TREND MICRO

XG

OfficeScan™

설치 및 업그레이드 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: OSKMXG7613/161028

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 vii

OfficeScan 설명서 viii

대상 viii

문서 규칙 ix

용어 x

장 1 : OfficeScan 설치 및 업그레이드 계획

새로 설치 및 업그레이드 요구 사항 1-2

제품 버전 1-2

등록 키 및 정품 인증 코드 1-3

새로 설치 고려 사항 1-4

- IPv6 지원 1-4
- OfficeScan 서버의 위치 1-5
- 원격 설치 1-6
- 서버 성능 1-6
- 전용 서버 1-7
- 설치 도중 검색 방법 개발 1-7
- 네트워크 트래픽 1-8
- 타사 보안 소프트웨어 1-10
- Active Directory 1-10
- IIS Web Server 1-10

업그레이드 고려 사항 1-11

- IPv6 지원 1-11
- 지원되지 않는 운영 체제 1-12
- OfficeScan 설정 및 구성 1-13
- 업그레이드 도중 검색 방법 개발 1-14

설치 및 업그레이드 체크리스트 1-15

파일럿 배포 계획 1-21
파일럿 사이트 선택 1-22
롤백 계획 수립 1-22
파일럿 배포 평가 1-22
알려진 호환성 문제 1-22
Microsoft 잠금 도구 및 URLScan 1-22
Microsoft Exchange Server 1-23
데이터베이스 서버 1-23

장 2 : OfficeScan 설치

OfficeScan 서버 새로 설치 수행 2-2
자동 설치 2-2
자동 설치 준비 2-2
응답 파일에 설치 구성 기록 2-3
자동 설치 실행 2-3
설치 프로그램 설치 화면 2-4
사용권 계약 2-7
설치 대상 2-8
엔드포인트 설치 전 검색 2-10
설치 경로 2-12
프록시 서버 2-13
Web Server 2-14
서버 식별 2-17
등록 및 정품 인증 2-19
OfficeScan 에이전트 배포 2-21
통합 스마트 보호 서버 설치 2-22
설치 대상 2-26
대상 엔드포인트 분석 2-28
OfficeScan 에이전트 설치 2-30
스마트 보호 네트워크 2-32
관리자 계정 암호 2-34
OfficeScan 에이전트 설치 2-35
OfficeScan 방화벽 2-37
Anti-spyware 기능 2-39
웹 검증 기능 2-40
서버 인증 인증서 2-41

OfficeScan 프로그램 바로 가기 2-44
설치 정보 2-45
InstallShield 마법사 완료 2-46

장 3 : OfficeScan 업그레이드

OfficeScan 서버 및 에이전트 업그레이드 3-2
OfficeScan 서버 및 에이전트를 업그레이드하기 전 3-2

로컬 업그레이드 수행 3-19
Apache가 포함된 OfficeScan 10.6 SP3에서 업그레이드 3-20
IIS가 포함된 OfficeScan 10.6 SP3에서 업그레이드 3-37
OfficeScan 11.x에서 업그레이드 3-49

원격 업그레이드 수행 3-60
사용권 계약 3-61
설치 대상 3-62
엔드포인트 설치 전 검색 3-64
설치 경로 3-66
프록시 서버 3-67
Web Server 3-68
서버 식별 3-71
등록 및 정품 인증 3-73
OfficeScan 에이전트 배포 3-75
통합 스마트 보호 서버 설치 3-76
설치 대상 3-80
대상 엔드포인트 분석 3-82
OfficeScan 에이전트 다시 시작 경고 3-84
데이터베이스 백업 3-84
서버 인증 인증서 3-85
설치 정보 3-88
InstallShield 마법사 완료 3-89

장 4 : 사후 설치 작업

서버 설치 또는 업그레이드 확인 4-2
통합 스마트 보호 서버 설치 확인 4-4

OfficeScan 구성 요소 업데이트 4-4
OfficeScan 서버 업데이트 4-4

기본 설정 확인 4-5
검색 설정 4-5
에이전트 설정 4-5
에이전트 권한 4-5
OfficeScan을 Control Manager에 등록 4-6

장 5 : OfficeScan 제거 및 롤백

제거 및 롤백 고려 사항 5-2
OfficeScan 서버를 제거하기 전에 5-2
다른 OfficeScan 서버로 에이전트 이동 5-2
OfficeScan 데이터베이스와 구성 파일 백업 및 복원 5-3
OfficeScan 서버 제거 5-4
제거 프로그램을 사용하여 OfficeScan 서버 제거 5-5
수동으로 OfficeScan 서버 제거 5-6
서버 백업 패키지를 사용하여 OfficeScan 서버 및 OfficeScan 에이전트 롤백 5-8
OfficeScan 에이전트 롤백 5-9
이전 OfficeScan 서버 버전 복원 5-10
이전 OfficeScan 버전으로 수동 롤백 5-14
파트 1: 이전 OfficeScan 서버 버전 준비 5-15
파트 2: 롤백할 에이전트의 업데이트 소스 준비 5-17
파트 3: OfficeScan 에이전트 롤백 5-20

장 6 : OfficeScan 문제 해결 리소스

지원 정보 시스템 6-2
Case Diagnostic Tool 6-2
Trend Micro 성능 조정 도구 6-2
시스템 집약적인 응용 프로그램 식별 6-2
설치 로그 6-4
서버 디버그 로그 6-5
OfficeScan 서버 컴퓨터에서 디버그 로깅 사용 6-5
에이전트 디버그 로그 6-7
OfficeScan 에이전트에서 디버그 로깅 사용 6-7

장 7 : 기술 지원

문제 해결 리소스 7-2
지원 포털 사용 7-2
위협 백과사전 7-2

Trend Micro 연락처 7-3
신속한 기술 지원을 받는 방법 7-4

의심스러운 콘텐츠를 Trend Micro로 보내기 7-4
전자 메일 검증 서비스 7-4
파일 검증 서비스 7-5
웹 검증 서비스 7-5

기타 리소스 7-5
다운로드 센터 7-5
문서 피드백 7-6

부록 A : 샘플 배포

기본 네트워크 A-2

다중 사이트 네트워크 A-3
다중 사이트 네트워크 준비 A-4
본사 배포 A-5
원격 사이트 1 배포 A-5
원격 사이트 2 배포 A-6

색인

색인 IN-1

서문

서문

Trend Micro™ OfficeScan™ *설치 및 업그레이드 안내서*입니다. 이 문서에서는 OfficeScan 서버를 설치하고 서버 및 에이전트를 업그레이드하는 데 필요한 사항과 절차를 설명합니다.

이 장의 내용:

- OfficeScan 설명서 페이지 viii
- 대상 페이지 viii
- 문서 규칙 페이지 ix
- 용어 페이지 x

참고

에이전트 설치에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

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

장 1

OfficeScan 설치 및 업그레이드 계획

이 장에서는 Trend Micro™ OfficeScan™ 설치 및 업그레이드를 위한 준비 및 설치 전 정보에 대해 설명합니다.

이 장의 내용:

- 새로 설치 및 업그레이드 요구 사항 페이지 1-2
- 제품 버전 페이지 1-2
- 등록 키 및 정품 인증 코드 페이지 1-3
- 새로 설치 고려 사항 페이지 1-4
- 업그레이드 고려 사항 페이지 1-11
- 설치 및 업그레이드 체크리스트 페이지 1-15
- 파일럿 배포 계획 페이지 1-21
- 알려진 호환성 문제 페이지 1-22

새로 설치 및 업그레이드 요구 사항

지원되는 Windows Server 플랫폼에서 OfficeScan 서버 및 에이전트에 대한 새로 설치를 수행합니다.

또한 이 OfficeScan 버전에서는 다음 버전에서의 업그레이드를 지원합니다.

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3

참고

Trend Micro에서는 업그레이드를 수행하기 전에 현재 OfficeScan 서버에 사용 가능한 모든 패치 및 핫픽스를 적용할 것을 권장합니다.

새로 설치 요구 사항의 전체 목록은 다음 웹 사이트

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

제품 버전

OfficeScan의 정식 버전 또는 평가판을 설치합니다. 이 두 버전에는 서로 다른 유형의 정품 인증 코드가 필요합니다. 정품 인증 코드를 가져오려면 Trend Micro에 제품을 등록합니다.

표 1-1. 버전 비교

버전	설명
정식 버전	정식 버전은 모든 제품 기능 및 기술 지원을 포함하며 라이선스 만료 후 유예 기간(일반적으로 30일)을 제공합니다. 유예 기간이 만료된 후에는 기술 지원 및 구성 요소 업데이트를 사용할 수 없습니다. 검색 엔진은 계속해서 오래된 구성 요소를 사용하여 엔드포인트를 검색합니다. 이러한 오래된 구성 요소로는 최신 보안 위협으로부터 엔드포인트를 완벽하게 보호할 수 없습니다. 라이선스 만료 전후에 유지 관리 계약 갱신 비용을 지불하여 라이선스를 갱신하십시오.
평가판	평가판은 모든 제품 기능을 포함합니다. 언제든지 평가판을 정식 버전으로 업그레이드하십시오. 평가 기간이 만료될 때까지 업그레이드하지 않으면 OfficeScan에서 구성 요소 업데이트, 검색 및 모든 에이전트 기능을 사용할 수 없습니다.

등록 키 및 정품 인증 코드

설치 중 다음 서비스에 대한 정품 인증 코드를 지정합니다.

- 바이러스 방역
- Damage Cleanup Services™(선택 사항)
- 웹 검증 및 Anti-spyware(선택 사항)

제품과 함께 제공되는 등록 키를 사용하여 정품 인증 코드를 가져옵니다(아직 가져오지 않은 경우). 제품 등록을 위한 Trend Micro 웹 사이트로 자동으로 리디렉션됩니다.

http://olr.trendmicro.com

제품을 등록하고 나면 Trend Micro에서 정품 인증 코드를 보냅니다.

설치 시 등록 키나 정품 인증 코드 중 어느 것도 사용할 수 없는 경우 Trend Micro 대리점에 문의하여 등록 키 또는 정품 인증 코드를 획득하십시오. 자세한 내용은 Trend Micro 연락처 페이지 7-3를 참조하십시오.

참고

등록에 대한 질문은 다음을 참조하십시오.

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326.

새로 설치 고려 사항

OfficeScan 서버에 대한 새로 설치를 수행할 때 다음을 고려합니다.

- IPv6 지원 페이지 1-4
- OfficeScan 서버의 위치 페이지 1-5
- 원격 설치 페이지 1-6
- 서버 성능 페이지 1-6
- 전용 서버 페이지 1-7
- 설치 도중 검색 방법 개발 페이지 1-7
- 네트워크 트래픽 페이지 1-8
- 타사 보안 소프트웨어 페이지 1-10
- Active Directory 페이지 1-10
- IIS Web Server 페이지 1-10

IPv6 지원

OfficeScan 서버 새로 설치에 대한 IPv6 요구 사항은 다음과 같습니다.

- 서버에서 IIS Web server를 사용해야 합니다.
- 서버에서 IPv4 및 IPv6 에이전트를 관리하는 경우 IPv4 주소와 IPv6 주소를 둘 다 사용하고 해당 호스트 이름으로 식별해야 합니다. 서버가 IPv4 주소로 식별되면 IPv6 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.

- 호스트 컴퓨터의 IPv6 또는 IPv4 주소를 "`ping`" 또는 "`nslookup`" 등의 명령을 사용하여 검색할 수 있는지 확인합니다.
- OfficeScan 서버를 순수 IPv6 엔드포인트에 설치하는 경우
  - IPv4 주소와 IPv6 주소 간에 변환할 수 있는 이중 스택 프록시 서버를 설치합니다(예: DeleGate). 프록시 서버를 OfficeScan 서버와 인터넷 사이에 배치하여 서버가 Trend Micro 호스팅 서비스(예: 액티브업데이트 서버, Online Registration 웹 사이트 및 스마트 보호 네트워크)에 연결할 수 있도록 합니다.

OfficeScan 서버의 위치

OfficeScan은 다양한 네트워크 환경을 수용할 수 있습니다. 예를 들어, OfficeScan 서버와 해당 에이전트 간에 방화벽을 배치하거나 단일 네트워크 방화벽 뒤에 서버와 모든 에이전트를 배치할 수 있습니다. 서버와 해당 에이전트 간에 방화벽이 있는 경우 에이전트 수신 포트와 서버 수신 포트 간에 트래픽을 허용하도록 방화벽을 구성합니다.

NAT(Network Address Translation)를 사용하는 네크워크에서 OfficeScan 에이전트를 관리할 때 발생할 수 있는 문제 해결에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

중요

Trend Micro에서는 보안을 고려하여 회사 인트라넷 내에 OfficeScan 서버를 설치하는 것을 권장합니다. 로컬 인트라넷에서 나가는 엔드포인트를 관리해야 하는 경우에는 DMZ에 OfficeScan Edge 릴레이 서버를 설치하는 것이 좋습니다.

원격 설치

원격 설치를 통해 하나의 엔드포인트에서 설치를 시작하고 다른 엔드포인트에서 OfficeScan을 설치할 수 있습니다. 원격 설치를 수행할 경우 설치 프로그램에서는 대상 엔드포인트가 서버 설치 요구 사항을 만족하는지 확인합니다.

설치가 진행될 수 있도록 하려면

- 각 대상 엔드포인트에서 로컬 시스템 계정이 아닌 관리자 계정을 사용하여 원격 레지스트리 서비스를 시작합니다. 원격 레지스트리 서비스는 Microsoft Management Console에서 관리됩니다(**시작** > **실행**을 클릭하고 `services.msc` 입력).
- 엔드포인트의 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록해 둡니다.
- 엔드포인트가 OfficeScan 서버 시스템 요구 사항을 만족하는지 확인합니다. 자세한 내용은 새로 설치 및 업그레이드 요구 사항 페이지 1-2을 참조하십시오.

서버 성능

엔터프라이즈 네트워크에서는 중소기업에 필요한 사양보다 높은 사양의 서버가 필요합니다.

팁

OfficeScan 서버에는 2GHz 이상의 이중 프로세서와 2GB 이상의 RAM을 사용하는 것이 좋습니다.

단일 OfficeScan 서버가 관리할 수 있는 네트워크로 연결된 엔드포인트 에이전트 수는 사용 가능한 서버 리소스 및 네트워크 토폴로지와 같은 여러 가지 요소

에 따라 다릅니다. 서버가 관리할 수 있는 에이전트 수를 확인하려면 Trend Micro 대리점에 문의하십시오.

전용 서버

OfficeScan 서버를 호스팅할 엔드포인트를 선택할 때에는 다음을 고려합니다.

- 엔드포인트가 처리하는 CPU 로드 상황
- 엔드포인트가 다른 기능을 수행하는지 여부

다른 기능을 수행하고 있는 대상 엔드포인트일 경우 중요하거나 리소스 집약적인 응용 프로그램을 실행하지 않는 다른 엔드포인트를 선택합니다.

설치 도중 검색 방법 개발

이 OfficeScan 버전에서는 스마트 스캔 또는 표준 스캔을 사용하도록 에이전트를 구성할 수 있습니다.

표준 스캔

표준 스캔은 모든 이전 OfficeScan 버전에서 사용되는 검색 방법입니다. 표준 스캔 에이전트는 모든 OfficeScan 구성 요소를 에이전트 엔드포인트에 저장하고 모든 파일을 로컬로 검색합니다.

스마트 스캔

스마트 스캔은 인 더 클라우드에 저장된 위협 서명을 활용합니다. 스마트 스캔 모드에 있을 때 OfficeScan 에이전트는 우선 로컬로 보안 위험을 검색합니다. 에이전트가 검색 중에 파일의 위험을 판별할 수 없는 경우 에이전트는 스마트 보호 서버에 연결합니다.

스마트 스캔은 다음과 같은 기능 및 장점을 제공합니다.

- 클라우드에 빠른 실시간 보안 상태 조회 기능 제공
- 새로운 위협에 대한 보호 기능을 제공하는 데 걸리는 전체적인 시간 단축

- 패턴 업데이트 시 사용되는 네트워크 대역폭 감소. 대량의 패턴 정의 업데이트가 많은 에이전트에 모두 전달될 필요 없이 클라우드에만 전달되면 됩니다.
- 회사 전체의 패턴 배포와 관련된 비용 및 오버헤드 감소
- 엔드포인트의 커널 메모리 사용량 감소. 메모리 사용량은 시간이 지나면서 최소한으로만 증가합니다.

검색 방법 개발

새로 설치 동안 에이전트의 기본 검색 방법은 스마트 스캔입니다. OfficeScan에서는 서버 설치 후 각 도메인에 대한 검색 방법을 사용자 정의할 수도 있습니다. 다음을 고려합니다.

- 서버 설치 후 검색 방법을 변경하지 않은 경우 설치하는 모든 에이전트에서는 스마트 스캔을 사용합니다.
- 모든 에이전트에 대해 표준 스캔을 사용하려는 경우 서버 설치 후 루트 수준 검색 방법을 표준 스캔으로 변경합니다.
- 표준 스캔과 스마트 스캔을 둘 다 사용하려는 경우 루트 수준 검색 방법으로 스마트 스캔을 유지한 다음 표준 스캔을 적용할 도메인의 검색 방법을 변경하는 것이 좋습니다.

네트워크 트래픽

배포를 계획할 때 OfficeScan이 생성하는 네트워크 트래픽을 고려합니다. 서버는 다음과 같은 경우에 트래픽을 생성합니다.

- Trend Micro 액티브업데이트 서버에 연결하여 업데이트된 구성 요소를 확인하고 다운로드하는 경우
- 업데이트된 구성 요소를 다운로드하도록 에이전트에 알리는 경우
- 구성 요소 변경을 에이전트에 알리는 경우

OfficeScan 에이전트는 다음과 같은 경우에 트래픽을 생성합니다.

- 시작하는 경우

- 구성 요소를 업데이트하는 경우
- 설정을 업데이트하고 핫픽스를 설치하는 경우
- 보안 위험을 검색하는 경우
- “독립” 모드와 “일반” 모드 간을 전환하는 경우
- 표준 스캔과 스마트 스캔 간을 전환하는 경우

구성 요소 업데이트 중의 네트워크 트래픽

OfficeScan은 구성 요소를 업데이트할 때 상당한 네트워크 트래픽을 생성합니다. OfficeScan은 구성 요소 업데이트 중에 생성되는 네트워크 트래픽을 줄이기 위해 구성 요소 복제를 수행합니다. 업데이트된 전체 패턴 파일을 다운로드하는 대신 OfficeScan은 "인크리멘탈" 패턴(전체 패턴 파일보다 작은 버전)만 다운로드한 후에 이전 패턴 파일에 병합합니다.

정기적으로 업데이트되는 OfficeScan 에이전트는 인크리멘탈 패턴만 다운로드합니다. 그렇지 않으면 전체 패턴 파일을 다운로드합니다.

Trend Micro에서는 새로운 패턴 파일을 정기적으로 릴리스합니다. 또한 Trend Micro는 위험하고 급속도로 확산되는 바이러스/악성 프로그램이 발견되는 즉시 새로운 패턴 파일을 릴리스합니다.

업데이트 에이전트 및 네트워크 트래픽

에이전트와 OfficeScan 서버 사이의 네트워크에 낮은 대역폭 또는 과중한 트래픽 섹션이 있는 경우 선택한 OfficeScan 에이전트를 업데이트 에이전트 또는 다른 에이전트의 업데이트 소스로 지정합니다. 이렇게 하면 구성 요소를 모든 에이전트에 배포하는 부담이 줄어듭니다.

예를 들어, 20개 이상의 엔드포인트가 있는 원격 사무실의 경우 OfficeScan 서버에서 업데이트를 복제하고 로컬 네트워크에 있는 다른 에이전트 엔드포인트의 배포 지점으로 작동할 업데이트 에이전트를 지정합니다. 업데이트 에이전트에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

Trend Micro Control Manager 및 네트워크 트래픽

Trend Micro Control Manager™는 Trend Micro 제품 및 서비스를 게이트웨이, Mail Server, 파일 서버 및 기업 데스크톱 수준에서 관리합니다. Control Manager 웹 기반 관리 콘솔은 네트워크 전체의 제품과 서비스를 단일 위치에서 모니터링할 수 있습니다.

Control Manager를 사용하여 단일 위치에서 여러 OfficeScan 서버를 관리합니다. Control Manager 서버는 빠르고 안정적인 인터넷 연결을 통해 Trend Micro 액티브업데이트 서버에서 구성 요소를 다운로드할 수 있습니다. Control Manager는 그런 다음 인터넷 연결이 안정적이지 않거나 인터넷 연결이 없는 하나 이상의 OfficeScan 서버에 구성 요소를 배포합니다.

자세한 내용은 Control Manager 설명서를 참조하십시오.

타사 보안 소프트웨어

OfficeScan 서버를 설치할 엔드포인트에서 타사 엔드포인트 보안 소프트웨어를 제거합니다. 이러한 응용 프로그램은 OfficeScan 서버 설치를 방해하거나 성능에 영향을 줄 수 있습니다. 엔드포인트를 보안 위험으로부터 계속 보호할 수 있도록, 타사 보안 소프트웨어를 제거한 후 즉시 OfficeScan 서버 및 OfficeScan 에이전트를 설치합니다.

참고

OfficeScan에서 타사 바이러스 백신 제품의 서버 구성 요소를 자동으로 제거할 수 없지만 에이전트 구성 요소는 제거할 수 있습니다. 자세한 내용은 *OfficeScan 관리자 안내서*를 참조하십시오.

Active Directory

역할 기반 관리 및 보안 준수 기능을 활용하려면 모든 OfficeScan 서버가 Active Directory 도메인에 속해야 합니다.

IIS Web Server

OfficeScan Web Server 기능은 다음과 같습니다.

- 사용자가 웹 콘솔에 액세스할 수 있도록 해줍니다.
- 에이전트에서 명령을 받습니다.
- 에이전트가 서버 알림에 응답하도록 합니다.

IIS Web Server의 경우, 서버 컴퓨터가 IIS 잠금 응용 프로그램을 실행하지 않는지 확인합니다. 설치 과정에서 IIS 서비스가 자동으로 중지된 다음 다시 시작됩니다.

업그레이드 고려 사항

OfficeScan 서버 및 에이전트를 업그레이드할 때 다음을 고려합니다.

- IPv6 지원 페이지 1-11
- 지원되지 않는 운영 체제 페이지 1-12
- OfficeScan 설정 및 구성 페이지 1-13
- 업그레이드 도중 검색 방법 개발 페이지 1-14

IPv6 지원

OfficeScan 서버 및 에이전트 업그레이드에 대한 IPv6 요구 사항은 다음과 같습니다.

- 업그레이드할 OfficeScan 서버는 버전 10.6 SP3 또는 11.x여야 합니다.
- 서버에서 IIS Web server를 이미 사용 중이어야 합니다.
- 서버에 IPv6 주소를 할당합니다. 또한 서버를 해당 호스트 이름(가급적이면 FQDN(정규화된 도메인 이름))으로 식별해야 합니다. 서버가 IPv6 주소로 식별되는 경우 현재 서버에서 관리하는 모든 에이전트가 서버에서 연결이 끊어집니다. 서버가 IPv4 주소로 식별되는 경우 에이전트를 순수 IPv6 엔드포인트에 배포할 수 없습니다.
- 호스트 컴퓨터의 IPv6 또는 IPv4 주소를 **`ping`** 또는 **`nslookup`** 등의 명령을 사용하여 검색할 수 있는지 확인합니다.

지원되지 않는 운영 체제

OfficeScan에서는 Windows 95, 98, Me, NT, 2000 또는 Itanium 아키텍처 플랫폼을 더 이상 지원하지 않습니다.

이 버전으로 업그레이드를 계획 중이고 이러한 운영 체제를 실행하는 OfficeScan 에이전트가 있는 경우

- 모든 OfficeScan 서버를 이 OfficeScan 버전으로 업그레이드하지 마십시오.
- 지원되지 않는 운영 체제를 실행하는 에이전트를 관리하기 위해 OfficeScan 서버(상위 서버)를 하나 이상 지정합니다.
- 다른 서버를 업그레이드하기 전:
  - OfficeScan 10.x 서버의 경우:
    - 웹 콘솔에 로그온하여 기본 메뉴에서 **네트워크로 연결된 컴퓨터** > **클라이언트 관리**를 클릭합니다.
    - 클라이언트 트리에서 이동할 클라이언트를 선택한 다음 **클라이언트 트리 관리** > **클라이언트 이동**을 클릭합니다.
    - **선택한 클라이언트를 다른 OfficeScan 서버로 이동**에서 상위 서버의 컴퓨터 이름/IP 주소 및 서버 수신 포트를 지정합니다.
    - **이동**을 클릭합니다.
  - OfficeScan 11.x 서버의 경우:
    - 웹 콘솔에 로그온한 다음 기본 메뉴에서 **에이전트** > **에이전트 관리**를 클릭합니다.
    - 에이전트 트리에서 이동할 에이전트를 선택한 다음 **에이전트 트리 관리** > **에이전트 이동**을 클릭합니다.
    - **선택한 에이전트를 다른 OfficeScan 서버로 이동**에서 상위 서버의 컴퓨터 이름/IP 주소 및 서버 수신 포트를 지정합니다.
    - **이동**을 클릭합니다.

OfficeScan 설정 및 구성

OfficeScan 서버를 업그레이드하기 전에 OfficeScan 데이터베이스와 중요 구성 파일을 백업합니다. OfficeScan 서버 데이터베이스를 OfficeScan 프로그램 디렉터리 이외의 위치에 백업합니다.

팁

이 OfficeScan 버전은 롤백용 백업 메커니즘을 제공합니다. 설치 시 자동 백업을 사용할 계획이 아니라면 수동 데이터베이스 백업을 수행합니다.

OfficeScan 데이터베이스와 구성 파일 백업 및 복원

절차

1. **관리** > **데이터베이스 백업**으로 이동하여 OfficeScan 10.x 또는 11.x 웹 콘솔에서 데이터베이스를 백업합니다.

   자세한 지침은 이 제품 버전의 *관리자 안내서* 또는 *서버 도움말*을 참조하십시오.

   경고!

   다른 유형의 백업 도구 또는 응용 프로그램을 사용하지 마십시오.

2. Microsoft Management Console에서 OfficeScan Master Service를 중지합니다.
3. <서버 설치 폴더>₩PCCSRV에 있는 다음 파일과 폴더를 수동으로 백업합니다.

   참고

   업그레이드 문제가 발생하는 경우에만 이러한 파일과 폴더를 백업하여 OfficeScan을 롤백합니다.

   - ofcscan.ini: 글로벌 에이전트 설정이 들어 있습니다.
   - ous.ini: 바이러스 방역 구성 요소 배포를 위한 업데이트 소스 테이블이 들어 있습니다.

- Private 폴더: 방화벽 및 업데이트 소스 설정이 들어 있습니다.
- Web₩tmOPP 폴더: 바이러스 사전 방역 설정이 들어 있습니다.
- Pccnt₩Common₩OfcPfw*.dat: 방화벽 설정이 들어 있습니다.
- Download₩OfcPfw*.dat: 방화벽 배포 설정이 들어 있습니다.
- Log 폴더: 시스템 이벤트 및 연결 확인 로그가 들어 있습니다.
- Virus 폴더: 격리된 파일이 들어 있습니다.
- HTTPDB 폴더: OfficeScan 데이터베이스가 들어 있습니다.

4. OfficeScan 서버를 업그레이드합니다.

참고

업그레이드 문제가 발생하는 경우 3단계의 백업 파일을 대상 엔드포인트의 <서버 설치 폴더>₩PCCSRV 폴더에 복사한 후 OfficeScan Master Service를 다시 시작합니다.

업그레이드 도중 검색 방법 개발

이 OfficeScan 버전에서는 관리자가 에이전트가 스마트 스캔 또는 표준 스캔을 사용하도록 구성할 수 있습니다.

이전 버전에서 OfficeScan을 업그레이드하는 경우 선택한 업그레이드 방법에 따라 각 도메인의 검색 방법을 유지하거나 사용자 정의합니다. 다음을 고려합니다.

- 서버 컴퓨터에서 직접 OfficeScan 10.x 또는 11.x 서버를 업그레이드하려는 경우 에이전트가 업그레이드 후 검색 방법 설정을 유지하므로 웹 콘솔에서 검색 방법을 변경할 필요가 없습니다.
- OfficeScan 10.x 또는 11.x 에이전트를 OfficeScan XG 서버로 이동하여 업그레이드하려는 경우
  - OfficeScan XG 서버에서 수동 에이전트 그룹화를 선택합니다. 이 에이전트 그룹화 방법에서는 새 도메인 만들기를 감안합니다.

참고

자동 에이전트 그룹화를 사용할 경우, 에이전트를 업그레이드하는 동안 모든 검색 방법 설정이 유지되도록 모든 에이전트가 업그레이드된 이후에만 자동 에이전트 그룹화를 사용하도록 설정합니다.

- OfficeScan 10.x 또는 11.x 서버의 도메인 구조 및 검색 방법 설정을 OfficeScan XG 서버에 복제합니다. 두 서버의 도메인 구조 및 검색 방법 설정이 서로 다르면 OfficeScan XG 서버로 이동한 일부 에이전트가 원래 검색 방법 설정을 적용하지 않을 수 있습니다.

설치 및 업그레이드 체크리스트

OfficeScan 서버를 설치하거나 업그레이드할 때 다음 정보를 확인하라는 메시지가 나타납니다.

표 1-2. 설치 및 업그레이드 체크리스트

설치 정보	아래의 경우에 필요한 정보			
	로컬/자동 새로 설치	원격 새로 설치	로컬/자동 업그레이드	원격 업그레이드
OfficeScan 설치 경로 기본 서버 설치 경로는 다음과 같습니다. • C:₩Program Files₩Trend Micro ₩OfficeScan • C:₩Program Files (x86)₩Trend Micro ₩OfficeScan(**x64** 유형 플랫폼) 설치 경로를 식별하거나 기본 경로를 사용합니다. 경로가 존재하지 않는 경우 자동으로 만들어집니다.	예	예	아니요	예

설치 정보	아래의 경우에 필요한 정보			
	로컬/자동 새로 설치	원격 새로 설치	로컬/자동 업그레이드	원격 업그레이드
프록시 서버 설정 OfficeScan 서버가 프록시 서버를 통해 인터넷에 연결되는 경우 다음을 지정합니다. • 프록시 유형(HTTP 또는 SOCKS 4) • 서버 이름 또는 IP 주소 • 포트 • 프록시 인증 자격 증명	예	예	아니요	예

설치 정보	아래의 경우에 필요한 정보			
	로컬/자동 새로 설치	원격 새로 설치	로컬/자동 업그레이드	원격 업그레이드
Web Server 설정 Web Server는 웹 콘솔 CGI를 실행하고 에이전트에서 명령을 받습니다. 다음을 지정합니다. • HTTP 포트: 기본 포트는 8080입니다. IIS 기본 웹 사이트를 사용하는 중인 경우 HTTP 서버의 TCP 포트를 확인합니다. **경고!** HTTP를 통해 전달되는 많은 해커 및 바이러스/악성 프로그램 공격은 포트 80 및/또는 8080을 사용합니다. 대부분의 조직에서는 HTTP 통신에 이러한 포트 번호를 기본 TCP 포트로 사용합니다. 기본 포트 번호를 현재 사용 중인 경우 다른 포트 번호를 사용합니다. 보안 연결이 사용하도록 설정된 경우 • SSL 인증서 유효 기간 • SSL 포트(기본값: 4343)	예	예	아니요	예

설치 정보	아래의 경우에 필요한 정보			
	로컬/자동 새로 설치	원격 새로 설치	로컬/자동 업그레이드	원격 업그레이드

등록
정품 인증 코드를 받으려면 제품을 등록합니다. 제품을 등록하려면 다음 정보가 필요합니다.
• 기존 사용자의 경우
  • 온라인 등록 계정(로그온 이름 및 암호)
• 계정 없는 사용자의 경우
  • 등록 키
	예	예	예	예

정품 인증 다음 제품 서비스에 대한 정품 인증 코드를 가져옵니다. • 바이러스 방역 • DCS(Damage Cleanup Services) • 웹 검증 및 Anti-spyware	예	예	예	예
통합 스마트 보호 서버 설치 통합 서버 설치 시 다음을 지정합니다. • SSL 인증서 유효 기간 • SSL 포트	예	예	예	예

설치 정보	아래의 경우에 필요한 정보			
	로컬/자동 새로 설치	원격 새로 설치	로컬/자동 업그레이드	원격 업그레이드

원격 설치 대상
 	
OfficeScan 서버 설치/업그레이드가 수행되는 엔드포인트를 식별합니다. 다음을 준비합니다.
• 엔드포인트 이름 또는 IP 주소 목록
• (선택 사항) 대상 엔드포인트 또는 IP 주소 목록이 포함된 텍스트 파일
 	
샘플 텍스트 파일 내용
 	
`us-user_01`
 	
`us-admin_01`
 	
`123.12.12.123`
	아니요	예	아니요	예

원격 설치 엔드포인트 분석 대상 엔드포인트 분석을 수행하기 전에 다음 정보를 입력하라는 메시지가 나타납니다. • 대상 엔드포인트에 "서비스로 로그온" 권한이 있는 관리자 계정의 사용자 이름 및 암호	아니요	예	아니요	예
OfficeScan 에이전트를 설치합니다.	예	아니요	아니요	아니요

설치 정보	아래의 경우에 필요한 정보			
	로컬/자동 새로 설치	원격 새로 설치	로컬/자동 업그레이드	원격 업그레이드
관리자 계정 암호 설치 프로그램에서 웹 콘솔 로그온을 위한 루트 계정을 만듭니다. 다음을 지정합니다. • 루트 계정 암호 다음을 지정하여 OfficeScan 에이전트가 무단으로 제거 또는 종료되는 것을 방지합니다. • OfficeScan 에이전트 제거/종료 암호	예	예	아니요	아니요
OfficeScan 에이전트 설치 경로 에이전트 엔드포인트에서 OfficeScan 에이전트가 설치될 디렉터리를 지정합니다. 다음을 지정합니다. • 설치 경로: 기본 에이전트 설치 경로는 $ProgramFiles₩Trend Micro ₩OfficeScan Client입니다. 설치 경로를 식별하거나 기본 경로를 사용합니다. 경로가 존재하지 않는 경우 에이전트 설치 중에 만들어집니다. • OfficeScan 에이전트 통신 포트 번호: OfficeScan에서 포트 번호를 임의로 생성합니다. 생성된 포트 번호를 적용하거나 새 포트 번호를 지정합니다.	예	예	아니요	아니요

설치 정보	아래의 경우에 필요한 정보			
	로컬/자동 새로 설치	원격 새로 설치	로컬/자동 업그레이드	원격 업그레이드
데이터베이스 백업 롤백용으로 OfficeScan 데이터베이스를 백업할 서버 컴퓨터의 위치를 지정합니다. **참고** 백업 패키지에 최소 300MB의 사용 가능한 공간이 필요하며 완료하는 데 시간이 걸릴 수 있습니다.	아니요	아니요	예	예
서버 인증 인증서 OfficeScan은 설치 중에 기존 인증 인증서에 대한 검색을 시도합니다. If OfficeScan이 인증서를 검색하지 않으면 새 인증서에 대한 백업 암호를 지정합니다.	예	예	예 (OfficeScan 10.6 SP3에서 업그레이드할 때)	예
프로그램 폴더 바로 가기 OfficeScan 서버 설치 폴더 바로 가기는 Windows 시작 메뉴에서 표시됩니다. 기본 바로 가기 이름은 Trend Micro OfficeScan 서버-<Server_name>입니다. 다른 이름을 식별하거나 기본 이름을 사용합니다.	예	아니요	아니요	아니요

파일럿 배포 계획

대규모 배포를 수행하기 전에 통제된 환경에서 파일럿 배포를 수행합니다. 파일럿 배포를 통해 전체 배포 이후에 기능이 작동하는 방식과 필요한 지원 수준을 파악할 수 있습니다. 설치 팀에 배포 프로세스를 연습 및 개선할 기회를 제공합니다. 또한 관리자가 배포 계획이 조직의 보안 기본 방안에 부합하는지를 테스트할 수 있습니다.

샘플 OfficeScan 배포는 샘플 배포 페이지 A-1 항목을 참조하십시오.

파일럿 사이트 선택

작업 환경과 일치하는 파일럿 사이트를 선택합니다. 작업 환경을 대표적으로 보여줄 수 있는 네트워크 토폴로지 유형을 시뮬레이션해 봅니다.

롤백 계획 수립

설치 또는 업그레이드 프로세스에 문제가 있을 경우를 대비하여 복구 또는 롤백 계획을 수립합니다.

파일럿 배포 평가

파일럿 프로세스 중에 발생하는 성공 및 실패 목록을 만듭니다. 잠재적인 문제점을 확인하고 그에 따라 배포 계획을 수립합니다. 전체 제품 배포 계획에 이 파일럿 평가 계획을 포함시킵니다.

알려진 호환성 문제

이 섹션은 특정 타사 응용 프로그램이 설치되어 있는 동일한 엔드포인트에 OfficeScan 서버를 설치할 때 발생할 수 있는 호환성 문제에 대해 설명합니다. 자세한 내용은 타사 응용 프로그램 설명서를 참조하십시오.

Microsoft 잠금 도구 및 URLScan

Microsoft IIS 잠금 도구 또는 URLScan을 사용하는 경우 다음 OfficeScan 파일의 잠금이 OfficeScan 에이전트와 서버의 통신을 차단할 수 있습니다.

- 구성 파일(.ini)
- 데이터 파일(.dat)
- 동적 링크 라이브러리 파일(.dll)

- 실행 파일(.exe)

에이전트와 서버 간 통신에서 URLScan 간섭 방지

절차

1. OfficeScan 서버 컴퓨터에서 World Wide Web Publishing 서비스를 중지합니다.
2. 위에서 지정한 파일 형식을 허용하도록 URLScan 구성 파일을 수정합니다.
3. World Wide Web Publishing 서비스를 다시 시작합니다.

Microsoft Exchange Server

서버 설치 중 OfficeScan 에이전트를 설치할 때 OfficeScan은 에이전트가 검색하는 모든 파일에 액세스해야 합니다. Microsoft Exchange Server가 로컬 디렉터리에 메시지를 대기시키므로 Exchange Server가 전자 메일 메시지를 처리할 수 있도록 검색에서 해당 디렉터리를 제외시켜야 합니다.

OfficeScan이 자동으로 검색에서 모든 Microsoft Exchange 2000/2003 디렉터리를 제외시킵니다. 웹 콘솔에서 이 설정을 구성합니다(**보안 설정** 탭의 **에이전트 > 글로벌 에이전트 설정 > 검색 설정**). Microsoft Exchange 2007 검색 제외에 대한 자세한 내용은 다음을 참조하십시오.

http://technet.microsoft.com/en-us/library/bb332342(EXCHG.80).aspx

데이터베이스 서버

관리자가 데이터베이스 서버를 검색할 수 있습니다. 그러나 이 경우 데이터베이스에 액세스하는 응용 프로그램의 성능이 저하될 수 있습니다. 데이터베이스 및 해당 백업 폴더는 실시간 검색에서 제외하는 것을 고려해 보십시오. 데이터베이스 검색의 영향을 최소화하려면 사용량이 많지 않은 시간대에 수동 검색을 수행하십시오.

장 2

OfficeScan 설치

이 장에서는 Trend Micro™ OfficeScan™ 설치 단계에 대해 설명합니다.

이 장의 내용:

- OfficeScan 서버 새로 설치 수행 페이지 2-2
- 자동 설치 페이지 2-2
- 설치 프로그램 설치 화면 페이지 2-4

OfficeScan 서버 새로 설치 수행

새로 설치를 수행하려면 OfficeScan 서버 설치 및 업그레이드 요구 사항을 충족하는 엔드포인트에서 설치 프로그램을 실행합니다(자세한 내용은 새로 설치 및 업그레이드 요구 사항 페이지 1-2 참조).

OfficeScan 서버 및 Plug-in Manager 2.3이 설치됩니다. 이 Plug-in Manager 버전은 OfficeScan에 위젯 기능을 제공합니다. 설치 화면 및 구성 옵션에 대한 자세한 내용은 설치 프로그램 설치 화면 페이지 2-4을 참조하십시오.

에이전트 새로 설치 방법 및 지침 또는 Edge 릴레이 서버 설치 절차는 *관리자 안내서*를 참조하십시오.

자동 설치

서버가 동일한 설치 설정을 사용하는 경우 여러 OfficeScan 서버를 자동으로 설치하거나 업그레이드합니다.

대상 엔드포인트에서 자동 설치가 실행되면 설치 프로그램에서 OfficeScan XG 및 Plug-in Manager 2.3을 설치합니다. Plug-in Manager 2.3은 OfficeScan에 위젯 기능을 제공합니다.

자동 설치 준비

절차

1. 설치 프로그램을 실행하고 설치 설정을 .iss 파일에 기록하여 응답 파일을 만듭니다. 응답 파일을 사용하여 자동으로 설치된 모든 서버에서 해당 설정을 사용합니다.

   중요

   - 설치 프로그램은 로컬 설치에 대한 화면만 표시합니다.
   - 새로 설치의 경우 OfficeScan 서버를 설치하지 않고 엔드포인트에서 응답 파일을 만듭니다.

2. 명령 프롬프트에서 설치 프로그램을 실행하고 자동 설치에 사용할 응답 파일의 위치를 지정합니다.

응답 파일에 설치 구성 기록

이 절차는 OfficeScan을 설치하지 않고 설치 구성을 응답 파일에 기록하기만 합니다.

절차

1. OSCE.exe 파일을 다운로드하고 내용을 추출합니다.
2. 명령 프롬프트를 열고 OfficeScan setup.exe 파일의 디렉터리를 입력합니다.

   예를 들면 "`CD C:\OfficeScan Installer\setup.exe`"입니다.
3. 다음과 같이 입력합니다.

   ```
   setup.exe -r
   ```

   `-r` 매개 변수는 설치 프로그램을 실행시키고 설치 세부 정보를 응답 파일에 기록하도록 합니다.
4. 설치 프로그램의 설치 단계를 수행합니다.
5. 단계를 완료한 후 %windir%에서 응답 파일 setup.iss를 확인합니다.

자동 설치 실행

절차

1. 설치 패키지 및 setup.iss를 대상 엔드포인트에 복사합니다.
2. 대상 엔드포인트에서 명령 프롬프트를 열고 설치 패키지의 디렉터리를 입력합니다.
3. 다음과 같이 입력합니다.

   ```
   setup.exe -s <-f1path>setup.iss <-f2path>setup.log.
   ```

예: C:₩setup.exe -s -f1C:₩setup.iss -f2C:₩setup.log

여기서 각 항목은 다음과 같습니다.

- `-s`: 설치 프로그램이 자동 설치를 수행하도록 합니다.
- `<-f1path>setup.iss`: 응답 파일의 위치입니다. 경로에 공백이 있으면 따옴표(")로 경로를 묶습니다. 예를 들면 `-f1"C:₩osce script ₩setup.iss"`입니다.
- `<-f2path>setup.log`: 설치 후 설치 프로그램이 만드는 로그 파일의 위치입니다. 경로에 공백이 있으면 따옴표(")로 경로를 묶습니다. 예를 들면 `-f2"C:₩osce log₩setup.log"`입니다.

4. Enter 키를 누릅니다.

   설치 프로그램이 엔드포인트에 서버를 자동으로 설치합니다.

5. 설치에 성공했는지 확인하려면
   - 대상 엔드포인트에서 OfficeScan 프로그램 바로 가기를 확인합니다. 바로 가기를 사용할 수 없는 경우 다시 설치해 보십시오.
   - OfficeScan 웹 콘솔에 로그온합니다.

설치 프로그램 설치 화면

다음은 OfficeScan 서버를 로컬, 원격 또는 자동으로 새로 설치할 때 표시되는 설치 화면(순차적으로 정렬됨) 목록입니다.

