TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Indegy

Contents

Partner Information

Partner information	
Date	December 13, 2019
Partner Name	Indegy
Web Site	www.indegy.com
Product Name	Indegy Cyber Security Platform
Partner Contact	Joel Silberman (VP Business Development; joel@indegy.com), +1 (866) 801 5394)
Support Contact	support@indegy.com
Product Description	ICS Cyber Security and asset management solution

Use cases for integration into Palo Alto Networks Next-Generation Security Operating Platform

- Remote access to specific elements on the ICS network can be allowed or block based on specific information such as asset type or vendor name.

Palo Alto Networks Products for Integration

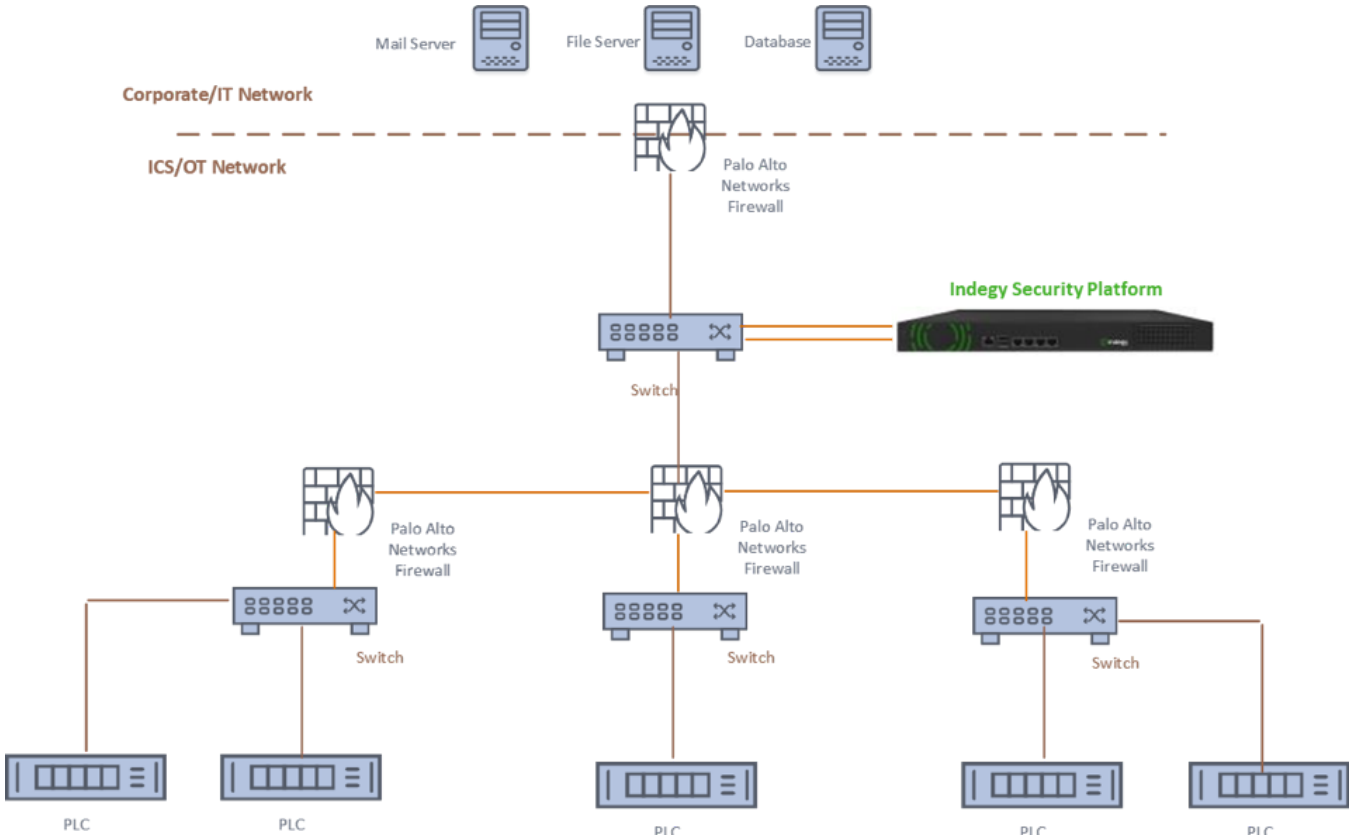
Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Indegy versions tested
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW	Validated	PAN-OS 9.0	2.7+
Panorama			
Prisma Access			
Prisma Cloud			
Prisma Cloud Compute Edition			
Prisma SaaS			
Traps			

VM-Series			
WildFire			
Other			

Integration Benefits

- Visibility – The Palo Alto Networks Firewall receives important asset information on ICS devices
- Increased security for ICS networks – Firewall rules can be set and updated according to accurate asset identification and categorization information.

