

AMP for Endpoints 자격

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[AMP for Endpoints 자격 증명](#)

[새로운 퍼블릭 클라우드 설정 방법](#)

소개

이 문서에서는 AMP(Advanced Malware Protection) 라이선스를 얻고 대시보드에 액세스하는 프로세스에 대해 설명합니다.

기고자: Uriel Islas, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

Cisco는 다음과 같은 정보를 얻을 것을 권장합니다.

- AMP for Endpoints 라이선스
- 이메일 계정
- 컴퓨터

사용되는 구성 요소

- AMP 퍼블릭 클라우드
- Outlook

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 단계의 잠재적 영향을 이해해야 합니다.

구성

AMP4E(AMP For Endpoints) 제품을 인증하려면 eDelivery 이메일 또는 엔타이틀먼트 이메일을 참조하십시오.

참고: eDelivery 이메일에 대한 액세스 권한이 없는 경우 다음에 문의할 수 있습니다
.licensing@cisco.com 또는 온라인 포털(<http://cisco.com/tac/caseopen>)을 [방문하십시오](#). 적절

한 기술 및 하위 기술을 선택한 후 Type of Problem(문제 유형) 아래 **Licensing(라이선싱)**을 선택합니다.

AMP for Endpoints 자격 증명

AMP4E 자격 증명은 Cisco CSA(Security Account) 도메인에 속합니다. 첫 번째 Cisco Security 어카운트가 설정되는 즉시 조직 내에 보안 관리자를 더 추가할 수 있습니다. 새 클라우드 인스턴스를 생성하기 위해 라이선스를 적용하는 즉시 CSA를 생성하거나 기존 CSA 자격 증명을 사용하여 라이선스를 입력할 수 있습니다. 작업을 마치면 조직은 반드시 비즈니스와 연계되어야 합니다.

새로운 퍼블릭 클라우드 설정 방법

1단계. eDelivery 이메일 또는 자격 이메일에 제공된 URL로 이동합니다.

2단계. 선호하는 클라우드 데이터 센터를 선택합니다.



참고:미주 클라우드는 모든 국가에서 사용할 수 있습니다. 멀리 떨어져 있는 국가의 레이턴시와 관련된 문제는 없습니다.

3단계. Cisco Security Account를 AMP 클라우드에 연결합니다.



Security

Existing Customers

Log in with an Administrator account

Log In

New Customers

Welcome to Cisco Security

Create Account

a) CSA에 대한 자격 증명이 있지만 AMP4E에 대해서는 없는 경우 Log in(로그인)을 클릭합니다. 이 옵션은 CSA를 AMP 클라우드에 연결해야 합니다.

b) AMP 클라우드 또는 Cisco Security Org가 설정되지 않은 경우 Create Account(계정 생성)를 클릭하여 회사 라이선스를 적용합니다.

4단계. 회사에 CSA가 없는 경우 설정 요청에 따라 모든 필드의 값을 입력합니다.



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.



Already have an account? [Log in](#)

Account Registration

First name

Last name

Organization name

Email

Password

- be between 8 and 50 characters.
- contain at least one upper case, one lower case, and one numeric character.
- contain at least one of these following special characters:
!#\$%&'()*+,-./:;<=>?@[\]^_`{|}~
- must not contain two consecutive repeating characters.
- follow above rules or be a unicode password (8 characters minimum).

Password confirmation

Create Account

참고: 회사에 이미 CSA가 있는 경우 Castle 웹 사이트에서 자격 증명을 인증합니다. 2번에 구성된 클라우드를 기반으로 URL을 선택합니다. 미주 클라우드: <https://castle.amp.cisco.com> 유럽 클라우드: <https://castle.eu.amp.cisco.com> 아시아 태평양 클라우드: <https://castle.apjc.amp.cisco.com>

5단계. CSA가 생성되면 계정 등록 완료 페이지가 표시됩니다.



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

-  AMP for Endpoints
 -  Threat Grid
 -  Threat Response
- and more...

Account Registration Complete

Thank you for provisioning your Cisco Security account. This account will allow you to access multiple Cisco Security applications in which you are entitled to.

As soon as your account is provisioned, we will email you a link to validate your account.

6단계. no-reply@amp.cisco.com에서 새로운 Welcome to Cisco Security 이메일을 [확인합니다](#).

Welcome to Cisco Security



○ [Redacted]

Tuesday, December 17, 2019 at 4:24 PM

○ [Redacted]

[Show Details](#)

Dear [Redacted],

Congratulations, your Cisco Security account has been provisioned. To finalize your order, follow these steps:

Step One: Click [here](#) to activate your account.

Step Two: Click [here](#) to claim your order.

Thank you.

Cisco Security




If you feel you have received this email in error or need assistance go [here](#) to open a support case.

7단계. 1단계의 시작 이메일에서 계정을 활성화합니다.



Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

-  AMP for Endpoints
-  Threat Grid
-  Threat Response
and more...

✔ Your account has been activated. ✕


 

Log In

[Use Single Sign-On](#)

[Can't access your account?](#)


8단계. 성 웹 사이트에 대한 인증은 비즈니스에 구성된 이전 클라우드에 따라 달라집니다.




Tr
Threat Response

Advanced threat intelligence at your fingertips
Threat Response centralizes security events and alerts, and enriches them using data from other security services. It provides incident responders and SOC analysts with the data needed to detect, correlate, and prioritize security events.

