Cisco IronPort Email Security Plug-in 7.1 관리자 설명서

2010년 12월 6일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
미국
http://www.cisco.com
전화: 408 526-4000
800 553-NETS (6387)
팩스: 408 527-0883

이 설명서의 제품 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항은 정확한 것으로 간주되지만 이에 대해 명시적이든 묵시적이든 어떠한 보증도 없이 제공됩니다. 모든 제품의 애플리케이션 사용에 대한 책임은 전적으로 사용자에게 있습니다.

동봉된 제품의 소프트웨어 라이센스 및 제한 보증은 제품과 함께 제공되는 정보 패킷에 설명되어 있으며 본 참조 문서에 통합되어 있습니다. 소프트웨어 라이센스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청해 주십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 DUB 공개 도메인 버전의 일부로서 UCB(University of California, Berkeley)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화번호는 실제 주소와 전화번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

Cisco IronPort Email Security Plug-in 7.1 관리자 설명서

목 차

1 장

Cisco IronPort Email Security 플러그인 시작하기

이 장에는 다음 섹션이 포함되어 있습니다.

이 릴리스의 새로운 사항

이 릴리스는 사용자가 이메일 프로그램에서 메시지를 암호화할 수 있도록 지원하는 Cisco 암호화 플러그인과 사용자가 스팸, 바이러스 또는 잘못 분류된 이메일을 보고하는 데 사용할 수 있는 Cisco 보고 플러그인 등 자주 사용되는 두 가지 이메일 보안 플러그인을 결합합니다. 이러한 플러그인을 통합함으로써, Cisco는 사용자가 이메일 보안 플러그인에 더욱 간편하게 액세스하고 수정할 수 있도록 하며 이메일 보안 플러그인을 설치 및 업데이트하는 과정도 간소화합니다. 또한 Cisco IronPort Email Security 플러그인은 Windows Installer를 기반으로 한 표준 설치 프로그램을 제공합니다. 설치 프로그램은 응답 파일을 통한 자동 설치를 포함한 표준 Windows Installer 명령줄 옵션을 지원합니다.

지원되는 컨피그레이션

다음 컨피그레이션이 지원됨:

Cisco IronPort Email Security Plug-in 7.1.x	Outlook 2003	Outlook 2007	Outlook 2010	Notes 6.x	Notes 7.x	Notes 8.0.x	Notes 8.5.x
XP 32비트	인증 완료	인증 완료	인증 완료	인증 완료	인증 완료	인증 완료	인증 완료
XP 64비트	호환 가능	호환 가능	호환 가능	호환 가능	호환 가능	호환 가능	호환 가능
Vista 32비트	인증 완료	인증 완료	인증 완료	호환 가능	호환 가능	호환 가능	인증 완료
Vista 64비트	호환 가능	인증 완료	인증 완료	호환 가능	호환 가능	인증 완료	호환 가능
Win 7 32비트	인증 완료	인증 완료	인증 완료	호환 가능	호환 가능	인증 완료	인증 완료
Win 7 64비트	호환 가능	인증 완료	인증 완료	호환 가능	호환 가능	호환 가능	인증 완료
Citrix	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음	지원되지 않음

참고 Cisco IronPort Email Security 플러그인에는 Wndows Installer 2.0 이상이 필요합니다.

관련 문서

암호화 플러그인을 사용하려면, 암호화 플러그인과 함께 작동하도록 적합하게 구성되고 실행되는 Cisco IronPort Encryption 어플라이언스가 있어야 합니다. Cisco IronPort Encryption 어플라이언스 구성 방법을 이해하려면 다음 설명서를 참조하십시오.

- *IronPort AsyncOS for Email Encryption User Guide*. 이 설명서는 이메일 암호화를 구성하기 위한 지침을 제공하며 사용자가 구성한 플러그인 설정과 함께 작동할 수 있게 암호화 어플라이언스 설정을 구성하는 방법을 이해하는 데 도움이 될 수 있습니다.

Cisco IronPort Email Security 작동 방식을 더 잘 이해하기 위해서는 이메일이 스팸, 바이러스 또는 스팸 아님으로 분류되는 방식에 대한 기본 정보를 검토하는 것이 도움이 될 수 있습니다. 이러한 주제에 대한 자세한 내용은 다음 설명서를 통해 확인할 수 있습니다.

- *Cisco IronPort AsyncOS for Email Configuration Guide*. 이 설명서에는 스팸 및 바이러스 보호에 대한 정보가 포함되어 있습니다. 사용자는 스팸 및 바이러스 플러그인을 사용함으로써 SenderBase 네트워크의 효율성을 개선할 수 있습니다. 사용자가 이메일을 "스팸", "바이러스", "스팸 아님"으로 표시하면 필터의 효율성을 향상시켜 모든 Cisco IronPort 어플라이언스의 성능을 개선할 수 있습니다.

이 설명서 사용 방법

이 설명서를 Cisco IronPort Email Security 플러그인의 기능에 대해 알아볼 수 있는 리소스로 사용하십시오. 주제는 논리적 순서로 정리되어 있지만 책의 모든 장을 읽을 필요는 없습니다. 목차와 이 문서의 구성 방식, 1-4페이지라는 섹션을 검토하여 사용자의 특정 컨피그레이션과 관련 있는 장을 파악해 보십시오.

설명서는 PDF로 전자 배포됩니다. 설명서의 전자 버전은 Cisco IronPort Customer 지원 포털에서 사용 가능합니다. 또한 도움말 버튼을 클릭하여 어플라이언스 GUI의 HTML 온라인 도움말 도구에 액세스할 수 있습니다.

이 문서의 구성 방식

1장, "Cisco IronPort Email Security 플러그인 시작하기"에서는 IronPort 보안 플러그인에 대해 소개하고 네트워크 보안 컨피그레이션에서의 핵심 기능 및 역할을 정의합니다. 현재 릴리스의 새로운 기능은 기타 정보 리소스 및 지원 연락처 정보에 대한 내용과 함께 설명됩니다.

2장, "개요"에서는 보고 플러그인과 암호화 플러그인에 대해 소개합니다. 이 섹션은 이러한 각 도구의 개요를 설명합니다.

3장, "대량 설치 수행"에서는 대량 설치를 수행하는 방법에 대해 설명합니다. 지침은 응답 파일을 생성하고 설치를 실행하는 단계와 설치하기 전에 수정이 필요할 수 있는 파일에 대해 설명합니다.

4장, "Outlook용 Cisco IronPort Email Security 플러그인 구성 및 사용"에서는 Outlook용 Cisco IronPort Email Security 플러그인 구성을 위한 지침을 제공합니다. 여기에는 보고 플러그인과 암호화 플러그인을 구성하는 단계도 포함됩니다.

5장, "Lotus Notes용 Cisco IronPort Email Security 플러그인 구성 및 사용"에서는 Lotus Notes용 Cisco IronPort Email Security 플러그인 구성을 위한 지침을 제공합니다. 여기에는 Lotus Notes 메일 프로그램에서 플러그인을 사용하기 위한 지침과 더불어 보고 플러그인 및 암호화 플러그인을 구성하는 단계가 포함됩니다.

부록 A, "Cisco IronPort Systems, LLC 소프트웨어 라이센스 계약"에는 Cisco IronPort 제품을 위한 라이센스 계약에 대한 상세 정보가 포함되어 있습니다.

표기 규칙

서체	의미	예
AaBbCc123	명령, 파일, 디렉터리의 이름 또는 컴퓨터 화면 출력	`Please choose an IP interface for this Listener.` `sethostname` 명령은 IronPort 어플라이언스의 이름을 설정합니다.
AaBbCc123	사용자 입력. 화면상의 컴퓨터 출력과 대조	`mail3.example.com>` **`commit`** `Please enter some comments describing your changes:` `[]>` **`Changed the system hostname`**

AaBbCc123	문서 제목, 새 항목, 강조된 단어 및 명령줄 변수. 명령줄 변수의 경우 이탤릭체로 표시된 텍스트는 실제 이름 또는 값의 자리 표시자입니다.	*IronPort Quickstart Guide*를 참조하십시오.
		
		IronPort 어플라이언스는 송신 패킷을 전송하기 위해 인터페이스를 고유한 방식으로 선택*해야 합니다*.
		
		`Before you begin, please reset your password to a new value.`
		`Old password:` **`ironport`**
		`New password:` *`your_new_password`*
		`Retype new password:`
		`your_new_password`

추가 정보 확인 위치

IronPort는 Cisco IronPort Email Security 플러그인에 대해 자세히 알아볼 수 있도록 다음의 리소스를 제공합니다.

IronPort 기술 교육

Cisco IronPort Systems 기술 교육 서비스는 고객이 Cisco IronPort 보안 제품 및 솔루션을 평가, 통합, 구축, 관리, 지원하는 데 필요한 지식과 기술을 습득하는 데 도움이 될 수 있습니다.

다음 방법 중 하나를 사용하여 Cisco IronPort 기술 교육 서비스팀에 문의해 주십시오.

교육. 등록 및 일반 교육에 대한 문의인 경우:

- http://training.ironport.com
- training@ironport.com

인증. 인증 및 인증 시험 관련 문의인 경우:

- http://training.ironport.com/certification.html
- certification@ironport.com

기술 자료

다음 URL에서 Cisco IronPort 고객 지원 사이트 기반의 Cisco IronPort 기술 자료에 액세스할 수 있습니다.

`http://www.cisco.com/web/ironport/knowledgebase.html`

참고 Cisco.com 사용자 ID가 있어야 사이트에 액세스할 수 있습니다. Cisco.com 사용자 ID가 없을 경우 다음 사이트에서 등록할 수 있습니다.
`https://tools.cisco.com/RPF/register/register.do`

기술 자료에는 Cisco IronPort 제품과 관련된 주제에 대한 다양한 정보가 포함되어 있습니다.

문서는 일반적으로 다음 범주 중 하나로 분류됩니다.

- **사용 방법.** 이 문서는 Cisco IronPort 제품의 기능에 대해 설명합니다. 예를 들어, 사용법 문서는 어플라이언스 데이터베이스를 백업 및 복원하는 절차에 대해 설명할 수 있습니다.
- **문제 및 해결책.** 문제 및 해결책 문서는 Cisco IronPort 제품을 사용하면서 겪을 수 있는 특정 오류나 문제에 대해 다룹니다. 예를 들어, 문제 및 해결책 문서는 제품을 새 버전으로 업그레이드하는 동안 특정 오류 메시지가 표시될 경우 수행할 작업에 대해 설명할 수 있습니다.

- **참조.** 참조 문서는 일반적으로 특정 하드웨어와 관련된 오류 코드 등의 정보 목록을 제공합니다.
- **문제 해결.** 문제 해결 문서는 Cisco IronPort 제품과 관련된 일반적인 문제를 분석하고 해결하는 방법에 대해 설명합니다. 예를 들어, 문제 해결 문서는 DNS에 문제가 있을 경우 따라야 하는 단계를 제공할 수도 있습니다.

Cisco Support Community

Cisco 지원 커뮤니티는 Cisco 고객, 파트너, 직원을 위한 온라인 포럼입니다. 이 커뮤니티에서는 일반적인 이메일 및 웹 보안 문제뿐만 아니라 특정한 Cisco 제품에 대한 기술 정보에 대해서도 논의할 수 있습니다. 질문을 하거나 다른 Cisco 및 Cisco IronPort 사용자와 정보를 공유하기 위해 포럼에 주제를 게시할 수 있습니다.

다음 URL에서 Cisco 지원 커뮤니티에 액세스하십시오.

`https://supportforums.cisco.com`

Cisco IronPort 고객 지원

전화, 이메일 또는 온라인을 통해 연중무휴 24시간 지원을 요청하실 수 있습니다. Cisco IronPort 고객 지원 서비스 수준 계약의 세부 정보는 지원 포털에서 제공됩니다.

고객 지원팀 업무 시간 외의 시간에 긴급한 지원이 필요한 중요한 문제가 발생했다면 다음 방법 중 하나를 사용하여 Cisco IronPort에 문의하십시오.

미국 무료 전화: 1 (877) 646-4766

지원 사이트: `http://www.cisco.com/web/ironport/index.html`

리셀러 또는 다른 공급업체를 통해 지원을 구매한 경우 해당 공급업체에 직접 제품 지원 문제를 문의하십시오.

서드파티 지원업체

IronPort AsyncOS에 포함되는 일부 소프트웨어는 FreeBSD, Inc., Stichting Mathematisch Centrum, Corporation for National Research Initiatives, Inc. 및 기타 서드파티 지원업체의 소프트웨어 라이센스 계약 약관, 통지 및 조건에 따라 배포되며 이러한 모든 약관과 조건은 IronPort 라이센스 계약에 통합됩니다.

이 계약에 대한 전체 내용은 다음에서 확인할 수 있습니다.

https://support.ironport.com/3rdparty/AsyncOS_User_Guide-1-1.html.

IronPort AsyncOS에 포함되는 소프트웨어 일부는 Tobi Oetiker가 명시적으로 서면 동의한 RRDtool을 기반으로 합니다.

이 문서의 일부는 Dell Computer Corporation의 허가 하에 복제되었습니다. 이 문서의 일부는 McAfee, Inc.의 허가 하에 복제되었습니다. 이 문서의 일부는 Sophos Plc.의 허가 하에 복제되었습니다.

Cisco IronPort에 의견 보내기

Cisco IronPort 기술 출판 팀은 더 우수한 제품 설명서를 제공하기 위해 최선을 다하고 있습니다. 소중한 의견과 제안을 언제라도 보내주십시오. 다음 이메일 주소로 보내시면 됩니다.

docfeedback@ironport.com

Cisco IronPort Email Security 플러그인 개요

Cisco IronPort Email Security 플러그인은 Outlook 또는 Lotus Notes 이메일 프로그램에 보고 및 암호화 메뉴를 설치합니다. 보고 플러그인을 사용하면 사용자가 수신하는 메일 유형에 관한 피드백(스팸, 피싱, 바이러스 이메일 등)을 제출할 수 있으며 암호화 플러그인은 툴바에 "메시지 암호화" 버튼을 배치하며 이를 통해 사용자는 이메일 프로그램에서 암호화된 이메일을 전송할 수 있습니다.

Cisco 보안 플러그인이 설치되면, Outlook 메일 클라이언트나 Lotus Notes 메일 클라이언트의 구성 요소가 활성화됩니다. 이 단일 인터페이스를 통해 엔드 유저는 문제 이메일을 원활하게 보고하거나 이메일 프로그램 내에서 암호화된 이메일을 전송할 수 있습니다. 이러한 플러그인을 결합하면 설치가 더욱 간편해지며 사용자가 수정할 수 있는 단일 인터페이스가 제공됩니다.

보고 및 암호화 플러그인은 툴바 버튼과 마우스 오른쪽 버튼 클릭 상황별 메뉴를 사용하여 피드백을 제출하고 암호화된 메시지를 전송할 수 있는 간편한 인터페이스를 제공합니다. 보고 플러그인을 사용하여 메시지를 보고하는 경우 메시지가 제출되었음을 나타내는 대화상자가 표시됩니다. 암호화 플러그인은 이메일 메시지의 메뉴 모음에 **Encrypt Message(메시지 암호화)** 버튼을 배치하여 발신자가 발송하기 전에 암호화 및 보호된 메시지를 표시할 수 있는 간편한 방식을 제공합니다. 암호화 플러그인의 정확한 기능은 암호화 라이센스가 포함된 Cisco IronPort Email Security 어플라이언스의 존재와 적합한 컨피그레이션에 달려 있습니다.

2 장

개요

Cisco IronPort Email Security 플러그인은 보고 플러그인과 암호화 플러그인을 포함한 몇 가지 Cisco IronPort Email Security 플러그인을 지원하는 프레임워크입니다.

이 장에는 다음 섹션이 포함되어 있습니다.

Cisco IronPort Email Security 플러그인

Cisco IronPort Email Security 플러그인은 보고 플러그인 및 암호화 플러그인 등 가장 보편적으로 사용되는 이메일 보안 플러그인 두 가지로 구성됩니다. Outlook 또는 Lotus Notes에 Cisco Email Security를 구축할 수 있습니다. Cisco IronPort Email Security 플러그인을 구축하는 경우 다음 애플리케이션 중 하나 또는 두 가지를 설치합니다.

- **보고 플러그인**. 보고 플러그인을 사용하면 Outlook 및 Lotus Notes 사용자가 스팸, 바이러스, 피싱 메시지 등 원하지 않는 이메일 메시지에 관해 Cisco IronPort Systems에 피드백을 제출할 수 있습니다. 자세한 내용은 보고 플러그인, 2-10페이지를 참고하십시오.
- **암호화 플러그인**. 암호화 플러그인은 이메일 메시지의 메뉴 모음에 메시지 암호화 버튼을 배치하여 발신자가 발송하기 전에 암호화 및 보호된 메시지를 표시할 수 있는 간편한 방식을 제공합니다. 자세한 내용은 암호화 플러그인, 2-10페이지를 참고하십시오.

보고 플러그인

보고 플러그인을 사용하면 Outlook 및 Lotus Notes 사용자가 스팸, 바이러스, 피싱 메시지 등 원하지 않는 이메일 메시지에 관해 Cisco IronPort Systems에 피드백을 제출할 수 있습니다. Cisco IronPort Systems는 이 피드백을 사용하여 원하지 않는 메시지가 받은 편지함으로 수신되는 것을 방지하도록 필터를 업데이트할 수 있습니다.

