

Guida alle best practice per Advanced Malware Protection (AMP) su Cisco Email Security

Sommario

[Introduzione](#)

[Verifica chiavi funzionalità](#)

[Abilita Advanced Malware Protection](#)

[Personalizza impostazioni globali di Advanced Malware Protection](#)

[Impostazione soglia analisi file](#)

[Integrazione di ESA con AMP for Endpoints Console](#)

[Abilita correzione automatica cassetta postale \(MAR\)](#)

[Configura Advanced Malware Protection \(AMP\) nei criteri di posta](#)

[Integrazione di SMA con Cisco Threat Response \(CTR\)](#)

[Conclusioni](#)

Introduzione

Advanced Malware Protection (AMP) è una soluzione completa che consente il rilevamento e il blocco di malware, l'analisi continua e la segnalazione retrospettiva. L'utilizzo di AMP con Cisco Email Security consente una protezione superiore attraverso il continuum degli attacchi, prima, durante e dopo un attacco, con l'approccio più conveniente e facile da implementare alla difesa avanzata dal malware.

Questo documento sulle best practice tratterà le funzionalità principali di AMP su Cisco Email Security Appliance (ESA), come indicato di seguito:

- **Reputazione dei file:** rileva un'impronta digitale di ciascun file mentre attraversa l'ESA e lo invia alla rete di intelligence basata su cloud di AMP per un verdetto di reputazione. Dati questi risultati, è possibile bloccare automaticamente i file dannosi e applicare i criteri definiti dall'amministratore.
- **Analisi dei file:** consente di analizzare i file sconosciuti che attraversano l'ESA. Un ambiente sandbox altamente sicuro consente ad AMP di ottenere dettagli precisi sul comportamento del file e di combinare tali dati con un'analisi dettagliata di persone e macchine per determinare il livello di rischio del file. Questa disposizione viene quindi inserita nella rete di intelligence basata su cloud AMP e utilizzata per aggiornare ed espandere dinamicamente il set di dati cloud AMP per una protezione avanzata.
- **Monitoraggio e aggiornamento automatici delle caselle di posta (MAR):** per Microsoft Office 365 ed Exchange 2013/2016 automatizza la rimozione dei messaggi di posta elettronica contenenti file che diventano dannosi dopo il punto di ispezione iniziale. Ciò consente agli amministratori di risparmiare ore di lavoro e di contenere l'impatto di una minaccia.
- **Cisco AMP Unity:** funzionalità che consente a un'organizzazione di registrare il proprio dispositivo abilitato per AMP, inclusa l'abbonamento ESA con AMP, nella console AMP for Endpoints. Con questa integrazione, Cisco Email Security può essere visto e interrogato per osservazioni di esempio allo stesso modo in cui la console AMP for Endpoints offre già per gli

endpoint e consente di correlare i dati di propagazione dei file tra tutti i vettori di minaccia in una singola interfaccia utente.

- **Cisco Threat Response:** è una piattaforma di orchestrazione che riunisce le informazioni sulla sicurezza provenienti da Cisco e da fonti di terze parti in un'unica console di indagine e risposta intuitiva. Lo fa attraverso un design modulare che funge da struttura di integrazione per i log degli eventi e le informazioni sulle minacce. I moduli consentono una rapida correlazione dei dati creando grafici delle relazioni che, a loro volta, consentono ai team di sicurezza di ottenere una visione chiara dell'attacco e di intraprendere rapidamente azioni di risposta efficaci.

Verifica chiavi funzionalità

- Sull'ESA, selezionare **System Administration > Feature Keys (Amministrazione sistema)**
- Cercate le chiavi della feature Reputazione file (File Reputation) e Analisi file (File Analysis) e assicuratevi che gli stati siano **Attivo (Active)**

Abilita Advanced Malware Protection

- Sull'ESA, selezionare **Security Services > Advanced Malware Protection - File Reputation and Analysis**
- Fare clic sul pulsante **Enable (Abilita)** in **Advanced Malware Protection Global Settings** (Impostazioni globali di protezione da malware avanzato):



- Eseguire il **commit** delle modifiche.

Personalizza impostazioni globali di Advanced Malware Protection

- AMP è ora abilitato. Fare clic su **Modifica impostazioni globali** per personalizzare le impostazioni globali.
- L'elenco delle estensioni di file verrà aggiornato automaticamente di tanto in tanto, quindi visitare sempre questa impostazione e assicurarsi che tutte le estensioni di file siano selezionate:



- Espandi **impostazioni avanzate per reputazione file**
- La selezione predefinita per File Reputation Server è **AMERICA (cloud-sa.amp.cisco.com)**
- Fare clic sul menu a discesa e scegliere i File Reputation Server più vicini (in particolare per i

clienti APJC ed EUROPE):



- Espandi **impostazioni avanzate per analisi file**
- La selezione predefinita per l'URL di File Analysis Server è **AMERICAS** (<https://panacea.threatgrid.com>)
- Fare clic sul menu a discesa e scegliere i File Reputation Server più vicini (in particolare per i clienti EUROPA):



Impostazione soglia analisi file

(Facoltativo) È possibile impostare il limite superiore per il punteggio accettabile dell'analisi del file. I file bloccati in base alle impostazioni di soglia vengono visualizzati come Soglia personalizzata nella sezione File delle minacce di malware in ingresso del report Protezione avanzata da malware.

