

Droits pour AMP for Endpoints

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Informations d'identification d'AMP for Endpoints](#)

[Comment configurer un nouveau cloud public](#)

Introduction

Ce document décrit le processus d'obtention de la licence AMP (Advanced Malware Protection) et d'accès au tableau de bord.

Contribué par Uriel Islas, ingénieur du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître :

- Licence AMP for Endpoints
- Compte de messagerie
- Ordinateur

Components Used

Ce document n'est pas limité à une version spécifique du logiciel, mais ce document est basé sur ce logiciel :

- Cloud public AMP
- Outlook

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de n'importe quelle étape.

Configuration

Afin d'autoriser votre produit AMP For Endpoints (AMP4E), vous pouvez vous référer à l'e-mail de livraison électronique ou à un e-mail d'autorisation.

Note: Si vous n'avez pas accès à l'e-mail de livraison électronique, vous pouvez contacter : licensing@cisco.com ou visitez le portail en ligne à l'adresse <http://cisco.com/tac/caseopen>.

Après avoir sélectionné la technologie et la sous-technologie appropriées, sélectionnez **Licences** sous **Type de problème**.

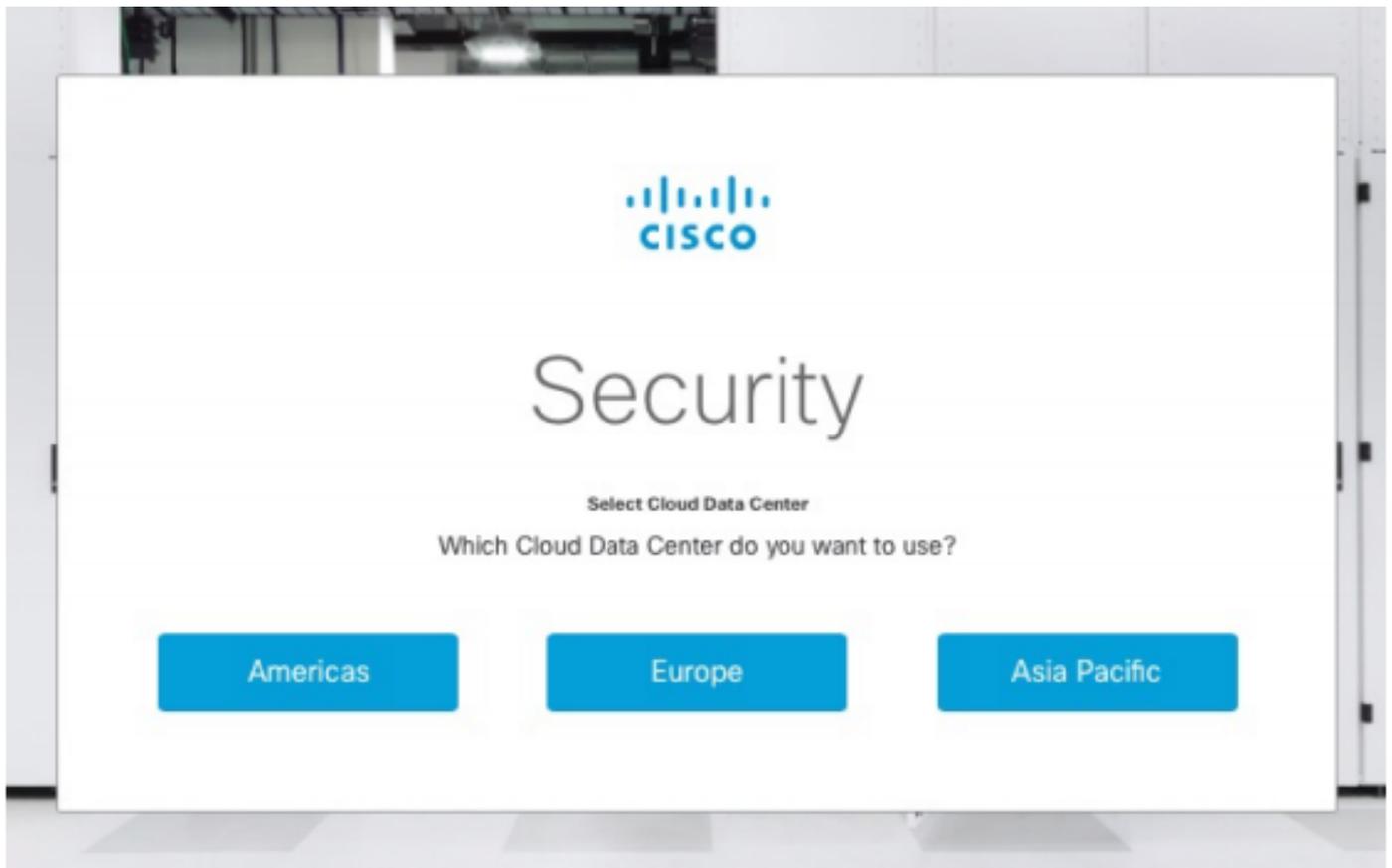
Informations d'identification d'AMP for Endpoints

