사용설명서

엠시소프트



(한글판 사용자 설명서)

	$=$ Emsisoft - \Box ×								
لي ب	사용자 컴퓨터가 보	호되고 있습니다!							
Q Q	$\overline{\nabla}$	Q		•					
	보호	검사	로그	설정					
~~~	<ul> <li>✓ 웹서핑 보호</li> <li>✓ 파일 보호</li> <li>✓ 행동 차단기</li> <li>✓ 안티-랜섬웨어</li> </ul>	→ 빠른 검사     Q 말웨어 검사     낚 사용자 정의 검사     ☆ 검역소	5 멀웨어 개체 가 발견되었습니다	보안 설정 및 알림					
ب ب	♪ 고객 님의 라이선스 잔여 기간	은 363 일. 세부 정보 보기 업데이트							
?	참고할 만한 보안 뉴스 Why are so many US public er	tities being hit by ransomware?	© 20 ©	03-2019 Emsisoft Ltd 세품 정보 잘 팔로우 f 💓 💷					

#### 저작권 (저) 2019 ㈜소프트메일

이 사용설명서의 내용과 엠시소프트 프로그램은 저작권법과 컴퓨터 프로그램 보호법에 의해 보호받고 있습니다.

### 최종 사용자 라이센스 약관

중요한 내용이므로 자세히 읽어 보시기 바랍니다. 본 소프트웨어 사용권 계약서('사용권 계 약서')는 ㈜소프트메일(이하 회사) 소프트웨어 제품에 대한 귀하(개인 또는 단체, 업체)와 회 사 간에 체결되는 명시적 계약입니다. 본 회사 제품에는 컴퓨터 소프트웨어뿐만 아니라, 관 련 매체, 인쇄물 및 '온라인' 또는 전자 문서('소프트웨어')가 포함됩니다. 귀하는 '소프트웨 어'를 설치, 복사하거나 사용함으로써 본 소프트웨어 사용권 계약서 내용에 동의하는 것으 로 간주됩니다. 귀하는 본 소프트웨어 사용권 계약서 내용에 동의하지 않을 경우에는 '소프 트웨어'를 사용할 수 없습니다.

이 패키지는 소프트웨어와 관련된 명시적 문서 등을 담고 있습니다. 소프트웨어는 업그레이 드, 통지된 버전, 업데이트, 기타 추가분, 소프트웨어의 사본을 포함하고 있으며 사용자에게 라이센스 합니다. 회사는 사용자에게 소프트웨어와 문서의 사용을 비배타적인 라이센스를 허용합니다:

#### 1. 소프트웨어의 사용

사용자는 하나의 하드 디스크 상의 한 위치에서만 소프트웨어를 설치하여야 하며, 또는 라이센스 계약에서 지정된 컴퓨터의 숫자 만큼의 각 저장 디바이스에 설치하여야 합니 다.

제공된 소프트웨어는 네트워크 사용 목적으로서 다음 목적 중에 하나(둘이 아님) 만을 위한 것으로 하나의 로컬 영역 네트워크 상의 하나의 파일 서버에 대한 사용으로만 설 정할 수 있습니다:

- 하나의 하드 디스크나 컴퓨터의 허용된 수에 따른 기타 다른 저장장소에 영구적으로 설치하거나,
- 1.2. 소프트웨어가 허용된 컴퓨터 수를 초과하지 않는 범위 내에서 다른 컴퓨터에 소프트 웨어를 허용된 수 만큼 설치할 수 있습니다.

사용자는 집이나 이동 가능한 컴퓨터에 각각의 라이센스가 있는 소프트웨어를 설치할 수 있습니다. 이는 동일한 라이센스를 여러 대의 컴퓨터에 설치할 수 없음을 말합니다. 소프트웨어는 동시에 다른 사람의 컴퓨터나 자신의 두 번째 컴퓨터에 사용할 수 없습니 소프트웨어의 백업 복사본은 가능하지만 다른 컴퓨터에서의 사용이나 설치는 불가능합 니다.

회사는 사용자가 소프트웨어와 문서를 사용하여 얻은 결과에 대해서는 어떤 보증도 하 지 않습니다. 소프트웨어의 사용에 대한 결과는 전적으로 사용자의 책임 하에 있으며, 사용자의 소프트웨어 사용 목적에 대한 적합성, 품질 등에 대한 책임은 사용자의 목이 며, 저장된 내용의 손실, 이익의 손실, 어떤 손상, 제3자의 제품에 대한 어떤 문제 등에 대하여 회사는 어떠한 책임을 지지 아니합니다.

보다 상세한 내용은 소프트웨어 상에 표기된 개인정보 및 소프트웨어사용권 이용약관을 참고하여 주십시오.

# 제 1 장 엠시소프트 클라우드 콘솔 관리자

#### '엠시소프트' 클라우드 콘솔

엠시소프트 클라우드 콘솔은 중앙관리를 필요로 하는 기업 및 IT 서비스 업체, MSP 등의 사업자를 위한 용도로 제작된 클라우드 기반의 중앙관리 콘솔입니다.

전통적인 설치형 중앙관리 콘솔에 비하여 빠르고 가볍게 장소와 시간 관계없이 웹기반으로 접속하여 관리가 가능합니다. 클라우드 콘솔은 my.emsisoft.com 사이트로 접속하여 먼저 계정 생성후에 로그인을 하여야 합니다. 클라우드 콘솔은 마치 내 서버나 PC 에 설치된 엠시소프트 소프트웨어를 동일하게 사용하는 것과 같습니다. 중앙관리를 사용하지 않는 경우는 활성화코드를 사용하여 단독버전으로도 사용할 수 있습니다.



# 제 2 장 워크스페이스

워크스페이스는 일반적으로 회사나 조직을 대표하는 것을 말하며, MSP 사업자의 경우 고객사명으로 분류하여 정의하면 됩니다.

