# Best Practice-Leitfaden für Advanced Malware Protection (AMP) für Cisco Email Security

### Inhalt

Einführung Feature-Schlüssel überprüfen Advanced Malware Protection (AMP) aktivieren Globale Einstellungen für Advanced Malware Protection (AMP) anpassen Dateianalyse-Schwellenwert-Einstellung Integration der ESA in die AMP-Konsole für Endgeräte Automatische Mailbox-Bereinigung aktivieren (MAR) Konfigurieren von Advanced Malware Protection (AMP) in Mail-Richtlinien Integration von SMA mit Cisco Threat Response (CTR) Fazit

## Einführung

Advanced Malware Protection (AMP) ist eine umfassende Lösung, die Malware erkennt und blockiert, kontinuierliche Analysen durchführt und retrospektive Warnmeldungen ausgibt. AMP mit Cisco Email Security bietet erstklassigen Schutz über das gesamte Angriffskontinuum hinweg vor, während und nach einem Angriff - mit dem kostengünstigsten und einfach bereitzustellenden Ansatz für Advanced Malware Defense.

In diesem Dokument mit Best Practices werden die wichtigsten Funktionen von AMP auf der Cisco E-Mail Security Appliance (ESA) wie unten beschrieben behandelt:

- Dateireputation erfasst einen Fingerabdruck jeder Datei, die die ESA passiert, und sendet diesen an das Cloud-basierte Informationsnetzwerk von AMP, um die Reputation zu überprüfen. Anhand dieser Ergebnisse können Sie schädliche Dateien automatisch blockieren und vom Administrator definierte Richtlinien anwenden.
- Dateianalyse ermöglicht die Analyse unbekannter Dateien, die die ESA passieren. Eine hochsichere Sandbox-Umgebung ermöglicht es AMP, präzise Details über das Verhalten der Datei zu erfassen und diese Daten mit detaillierten menschlichen und maschinellen Analysen zu kombinieren, um das Bedrohungspotenzial der Datei zu bestimmen. Diese Einstufung wird dann in das Cloud-basierte Informationsnetzwerk von AMP eingespeist und zur dynamischen Aktualisierung und Erweiterung des AMP-Cloud-Datensatzes für erweiterten Schutz verwendet.
- Cisco AMP Unity ist die Funktion, mit der ein Unternehmen sein AMP-fähiges Gerät einschließlich ESA mit AMP-Abonnement in der AMP für Endpoints-Konsole registrieren kann. Dank dieser Integration kann Cisco Email Security auf die gleiche Weise gesehen und

abgefragt werden, wie die AMP für Endgeräte-Konsole bereits für Endgeräte bietet, und es können Daten zur Dateiübertragung über alle Bedrohungsvektoren in einer einzigen Benutzeroberfläche korreliert werden.

 Cisco Threat Response - eine Orchestrierungsplattform, die sicherheitsrelevante Informationen von Cisco und Drittanbietern in einer zentralen, intuitiven Analyse- und Antwortkonsole zusammenführt. Dies wird durch ein modulares Design erreicht, das als Integrations-Framework für Ereignisprotokolle und Threat Intelligence dient. Module ermöglichen die schnelle Korrelation von Daten durch Erstellung von Beziehungsdiagrammen, die es Sicherheitsteams wiederum ermöglichen, einen klaren Überblick über den Angriff zu erhalten und schnell effektive Gegenmaßnahmen zu ergreifen.

### Feature-Schlüssel überprüfen

- Navigieren Sie auf der ESA zu Systemverwaltung> Feature Keys (Funktionstasten).
- Suchen Sie nach den Feature-Schlüsseln Dateireputation und Dateianalyse, und stellen Sie sicher, dass die Status **aktiv** sind.

### Advanced Malware Protection (AMP) aktivieren

- Navigieren Sie in der ESA zu Security Services >Advanced Malware Protection File Reputation and Analysis
- Klicken Sie unter Advanced Malware Protection Global Settings auf Aktivieren:

Advanced Malware Protection	
File Reputation:	Enabled
File Analysis:	Enabled
	Edit Global Settings

• Bestätigen Sie Ihre Änderungen.

