Best Practice Guide for Advanced Malware Protection (AMP) op Cisco Email Security

Inhoud

Inleiding

Advanced Malware Protection (AMP) is een uitgebreide oplossing voor het detecteren en blokkeren van malware, continue analyse en retrospectieve signalering. Gebruikmaken van AMP met Cisco Email Security maakt superieure bescherming in het aanvalsspectrum mogelijk - voor, tijdens en na een aanval met de meest rendabele, eenvoudig uitgeruste benadering van geavanceerde malware-verdediging.

Dit document met optimale werkmethoden bevat de belangrijkste functies van Advanced Malware Protection op de Cisco e-mail security applicatie (ESA), zoals hieronder vermeld:

- **File Reputation** - neemt een vingerafdruk van elk bestand op terwijl het de ESA doorkruist en stuurt het naar het op de cloud gebaseerde inlichtingennetwerk van AMP voor een reputatieoordeel. Gezien deze resultaten kunt u automatisch kwaadaardige bestanden blokkeren en beheerder-gedefinieerd beleid toepassen.
- **File Analysis** - biedt de mogelijkheid om onbekende bestanden te analyseren die het ESA oversteken. Een zeer veilige zandbak-omgeving stelt AMP in staat om precieze details te geven over het gedrag van het bestand en die gegevens te combineren met gedetailleerde menselijke en machinale analyse om het bedreigingsniveau van het bestand te bepalen. Deze dispositie wordt vervolgens in een op de AMP cloud gebaseerd inlichtingennetwerk van de AMP gevoed en gebruikt om de AMP-cloudgegevens dynamisch te actualiseren en uit te breiden voor verbeterde bescherming.
- **Auto Remediation (MAR)** van een **postbus** - voor Microsoft Office 365 en Exchange 2013/2016 automatiseert het verwijderen van e-mails met bestanden die na het eerste inspectiepunt kwaadaardig worden. Hiermee worden beheersuren aan het werk bespaard en wordt de impact van een bedreiging beperkt.
- **Cisco Advanced Malware** Protection **Unity** - is de mogelijkheid die een organisatie toestaat om haar op AMP gebaseerde apparaat, inclusief ESA, te registreren met AMP-abonnement in de AMP voor Endpoints Console. Dankzij een dergelijke integratie kan Cisco Email Security

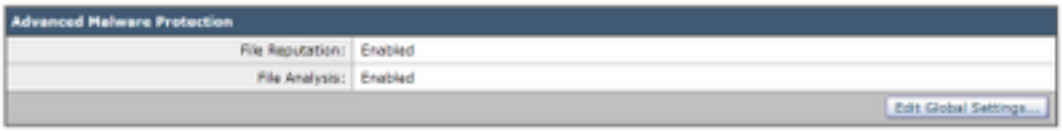
worden gezien en gevraagd voor voorbeeldwaarnemingen op dezelfde manier als de AMP voor Endpoints console al biedt voor endpoints en maakt u correlerende gegevens voor bestandspropagatie over alle bedreigingssectoren in één gebruikersinterface mogelijk.
- **Cisco Threat Response** - een orkestratieplatform dat security-gerelateerde informatie van Cisco en bronnen van derden samenbrengt in één intuïtief onderzoek- en responsconsole. Dit gebeurt door middel van een modulair ontwerp dat fungeert als een integratiekader voor het wekken van gebeurtenissen en dreigingsinformatie. De modules maken een snelle correlatie tussen de gegevens mogelijk door relatievlakken op te bouwen die op hun beurt beveiligingsteams in staat stellen een duidelijke visie op de aanval te verkrijgen en snel doeltreffende responsacties te ondernemen.