라이선스는 워크스페이스 별로 적용이 되며 워크스페이스에 등록된 모든 기기에 적용할 라이선스를 말하여 라이선스는 서버용, PC용 또는 개인용을 등록할 수 있습니다. 평가판 라이선스 역시 포함될 수 있습니다.

#### 2-1. 새 워크스페이스 생성

MyEmsisoft 클라우드 콘솔에 접속하고 대시보드의 워크스페이스 메뉴로 이동하여 '**워크스페이스 생성(Create Workspace)**'을 클릭하고 영문으로 워크스페이스 이름을 생성합니다. 한글 이름은 사용이 불가능합니다.

새 워크스페이스를 생성하면 자동으로 기본 관리자로 등록되며 다른 사람을 워크스페이스 관리자나 사용자로 초대할 수 있습니다. 다른 사용자의 초대는 '설정(Settings)' 메뉴에서 '사용자(Users)'의 '사용자 초대(Invite a user)' 버튼을 클릭하여 초대할 수 있습니다.

#### 2-2. 워크스페이스에 기기 추가

워크스페이스 이름을 클릭하면 우측 창에 '기기 추가(Add Device)' 버튼을 통해 해당 워크스페이스에서 사용할 설치파일을 다운로드하거나 이메일로 다운로드 링크를 배포할 수 있습니다.

му <b>EMSISOFT</b> =		🐣 Christian Mairoll
	Con Add device	iew computers B edits
	Install Emsisoft protection	lew computers 🛛 edits 📃 😁
	With Install protection on this device Download	lew computers 6 edits = ···
	With Alternative downloads	lew computers 7 edits 📃 🚥
	VM. Send download instructions by email	lew computers 3 edits .
	VM-	Vanagers 1 edit 🚍 🚥
	VM	dmin 2 edits
	$\phi$ Device "WIN10-PROD2" hasn't updated for 2 days. Fix now	Chat now

다운로드 또는 이메일로 설치파일 배포

기기상에 설치파일 다운로드(Install protection on this device)
 이 메뉴에서 Download 버튼을 클릭하면 즉각적으로 설치파일을 다운로드할 수 있습니다. 설치를 진행하면 설치한 기기명이 디바이스 목록으로 표시됩니다. 이 설치파일은 통해 설치하면 개별 사용자는 별도로 로그인이나 라이선스 등록을 할 필요가 없습니다.

#### ■ 이메일로 다운로드 전송(Send download instructions by email)

이 옵션은 이메일을 통해 사용자들에게 설치파일을 배포하는 메뉴로 수신자 메일주소를 등록하여 Send email 버튼을 눌러 설치파일을 발송할 수 있습니다. 이메일에는 개별 다운로드 링크가 포함되어 있습니다. 설치파일은 설치 토큰을 통해 보안성을 강화하였습니다. 주의 : 다운로드시 파일명은 변경하지 마십시오. 파일명에서 식별자/보안 토큰이 포함되어 있어 중앙관리 서버에 접속되는 인증으로 사용됩니다. **설치파일은 내부 사용자** 외에 익명의 다른 사람들과 공유하거나 배포하지 않으셔야 합니다.

#### 설치 토큰 및 기본 보호 정책

기본적으로 새로 설치되는 기기는 해당 워크스페이스의 '새 컴퓨터(New computers)' 보호 정책으로 추가됩니다.

만약 다른 정책 그룹으로 추가하거나 변경하려면 정책 설정에서 설정을 변경하거나 그에 맞는 다운로드를 새롭게 추가하면 됩니다. 설치파일은 특정 워크스페이스와 정책으로 분류하여 설치되도록 사전에 설정된 값으로 만들어진 다운로드 파일을 사용하면 해당 워크스페이스로 자동으로 지정됩니다.

#### 커맨드라인을 통한 수동 연결

대량의 PC가 있는 기업이라면 자동으로 엠시소프트가 워크스페이스에 연결되도록 할 필요가 있습니다. 다음 커맨드라인 명령을 사용하여 연결 정보를 설정하면 됩니다 :

%ProgramFiles%\Emsisoft Anti-Malware\a2start.exe /applytoken=<installtoken>

<installtoken>: 사용자 설치 토큰은 '보호 정책(Protection Policies)' > '새 컴 퓨터(New computers)' > '정책 설정(POLICY SETTINGS)'의 '설치 토큰 (Installation token)' 메뉴에서 복잡한 코드로 표시되어 있는 것입니다.

#### 2-3. 워크스페이스에 라이선스 적용

새로운 워크스페이스를 생성하면, 첫 번째 기기에 설치 시 자동으로 평가판 라이선스로 적용이 됩니다. 평가판 기간 동안 여러 기기를 추가할 수 있습니다.

유료 버전으로 변환하려면 워크스페이스 설정 메뉴에서 '라이선스 키 적용(Apply license key)' 메뉴로 이동하여 구입하신 라이선스를 등록 적용하면 됩니다.

#### 2-4. 워크스페이스 사용자 초대

워크스페이스의 기본 관리자로서 관리자는 관리권한을 차등적으로 적용하여 부관리자를 추가할 수 있으며 추가할 관리자를 초대하여 권한을 부여할 수 있습니다. 기본 관리자를 대신하여 부관리자는 자신의 회사 또는 그룹을 관리할 수 있습니다. 본 기능은 MSP 사업자의 경우 고객사 관리자를 부가적으로 등록하여 고객 스스로 워크스페이스를 관리하도록 권한을 위임할 수 있습니다. 워크스페이스의 설정 메뉴에서 '사용자(Users)' 섹션에서 '사용자 초대(Invite a user)' 버튼을 통해 이메일로 초대할 수 있습니다.

초대하는 부관리자의 경우 엠시소프트 계정을 생성하여 로그인하여야 합니다.