표 2-1. 설치 화면 및 작업

화면	로컬/자동 새로 설치	원격 새로 설치
OfficeScan 설치 프로그램 사전 필수 단계	✔	✔
시작	✔	✔

화면	로컬/자동 새로 설치	원격 새로 설치
사용권 계약 페이지 2-7	✔	✔
설치 대상 페이지 2-8	✔	✔
엔드포인트 설치 전 검색 페이지 2-10	✔	✔
설치 상태(엔드포인트 분석) **참고** 분석을 완료하면서 특히 HTTP 서버 초기화 중에 시간이 걸릴 수 있습니다.	✔	
설치 경로 페이지 2-12	✔	✔
프록시 서버 페이지 2-13	✔	✔
Web Server 페이지 2-14	✔	✔
서버 식별 페이지 2-17	✔	✔
등록 및 정품 인증 페이지 2-19	✔	✔
OfficeScan 에이전트 배포 페이지 2-21	✔	✔
통합 스마트 보호 서버 설치 페이지 2-22	✔	✔
설치 대상 페이지 2-26		✔
대상 엔드포인트 분석 페이지 2-28		✔
OfficeScan 에이전트 설치 페이지 2-30	✔	✔

화면	로컬/자동 새로 설치	원격 새로 설치
스마트 보호 네트워크 페이지 2-32	✓	✓
관리자 계정 암호 페이지 2-34	✓	✓
OfficeScan 에이전트 설치 페이지 2-35	✓	✓
OfficeScan 방화벽 페이지 2-37	✓	✓
Anti-spyware 기능 페이지 2-39	✓	✓
웹 검증 기능 페이지 2-40	✓	✓
서버 인증 인증서 페이지 2-41	✓	✓
OfficeScan 프로그램 바로 가기 페이지 2-44	✓	
설치 정보 페이지 2-45	✓	✓
OfficeScan 서버 설치	✓	✓
InstallShield 마법사 완료 페이지 2-46	✓	✓

사용권 계약

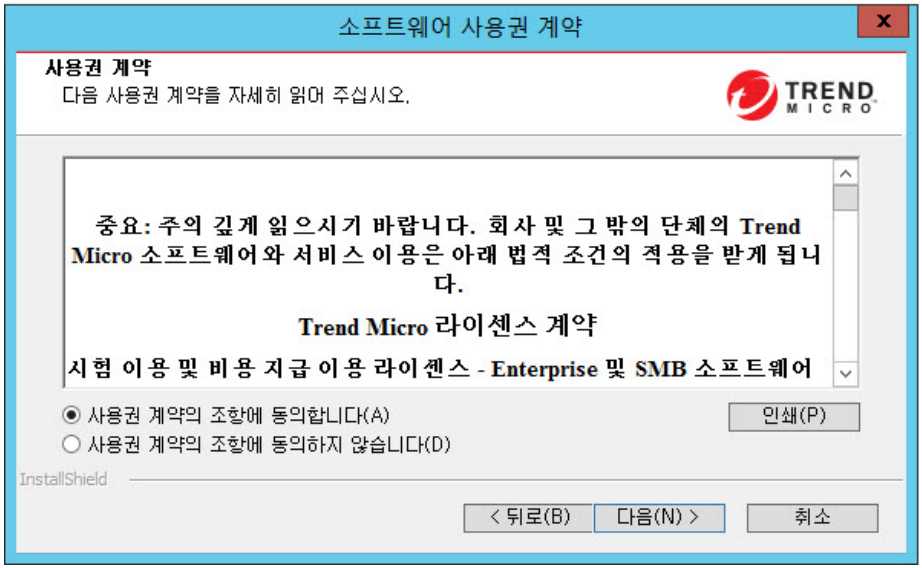

그림 2-1. 사용권 계약 화면

설치를 계속하려면 사용권 계약 내용을 주의 깊게 읽고 사용권 계약 조건에 동의합니다. 사용권 계약 조건에 동의하지 않으면 설치를 진행할 수 없습니다.

설치 대상

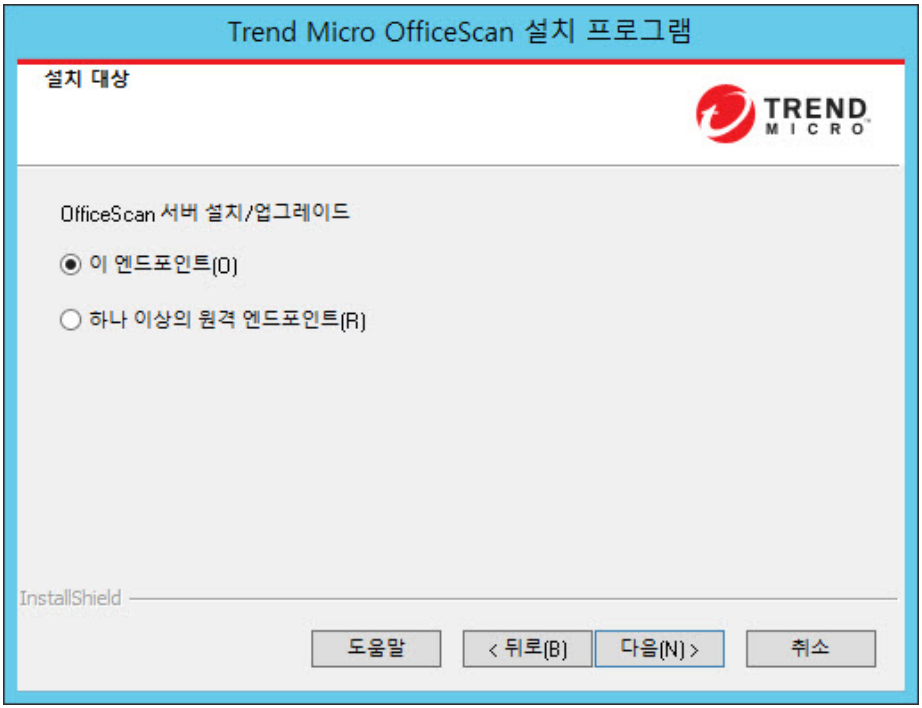

그림 2-2. 설치 대상 화면

현재 엔드포인트나 네트워크의 다른 엔드포인트에서 설치 프로그램을 실행하고 OfficeScan 서버를 설치합니다. 설치 프로그램이 대상 엔드포인트에서 이전 버전의 OfficeScan을 탐지하면 자동으로 업그레이드가 수행됩니다. 다음 버전의 OfficeScan만 이 버전으로 업그레이드할 수 있습니다.

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3

참고

Trend Micro에서는 업그레이드를 수행하기 전에 현재 OfficeScan 서버에 사용 가능한 모든 패치 및 핫픽스를 적용할 것을 권장합니다.

원격 설치 참고 사항

원격으로 설치할 경우 설치 프로그램에서는 대상 엔드포인트가 서버 설치 요구 사항을 만족하는지 확인합니다. 진행하기 전에

- 대상 엔드포인트에 대한 관리자 권한을 얻습니다.
- 대상 엔드포인트에 대한 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록합니다.
- 대상 엔드포인트가 OfficeScan 서버 설치에 대한 요구 사항을 만족하는지 확인합니다.
- Microsoft IIS Server를 Web Server로 사용할 경우 엔드포인트에 버전 7.0 이상이 있는지 확인합니다.

엔드포인트 설치 전 검색

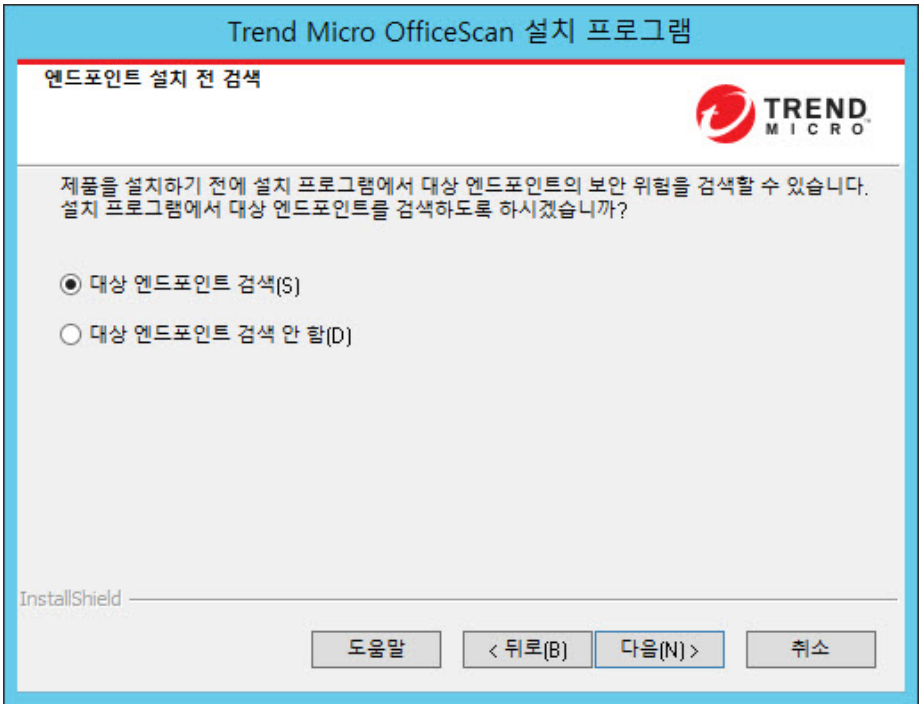

그림 2-3. 엔드포인트 설치 전 검색 화면

설치 프로그램은 OfficeScan 서버 설치를 시작하기 전에 대상 엔드포인트에서 바이러스 및 악성 프로그램을 검색할 수 있습니다. 엔드포인트에서 다음을 비롯한 가장 취약한 영역을 검색합니다.

- 부트 영역 및 부트 디렉터리(부트 바이러스 대상)
- Windows 폴더
- Program Files 폴더

설치 프로그램은 발견된 바이러스/악성 프로그램 및 트로이 목마 프로그램에 대해 다음과 같은 조치를 수행할 수 있습니다.

- **삭제**: 감염된 파일을 삭제합니다.
- **치료**: 파일에 대한 전체 액세스를 허용하기 전에 치료 가능 파일을 치료하거나 지정된 다음 처리 방법으로 치료할 수 없는 파일을 처리합니다.
- **파일명 변경**: 감염된 파일의 확장자를 "vir"로 변경합니다. 사용자가 처음에는 파일을 열 수 없지만 파일을 특정 응용 프로그램에 연결하는 경우 열 수 있습니다. 파일명이 변경된 감염 파일을 열면 바이러스/악성 프로그램이 실행될 수 있습니다.
- **그대로 두기**: 감염된 파일에 대해 아무 조치도 취하지 않고 파일에 대한 전체 액세스를 허용합니다. 사용자가 파일을 열기/복사/삭제할 수 있습니다.

로컬 설치를 수행할 경우 **다음**을 클릭하면 검색이 수행됩니다. 원격 설치를 수행할 경우 실제 설치 직전에 검색이 수행됩니다.

중요

설치 프로그램은 로컬 업그레이드 설치 중 랜섬웨어 위협으로부터 최적화된 보호를 받을 수 있도록 랜섬웨어 보호 설정을 업데이트하라는 메시지를 표시합니다.

업데이트된 설정을 적용하면 이미 동작 모니터링이 사용되도록 설정된 에이전트의 설정만 변경됩니다.

설치 경로

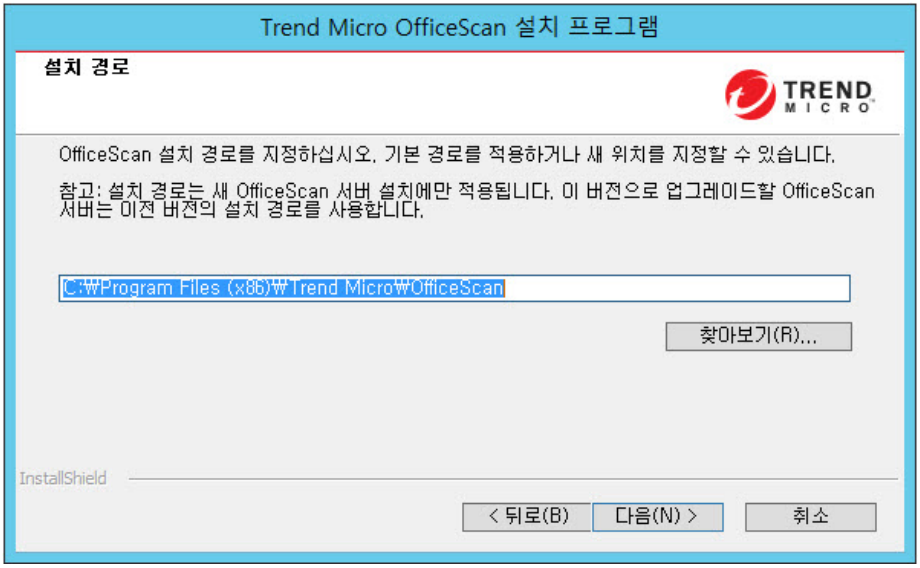

그림 2-4. 설치 경로 화면

기본 설치 경로를 적용하거나 새 경로를 지정합니다.

지정한 설치 경로는 원격 새로 설치를 수행하는 경우에만 적용됩니다. 원격 업그레이드의 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

프록시 서버

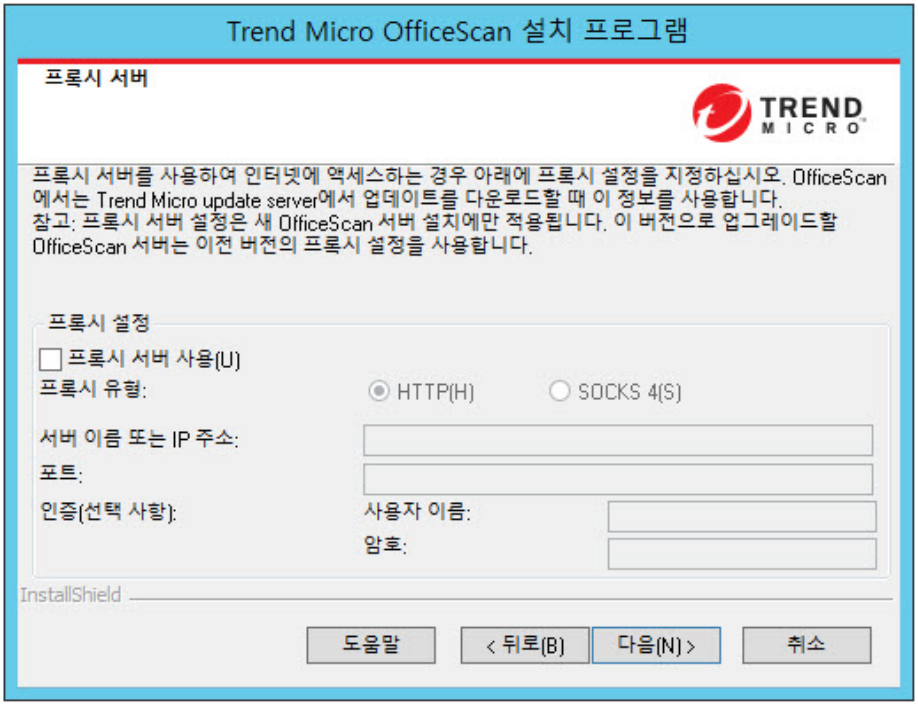

그림 2-5. 프록시 서버 화면

OfficeScan 서버는 HTTP 프로토콜을 사용하여 에이전트-서버 통신을 수행하고 Trend Micro 액티브업데이트 서버에 연결하여 업데이트를 다운로드합니다. 프록시 서버에서 네트워크의 인터넷 트래픽을 처리하는 경우 프록시 서버가 액티브업데이트 서버에서 업데이트를 다운로드할 수 있도록 OfficeScan에 프록시 설정을 지정해야 합니다.

관리자는 프록시 설정을 설치하는 동안 지정하지 않고 설치 후에 OfficeScan 웹 콘솔에서 지정할 수 있습니다.

원격 새로 설치를 수행하는 경우에만 프록시 설정이 적용됩니다. 원격 업그레이드의 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

참고

순수 IPv6 엔드포인트에 OfficeScan 서버를 설치하는 경우 IP 주소 간에 변환할 수 있는 이중 스택 프록시 서버를 설치합니다. 그러면 서버를 액티브업데이트 서버에 연결할 수 있습니다.

Web Server

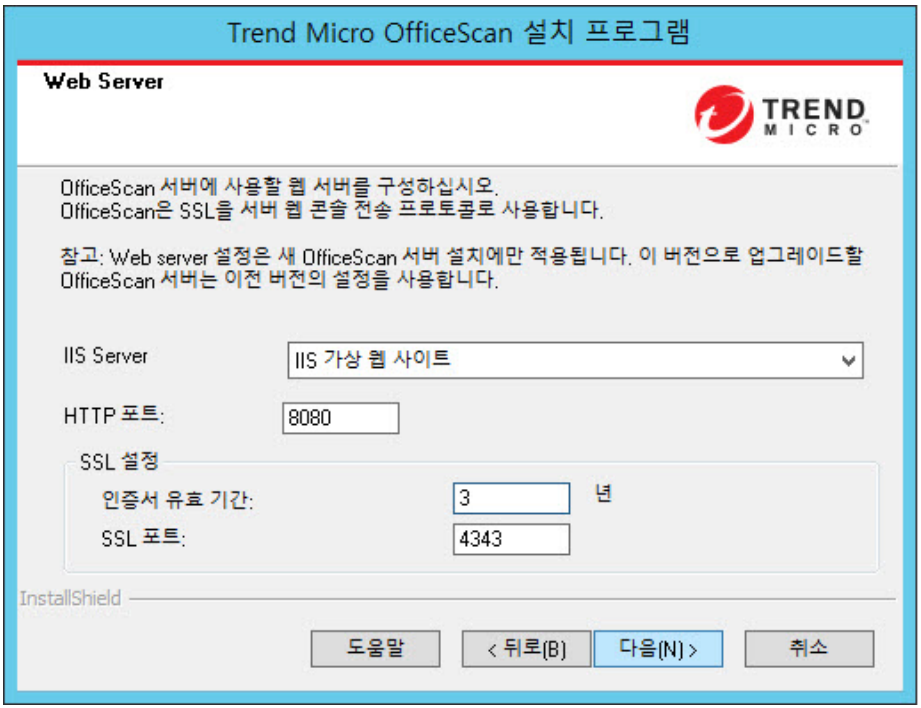

그림 2-6. Web Server 화면

OfficeScan Web Server는 웹 콘솔을 호스팅하고, 관리자가 콘솔 CGI(Common Gateway Interface)를 실행할 수 있도록 하며, 에이전트에서 명령을 받습니다. Web Server에서는 에이전트에서 들어오는 명령을 수신하여 이러한 명령을 에이전트 CGI로 변환한 다음 OfficeScan Master Service로 전달합니다.

원격 새로 설치를 수행하는 경우에만 Web Server 설정이 적용됩니다. 원격 업그레이드를 수행하는 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

IPv6 지원

새로 설치하는 경우 IIS Server를 선택하여 IPv6 지원을 사용하도록 설정합니다.

이 OfficeScan 버전으로 업그레이드하는 경우 업그레이드할 OfficeScan 서버에서 이미 IIS를 사용하고 있어야 합니다.

중요

이전 OfficeScan 서버 설치 패키지를 사용하여 Apache를 설치한 경우 OfficeScan은 업그레이드 프로세스 중에 IIS Web Server를 자동으로 설치하고 구성합니다. Apache 서버를 수동으로 설치했다면 OfficeScan 서버를 업그레이드하기 전에 Apache를 수동으로 제거해야 합니다.

Web Server IIS 지원

- 다음 Microsoft IIS(Internet Information Server) 버전이 필요합니다.
  - Windows Server 2008의 경우 버전 7.0
  - Windows Server 2008 R2의 경우 버전 7.5
  - Windows Server 2012의 경우 버전 8.0
  - Windows Server 2012 R2의 경우 버전 8.5
  - Windows Server 2016의 경우 버전 10.0

  설치가 실패할 수 있으므로 IIS 잠금 응용 프로그램을 실행하는 엔드포인트에는 Web Server를 설치하지 마십시오. 자세한 내용은 IIS 설명서를 참조하십시오.

HTTP 포트

Web Server는 HTTP 포트에서 에이전트 요청을 수신하고 이러한 요청을 OfficeScan Master Service로 전달합니다. 이 서비스는 정보를 지정된 에이전트 통

신 포트에 있는 에이전트에 반환합니다. 설치 프로그램에서는 에이전트 통신 포트 번호를 설치 중에 임의로 생성합니다.

SSL 지원

OfficeScan은 웹 콘솔과 서버 간의 보안 통신을 위해 SSL(Secure Sockets Layer)을 사용합니다. SSL은 해커로부터 보호하는 추가 레이어를 제공합니다. OfficeScan에서는 웹 콘솔에 지정된 암호를 OfficeScan 서버로 보내기 전에 암호화하지만 그럼에도 불구하고 해커가 해당 패킷을 스니핑한 다음 해독하지 않고 "재생"하여 콘솔에 액세스할 수 있습니다. SSL 터널링은 해커가 네트워크를 통과하는 패킷을 몰래 스니핑하지 못하도록 방지합니다.

사용되는 SSL 버전은 Web Server에서 지원하는 버전에 따라 다릅니다.

SSL을 선택하면 설치 프로그램에서 SSL 연결에 대한 요구 사항인 SSL 인증서를 자동으로 만듭니다. 인증서에는 서버 정보, 공개 키 및 개인 키가 들어 있습니다.

SSL 인증서의 유효 기간은 1~20년이어야 합니다. 관리자는 인증서가 만료된 후에도 계속 사용할 수 있습니다. 그러나 해당 인증서를 사용하여 SSL 연결을 요청할 때마다 경고 메시지가 표시됩니다.

SSL을 통한 통신이 작동하는 방법:

1. 관리자는 SSL 연결을 통해 웹 콘솔에서 Web Server로 정보를 보냅니다.
2. Web Server에서는 필요한 인증서를 사용하여 웹 콘솔에 응답합니다.
3. 브라우저에서는 RSA 암호화를 사용하여 키 교환을 수행합니다.
4. 웹 콘솔에서는 RC4 암호화를 사용하여 Web Server로 데이터를 보냅니다.

RSA 암호화가 훨씬 안전하지만 통신 흐름을 더디게 합니다. 따라서 RSA 암호화는 키 교환에만 사용되고 데이터 전송에는 속도가 더 빠른 RC4가 사용됩니다.

Web Server 포트

다음 표에는 Web Server의 기본 포트 번호가 나열되어 있습니다.

표 2-2. OfficeScan Web Server의 포트 번호

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

서버 식별

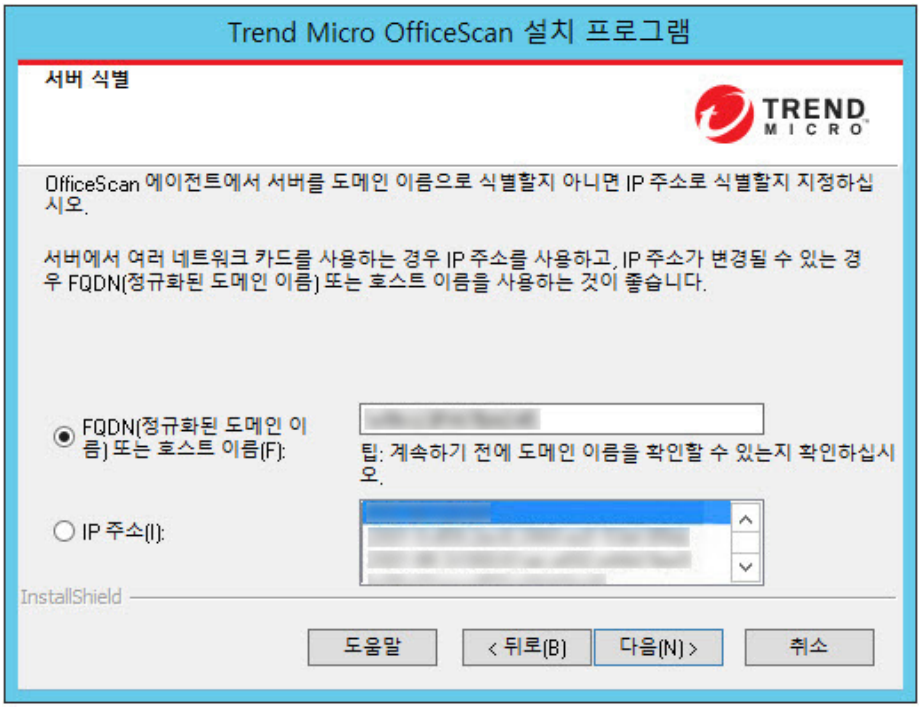

그림 2-7. 서버 식별 화면

이 화면에서 선택한 옵션은 원격 새로 설치를 수행하는 경우에만 적용됩니다. 원격 업그레이드를 수행하는 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

OfficeScan 에이전트에서 서버 컴퓨터를 FQDN(정규화된 도메인 이름), 호스트(도메인) 이름 또는 IP 주소로 식별할지를 지정합니다.

서버 컴퓨터와 에이전트 간 통신은 지정한 IP 주소에 종속됩니다. 에이전트에서 IP 주소를 변경하면 OfficeScan 서버와 통신할 수 없게 됩니다. 통신을 복원하려면 모든 에이전트를 다시 배포해야 합니다. 서버 컴퓨터를 변경되는 호스트 이름으로 식별하는 경우에도 동일한 상황이 적용됩니다.

대부분의 네트워크에서 서버 컴퓨터의 IP 주소는 호스트 이름보다 변경될 가능성이 크므로 일반적으로 서버 컴퓨터는 호스트 이름으로 식별하는 것이 좋습니다.

팁

호스트 이름 대신 IP 주소를 사용하는 관리자의 경우 설치 후 IP 주소(DHCP 서버에서 가져옴)를 변경하지 않는 것이 좋습니다. 관리자는 DHCP 서버에서 가져온 동일한 IP 주소 정보로 IP 주소 구성을 정적으로 설정하여 OfficeScan 에이전트와의 추가적인 통신 문제를 방지할 수 있습니다.

IP 주소 구성을 유지하는 다른 방법은 OfficeScan 서버에 대해서만 IP 주소를 예약하는 것입니다. 이렇게 하면 DHCP가 사용하도록 설정된 경우에도 DHCP 서버가 OfficeScan에 동일한 IP 주소를 할당합니다.

고정 IP 주소를 사용할 경우 서버를 IP 주소로 식별합니다. 또한 서버 컴퓨터에 여러 개의 NIC(네트워크 인터페이스 카드)를 사용하는 경우에는 에이전트와 서버 간 통신이 제대로 이루어지도록 호스트 이름 대신 IP 주소 중 하나를 사용해 보십시오.

IPv6 지원

서버에서 IPv4 및 IPv6 에이전트를 관리하는 경우 IPv4 주소와 IPv6 주소를 둘 다 사용해야 하고 관리자는 해당 서버를 호스트 이름으로 식별해야 합니다. 관리자가 서버를 IPv4 주소로 식별하면 IPv6 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 서버를 호스트 이름 또는 IPv6 주소로 식별할 수 있습니다. 관리자가 서버를 호스트 이름으로 식별하는 경우에는 FQDN(정규화된 도메인 이름)을 사용하는 것이 좋습니다. 순수 IPv6 환경에서는 WINS 서버가 호스트 이름을 해당 IPv6 주소로 인식할 수 없기 때문입니다.

참고

서버의 로컬 설치를 수행하는 경우에만 FQDN을 지정합니다. 원격 설치에 대해서는 FQDN이 지원되지 않습니다.

등록 및 정품 인증

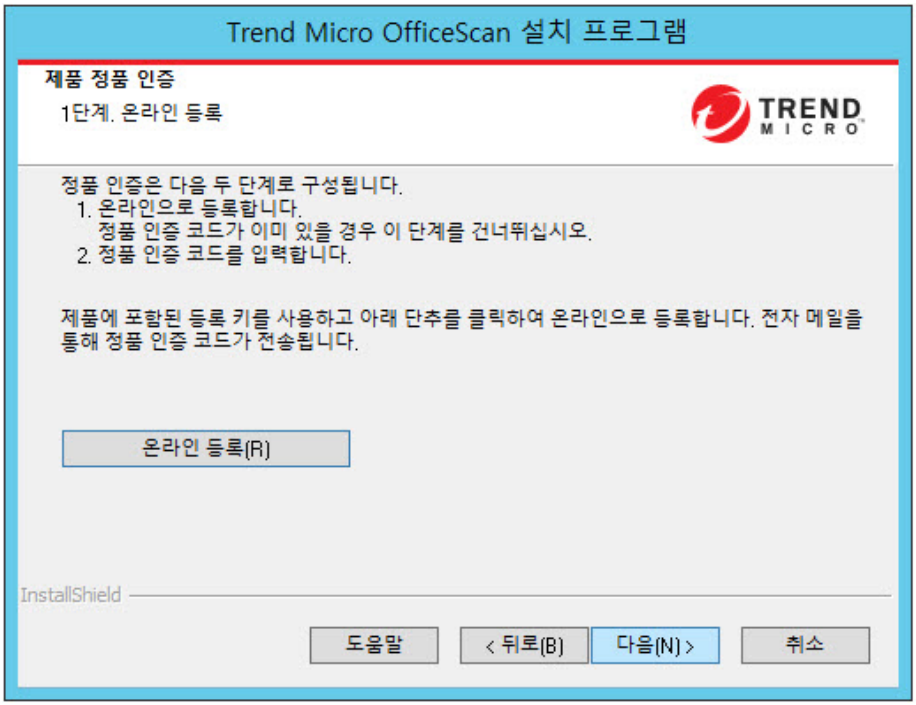

그림 2-8. 제품 정품 인증 - 1단계 화면

제품과 함께 제공된 등록 키를 사용하여 OfficeScan을 등록한 다음 정품 인증 코드를 가져옵니다. 정품 인증 코드를 이미 사용할 수 있는 경우 이 단계를 건너뜁니다.

정품 인증 코드를 가져오려면 **온라인 등록**을 클릭합니다. Trend Micro 등록 웹 사이트가 열립니다. 등록 양식을 완료하면 Trend Micro에서 전자 메일로 정품 인증 코드를 보냅니다. 코드를 받은 후 설치 프로세스를 계속합니다.

순수 IPv6 엔드포인트에 OfficeScan 서버를 설치하는 경우 IP 주소 간에 변환할 수 있는 이중 스택 프록시 서버를 설치합니다. 그러면 서버를 Trend Micro 등록 웹 사이트에 연결할 수 있습니다.

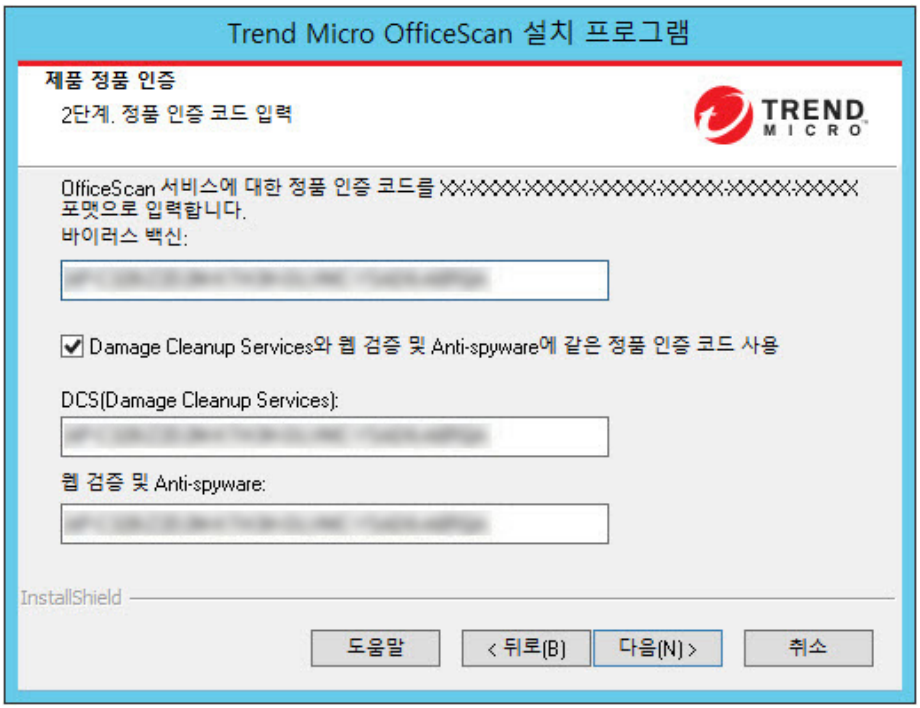

그림 2-9. 제품 정품 인증 - 2단계 화면

정품 인증 코드를 지정합니다. 정품 인증 코드는 대소문자가 구분됩니다.

정품 인증 코드가 모든 서비스에 대해 유효한 경우

1. **바이러스 방역** 텍스트 상자에 정품 인증 코드를 입력합니다.
2. **Damage Cleanup Services와 웹 검증 및 Anti-spyware에 같은 정품 인증 코드 사용**을 선택합니다.
3. **다음**을 클릭하고 라이선스 정보를 확인합니다.

OfficeScan 에이전트 배포

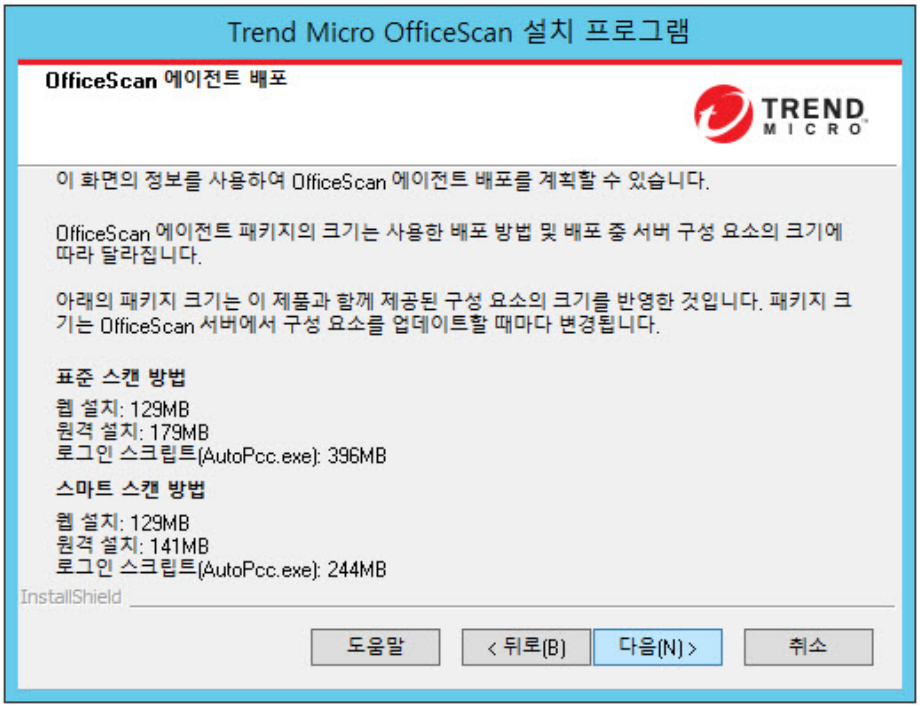

그림 2-10. OfficeScan 에이전트 배포 화면

OfficeScan 에이전트를 설치하거나 업그레이드하는 방법에는 몇 가지가 있습니다. 이 화면에는 서로 다른 배포 방법과 필요한 대략적인 네트워크 대역폭이 나열되어 있습니다.

이 화면을 통해, 대상 엔드포인트에 에이전트를 배포할 때 서버에 필요한 크기와 대역폭 사용량을 예측할 수 있습니다.

참고

이러한 모든 설치 방법에는 대상 엔드포인트의 로컬 관리자 또는 도메인 관리자 권한이 필요합니다.

통합 스마트 보호 서버 설치

참고

로컬 업그레이드 설치 시 IIS 가상 웹 사이트를 사용하는 경우에는 이 화면이 표시되지 않습니다.

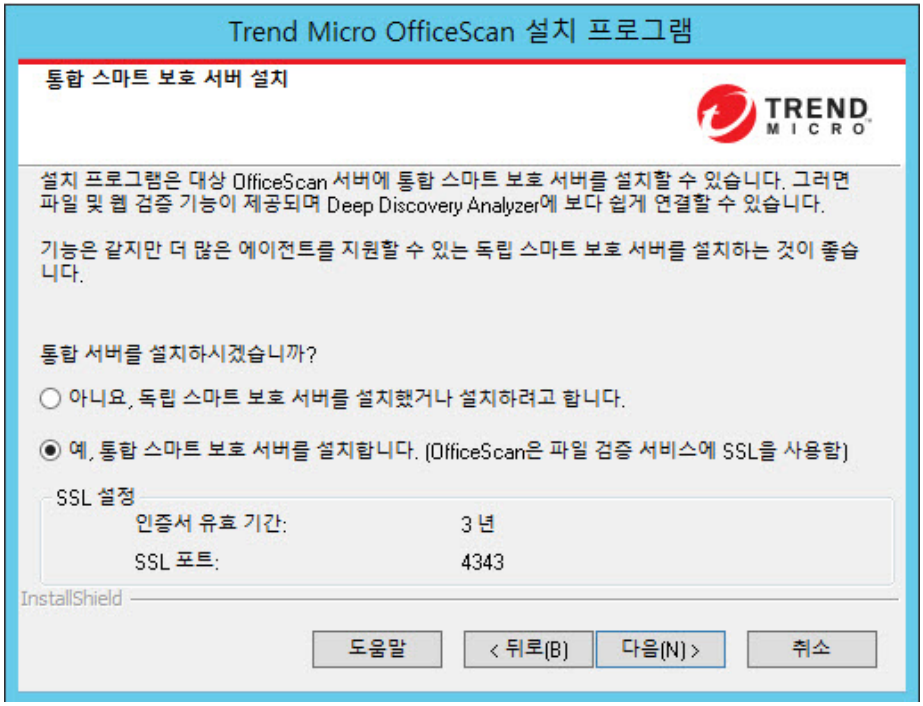

그림 2-11. 통합 스마트 보호 서버 설치 화면

설치 프로그램은 대상 엔드포인트에 통합 스마트 보호 서버를 설치할 수 있습니다. 통합 서버는 스마트 스캔을 사용하는 에이전트에 파일 검증 서비스를 제공하고, 웹 검증 정책이 적용되는 에이전트에 웹 검증 서비스를 제공합니다. OfficeScan 웹 콘솔에서 통합 서버를 관리합니다.

Trend Micro에서는 통합 서버와 기능은 같지만 더 많은 에이전트에 서비스를 제공할 수 있는 독립 스마트 보호 서버를 설치하는 것을 권장합니다. 독립 서버는 별도로 설치되고 자체 관리 콘솔을 포함합니다. 독립 서버에 대한 자세한 내용은 *Trend Micro 스마트 보호 서버 관리자 안내서*를 참조하십시오.

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. 에이전트에 대한 스마트 보호 소스 구성에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

파일 검증 서비스용 에이전트 연결 프로토콜

OfficeScan 에이전트는 HTTP를 사용하여 통합 스마트 보호 서버의 파일 검증 서비스에 연결할 수 있습니다. HTTPS를 사용하면 보다 안전하게 연결할 수 있지만 HTTP가 대역폭을 더 적게 사용합니다.

참고

엔드포인트가 프록시 서버를 통해 통합 서버에 연결되는 경우 웹 콘솔에서 내부 프록시 설정을 구성합니다. 프록시 설정 구성에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

파일 검증 서비스에 사용되는 포트 번호는 OfficeScan 서버에서 사용하는 웹 서버에 따라 다릅니다. 자세한 내용은 Web Server 페이지 2-14를 참조하십시오.

HTTP 포트는 설치 화면에 표시되지 않습니다. HTTPS 포트는 표시되지만 구성은 선택 사항입니다.

표 2-3. 통합 스마트 보호 서버의 파일 검증 서비스에 사용되는 포트

WEB SERVER 및 설정	파일 검증 서비스에 사용되는 포트	
	HTTP	HTTPS (SSL)
IIS 기본 웹 사이트	80	443
IIS 가상 웹 사이트	8080	4343

통합 서버가 설치되어 있지 않음

새로 설치를 수행할 때 통합 서버 설치를 선택하지 않은 경우

- 표준 스캔이 기본 검색 방법이 됩니다.
- 별도의 설치 화면에서 웹 검증 정책을 사용하도록 설정한 경우(자세한 내용은 웹 검증 기능 페이지 2-40 참조) OfficeScan에서는 스마트 보호 서버가 설치되지 않았다고 가정하므로 에이전트가 웹 검증 쿼리를 보낼 수 없습니다.

OfficeScan 설치 후 독립 서버를 사용할 수 있는 경우 OfficeScan 웹 콘솔에서 다음 작업을 수행합니다.

- 검색 방법을 스마트 스캔으로 변경합니다.
- 에이전트가 파일 및 웹 검증 쿼리를 서버에 보낼 수 있도록 독립 서버를 스마트 보호 소스 목록에 추가합니다.

통합 서버를 사용하지 않도록 설정한 OfficeScan 10.x 서버에서 업그레이드하는 경우 통합 서버가 설치되지 않습니다. OfficeScan 에이전트는 검색 방법과 쿼리를 보내는 스마트 보호 소스를 유지합니다.

설치 대상

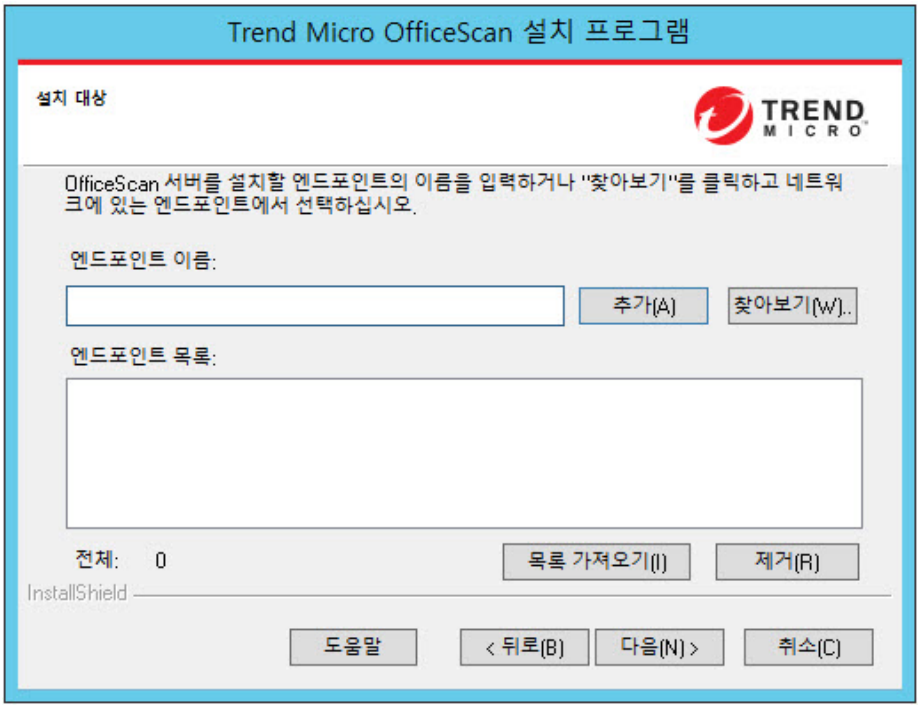

그림 2-12. 설치 대상 화면

OfficeScan이 설치되는 대상 엔드포인트를 지정합니다. 엔드포인트의 호스트 이름 또는 IP 주소를 수동으로 입력합니다. 네트워크에서 엔드포인트를 검색하려면 **찾아보기**를 클릭합니다.

목록 가져오기를 클릭하여 텍스트 파일에서 엔드포인트 이름을 가져옵니다. 여러 엔드포인트에 동시에 설치하고 모든 엔드포인트가 분석을 통과하는 경우 설치 프로그램에서 텍스트 파일에 나열된 순서대로 OfficeScan 서버를 설치합니다.

텍스트 파일에서 다음을 수행합니다.

- 줄당 하나의 엔드포인트 이름을 지정합니다.
- UNC(Unified Naming Convention) 포맷(예: ₩₩test)을 사용합니다.
- a-z, A-Z, 0-9, 마침표(.) 및 하이픈(-) 문자만 사용합니다.

예:

₩₩domain1₩test-abc

₩₩domain2₩test-123

원격 설치를 계속하는 데 필요한 팁:

- 대상 엔드포인트에 대한 관리자 권한을 얻습니다.
- 엔드포인트의 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록해 둡니다.
- 대상 엔드포인트가 OfficeScan 서버 설치에 대한 시스템 요구 사항을 만족하는지 확인합니다.
- Microsoft IIS Server를 Web Server로 사용할 경우 엔드포인트에 버전 7.0 이상이 있는지 확인합니다.
- 설치 프로그램을 시작한 엔드포인트를 대상 엔드포인트로 지정하지 마십시오. 해당 엔드포인트에서 로컬 설치를 실행하십시오.

대상 엔드포인트를 지정한 후 **다음**을 클릭합니다. 설치 프로그램에서 엔드포인트가 OfficeScan 설치 요구 사항을 만족하는지 확인합니다.