Functiesets controleren

- Raadpleeg in het ESR **systeembeheerdershandleidingen> Functiesets**
- Zoek naar de functiekaarten voor bestanduploaden en Bestandsanalyse en controleer of de statussen **actief** zijn

Advanced Malware Protection

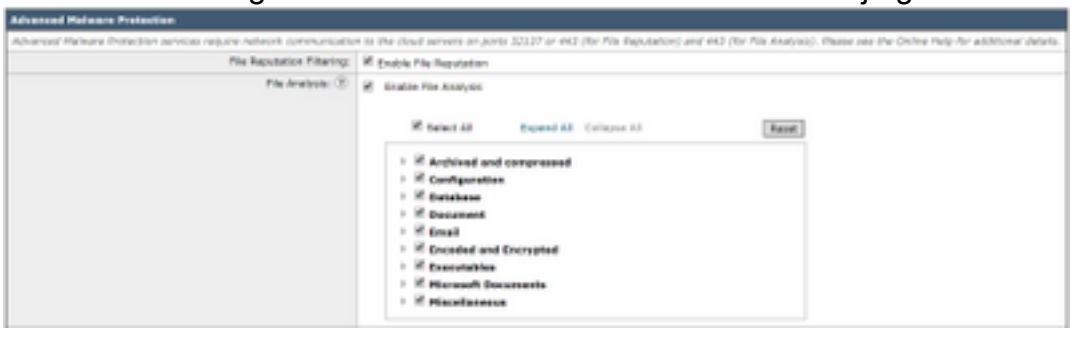
- Ga in het ESR naar **Security Services >Advanced Malware Protection - File Reputation and Analysis**
- Klik op de knop **Enable** op **Advanced Malware Protection** Global Settings:



- **Doe** je wijzigingen.

Pas de mondiale instellingen voor Advanced Malware Protection (AMP) aan

- AMP is nu ingeschakeld en klik op **Global Settings** om de mondiale instellingen aan te passen.
- De lijst met bestandsextensies wordt van tijd tot tijd automatisch bijgewerkt, dus ga altijd naar deze instelling en controleer of alle bestandsextensies zijn geselecteerd:



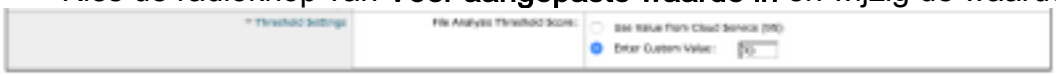
- **Geavanceerde instellingen** uitvouwen **voor bestandsomzetting**
- De standaardselectie voor File Reputation Server is **AMERICA (cloud-sa.amp.cisco.com)**
- Klik op het vervolgkeuzemenu en kies de dichtstbijzijnde File Reputation Server (met name voor APJC- en EUROPE-klanten):

- **Geavanceerde instellingen** uitvouwen **voor bestandsanalyse**
- De standaardselectie voor de URL van de server voor bestandanalyse is **AMERIKAS** (**https://panacea.threatgrid.com**)
- Klik op het vervolgkeuzemenu en kies de dichtstbijzijnde File Reputation Server (met name voor klanten uit EUROPA):

Drempelinstelling voor bestandsanalyse

(Optioneel) U mag de bovenste drempelwaarde voor de acceptabele score voor bestandsanalyse instellen. De bestanden die geblokkeerd zijn op basis van de drempelinstellingen worden weergegeven als Aangepaste drempel in het gedeelte Inkomende Malware Threat Files van het Advanced Malware Protection-rapport.

- In de globale instellingspagina van AMP, uitvouwt u **Drempel** Instellingen.
- De standaardwaarde van de cloudservice is **95**.
- Kies de radioknop van **Voer aangepaste waarde in** en wijzig de waarde (bijvoorbeeld 70):