시	- 8-	자	역	할
---	------	---	---	---

	Billing	Protection	Workspace	Primary
	Contact	Manager	Admin	Workspace
				Owner
Devices		Х	X	Х
Policies		Х	X	Х
Licensing	Х		X	Х
Edit users			X	Х
Change				Х
owner				

#### 기본 워크스페이스 관리자

워크스페이스 전체를 관리하는 시스템관리자로서 모든 권한을 갖고 있습니다. 일반적으로 라이선스를 구매한 구매자를 말합니다.

#### 워크스페이스 관리자 (Workspace admin)

자신의 워크스페이스를 관리할 수 있는 일반 관리자를 말하여 모든 디바이스, 정책, 알림, 로그, 보고서 등에 접근할 수 있습니다. 워크스페이스 관리자는 기본 관리자를 제외한 모든 사용자를 관리할 수 있습니다. 일반적으로 고객사 관리자를 의미하며 여러 명의 관리자를 부여할 수 있습니다.

#### 보호 관리자 (Protection Manager)

모든 기기, 정책, 알림, 로그, 보고서를 보거나 수정할 수 있지만 워크스페이스 자체에 대한 설정이나 사용자관리, 라이선스 관리는 불가능합니다. 일반적으로 이 관리자는 부서관리자나 고객사(MSP)의 고객사를 위한 하위 관리자로 사용됩니다.

#### 빌링 연락처 (Billing Contact)

빌링 연락처는 고객사나 파트너에게는 보이지 않는 메뉴이며 설명은 생략하겠습니다.

#### 2-5 워크스페이스 개요 : 기기에 대한 보호 상태

워크스페이스는 대시보드에서 '워크스페이스(Workspaces)'와 새로 만든 워크스페이스 들이 보여집니다. 워크스페이스는 일종의 그룹으로 이해하시면 되며 하나 하나의 고객사를 분류한 작업공간으로 볼 수 있습니다. 워크스페이스 명을 클릭하면 해당 워크스페이스의 대시보드가 나타나고 여기서 전체 워크스페이스 목록과 설치 수량 등의 정보를 보실 수 있습니다. 보호 상태와 마지막 업데이트 등의 보안 정보 확인이 가능합니다.

그리고 각 워크스페이스에는 '보호 정책(Protection Policies)', '권한 정책(Permission Policies)', '설정(Settings)' 3 개의 하위 메뉴가 있습니다. 워크스페이스 이름을 클릭하면 관리되는 기기들 목록과 각 기기에 설정된 정책과 보안 상태, 최근 접속 날짜, 설정된 정책 등의 정보를 확인할 수 있습니다.

마지막 열에 있는 3 줄 메뉴에서는 멀웨어 검사, 기기 설정 수정 등의 작업 메뉴가 제공됩니다.

팁: 좌측 메뉴에 있는 워크스페이스 이름 옆의 핀을 눌러 메뉴 확장 및 접기를 선택하고 유지할 수 있습니다.

#### 2-6 그룹에 대한 전역 보호 정책 (Protection Policies)

내부 조직 구조나 고객사 구분을 통한 기기 그룹 설정을 하여 사용할 것을 추천 드립니다. MSP 의 경우 고객사로 그룹을 만들어 각각의 고객사별 정책과 관리자를 부여하여 고객이 직접 자사 워크스페이스를 관리할 수 있도록 하면 좋습니다. 고객사별 특성에 따라 일부 기능을 끄거나 일부 경로를 예외 처리할 수 있도록 그룹을 구분하여 각각의 정책을 부여하여 사용합니다.

개별적으로 각각의 기기에 대한 설정을 개별적으로 변경하지 않고 그룹에 속한 전체 기기에 대해 일괄적으로 정책을 부여할 수 있습니다. 메뉴 좌측에 그룹은 계층적으로 구조화되어 있으며 우측 화면에서 상세한 정보가 표시됩니다.

Y OWN	Contoso Ltd. / Protection F	Policies			
Devices	Policy groups	Devices		POLICY SETTINGS	
Dicenses	- Workspace	0	=		
OUD CONSOLE	New computers	7	≡	Traffic relay	None •
Workspaces	Managers • Public	1 0	=	Installation token	859cfdd2-c55b-470c-b12b-432e3718423c
CONTOSO LTD. 早~	Admin	1	=	Template	None Select template
<ul> <li>Protection Policies</li> <li>Permission Policies</li> </ul>				BEHAVIOR BLOCKER	
Settings	7 devices in 'New computers'				
교 asus-rog 후 ✓ ⑦ Protection Settings	WORKGROUP/asus-rog WORKGROUP/vm2-win7x64 WORKGROUP/WIN10-PROD		=	Suspicious programs ①	Auto resolve, with lookup notifications
Quarantine 2	WORKGROUP/WIN10-PROD2 WORKGROUP/WIN10-SNAP		=	FILE GUARD	ON ON
E Logs	WORKGROUP/WIN10-SNAP2		=	Scan Level ③	Default
	WORKGROUP/WIN10-SNAP3		≡	Malware detections (i)	Quarantine with notification •
Customer Support	Add device			PUP detections ()	Quarantine with notification •
Help & Docs				<ul> <li>Only scan files with</li> </ul>	Chat now

모든 소프트웨어 설정이 가능한 보호 정책

엔드포인트에 표시되는 메뉴 그대로 모든 설정이 이곳 콘솔에서 동일하게 관리할 수 있습니다. 또한 일부 속성에 대한 커스터마이징이 가능합니다. '커스터머 케어(CUSTOMER CARE)' 메뉴에서는 뉴스 팝업 표시를 켜거나 끌 수 있으며 제품 라이선스 구매 페이지에 대한 링크도 변경할 수 있습니다.

#### 정책 상속

가장 높은 계층은 제일 처음 표시되는 Workspace 그룹입니다. 워크스페이스 밑에 있는 하위 그룹은 상위 그룹의 정책을 자동으로 상속받게 됩니다. 그룹은 다단계로 하위 그룹을 만들어 포함할 수 있습니다. 그룹은 드래그&드롭으로 레벨을 변경할 수 있습니다.