Les informations d'identification AMP4E appartiennent au domaine Cisco Security Account (CSA). Dès que le premier compte de sécurité Cisco est configuré, vous pouvez ajouter d'autres administrateurs de sécurité au sein de votre entreprise. Au moment où vous appliquez votre licence pour créer une nouvelle instance de cloud, vous créez une CSA ou vous pouvez entrer la licence à l'aide de vos identifiants CSA existants. Une fois terminé, une organisation doit être liée à votre entreprise.

Comment configurer un nouveau cloud public

Étape 1. Naviguez sous l'URL fournie dans l'e-mail de livraison électronique ou dans l'e-mail d'autorisation.

Étape 2. Sélectionnez votre data center cloud préféré.



Note: Le cloud américain peut être utilisé pour tous les pays. Il n'y a aucun problème de latence pour les pays qui sont loin.

Étape 3. Liez votre compte de sécurité Cisco au cloud AMP.



Security

Existing Customers

Log in with an Administrator account

Log In

New Customers

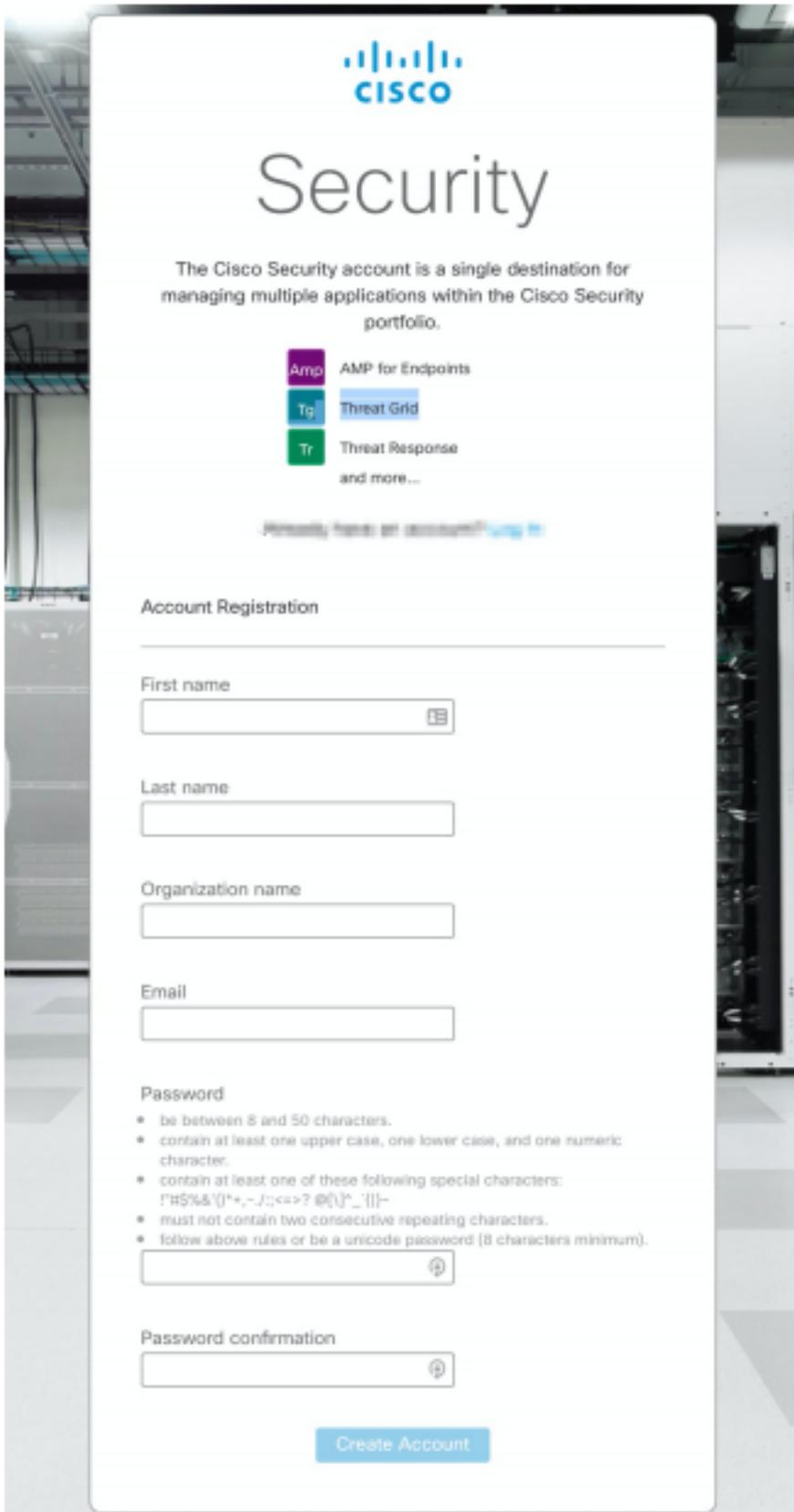
Welcome to Cisco Security

Create Account

a) Si vous avez déjà les informations d'identification d'une CSA, mais pas pour AMP4E, cliquez sur **Se connecter**. Cette option doit lier votre CSA au cloud AMP.

b) Si aucun cloud AMP ou Cisco Security Org n'est configuré, cliquez sur **Créer un compte** pour appliquer la licence à votre société.

Étape 4. Si votre société n'a pas de CSA, saisissez les valeurs de tous les champs comme demandé pour la configuration.



Note: Si quelqu'un a déjà un CSA dans votre entreprise, naviguez sous le site web du château pour authentifier vos informations d'identification. Sélectionnez l'URL en fonction du cloud configuré sur le numéro 2. **Cloud Amérique** : <https://castle.amp.cisco.com> **Cloud Europe** : <https://castle.eu.amp.cisco.com> **Le cloud Asie-Pacifique** : <https://castle.apjc.amp.cisco.com>.