Integration Diagram

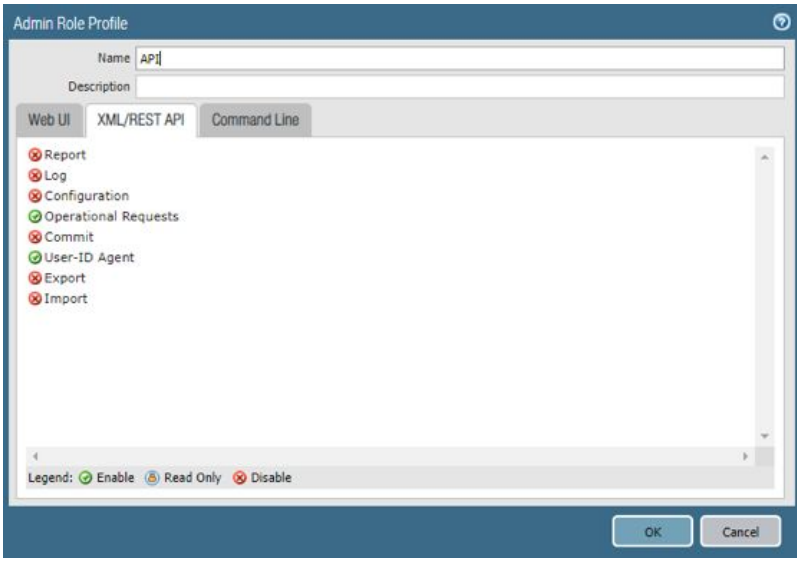


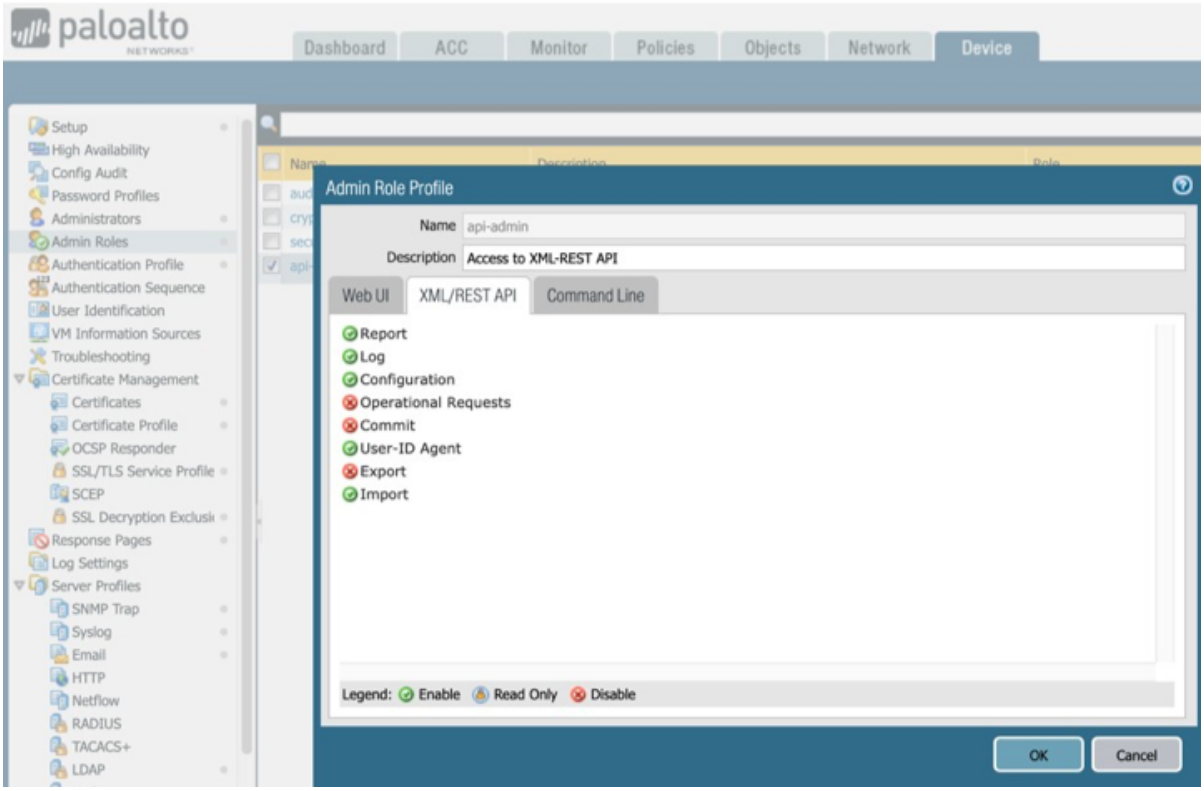
- The data shared between Palo Alto Networks and Indegy is ICS asset type (e.g., PLCs, Eng. Station, HMI...) and asset vendor (e.g., Rockwell, Siemens....) which is shared to the Palo Alto Networks Firewall.
    - Example of information sent from the Indegy Security Platform to the Palo Alto Networks Firewall:
        - IP Address: 10.100.12.20 – Type: HMI, Vendor: Siemens
        - IP Address: 10.100.20.45 – Type: Engineering Station, Vendor: ABB
        - IP Address: 10.100.20.68 – Type: PLC, Vendor: Rockwell
- Data is shared through Palo Alto Networks Firewall API.