대상 엔드포인트 분석

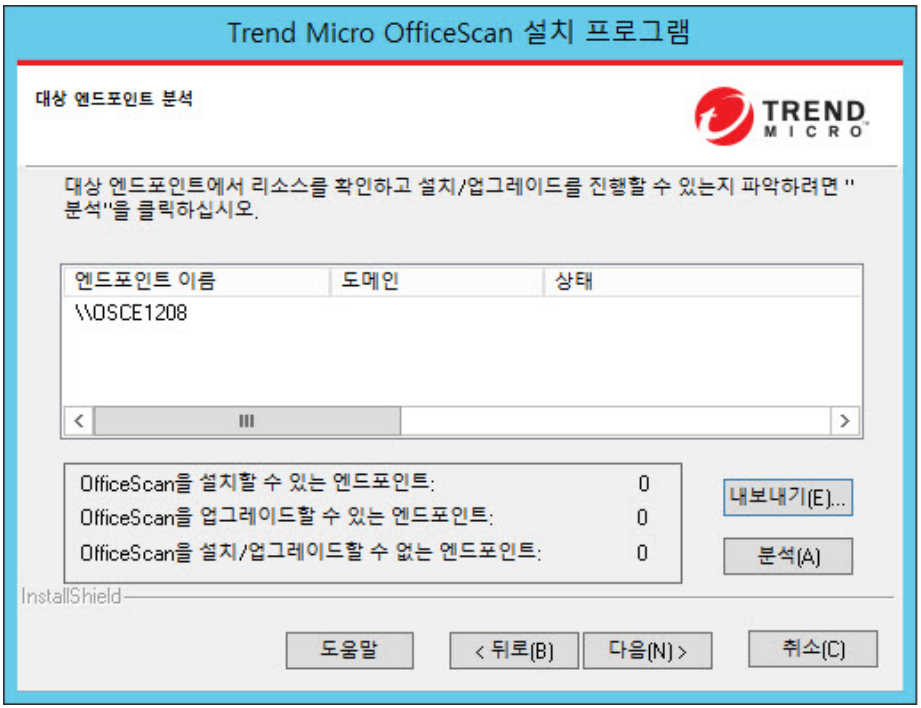

그림 2-13. 대상 엔드포인트 분석 화면

중요

설치 프로그램은 Apache Web Server를 사용하는 OfficeScan 서버의 원격 업그레이드를 지원하지 않습니다. OfficeScan의 원격 업그레이드를 시도하기 전에 Apache Web Server를 수동으로 제거해야 합니다.

원격 설치를 진행하기 전에 설치 프로그램에서는 선택한 대상 엔드포인트에 OfficeScan 서버를 설치할 수 있는지 확인해야 합니다. 분석을 시작하려면 **분석**을 클릭합니다. 대상 엔드포인트에 로그온하는 데 사용되는 관리자 사용자 이름 및 암호를 입력하라는 메시지가 표시될 수 있습니다. 분석 후에는 결과가 화면에 표시됩니다.

중요

설치 프로그램은 서버 분석 중 랜섬웨어 위협으로부터 최적화된 보호를 받을 수 있도록 랜섬웨어 보호 설정을 업데이트하라는 메시지를 표시합니다.

업데이트된 설정을 적용하면 이미 동작 모니터링이 사용되도록 설정된 에이전트의 설정만 변경됩니다.

여러 엔드포인트에 설치하는 경우 하나 이상의 엔드포인트가 분석을 통과하면 설치가 진행됩니다. OfficeScan 서버가 해당 엔드포인트에 설치되고 분석을 통과하지 못한 엔드포인트는 무시됩니다.

원격 설치 중에 설치 진행률은 설치 프로그램을 시작한 엔드포인트에만 표시되고 대상 엔드포인트에는 표시되지 않습니다.

OfficeScan 에이전트 설치

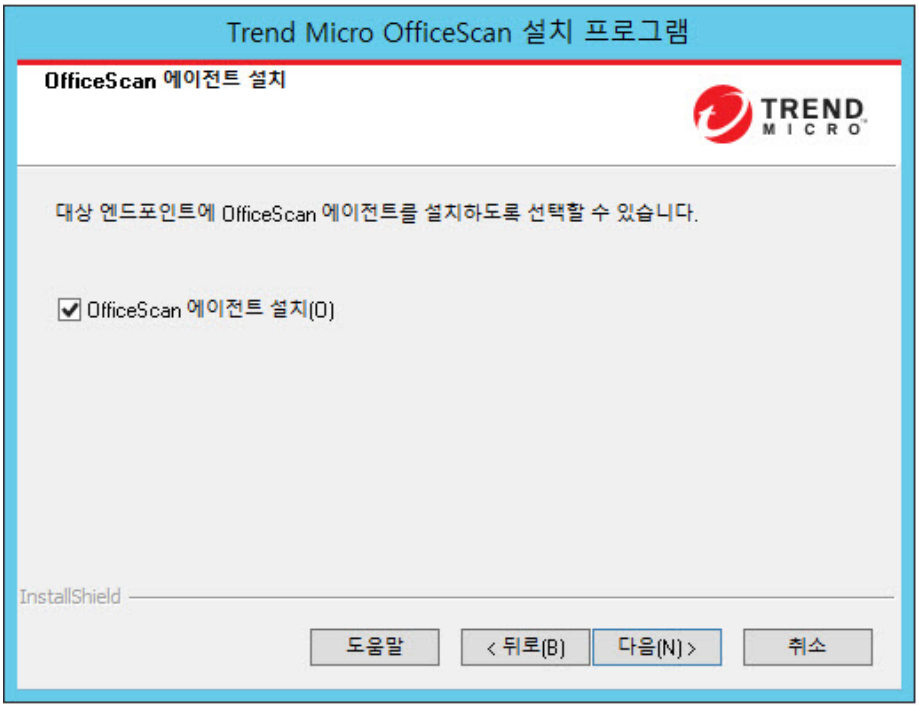

그림 2-14. OfficeScan 에이전트 화면 설치

대상 서버에 OfficeScan 에이전트를 설치하도록 선택할 수 있습니다.

OfficeScan 에이전트

OfficeScan 에이전트 프로그램은 보안 위험으로부터 실제적인 보호를 제공합니다. 따라서 보안 위험으로부터 OfficeScan 서버 엔드포인트를 보호하려면 OfficeScan 에이전트 프로그램이 있어야 합니다. 서버 설치 중에 OfficeScan 에이전트를 설치하도록 선택하면 서버가 자동으로 보호됩니다. 또한 서버 설치 후에 OfficeScan 에이전트를 설치하는 추가 작업을 수행하지 않아도 됩니다.

참고

서버 설치 후 OfficeScan 에이전트를 네트워크의 다른 엔드포인트에 설치합니다. OfficeScan 에이전트 설치 방법에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

Trend Micro 또는 타사 엔드포인트 보안 소프트웨어가 현재 서버 컴퓨터에 설치되어 있는 경우 OfficeScan이 해당 소프트웨어를 자동으로 제거하고 OfficeScan 에이전트로 바꾸지 못할 수도 있습니다. OfficeScan이 자동으로 제거하는 소프트웨어 목록을 보려면 지원 센터에 문의하십시오. 소프트웨어를 자동으로 제거할 수 없는 경우에는 OfficeScan 설치를 진행하기 전에 소프트웨어를 수동으로 제거합니다.

스마트 보호 네트워크

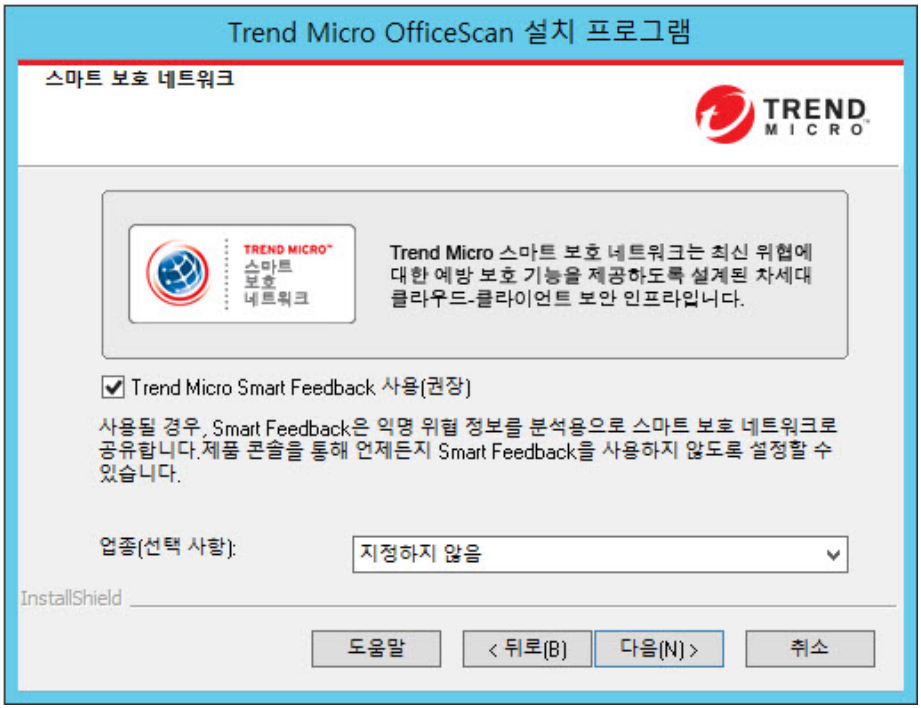

그림 2-15. 스마트 보호 네트워크 화면

Trend Micro™ 스마트 보호 네트워크는 고객을 보안 위험과 웹 위협으로부터 보호하기 위해 설계된 차세대 클라우드-클라이언트 콘텐츠 보안 인프라입니다. 사용자가 네트워크에 있는지, 집에 있는지 또는 일하고 있는지에 관계없이 경량 에이전트를 사용하여 전자 메일, 웹 및 파일 검증 기술에 대해 고유한 인 더 클라우드 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. 스마트 보호 네트워크 솔루션은 in-the-cloud 보호를 위해 스마트 보호 네트워크를 활용합니다.

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

관리자 계정 암호

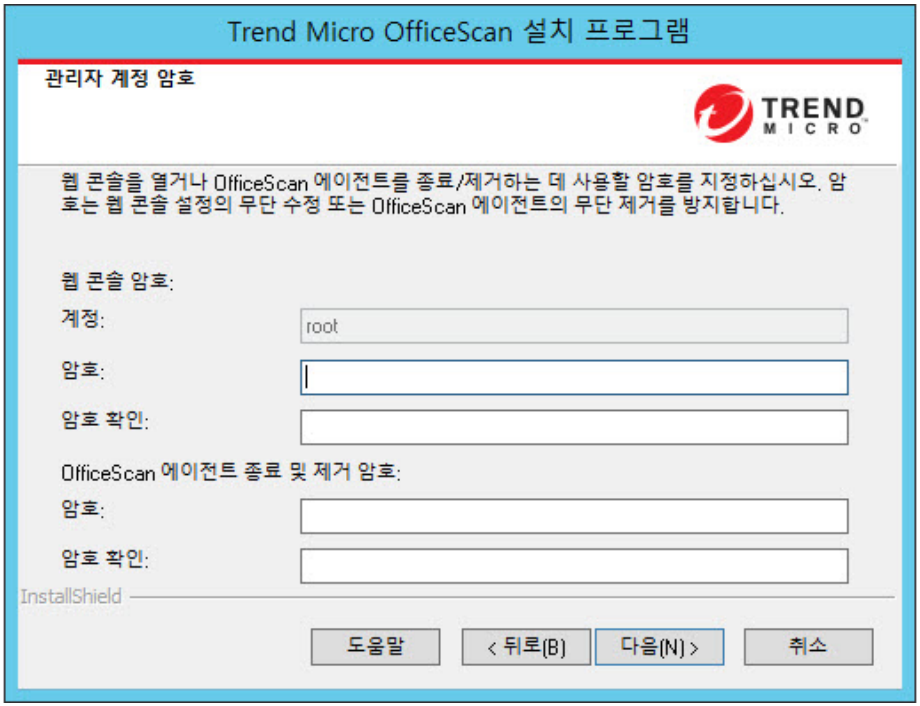

그림 2-16. 관리 계정 암호 화면

웹 콘솔에 액세스하고 OfficeScan 에이전트를 종료 및 제거하는 데 사용할 암호를 지정합니다.

웹 콘솔 액세스

설치 프로그램은 설치 중에 루트 계정을 만듭니다. 루트 계정은 모든 OfficeScan 웹 콘솔 기능에 대한 전체 액세스 권한을 갖습니다. 이 계정을 사용하여 로그온하면 관리자는 다른 사용자가 웹 콘솔에 로그온할 때 사용할 수 있는 사용자 정의 사용자 계정을 만들 수 있습니다. 사용자는 자신의 계정에 부여된 액세스 권한에 따라 하나 또는 여러 개의 웹 콘솔 기능을 구성하거나 볼 수 있습니다.

OfficeScan 관리자만 알고 있는 암호를 지정합니다. 잊어버린 암호를 초기화하는 데 지원이 필요한 경우 지원 센터에 문의하십시오.

OfficeScan 에이전트 종료 및 제거

OfficeScan 에이전트의 무단 제거 또는 종료를 방지하기 위해 암호를 지정합니다. 에이전트 기능에 문제가 있는 경우에만 에이전트를 제거하거나 종료하고 즉시 설치/다시 로드합니다.

OfficeScan 에이전트 설치

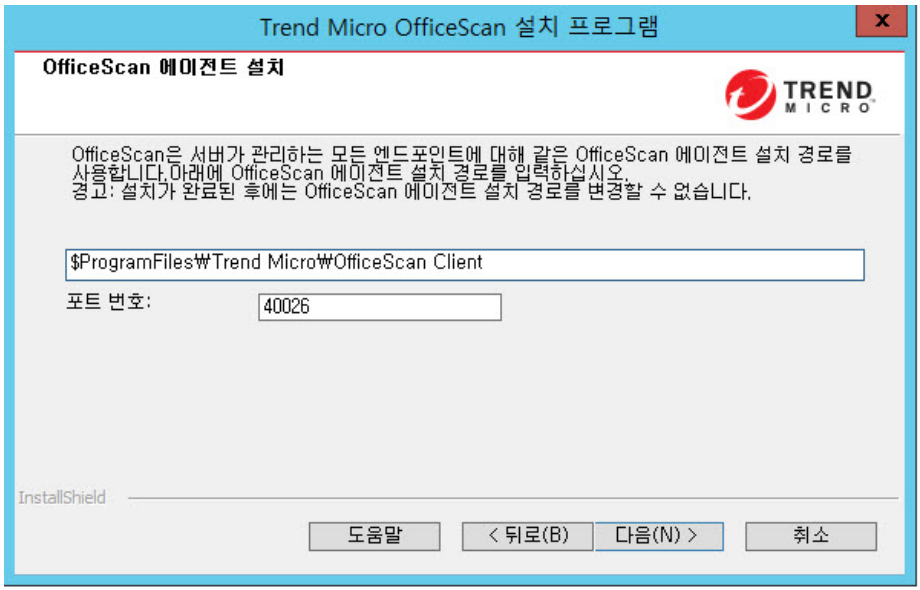

그림 2-17. OfficeScan 에이전트 설치 화면

기본 에이전트 설치 설정을 적용하거나 다른 OfficeScan 에이전트 설치 경로를 지정합니다. 설치 디렉터리에 디스크 공간이 부족한 경우 이 경로를 변경합니다.

팁

Trend Micro에서는 기본 설정을 사용할 것을 권장합니다.

다른 설치 경로를 지정할 경우 고정 경로를 입력하거나 변수를 사용합니다. 지정한 경로에 에이전트에는 없는 디렉터리가 포함되어 있으면 설치 프로그램에서는 에이전트를 설치할 때 해당 디렉터리를 자동으로 만듭니다.

고정 OfficeScan 에이전트 설치 경로를 입력하려면 드라이브 문자를 포함한 드라이브 경로를 입력합니다. 예를 들면 C:₩Program Files₩Trend Micro ₩OfficeScan Agent입니다.

참고

OfficeScan 서버 설치가 완료된 후에는 OfficeScan 에이전트 설치 경로를 수정할 수 없습니다. 설치된 모든 OfficeScan 에이전트에서 동일한 설치 경로를 사용합니다.

OfficeScan 에이전트 설치 경로에 변수를 지정할 때 다음을 사용합니다.

- $BOOTDISK: 엔드포인트가 부팅되는 하드 디스크의 드라이브 문자(기본적으로 C:₩)
- $WINDIR: Windows 디렉터리(기본적으로 C:₩Windows)
- $ProgramFiles: Windows에서 자동으로 설치되며 소프트웨어를 설치하는 데 일반적으로 사용되는 Program Files 디렉터리(기본적으로 C:₩Program Files)

또한 이 화면에서 다음을 구성합니다.

- **포트 번호**: 설치 프로그램에서는 이 포트 번호를 임의로 생성하며 OfficeScan 서버에서 에이전트와 통신하는 데 사용합니다. 기본값을 적용하거나 새 값을 입력합니다.
- **보안 수준**: OfficeScan 설치 후 OfficeScan 콘솔에서 보안 수준을 변경합니다.

  에이전트 > **에이전트 관리**으로 이동합니다. **설정** > **권한 및 기타 설정** > **기타 설정**을 클릭합니다.

  - **보통**: 이 권한은 모든 사용자("Everyone" 사용자 그룹)에게 에이전트 프로그램 디렉터리 및 에이전트 레지스트리 항목에 대한 모든 권한을 부여합니다.

- **높음**: 에이전트 설치 디렉터리는 Program Files 폴더의 권한을 상속하고, 에이전트의 레지스트리 항목은 `HKLM\Software` 키에서 권한을 상속합니다. 대부분의 Active Directory 구성에서 이 권한은 "일반" 사용자(관리자 권한이 없는 사용자)를 읽기 전용 액세스로 자동으로 제한합니다.

OfficeScan 방화벽

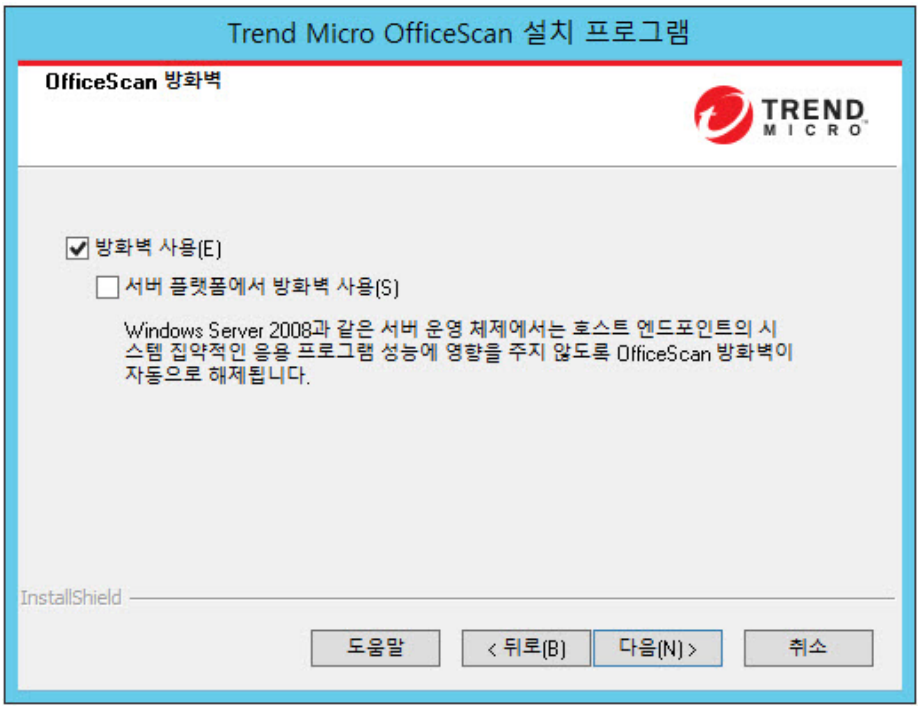

그림 2-18. OfficeScan 방화벽 화면

이 화면은 바이러스 방역 서비스를 활성화한 후에만 표시됩니다.

OfficeScan 방화벽

OfficeScan 방화벽은 상태 기반 검사, 고성능 네트워크 바이러스 검색 및 제거를 통해 네트워크의 에이전트와 서버를 보호합니다. IP 주소, 포트 번호 또는 프로토콜에 따라 연결을 필터링할 규칙을 작성한 다음 여러 사용자 그룹에 적용합니다.

선택적으로 방화벽을 사용하지 않도록 설정하고 나중에 OfficeScan 서버 웹 콘솔에서 방화벽을 사용하도록 설정합니다.

선택적으로 서버 플랫폼에서 방화벽을 사용하도록 설정합니다. 업그레이드 시 서버 플랫폼에서 방화벽 서비스가 이미 사용되도록 설정되어 있으면 업그레이드 후 OfficeScan에서 방화벽 서비스를 해제하지 않도록 **서버 플랫폼에서 방화벽 사용**을 선택합니다.

Anti-spyware 기능

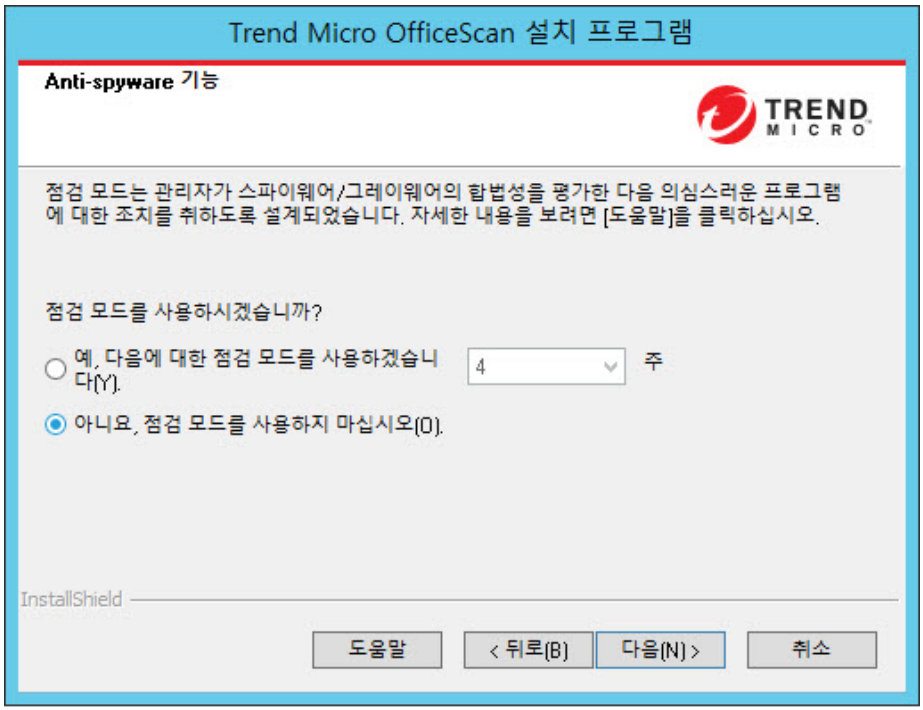

그림 2-19. Anti-spyware 기능 화면

이 화면은 웹 검증 및 Anti-spyware 서비스를 활성화한 후에만 표시됩니다.

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 Micro에서는 Trend Micro에서 스파이웨어/그레이웨어로 탐지한 항목의 평가를 감한하는 점검 모드를 제공합니다. 그러면 관리자는 적절한 처리 방법을 구성할 수 있습니다. 예를 들어, 보안 위험으로 탐지된 스파이웨어/그레이웨어를 스파이웨어/그레이웨어 승인된 목록에 추가합니다.

설치 후에 점검 모드에서 취할 수 있는 권장 조치는 *관리자 안내서*를 참조하십시오.

이 화면에서 주 수를 지정하여 특정 기간에만 적용되도록 점검 모드를 구성합니다. 설치 후 웹 콘솔에서 점검 모드 설정을 변경합니다 (**에이전트 > 글로벌 에이전트 설정**, **스파이웨어/그레이웨어 설정** 섹션).

웹 검증 기능

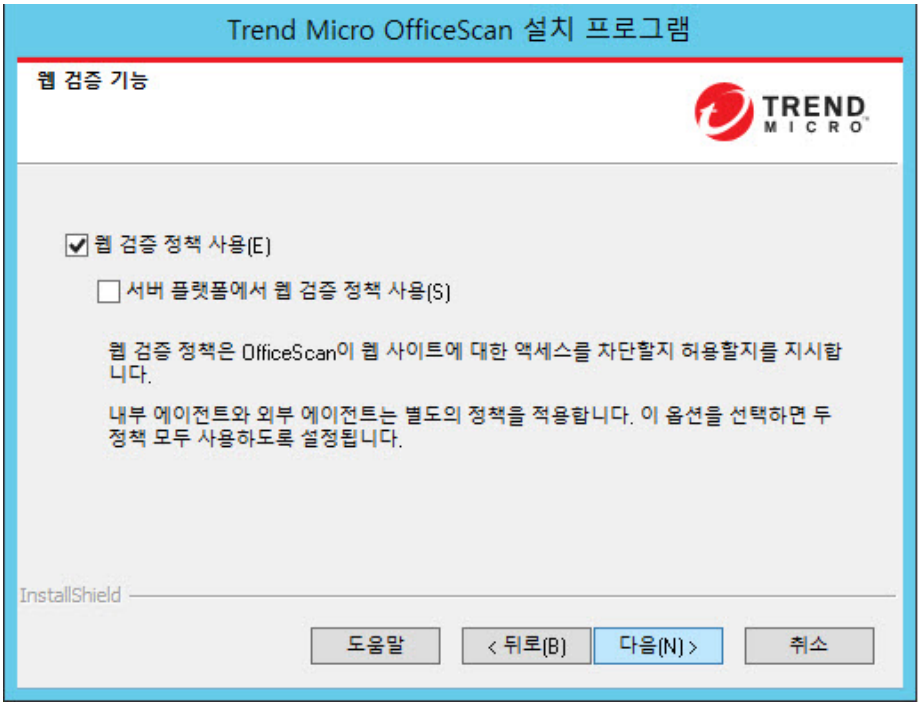

그림 2-20. 웹 검증 기능 화면

웹 검증 정책은 OfficeScan이 웹 사이트에 대한 액세스를 차단할지 허용할지를 지시합니다. 정책에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

웹 검증 정책 사용을 선택하면 데스크톱 플랫폼(예: Windows XP, Vista, Windows 7, Windows 8 및 Windows 8.1)에 설치된 내부 및 외부 에이전트에 대한 정책을 사

용할 수 있습니다. 서버 플랫폼(예: Windows Server 2003, Windows Server 2008 및 Windows Server 2012)에 데스크톱 플랫폼과 동일한 수준의 웹 위협 보안이 필요한 경우 **서버 플랫폼에서 웹 검증 정책 사용**을 선택합니다.

OfficeScan 에이전트은 웹 콘솔의 **엔드포인트 위치** 화면에 구성된 위치 기준을 사용하여 해당 위치와 적용할 정책을 결정합니다. OfficeScan 에이전트는 위치가 변경될 때마다 정책을 전환합니다.

설치 후 웹 콘솔에서 웹 검증 정책 설정을 구성합니다. OfficeScan 관리자는 일반적으로 외부 에이전트에 대해 더 엄격한 정책을 구성합니다.

웹 검증 정책은 OfficeScan 에이전트 트리의 개별 설정입니다. 특정 정책을 모든 에이전트, 에이전트 그룹 또는 개별 에이전트에 적용합니다.

웹 검증 정책을 사용하는 경우 스마트 보호 서버(통합 또는 독립)를 설치하고 이를 OfficeScan 웹 콘솔의 스마트 보호 소스 목록에 추가합니다. OfficeScan 에이전트는 웹 검증 쿼리를 서버에 전송하여 사용자가 액세스 중인 웹 사이트의 안전성을 확인합니다.

참고

통합 서버는 OfficeScan 서버와 함께 설치됩니다. 자세한 내용은 통합 스마트 보호 서버 설치 페이지 2-22를 참조하십시오. 독립 서버는 별도로 설치됩니다.

서버 인증 인증서

설치 프로그램은 설치 중에 기존 인증 인증서에 대한 검색을 시도합니다. 기존 인증서가 있는 경우 OfficeScan은 해당 파일을 **서버 인증 인증서** 화면에 매핑합니다. 기존 인증서가 없을 경우에는 OfficeScan이 **새 인증 인증서 생성** 옵션을 기본적으로 사용합니다.

참고

원격 업그레이드 설치 중 **서버 인증 인증서** 화면은 OfficeScan 10.6 SP3 서버를 업그레이드하는 경우에만 나타납니다.

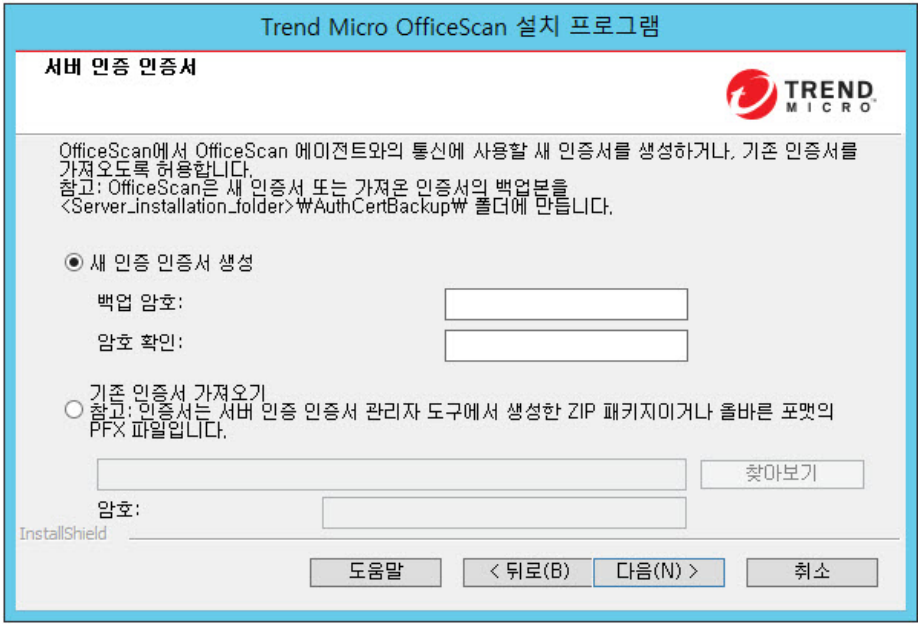

그림 2-21. 새 인증서를 위한 서버 인증 인증서 화면

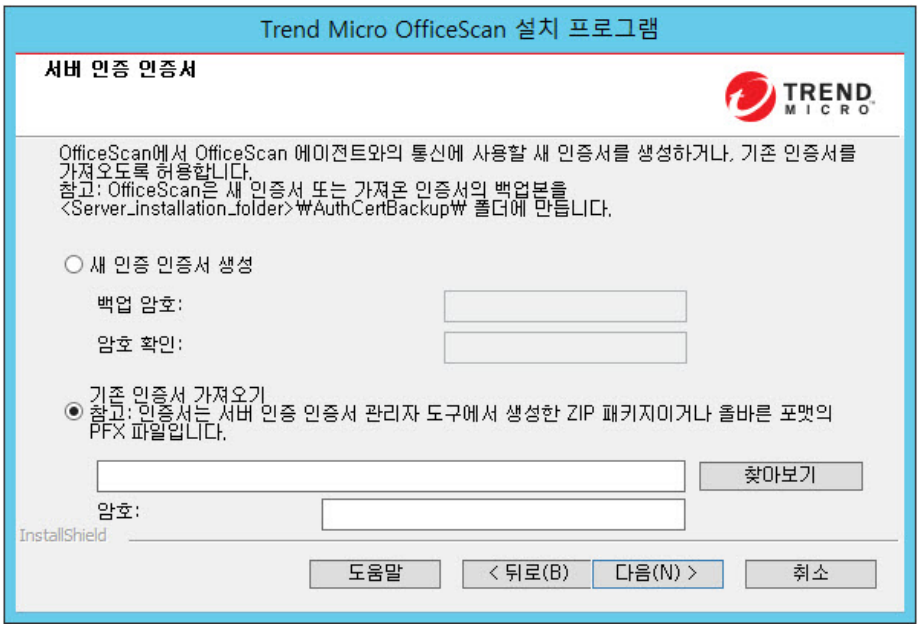

그림 2-22. 기존 인증서를 위한 서버 인증 인증서 화면

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.

OfficeScan이 설치 중에 인증 인증서를 생성하거나 관리자가 다른 OfficeScan 서버에서 기존 인증 인증서를 가져올 수 있습니다.

팁

인증서를 백업할 때는 암호로 인증서를 암호화하는 것이 좋습니다.

OfficeScan 프로그램 바로 가기

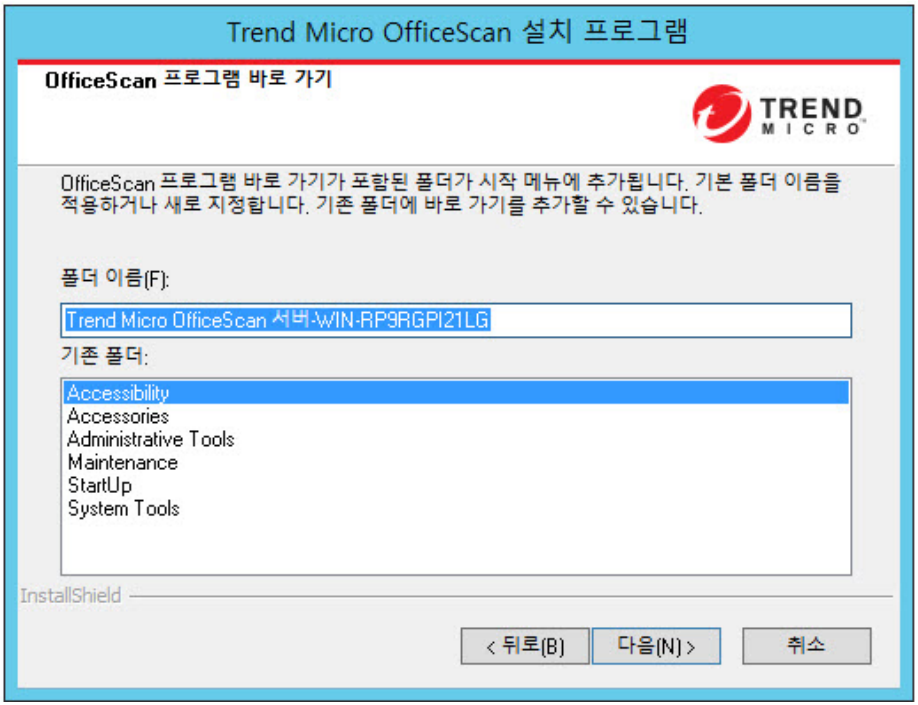

그림 2-23. OfficeScan 프로그램 바로 가기 화면

기본 폴더 이름을 적용하거나 새 폴더 이름을 지정하거나 설치 프로그램에서 프로그램 바로 가기를 추가하는 기존 폴더를 선택합니다.

설치 정보

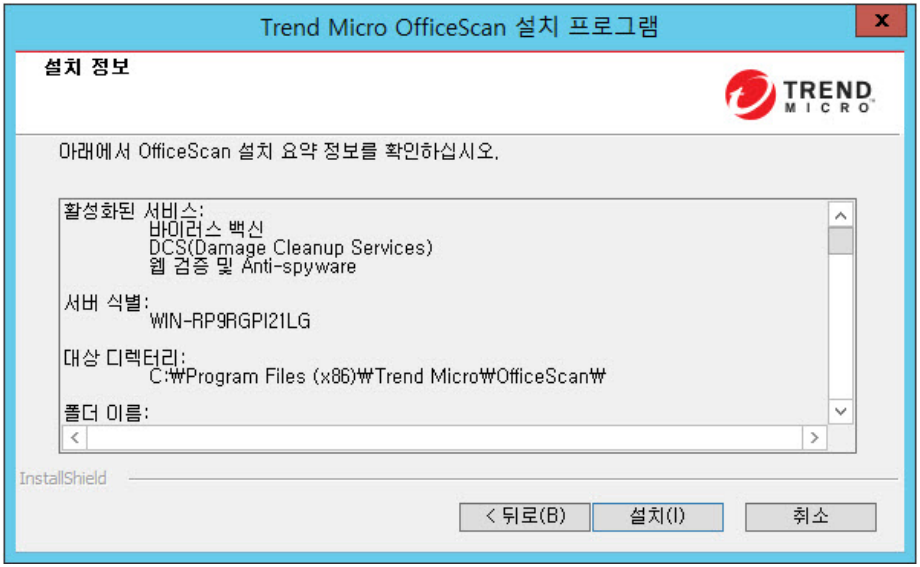

그림 2-24. 설치 정보 화면

이 화면은 설치 설정에 대한 요약을 제공합니다. 설치 정보를 검토하고 **뒤로**를 클릭하여 설정이나 옵션을 변경합니다. 설치를 시작하려면 **설치**를 클릭합니다.

InstallShield 마법사 완료

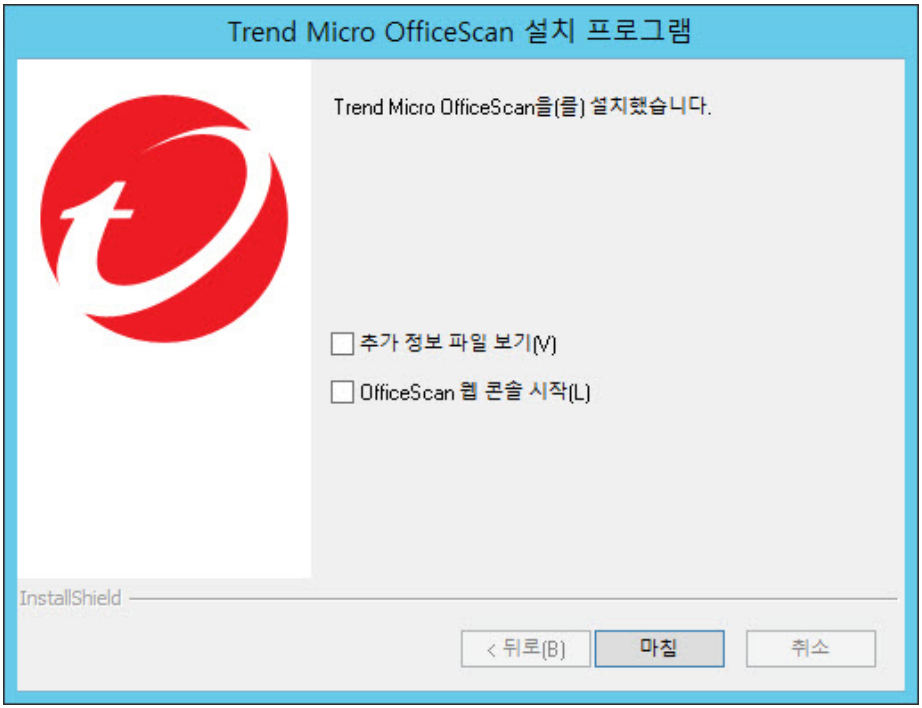

그림 2-25. InstallShield 마법사 완료 화면

설치가 완료되면 추가 정보 파일에서 제품 및 알려진 문제점에 대한 기본 정보를 확인합니다.

관리자는 웹 콘솔을 시작하여 OfficeScan 설정 구성을 시작할 수 있습니다.

장 3

OfficeScan 업그레이드

이 장에서는 Trend Micro™ OfficeScan™ 업그레이드 단계에 대해 설명합니다.

이 장의 내용:

- OfficeScan 서버 및 에이전트 업그레이드 페이지 3-2
- 로컬 업그레이드 수행 페이지 3-19
- 원격 업그레이드 수행 페이지 3-60

OfficeScan 서버 및 에이전트 업그레이드

기존에 구성된 OfficeScan 10.x 또는 11.x 서버에서 설치 프로그램을 실행하면 서버가 업그레이드됩니다. 엔드포인트에 Plug-in Manager가 설치되어 있는 경우 Plug-in Manager도 버전 2.3로 업그레이드됩니다. Plug-in Manager가 설치되어 있지 않은 경우 버전 2.3이 자동으로 설치됩니다. 이 Plug-in Manager 버전은 OfficeScan에 위젯 기능을 제공합니다.

OfficeScan 서버에서 에이전트가 OfficeScan 에이전트 프로그램을 업그레이드할 수 있도록 허용하는 경우 서버 설치가 완료된 후 설치 패키지는 즉시 모든 에이전트를 업그레이드합니다.

OfficeScan 서버가 에이전트 업그레이드를 차단하는 경우 네트워크 대역폭 및 OfficeScan 서버에서 관리하는 에이전트 수에 따라 그룹별로 에이전트 업그레이드를 수행합니다.

팁

모든 OfficeScan 구성 요소가 업데이트되도록 업그레이드 후 OfficeScan 에이전트를 다시 시작하는 것이 좋습니다.

OfficeScan 서버 및 에이전트를 업그레이드하기 전

OfficeScan 서버 및 에이전트를 업그레이드하기 전에 다음 사항에 유의하십시오.

1. 설치 패키지에는 OfficeScan 방화벽 드라이버에 대한 업데이트가 포함되어 있습니다. 현재 OfficeScan 버전에서 OfficeScan 방화벽을 사용하도록 설정한 경우 패키지를 배포하면 에이전트 엔드포인트에서 다음과 같은 중단이 발생할 수 있습니다.

   - 방화벽 드라이버 업데이트가 시작되면 일시적으로 에이전트 엔드포인트가 네트워크에서 연결이 끊어집니다. 연결이 끊어지기 전에 이에 대한 메시지가 사용자에게 표시되지 않습니다.

     OfficeScan 웹 콘솔에 대한 옵션(기본적으로 사용하도록 설정됨)이 에이전트 엔드포인트가 다시 시작될 때까지 방화벽 드라이버 업데이트를 연기합니다. 연결이 끊어지는 문제를 방지하려면 이 옵션이 사용하도록 설정되어 있는지 확인합니다.

이 옵션의 상태를 확인하려면 다음을 수행합니다.

a. • OfficeScan 10.x 버전의 경우 **네트워크로 연결된 컴퓨터** > **글로벌 클라이언트 설정**으로 이동합니다.

   • OfficeScan 11.x 버전의 경우 **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.

b. **방화벽 설정** 섹션으로 이동합니다. 옵션은 **시스템 다시 시작 후 OfficeScan 방화벽 드라이버만 업데이트**입니다.

- 패키지를 배포한 후 OfficeScan TDI 드라이버의 이전 버전은 에이전트 엔드포인트에 계속 남아있으며, 새 버전은 엔드포인트를 다시 시작한 후에야 로드됩니다. 즉시 다시 시작하지 않을 경우 OfficeScan 에이전트에 문제가 발생할 가능성이 있습니다.

  다시 시작 알림 메시지를 표시하는 옵션이 웹 콘솔에 사용하도록 설정되어 있는 경우 다시 시작하라는 메시지가 표시됩니다. 그러나 나중에 다시 시작하기로 선택한 경우 메시지가 다시 표시되지 않습니다. 이 옵션을 사용하지 않도록 설정한 경우 해당 알림 메시지가 표시되지 않습니다.

  다시 시작 알림 메시지를 표시하는 옵션은 기본적으로 사용하도록 설정되어 있습니다. 이 옵션의 상태를 확인하려면 다음을 수행합니다.

  - OfficeScan 10.x 버전의 경우:

    a. **네트워크로 연결된 컴퓨터** > **글로벌 클라이언트 설정**으로 이동합니다.

    b. **경고 설정** 섹션으로 이동합니다. 이 옵션은 **클라이언트 컴퓨터를 다시 시작하여 커널 모드 드라이버를 로드해야 하는 경우 알림 메시지 표시**입니다.

  - OfficeScan 11.x 버전의 경우:

    a. **에이전트** > **글로벌 에이전트 설정**으로 이동합니다.

    b. **경고 설정** 섹션으로 이동합니다. 옵션은 **엔드포인트를 다시 시작하여 커널 모드 드라이버를 로드해야 하는 경우 알림 메시지 표시**입니다.

2. 다음의 경우 OfficeScan 서버를 이 버전으로 업그레이드할 수 없습니다.

   - 서버 업그레이드 시 에이전트가 로그인 스크립트(AutoPcc.exe)를 실행 중인 경우. 서버를 업그레이드하기 전에 로그인 스크립트를 실행 중인 에이전트가 없도록 합니다.
   - 서버에서 데이터베이스 관련 작업을 수행 중인 경우. 업그레이드하기 전에 OfficeScan 데이터베이스(DbServer.exe)의 상태를 확인합니다. 예를 들어, Windows 작업 관리자를 열고 DbServer.exe의 CPU 사용량이 00인지 확인합니다. CPU 사용량이 높은 경우 사용량이 00이 될 때까지 기다립니다. 00이면 데이터베이스 관련 작업이 완료된 것입니다. 업그레이드를 실행했는데 업그레이드 문제가 발생하면 데이터베이스 파일이 잠긴 것일 수 있습니다. 이 경우 서버 컴퓨터를 다시 시작하여 파일의 잠금을 해제한 다음 다른 업그레이드를 실행합니다.