또한 **Not Spam(스팸 아님)** 버튼을 사용하여 스팸으로 표시된 정상적인 이메일 메시지를 잘못 분류된 메시지로 Cisco IronPort Systems에 보고할 수도 있습니다. Cisco IronPort Systems는 이러한 보고를 사용하여 스팸 필터를 조정해 효율성을 증대시킵니다.

이 플러그인은 툴바 버튼과 마우스 오른쪽 버튼 클릭 상황별 메뉴를 사용하여 피드백을 제출할 수 있는 간편한 인터페이스를 제공합니다. 메시지를 보고하는 경우 대화상자가 나타나 메시지가 제출되었음을 나타내는 대화상자가 표시됩니다. 제출하는 메시지 데이터는 Cisco IronPort 필터를 개선하기 위해 자동화된 시스템에서 사용됩니다. 메시지 데이터를 제출하여 받은 편지함으로 수신되는 원하지 않는 메일의 전체적인 양을 줄일 수 있습니다.

암호화 플러그인

암호화 플러그인은 이메일 메시지의 메뉴 모음에 **Encrypt Message(메시지 암호화)** 버튼을 배치하여 발신자가 발송하기 전에 암호화 및 보호된 메시지를 표시할 수 있는 간편한 방식을 제공합니다. 암호화 플러그인은 제대로 작동하고 구성된 Cisco IronPort Encryption 어플라이언스 및 Cisco IronPort Email Security 어플라이언스(네트워크에 있는 경우)와 함께 작동하도록 설계되었습니다. 암호화 플러그인에 사용하는 컨피그레이션은 이러한 어플라이언스에 대한 설정과 함께 개발되어야 합니다. 이 어플라이언스에 대해 동일한 컨피그레이션을 사용하지 않는 경우, 암호화된 메시지를 보낼 때 문제가 발생할 수 있습니다.

플러그인 설치

사용자 그룹을 위해 Cisco IronPort Email Security 플러그인을 설치하려면 자동 설치가 효율적일 수 있습니다. 자동 설치를 이용하면 최종 사용자에게 입력을 요청하지 않고 설치를 수행할 수 있습니다. Cisco IronPort Email Security 플러그인 자동 설치를 수행하려면 응답 파일(설치 프로세스 중에 제시된 모든 질문에 대한 답변을 담은 텍스트 파일)을 생성해야 합니다. 그런 다음 SMS(Systems Management Server) 또는 SCCM(System Center Configuration Manager) 등의 시스템 관리 소프트웨어를 통해 응답 파일을 사용하여 설치를 실행합니다. 자동 설치 수행 지침은 3장, "대량 설치 수행"을 참조하십시오.

Cisco IronPort Email Security 플러그인을 위한 설정 구성

Cisco IronPort Email Security 플러그인을 설치한 후 **Tools(도구)** > **Options(옵션)** > Outlook의 **Cisco Email Security** 메뉴 및 **Actions(작업)** > Lotus Notes의 **Cisco Email Security** 메뉴에서 컨피그레이션을 변경할 수 있습니다.

보고 플러그인 설치 또는 암호화 플러그인 설치를 변경하거나 두 플러그인 설치 모두에 영향을 미치는 일반 옵션을 변경할 수 있습니다. 예를 들어, 암호화 및 보고 플러그인 모두에 대한 로깅을 활성화하거나 암호화(이러한 설정은 Cisco IronPort Encryption 어플라이언스와 호환되어야 함)할 이메일에 표시하는 방법을 변경할 수 있습니다.

Outlook 설치에 대한 컨피그레이션을 변경하려면 4장, "Outlook용 Cisco IronPort Email Security 플러그인 구성 및 사용"을 참고하십시오.

Lotus Notes 설치에 대한 컨피그레이션을 변경하려면 5장, "Lotus Notes용 Cisco IronPort Email Security 플러그인 구성 및 사용"을 참고하십시오.

3 장

대량 설치 수행

이 장에서는 여러 데스크톱에 대량 설치를 수행하는 방법에 대해 설명합니다. 이 장에는 다음 섹션이 포함되어 있습니다.

개요

사용자 그룹을 위해 Cisco IronPort Email Security 플러그인을 설치하려면 설치 중에 사용할 응답 파일을 생성하기 위해 로컬 자동 설치를 수행하여 준비해야 합니다. 자동 설치를 이용하면 최종 사용자에게 입력을 요청하지 않고 설치를 수행할 수 있습니다. Cisco IronPort Email Security 플러그인 대량 설치를 수행하려면 응답 파일(설치 과정 중에 제시된 모든 질문에 대한 답변을 담은 텍스트 파일)을 생성해야 합니다. 그런 다음 SMS(Systems Management Server) 또는 SCCM(System Center Configuration Manager) 등의 시스템 관리 소프트웨어를 통해 응답 파일을 사용하여 설치를 실행합니다.

대량 설치를 수행하는 기본 단계에는 다음이 포함됩니다.

1. 보안 플러그인(Outlook용 데스크탑 암호화 플러그인, Outlook용 데스크탑 플래그 플러그인, Outlook용 IronPort 플러그인, Lotus Notes용 IronPort 플러그인 등 포함)을 구성하는 플러그인의 모든 기존 버전을 설치 제거합니다. 또는 현재 실행 중인 Cisco IronPort Email Security 플러그인의 모든 버전을 설치 제거합니다.

2. 설치하기 전에 Outlook 또는 Lotus Notes를 종료합니다.
3. 응답 파일을 만들려면 로컬 버전의 설치를 실행하고 해당 응답 파일이 제대로 생성되었는지 확인하십시오. 응답 파일 만들기, 3-14페이지를 참조하십시오.
4. 응답 파일이 생성된 후, 로컬 컴퓨터에 설치한 Cisco IronPort Email Security 플러그인을 설치 제거합니다. 응답 파일 테스트를 위한 다음 단계를 수행하는 동안 플러그인이 다시 설치됩니다.
5. 생성한 응답 파일을 사용하여 로컬 컴퓨터에서 설치를 실행합니다. Outlook 또는 Lotus Notes에 프로그램이 제대로 설치되었는지 확인합니다.
6. 설치를 확인한 후 SCCM(System Center Configuration Manager)과 같은 시스템 관리 소프트웨어를 사용하여 대상 컴퓨터에 대량 설치를 실행합니다. SCCM를 사용하여 설치를 수행하려면 SCCM을 사용하여 대량 설치 수행, 3-15페이지를 참조하십시오.

응답 파일 만들기

응답 파일을 만들려면, 응답을 파일에 기록하는 특수 옵션이 있는 플러그인 설치를 실행하십시오. 기록된 응답으로 응답 파일을 생성하면 Cisco IronPort Email Security 플러그인을 설치하고자 할 때 설치 중에 이를 사용하여 모든 컴퓨터에서 설치 질문에 자동으로 응답할 수 있습니다.

1단계 응답 파일을 생성하려면, **/r** 키 옵션을 사용하여 명령줄에서 설치를 수행합니다. **/r** 키 옵션은 InstallShield에 지시하여 응답 파일에 결과를 기록합니다. 기본적으로 InstallShield는 다음 이름 및 위치에 응답 파일을 저장합니다.

c:\windows\setup.iss.

2단계 응답 파일의 위치를 지정하려면, **/f1** 옵션을 사용합니다. **/f1** 옵션을 이용하면 대체 응답 파일 이름 및 경로를 지정할 수 있습니다. 예를 들어, 명령줄에서 다음 명령을 실행하면 C 드라이브의 *install_034.iss* 파일에 응답을 쓰도록 InstallShield에 지시합니다.

C:\Users\user1\Desktop\CiscoEmailSecurity.7.1.0.34.exe /r /f1"C:\install_034.iss"

*C:\Users\user1\Desktop\CiscoEmailSecurity.7.1.0.34.exe*가 .exe 파일의 경로인 경우

키 사이에 공간이 있는지 확인(모든 슬래시 앞): */s /v /qn /f1*

.exe 파일 이름 및 *.iss* 파일 이름은 예시로 든 파일 이름입니다. .exe 파일 이름이 위에 나열된 것과 다른 경우에도 설치 성능에 영향을 미치지 않습니다.

각 설치 단계를 수행하면 응답이 대량 설치 중에 사용될 수 있도록 응답 파일에 저장됩니다.

정보 Cisco IronPort는 **/f1** 옵션을 사용하여 경로 및 파일 이름을 변경할 경우 절대 경로를 입력할 것을 권장합니다. 또한 응답 파일을 생성할 때 **/f1** 옵션을 사용하는 경우 자동 설치(**/s** 옵션 사용)를 실행하는 동안 응답 파일에 대한 경로를 지정해야 함에 유의하십시오.

3단계 *install_file.iss*가 생성되었는지 확인합니다.

4단계 *install_file.iss* 가 생성된 것을 확인한 후 플러그인을 제거합니다(명령줄 매개변수와 키를 사용하지 않아야 함).

5단계 로컬 컴퓨터에서 설치 관리자를 실행하여 응답 파일을 테스트합니다. 이를 위해 명령줄에서 다음을 실행합니다.

C:\Users\user1\Desktop\CiscoEmailSecurity.7.1.0.34.exe /s /v /qn /f1"C:\install_034.iss"

/s - 옵션은 setup.exe를 자동으로 설치하며

/v - 옵션은 MSI 패키지로 매개변수를 전달하고

/qn - 옵션은 *setup.exe*를 자동으로 설치하는 것 외의 모든 작업을 가능하게 하며

/f1 - 옵션은 프로그램이 여기에 있는 응답 파일을 사용하게 합니다.

6단계 이메일 프로그램(Outlook 또는 Lotus Notes)을 열고, Cisco IronPort Email Security 플러그인이 올바르게 설치되었는지 확인합니다.

참고 일단 *install_file.iss*가 생성되면 Cisco IronPort Email Security 플러그인을 업데이트할 때도 사용할 수 있습니다.

SCCM을 사용하여 대량 설치 수행

시작하기 전에 Cisco IronPort Email Security 플러그인을 설치하려는 클라이언트 머신에서 다음 단계를 수행했는지 확인하십시오.

- .Net 3.5를 클라이언트 머신에 설치하십시오(설치 프로세스는 필요한 경우 누락된 프레임워크를 다운로드 및 설치하지만 .Net 3.5를 사전 설치한 경우 설치가 더욱 빠르게 실행됨).
- Outlook 또는 Lotus Notes를 종료합니다.
- Cisco IronPort Email Security 플러그인의 현재 버전을 설치 제거합니다(설치된 경우).
- 보안 플러그인(Outlook용 데스크탑 암호화 플러그인, Outlook용 데스크탑 플래그 플러그인, Outlook용 IronPort 플러그인, Lotus Notes용 IronPort 플러그인 등 포함)을 구성하는 플러그인의 모든 기존 버전을 설치 제거합니다.
- *install_file.iss* 파일을 생성했는지 확인합니다. 응답 파일 만들기, 3-14페이지를 참조하십시오.

설치를 시작하기 전에 SCCM에 다음 조건이 있는지 확인하십시오.

- Cisco IronPort Email Security 플러그인을 설치해야 하는 클라이언트 목록 모음을 생성했습니다.

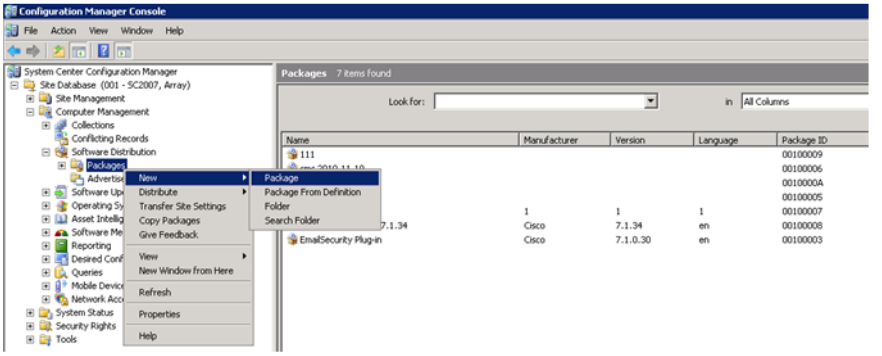
설치 수행 방법:

1단계 네트워크 공유 폴더를 생성하고 사용자에게 이에 대한 액세스를 제공하십시오.

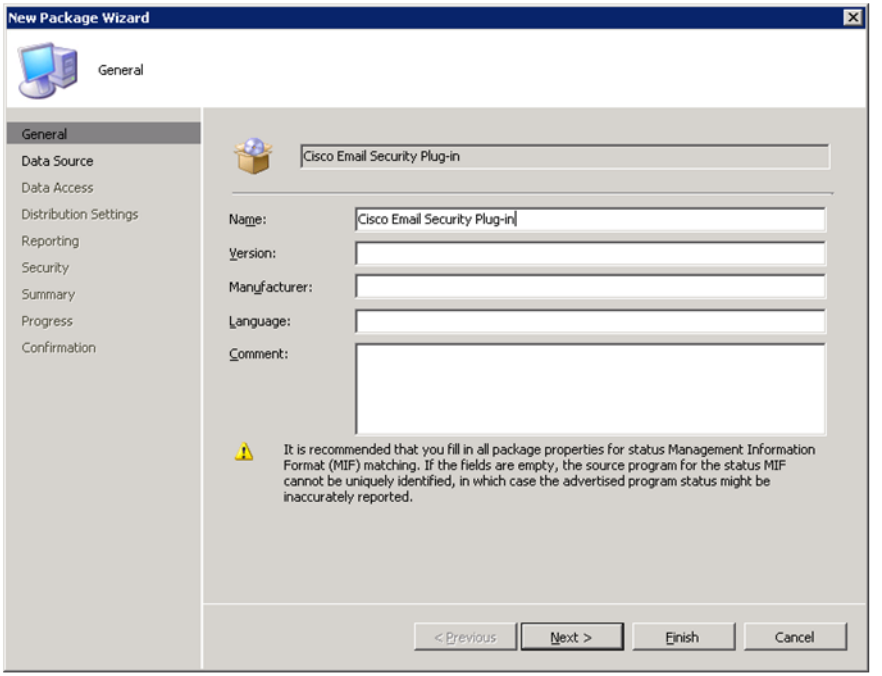
2단계 설치 프로그램 및 *install_file.iss* 파일을 이 폴더에 넣으십시오.

3단계 SCCM 관리 도구를 엽니다.

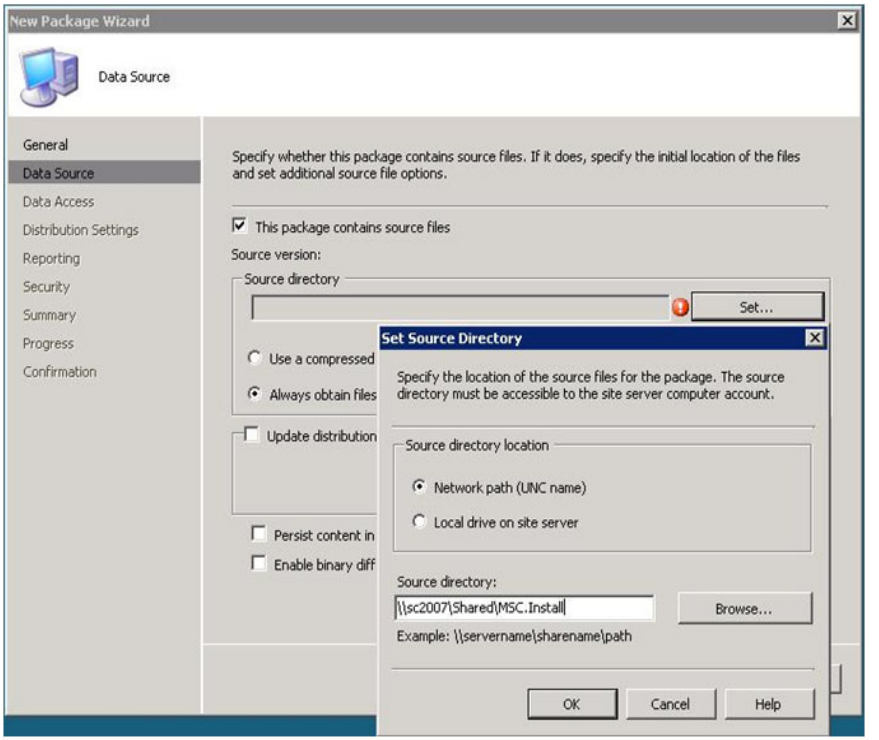
4단계 새 소프트웨어 배포 패키지를 만듭니다.



5단계 패키지의 이름을 입력하고 **Next(다음)**를 클릭합니다.