- Nella pagina delle impostazioni globali dell'AMP, espandere Impostazioni **soglia**.
- Il valore predefinito del servizio cloud è **95**.
- Scegliere il pulsante di opzione **Immettere valore personalizzato** e modificare il valore (ad esempio 70):



- Fare clic su **Sottometti** e su **Conferma** modifiche

Integrazione di ESA con AMP for Endpoints Console

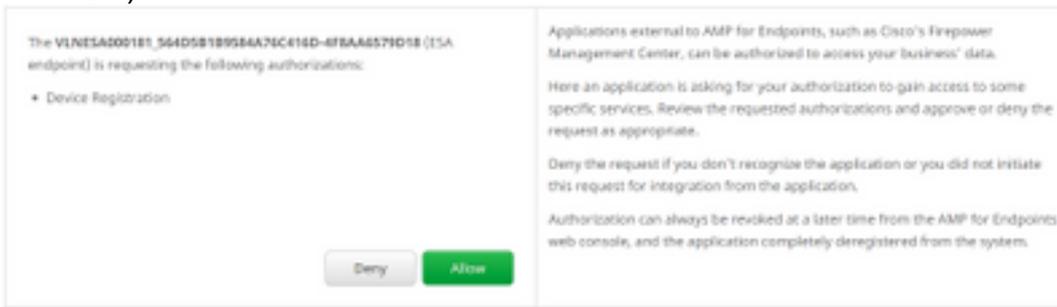
(Solo per i clienti di AMP for Endpoints) Tramite la console di AMP for Endpoints è possibile creare un elenco di blocco dei file personalizzato unificato (o un elenco dei file consentiti) che può essere distribuito senza problemi in tutta l'architettura di sicurezza, compresa l'ESA.

- Nella pagina delle impostazioni globali di AMP espandere **Impostazioni avanzate per la reputazione dei file**
- Fare clic sul pulsante **Registra accessorio con AMP for Endpoints**:



- Fare clic su **OK** per reindirizzare al sito della console AMP for Endpoints per completare la registrazione.
- Accedere alla console AMP for Endpoints con le credenziali utente
- Fare clic su **Allow** authoring the ESA registration (Consenti autorizzazione alla registrazione)

ESA):



- La console AMP for Endpoints esegue automaticamente il pivot della pagina verso ESA.
- Verificare che lo stato della registrazione sia **SUCCESS**:



- Fare clic su **Invia** e su **Conferma** modifiche

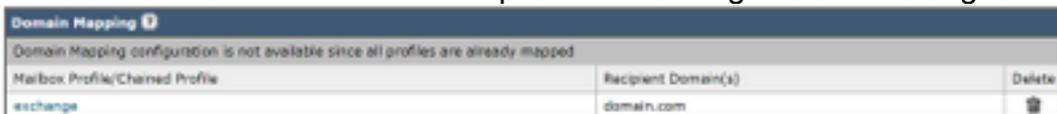
Abilita correzione automatica cassetta postale (MAR)

Se si dispone di cassette postali O365 o di Microsoft Exchange 2013/2016, la funzione di risoluzione automatica delle cassette postali (MAR) consente di eseguire l'azione quando il verdetto della reputazione del file passa da Pulito/Sconosciuto a Dannoso.

- Passare a **Amministrazione sistema > Impostazioni account**
- In **Profilo account**, fare clic su **Crea profilo account** per creare un profilo di connessione API con Office 365 e/o le cassette postali di Microsoft Exchange:



- Fare clic su **Invia** e su **Conferma** modifiche
- **(Facoltativo)** Profilo concatenato è un insieme di profili. È possibile configurare il profilo concatenato solo quando gli account a cui accedere risiedono in tenant diversi di tipi diversi di distribuzioni.
- Fare clic sul pulsante **Crea mapping di dominio** per mappare il profilo dell'account con il dominio del destinatario. Le impostazioni consigliate sono le seguenti:



- Fare clic su **Invia** e su **Conferma** modifiche

Configura Advanced Malware Protection (AMP) nei criteri di posta

Dopo aver configurato AMP e MAR a livello globale, è possibile abilitare i servizi per le policy di posta.