다음 업그레이드 방법 중 하나를 사용합니다.

- 업그레이드 방법 1: 자동 에이전트 업그레이드를 사용하지 않도록 설정 페이지 3-4
- 업그레이드 방법 2: 업데이트 에이전트 업그레이드 페이지 3-7
- 업그레이드 방법 3: OfficeScan XG 서버로 에이전트 이동 페이지 3-14
- 업그레이드 방법 4: 자동 에이전트 업그레이드를 사용하도록 설정 페이지 3-17

업그레이드 방법 1: 자동 에이전트 업그레이드를 사용하지 않도록 설정

자동 에이전트 업그레이드를 사용하지 않도록 설정하면 서버를 먼저 업그레이드한 다음 에이전트를 그룹별로 업그레이드할 수 있습니다. 업그레이드할 에이전트 수가 많을 경우 이 업그레이드 방법을 사용합니다.

파트 1: OfficeScan 서버에 대한 업데이트 설정 구성

절차

- OfficeScan 10.x 서버의 경우:

a. **네트워크로 연결된 컴퓨터** > **클라이언트 관리**로 이동합니다.

b. 클라이언트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 클라이언트를 선택합니다.

c. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.

d. **클라이언트가 구성 요소를 업데이트할 수 있지만 클라이언트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음** 옵션을 선택합니다.

e. **모든 클라이언트에 적용**을 클릭합니다.

팁

네트워크 환경이 복잡하고 클라이언트 수가 많은 경우 온라인 클라이언트에 설정을 배포하는 데 시간이 걸릴 수 있습니다. 업그레이드하기 전에 모든 클라이언트에 설정이 배포되도록 충분한 시간을 할당합니다. 설정을 적용하지 않은 OfficeScan 클라이언트는 자동으로 업그레이드됩니다.

- OfficeScan 11.x 서버의 경우:

a. **에이전트** > **에이전트 관리**로 이동합니다.

b. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 선택합니다.

c. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.

d. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음**을 선택합니다.

e. **모든 에이전트에 적용**을 클릭합니다.

네트워크 환경이 복잡하고 에이전트 수가 많은 경우 온라인 에이전트에 설정을 배포하는 데 시간이 걸릴 수 있습니다. 업그레이드하기 전에 모든 에이전트에 설정이 배포되도록 충분한 시간을 할당합니다. 설정을 적용하지 않은 OfficeScan 에이전트는 자동으로 업그레이드됩니다.

파트 2: OfficeScan 서버 업그레이드

OfficeScan 서버 업그레이드에 대한 자세한 내용은 로컬 업그레이드 수행 페이지 3-19 또는 원격 업그레이드 수행 페이지 3-60 항목을 참조하십시오.

참고

업그레이드 프로세스를 신속하게 진행하려면 Windows Server 2008 Standard 64비트를 실행하는 OfficeScan 서버를 업그레이드하기 전에 OfficeScan 에이전트를 종료합니다.

설치 완료 후 에이전트를 업그레이드하기 전에 즉시 웹 콘솔을 사용하여 OfficeScan 서버 설정을 구성합니다.

OfficeScan 설정을 구성하는 방법에 대한 자세한 지침은 *관리자 안내서* 또는 *OfficeScan 서버 도움말*을 참조하십시오.

파트 3: OfficeScan 에이전트 업그레이드

절차

1. **업데이트** > **에이전트** > **자동 업데이트** 항목으로 이동하고 다음 옵션이 사용되도록 설정되어 있는지 확인합니다.
   - **OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 에이전트에서 구성 요소 업데이트 시작**
   - **에이전트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(독립 에이전트 제외)**
2. **에이전트** > **에이전트 관리**으로 이동합니다.
3. 에이전트 트리에서 업그레이드할 에이전트를 선택합니다. 하나 또는 여러 개의 도메인을 선택하거나 도메인 내의 개별/모든 에이전트를 선택할 수 있습니다.
4. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.

5. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음**을 사용하지 않도록 설정합니다.
6. **저장**을 클릭합니다.
7. 업그레이드 결과를 확인합니다.
   - 온라인 에이전트 페이지 3-12
   - 오프라인 에이전트 페이지 3-14
   - 독립(로밍) 에이전트 페이지 3-14
8. 에이전트 엔드포인트를 다시 시작하여 에이전트 업그레이드를 완료합니다.
9. 모든 에이전트가 업그레이드될 때까지 2~8단계를 반복합니다.

업그레이드 방법 2: 업데이트 에이전트 업그레이드

업데이트 에이전트에서 업데이트할 에이전트 수가 많은 경우 이 업그레이드 방법을 사용합니다. 이러한 에이전트는 각 업데이트 에이전트에서 업그레이드됩니다.

업데이트 에이전트에서 업데이트되지 않은 OfficeScan 에이전트는 OfficeScan 서버에서 업그레이드됩니다.

파트 1: OfficeScan 서버에 대한 업데이트 설정 구성

절차

- OfficeScan 10.x 서버의 경우:
  a. **네트워크로 연결된 컴퓨터** > **클라이언트 관리**로 이동합니다.
  b. 클라이언트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 클라이언트를 선택합니다.
  c. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.

d. **클라이언트가 구성 요소를 업데이트할 수 있지만 클라이언트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음** 옵션을 선택합니다.

e. **모든 클라이언트에 적용**을 클릭합니다.

> **팁**
>
> 네트워크 환경이 복잡하고 클라이언트 수가 많은 경우 온라인 클라이언트에 설정을 배포하는 데 시간이 걸릴 수 있습니다. 업그레이드하기 전에 모든 클라이언트에 설정이 배포되도록 충분한 시간을 할당합니다. 설정을 적용하지 않은 OfficeScan 클라이언트는 자동으로 업그레이드됩니다.

- OfficeScan 11.x 서버의 경우:

  a. **에이전트** > **에이전트 관리**로 이동합니다.

  b. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 선택합니다.

  c. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.

  d. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음**을 선택합니다.

  e. **모든 에이전트에 적용**을 클릭합니다.

  네트워크 환경이 복잡하고 에이전트 수가 많은 경우 온라인 에이전트에 설정을 배포하는 데 시간이 걸릴 수 있습니다. 업그레이드하기 전에 모든 에이전트에 설정이 배포되도록 충분한 시간을 할당합니다. 설정을 적용하지 않은 OfficeScan 에이전트는 자동으로 업그레이드됩니다.

파트 2: OfficeScan 서버 업그레이드

OfficeScan 서버 업그레이드에 대한 자세한 내용은 로컬 업그레이드 수행 페이지 3-19 또는 원격 업그레이드 수행 페이지 3-60 항목을 참조하십시오.

참고

업그레이드 프로세스를 신속하게 진행하려면 Windows Server 2008 Standard 64비트를 실행하는 OfficeScan 서버를 업그레이드하기 전에 OfficeScan 에이전트를 종료합니다.

설치 완료 후 에이전트를 업그레이드하기 전에 즉시 웹 콘솔을 사용하여 OfficeScan 서버 설정을 구성합니다.

OfficeScan 설정을 구성하는 방법에 대한 자세한 지침은 *관리자 안내서* 또는 *OfficeScan 서버 도움말*을 참조하십시오.

파트 3: 업데이트 에이전트 업그레이드

절차

1. **에이전트** > **에이전트 관리**으로 이동합니다.
2. 에이전트 트리에서 업그레이드할 업데이트 에이전트를 선택합니다.

   팁

   업데이트 에이전트를 쉽게 찾으려면 도메인을 선택하고 에이전트 트리의 맨 위에 있는 **에이전트 트리 보기**로 이동한 다음 **업데이트 에이전트 보기**를 선택합니다.

3. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.
4. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음**을 사용하지 않도록 설정합니다.
5. **저장**을 클릭합니다.
6. **업데이트** > **에이전트** > **수동 업데이트**으로 이동합니다.
7. **수동으로 에이전트 선택** 옵션을 선택하고 **선택**을 클릭합니다.
8. 열리는 에이전트 트리에서 업그레이드할 업데이트 에이전트를 선택합니다.

팁

업데이트 에이전트를 쉽게 찾으려면 도메인을 선택하고 에이전트 트리의 맨 위에 있는 **에이전트 트리 보기**로 이동한 다음 **업데이트 에이전트 보기**를 선택합니다.

9. 에이전트 트리 맨 위에서 **업데이트 시작**을 클릭합니다.
10. 업그레이드 결과를 확인합니다.
    - 구성 요소 업데이트를 시작한 직후 온라인 업데이트 에이전트가 업그레이드됩니다.
    - 오프라인 업데이트 에이전트가 온라인 상태가 되면 업그레이드됩니다.
    - 독립(이전의 로밍) 업데이트 에이전트가 온라인 상태가 되거나, 해당 업데이트 에이전트에 예약 업데이트 권한이 있는 경우 예약된 업데이트가 실행되면 독립 업데이트 에이전트가 업그레이드됩니다.
11. 업데이트 에이전트 엔드포인트를 다시 시작하여 에이전트 업그레이드를 완료합니다.
12. 모든 업데이트 에이전트가 업그레이드될 때까지 1~11단계를 반복합니다.

파트 4: 업데이트 에이전트 설정 구성

절차

1. **에이전트** > **에이전트 관리**으로 이동합니다.
2. 에이전트 트리에서 업그레이드할 업데이트 에이전트를 선택합니다.

팁

업데이트 에이전트를 쉽게 찾으려면 도메인을 선택하고 에이전트 트리의 맨 위에 있는 **에이전트 트리 보기**로 이동한 다음 **업데이트 에이전트 보기**를 선택합니다.

3. 업데이트 에이전트에 최신 구성 요소가 있는지 확인합니다.

4. **설정** > **업데이트 에이전트 설정**을 클릭합니다.
5. 다음 옵션을 선택합니다.
   - **구성 요소 업데이트**
   - **도메인 설정**
   - **OfficeScan 에이전트 프로그램 및 핫픽스**
6. **저장**을 클릭합니다.

   파트 5를 진행하기 전에 업데이트 에이전트가 에이전트 프로그램 다운로드를 완료할 때까지 기다립니다.
7. 모든 업데이트 에이전트가 필요한 설정을 적용할 때까지 1~6단계를 반복합니다.

파트 5: OfficeScan 에이전트 업그레이드

절차

1. **업데이트** > **에이전트** > **자동 업데이트** 항목으로 이동하고 다음 옵션이 사용되도록 설정되어 있는지 확인합니다.
   - **OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 에이전트에서 구성 요소 업데이트 시작**
   - **에이전트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(독립 에이전트 제외)**
2. **에이전트** > **에이전트 관리**으로 이동합니다.
3. 에이전트 트리에서 업그레이드할 에이전트를 선택합니다. 하나 또는 여러 개의 도메인을 선택하거나 도메인 내의 개별/모든 에이전트를 선택할 수 있습니다.
4. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.
5. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음**을 사용하지 않도록 설정합니다.

6. **저장**을 클릭합니다.
7. 업그레이드 결과를 확인합니다.
   - 온라인 에이전트 페이지 3-12
   - 오프라인 에이전트 페이지 3-14
   - 독립(로밍) 에이전트 페이지 3-14
8. 에이전트 엔드포인트를 다시 시작하여 에이전트 업그레이드를 완료합니다.
9. 모든 에이전트가 업그레이드될 때까지 2~8단계를 반복합니다.

업그레이드 결과

온라인 에이전트

참고

업그레이드 후에 에이전트 엔드포인트를 다시 시작합니다.

- 자동 업그레이드

  다음과 같은 이벤트가 발생할 경우 온라인 에이전트에서 업그레이드를 시작합니다.

  - OfficeScan 서버가 새 구성 요소를 다운로드한 다음 에이전트에 업데이트하도록 알릴 경우
  - 에이전트가 다시 로드된 경우
  - 에이전트가 다시 시작된 다음 OfficeScan 서버에 연결된 경우
  - Windows Server 2003 또는 Windows XP Professional을 실행 중인 에이전트 엔드포인트에서 로그인 스크립트 설정(AutoPcc.exe)을 사용하여 로그인 스크립트를 수정한 서버에 로그온하는 경우
  - 업데이트 일정이 에이전트 엔드포인트에서 실행되는 경우(예약 업데이트 권한이 있는 에이전트만 해당)

- 수동 업그레이드

  위의 이벤트 중 아무것도 발생하지 않은 경우에는 다음 작업 중 하나를 수행하여 에이전트를 즉시 업그레이드합니다.

  - EXE 또는 MSI OfficeScan 에이전트 패키지를 만들어 배포합니다.

    참고

    에이전트 패키지를 만드는 방법에 대한 지침은 *관리자 안내서*를 참조하십시오.

  - 사용자에게 에이전트 엔드포인트에서 **지금 업데이트**를 실행하도록 지시합니다.
  - 에이전트 엔드포인트에서 Windows Server 2003, XP Professional, Server 2008, Vista™(Vista Home을 제외한 모든 에디션), 7™(7 Home을 제외한 모든 에디션), Windows 8(Pro/Enterprise), Windows Server 2012 또는 Windows Server 2016을 실행하는 경우 사용자에게 다음 단계를 수행하도록 지시합니다.
    - 서버 컴퓨터에 연결합니다.
    - ₩₩<서버 컴퓨터 이름>₩ofcscan으로 이동합니다.
    - AutoPcc.exe를 실행합니다.
  - 에이전트 엔드포인트에서 Windows Vista Home, Windows 7 Home, Windows 8 또는 Windows 10을 실행하는 경우 사용자에게 AutoPcc.exe를 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택하도록 지시합니다.
  - 수동 에이전트 업데이트를 시작합니다.

  수동 업데이트를 시작하려면

  1. **업데이트** > **에이전트** > **수동 업데이트** 항목으로 이동합니다.
  2. **수동으로 에이전트 선택** 옵션을 선택하고 **선택**을 클릭합니다.
  3. 열리는 에이전트 트리에서 업그레이드할 에이전트를 선택합니다.
  4. 에이전트 트리 맨 위에서 **구성 요소 업데이트 시작**을 클릭합니다.

오프라인 에이전트

오프라인 에이전트가 온라인 상태가 되면 업그레이드됩니다.

독립(로밍) 에이전트

독립 에이전트(이전에는 로밍 에이전트라고 함)가 온라인 상태가 되거나, 해당 에이전트에 예약 업데이트 권한이 있는 경우 예약된 업데이트가 실행되면 독립 에이전트가 업그레이드됩니다.

업그레이드 방법 3: OfficeScan XG 서버로 에이전트 이동

OfficeScan XG 서버를 새로 설치한 다음 에이전트를 이 서버로 이동합니다. 에이전트를 이동하면 해당 에이전트가 자동으로 OfficeScan XG으로 업그레이드됩니다.

파트 1: OfficeScan 서버를 새로 설치한 다음 업데이트 설정 구성

절차

1. OfficeScan XG 서버의 새로 설치를 수행합니다.

   자세한 내용은 설치 프로그램 설치 화면 페이지 2-4를 참조하십시오.

2. 웹 콘솔에 로그온합니다.

3. **업데이트** > **에이전트** > **자동 업데이트** 항목으로 이동하고 다음 옵션이 사용되도록 설정되어 있는지 확인합니다.

   - **OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 에이전트에서 구성 요소 업데이트 시작**
   - **에이전트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(독립 에이전트 제외)**

4. **에이전트** > **에이전트 관리**으로 이동합니다.

5. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 선택합니다.

6. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.
7. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음**을 사용하지 않도록 설정합니다.
8. **모든 에이전트에 적용**을 클릭합니다.
9. 다음 OfficeScan XG 서버 정보를 기록합니다. 에이전트를 이동할 때 OfficeScan 10.x 서버에서 이 정보를 지정합니다.
   - 엔드포인트 이름 또는 IP 주소
   - 서버 수신 포트

     서버 수신 포트를 보려면 **관리** > **설정** > **에이전트 연결** 항목으로 이동합니다. 포트 번호가 화면에 표시됩니다.

파트 2: OfficeScan 에이전트 업그레이드

절차

1. 이전 버전의 OfficeScan 웹 콘솔에서 **업데이트** > **요약**으로 이동합니다.
2. **알림 취소**를 클릭합니다. 이 기능은 서버 알림 대기열을 지워 클라이언트/에이전트를 OfficeScan XG 서버로 이동할 때 문제가 발생하지 않게 해줍니다.

   경고!

   다음 단계를 즉시 수행합니다. 클라이언트/에이전트를 이동하기 전에 서버 알림 대기열이 업데이트된 경우에는 클라이언트/에이전트가 이동하지 않을 수 있습니다.
3. 다음 화면으로 이동합니다.
   - OfficeScan 10.x 서버의 경우: **네트워크로 연결된 컴퓨터** > **클라이언트 관리**
   - OfficeScan 11.x 서버의 경우: **에이전트** > **에이전트 관리**

4. 클라이언트/에이전트 트리에서 업그레이드할 클라이언트/에이전트를 선택합니다. 오프라인 및 로밍 클라이언트/에이전트는 이동할 수 없으므로 온라인 클라이언트/에이전트만 선택합니다.

5. 클라이언트/에이전트를 다음과 같이 이동합니다.

   - OfficeScan 10.x 서버의 경우:

     a. **클라이언트 트리 관리** > **클라이언트 이동**을 클릭합니다.

     b. **선택한 클라이언트를 온라인으로 다른 OfficeScan 서버로 이동**에서 OfficeScan XG 서버 컴퓨터 이름/IP 주소 및 서버 수신 포트를 지정합니다.

   - OfficeScan 11.x 서버의 경우:

     a. **에이전트 트리 관리** > **에이전트 이동**을 클릭합니다.

     b. **선택한 에이전트를 온라인으로 다른 OfficeScan 서버로 이동**에서 OfficeScan XG 서버 컴퓨터 이름/IP 주소 및 서버 수신 포트를 지정합니다.

6. **이동**을 클릭합니다.

업그레이드 결과

- 온라인 에이전트가 이동 및 업그레이드를 시작합니다.
- 오프라인 및 독립(이전의 로밍) 에이전트 관리 팁:
  - 에이전트를 업그레이드하려면 에이전트에서 독립(이전의 로밍) 모드를 사용하지 않도록 설정합니다.
  - 오프라인 에이전트의 경우 에이전트가 온라인 상태가 될 수 있도록 사용자에게 네트워크에 연결하도록 지시합니다. 장시간 오프라인 상태인 에이전트의 경우 사용자에게 엔드포인트에서 에이전트를 제거한 다음 *관리자 안내서*에 설명되어 있는 적절한 에이전트 설치 방법(예: 에이전트 패키지 도구)을 사용하여 OfficeScan 에이전트를 설치하도록 지시합니다.

참고

에이전트 엔드포인트를 다시 시작하여 에이전트 업그레이드를 완료합니다.

업그레이드 방법 4: 자동 에이전트 업그레이드를 사용하도록 설정

OfficeScan 서버를 이 버전으로 업그레이드한 후 서버는 관리하는 모든 에이전트에 업그레이드하도록 알립니다.

서버에서 관리하는 에이전트 수가 많지 않은 경우 에이전트를 바로 업그레이드할 수 있도록 합니다. 앞에서 설명한 업그레이드 방법을 사용할 수 있습니다.

파트 1: OfficeScan 서버에 대한 업데이트 설정 구성

절차

- OfficeScan 10.x 서버의 경우:
  a. **업데이트** > **네트워크로 연결된 컴퓨터** > **액티브업데이트**로 이동하고 다음 옵션이 사용되도록 설정되어 있는지 확인합니다.
     - **OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 클라이언트에서 구성 요소 업데이트 시작**
     - **클라이언트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(로밍 클라이언트 제외)**
  b. **네트워크로 연결된 컴퓨터** > **클라이언트 관리**로 이동합니다.
  c. 클라이언트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 클라이언트를 선택합니다.
  d. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.
  e. **클라이언트가 구성 요소를 업데이트할 수 있지만 클라이언트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음** 옵션을 선택합니다.
  f. **모든 클라이언트에 적용**을 클릭합니다.

팁

네트워크 환경이 복잡하고 클라이언트 수가 많은 경우 온라인 클라이언트에 설정을 배포하는 데 시간이 걸릴 수 있습니다. 업그레이드하기 전에 모든 클라이언트에 설정이 배포되도록 충분한 시간을 할당합니다. 설정을 적용하지 않은 OfficeScan 클라이언트는 자동으로 업그레이드됩니다.

- OfficeScan 11.x 서버의 경우:

  a. **업데이트** > **에이전트** > **자동 업데이트**로 이동하고 다음 옵션이 사용되도록 설정되어 있는지 확인합니다.

  - **OfficeScan 서버가 새 구성 요소를 다운로드하는 즉시 에이전트에서 구성 요소 업데이트 시작**
  - **에이전트가 다시 시작되어 OfficeScan 서버에 연결될 때 구성 요소 업데이트 시작(로밍 에이전트 제외)**

  b. **에이전트** > **에이전트 관리**로 이동합니다.

  c. 에이전트 트리에서 루트 도메인 아이콘( )을 클릭하여 모든 에이전트를 선택합니다.

  d. **설정** > **권한 및 기타 설정**을 클릭하고 **기타 설정** 탭으로 이동합니다.

  e. **OfficeScan 에이전트가 구성 요소를 업데이트할 수 있지만 에이전트 프로그램을 업그레이드하거나 핫픽스를 배포할 수 없음**을 선택합니다.

  f. **모든 에이전트에 적용**을 클릭합니다.

  네트워크 환경이 복잡하고 에이전트 수가 많은 경우 온라인 에이전트에 설정을 배포하는 데 시간이 걸릴 수 있습니다. 업그레이드하기 전에 모든 에이전트에 설정이 배포되도록 충분한 시간을 할당합니다. 설정을 적용하지 않은 OfficeScan 에이전트는 자동으로 업그레이드됩니다.

파트 2: OfficeScan 서버 업그레이드

OfficeScan 서버 업그레이드에 대한 자세한 내용은 로컬 업그레이드 수행 페이지 3-19 또는 원격 업그레이드 수행 페이지 3-60 항목을 참조하십시오.

참고

업그레이드 프로세스를 신속하게 진행하려면 Windows Server 2008 Standard 64비트를 실행하는 OfficeScan 서버를 업그레이드하기 전에 OfficeScan 에이전트를 종료합니다.

설치 완료 후 에이전트를 업그레이드하기 전에 즉시 웹 콘솔을 사용하여 OfficeScan 서버 설정을 구성합니다.

OfficeScan 설정을 구성하는 방법에 대한 자세한 지침은 *관리자 안내서* 또는 *OfficeScan 서버 도움말*을 참조하십시오.

업그레이드 결과

- 서버 업그레이드가 완료된 직후 온라인 에이전트가 업그레이드됩니다.
- 오프라인 에이전트가 온라인 상태가 되면 업그레이드됩니다.
- 독립(이전의 로밍) 에이전트가 온라인 상태가 되거나, 해당 에이전트에 예약 업데이트 권한이 있는 경우 예약된 업데이트가 실행되면 독립 에이전트가 업그레이드됩니다.

참고

에이전트 엔드포인트를 다시 시작하여 에이전트 업그레이드를 완료합니다.

로컬 업그레이드 수행

로컬 업그레이드 수행 시 OfficeScan은 이전 OfficeScan 서버 버전에서 사용된 설정을 적용합니다. OfficeScan XG의 새 기능을 구성할 수 있는 화면 하위 집합이 제한적으로 표시됩니다.

Apache가 포함된 OfficeScan 10.6 SP3에서 업그레이드

이 OfficeScan 릴리스는 Apache Web Server를 더 이상 지원하지 않습니다. Apache 서버를 사용하는 OfficeScan 10.6 SP3에서 업그레이드하는 동안 OfficeScan은 설치 프로그램이 서버에 IIS Web Server 역할을 설치할 것임을 알려줍니다. 설치가 완료되면 OfficeScan은 더 이상 Apache 서버를 사용하지 않습니다.

중요

이전 OfficeScan 설치 프로그램을 사용하여 Apache 서버를 설치한 경우에만 OfficeScan이 Apache 서버를 IIS 서버로 바꿀 수 있습니다. Apache를 수동으로 설치했다면 OfficeScan을 업그레이드하기 전에 Apache 서버를 제거해야 합니다.

사용권 계약

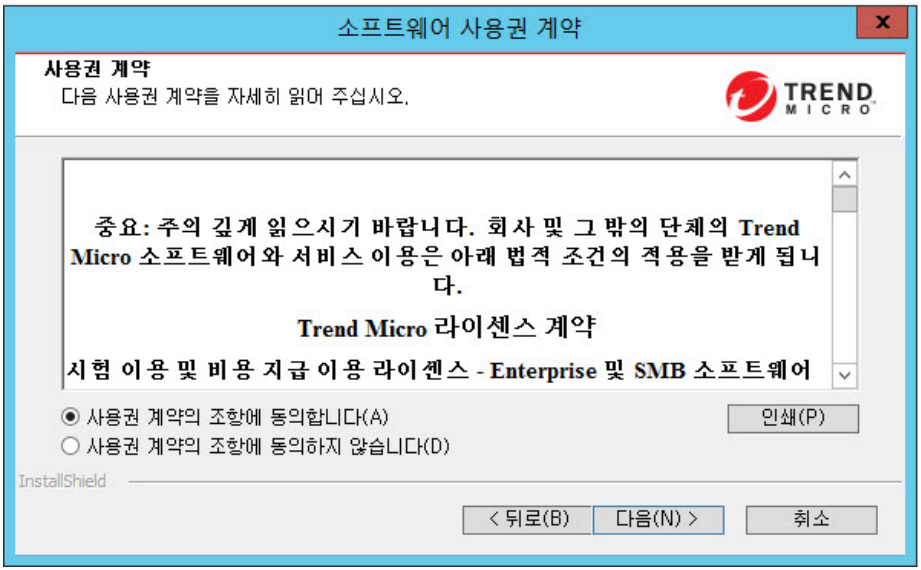

그림 3-1. 사용권 계약 화면

설치를 계속하려면 사용권 계약 내용을 주의 깊게 읽고 사용권 계약 조건에 동의합니다. 사용권 계약 조건에 동의하지 않으면 설치를 진행할 수 없습니다.

설치 대상

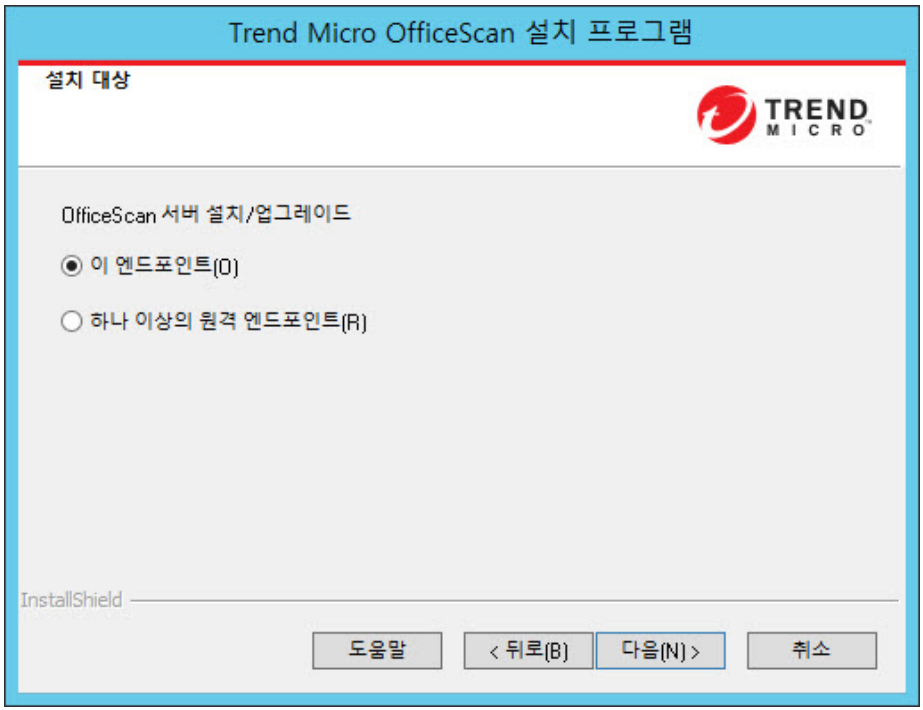

그림 3-2. 설치 대상 화면

현재 엔드포인트나 네트워크의 다른 엔드포인트에서 설치 프로그램을 실행하고 OfficeScan 서버를 설치합니다. 설치 프로그램이 대상 엔드포인트에서 이전 버전의 OfficeScan을 탐지하면 자동으로 업그레이드가 수행됩니다. 다음 버전의 OfficeScan만 이 버전으로 업그레이드할 수 있습니다.

- 11.0 Service Pack 1
- 11.0

- 10.6 Service Pack 3

참고

Trend Micro에서는 업그레이드를 수행하기 전에 현재 OfficeScan 서버에 사용 가능한 모든 패치 및 핫픽스를 적용할 것을 권장합니다.

원격 업그레이드 참고 사항

원격으로 업그레이드할 경우 설치 프로그램에서는 대상 엔드포인트가 서버 업그레이드 요구 사항을 만족하는지 확인합니다. 진행하기 전에

- 대상 엔드포인트에 대한 관리자 권한을 얻습니다.
- 대상 엔드포인트에 대한 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록합니다.
- 대상 엔드포인트가 OfficeScan 서버 설치에 대한 요구 사항을 만족하는지 확인합니다.
- Microsoft IIS Server를 Web Server로 사용할 경우 엔드포인트에 버전 7.0 이상이 있는지 확인합니다.

로컬 업그레이드의 경우 OfficeScan은 서버 이름, 프록시 서버 정보 및 포트 번호를 포함한 이전 설치의 원래 설정을 보존합니다. 업그레이드 시 이러한 설정을 수정할 수 없습니다. 업그레이드한 후에 OfficeScan 웹 콘솔에서 수정합니다.

중요

원격 업그레이드의 경우 모든 설정을 다시 입력합니다. 그러나 서버에서 이전 버전의 설정을 사용하므로 서버 업그레이드 후 이러한 설정은 삭제됩니다.

엔드포인트 설치 전 검색

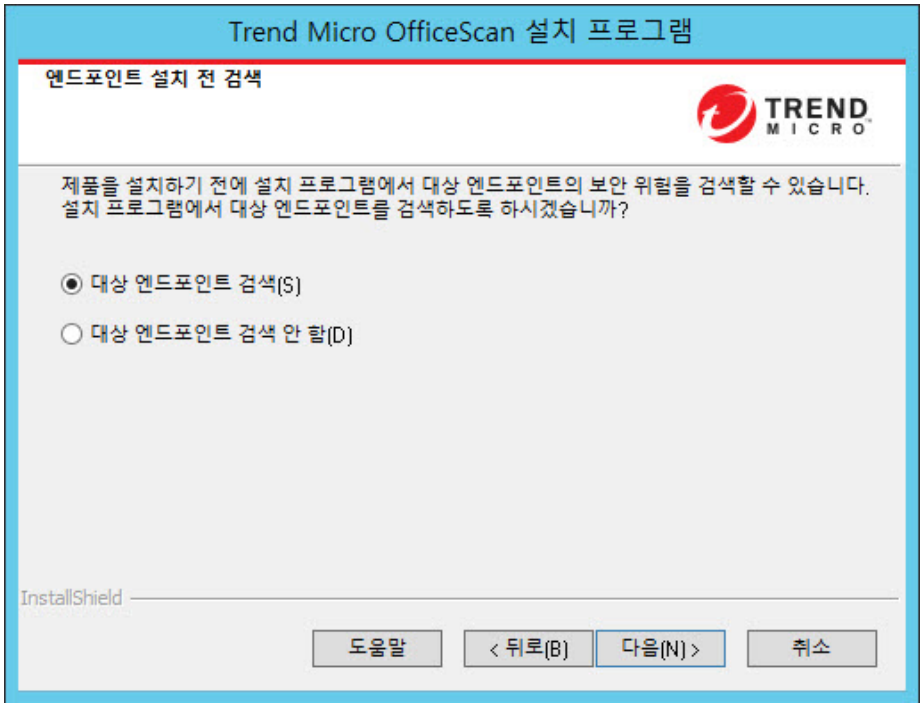

그림 3-3. 엔드포인트 설치 전 검색 화면

설치 프로그램은 OfficeScan 서버 설치를 시작하기 전에 대상 엔드포인트에서 바이러스 및 악성 프로그램을 검색할 수 있습니다. 엔드포인트에서 다음을 비롯한 가장 취약한 영역을 검색합니다.

- 부트 영역 및 부트 디렉터리(부트 바이러스 대상)
- Windows 폴더
- Program Files 폴더

설치 프로그램은 발견된 바이러스/악성 프로그램 및 트로이 목마 프로그램에 대해 다음과 같은 조치를 수행할 수 있습니다.

- **삭제**: 감염된 파일을 삭제합니다.
- **치료**: 파일에 대한 전체 액세스를 허용하기 전에 치료 가능 파일을 치료하거나 지정된 다음 처리 방법으로 치료할 수 없는 파일을 처리합니다.
- **파일명 변경**: 감염된 파일의 확장자를 "vir"로 변경합니다. 사용자가 처음에는 파일을 열 수 없지만 파일을 특정 응용 프로그램에 연결하는 경우 열 수 있습니다. 파일명이 변경된 감염 파일을 열면 바이러스/악성 프로그램이 실행될 수 있습니다.
- **그대로 두기**: 감염된 파일에 대해 아무 조치도 취하지 않고 파일에 대한 전체 액세스를 허용합니다. 사용자가 파일을 열기/복사/삭제할 수 있습니다.

로컬 설치를 수행할 경우 **다음**을 클릭하면 검색이 수행됩니다. 원격 설치를 수행할 경우 실제 설치 직전에 검색이 수행됩니다.

중요

설치 프로그램은 로컬 업그레이드 설치 중 랜섬웨어 위협으로부터 최적화된 보호를 받을 수 있도록 랜섬웨어 보호 설정을 업데이트하라는 메시지를 표시합니다.

업데이트된 설정을 적용하면 이미 동작 모니터링이 사용되도록 설정된 에이전트의 설정만 변경됩니다.

OfficeScan 에이전트 다시 시작 경고

설치 프로그램은 대상 엔드포인트의 리소스를 점검합니다. 업그레이드 시나리오에서 OfficeScan 에이전트 프로그램이 대상 엔드포인트에 있으면 경고 화면이 표시됩니다.

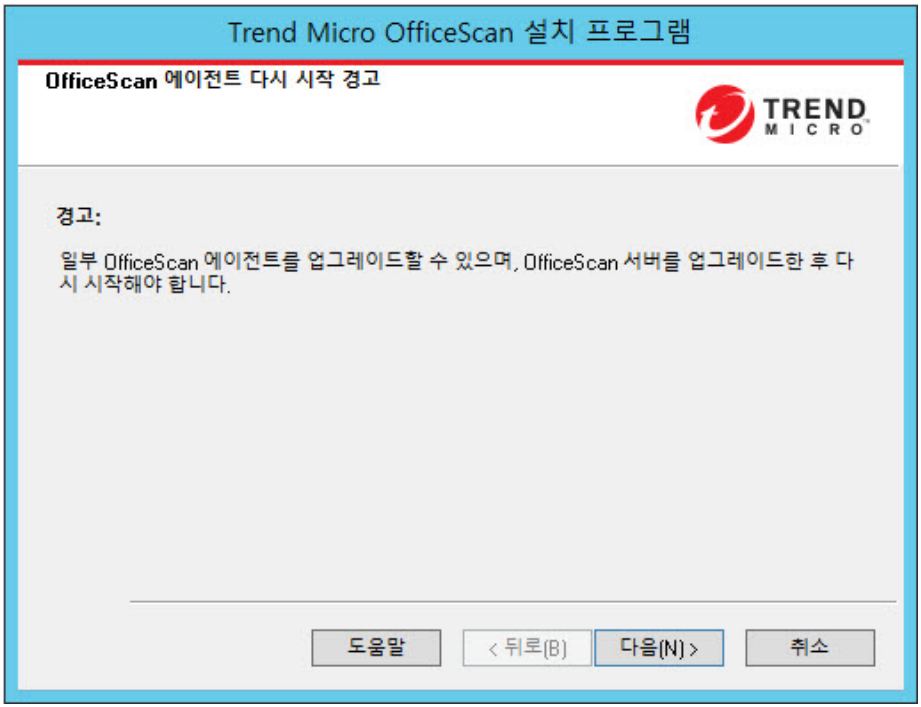

그림 3-4. OfficeScan 에이전트 다시 시작 경고

Apache 제거 경고

OfficeScan XG으로 업그레이드할 때 이전 OfficeScan 서버에 Apache Web Server가 구성되어 있는 경우 경고가 표시됩니다. OfficeScan은 더 이상 Apache Web Server를 지원하지 않습니다.

- 이전 OfficeScan 버전에서 설치 프로그램을 사용하여 Apache Web Server를 설치한 경우 OfficeScan은 Web Server를 자동으로 제거하고 설치 중에 IIS Web Server를 설치할 수 있습니다.
- 이전 OfficeScan 버전을 설치하기 전에 Apache Web Server를 수동으로 설치했다면 OfficeScan 서버 업그레이드를 계속하기 전에 Apache Web Server를 수동으로 제거해야 합니다.

참고

이전의 OfficeScan 서버 버전을 IIS Web Server와 함께 구성한 경우에는 이 경고가 표시되지 않습니다.

데이터베이스 백업

업그레이드할 때 설치 프로그램에서는 최신 버전으로 업그레이드하기 전에 OfficeScan 데이터베이스를 백업할 수 있는 옵션을 제공합니다. 이 백업 정보를 롤백에 사용할 수 있습니다.

참고

백업 패키지에는 300MB를 넘는 사용 가능한 디스크 공간이 필요할 수 있습니다.

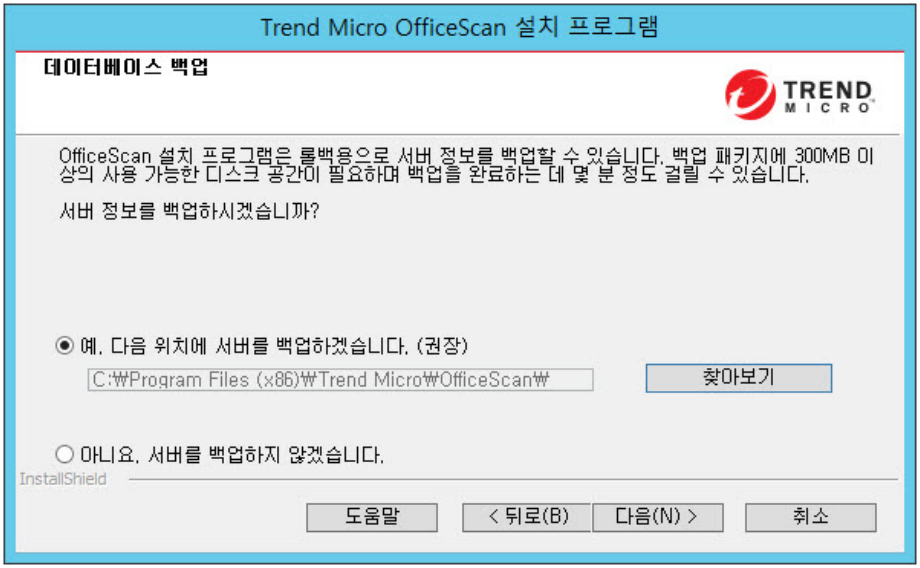

그림 3-5. 데이터베이스 백업 화면

OfficeScan 에이전트 배포

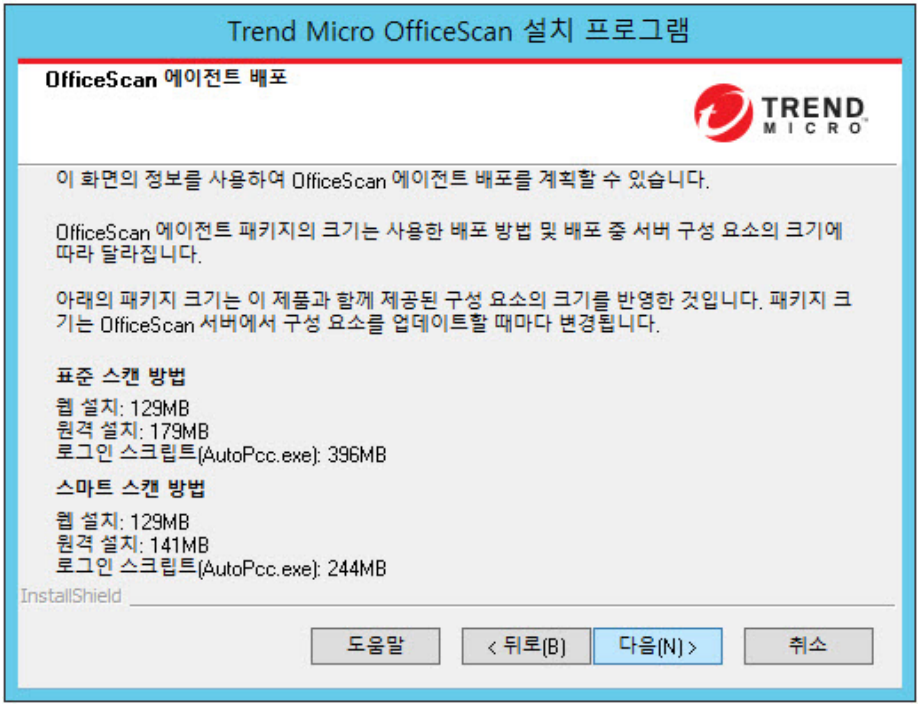

그림 3-6. OfficeScan 에이전트 배포 화면

OfficeScan 에이전트를 설치하거나 업그레이드하는 방법에는 몇 가지가 있습니다. 이 화면에는 서로 다른 배포 방법과 필요한 대략적인 네트워크 대역폭이 나열되어 있습니다.

이 화면을 통해, 대상 엔드포인트에 에이전트를 배포할 때 서버에 필요한 크기와 대역폭 사용량을 예측할 수 있습니다.

참고

이러한 모든 설치 방법에는 대상 엔드포인트의 로컬 관리자 또는 도메인 관리자 권한이 필요합니다.

통합 스마트 보호 서버 설치

참고

로컬 업그레이드 설치 시 IIS 가상 웹 사이트를 사용하는 경우에는 이 화면이 표시되지 않습니다.

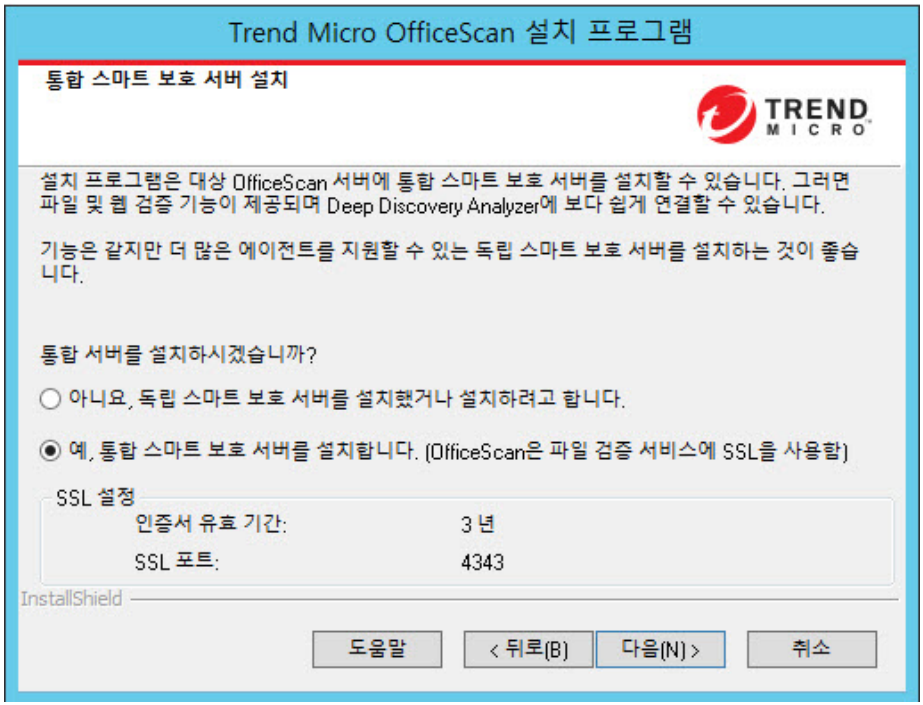

그림 3-7. 통합 스마트 보호 서버 설치 화면

설치 프로그램은 대상 엔드포인트에 통합 스마트 보호 서버를 설치할 수 있습니다. 통합 서버는 스마트 스캔을 사용하는 에이전트에 파일 검증 서비스를 제공하고, 웹 검증 정책이 적용되는 에이전트에 웹 검증 서비스를 제공합니다. OfficeScan 웹 콘솔에서 통합 서버를 관리합니다.

