NetWitness® Platform

Version 12.5.1

Palo Alto Prisma SASE Configuration Guide

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November, 2024

Contents

Getting Started

NetWitness SASE, combined with Palo Alto Networks, provides unprecedented visibility into behavior and communication among devices and services in remote and distributed networks across on-premises, hybrid, and cloud deployments.

What NetWitness SASE does:

- **Streamline searches and investigations**: Log into a single user interface to perform index searches, pivot through metadata, and reconstruct network sessions to receive results quickly.
- **Leverage retained data**: Empower analysts to perform forensic examinations on a triggered detection and threat hunt for unknown threats against retained raw network communications.
- **Correlate disparate data sets**: Enrich the context of investigations by correlating data from the actual network traffic of remote users with other access by those same users for a complete end-to-end story of what transpired.
- **Minimize costs**: Optimize storage and reduce operating costs using new compression algorithms, selective retention, and the ability to split network decoder components to limit what must run in the cloud.

About NetWitness SASE

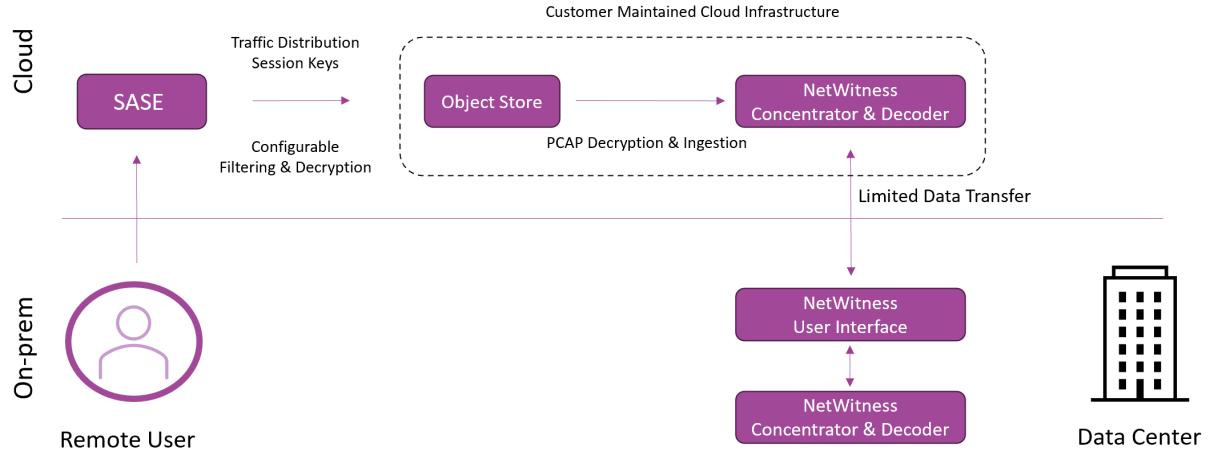
NetWitness supports SASE and critical hybrid use cases across on-premises and in the cloud by partnering with Palo Alto Networks on technical integrations. NetWitness SASE Integrations give organizations complete visibility into encrypted traffic, remote users, and cloud workloads. With NetWitness SASE integrations, customers can achieve SASE flexibility, inherent security advantages, and complete visibility into threat detection and response.

NetWitness SASE provides the following capabilities:

- **Flexible**, **secure**, **real-time traffic monitoring**: NetWitness SASE integrations capture all network traffic from remote users in near real-time, enabling immediate response to any potential threats. Regardless of the location of the data collected, the data is available in the detection engine, and analysts can easily find the anomalies. The customization opens available in NetWitness SASE reduce the risk of storing sensitive, personally identifiable information.
- **Get scalable**, **high-performance cloud security**: With NetWitness SASE integrations, enhance total visibility and threat detection capabilities across your enterprise using well-known on-premises mechanisms such as rules, parsers, feeds, and machine learning. Perform searches and investigations and swiftly receive results with a single user interface. The integration supports forensic examinations on triggered detections and facilitates threat hunting against retained network communications, empowering analysts to combat unknown threats effectively.
- **Eliminate blind spots**: NetWitness SASE integrations empower organizations to retain complete visibility into their cloud security stack, cost-effectively eliminating blind spots in their cloud traffic and maximizing the effectiveness of their security infrastructure investments. Organizations have the visibility and control they need over encrypted traffic to ensure compliance with their privacy, regulatory, and acceptable use policies, whether on-premises or in the cloud.

- **Unparalleled network visibility to strengthen SASE security**: The improved visibility provided by the integration allows organizations to close gaps in their zero trust security posture and enable better detection capabilities.