#### 기기를 그룹에 할당

그룹에 포함된 기기를 마우스로 드래그 하여 하위 폴더로 이동할 수 있으며 하위 폴더에 할당된 정책을 사용할 수 있습니다.

새로 추가된 기기는 자동으로 '새 기기(New devices)' 그룹으로 위치되며 사용자 선택에 의해 다른 그룹으로 이동할 수 있습니다.

#### 그룹 설정 수정

좌측 메뉴에서 그룹을 선택하면 우측에 전체 보호 설정을 볼 수 있습니다. 모든 설정은 다음 우선 순위 수준과 다른 밝은 회색 배경의 굵은 파란색 글자로 표시됩니다. 리셋(Reset)'아이콘은 특정 설정의 상속 전 상태로 복원합니다.

설정은 실시간으로 저장되고 몇 분 안에 엔드포인트 기기로 상속 적용됩니다.

#### 정책 템플릿 (Policy templates)

복 수의 워크스페이스 정책을 관리하기 위한 정책 적용은 "MSP 를 위한 베스트 정책" 편을 참고하여 주십시오

#### 2-7 그룹에 대한 로컬 사용자 권한 (Permission Policies)

보호 정책과 유사하게 사용자 계정에 대한 기본 권한을 설정할 수 있습니다. 좌측에서 사용자 그룹을 선택하고 오른쪽의 '사용자(Users)' 탭으로 전환하여 할당된 사용자를 확인합니다.

사용자는 기기 상에서 로컬 사용자 계정이거나 네트워크의 Active Directory 도메인 사용자일 수 있습니다. 새 사용자를 추가하려면 '추가(Add)' 버튼을 클릭합니다.

일반적으로 기본 그룹을 권한을 사용하면 편리합니다. 엔드포인트 기기 상의 보호 소프트웨어는 자동으로 로컬 계정 권한으로 적용됩니다.

#### 기본 권한:

- '전체 접속 (Full access)'은 기본 관리자 권한이며 모든 소프트웨어 설정을 보거나 수정할 수 있습니다.
- '기본 접속 (Basic access)' 권한을 갖는 사용자는 설정을 볼 수는 있지만 변경을 불가능합니다. 이들 계정은 멀웨어 검사를 수행하거나 알림에 대한 처리, 격리 보관된 내용 확인을 할 수 있습니다. 일반 사용자들은 이 기본 접속 권한을 부여하는 것을 추천 드립니다. 언제든지 사용자 권한을 관리자는 다른 권한으로 변경할 수 있습니다.
- '읽기전용 접속 (Read-only access)' 권한은 설정을 볼 수는 있지만 변경은 할 수 없습니다. 모든 알림이나 이벤트는 소프트웨어가 자동으로 처리합니다. 보통 회사에서 보안정책을 강제화 할 때 사용하거나 컴퓨터를 잘 모르는 사용자를 대상으로 합니다.
- '접속 불가 (No access)' 권한은 프로그램을 볼 수가 없습니다. 모든 알림이나 이벤트는 소프트웨어가 자동으로 처리합니다.

#### 2-8 감염 알림 수신

워크스페이스 > '설정(Settings)' > '알림(Notification)' 메뉴에서 알림에 관한 설정을 추가하거나 변경할 수 있습니다. 알림은 몇 가지 종류별 이벤트에 관리자에게 알림을 제공해 줍니다. 예를 들어 실시간 감시 엔진에서 바이러스 감염에 대한 알림을 설정할 수 있습니다.

- 이메일(Email): 이메일을 통해 특정 수신자에게 알림 메일을 발송합니다.
- 웹후크(Webhook): 자동화된 이벤트 처리를 위해 실시간으로 알림을 제공하기 위해 web-API를 사용하여 알림을 제공합니다. 특정 URL을 지정하여 알림을 전송합니다.

#### 2-9 워크스페이스 삭제

고객의 해지나 잘못된 워크스페이스를 삭제하려면 해당 워크스페이스로 이동하여 워크스페이스의 설정(Settings)을 클릭하고 화면 맨 아랫줄의 '워크스페이스 삭제(Delete workspace)' 버튼을 눌러 삭제할 수 있습니다.

# 제 3 장 기기 관리

#### 3-1 기기 개요 : 보호 상태 및 빠른 접속

클라우드 콘솔의 워크스페이스 이름을 클릭하면 기기 목록이 표시됩니다. 기기 목록에서 '기기 명(device name)'을 더블 클릭하여 사용자 컴퓨터 상에 설치된 엠시소프트에 접근할 수 있습니다.



로컬 기기에 설치되어있는 엠시소프트 상태 보기

첫 번째 **'보호(Protection)'** 박스에 보여지는 것은 실시간 보호 상태입니다. 배경 색상에 따라 상태를 파악할 수 있습니다 :

- 초록(Green): 모든 실시간 감시 보호가 정상이고 최신 업데이트 상태입니다.
- 오렌지(Orange): 한 개 이상의 보호가 중지되어 있거나 최신 업데이트 상태가 아닙니다. 문제를 해결할 필요가 있습니다.
- 빨강(Red): 모든 실시간 감시 보호가 꺼져 있는 경우입니다. 문제를 해결할 필요가 있습니다.
- 회색(Grey): 이 기기는 현재 오프라인 상태입니다. 가능한한 기기가 온라인으로 동기화하도록 합니다. 그러나 이 경우 온라인 상에서 검사나 설정을 수행할 수 없습니다.

'기기 건강도(Device Health)' 메뉴에서 이 기기에 대한 보안 정보를 빠르게 확인할 수 있습니다. 여기서 간단한 메모를 작성할 수 있습니다.

'기기 세부정보(Device Details)'에서는 하드웨어와 소프트웨어 정보를 볼 수 있습니다.

