 있는 Tmudump.txt에서 다운로드 실패 원인을 확인합니다.

   참고

   에이전트가 성공적으로 설치된 경우 <에이전트 설치 폴더>₩AOSSvcInfo.xml에서 에이전트 정보를 확인할 수 있습니다.

3. 에이전트 설치에 실패하거나 추가 작업이 필요한 경우. Plug-in 프로그램의 관리 콘솔에서 설치 상태를 확인하고 설치 후 OfficeScan 에이전트 엔드포

인트를 다시 시작하거나 설치 전 필요한 운영 체제 패치를 설치하는 등의 작업을 수행할 수 있습니다.

Internet Explorer의 자동 구성 스크립트 설정이 프록시 서버로 리디렉션되는 경우 엔드포인트의 에이전트를 시작할 수 없음

에이전트 시작 명령이 프록시 서버로 리디렉션되기 때문에 OfficeScan 에이전트 Plug-in Manager(CNTAosMgr.exe)에서 엔드포인트의 에이전트를 시작할 수 없습니다. 프록시 설정이 사용자의 HTTP 트래픽을 127.0.0.1로 리디렉션하는 경우에만 이 문제가 발생합니다.

이 문제를 해결하려면 잘 정의된 프록시 서버 정책을 사용합니다. 예: HTTP 트래픽 경로를 127.0.0.1로 조정하지 마십시오.

127.0.0.1 HTTP 요청을 제어하는 프록시 구성을 사용해야 하는 경우 다음 작업을 수행합니다.

절차

1. OfficeScan 웹 콘솔에서 OfficeScan 방화벽 설정을 구성합니다.

   참고

   OfficeScan 에이전트에서 OfficeScan 방화벽을 사용하는 경우에만 이 단계를 수행하십시오.

   a. 웹 콘솔에서 **에이전트** > **방화벽** > **정책**으로 이동한 다음 **예외 템플릿 편집**을 클릭합니다.

   b. 예외 템플릿 편집 화면에서 **추가**를 클릭합니다.

   c. 다음 정보를 사용합니다.

      - **이름**: 원하는 이름
      - **처리 방법**: 네트워크 트래픽 허용
      - **방향**: 인바운드

- **프로토콜**: TCP
- **포트**: 5,000에서 49,151 사이의 포트 번호

d. **IP 주소**: **단일 IP 주소**를 선택하고 프록시 서버의 IP 주소를 지정하거나(권장) **모든 IP 주소**를 선택합니다.

e. **저장**을 클릭합니다.

f. 예외 템플릿 편집 화면에 돌아가 **저장 후 기존 정책에 적용**을 클릭합니다.

g. **에이전트** > **방화벽** > **프로필**로 이동하여 **에이전트에 프로필 할당**을 클릭합니다.

방화벽 프로필이 없으면 추가를 클릭하여 방화벽 프로필을 만듭니다. 다음 설정을 사용합니다.

- **이름**: 원하는 이름
- **설명**: 원하는 설명
- **정책**: 모든 액세스 정책

새 프로필을 저장한 다음 **에이전트에 프로필 할당**을 클릭합니다.

2. ofcscan.ini 파일을 수정합니다.

a. 텍스트 편집기를 사용하여 <서버 설치 폴더>에서 ofcscan.ini 파일을 엽니다.

b. **[Global Setting]**을 검색하여 다음 행에 `FWPortNum=21212`를 추가합니다. "21212"를 위의 c 단계에서 지정한 포트 번호로 변경합니다.

예:

```
[Global Setting]

FWPortNum=5000
```

c. 파일을 저장합니다.

3. 웹 콘솔에서 **에이전트** > **글로벌 에이전트 설정**으로 이동하고 **저장**을 클릭합니다.

시스템, 업데이트 모듈 또는 Plug-in Manager 프로그램에서 오류가 발생하고 오류 메시지에 특정 오류 코드가 제공됨

Plug-in Manager의 오류 메시지에 다음 오류 코드 중 하나가 표시됩니다. 아래 표에 제공된 해결 방법을 참조한 후에도 문제를 해결할 수 없으면 지원 센터에 문의하십시오.

표 17-1. Plug-in Manager 오류 코드

오류 코드	메시지, 원인 및 해결 방법
001	Plug-in Manager 프로그램에서 오류가 발생했습니다. 업데이트 작업의 진행률을 쿼리할 때 Plug-in Manager 업데이트 모듈이 응답하지 않습니다. 모듈 또는 명령 처리기가 초기화되지 않았을 수 있습니다. OfficeScan Plug-in Manager 서비스를 다시 시작하고 작업을 다시 수행하십시오.
002	시스템 오류가 발생했습니다. 레지스트리 키 `SOFTWARE\TrendMicro\OfficeScan\service\AoS`가 삭제되었으므로 Plug-in Manager 업데이트 모듈에서 이 레지스트리 키를 열 수 없습니다. 다음 단계를 수행합니다. 1. 레지스트리 편집기를 열고 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`으로 이동합니다. 값을 1.0.1000으로 초기화합니다. 2. OfficeScan Plug-in Manager 서비스를 다시 시작합니다. 3. Plug-in 프로그램을 다운로드/제거합니다.

오류 코드	메시지, 원인 및 해결 방법
028	업데이트 오류가 발생했습니다. 가능한 원인은 다음과 같습니다. • Plug-in Manager 업데이트 모듈에서 Plug-in 프로그램을 다운로드할 수 없습니다. 네트워크 연결이 작동하는지 확인한 후 다시 수행합니다. • AU 패치 에이전트에서 오류가 반환되어 Plug-in Manager 업데이트 모듈에서 Plug-in 프로그램을 설치할 수 없습니다. AU 패치 에이전트에서 오류가 발생했습니다. 오류의 정확한 원인을 알아보려면 \PCCSRV\Web\Service\AU_Data\AU_Log에서 액티브업데이트 모듈 디버그 로그 "TmuDump.txt"를 확인하십시오. 다음 단계를 수행합니다. 1. 레지스트리 편집기를 열고 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version으로 이동합니다. 값을 1.0.1000으로 초기화합니다. 2. Plug-in 프로그램 등록 키 HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_ADDON_xxxx를 삭제합니다. 3. OfficeScan Plug-in Manager 서비스를 다시 시작합니다. 4. Plug-in 프로그램을 다운로드하여 설치합니다.
170	시스템 오류가 발생했습니다. 현재 다른 작업을 처리 중이기 때문에 Plug-in Manager 업데이트 모듈이 들어오는 작업을 처리할 수 없습니다. 나중에 작업을 수행하십시오.
202	Plug-in Manager 프로그램에서 오류가 발생했습니다. Plug-in Manager 프로그램이 웹 콘솔에서 실행 중인 작업을 처리할 수 없습니다. 웹 콘솔을 새로 고치거나 프로그램 업그레이드가 있는 경우 Plug-in Manager를 업그레이드하십시오.

오류 코드	메시지, 원인 및 해결 방법
203	Plug-in Manager 프로그램에서 오류가 발생했습니다. Plug-in Manager 백엔드 서비스와 통신을 시도하는 중 Plug-in Manager 프로그램에서 IPC(프로세스 간 통신) 오류가 발생했습니다. OfficeScan Plug-in Manager 서비스를 다시 시작하고 작업을 다시 수행하십시오.
기타 오류 코드	시스템 오류가 발생했습니다. 새 Plug-in 프로그램을 다운로드할 때 Plug-in Manager는 액티브업데이트 서버에서 Plug-in 프로그램 목록을 확인합니다. Plug-in Manager가 이 목록을 가져올 수 없습니다. 다음 단계를 수행합니다. 1. 레지스트리 편집기를 열고 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\ service\AoS\OSCE_Addon_Service_CompList_Version`으로 이동합니다. 값을 `1.0.1000`으로 초기화합니다. 2. OfficeScan Plug-in Manager 서비스를 다시 시작합니다. 3. Plug-in 프로그램을 다운로드하여 설치합니다.

장 18

문제 해결 리소스

이 장에서는 OfficeScan 서버 및 OfficeScan 에이전트 문제를 해결하는 데 사용할 수 있는 리소스 목록을 제공합니다.

다음과 같은 항목이 포함됩니다.

- 지원 정보 시스템 페이지 18-2
- Case Diagnostic Tool 페이지 18-2
- Trend Micro 성능 조정 도구 페이지 18-2
- OfficeScan 서버 로그 페이지 18-2
- OfficeScan 에이전트 로그 페이지 18-14

지원 정보 시스템

지원 정보 시스템은 분석을 위해 파일을 Trend Micro에 쉽게 보낼 수 있는 페이지입니다. 이 시스템은 OfficeScan 서버 GUID를 확인하고 해당 정보를 보내는 파일과 함께 보냅니다. OfficeScan 서버 GUID를 제공하면 Trend Micro에서 평가를 위해 보낸 파일과 관련된 피드백을 제공할 수 있습니다.

Case Diagnostic Tool

Trend Micro CDT(Case Diagnostic Tool)는 문제가 발생할 때마다 고객의 제품에서 필요한 디버깅 정보를 수집합니다. 이 도구는 제품의 디버그 상태를 자동으로 설정하거나 해제하고 문제 범주에 따라 필요한 파일을 수집합니다. Trend Micro에서는 이 정보를 사용하여 제품 관련 문제를 해결합니다.

OfficeScan이 지원하는 모든 플랫폼에서 이 도구를 실행합니다. 이 도구 및 해당 설명서를 구하려면 지원 센터에 문의하십시오.

Trend Micro 성능 조정 도구

Trend Micro는 잠재적으로 성능 문제가 발생할 수 있는 응용 프로그램을 식별하기 위해 독립 성능 조정 도구를 제공합니다. Trend Micro 성능 조정 도구(Trend Micro 기술 자료에서 제공)는 동작 모니터링 및 장치 제어의 실제 배포에서 성능 문제를 미리 파악하기 위해 파일럿 프로세스 동안 표준 워크스테이션 이미지 및/또는 일부 대상 워크스테이션에서 실행되어야 합니다.

자세한 내용은 http://esupport.trendmicro.com/solution/en-us/1056425.aspx를 참조하십시오.

OfficeScan 서버 로그

웹 콘솔에서 사용할 수 있는 로그 이외에도 제품 문제 해결을 위해 다른 유형의 로그(예: 디버그 로그)를 사용할 수 있습니다.

경고!

디버그 로그는 서버 성능에 영향을 미치고 많은 디스크 공간을 사용할 수 있습니다. 필요한 경우에만 디버그 로깅을 사용하도록 설정하고 더 이상 디버그 데이터가 필요하지 않으면 즉시 사용 안 함으로 설정하십시오. 디스크 공간을 절약하려면 로그 파일을 제거하십시오.

LogServer.exe를 사용하는 서버 디버그 로그

LogServer.exe를 사용하여 다음에 대한 디버그 로그를 수집합니다.

- OfficeScan 서버 기본 로그
- Trend Micro Vulnerability Scanner
- Active Directory 통합 로그
- 에이전트 그룹화 로그
- 보안 준수 로그
- 역할 기반 관리
- 스마트 스캔

디버그 로깅 사용

절차

1. 웹 콘솔에 로그온합니다.
2. 웹 콘솔 배너에서 "OfficeScan"의 첫 번째 "O"를 클릭합니다.
3. **디버그 로그 사용**을 선택합니다.
4. 디버그 로그 설정을 지정합니다.
5. **저장**을 클릭합니다.

6. 기본 위치 <서버 설치 폴더>₩PCCSRV₩Log>의 로그 파일(ofcdebug.log)을 확인합니다.

디버그 로깅 사용 안 함

절차

1. 웹 콘솔에 로그온합니다.
2. 웹 콘솔 배너에서 "OfficeScan"의 첫 번째 "O"를 클릭합니다.
3. **디버그 로그 사용**의 선택을 지웁니다.
4. **저장**을 클릭합니다.

서버 설치 및 업그레이드에 대한 디버그 로깅 사용

다음 작업을 수행하기 전에 디버그 로깅을 사용하도록 설정합니다.

- 서버를 제거한 후 다시 설치
- OfficeScan을 새 버전으로 업그레이드
- 원격 설치/업그레이드 수행(디버그 로깅은 원격 엔드포인트에서 사용하도록 설정하지 않고 설치를 시작한 엔드포인트에서 사용하도록 설정함)

절차

1. <서버 설치 폴더>₩PCCSRV₩Private에 있는 LogServer 폴더를 C:₩에 복사합니다.
2. cdebug.ini라는 파일을 만들어 다음 내용으로 구성합니다.

```
[debug]

debuglevel=9

debuglog=c:₩LogServer₩ofcdebug.log
```

```
debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. C:₩LogServer에 ofcdebug.ini를 저장합니다.
4. 적절한 작업을 수행합니다(서버 제거/재설치, 새 서버 버전으로 업그레이드 또는 원격 설치/업그레이드 수행).
5. C:₩LogServer에서 ofcdebug.log를 확인합니다.

설치 로그

- 로컬 설치/업그레이드 로그

  파일 이름: OFCMAS.LOG

  위치: %windir%

- 원격 설치/업그레이드 로그
  - 설치를 시작한 엔드포인트에서:

    파일 이름: ofcmasr.log

    위치: %windir%
  - 대상 엔드포인트에서:

    파일 이름: OFCMAS.LOG

    위치: %windir%

Active Directory 로그

- 파일 이름: ofcdebug.log

- 파일 이름: ofcserver.ini

  위치: <서버 설치 폴더>₩PCCSRV₩Private₩

- 파일 이름:
  - dbADScope.cdx
  - dbADScope.dbf
  - dbADPredefinedScope.cdx
  - dbADPredefinedScope.dbf
  - dbCredential.cdx
  - dbCredential.dbf

  위치: <서버 설치 폴더>₩PCCSRV₩HTTPDB₩

역할 기반 관리 로그

자세한 역할 기반 관리 정보를 얻으려면 다음 중 하나를 수행합니다:

- Trend Micro Case Diagnostics Tool을 실행합니다. 자세한 내용은 Case Diagnostic Tool 페이지 18-2을 참조하십시오.
- 다음 로그를 수집합니다.
  - <서버 설치 폴더>₩PCCSRV₩Private₩AuthorStore 폴더에 있는 모든 파일
  - OfficeScan 서버 로그 페이지 18-2

OfficeScan 에이전트 그룹화 로그

- 파일 이름: ofcdebug.log
- 파일 이름: ofcserver.ini

  위치: <서버 설치 폴더>₩PCCSRV₩Private₩

- 파일 이름: SortingRule.xml

  위치: <서버 설치 폴더>₩PCCSRV₩Private₩SortingRuleStore₩

- 파일 이름:

  - dbADScope.cdx
  - dbADScope.dbf

  위치: <서버 설치 폴더>₩HTTPDB₩

구성 요소 업데이트 로그

파일 이름: TmuDump.txt

위치: <서버 설치 폴더>₩PCCSRV₩Web₩Service₩AU_Data₩AU_Log

서버 업데이트에 대한 세부 정보 확인

절차

1. aucfg.ini라는 파일을 만들어 다음 내용으로 구성합니다.

   ```
   [Debug]

   level=-1

   [Downloader]

   ProxyCache=0
   ```

2. 파일을 <서버 설치 폴더>₩PCCSRV₩Web₩Service에 저장합니다.
3. OfficeScan Master Service를 다시 시작합니다.

서버 업데이트에 대한 세부 정보 수집 중지

절차

1. aucfg.ini를 삭제합니다.
2. OfficeScan Master Service를 다시 시작합니다.

에이전트 패키지 도구 로그

에이전트 패키지 도구 생성에 대한 로깅 사용

절차

1. <서버 설치 폴더>₩PCCSRV₩Admin₩Utility₩ClientPackager에 있는 ClnExtor.ini를 다음과 같이 수정합니다.

   ```
   [Common]

   DebugMode=1
   ```

2. C:₩에서 ClnPack.log를 확인합니다.

에이전트 패키지 도구 생성에 대한 로깅 사용 안 함

절차

1. ClnExtor.ini를 엽니다.
2. "DebugMode" 값을 1에서 0으로 변경합니다.

보안 준수 보고서 로그

자세한 보안 준수 정보를 확인하려면 다음을 수집합니다.

- 파일 이름: RBAUserProfile.ini

  위치: <서버 설치 폴더>₩PCCSRV₩Private₩AuthorStore₩

- <서버 설치 폴더>₩PCCSRV₩Log₩Security Compliance Report 폴더에 있는 모든 파일

- OfficeScan 서버 로그 페이지 18-2

외부 서버 관리 로그

- 파일 이름: ofcdebug.log

- 파일 이름: ofcserver.ini

  위치: <서버 설치 폴더>₩PCCSRV₩Private₩

- <서버 설치 폴더>₩PCCSRV₩Log₩Outside Server Management Report₩ 폴더에 있는 모든 파일

- 파일 이름:

  - dbADScope.cdx
  - dbADScope.dbf
  - dbClientInfo.cdx
  - dbclientInfo.dbf

  위치: <서버 설치 폴더>₩HTTPDB₩

장치 제어 예외 로그

자세한 장치 제어 예외 정보를 확인하려면 다음을 수집합니다.

- 파일 이름: ofcscan.ini

  위치: <서버 설치 폴더>₩

- 파일 이름: dbClientExtra.dbf

위치: <서버 설치 폴더>₩HTTPDB₩

- OfficeScan 웹 콘솔의 장치 제어 예외 목록

통합 스마트 보호 서버 웹 검증 로그

파일 이름: diagnostic.log

위치: <서버 설치 폴더>₩PCCSRV₩LWCS₩

ServerProtect 일반 서버 마이그레이션 도구 로그

ServerProtect 일반 서버 마이그레이션 도구에 대한 디버그 로깅을 사용하려면

절차

1. ofcdebug.ini라는 파일을 만들어 다음 내용으로 구성합니다.

   ```
   [Debug]

   DebugLog=C:₩ofcdebug.log

   DebugLevel=9
   ```

2. 파일을 C:₩에 저장합니다.
3. C:₩에서 ofcdebug.log를 확인합니다.

참고

디버그 로깅을 사용하지 않으려면 ofcdebug.ini 파일을 삭제합니다.

VSEncrypt 로그

OfficeScan이 디버그 로그(VSEncrypt.log)를 사용자 계정의 임시 폴더에 자동으로 만듭니다. 예를 들면 C:₩Documents and Settings₩<사용자 이름>₩Local Settings₩Temp와 같습니다.

Control Manager MCP Agent 로그

<서버 설치 폴더>₩PCCSRV₩CMAgent 폴더에 있는 디버그 파일

- Agent.ini
- Product.ini
- Control Manager 설정 페이지의 스크린샷
- ProductUI.zip

MCP 에이전트에 대한 디버그 로깅 사용

절차

1. <서버 설치 폴더>₩PCCSRV₩CmAgent에 있는 product.ini를 다음과 같이 수정합니다.