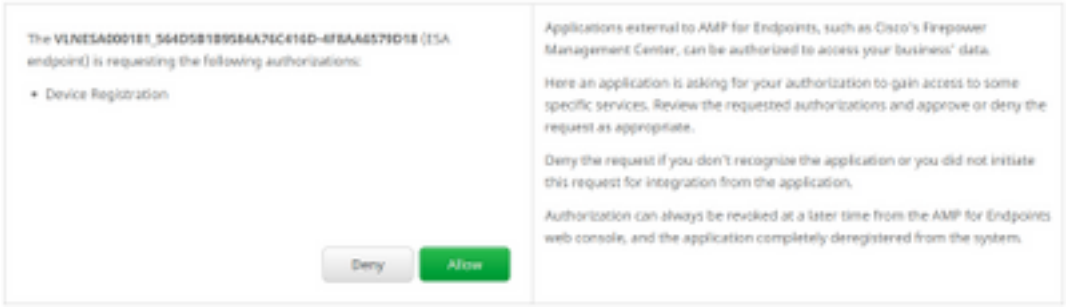
- Klik op **Inzenden en** Commiteer de wijzigingen

ESA met AMP integreren voor endpoints

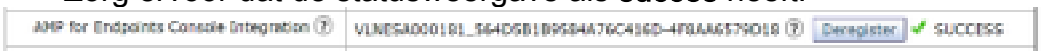
(Alleen voor klanten van AMP voor endpoints) Een verenigde aangepaste bestands blokklist (of een lijst met bestandstypes) kan via de AMP voor Endpoints console worden gemaakt en kan de containment-strategie naadloos verdelen over de security architectuur, inclusief de ESA.

- Wilt u in de globale instellingspagina van AMP **geavanceerde instellingen voor bestandsreputatie** uitvouwen**?**
- Klik op deze knop - **Registreer applicatie met AMP voor endpoints**:

- Klik op **OK** om de AMP voor Endpoints-console opnieuw te richten om de registratie te voltooien.
- Meld u aan bij de Advanced Malware Protection voor endpoints en uw gebruikersvertrouwen
- Klik op **Toestaan** voor het autoriseren van de ESR-registratie:



- De AMP voor Endpoints-console voert de pagina automatisch terug naar ESA.
- Zorg ervoor dat de statusweergave als **succes** heeft:



- Klik op **Inzenden** en **Commiteer** uw wijzigingen

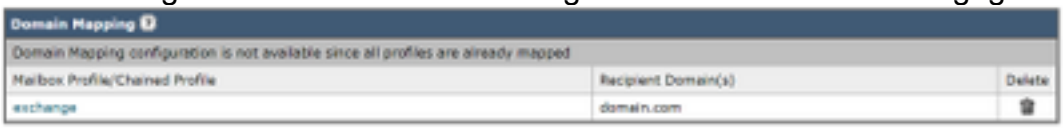
Auto-revisie van postbus inschakelen (MAR)

Als u O365-mailboxen hebt voor Microsoft Exchange 2013/2016, wordt de optie Auto Remediation (MAR) van de postbus ingeschakeld om de actie uit te voeren wanneer het vonnis over de bestands reputatie verandert van Clean/Onbekend naar kwaadaardig.

- Navigeren in naar **systeembeheer > accountinstellingen**
- Klik onder **Accountprofiel** op **Accountprofiel maken** om een API-verbindingsprofiel te maken met de mailboxen van uw Office 365 en/of Microsoft Exchange:

- Klik op **Inzenden** en **Commiteer** uw wijzigingen

- (Optioneel) Profiel gekoppeld is een verzameling profielen, u vormt alleen een gekoppeld profiel wanneer de rekeningen die u wilt benaderen, afkomstig zijn van verschillende huurders van verschillende implementaties.
- Klik op de knop **Domain mapping** om uw accountprofiel met het ontvangende domein in kaart te brengen. De aanbevolen instellingen worden hieronder weergegeven:



- Klik op **Inzenden** en **Commiteer** uw wijzigingen

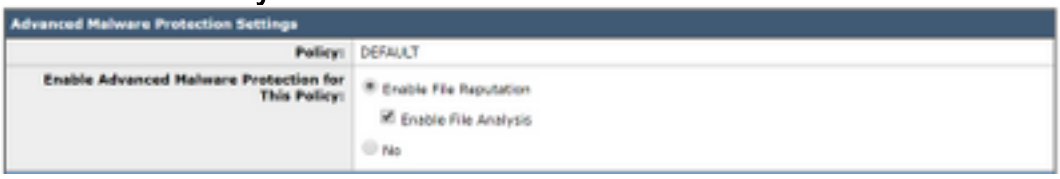
Advanced Malware Protection (AMP) configureren in e-mailbeleid

Nadat AMP en MAR mondiaal zijn geconfigureerd kunt u de services nu in staat stellen om beleid te mailen.