#### 3-2 기기에 대한 보호 설정

보호 정책과 그룹에서 정책을 설정하여 관리할 것을 추천하지만 사용자는 개별 기기에서 설정을 변경할 수 있습니다. 이런 개별 PC 에서 설정은 상속된 정책을 반영하지 않고 개인 설정을 사용하게 됩니다.

중앙에서 수정이 반영되면 기기에 몇 분 내에 정책이 상속되어 동기화되어 집니다. 기기와 동기화가 완전히 되면 설정 메뉴에서 회색 배경에 굵은 파란색으로 기기명이 표시됩니다. 우측에 있는 '리셋(Reset)' 아이콘은 상속된 설정 값을 복원합니다.

#### 3-3 멀웨어 검사

엠시소프트를 설치한 후에 수동 검사를 수행할 것을 추천 드립니다. 검사는 언제든지 실행할 수 있습니다. 실시간 감시 엔진은 시스템을 랜섬웨어나 악성코드로부터 보호하기 때문에 항상 켜진 상태로 운영하시기 바랍니다.

검사 형태는 다음과 같이 3가지로 제공됩니다 :

- 빠른 검사(Quick Scan) 현재 활동 중인 프로그램을 검사하고 멀웨어 흔적을 체크합니다. 빠른 검사는 시스템이 안전하다고 생각할 때 빠르게 검사하는 목적으로 수행합니다.
- **멀웨어 검사(Malware Scan)** 일반적으로 멀웨어에 감염된 여부를 검사하기 위해 전체를 검사합니다. 멀웨어 검사는 대부분 사용자가 수행하여야 하는 검사입니다.
- 사용자 정의 검사(Custom Scan) 모든 검사는 수동으로 설정하여야 합니다. 외부 디바이스나 이동식 드라이브, 특정 경로에 대해 필요에 따라 검사를 수행합니다. 기본 설정은 모든 드라이브를 포함한 전체 시스템 검사입니다.

#### 3-4 격리 보관된 개체 관리

수동 검사 및 실시간 보호에서 발견한 위험은 바로 삭제하기 보다는 검역소로 격리하는 것을 추천합니다. 위험 진단 결과는 오탐 가능성이 있기 때문에 추후 복구가 가능하도록 격리보관하시면 도움이 됩니다.

엠시소프트는 온라인 업데이트가 진행된 후 격리 보관된 항목에 대해 자동으로 재검사하여 원본이 잘못 격리된 파일이 라면 자동으로 원래 위치로 복원해 줍니다. 사용자는 수동으로 격리 보관된 파일을 우측 하단의 '재검사 버튼(Re-scan all)'을 눌러 언제든지 다시 검사할 수 있습니다.

오진이 의심된다면 해당 항목 앞쪽의 체크박스를 선택하고 아래쪽 '오탐 발견(False detection)' 버튼을 사용하여 엠시소프트 연구소로 제출할 수 있습니다.

항목을 선택하고 '복원(Restore)' 버튼을 사용하면 원래 위치로 격리된 파일을 복원합니다. '삭제(Delete)' 버튼은 영구적으로 파일을 제거하기 때문에 복원이 불가능합니다.

#### 3-5 디바이스 로그

엠시소프트 보호 소프트웨어 로그는 수 많은 이벤트를 저장합니다. 날짜/시간, 업데이트, 멀웨어 검사 결과, 실시간 감시 내역, 보안 알람 등의 정보가 저장됩니다. 이러한 로그는 소프트웨어 사용에 대한 이슈를 해결하기 위해 사용될 수 있습니다.

## 제 4 장 고급 설정 가이드

#### 4-1 릴레이 기능을 사용한 네트워크 트래픽 절감 (프록시, 케시) 가이드

엠시소프트 클라우드 콘솔은 불필요한 인터넷 트래픽을 절감하기 위한 릴레이 설정 기능을 제공합니다.

배경:

엠시소프트 보호 기능은 자동으로 매시간 마다 업데이트를 하여 모든 멀웨어 식별 패턴을 최신 상태로 유지할 수 있도록 업데이트합니다. 온라인 업데이트 시에 소프트웨어는 특정 기기에 누락된 최신 데이터만을 다운로드합니다. 증분 및 차이에 따른 결합 업데이트 기술을 사용하여 하루에 약 20~3-MB 정도의 인터넷 트래픽을 사용합니다.

이는 매우 작아 보이지만 한달을 기준으로 한다면 엄청난 데이터 트래픽을 사용하게 됩니다. 만약 제한된 데이터 이용 플랜을 사용한다면 많은 데이터 사용량은 비용을 더 많이 발생시킵니다. IDC 에서 사용시 또는 모바일 요금제를 사용하는 경우 많은 기기를 보유했다면 엄청난 트래픽 비용을 부담하여야 합니다.

전체 업데이트 트래픽을 절감하기 위해 1 대 이상의 엠시소프트 기기를 정하여 릴레이 혹은 캐시 프록시 서버로 사용하여 전체 기기에서 직접적으로 많은 데이터를 다운로드하지 않고 지정된 서버를 통해 업데이트하고 모든 데이터를 내부 네트워크 기기로 확산시킬 수 있습니다.

일단 다운로드한 모든 데이터는 불필요한 반복 다운로드를 피하기 위해 캐싱됩니다. 회사 내에서 많은 기기를 보유하고 있다면 릴레이 기능을 사용하여 엄청난 트래픽을 절감할 수 있습니다. 예를 들어 10 기기를 갖고 있는 회사라면 전체 트래픽은 전체 데이터 트래픽 대비 10분의 1로 절감할 수 있습니다.

릴레이 기능 사용의 장점

■ 케싱(Caching): 한 개의 릴레이를 사용하여 각각의 파일은 1 대로만 전송되고 로컬 케시에서 다른 기기들로 공급 배포됩니다.

- 속도(Speed): 온라인 업데이트는 가속화되고, 느린 인터넷 연결 시 더욱 효과적입니다.
- 대역폭(Bandwidth): 대규모 네트워크에서 아침 출근시간 대의 인터넷 사용량은 병목현상이 생기는데 이 때 릴레이 서버 사용은 트래픽 절감에 매우 효과적입니다.
