

Trend Micro Vision One

Como vincular el AD a Vision One mediante el Service Gateway

Objetivo:

En el siguiente documento se detallará la configuración del Service Gateway para la vinculación del Active Directory.



- 1- Una vez vinculado el Service Gateway a nuestra consola mediante la API, nos debería aparecer en el modulo de “Workflow and Automation” / “Service Gateway Management” el nuevo Service Gateway vinculado, en este debemos clickear y entrar.

+ Download Virtual Appliance							
Service Gateway		Connection status	Version	Services	Uploaded	Downloaded	Last connected
localhost.localdomain(10.1.2.240)		Healthy	2.0.9	2	30.95MB	127.94MB	6m (2023-03-13 11:51:40)

- 2- Una vez dentro del mismo debemos buscar la opción de “Manage Services” y ahí gestionaremos los servicios que vamos a utilizar.

Back

Manage Services

Configure Service Gateway

Support

localhost.localdomain

IPv4 address: 10.1.2.240

IPv6 address: -

Appliance ID: b80565ca-ff32-4381-8b97-11339c06d90d

Connection status: Healthy

Last connected: 2023-03-13 11:51:40

Version: 2.0.9

Storage: 184.1 GB free (Total:200 GB)

Installed Services

Service Name	Version	Status	Description	Connection Status
Syslog Connector	1.0.4	Enable	Enables sharing data from Trend Vision One with your local syslog server.	Healthy
On-premises directory connection	1.0.5	Enable	Once enabled, the Service Gateway can help send data from on-premises directory servers to Trend Vision On...	Healthy

System Resource Usage History

CPU

Memory: 12077 MB

- 3- Dentro del menu vamos a tener que descargar los servicios “On-premises directory connection” y “Syslog Connector”.

Manage Services

On-premises directory connection (Version 1.0.5)

Uninstall

Minimum system requirements: 2 CPUs, 4.00GB Virtual Memory

Once enabled, the Service Gateway can help send data from on-premises directory servers to Trend Vision One. This service is required to set up "Active Directory (on-premises)", and "OpenLDAP" in Third-Party Integration.

Rapid7 - InsightVM / Nexpose (Version 1.0.5)

Minimum system requirements: 0.5 CPUs, 500.00MB Virtual Memory

When enabled, the Service Gateway can send device and vulnerability data from the Rapid7 server to Trend Vision One.

Smart Protection Services (Version 1.0.1)

Minimum system requirements: 2 CPUs, 2.00GB Virtual Memory

Smart Protection Services provide File Reputation and Web Reputation Services to connected products.

Suspicious Object List Synchronization (Version 1.0.1)

Minimum system requirements: 1 CPUs, 2.00GB Virtual Memory

Once enabled, the Service Gateway can send the Suspicious Object List in the Threat Intelligence app to connected Trend Micro products, which can also upload the Virtual Analyzer Suspicious Object List and reports to the Service Gateway.

Syslog Connector (Version 1.0.4)

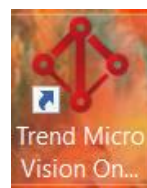
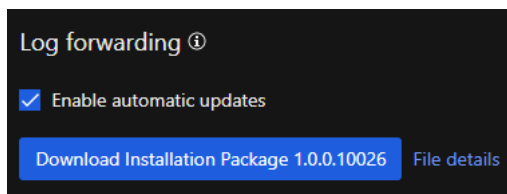
Uninstall

Minimum system requirements: 2 CPUs, 512.00MB Virtual Memory

Enables sharing data from Trend Vision One with your local syslog server.

Cancel

- 4- En el módulo “Workflow and Automation” nos debemos dirigir a “Third-Party Integration” / “Active Directory (on-premises)” y en este vamos a configurar el “Log Forwarding”. Para eso necesitamos un Conector de Ad que vamos a poder descargarlo de esta ventana.



- 5- El conector de “Log Forwarding” se tiene que instalar en el AD y este hay que configurar la API key y la Ip de nuestro Service Gateway para que envíe la información a la consola.

Trend Micro Vision One - Active Directory Connector

Service Gateway Connection

Server address:-

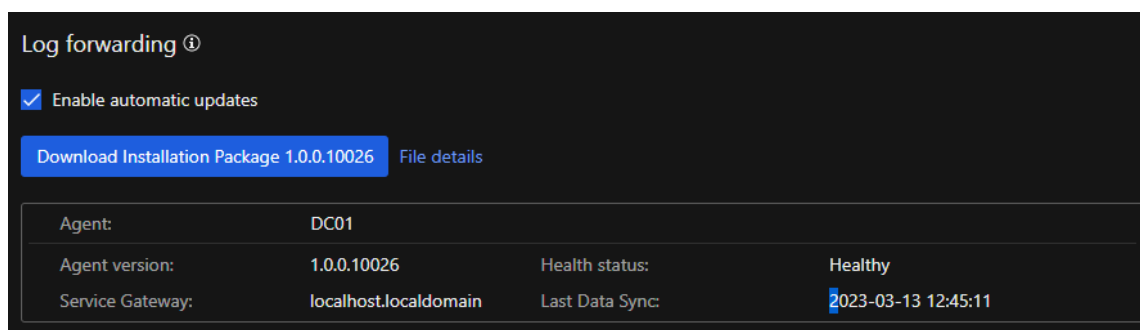
API key:-

To get the key, open Trend Micro Vision One, go to Inventory Management > Service Gateway Inventory, and click Manage API Key.

☐ Use a proxy server

☐ Import certificate

Luego de esto nos debería aparecer en la consola la correcta vinculacion.



- 6- Luego en la misma ventana debemos configurar “Data Synchronization & User Access Control” y para eso debemos generar un “Connect Active Directory Server” y completar con la información del AD.

×

Connection Settings

Active Directory Server Settings

Server Type:

Microsoft Active Directory

Server address:

IP address or public FQDN

Encryption:

NONE

Port:

389

Base Distinguished Name:

DC=Foo, DC=foonet, DC=org

User name:

User@Domain.com or Domain\User

To manage user access control from Trend Vision One, specify your server's administrator credentials. [Learn more.](#)

Password:

Service Gateway Connection

Service Gateway:

Select a Service Gateway

Connect

Cancel

Test Connection

- 7- Una vez hecho las dos configuraciones deberían ir llegando los usuarios del AD a la consola de Vision One.