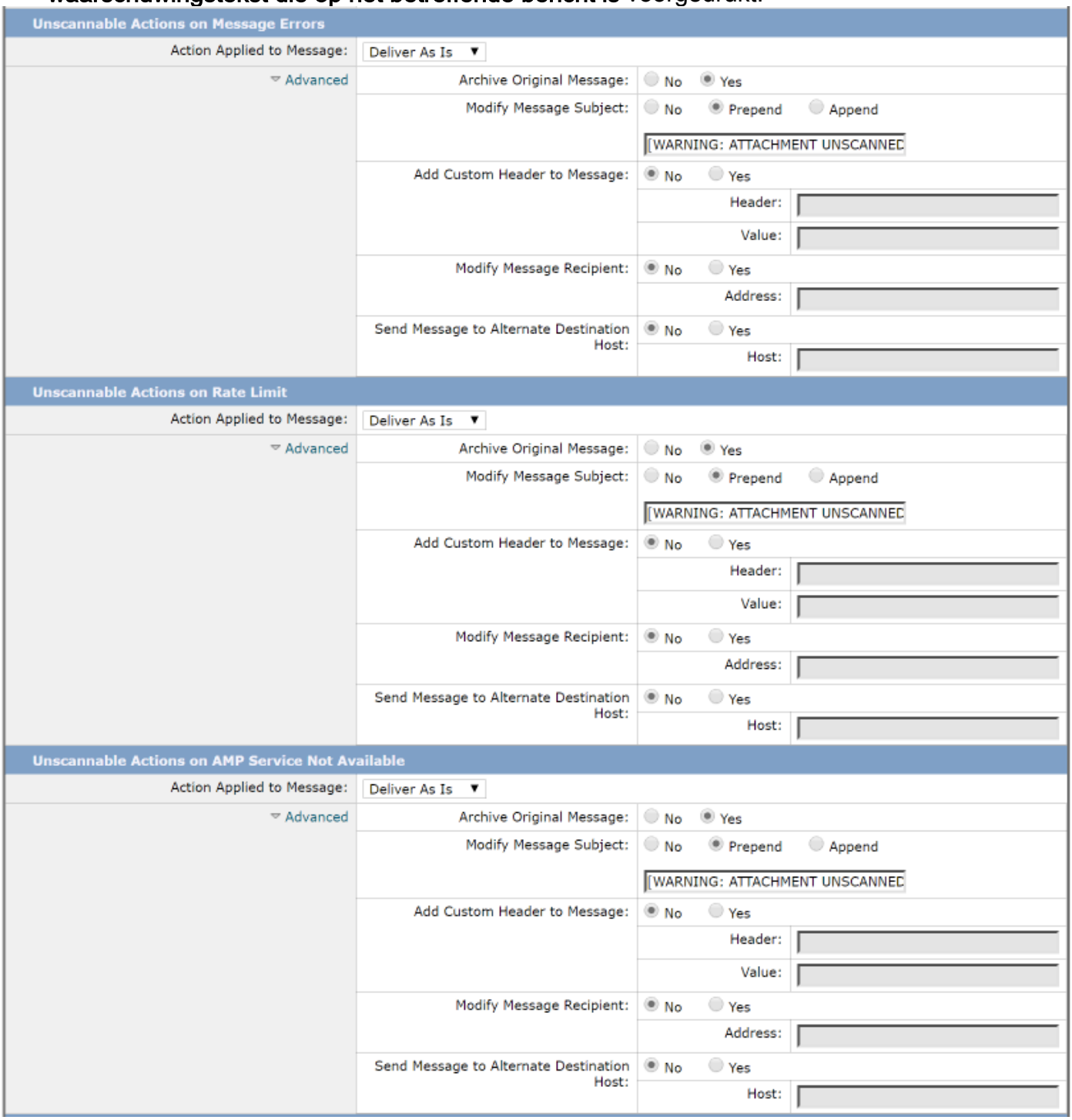
- Navigeren in op **e-mailbeleid > Inkomend postbeleid**
- Pas de instellingen voor **Advanced Malware Protection** aan voor een inkomende e-mailbeleid door op de blauwe link onder **Advanced Malware Protection** te klikken voor het beleid dat u