```
[Debug]

debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:₩CMAgent_debug.log
```

2. Microsoft Management Console에서 OfficeScan Control Manager Agent 서비스를 다시 시작합니다.
3. C:₩에서 CMAgent_debug.log를 확인합니다.

MCP 에이전트에 대한 디버그 로깅 사용 안 함

절차

1. product.ini를 열어 다음 내용을 삭제합니다.

```
debugmode = 3

debuglevel= 3

debugtype = 0

debugsize = 10000

debuglog = C:₩CMAgent_debug.log
```

2. OfficeScan Control Manager 서비스를 다시 시작합니다.

바이러스/악성 프로그램 로그

파일 이름:

- dbVirusLog.dbf
- dbVirusLog.cdx

위치: <서버 설치 폴더>₩PCCSRV₩HTTPDB₩

스파이웨어/그레이웨어 로그

파일 이름:

- dbSpywareLog.dbf
- dbSpywareLog.cdx

위치: <서버 설치 폴더>₩PCCSRV₩HTTPDB₩

비상 발생 로그

로그 형식	파일
현재 방화벽 위반 비상 발생 로그	파일 이름: Cfw_Outbreak_Current.log 위치: <서버 설치 폴더>₩PCCSRV₩Log₩
최근 방화벽 위반 비상 발생 로그	파일 이름: Cfw_Outbreak_Last.log 위치: <서버 설치 폴더>₩PCCSRV₩Log₩
현재 바이러스/악성 프로그램 발생 로그	파일 이름: Outbreak_Current.log 위치: <서버 설치 폴더>₩PCCSRV₩Log₩
최근 바이러스/악성 프로그램 발생 로그	파일 이름: Outbreak_Last.log 위치: <서버 설치 폴더>₩PCCSRV₩Log₩
현재 스파이웨어/그레이웨어 비상 발생 로그	파일 이름: Spyware_Outbreak_Current.log 위치: <서버 설치 폴더>₩PCCSRV₩Log₩
최근 스파이웨어/그레이웨어 비상 발생 로그	파일 이름: Spyware_Outbreak_Last.log 위치: <서버 설치 폴더>₩PCCSRV₩Log₩

가상 데스크톱 지원 로그

- 파일 이름: vdi_list.ini

  위치: <서버 설치 폴더>₩PCCSRV₩TEMP₩
- 파일 이름: vdi.ini

  위치: <서버 설치 폴더>₩PCCSRV₩Private₩
- 파일 이름: ofcdebug.txt

  위치: <서버 설치 폴더>₩PCCSRV₩

ofcdebug.txt를 생성하려면 디버그 로깅을 사용하도록 설정합니다. 디버그 로깅을 사용하도록 설정하는 방법에 대한 지침은 디버그 로깅 사용 페이지 18-3을 참조하십시오.

OfficeScan 에이전트 로그

OfficeScan 에이전트 로그(예: 디버그 로그)를 사용하여 OfficeScan 에이전트 문제를 해결할 수 있습니다.

경고!

디버그 로그는 에이전트 성능에 영향을 미치고 디스크 공간을 많이 사용할 수 있습니다. 필요한 경우에만 디버그 로깅을 사용하도록 설정하고 더 이상 디버그 데이터가 필요하지 않으면 즉시 사용 안 함으로 설정하십시오. 파일 크기가 커지면 로그 파일을 제거하십시오.

LogServer.exe를 사용하는 OfficeScan 에이전트 디버그 로그

OfficeScan 에이전트에 대해 디버그 로깅을 사용하도록 설정하려면

절차

1. ofcdebug.ini라는 파일을 만들어 다음 내용으로 구성합니다.

```
[Debug]

Debuglog=C:₩ofcdebug.log

debuglevel=9

debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

2. 사용자에게 ofcdebug.ini를 보내 C:₩에 저장하도록 합니다.

참고

LogServer.exe는 OfficeScan 에이전트 엔드포인트가 시작할 때마다 자동으로 실행됩니다. 엔드포인트가 시작할 때 열리는 LogServer.exe 명령 창을 닫으면 OfficeScan이 디버그 로깅을 중지하므로 사용자가 이 창을 닫지 않도록 하십시오. 사용자가 명령 창을 닫으면 <에이전트 설치 폴더>에 있는 LogServer.exe를 실행하여 디버그 로깅을 다시 시작할 수 있습니다.

3. 각 OfficeScan 에이전트 엔드포인트의 C:₩에서 ofcdebug.log를 확인합니다.

참고

OfficeScan 에이전트에 대해 디버그 로깅을 사용하지 않도록 설정하려면 ofcdebug.ini를 삭제합니다.

새 설치 로그

MSI 패키지 설치의 경우

- 파일 이름: OFCNT.LOG
- 위치: <에이전트 설치 폴더>

웹 설치의 경우

- 파일 이름: WebInstall.log
- 위치: C:₩

원격 설치의 경우

- 파일 이름: OFCNT.LOG
- 위치: C:₩

Autopcc 및 EXE 패키지 설치의 경우

- 파일 이름: OFCNT.LOG

- 위치: <에이전트 설치 폴더>%windir%₩

업그레이드/핫픽스 로그

파일 이름: upgrade_yyyymmddhhmmss.log

위치: <에이전트 설치 폴더>₩Temp

Damage Cleanup Services 로그

Damage Cleanup Services에 대한 디버그 로깅 사용 안 함

절차

1. <에이전트 설치 폴더>에서 TSC.ini를 엽니다.
2. 다음 행을 다음과 같이 수정합니다.

   ```
   DebugInfoLevel=5
   ```

3. <에이전트 설치 폴더>₩debug에서 TSCDebug.log를 확인합니다.

Damage Cleanup Services에 대한 디버그 로깅 사용

TSC.ini를 열어 "`DebugInfoLevel`" 값을 5에서 0으로 변경합니다.

Cleanup 로그

파일 이름: yyyymmdd.log

위치: <에이전트 설치 폴더>₩report₩

메일 검색 로그

파일 이름: SmolDbg.txt

위치: <에이전트 설치 폴더>

OfficeScan 에이전트 연결 로그

파일 이름: Conn_YYYYMMDD.log

위치: <에이전트 설치 폴더>₩ConnLog

OfficeScan 에이전트 업데이트 로그

파일 이름: Tmudump.txt

위치: <에이전트 설치 폴더>₩AU_Data₩AU_Log

OfficeScan 에이전트 업데이트에 대한 세부 정보 확인

절차

1. aucfg.ini라는 파일을 만들어 다음 내용으로 구성합니다.

```
[Debug]

level=-1

[Downloader]

ProxyCache=0
```

2. 파일을 <에이전트 설치 폴더>에 저장합니다.
3. OfficeScan 에이전트를 다시 로드합니다.

참고

에이전트 업데이트에 대한 세부 정보 수집을 중지하려면 aucfg.ini 파일을 삭제하고 OfficeScan 에이전트를 다시 로드합니다.

바이러스 검색 엔진 로그

바이러스 검색 엔진에 대한 디버그 로깅을 사용하려면

절차

1. 레지스트리 편집기(regedit.exe)를 엽니다.
2. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TMFilter\Parameters`로 이동합니다.
3. "`DebugLogFlags`"의 값을 "`00003eff`"로 변경합니다.
4. 발생한 검색 문제를 유발한 단계를 수행합니다.
5. %windir%에서 TMFilter.log를 확인합니다.

참고

디버그 로깅을 사용하지 않으려면 "`DebugLogFlags`"의 값을 "`00000000`"으로 복원합니다.

바이러스 사전 방역 로그

파일 이름: OPPLogs.log

위치: <에이전트 설치 폴더>₩OppLog

바이러스 사전 방역 복원 로그

파일 이름:

- TmOPP.ini
- TmOPPRestore.ini

위치: <에이전트 설치 폴더>₩

동작 모니터링 디버그 로그

동작 모니터링을 위해 디버그 로깅을 사용하도록 설정하려면 다음을 수행합니다.

절차

1. 레지스트리 편집기(regedit.exe)를 엽니다.
2. `HKLM\SOFTWARE\TrendMicro\Aegis`로 이동합니다.
3. "`DebugLogFlags`"의 값을 "`dword:00000032`"로 변경합니다.
4. 문제를 유발한 단계를 수행합니다.
5. C:₩Program Files (x86)₩Trend Micro₩BM₩log₩ 폴더에서 다음 로그를 확인합니다.
   - TmCommengyyyymmdd_nn.log
   - TMPEMyyyymmdd_nn.log

OfficeScan 방화벽 로그

Windows Vista/Server 2008/7/Server 2012/8/8.1/10 컴퓨터에서 방화벽 드라이버에 대한 디버그 로깅 사용

절차

1. 다음 레지스트리 값을 수정합니다.

레지스트리 키	값
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmwfp\Parameters	종류: DWORD 값 (REG_DWORD) 이름: DebugCtrl 값: 0x00001111
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmlwf\Parameters	종류: DWORD 값 (REG_DWORD) 이름: DebugCtrl 값: 0x00001111

2. 엔드포인트를 다시 시작합니다.
3. C:₩에서 wfp_log.txt 및 lwf_log.txt를 확인합니다.

Windows XP 및 Windows Server 2003 컴퓨터에서 방화벽 드라이버에 대한 디버그 로깅 사용

절차

1. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\tmcfw\Parameters에 다음 데이터를 추가합니다.
   - 종류: DWORD 값 (REG_DWORD)
   - 이름: DebugCtrl
   - 값: 0x00001111
2. 엔드포인트를 다시 시작합니다.
3. C:₩에서 cfw_log.txt를 확인합니다.

방화벽 드라이버에 대한 디버그 로깅 사용 안 함(모든 운영 체제)

절차

1. 레지스트리 키에서 "DebugCtrl"을 삭제합니다.
2. 엔드포인트를 다시 시작합니다.

OfficeScan NT 방화벽 서비스에 대한 디버그 로깅 사용

절차

1. <에이전트 설치 폴더>에 있는 TmPfw.ini를 다음과 같이 편집합니다.

   ```
   [ServiceSession]

   Enable=1
   ```

2. 에이전트를 다시 로드합니다.
3. C:₩temp에서 ddmmyyyy_NSC_TmPfw.log를 확인합니다.

OfficeScan NT 방화벽 서비스에 대한 디버그 로깅 사용 안 함

절차

1. TmPfw.ini를 열고 "Enable" 값을 1에서 0으로 변경합니다.
2. OfficeScan 에이전트를 다시 로드합니다.

웹 검증 및 POP3 메일 검색 로그

웹 검증 및 POP3 메일 검색 기능에 대한 디버그 로깅 사용

절차

- Windows Vista 또는 Windows Server 2008을 실행하는 에이전트의 경우:
  a. <에이전트 설치 폴더>에 있는 TmProxy.ini를 다음과 같이 편집합니다.

```
[InteractiveSession]

Enable=1

LogFolder=C:₩temp

[ServiceSession]

Enable=1

LogFolder=C:₩temp
```

  b. OfficeScan 에이전트를 다시 로드합니다.
  c. C:₩temp에서 ddmmyyyy_NSC_TmProxy.log를 확인합니다.
- 다른 Windows 버전을 실행하는 에이전트의 경우:
  a. <에이전트 설치 폴더>에 있는 TmOsprey.ini를 다음과 같이 편집합니다.

```
[InteractiveSession]

Enable=1

LogFolder=C:₩temp

[ServiceSession]

Enable=1

LogFolder=C:₩temp
```

b. OfficeScan 에이전트를 다시 로드합니다.

c. C:₩temp에서 ddmmyyyy_NSC_TmProxy.log를 확인합니다.

웹 검증 및 POP3 메일 검색 기능에 대한 디버그 로깅 사용 안 함

절차

- Windows Vista 또는 Windows Server 2008을 실행하는 에이전트의 경우:

  a. <에이전트 설치 폴더>에 있는 TmProxy.ini를 다음과 같이 편집합니다.

  ```
  [InteractiveSession]

  Enable=0

  LogFolder=C:₩temp

  [ServiceSession]

  Enable=0

  LogFolder=C:₩temp
  ```

  b. OfficeScan 에이전트를 다시 로드합니다.

- 다른 Windows 버전을 실행하는 에이전트의 경우:

  a. <에이전트 설치 폴더>에 있는 TmOsprey.ini를 다음과 같이 편집합니다.

  ```
  [InteractiveSession]

  Enable=0

  LogFolder=C:₩temp

  [ServiceSession]

  Enable=0

  LogFolder=C:₩temp
  ```

b. OfficeScan 에이전트를 다시 로드합니다.

장치 제어 예외 목록 로그

파일 이름: DAC_ELIST

위치: <에이전트 설치 폴더>₩

데이터 보호 디버그 로그

데이터 보호 디버그 로그를 사용하도록 설정하려면

절차

1. 지원 센터에서 logger.cfg 파일을 받습니다.
2. `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\DlpLite`에 다음 데이터를 추가합니다.
   - 종류: `String`
   - 이름: `debugcfg`
   - 값: C:₩Log₩logger.cfg
3. C:₩ directory에 "Log" 폴더를 만듭니다.
4. logger.cfg를 Log 폴더에 복사합니다.
5. 웹 콘솔에서 데이터 손실 방지 및 장치 제어 설정을 배포하여 로그 수집을 시작합니다.

참고

레지스트리 키에서 `debugcfg`를 삭제하고 엔드포인트를 다시 시작하여 데이터 보호 모듈에 대한 디버그 로깅을 사용하지 않도록 설정할 수 있습니다.

Windows 이벤트 로그

Windows 이벤트 뷰어는 로그온 또는 계정 설정 변경과 같이 성공적인 응용 프로그램 이벤트를 기록합니다.

절차

1. 다음 중 하나를 수행합니다.
   - **시작** > **제어판** > **성능 및 유지 관리** > **관리 도구** > **컴퓨터 관리**를 클릭합니다.
   - 이벤트 뷰어 스냅인이 포함된 MMC를 엽니다.
2. **이벤트 뷰어**를 클릭합니다.

TDI(Transport Driver Interface) 로그

TDI(Transport Driver Interface) 로그를 사용하도록 설정하려면

절차

1. `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\tmtdi\Parameters`에 다음 데이터를 추가합니다.

매개 변수	값
키 1	종류: `DWORD 값 (REG_DWORD)` 이름: `Debug` 값: `1111(16진수)`
키 2	종류: 문자열 값`(REG_SZ)` 이름: `LogFile` 값: C:₩tmtdi.log

2. 엔드포인트를 다시 시작합니다.

3. C:₩에서 tmtdi.log를 확인합니다.

참고

TDI에 대한 디버그 로깅을 사용하지 않도록 설정하려면 레지스트리 키에서 `Debug` 및 `LogFile`을 삭제하고 엔드포인트를 다시 시작합니다.

장 19

기술 지원

다음 항목에 대해 자세히 알아보십시오.

- 문제 해결 리소스 페이지 19-2
- Trend Micro 연락처 페이지 19-3
- 의심스러운 콘텐츠를 Trend Micro로 보내기 페이지 19-4
- 기타 리소스 페이지 19-5

문제 해결 리소스

기술 지원에 문의하기 전에 다음 Trend Micro 온라인 리소스를 방문하십시오.

지원 포털 사용

Trend Micro 지원 포털은 연중무휴로 운영되는 온라인 리소스로, 일반 문제뿐 아니라 특수한 문제에 대한 최신 정보도 포함합니다.

절차

1. http://esupport.trendmicro.com으로 이동합니다.
2. 사용 가능한 제품 중에서 선택하거나 해당 단추를 클릭하여 솔루션을 검색합니다.
3. **Search Support(지원 검색)**를 사용하여 제공되는 솔루션을 검색합니다.
4. 솔루션을 찾을 수 없는 경우 **Contact Support(지원 센터에 문의)**를 클릭하고 필요한 지원 유형을 선택합니다.

   팁

   지원 사례를 온라인으로 제출하려면 다음 URL을 방문합니다.

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   Trend Micro 지원 엔지니어가 사례를 조사하고 24시간 내에 응답을 제공합니다.