[Launch](#) [Learn More](#)







Amp
AMP for Endpoints

Visibility and control to defeat advanced attacks
Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

[Learn More](#)






Tg
Threat Grid

Understand and prioritize threats faster
Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

[Learn More](#)



미주 클라우드- <https://castle.amp.cisco.com>

유럽 클라우드 - <https://castle.eu.amp.cisco.com>

아시아 태평양 클라우드 - <https://castle.apjc.amp.cisco.com>

9단계. 2단계에서 라이선스를 적용합니다.

Welcome to Cisco Security



○ [Redacted]

Tuesday, December 17, 2019 at 4:24 PM


○ [Redacted]

[Show Details](#)

Dear [Redacted]

Congratulations, your Cisco Security account has been provisioned. To finalize your order, follow these steps:

Step One: Click [here](#) to activate your account.

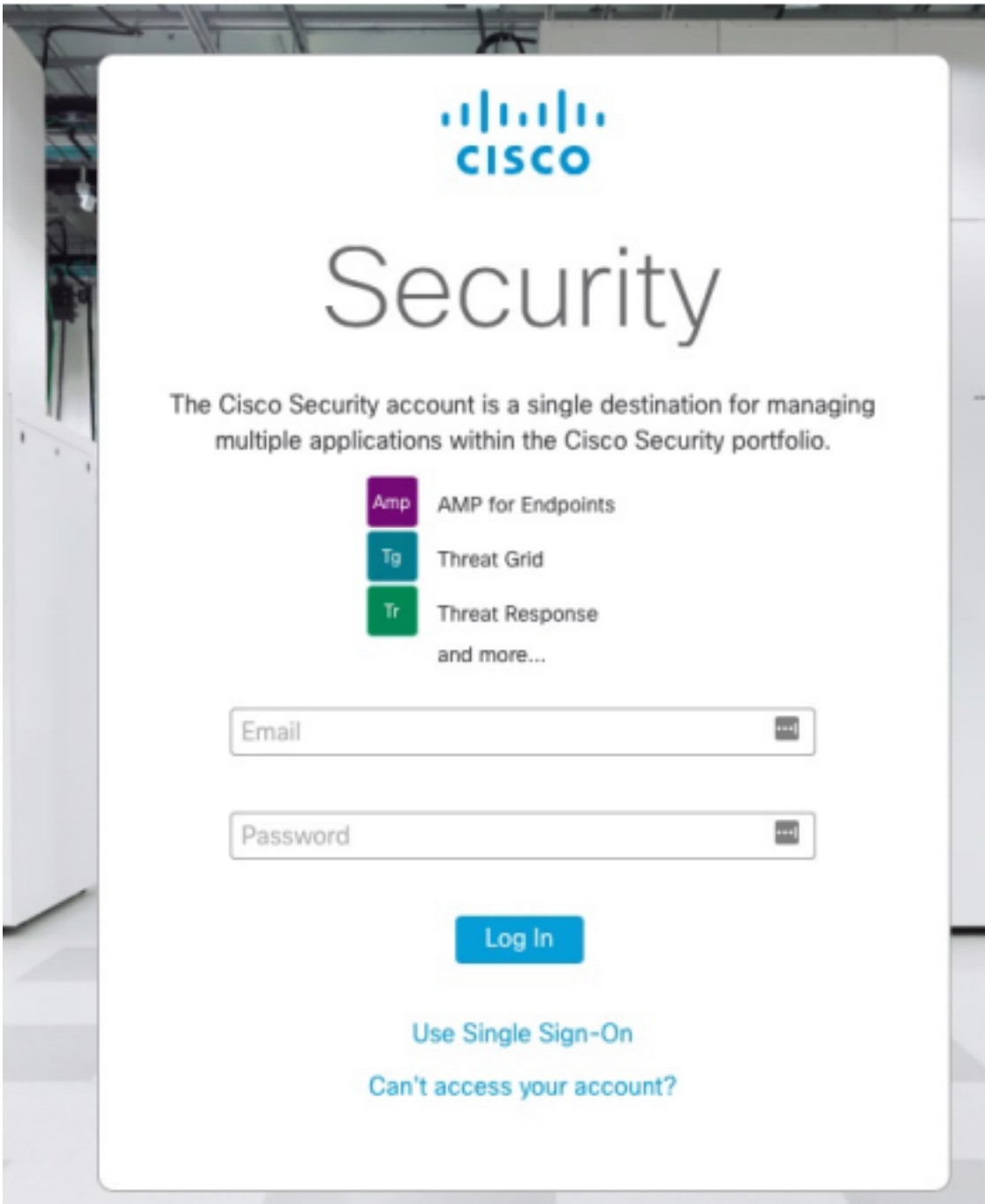
Step Two: Click [here](#) to claim your order. 

Thank you.

Cisco Security

If you feel you have received this email in error or need assistance go [here](#) to open a support case.

10단계. Cisco 보안 계정으로 로그인합니다.



11단계. 로그인한 후 주문 청구를 클릭합니다.



12단계. 이제 주문이 성공적으로 신청되었으며 AMP4E 콘솔을 시작할 수 있습니다.

An order was successfully claimed. ✕



Advanced threat intelligence at your fingertips

Threat Response centralizes security events and alerts, and enriches them using data from other security services. It provides incident responders and SOC analysts with the data needed to detect, correlate, and prioritize security events.

[Launch](#)

[Learn More](#)



Visibility and control to defeat advanced attacks

Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can't rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

[Launch](#)

[Learn More](#)



Understand and prioritize threats faster

Threat Grid combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. With a robust, context-rich malware knowledge base, you will understand what malware is doing, or attempting to do, how large a threat it poses, and how to defend against it.

[Learn More](#)