Trend Micro에서는 통합 서버와 기능은 같지만 더 많은 에이전트에 서비스를 제공할 수 있는 독립 스마트 보호 서버를 설치하는 것을 권장합니다. 독립 서버는

별도로 설치되고 자체 관리 콘솔을 포함합니다. 독립 서버에 대한 자세한 내용은 *Trend Micro 스마트 보호 서버 관리자 안내서*를 참조하십시오.

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. 에이전트에 대한 스마트 보호 소스 구성에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

파일 검증 서비스용 에이전트 연결 프로토콜

OfficeScan 에이전트는 HTTP를 사용하여 통합 스마트 보호 서버의 파일 검증 서비스에 연결할 수 있습니다. HTTPS를 사용하면 보다 안전하게 연결할 수 있지만 HTTP가 대역폭을 더 적게 사용합니다.

참고

엔드포인트가 프록시 서버를 통해 통합 서버에 연결되는 경우 웹 콘솔에서 내부 프록시 설정을 구성합니다. 프록시 설정 구성에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

파일 검증 서비스에 사용되는 포트 번호는 OfficeScan 서버에서 사용하는 웹 서버에 따라 다릅니다. 자세한 내용은 Web Server 페이지 2-14를 참조하십시오.

HTTP 포트는 설치 화면에 표시되지 않습니다. HTTPS 포트는 표시되지만 구성은 선택 사항입니다.

표 3-1. 통합 스마트 보호 서버의 파일 검증 서비스에 사용되는 포트

WEB SERVER 및 설정	파일 검증 서비스에 사용되는 포트	
	HTTP	HTTPS (SSL)
IIS 기본 웹 사이트	80	443
IIS 가상 웹 사이트	8080	4343

통합 서버가 설치되어 있지 않음

새로 설치를 수행할 때 통합 서버 설치를 선택하지 않은 경우

- 표준 스캔이 기본 검색 방법이 됩니다.
- 별도의 설치 화면에서 웹 검증 정책을 사용하도록 설정한 경우(자세한 내용은 웹 검증 기능 페이지 2-40 참조) OfficeScan에서는 스마트 보호 서버가 설치되지 않았다고 가정하므로 에이전트가 웹 검증 쿼리를 보낼 수 없습니다.

OfficeScan 설치 후 독립 서버를 사용할 수 있는 경우 OfficeScan 웹 콘솔에서 다음 작업을 수행합니다.

- 검색 방법을 스마트 스캔으로 변경합니다.
- 에이전트가 파일 및 웹 검증 쿼리를 서버에 보낼 수 있도록 독립 서버를 스마트 보호 소스 목록에 추가합니다.

통합 서버를 사용하지 않도록 설정한 OfficeScan 10.x 서버에서 업그레이드하는 경우 통합 서버가 설치되지 않습니다. OfficeScan 에이전트는 검색 방법과 쿼리를 보내는 스마트 보호 소스를 유지합니다.

웹 검증 서비스 사용

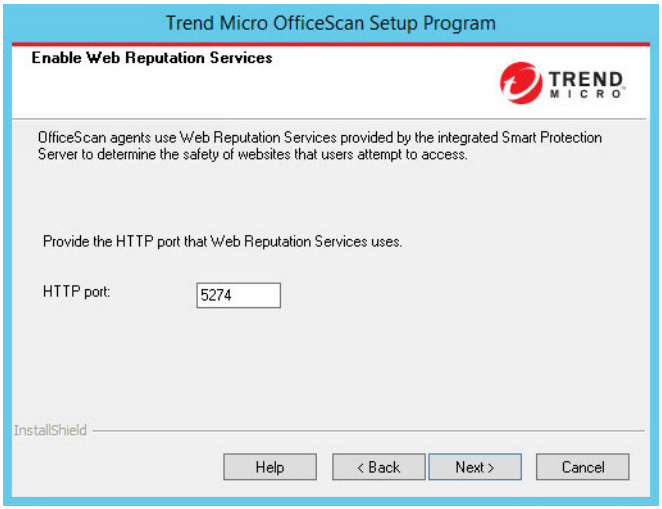

그림 3-8. 웹 검증 서비스 사용 화면

웹 검증 서비스는 각 HTTP 요청 시 요청된 모든 URL의 잠재적 보안 위험을 평가합니다. 데이터베이스에서 반환한 등급과 구성된 보안 수준에 따라 웹 검증에서는 요청을 차단하거나 승인합니다. OfficeScan 서버와 함께 설치된 통합 스마트 보호 서버는 웹 검증 서비스를 제공합니다.

웹 검증 서비스를 사용하도록 설정하면(LWCSService.exe라는 프로세스 이름으로 실행됨) 전체적인 대역폭 사용량이 감소합니다. 이는 OfficeScan 에이전트가 스마트 보호 네트워크에 연결하는 대신 로컬 서버에서 웹 검증 데이터를 가져오기 때문입니다.

서버 인증 인증서

설치 프로그램은 설치 중에 기존 인증 인증서에 대한 검색을 시도합니다. 기존 인증서가 있는 경우 OfficeScan은 해당 파일을 **서버 인증 인증서** 화면에 매핑합니다. 기존 인증서가 없을 경우에는 OfficeScan이 **새 인증 인증서 생성** 옵션을 기본적으로 사용합니다.

참고

원격 업그레이드 설치 중 **서버 인증 인증서** 화면은 OfficeScan 10.6 SP3 서버를 업그레이드하는 경우에만 나타납니다.

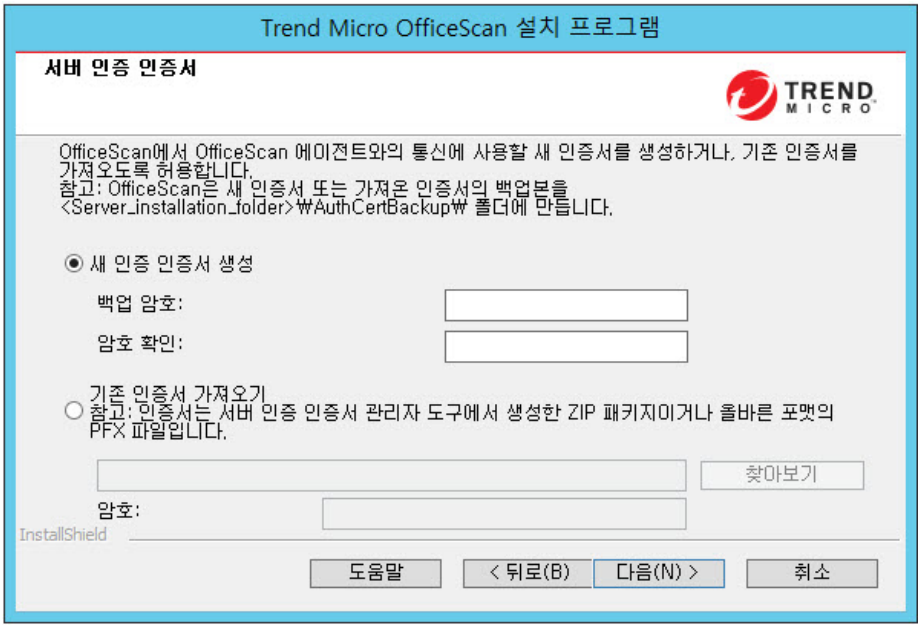

그림 3-9. 새 인증서를 위한 서버 인증 인증서 화면

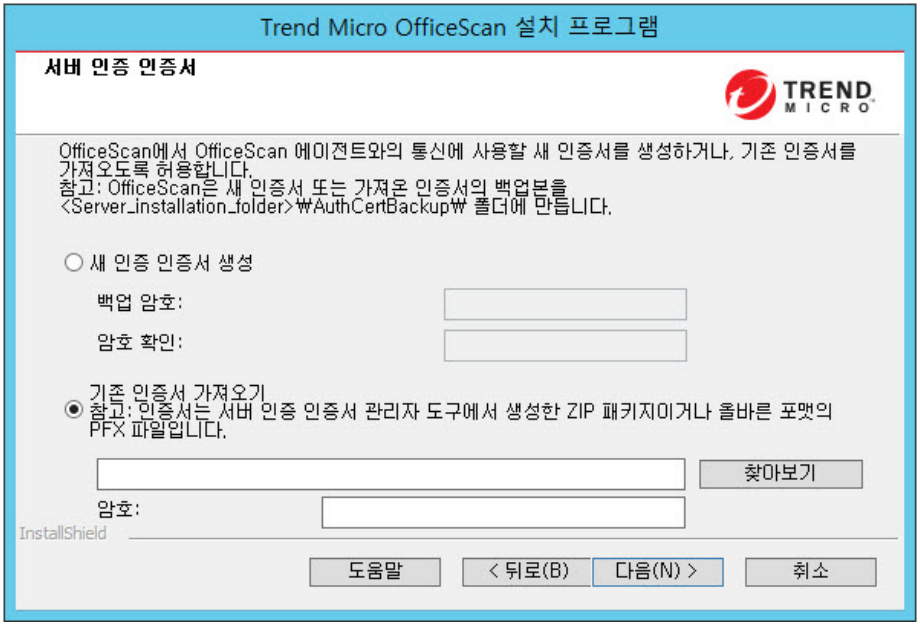

그림 3-10. 기존 인증서를 위한 서버 인증 인증서 화면

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.

OfficeScan이 설치 중에 인증 인증서를 생성하거나 관리자가 다른 OfficeScan 서버에서 기존 인증 인증서를 가져올 수 있습니다.

팁

인증서를 백업할 때는 암호로 인증서를 암호화하는 것이 좋습니다.

설치 정보

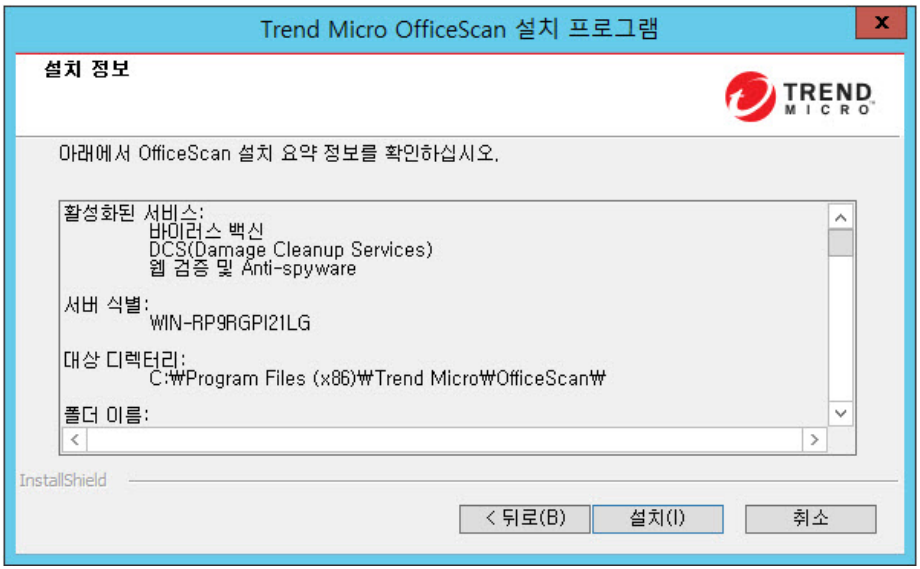

그림 3-11. 설치 정보 화면

이 화면은 설치 설정에 대한 요약을 제공합니다. 설치 정보를 검토하고 **뒤로**를 클릭하여 설정이나 옵션을 변경합니다. 설치를 시작하려면 **설치**를 클릭합니다.

InstallShield 마법사 완료

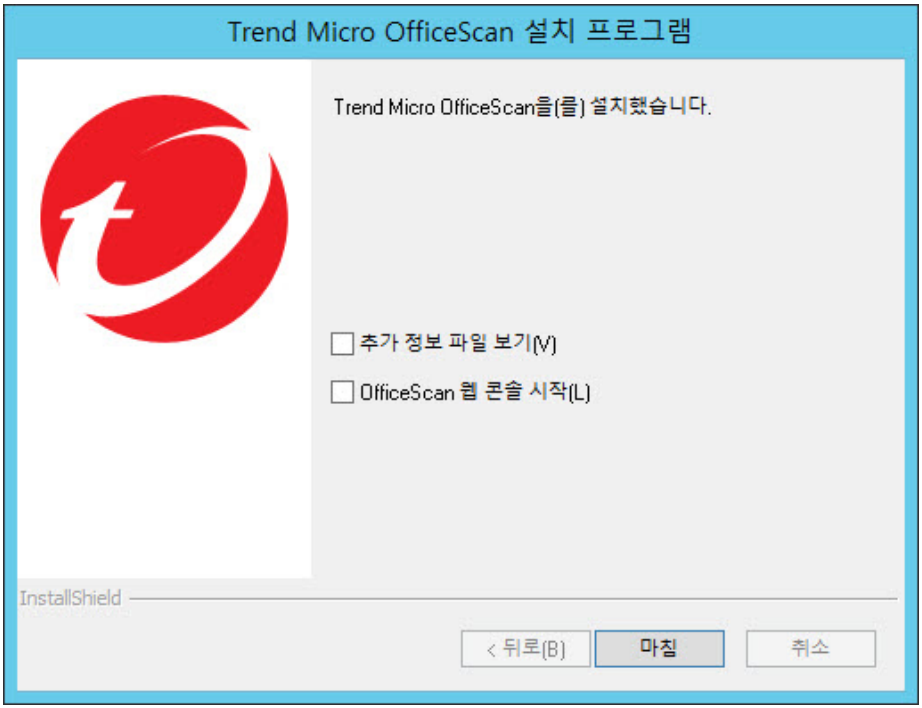

그림 3-12. InstallShield 마법사 완료 화면

설치가 완료되면 추가 정보 파일에서 제품 및 알려진 문제점에 대한 기본 정보를 확인합니다.

관리자는 웹 콘솔을 시작하여 OfficeScan 설정 구성을 시작할 수 있습니다.

IIS가 포함된 OfficeScan 10.6 SP3에서 업그레이드

사용권 계약

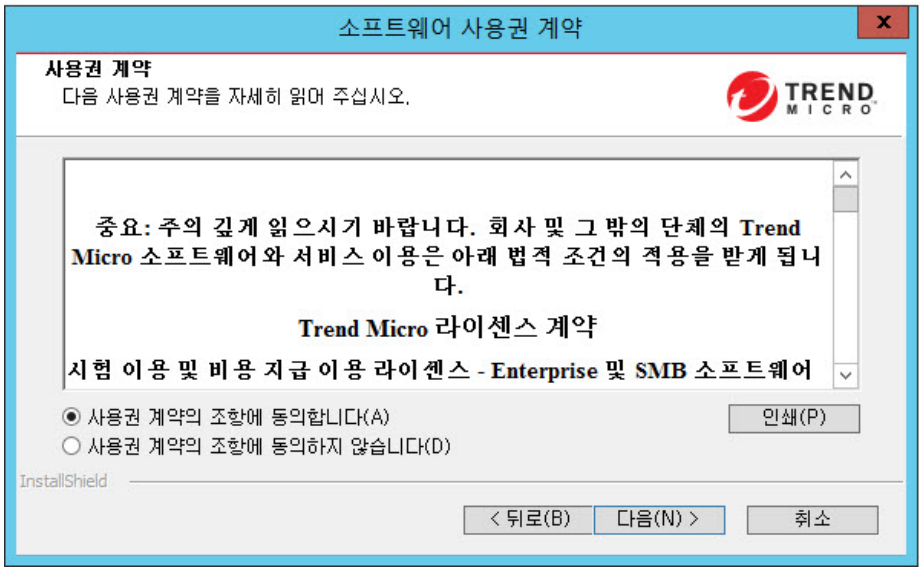

그림 3-13. 사용권 계약 화면

설치를 계속하려면 사용권 계약 내용을 주의 깊게 읽고 사용권 계약 조건에 동의합니다. 사용권 계약 조건에 동의하지 않으면 설치를 진행할 수 없습니다.

설치 대상

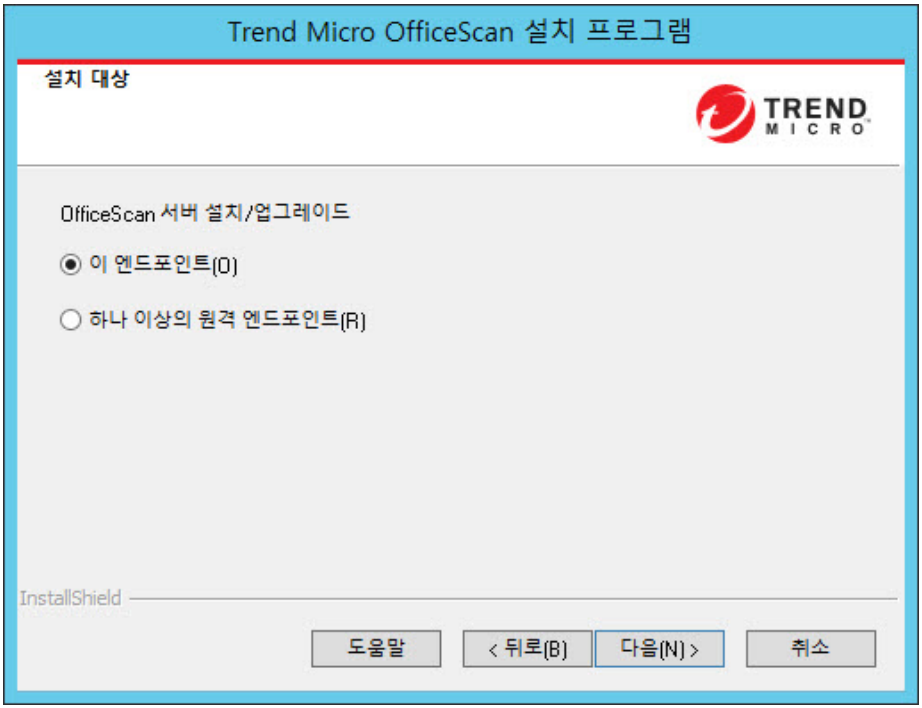

그림 3-14. 설치 대상 화면

현재 엔드포인트나 네트워크의 다른 엔드포인트에서 설치 프로그램을 실행하고 OfficeScan 서버를 설치합니다. 설치 프로그램이 대상 엔드포인트에서 이전 버전의 OfficeScan을 탐지하면 자동으로 업그레이드가 수행됩니다. 다음 버전의 OfficeScan만 이 버전으로 업그레이드할 수 있습니다.

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3

참고

Trend Micro에서는 업그레이드를 수행하기 전에 현재 OfficeScan 서버에 사용 가능한 모든 패치 및 핫픽스를 적용할 것을 권장합니다.

원격 업그레이드 참고 사항

원격으로 업그레이드할 경우 설치 프로그램에서는 대상 엔드포인트가 서버 업그레이드 요구 사항을 만족하는지 확인합니다. 진행하기 전에

- 대상 엔드포인트에 대한 관리자 권한을 얻습니다.
- 대상 엔드포인트에 대한 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록합니다.
- 대상 엔드포인트가 OfficeScan 서버 설치에 대한 요구 사항을 만족하는지 확인합니다.
- Microsoft IIS Server를 Web Server로 사용할 경우 엔드포인트에 버전 7.0 이상이 있는지 확인합니다.

로컬 업그레이드의 경우 OfficeScan은 서버 이름, 프록시 서버 정보 및 포트 번호를 포함한 이전 설치의 원래 설정을 보존합니다. 업그레이드 시 이러한 설정을 수정할 수 없습니다. 업그레이드한 후에 OfficeScan 웹 콘솔에서 수정합니다.

중요

원격 업그레이드의 경우 모든 설정을 다시 입력합니다. 그러나 서버에서 이전 버전의 설정을 사용하므로 서버 업그레이드 후 이러한 설정은 삭제됩니다.

엔드포인트 설치 전 검색

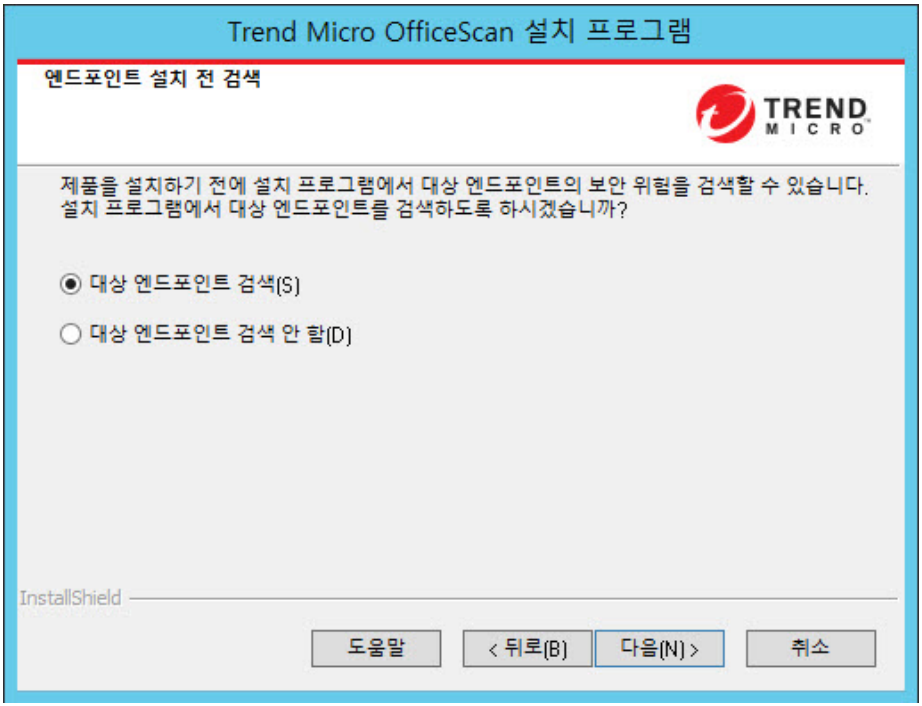

그림 3-15. 엔드포인트 설치 전 검색 화면

설치 프로그램은 OfficeScan 서버 설치를 시작하기 전에 대상 엔드포인트에서 바이러스 및 악성 프로그램을 검색할 수 있습니다. 엔드포인트에서 다음을 비롯한 가장 취약한 영역을 검색합니다.

- 부트 영역 및 부트 디렉터리(부트 바이러스 대상)
- Windows 폴더
- Program Files 폴더

설치 프로그램은 발견된 바이러스/악성 프로그램 및 트로이 목마 프로그램에 대해 다음과 같은 조치를 수행할 수 있습니다.

- **삭제**: 감염된 파일을 삭제합니다.
- **치료**: 파일에 대한 전체 액세스를 허용하기 전에 치료 가능 파일을 치료하거나 지정된 다음 처리 방법으로 치료할 수 없는 파일을 처리합니다.
- **파일명 변경**: 감염된 파일의 확장자를 "vir"로 변경합니다. 사용자가 처음에는 파일을 열 수 없지만 파일을 특정 응용 프로그램에 연결하는 경우 열 수 있습니다. 파일명이 변경된 감염 파일을 열면 바이러스/악성 프로그램이 실행될 수 있습니다.
- **그대로 두기**: 감염된 파일에 대해 아무 조치도 취하지 않고 파일에 대한 전체 액세스를 허용합니다. 사용자가 파일을 열기/복사/삭제할 수 있습니다.

로컬 설치를 수행할 경우 **다음**을 클릭하면 검색이 수행됩니다. 원격 설치를 수행할 경우 실제 설치 직전에 검색이 수행됩니다.

중요

설치 프로그램은 로컬 업그레이드 설치 중 랜섬웨어 위협으로부터 최적화된 보호를 받을 수 있도록 랜섬웨어 보호 설정을 업데이트하라는 메시지를 표시합니다.

업데이트된 설정을 적용하면 이미 동작 모니터링이 사용되도록 설정된 에이전트의 설정만 변경됩니다.

OfficeScan 에이전트 다시 시작 경고

설치 프로그램은 대상 엔드포인트의 리소스를 점검합니다. 업그레이드 시나리오에서 OfficeScan 에이전트 프로그램이 대상 엔드포인트에 있으면 경고 화면이 표시됩니다.

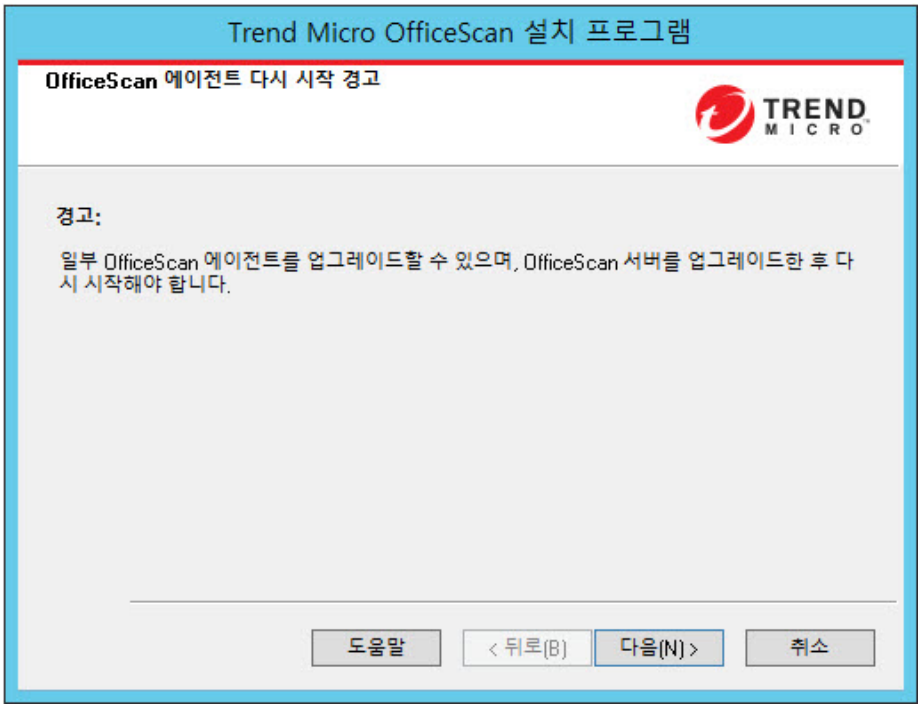

그림 3-16. OfficeScan 에이전트 다시 시작 경고

데이터베이스 백업

업그레이드할 때 설치 프로그램에서는 최신 버전으로 업그레이드하기 전에 OfficeScan 데이터베이스를 백업할 수 있는 옵션을 제공합니다. 이 백업 정보를 롤백에 사용할 수 있습니다.

참고

백업 패키지에는 300MB를 넘는 사용 가능한 디스크 공간이 필요할 수 있습니다.

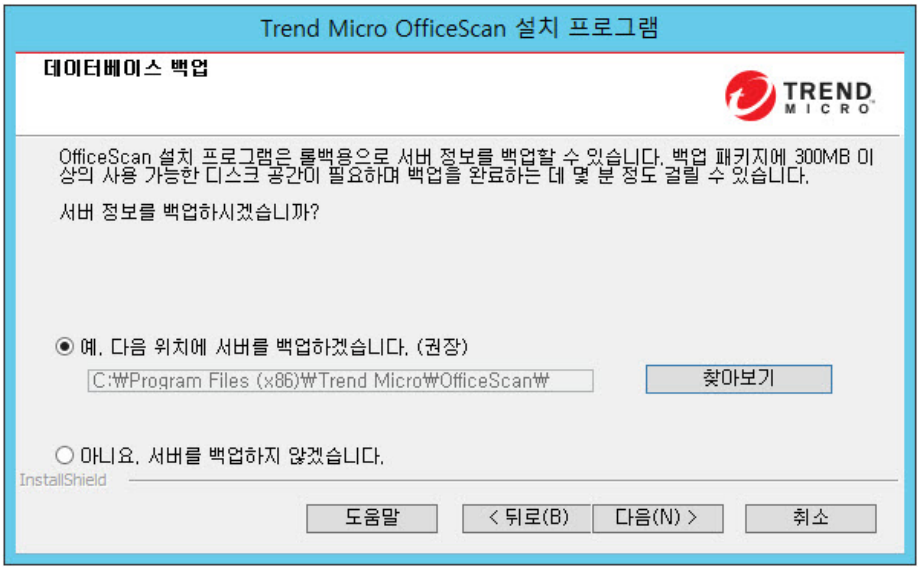

그림 3-17. 데이터베이스 백업 화면

OfficeScan 에이전트 배포

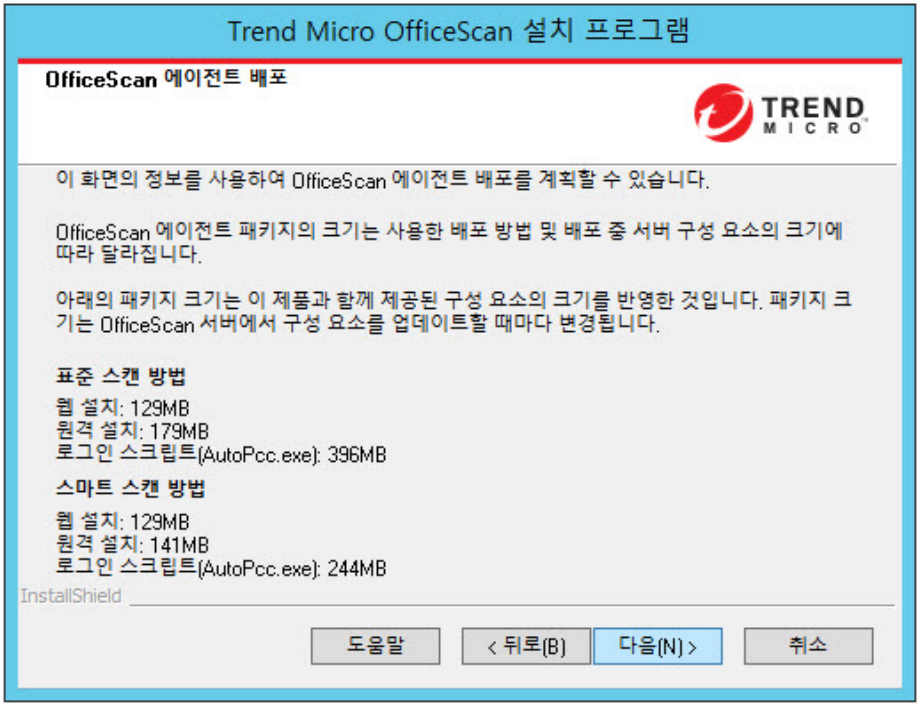

그림 3-18. OfficeScan 에이전트 배포 화면

OfficeScan 에이전트를 설치하거나 업그레이드하는 방법에는 몇 가지가 있습니다. 이 화면에는 서로 다른 배포 방법과 필요한 대략적인 네트워크 대역폭이 나열되어 있습니다.

이 화면을 통해, 대상 엔드포인트에 에이전트를 배포할 때 서버에 필요한 크기와 대역폭 사용량을 예측할 수 있습니다.

참고

이러한 모든 설치 방법에는 대상 엔드포인트의 로컬 관리자 또는 도메인 관리자 권한이 필요합니다.

OfficeScan 방화벽

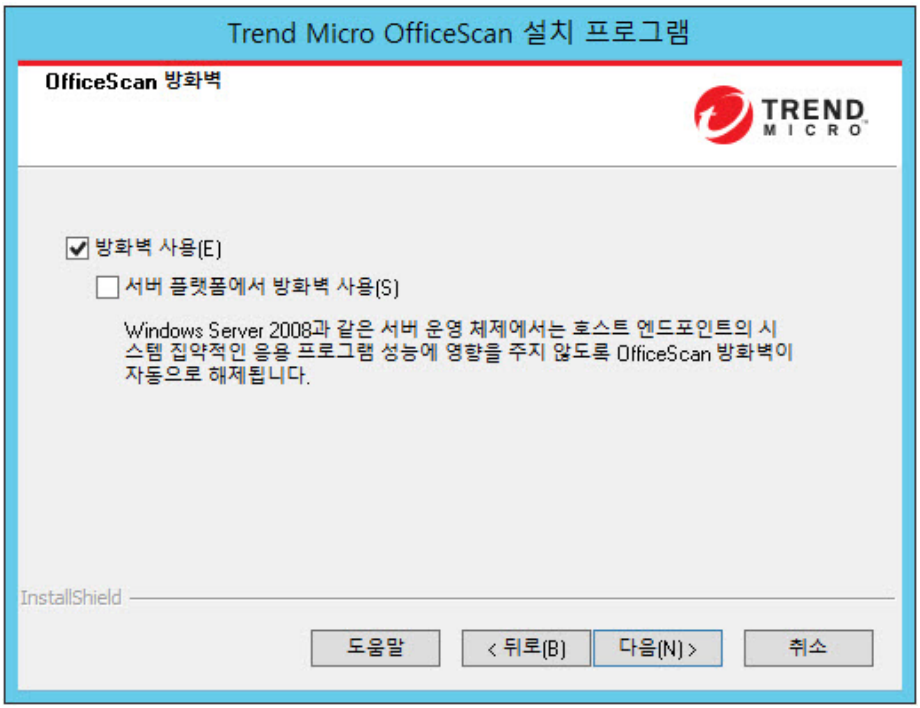

그림 3-19. OfficeScan 방화벽 화면

이 화면은 바이러스 방역 서비스를 활성화한 후에만 표시됩니다.

OfficeScan 방화벽

OfficeScan 방화벽은 상태 기반 검사, 고성능 네트워크 바이러스 검색 및 제거를 통해 네트워크의 에이전트와 서버를 보호합니다. IP 주소, 포트 번호 또는 프로토콜에 따라 연결을 필터링할 규칙을 작성한 다음 여러 사용자 그룹에 적용합니다.

선택적으로 방화벽을 사용하지 않도록 설정하고 나중에 OfficeScan 서버 웹 콘솔에서 방화벽을 사용하도록 설정합니다.

선택적으로 서버 플랫폼에서 방화벽을 사용하도록 설정합니다. 업그레이드 시 서버 플랫폼에서 방화벽 서비스가 이미 사용되도록 설정되어 있으면 업그레이드 후 OfficeScan에서 방화벽 서비스를 해제하지 않도록 **서버 플랫폼에서 방화벽 사용**을 선택합니다.

서버 인증 인증서

설치 프로그램은 설치 중에 기존 인증 인증서에 대한 검색을 시도합니다. 기존 인증서가 있는 경우 OfficeScan은 해당 파일을 **서버 인증 인증서** 화면에 매핑합니다. 기존 인증서가 없을 경우에는 OfficeScan이 **새 인증 인증서 생성** 옵션을 기본적으로 사용합니다.

참고

원격 업그레이드 설치 중 **서버 인증 인증서** 화면은 OfficeScan 10.6 SP3 서버를 업그레이드하는 경우에만 나타납니다.

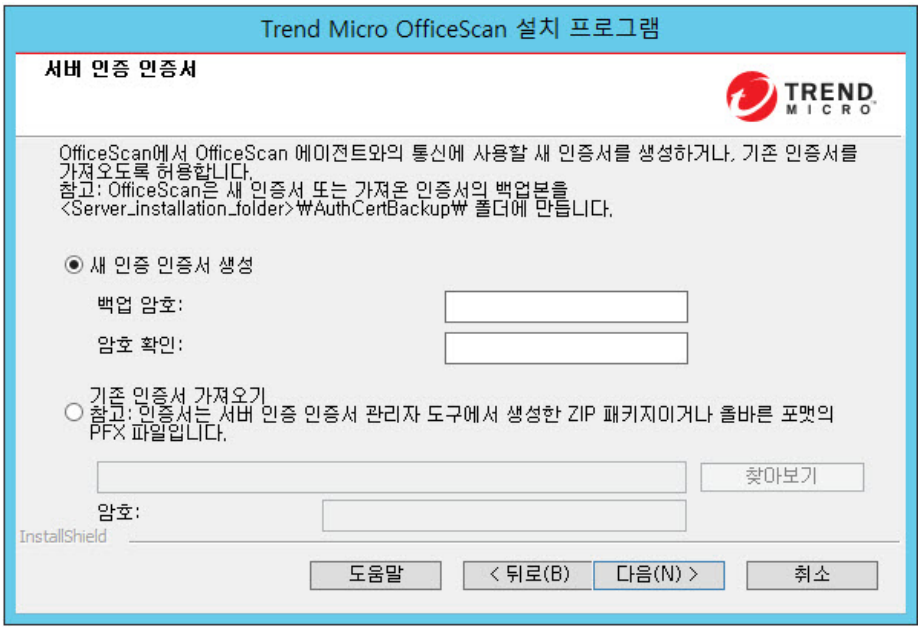

그림 3-20. 새 인증서를 위한 서버 인증 인증서 화면

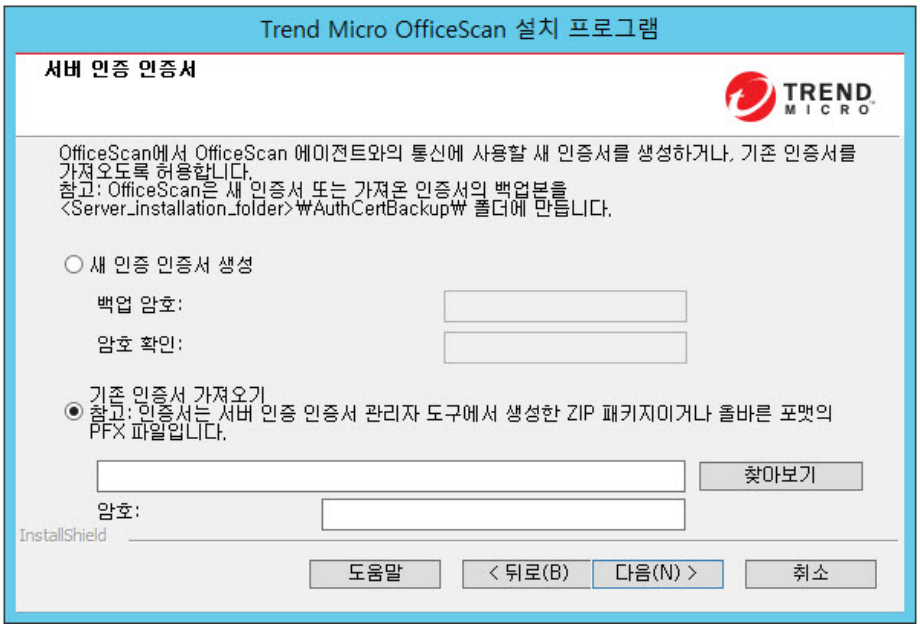

그림 3-21. 기존 인증서를 위한 서버 인증 인증서 화면

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.

OfficeScan이 설치 중에 인증 인증서를 생성하거나 관리자가 다른 OfficeScan 서버에서 기존 인증 인증서를 가져올 수 있습니다.

팁

인증서를 백업할 때는 암호로 인증서를 암호화하는 것이 좋습니다.

설치 정보

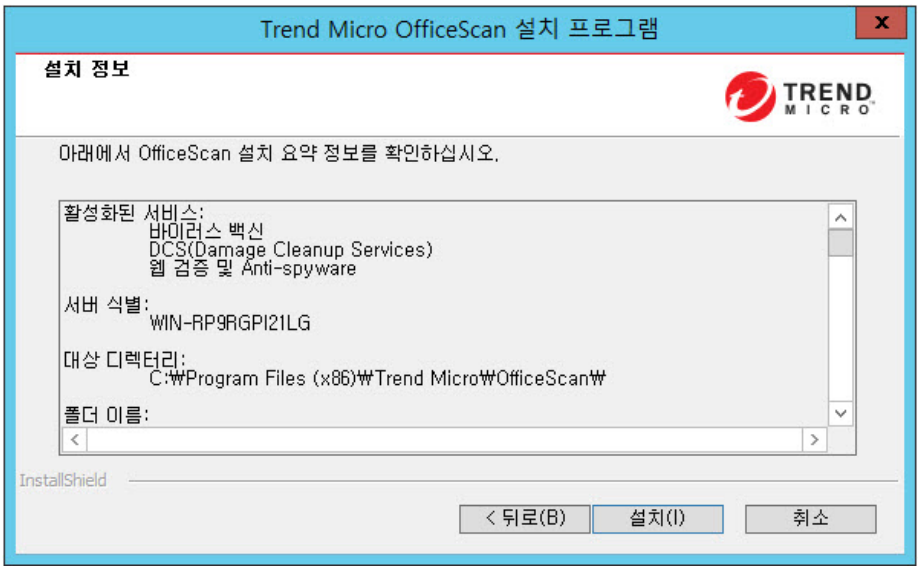

그림 3-22. 설치 정보 화면

이 화면은 설치 설정에 대한 요약을 제공합니다. 설치 정보를 검토하고 **뒤로**를 클릭하여 설정이나 옵션을 변경합니다. 설치를 시작하려면 **설치**를 클릭합니다.

InstallShield 마법사 완료

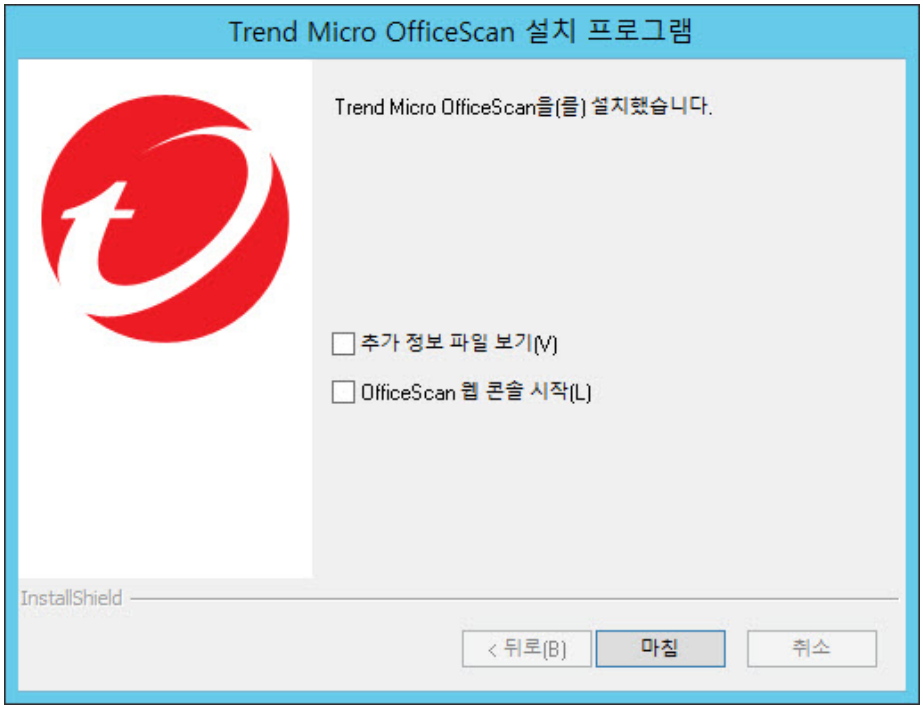

그림 3-23. InstallShield 마법사 완료 화면

설치가 완료되면 추가 정보 파일에서 제품 및 알려진 문제점에 대한 기본 정보를 확인합니다.

관리자는 웹 콘솔을 시작하여 OfficeScan 설정 구성을 시작할 수 있습니다.

OfficeScan 11.x에서 업그레이드

이 OfficeScan 릴리스는 Apache Web Server를 더 이상 지원하지 않습니다. Apache 서버를 사용하는 OfficeScan 11.0에서 업그레이드하는 동안 OfficeScan은 설치 프로그램이 서버에 IIS Web Server 역할을 설치할 것임을 알려줍니다. 설치가 완료되면 OfficeScan은 더 이상 Apache 서버를 사용하지 않습니다.

중요

이전 OfficeScan 설치 프로그램을 사용하여 Apache 서버를 설치한 경우에만 OfficeScan이 Apache 서버를 IIS 서버로 바꿀 수 있습니다. Apache를 수동으로 설치했다면 OfficeScan을 업그레이드하기 전에 Apache 서버를 제거해야 합니다.