Étape 5. Une fois l'ASC créée, une page Enregistrement de compte terminé s'affiche.



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.

Étape 6. Vérifiez un nouvel e-mail de bienvenue sur Cisco Security à partir de [no-reply@amp.cisco.com](mailto:reply@amp.cisco.com).

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.

Étape 7. Activez votre compte à partir de l'e-mail de bienvenue à l'étape 1



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. 

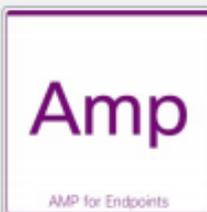
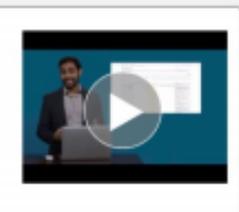
 

Log In

[Use Single Sign-On](#)

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

Étape 8. L'authentification sur le site web de château dépend du cloud précédent configuré pour votre entreprise.

 <p>Threat Response</p>	<p>Advanced threat intelligence at your fingertips</p> <p>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.</p> <p>Launch Learn More</p>	
 <p>AMP for Endpoints</p>	<p>Visibility and control to defeat advanced attacks</p> <p>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.</p> <p>Learn More</p>	
 <p>Threat Grid</p>	<p>Understand and prioritize threats faster</p> <p>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.</p> <p>Learn More</p>	

Cloud Amérique - <https://castle.amp.cisco.com>

Europe Cloud - <https://castle.eu.amp.cisco.com>

Le cloud Asie-Pacifique - <https://castle.apjc.amp.cisco.com>

Étape 9. Appliquez votre licence à l'étape 2.

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.