위협 백과사전

오늘날 대부분의 악성 프로그램은 컴퓨터 보안 프로토콜을 우회하기 위해 두 가지 이상의 기술이 결합된 혼합된 위협으로 이루어집니다. Trend Micro에서는 방어 전략을 사용자 정의해 주는 제품을 통해 이러한 복잡한 악성 프로그램으로부터 시스템을 방어합니다. 위협 백과사전에서는 알려진 악성 프로그램, 스

팸, 유해 URL 및 알려진 취약점을 비롯한 다양한 혼합 위협의 이름 및 증상을 포괄하는 목록을 제공합니다.

http://about-threats.trendmicro.com/apac/threatencyclopedia#malware로 이동하여 다음에 대해 자세히 알아보십시오.

- 현재 "활동 중(in the wild)"이거나 활성 상태인 악성 프로그램과 악성 모바일 코드
- 상호 연관된 위협 정보 페이지를 통해 완벽한 웹 공격 사례 구성
- 대상 지정 공격 및 보안 위협에 대한 인터넷 위협 권고
- 웹 공격 및 온라인 동향 정보
- 매주 제공되는 악성 프로그램 보고서

Trend Micro 연락처

한국 사용자는 아래의 전화 또는 전자 메일을 통해 Trend Micro 대리점에 연락할 수 있습니다.

주소	한국트렌드마이크로 서울 강남구 대치동 945-1 홍우빌딩 6층 (우편번호: 135-846)
전화	전화: 02-561-0990 +1 (817) 569-8900 팩스: 02-561-0660 (888) 762-8736
웹 사이트	http://www.trendmicro.co.kr/kr/index.html
전자 메일 주소	support@trendmicro.co.kr

- 전 세계 지원 센터:

  http://kr.trendmicro.com/kr/about/contact_us/index.html

- Trend Micro 제품 설명서:

http://docs.trendmicro.com/ko-kr/home.aspx

신속한 기술 지원을 받는 방법

보다 원활한 문제 해결을 위해 다음 정보를 준비하십시오.

- 문제 재현 절차
- 어플라이언스 또는 네트워크 정보
- 컴퓨터 브랜드, 모델 및 연결된 추가 하드웨어 또는 장치
- 메모리 용량 및 사용 가능한 하드 디스크 공간
- 운영 체제 및 Service Pack 버전
- 설치된 에이전트의 버전
- 일련 번호 또는 정품 인증 코드
- 설치 환경에 대한 자세한 설명
- 표시된 정확한 오류 메시지 텍스트

의심스러운 콘텐츠를 Trend Micro로 보내기

여러 옵션을 통해 의심스러운 콘텐츠를 Trend Micro로 보내 추가 분석을 받을 수 있습니다.

전자 메일 검증 서비스

특정 IP 주소에 대한 검증 내용을 쿼리하고 글로벌 승인 목록에 포함할 메시지 전송 에이전트를 추천하십시오.

https://ers.trendmicro.com/

다음 기술 자료 항목을 참조하여 메시지 샘플을 Trend Micro로 보내십시오.

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

파일 검증 서비스

시스템 정보를 수집하고 의심스러운 파일 콘텐츠를 Trend Micro에 제출하십시오.

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

추적을 위해 사례 번호를 기록하십시오.

웹 검증 서비스

피싱 사이트로 의심되는 웹 사이트나 기타 "악성 벡터", 즉 스파이웨어 및 악성 프로그램 같은 인터넷 위협을 의도적으로 제공하는 URL의 안전 등급 및 콘텐츠 형식을 쿼리하십시오.

http://global.sitesafety.trendmicro.com/

등급이 잘못 할당된 경우 Trend Micro에 재분류 요청을 보내십시오.

기타 리소스

솔루션 및 지원 외에도 온라인으로 제공되는 여러 유용한 리소스를 통해 최신 정보를 얻고, 혁신적인 기능에 대해 알아보고, 최근의 보안 경향을 확인할 수 있습니다.

다운로드 센터

Trend Micro에서 보고된 알려진 문제에 대한 패치나 특정 제품 또는 서비스에 적용되는 업그레이드를 릴리스하는 경우가 있을 수 있습니다. 사용 가능한 패치가 있는지 확인하려면 다음으로 이동하십시오.

http://www.trendmicro.com/download/

패치를 적용하지 않은 경우(패치가 오래된 경우), 추가 정보 파일을 열어 자신의 환경과 관련이 있는지 확인하십시오. 추가 정보 파일에는 설치 지침도 포함되어 있습니다.

문서 피드백

Trend Micro에서는 설명서의 내용을 개선하기 위해 지속적인 노력을 기울이고 있습니다. 이 문서나 기타 Trend Micro 문서에 대한 질문, 의견 또는 제안이 있으면 다음 사이트를 방문하십시오.

http://www.trendmicro.com/download/documentation/rating.asp

부록

부록

부록 A

OfficeScan의 IPv6 지원

IPv6 주소 지정을 지원하는 환경에서 OfficeScan을 배포하려는 사용자는 이 부록을 읽어야 합니다. 이 부록에는 OfficeScan의 IPv6 지원 범위에 대한 정보가 수록되어 있습니다.

Trend Micro에서는 독자가 IPv6의 개념 및 IPv6 주소 지정을 지원하는 네트워크 설정 관련 작업에 익숙한 것으로 가정합니다.

OfficeScan 서버 및 에이전트에 대한 IPv6 지원

IPv6은 OfficeScan 버전 10.6부터 지원됩니다. 이전 버전의 OfficeScan에서는 IPv6 주소 지정을 지원하지 않습니다. IPv6 요구 사항을 충족하는 OfficeScan 서버 및 OfficeScan 에이전트를 설치하거나 업그레이드하면 IPv6 지원이 자동으로 사용하도록 설정됩니다.

OfficeScan 서버 요구 사항

OfficeScan 서버에 대한 IPv6 요구 사항은 다음과 같습니다.

- 서버는 Windows Server 2008, Windows Server 2012 또는 Windows Server 2016에 설치해야 합니다.
- 서버에서 IIS Web server를 사용해야 합니다.
- 서버에서 IPv4 및 IPv6 OfficeScan 에이전트를 관리하는 경우 IPv4 주소와 IPv6 주소를 둘 다 사용하고 해당 호스트 이름으로 식별해야 합니다. 서버가 IPv4 주소로 식별되면 IPv6 OfficeScan 에이전트에서 서버에 연결할 수 없습니다. 순수 IPv4 에이전트가 IPv6 주소로 식별되는 서버에 연결하는 경우에도 같은 문제가 발생합니다.
- 서버에서 IPv6 에이전트만 관리하는 경우 최소 요구 사항은 IPv6 주소입니다. 이 경우 서버는 호스트 이름 또는 IPv6 주소로 식별될 수 있습니다. 서버가 호스트 이름으로 식별되는 경우에는 FQDN(정규화된 도메인 이름)을 사용하는 것이 좋습니다. 순수 IPv6 환경에서는 WINS 서버가 호스트 이름을 해당 IPv6 주소로 인식할 수 없기 때문입니다.

참고

FQDN은 서버의 로컬 설치를 수행할 때만 지정할 수 있습니다. 원격 설치에서는 지원되지 않습니다.

OfficeScan 에이전트 요구 사항

OfficeScan 에이전트는 다음 운영 체제에 설치해야 합니다.

- Windows 7
- Windows Server 2008
- Windows Vista
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows 10
- Windows Server 2016

OfficeScan 에이전트가 연결하는 엔터티 중 일부는 IPv4 주소 지정만 지원하므로 에이전트에서 IPv4 주소와 IPv6 주소를 둘 다 사용하는 것이 좋습니다.

순수 IPv6 서버 제한 사항

다음 표에는 OfficeScan 서버에서 IPv6 주소만 사용하는 경우의 제한 사항이 나와 있습니다.

표 A-1. 순수 IPv6 서버 제한 사항

항목	제한 사항
에이전트 관리	순수 IPv6 서버에서는 다음 작업을 수행할 수 없습니다. • 순수 IPv4 엔드포인트에 OfficeScan 에이전트 배포 • 순수 IPv4 OfficeScan 에이전트 관리
업데이트 및 중앙 집중식 관리	순수 IPv6 서버는 다음과 같은 순수 IPv4 업데이트 소스에서 업데이트할 수 없습니다. • Trend Micro 액티브업데이트 서버 • 모든 순수 IPv4 사용자 정의 업데이트 소스
제품 등록, 활성화 및 갱신	순수 IPv6 서버에서는 Trend Micro Online Registration Server에 연결하여 제품을 등록하거나 라이선스를 얻거나 라이선스를 활성화/갱신할 수 없습니다.

항목	제한 사항
프록시 연결	순수 IPv6 서버는 순수 IPv4 프록시 서버를 통해 연결할 수 없습니다.
플러그인 솔루션	순수 IPv6 서버에서는 Plug-in Manager가 제공하지만 플러그인 솔루션을 다음 대상에 배포할 수 없습니다. • 순수 IPv4 OfficeScan 에이전트 또는 순수 IPv4 호스트(직접 연결이 없기 때문) • 순수 IPv6 OfficeScan 에이전트 또는 순수 IPv6 호스트(플러그인 솔루션이 IPv6을 지원하지 않기 때문)

이러한 제한 사항은 대부분 IPv4 주소와 IPv6 주소 간에 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)를 설치하여 해결할 수 있습니다. OfficeScan 서버와 연결 대상 또는 서비스 대상 사이에 프록시 서버를 배치하십시오.

순수 IPv6 OfficeScan 에이전트 제한 사항

다음 표에는 OfficeScan 에이전트에서 IPv6 주소만 사용하는 경우의 제한 사항이 나와 있습니다.

표 A-2. 순수 IPv6 OfficeScan 에이전트 제한 사항

항목	제한 사항
상위 OfficeScan 서버	순수 IPv6 OfficeScan 에이전트는 순수 IPv4 OfficeScan 서버에서 관리할 수 없습니다.
업데이트	순수 IPv6 OfficeScan 에이전트는 다음과 같은 순수 IPv4 업데이트 소스에서 업데이트할 수 없습니다. • Trend Micro 액티브업데이트 서버 • 순수 IPv4 OfficeScan 서버 • 순수 IPv4 업데이트 에이전트 • 모든 순수 IPv4 사용자 정의 업데이트 소스

항목	제한 사항
검색 쿼리, 웹 검증 쿼리 및 Smart Feedback	순수 IPv6 OfficeScan 에이전트는 다음과 같은 스마트 보호 소스에 쿼리를 보낼 수 없습니다. • 스마트 보호 서버 2.0(통합 또는 독립) **참고** 스마트 보호 서버에 대한 IPv6 지원은 버전 2.5부터 제공됩니다. • Trend Micro 스마트 보호 네트워크(Smart Feedback이라고도 함)
소프트웨어 안전	순수 IPv6 OfficeScan 에이전트는 Trend Micro에서 호스팅하는 인증된 안전한 소프트웨어 서비스에 연결할 수 없습니다.
플러그인 솔루션	플러그인 솔루션은 IPv6을 지원하지 않으므로 순수 IPv6 OfficeScan 에이전트는 플러그인 솔루션을 설치할 수 없습니다.
프록시 연결	순수 IPv6 OfficeScan 에이전트는 순수 IPv4 프록시 서버를 통해 연결할 수 없습니다.

이러한 제한 사항은 대부분 IPv4 주소와 IPv6 주소 간에 변환할 수 있는 이중 스택 프록시 서버(예: DeleGate)를 설치하여 해결할 수 있습니다. OfficeScan 에이전트와 이 에이전트가 연결하는 엔터티 사이에 프록시 서버를 배치하십시오.

IPv6 주소 구성

웹 콘솔에서 IPv6 주소 또는 IPv6 주소 범위를 구성할 수 있습니다. 다음은 몇 가지 구성 지침입니다.

- OfficeScan에서는 표준 IPv6 주소 표시를 사용합니다.

  예:

  ```
  2001:0db7:85a3:0000:0000:8a2e:0370:7334
  ```

  ```
  2001:db7:85a3:0:0:8a2e:370:7334
  ```

```
2001:db7:85a3::8a2e:370:7334
```

```
::ffff:192.0.2.128
```

- OfficeScan에서는 다음과 같은 링크-로컬 IPv6 주소도 사용합니다.

```
fe80::210:5aff:feaa:20a2
```

경고!

OfficeScan에서 링크-로컬 IPv6 주소를 사용할 수 있지만 경우에 따라 예상대로 작동하지 않을 수도 있으므로 링크-로컬 IPv6 주소를 지정할 때 각별히 주의해야 합니다. 예를 들어 소스가 다른 네트워크 세그먼트에 있고 링크-로컬 IPv6 주소로 식별되는 경우 OfficeScan 에이전트가 업데이트 소스에서 업데이트할 수 없습니다.

- IPv6 주소가 URL의 일부인 경우 대괄호([])로 주소를 묶습니다.
- IPv6 주소 범위의 경우 일반적으로 접두사와 접두사 길이가 필요합니다. 서버에서 IP 주소를 쿼리해야 하는 구성의 경우 서버에서 많은 수의 IP 주소를 쿼리할 때 발생할 수 있는 성능 문제를 방지하기 위해 접두사 길이 제한이 제한됩니다. 예를 들어 외부 서버 관리 기능의 경우 접두사 길이는 112자(65,536개의 IP 주소)에서 128자(2개의 IP 주소) 사이여야 합니다.
- IPv6 주소 또는 주소 범위가 포함된 일부 설정은 OfficeScan 에이전트에 배포되지만 OfficeScan 에이전트에서 무시됩니다. 예를 들어 스마트 보호 소스 목록을 구성하고 해당 IPv6 주소로 식별되는 스마트 보호 서버를 포함한 경우 순수 IPv4 OfficeScan 에이전트는 이러한 서버를 무시하고 다른 스마트 보호 소스에 연결합니다.

IP 주소가 표시되는 화면

이 항목에서는 IP 주소가 표시되는 웹 콘솔의 위치를 설명합니다.

위치	설명
에이전트 트리	에이전트 트리가 표시될 때마다 순수 IPv6 OfficeScan 에이전트의 IPv6 주소가 **IP 주소** 열 아래에 표시됩니다. 이중 스택 OfficeScan 에이전트의 경우 IPv6 주소를 사용하여 서버에 등록하는 경우 해당 IPv6 주소가 표시됩니다. **참고** 이중 스택 OfficeScan 에이전트에서 서버에 등록할 때 사용하는 IP 주소는 **에이전트** > **글로벌 에이전트 설정 > 네트워크** > **기본 IP 주소**에서 제어할 수 있습니다. 에이전트 트리 설정을 파일로 내보내면 IPv6 주소도 내보낸 파일에 표시됩니다.
에이전트 상태	자세한 에이전트 정보는 **에이전트** > **에이전트 관리 > 상태**에서 확인할 수 있습니다. 이 화면에서는 순수 IPv6 OfficeScan 에이전트의 IPv6 주소와 IPv6 주소를 사용하여 서버에 등록한 이중 스택 OfficeScan 에이전트의 IPv6 주소가 표시됩니다.
로그	이중 스택 및 순수 IPv6 OfficeScan 에이전트의 IPv6 주소는 다음 로그에 표시됩니다. • 바이러스/악성 프로그램 로그 • 스파이웨어/그레이웨어 로그 • 방화벽 로그 • 연결 확인 로그
Control Manager 콘솔	다음 표에는 Control Manager 콘솔에 표시되는 OfficeScan 서버 및 OfficeScan 에이전트의 IP 주소가 나와 있습니다. • 이중 스택 서버: IPv4 및 IPv6 • 순수 IPv4 서버: IPv4 • 순수 IPv6 서버: IPv6 • 이중 스택 OfficeScan 에이전트: OfficeScan 에이전트를 OfficeScan 서버에 등록할 때 사용한 IP 주소 • 순수 IPv4 OfficeScan 에이전트: IPv4 • 순수 IPv6 OfficeScan 에이전트: IPv6

부록 B

Windows Server Core 지원

이 부록에서는 Windows Server Core에 대한 OfficeScan 지원 기능을 설명합니다.

Windows Server Core 지원

Windows Server Core는 Windows Server 버전의 "최소" 설치입니다. Server Core에서는

- 대부분의 Windows Server 옵션 및 기능이 제거됩니다.
- 서버에서 훨씬 가벼운 핵심 운영 체제를 실행합니다.
- 작업이 주로 명령줄 인터페이스에서 수행됩니다.
- 운영 체제에서 보다 적은 서비스를 실행하므로 시작 중에 필요한 리소스가 적습니다.

OfficeScan에서는 다음과 같은 Windows Server Core 버전에서 OfficeScan 에이전트 설치를 지원합니다.

- Windows Server Core 2008
- Windows Server Core 2008 R2
- Windows Server Core 2012
- Windows Server Core 2012 R2
- Windows Server Core 2016

OfficeScan 에이전트는 Server Core를 지원합니다. 이 섹션에는 Server Core의 지원 범위에 대한 정보가 수록되어 있습니다.

OfficeScan 서버는 Server Core를 지원하지 않습니다.

Windows Server Core 설치 방법

다음 설치 방법은 지원되지 않거나 부분적으로 지원됩니다.

- 웹 설치 페이지: 이 방법은 Server Core에 Internet Explorer가 없으므로 지원되지 않습니다.

- Trend Micro Vulnerability Scanner: Vulnerability Scanner 도구는 Server Core에서 로컬로 실행할 수 없습니다. OfficeScan 서버 또는 다른 엔드포인트에서 도구를 실행할 수 있습니다.