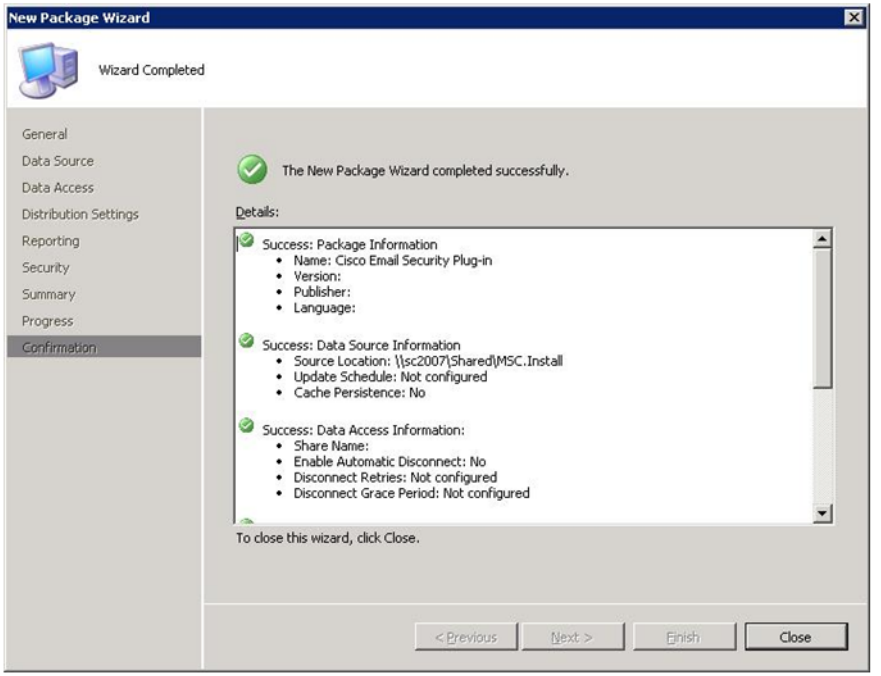


6단계 네트워크 공유 폴더에 대한 경로를 입력하여 단계 1에서 생성한 네트워크 소스 디렉터리를 지정합니다. 경로를 입력하거나 폴더를 탐색할 수 있습니다. **Next(다음)**를 클릭합니다.

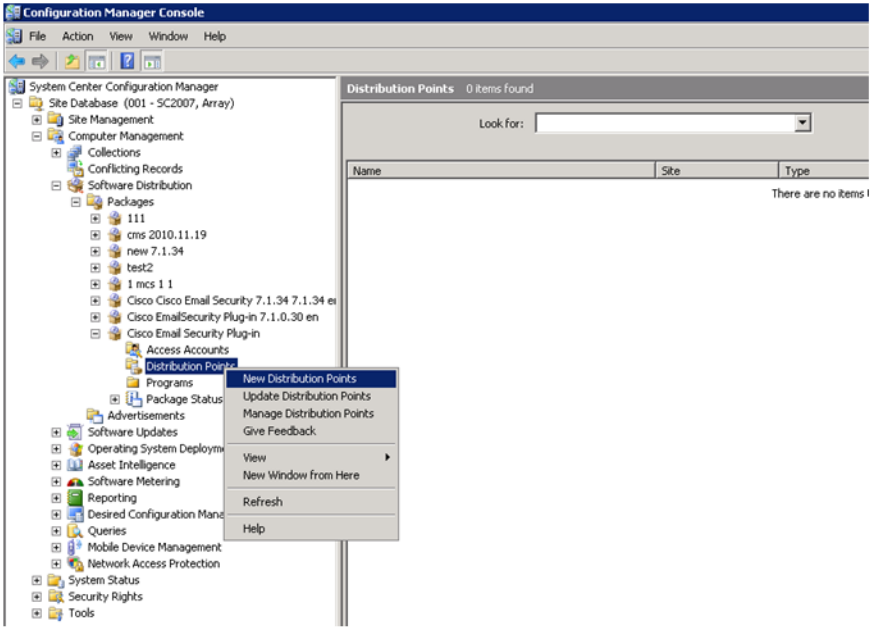


7단계 새 패키지 마법사의 다음 단계로 진행하여 **Next(다음)**를 클릭합니다.

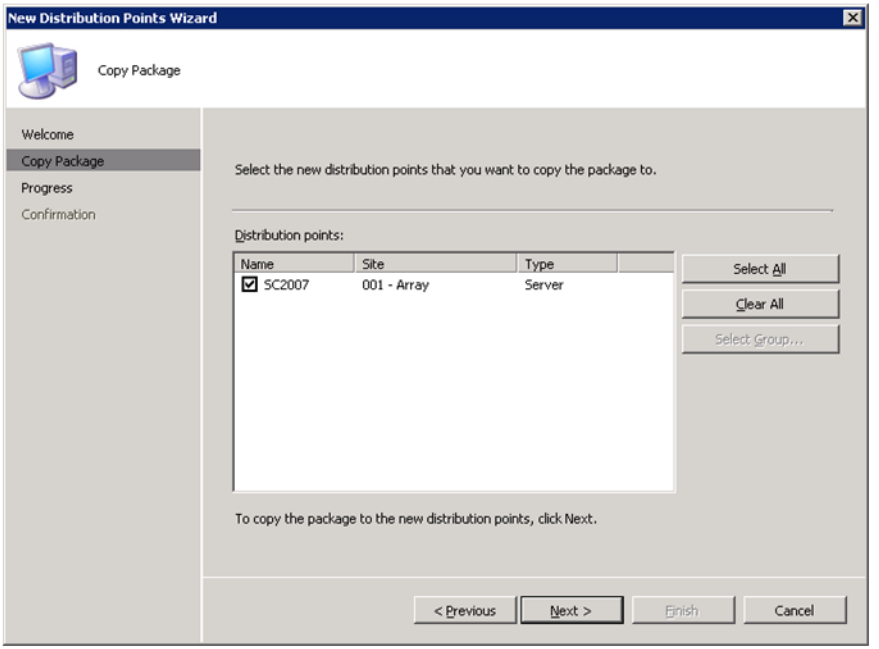
8단계 새 패키지 마법사가 성공적으로 완료되었다는 확인 메시지가 표시되면 **Close(닫기)**를 클릭합니다.



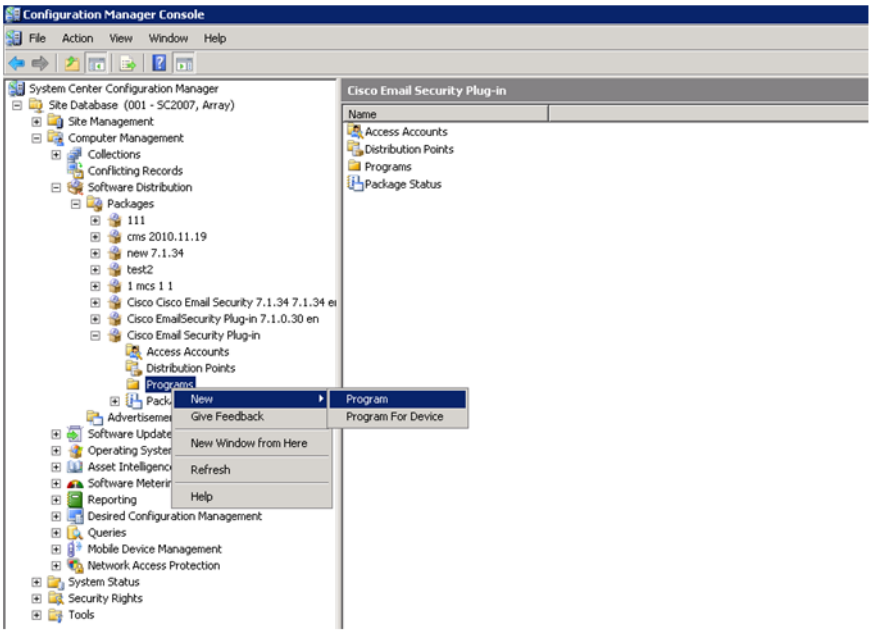
9단계 새 배포 지점을 생성하고, 시작 페이지에서 **Next(다음)**를 클릭합니다.



10단계 새 배포 지점을 선택합니다. 새 배포 지점 마법사에서 다음 페이지를 클릭하고 **Close(닫기)**를 클릭합니다.

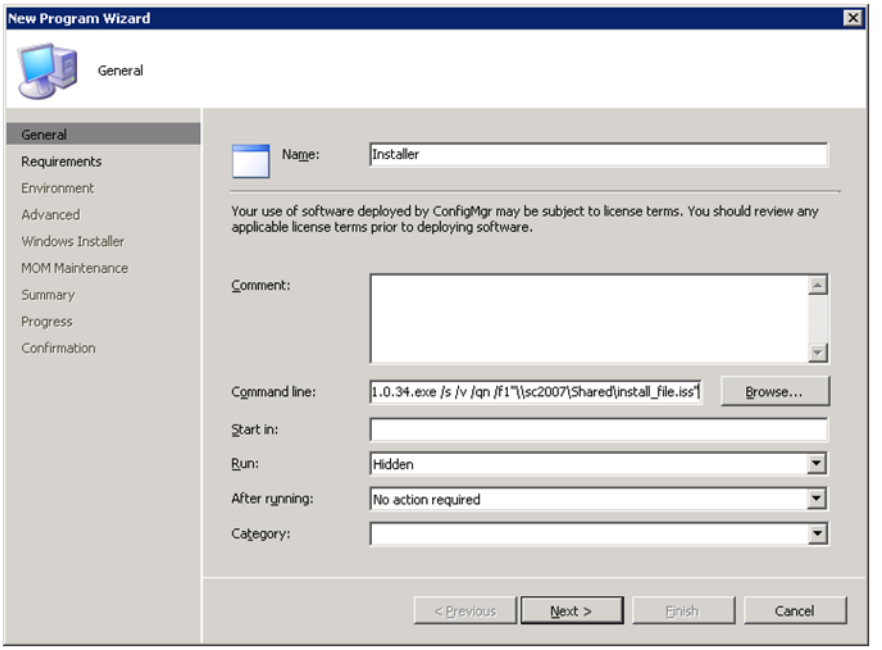


11단계 새 프로그램을 생성합니다.



12단계 명령줄에서, 프로그램 이름 및 다음 명령을 입력합니다.
\\sc2007\Shared\CiscoEmailSecurity.7.1.0.34.exe /s /v /qn /f1"\\sc2007\Shared\install_file.iss"

*\\sc2007\Shared\CiscoEmailSecurity.7.1.0.34.exe*는 "\\sc2007\Shared\install_file.iss" 네트워크 공유 폴더의 .exe 파일에 대한 전체 네트워크 경로입니다.



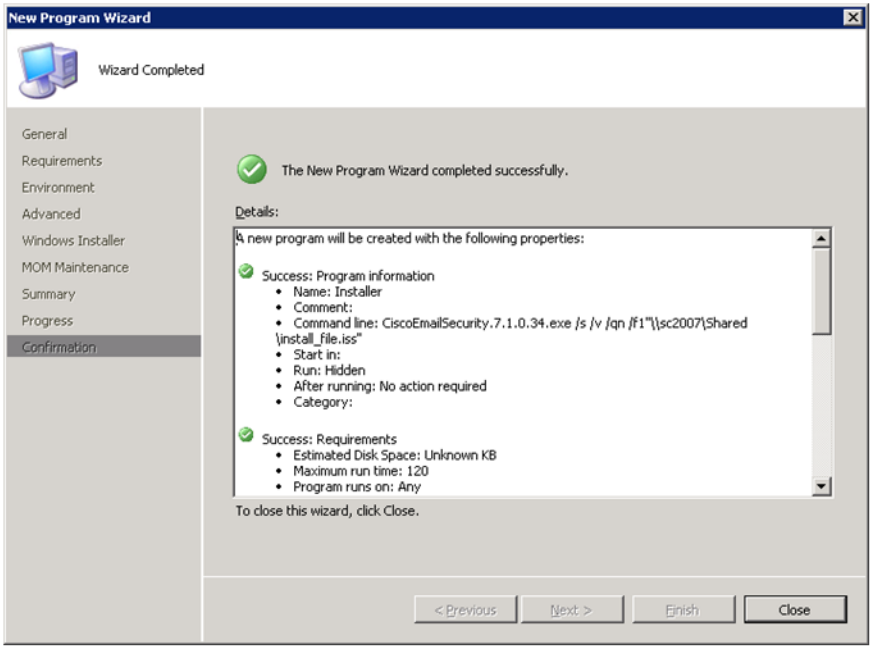
13단계 **Run(실행)** 필드에 **Hidden(숨김)**을 입력하고 **Next(다음)**를 클릭합니다.

14단계 요구 사항 페이지를 클릭하여 **Next(다음)**를 클릭합니다.

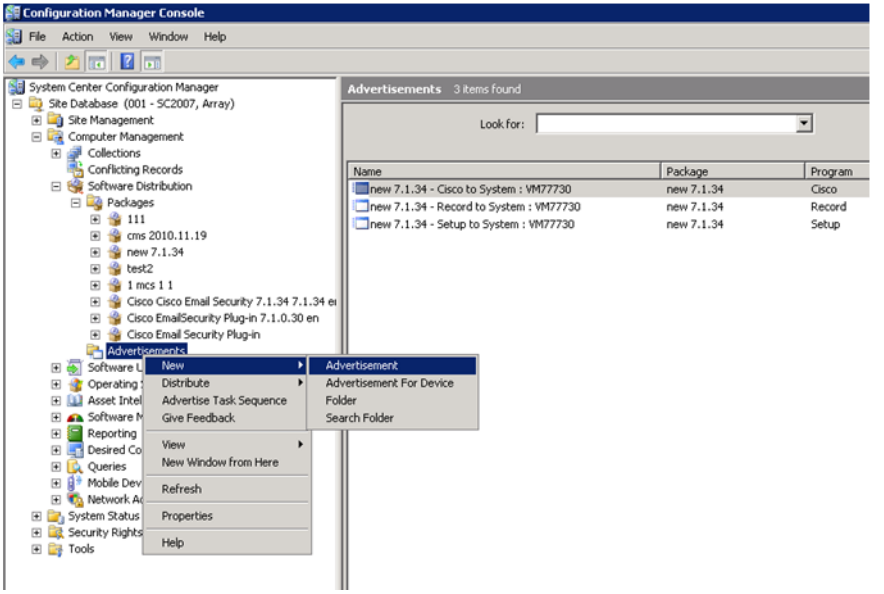
15단계 다음 환경 옵션을 선택합니다.

- **Program can run(프로그램 실행 가능 시점)**: 사용자가 로그인되어 있는 경우에만
- **Run mode(실행 모드)**: 사용자 권한으로 실행하거나 사용자가 새 소프트웨어 설치에 필요한 권한이 없는 경우 관리자 권한으로 실행합니다.

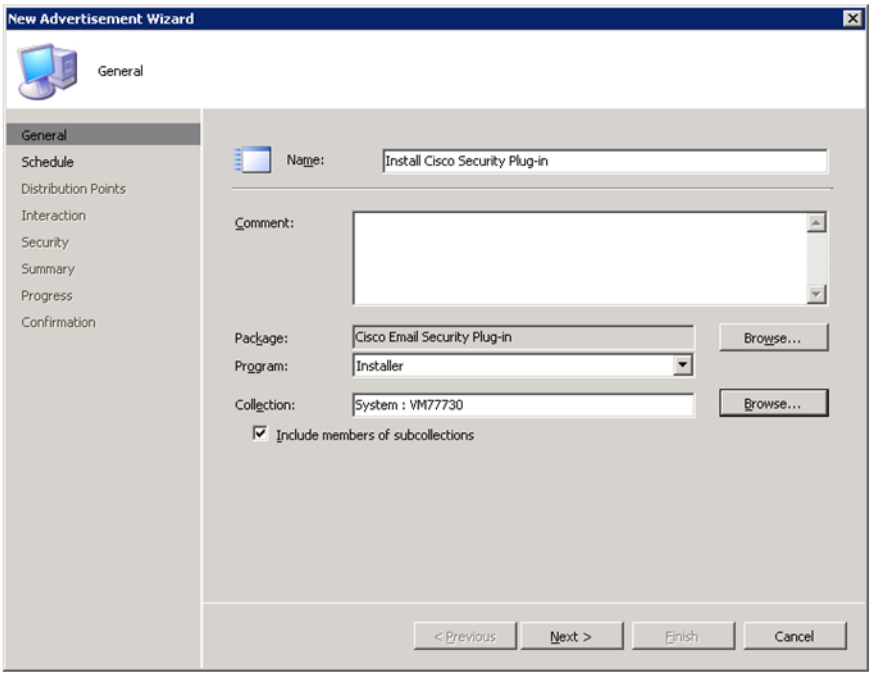
16단계 새 프로그램 마법사가 성공적으로 완료되었는지 확인하고, **Close(닫기)**를 클릭합니다.



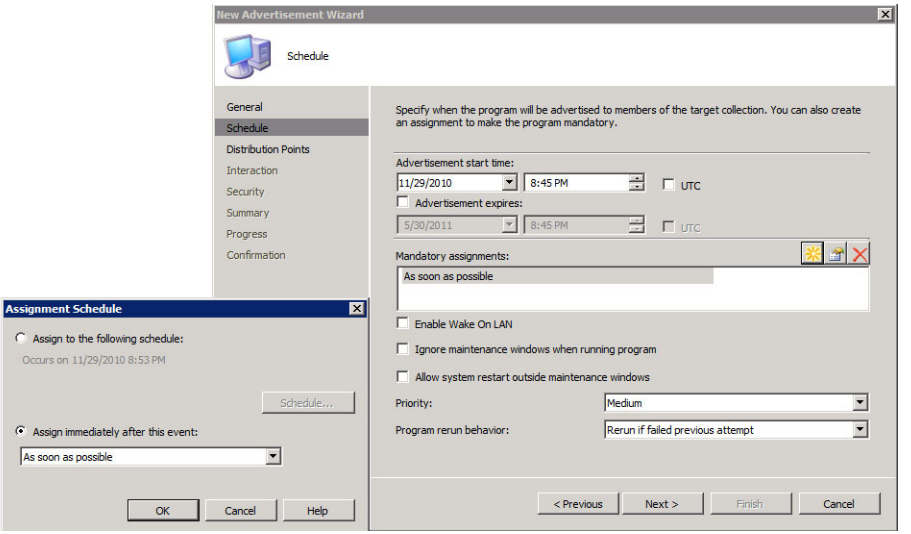
17단계 새 알림을 생성합니다.



