Integrazione di AMP for Endpoints and Threat Grid con WSA

Sommario

Introduzione

In questo documento viene descritta la procedura per integrare Advanced Malware Protection (AMP) per gli endpoint e Threat Grid (TG) con Web Security Appliance (WSA).

Contributo di Uriel Montero e modificato da Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AMP for endpoints access
- TG premium access
- WSA con analisi dei file e chiavi delle funzionalità di reputazione dei file

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Console cloud pubblica AMP
- GUI WSA
- Console TG

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, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

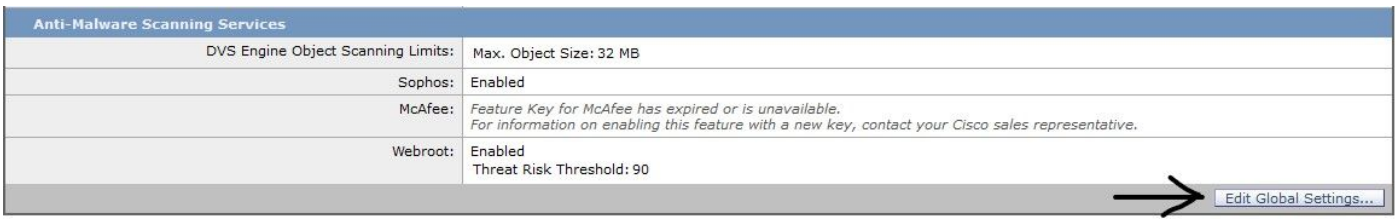
Configurazione

Accedere alla console WSA.

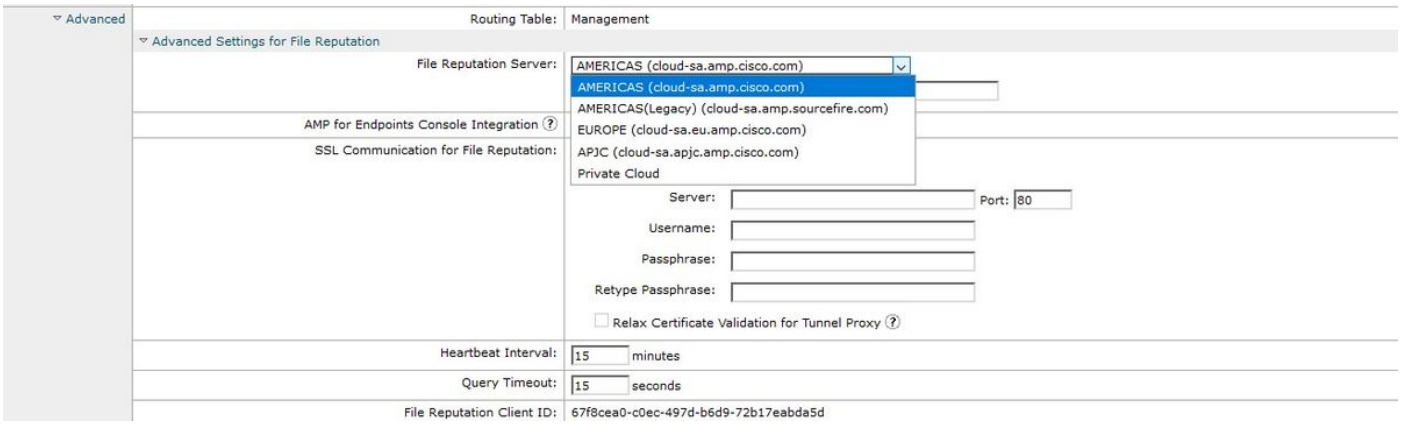
Una volta eseguito l'accesso, selezionare **Security Services > Anti-Malware and Reputation** (Servizi di sicurezza > Antimalware e reputazione). In questa sezione sono disponibili le opzioni per l'integrazione di AMP e TG.

Integrazione AMP

Nella sezione Servizi di scansione antimalware fare clic su **Modifica impostazioni globali**, come mostrato nell'immagine.