- Selezionare **Mail Policies > Incoming Mail Policies** (Policy di posta > Criteri posta in arrivo)
- Personalizzare le impostazioni di **Advanced Malware Protection** per un criterio Posta in arrivo facendo clic sul collegamento blu in **Advanced Malware Protection** per il criterio che si desidera personalizzare.
- Ai fini di questo documento, fare clic sul pulsante di opzione accanto a **Abilita reputazione file** e selezionare **Abilita analisi file**:

Advanced Malware Protection Settings	
Policy:	DEFAULT
Enable Advanced Malware Protection for This Policy:	<input checked="" type="radio"/> Enable File Reputation <input checked="" type="radio"/> Enable File Analysis <input type="radio"/> No

- Si consiglia di **includere un'intestazione X con il risultato AMP in un messaggio**.
- Le tre sezioni seguenti consentono di selezionare l'azione che l'ESA deve eseguire se un allegato viene considerato non scansionabile a causa di errori nei messaggi, limiti di velocità o se il servizio AMP non è disponibile. L'azione consigliata è **Consegna così com'è con testo di avviso anteposto all'oggetto del messaggio**:

Unscannable Actions on Message Errors	
Action Applied to Message:	Deliver As Is ▼
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>
Unscannable Actions on Rate Limit	
Action Applied to Message:	Deliver As Is ▼
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>
Unscannable Actions on AMP Service Not Available	
Action Applied to Message:	Deliver As Is ▼
▼ Advanced	Archive Original Message: <input type="radio"/> No <input checked="" type="radio"/> Yes Modify Message Subject: <input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: ATTACHMENT UNSCANNED]
Add Custom Header to Message:	<input checked="" type="radio"/> No <input type="radio"/> Yes Header: <input type="text"/> Value: <input type="text"/>
Modify Message Recipient:	<input checked="" type="radio"/> No <input type="radio"/> Yes Address: <input type="text"/>
Send Message to Alternate Destination Host:	<input checked="" type="radio"/> No <input type="radio"/> Yes Host: <input type="text"/>

- La sezione successiva configura l'ESA in modo che elimini il messaggio se un allegato è considerato dannoso:

Messages with Malware Attachments:	
Action Applied to Message:	Drop Message ▼
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Drop Malware Attachments:	<input checked="" type="radio"/> No <input type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append [WARNING: MALWARE DETECTED]
▶ Advanced	Optional settings

- L'azione consigliata è quella di mettere in quarantena il messaggio se l'allegato viene inviato per l'analisi dei file:

Messages with File Analysis Pending:	
Action Applied to Message:	Quarantine ▾
Archive Original Message:	<input type="radio"/> No <input checked="" type="radio"/> Yes
Modify Message Subject:	<input type="radio"/> No <input checked="" type="radio"/> Prepend <input type="radio"/> Append
<input type="checkbox"/> Advanced Optional settings.	

- (Solo per i criteri della posta in arrivo) Configurare le azioni correttive da eseguire sul messaggio recapitato agli utenti finali quando il verdetto della minaccia diventa dannoso. Le impostazioni consigliate sono le seguenti:

Enable Mailbox Auto Remediation (MAR)	
Mailbox Auto Remediation Actions apply only if Account Settings are configured. See System Administrator > Account Settings.	
Action to be taken on message(s) in user's mailbox:	<input type="radio"/> Forward to: <input type="text"/>
	<input checked="" type="radio"/> Delete
	<input type="radio"/> Forward to: <input type="text"/> and Delete

- Fare clic su **Invia** e su **Conferma** modifiche

Integrazione di SMA con Cisco Threat Response (CTR)

L'integrazione di un modulo di posta elettronica SMA richiede l'utilizzo di SSE (Security Services Exchange) tramite CTR. SSE consente a uno SMA di effettuare la registrazione con Exchange e consente esplicitamente a Cisco Threat Response di accedere ai dispositivi registrati. Il processo prevede il collegamento dell'SMA all'SSE tramite un token generato quando si è pronti per il collegamento.