- The action taken as a result of this data sharing is an administrator can set firewall rules based on Dynamic Address Groups (DAG) that were created for ICS assets.

Before you begin

- Dependencies: Indegy product version: 2.2 and up, Palo Alto Networks firewall version: 9.0.0
- Requirements for successful integration: Indegy and Palo Alto Networks should support the minimum required versions and have network connectivity between them. Indegy version should be 2.7.
- API key requirements: None. The only requirements is to enable the “Operational Requests” and “User-ID Agent” on the XML/REST API tab. The Web UI and Command Line can be disabled.





- Configure Admin Role Profile – PAN-OS 9.0
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-an-admin-role-profile.html
- Enable API Access – PAN-OS and Panorama API Guide
  https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/enable-api-access.html

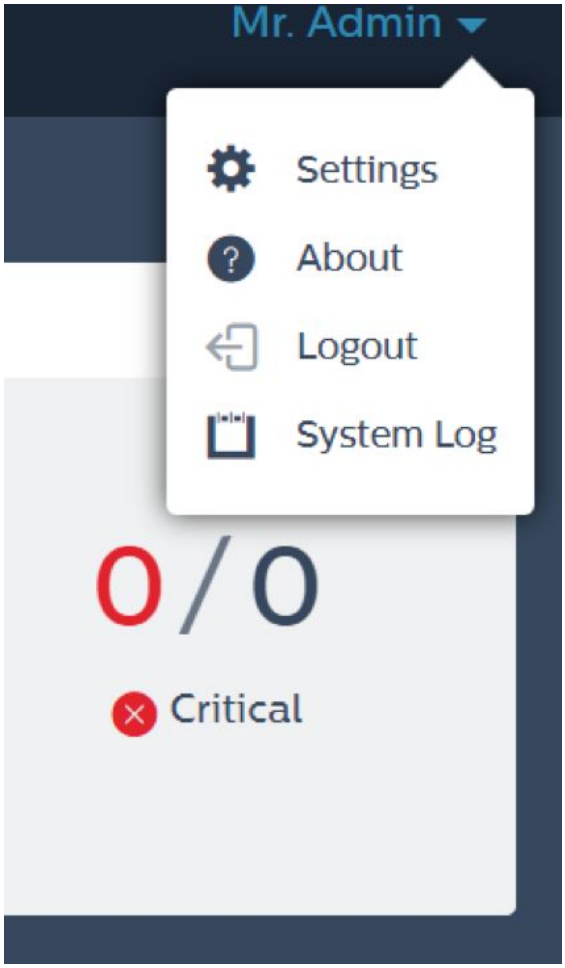
Palo Alto Networks Configuration

1. Create an API user
2. Use the user and password when configuring the interface on the Indegy platform.