사용권 계약

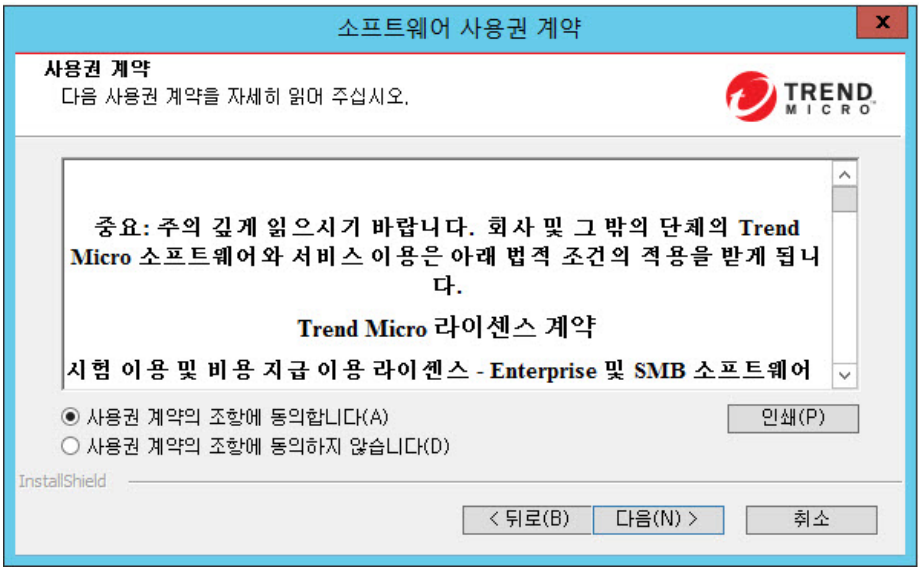

그림 3-24. 사용권 계약 화면

설치를 계속하려면 사용권 계약 내용을 주의 깊게 읽고 사용권 계약 조건에 동의합니다. 사용권 계약 조건에 동의하지 않으면 설치를 진행할 수 없습니다.

설치 대상

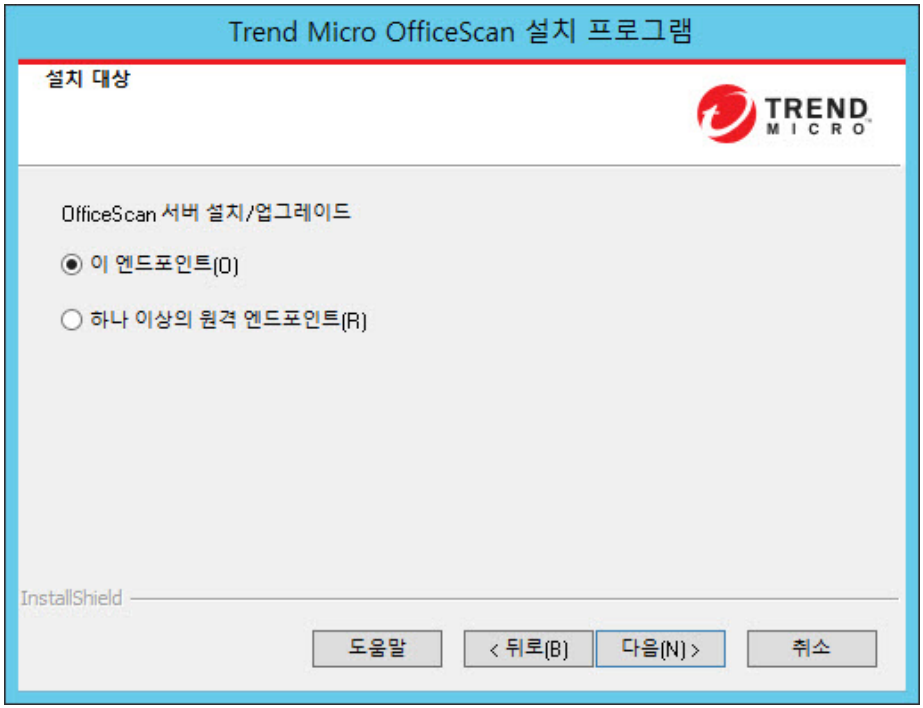

그림 3-25. 설치 대상 화면

현재 엔드포인트나 네트워크의 다른 엔드포인트에서 설치 프로그램을 실행하고 OfficeScan 서버를 설치합니다. 설치 프로그램이 대상 엔드포인트에서 이전 버전의 OfficeScan을 탐지하면 자동으로 업그레이드가 수행됩니다. 다음 버전의 OfficeScan만 이 버전으로 업그레이드할 수 있습니다.

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3

참고

Trend Micro에서는 업그레이드를 수행하기 전에 현재 OfficeScan 서버에 사용 가능한 모든 패치 및 핫픽스를 적용할 것을 권장합니다.

원격 업그레이드 참고 사항

원격으로 업그레이드할 경우 설치 프로그램에서는 대상 엔드포인트가 서버 업그레이드 요구 사항을 만족하는지 확인합니다. 진행하기 전에

- 대상 엔드포인트에 대한 관리자 권한을 얻습니다.
- 대상 엔드포인트에 대한 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록합니다.
- 대상 엔드포인트가 OfficeScan 서버 설치에 대한 요구 사항을 만족하는지 확인합니다.
- Microsoft IIS Server를 Web Server로 사용할 경우 엔드포인트에 버전 7.0 이상이 있는지 확인합니다.

로컬 업그레이드의 경우 OfficeScan은 서버 이름, 프록시 서버 정보 및 포트 번호를 포함한 이전 설치의 원래 설정을 보존합니다. 업그레이드 시 이러한 설정을 수정할 수 없습니다. 업그레이드한 후에 OfficeScan 웹 콘솔에서 수정합니다.

중요

원격 업그레이드의 경우 모든 설정을 다시 입력합니다. 그러나 서버에서 이전 버전의 설정을 사용하므로 서버 업그레이드 후 이러한 설정은 삭제됩니다.

엔드포인트 설치 전 검색

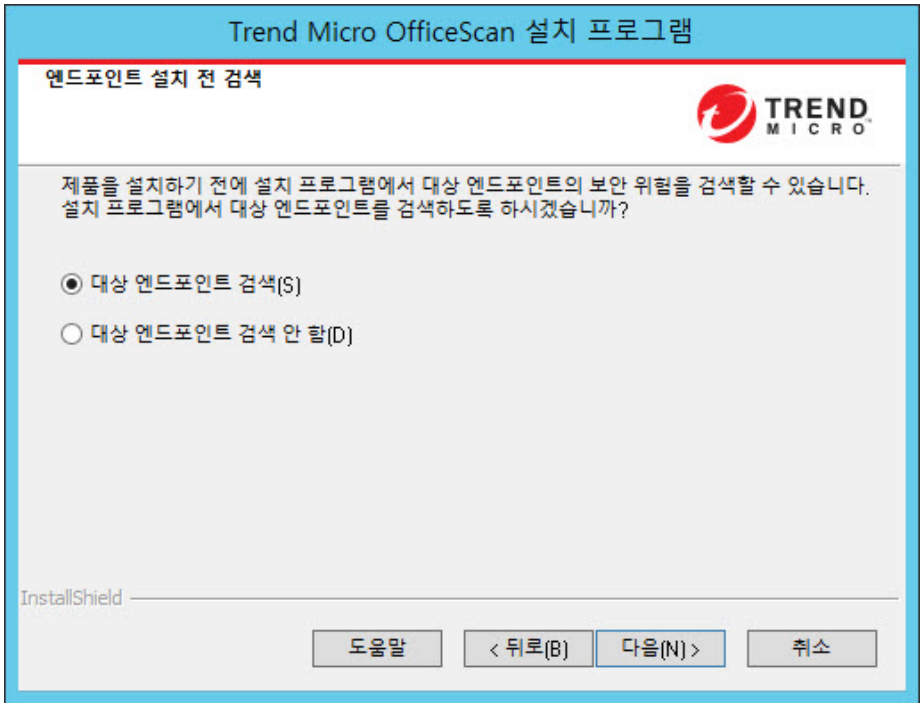

그림 3-26. 엔드포인트 설치 전 검색 화면

설치 프로그램은 OfficeScan 서버 설치를 시작하기 전에 대상 엔드포인트에서 바이러스 및 악성 프로그램을 검색할 수 있습니다. 엔드포인트에서 다음을 비롯한 가장 취약한 영역을 검색합니다.

- 부트 영역 및 부트 디렉터리(부트 바이러스 대상)
- Windows 폴더
- Program Files 폴더

설치 프로그램은 발견된 바이러스/악성 프로그램 및 트로이 목마 프로그램에 대해 다음과 같은 조치를 수행할 수 있습니다.

- **삭제**: 감염된 파일을 삭제합니다.
- **치료**: 파일에 대한 전체 액세스를 허용하기 전에 치료 가능 파일을 치료하거나 지정된 다음 처리 방법으로 치료할 수 없는 파일을 처리합니다.
- **파일명 변경**: 감염된 파일의 확장자를 "vir"로 변경합니다. 사용자가 처음에는 파일을 열 수 없지만 파일을 특정 응용 프로그램에 연결하는 경우 열 수 있습니다. 파일명이 변경된 감염 파일을 열면 바이러스/악성 프로그램이 실행될 수 있습니다.
- **그대로 두기**: 감염된 파일에 대해 아무 조치도 취하지 않고 파일에 대한 전체 액세스를 허용합니다. 사용자가 파일을 열기/복사/삭제할 수 있습니다.

로컬 설치를 수행할 경우 **다음**을 클릭하면 검색이 수행됩니다. 원격 설치를 수행할 경우 실제 설치 직전에 검색이 수행됩니다.

중요

설치 프로그램은 로컬 업그레이드 설치 중 랜섬웨어 위협으로부터 최적화된 보호를 받을 수 있도록 랜섬웨어 보호 설정을 업데이트하라는 메시지를 표시합니다.

업데이트된 설정을 적용하면 이미 동작 모니터링이 사용되도록 설정된 에이전트의 설정만 변경됩니다.

OfficeScan 에이전트 다시 시작 경고

설치 프로그램은 대상 엔드포인트의 리소스를 점검합니다. 업그레이드 시나리오에서 OfficeScan 에이전트 프로그램이 대상 엔드포인트에 있으면 경고 화면이 표시됩니다.

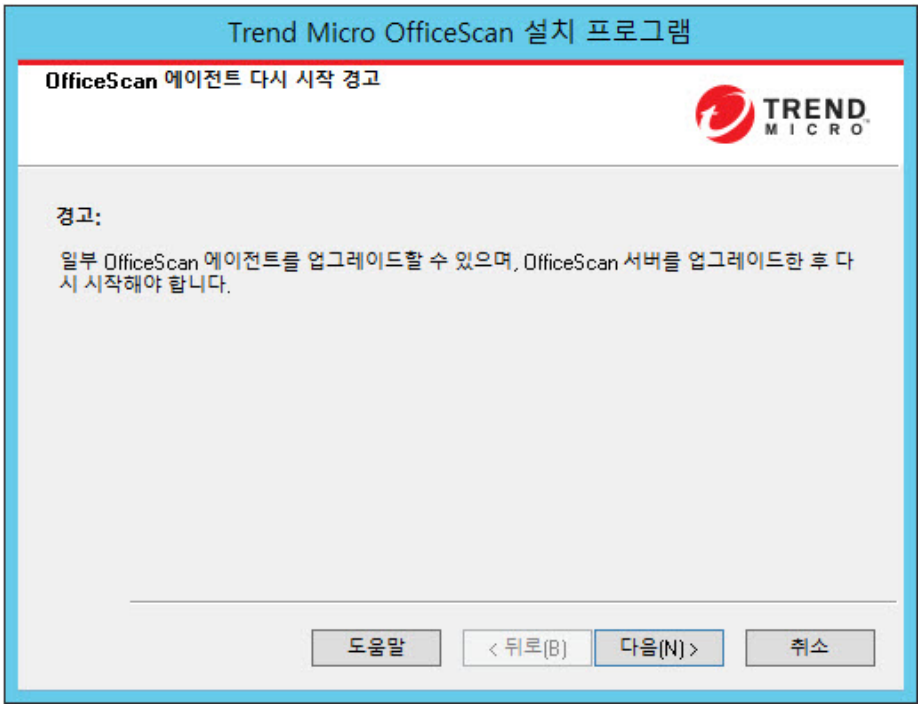

그림 3-27. OfficeScan 에이전트 다시 시작 경고

Apache 제거 경고

OfficeScan XG으로 업그레이드할 때 이전 OfficeScan 서버에 Apache Web Server가 구성되어 있는 경우 경고가 표시됩니다. OfficeScan은 더 이상 Apache Web Server를 지원하지 않습니다.

- 이전 OfficeScan 버전에서 설치 프로그램을 사용하여 Apache Web Server를 설치한 경우 OfficeScan은 Web Server를 자동으로 제거하고 설치 중에 IIS Web Server를 설치할 수 있습니다.
- 이전 OfficeScan 버전을 설치하기 전에 Apache Web Server를 수동으로 설치했다면 OfficeScan 서버 업그레이드를 계속하기 전에 Apache Web Server를 수동으로 제거해야 합니다.

참고

이전의 OfficeScan 서버 버전을 IIS Web Server와 함께 구성한 경우에는 이 경고가 표시되지 않습니다.

데이터베이스 백업

업그레이드할 때 설치 프로그램에서는 최신 버전으로 업그레이드하기 전에 OfficeScan 데이터베이스를 백업할 수 있는 옵션을 제공합니다. 이 백업 정보를 롤백에 사용할 수 있습니다.

참고

백업 패키지에는 300MB를 넘는 사용 가능한 디스크 공간이 필요할 수 있습니다.

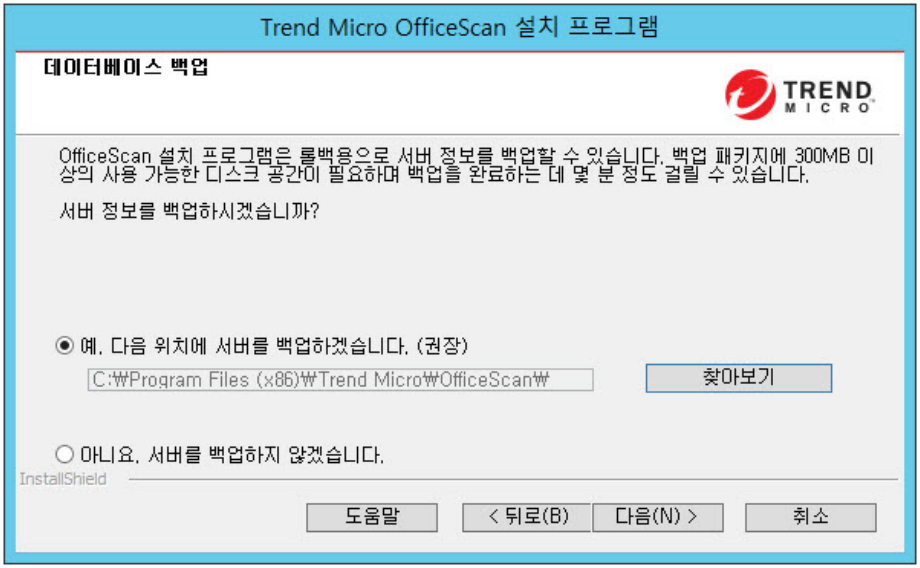

그림 3-28. 데이터베이스 백업 화면

OfficeScan 에이전트 배포

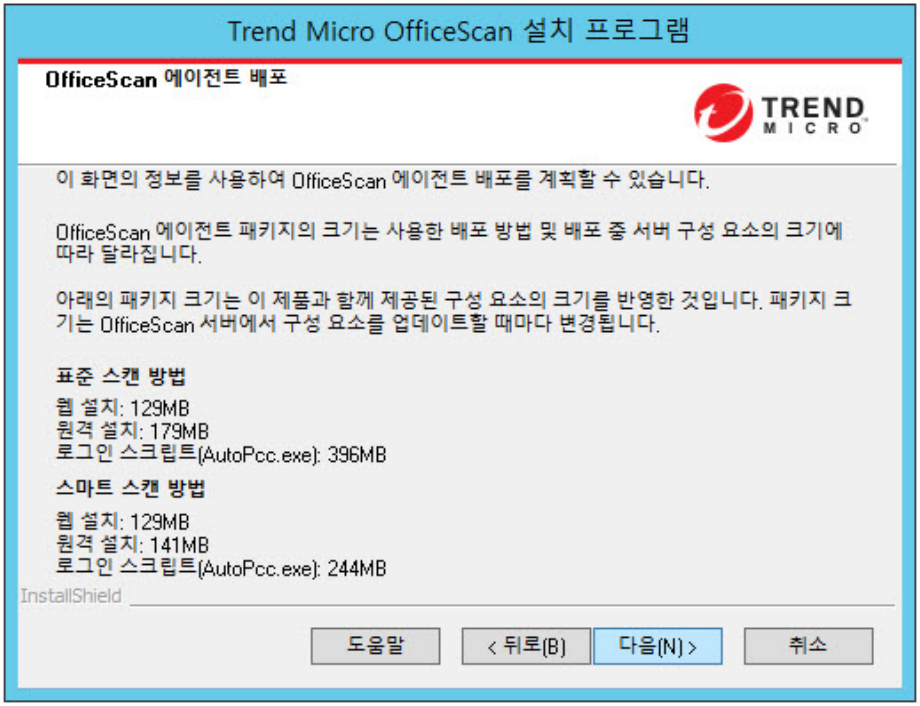

그림 3-29. OfficeScan 에이전트 배포 화면

OfficeScan 에이전트를 설치하거나 업그레이드하는 방법에는 몇 가지가 있습니다. 이 화면에는 서로 다른 배포 방법과 필요한 대략적인 네트워크 대역폭이 나열되어 있습니다.

이 화면을 통해, 대상 엔드포인트에 에이전트를 배포할 때 서버에 필요한 크기와 대역폭 사용량을 예측할 수 있습니다.

참고

이러한 모든 설치 방법에는 대상 엔드포인트의 로컬 관리자 또는 도메인 관리자 권한이 필요합니다.

설치 정보

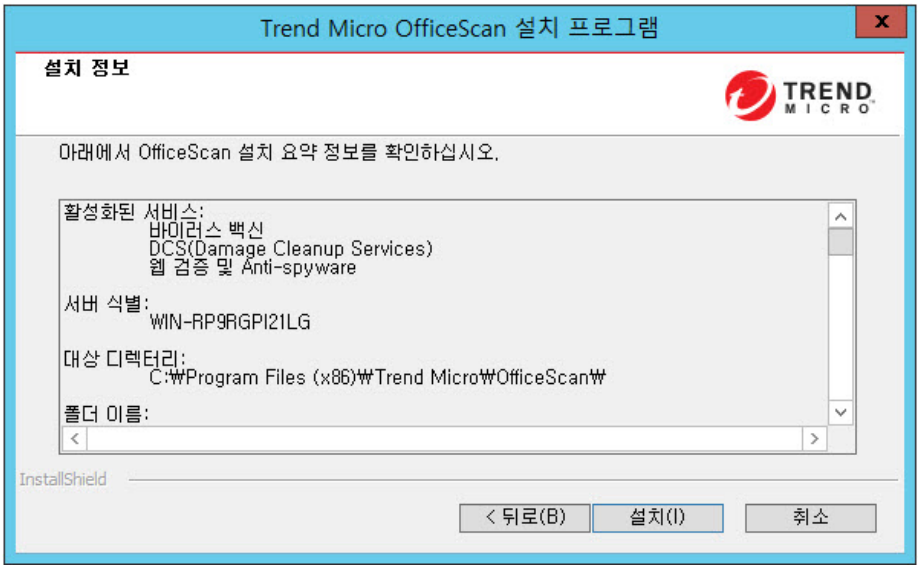

그림 3-30. 설치 정보 화면

이 화면은 설치 설정에 대한 요약을 제공합니다. 설치 정보를 검토하고 **뒤로**를 클릭하여 설정이나 옵션을 변경합니다. 설치를 시작하려면 **설치**를 클릭합니다.

InstallShield 마법사 완료

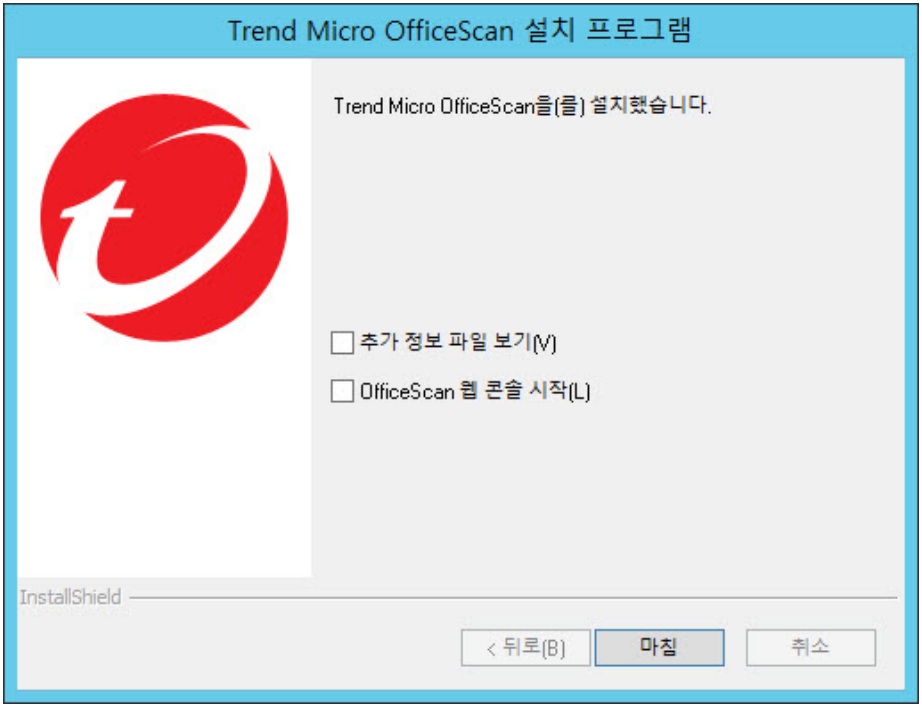

그림 3-31. InstallShield 마법사 완료 화면

설치가 완료되면 추가 정보 파일에서 제품 및 알려진 문제점에 대한 기본 정보를 확인합니다.

관리자는 웹 콘솔을 시작하여 OfficeScan 설정 구성을 시작할 수 있습니다.

원격 업그레이드 수행

원격 업그레이드를 수행할 경우 OfficeScan에서는 업그레이드 시작 전에 이전의 OfficeScan 서버에 구성되어 있는 모든 설정을 확인할 수 없으므로 더 많은 구성 옵션을 제공합니다. 업그레이드할 때 OfficeScan은 업그레이드 설치 중 구성한

설정 대신 이전 OfficeScan 버전 서버의 구성 설정을 사용합니다. 이전 OfficeScan 서버 버전에 설정이 없는 경우에는 OfficeScan이 업그레이드 설치 중에 구성한 설정을 사용합니다.

중요

설치 프로그램은 Apache Web Server를 사용하는 OfficeScan 서버의 원격 업그레이드를 지원하지 않습니다. 로컬 업그레이드를 수행해야 합니다.

사용권 계약

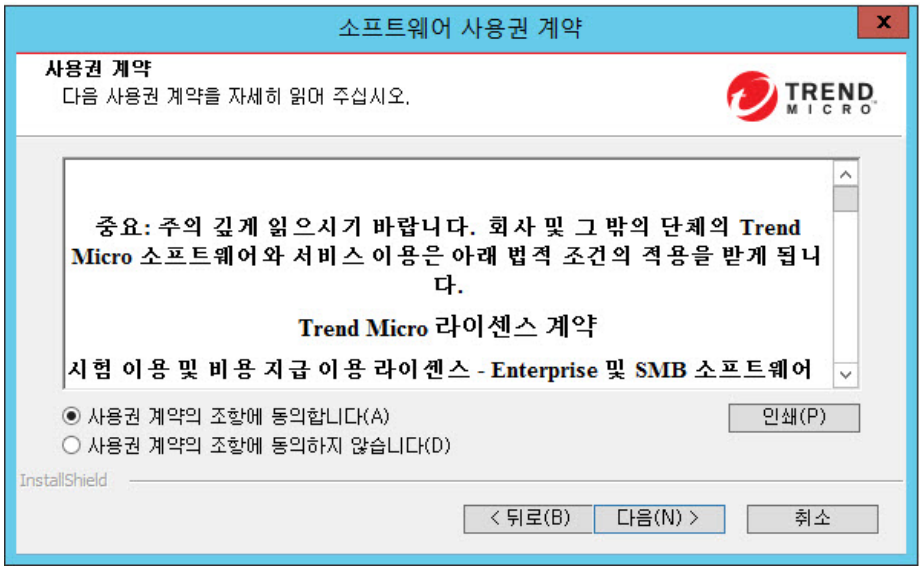

그림 3-32. 사용권 계약 화면

설치를 계속하려면 사용권 계약 내용을 주의 깊게 읽고 사용권 계약 조건에 동의합니다. 사용권 계약 조건에 동의하지 않으면 설치를 진행할 수 없습니다.

설치 대상

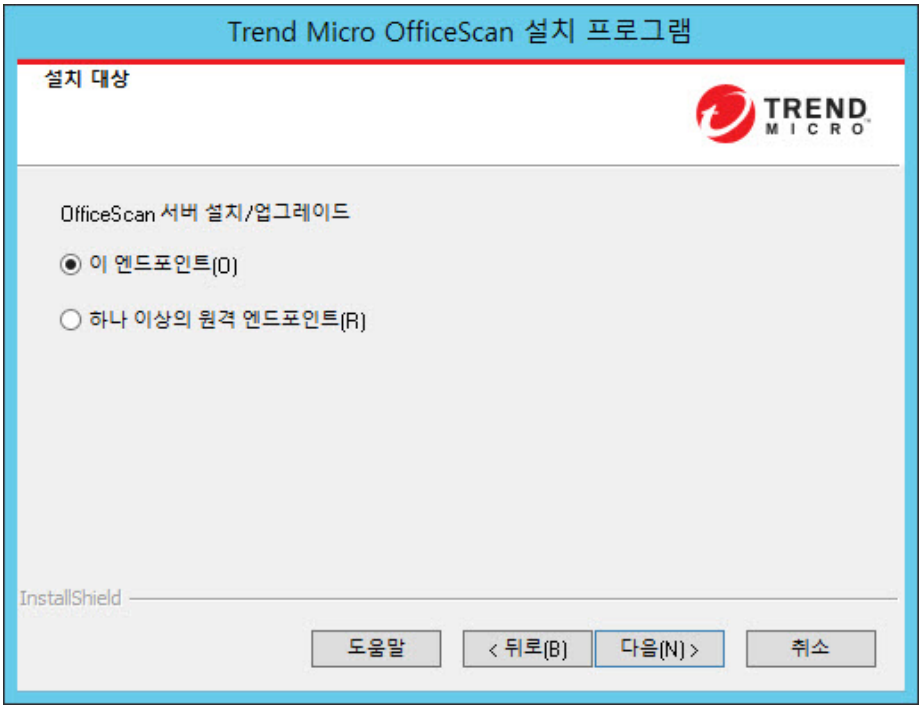

그림 3-33. 설치 대상 화면

현재 엔드포인트나 네트워크의 다른 엔드포인트에서 설치 프로그램을 실행하고 OfficeScan 서버를 설치합니다. 설치 프로그램이 대상 엔드포인트에서 이전 버전의 OfficeScan을 탐지하면 자동으로 업그레이드가 수행됩니다. 다음 버전의 OfficeScan만 이 버전으로 업그레이드할 수 있습니다.

- 11.0 Service Pack 1
- 11.0
- 10.6 Service Pack 3

참고

Trend Micro에서는 업그레이드를 수행하기 전에 현재 OfficeScan 서버에 사용 가능한 모든 패치 및 핫픽스를 적용할 것을 권장합니다.

원격 업그레이드 참고 사항

원격으로 업그레이드할 경우 설치 프로그램에서는 대상 엔드포인트가 서버 업그레이드 요구 사항을 만족하는지 확인합니다. 진행하기 전에

- 대상 엔드포인트에 대한 관리자 권한을 얻습니다.
- 대상 엔드포인트에 대한 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록합니다.
- 대상 엔드포인트가 OfficeScan 서버 설치에 대한 요구 사항을 만족하는지 확인합니다.
- Microsoft IIS Server를 Web Server로 사용할 경우 엔드포인트에 버전 7.0 이상이 있는지 확인합니다.

로컬 업그레이드의 경우 OfficeScan은 서버 이름, 프록시 서버 정보 및 포트 번호를 포함한 이전 설치의 원래 설정을 보존합니다. 업그레이드 시 이러한 설정을 수정할 수 없습니다. 업그레이드한 후에 OfficeScan 웹 콘솔에서 수정합니다.

중요

원격 업그레이드의 경우 모든 설정을 다시 입력합니다. 그러나 서버에서 이전 버전의 설정을 사용하므로 서버 업그레이드 후 이러한 설정은 삭제됩니다.

엔드포인트 설치 전 검색

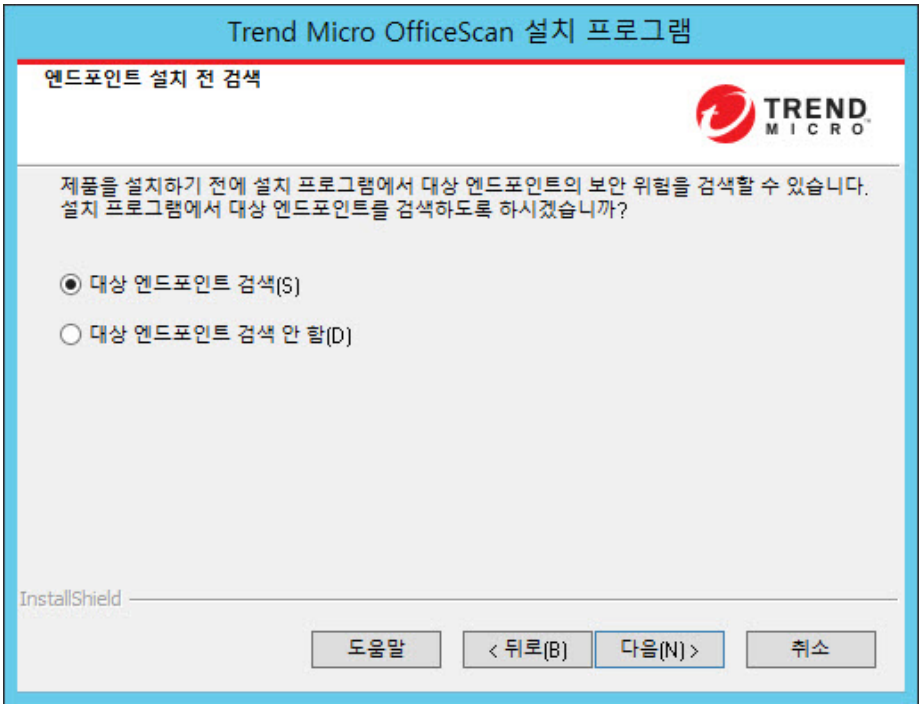

그림 3-34. 엔드포인트 설치 전 검색 화면

설치 프로그램은 OfficeScan 서버 설치를 시작하기 전에 대상 엔드포인트에서 바이러스 및 악성 프로그램을 검색할 수 있습니다. 엔드포인트에서 다음을 비롯한 가장 취약한 영역을 검색합니다.

- 부트 영역 및 부트 디렉터리(부트 바이러스 대상)
- Windows 폴더
- Program Files 폴더

설치 프로그램은 발견된 바이러스/악성 프로그램 및 트로이 목마 프로그램에 대해 다음과 같은 조치를 수행할 수 있습니다.

- **삭제**: 감염된 파일을 삭제합니다.
- **치료**: 파일에 대한 전체 액세스를 허용하기 전에 치료 가능 파일을 치료하거나 지정된 다음 처리 방법으로 치료할 수 없는 파일을 처리합니다.
- **파일명 변경**: 감염된 파일의 확장자를 "vir"로 변경합니다. 사용자가 처음에는 파일을 열 수 없지만 파일을 특정 응용 프로그램에 연결하는 경우 열 수 있습니다. 파일명이 변경된 감염 파일을 열면 바이러스/악성 프로그램이 실행될 수 있습니다.
- **그대로 두기**: 감염된 파일에 대해 아무 조치도 취하지 않고 파일에 대한 전체 액세스를 허용합니다. 사용자가 파일을 열기/복사/삭제할 수 있습니다.

로컬 설치를 수행할 경우 **다음**을 클릭하면 검색이 수행됩니다. 원격 설치를 수행할 경우 실제 설치 직전에 검색이 수행됩니다.

중요

설치 프로그램은 로컬 업그레이드 설치 중 랜섬웨어 위협으로부터 최적화된 보호를 받을 수 있도록 랜섬웨어 보호 설정을 업데이트하라는 메시지를 표시합니다.

업데이트된 설정을 적용하면 이미 동작 모니터링이 사용되도록 설정된 에이전트의 설정만 변경됩니다.

설치 경로

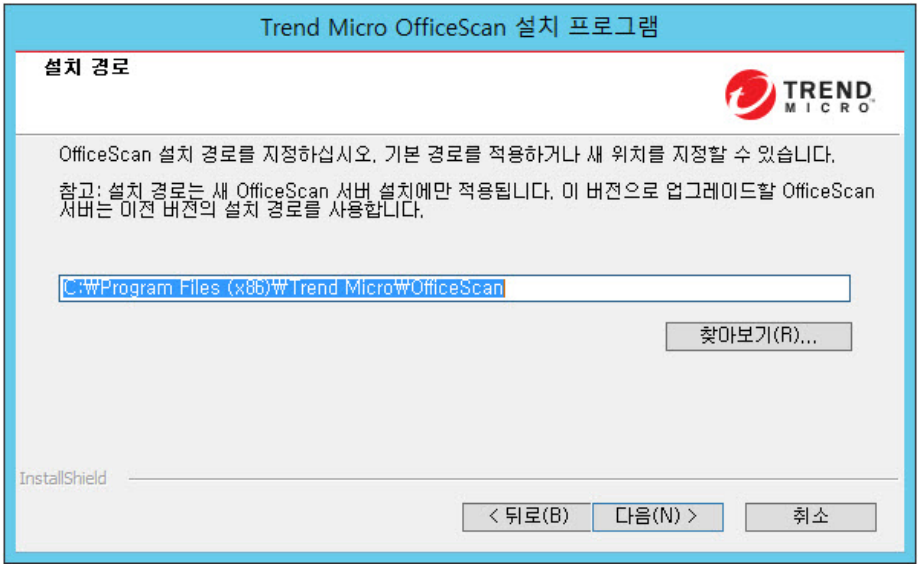

그림 3-35. 설치 경로 화면

기본 설치 경로를 적용하거나 새 경로를 지정합니다.

지정한 설치 경로는 원격 새로 설치를 수행하는 경우에만 적용됩니다. 원격 업그레이드의 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

프록시 서버

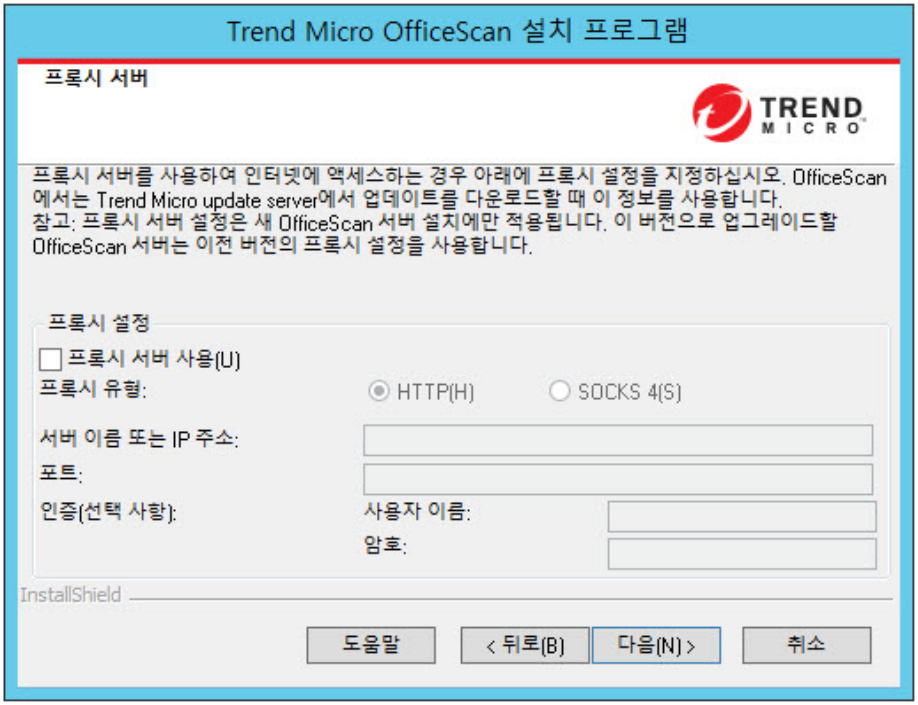

그림 3-36. 프록시 서버 화면

OfficeScan 서버는 HTTP 프로토콜을 사용하여 에이전트-서버 통신을 수행하고 Trend Micro 액티브업데이트 서버에 연결하여 업데이트를 다운로드합니다. 프록시 서버에서 네트워크의 인터넷 트래픽을 처리하는 경우 프록시 서버가 액티브업데이트 서버에서 업데이트를 다운로드할 수 있도록 OfficeScan에 프록시 설정을 지정해야 합니다.

관리자는 프록시 설정을 설치하는 동안 지정하지 않고 설치 후에 OfficeScan 웹 콘솔에서 지정할 수 있습니다.

원격 새로 설치를 수행하는 경우에만 프록시 설정이 적용됩니다. 원격 업그레이드의 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

참고

순수 IPv6 엔드포인트에 OfficeScan 서버를 설치하는 경우 IP 주소 간에 변환할 수 있는 이중 스택 프록시 서버를 설치합니다. 그러면 서버를 액티브업데이트 서버에 연결할 수 있습니다.

Web Server

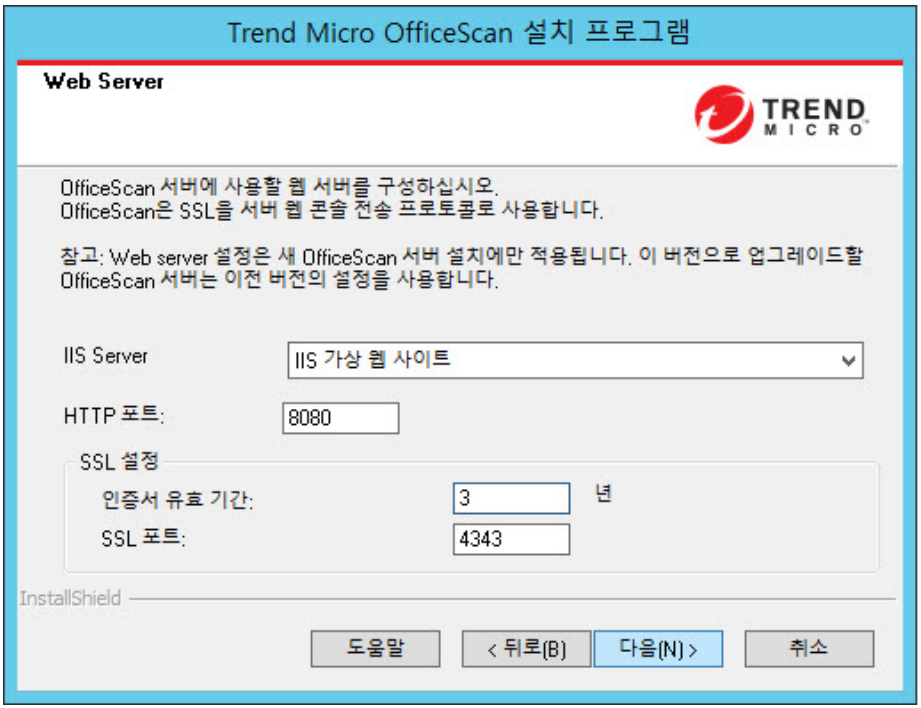

그림 3-37. Web Server 화면

OfficeScan Web Server는 웹 콘솔을 호스팅하고, 관리자가 콘솔 CGI(Common Gateway Interface)를 실행할 수 있도록 하며, 에이전트에서 명령을 받습니다. Web Server에서는 에이전트에서 들어오는 명령을 수신하여 이러한 명령을 에이전트 CGI로 변환한 다음 OfficeScan Master Service로 전달합니다.

원격 새로 설치를 수행하는 경우에만 Web Server 설정이 적용됩니다. 원격 업그레이드를 수행하는 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

IPv6 지원

새로 설치하는 경우 IIS Server를 선택하여 IPv6 지원을 사용하도록 설정합니다.

이 OfficeScan 버전으로 업그레이드하는 경우 업그레이드할 OfficeScan 서버에서 이미 IIS를 사용하고 있어야 합니다.

중요

이전 OfficeScan 서버 설치 패키지를 사용하여 Apache를 설치한 경우 OfficeScan은 업그레이드 프로세스 중에 IIS Web Server를 자동으로 설치하고 구성합니다. Apache 서버를 수동으로 설치했다면 OfficeScan 서버를 업그레이드하기 전에 Apache를 수동으로 제거해야 합니다.

Web Server IIS 지원

- 다음 Microsoft IIS(Internet Information Server) 버전이 필요합니다.
  - Windows Server 2008의 경우 버전 7.0
  - Windows Server 2008 R2의 경우 버전 7.5
  - Windows Server 2012의 경우 버전 8.0
  - Windows Server 2012 R2의 경우 버전 8.5
  - Windows Server 2016의 경우 버전 10.0

  설치가 실패할 수 있으므로 IIS 잠금 응용 프로그램을 실행하는 엔드포인트에는 Web Server를 설치하지 마십시오. 자세한 내용은 IIS 설명서를 참조하십시오.

HTTP 포트

Web Server는 HTTP 포트에서 에이전트 요청을 수신하고 이러한 요청을 OfficeScan Master Service로 전달합니다. 이 서비스는 정보를 지정된 에이전트 통

신 포트에 있는 에이전트에 반환합니다. 설치 프로그램에서는 에이전트 통신 포트 번호를 설치 중에 임의로 생성합니다.

SSL 지원

OfficeScan은 웹 콘솔과 서버 간의 보안 통신을 위해 SSL(Secure Sockets Layer)을 사용합니다. SSL은 해커로부터 보호하는 추가 레이어를 제공합니다. OfficeScan에서는 웹 콘솔에 지정된 암호를 OfficeScan 서버로 보내기 전에 암호화하지만 그럼에도 불구하고 해커가 해당 패킷을 스니핑한 다음 해독하지 않고 "재생"하여 콘솔에 액세스할 수 있습니다. SSL 터널링은 해커가 네트워크를 통과하는 패킷을 몰래 스니핑하지 못하도록 방지합니다.

사용되는 SSL 버전은 Web Server에서 지원하는 버전에 따라 다릅니다.

SSL을 선택하면 설치 프로그램에서 SSL 연결에 대한 요구 사항인 SSL 인증서를 자동으로 만듭니다. 인증서에는 서버 정보, 공개 키 및 개인 키가 들어 있습니다.

SSL 인증서의 유효 기간은 1~20년이어야 합니다. 관리자는 인증서가 만료된 후에도 계속 사용할 수 있습니다. 그러나 해당 인증서를 사용하여 SSL 연결을 요청할 때마다 경고 메시지가 표시됩니다.

SSL을 통한 통신이 작동하는 방법:

1. 관리자는 SSL 연결을 통해 웹 콘솔에서 Web Server로 정보를 보냅니다.
2. Web Server에서는 필요한 인증서를 사용하여 웹 콘솔에 응답합니다.
3. 브라우저에서는 RSA 암호화를 사용하여 키 교환을 수행합니다.
4. 웹 콘솔에서는 RC4 암호화를 사용하여 Web Server로 데이터를 보냅니다.

RSA 암호화가 훨씬 안전하지만 통신 흐름을 더디게 합니다. 따라서 RSA 암호화는 키 교환에만 사용되고 데이터 전송에는 속도가 더 빠른 RC4가 사용됩니다.

Web Server 포트

다음 표에는 Web Server의 기본 포트 번호가 나열되어 있습니다.

표 3-2. OfficeScan Web Server의 포트 번호

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

서버 식별

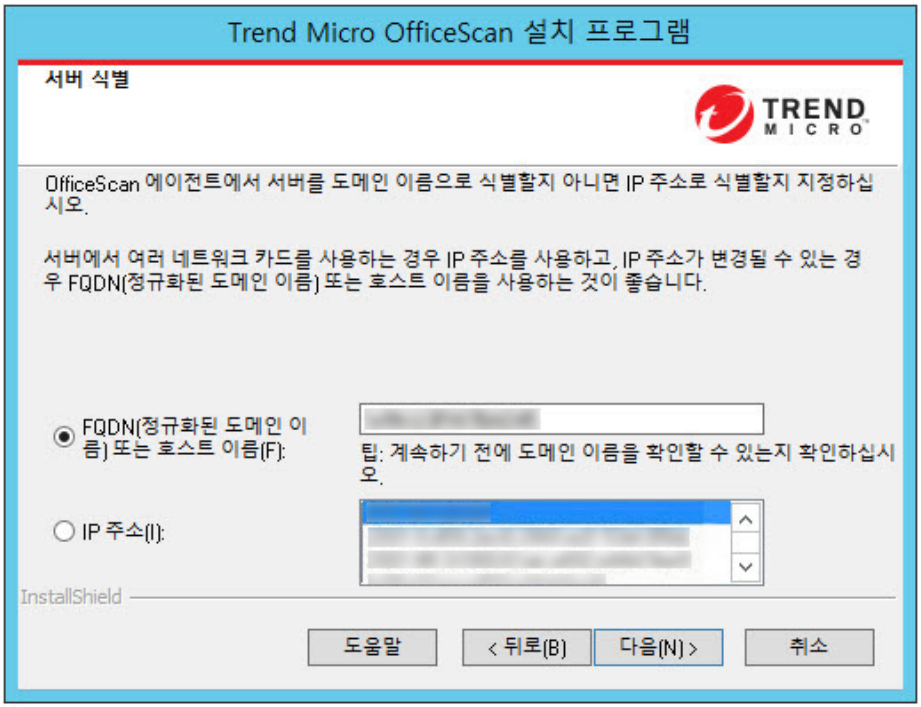

그림 3-38. 서버 식별 화면

이 화면에서 선택한 옵션은 원격 새로 설치를 수행하는 경우에만 적용됩니다. 원격 업그레이드를 수행하는 경우 OfficeScan에서 이전 버전의 설정을 사용합니다.