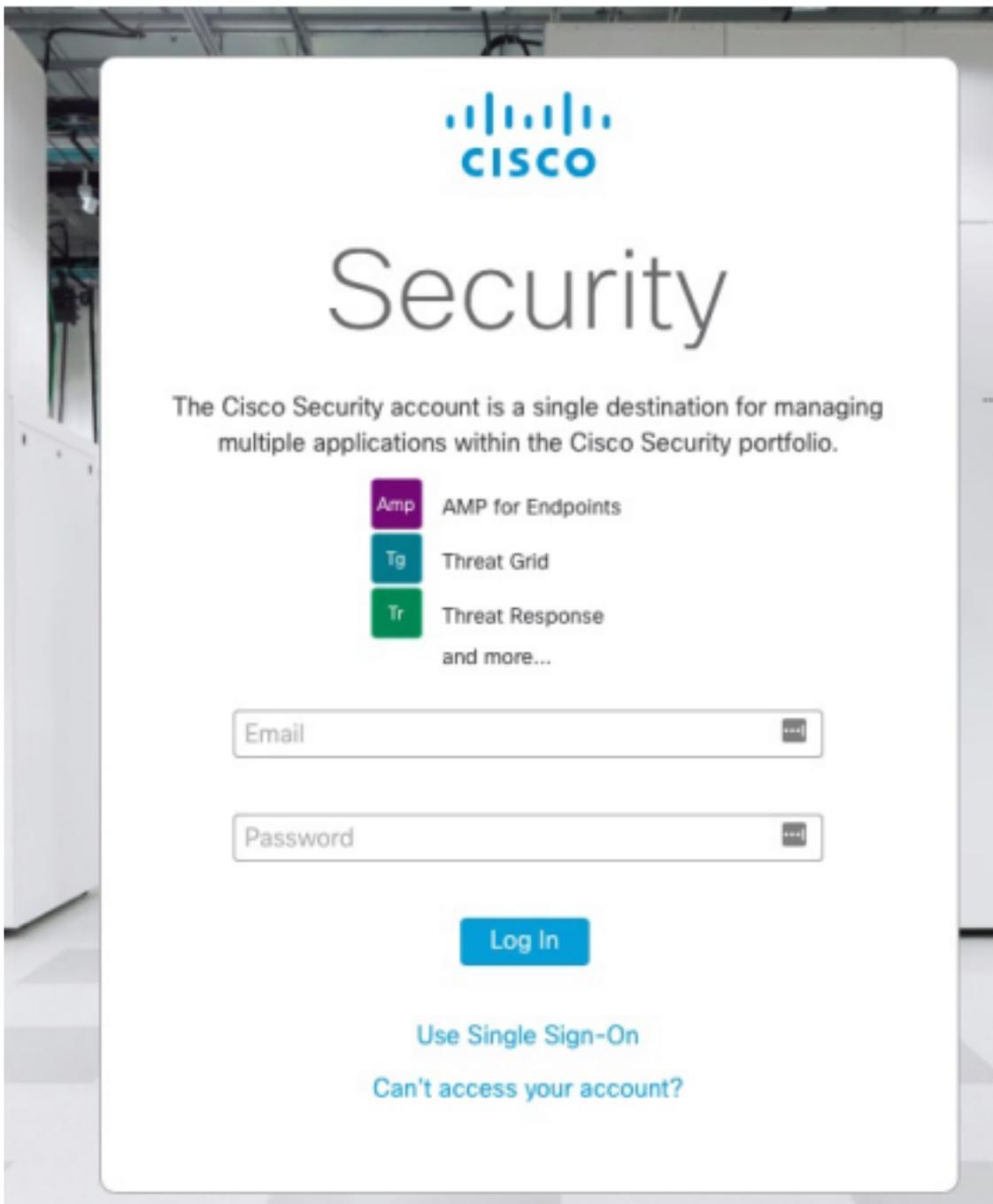
Step Two: Click [here](#) to claim your order. 

Thank you.

Cisco Security

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

Étape 10. Connectez-vous avec votre compte de sécurité Cisco.



Étape 11. Une fois entré, cliquez sur **Ordre de demande**.



Étape 12. Votre commande est maintenant demandée et vous pourrez lancer la console AMP4E.

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