18단계 이름을 입력하고, 생성한 패키지와 프로그램을 선택합니다. 플러그인을 설치할 클라이언트 그룹을 포함하는 모음을 선택하고 **Next(다음)**를 클릭합니다.



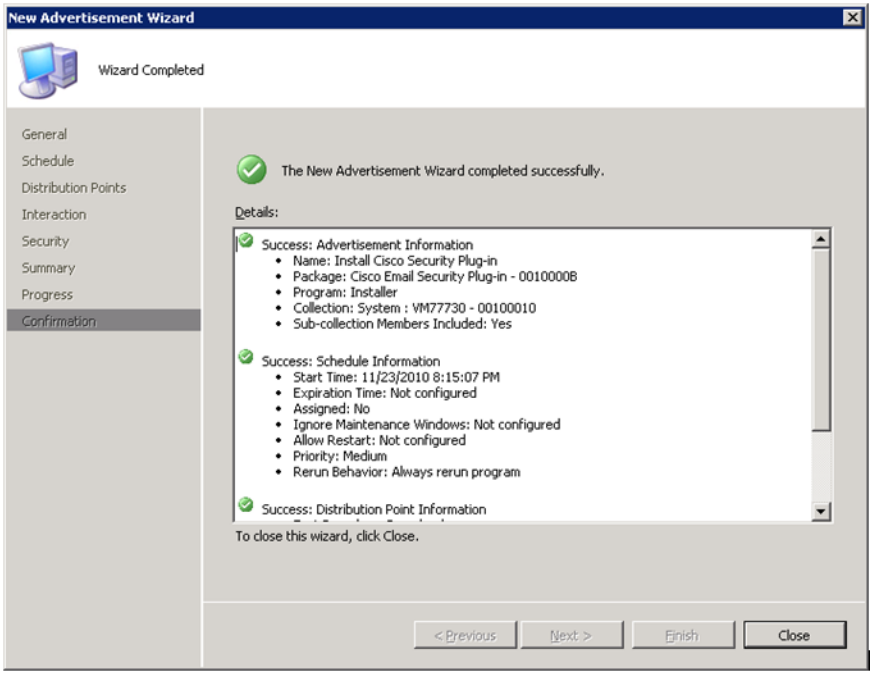
19단계 할당을 필수로 설정합니다. **Next(다음)**를 클릭합니다.



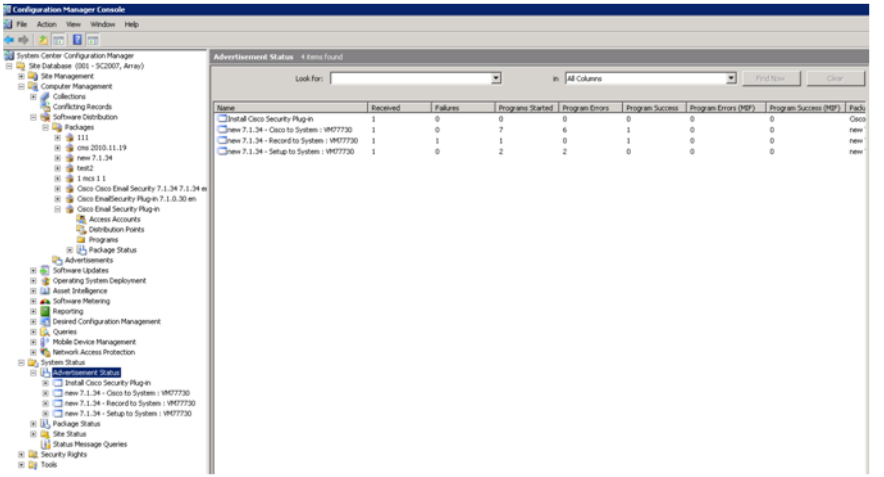
20단계 기본 설정을 바탕으로 스위치를 선택하되 연결이 느릴 경우 프로그램이 시작되지 않으므로 **Do Not Run Program(프로그램 실행 안 함)**을 선택하지 마십시오**. Next(다음)**를 클릭합니다.

21단계 새 알림 마법사를 클릭하고 **Next(다음)**를 클릭합니다.

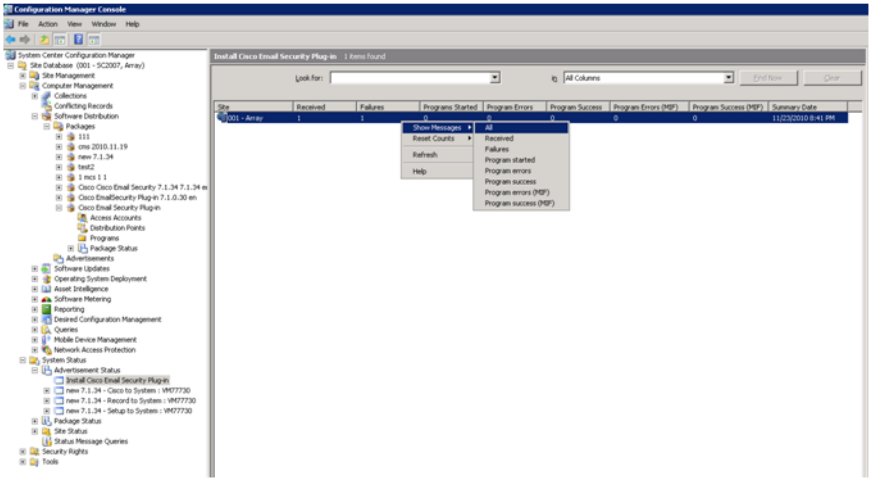
22단계 새 알림 마법사가 성공적으로 완료되었다는 확인 메시지가 표시되면 **Close(닫기)**를 클릭합니다.



23단계 알림 상태 창에서 알림 상태를 확인합니다.



24단계 컨텍스트 메뉴에서 **Show message(메시지 표시) > All(모두)**을 선택하여 더 많은 세부 정보를 볼 수 있도록 알림 보고서를 작성할 수 있습니다. 오류가 발생하면 보고서를 검토하여 오류가 발생한 위치를 파악할 수 있습니다.



플러그인 컨피그레이션 파일 변경

Cisco IronPort Email Security 플러그인을 설치할 때 구성 데이터가 생성되어 다음 XML 파일로 저장됩니다.

- **CommonConfig.xml**. 보고 및 암호화 플러그인 모두에서 공통으로 사용되는 로깅 정보 등 기본 컨피그레이션 데이터를 포함합니다.
- **Reporting.xml**. 보고 플러그인과 관련된 최대 이메일 크기 등의 보고 가능한 컨피그레이션 데이터를 포함합니다.
- **Encryption.xml**. 암호화 플러그인과 관련된 플래그 지정 방법(제목 문자열 또는 x-헤더 등) 등의 컨피그레이션 데이터를 포함합니다.

Cisco IronPort Email Security 플러그인 설치 프로그램을 사용하면 기본 컨피그레이션 파일을 변경할 수 있습니다. 설치에 대한 기본 기능을 변경하려면 다른 컨피그레이션 파일을 사용할 수도 있습니다. 예를 들어, 암호화 컨피그레이션 파일에서, 파일 플래그 지정 방법을 변경할 수도 있습니다(암호화 어플라이언스에 대한 방법도 변경할 수 있을 경우에만 변경됨). 보고 컨피그레이션 파일에서 보고를 위한 최대 이메일 크기나 보고 후 파일 사본 유지 여부 등 기본 옵션 몇 가지를 변경할 수도 있습니다. 기본 컨피그레이션 파일에서 기록을 활성화 또는 비활성화하거나 기록 수준을 변경할 수 있습니다.

사용자 정의 컨피그레이션 파일을 사용하려는 경우, 다음 구문을 사용하여 명령줄에서 특수 키를 추가해야 합니다.

```
CiscoEmailSecurity-7.0.0.005.exe /s
/v"UseCustomConfigs=\"\\smsarray\SMSClient\config\"" /qn
/"f1CiscoEmailSecurity.7.0.0.005.iss"
```

UseCustomConfigs 명령줄 매개변수는 사용자 정의 컨피그레이션 파일의 사용을 활성화하고 설치 중에 사용되어야 하는 컨피그레이션 파일이 포함된 폴더 경로를 지정하는 데 사용됩니다.

기본적으로 플러그인은 다음과 같은 Outlook 및 Lotus Notes 위치의 %appdata% 디렉터리에 컨피그레이션 파일을 설치합니다.

```
%appdata%\Cisco\Cisco IronPort Email Security Plug In\Outlook\

%appdata%\Cisco\Cisco IronPort Email Security Plug In\LotusNotes\
```

UseCustomConfigs 명령줄 매개변수를 사용하여 설치할 자체 컨피그레이션 파일의 이름과 위치를 지정할 수 있습니다. 그러나, 유효성을 유지하려면 원래 파일의 구조를 유지해야 합니다. 기본 컨피그레이션 파일은 config.zip 파일에 있습니다. 폴더를 생성할 경우, 파일 구조를 유지하고 컨피그레이션 파일이 포함된 Outlook 또는 Lotus 하위 폴더를 포함시켜야 합니다(Outlook 플러그인만 설치할 경우 LotusNotes 폴더를 제외해도 무방하며 반대의 경우도 마찬가지임).

4 장

Outlook용 Cisco IronPort Email Security 플러그인 구성 및 사용

이 장에서는 Outlook용 Cisco IronPort Email Security 플러그인에서 제공되는 기능에 대해 소개합니다. Cisco IronPort Email Security 플러그인에는 Outlook 이메일 프로그램에서 작동하는 몇 가지 보안 플러그인 유형이 포함되어 있습니다. 이 장에는 다음 섹션이 포함되어 있습니다.

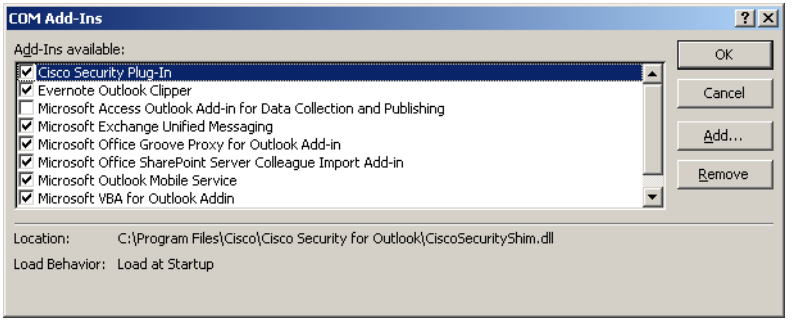
Outlook용 Cisco IronPort Email Security 플러그인 일반 설정

Cisco IronPort Email Security 플러그인은 암호화 플러그인 및 보고 플러그인을 포함하는 몇 가지의 Cisco 플러그인을 지원하는 플랫폼입니다. 옵션 페이지에서 Cisco IronPort Email Security 플러그인에 대한 일반 설정을 구성할 수 있습니다.

사용/사용 안 함

기본적으로 Cisco IronPort Email Security 플러그인은 설치 시 활성화됩니다. Cisco IronPort Email Security 플러그인을 비활성화하려는 경우 다음 위치에서 수행할 수 있습니다.

- Outlook2003/2007에서, **Tools(도구)** > **Options(옵션)** > **Cisco Email Security**로 이동합니다.
- Outlook 2010에서는, **File(파일)** >**Options(옵션)** > **Add-ins(애드인)**로 이동합니다. 그런 다음 COM 애드인에 대한 관리 드롭다운 목록을 선택하여 **Go(이동)**를 클릭합니다.



COM 애드인 창에서 Cisco IronPort Email Security 플러그인 확인란의 선택을 취소하고 **OK(확인)**를 클릭합니다.

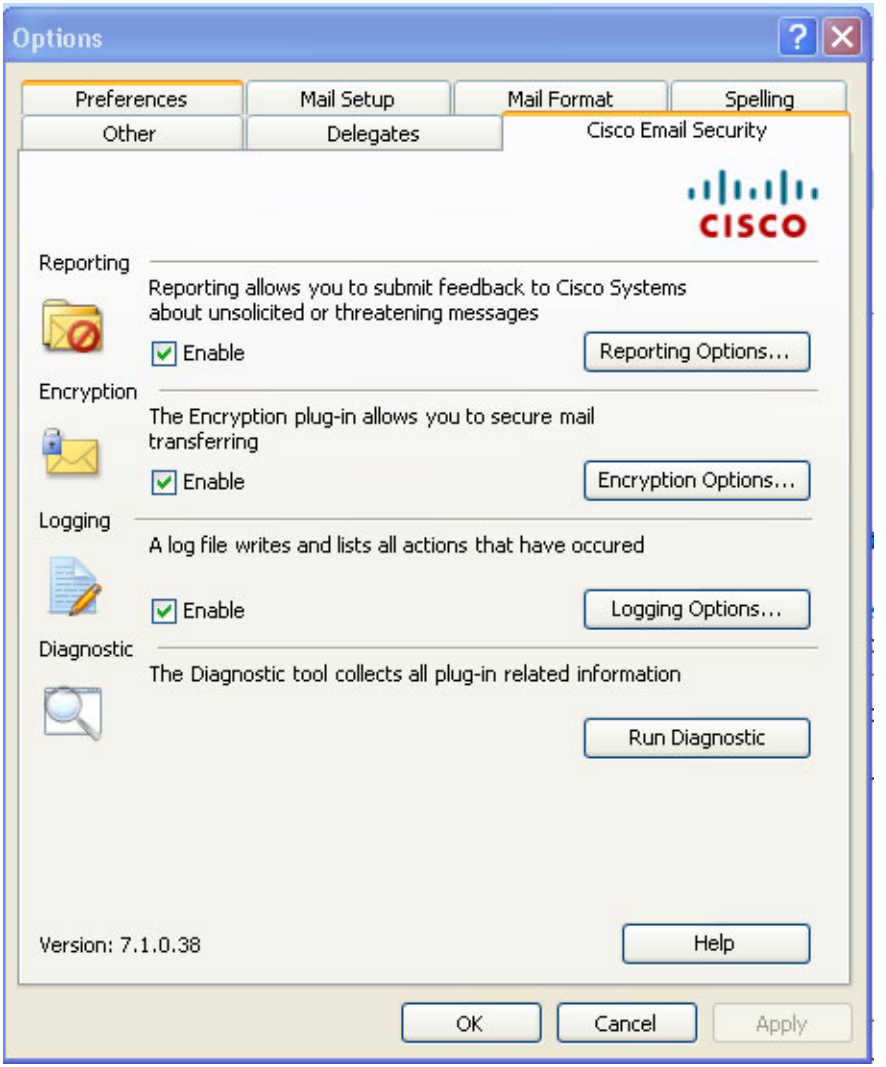
Outlook 플러그인에 대한 기본 설정 구성

Cisco Email Security 탭에서 기본 설정을 구성할 수 있습니다. Outlook 2003/2007에서 Cisco Email Security 탭을 열려면, **Tools(도구)** > **Options(옵션)** > **Cisco Email Security**로 이동합니다.

또는

Outlook 2010에서는 **File(파일)** > **Options(옵션)** > **Add-ins(애드인)** > **Add-in Options(애드인 옵션)** > **Cisco Email Security**로 이동합니다.

Cisco Email Security 탭:



이 탭에서, **Enable(활성화)** 확인란을 선택하여 보고, 암호화, 로깅을 활성화할 수 있습니다. 추가 설정을 구성하려면, **Reporting Options...(보고 옵션...)**, **Encryption Options(암호화 옵션)**, 또는 **Logging Options...(로깅 옵션...)** 버튼을 클릭하십시오. 또한 문제 해결 시 Cisco 지원 부서에 전송할 Cisco IronPort Email Security 플러그인에 대한 보고를 실행하기 위한 진단 도구도 사용할 수 있습니다.

보고 플러그인

보고 설정을 이용하면 플러그인을 활성화 또는 비활성화할 수 있습니다. 보고 플러그인을 사용하면 사용자가 수신한 이메일이 스팸, 피싱 공격, 바이러스인지 또는 스팸("햄"이라고도 불림)으로 잘못 분류되었는지를 보고할 수 있습니다.

Outlook의 옵션 페이지를 통해 Cisco IronPort Email Security 보고 플러그인을 구성할 수 있습니다.

Outlook 2003/2007의 보고 플러그인을 활성화하려면, **Tools(도구)** > **Options(옵션)** > **Cisco Email Security** 탭으로 이동하여 Cisco Email Security 탭의 Reporting(보고) 필드에서 **Enable(활성화)** 확인란을 선택합니다.

