

# Integration von AMP für Endgeräte und Threat Grid mit der WSA

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[AMP-Integration](#)

[Threat Grid-Integration](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[WSA leitet nicht zur AMP-Seite um](#)

[Die WSA blockiert die angegebenen SHAs nicht.](#)

[WSA wird in meiner TG-Organisation nicht angezeigt.](#)

## Einführung

Dieses Dokument beschreibt die Schritte zur Integration von Advanced Malware Protection (AMP) für Endgeräte und Threat Grid (TG) in die Web Security Appliance (WSA).

Verfasst von Uriel Montero und herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AMP für Endgerätezugriff
- TG Premium-Zugriff
- WSA mit Feature-Schlüsseln für Dateianalyse und Dateireputation

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- AMP Public Cloud-Konsole
- WSA-Benutzeroberfläche
- TG-Konsole

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 eines Befehls verstehen.

## Konfigurieren

Melden Sie sich bei der WSA-Konsole an.




Wenn Sie sich angemeldet haben, navigieren Sie zu **Security Services > Anti-Malware and Reputation**. In diesem Abschnitt finden Sie Optionen zur Integration von AMP und TG.

### AMP-Integration

Klicken Sie im Bereich Anti-Malware Scanning Services auf **Globale Einstellungen bearbeiten**, wie im Bild gezeigt.

| Anti-Malware Scanning Services     |  |
|------------------------------------|--|
| DVS Engine Object Scanning Limits: | Max. Object Size: 32 MB  |
| Sophos:                            | Enabled  |
| McAfee:                            | <i>Feature Key for McAfee has expired or is unavailable.<br/>For information on enabling this feature with a new key, contact your Cisco sales representative.</i> |
| Webroot:                           | Enabled<br>Threat Risk Threshold: 90   |

 [Edit Global Settings...](#)

Suchen Sie nach dem Abschnitt **Erweitert > Erweiterte Einstellungen für Dateireputation**, und erweitern Sie diesen. Dann werden eine Reihe von Cloud-Serveroptionen angezeigt, und wählen Sie die Ihrem Standort am nächsten gelegene aus.

|   |  |
|---|--|
| Advanced                                | Routing Table: Management  |
| Advanced Settings for File Reputation   | File Reputation Server: AMERICAS (cloud-sa.amp.cisco.com)                |
|   | AMERICAS (cloud-sa.amp.cisco.com)  |
| AMP for Endpoints Console Integration ? | AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com)                           |
|   | EUROPE (cloud-sa.eu.amp.cisco.com)                                       |
| SSL Communication for File Reputation:  | APJC (cloud-sa.apjc.amp.cisco.com)                                       |
|   | Private Cloud  |
|   | Server: <input type="text"/> Port: 80                                    |
|   | Username: <input type="text"/>   |
|   | Password: <input type="text"/>   |
|   | Retype Password: <input type="text"/>                                    |
|   | <input type="checkbox"/> Relax Certificate Validation for Tunnel Proxy ? |
| Heartbeat Interval:                     | 15 minutes   |
| Query Timeout:                          | 15 seconds   |
| File Reputation Client ID:              | 67f8cea0-c0ec-497d-b6d9-72b17eabda5d                                     |

Nachdem die Cloud ausgewählt wurde, klicken Sie auf die Schaltfläche **Einheit mit AMP für Endgeräte registrieren**.

Es wird ein Popup angezeigt, das zur AMP-Konsole umgeleitet wird. Klicken Sie auf die **Schaltfläche OK**, wie im Bild gezeigt.

### Creating AMP for Endpoints Connection ✕

Do you want to be redirected to the AMP for Endpoints console site to complete the registration?

Sie müssen gültige AMP-Anmeldeinformationen eingeben und auf **Anmelden** klicken, wie im Bild gezeigt.



# Security

The Cisco Security account is a single destination for managing multiple applications within the Cisco Security portfolio.