지원되는 설치 방법은 다음과 같습니다.

- 원격 설치. 자세한 내용은 OfficeScan 웹 콘솔에서 원격으로 설치 페이지 5-20를 참조하십시오.
- 로그인 스크립트 설정
- 에이전트 패키지 도구

로그인 스크립트 설정을 사용한 OfficeScan 에이전트 설치

절차

1. 대상 엔드포인트에서 명령 프롬프트를 엽니다.
2. 다음 명령을 입력하여 OfficeScan 서버에서 AutoPcc.exe 파일 위치를 매핑합니다.

   ```
   net use <매핑된 드라이브 문자> \\<OfficeScan 서버 호스트 이름 또는 IP 주소>\ofcscan
   ```

   예:

   ```
   net use P: \\10.1.1.1\ofcscan
   ```

3. 대상 서버의 사용자 이름과 암호를 제공합니다.

   AutoPcc.exe의 위치가 성공적으로 매핑되었다고 알리는 메시지가 나타납니다.

4. 매핑된 드라이브 문자와 콜론을 입력하여 AutoPcc.exe 위치로 변경합니다.
   예:

   ```
   P:
   ```

5. 다음을 입력하여 설치를 시작합니다.

   ```
   AutoPcc.exe
   ```

다음 그림에서는 명령 프롬프트의 명령과 결과를 보여 줍니다.

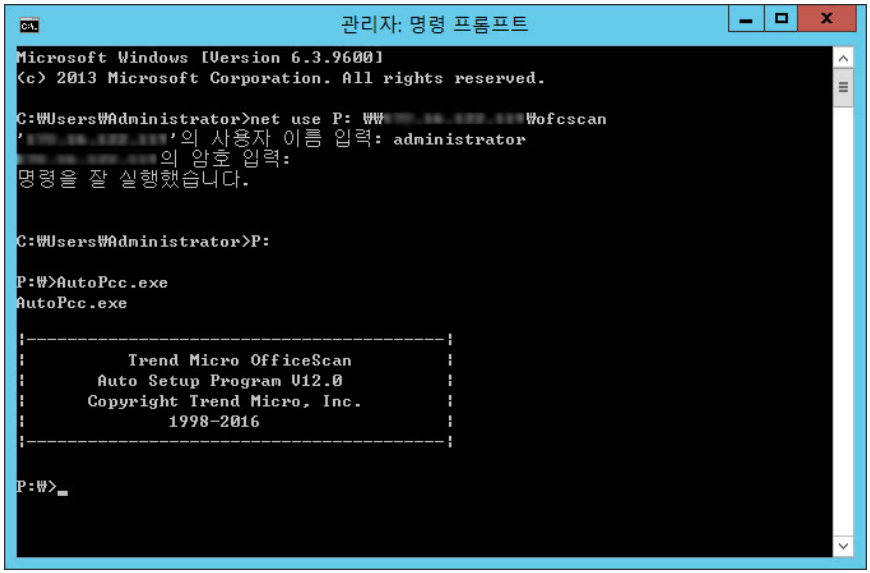


그림 B-1. 로그인 스크립트 설정을 사용하여 OfficeScan 에이전트를 설치하는 방법을 보여 주는 명령 프롬프트

OfficeScan 에이전트 패키지를 사용하여 OfficeScan 에이전트 설치

절차

1. 패키지를 만듭니다.

   자세한 내용은 에이전트 패키지 도구를 사용한 설치 페이지 5-26를 참조하십시오.

2. 명령 프롬프트를 엽니다.

3. 다음 명령을 입력하여 OfficeScan 에이전트 패키지 위치를 매핑합니다.

```
net use <매핑된 드라이브 문자> \\<에이전트 패키지 위치>
```

예:

```
net use P: \\10.1.1.1\Package
```

OfficeScan 에이전트 패키지 위치가 성공적으로 매핑되었는지를 알리는 메시지가 나타납니다.

4. 매핑된 드라이브 문자와 콜론을 입력하여 OfficeScan 에이전트 패키지 위치로 변경합니다. 예:

   ```
   P:
   ```

5. 다음 명령을 입력하여 Server Core 엔드포인트의 로컬 디렉터리에 OfficeScan 에이전트 패키지를 복사합니다.

   ```
   copy <패키지 파일 이름> <패키지를 복사할 Server Core 엔드포인트의 디렉터리>
   ```

   예:

   ```
   copy officescan.msi C:\Client Package
   ```

   OfficeScan 에이전트 패키지가 성공적으로 매핑되었는지를 알리는 메시지가 나타납니다.

6. 로컬 디렉터리로 변경합니다. 예:

   ```
   C:
   ```

   ```
   cd C:\Client Package
   ```

7. 패키지 파일 이름을 입력하여 설치를 시작합니다. 예:

   ```
   officescan.msi
   ```

다음 그림에서는 명령 프롬프트의 명령과 결과를 보여 줍니다.

그림 B-2. 에이전트 패키지를 사용하여 OfficeScan 에이전트를 설치하는 방법을 보여 주는 명령 프롬프트

Windows Server Core의 OfficeScan 에이전트 기능

대부분의 OfficeScan 에이전트 기능을 Server Core의 Windows Server 2008/2012/2016 작업에서 사용할 수 있습니다. 지원되지 않는 기능은 독립 모드뿐입니다.

Windows Server 2008/2012/2016에서 사용할 수 있는 기능의 목록은 OfficeScan 에이전트 기능 페이지 5-3 항목을 참조하십시오.

OfficeScan 에이전트 콘솔은 명령줄 인터페이스에서만 액세스할 수 있습니다.

참고

일부 OfficeScan 에이전트 콘솔 화면에는 도움말 단추가 포함되어 있으며, 이 단추를 클릭하면 상황에 맞는 HTML 기반 도움말이 열립니다. Windows Server Core 2008/2012/2016에는 브라우저가 없으므로 사용자는 도움말을 사용할 수 없습니다. 도움말을 보려면 브라우저를 설치해야 합니다.

Windows Server Core 명령

명령줄 인터페이스에서 명령을 실행하여 OfficeScan 에이전트 작업을 수행합니다.

명령을 실행하려면 PccNTMon.exe의 위치로 이동합니다. 이 프로세스는 OfficeScan 에이전트 콘솔을 시작합니다. 이 프로세스는 <에이전트 설치 폴더> 아래에 있습니다.

다음 표에는 사용 가능한 명령이 나와 있습니다.

표 B-1. Windows Server Core 명령

명령	조치
`pccnt <드라이브 또는 폴더 경로>`	지정된 드라이브 또는 폴더에서 보안 위험을 검색합니다. 지침: • 폴더 경로에 공백이 있으면 따옴표로 전체 경로를 묶습니다. • 개별 파일 검색은 지원되지 않습니다. 올바른 명령: • `pccnt C:₩` • `pccnt D:₩Files` • `pccnt "C:₩Documents and Settings"` 잘못된 명령: • `pccnt C:₩Documents and Settings` • `pccnt D:₩Files₩example.doc`
`pccntmon -r`	실시간 모니터를 엽니다.
`pccntmon -v`	에이전트 구성 요소 및 해당 버전을 나열합니다.
`pccntmon -u`	OfficeScan 에이전트 구성 요소를 업데이트합니다.

명령	조치
`pccntmon -n <unload_password>`	OfficeScan 에이전트을(를) 종료합니다. OfficeScan 에이전트를 다시 로드하려면 다음 명령을 입력합니다. `pccntmon`
`pccntmon -m <uninstall_password>`	OfficeScan 에이전트을(를) 제거합니다.

명령	조치

pccntmon -c	명령줄에 다음 정보를 표시합니다.
	• 검색 방법
	  • 스마트 스캔
	  • 표준 스캔
	• 패턴 상태
	  • 업데이트된 날짜
	  • 오래됨
	• 실시간 검색 서비스
	  • 작동 중
	  • 사용 안 함 또는 작동하지 않음
	• 에이전트 연결 상태
	  • 온라인
	  • 독립
	  • 오프라인
	• 웹 검증 서비스
	  • 사용 가능
	  • 다시 연결하는 중
	• 파일 검증 서비스
	  • 사용 가능
	  • 다시 연결하는 중

pccntmon -h	사용 가능한 모든 명령을 표시합니다.

부록 C

Windows 8/8.1/10 및 Windows Server 2012/2016 지원

이 부록에서는 OfficeScan의 Windows 8/8.1/10 및 Windows Server 2012/2016 지원 기능을 설명합니다.

Windows 8/8.1/10 및 Windows Server 2012/2016 정보

Windows 8/8.1 및 Windows Server 2012/2016은 데스크톱 모드와 Windows UI 모드의 두 가지 작동 모드를 제공합니다. 사용자는 Windows 10을 데스크톱 모드로 실행할지 태블릿 모드로 실행할지 선택할 수 있습니다. 데스크톱 모드는 클래식 Windows **시작** 화면과 유사합니다.

Windows UI 모드는 Windows Phone에서 사용된 것과 유사한 새로운 사용자 인터페이스 환경을 제공합니다. 새로운 기능에는 스크롤 터치 스크린 인터페이스, 타일, 알림 메시지 등이 있습니다.

표 C-1. 타일 및 알림 메시지

제어	설명
타일	타일은 이전 Windows 릴리스에서 사용된 데스크톱 아이콘과 유사합니다. 사용자는 타일을 클릭하거나 탭하여 타일과 연결된 응용 프로그램을 시작할 수 있습니다. 라이브 타일은 동적으로 업데이트되는 응용 프로그램 관련 정보를 제공합니다. 응용 프로그램은 실행 중이지 않은 경우에도 타일에 정보를 게시할 수 있습니다.
알림 메시지	알림 메시지는 팝업 메시지와 유사합니다. 이러한 알림은 응용 프로그램이 실행되는 동안 발생하는 이벤트에 대한 시간을 다투는 정보를 제공합니다. 알림 메시지는 Windows가 현재 데스크톱 모드에서 실행되든, 잠금 화면을 표시하든, 다른 응용 프로그램을 실행 중이든 관계없이 전경에 나타납니다. **참고** 응용 프로그램에 따라 일부 화면 또는 각 모드에 알림 메시지가 나타나지 않을 수도 있습니다.

OfficeScan의 타일 및 알림 지원

다음 표에서는 OfficeScan에서 Windows UI 모드의 타일 및 알림 메시지를 지원하는 방식을 설명합니다.

표 C-2. OfficeScan의 타일 및 알림 지원

제어	OFFICESCAN 지원
타일	OfficeScan은 사용자에게 OfficeScan 에이전트 프로그램에 연결하는 타일을 제공합니다. 사용자가 타일을 클릭하면 Windows가 데스크톱 모드로 전환되고 OfficeScan 에이전트 프로그램이 표시됩니다. **참고** OfficeScan은 라이브 타일을 지원하지 않습니다.
알림 메시지	OfficeScan은 다음과 같은 알림 메시지를 제공합니다. • 의심스러운 프로그램 발견 • 예약 검색 • 위협 해결 • 컴퓨터를 다시 시작해야 합니다. • USB 저장 장치 발견 • 비상 발견 **참고** OfficeScan은 Windows UI 모드에서만 알림 메시지를 표시할 수 있습니다.

Windows 8/8.1 및 Windows Server 2012에서 알림 메시지 사용

사용자는 OfficeScan 에이전트 엔드포인트에서 **PC 설정**을 수정하여 알림 메시지를 받도록 선택할 수 있습니다. OfficeScan을 사용할 때는 알림 메시지를 사용하는 것이 좋습니다.

절차

1. 마우스 포인터를 화면 오른쪽 아래로 이동하여 **참** 메뉴 모음을 표시합니다.

2. **설정** > **PC 설정 변경**을 클릭합니다.

   PC 설정 화면이 나타납니다.

3. **알림**을 클릭합니다.

4. **알림** 섹션에서 다음 설정을 **설정**으로 지정합니다.

   - **앱 알림 표시**
   - **잠금 화면에 앱 알림 표시**(선택 사항)
   - **알림 사운드**(선택 사항)

Windows 10 및 Windows Server 2016에서 알림 메시지 사용

사용자는 OfficeScan 에이전트 엔드포인트에서 **Active Center**에 액세스하여 알림 메시지를 받도록 선택할 수 있습니다. OfficeScan을 사용할 때는 알림 메시지를 사용하도록 설정해야 합니다.

절차

1. 시스템 트레이에서 알림 아이콘을 클릭하고 **모든 설정**을 클릭합니다.
2. 설정 화면에서 **시스템** 및 **알림 & 작업**을 클릭합니다.
3. **알림** 섹션에서 **앱 알림 표시** 설정을 **설정**으로 지정합니다.

UI 모드의 OfficeScan 기능 지원

사용자가 Windows 8/8.1 또는 Windows Server 2012/2016을 작동하는 모드는 사용되는 Internet Explorer 10 이상 버전에 영향을 주며 이로 인해 OfficeScan 기능마다 제공하는 지원 수준이 달라집니다. 다음 표에는 데스크톱 모드와 Windows UI 모드에서 여러 가지 OfficeScan 기능의 지원 수준이 나와 있습니다.

참고

나열되지 않은 기능은 두 Windows 작동 모드 모두에서 완전한 지원을 제공합니다.

표 C-3. UI 모드의 OfficeScan 기능 지원

기능	데스크톱 모드	WINDOWS UI
Web server 콘솔	전체 지원	지원되지 않음
웹 검증	전체 지원	제한된 지원 • HTTPS 검색을 사용할 수 없음
방화벽	전체 지원	제한된 지원 • 응용 프로그램 필터링을 사용할 수 없음

Internet Explorer 10/11 및 Microsoft Edge

Internet Explorer(IE) 10은 Windows 8/8.1 및 Windows Server 2012의 기본 브라우저입니다. Internet Explorer 10 이상은 Windows UI용과 데스크톱 모드용의 두 가지 버전으로 제공됩니다.

Microsoft Edge는 Windows 10 및 Windows Server 2016의 기본 브라우저입니다.

참고

Microsoft Edge는 Plug-in 확장 프로그램을 지원하지 않기 때문에 HTTPS 검색은 Microsoft Edge에서 사용하지 않도록 설정됩니다.

Windows UI용 Internet Explorer 10 이상에서는 플러그인 없는 검색 환경을 제공합니다. 웹 검색용 Plug-in 프로그램은 이전에 설정된 표준이 없었으므로 이러한 Plug-in 프로그램에서 사용하는 코드의 품질이 변수입니다. 또한 플러그인은 추가 시스템 리소스를 사용하므로 악성 프로그램에 감염될 위험이 증가합니다.

Microsoft에서 이전에 사용한 플러그인 솔루션을 대체하기 위해 새로운 표준 기반 기술을 따르는 Windows UI용 Internet Explorer 10 이상을 개발했습니다. 다음

표에는 Internet Explorer 10 이상에서 이전의 플러그인 기술 대신 사용하는 기술이 나와 있습니다.

표 C-4. 표준 기반 기술과 Plug-in 프로그램의 비교

기능	W3C(World Wide Web) 표준 기술	플러그인에 상응하는 예
비디오 및 오디오	HTML5 비디오 및 오디오	• 플래시 • Apple QuickTime • Silverlight
그래픽	• HTML5 캔버스 • SVG(스케일러블 벡터 그래픽) • CSS 스타일시트, 레벨 3(CSS3) 변환 및 애니메이션 • CSS 변환	• 플래시 • Apple QuickTime • Silverlight • Java 애플릿
오프라인 저장	• 웹 저장 • 파일 API • IndexedDB • 응용 프로그램 캐시 API	• 플래시 • Java 애플릿 • Google Gears
네트워크 통신, 리소스 공유, 파일 업로드	• HTML 웹 메시징 • CORS(Cross-origin resource sharing)	• 플래시 • Java 애플릿

Microsoft에서는 데스크톱 모드용 플러그인 호환 Internet Explorer 10 이상 버전도 개발했습니다. Windows UI 모드 사용자가 추가 Plug-in 프로그램이 필요한 웹 사이트를 방문한 경우 Internet Explorer 10 이상에 데스크톱 모드로 전환하라는 알림이 표시됩니다. 데스크톱 모드에서는 타사 Plug-in 프로그램을 사용하거나 설치해야 하는 웹 사이트를 볼 수 있습니다.

부록 D

OfficeScan 롤백

이 부록에서는 OfficeScan 서버 및 에이전트 롤백 지원에 대해 설명합니다.

서버 백업 패키지를 사용하여 OfficeScan 서버 및 OfficeScan 에이전트 롤백

OfficeScan 롤백 절차에서는 OfficeScan 에이전트를 롤백한 다음 OfficeScan 서버를 롤백합니다.

중요

- 관리자는 설치 프로세스 중 서버를 백업하도록 선택한 경우에만 다음 절차에 따라 OfficeScan 서버 및 에이전트를 롤백할 수 있습니다. 서버 백업 파일을 사용할 수 없는 경우에는 기존에 설치한 OfficeScan 버전의 *설치 및 업그레이드 안내서*에서 수동 롤백 절차를 참조하십시오.
- 이 OfficeScan 버전에서는 다음 OfficeScan 버전으로의 롤백만 지원합니다.
  - 중요한 패치가 포함된 OfficeScan 11.0 Service Pack 1
  - OfficeScan 11.0 Service Pack 1
  - OfficeScan 11.0
  - OfficeScan 10.6 Service Pack 3

OfficeScan 에이전트 롤백

OfficeScan에서는 복원 중인 서버와 동일한 버전으로만 OfficeScan 에이전트를 롤백할 수 있습니다. OfficeScan 에이전트를 서버보다 이전 버전으로 롤백할 수는 없습니다.