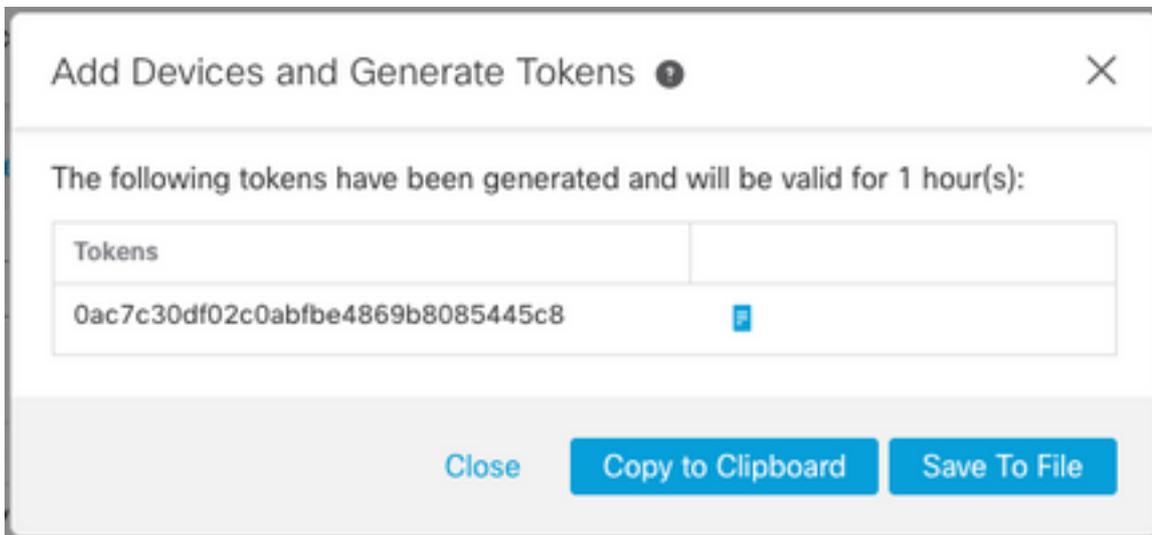
- Sul portale CTR (<https://visibility.amp.cisco.com>), eseguire l'accesso con le credenziali utente.
- CTR utilizza un modulo per l'integrazione con altri prodotti di sicurezza Cisco, tra cui ESA. Fare clic sulla scheda **Moduli**.
- Scegliere **Dispositivi** e fare clic su **Gestisci dispositivi**:


Threat Response
Investigate
Snapshots
Incidents Beta
Intelligence
Modules

Settings > Devices

Settings	<h3>Devices</h3> <div style="display: flex; justify-content: space-around; margin-top: 20px;"> Manage Devices Reload Devices </div>
Your Account	
Devices	
API Clients	

- CTR eseguirà il pivot della pagina su SSE.
- Fare clic sull'icona **+** per generare un nuovo token e fare clic su **Continua**.
- Copiare il nuovo token prima di chiudere la casella:



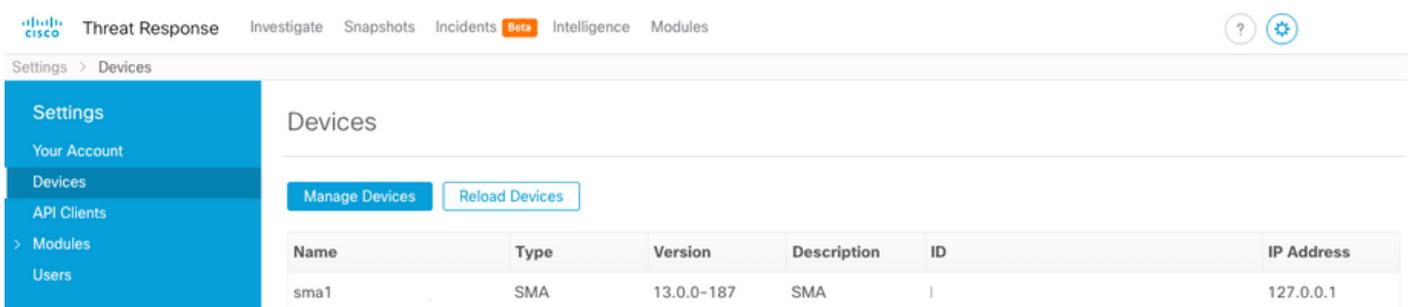
- Nella scheda SMA, selezionare **Management Appliance > Rete > Impostazioni servizio cloud**
- Fare clic su **Modifica impostazione** e verificare che l'opzione Risposta alla minaccia sia **Abilita**.
- La selezione predefinita per l'URL del server di risposta alle minacce è **AMERICAS (api-sse.cisco.com)**. Per i clienti EUROPA, fare clic sul menu a discesa e scegliere **EUROPA (api.eu.sse.itd.cisco.com)**:



- Fare clic su **Invia** e su **Conferma** modifiche
- Incollare la chiave del token (generata dal portale CTR) nell'impostazione dei servizi cloud e fare clic su **Registra**:



- Il completamento del processo di registrazione richiederà alcuni minuti. Tornare a questa pagina dopo alcuni minuti per verificare di nuovo lo stato.
- Tornare a **CTR > Moduli > Dispositivo** e fare clic sul pulsante **Ricarica dispositivo** per verificare che lo SMA sia visualizzato nell'elenco:



Conclusioni

Questo documento ha lo scopo di descrivere le configurazioni predefinite o le best practice per Cisco Advanced Malware Protection (AMP) in Email Security Appliance. La maggior parte di queste impostazioni è disponibile nei criteri per la posta elettronica in entrata e in uscita e la

configurazione e il filtro sono consigliati in entrambe le direzioni.