

# Diritti per AMP for Endpoints

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Credenziali AMP For Endpoints](#)

[Come configurare un nuovo cloud pubblico](#)

## Introduzione

In questo documento viene descritto il processo per ottenere il diritto alla licenza Advanced Malware Protection (AMP) e l'accesso al dashboard.

Contributo di Uriel Islas, Cisco TAC Engineer.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza di:

- Licenza AMP for Endpoints
- Account di posta elettronica
- Computer

### Componenti usati

Il documento può essere consultato per tutte le versioni software, ma in base a quanto riportato di seguito:

- AMP Public Cloud
- Outlook

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, verificare di aver compreso l'impatto potenziale di qualsiasi passaggio.

## Configurazione

Per accedere al prodotto AMP For Endpoints (AMP4E), è possibile fare riferimento all'e-mail di eDelivery o a un'e-mail di conferma.

**Nota:** Se non hai accesso all'e-mail di eDelivery, puoi contattare: [licensing@cisco.com](mailto:licensing@cisco.com) o

visitare il portale online all'indirizzo <http://cisco.com/tac/caseopen>. Dopo aver selezionato la tecnologia e la sottotecnologia appropriate, selezionare **Licenze** nell'elenco **Tipo di problema**.

## Credenziali AMP For Endpoints

Le credenziali AMP4E appartengono al dominio Cisco Security Account (CSA). Non appena i primi account Cisco Security sono configurati, è possibile aggiungere altri amministratori della sicurezza all'interno dell'organizzazione. Quando si applica la licenza per generare una nuova istanza del cloud, è possibile creare una CSA o immettere la licenza utilizzando le credenziali CSA esistenti. Una volta completata questa operazione, un'organizzazione deve essere legata alla propria attività.

### Come configurare un nuovo cloud pubblico

Passaggio 1. Accedere all'URL fornito nell'e-mail di eDelivery o nell'e-mail di adesione.

Passaggio 2. Selezionare il centro dati cloud preferito.



**Nota:** Il cloud americano può essere utilizzato per tutti i paesi. Non ci sono problemi legati alla latenza per i paesi che sono lontani.

Passaggio 3. Collegare l'account di sicurezza Cisco al cloud AMP.



# Security

Existing Customers

Log in with an Administrator account

Log In

New Customers

Welcome to Cisco Security

Create Account

a) Se si dispone già delle credenziali per un CSA, ma non per AMP4E, fare clic su **Log in**. Questa opzione deve collegare il CSA al cloud AMP.

b) Se non è stato configurato un cloud AMP o un Cisco Security Org, fare clic su **Create Account** (Crea account) per applicare la licenza alla propria azienda.

Passaggio 4. Se la società non dispone di un CSA, immettere i valori per tutti i campi come richiesto per l'impostazione.



# 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

**Nota:** Se qualcuno ha già un CSA nella tua azienda, naviga sotto castello sito web per autenticare le tue credenziali. Selezionare l'URL in base al cloud configurato sul numero 2.  
**Americhe:** <https://castle.amp.cisco.com> **Europe Cloud:** <https://castle.eu.amp.cisco.com> **Asia Pacifico Cloud:** <https://castle.apjc.amp.cisco.com>.

Passaggio 5. Dopo aver creato l'account CSA, viene visualizzata la pagina Registrazione account completata.



# 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.

Passaggio 6. Verificare una nuova e-mail di benvenuto in Cisco Security da [no-reply@amp.cisco.com](mailto:no-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.

Passaggio 7. Attiva il tuo account dall'email di benvenuto nel passaggio 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. 