NetWitness SASE Integration with Palo Alto Architecture



As hybrid and remote work environments become the norm, Secure Access Service Edge (SASE) has emerged as the gold standard in network technology. It empowers modern workforces to securely access corporate resources from any location. By enabling full packet capture and log monitoring directly on SASE nodes and integrating them with on-premises, cloud, and SaaS sources, the NetWitness Platform ensures enterprise-grade security—regardless of where the data originates. With robust encryption and Zero Trust access baked in, SASE provides significant benefits to today's distributed organizations.

Historically, network edge security has introduced blind spots for critical security technologies that perform threat detection, analysis, and response. Traditional network and security architectures were not built to handle the current landscape, where data and traffic come from globally distributed sources and thousands of devices. Network managers, accustomed to relying on VPNs and proxies, face new visibility challenges. These legacy solutions increase complexity, drive up costs, and struggle to scale efficiently as demand grows.

The NetWitness Platform SASE integration with Palo Alto Networks addresses these challenges, providing comprehensive visibility into all SASE data streams. SASE converges networking and security services in the cloud to ensure seamless, secure access for users, devices, and applications—anywhere. This architecture not only improves security but also enhances the user experience, empowering organizations to thrive in today's decentralized work environments.

Configure Palo Alto Prisma Integration

There are two methods to configure Palo Alto Prisma Integration from NetWitness Platform.

Note: NetWitness recommends you to use the Centralized Content Management (CCM) method for a more streamlined deployment process.

- Deploy Palo Alto Prisma Integration using CCM
- Deploy Palo Alto Prisma Integration using NwConsole

Deploy Palo Alto Prisma Integration using CCM

This topic describes how to deploy the Palo Alto Prisma Integration for users using the Policy based CCM.

Prerequisites

Before proceeding, it is important to make sure the following:

- The NetWitness Platform (Admin Server and Packet Decoder Host) is on version 12.5 or later.
- You are connected to Live Services under the **(Admin)** > **System** > **Live Services** page.
- The Decoder services are managed by CCM. If CCM does not manage it, you can enable CCM for the particular decoder service. For more information, see the topic Enable or Disable CCM for Individual Decoder Services.
- You must have the Private Key (.pem file), optional Bucket Authentication (.JSON file), GCP bucket names, local GCP project ID, and Pub/Sub Subscription ID available for configuration:
  - The Private Key (.pem file) is used to decrypt the AES key, which is used to decrypt the PCAPs. For more general information on managing and using the Private Key, please refer to Palo Alto's Traffic Replication in Prisma Access documentation.
  - The optional Bucket Authentication Key (.JSON file) is used to authenticate access to a bucket in GCP. Creating a Bucket Authentication Key (.JSON file) is a two-step process:
    - Create a service account in GCP with **Storage Object Viewer (roles/storage.objectViewer)**. For more information, see topic Create service accounts.
    - Create a service account key in GCP. For more information, see Create and delete service account keys.

Create Google Cloud Pub/Sub Subscription

The Subscription ID is unique to each Pub/Sub subscription within a project. Each subscription enables users to receive messages from a designated Pub/Sub topic, creating a direct link between the subscription and its corresponding topic. This setup allows for efficient message delivery, ensuring users can manage and retrieve relevant information in real-time.

To create a subscription, use the gcloud tool available on the SASE head nodes.

```
gcloud pubsub subscriptions create <SUBSCRIPTION ID> --topic-
project=<PAN GCP PROJECT ID> --topic=<PAN GCP PUB/SUB TOPIC ID> --
message-filter='attributes.bucketId="<PAN GCS BUCKET>"' --enable-
message-ordering

Created subscription [projects/<LOCAL GCP PROJECT
ID>/subscriptions/<SUBSCRIPTION ID>].
```

`--topic-project` is the home project of the topic, where all subscriptions will be received.

`--topic` is the topic ID.

`--message-filter` is the subscription filtering criteria based on the message payload. In this case, it retrieves messages containing an attribute that specifies a particular bucket ID, which is required for the integration plugin.

`--enable-message-ordering` ensures that subscription messages from the topic, which share the same ordering key (in this case, the GCS bucket of interest), are **ordered/delivered** in the same order they were published. If message ordering is not enabled, it may result in disruptions or breaks in the continuity of the incoming session data.

Any policies specific to custom messages, such as retention, must be determined by the customer according to their needs.

Note: Files in the PAN GCS bucket will have a retention period of three days.

Configure Permissions for Google Cloud Platform

By setting these permissions, the service account will have the necessary access to perform its functions effectively within the Google Cloud Platform (GCP) infrastructure.