#### Globale Einstellungen für Advanced Malware Protection (AMP) anpassen

- AMP ist jetzt aktiviert. Klicken Sie auf **Globale Einstellungen bearbeiten**, um die globalen Einstellungen anzupassen.
- Die Liste der Dateierweiterungen wird von Zeit zu Zeit automatisch aktualisiert. Rufen Sie daher diese Einstellung immer auf, und stellen Sie sicher, dass alle Dateierweiterungen ausgewählt sind:



- Erweitern der erweiterten Einstellungen für Dateireputation
- Die Standardauswahl für File Reputation Server ist AMERICA (cloud-sa.amp.cisco.com).
- Klicken Sie auf das Dropdown-Menü, und wählen Sie die nächstgelegenen Dateireputations-

Server (insbesondere für APJC- und EUROPE-Kunden) aus:

** Advanced Settings for File Reputation	File Reputation Serveri	W ANERCAS (cloud-ox ang clico port)	
	ANP for Endpoints Console Integration $\langle\Xi\rangle$	AMERICAD(Lagacy) (claud-sa ang-caustofin con) EUROPE (cloud-sa au ang-clock cont)	Prote
	SSI, Communication for Rise Republication:	APUC (cloud-exact class core) Protecte republication data Turnel Precept (bytowar): Server: Server: Server: Peespitrase: Pethope Receptivase: Pethope Recept	
	readbeat Interval	23 minutes	
	Query Timesut:	D Hornth	
	Processing Timesus:	111 month	
	File Reputation-Chart 30:	be79ab00-4463-4658-868a-73a3912a0434	
	file Retraspective:	Suppress the vertilat update alorts (8)	

- Erweitern der erweiterten Einstellungen für die Dateianalyse
- Die Standardauswahl für den File Analysis Server-URL ist **AMERICAS** (<u>https://panacea.threatgrid.com</u>).
- Klicken Sie auf das Dropdown-Menü, und wählen Sie den nächstgelegenen Dateireputations-Server (insbesondere für EUROPE-Kunden) aus:

	/		
File Analysis Server URL:	2 AMERICAS Detes Strangers President com		
File Analysis Clarg 22:	EURIPE (https://paracas.tryantgrid.au/	F-40577168/93C_CLORV_000088	
Advanced settings for Cache			
	File Analysis Server URL: File Analysis Clerif 32: Advanced settings for Capite	File Analysis Server URL: Else Analysis Oanre ID: Else Analysis Oanre ID: Annexed settings for Carrie	File Analysis Server URL:  Control Con

#### Dateianalyse-Schwellenwert-Einstellung

(Optional) Sie können den oberen Grenzwert für das akzeptable Dateianalyseergebnis festlegen. Die Dateien, die anhand der Schwellenwerteinstellungen blockiert werden, werden im Abschnitt "Incoming Malware Threat Files" (Dateien mit eingehenden Malware-Bedrohungen) des Berichts über Advanced Malware Protection (erweiterter Malware-Schutz) als benutzerdefinierter Grenzwert angezeigt.

- Erweitern Sie auf der Seite für die globalen AMP-Einstellungen die Option **Schwellenwerteinstellungen**.
- Der Standardwert für den Cloud-Service ist 95.
- Wählen Sie das Optionsfeld **Benutzerdefinierten Wert eingeben**, und ändern Sie den Wert (z. B. 70):

* Threshold Settings	File Analysis Threshold Score:	see Take From Clead Service (10)     Drian Gustern Weier: 10
----------------------	--------------------------------	--

• Klicken Sie auf Senden und Änderungen bestätigen.

#### Integration der ESA in die AMP-Konsole für Endgeräte

(Nur für AMP für Endpoints-Kunden) Über die AMP für Endpoints-Konsole kann eine einheitliche, benutzerdefinierte Datei-Sperrliste (oder eine Dateizulassung) erstellt werden und die Eindämmungsstrategie nahtlos über die Sicherheitsarchitektur, einschließlich der ESA, verteilen.

- Erweitern Sie auf der Seite für die globalen AMP-Einstellungen die Option **Erweiterte** Einstellungen für die Dateireputation.
- Klicken Sie auf die Schaltfläche Einheit bei AMP für Endgeräte registrieren:

• Klicken Sie auf **OK**, um zur AMP für Endpoints-Konsolensite umzuleiten, um die Registrierung abzuschließen.

- Melden Sie sich mit Ihren Anmeldeinformationen bei der AMP für Endpoints-Konsole an.
- Klicken Sie auf Zulassen der ESA-Registrierung:



• Die AMP für Endgeräte-Konsole fährt die Seite automatisch zurück zur ESA.

Stellen Sie sicher, dass der Registrierungsstatus als ERFOLGREICH	angezeigt wird:
---	-----------------

```
AMP for Endpoints Conscie Integration (?) VLNESAD00181_564D58189584A76C416D-4F8AA6579D18 (?) Deregister 🗸 SUCCESS
```

• Klicken Sie auf Senden und Bestätigen Sie Ihre Änderungen.