또는

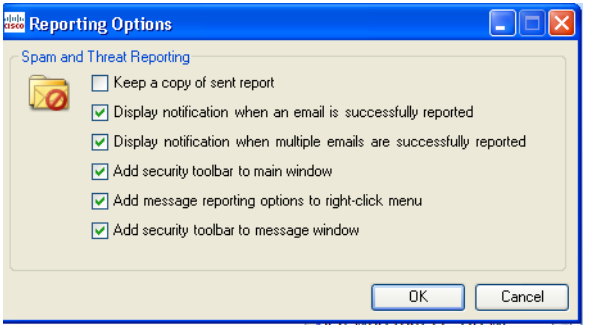
Outlook 2010의 보고 플러그인을 활성화하려면, **File(파일)** > **Options(옵션)** > **Add-ins(애드인)** > **Add-in Options(애드인 옵션)** > **Cisco Email Security** 탭으로 이동하여 Cisco Email Security 탭의 Reporting(보고) 필드에서 **Enable(활성화)** 확인란을 선택합니다.

보고 옵션

Outlook 2003/2007의 보고 옵션 페이지에 액세스하려면, **Tools(도구)** > **Options(옵션)** > **Cisco Email Security** 탭으로 이동하여 **Reporting Options(보고 옵션)** 버튼을 클릭합니다.

Outlook 2010의 암호화 설정에 대한 변경 사항을 수정하려면, **File(파일)** > **Options(옵션)** > **Add-ins(애드인)** > **Add-in Options(애드인 옵션)** > **Cisco Email Security**로 이동하여 **Reporting Options(보고 옵션)** 버튼을 클릭합니다.

보고 옵션 페이지:



옵션

이 섹션에서는 구성 가능한 보고 옵션에 대해 설명합니다.

- **전송된 보고서의 복사본 보관**. 기본적으로 Cisco에 스팸, 바이러스, 잘못 분류된 스팸 또는 바이러스로 이메일 메시지를 보고하면 전송한 보고 이메일이 삭제됩니다. 이 옵션을 선택하면 이메일이 삭제되는 것을 방지합니다.
- **이메일이 성공적으로 보고되었을 경우 알림 표시** 이메일을 스팸이나 바이러스로 성공적으로 보고한 경우 대화상자에 성공 메시지를 표시하도록 Outlook을 활성화할 수 있습니다. 이 옵션을 제거하면 이 대화 상자가 표시되지 않습니다.
- **여러 이메일이 성공적으로 보고되었을 경우 알림 표시** 여러 이메일이 성공적으로 보고된 경우(스팸, 바이러스, 피싱 또는 스팸 아님) Outlook을 활성화하여 대화상자에 성공 메시지를 표시하도록 할 수 있습니다. 이 옵션을 제거하면 이 대화 상자가 표시되지 않습니다.
- **메인 창에 보안 툴바 추가** 기본적으로 Cisco IronPort Email Security 플러그인을 설치할 경우 플러그인 툴바가 메인 Outlook 창에 추가됩니다. 이 옵션을 취소하면 이 툴바가 메인 Outlook 창에 추가되는 것을 방지할 수 있습니다.
- **마우스 오른쪽 버튼으로 클릭 메뉴에 메시지 보고 옵션 추가** 기본적으로 Cisco IronPort Email Security 플러그인을 설치할 때 보고 플러그인 메뉴 항목이 Outlook의 상황에 맞는 마우스 오른쪽 버튼으로 클릭 메뉴에 추가됩니다. 이 옵션을 취소하면 이 메뉴 항목이 상황에 맞는 마우스 오른쪽 버튼으로 클릭 메뉴에 추가되는 것을 방지할 수 있습니다.
- **메시지 창에 보안 툴바 추가** 기본적으로 Cisco IronPort Email Security 플러그인을 설치할 경우 플러그인 툴바가 이메일 메시지 창에 추가됩니다. 이 옵션을 취소하면 이 툴바가 이메일 메시지 창에 추가되는 것을 방지할 수 있습니다.

Outlook용 보고 플러그인 사용

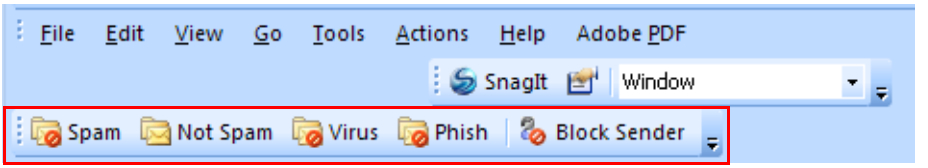
개요

Outlook용 Cisco IronPort Email Security 플러그인을 사용하면 사용자가 받은 편지함으로 수신한 스팸, 바이러스 또는 피싱 이메일에 관해 Cisco에 피드백을 제출할 수 있습니다. 이메일 메시지가 잘못 분류되었을 경우, 또는 예를 들어 스팸으로 처리되어야 하는 경우 Cisco에 이를 알릴 수 있습니다. Cisco는 이 피드백을 사용하여 원하지 않는 메시지가 받은 편지함으로 수신되는 것을 방지하는 이메일 필터를 업데이트할 수 있습니다.

플러그인은 Outlook의 메뉴 모음 및 마우스 오른쪽 버튼으로 클릭 메시지 메뉴를 통해 스팸, 바이러스, 피싱 및 잘못 분류된 이메일을 보고할 수 있는 편리한 인터페이스를 제공합니다. 이메일 보고 후 보고서가 제출되었음을 보여주는 메시지가 나타납니다. 보고하는 메시지는 Cisco의 이메일 필터 개선에 사용되어 받은 편지함으로 수신되는 원치 않는 메일의 전체적인 양을 줄일 수 있습니다.

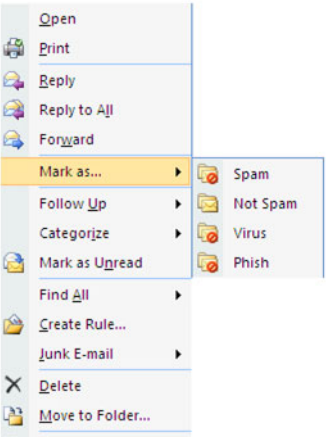
Cisco에 피드백 제공

플러그인은 Outlook에 다음 버튼을 포함하는 새로운 툴바를 제공합니다. 스팸, 스팸 아님, 바이러스, 피싱 및 발신자 차단(발신자 차단은 정크 메일함의 메시지를 차단하지 않음)

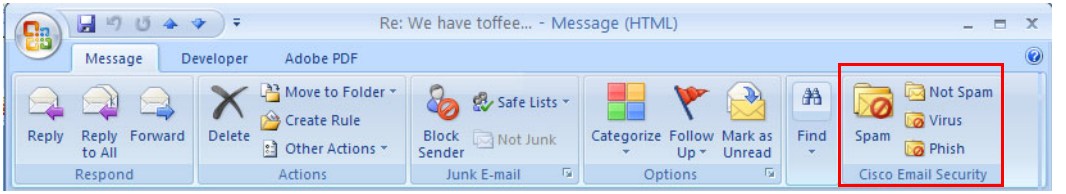


이러한 버튼은 스팸, 바이러스 및 피싱 이메일을 보고하는 데 사용됩니다(피싱 공격은 수신자를 속여 신용카드 번호, 계정 사용자 이름 및 비밀번호, 사회 보장 번호 등의 개인 재정 데이터를 누설하도록 고안된 사기 목적의 '스푸핑된' 웹사이트로 연결되는 이메일). 예를 들어 *infos@paypals.com*으로부터 사기 목적으로 개인 계좌 정보를 요청하는 이메일을 수신하는 경우가 있을 수 있습니다.

또한 스팸, 잘못 분류된 메일, 바이러스 및 피싱을 보고하기 위해 상황에 맞는 마우스 오른쪽 버튼으로 클릭하는 메뉴를 사용할 수 있습니다.

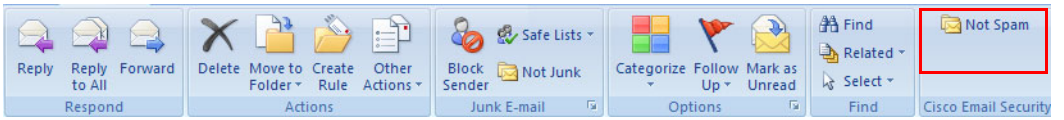


또한 메시지 창의 버튼을 사용하여 스팸, 바이러스, 피싱 및 잘못 분류된 메일을 보고할 수 있습니다(잘못 분류된 메일은 스팸, 바이러스 또는 피싱으로 잘못 표시된 메일을 의미).

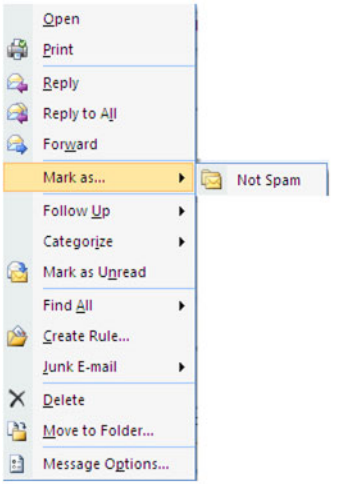


수신한 메일이 스팸으로 잘못 분류되는 경우(즉, 필터링되어 스팸 폴더로 옮겨진 경우) **Not Spam(스팸 아님)** 버튼을 클릭하여 이 이메일을 잘못 분류된 이메일로 보고할 수 있습니다. 이렇게 하면 해당 이메일의 발신자로부터 받은 이메일이 향후 스팸으로 분류되지 않게 됩니다.

또한 정크 메일 폴더에서 메시지 창의 **Not Spam(스팸 아님)** 버튼을 클릭하여 잘못 분류된 메시지로 표시할 수 있습니다.



또한 마우스 오른쪽 버튼으로 클릭 메뉴에서 잘못 분류된 이메일을 표시할 수도 있습니다.



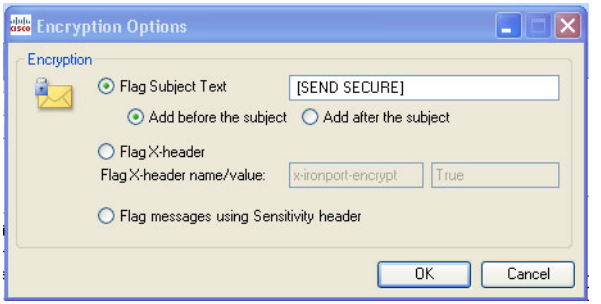
암호화 플러그인

암호화 설정은 Cisco Email Security 페이지에 있습니다. Outlook 2003/2007에서 암호화 설정 변경 사항을 수정하려면, **Tools(도구)** > **Options(옵션)** > **Cisco Email Security**로 이동하여 **Encryption Options(암호화 옵션)**를 클릭합니다.

Outlook 2010의 암호화 설정에 대한 변경 사항을 수정하려면, **File(파일)** > **Options(옵션)** > **Add-ins(애드인)** > **Add-in Options(애드인 옵션)** > **Cisco Email Security**로 이동하여 **Encryption Options(암호화 옵션)** 버튼을 클릭합니다.

Cisco Email Security 탭의 암호화 필드에서 **Enable(활성화)** 확인란을 선택하거나 선택 해제하여 암호화 플러그인을 활성화 및 비활성화할 수 있습니다.

암호화 옵션:



옵션

암호화된 이메일 전송을 위한 옵션

발신 이메일을 암호화하고자 할 때, 암호화할 이메일을 표시 또는 "플래그 지정"해야 합니다. 이렇게 해야 시스템 관리자가 생성한 필터가 암호화를 해야 하는 메시지를 식별할 수 있습니다.

경고 **시스템 관리자와 상의하지 않고 암호화할 이메일의 플래그 지정 방식을 변경하지 마십시오. 이 방법을 적절하게 사용하려면 Cisco IronPort Encryption 어플라이언스의 설정을 변경해야 하며 시스템 관리자만 이를 변경할 수 있습니다.**

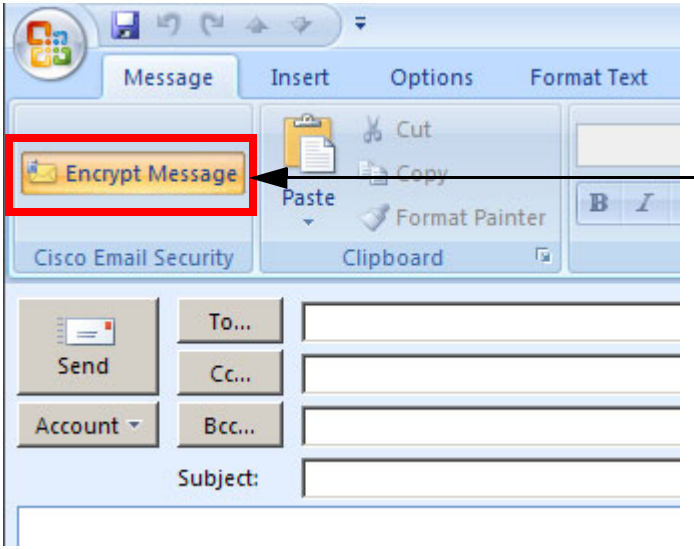
다음과 같은 방법 중 하나를 사용하여 암호화할 이메일을 표시할 수 있습니다.

- **제목 텍스트 플래그 지정**. 암호화를 위해 이메일에 플래그를 지정할 발신 이메일의 제목 필드에 텍스트를 추가할 수 있습니다. 제목 필드에 접두어로 붙일 텍스트를 입력하여 암호화되어야 하는 이메일을 표시할 수 있습니다(기본값은 *[보안 전송]*)입니다.
- **X-헤더 이름/값 플래그 지정** X-헤더는 발신 이메일에 추가될 수 있으며 암호화할 이메일로 플래그를 지정하게 됩니다. 첫 번째 필드에 X-헤더를 입력합니다(기본값은 *x-ironport-encrypt*임). 두 번째 필드에, *참* 또는 *거짓* 값을 입력합니다. *참*을 입력하면 X-헤더가 지정된 메시지가 암호화됩니다(기본값은 *참*임).

- **Outlook 민감도 헤더.** Outlook은 이메일 암호화를 위한 메시지에 플래그를 지정하기 위해 민감도 헤더를 추가할 수 있습니다. 이 방법을 선택하면 암호화할 이메일을 표시하는 데 Outlook의 민감도 헤더를 사용할 수 있습니다.

암호화된 이메일 보내기

이메일을 작성하면서 "메시지 암호화" 버튼을 선택하여 보안 이메일을 전송할 수 있습니다. 보안 메시지를 전송하기 전에 아래와 같이 Encrypt Message(메시지 암호화) 버튼이 선택되어 있는지 확인하십시오.

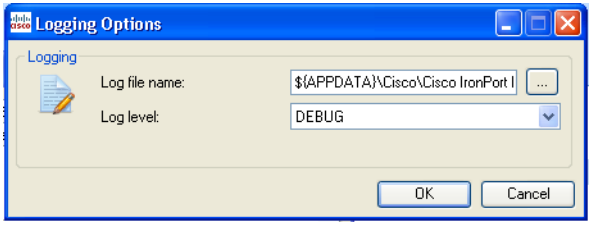


메시지 암호화 버튼은 이메일을 작성할 때 사용할 수 있습니다.

로깅 설정 변경

Logging Options...(로깅 옵션...)을 클릭하여 로깅 옵션 페이지를 엽니다.

기록 옵션:



옵션

로깅 메뉴에서 다음 옵션을 구성할 수 있습니다.

로그 파일 이름

%appdata%\Cisco에 저장될 로그 파일의 이름을 지정할 수 있습니다. 로그 파일 이름에는 .log 확장자가 붙어야 합니다.

로그 레벨

로그 수준은 해당 로그 파일에 기록할 정보를 지정합니다. 다음 로깅 수준 중 하나를 선택할 수 있습니다.

- **오류** 오류 메시지 및 예외 상황이 기록됩니다.
- **경고** 경고 메시지는 오류 메시지와 마찬가지로 기록됩니다.
- **정보** 기본 정보 및 기타 상태 메시지가 기록됩니다. 자동 업데이트 프로세스 상태 메시지가 기록됩니다. 경고 및 오류 메시지도 기록됩니다.
- **디버그** 컨피그레이션 설정에 대한 자세한 정보가 기록됩니다. 모든 오류, 경고 및 정보 오류 메시지가 기록되며 문제 해결에 도움이 될 수 있는 정보가 기록됩니다.

주어진 상황에서 필요한 문제 해결의 수준을 바탕으로 기록 수준을 변경하고자 하는 경우도 있습니다. 예를 들어, Cisco IronPort Email Security 플러그인에 문제가 있다면 개발자에게 최대한의 정보를 제공하기 위해 로깅 수준을 디버그로 설정하여 개발자가 문제를 재현해 진단을 실행하도록 도울 수 있습니다.

진단 도구를 사용한 문제 해결

Cisco IronPort Email Security 플러그인에는 문제를 해결하는 Cisco 지원 부서를 돕기 위한 진단 도구가 포함되어 있습니다. 진단 도구는 플러그인에서 중요한 데이터를 수집하며 이는 그 후에 Cisco 지원 부서로 전송되어 문제 해결을 돕는 데 사용됩니다.

오류를 수신하거나 Cisco IronPort Email Security 플러그인에 복원 절차로도 해결되지 않는 문제가 있는 경우 진단 도구를 사용하고자 할 수 있습니다. 또한 진단 도구를 사용하여 버그를 보고할 때 Cisco 엔지니어와 중요한 정보를 공유할 수도 있습니다.