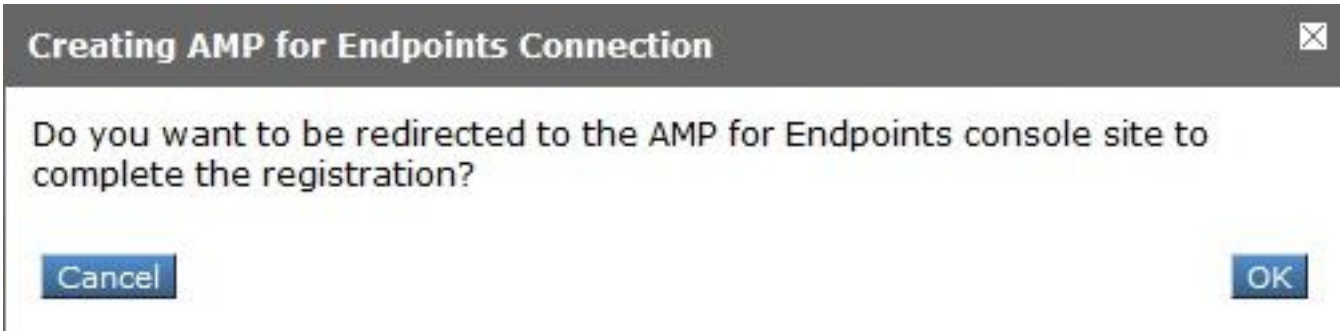


Cercare la sezione **Avanzate > Impostazioni avanzate per la reputazione del file** ed espanderla, quindi vengono visualizzate una serie di opzioni di server cloud, scegliere la posizione più vicina.