OfficeScan 에이전트에서 서버 컴퓨터를 FQDN(정규화된 도메인 이름), 호스트(도메인) 이름 또는 IP 주소로 식별할지를 지정합니다.

서버 컴퓨터와 에이전트 간 통신은 지정한 IP 주소에 종속됩니다. 에이전트에서 IP 주소를 변경하면 OfficeScan 서버와 통신할 수 없게 됩니다. 통신을 복원하려면 모든 에이전트를 다시 배포해야 합니다. 서버 컴퓨터를 변경되는 호스트 이름으로 식별하는 경우에도 동일한 상황이 적용됩니다.

대부분의 네트워크에서 서버 컴퓨터의 IP 주소는 호스트 이름보다 변경될 가능성이 크므로 일반적으로 서버 컴퓨터는 호스트 이름으로 식별하는 것이 좋습니다.

팁

호스트 이름 대신 IP 주소를 사용하는 관리자의 경우 설치 후 IP 주소(DHCP 서버에서 가져옴)를 변경하지 않는 것이 좋습니다. 관리자는 DHCP 서버에서 가져온 동일한 IP 주소 정보로 IP 주소 구성을 정적으로 설정하여 OfficeScan 에이전트와의 추가적인 통신 문제를 방지할 수 있습니다.

IP 주소 구성을 유지하는 다른 방법은 OfficeScan 서버에 대해서만 IP 주소를 예약하는 것입니다. 이렇게 하면 DHCP가 사용하도록 설정된 경우에도 DHCP 서버가 OfficeScan에 동일한 IP 주소를 할당합니다.

고정 IP 주소를 사용할 경우 서버를 IP 주소로 식별합니다. 또한 서버 컴퓨터에 여러 개의 NIC(네트워크 인터페이스 카드)를 사용하는 경우에는 에이전트와 서버 간 통신이 제대로 이루어지도록 호스트 이름 대신 IP 주소 중 하나를 사용해 보십시오.

IPv6 지원

서버에서 IPv4 및 IPv6 에이전트를 관리하는 경우 IPv4 주소와 IPv6 주소를 둘 다 사용해야 하고 관리자는 해당 서버를 호스트 이름으로 식별해야 합니다. 관리자가 서버를 IPv4 주소로 식별하면 IPv6 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 서버를 호스트 이름 또는 IPv6 주소로 식별할 수 있습니다. 관리자가 서버를 호스트 이름으로 식별하는 경우에는 FQDN(정규화된 도메인 이름)을 사용하는 것이 좋습니다. 순수 IPv6 환경에서는 WINS 서버가 호스트 이름을 해당 IPv6 주소로 인식할 수 없기 때문입니다.

참고

서버의 로컬 설치를 수행하는 경우에만 FQDN을 지정합니다. 원격 설치에 대해서는 FQDN이 지원되지 않습니다.

등록 및 정품 인증

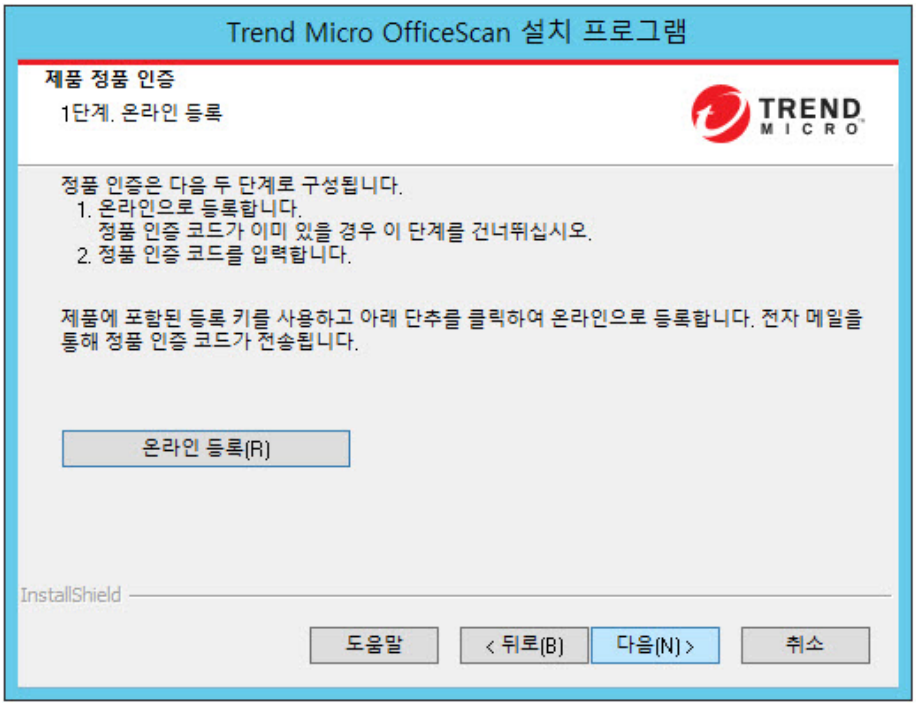

그림 3-39. 제품 정품 인증 - 1단계 화면

제품과 함께 제공된 등록 키를 사용하여 OfficeScan을 등록한 다음 정품 인증 코드를 가져옵니다. 정품 인증 코드를 이미 사용할 수 있는 경우 이 단계를 건너뜁니다.

정품 인증 코드를 가져오려면 **온라인 등록**을 클릭합니다. Trend Micro 등록 웹 사이트가 열립니다. 등록 양식을 완료하면 Trend Micro에서 전자 메일로 정품 인증 코드를 보냅니다. 코드를 받은 후 설치 프로세스를 계속합니다.

순수 IPv6 엔드포인트에 OfficeScan 서버를 설치하는 경우 IP 주소 간에 변환할 수 있는 이중 스택 프록시 서버를 설치합니다. 그러면 서버를 Trend Micro 등록 웹 사이트에 연결할 수 있습니다.

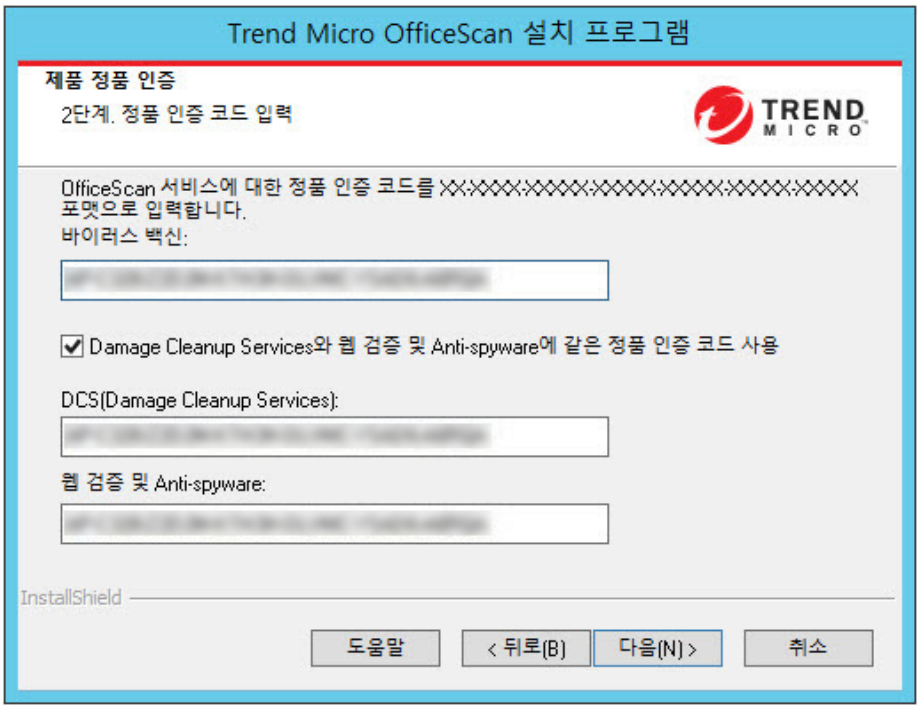

그림 3-40. 제품 정품 인증 - 2단계 화면

정품 인증 코드를 지정합니다. 정품 인증 코드는 대소문자가 구분됩니다.

정품 인증 코드가 모든 서비스에 대해 유효한 경우

1. **바이러스 방역** 텍스트 상자에 정품 인증 코드를 입력합니다.
2. **Damage Cleanup Services와 웹 검증 및 Anti-spyware에 같은 정품 인증 코드 사용**을 선택합니다.
3. **다음**을 클릭하고 라이선스 정보를 확인합니다.

OfficeScan 에이전트 배포

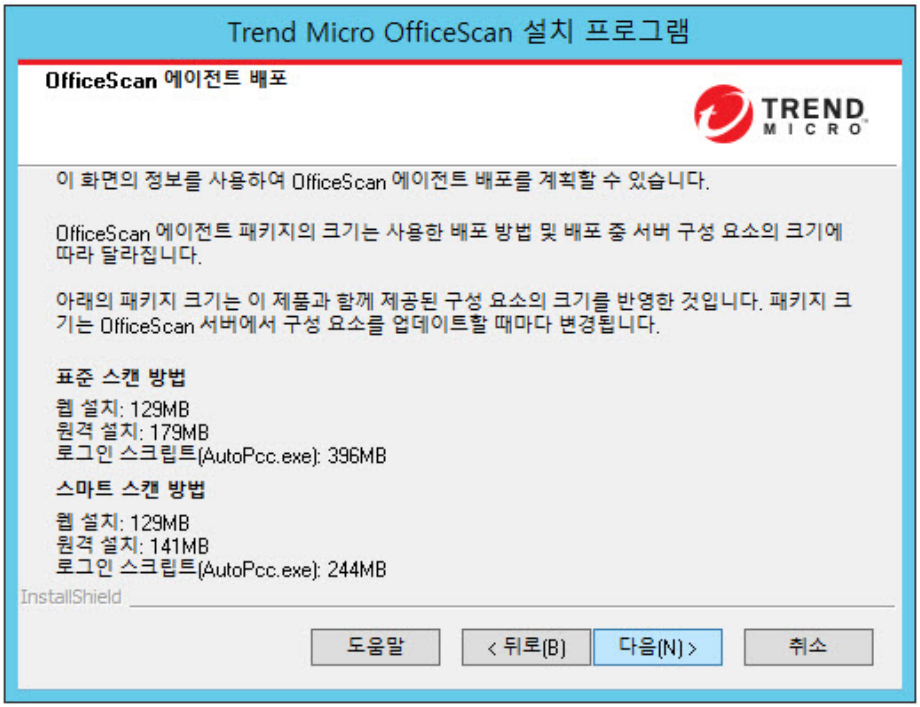

그림 3-41. OfficeScan 에이전트 배포 화면

OfficeScan 에이전트를 설치하거나 업그레이드하는 방법에는 몇 가지가 있습니다. 이 화면에는 서로 다른 배포 방법과 필요한 대략적인 네트워크 대역폭이 나열되어 있습니다.

이 화면을 통해, 대상 엔드포인트에 에이전트를 배포할 때 서버에 필요한 크기와 대역폭 사용량을 예측할 수 있습니다.

참고

이러한 모든 설치 방법에는 대상 엔드포인트의 로컬 관리자 또는 도메인 관리자 권한이 필요합니다.

통합 스마트 보호 서버 설치

참고

로컬 업그레이드 설치 시 IIS 가상 웹 사이트를 사용하는 경우에는 이 화면이 표시되지 않습니다.

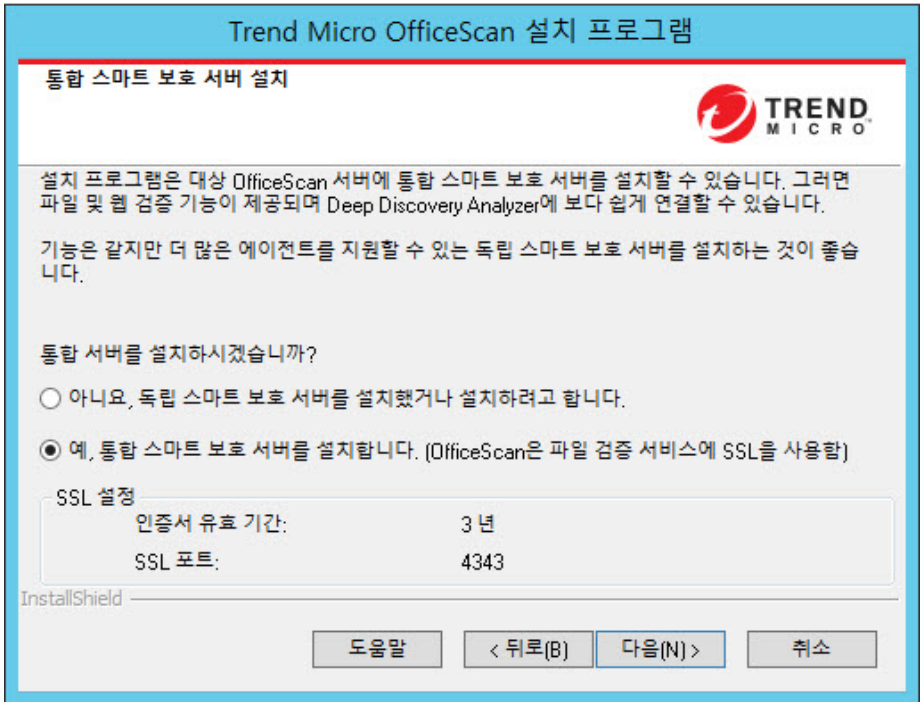

그림 3-42. 통합 스마트 보호 서버 설치 화면

설치 프로그램은 대상 엔드포인트에 통합 스마트 보호 서버를 설치할 수 있습니다. 통합 서버는 스마트 스캔을 사용하는 에이전트에 파일 검증 서비스를 제공하고, 웹 검증 정책이 적용되는 에이전트에 웹 검증 서비스를 제공합니다. OfficeScan 웹 콘솔에서 통합 서버를 관리합니다.

Trend Micro에서는 통합 서버와 기능은 같지만 더 많은 에이전트에 서비스를 제공할 수 있는 독립 스마트 보호 서버를 설치하는 것을 권장합니다. 독립 서버는 별도로 설치되고 자체 관리 콘솔을 포함합니다. 독립 서버에 대한 자세한 내용은 *Trend Micro 스마트 보호 서버 관리자 안내서*를 참조하십시오.

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. 에이전트에 대한 스마트 보호 소스 구성에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

파일 검증 서비스용 에이전트 연결 프로토콜

OfficeScan 에이전트는 HTTP를 사용하여 통합 스마트 보호 서버의 파일 검증 서비스에 연결할 수 있습니다. HTTPS를 사용하면 보다 안전하게 연결할 수 있지만 HTTP가 대역폭을 더 적게 사용합니다.

참고

엔드포인트가 프록시 서버를 통해 통합 서버에 연결되는 경우 웹 콘솔에서 내부 프록시 설정을 구성합니다. 프록시 설정 구성에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

파일 검증 서비스에 사용되는 포트 번호는 OfficeScan 서버에서 사용하는 웹 서버에 따라 다릅니다. 자세한 내용은 Web Server 페이지 2-14를 참조하십시오.

HTTP 포트는 설치 화면에 표시되지 않습니다. HTTPS 포트는 표시되지만 구성은 선택 사항입니다.

표 3-3. 통합 스마트 보호 서버의 파일 검증 서비스에 사용되는 포트

WEB SERVER 및 설정	파일 검증 서비스에 사용되는 포트	
	HTTP	HTTPS (SSL)
IIS 기본 웹 사이트	80	443
IIS 가상 웹 사이트	8080	4343

통합 서버가 설치되어 있지 않음

새로 설치를 수행할 때 통합 서버 설치를 선택하지 않은 경우

- 표준 스캔이 기본 검색 방법이 됩니다.
- 별도의 설치 화면에서 웹 검증 정책을 사용하도록 설정한 경우(자세한 내용은 웹 검증 기능 페이지 2-40 참조) OfficeScan에서는 스마트 보호 서버가 설치되지 않았다고 가정하므로 에이전트가 웹 검증 쿼리를 보낼 수 없습니다.

OfficeScan 설치 후 독립 서버를 사용할 수 있는 경우 OfficeScan 웹 콘솔에서 다음 작업을 수행합니다.

- 검색 방법을 스마트 스캔으로 변경합니다.
- 에이전트가 파일 및 웹 검증 쿼리를 서버에 보낼 수 있도록 독립 서버를 스마트 보호 소스 목록에 추가합니다.

통합 서버를 사용하지 않도록 설정한 OfficeScan 10.x 서버에서 업그레이드하는 경우 통합 서버가 설치되지 않습니다. OfficeScan 에이전트는 검색 방법과 쿼리를 보내는 스마트 보호 소스를 유지합니다.

설치 대상

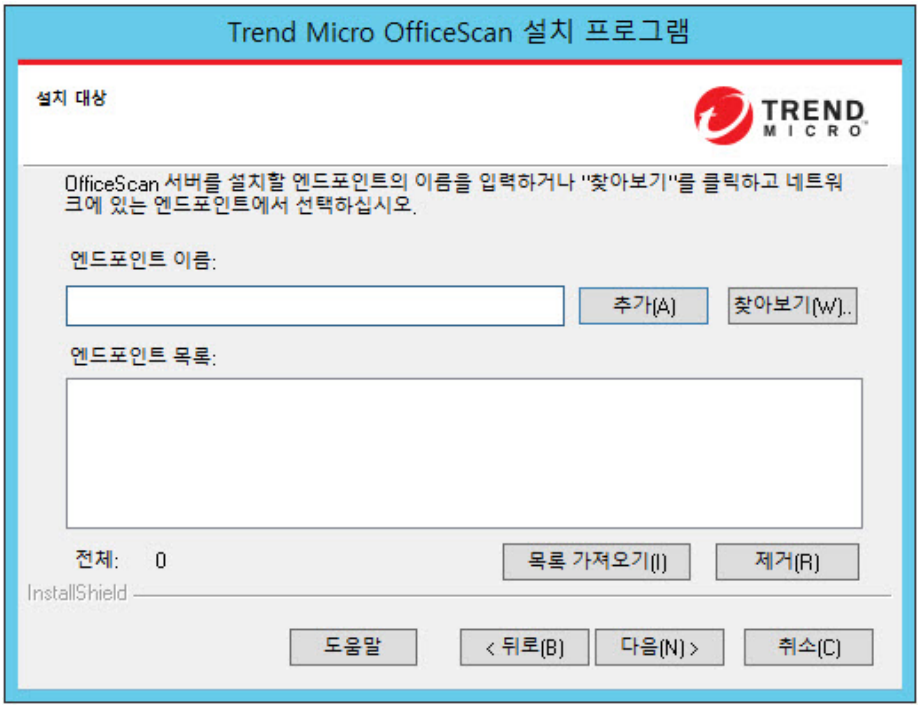

그림 3-43. 설치 대상 화면

OfficeScan이 설치되는 대상 엔드포인트를 지정합니다. 엔드포인트의 호스트 이름 또는 IP 주소를 수동으로 입력합니다. 네트워크에서 엔드포인트를 검색하려면 **찾아보기**를 클릭합니다.

목록 가져오기를 클릭하여 텍스트 파일에서 엔드포인트 이름을 가져옵니다. 여러 엔드포인트에 동시에 설치하고 모든 엔드포인트가 분석을 통과하는 경우 설치 프로그램에서 텍스트 파일에 나열된 순서대로 OfficeScan 서버를 설치합니다.

텍스트 파일에서 다음을 수행합니다.

- 줄당 하나의 엔드포인트 이름을 지정합니다.
- UNC(Unified Naming Convention) 포맷(예: ₩₩test)을 사용합니다.
- a-z, A-Z, 0-9, 마침표(.) 및 하이픈(-) 문자만 사용합니다.

예:

₩₩domain1₩test-abc

₩₩domain2₩test-123

원격 설치를 계속하는 데 필요한 팁:

- 대상 엔드포인트에 대한 관리자 권한을 얻습니다.
- 엔드포인트의 호스트 이름과 로그온 자격 증명(사용자 이름 및 암호)을 기록해 둡니다.
- 대상 엔드포인트가 OfficeScan 서버 설치에 대한 시스템 요구 사항을 만족하는지 확인합니다.
- Microsoft IIS Server를 Web Server로 사용할 경우 엔드포인트에 버전 7.0 이상이 있는지 확인합니다.
- 설치 프로그램을 시작한 엔드포인트를 대상 엔드포인트로 지정하지 마십시오. 해당 엔드포인트에서 로컬 설치를 실행하십시오.

대상 엔드포인트를 지정한 후 **다음**을 클릭합니다. 설치 프로그램에서 엔드포인트가 OfficeScan 설치 요구 사항을 만족하는지 확인합니다.

대상 엔드포인트 분석

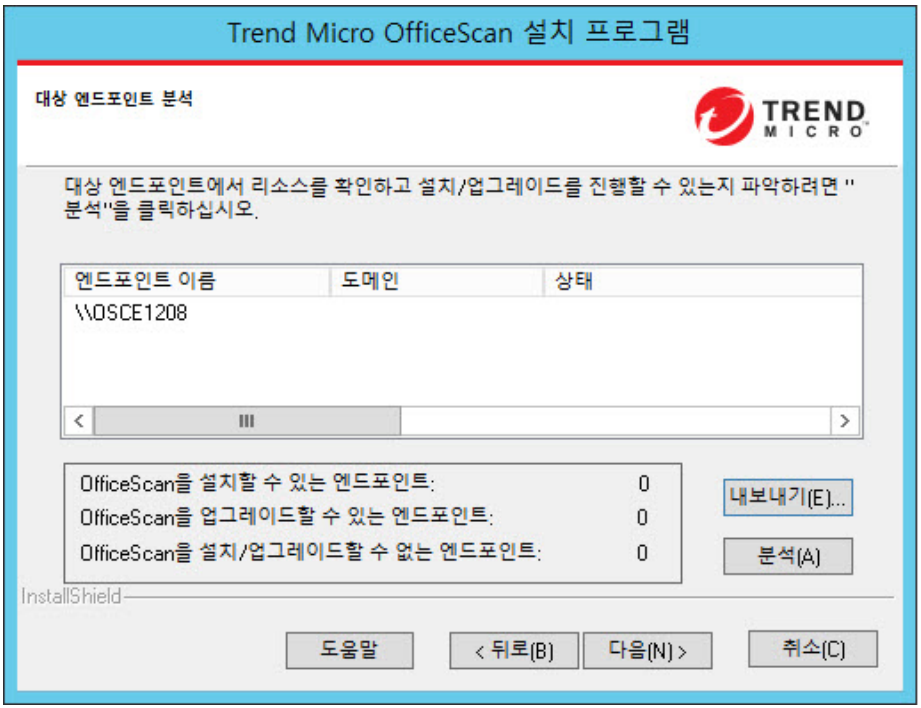

그림 3-44. 대상 엔드포인트 분석 화면

중요

설치 프로그램은 Apache Web Server를 사용하는 OfficeScan 서버의 원격 업그레이드를 지원하지 않습니다. OfficeScan의 원격 업그레이드를 시도하기 전에 Apache Web Server를 수동으로 제거해야 합니다.

원격 설치를 진행하기 전에 설치 프로그램에서는 선택한 대상 엔드포인트에 OfficeScan 서버를 설치할 수 있는지 확인해야 합니다. 분석을 시작하려면 **분석**을 클릭합니다. 대상 엔드포인트에 로그온하는 데 사용되는 관리자 사용자 이름 및 암호를 입력하라는 메시지가 표시될 수 있습니다. 분석 후에는 결과가 화면에 표시됩니다.

중요

설치 프로그램은 서버 분석 중 랜섬웨어 위협으로부터 최적화된 보호를 받을 수 있도록 랜섬웨어 보호 설정을 업데이트하라는 메시지를 표시합니다.

업데이트된 설정을 적용하면 이미 동작 모니터링이 사용되도록 설정된 에이전트의 설정만 변경됩니다.

여러 엔드포인트에 설치하는 경우 하나 이상의 엔드포인트가 분석을 통과하면 설치가 진행됩니다. OfficeScan 서버가 해당 엔드포인트에 설치되고 분석을 통과하지 못한 엔드포인트는 무시됩니다.

원격 설치 중에 설치 진행률은 설치 프로그램을 시작한 엔드포인트에만 표시되고 대상 엔드포인트에는 표시되지 않습니다.

OfficeScan 에이전트 다시 시작 경고

설치 프로그램은 대상 엔드포인트의 리소스를 점검합니다. 업그레이드 시나리오에서 OfficeScan 에이전트 프로그램이 대상 엔드포인트에 있으면 경고 화면이 표시됩니다.

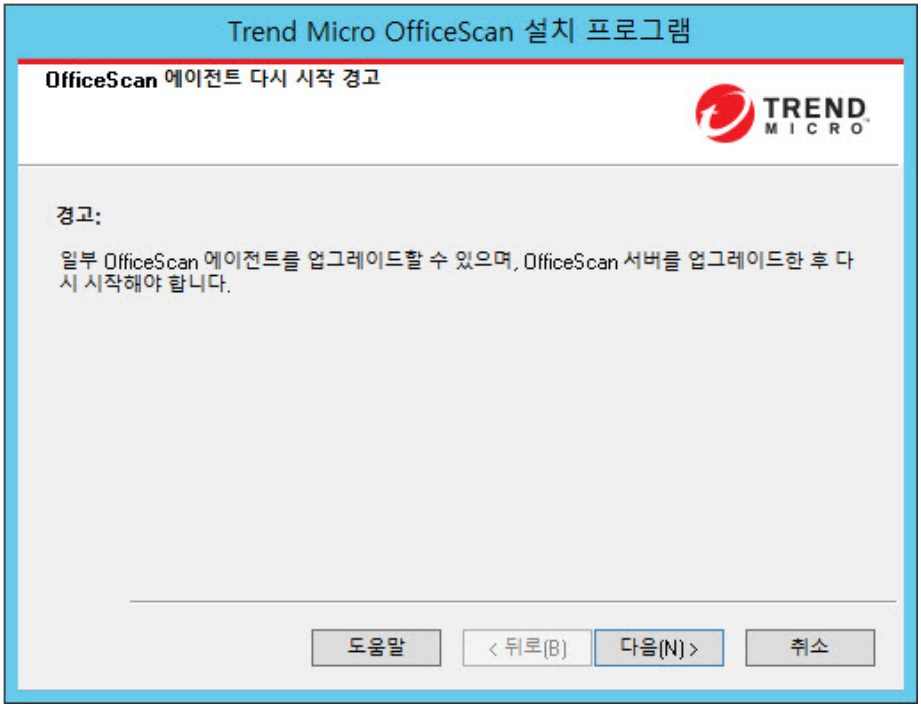

그림 3-45. OfficeScan 에이전트 다시 시작 경고

데이터베이스 백업

업그레이드할 때 설치 프로그램에서는 최신 버전으로 업그레이드하기 전에 OfficeScan 데이터베이스를 백업할 수 있는 옵션을 제공합니다. 이 백업 정보를 롤백에 사용할 수 있습니다.

참고

백업 패키지에는 300MB를 넘는 사용 가능한 디스크 공간이 필요할 수 있습니다.

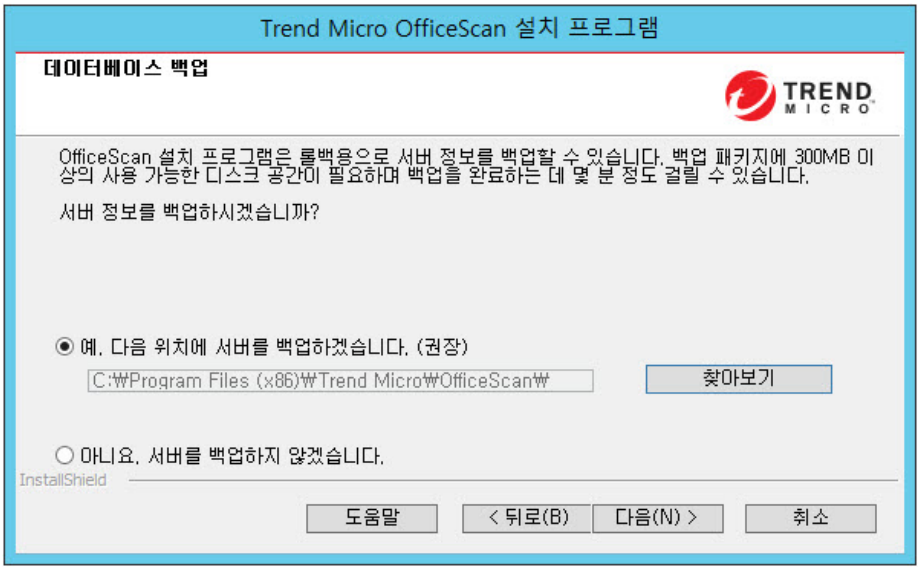

그림 3-46. 데이터베이스 백업 화면

서버 인증 인증서

설치 프로그램은 설치 중에 기존 인증 인증서에 대한 검색을 시도합니다. 기존 인증서가 있는 경우 OfficeScan은 해당 파일을 **서버 인증 인증서** 화면에 매핑합니다. 기존 인증서가 없을 경우에는 OfficeScan이 **새 인증 인증서 생성** 옵션을 기본적으로 사용합니다.

참고

원격 업그레이드 설치 중 **서버 인증 인증서** 화면은 OfficeScan 10.6 SP3 서버를 업그레이드하는 경우에만 나타납니다.

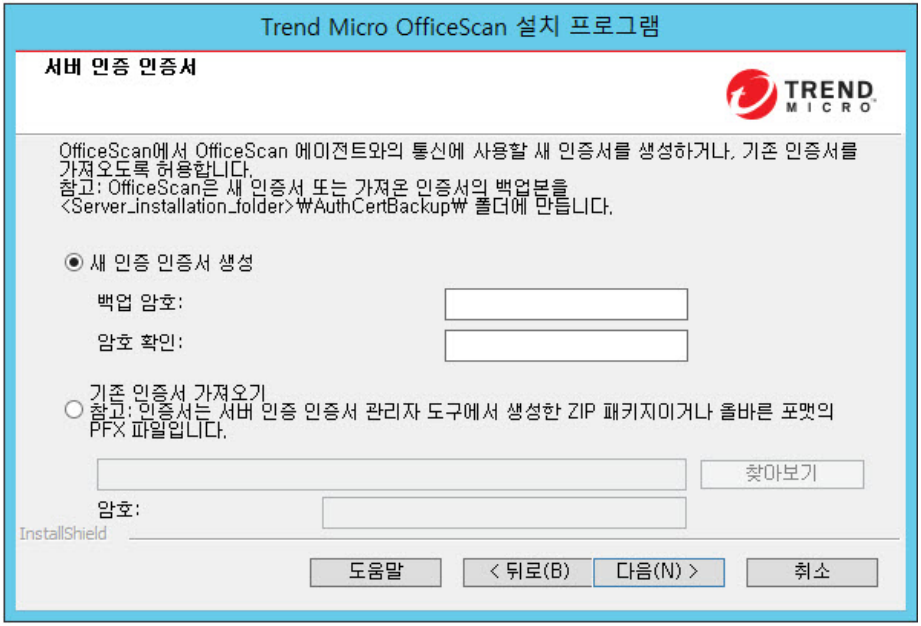

그림 3-47. 새 인증서를 위한 서버 인증 인증서 화면

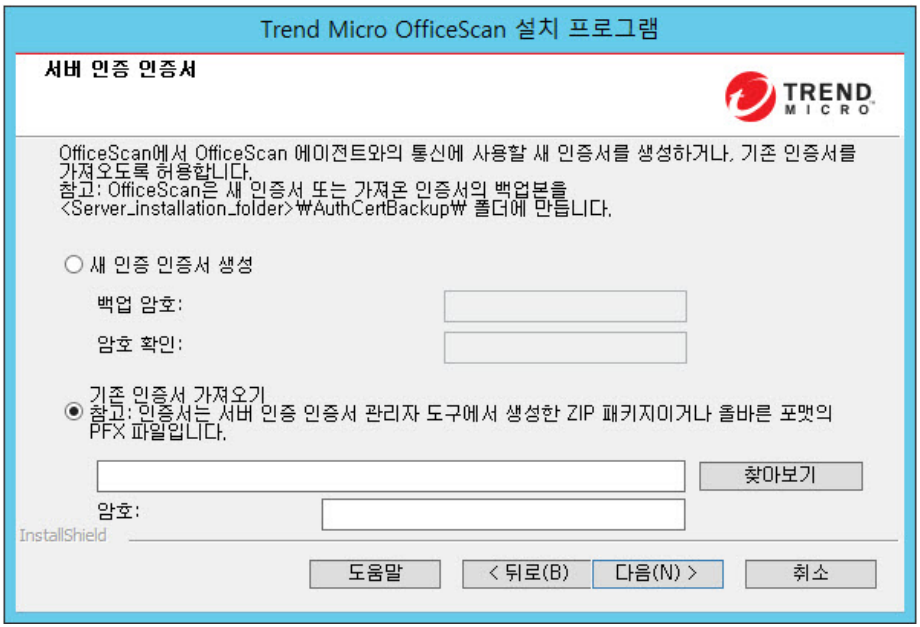

그림 3-48. 기존 인증서를 위한 서버 인증 인증서 화면

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.

OfficeScan이 설치 중에 인증 인증서를 생성하거나 관리자가 다른 OfficeScan 서버에서 기존 인증 인증서를 가져올 수 있습니다.

팁

인증서를 백업할 때는 암호로 인증서를 암호화하는 것이 좋습니다.

설치 정보

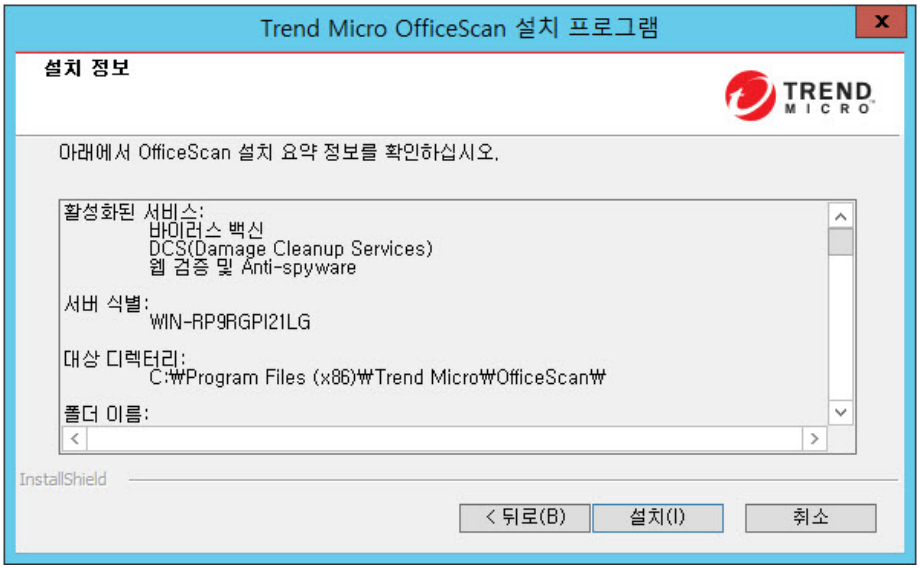

그림 3-49. 설치 정보 화면

이 화면은 설치 설정에 대한 요약을 제공합니다. 설치 정보를 검토하고 **뒤로**를 클릭하여 설정이나 옵션을 변경합니다. 설치를 시작하려면 **설치**를 클릭합니다.

InstallShield 마법사 완료

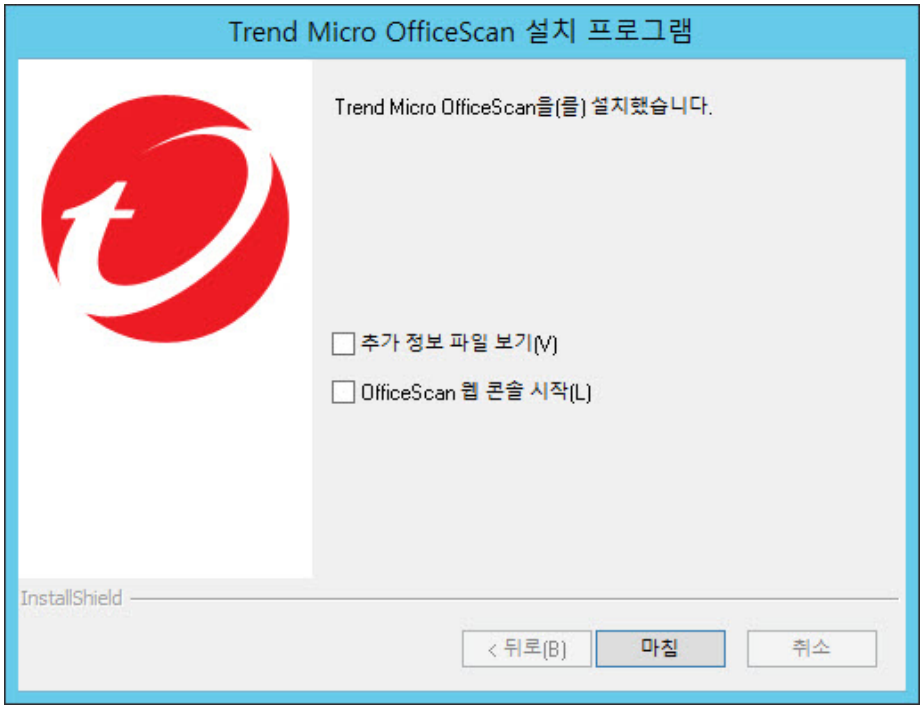

그림 3-50. InstallShield 마법사 완료 화면

설치가 완료되면 추가 정보 파일에서 제품 및 알려진 문제점에 대한 기본 정보를 확인합니다.

관리자는 웹 콘솔을 시작하여 OfficeScan 설정 구성을 시작할 수 있습니다.

장 4

사후 설치 작업

OfficeScan 서버 설치가 완료되면 다음 작업을 수행합니다.

이 장의 내용:

- 서버 설치 또는 업그레이드 확인 페이지 4-2
- OfficeScan 구성 요소 업데이트 페이지 4-4
- 기본 설정 확인 페이지 4-5
- OfficeScan을 Control Manager에 등록 페이지 4-6

서버 설치 또는 업그레이드 확인

설치 또는 업그레이드를 완료한 후 다음을 확인합니다.

표 4-1. OfficeScan 설치 후 확인할 항목

확인할 항목	세부 정보
OfficeScan 서버 바로 가기	Trend Micro OfficeScan 서버 바로 가기는 서버 컴퓨터의 Windows **시작** 메뉴에 표시됩니다.
프로그램 목록	Trend Micro OfficeScan 서버는 서버 컴퓨터의 제어판에 있는 **프로그램 추가/제거** 목록에 나열됩니다.
OfficeScan 웹 콘솔	Internet Explorer 브라우저에 다음 URL을 입력합니다. • HTTPS 연결: `https://<OfficeScan 서버 이름>:<포트 번호>/OfficeScan` 여기서 <OfficeScan 서버 이름>은 OfficeScan 서버의 이름 또는 IP 주소입니다. 웹 콘솔 로그온 화면이 표시됩니다.

확인할 항목	세부 정보
OfficeScan 서버 서비스	다음 OfficeScan 서버 서비스가 Microsoft Management Console에 표시됩니다. • OfficeScan Active Directory Integration Service: 이 서비스는 Active Directory 통합 및 역할 기반 관리 기능이 제대로 작동하는지 여부를 표시합니다. • OfficeScan Control Manager Agent: OfficeScan 서버를 Control Manager에 등록한 경우 이 서비스의 상태는 "시작됨"이어야 합니다. • OfficeScan Deep Discovery Service: 이 서비스의 상태는 "시작됨"이어야 합니다. • OfficeScan Master Service: 이 서비스의 상태는 "시작됨"이어야 합니다. • OfficeScan Log Receiver Service: 이 서비스의 상태는 "시작됨"이어야 합니다. • OfficeScan Plug-in Manager: 이 서비스의 상태는 "시작됨"이어야 합니다. • Trend Micro Smart Scan Server: 이 서비스의 상태는 "시작됨"이어야 합니다. • Trend Micro Local Web Classification Server: 설치하는 동안 웹 검증 서비스를 사용하도록 설정한 경우 이 서비스의 상태는 "시작됨"이어야 합니다.
OfficeScan 서버 프로세스	Windows 작업 관리자를 열면 DBServer.exe가 실행 중입니다.
서버 설치 로그	서버 설치 로그 OFCMAS.LOG는 %windir%에 있습니다.
레지스트리 키	다음 레지스트리 키가 있습니다. • 32비트 플랫폼인 경우: HKEY_LOCAL_MACHINE₩Software₩TrendMicro₩OfficeScan • 64비트 플랫폼인 경우: HKEY_LOCAL_MACHINE₩Software₩Wow6432Node₩TrendMicro₩OfficeScan

확인할 항목	세부 정보
프로그램 폴더	OfficeScan 서버 파일은 <서버 설치 폴더>에 있습니다.

통합 스마트 보호 서버 설치 확인

OfficeScan은 새로 설치하는 동안 자동으로 통합 스마트 보호 서버를 설치합니다.

절차

1. 서버 웹 콘솔에서 **관리** > **스마트 보호** > **스마트 보호 소스**로 이동합니다.
2. **표준 목록** 링크를 클릭합니다.
3. 열리는 화면에서 **통합 스마트 보호 서버**를 클릭합니다.
4. 표시되는 화면에서 **연결 테스트**를 클릭합니다.

   통합 서버와의 연결에 성공해야 합니다.

OfficeScan 구성 요소 업데이트

OfficeScan을 설치한 후 서버에서 구성 요소를 업데이트합니다.

참고

이 섹션은 수동 업데이트 수행에 대해 설명합니다. 예약 업데이트 및 업데이트 구성에 대한 자세한 내용은 *OfficeScan 서버 도움말*을 참조하십시오.

OfficeScan 서버 업데이트

절차

1. 웹 콘솔에 로그온합니다.

2. 기본 메뉴에서 **업데이트** > **서버** > **수동 업데이트** 항목을 클릭합니다.

   현재 구성 요소, 해당 버전 번호 및 최신 업데이트 날짜를 보여주는 **수동 업데이트** 화면이 나타납니다.

3. 업데이트할 구성 요소를 선택합니다.

4. **업데이트**를 클릭합니다. 서버가 업데이트 서버에서 업데이트된 구성 요소를 확인합니다. 업데이트 진행률 및 상태가 표시됩니다.

기본 설정 확인

OfficeScan은 기본 설정으로 설치됩니다. 이러한 설정이 보안 요구 사항에 맞지 않으면 웹 콘솔에서 설정을 수정합니다. 웹 콘솔에서 사용할 수 있는 설정에 대한 자세한 내용은 *OfficeScan 서버 도움말* 및 *관리자 안내서*를 참조하십시오.

검색 설정

OfficeScan에서는 보안 위험으로부터 엔드포인트를 보호하기 위해 몇 가지 검색 유형을 제공합니다. **에이전트** > **에이전트 관리** 항목으로 이동한 다음 **설정** > **{검색 유형}**을 클릭하여 웹 콘솔에서 검색 설정을 수정합니다.

에이전트 설정

OfficeScan은 서버에 등록된 모든 에이전트 또는 특정 권한을 가진 모든 에이전트에 적용되는 몇 가지 설정 유형을 제공합니다. **에이전트** > **글로벌 에이전트 설정**으로 이동하여 웹 콘솔에서 에이전트 설정을 수정합니다.

에이전트 권한

기본 에이전트 권한에는 OfficeScan 에이전트 엔드포인트에 시스템 트레이 아이콘을 표시하는 것이 포함됩니다. 웹 콘솔에서 기본 에이전트 권한을 수정합니다.