중요

OfficeScan 서버를 롤백하기 전에 OfficeScan 에이전트를 롤백해야 합니다.

절차

1. OfficeScan 에이전트에서 에이전트 프로그램을 업그레이드할 수 있는지 확인합니다.

a. OfficeScan XG 웹 콘솔에서 **에이전트** > **에이전트 관리**로 이동합니다.

b. 롤백할 OfficeScan 에이전트를 선택합니다.

c. **설정** > **권한 및 기타 설정** > **기타 설정** 탭을 클릭합니다.

d. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음** 옵션을 사용하도록 설정합니다.

2. OfficeScan XG 웹 콘솔에서 **업데이트** > **에이전트** > **업데이트 소스**로 이동합니다.

3. **사용자 정의 업데이트 소스**를 선택합니다.

4. **사용자 정의 업데이트 소스 목록**에서 **추가**를 클릭합니다.

   새 화면이 열립니다.

5. 롤백할 OfficeScan 에이전트의 IP 주소를 입력합니다.

6. 업데이트 소스 URL을 입력합니다.

   예를 들어 다음과 같이 입력합니다.

   ```
   http://<OfficeScan 서버의 IP 주소>:<포트>/OfficeScan/download/Rollback
   ```

7. **저장**을 클릭합니다.

8. **모든 에이전트에 알림**을 클릭합니다.

   롤백할 OfficeScan 에이전트를 업데이트 소스에서 업데이트하면 OfficeScan 에이전트가 제거되고 이전 OfficeScan 에이전트 버전이 설치됩니다.

   팁

   관리자는 OfficeScan 에이전트에서 수동 업데이트를 시작하여 롤백 프로세스에 소요되는 시간을 단축할 수 있습니다. 자세한 내용은 수동으로 OfficeScan 에이전트 업데이트 페이지 6-42를 참조하십시오.

9. 이전 OfficeScan 에이전트 버전이 설치된 후 사용자에게 엔드포인트를 다시 시작하도록 알립니다.

롤백 프로세스가 완료된 후 OfficeScan 에이전트는 동일한 OfficeScan 서버에 계속 보고합니다.

참고

OfficeScan 에이전트를 롤백하면 바이러스 패턴을 비롯한 구성 요소도 모두 이전 버전으로 롤백됩니다. 관리자가 OfficeScan 서버를 롤백하지 않은 경우 롤백한 OfficeScan 에이전트에서 구성 요소를 업데이트할 수 없습니다. 관리자가 롤백한 OfficeScan 에이전트의 업데이트 소스를 표준 업데이트 소스로 변경해야만 이후 구성 요소 업데이트를 받을 수 있습니다.

이전 OfficeScan 서버 버전 복원

OfficeScan 서버 복원 절차를 수행하려면 관리자가 OfficeScan XG 서버를 제거하고, 이전 서버 버전을 다시 설치하고, Windows 서비스를 수동으로 중지하고, 시스템 레지스트리를 업데이트하고, OfficeScan 설치 디렉터리의 OfficeScan 서버 파일을 바꿔야 합니다.

중요

OfficeScan 서버를 복원하기 전에 OfficeScan 에이전트를 롤백해야 합니다.

절차

1. OfficeScan XG 서버를 제거합니다.
2. 이전 OfficeScan 서버 버전을 설치합니다.

팁

서버를 복원할 때 호스트 이름이나 IP 주소를 변경하지 않는 것이 좋습니다.

이전 서버 버전을 확인하려면 <서버 설치 폴더>로 이동하여 OfficeScan XG 서버 설치 시 생성된 복원 폴더를 확인합니다. 폴더 이름은(<복원 폴더 버전>이라고도 함) 다음 중 하나입니다.

- OSCE11_SP1: OfficeScan 11.0 Service Pack 1
- OSCE11: OfficeScan 11.0
- OSCE106_SP3: OfficeScan 10.6 Service Pack 3

3. OfficeScan 서버 컴퓨터에서 다음 서비스를 중지합니다.
   - 침입 탐지 방화벽(설치된 경우)
   - Trend Micro Local Web Classification Server
   - Trend Micro Smart Scan Server
   - OfficeScan Active Directory Integration Service
   - OfficeScan Control Manager Agent
   - OfficeScan Plug-in Manager
   - OfficeScan Master Service
   - World Wide Web Publishing 서비스
4. <서버 설치 폴더>₩<복원 폴더 버전>₩ 디렉터리의 모든 파일과 디렉터리를 <서버 설치 폴더>₩PCCSRV₩ 디렉터리에 복사하고 대체합니다.
5. OfficeScan 레지스트리를 복원합니다.
   a. **레지스트리 편집기**(`regedit.exe`)를 엽니다.
   b. 왼쪽 탐색 창에서 다음 레지스트리 키 중 하나를 선택합니다.
      - 32비트 시스템의 경우 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\OfficeScan\service`
      - 64비트 시스템의 경우 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Officescan\service`

c. **파일** > **가져오기...**로 이동합니다.

d. <서버 설치 폴더>₩<복원 폴더 버전>₩ 디렉터리에 있는 일반 OfficeScan 서버 .reg 파일을 선택합니다.

레지스트리 파일 이름의 형식은 다음과 같습니다.

RegBak_<복원 폴더 버전>.reg

e. **예**를 클릭하여 이전 OfficeScan 버전 키를 모두 복원합니다.

6. 선택적으로 데이터베이스 백업 일정을 복원합니다.

a. **레지스트리 편집기**(`regedit.exe`)를 엽니다.

b. 왼쪽 탐색 창에서 다음 레지스트리 키 중 하나를 선택합니다.

- 32비트 시스템의 경우 `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\Database Backup`
- 64비트 시스템의 경우 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\TrendMicro\Database Backup`

c. **파일** > **가져오기...**로 이동합니다.

d. <서버 설치 폴더>₩<복원 폴더 버전>₩ 디렉터리에 있는 데이터베이스 .reg 파일을 선택합니다.

레지스트리 파일 이름의 형식은 다음과 같습니다.

RegBak_DBBak_<복원 폴더 버전>.reg

e. **예**를 클릭하여 이전 OfficeScan 버전 키를 모두 복원합니다.

7. 명령줄 편집기를 열고(`cmd.exe`) 다음 명령을 입력하여 Local Web Classification Server 성능 카운터를 초기화합니다.

```
cd <서버 설치 폴더>\PCCSRV\LWCS

regsvr32.exe /u /s perfLWCSPerfMonMgr.dll

regsvr32.exe /s perfLWCSPerfMonMgr.dll
```

8. 다음 서비스를 다시 시작합니다.

- 침입 탐지 방화벽(설치된 경우)
- Trend Micro Local Web Classification Server
- Trend Micro Smart Scan Server
- OfficeScan Active Directory Integration Service
- OfficeScan Control Manager Agent
- OfficeScan Plug-in Manager
- OfficeScan Master Service
- Apache 2(Apache Web Server를 사용하는 경우)
- World Wide Web Publishing 서비스(IIS Web Server를 사용하는 경우)

9. Internet Explorer 캐시를 지우고 ActiveX 컨트롤을 수동으로 제거합니다. Internet Explorer 9에서 ActiveX 컨트롤을 제거하는 방법에 대한 자세한 내용은 http://windows.microsoft.com/en-us/internet-explorer/manage-add-ons#ic=ie-9를 참조하십시오.

   이전 OfficeScan 서버 버전 설정이 복원되었습니다.

팁

관리자는 **정보** 화면(**도움말** > **정보**)에서 OfficeScan 버전 번호를 확인하여 롤백 성공 여부를 확인할 수 있습니다.

10. 필요한 경우 웹 콘솔을 사용하여 OfficeScan 서버를 Control Manager 서버에 등록합니다.

11. 필요한 경우 웹 콘솔을 사용하여 OfficeScan 서버를 Deep Discovery 서버에 등록합니다.

참고

OfficeScan 서버와의 Deep Discovery 통합은 OfficeScan 10.6 Service Pack 2 이상에서 지원됩니다.

12. OfficeScan이 롤백되었는지 확인한 후 <서버 설치 폴더>₩<복원 폴더 버전>₩ 디렉터리의 파일을 모두 삭제합니다.

부록 E

용어집

이 용어집에 포함된 용어는 Trend Micro 제품 및 기술을 비롯하여 흔히 참조되는 엔드포인트 용어에 대한 추가 정보를 제공합니다.

액티브업데이트

액티브업데이트는 여러 Trend Micro 제품에 있는 공통적 기능입니다. Trend Micro 업데이트 웹 사이트에 연결되어 있을 때 액티브업데이트를 사용하면 인터넷을 통해 패턴 파일, 검색 엔진, 프로그램 및 기타 Trend Micro 구성 요소 파일의 최신 버전을 다운로드할 수 있습니다.

압축 파일

한 개 이상의 개별 파일과 적합한 프로그램(예: WinZip)을 통한 추출 정보가 들어 있는 단일 파일입니다.

Cookie

인터넷 사용자에 대한 정보(예: 이름, 기본 설정 및 관심 분야)를 저장하는 메커니즘으로, 이러한 정보는 나중에 사용할 수 있도록 웹 브라우저에 저장됩니다. 다음에 브라우저에 쿠키가 있는 웹 사이트에 액세스하면 브라우저에서 쿠키를 Web server로 보내기 때문에, Web server는 이 쿠키를 사용하여 사용자 정의 웹 페이지를 표시할 수 있습니다. 예를 들어 웹 사이트를 표시하면 사용자의 이름과 함께 환영 메시지가 표시되는 경우가 있습니다.

서비스 거부(DoS) 공격

서비스 거부(DoS) 공격은 엔드포인트나 네트워크를 대상으로 "서비스", 즉 네트워크 연결을 끊는 공격을 말합니다. 일반적으로 DoS 공격은 네트워크 대역폭에 부정적인 영향을 미치거나 엔드포인트 메모리와 같은 시스템 리소스의 과부하를 야기합니다.

DHCP

DHCP(Dynamic Host Control Protocol)는 동적 IP 주소를 네트워크의 장치에 할당하는 프로토콜입니다. 동적 주소 지정을 사용하면 장치가 네트워크에 연결될

때마다 다른 IP 주소를 가질 수 있습니다. 일부 시스템의 경우 장치가 네트워크에 연결되어 있는 동안에도 해당 IP 주소가 변경될 수 있습니다. DHCP는 정적 IP 주소와 동적 IP 주소를 함께 사용하는 것도 지원합니다.

DNS

DNS(Domain Name System)는 호스트 이름을 IP 주소로 변환하기 위해 인터넷에 주로 사용되는 범용 데이터 쿼리 서비스입니다.

DNS 에이전트가 DNS Server에서 호스트 이름과 주소 데이터를 요청하는 프로세스를 확인 프로세스라고 합니다. 기본 DNS 구성에서는 한 서버에서 기본 확인을 수행합니다. 예를 들면 원격 서버가 다른 서버에 현재 영역에 있는 시스템의 데이터에 대해 쿼리합니다. 그러면 원격 서버의 에이전트 소프트웨어가 확인 프로그램에 쿼리하면 이 프로그램이 해당 데이터베이스 파일의 요청에 응답합니다.

도메인 이름

로컬 호스트 이름과 도메인 이름으로 구성된 시스템의 전체 이름(예: tellsitall.com)입니다. 도메인 이름은 인터넷에서 호스트에 대한 고유한 인터넷 주소를 확인할 수 있어야 합니다. 이 프로세스를 "이름 확인"이라고 하며, DNS(Domain Name System)가 사용됩니다.

동적 IP 주소

DIP 주소는 DHCP 서버에 의해 할당된 IP 주소입니다. 엔드포인트의 MAC 주소는 동일하게 유지되지만 DHCP 서버가 엔드포인트에 새 IP 주소(사용 가능한 경우)를 할당할 수 있습니다.

ESMTP

ESMTP(Enhanced Simple Mail Transport Protocol)는 보안, 인증 및 기타 장치를 포함하여 대역폭을 절감하고 서버를 보호합니다.

최종 사용자 사용권 계약

최종 사용자 사용권 계약 또는 EULA는 소프트웨어 게시자와 소프트웨어 사용자 간의 법적 계약입니다. 이 계약에는 일반적으로 사용자측에 대한 제한 사항이 요약되어 있으며, 사용자가 설치 중에 "동의함"을 클릭하지 않을 경우 계약을 맺을 수 없습니다. 물론 "동의하지 않음"을 클릭하는 경우 소프트웨어 제품의 설치가 종료됩니다.

일부 무료 소프트웨어를 설치하는 동안 표시되는 EULA 화면에서 실수로 "동의함"을 클릭하는 경우 스파이웨어 및 기타 다른 유형의 그레이웨어가 사용자 컴퓨터에 설치될 수 있습니다.

잘못된 판정

잘못된 판정은 파일이 보안 소프트웨어에 의해 감염된 것으로 잘못 판별될 경우 발생합니다.

FTP

FTP(File Transfer Protocol)는 인터넷을 통해 서버에서 클라이언트로 파일을 전송하는 데 사용되는 표준 프로토콜입니다. 자세한 내용은 Network Working Group RFC 959를 참조하십시오.

GeneriClean

참조 치료라고도 하는 GeneriClean은 바이러스 클린업 구성 요소를 사용하지 않고도 바이러스/악성 프로그램을 치료하는 새로운 기술입니다. GeneriClean에서

는 발견된 파일을 기준으로 사용하여 발견된 파일의 메모리와 레지스트리 항목에 해당 프로세스/서비스가 있는지 확인한 후 함께 제거합니다.

핫픽스

핫픽스는 단일 고객 관련 문제에 대한 해결 방법 또는 솔루션입니다. 핫픽스는 문제별로 제공되므로 모든 고객에게 릴리스되지는 않습니다. Windows 핫픽스에는 설치 프로그램이 포함되어 있는 반면, 비 Windows 핫픽스는 그렇지 않습니다. 따라서 일반적으로 프로그램 디먼을 중지한 후 파일을 복사하여 설치 프로그램의 해당 파일을 덮어 쓴 다음 디먼을 다시 시작해야 합니다.

기본적으로 OfficeScan 에이전트는 핫픽스를 설치할 수 있습니다. OfficeScan 에이전트에서 핫픽스를 설치하지 않게 하려면 웹 콘솔에서 **에이전트** > **에이전트 관리**로 이동하여 **설정** > **권한 및 기타 설정** > **기타 설정** 탭에서 에이전트 업데이트 설정을 변경합니다.

OfficeScan 서버에 핫픽스를 배포하려 했지만 제대로 배포되지 않은 경우, 터치 도구를 사용하여 핫픽스의 타임스탬프를 변경하십시오. 그러면 OfficeScan이 핫픽스 파일을 새 파일로 해석하여 서버가 자동으로 핫픽스를 다시 배포합니다. 이 도구에 대한 자세한 내용은 OfficeScan 에이전트 핫픽스에 대한 터치 도구 실행 페이지 6-50를 참조하십시오.

HTTP

HTTP(Hypertext Transfer Protocol)는 인터넷을 통해 서버에서 클라이언트로 웹 페이지(그래픽 및 멀티미디어 콘텐츠 포함)를 전송하는 데 사용되는 표준 프로토콜입니다.

HTTPS

SSL(Secure Socket Layer)을 사용한 HTTP(Hypertext Transfer Protocol)입니다. HTTPS는 보안 트랜잭션을 처리하는 데 사용되는 변형된 HTTP입니다.

ICMP

게이트웨이 또는 대상 호스트는 데이터그램 처리 오류를 보고하는 경우와 같이 ICMP(Internet Control Message Protocol)를 사용하여 소스 호스트와 통신하는 경우가 종종 있습니다. ICMP는 IP의 상위 프로토콜인 것처럼 IP의 기본 지원을 사용하지만 실제로는 IP의 필수 부분으로서 모든 IP 모듈에서 구현되어야 합니다. ICMP 메시지는 여러 가지 상황에서 송신됩니다. 예를 들어 데이터그램이 대상에 도달할 수 없을 때, 게이트웨이가 데이터그램을 전달할 버퍼링 용량을 가지지 못할 때, 게이트웨이가 트래픽을 짧은 경로로 전송하기 위해 호스트를 지정할 때 등입니다. 인터넷 프로토콜이 절대적으로 신뢰성 있게 설계되지는 않으며 이 제어 메시지의 목적은 IP를 신뢰할 수 있도록 만들려는 것이 아니라 통신 환경의 문제에 대한 피드백을 제공하는 데 있습니다.

IntelliScan

IntelliScan은 검색할 파일을 식별하는 수단입니다. 실행 파일(예: .exe)의 경우 실제 파일 형식은 파일 내용에 따라 결정됩니다. 실행 파일이 아닌 파일(예: .txt)의 경우 실제 파일 형식은 파일 헤더에 따라 결정됩니다.

IntelliScan을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 성능 최적화: IntelliScan은 시스템 리소스를 최소로만 사용하므로 에이전트의 응용 프로그램에 영향을 미치지 않습니다.
- 검색 기간 단축: IntelliScan은 실제 파일 형식 식별을 사용하므로 감염에 취약한 파일만 검색합니다. 따라서 검색 시간은 모든 파일을 검색할 때보다 크게 단축됩니다.