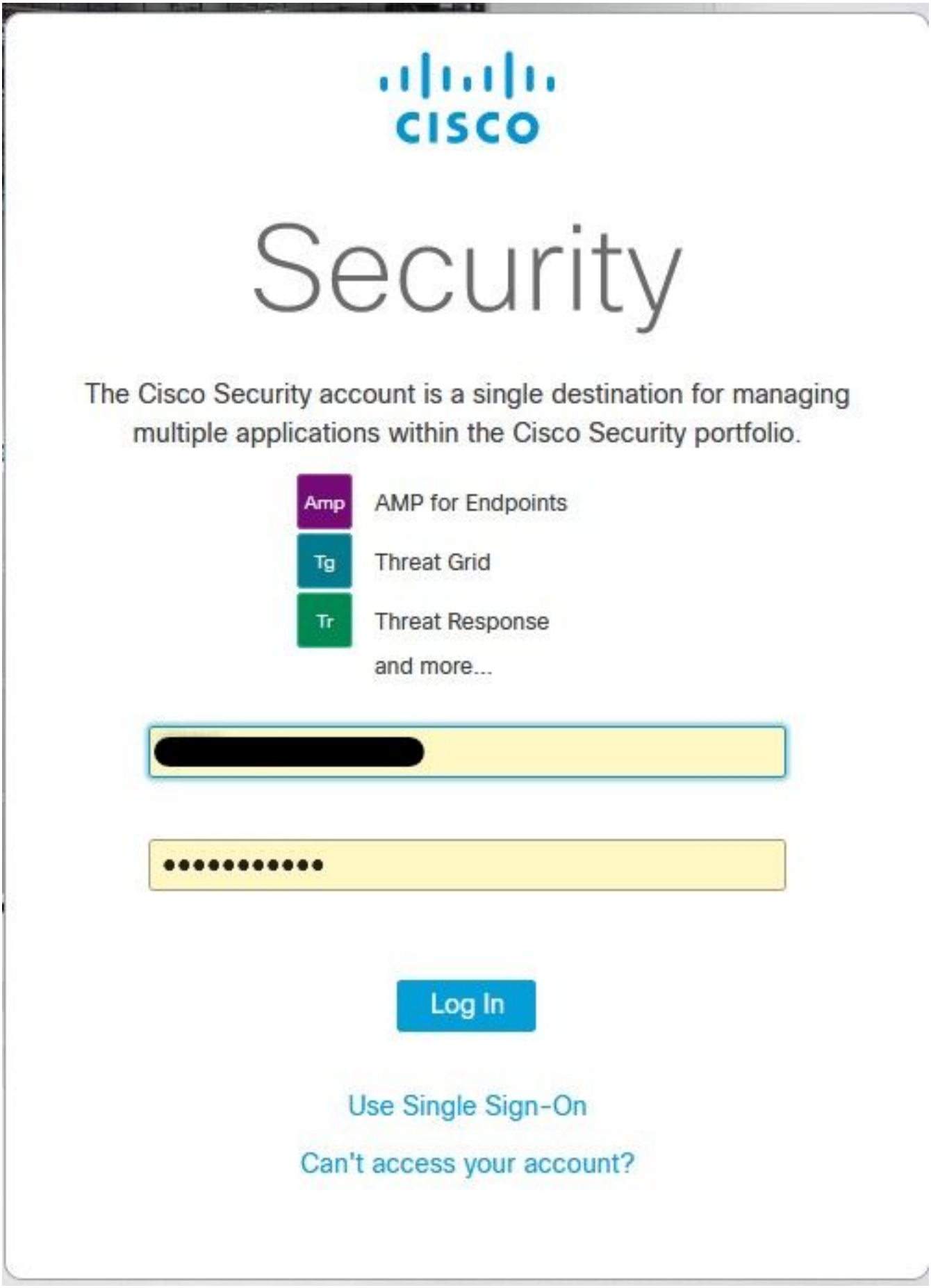


Una volta selezionato il cloud, fare clic sul pulsante **Register Appliance with AMP for Endpoints**.

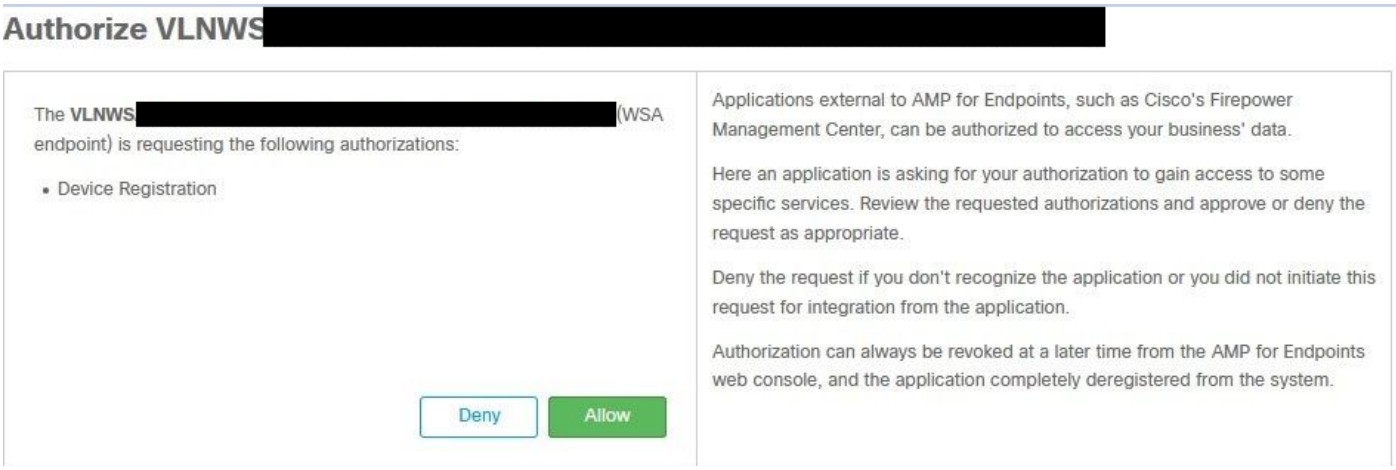
Viene visualizzata una schermata di popup che reindirizza alla console AMP, fare clic sul **pulsante OK,** come mostrato nell'immagine.



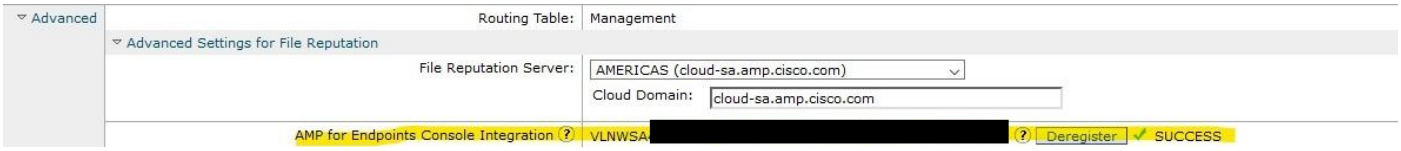
Ènecessario immettere le credenziali AMP valide e fare clic su **Log In,** come mostrato nell'immagine.



Accettare Device Registration (Registrazione dispositivo), prendere nota dell'ID client, in quanto aiuta a trovare il WSA più avanti sulla console.



