

Intégrer AMP for Endpoints and Threat Grid à WSA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Intégration AMP](#)

[Intégration de Threat Grid](#)

[Vérification](#)

[Dépannage](#)

[WSA ne redirige pas vers la page AMP](#)

[WSA ne bloque pas les SHA spécifiés](#)

[WSA n'apparaît pas sur mon organisation TG](#)

Introduction

Ce document décrit les étapes à suivre pour intégrer Advanced Malware Protection (AMP) pour les terminaux et Threat Grid (TG) avec l'appareil de sécurité Web (WSA).

Contribué par Uriel Montero et édité par Yeraldin Sanchez, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- AMP pour l'accès aux terminaux
- Accès Premium TG
- WSA avec clés de fonction d'analyse de fichiers et de réputation de fichiers

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console de cloud public AMP
- Interface utilisateur WSA
- Console TG

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Connectez-vous à la console WSA.



Une fois connecté, accédez à **Security Services > Anti-Malware and Reputation**, dans cette section vous trouverez les options d'intégration d'AMP et TG.

Intégration AMP

Dans la section Anti-Malware Scanning Services, cliquez sur **Edit Global Settings**, comme illustré dans l'image.

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. For information on enabling this feature with a new key, contact your Cisco sales representative.
Webroot:	Enabled Threat Risk Threshold: 90
 Edit Global Settings...	

Recherchez la section **Advanced > Advanced Settings for File Reputation** et développez-la, puis une série d'options de serveurs cloud s'affiche, choisissez la plus proche de votre emplacement.

Advanced	Routing Table:	Management
Advanced Settings for File Reputation		
File Reputation Server:	AMERICAS (cloud-sa.amp.cisco.com) [v] AMERICAS (cloud-sa.amp.cisco.com) AMERICAS(Legacy) (cloud-sa.amp.sourcefire.com) EUROPE (cloud-sa.eu.amp.cisco.com) APJC (cloud-sa.apjc.amp.cisco.com) Private Cloud	
AMP for Endpoints Console Integration ?		
SSL Communication for File Reputation:	Server: [] Port: [80] Username: [] Passphrase: [] Retype Passphrase: [] <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	

Une fois le cloud sélectionné, cliquez sur le bouton **Register Appliance with AMP for Endpoints**.

Une fenêtre contextuelle s'affiche et redirige vers la console AMP, cliquez sur le bouton **Ok**, comme indiqué dans l'image.

Creating AMP for Endpoints Connection ✕

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

Cancel **OK**

Vous devez saisir des informations d'identification AMP valides et cliquer sur **Se connecter**, comme indiqué dans l'image.



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?](#)

Acceptez l'enregistrement du périphérique, prenez note de l'ID du client, car il permet de trouver le WSA ultérieurement sur la console.

Authorize VLNWS [REDACTED]

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

- Device Registration

Deny Allow

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.

Revenez à la console WSA, une vérification s'affiche dans la section Amp for Endpoints Console Integration, comme illustré dans l'image.

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 [REDACTED] [?] Deregister [X] SUCCESS

Remarque : n'oubliez pas de cliquer sur **Soumettre** et **valider** les modifications (si vous y êtes invité), sinon le processus doit être recommencé.

Intégration de Threat Grid

Naviguez jusqu'à **Services de sécurité > Anti-Malware and Reputation**, puis dans les Services de protection contre les programmes malveillants, cliquez sur le bouton **Edit Global Settings**, comme illustré dans l'image.

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. For information on enabling this feature with a new key, contact your Cisco sales representative.
Webroot:	Enabled Threat Risk Threshold: 90

Edit Global Settings...

Recherchez la section **Advanced > Advanced Settings for File Analysis** et développez-la, choisissez l'option la plus proche de votre emplacement, comme illustré dans l'image.

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) Port: 80

Private Cloud

Username: [REDACTED]

Password: [REDACTED]

Retype Password: [REDACTED]

File Analysis Client ID: 02_VLNWS [REDACTED]

Advanced Settings for Cache

Cliquez sur **Soumettre** et **valider** les modifications.

Du côté du portail TG, recherchez le périphérique WSA sous l'onglet Users si l'appliance a été correctement intégrée à AMP/TG.

Threat Grid [Submit Sample](#) Dashboard Samples Reports Indicators Administration adminmontero

Users - vrt/wsa/EC2ACF1150F19CCEF2DB-178D3EFDBAD1 + New User Feedback

Filter

Login	Name	Email	Title	Organization	Role	Status	Integration	Type	Actions
484c72c8-5321-477c-...	WSA Device	/	/	vrt/wsa/EC2ACF1150F...	user	Active	WSA	device	...