참고: 오류가 발생하면 진단 섹션에서 문제 해결 팁을 찾아 참조하십시오.

Cisco IronPort Email Security 진단 도구가 수집한 데이터

진단 도구는 컴퓨터에서 다음 정보를 수집합니다.

- 일부 COM 구성 요소에 대한 등록 정보
- 환경 변수
- Cisco IronPort Email Security 플러그인 출력 파일
- Windows 및 Outlook에 대한 정보
- 시스템 사용자 이름 및 PC 이름
- 다른 Outlook 플러그인에 대한 정보

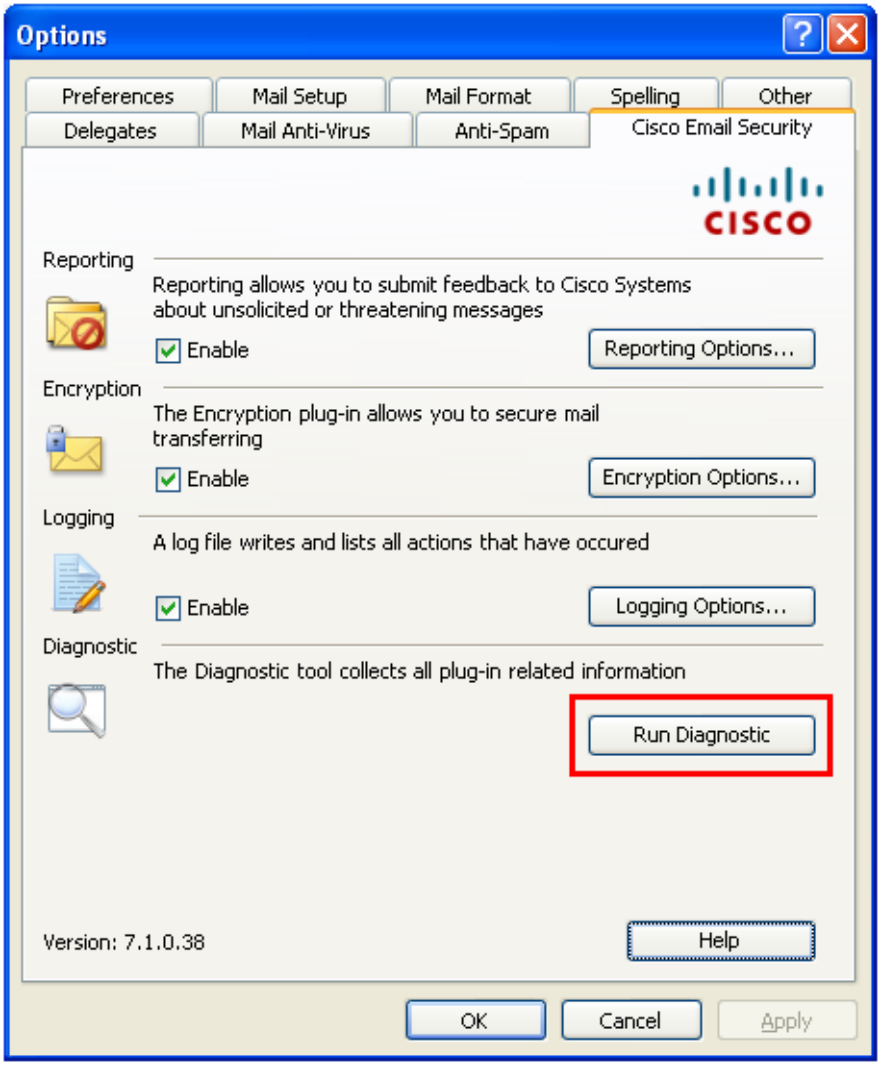
Cisco IronPort Email Security 진단 도구 실행

다음 위치 중 한 곳에서 Cisco Email Security 진단 도구를 실행할 수 있습니다.

- **Cisco Email Security 옵션 탭에서**. 일반적으로, Cisco Email Security 옵션 탭에서 진단 도구를 실행합니다.
- **"Program Files\ Cisco IronPort Email Security 플러그인" 폴더에서** (보통 C:\Program Files\Cisco\Cisco IronPort Email Security 플러그인) 이는 Cisco IronPort Email Security 플러그인이 설치된 폴더입니다.
- **Start Menu(시작 메뉴)> All Programs(모든 프로그램) > Cisco IronPort Email Security 플러그인> Diagnostic Tool(진단 도구)에서**

Outlook 옵션 탭에서 진단 도구 실행

Outlook 2003/2007에서, **Tools(도구)** > **Options(옵션)** > **Cisco Email Security** 탭으로 이동하고 **Run Diagnostics(진단 실행)**를 클릭합니다. 또는 Outlook 2010에서 **File(파일)** > **Options(옵션)** > **Add-ins(애드인)** > **Add-in Options(애드인 옵션)** > **Cisco Email Security**로 이동하여 **Run Diagnostics(진단 실행)**를 클릭합니다.



1. 진단 도구가 데이터를 수집할 수 있도록 몇 초 정도 기다립니다.
2. 진단 도구가 데이터 수집을 완료하면 성공적으로 데이터를 수집했음을 나타내는 메시지가 표시됩니다.

CiscoDiagnosticReport.zip 파일로 이동하여 이를 시스템 관리자나 Cisco 지원 담당자에게 수동으로 전송할 수 있습니다.

프로그램 파일에서 진단 도구 실행

Cisco IronPort Email Security 플러그인이 설치된 폴더(일반적으로 C:\Program Files\Cisco\Cisco IronPort Email Security 플러그인)를 찾아 *Cisco.EmailSecurity.Framework.Diagnostic.exe* 파일을 두 번 클릭합니다.

시작 메뉴에서 진단 도구 실행

Start(시작) > **Programs(프로그램)** > Cisco IronPort Email Security 플러그인에서 진단 도구를 실행합니다. **Diagnostic Tool(진단 도구)**을 클릭합니다. 보고서를 보려면, **Go to Report(보고서로 이동)**를 클릭합니다. 보고서가 zip 파일인 *CiscoDiagnosticsReport.zip*으로 저장됩니다.

Cisco IronPort Email Security 플러그인 설치 제거

Control Panel(제어판) > **Add/Remove Program(프로그램 추가/제거)** 옵션을 사용하거나 setup.exe 프로그램을 실행하여 Cisco IronPort Email Security 플러그인을 설치 제거할 수 있습니다.

설치 제거 중에 다음 항목이 제거됩니다.

- 플러그인이 생성한 모든 레지스트리 항목.
- 프로그램 추가/제거 목록의 플러그인에 대한 항목.
- 플러그인 관련 파일.
- 플러그인 툴바(Outlook에서 제거)

참고 플러그인을 설치 제거해도 Outlook 성능에 영향을 주지 않습니다.

Outlook용 Cisco IronPort Email Security 플러그인 설치 제거

Outlook용 Cisco IronPort Email Security 플러그인은 2가지 방법으로 설치 제거할 수 있습니다.

- **Start(시작)** > **Control Panel(제어판)** > Add/Remove Programs(프로그램 추가/제거)를 클릭합니다. Cisco IronPort Email Security 플러그인을 선택하고 **Remove(제거)**를 클릭합니다.

  또는

- 플러그인 설정 파일(플러그인을 설치하는 데 사용한 파일)을 두 번 클릭하고 **Remove(제거)** 옵션을 선택하여 Cisco IronPort Email Security 플러그인을 설치 제거합니다.

5 장

Lotus Notes용 Cisco IronPort Email Security 플러그인 구성 및 사용

이 장에서는 Lotus Notes용 Cisco IronPort Email Security 플러그인에서 제공되는 기능에 대해 소개합니다. Cisco IronPort Email Security 플러그인에는 일반적인 이메일 보안 플러그인이 몇 가지 포함되어 있습니다. 이 장에는 다음 섹션이 포함되어 있습니다.

Lotus Notes용 Cisco IronPort Email Security 플러그인 일반 설정

Lotus Notes용 Cisco IronPort Email Security 플러그인은 몇 가지 Cisco IronPort Email Security 플러그인을 지원하는 프레임워크입니다.

- 보고 플러그인. 이 플러그인을 사용하면 스팸, 바이러스, 피싱 공격 또는 스팸으로 잘못 분류된 이메일을 보고할 수 있습니다.
- 암호화 플러그인. 이 플러그인을 사용하면 암호화된 보안 이메일을 전송할 수 있습니다.

옵션 페이지를 통해 Cisco IronPort Email Security 플러그인을 구성할 수 있습니다. 옵션 페이지에 액세스하려면 **Actions(작업)** > **Cisco Email Security**로 이동하십시오.

Cisco Email Security 옵션 페이지:

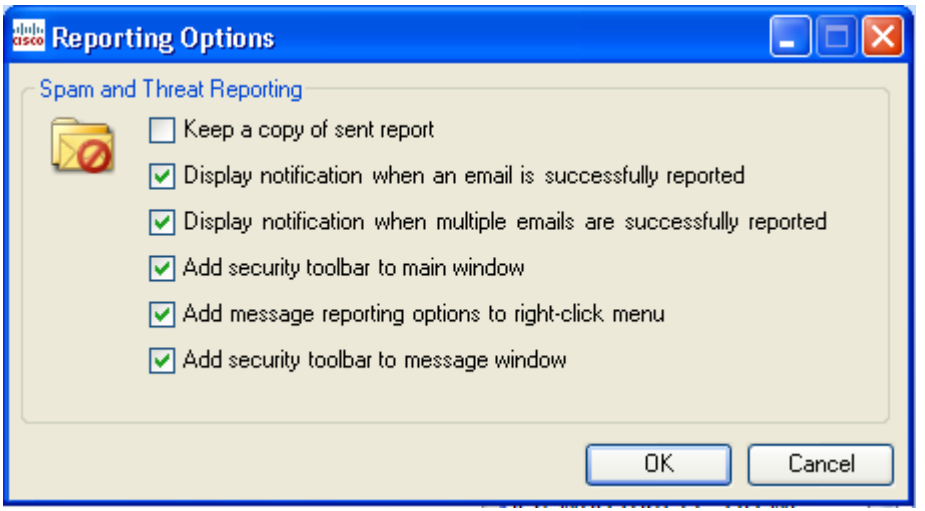
이 탭에서 해당 옵션에 대한 **Enable(활성화)** 확인란을 선택하여 보고, 암호화 및 로깅을 활성화할 수 있습니다. 추가 설정을 구성하려면, **Reporting Options...(보고 옵션...)**, **Encryption Options...(암호화 옵션...)** 또는 **Logging Options...(로깅 옵션...)** 버튼을 클릭하십시오. 또한 문제 해결 시 Cisco 지원 부서에 전송할 Cisco IronPort Email Security 플러그인에 대한 보고를 실행하기 위한 진단 도구도 사용할 수 있습니다.

보고 플러그인

옵션 대화상자

보고 플러그인을 사용하면 사용자가 수신한 이메일이 스팸, 피싱 공격, 바이러스인지 또는 스팸으로 잘못 분류되었는지를 Cisco에 보고할 수 있습니다.

옵션 대화상자를 통해 Lotus Notes용 Cisco Email Security 보고 플러그인을 구성할 수 있습니다. 보고 옵션 페이지에 액세스하려면, **Actions(작업)** > **Cisco Email Security Options(Cisco Email Security 옵션)**로 이동하여 대화상자에서 **Reporting(보고)** 탭을 선택합니다.



옵션

이 섹션에서는 수정 가능한 보고 옵션에 대해 설명합니다.

전송된 보고서의 복사본 보관

기본적으로 Cisco에 스팸, 바이러스, 잘못 분류된 스팸 또는 바이러스로 이메일 메시지를 보고하면 전송한 보고 이메일이 삭제됩니다. 이 옵션을 선택하면 이메일이 삭제되는 것을 방지합니다.

이메일이 성공적으로 보고되었을 경우 알림 표시

이메일이 보고되면 이메일이 성공적으로 보고되었음을 나타내는 알림을 표시하기 위해 이 옵션을 선택할 수 있습니다.

여러 이메일이 성공적으로 보고되었을 경우 알림 표시

여러 이메일이 보고되면 이메일이 성공적으로 보고되었음을 나타내는 알림을 표시하기 위해 이 옵션을 선택할 수 있습니다.

기본 창에 보안 툴바 추가

이 옵션을 사용하여 기본 창에 보안 툴바를 추가할 수 있습니다.

마우스 오른쪽 버튼으로 클릭 창에 메시지 보고 옵션 추가

이 옵션을 사용하여 마우스 오른쪽 버튼으로 클릭 창에 메시지 보고 옵션을 추가할 수 있습니다.

메시지 창에 보안 툴바 추가

이 옵션을 사용하여 메시지 창에 보안 툴바를 추가할 수 있습니다.

Lotus Notes용 보고 플러그인 사용

Lotus Notes용 Cisco Email Security 보고 플러그인을 사용하면 사용자가 받은 편지함으로 수신한 스팸, 바이러스 또는 피싱 이메일에 관해 Cisco에 피드백을 제출할 수 있습니다. Cisco는 이 피드백을 사용하여 원하지 않는 메시지가 받은 편지함으로 수신되는 것을 방지하는 이메일 필터를 업데이트할 수 있습니다.

Lotus Notes가 스팸, 바이러스, 피싱 및 잘못 분류된 이메일을 보고할 수 있도록 메인 메뉴 모음을 통해 설정을 구성할 수 있습니다. 이메일 보고 후 보고서가 제출되었음을 보여주는 메시지가 나타납니다. 보고하는 메시지는 Cisco의 이메일 필터 개선에 사용되어 받은 편지함으로 수신되는 원치 않는 메일의 전체적인 양을 줄일 수 있습니다.

암호화 플러그인

암호화 옵션 구성

Cisco Email Security 옵션 대화상자에서 암호화 플러그인 설정을 수정할 수 있습니다. 암호화 설정을 수정하려면, **Actions(작업)** > **Cisco Email Security Options(Cisco Email Security 옵션)**로 이동하여 **Encryption Options(암호화 옵션)**를 클릭합니다.

옵션

암호화된 이메일 전송을 위한 옵션

발신 이메일을 암호화하고자 할 때, 암호화할 이메일을 표시 또는 "플래그 지정"해야 합니다. 이렇게 해야 시스템 관리자가 생성한 필터가 암호화를 해야 하는 메시지를 식별할 수 있습니다.

경고 **시스템 관리자와 상의하지 않고 암호화할 이메일의 플래그 지정 방식을 변경하지 마십시오. 이 방법을 사용하려면 Cisco IronPort Encryption 어플라이언스에 변경 사항을 적용해야 하며 시스템 관리자만 변경할 수 있습니다.**

다음과 같은 방법 중 하나를 사용하여 암호화할 이메일을 표시할 수 있습니다.

- **제목 텍스트 플래그 지정**. 암호화를 위해 이메일에 플래그를 지정할 발신 이메일의 제목 필드에 텍스트를 추가할 수 있습니다. 제목 필드에 접두어로 붙일 텍스트를 입력하여 암호화되어야 하는 이메일을 표시할 수 있습니다(기본값은 *[보안 전송]*입니다).
- **X-헤더 이름/값 플래그 지정** X-헤더는 발신 이메일에 추가될 수 있으며 암호화할 이메일로 플래그를 지정하게 됩니다. 첫 번째 필드에 X-헤더를 입력합니다(기본값은 *x-ironport-encrypt*임). 두 번째 필드에, 참 또는 거짓 값을 입력합니다. *참*을 입력하면 X-헤더가 지정된 메시지가 암호화됩니다(기본값은 *참*임).

암호화 플러그인 사용

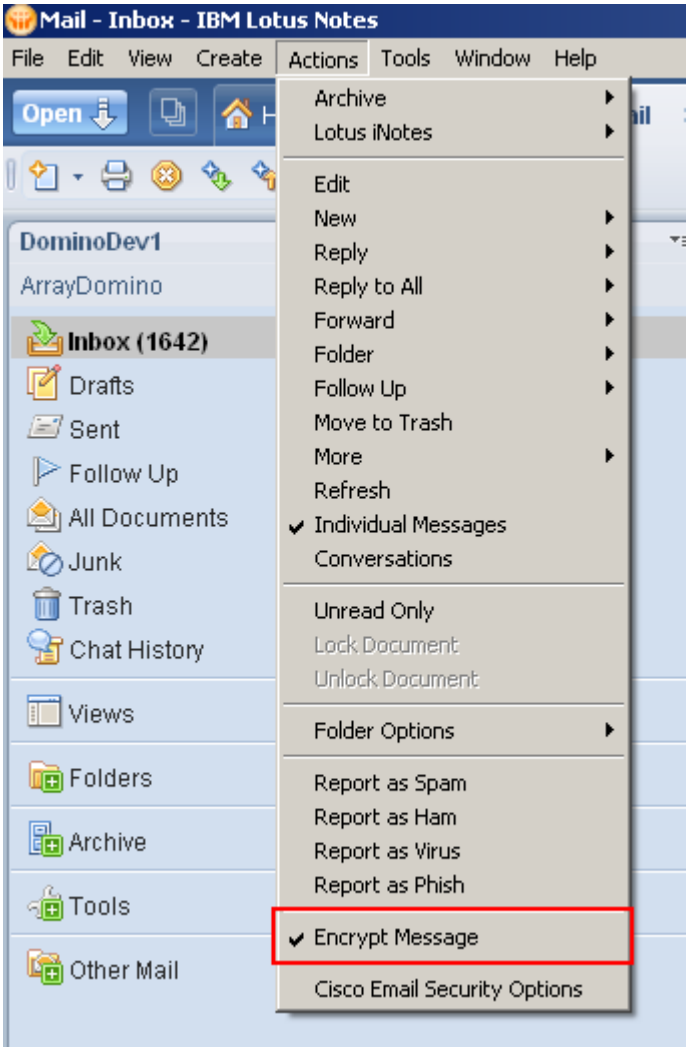
개요

암호화 플러그인을 사용하면 Lotus Notes 이메일 프로그램에서 암호화된 이메일을 전송할 수 있습니다. 보안 이메일을 보낼 때, Cisco Email Security 암호화 플러그인이 암호화가 표시된 이메일을 안전하게 전송하여 대상 수신자만 해당 이메일을 읽을 수 있도록 합니다.