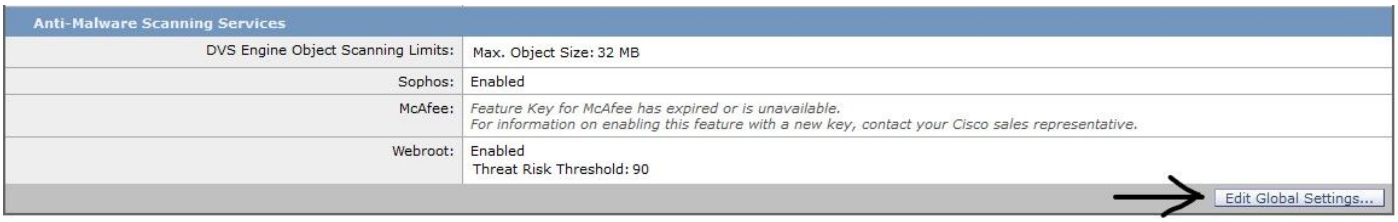
Tornando alla console WSA, viene visualizzato un segno di spunta nella sezione Integrazione console Amp for Endpoints, come mostrato nell'immagine.



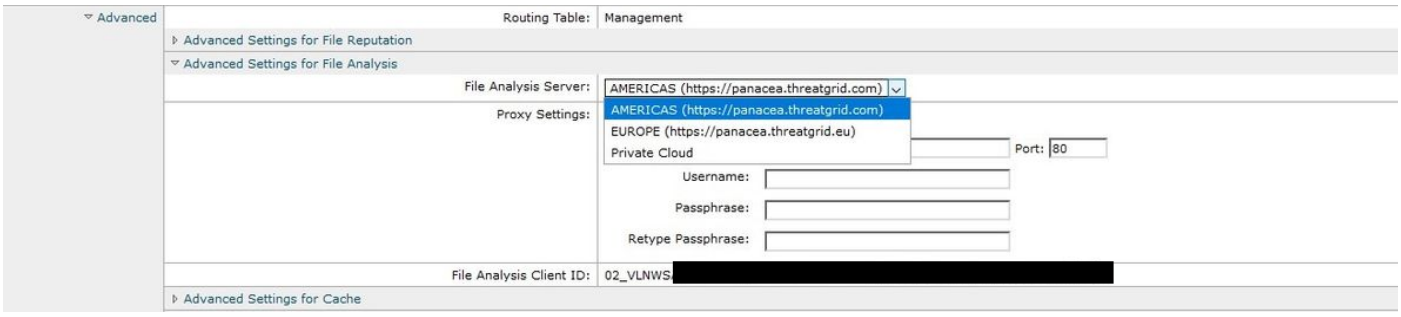
> **Nota**: non dimenticare di fare clic su **Invia** e **Conferma** le modifiche (se richiesto), altrimenti il processo deve essere eseguito nuovamente.

Integrazione Threat Grid

Selezionare **Security Services > Anti-Malware and Reputation** (Servizi di sicurezza > Antimalware e reputazione), quindi in Anti-Malware Protection Services (Servizi di protezione antimalware), fare clic sul pulsante **Edit Global Settings** (Modifica impostazioni globali), come mostrato nell'immagine.