1. **에이전트** > **에이전트 관리**으로 이동합니다.
2. **설정** > **권한 및 기타 설정**을 클릭합니다.

OfficeScan을 Control Manager에 등록

Control Manager 서버가 새로 설치된 OfficeScan 서버를 관리하는 경우, 설치 후에 OfficeScan을 Control Manager에 등록합니다.

참고

Control Manager 등록은 새로 설치된 OfficeScan 서버에만 적용됩니다.

OfficeScan 웹 콘솔에서 **관리** > **설정** > **Control Manager** 항목으로 이동합니다.

절차는 *OfficeScan 서버 도움말* 또는 *OfficeScan 관리자 안내서*를 참조하십시오.

장 5

OfficeScan 제거 및 롤백

이 장에서는 Trend Micro™ OfficeScan™을 제거 또는 롤백하는 단계에 대해 설명합니다.

이 장의 내용:

- 제거 및 롤백 고려 사항 페이지 5-2
- OfficeScan 서버를 제거하기 전에 페이지 5-2
- OfficeScan 서버 제거 페이지 5-4
- 서버 백업 패키지를 사용하여 OfficeScan 서버 및 OfficeScan 에이전트 롤백 페이지 5-8
- 이전 OfficeScan 버전으로 수동 롤백 페이지 5-14

제거 및 롤백 고려 사항

OfficeScan에 문제가 있을 경우 다음을 시도해 보십시오.

- 제거 프로그램을 사용하여 엔드포인트에서 OfficeScan 서버를 안전하게 제거합니다. 서버를 제거하기 전에 서버에서 관리하는 에이전트를 다른 OfficeScan 서버로 이동합니다.
- OfficeScan 서버를 제거하는 대신 에이전트를 이전 OfficeScan 버전으로 롤백합니다. 서버 백업 패키지를 사용하여 OfficeScan 서버 및 OfficeScan 에이전트 롤백 페이지 5-8를 참조하십시오.

OfficeScan 서버를 제거하기 전에

제거 프로그램을 사용하여 OfficeScan 서버를 안전하게 제거합니다.

서버를 제거하기 전에 서버에서 관리하는 에이전트를 동일한 버전의 다른 OfficeScan 서버로 이동합니다. 나중에 서버를 다시 설치하려는 경우 서버 데이터베이스와 구성 파일을 백업해두는 것이 좋습니다.

다른 OfficeScan 서버로 에이전트 이동

OfficeScan 웹 콘솔은 서버에서 관리하는 에이전트를 다른 OfficeScan 서버로 이동할 수 있는 옵션을 제공합니다.

절차

1. 다른 OfficeScan 서버에 대한 다음 정보를 기록합니다. 이 정보는 에이전트 이동 시 필요합니다.
   - 엔드포인트 이름 또는 IP 주소
   - 서버 수신 포트

   서버 수신 포트를 보려면 **관리** > **설정** > **에이전트 연결**으로 이동합니다. 포트 번호가 화면에 표시됩니다.

2. 제거할 서버의 웹 콘솔에서 **에이전트** > **에이전트 관리** 항목으로 이동합니다.
3. 에이전트 트리에서 업그레이드할 에이전트를 선택한 다음 **에이전트 트리 관리** > **에이전트 이동**을 클릭합니다.
4. **선택한 에이전트를 다른 OfficeScan 서버로 이동**에서 다른 OfficeScan 서버의 서버 컴퓨터 이름/IP 주소 및 서버 수신 포트를 지정합니다.
5. **이동**을 클릭합니다.

모든 에이전트가 이동하여 이미 다른 OfficeScan 서버에 의해 관리되고 있다면 OfficeScan 서버를 제거해도 안전합니다.

OfficeScan 데이터베이스와 구성 파일 백업 및 복원

OfficeScan 서버를 제거하기 전에 OfficeScan 데이터베이스와 중요 구성 파일을 백업합니다. OfficeScan 서버 데이터베이스를 OfficeScan 프로그램 디렉터리 이외의 위치에 백업합니다.

절차

1. **관리** > **설정** > **데이터베이스 백업**으로 이동하여 웹 콘솔에서 데이터베이스를 백업합니다. 지침은 *관리자 안내서* 또는 *OfficeScan 서버 도움말*을 참조하십시오.

   경고!
   다른 유형의 백업 도구 또는 응용 프로그램을 사용하지 마십시오.

   ---

2. Microsoft Management Console에서 OfficeScan Master Service를 중지합니다.
3. <서버 설치 폴더>₩PCCSRV에 있는 다음 파일과 폴더를 수동으로 백업합니다.
   - ofcscan.ini: 글로벌 에이전트 설정이 들어 있습니다.
   - ous.ini: 바이러스 방역 구성 요소 배포를 위한 업데이트 소스 테이블이 들어 있습니다.

- Private 폴더: 방화벽 및 업데이트 소스 설정이 들어 있습니다.
- Web₩tmOPP 폴더: 바이러스 사전 방역 설정이 들어 있습니다.
- Pccnt₩Common₩OfcPfw*.dat: 방화벽 설정이 들어 있습니다.
- Download₩OfcPfw.dat: 방화벽 배포 설정이 들어 있습니다.
- Log 폴더: 시스템 이벤트 및 연결 확인 로그가 들어 있습니다.
- Virus 폴더: 격리된 파일이 들어 있습니다.
- HTTPDB 폴더: OfficeScan 데이터베이스가 들어 있습니다.

4. OfficeScan 서버를 제거합니다. 자세한 내용은 OfficeScan 서버 제거 페이지 5-4를 참조하십시오.
5. 새로 설치를 수행합니다. 자세한 내용은 OfficeScan 서버 새로 설치 수행 페이지 2-2를 참조하십시오.
6. 설치가 완료되면 Microsoft Management Console을 엽니다(`services.msc`).
7. **OfficeScan Master Service**를 마우스 오른쪽 단추로 클릭한 다음 **중지**를 클릭합니다.
8. 백업 파일을 대상 엔드포인트의 <서버 설치 폴더>₩PCCSRV 폴더에 복사합니다. 이렇게 하면 OfficeScan 서버 데이터베이스, 관련 파일 및 폴더를 덮어씁니다.
9. OfficeScan Master Service를 다시 시작합니다.

OfficeScan 서버 제거

제거 프로그램을 사용하여 OfficeScan 서버 및 통합 스마트 보호 서버를 제거합니다.

제거 프로그램에 문제가 발생하면 서버를 수동으로 제거합니다.

참고

OfficeScan 에이전트 제거 지침에 대해서는 관리자 안내서를 참조하십시오.

제거 프로그램을 사용하여 OfficeScan 서버 제거

절차

1. 제거 프로그램 실행 제거 프로그램에 액세스하는 방법에는 두 가지가 있습니다.

   - 방법 A

   a. OfficeScan 서버 컴퓨터에서 **시작** > **프로그램** > **Trend Micro OfficeScan 서버** > **OfficeScan 제거**를 클릭합니다. 확인 화면이 나타납니다.

   b. **예**를 클릭합니다. 서버 제거 프로그램에서 관리자 암호를 입력하라는 메시지를 표시합니다.

   c. 관리자 암호를 입력하고 **확인**을 클릭합니다. 서버 제거 프로그램이 서버 파일 제거를 시작합니다. 확인 메시지가 나타납니다.

   d. **확인**을 클릭하여 제거 프로그램을 닫습니다.

   - 방법 B

   a. **Windows 프로그램 추가/제거** 화면에서 OfficeScan 서버 프로그램을 두 번 클릭합니다.

   b. **제어판** > **프로그램 추가/제거**를 클릭합니다. "Trend Micro OfficeScan 서버"를 찾아 두 번 클릭합니다. 관리자 암호를 묻는 메시지가 표시될 때까지 화면의 지침을 따릅니다.

   c. 관리자 암호를 입력하고 **확인**을 클릭합니다. 서버 제거 프로그램이 서버 파일 제거를 시작합니다. 확인 메시지가 나타납니다.

   d. **확인**을 클릭하여 제거 프로그램을 닫습니다.

수동으로 OfficeScan 서버 제거

파트 1: 통합 스마트 보호 서버 제거

절차

1. Microsoft Management Console을 열고 OfficeScan Master Service를 중지합니다.
2. 명령 프롬프트를 연 다음 <서버 설치 폴더>₩PCCSRV로 이동합니다.
3. 다음 명령을 실행합니다.

   ```
   SVRSVCSETUP.EXE -uninstall
   ```

   이 명령은 OfficeScan 관련 서비스를 제거하지만 구성 파일이나 OfficeScan 데이터베이스는 제거하지 않습니다.
4. <서버 설치 폴더>₩PCCSRV₩private으로 이동하고 ofcserver.ini를 엽니다.
5. 다음 설정을 수정합니다.

   표 5-1. ofcserver.ini 설정

설정	지침
`WSS_INSTALL`	1에서 0으로 변경
`WSS_ENABLE=1`	이 줄 삭제
`WSS_URL=https://<computer_name>:4345/tmcss/`	이 줄 삭제

6. <서버 설치 폴더>₩PCCSRV로 이동하고 OfUninst.ini를 엽니다. 다음 줄을 삭제합니다.

   ```
   [WSS_WEB_SERVER]

   ServerPort=8082

   IIS_VhostName=스마트 보호 서버(통합)

   IIS_VHostIdx=5
   ```

참고

IIS_VHostidx 값은 다음 줄에 표시된 "isapi" 값과 같아야 합니다.

```
ROOT=/tmcss,C:\Program Files\Trend Micro\OfficeScan\PCCSRV
\WSS\isapi,,<값>
```

```
[WSS_SSL]

SSLPort=<SSL 포트>
```

7. 명령 프롬프트를 연 다음 <서버 설치 폴더>₩PCCSRV로 이동합니다.
8. 다음 명령을 실행합니다.

```
Svrsvcsetup -install

Svrsvcsetup -enablessl

Svrsvcsetup -setprivilege
```

9. 다음 항목이 제거되었는지 확인합니다.
   - Microsoft Management Console의 Trend Micro 스마트 보호 서버 서비스
   - 스마트 보호 서버 성능 카운터
   - 스마트 보호 서버(통합) 웹 사이트

파트 2: OfficeScan 서버 제거

절차

1. 레지스트리 편집기를 열고 다음 단계를 수행합니다.

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.

a. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\로 이동합니다.

b. ofcservice 하이브가 삭제되었는지 확인합니다.

c. HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\으로 이동하고 OfficeScan 하이브를 삭제합니다.

64비트 엔드포인트의 경우 경로는 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\입니다.

d. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\으로 이동합니다. OfficeScan 관리 콘솔-<서버 이름> 폴더를 삭제합니다.

2. <서버 설치 폴더>₩PCCSRV 폴더로 이동하고 PCCSRV 폴더의 공유를 해제합니다.

3. 서버 컴퓨터를 다시 시작합니다.

4. <서버 설치 폴더>₩PCCSRV로 이동하고 PCCSRV 폴더를 삭제합니다.

5. IIS(인터넷 정보 서비스) 콘솔에서 OfficeScan 웹 사이트를 삭제합니다.

a. IIS 콘솔을 엽니다.

b. ServerName을 확장합니다.

c. OfficeScan을 별도의 웹 사이트에 설치한 경우에는 Web Sites 폴더로 이동한 다음 OfficeScan을 삭제합니다.

d. OfficeScan 가상 디렉터리를 기본 웹 사이트에 설치한 경우에는 기본 웹 사이트로 이동한 다음 OfficeScan 가상 디렉터리를 삭제합니다.

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.
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, 시

스템 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.

이전 OfficeScan 버전으로 수동 롤백

OfficeScan 에이전트 업그레이드 시 문제가 발생하면 에이전트를 이전 버전으로 롤백할 수 있습니다.

참고

설치할 때 서버 정보를 백업하지 않은 경우에는 수동 롤백을 수행합니다. 서버 설치 시 서버 정보를 백업하지 않았다면 서버 백업 패키지를 사용하여 OfficeScan 서버 및 OfficeScan 에이전트 롤백 페이지 5-8에 설명되어 있는 롤백 절차를 수행합니다.

롤백하려면 다음을 준비합니다.

- 롤백된 에이전트를 관리할 OfficeScan 서버. 서버 버전은 다음 중 하나여야 합니다.
  - 11.0(모든 Service Pack 포함)

  - 10.6(모든 Service Pack 포함)
- 업데이트 소스로 작동할 엔드포인트. 이 업데이트 소스에는 롤백 파일 및 구성 요소가 포함됩니다. 롤백할 에이전트를 이 소스에서 업데이트하면 OfficeScan 에이전트가 제거된 다음 에이전트의 이전 버전이 설치됩니다.
- 롤백할 에이전트를 관리하는 OfficeScan XG 서버
- 롤백할 OfficeScan XG 에이전트

파트 1: 이전 OfficeScan 서버 버전 준비

절차

1. 이전 OfficeScan 서버 버전이 설치되어 있는 서버를 준비합니다.
2. 이전 OfficeScan 서버 버전용 최신 핫픽스, 패치 또는 서비스 팩을 적용합니다.
3. 다음 OfficeScan XG 서버 설정을 이전 OfficeScan 서버 버전에 복제합니다.
   a. 에이전트 설정

      검색

      업데이트 에이전트

      권한

      스파이웨어/그레이웨어 승인된 목록(OfficeScan 8.0 SP1 이상의 경우)

      동작 모니터링 예외 목록(OfficeScan 10.0 SP1 이상의 경우)

   b. 글로벌 OfficeScan 에이전트 설정

   c. 웹 검증 설정(OfficeScan 8.0 SP1 이상의 경우)

      엔드포인트 위치

      정책

      프록시

d. OfficeScan 방화벽 설정

   정책

   프로필

e. 연결 확인 일정

f. 웹 검증 설정(OfficeScan 8.0 SP1 이상의 경우)

   서버 예약 업데이트

   서버 업데이트 소스

   에이전트 예약 업데이트

   에이전트 업데이트 소스

g. 로그 유지 관리 설정

h. 알림 - 모든 알림 설정

i. 관리 설정

   격리 보관 관리자

   Control Manager

   데이터베이스 백업

4. 이전 OfficeScan 서버 버전에서 클라이언트 패키지 도구를 두 번 실행하여 두 개의 OfficeScan 에이전트 설치 패키지(하나는 x86 엔드포인트용, 다른 하나는 x64 엔드포인트용)를 만듭니다.

   x86 엔드포인트용 OfficeScan 에이전트 설치 패키지의 설정:

   - 패키지 유형: 설정
   - Windows 운영 체제 유형: 32비트
   - 출력 파일: InstNTPkg.exe

   x64 엔드포인트용 OfficeScan 에이전트 설치 패키지의 설정:

   - 패키지 유형: Setup

- Windows 운영 체제 유형: 64비트
- 출력 파일: InstNTPkg.exe

두 출력 파일의 파일 이름이 같기 때문에 한 파일이 다른 파일을 덮어쓰지 않도록 두 출력 파일을 별도의 위치에 저장합니다.

파트 2: 롤백할 에이전트의 업데이트 소스 준비

절차

1. 업데이트 소스로 작동할 엔드포인트를 준비합니다.
2. OfficeScan XG 서버 컴퓨터에서 <서버 설치 폴더>₩PCCSRV로 이동하고 Download 폴더(하위 폴더 포함)를 업데이트 소스 엔드포인트(이전 단계에서 준비한 엔드포인트)에 복사합니다.

   예를 들어, Download 폴더를 업데이트 소스 엔드포인트의 다음 디렉터리에 복사합니다.

   C:₩OfficeScanUpdateSource
3. OfficeScan XG 서버 컴퓨터에서 다음을 수행합니다.
   a. 임시 폴더를 만듭니다.
   b. <서버 설치 폴더>₩PCCSRV₩Admin으로 이동하고 다음 파일을 임시 폴더에 복사합니다.

      RollbackAgent.dll

      RollbackAgent_64x.dll

      ClientRollback.exe
   c. 임시 폴더에서 RollbackAgent.dll을 RollbackAgent.zip으로 압축합니다.
   d. 임시 폴더에서 RollbackAgent_64x.dll을 RollbackAgent_64x.zip으로 압축합니다.
   e. 임시 폴더에서 하위 폴더를 만들고 이름을 RollBackNTPkg로 지정합니다.

f. 다음 파일을 RollBackNTPkg 하위 폴더에 복사합니다.

ClientRollback.exe

파트 1, 4단계에서 만든 x86 엔드포인트용 OfficeScan 에이전트 설치 패키지(InstPkg.exe)

g. RollbackNTPkg 하위 폴더를 RollbackNTPkg.zip으로 압축합니다.

h. 임시 폴더에서 하위 폴더를 만들고 이름을 RollBackNTPkgx64로 지정합니다.

i. 다음 파일을 RollBackNTPkgx64 하위 폴더에 복사합니다.

ClientRollback.exe

파트 1, 4단계에서 만든 x64 엔드포인트용 에이전트 설치 패키지(InstPkg.exe)

j. RollbackNTPkgx64 하위 폴더를 RollbackNTPkgx64.zip으로 압축합니다.

k. 임시 폴더의 다음 압축 파일을 업데이트 소스 엔드포인트에 복사합니다.

RollbackAgent.zip

RollbackAgent_64x.zip

RollbackNTPkg.zip

RollbackNTPkgx64.zip

참고

파일을 업데이트 소스 엔드포인트의 ₩Download₩Product 폴더에 복사합니다. 예를 들어, 파일을 C:₩OfficeScanUpdateSource₩Download₩Product에 복사합니다.

4. 업데이트 소스 엔드포인트에서 다음을 수행합니다.

a. "인터넷 게스트 계정"에 ₩Download₩Product(예: C:₩OfficeScanUpdateSource₩Download₩Product)의 다음 압축 파일에 대한 읽기 권한이 있는지 확인합니다.

RollbackAgent.zip

RollbackAgent_64x.zip

RollbackNTPkg.zip

RollbackNTPkgx64.zip

팁

액세스 권한을 확인하려면 각 파일을 마우스 오른쪽 단추로 클릭하고 속성을 선택합니다. 보안 탭에서 인터넷 게스트 계정의 사용 권한이 "읽기"여야 합니다.

5. ₩Download₩Product 폴더에서 텍스트 편집기(예: 메모장)를 사용하여 server.ini 파일을 엽니다.

6. server.ini 파일의 다음 줄을 수정한 다음 파일을 저장합니다.

경고!

server.ini 파일의 다른 설정은 변경하지 마십시오.

```
[All_Product]

MaxProductID=109

Product.109=OfficeScan Rollback, 3.5, <현재 OfficeScan 버전>

[Info_109_35000_1_5633]

Version=<이전 OfficeScan 버전>

Update_Path=product/RollbackAgent_64x.zip, <RollbackAgent64 파일 크기>

Path=product/RollBackNTPkgx64.zip, <RollBackNTPkg64 파일 크기>
```

여기서 각 항목은 다음과 같습니다.

<RollbackAgent 파일 크기>: "RollbackAgent.zip"의 파일 크기는 바이트 단위입니다. 예를 들면 90517입니다.

<RollBackNTPkg 파일 크기>: "RollbackNTPkg.zip"의 파일 크기는 바이트 단위입니다. 예를 들면 32058256입니다.

<RollbackAgent64 파일 크기>: "RollbackAgent_64x.zip"의 파일 크기는 바이트 단위입니다. 예를 들면 90517입니다.

<RollBackNTPkg64 파일 크기>: RollbackNTpkgx64.zip의 파일 크기는 바이트 단위입니다. 예를 들면 36930773입니다.

팁

파일 크기를 확인하려면 .zip 파일을 마우스 오른쪽 단추로 클릭하고 **속성**을 클릭합니다. 디스크에서의 크기가 아니라 이 크기에 유의하십시오.

<현재 OfficeScan 버전>: 현재 OfficeScan 버전(XG)

<이전 OfficeScan 버전>: 이전 OfficeScan 버전입니다. 예를 들면 10.0입니다.

파트 3: OfficeScan 에이전트 롤백

절차

1. OfficeScan XG 웹 콘솔에서 **업데이트** > **에이전트** > **업데이트 소스**로 이동합니다.
   a. **사용자 정의 업데이트 소스**를 선택합니다.
   b. **사용자 정의 업데이트 소스 목록**에서 **추가**를 클릭합니다. 새 화면이 열립니다.
   c. 롤백할 에이전트의 IP 주소를 입력합니다.
   d. 업데이트 소스 URL을 입력합니다. 예를 들어 다음과 같이 입력합니다.

      `http://<업데이트 소스의 IP 주소>/OfficeScanUpdateSource/`

   e. **저장**을 클릭합니다.

      화면이 닫힙니다.

f. **모든 에이전트에 알림**을 클릭합니다.

롤백할 에이전트를 업데이트 소스에서 업데이트하면 OfficeScan 에이전트가 제거되고 이전 클라이언트 버전이 설치됩니다.

2. 이전 클라이언트 버전이 설치된 후 사용자에게 엔드포인트를 다시 시작하도록 알립니다. 다시 시작하고 나면 OfficeScan 에이전트가 파트 1에서 준비한 OfficeScan 서버에 보고합니다.

장 6

OfficeScan 문제 해결 리소스

이 장에서는 이 OfficeScan 버전에서 발생할 수 있는 문제를 해결하는 데 사용할 수 있는 리소스에 대해 설명합니다.

이 장의 내용:

- 지원 정보 시스템 페이지 6-2
- Case Diagnostic Tool 페이지 6-2
- Trend Micro 성능 조정 도구 페이지 6-2
- 설치 로그 페이지 6-4
- 서버 디버그 로그 페이지 6-5
- 에이전트 디버그 로그 페이지 6-7

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. GUID를 제공하면 Trend Micro가 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.

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 도구는 동작 모니터링 및 장치 제어의 실제 배포에서 성능 문제를 미리 파악하기 위해 파일 럿 프로세스 동안 표준 워크스테이션 이미지 및/또는 일부 대상 워크스테이션에서 실행되어야 합니다.

참고

Trend Micro 성능 조정 도구는 32비트 플랫폼만 지원합니다.

시스템 집약적인 응용 프로그램 식별

절차

1. 다음 위치에서 Trend Micro 성능 조정 도구를 다운로드합니다.

http://solutionfile.trendmicro.com/solutionfile/1054312/EN/TMPerfTool_2_90_1131.zip

2. TMPerfTool.zip의 압축을 풀어 TMPerfTool.exe를 추출합니다.
3. TMPerfTool.exe를 <클라이언트 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. 도구가 CPU 사용량 및 이벤트 로드를 모니터링하기 시작합니다.

   시스템 집약적인 프로세스는 빨간색으로 강조 표시됩니다.

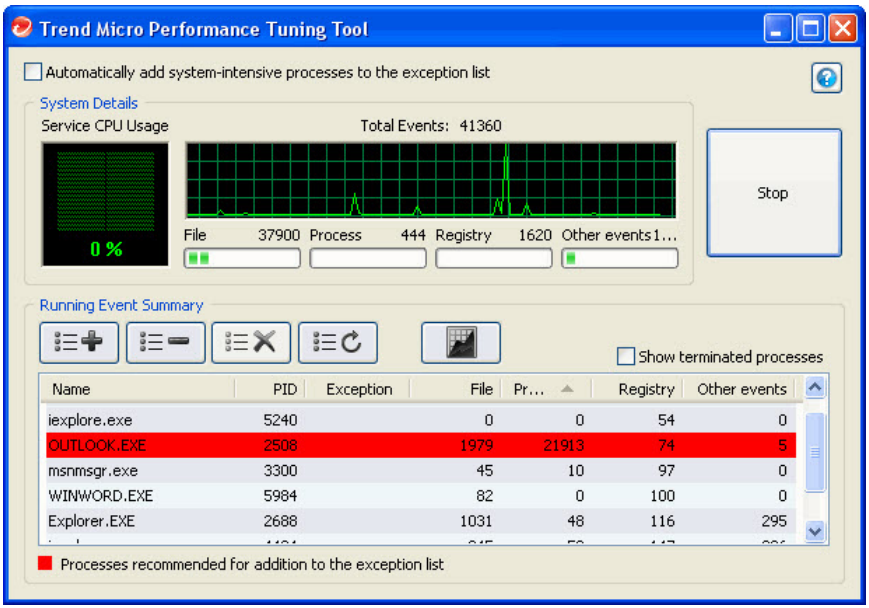

그림 6-1. 강조 표시된 시스템 집약적인 프로세스

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 클릭한 다음 .xml 파일을 저장합니다.
    d. 충돌하는 것으로 식별된 응용 프로그램을 검토하여 동작 모니터링 예외 목록에 추가합니다. 자세한 내용은 *관리자 안내서*를 참조하십시오.

설치 로그

OfficeScan에서 자동으로 생성하는 설치 로그 파일을 사용하여 설치 문제점을 해결합니다.

표 6-1. 설치 로그 파일

로그 파일	파일 이름	위치
서버 로컬 설치/업그레이드 로그	OFCMAS.LOG	%windir%
서버 원격 설치/업그레이드 로그	OFCMAS.LOG(설치를 시작한 엔드포인트) OFCMAS.LOG(대상 엔드포인트)	%windir%

로그 파일	파일 이름	위치
OfficeScan 에이전트 설치 로그	OFCNT.LOG	%windir%(MSI 패키지를 제외한 모든 설치 방법에 해당) %temp%(MSI 패키지 설치 방법에 해당)

서버 디버그 로그

다음 서버 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)

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. 파일 크기가 커지면 로그 파일을 제거하십시오.

OfficeScan 서버 컴퓨터에서 디버그 로깅 사용

옵션 1:

절차

1. 웹 콘솔에 로그온합니다.
2. 웹 콘솔 배너에서 "OfficeScan"의 "**O**"를 클릭합니다. 그러면 **디버그 로그 설정** 화면이 열립니다.

3. 디버그 로그 설정을 지정합니다.
4. **저장**을 클릭합니다.
5. 다음 기본 위치의 로그 파일(ofcdebug.log)을 확인합니다: <서버 설치 폴더>₩PCCSRV₩Log.

옵션 2:

절차

1. <서버 설치 폴더>₩PCCSRV₩Private에 있는 "LogServer" 폴더를 C:₩에 복사합니다.
2. ofcdebug.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 재설치, 새 서버 버전으로 업그레이드 또는 원격 설치/업그레이드 수행).
5. C:₩LogServer에서 ofcdebug.log를 확인합니다.

참고

OfficeScan 에이전트가 OfficeScan 서버에 있는 경우 에이전트는 해당 디버그 로그를 서버의 디버그 로그에도 출력합니다.

에이전트 디버그 로그

OfficeScan 에이전트를 설치하기 전에 디버그 로깅을 사용하도록 설정합니다.

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.

OfficeScan 에이전트에서 디버그 로깅 사용

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. 에이전트 사용자에게 ofcdebug.ini를 보내 C:₩에 파일을 저장하도록 지시합니다.

LogServer.exe는 에이전트 엔드포인트가 시작할 때마다 자동으로 실행됩니다.

3. 디버그 로깅을 시작하려면 OfficeScan 에이전트를 다시 로드하거나 엔드포인트를 다시 시작합니다.

   엔드포인트가 시작될 때 열리는 LogServer.exe 명령 창을 닫으면 OfficeScan이 디버그 로깅을 중지하므로 사용자에게 이 창을 닫지 않도록 지시합니다. 사용자가 명령 창을 닫은 경우 ₩OfficeScan Client에 있는 LogServer.exe를 실행하여 다시 디버그 로깅을 시작할 수 있습니다.

4. 각 에이전트 엔드포인트의 C:₩에서 ofcdebug.log를 확인합니다.

5. OfficeScan 에이전트에 대해 디버그 로깅을 사용하지 않도록 설정하려면 ofcdebug.ini를 삭제합니다.

장 7

기술 지원

다음 항목에 대해 자세히 알아보십시오.

- 문제 해결 리소스 페이지 7-2
- Trend Micro 연락처 페이지 7-3
- 의심스러운 콘텐츠를 Trend Micro로 보내기 페이지 7-4
- 기타 리소스 페이지 7-5

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 A

샘플 배포

이 섹션에서는 네트워크 토폴로지 및 사용 가능한 네트워크 리소스를 기반으로 OfficeScan을 배포하는 방법에 대해 설명합니다. 조직에서 OfficeScan 배포를 계획할 때 본 문서를 참조로 사용하십시오.

기본 네트워크

그림 1은 OfficeScan 서버와 에이전트가 직접 연결되어 있는 기본 네트워크를 보여줍니다. 이 구성은 LAN(및/또는 WAN) 액세스 속도가 10Mbps, 100Mbps 또는 1Gbps로서 대부분의 비즈니스 네트워크에 적용됩니다. 이 시나리오에서는 OfficeScan 시스템 요구 사항을 만족하고 충분한 리소스가 있는 엔드포인트가 OfficeScan 서버 설치에 가장 적합합니다.

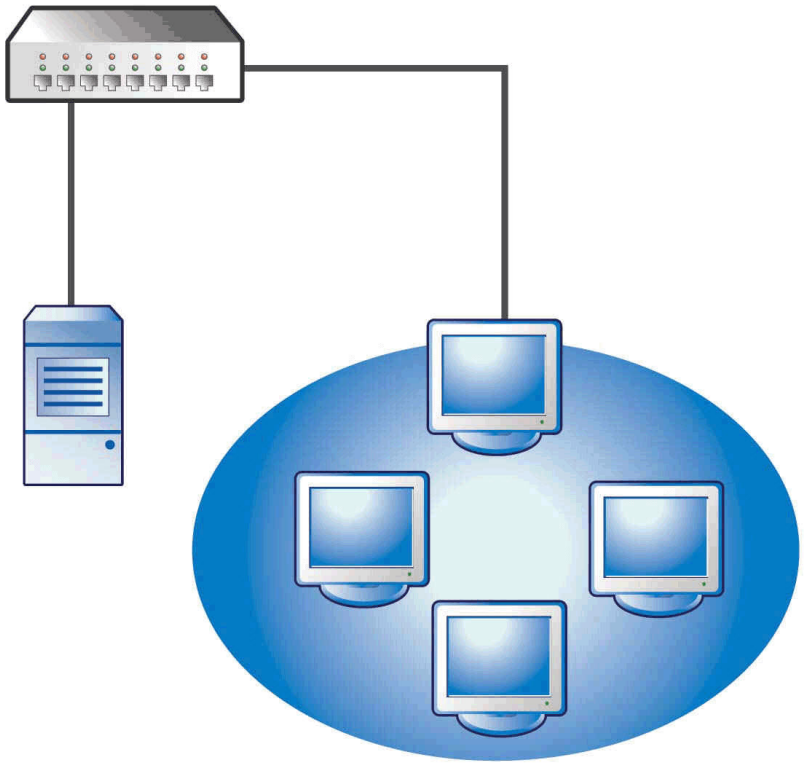

그림 A-1. 기본 네트워크 토폴로지

다중 사이트 네트워크

대역폭이 다른 원격 사이트와 액세스 포인트가 여러 개 있는 네트워크의 경우

- 사무실 및 네트워크 대역폭과 관련하여 통합 포인트를 분석합니다.
- 각 사무실의 현재 대역폭 사용률을 파악합니다.

이렇게 하면 최상의 OfficeScan 배포 방법에 대해 보다 명확히 알 수 있습니다. 그림 1은 다중 사이트 네트워크 토폴로지를 보여줍니다.

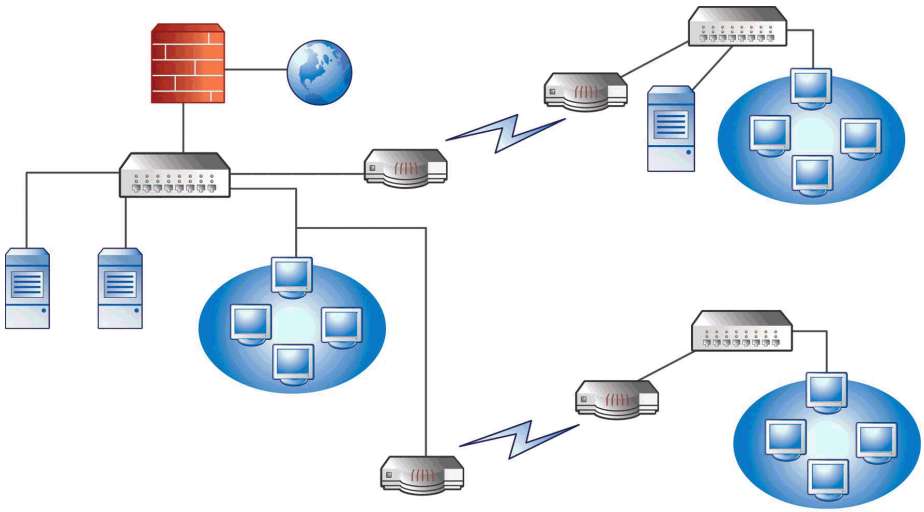

그림 A-2. 다중 사이트 네트워크 토폴로지

네트워크 정보:

- 원격 사이트 1 WAN 링크는 업무 시간 중 평균 사용률이 약 70%입니다. 이 사이트에는 35개의 에이전트 엔드포인트가 있습니다.
- 원격 사이트 2 WAN 링크는 업무 시간 중 평균 사용률이 약 40%입니다. 이 사이트에는 9개의 에이전트 엔드포인트가 있습니다.

- 서버 3은 원격 사이트 1의 그룹에 대해 파일 및 인쇄 서버로만 작동합니다. 이 엔드포인트에는 OfficeScan 서버를 설치할 수 있지만 추가 관리 오버헤드를 지출할 만한 가치는 없습니다. 모든 서버가 Windows Server 2012을 실행합니다. 네트워크에서는 Active Directory를 사용하지만 주로 네트워크 인증에 사용됩니다.
- 본사, 원격 사이트 1 및 원격 사이트 2의 모든 에이전트 엔드포인트는 Windows Server 2012 또는 Windows 7을 실행합니다.

다중 사이트 네트워크 준비

절차

1. OfficeScan 서버를 설치할 엔드포인트를 식별합니다. 설치 절차는 OfficeScan 서버 새로 설치 수행 페이지 2-2을 참조하십시오.
2. 사용 가능한 에이전트 설치 방법을 식별하고 요구 사항에 맞지 않는 방법은 무시합니다. 에이전트 설치 방법에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

   가능한 설치 방법:

   - 로그인 스크립트 설정

     로그인 스크립트 설정은 로컬 트래픽이 중요하지 않기 때문에 WAN이 없는 경우에 적합합니다. 그러나 50MB 이상의 데이터가 각 엔드포인트에 전송되는 경우 이 옵션을 실행할 수 없습니다.

   - 웹 콘솔에서 원격 설치

     이 방법은 본사에서 LAN으로 연결된 모든 엔드포인트에 적합합니다. 이러한 엔드포인트는 모두 Windows Server 2012을 실행하기 때문에 패키지를 해당 엔드포인트에 간단히 배포할 수 있습니다.

     두 원격 사이트 간의 링크 속도가 느리기 때문에 업무 시간 중에 OfficeScan을 배포하는 경우 이 배포 방법은 사용 가능한 대역폭에 영향을 줄 수 있습니다. 대부분의 사람들이 근무하지 않는 비업무 시간에 전체 링크 용량을 사용하여 OfficeScan을 배포합니다. 그러나 사용자가 엔드포인트를 꺼놓으면 해당 엔드포인트에 성공적으로 OfficeScan을 배포할 수 없습니다.

- OfficeScan 에이전트 패키지 배포

  OfficeScan 에이전트 패키지 배포는 원격 사이트 배포를 위한 최상의 옵션일 수 있습니다. 그러나 원격 사이트 2에는 이 옵션을 제대로 지지할 로컬 서버가 없습니다. 모든 옵션을 자세히 살펴보면 이 옵션이 대부분의 엔드포인트에 가장 적합함을 알 수 있습니다.

본사 배포

본사에서 구현할 수 있는 가장 쉬운 에이전트 배포 방법은 OfficeScan 웹 콘솔에서 원격으로 설치하는 것입니다. 절차에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오.

원격 사이트 1 배포

원격 사이트 1에 배포하려면 Microsoft DFS(분산 파일 시스템)를 구성해야 합니다. DFS에 대한 자세한 내용은 http://support.microsoft.com/?kbid=241452를 참조하십시오. DFS를 구성한 후 원격 사이트 1에 있는 서버 3에서 DFS를 사용하도록 설정하여 기존 DFS 환경을 복제하거나 새로 만들어야 합니다.

적합한 배포 방법은 MSI(Microsoft Installer) 패키지 포맷으로 에이전트 패키지를 만들고 DFS에 해당 에이전트 패키지를 배포하는 것입니다. 절차에 대한 자세한 내용은 *관리자 안내서*를 참조하십시오. 패키지가 다음 예약 업데이트 중에 서버 3에 복제되므로 에이전트 패키지 배포가 대역폭에 가장 적은 영향을 줍니다.

Active Directory를 통해 에이전트 패키지를 배포할 수도 있습니다. 자세한 내용은 *관리자 안내서*를 참조하십시오.

WAN에서 구성 요소 업데이트에 대한 영향 최소화

절차

1. 한 에이전트를 원격 사이트 1의 업데이트 에이전트로 작동하도록 지정합니다.

a. 웹 콘솔에 로그인하고 **에이전트** > **에이전트 관리** 항목으로 이동합니다.

b. 에이전트 트리에서 업데이트 에이전트로 작동할 에이전트를 선택하고 **설정** > **업데이트 에이전트 설정**을 클릭합니다.

2. 원격 사이트 1에서 업데이트 에이전트로부터 구성 요소를 업데이트할 에이전트를 선택합니다.

a. **업데이트** > **서버** > **업데이트 소스** 항목으로 이동합니다.

b. **사용자 정의 업데이트 소스**를 선택하고 **추가**를 클릭합니다.

c. 표시된 화면에서 원격 사이트 1의 엔드포인트에 대한 IP 주소 범위를 입력합니다.

d. **업데이트 소스**를 선택한 다음 드롭다운 목록에서 지정한 업데이트 에이전트를 선택합니다.

원격 사이트 2 배포

원격 사이트 2의 핵심적인 문제는 낮은 대역폭입니다. 그러나 약 154Kbit의 대역폭이 제공되는 경우 업무 시간에 대역폭의 60%를 사용할 수 있습니다.

OfficeScan 에이전트를 설치하는 가장 좋은 방법은 원격 사이트 1에서 사용된 것과 동일한 MSI 포맷의 에이전트 패키지를 사용하는 것입니다. 그러나 사용 가능한 서버가 없기 때문에 DFS(분산 파일 시스템)를 사용할 수 없습니다.

한 가지 옵션은 관리자가 실제로 액세스하지 않고 원격 엔드포인트에서 공유 디렉터리를 구성하거나 만들 수 있는 타사 관리 도구를 사용하는 것입니다. 단일 엔드포인트에 이 공유 디렉터리를 만든 후 디렉터리에 에이전트 패키지를 복사하면 9개의 엔드포인트에 에이전트를 설치하는 것보다 오버헤드가 적습니다.

다른 Active Directory 정책을 사용하되 DFS 공유를 소스로 지정하지 않아야 합니다.

이러한 방법은 설치 트래픽을 로컬 네트워크에서 유지하므로 WAN에 흐르는 트래픽을 최소화합니다.

WAN에서 구성 요소 업데이트에 대한 영향을 최소화하려면 업데이트 에이전트로 작동할 에이전트 1개를 지정합니다. 자세한 내용은 원격 사이트 1 배포 페이지 A-5를 참조하십시오.

색인

A

Active Directory, 1-10, A-5

C

Case Diagnostic Tool, 6-2
Client Mover, 5-2
Control Manager, 1-10

D

DFS(분산 파일 시스템), A-5

H

HTTP 포트, 1-17, 2-15, 3-69

I

IPv6 지원, 1-4

M

Microsoft Exchange Server, 1-23
MSI 패키지 배포, A-5

O

OfficeScan
  설명서, viii
OfficeScan 방화벽, 2-38, 3-45
OfficeScan 서버
  Control Manager를 사용하여 관리, 1-10
  master service, 4-3
  Master Service, 2-14, 3-68
  services, 4-3
  기능, 1-7
  기본 설정, 4-5
  디버그 로그, 6-5
  레지스트리 키, 4-3
  새로 설치, 2-2
  설치 로그, 4-3
  설치 요약, 2-45, 3-35, 3-48, 3-59, 3-88
  성능, 1-6
  수동 업데이트, 4-4
  위치, 1-5
  제품 서비스, 1-3
  프로세스, 4-3
OfficeScan 에이전트
  보안 수준, 2-36
  종료, 2-35

R

RSA 암호화, 2-16, 3-70

S

SQL server, 1-23
SSL 터널링, 2-16, 3-70
SSL 포트, 1-17, 2-16, 3-70

T

TMPerftool, 6-2

W

web server, 1-10, 1-17, 2-14, 3-68

ㄱ

검색 방법, 1-7
고려 사항
  새로 설치, 1-4
  업그레이드, 1-11
구성 요소, 4-4
구성 요소 복제, 1-9
구성 요소 업데이트, 1-9
기본 설정
  검색 설정, 4-5
  글로벌 에이전트 설정, 4-5

에이전트 권한, 4-5

ㄴ

네트워크 트래픽, 1-8

ㄷ

데이터베이스 백업, 1-13, 1-21, 5-3
등록, 1-18, 2-20, 3-74
등록 키, 1-3
디버그 로그
서버, 6-5

ㄹ

로그인 스크립트 설정, A-4
루트 계정, 1-20, 2-34

ㅁ

문서 피드백, 7-6
문제 해결, 6-1

ㅂ

방화벽, 2-38, 3-45
백업
OfficeScan 데이터베이스, 5-3
OfficeScan 서버 파일 및 폴더, 5-3

ㅅ

사후 설치, 4-1
새로 설치, 2-2
summary, 2-45, 3-35, 3-48, 3-59, 3-88
고려 사항, 1-4
시스템 요구 사항, 1-2
체크리스트, 1-15
확인, 4-2
서버
식별, 2-18, 3-72
서버 인증 인증서, 1-21
설명서, viii
설치
로그, 6-4
설치 후 작업, 4-1
설치 경로
서버, 1-15, 2-12, 3-66
에이전트, 1-20, 2-35
설치 대상, 2-8, 3-21, 3-38, 3-51, 3-62
설치 전 검색, 2-10, 3-23, 3-40, 3-53, 3-64
성능 조정 도구, 6-2
수동 업데이트, 4-4
수동 에이전트 업그레이드, 3-13
스마트 보호 네트워크, 2-32
스마트 보호 서버, 1-7, 2-23, 2-24, 3-29, 3-30, 3-77, 3-78, 5-4, 5-6
스마트 스캔, 1-7
시스템 요구 사항
새로 설치, 1-2

ㅇ

암호, 1-20, 2-34
업그레이드
summary, 2-45, 3-35, 3-48, 3-59, 3-88
고려 사항, 1-11
에이전트, 3-12, 3-16
체크리스트, 1-15
확인, 4-2
업데이트, 1-9
업데이트 에이전트, 1-9
에이전트 설치 경로, 1-20, 2-35
예외
성능 조정 도구, 6-2
용어, x
원격 설치, 1-6, 1-19, 2-9, 2-26, 2-28, 3-80, 3-82, A-4
원격 업그레이드, 3-22, 3-39, 3-52, 3-63
웹 콘솔, 2-34, 2-46, 3-36, 3-49, 3-60, 3-89, 4-2
응답 파일, 2-2
인크리멘탈 패턴, 1-9

ㅈ
자동 에이전트 업그레이드, 3-4, 3-12, 3-17
점검 모드, 2-39
정식 버전, 1-3
정품 인증, 1-18, 2-20, 3-74
정품 인증 코드, 1-3, 2-20, 3-74
제거
    제거 프로그램 사용, 5-5
지원
    신속한 문제 해결, 7-4
지원되지 않는 운영 체제, 1-12
지원 정보 시스템, 6-2

ㅊ
추가 정보 파일, 2-46, 3-36, 3-49, 3-60, 3-89

ㅋ
클라이언트 패키지 도구, A-5

ㅌ
타사 보안 소프트웨어, 1-10
통합 스마트 보호 서버, 1-7, 5-4
    설치, 2-23, 3-29, 3-77
    에이전트 연결 프로토콜, 2-24, 3-30, 3-78
    제거, 5-6

ㅍ
파일럿 배포
    롤백 계획, 1-22
    파일럿 사이트, 1-22
    평가, 1-22
평가판, 1-3
포트
    HTTP 포트, 1-17, 2-15, 3-69
    SSL 포트, 1-17
    서버 수신 포트, 1-12, 3-15
    에이전트 통신 포트, 1-20, 2-36
    프록시 서버 포트, 1-16
표준 스캔, 1-7
프로그램 설정, 5-3
프로그램 폴더 바로 가기, 1-21, 2-44, 4-2
프록시 서버, 1-16

ㅎ
호환성 문제, 1-22

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: OSKMXG7613/161028