- 방화벽 호환성(Firewall compatible): 릴레이로 사용하는 기기만 인터넷에 연결하도록 설정하고 다른 기기들은 방화벽 안쪽에 인터넷에 바로 연결될 필요가 없습니다.
- 프록시 보호(Proxy protection): 엠시소프트 릴레이는 데이터만을 전송하는 방화벽 정책만 수행하면 되고 다른 장비에 대한 방화벽 변경은 하지 않아도 됩니다.

#### 트래픽 릴레이 설정 방법

릴레이 기능은 엠시소프트 클라우드 콘솔 워크스페이스에 있는 개별 기기에서 설정할 수 있습니다.

 클라우드 콘솔에 로그인하고 릴레이로 설정할 기기를 워크스페이스에서 선택합니다. 해당 기기의 '보호 설정(Protection Settings)' 메뉴에서 설정 아래 부분의 '릴레이(RELAY)' 섹션으로 이동하여 '기기는 트래픽 릴레이로 사용(Device can be used as traffic relay)'을 체크합니다.

RELAY	
Device can be used as traffic relay	5

대상 기기로 릴레이 사용 선택

 다시 상위의 워크스페이스 이름을 클릭하여 '보호 설정(Protection Policies)'
 메뉴에서 우측의 '정책 설정(POLICY SETTING)' 화면에서 '트래픽 릴레이(Traffic relay)' 항목에서 기기를 선택합니다. 드롭박스 메뉴에 앞서서 체크박스로 선택한 기기를 선택합니다.

POLICY SETTINGS		
Fraffic relay		
laptop17		•
None		
laptop17		
lemplate		
lone		
Select template		
)		

그룹 정책에서 릴레이 기기 선택

이렇게 설정하면 릴레이 기기 설정이 완료됩니다. 이 정책 그룹에 있는 모든 기기는 지금부터 릴레이 기기를 통해 업데이트를 진행합니다. 릴레이가 어떤 이유로 사용이 불가한 상태가 되면 (기기가 꺼져 있는 경우 등), 다른 기기들은 인터넷으로 직접 업데이트 서버에 연결 시도하며 또는 로컬 프록시 설정을 통해 업데이트 시도합니다.

릴레이 사용하고자 하는 경우 설정이 정확하게 되었는지 다시한번 확인하시기 바랍니다.



엠시소프트 -> 설정(Settings) -> 원격 관리(Remote management)



엠시소프트 클라우드 콘솔 -> 워크스페이스 -> 기기

#### 4-2 윈도우 서버/Active Directory 상에서 그룹 정책을 통해 원격설치

#### GPO를 통한 대량 채택

본 설명은 Active Directory 그룹 정책을 사용하여 자동으로 엠시소프트를 클라이언트 컴퓨터에 설치하는 방법에 대한 것입니다. 윈도우 네트워크에 대해 익숙하다는 전제하에 Active Directory 에서의 그룹과 사용자 설정, 그리고 서버 설정이 된 상태에서 엠시소프트 설치를 설명합니다.

#### GPO를 통한 엠시소프트 설치의 장점:

- 온라인 클릭 설치(One click installation), 로그인이나 키보드 입력이 불필요합니다. /Quiet 매개변수를 사용하면 설치는 백그라운드로 진행되며 사용자 간섭이 필요 없습니다.
- 설치된 기기는 클라우드 콘솔 상에 몇 초 뒤에 자동으로 표시가 됩니다.
- 관리자는 새로 추가된 기기에 대해 사용할 정책 그룹을 설정할 수 있습니다.
- 스크립트를 작성할 필요없이 기본 절차로 진행됩니다.

1. 배포 파일의 생성

엠시소프트의 윈도우 인스톨 파일인 .MSI 파일로 된 파일을 배포하기 위해 서버에 접속하여 공유 네트워크 폴더를 생성합니다. 그리고 사용자 권한을 클라이언트가 접속이 가능하도록 설정합니다.

#### 2. 엠시소프트 워크스페이스에서 설치파일 다운로드

MyEmsisoft 에 로그인하고 자신의 워크스페이스로 클릭합니다.

#### 옵션 (A)

기본 값이 '새 기기(New devices)'정책 그룹에서 설치파일을 추가하기 위해 '기기 추가(Add device)' 버튼을 클릭하고 소프트웨어를 다운로드합니다. 기본 다운로드 파일의 형식은 .EXE 입니다. AD 를 사용하는 경우 설치파일을 '대안 다운로드(Alternative downloads)' 메뉴를 클릭하여 MSI 설치파일로 다운로드하여야 합니다.

#### 옵션 (B)

워크스페이스에서 '보호 정책(Protection policies)'로 가서 해당 정책 그룹으로 적용될 설치파일을 만들기 위해 목표 그룹을 지정할 수 있습니다. 새로운 하위 그룹을 선택하거나 새로 그룹을 추가하여 '정책 설정(Policy Settings)' 섹션에서 '생성(Create)' 버튼을 눌러 개별로 '설치 토큰(installation token)'을 생성합니다. 토큰의 유효기간을 선택할 수 있으며 기본 30 일 동안 해당 토큰이 유효합니다. 토큰은 '만료없이(Never)' 영구적으로 사용하거나 24 시간, 7 일, 30 일 중 유효기간을 선택할 수 있습니다. 유효기간을 선택하고 MSI 설치파일을 다운로드할 수 있습니다.

다운로드한 파일은 좀 전에 설명한 윈도우 공유 폴더에 저장합니다.

#### 3. 배포파일을 초기화 하기 위한 그룹 정책 개체(Group Policy Object, GPO) 생성

윈도우에서 '액티브 디렉토리 사용자 및 컴퓨터(Active Directory Users and Computers)' 패널을 열고 도메인에 있는 '그룹 정책(Group Policies)' 메뉴로 이동합니다. 새로운 정책에 대한 적절한 이름을 넣고 생성(예. Emsisoft Installation Policy) 하고 'Source Starter GPO'as '(none)'와 같이 저장합니다.