IntelliTrap

바이러스 제작자는 종종 실시간 압축 알고리즘을 사용하여 바이러스 필터링을 회피하려고 시도합니다. IntelliTrap을 사용하면 실시간 압축 실행 파일을 차단하고 다른 악성 프로그램 특징과 연계하여 해당 바이러스가 네트워크에 들어올 위험을 줄일 수 있습니다. IntelliTrap에서 안전한 파일을 보안 위험으로 식별하고 잘못 차단할 수도 있기 때문에 IntelliTrap을 사용하는 경우에는 파일을 삭제

하거나 치료하지 않고 격리 보관하십시오. 사용자가 정기적으로 실시간 압축 실행 파일을 교환하는 경우에는 IntelliTrap을 해제하십시오.

IntelliTrap에서는 다음 구성 요소를 사용합니다.

- 바이러스 검색 엔진
- IntelliTrap 패턴
- IntelliTrap 예외 패턴

IP

"IP(인터넷 프로토콜)는 데이터그램이라고 하는 데이터 블록을 소스에서 대상으로 전송합니다. 여기서, 소스 및 대상은 고정된 길이의 주소로 식별되는 호스트입니다." (RFC 791)

Java 파일

Java는 Sun Microsystems에서 개발한 범용 프로그래밍 언어입니다. Java 파일에는 Java 코드가 들어 있습니다. Java는 플랫폼 독립적인 Java "애플릿" 형식으로 된 인터넷 프로그래밍을 지원합니다. 애플릿은 HTML 페이지에 포함할 수 있는 Java 프로그래밍 언어로 작성된 프로그램입니다. Java 기술을 사용할 수 있는 브라우저에서 애플릿이 포함된 페이지를 보는 경우, 애플릿은 해당 코드를 엔드포인트로 전송하고 브라우저의 Java Virtual Machine이 이 애플릿을 실행합니다.

LDAP

LDAP(Lightweight Directory Access Protocol)는 TCP/IP를 통해 실행되는 디렉터리 서비스를 쿼리하고 수정하기 위한 응용 프로그램 프로토콜입니다.

수신 포트

수신 포트는 데이터 교환을 위한 에이전트 연결 요청에 사용됩니다.

MCP 에이전트

Trend Micro MCP(Management Communication Protocol)는 관리되는 제품을 위한 Trend Micro의 차세대 에이전트입니다. Control Manager에서 OfficeScan과 통신하는 방식인 MCP는 TMI(Trend Micro Management Infrastructure)를 대체합니다. MCP는 다음과 같이 다양한 새로운 기능을 제공합니다.

- 네트워크 로드 및 패키지 크기 감소
- NAT 및 방화벽 통과 지원
- HTTPS 지원
- 단방향 및 양방향 통신 지원
- SSO(Single Sign-On) 지원
- 클러스터 노드 지원

혼합된 형태의 위협 공격

혼합된 형태의 위협 공격은 "Nimda" 또는 "Code Red" 위협처럼 엔터프라이즈 네트워크의 여러 진입점과 취약점을 이용합니다.

NAT

NAT(Network Address Translation)는 보안 IP 주소를 주소 풀의 등록된 임시 외부 IP 주소로 변환하는 표준입니다. NAT를 사용하면 개인적으로 할당된 IP 주소가 있는 신뢰할 수 있는 네트워크에서 인터넷에 액세스할 수 있습니다. 또한 네트워크에 있는 모든 시스템에 대해 등록된 IP 주소를 얻을 필요가 없습니다.

NetBIOS

NetBIOS(Network Basic Input Output System)는 DOS(디스크 운영 체제) BIOS(기본 입/출력 시스템)에 네트워크 기능과 같은 기능을 추가하는 API(응용 프로그램 인터페이스)입니다.

단방향 통신

NAT 통과는 현재 실제 네트워크 환경에서 점차 심각한 문제가 되고 있습니다. 이 문제를 해결하기 위해 MCP에는 단방향 통신이 사용됩니다. 단방향 통신에서는 MCP 에이전트가 서버로의 연결을 시작하고 서버에서 명령을 폴링합니다. 각 요청은 CGI 같은 명령 쿼리 또는 로그 전송입니다. 네트워크에 미치는 영향을 줄이기 위해 MCP 에이전트는 연결을 활성 상태로 유지하고 가능한 많은 연결을 엽니다. 후속 요청에는 열려 있는 기존의 연결이 사용됩니다. 연결이 끊어지는 경우 동일한 호스트에 대한 모든 SSL 연결에 세션 ID 캐시를 사용할 수 있으므로 재연결 시간이 크게 감소합니다.

패치

패치는 여러 프로그램 문제를 해결하는 핫픽스 및 보안 패치 그룹입니다. Trend Micro에서는 정기적으로 패치를 제공합니다. Windows 패치에는 설치 프로그램이 포함되는 반면, 일반적으로 비 Windows 패치에는 설치 스크립트가 들어 있습니다.

피싱 공격

피싱은 적법한 웹 사이트를 모방하여 웹 사용자의 개인 정보를 누설하도록 하는 급속하게 확산되고 있는 사기의 한 형태입니다.

대개의 경우 사용자 계정에 문제가 있어 즉시 수정하지 않으면 계정이 폐쇄될 것임을 알리는, 진짜처럼 보이는 긴급한 전자 메일을 받게 됩니다. 이러한 전자 메일에는 실제 사이트와 똑같아 보이는 웹 사이트에 대한 URL이 포함되어 있

습니다. 합법적인 전자 메일과 합법적인 웹 사이트를 복사한 후 수집된 데이터를 수신하는 백 엔드를 변경하는 것은 간단한 작업입니다.

이 전자 메일에서는 사용자에게 사이트에 로그온하여 특정 계정 정보를 확인하도록 알립니다. 해커는 사용자가 제공하는 로그온 이름, 암호, 신용 카드 번호 또는 주민 등록 번호 같은 데이터를 받습니다.

피싱 사기는 빠르고 저렴하여 지속하기 쉽습니다. 또한 해커는 사기를 통해 상당한 수익을 얻기도 합니다. 피싱은 컴퓨터를 잘 아는 사용자도 검색하기 어려우며 경찰에서 추적하기도 어렵습니다. 더욱이 고소하기는 거의 불가능합니다.

피싱 사이트로 의심되는 모든 웹 사이트를 Trend Micro에 보고해 주십시오.

Ping

Ping은 IP 주소로 ICMP 에코 요청을 전송하고 응답을 기다리는 유틸리티입니다. Ping 유틸리티를 통해 지정한 IP 주소를 사용하는 엔드포인트가 온라인 상태인지 여부를 확인할 수 있습니다.

POP3

POP3(우체국 프로토콜 3)는 전자 메일 메시지를 저장하고 이 메시지를 서버에서 클라이언트 전자 메일 응용 프로그램으로 전송하는 표준 프로토콜입니다.

프록시 서버

프록시 서버는 로컬 캐시나 원격 서버에서 문서를 가져오는 데 사용되는 특정 접두사가 포함된 URL을 사용한 다음 해당 URL을 요청자에게 반환하는 World Wide Web 서버입니다.

RPC

RPC(원격 프로시저 호출)는 한 호스트에서 프로그램을 실행하여 다른 호스트에서 코드가 실행되게 할 수 있는 네트워크 프로토콜입니다.

보안 패치

보안 패치는 모든 고객에게 배포하기에 적합한 보안 문제에 중점을 둡니다. Windows 보안 패치에는 설치 프로그램이 포함되는 반면, 비 Windows 패치에는 일반적으로 설치 스크립트가 들어 있습니다.

Service Pack

Service Pack은 다양한 핫픽스, 패치 및 기능 향상이 통합된 것으로, 제품 업그레이드로 간주됩니다. Windows 및 비 Windows Service Pack 모두에 설치 프로그램과 설치 스크립트가 포함됩니다.

SMTP

SMTP(Simple Mail Transport Protocol)는 인터넷을 통해 서버 간 및 에이전트와 서버 간에 전자 메일 메시지를 전송하는 데 사용되는 표준 프로토콜입니다.

SNMP

SNMP(Simple Network Management Protocol)는 관리 주의가 필요한 조건과 관련해 네트워크에 연결된 장치를 모니터링할 수 있는 프로토콜입니다.

SNMP 트랩

SNMP(Small Network Management Protocol) 트랩은 이 프로토콜을 지원하는 관리 콘솔을 사용하는 네트워크 관리자에게 알림을 전송하는 방법입니다.

OfficeScan은 MIB(Management Information Base)에 알림을 저장할 수 있습니다. 사용자는 MIB 브라우저를 사용하여 SNMP 트랩 알림을 볼 수 있습니다.

SSL

SSL(Secure Socket Layer)은 응용 프로그램 프로토콜(예: HTTP, Telnet 또는 FTP)과 TCP/IP 간에 계층적 데이터 보안을 제공하기 위해 Netscape에서 설계한 프로토콜입니다. 이 보안 프로토콜은 TCP/IP 연결에 대한 데이터 암호화, 서버 인증, 메시지 무결성 및 선택적 에이전트 인증을 제공합니다.

SSL 인증서

이 디지털 인증서는 보안 HTTPS 통신을 설정합니다.

TCP

TCP(Transmission Control Protocol)는 다중 네트워크 응용 프로그램을 지원하는 계층형 프로토콜의 한 계층에 맞게 설계된 연결 지향적인 종단 간 방식의 신뢰할 수 있는 프로토콜입니다. TCP는 주소 분석에 IP 데이터그램을 사용합니다. 자세한 내용은 DARPA Internet Program RFC 793을 참조하십시오.

Telnet

Telnet는 "네트워크 가상 터미널"을 생성함으로써 TCP에서 터미널 장치에 접속하는 표준 방법입니다. 자세한 내용은 Network Working Group RFC 854를 참조하십시오.

트로이 목마 포트

트로이 목마 포트는 대개 트로이 목마 프로그램에서 엔드포인트에 연결할 때 사용됩니다. 비상 발생 시 OfficeScan은 트로이 목마 프로그램에서 사용할 수 있는 다음 포트 번호를 차단합니다.

표 E-1. 트로이 목마 포트

포트 번호	트로이 목마 프로그램	포트 번호	트로이 목마 프로그램
23432	Asylum	31338	Net Spy
31337	Back Orifice	31339	Net Spy
18006	Back Orifice 2000	139	Nuker
12349	Bionet	44444	Prosiak
6667	Bionet	8012	Ptakks
80	Codered	7597	Qaz
21	DarkFTP	4000	RA
3150	Deep Throat	666	Ripper
2140	Deep Throat	1026	RSM
10048	Delf	64666	RSM
23	EliteWrap	22222	Rux
6969	GateCrash	11000	Senna Spy
7626	Gdoor	113	Shiver
10100	Gift	1001	Silencer
21544	Girl Friend	3131	SubSari
7777	GodMsg	1243	Sub Seven
6267	GW Girl	6711	Sub Seven

포트 번호	트로이 목마 프로그램	포트 번호	트로이 목마 프로그램
25	Jesrto	6776	Sub Seven
25685	Moon Pie	27374	Sub Seven
68	Mspy	6400	Thing
1120	Net Bus	12345	Valvo line
7300	Net Spy	1234	Valvo line

트러스트된 포트

서버와 OfficeScan 에이전트는 트러스트된 포트를 사용하여 서로 통신합니다.

트러스트된 포트를 차단한 다음 바이러스 비상 발생 후에 네트워크 설정을 정상으로 복원하는 경우 OfficeScan 에이전트에서 서버와 통신을 곧바로 다시 시작하지는 못합니다. 에이전트-서버 통신은 바이러스 사전 방역 설정 화면에서 지정한 시간이 경과한 후에야 복원됩니다.

OfficeScan에서는 HTTP 포트(기본적으로 8080)를 서버의 트러스트된 포트로 사용합니다. 설치 중에 다른 포트 번호를 입력할 수 있습니다. 이 트러스트된 포트 및 OfficeScan 에이전트의 트러스트된 포트를 차단하려면 포트 차단 화면에서 트러스트된 포트 차단 확인란을 선택합니다.

마스터 설치 관리자는 OfficeScan 에이전트의 트러스트된 포트를 설치 중에 임의로 생성합니다.

트러스트된 포트 확인

절차

1. <서버 설치 폴더>₩PCCSRV에 액세스합니다.
2. 메모장과 같은 텍스트 편집기를 사용하여 ofcscan.ini 파일을 엽니다.

3. 서버의 트러스트된 포트는 문자열 "Master_DomainPort"를 검색하여 그 옆의 값을 확인하십시오.

   예를 들어, 문자열이 `Master_DomainPort=80`으로 나타나면 서버의 트러스트된 포트는 포트 80입니다.

4. 에이전트의 트러스트된 포트는 문자열 "Client_LocalServer_Port"를 찾고 그 옆의 값을 확인합니다.

   예를 들어 문자열이 `Client_LocalServer_Port=41375`로 나타나면 에이전트의 트러스트된 포트는 포트 41375입니다.

양방향 통신

양방향 통신은 단방향 통신의 대체 방법입니다. 단방향 통신을 기반으로 하지만 서버 알림을 받는 추가 HTTP 기반 채널을 사용하는 양방향 통신은 MCP 에이전트에 의한 서버의 명령을 실시간으로 발송 및 처리하는 기능을 향상시킬 수 있습니다.

UDP

UDP(User Datagram Protocol)는 응용 프로그램에서 메시지를 다른 프로그램으로 전송하기 위해 IP와 함께 사용하는 비연결형 통신 프로토콜입니다. 자세한 내용은 DARPA Internet Program RFC 768을 참조하십시오.

치료할 수 없는 파일

바이러스 검색 엔진에서는 다음 파일을 치료할 수 없습니다.

표 E-2. 치료할 수 없는 파일 솔루션

치료할 수 없는 파일	설명 및 솔루션
트로이 목마에 감염된 파일	트로이 목마는 메시지를 표시하거나, 파일을 지우거나, 디스크를 포맷하는 등 대체로 유해한 동작을 의도하지 않게 무단으로 수행하는 프로그램입니다. 트로이 목마는 파일을 감염시키지 않으므로 치료할 필요가 없습니다. 솔루션: DCE(Damage Cleanup Engine) 및 Damage Cleanup 템플릿을 사용하여 트로이 목마를 제거합니다.
웜에 감염된 파일	웜은 자체 복사본이나 일부를 다른 엔드포인트 시스템으로 전파할 수 있는 독립형 프로그램(또는 프로그램 집합)입니다. 웜은 일반적으로 네트워크 연결이나 전자 메일 첨부 파일을 통해 전파됩니다. 웜은 독립형 프로그램이기 때문에 치료가 불가능합니다. 솔루션: Trend Micro에서는 웜을 삭제할 것을 권장합니다.
쓰기 방지 감염된 파일	솔루션: 파일을 치료할 수 있도록 쓰기 보호를 제거합니다.
암호로 보호된 파일	암호로 보호된 파일에는 암호로 보호된 압축 파일, 암호로 보호된 Microsoft Office 파일 등이 있습니다. 솔루션: 파일을 치료할 수 있도록 암호 보호를 제거합니다.
백업 파일	확장자가 RB0~RB9인 파일은 감염된 파일의 백업 복사본입니다. 치료 과정 중에 바이러스/악성 프로그램에 의해 파일이 손상되는 경우를 대비하여 감염된 파일의 백업본을 만듭니다. 솔루션: 감염된 파일을 성공적으로 치료한 경우에는 이 파일의 백업 복사본을 보관할 필요가 없습니다. 엔드포인트가 정상적으로 작동하는 경우 백업 파일을 삭제해도 됩니다.
휴지통에 있는 감염된 파일	시스템이 실행 중이기 때문에 휴지통에 있는 감염된 파일을 제거할 수 없습니다.
	NTFS 파일 시스템을 사용하는 Windows XP 또는 Windows Server 2003에서의 솔루션: 1. 관리자 권한으로 엔드포인트에 로그온합니다. 2. 응용 프로그램에서 파일을 잠그지 못하도록 하려면 실행 중인 모든 응용 프로그램을 닫습니다. 파일이 잠기면 Windows에서 이 파일을 삭제할 수 없습니다.

치료할 수 없는 파일	설명 및 솔루션

	3. 명령 프롬프트를 엽니다.
	4. 다음을 입력하여 파일을 삭제합니다.
	`cd \`
	`cd recycled`
	`del *.* /S`
	위의 마지막 명령은 휴지통에 있는 모든 파일을 삭제합니다
	5. 파일이 제거되었는지 확인합니다.