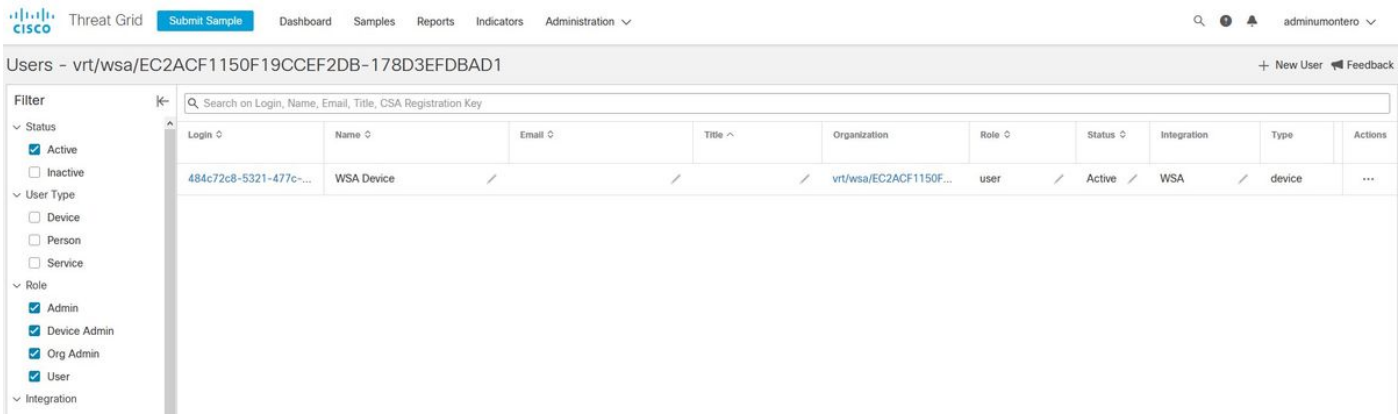


Cercare la sezione **Advanced> Advanced Settings for File Analysis** ed espanderla, scegliere l'opzione più vicina alla propria posizione, come mostrato nell'immagine.



Fare clic su **Submit** (Invia) e **Commit** delle modifiche.

Sul portale TG, cercare il dispositivo WSA nella scheda Utenti se l'accessorio è stato integrato con AMP/TG.



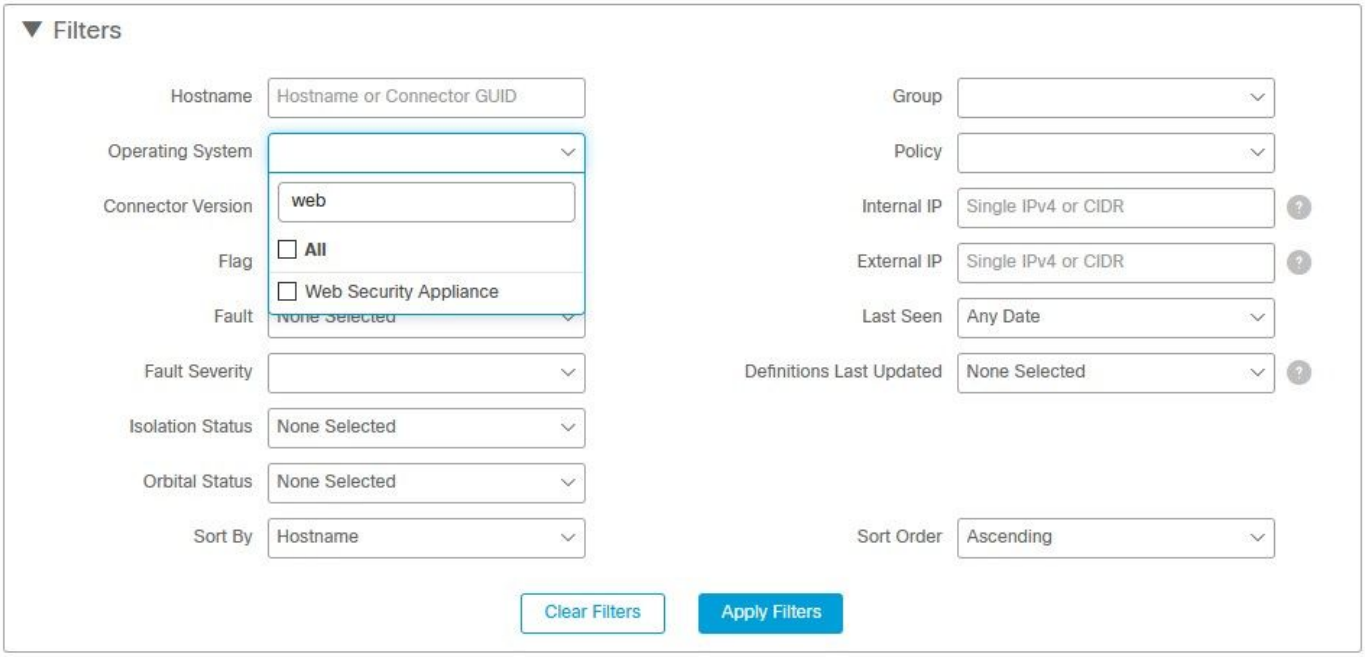
Se si fa clic su Login, è possibile accedere alle informazioni di tale accessorio.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