### Automatische Mailbox-Bereinigung aktivieren (MAR)

Wenn Sie O365-Mailboxen oder Microsoft Exchange 2013/2016 haben, ermöglicht die Funktion für die automatische Mailbox-Bereinigung (MAR) die Durchführung von Aktionen, wenn sich das Dateireputations-Urteil von "Sauber/Unbekannt" in "Bösartig" ändert.

- Navigieren Sie zu Systemverwaltung > Kontoeinstellungen.
- Klicken Sie unter Kontoprofil auf Kontoprofil erstellen, um ein API-Verbindungsprofil mit den Mailboxen von Microsoft Office 365 und/oder Microsoft Exchange zu erstellen:

Account Profiles U			
Create Account Profile			
Account Profile Name	Profile Type	Description	Delete
exchange	Exchange On Premise		8

- Klicken Sie auf Senden und Bestätigen Sie Ihre Änderungen.
- (Optional) Das verkettete Profil ist eine Sammlung von Profilen. Sie konfigurieren das verkettete Profil nur, wenn der Zugriff auf Konten über verschiedene Tenants unterschiedlicher Bereitstellungen hinweg möglich ist.
- Klicken Sie auf die Schaltfläche Domänenzuordnung erstellen, um Ihr Kontoprofil der Empfängerdomäne zuzuordnen. Die empfohlenen Einstellungen sind im Folgenden aufgeführt:

Domain Mapping 🕑		
Domain Mapping configuration is not available since all profiles are	aiready mapped	
Mailbox Profile/Chained Profile	Recipient Domain(s)	Delete
exchange	domain.com	<b>\$</b>

• Klicken Sie auf Senden und Bestätigen Sie Ihre Änderungen.

### Konfigurieren von Advanced Malware Protection (AMP) in Mail-Richtlinien

Nachdem AMP und MAR global konfiguriert wurden, können Sie die Dienste jetzt zum Senden

von Richtlinien aktivieren.

- Navigieren Sie zu Mail-Policys > Mail-Policys für eingehende E-Mails.
- Passen Sie die Einstellungen für Advanced Malware Protection für eine Richtlinie für eingehende E-Mails an, indem Sie auf den blauen Link unter Advanced Malware Protection für die Richtlinie klicken, die Sie anpassen möchten.
- Für die Zwecke dieses Dokuments für bewährte Verfahren klicken Sie auf das Optionsfeld neben **Dateireputation aktivieren** und wählen **Dateianalyse aktivieren**:

Advanced Malware Protection Settings		
Policy: DEFAULT		
Enable Advanced Malware Protection for This Policy:	<ul> <li>Enable File Reputation</li> <li>              Enable File Analysis</li></ul>	

- Es wird empfohlen, einen X-Header mit dem AMP-Ergebnis in eine Nachricht einzuschließen.
- In den nächsten drei Abschnitten können Sie auswählen, welche Aktion die ESA ausführen muss, wenn ein Anhang aufgrund von Nachrichtenfehlern als nicht scanbar gilt, die Ratenbeschränkung gilt oder wenn der AMP-Dienst nicht verfügbar ist. Es wird empfohlen, den aktuellen Zustand mit dem für die Nachricht angegebenen Warntext bereitzustellen:

Unscannable Actions on Message Errors		
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No 🖲 Yes
	Modify Message Subject:	No Prepend Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination	No Yes
		Host:
Unscannable Actions on Rate Limit		
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No Yes
	Modify Message Subject:	No   Prepend   Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No     Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination	No Yes
		Host:
Unscannable Actions on AMP Service Not Av	ailable	
Action Applied to Message:	Deliver As Is 🔻	
	Archive Original Message:	No Yes
	Modify Message Subject:	No   Prepend   Append
		[WARNING: ATTACHMENT UNSCANNED
	Add Custom Header to Message:	No Yes
		Header:
		Value:
	Modify Message Recipient:	No Yes
		Address:
	Send Message to Alternate Destination	No Yes
	nost.	Host:

• Im nächsten Abschnitt wird die ESA so konfiguriert, dass die Nachricht verworfen wird, wenn eine Anlage als schädlich gilt:

Messages with Halware Attachments:	
Action Applied to Message:	Drop Hessage *
Archive Original Message:	© No
Drop Malware Attachments:	® No. 0 Yes
Hodily Hessage Subject:	O No R Prepend O Append
	WARNING: MALWARE DETECTED)
> Advanced	Optione' settings.