Filter

- Status
 - Active
 - Inactive
- User Type
 - Device
 - Person
 - Service
- Role
 - Admin
 - Device Admin
 - Org Admin
 - User
- Integration

Si vous cliquez sur Connexion, vous pouvez accéder aux informations de ladite appliance.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Afin de vérifier que l'intégration entre AMP et WSA est réussie, vous pouvez vous connecter à la console AMP et rechercher votre périphérique WSA.

Accédez à **Management > Computers**, dans la section Filtres, recherchez **Web Security Appliance** et appliquez le filtre

Filters

Hostname

Operating System

Connector Version

Flag All Web Security Appliance

Fault

Fault Severity

Isolation Status

Orbital Status

Sort By

Group

Policy

Internal IP

External IP

Last Seen

Definitions Last Updated

Sort Order

[Clear Filters](#) [Apply Filters](#)

Si plusieurs périphériques WSA sont enregistrés, vous pouvez les identifier avec l'ID client d'analyse de fichiers.

Si vous développez le périphérique, vous pouvez voir à quel groupe il appartient, la stratégie appliquée et le GUID du périphérique peuvent être utilisés pour afficher la trajectoire du périphérique.

VLNWSA [redacted] in group [redacted]-Group			
Hostname	VLNWSA [redacted] ...	Group	[redacted]-Group
Operating System	Web Security Appliance	Policy	[redacted].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](#)

Dans la section Stratégie, vous pouvez configurer des détections personnalisées simples et le contrôle d'application - Autorisé qui est appliqué au périphérique.

Edit Policy

Network

Name:

Description:

Outbreak Control

Custom Detections - Simple:

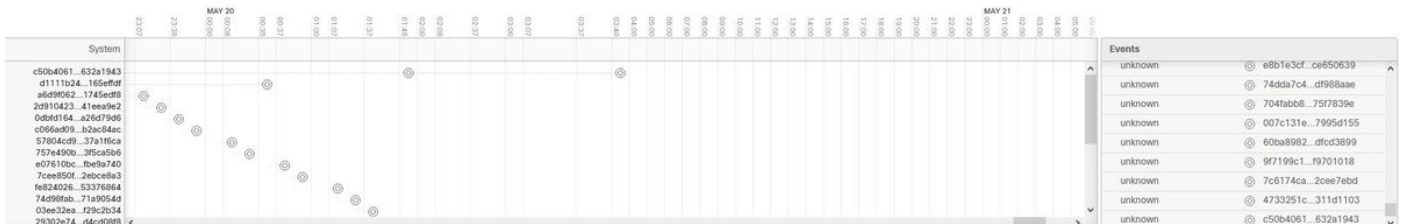
Application Control - Allowed:

Il y a une astuce pour afficher la section Trajectoire du périphérique du WSA, vous devez ouvrir la trajectoire du périphérique d'un autre ordinateur et utiliser le GUID du périphérique.

La modification est appliquée à l'URL, comme le montrent les images.

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

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



Pour Threat Grid, il y a un seuil de 90, si un fichier obtient un score sous ce numéro, le fichier n'est pas placé malveillant, mais vous pouvez configurer un seuil personnalisé sur le WSA.

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 [REDACTED]

Advanced Settings for Cache

Threshold Settings

File Analysis Threshold Score:

Use value from cloud service: 90

Enter custom value:

(valid range 1 through 100)

Dépannage

WSA ne redirige pas vers la page AMP

- Assurez-vous que le pare-feu autorise les adresses requises pour AMP, cliquez [ici](#).
- Vérifiez que vous avez sélectionné le cloud AMP approprié (évitiez de choisir le cloud hérité).

WSA ne bloque pas les SHA spécifiés

- Assurez-vous que votre WSA se trouve dans le groupe approprié.
- Assurez-vous que votre WSA utilise la stratégie appropriée.
- Assurez-vous que le SHA n'est pas propre sur le cloud, sinon WSA ne pourrait pas le bloquer.

WSA n'apparaît pas sur mon organisation TG

- Vérifiez que vous avez sélectionné le cloud TG approprié (Amérique ou Europe).
- Assurez-vous que le pare-feu autorise les adresses requises pour TG.
- Prenez note de l'ID du client d'analyse de fichiers.
- Recherchez-le dans la section Utilisateurs.
- Si vous ne le trouvez pas, contactez l'assistance Cisco afin qu'elle vous aide à le déplacer d'une organisation à l'autre.