wilt aanpassen.

- Klik voor dit best practice-document op de radioknop naast **Bestand uploaden** en selecteer **Bestandsanalyse inschakelen**:

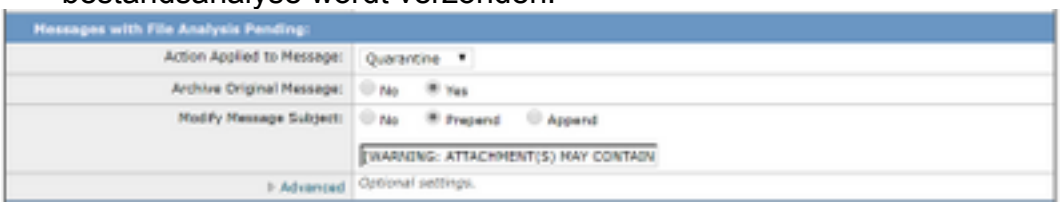


- Aanbevolen wordt om **een X-header met het AMP-resultaat op te nemen in een bericht**.
- Met de volgende drie secties kunt u de actie selecteren die de ESA moet uitvoeren als een bijlage als niet-scannbaar wordt beschouwd als gevolg van berichtfouten, tariefbeperkingen of als de AMP-service niet beschikbaar is. De aanbevolen actie is om **AS-is** te leveren **met waarschuwingstekst die op het betreffende bericht is** voorgedrukt:

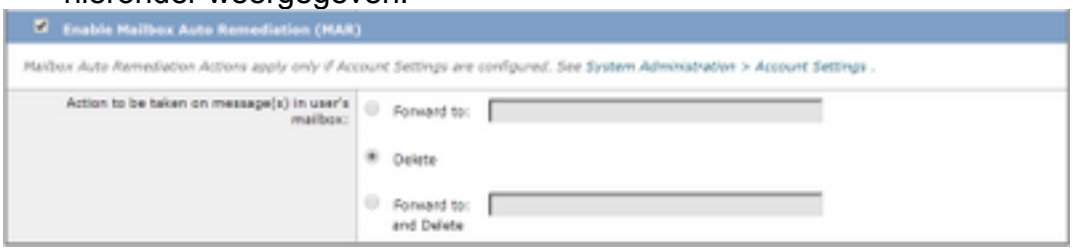


- De volgende sectie vormt de ESA om het bericht te laten vallen als een bijlage wordt geacht kwaadaardig te zijn:

- De aanbevolen actie is om het bericht in quarantaine te plaatsen als de bijlage voor bestandsanalyse wordt verzonden:



- (Alleen voor inkomend postbeleid) Configureer de corrigerende acties die moeten worden uitgevoerd op het bericht dat aan de eindgebruikers wordt geleverd wanneer het bedreigingsvonnis in kwaadwillige vorm verandert. De aanbevolen instellingen worden hieronder weergegeven:

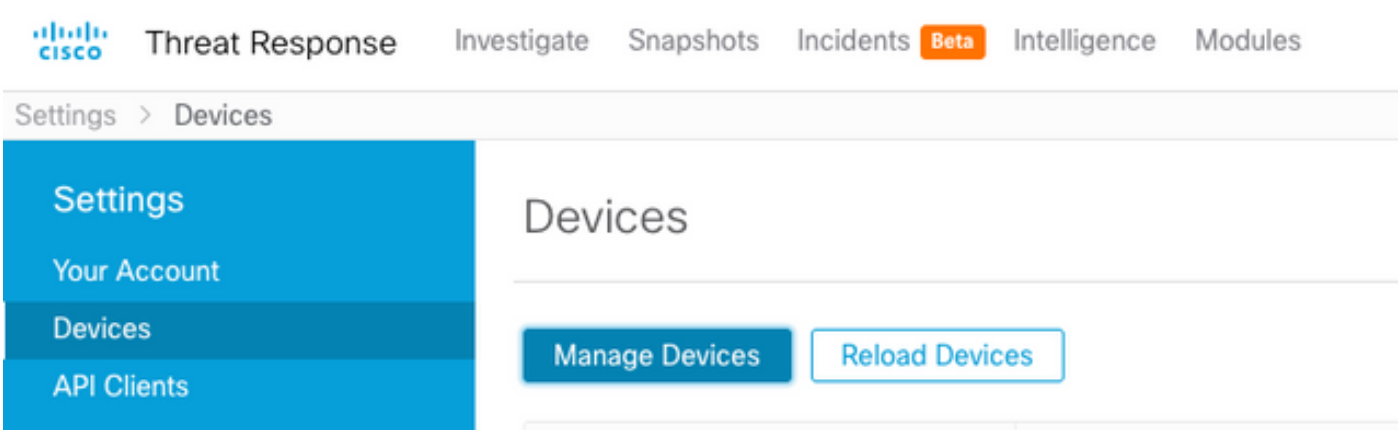


- Klik op **Inzenden** en **Commiteer** uw wijzigingen

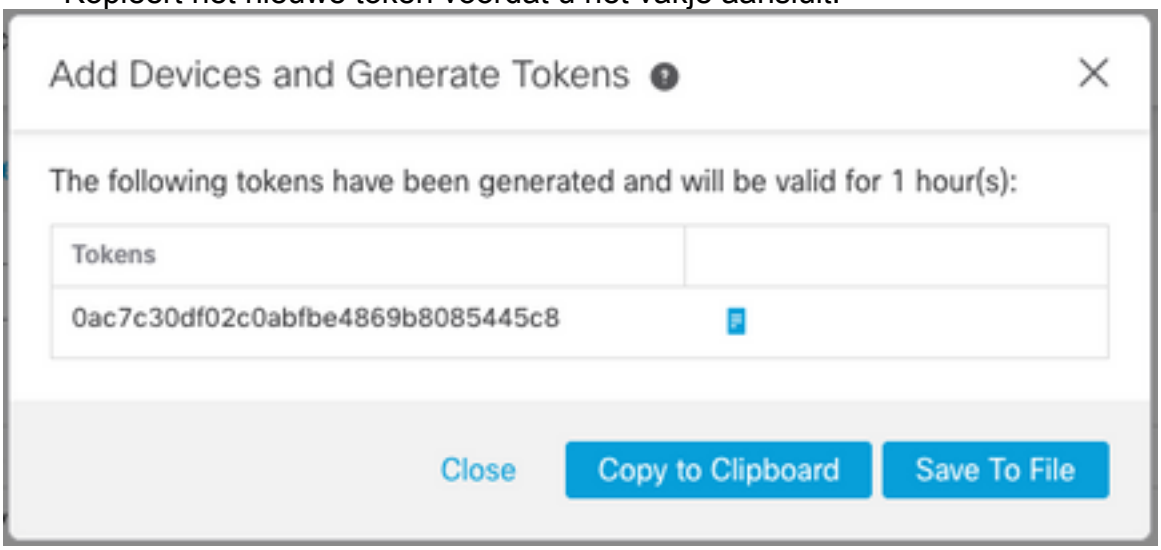
SMA integreren met Cisco Threat Response (CTR)

De integratie van een SMA Email Module vereist het gebruik van de Security Services Exchange (SSE) via CTR. SSE staat een SMA toe om met de Exchange te registreren en u verstrekt expliciete toestemming voor Cisco Threat Response om toegang tot de geregistreerde apparaten te krijgen. Het proces betreft het koppelen van uw SMA aan SSE via een token die gegenereerd wordt wanneer u klaar bent om het te verbinden.