보안 이메일 전송

작업 메뉴에서 **Encrypt message(메시지 암호화)**를 선택하여 보안 이메일을 전송하도록 메일 시스템을 설정할 수 있습니다.

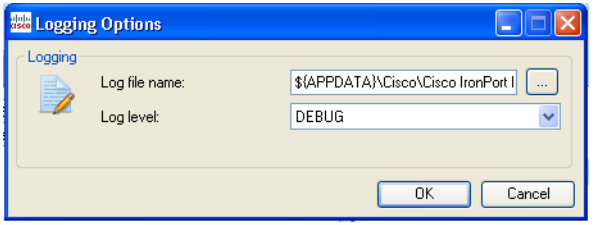
보안 메시지를 전송하려면 아래와 같이 **Encrypt message(메시지 암호화)** 버튼이 선택되어 있는지 확인하십시오.



로깅 옵션 변경

Logging Options...(로깅 옵션...)을 클릭하여 로깅 옵션 페이지를 엽니다.

기록 옵션:



옵션

로깅 메뉴에서 다음 옵션을 구성할 수 있습니다.

로그 파일 이름

%appdata%\Cisco에 저장될 로그 파일의 이름을 지정할 수 있습니다. 로그 파일 이름에는 .log 확장자가 붙어야 합니다.

로그 레벨

로그 수준은 해당 로그 파일에 기록할 정보를 지정합니다. 다음 로깅 수준 중 하나를 선택할 수 있습니다.

- **오류** 오류 메시지 및 예외 상황이 기록됩니다.
- **경고** 경고 메시지는 오류 메시지와 마찬가지로 기록됩니다.
- **정보** 기본 정보 및 기타 상태 메시지가 기록됩니다. 자동 업데이트 프로세스 상태 메시지가 기록됩니다. 경고 및 오류 메시지도 기록됩니다.
- **디버그** 컨피그레이션 설정에 대한 자세한 정보가 기록됩니다. 모든 오류, 경고 및 정보 오류 메시지가 기록되며 문제 해결에 도움이 될 수 있는 정보가 기록됩니다.

주어진 상황에서 필요한 문제 해결의 수준을 바탕으로 기록 수준을 변경하고자 하는 경우도 있습니다. 예를 들어, Cisco IronPort Email Security 플러그인에 문제가 있다면 개발자에게 최대한의 정보를 제공하기 위해 로깅 수준을 디버그로 설정하여 개발자가 문제를 재현해 진단을 실행하도록 도울 수 있습니다.

문제 해결 및 진단

이 섹션에서는 Lotus Notes용 Cisco IronPort Email Security 플러그인을 사용하는 동안 발생할 수 있는 일반적인 오류와 이러한 문제를 해결하기 위한 몇 가지 문제 해결 팁에 대해 소개합니다.

참고 동일한 오류 메시지가 여러 번 표시되거나 Lotus Notes용 Cisco IronPort Email Security 플러그인 기능이 중단되는 경우 복구 프로세스를 실행해 보십시오. 복구 프로세스를 실행한 후에도 같은 오류가 발생하면 다음 단계에 따라 Cisco에 Cisco Email Security 진단 도구에 대한 피드백을 보내 주십시오.

일반적인 시작 오류

컨피그레이션 파일을 초기화하는 동안 오류 발생.

다음 메시지는 Outlook을 시작할 때 나타날 수 있습니다.

- Cisco IronPort Email Security 플러그인 컨피그레이션 파일을 초기화하는 동안 오류 발생. 일부 설정을 기본값으로 설정합니다.
- 보고 구성 요소에 대한 컨피그레이션을 읽는 동안 오류 발생. 일부 설정을 기본값으로 설정합니다.
- 암호화 구성 요소에 대한 컨피그레이션을 읽는 동안 오류 발생. 일부 설정을 기본값으로 설정합니다.

컨피그레이션 파일(*%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes\CommonConfig.xml*) 의 일부 값이 손상된 경우 이러한 오류 메시지가 발생합니다.

해결책

플러그인이 손상된 컨피그레이션 파일에서 기본값을 복원합니다. 하지만 오류 메시지를 계속 수신하는 경우 복원 프로세스를 실행하여 컨피그레이션 파일을 수정하십시오.

컨피그레이션 파일 없음. 기본값으로 설정 구성.

다음 오류 메시지 중 하나는 Outlook을 시작할 때 표시될 수 있습니다.

- Cisco IronPort Email Security 플러그인 컨피그레이션 파일을 찾을 수 없습니다. 기본값으로 설정 구성.
- 암호화 구성 요소에 대한 컨피그레이션 파일을 찾을 수 없습니다. 기본값으로 설정 구성.
- 보고 구성 요소에 대한 컨피그레이션 파일을 찾을 수 없습니다. 기본값으로 설정 구성.

해결책

플러그인이 손상된 컨피그레이션 파일에서 기본값을 복원합니다. 하지만 오류 메시지를 계속 수신하는 경우 복원 프로세스를 실행하여 컨피그레이션 파일을 수정하십시오.

메시지 보고 오류

이메일 주소가 올바르지 않습니다.

Lotus Notes에서 **Report as Spam(스팸으로 보고)**, **Report as Virus(바이러스로 보고)**, **Report as Phish(피싱으로 보고)** 또는 **Report as Not Spam(스팸이 아닌 것으로 보고)** 버튼을 클릭하면 다음 메시지가 표시될 수 있습니다.

보고서 유형의 주소가 올바르지 않습니다. 컨피그레이션 파일을 업데이트해 주십시오.

보고 플러그인을 사용 중이며 보고하려는 이메일 유형이 잘못된 경우 이 오류 메시지가 표시됩니다. 스팸 및 피싱 이메일을 보고하고 합법적 이메일을 "스팸 아님"으로 보고하려면 보고 플러그인 파일을 복구해야 합니다.

해결책

%appdata%\Cisco\Cisco Email Security Plug In\LotusNotes 폴더에서 보고 컨피그레이션을 확인합니다. 이를 삭제하고 복원 프로세스를 실행하여 기본값을 복원합니다.

Lotus Notes용 Cisco IronPort Email Security 플러그인 파일 복원

1. **Control Panel(제어판)** > **Add(추가)** 또는 **Remove Programs(프로그램 제거)**로 이동합니다.
2. 프로그램 목록에서 Cisco IronPort Email Security 플러그인을 찾아 **Change(변경)**를 클릭합니다.
3. Lotus Notes가 닫혔는지 확인합니다.
4. Cisco IronPort Email Security 플러그인 설치 프로그램을 선택하고 **Repair radio(라디오 복원)** 버튼을 클릭합니다.
5. **Next(다음)**을 클릭합니다. 설치 프로그램 복원 프로세스가 실행됩니다.
6. 오류를 야기한 작업을 수행합니다. 복구 프로세스를 실행한 후에도 같은 오류가 발생하면 다음 단계에 따라 Cisco에 진단 도구에 대한 피드백을 보내 주십시오.

Cisco Email Security 진단 도구

Cisco는 Cisco IronPort Email Security 플러그인을 위한 진단 도구를 제공하며 이를 통해 문제에 대한 전체 분석에 필요한 세부 정보를 Cisco에 전송할 수 있습니다. 오류를 수신하거나 Cisco IronPort Email Security 플러그인에 복원 절차로도 해결되지 않는 문제가 있는 경우 진단 도구를 사용하고자 할 수 있습니다. 또한 진단 도구를 사용하여 버그를 보고할 때 Cisco 엔지니어와 중요한 정보를 공유할 수도 있습니다.

오류가 발생하면 진단 섹션에서 문제 해결 팁을 찾아 참조하십시오.

Cisco Email Security 진단 도구가 수집한 데이터

진단 도구는 컴퓨터에서 다음 정보를 수집합니다.

- 일부 COM 구성 요소에 대한 등록 정보
- 환경 변수
- Cisco Email Security 출력 파일
- Windows 및 Lotus Notes에 대한 정보
- 시스템 사용자 이름 및 PC 이름
- 다른 Lotus Notes 플러그인에 대한 정보

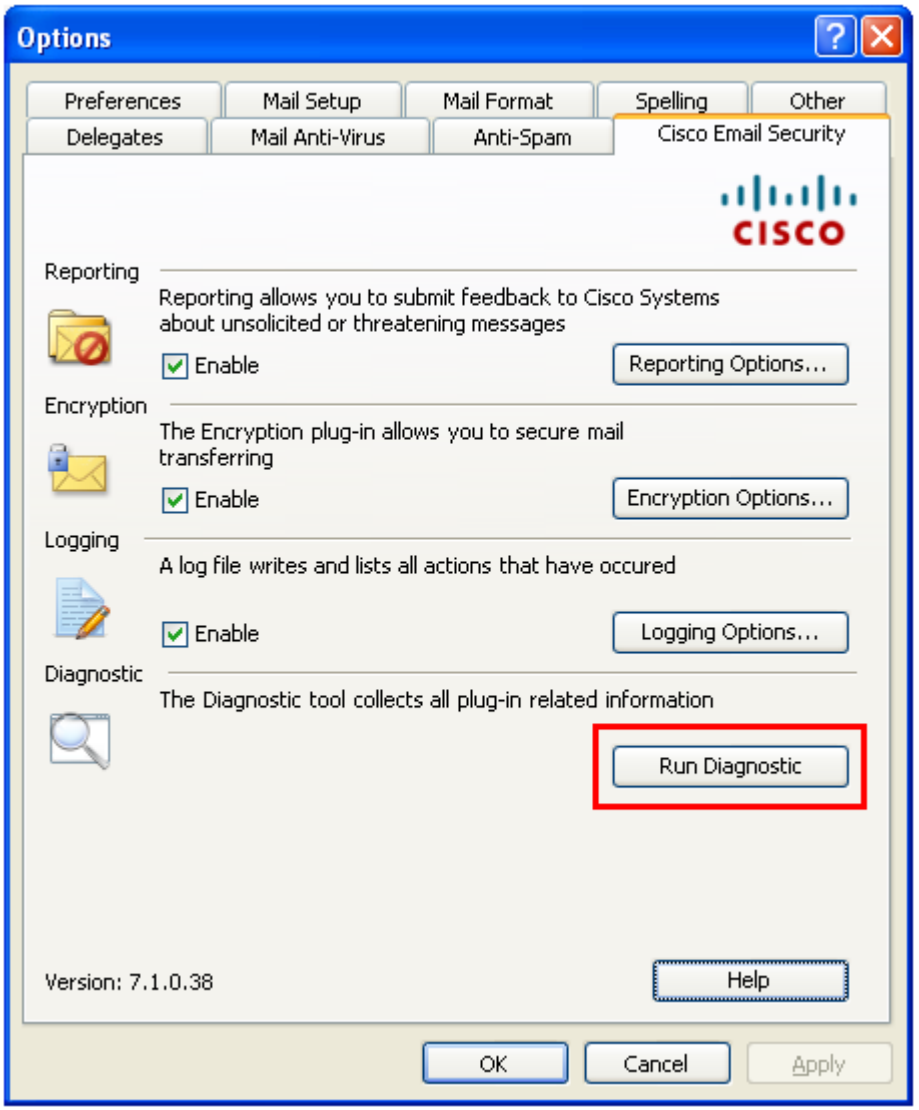
Cisco Email Security 진단 도구 실행

다음 위치 중 한 곳에서 Cisco Email Security 진단 도구를 실행할 수 있습니다.

- **Cisco Email Security 옵션 대화상자에서**. 일반적으로, Cisco Email Security 옵션 대화상자에서 진단 도구를 실행합니다. **Actions(작업)** > **Cisco Options(Cisco 옵션)**에서 진단 도구에 액세스할 수 있습니다.
- **Program Files\Cisco IronPort Email Security 플러그인 폴더에서**(보통 C:\Program Files\Cisco\Cisco IronPort Email Security 플러그인) 이는 Cisco IronPort Email Security 플러그인이 설치된 폴더입니다.

옵션 대화상자에서 진단 도구 실행

Actions(작업) > **Cisco Email Security Options(Cisco Email Security 옵션)**로 이동하여 **Run Diagnostics(진단 실행)**를 클릭합니다. 진단 도구가 데이터를 수집할 수 있도록 몇 초 정도 기다립니다.



진단 도구가 데이터 수집을 완료하면 성공적으로 데이터를 수집했음을 나타내는 메시지가 표시됩니다. 도구는 해당 데이터를 *CiscoDiagnosticReport.zip*이라는 이름의 zip 파일로 보관합니다.

Go to Report(보고서로 이동)를 클릭하여 *CiscoDiagnosticReport.zip* 파일에 액세스함으로써 이를 시스템 관리자나 Cisco Security 관리자에게 수동으로 전송할 수 있습니다.

프로그램 파일에서 진단 도구 실행

Start(시작) > **Programs(프로그램)** > **Cisco Email Security for Lotus Notes(Lotus Notes용 Cisco Email Security)**에서 진단 도구를 실행합니다. 또는 Cisco Email Security가 설치된 폴더(일반적으로 C:\Program Files\Cisco\Cisco IronPort Email Security 플러그인)를 찾아 *Cisco.EmailSecurity.Framework.Diagnostic.exe* 파일을 두 번 클릭합니다.

설치 제거

Control Panel(제어판) > Add/Remove Program(프로그램 추가/제거)을 통해서나 setup.exe 프로그램을 실행하여 Cisco IronPort Email Security 플러그인을 설치 제거할 수 있습니다.

설치 제거 중에 다음 항목이 제거됩니다.

- 플러그인이 생성한 모든 레지스트리 항목.
- 프로그램 추가/제거 목록의 플러그인에 대한 항목.
- 플러그인 관련 파일.

참고 플러그인을 설치 제거해도 Lotus Notes 성능에 영향을 주지 않습니다.

플러그인 설치 제거

Cisco IronPort Email Security 플러그인은 2가지 방법으로 설치 제거할 수 있습니다.

- **Start(시작)** > **Control Panel(제어판)** > **Add/Remove Programs(프로그램 추가/제거)**를 클릭합니다. Cisco IronPort Email Security 플러그인을 선택한 다음 **Remove(제거)**를 클릭합니다.

  또는

- 플러그인 설정 파일(플러그인을 설치하는 데 사용한 파일)을 두 번 클릭하고 **Remove(제거)** 옵션을 선택하여 Cisco IronPort Email Security 플러그인을 설치 제거합니다.

부 록 A

IronPort 최종 사용자 라이센스 계약

이 부록에는 다음 섹션이 포함되어 있습니다.

Cisco IronPort Systems, LLC 소프트웨어 라이센스 계약

모든 사용자를 대상으로 한 알림: 소프트웨어 라이센스(아래 정의 참조)에 대한 다음 법적 동의서("계약")를 신중하게 읽어주십시오. 메시지가 표시될 때 수락 버튼 또는 "예"를 입력하면 사용자(개인 또는 단일 단체, 통칭 "회사")는 CISCO IRONPORT SYSTEMS, LLC, A DELAWARE CORPORATION("IRONPORT") 및 회사(통칭, "당사자") 간의 다음 계약이 체결되며 해당 계약의 한 당사자가 된다는 점에 동의하게 됩니다. 메시지가 표시될 때 수락 버튼 또는 "예"를 입력하면 사용자는 (A) 회사를 대표할 정당한 권한을 보유하며 (B) 회사를 대표하여 이 계약의 약관을 수락하며, 이에 따라 계약이 체결됩니다. 사용자나 사용자가 대표하고 있는 회사(통칭 "회사")가 이 계약서의 약관에 동의하지 않는 경우 메시지가 표시될 때 취소 버튼을 클릭하거나 "N"을 입력하고 해당 소프트웨어에 대해 지급된 가격을 전액 환불받을 수 있도록 IRONPORT 또는 이 소프트웨어를 제공한 리셀러에게 즉시(아래에 정의된 바와 같이 배송일로부터 30일 경과 시 불가) 이를 알려주시기 바랍니다.

1. 정의

1.1 "기업 서비스"는 회사의 내부 비즈니스를 수행할 목적으로 최종 사용자에게 제공되었으며 구매 계약서, 평가 합의서, 베타 또는 출시 전 합의, 구매 발주서, 판매 견적서 또는 회사와 IronPort 또는 이의 리셀러 사이에 체결된 기타 모든 합의 사항에 설명된 바와 같이 회사의 제품을 통해 활성화된 회사의 이메일 또는 인터넷 서비스를 비롯하여 해당하는 사용자 인터페이스 및 시스템 아키텍처와 인터페이스 개요를 설명하는 IronPort의 표준 시스템 설명서 문서("라이센스 문서")를 의미합니다.