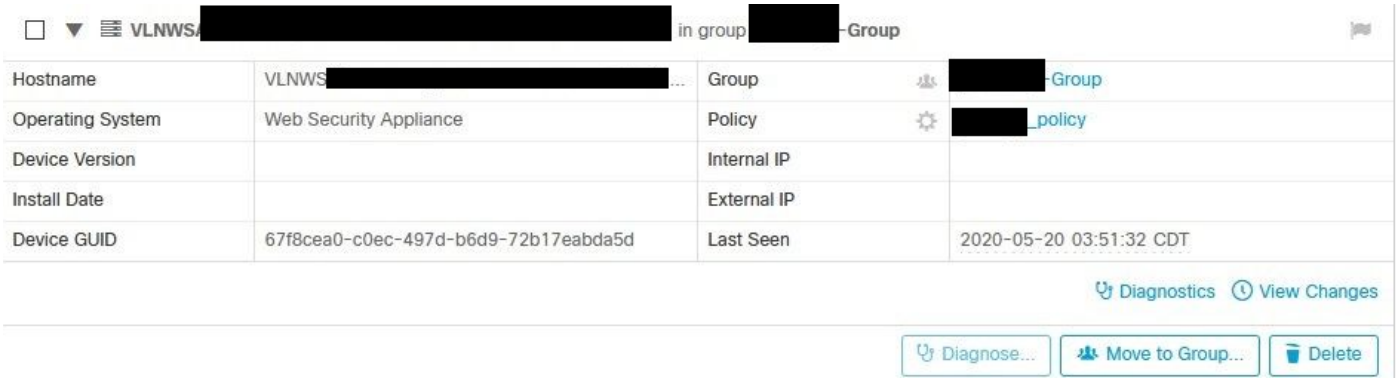
Per verificare che l'integrazione tra AMP e WSA abbia esito positivo, è possibile accedere alla console AMP e cercare il dispositivo WSA.

Passare a **Gestione > Computer**, nella sezione filtri cercare **Web Security Appliance** e applicare il filtro

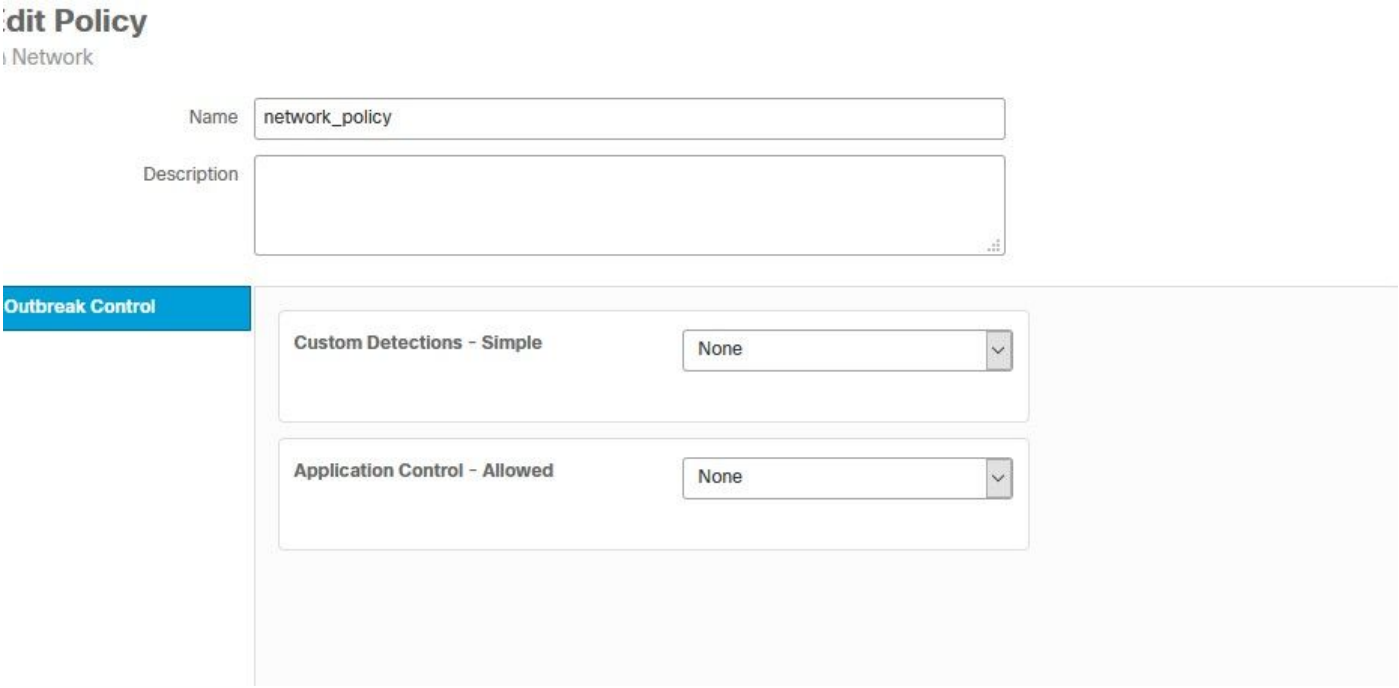


Se sono stati registrati più dispositivi WSA, è possibile identificarli con l'ID del client di analisi dei file.