• Es wird empfohlen, die Nachricht zu isolieren, wenn die Anlage zur Dateianalyse gesendet wird:

Hessages with File Analysis Pending:	
Action Applied to Message:	Quarantine *
Archive Original Message:	⊙ No ® Yes
NodFy Nessage Subject:	No      Prepard     Appand
	[WARNING: ATTACHMENT(S) HAY CONTAIN
F Advanced	Optional settings.

 (Nur für Richtlinien für eingehende E-Mails) Konfigurieren Sie die Abhilfemaßnahmen, die für die an Endbenutzer gesendete Nachricht durchgeführt werden sollen, wenn sich das Bedrohungsurteil auf schädlich ändert. Die empfohlenen Einstellungen sind im Folgenden aufgeführt:

🖉 Enable Mailbox Auto Remediation (HAR)		
Maibax Auto Remediation Actions apply only if Acc	Mailton Auto Remediation Actions apply only if Account Settings are configured. See System Administration > Account Settings .	
Action to be taken on message(s) in user's mailbox:	Forward to:     Forward to:	
	and Delete	

• Klicken Sie auf Senden und Bestätigen Sie Ihre Änderungen.

### Integration von SMA mit Cisco Threat Response (CTR)

Die Integration eines SMA Email Moduls erfordert die Verwendung von Security Services Exchange (SSE) über CTR. SSE ermöglicht es SMA, sich bei der Exchange zu registrieren, und Sie geben explizite Erlaubnis für Cisco Threat Response, auf die registrierten Geräte zuzugreifen. Der Prozess besteht darin, Ihre SMA mit SSE über ein Token zu verknüpfen, das generiert wird, wenn Sie bereit sind, es zu verknüpfen.

- Melden Sie sich im CTR-Portal (<u>https://visibility.amp.cisco.com</u>) mit Ihren Anmeldeinformationen an.
- CTR verwendet ein Modul zur Integration in andere Cisco Security-Produkte, einschließlich ESA. Klicken Sie auf die Registerkarte **Module**.
- Wählen Sie Geräte aus, und klicken Sie auf Geräte verwalten:



- CTR verschiebt die Seite auf SSE.
- Klicken Sie auf das + Symbol, um ein neues Token zu generieren, und klicken Sie auf Weiter.
- Kopieren Sie den neuen Token, bevor Sie das Feld schließen:

Add Devices and Generate Tokens						
The following tokens have been generated and will be valid for 1	hour(s):					
Tokens						
0ac7c30df02c0abfbe4869b8085445c8						
Close Copy to Clipboard	Save To File					

- Navigieren Sie in Ihrem SMA zu Management Appliances Registerkarte > Network > Cloud Service Settings.
- Klicken Sie auf **Edit Setting,** und stellen Sie sicher, dass die Option Threat Response **Enable** ist.
- Die Standardauswahl f
  ür die URL des Threat Response-Servers ist AMERICAS (apisse.cisco.com). F
  ür EUROPE-Kunden klicken Sie auf das Dropdown-Men
  ü, und w
  ählen Sie EUROPE (api.eu.sse.itd.cisco.com):

Cloud Service Settings						
Edit Cloud Services						
Threat Response:	il Erable					
Threat Response Server:	AMERICAS (api-see.cisco.com) •					
Carcol	EUROPE (api eux see .td. cisco.com)					

- Klicken Sie auf Senden und Bestätigen Sie Ihre Änderungen.
- Fügen Sie den Tokenschlüssel (den Sie über das CTR-Portal generiert haben) in die Cloud Services Setting ein, und klicken Sie auf **Registrieren**:



- Es wird eine Weile dauern, den Registrierungsprozess abzuschließen. Bitte navigieren Sie nach ein paar Minuten zurück zu dieser Seite, um den Status erneut zu überprüfen.
- Kehren Sie zu CTR > Modules > Device zurück, und klicken Sie auf die Schaltfläche Gerät neu laden, um sicherzustellen, dass SMA in der Liste angezeigt wird:

threat Response In	vestigate Snapshots Incidents	Beta Intelligence	Modules			? 🔅	
Settings > Devices							
Settings	Devices						
Your Account							
Devices	Manage Devices Reload						
API Clients	Hallage Devices						
> Modules	Name	Туре	Version	Description	ID	IP Address	
Users	sma1	SMA	13.0.0-187	SMA	1	127.0.0.1	

### Fazit

Dieses Dokument beschreibt die Standard- oder Best Practice-Konfigurationen für Cisco

Advanced Malware Protection (AMP) in der E-Mail Security Appliance. Die meisten dieser Einstellungen sind sowohl für eingehende als auch für ausgehende E-Mail-Richtlinien verfügbar. Konfigurations- und Filterfunktionen werden in beide Richtungen empfohlen.