

エンドポイント向けAMPの権限

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[エンドポイント用AMPクレデンシャル](#)

[新しいパブリッククラウドのセットアップ方法](#)

概要

このドキュメントでは、Advanced Malware Protection(AMP)ライセンスを取得し、ダッシュボードにアクセスするプロセスについて説明します。

著者：Cisco TACエンジニア、Uriel Islas

前提条件

要件

次の知識があることが推奨されます。

- AMP for Endpointsライセンス
- 電子メールアカウント
- コンピュータ

使用するコンポーネント

- AMPパブリッククラウド
- Outlook

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、すべてのステップの潜在的な影響を確実に理解してください。

設定

AMP For Endpoints(AMP4E)製品のライセンスを取得するには、eDelivery電子メールまたは権限付与の電子メールを参照できます。

注：eDeliveryの電子メールにアクセスできない場合は、次の連絡先にお問い合わせください

い。licensing@cisco.comまたはオンラインポータル(<http://cisco.com/tac/caseopen>)をご覧ください。適切なテクノロジーとサブテクノロジーを選択した後、[問題のタイプ]の下に表示される[ライセンス]を選択します。

エンドポイント用AMPクレデンシャル

AMP4Eのクレデンシャルは、シスコセキュリティアカウント(CSA)ドメインに属しています。最初のシスコセキュリティアカウントが設定されると、組織内のセキュリティ管理者をさらに追加できるようになります。ライセンスを適用して新しいクラウドインスタンスを作成する時点で、CSAを作成するか、既存のCSA認証情報を使用してライセンスを入力できます。完了したら、組織をビジネスに結び付ける必要があります。

新しいパブリッククラウドのセットアップ方法

ステップ1:eDeliveryの電子メールまたは権限付与の電子メールで指定されたURLで移動します。

ステップ2：好みのクラウドデータセンターを選択します。



注：アメリカクラウドはすべての国で使用できます。遠い国の遅延に関する問題はありません。

ステップ3：シスコセキュリティアカウントをAMPクラウドにリンクします。



Security

Existing Customers

Log in with an Administrator account

Log In

New Customers

Welcome to Cisco Security

Create Account

a) CSAの認証情報をすでに持っていて、AMP4Eの認証情報を持っていない場合は、[Log in]をクリックします。このオプションは、CSAをAMPクラウドにリンクする必要があります。

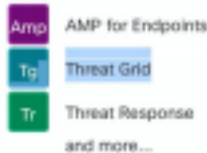
b) AMPクラウドまたはCisco Security Orgが設定されていない場合は、[アカウントの作成(Create Account)]をクリックして、会社のライセンスを適用します。

ステップ 4： 会社にCSAがない場合は、設定の要求に応じてすべてのフィールドの値を入力します。



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




注：会社にすでにCSAがある場合は、城下のWebサイトに移動して認証情報を認証します。番号2に設定されたクラウドに基づいてURLを選択します。アメリカクラウド：<https://castle.amp.cisco.com>ヨーロッパクラウド：<https://castle.eu.amp.cisco.com>アジア太平洋クラウド：<https://castle.apjc.amp.cisco.com> にアクセスしてください。

ステップ5: CSAが作成されると、[Account Registration Complete]ページが表示されます。



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.

ステップ6: no-reply@amp.cisco.comから新しいWelcome to Cisco Security電子メールを確認しま
す。

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.



ステップ7 : ステップ1のウェルカムメールからアカウントをアクティブ化します



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?](#)

ステップ8:castle Webサイトへの認証は、ビジネスで設定された以前のクラウドによって異なります。

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

アメリカクラウド – <https://castle.amp.cisco.com>

欧州クラウド – <https://castle.eu.amp.cisco.com>

アジア太平洋クラウド – <https://castle.apjc.amp.cisco.com>

ステップ 9 : ステップ2でライセンスを適用します。

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.