새로 생성한 정책을 클릭하고 우측에서 '설정(Settings)' 탭을 선택합니다. 우 클릭을 하고 '수정(Edit)…' 버튼을 클릭합니다. '사용자 구성(User Configuration)' > '정책(Policies)' > '소프트웨어 설정(Software Settings)' 메뉴로 이동하여, '소프트웨어 설치(Software installation)'를 우 클릭하고 'New > Package…'를 선택합니다. 엠시소프트 설치파일이 저장된 폴더를 선택합니다. 그러면 '할당(Assigned)' 가 표시되고 'OK'를 클릭합니다.

#### 4. 로그온 시에 설치

설정한 컴퓨터가 시작되면 자동으로 엠시소프트 소프트웨어가 설치됩니다.

엠시소프트는 자동으로 워크스페이스에 연결되고 설치시에 보았던 보호 정책 그룹에 할당되어 등록된 것을 볼 수 있습니다. 이때 라이선스도 자동으로 승계됩니다.

라이선스 키를 따로 등록할 필요가 없으며 설치 중에 사용자 계정이 자동 등록됩니다. 사용자 간섭없이 백그라운드 설치를 하려면 MSI 설치파일에서 /Quiet 매개변수를 사용하면 됩니다.

#### 4-3 MSP 를 위한 베스트 정책

엠시소프트 클라우드 콘솔은 대규모 유저를 지원하기 위한 목적으로 효율적으로 전체 시스템을 관리하도록 설계되었습니다. 본 서비스를 통해 MSP 서비스사를 위한 효과적인 설정 방법에 대해 알아보겠습니다.

#### MSP 업체를 위한 기능:

- 새 고객사를 위한 워크스페이스 생성
- 복수의 워크스페이스에서 사용할 정책 템플릿
- 커스터머 케어 설정으로 소프트웨어 커스터마이징

му <b>EMSI</b> SOFT =						🧶 🛛 John Doe 🗸 🗸
MY OWN	♠ Workspaces					
ධ Devices						
₽ Licenses	Workspaces			Q Se	arch	Create workspace
≔ Policy Templates	Workspace ↑	Devices	Unused seats	License renewal due	Last alert	Findings last 30 days
CLOUD CONSOLE	Contoso Ltd.	9	0	03/07/2021	04/11/2019	-
I Workspaces	Dana's workspace	8	1	Next billing 05/31/2020	02/27/2019	-
围 CONTOSO LTD. 平 ~	Emsi NZ	3	2	12/01/2019	08/14/2018	
Protection Policies	Homegroup	2	2	03/19/2020	-	-
Permission Policies	Expand all - Collapse all					
Settings						
모 ASUS-ROG 후 ~	Protection alerts			Friday, August Scanner: 4	9, 2019	
♡ Protection Settings	6			CONTOSO LTD.	2	
Q Scan	5			VM2-WIN7X	64: 2	
<ul> <li>Quarantine</li> <li>2</li> </ul>	4					
≣ Logs	3					
	2-					
	1					
💬 Customer Support	0 July 23 July 25	July 27 July 29	July 31 August 2 A	ugust 4 August 6 August 8 Augus	st 10 August 12 August 1	14 August 16 August 18 August 20
? Help & Docs			Scanner Su	rf Protection File Guard Behavior Blocke	r	Leave a message 💬

#### 새 고객사를 위한 워크스페이스 생성

고객사 관리를 위해 고객사마다 개별 워크스페이스를 등록하여 고객사에 맞는 정책으로 독립적으로 관리할 수 있습니다. 워크스페이스 별로 정책, 라이선스, 관리자를 부여할 수 있습니다.

사전 준비:

- 라이선스: 워크스페이스에서 사용할 라이선스를 워크스페이스 설정 메뉴의 라이선스에서 등록할 수 있습니다. 라이선스 보유 수량 내에서 디바이스를 추가할 수 있으며 기본 30일 평가판으로 사용이 가능합니다.
- **정책(Policies)**: 기본 설정 또는 미리 만든 템플릿 정책을 통해 정책을 고객사의 워크스페이스에 부여합니다.

고객사를 위한 새 워크스페이스 준비:

- 클라우드 콘솔 워크스페이스를 클릭하여 '워크스페이스 생성(Create workspace)'을 클릭.
- 워크스페이스 이름(영문)을 등록하고 간단한 설명과 고객사 이메일 주소를 입력합니다. 이메일 주소는 해당 워크스페이스 관리자로 초대하여 고객사가 직접 워크스페이스를 관리할 수 있도록 권한을 위양할 수 있습니다.
- 해당 고객사에 맞는 설치파일 제공

	Install Emsisoft prot	ection
<b>.</b>	Install protection on this device	Download Alternative downloads
$\sim$	Send download instructions by email	Send email

사용자 워크스페이스에 새 기기 추가

라이선스 활성화 정보:

실제 최종사용자는 라이선스 키를 필요하지 않습니다. 사용자 계정으로 설치하거나

배포한 설치파일로 설치하면 라이선스가 상속되어 최종사용자는 라이선스 활성화가 필요 없습니다. 라이선스는 중앙에서 관리하게 됩니다.

#### 복수의 워크스페이스에서 사용할 정책 템플릿

많은 고객사를 관리하는 서비스 공급사의 경우 많은 사용자를 보유하게 됩니다. 각각의 고객사 마다 개별관리를 피하고 미리 설정한 정책 템플릿을 사용하면 각각의 워크스페이스에 미리 만들어 놓은 템플릿을 사용하여 정책을 관리하면 매우 편리합니다.

사용자의 템플릿을 관리하려면, 콘솔의 좌측 최상단의 'MY OWM'의 '정책 템플릿(Policy Templates)'을 클릭하여 '새 템플릿(New Template)' 버튼을 클릭하고 이름을 등록합니다.