1.2 "최종 사용자"는 회사에 의해 인터넷에 대한 액세스나 회사 서비스를 통한 이메일 서비스 사용을 공인받은 직원, 하청업체 또는 기타 에이전트를 의미합니다.

1.3 "서비스"는 (i) 업데이트 및 업그레이드를 포함한 소프트웨어 기능 제공, (ii) 상황에 따라 IronPort나 리셀러로부터의 지원 제공을 의미합니다.

1.4 "소프트웨어"는 (i) IronPort의 하드웨어 제품과 더불어 IronPort가 회사에 라이센스를 부여하는 IronPort의 독점 소프트웨어이며, (ii) IronPort 서드파티 라이센스 허가자에 의해 제공되는, IronPort의 하드웨어 제품과 사용하기 위해 구현할 수 있도록 회사에 라이센스가 제공된 모든 소프트웨어, (iii) IronPort의 하드웨어 제품과 더불어 IronPort가 회사에 라이센스 권한을 부여한 기타 모든 IronPort 소프트웨어 모듈, (iv) 그에 대한 모든 업데이트 및 업그레이드를 의미합니다.

1.5 "업데이트"는 소프트웨어에 중요한 새 기능을 추가하지는 않으며 IronPort나 서드파티 라이센스 허가자가 출시한 사소한 업데이트, 오류 수정 및 버그 픽스를 의미합니다. 업데이트는 소수점 오른쪽에 있는 소프트웨어의 릴리스 번호를 증가시키는 방식으로 지정되어 있습니다(예: 소프트웨어 1.0에서 소프트웨어 1.1로). 업데이트라는 용어는 IronPort나 서드파티 라이센스 허가자가 별도의 제품으로 출시하고 라이센스 권한을 확보한 업그레이드나 새로운 소프트웨어 버전을 명확히 제외합니다.

1.6 "업그레이드"는 소프트웨어 수정본을 의미합니다. 출시 여부와 그 시기는 전적으로 IronPort 또는 서드파티 라이센스 권한자의 재량에 따라 결정되며 기존 기능에 새로운 개선 사항을 추가합니다. 업그레이드는 소수점 왼쪽에 있는 소프트웨어의 릴리스 번호를 증가시키는 방식으로 지정되어 있습니다(예: 소프트웨어 1.0에서 소프트웨어 2.0으로). 업그레이드에는 IronPort나 서드파티 라이센스 허가자가 별도의 제품으로 출시하고 라이센스 권한을 확보한 새로운 버전의 소프트웨어가 포함되지 않습니다.

2. 라이센스 부여 및 데이터 수집에 동의

2.1 소프트웨어 라이센스. 소프트웨어 및 라이센스 문서를 사용하여 회사는 본 계약의 약관에 동의하는 것으로 간주되며 회사가 본 계약을 준수하는 한 IronPort는 이 기간 동안 최종 사용자에게 회사 서비스의 조항과 관련된 IronPort의 하드웨어 제품에서만 소프트웨어를 사용할 수 있는 비독점적이고 2차 라이센스를 제공할 수 없으며 양도할 수 없는 라이센스를 회사에 제공합니다. 이 라이센스의 기간 및 범위는 라이센스 문서에 추가로 정의됩니다. 본 계약에서 명시적으로 부여한 것을 제외한 모든 소프트웨어의 권한, 소유권 또는 이익은 IronPort, IronPort의 리셀러 또는 별도의 라이센스 허가자가 회사에 부여하지 않습니다. 본 라이센스 및 모든 서비스는 함께 종료됩니다.

2.2 데이터 사용에 대한 동의 및 라이센스. 본 계약의 섹션 8과 IronPort가 회사에 사전 고지한 후 때때로 수정할 수 있는 IronPort 개인정보 보호정책 (http://www.IronPort.com/privacy.html)에 따라 라이센스 문서에 설명된 바와 같이 회사는 IronPort에 회사에서 데이터를 수집하고 이를 사용할 수 있는 라이센스를 부여하며 이는 IronPort에 의해 때때로 업데이트될 수 있습니다("데이터"). 해당 데이터를 사용하여 보고서 또는 통계가 생성되는 경우 집계된 정보만을 공개해야 하며 사용자 이름, 전화번호, 애매하게 변경하지 않은 파일 이름, 이메일 주소, 실제 주소 및 파일 컨텐츠 등을 포함하는 데이터를 통해 최종 사용자를 식별할 수 있는 정보가 도출되어서는 안 됩니다. 전술한 내용에도 불구하고 회사는 사전 서면 알림이나 전자 알림을 통해 언제든지 데이터의 수집 및 사용 권한을 해지할 수 있으며 그러한 권한의 말소로 인해 회사는 소프트웨어나 소프트웨어 구성 요소를 사용하지 못할 수도 있습니다.

3. 기밀성. 각 당사자는 유사한 수준의 자사 기밀 정보를 보호하는 것과 동일한 정도로 상대방의 모든 기밀 정보를 엄수하고(어떤 경우에도 합리적인 엄수 수준을 고수해야 함) 그러한 기밀 정보를 이 계약서에서 허용하는 상황에서만 사용할 것에 동의합니다. 이 계약의 목적에 따른 "기밀 정보"는 당사자가 "기밀"로 표시했거나 공개하는 당사자에 의해 독점 또는 기밀의 특성이 있다고 합리적으로 간주되는 정보를 의미하며 그러한 표시의 유무에 상관없이 IronPort가 제공하는 소프트웨어의 설계 검토 및 사전 제작 버전에 공개된 데이터, 소프트웨어, 정보가 명시적으로 기밀 정보로 지정되었다면 이에 해당합니다.

4. 소유권. 소프트웨어 및 기타 자료, IronPort나 이의 리셀러가 회사에 제공한, 앞서 말한 자료와 관련 있는 모든 연관 지적 재산권(아래 정의 참조)의 법적 소유권 및 소유권은 IronPort 및/또는 이의 뛰어난 라이센스 허가자의 독점 자산으로 남아 있게 됩니다. 회사와 그 직원 및 에이전트는 IronPort 또는 이의 리셀러가 제공한 소프트웨어 또는 기타 자료 또는 사본에 표시된 상표나 기타 소유권 고지, 범례, 기호 또는 레이블을 제거하거나 변경할 수 없습니다. 회사는 해당 소프트웨어에 의해 생성된 모든 소프트웨어 또는 모든 내부 데이터 파일에서 수익을 창출하기 위해 수정, 전달, 재판매, 배포, 복사, 향상, 개조, 번역, 역컴파일, 역설계, 분해를 도모하거나 또는 소스 코드를 추출하고자 결심하거나 시도해서는 안 되고 소프트웨어나 라이센스 문서를 기반으로 어떤 파생물도 작성해서는 안 되며 다른 누군가에게 그렇게 하도록 허용하거나 그럴 권한을 부여하지 않을 것에 동의합니다. 서면 합의 없이는 이 계약을 수행하는 과정 중에 IronPort 또는 이의 우수한 라이센스 허가자가 생성했거나 개발한 모든 프로그램, 발명품, 컨셉, 문서, 사양 또는 그러한 작업 수행과 연관된 기타 서면이나 그래픽 자료 및 미디어 또는 모든 저작권, 데이터베이스 권한, 특허, 영업상 비밀, 상표, 저작 인격권 또는 기타 지적 재산권("지적 재산권")은 그 어떤 경우에도 미국 연방 법전의 표제 17(1976년 저작권법) 의미 내에서 회사를 위해 제작되고 하청된 작업으로 간주되지 않습니다.

5. 제한적 보증 및 보증 부인

5.1 제한적 보증. IronPort는 적합하게 설치되어 적절하게 사용된 경우 소프트웨어가 배송일로부터 90일 또는 라이센스 문서에서 명시한 기간 중 더 긴 기간("보증 기간") 동안 라이센스 문서에 기재된 사양과 상당히 일치하는 성능을 나타낼 것임을 보증합니다. 이 섹션에 포함된 보증의 모든 위반에 대해 회사의 독점적 해결 방안과 IRONPORT의 전체적 책임은 오류 또는 불일치함의 즉각적인 수정에 해당하며 이는 해당 불일치성에 대해 회사가 보증 기간 내에 IRONPORT 및/또는 이의 리셀러에 보고하는 것을 전제로 합니다. 이 보증은 회사에만 적용되는 것으로 다른 어떤 최종 사용자나 기타 서드파티에 이전될 수 없습니다. IronPort는 그러한 위반이 다음과 같은 사항과 직/간접적으로 관련되어 야기된 경우를 제외하고는 이 섹션에 따른 보증 위반에 대해 책임을 지지 않습니다. (i) 회사 또는 서드파티에 의한 소프트웨어의 무단, 부적절, 불완전 또는 부적당한 유지 관리나 교정, (ii) 모든 서드파티 하드웨어 소프트웨어, 서비스 또는 시스템, (iii) 소프트웨어 또는 서비스에 대한 모든 무단 수정 또는 변경, (iv) 소프트웨어의 모든 무단 또는 부적절한 사용이나 작동, 또는 회사가 해당하는 환경 사양을 준수하지 못한 경우, (v) IronPort 또는 리셀러가 때때로 제공하는 업데이트, 업그레이드, 픽스 또는 리비전을 설치 및/또는 사용하지 않은 경우.

5.2 보증 부인. 본 계약의 섹션 5.1에 기재된 명시적 보증은 소프트웨어 또는 서비스와 관련된 유일한 성능 보증으로 여겨집니다. IRONPORT는 "있는 그대로" 기반으로 이에 의거해 라이센스 관련 법령에서 허용하는 최대 규모로 소프트웨어 및 서비스 라이센스 권한을 부여합니다. 본 계약에서 특별히 명시한 경우를 제외하고 IRONPORT와 우수한 라이센스 허가자는 명시적이든 묵시적이든 법정 사항이든 이에 관계없이(사실 기반이든 법률 시행에 의한 것이든) 어떤 유형의 대표나 보증을 공언하지 않으며 특정 목적에 대한 적합성이나 상품성에 대한 묵시적 보증을 제한없이 포함하는 기타 모든 보증을 명시적으로 부인합니다. IRONPORT나 서드파티 라이센스 허가자는 소프트웨어 또는 서비스가 (i) 결함, 오류 또는 버그가 없고 (ii) 소프트웨어의 작동이 중단되지 않으며 (iii) 소프트웨어 사용으로 인해 파생되었거나 그로 인해 도출된 결과물이나 정보가 정확하고 완전하며 믿을 수 있거나 안전하다는 점을 보증하지 않습니다.

6. 책임의 제한. 수익 손실, 대체 상품 또는 서비스 조달 비용, 사업 기회 상실, 데이터 사용 권한 상실, 사업 중단 또는 특수한 간접 사고 또는 모든 유형의 결과적 손해에 대해 그러한 당사자가 손해의 가능성을 사전에 고지했다고 하더라도 양 당사자는 어떤 경우에도 상대방에 대해 관련 법령에서 허용되는 최대 규모로 법적 책임을 지지 않습니다. 그러한 손해가 계약, 불법 행위 또는 다른 법무상에 기반하는지 여부와 관계없이 그러한 책임을 야기한 이벤트 발생 이전의 12개월 동안 소프트웨어 및 서비스에 대해 지급한 총 금액을 초과하는 금액에 대해서는 어떤 경우에도 본 계약의 조항에 따라 쌍방에 책임이 부과되지 않습니다.

7. 기간 및 종료. 본 계약의 용어("용어")는 라이센스 문서에 명시된 바와 동일합니다. IronPort가 본 계약 또는 라이센스 문서의 실제 조항을 수행하지 못할 경우 회사는 계약 해지 30일 이전에 서면 고지를 통해 이를 알리고 해지할 수 있으며 이 30일 동안 불이행이 처리되지 않을 경우 계약은 해지됩니다. 회사가 본 계약 또는 라이센스 문서의 실제 조항을 수행하지 못할 경우 IronPort는 계약 해지 30일 이전에 서면 고지를 통해 이를 알리고 해지할 수 있으며 이 30일 동안 불이행이 처리되지 않을 경우 환불 없이 계약이 해지됩니다. 본 계약은 다음 조건에 해당하는 경우 한쪽 당사자가 사전 고지 없이 언제든지 해지할 수 있습니다. (i) 해당 기관이 지불 불능, 법정 관리 또는 파산 절차 또는 그러한 당사자의 채무 해결을 위한 기타 절차를 수행하거나 이에 대항하는 경우, (ii) 그러한 기타 당사자가 채권자의 이득을 위해 일반 할당을 수행하거나 (iii) 그러한 당사자의 해산. 섹션 2에서 부여된 라이센스 권한은 본 계약의 해지나 만료 시 즉시 말소됩니다. 본 계약의 해지 또는 만료 후 30일(역일) 이내에 회사는 소프트웨어 및 IronPort 또는 리셀러가 본 계약에 따라 제공한 모든 자료나 문서 및 그 사본을 IronPort 또는 리셀러에 반환하거나 폐기해야 합니다.

8. 미국 정부 제한 권한, 수출 규제 소프트웨어와 이에 수반되는 라이센스 문서는 해당하는 DFAR Section 227.7202 및 FAR Section 12.212에 따라 각각 "상용 컴퓨터 소프트웨어" 및 "상용 컴퓨터 소프트웨어 문서"로 간주됩니다. 미국 정부에 의한 소프트웨어와 이에 수반되는 라이센스 문서의 모든 사용, 수정, 복제, 릴리스, 수행, 제시 또는 공개는 본 계약의 약관에 의해서만 제어되며 본 계약의 약관이 명시적으로 허용하는 수준을 제외하고는 금지되어야 합니다. 회사는 소프트웨어 및 라이센스 문서가 미국 수출 관리 규정에 따라 수출되어야 하며 미국법에 반한 전환은 금지되어 있음을 인지하고 있습니다. 회사는 미국 수출 관리국이나 기타 어떤 연방 기관도 회사의 수출 권한을 중지, 취소 또는 거부하지 않았음을 공언합니다. 회사는 규정이나 특수 라이센스에 의해 미국 정부가 공인하지 않은 한 해당사가 최종 용도가 핵, 화학 또는 생물학적 무기나 미사일 기술과 관련된 소프트웨어를 사용하거나 전달하지 않음을 공언합니다. 회사는 미국 또는 기타 지역에서 일부 또는 모든 수입 및 수출 규정, 기타 해당하는 법을 준수할 궁극적 책임을 보유함을 인정하며 IronPort 또는 이의 리셀러는 원래 판매국 내에서 회사에 처음 판매한 이후로는 추가 책임을 지지 않습니다.

9. 기타. 이 계약은 법 원칙의 충돌과 관계없이 미국 연방법 및 캘리포니아 주법에 의해 제어됩니다. 국제 상품 판매에 대한 계약의 국제연합 협약 적용은 명시적으로 제외됩니다. 본 계약에 포함된 어떤 내용도 당사자 사이에 대리점, 파트너십 또는 기타 유형의 합작 회사를 구성하는 것으로 해석되지 않습니다. 어떤 당사자도 다음으로 인하여 본 계약에 따른 의무(대금 지급 제외)를 이행하지 못했거나 지연했다는 이유로 법적 책임을 지지 않습니다. (i) 현재 또는 미래의 법이나 미국 연방 규정 또는 해당 지역에 적용되는 법률에 포함되는 조항 (ii) 전기 공급 중단, 인터넷 장애, 파업, 정전, 폭동, 반란, 화재 홍수, 태풍, 폭발, 자연 재해, 전쟁, 테러, 정부 작전, 노동 조건, 지진 또는 기타 해당 당사자의 합리적인 제어력 범위를 벗어나는 기타 원인. 본 계약과 라이센스 문서는 소프트웨어 사용자의 모든 권한을 명시하고 있으며 양 당사자 간의 완전한 동의에 해당하며 소프트웨어 및 라이센스 문서에 대한 기타 모든 커뮤니케이션을 대신합니다. 본 계약의 약관은 라이센스 문서 및 구매 발주서, 한쪽 당사자가 제출한 서면 자료의 차이점과 다른 당사자가 이를 공식적으로 거부했는지 여부와 무관하게 전반적으로 적용됩니다. IronPort는 IronPort 개인정보 보호 정책을 재량에 따라 회사에 알리는 것을 통해 언제든지 수정할 수 있다는 점과 정당한 권한을 보유한 IronPort의 담당자에 의해 제기된 서면 수정안으로만 가능하다는 점을 제외하고는 본 계약은 수정될 수 없습니다. 그러한 수정은 http://www.IronPort.com/privacy.html에 게시됩니다. 본 계약서의 어떤 조항도 권한 포기로 간주되지 않습니다. 권한 포기는 서면으로 작성되어 IronPort나 정당한 권한이 있는 IronPort의 담당자의 서명을 받아야 합니다. 본 계약에 무효한 조항이 있는 경우 본 계약의 나머지 조항은 완전한 효력을 그대로 유지합니다. 양 당사자는 본 계약서를 영문으로만 작성하는 것이 자신들의 요청이라는 데 동의함을 확인합니다.

10. IRONPORT 연락처 정보. 회사가 IronPort에 어떤 이유로 연락하고자 한다면 IronPort Systems, Inc., 950 Elm Avenue, San Bruno, California 94066으로 서신을 보내시거나 전화(650.989.6500) 및 팩스(650.989.6543)를 이용하시기 바랍니다.