Se si espande la periferica, è possibile vedere a quale gruppo appartiene, il criterio applicato e il GUID della periferica possono essere utilizzati per visualizzare la traiettoria della periferica.



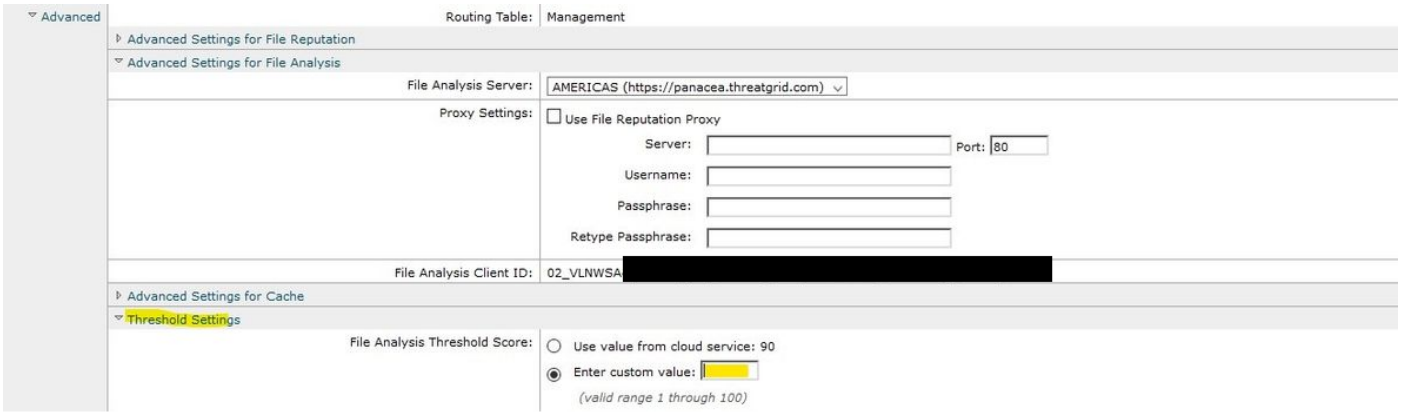
Nella sezione dei criteri è possibile configurare Rilevamenti personalizzati semplici e Controllo applicazione - Consentito che viene applicato al dispositivo.



Per visualizzare la sezione Traiettoria periferica di WSA, è necessario aprire la sezione Traiettoria periferica di un altro computer e utilizzare il GUID della periferica.

La modifica viene applicata all'URL, come mostrato nelle immagini.

Per Threat Grid, è prevista una soglia di 90; se un file ottiene un punteggio inferiore a tale numero, il file non è dannoso, tuttavia, è possibile configurare una soglia personalizzata sul WSA.



Risoluzione dei problemi

WSA non reindirizza alla pagina AMP

- Verificare che il firewall consenta gli indirizzi richiesti per AMP, fare clic qui.
- Accertarsi di aver selezionato il cloud AMP appropriato (evitare di scegliere il cloud legacy).

WSA non blocca gli Agenti integrità sistema specificati

- Verificare che il server WSA si trovi nel gruppo corretto.
- Assicurarsi che il WSA utilizzi i criteri corretti.
- Assicurarsi che l'Agente integrità sistema non sia pulito nel cloud, altrimenti WSA non sarà in grado di bloccarlo.

WSA non viene visualizzato nell'organizzazione TG

- Accertarsi di aver selezionato il cloud TG appropriato (Americhe o Europa).
- Assicurarsi che il firewall consenta gli indirizzi richiesti per TG.
- Prendere nota dell'ID del client di analisi file.
- Cercarlo nella sezione Utenti.
- Se non lo trovi, contatta il supporto Cisco in modo che possa aiutarti a spostarlo tra le organizzazioni.