	기타 운영 체제(또는 NTFS를 사용하지 않는 운영 체제)에서의 솔루션
	1. 엔드포인트를 MS-DOS 모드에서 다시 시작합니다.
	2. 명령 프롬프트를 엽니다.
	3. 다음을 입력하여 파일을 삭제합니다.
	`cd \`
	`cd recycled`
	`del *.* /S`
	위의 마지막 명령은 휴지통에 있는 모든 파일을 삭제합니다

Windows Temp 폴더 또는 Internet Explorer 임시 폴더에 있는 감염된 파일	엔드포인트에서 Windows Temp 폴더 또는 Internet Explorer 임시 폴더에 있는 감염된 파일을 사용하기 때문에 해당 파일을 치료하지 못할 수 있습니다. 치료할 파일이 Windows 작업에 필요한 임시 파일일 수 있습니다.
	NTFS 파일 시스템을 사용하는 Windows XP 또는 Windows Server 2003에서의 솔루션: 1. 관리자 권한으로 엔드포인트에 로그온합니다. 2. 응용 프로그램에서 파일을 잠그지 못하도록 하려면 실행 중인 모든 응용 프로그램을 닫습니다. 파일이 잠기면 Windows에서 이 파일을 삭제할 수 없습니다. 3. 감염된 파일이 Windows Temp 폴더에 있는 경우:

치료할 수 없는 파일	설명 및 솔루션

	a. 명령 프롬프트를 열고 Windows Temp 폴더(Windows XP 또는 Windows Server 2003 엔드포인트의 경우 기본적으로 C:₩Windows₩Temp)로 이동합니다.
	b. 다음을 입력하여 파일을 삭제합니다.
	`cd temp`
	`attrib -h`
	`del *.* /S`
	위의 마지막 명령은 Windows Temp 폴더에 있는 모든 파일을 삭제합니다.
	4. 감염된 파일이 Internet Explorer 임시 폴더에 있는 경우:
	a. 명령 프롬프트를 열고 Internet Explorer 임시 폴더(Windows XP 또는 Windows Server 2003 엔드포인트의 경우 기본적으로 C:₩Documents and Settings₩<사용자 이름>₩Local Settings₩Temporary Internet Files)로 이동합니다.
	b. 다음을 입력하여 파일을 삭제합니다.
	`cd tempor~1`
	`attrib -h`
	`del *.* /S`
	위의 마지막 명령은 Internet Explorer 임시 폴더에 있는 모든 파일을 삭제합니다.
	c. 파일이 제거되었는지 확인합니다.

	기타 운영 체제(또는 NTFS를 사용하지 않는 운영 체제)에서의 솔루션 1. 엔드포인트를 MS-DOS 모드에서 다시 시작합니다. 2. 감염된 파일이 Windows Temp 폴더에 있는 경우: a. 명령 프롬프트를 열고 Windows Temp 폴더(Windows XP 또는 Windows Server 2003 엔드포인트의 경우 기본적으로 C:₩Windows₩Temp)로 이동합니다.

치료할 수 없는 파일	설명 및 솔루션

	b. 다음을 입력하여 파일을 삭제합니다.
	
	`cd temp`
	
	`attrib -h`
	
	`del *.* /S`
	
	위의 마지막 명령은 Windows Temp 폴더에 있는 모든 파일을 삭제합니다.
	
	c. 엔드포인트를 일반 모드에서 다시 시작합니다.
	
	3. 감염된 파일이 Internet Explorer 임시 폴더에 있는 경우:
	
	a. 명령 프롬프트를 열고 Internet Explorer 임시 폴더 (Windows XP 또는 Windows Server 2003 엔드포인트의 경우 기본적으로 C:₩Documents and Settings₩<사용자 이름>₩Local Settings₩Temporary Internet Files)로 이동합니다.
	
	b. 다음을 입력하여 파일을 삭제합니다.
	
	`cd tempor~1`
	
	`attrib -h`
	
	`del *.* /S`
	
	위의 마지막 명령은 Internet Explorer 임시 폴더에 있는 모든 파일을 삭제합니다.
	
	c. 엔드포인트를 일반 모드에서 다시 시작합니다.

지원되지 않는 압축 포맷으로 압축된 파일	솔루션: 파일의 압축을 풉니다.
잠긴 파일 또는 현재 실행 중인 파일	솔루션: 파일 잠금을 해제하거나 파일 실행이 완료될 때까지 기다립니다.
손상된 파일	솔루션: 파일을 삭제합니다.

트로이 목마에 감염된 파일

트로이 목마는 메시지를 표시하거나, 파일을 지우거나, 디스크를 포맷하는 등 대체로 유해한 동작을 의도하지 않게 무단으로 수행하는 프로그램입니다. 트로이 목마는 파일을 감염시키지 않으므로 치료할 필요가 없습니다.

솔루션: OfficeScan에서는 Damage Cleanup 엔진 및 Damage Cleanup 템플릿을 사용하여 트로이 목마를 제거합니다.

웜에 감염된 파일

웜은 자체 복사본이나 일부를 다른 엔드포인트 시스템으로 전파할 수 있는 독립형 프로그램(또는 프로그램 집합)입니다. 웜은 일반적으로 네트워크 연결이나 전자 메일 첨부 파일을 통해 전파됩니다. 웜은 독립형 프로그램이기 때문에 치료가 불가능합니다.

솔루션: Trend Micro에서는 웜을 삭제할 것을 권장합니다.

쓰기 방지 감염된 파일

솔루션: OfficeScan이 파일을 치료할 수 있도록 쓰기 보호를 제거합니다.

암호로 보호된 파일

암호로 보호된 압축 파일 또는 암호로 보호된 Microsoft Office 파일이 포함됩니다.

솔루션: OfficeScan이 이러한 파일을 치료할 수 있도록 암호 보호를 제거합니다.

백업 파일

확장자가 RB0~RB9인 파일은 감염된 파일의 백업 복사본입니다. OfficeScan은 치료 과정 중에 바이러스/악성 프로그램에 의해 파일이 손상되는 경우를 대비하여 감염된 파일의 백업본을 만듭니다.

솔루션: OfficeScan에서 감염된 파일을 성공적으로 치료한 경우에는 백업 복사본을 보관할 필요가 없습니다. 엔드포인트가 정상적으로 작동하는 경우 백업 파일을 삭제해도 됩니다.

색인

A

ActiveAction, 7-37
Active Directory, 2-40–2-43, 2-57, 2-62, 5-14, 5-31
  구조 복제, 2-62
  동기화, 2-42, 2-43
  범위 및 쿼리, 15-69
  사용자 정의 에이전트 그룹, 2-41
  에이전트 그룹화, 2-57
  외부 서버 관리, 2-41
  자격 증명, 2-42
  통합, 2-40
ActiveSync, 11-37
ActiveX 악성 코드, 7-4
agent mover, 15-22
AutoPcc.exe, 5-12, 5-13, 5-23, 5-24

C

C&C(명령 및 제어) 연결 알림 서비스, 12-2
  Virtual Analyzer, 12-3
  Virtual Analyzer 목록, 12-3
  글로벌 정보 목록, 12-3
  스마트 보호 서버, 12-3
C&C 콜백
  글로벌 설정
    사용자 정의 IP 목록, 8-6
  위젯, 2-26
Case Diagnostic Tool, 18-2
COM 감염자, 7-4
Conflicted ARP, 13-4
Control Manager
  MCP Agent 로그, 18-11
  OfficeScan과 통합, 14-24
CPU 사용량, 7-29

D

Damage Cleanup 템플릿, 6-7
DCE(Damage Cleanup Engine), 6-7
DCS(Damage Cleanup Services), 1-6, 5-4, 5-6
DHCP 설정, 5-46
DSP, 10-8

E

Early Boot Cleanup 드라이버, 6-7
EICAR 테스트 스크립트, 5-69, 7-3
EXE 파일 감염자, 7-4

F

FakeAV, 7-42
Fragmented IGMP, 13-5
FTP, 11-26

H

HTML 바이러스, 7-4
HTTP 및 HTTPS, 11-27

I

IDS, 13-4
IM 응용 프로그램, 11-27
IntelliScan, 7-27
IntelliTrap 예외 패턴, 6-4
IntelliTrap 패턴, 6-4
IPv6, 4-21
  지원, 4-21
IPv6 지원, A-2
  IPv6 주소 표시, A-6
  제한 사항, A-3, A-4
IpXfer.exe, 15-22

J

JavaScript 바이러스, 7-4

Java 악성 코드, 7-4

L

LAND Attack, 13-5
LogServer.exe, 18-3, 18-14

M

MAC 주소, 15-3
Microsoft Exchange Server 검색, 7-72
Microsoft SMS, 5-14, 5-32
MSI 패키지, 5-14, 5-31, 5-32

N

NetBIOS, 2-57
Network VirusWall Enforcer, 4-29

O

OfficeScan
  web server, 14-52
  구성 요소, 2-35, 6-2
  구성 요소 업데이트, 5-69
  데이터베이스 검색, 7-72
  데이터베이스 백업, 14-45
  라이선스, 14-42
  로그, 14-39
  설명서, xii
  에이전트, 1-9
  에이전트 서비스, 15-11
  웹 콘솔, 2-2
  정보, 1-2
  주요 기능 및 장점, 1-5
  프로그램, 2-35
OfficeScan 서버, 1-7
  기능, 1-7
OfficeScan 업데이트, 6-12
OfficeScan 에이전트
  OfficeScan 서버와 연결, 15-26, 15-38
  레지스트리 키, 15-15
  비활성 에이전트, 15-25
  설정 가져오기 및 내보내기, 15-53
  설치 방법, 5-11
  스마트 보호 서버 연결, 15-39
  예약된 디스크 공간, 6-46
  자세한 에이전트 정보, 15-52
  제거, 5-70
  파일, 15-14
  프로세스, 15-16
Overlapping Fragment, 13-5

P

PCRE, 11-6
Perle Compatible Regular Expressions(Perle 호환 정규 표현식), 11-6
Ping of Death, 13-4
Plug-in Manager, 1-5, 5-5, 5-8, 17-2
  기본 OfficeScan 제품 기능 관리, 17-4
  문제 해결, 17-12
  설치, 17-3
  제거, 17-12
Plug-in 프로그램
  설치, 17-5
  정품 인증, 3-4, 17-6
  제거, 17-11
ptngrowth.ini, 4-16, 4-17

S

ServerProtect, 5-64
Smart Feedback, 4-3
SMB 프로토콜, 11-27
SQL Server 마이그레이션 도구, 14-47, 14-51
  경고 알림, 14-50
  구성, 14-48
SYN Flood, 13-5

T

Teardrop, 13-5

Tiny Fragment Attack, 13-5
TMPerftool, 18-2
TMTouch.exe, 6-50
Too Big Fragment, 13-4

U

URL 필터링 엔진, 6-11
USB 장치
    승인된 목록, 10-13
        구성, 10-13

V

VBScript 바이러스, 7-4
VDI, 15-73
    로그, 18-13
VDI 설치 전 검색 템플릿 생성 도구, 15-83
Vulnerability Scanner, 5-15, 5-38
    DHCP 설정, 5-46
    Ping 설정, 5-58
    엔드포인트 설명 검색, 5-56
    제품 쿼리, 5-52
    지원 프로토콜, 5-54
    효율성, 5-38

W

Web server 정보, 14-52
Windows Server Core, B-2
    명령, B-7
    사용 가능한 에이전트 기능, B-6
    지원되는 설치 방법, B-2
Windows 클립보드, 11-37

ㄱ

가능성이 있는 바이러스/악성 프로그램, 7-5, 7-91
가상 데스크톱 지원, 15-73
검색 권한, 7-53
검색 기준
    CPU 사용량, 7-29
    검색할 파일, 7-27
    예약, 7-30
    파일 압축, 7-28
    파일에 대한 사용자 작업, 7-26
검색 방법, 5-27
    기본, 7-9
검색 유형, 5-3, 5-6, 7-14
검색을 위한 캐시 설정, 7-64
검색 제외, 7-31
    디렉터리, 7-32
    파일, 7-34
    파일 확장자, 7-34
검색 제외 목록, 9-9
    동작 모니터링, 9-9
검색 조치, 7-35
    바이러스/악성 프로그램, 7-73
    스파이웨어/그레이웨어, 7-47
검색 캐시, 7-64
게이트웨이 IP 주소, 15-3
게이트웨이 설정 가져오기, 15-5
격리 보관 관리자, 14-59
격리 보관 디렉터리, 7-39, 7-44
고급 권한
    구성, 10-12
    저장 장치, 10-6, 10-7
고급 위협 검색 엔진, 6-5
고급 위협 상관 관계 패턴, 6-5
관련 규칙 패턴, 6-9
구성 요소, 2-35, 5-69, 6-2
    OfficeScan 서버에서, 6-14
    업데이트 권한 및 설정, 6-43
    업데이트 에이전트에서, 6-51
    업데이트 요약, 6-60
    에이전트에서, 6-26

구성 요소 복제, 6-19, 6-57
권한
    검색 권한, 7-54
    고급, 10-12
    독립 모드 권한, 15-19
    메일 검색 권한, 7-62
    방화벽 권한, 13-22, 13-24
    비저장 장치, 10-10
    예약 검색 권한, 7-57
    저장 장치, 10-4
    종료 권한, 15-18
    프로그램 경로 및 이름, 10-9
    프록시 구성 권한, 15-50
글로벌 C&C IP 목록, 6-9
기준
    사용자 정의 식, 11-7, 11-8
    키워드, 11-15, 11-16

ㄴ
네트워크로 연결된 엔드포인트에 대한 상위 10개 보안 위험 통계, 2-34
네트워크 바이러스, 7-4, 13-3
네트워크 채널, 11-23, 11-24, 11-26–11-28, 11-30, 11-31, 11-40
    FTP, 11-26
    HTTP 및 HTTPS, 11-27
    IM 응용 프로그램, 11-27
    SMB 프로토콜, 11-27
    모니터링되는 대상, 11-31, 11-40
    모니터링되지 않는 대상, 11-31, 11-40
    웹 메일, 11-28
    전송 범위, 11-31
        모든 전송, 11-28
        외부 전송, 11-30
        충돌, 11-31
    전송 범위 및 대상, 11-28
    전자 메일 클라이언트, 11-24
논리 연산자, 11-20

ㄷ
대시보드, 2-5
    사용자 계정, 2-5
    요약, 2-6, 2-7
데이터베이스 검색, 7-72
데이터베이스 백업, 14-45
데이터 보호, 11-2
    라이선스, 3-4
    배포, 3-6
    상태, 3-7
    설치, 3-2
    제거, 3-14
데이터 손실 방지, 11-2, 11-3, 11-5
    네트워크 채널, 11-24, 11-26–11-28, 11-30, 11-31, 11-40
    데이터 식별자, 11-5
    시스템 및 응용 프로그램 채널, 11-31, 11-32, 11-35–11-37
    식, 11-5–11-9
    압축 해제 규칙, 11-41
    위젯, 2-23, 2-24
    정책, 11-3, 11-45
    조치, 11-38
    채널, 11-23
    키워드, 11-13–11-16, 11-18
    템플릿, 11-19–11-21, 11-23
    파일 특성, 11-10–11-12
데이터 식별자, 11-5
    식, 11-5
    키워드, 11-5
    파일 특성, 11-5
도메인, 2-57, 2-64, 2-65
    삭제, 2-64
    에이전트 그룹화, 2-57
    추가, 2-64

파일명 변경, 2-65
독립 서버, 4-6
독립 스마트 보호 서버, 4-16
ptngrowth.ini, 4-16
독립 에이전트, 5-5, 5-8
동작 모니터링, 9-17
검색 제외 목록, 9-9
로그, 9-17
시스템 이벤트에 대한 조치, 9-8
동작 모니터링 구성 패턴, 6-8
동작 모니터링 드라이버, 6-7
동작 모니터링 탐지 패턴, 6-7
동작 모니터링 핵심 서비스, 6-8
디버그 로그
서버, 18-2
에이전트, 18-14
디지털 서명 공급자, 10-8
지정, 10-8
디지털 서명 캐시, 7-64

ㄹ

라이선스, 14-42
데이터 보호, 3-4
상태, 2-6
로그, 14-39
검색 로그, 7-102
동작 모니터링, 9-17
바이러스/악성 프로그램 로그, 7-70, 7-89
방화벽 로그, 13-23, 13-24, 13-28
보안 위험 로그, 7-88
스파이웨어/그레이웨어 로그, 7-96
스파이웨어/그레이웨어 복원 로그, 7-100
시스템 이벤트 로그, 14-37
알 수 없는 위협, 8-10
에이전트 업데이트 로그, 6-48
연결 확인 로그, 15-42
웹 검증 로그, 12-20
의심스러운 파일 로그, 7-100
장치 제어 로그, 10-18
정보, 14-39
중앙 격리 보관 복원 로그, 7-96
로그인 스크립트 설정, 5-12, 5-13, 5-23, 5-24
루트키트, 7-3
루트키트 탐지, 6-8

ㅁ

마이그레이션
ServerProtect 일반 서버에서, 5-64
타사 보안 소프트웨어에서, 5-63
매크로 바이러스, 7-4
메모리 검색 트리거 패턴, 6-8
메일 검색, 7-62
모니터링되는 대상, 11-29, 11-31
모니터링되는 시스템 이벤트, 9-6
모니터링되는 시스템 이벤트에 대한 조치, 9-8
모니터링되는 전자 메일 하위 도메인, 11-25
모니터링되지 않는 대상, 11-29, 11-30
모니터링되지 않는 전자 메일 도메인, 11-25
문서 피드백, 19-6
문제 해결
Plug-in Manager, 17-12
문제 해결 리소스, 18-1
미리 정의된 식, 11-5
보기, 11-6
미리 정의된 키워드
거리, 11-14
키워드 수, 11-14
미리 정의된 템플릿, 11-19