- Op het CTR portal (https://visibility.amp.cisco.com), log in met uw gebruikersreferenties.
- CTR gebruikt een module om te integreren met andere Cisco security producten waaronder ESA. Klik op het tabblad **Modules**.
- Kies **Apparaten** en klik op **Apparaten beheren:**



- CTR zal de pagina naar SSE draaien.
- Klik op het pictogram **+** om een nieuw token op te halen en klik op **Doorgaan**.
- Kopieert het nieuwe token voordat u het vakje aansluit:

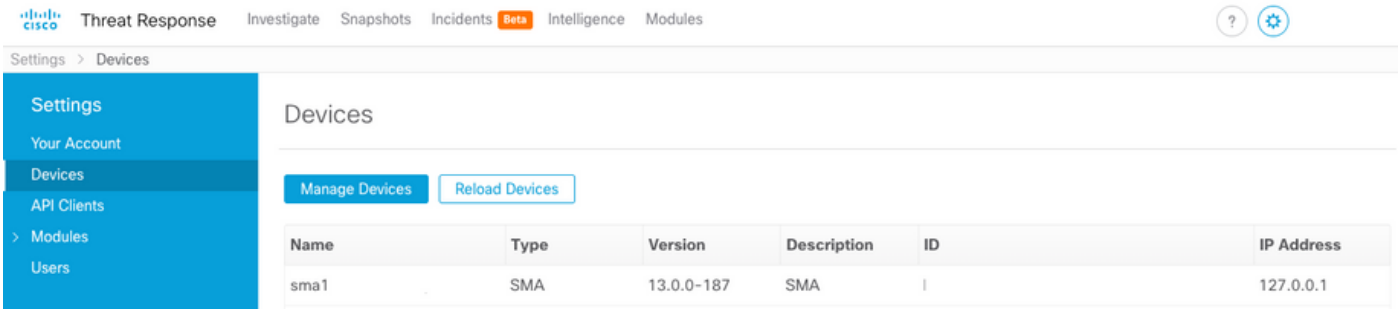


- Raadpleeg in uw SMA **het** tabblad **Management-applicaties > Network > Cloud Service-instellingen**
- Klik op **Instellingen bewerken** en zorg ervoor dat de optie Threat Response **is ingeschakeld**.
- De standaardselectie voor de URL van de Threat Response Server is **AMERICAS (api-sse.cisco.com).** Voor klanten van EUROPA klik op het vervolgkeuzemenu en kies **EUROPA (api.eu.sse.itd.cisco.com)**:

- Klik op **Inzenden** en **Commit** uw wijzigingen
- Plakt de Token-toets (die u vanuit het CTR-portal hebt gegenereerd) in de Cloud Services-instelling en klik op **Registreren**:

- Het duurt even om het registratieproces te voltooien. navigeer na een paar minuten terug naar deze pagina om de status opnieuw te controleren.
- Ga terug naar **CTR > Modules > Apparaat** en klik op de knop **Opnieuw laden** om er zeker van

te zijn dat het SMA in de lijst staat:



Conclusie

Dit document is bedoeld om de standaard- of best practice-configuraties te beschrijven voor Cisco Advanced Malware Protection (AMP) in de e-mail security applicatie. De meeste van deze instellingen zijn beschikbaar op zowel het inkomende als het uitgaande e-mailbeleid, en de configuratie en het filteren worden in beide richtingen aanbevolen.