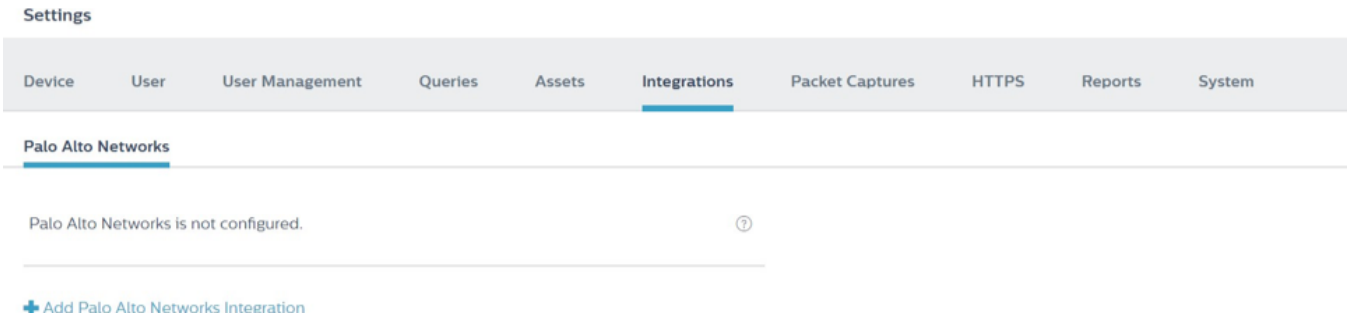
Partner Product Configuration

1. Open the Indegy user interface

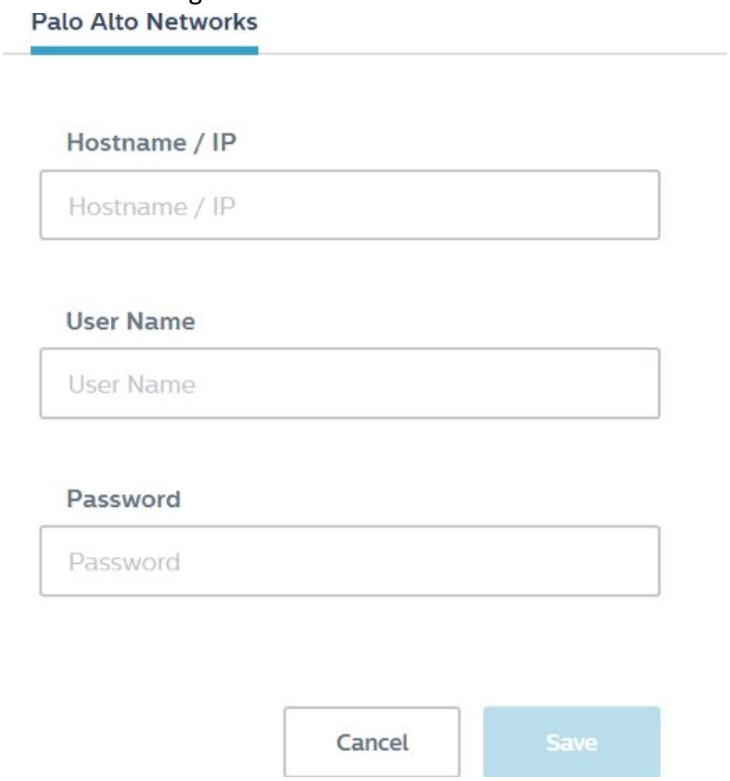
2. Open the settings



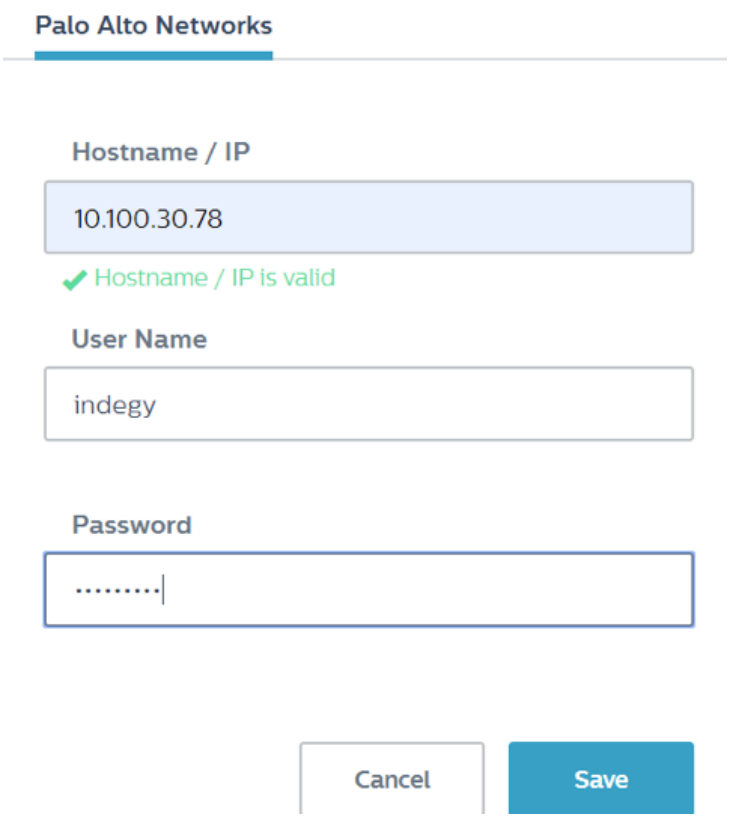
3. Click on the “Integrations” tab



4. Click on ”Add Palo Alto Networks Integration” button



5. Enter the IP/Host of the Palo Alto Networks Firewall
6. Enter the username and password of the Indegy API user that was configured on the Palo Alto Networks Firewall.



7. Click save. The connection status will appear as “Connected” once the Indegy Security Platform will be able to connect to the firewall.

Troubleshooting

- In case an error message appears on the status line please make sure to check the user configuration parameters on the firewall user interface, and try again to create the connection.
- Contact information for support: Support@indegy.com
- Indegy is a member of the Palo Alto Networks TSA Net group.

Technical Details

- API calls leveraged:
  - type=keygen
  - type=op, cmd=show system info
  - type=op, cmd=show object registered ip
  - type=user-id, cmd=update register and unregister