ㅂ

바이러스/악성 프로그램, 7-2–7-5
ActiveX 악성 코드, 7-4
COM 및 EXE 파일 감염자, 7-4
Java 악성 코드, 7-4
VBScript, JavaScript 또는 HTML 바이러스, 7-4
가능성이 있는 바이러스/악성 프로그램, 7-5
루트키트, 7-3
매크로 바이러스, 7-4
부트 섹터 바이러스, 7-4
웜, 7-4
유형, 7-2–7-5
조크 프로그램, 7-2
테스트 바이러스, 7-3
트로이 목마 프로그램, 7-3
패커, 7-2
바이러스/악성 프로그램 검색
결과, 7-90
글로벌 설정, 7-69
바이러스 검색 드라이버, 6-3
바이러스 검색 엔진, 6-3
바이러스 백과사전, 7-5
바이러스 사전 방역, 2-33
사용 안 함, 7-115
정책, 7-108
바이러스 사전 방역 정책
Mutex 처리, 7-112
공유 폴더에 대한 액세스 제한/거부, 7-109
상호 배제, 7-112
쓰기 액세스 금지, 7-111
압축된 실행 파일, 7-114
압축 파일 액세스 거부, 7-114
포트 차단, 7-110
바이러스 패턴, 6-3, 6-48, 6-49
방화벽, 5-4, 5-6, 13-2
권한, 13-6, 13-22
기본 정책 예외, 13-13, 13-14
바이러스 비상 발생 모니터링, 13-5
사용 안 함, 13-6
작업, 13-8
장점, 13-2
정책, 13-8
정책 예외, 13-13
테스트, 13-31
프로필, 13-3, 13-16
방화벽 드라이버, 6-7, 18-19, 18-20
방화벽 로그 수, 13-25
방화벽 패턴, 6-7
보안 위험, 7-2, 7-5–7-7
보호, 1-6
스파이웨어/그레이웨어, 7-5–7-7
피싱 공격, E-9
보안 준수, 15-55
검색, 15-60
구성 요소, 15-58
로그, 18-8
서비스, 15-56
설정, 15-62
설치, 5-61
업데이트 적용, 6-49
예약 평가, 15-67
외부 서버 관리, 2-41, 15-68
적용, 15-68
보안 패치, 6-10
보호 지속성, 4-10
부트 섹터 바이러스, 7-4
브라우저 위협 방지 패턴, 6-9
비상 발생 기준, 7-103, 12-18, 13-29
비저장 장치

권한, 10-10
비활성 에이전트, 15-25

ㅅ

사용자 계정, 2-5
대시보드, 2-5
사용자 역할
Trend 고급 사용자, 14-10
게스트 사용자, 14-9
관리자, 14-9
사용자 정의 식, 11-6–11-9
가져오기, 11-9
기준, 11-7, 11-8
사용자 정의 에이전트 그룹, 2-41, 2-58
사용자 정의 키워드, 11-15
가져오기, 11-18
기준, 11-15, 11-16
사용자 정의 템플릿, 11-20
가져오기, 11-23
만들기, 11-21
상황별 정보 엔진, 6-5
상황별 정보 쿼리 처리기, 6-5
상황별 정보 패턴, 6-5
서버 로그
Active Directory 로그, 18-5
Control Manager MCP Agent 로그, 18-11
ServerProtect 마이그레이션 도구 디버그 로그, 18-10
VSEncrypt 디버그 로그, 18-10
가상 데스크톱 지원 로그, 18-13
구성 요소 업데이트 로그, 18-7
디버그 로그, 18-3
로컬 설치/업그레이드 로그, 18-5
바이러스 검색 엔진 디버그 로그, 18-18
보안 준수 로그, 18-8
에이전트 그룹화 로그, 18-6
에이전트 패키지 도구 로그, 18-8
역할 기반 관리 로그, 18-6
외부 서버 관리 로그, 18-9
원격 설치/업그레이드 로그, 18-5
웹 검증 로그, 18-10
장치 제어 로그, 18-9
서버 업데이트
구성 요소 복제, 6-19
로그, 6-25
수동 업데이트, 6-24
업데이트 방법, 6-24
예약 업데이트, 6-25
프록시 설정, 6-18
서버 튜너, 14-60
서비스 다시 시작, 15-11
설명서, xii
설정 가져오기, 15-53
설정 내보내기, 15-53
설치, 5-2
Plug-in Manager, 17-3
Plug-in 프로그램, 17-5
데이터 보호, 3-2
보안 준수, 5-61
에이전트, 5-2
설치 전 작업, 5-17, 5-20, 5-61
성능 제어, 7-29
성능 조정 도구, 18-2
손상 복구 패턴, 6-8
수동 검색, 7-18
바로 가기, 7-71
수동 에이전트 그룹화, 2-57, 2-58
스마트 검색 패턴, 6-8, 7-64
스마트 보호, 4-3, 4-4, 4-6–4-9, 4-12, 4-21, 4-22
방대한 양의 위협, 4-3
소스, 4-7, 4-21, 4-22

IPv6 지원, 4-21
비교, 4-7
위치, 4-22
프로토콜, 4-7
스마트 보호 네트워크, 4-6
스마트 보호 서버, 4-6
웹 검증 서비스, 4-3, 4-4
파일 검증 서비스, 4-3
패턴 파일, 4-7–4-9
스마트 스캔 에이전트 패턴, 4-8
스마트 스캔 패턴, 4-8
업데이트 프로세스, 4-9
웹 차단 목록, 4-8
환경, 4-12
스마트 보호 네트워크, 1-2, 4-6
스마트 보호 서버, 4-6, 4-13, 4-16, 4-17, 4-19
독립, 4-6, 4-16
설치, 4-13
업데이트, 6-13, 6-26
최선의 방법, 4-16
통합, 4-6, 4-17, 4-19
스마트 스캔, 7-9–7-11
표준 스캔에서 전환, 7-11
스마트 스캔 에이전트 패턴, 4-8
스마트 스캔 패턴, 4-8
스크립트 분석자 통합 패턴, 6-9
스파이웨어/그레이웨어, 7-5–7-7
보호, 7-7
복원, 7-50
스파이웨어, 7-5
암호 해독 응용 프로그램, 7-6
애드웨어, 7-5
원격 액세스 도구, 7-6
잠재적 위협, 7-6
전화 걸기 프로그램, 7-6
조크 프로그램, 7-6
해킹 도구, 7-6
스파이웨어/그레이웨어 검색
결과, 7-98
승인된 목록, 7-48
조치, 7-47
스파이웨어/그레이웨어 검색 엔진, 6-6
스파이웨어/그레이웨어 패턴, 6-6
스파이웨어 활성 모니터링 패턴, 6-6
승인된 목록, 7-48
승인된 프로그램 목록, 9-9
시스템 및 응용 프로그램 채널, 11-23, 11-31, 11-32, 11-35–11-37
CD/DVD, 11-32
P2P(피어 투 피어), 11-35
PGP 암호화, 11-35
Windows 클립보드, 11-37
동기화 소프트웨어, 11-37
이동식 저장소, 11-36
클라우드 저장소 서비스, 11-32
프린터, 11-35
시스템 요구 사항
업데이트 에이전트, 6-52
식, 11-5
미리 정의됨, 11-5, 11-6
사용자 정의, 11-6, 11-9
기준, 11-7, 11-8
실시간 검색, 7-15
실시간 검색 서비스, 15-38

O

악성 프로그램 동작 차단, 9-2
알림
C&C 콜백 탐지, 12-17
관리자용, 11-51, 14-35
바이러스/악성 프로그램 발견, 7-42
방화벽 위반, 13-26
비상 발생, 7-103, 12-18, 13-29

스파이웨어/그레이웨어 발견, 7-48
에이전트 사용자용, 7-85, 11-55
에이전트 업데이트, 6-47
엔드포인트 다시 시작, 6-48
오래된 바이러스 패턴, 6-48
웹 위협 탐지, 12-13
장치 제어, 10-18
알 수 없는 위협, 8-10
로그, 8-10
암호, 14-58
암호화된 파일, 7-44
압축 파일, 7-28, 7-73
압축 해제 규칙, 11-41
압축 해제 규칙, 11-41
업데이트, 4-17, 4-19
OfficeScan 서버, 6-14
스마트 보호 서버, 6-13, 6-26
업데이트 에이전트, 6-51
에이전트, 6-26
적용, 6-49
통합 스마트 보호 서버, 4-17, 4-19
업데이트 방법
OfficeScan 서버, 6-24
업데이트 에이전트, 6-58
에이전트, 6-35
업데이트 소스
OfficeScan 서버, 6-17
업데이트 에이전트, 6-53
에이전트, 6-29
업데이트 에이전트, 5-3, 5-6, 6-51
구성 요소 복제, 6-57
분석 보고서, 6-59
시스템 요구 사항, 6-52
업데이트 방법, 6-58
표준 업데이트 소스, 6-54
할당, 6-52
에이전트, 2-57, 2-64, 2-66, 4-29, 5-2
그룹화, 2-57
기능, 5-3
삭제, 2-64
설치, 5-2
연결, 4-29
위치, 4-29
이동, 2-66
프록시 설정, 4-29
에이전트 그룹화, 2-57–2-59, 2-61–2-66
Active Directory, 2-57, 2-61
DNS, 2-57
IP 주소, 2-62
NetBIOS, 2-57
도메인 또는 에이전트 삭제, 2-64
도메인 이름 변경, 2-65
도메인 추가, 2-64
방법, 2-57
사용자 지정 그룹, 2-58
수동, 2-57, 2-58
에이전트 이동, 2-66
자동, 2-58, 2-59
작업, 2-63
에이전트 디스크 이미지, 5-14, 5-37
에이전트 로그
Damage Cleanup Services 로그, 18-16
OfficeScan 방화벽 디버그 로그, 18-19
TDI 디버그 로그, 18-25
데이터 보호 디버그 로그, 11-61, 18-24
동작 모니터링 디버그 로그, 18-19
디버그 로그, 18-14
메일 검색 로그, 18-16
바이러스 사전 방역 디버그 로그, 18-18
새 설치 로그, 18-15
업그레이드/핫픽스 로그, 18-16

에이전트 업데이트 로그, 18-17
에이전트 연결 로그, 18-17
에이전트 설치, 5-2, 5-23
Vulnerability Scanner 사용, 5-38
로그인 스크립트 설정, 5-23
보안 준수 사용, 5-61
브라우저 기반, 5-18
사후 설치, 5-67
시스템 요구 사항, 5-2
에이전트 디스크 이미지 사용, 5-37
에이전트 패키지 도구, 5-26
웹 설치 페이지에서, 5-16
웹 콘솔에서, 5-20
에이전트 업그레이드
사용 안 함, 6-44
에이전트 업데이트
NAT를 사용하여 예약 업데이트, 6-40
권한, 6-43
사용자 정의 소스, 6-31
수동, 6-42
액티브업데이트 서버에서, 6-44
예약 업데이트, 6-37
이벤트에 따른, 6-36
자동, 6-36
표준 소스, 6-29
에이전트 자기 보호, 15-12
에이전트 제거, 5-70
에이전트 콘솔
액세스 제한, 15-17
에이전트 트리, 2-44, 2-46–2-49, 2-53–2-55
고급 검색, 2-47, 2-48
보기, 2-47
일반 작업, 2-46
정보, 2-44
특정 작업, 2-49, 2-53–2-55
구성 요소 업데이트 롤백, 2-54
바이러스 사전 방역, 2-53
보안 위험 로그, 2-55
수동 구성 요소 업데이트, 2-53
에이전트 관리, 2-49
필터, 2-47
에이전트 패키지 도구, 5-13, 5-26, 5-29, 5-31, 5-33
배포, 5-26
설정, 5-28
역할 기반 관리, 14-3
사용자 계정, 14-13
사용자 역할, 14-3
연결할 수 없는 에이전트, 15-42
연결 확인, 15-41
예약 검색, 7-20
건너뛰기 및 중지, 7-57, 7-78
다시 시작, 7-78
미리 알림, 7-77
연기, 7-77
자동으로 중지, 7-77
예약 평가, 15-67
와일드카드, 11-11
장치 제어, 10-10
파일 특성, 11-11
외부 서버 관리, 2-41, 15-68
로그, 18-9
예약 쿼리, 15-72
쿼리 결과, 15-71
외부 장치
액세스 관리, 10-11, 10-15
외부 장치 보호, 6-8
요약
대시보드, 2-6, 2-7
업데이트, 6-60
요약 대시보드, 2-6, 2-7

구성 요소 및 프로그램, 2-35
위젯, 2-7
제품 라이선스 상태, 2-6
탭, 2-7
용어, xiv
원격 설치, 5-13
웜, 7-4
웹 검증, 1-6, 5-3, 5-6, 12-4
로그, 18-10
정책, 12-5
웹 검증 서비스, 4-3, 4-4
웹 메일, 11-28
웹 설치 페이지, 5-11, 5-16
웹 위협, 12-2
웹 차단 목록, 4-8, 4-19
웹 콘솔, 1-5, 2-2–2-4
URL, 2-3
로그온 계정, 2-4
배너, 2-4
암호, 2-4
요구 사항, 2-2
정보, 2-2
위젯, 2-7, 2-20–2-24, 2-26, 2-28–2-30, 2-32, 2-33, 2-35, 2-36, 17-3
C&C 콜백 이벤트, 2-26
Edge 릴레이 서버에 연결된 에이전트, 2-32
OfficeScan 및 플러그인 Mashup, 2-29
데이터 손실 방지 - 기간별 탐지, 2-23
데이터 손실 방지 - 상위 탐지, 2-24
바이러스 백신 에이전트 연결, 2-30
보안 위험 탐지, 2-28
비상 발생, 2-33
에이전트-서버 연결, 2-36
에이전트 업데이트, 2-35
웹 검증 상위 위협 대상 사용자, 2-21
웹 검증 상위 위협 소스, 2-22
파일 검증 위협 맵, 2-20
위치, 4-29
인식, 4-29
위치 인식, 15-2
응용 프로그램 필터링, 13-3
이벤트 모니터링, 9-6
인증된 안전한 소프트웨어 목록, 13-3
인증된 안전한 소프트웨어 서비스, 7-70, 9-13, 13-25
인크리멘탈 패턴, 6-19
인트라넷, 4-12

ㅈ

자동 에이전트 그룹화, 2-58, 2-59
장치 목록 도구, 10-14
장치 제어, 1-7, 10-2, 10-4, 10-6–10-13, 10-15
USB 장치, 10-13
고급 권한, 10-12
구성, 10-12
권한, 10-4, 10-6, 10-7, 10-9, 10-10
프로그램 경로 및 이름, 10-9
디지털 서명 공급자, 10-8
로그, 10-18, 18-9
비저장 장치, 10-10
승인된 목록, 10-13
알림, 10-18
액세스 관리, 10-11, 10-15
와일드카드, 10-10
외부 장치, 10-11, 10-15
요구 사항, 10-2
저장 장치, 10-4, 10-6, 10-7
장치 제어;장치 제어 목록;장치 제어 목록:프로그램 추가, 10-16
저장 장치
고급 권한, 10-6, 10-7

권한, 10-4
전자 메일 도메인, 11-25
점검 모드, 7-75
정책, 11-3
데이터 손실 방지, 11-45
방화벽, 13-3, 13-8
웹 검증, 12-5
정책 적용 패턴, 6-8
제거, 5-70
Plug-in Manager, 17-12
Plug-in 프로그램, 17-11
데이터 보호, 3-14
웹 콘솔에서, 5-71
제거 프로그램 사용, 5-71
조건문, 11-20
조치
데이터 손실 방지, 11-38
조크 프로그램, 7-2
주문형 검색 캐시, 7-65
준수 보고서, 15-55
지금 검색, 7-22
지금 업데이트, 6-45
지원
신속한 문제 해결, 19-4
지원 정보 시스템, 2-5, 18-2

ㅊ

차단된 프로그램 목록, 9-9
참조 서버, 14-33
최종 사용자 사용권 계약(EULA), E-4
추가 서비스 설정, 15-6, 15-7
침입 탐지 시스템(IDS), 13-4

ㅋ

쿠키 검색, 7-76
키워드, 11-5, 11-13
미리 정의됨, 11-13, 11-14
사용자 정의, 11-15, 11-16, 11-18

ㅌ

타사 보안 소프트웨어, 5-62
탭, 2-7
터치 도구, 6-50
테스트 검색, 5-69
테스트 바이러스, 7-3
템플릿, 11-19–11-21, 11-23
논리 연산자, 11-20
미리 정의됨, 11-19
사용자 정의, 11-20, 11-21, 11-23
조건문, 11-20
통합 서버, 4-6
통합 스마트 보호 서버, 4-17
ptngrowth.ini, 4-17
업데이트, 4-17, 4-19
구성 요소, 4-19
웹 차단 목록, 4-19
트로이 목마 프로그램, 1-6, 6-7, 7-3

ㅍ

파일 검증, 4-3
파일 검증 서비스, 4-3
파일 특성, 11-5, 11-10–11-12
가져오기, 11-12
만들기, 11-11
미리 정의됨, 11-11
와일드카드, 11-11
패치, 6-10
패커, 7-2
패턴 파일
스마트 보호, 4-7
스마트 스캔 에이전트 패턴, 4-8
스마트 스캔 패턴, 4-8
웹 차단 목록, 4-8
평가판, 14-42

포트 차단, 7-110
표준 스캔, 7-9–7-11
    스마트 스캔으로 전환, 7-11
프로그램, 2-35, 6-2
프로그램 검사 모니터링 패턴, 6-8
프록시 설정, 4-29
    권한, 15-50
    내부 연결용, 15-47
    서버 구성 요소 업데이트용, 6-18
    에이전트, 4-29
    외부 연결용, 15-48
    자동 프록시 설정, 15-51
피싱, E-9

ㅎ

핫픽스, 6-10, 6-50

TREND MICRO INCORPORATED
대한민국 서울시 강남구 대치동 945-1 홍우빌딩 6층
전화:+82-2-561-0990 팩스:+82-2-561-0660 support@trendmicro.co.kr
www.trendmicro.com
Item Code: OSKMXG7603/161028