To properly configure permissions for the service account used by the plugin, you need to grant the following access and permissions:

1. **GCS Bucket and Pub/Sub Topic Read Access**
   - Managed by **PAN** (Palo Alto Networks).
   - **GCS Bucket Read Access**: Required to retrieve new packets from the GCS bucket.
   - **Pub/Sub Topic Read Access**: It is necessary to subscribe to the Pub/Sub topic for real-time message processing.
2. **Pub/Sub Admin Role**
   - The service account must be assigned the "**Pub/Sub Admin Role**", which grants full permissions (pubsub.*) for managing topics and subscriptions.
   - This role is essential to onboard subscriptions locally within the GCP environment that hosts the NetWitness instance.
3. **Cloud API Access for Attached Service Accounts**
   - If the service account is directly attached to Decoder **VM**, it must be granted **full access to Cloud APIs** to ensure seamless communication with other GCP resources.

Deploy Palo Alto Prisma Integration

You must perform the following tasks to deploy the Palo Alto Prisma Integration on NetWitness Platform.

- Task 1. Map Network Adapter in Decoder for Palo Alto Prisma Integration
- Task 2. Create and Publish Policy for Palo Alto Prisma Integration
- Task 3. Configure Palo Alto Prisma Integration from Policy Details View
- Task 4. Verify Palo Alto Prisma Events Received at Decoder

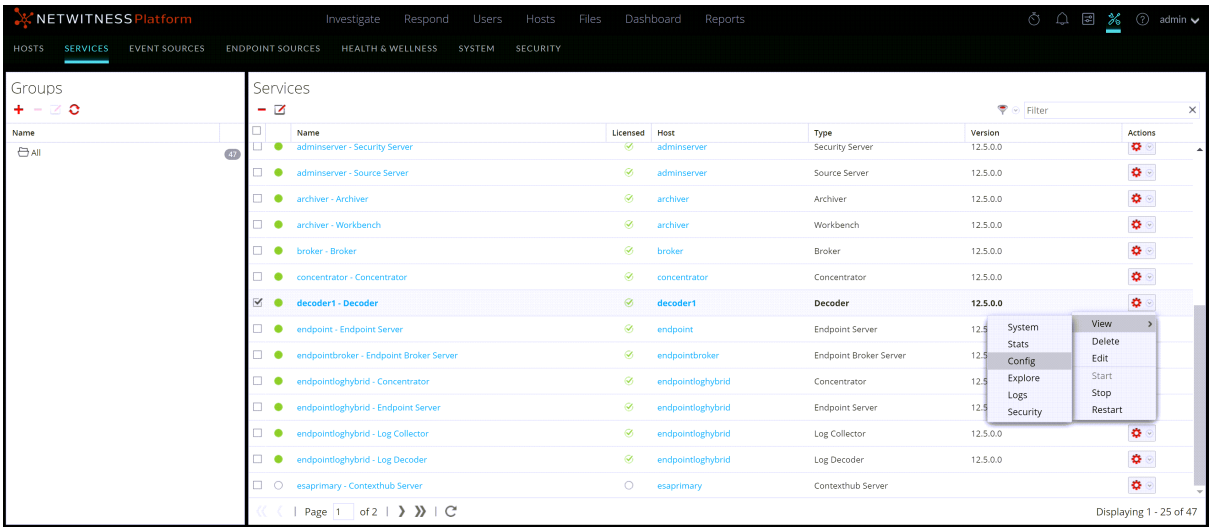
- Task 5. Verify Events Meta from Palo Alto Prisma in Investigate View

Task 1. Map Network Adapter in Decoder for Palo Alto Prisma Integration

You must select a network adapter **(pcap_stream,Pcap File Streamer)** and enable **Capture Autostart** option through which the Decoder captures packets and processes the data.

To Map the Network Adapter in Decoder for Palo Alto Prisma Integration

1. Log in to the NetWitness Platform.
2. Go to  **(Admin)** > **Services**.
3. Select the **Packet Decoder** service and click  > **View** > **Config**.