-  AMP for Endpoints
-  Threat Grid
-  Threat Response  
and more...

[Log In](#)

[Use Single Sign-On](#)

[Can't access your account?](#)

Akzeptieren Sie die Geräteregistrierung. Notieren Sie sich die Client-ID, da die WSA später auf der Konsole gefunden werden kann.

## Authorize VLNWS

The VLNWS (WSA endpoint) is requesting the following authorizations:

- Device Registration

Applications external to AMP for Endpoints, such as Cisco's Firepower Management Center, can be authorized to access your business' data.

Here an application is asking for your authorization to gain access to some specific services. Review the requested authorizations and approve or deny the request as appropriate.

Deny the request if you don't recognize the application or you did not initiate this request for integration from the application.

Authorization can always be revoked at a later time from the AMP for Endpoints web console, and the application completely deregistered from the system.

Kehren Sie zur WSA-Konsole zurück. Wie im Bild gezeigt, wird im Abschnitt AMP für Endpoints-Konsolenintegration ein Häkchen angezeigt.

Advanced Routing Table: Management

Advanced Settings for File Reputation

File Reputation Server: AMERICAS (cloud-sa.amp.cisco.com)

Cloud Domain: cloud-sa.amp.cisco.com

AMP for Endpoints Console Integration ? VLNWS ? Deregister ✓ SUCCESS

**Hinweis:** Vergessen Sie nicht, auf **Senden** und **Bestätigen** der Änderungen zu klicken (wenn Sie dazu aufgefordert werden). Andernfalls muss der Vorgang erneut durchgeführt werden.

## Threat Grid-Integration

Navigieren Sie zu **Sicherheitsdienste > Anti-Malware und Reputation**, und klicken Sie dann auf **Anti-Malware Protection Services (Anti-Malware-Schutzdienste)**, und klicken Sie auf die Schaltfläche **Edit Global Settings (Globale Einstellungen bearbeiten)**, wie im Bild gezeigt.

Anti-Malware Scanning Services

|                                    |  |
|------------------------------------|--|
| DVS Engine Object Scanning Limits: | Max. Object Size: 32 MB  |
| Sophos:                            | Enabled  |
| McAfee:                            | Feature Key for McAfee has expired or is unavailable.<br>For information on enabling this feature with a new key, contact your Cisco sales representative. |
| Webroot:                           | Enabled<br>Threat Risk Threshold: 90   |

Suchen Sie nach dem Abschnitt **Erweitert > Erweiterte Einstellungen für Dateianalyse**, und erweitern Sie ihn, und wählen Sie die Option aus, die Ihrem Speicherort am nächsten liegt, wie im Bild gezeigt.

Advanced Routing Table: Management

Advanced Settings for File Reputation

Advanced Settings for File Analysis

File Analysis Server: AMERICAS (https://panacea.threatgrid.com)

Proxy Settings: AMERICAS (https://panacea.threatgrid.com)

EUROPE (https://panacea.threatgrid.eu) Private Cloud Port: 80

Username:

Passphrase:

Retype Passphrase:

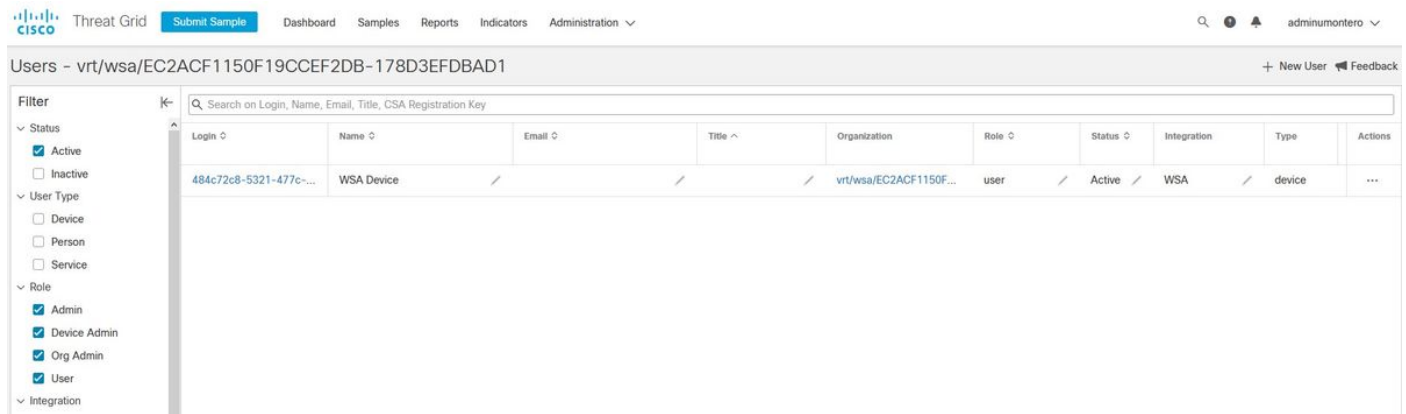
File Analysis Client ID: 02\_VLNWS

Advanced Settings for Cache

Klicken Sie auf **Senden** und **Bestätigen** der Änderungen.

Suchen Sie auf der Seite des TG-Portals unter der Registerkarte Benutzer nach dem WSA-Gerät,

wenn die Appliance erfolgreich in AMP/TG integriert wurde.



Wenn Sie auf "Anmelden" klicken, können Sie auf die Informationen dieser Appliance zugreifen.

## Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Um zu überprüfen, ob die Integration zwischen AMP und WSA erfolgreich ist, können Sie sich bei der AMP-Konsole anmelden und nach Ihrem WSA-Gerät suchen.

Navigieren Sie zu **Management > Computers**, suchen Sie im Abschnitt "Filter" nach der **Websicherheits-Appliance**, und wenden Sie den Filter an.

The screenshot shows the 'Filters' section of the Cisco Threat Grid interface. It contains several filter fields: Hostname (text input), Operating System (dropdown), Connector Version (text input with 'web' entered), Flag (checkboxes for 'All' and 'Web Security Appliance'), Fault (dropdown), Fault Severity (dropdown), Isolation Status (dropdown), Orbital Status (dropdown), Sort By (dropdown), Group (dropdown), Policy (dropdown), Internal IP (text input), External IP (text input), Last Seen (dropdown), Definitions Last Updated (dropdown), and Sort Order (dropdown). At the bottom, there are 'Clear Filters' and 'Apply Filters' buttons.

Wenn Sie mehrere WSA-Geräte registriert haben, können Sie diese mithilfe der Datei-Analyse-Client-ID identifizieren.

Wenn Sie das Gerät erweitern, sehen Sie, zu welcher Gruppe es gehört, die angewendete Richtlinie und die Geräte-GUID können zum Anzeigen des Device Trajectory verwendet werden.

▼  VLNWSA... in group ...-Group

|                  |                                      |             |                         |
|------------------|--------------------------------------|-------------|-------------------------|
| Hostname         | VLNWSA...                            | Group       | ...-Group               |
| Operating System | Web Security Appliance               | Policy      | ..._policy              |
| Device Version   |                                      | Internal IP |                         |
| Install Date     |                                      | External IP |                         |
| Device GUID      | 67f8cea0-c0ec-497d-b6d9-72b17eabda5d | Last Seen   | 2020-05-20 03:51:32 CDT |

[Diagnostics](#) [View Changes](#)

[Diagnose...](#) [Move to Group...](#) [Delete](#)

Im Richtlinienabschnitt können Sie Simple Custom Detections (Einfache benutzerdefinierte Erkennung) und Application Control (Anwendungskontrolle - Zulässig) konfigurieren, die auf das Gerät angewendet werden.

