Berechtigung für AMP für Endgeräte

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Anmeldeinformationen für AMP für Endgeräte Einrichten einer neuen Public Cloud

Einführung

In diesem Dokument wird beschrieben, wie Sie die AMP-Lizenz (Advanced Malware Protection) und den Zugriff auf das Dashboard erhalten.

Unterstützt von Uriel Islas, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AMP für Endgeräte-Lizenz
- E-Mail-Konto
- Computer

Verwendete Komponenten

Dieses Dokument ist nicht auf eine bestimmte Softwareversion beschränkt. Dieses Dokument basiert jedoch auf dieser Software:

- AMP Public Cloud
- Outlook

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Schritte verstehen.

Konfigurieren

Um Ihr AMP für Endgeräte-Produkt (AMP4E) zu erhalten, können Sie die eDelivery-E-Mail oder eine Berechtigungs-E-Mail lesen.

Hinweis: Wenn Sie nicht auf die eDelivery-E-Mail zugreifen können, wenden Sie sich an:

licensing@cisco.com oder besuchen Sie das Online-Portal unter <u>http://cisco.com/tac/caseopen</u>. Wählen Sie nach Auswahl der geeigneten Technologie und Subtechnologie die unter **Problemtyp** aufgelistete **Lizenzierung aus**.

Anmeldeinformationen für AMP für Endgeräte

AMP4E-Anmeldeinformationen gehören zur Cisco Security Account (CSA)-Domäne. Sobald die ersten Cisco Security-Konten eingerichtet sind, können Sie weitere Sicherheitsadministratoren hinzufügen. Wenn Sie Ihre Lizenz zum Auslösen einer neuen Cloud-Instanz anwenden, erstellen Sie ein CSA, oder Sie können die Lizenz mit Ihren vorhandenen CSA-Anmeldeinformationen eingeben. Anschließend muss ein Unternehmen an Ihr Unternehmen gebunden sein.

Einrichten einer neuen Public Cloud

Schritt 1: Navigieren Sie zu der URL, die in der eDelivery- oder der Berechtigungsemail angegeben ist.

	cisco	
	Security	
Which	Select Cloud Data Center Cloud Data Center do you want	to use?
Americas	Europe	Asia Pacific

Schritt 2: Wählen Sie Ihr bevorzugtes Cloud Data Center aus.

Hinweis: Die Nord- und Südamerika-Cloud kann in allen Ländern genutzt werden. In weit entfernten Ländern gibt es keine Latenzprobleme.

Schritt 3: Verbinden Sie Ihr Cisco Security Account mit der AMP Cloud.



a) Wenn Sie bereits über die Anmeldeinformationen für ein CSA, jedoch nicht für AMP4E verfügen, klicken Sie auf **Anmelden**. Diese Option muss Ihren CSA mit der AMP-Cloud verbinden.

b) Wenn Sie keine AMP-Cloud oder Cisco Security Org eingerichtet haben, klicken Sie auf **Konto** erstellen, um die Lizenz für Ihr Unternehmen anzuwenden.

Schritt 4: Wenn Ihr Unternehmen über keinen CSA verfügt, geben Sie die Werte für alle Felder wie gewünscht ein.

	Security	
The Ci managir	isco Security account is a single destination for ng multiple applications within the Cisco Security portfolio.	
	Amp AMP for Endpoints Tg Threat Grid Tr Threat Response and more	
	Presidy have an account? using the	
Account R	egistration	5
First name	13	
Last name		
Organizati	on name	
Email		
Password	en 8 and 50 characters.	
 contain at character. contain at !'#\$%&'()' must not o follow abo 	least one upper case, one lower case, and one numeric least one of these following special characters: *+,-,/;;<=>? @(\)^ - contain two consecutive repeating characters. we rules or be a unicode password (8 characters minimum).	
	Ð	
Password	confirmation	

Hinweis: Wenn jemand bereits ein CSA in Ihrem Unternehmen hat, dann navigieren Sie unter Schloss Website, um Ihre Anmeldeinformationen zu authentifizieren. Wählen Sie die URL basierend auf der Cloud aus, die für Nummer 2 konfiguriert wurde. Nord- und Südamerika-Cloud: <u>https://castle.amp.cisco.com</u> Europe Cloud: <u>https://castle.eu.amp.cisco.com</u> Asia Pacific Cloud: <u>https://castle.apjc.amp.cisco.com</u>

Schritt 5: Nach der Erstellung des CSA wird die Seite "Account Registration Complete"

(Kontoregistrierung abgeschlossen) angezeigt.



Schritt 6: Überprüfen Sie eine neue Welcome to Cisco Security-E-Mail von <u>no-reply@amp.cisco.com</u>.

Welcome to Cisco Security



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

Schritt 7: Aktivieren Sie Ihr Konto über die Begrüßungs-E-Mail in Schritt 1.

cisco	
Security The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio. AMP for Endpoints To Threat Grid Threat Response and more	
 Your account has been activated. 	
Log In	
Use Single Sign-On Can't access your account?	

Schritt 8: Die Authentifizierung auf der Schloss-Website hängt von der vorherigen Cloud ab, die für Ihr Unternehmen konfiguriert wurde.



Nord- und Südamerika Cloud - https://castle.amp.cisco.com

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

Asien-Pazifik-Cloud - https://castle.apjc.amp.cisco.com

Schritt 9: Wenden Sie Ihre Lizenz in Schritt 2 an.

Welcome to Cisco Security



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

Schritt 10: Melden Sie sich bei Ihrem Cisco Security Account an.

C		
	cisco	
	Security	
	The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.	
	Amp AMP for Endpoints	
	Tg Threat Grid	
	Tr Threat Response	
	and more	
	Email	
	Password	
/	Log In	
	Use Single Sign-On	
	Can't access your account?	

Schritt 11: Klicken Sie anschließend auf Bestellungsauftrag.

Security	Applications				
		Order: 0df5ae Would you like to [AMP4E-ADV-CL	8453ec24c6fa apply this order to L-LIC] Claim 5897	07903cdbe24cf18d o your organization? 145612 for AMP. Claim Order	
	My Orders				
		ID			Status

Schritt 12: Ihre Bestellung wurde erfolgreich angefordert, und Sie können die AMP4E-Konsole starten.

ciste	Security	Applications	Users	SAML Configuration	
	An order was successfully claimed.				×
		Tr Threat Respon	58	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	
		Am ANP for Endpoi	p	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 guickly detect, contain, and remove advanced malware. Launch	
		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	