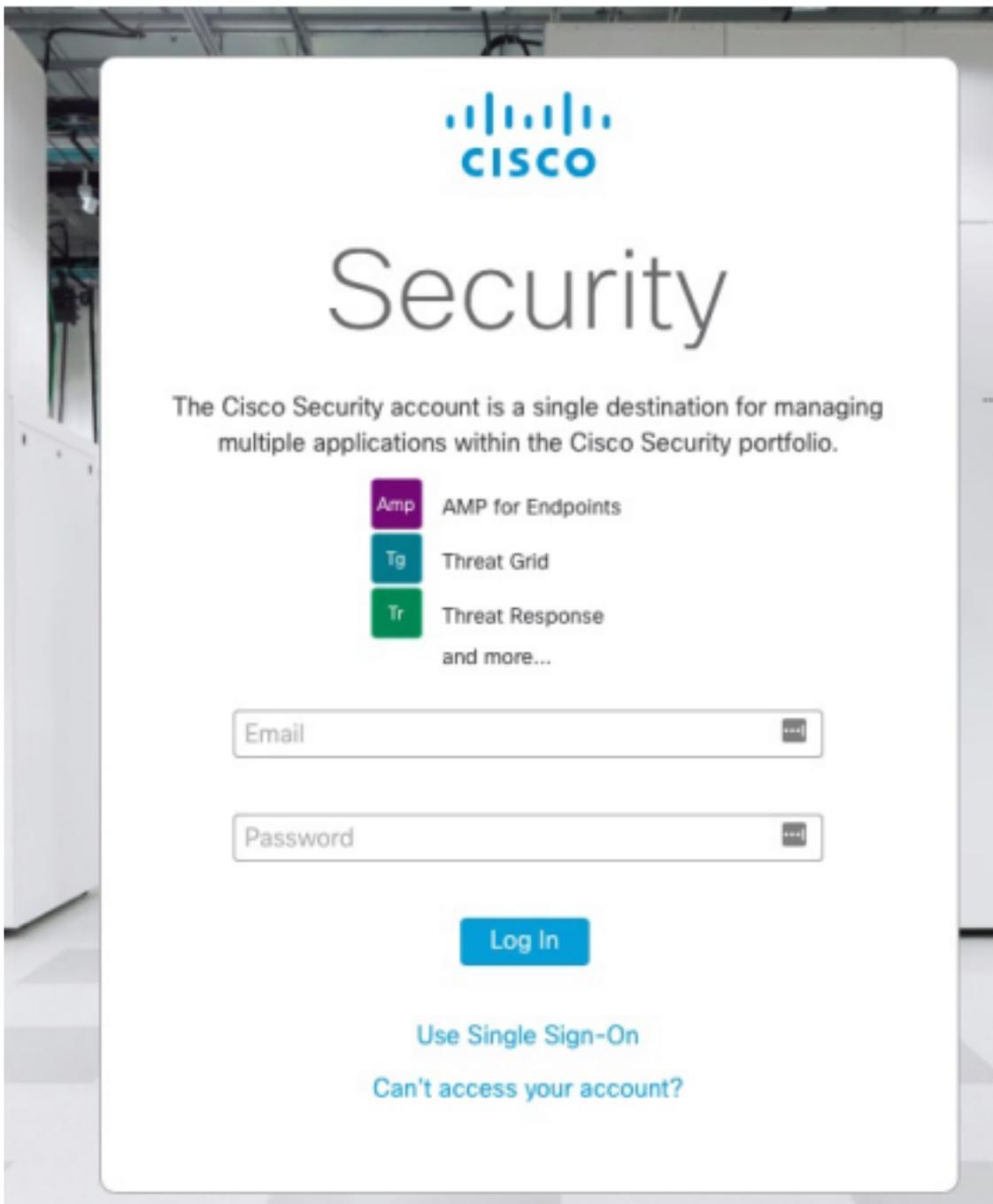
Log In

[Use Single Sign-On](#)

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

Passaggio 8. L'autenticazione nel sito Web del castello dipende dal cloud precedente configurato per l'azienda.





Passaggio 11. Una volta entrati, fare clic su **Richiedi ordine**.



Passaggio 12. L'ordine è stato inoltrato correttamente ed è possibile avviare la console AMP4E.

An order was successfully claimed. ✕

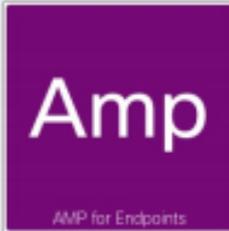
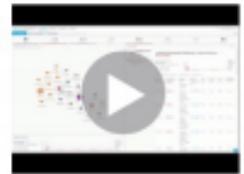


### Advanced threat intelligence at your fingertips

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](#)