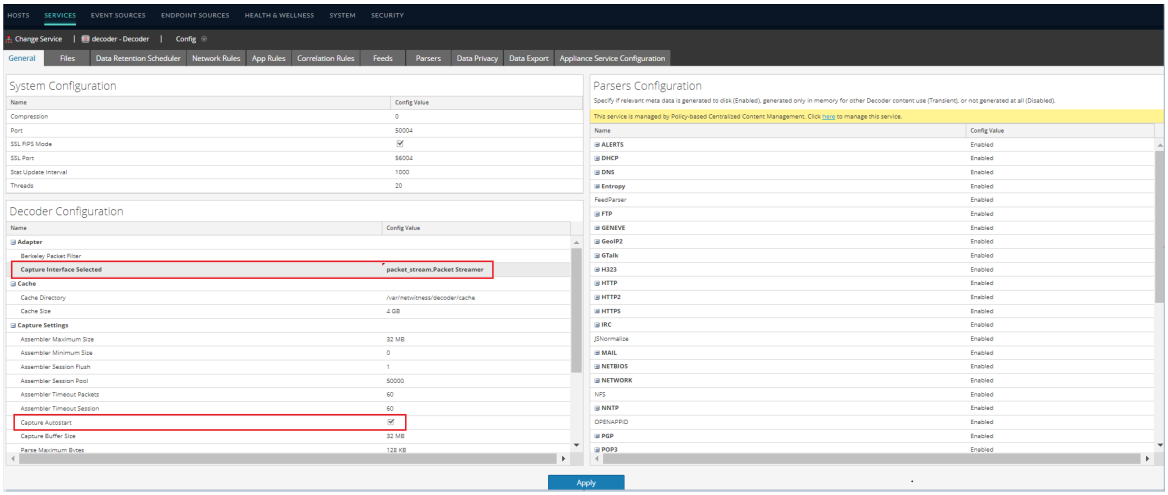


The Configure view for the Decoder service is displayed with the **General** tab open.

4. Under the **Decoder Configuration** section, do the following:
   a. Set the **Capture Interface Selected** to **pcap_stream,Pcap File Streamer** network adapter. (Applicable for 12.4 and 12.4.1)

      Set the **Capture Interface Selected** to **packet_stream,Packet Streamer** network adapter. (Applicable for 12.4.2 and above versions)

b. Enable the **Capture Autostart** option.



5. Click **Apply** to save the changes.

Task 2. Create and Publish Policy for Palo Alto Prisma Integration

You must create a policy with Palo Alto Prisma Integration plugin and assign it to one or more groups having a decoder service and publish the policy.

Prerequisites

- Ensure that the **Palo Alto Prisma Integration** plugin type is available at the **SASE Integration Plugin** tab.
- Ensure that the group with one or more decoder services is created.

Supported Hosts

- Packet Decoder
- Packet Hybrid

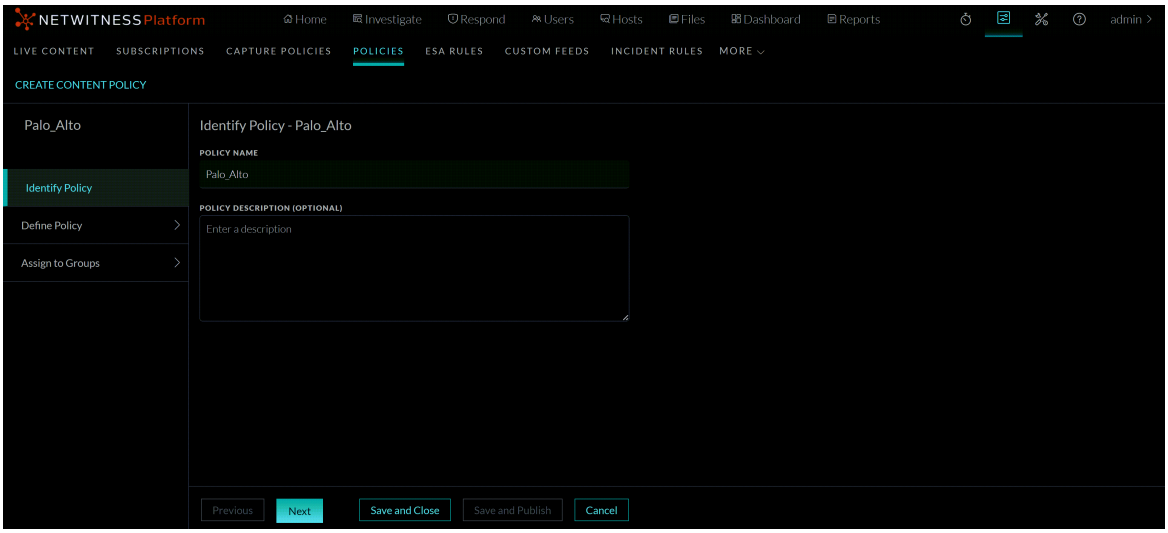
To create and publish policy for Palo Alto Prisma Integration

1. Go to **(Configure)** > **Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**.

   The available policies are displayed.
4. Click **+ Create New** to add a new policy.
5. In the **New Policy** panel, do the following:

a. Enter a unique policy name.