My Policy Templates			
Name	Applied		SHARING
My MSP Corp - Base Policy My MSP Corp - Tech departme	1 0	≡ ≡	This template can be applied by Only me -
My MSP Corp - All others	0	≡	
New template			BEHAVIOR BLOCKER ON
0 policies applied in 'My MSP Corp - All others'			Suspicious programs (i) Auto resolve polification
No applied policies			Auto resolve, notification

정책 템플릿

정책 템플릿은 사용자 프로필에 저장됩니다. 그러나 템플릿을 개인적으로 또는 다른 관리자와 공유하여 사용할 수 있도록 설정할 수 있습니다.

워크스페이스의 정책처럼, 템플릿도 계층구조로 관리할 수 있으며 이름은 한글 사용이 가능합니다. 자신의 루트 템플릿을 생성하여 변경하지 않고 사용할 기본 설정을 만들기를 추천합니다. 그리고 필요에 따라 하위 템플릿을 추가하여 그룹별, 고객별로 템플릿을 만들어 사용하면 효과적입니다. 예를 들어 어떤 템플릿은 서버용을 위한 것, 어떤 템플릿은 게임모드 설정을 위한 것 등으로 분류하여 관리하면 도움이 됩니다. 템플릿 적용은 고객의 워크스페이스 설정에서 '보호 정책(Protection Policies)' > '정책 설정(POLICY SETTINGS)'의 '템플릿(Template)'의 콤보박스 메뉴에서 선택할 수 있습니다. 보통은 새로 워크스페이스를 생성하였을 때 선택 적용합니다.

#### 4-4 커스터머 케어 설정으로 소프트웨어 커스터마이징

MSP 및 서비스업체를 위한 맞춤 인터페이스를 제공하기 위해 일부 정보를 커스터마이징 할 수 있습니다. 본 설정은 각 워크스페이스의 '보호 정책(Protection Policies)' 메뉴의 '커스터머 케어(CUSTOMER CARE)'에서 설정할 수 있습니다.

- 라이선스 만료 안내 사용 안함(Disable license expiration notifications):
   라이선스가 만료되기 30일, 14일, 7일 전에 모든 팝업 알림을 중단합니다.
   주의 : 이 기능을 해제하면 사용자가 라이선스 만료일에 대한 연장을 놓칠 수 있는 위험이 있습니다. 그러나 라이선스 연장이 제때 진행되지 않으면 만료 전 3일 전에 알림이 표시됩니다.
- 커스터머 소개 리워드 프로그램 숨김(Hide customer referral rewards program): 새로운 사용자 확보를 위한 무료 라이선스 제공 보상 프로그램 제안을 표시하지 않습니다. 기업 고객에게는 필요한 기능입니다.
- 라이선스 키 숨김(Hide license key): 라이선스 코드를 보이지 않도록 설정하여 외부로 라이선스 유출이 되지 않도록 합니다.
- 긴급구호 키트 제작 메뉴 숨김(Hide Emergency Kit Maker):
   검사 메뉴에서 긴급 구호 키트 제작 메뉴를 보이지 않게 합니다. 사용자는
   USB 용 긴급구호 키트를 사용할 수 없습니다. 일반적으로 기업고객은 이 기능을
   사용합니다.
- 제품 구입 및 재 연장 버튼 사용 안함(Disable purchase and renewal buttons): 직접 엠시소프트 본사 홈페이지로 제품 구매를 유도하지 않습니다.
- 제품 구입 및 연장 버튼에 대한 대안 메시지(Alternative message for purchase and renewal buttons): 관리자 연락처 정보를 변경할 수 있습니다. "제품 구매는 1661-9331 로 문의하여 주세요".

■ 제품 구입 및 연장 버튼에 대한 대안 URL(Alternative URL for purchase and renewal buttons):

사용자에게 보여지는 제품 구입을 위한 홈페이지 주소를 변경할 수 있습니다. "https://www.company.com/order/".

- 대시 보드 화면에서 뉴스 숨김(Hide news area on overview screen): 대시 보드 화면에 새로운 뉴스가 보이지 않도록 설정합니다. 이 구역은 광고가 표시되지 않으며 보안 교육이나 블로그 뉴스 등의 정보가 보여집니다. 뉴스 팝업은 그룹의 '알림(NOTIFICATIONS)' 메뉴에서 설정할 수 있습니다.
- 대안 문구 작성(Alternative static text_: 서비스 제공업체의 연락처 정보 등을 커스터마이징 "소프트메일에서 관리 1661-9331".

#### ■ 대안 URL:

사용자 들이 제품 구매와 연장 구매를 위한 홈페이지 주소를 설정할 수 있습니다. "https://www.company.com/order/".

CUSTOMER CARE	 ©	Protection	Scan & Clean	l	
Disable license expiration notifications Hide referral rewards program section Hide license key		<ul> <li>SURF PROTECTION</li> <li>FILE GUARD</li> <li>BEHAVIOR BLOCKER</li> <li>ANTI-RANSOMWARE</li> </ul>	<ul> <li>➡ QUICK SCAN</li> <li>Q MALWARE SCAN</li> <li>➡ CUSTOM SCAN</li> <li>O QUARANTINE</li> </ul>	13 MAU DETEC	
<ul> <li>Hide Emergency Kit Maker</li> <li>Disable purchase and renewal buttons</li> </ul>	Q Q	Your license ends in 111 days. 4 Last update: 52 min ago. Update:	View details ate now		
Alternative message or URL for purchase		⑦ This device is managed by My MSP Corp. +1 234 567 89			
Alternative message or URL for news section		E	dit		

고객사를 위한 뉴스 표시 설정 변경

# 엠시소프트

클라우드콘솔

# **EMSISOFT**

### (주)**소프트메일**

연락처: ㈜소프트메일 홈페이지: http://www.emsisoft.co.kr