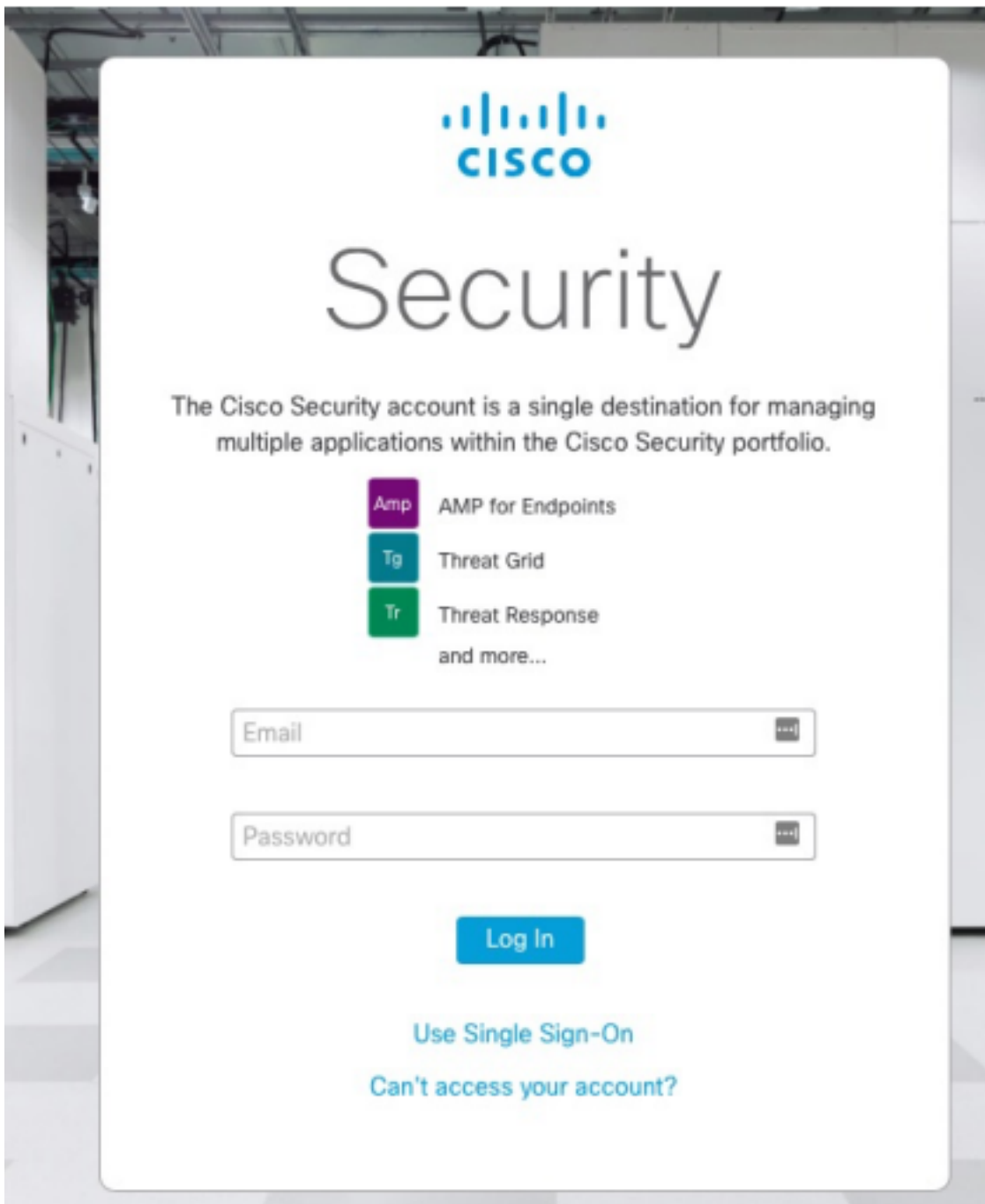
Step Two: Click [here](#) to claim your order.

Thank you.

Cisco Security

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

ステップ10 : シスコセキュリティアカウントでログインします。



ステップ11。入ったら、[Claim Order]をクリックします。

 Security Applications

Order: 0df5ae453ec24c6fa7903cdbe24cf18d

Would you like to apply this order to your organization?

[AMP4E-ADV-CL-LIC] Claim 589745612 for AMP.

[Claim Order](#)

My Orders

ID	Status
----	--------

ステップ12:注文が正常に要求され、AMP4Eコンソールを起動できるようになります。

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](#)