## dit Policy

Network

Name

Description

### Outbreak Control

Custom Detections - Simple

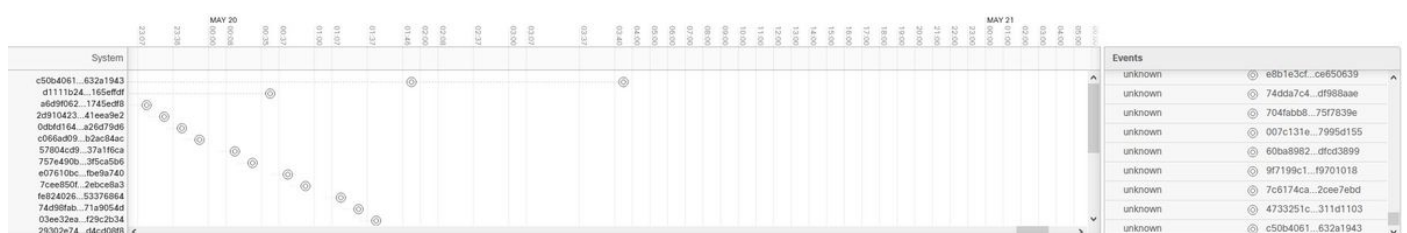
Application Control - Allowed

Es gibt einen Trick, den Abschnitt Device Trajectory der WSA anzuzeigen. Sie müssen die Device Trajectory eines anderen Computers öffnen und die Geräte-GUID verwenden.

Die Änderung wird auf den URL angewendet, wie in den Bildern gezeigt.

<https://console.amp.cisco.com/computers/c359f0b9-b4be-4071-9570-7d10c50df5bd/trajectory2>

<https://console.amp.cisco.com/computers/67f8cea0-c0ec-497d-b6d9-72b17eabda5d/trajectory2>



Für Threat Grid gibt es einen Schwellenwert von 90. Wenn eine Datei eine Bewertung unter dieser Nummer erhält, ist die Datei nicht schädlich. Sie können jedoch einen benutzerdefinierten Grenzwert auf der WSA konfigurieren.

Advanced Routing Table: Management

Advanced Settings for File Reputation

Advanced Settings for File Analysis

File Analysis Server: AMERICAS (https://panacea.threatgrid.com) ▾

Proxy Settings:  Use File Reputation Proxy

Server:  Port:

Username:

Passphrase:

Retype Passphrase:

File Analysis Client ID: 02\_VLNWSA XXXXXXXXXX

Advanced Settings for Cache

Threshold Settings

File Analysis Threshold Score:  Use value from cloud service: 90

Enter custom value:

(valid range 1 through 100)

## Fehlerbehebung

### WSA leitet nicht zur AMP-Seite um

- Stellen Sie sicher, dass die Firewall die erforderlichen Adressen für AMP bereitstellt. Klicken Sie [hier](#).
- Stellen Sie sicher, dass Sie die richtige AMP-Cloud ausgewählt haben (vermeiden Sie die Wahl der Legacy-Cloud).

### Die WSA blockiert die angegebenen SHAs nicht.

- Stellen Sie sicher, dass Ihre WSA in der richtigen Gruppe ist.
- Stellen Sie sicher, dass Ihre WSA die richtigen Richtlinien verwendet.
- Stellen Sie sicher, dass die SHA nicht in der Cloud sauber ist. Andernfalls kann die WSA sie nicht blockieren.

### WSA wird in meiner TG-Organisation nicht angezeigt.

- Stellen Sie sicher, dass Sie die richtige TG-Cloud (Nord- und Südamerika oder Europa) ausgewählt haben.
- Stellen Sie sicher, dass die Firewall die erforderlichen Adressen für TG zulässt.
- Notieren Sie sich die File Analysis Client-ID.
- Suchen Sie im Abschnitt "Benutzer" danach.
- Wenn Sie es nicht finden, wenden Sie sich bitte an den Cisco Support, damit dieser Ihnen beim Umzug zwischen verschiedenen Organisationen behilflich sein kann.