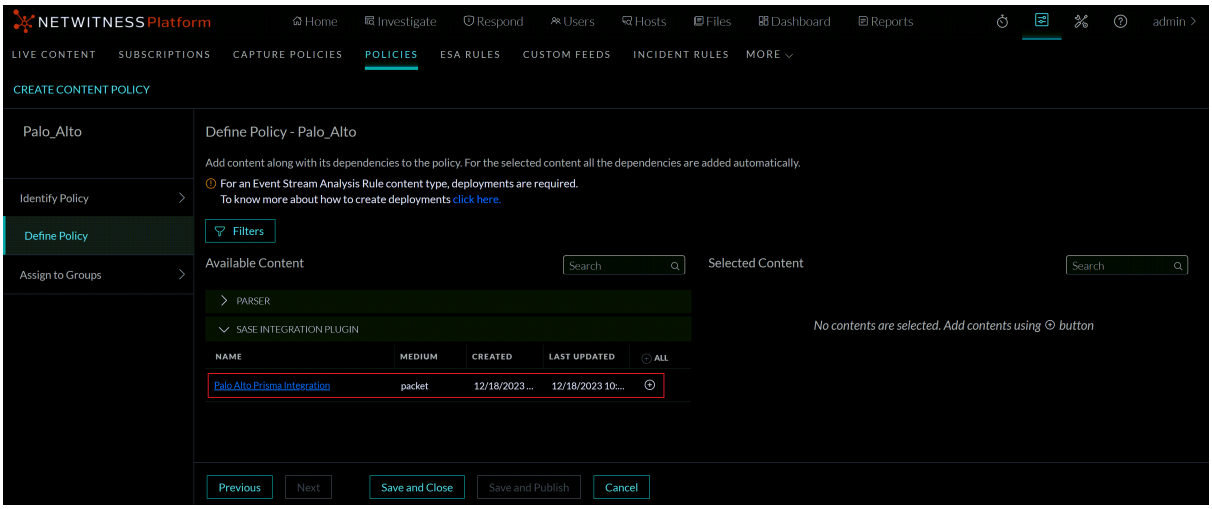
b. (Optional) Enter a description for the policy.



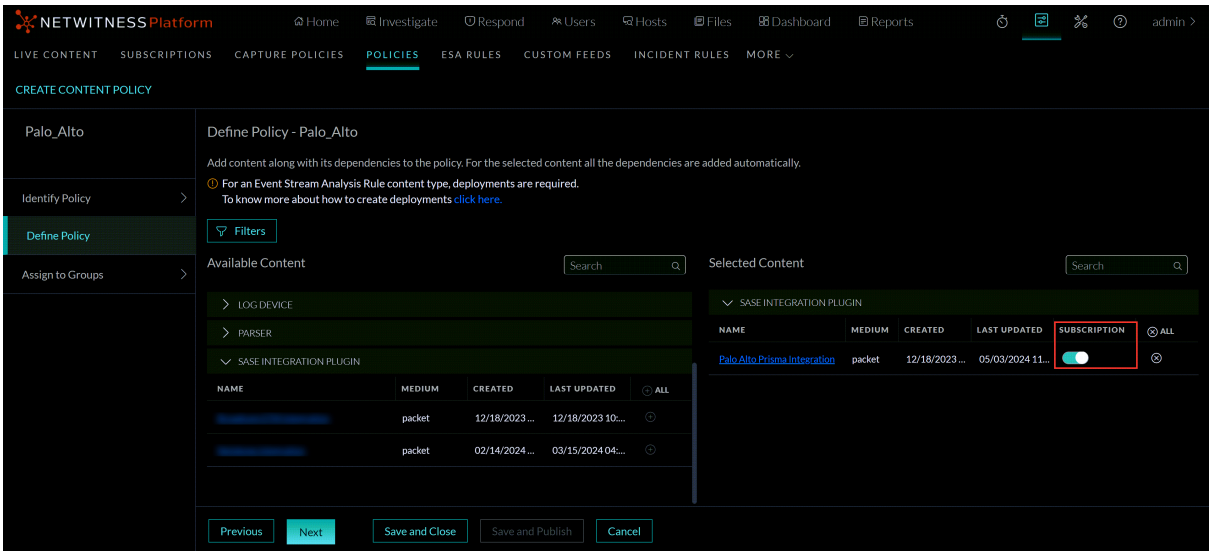
6. Click **Next**.

7. In the **Available Content**, select the plugin type and click + to add the **Palo Alto Prisma Integration** plugin to the policy.

Note: You can add only one **SASE Integration Plugin** to any particular policy.



8. Enable the subscription (if required) by clicking the subscribed toggle. Once the content is subscribed to, the updates are pushed automatically.

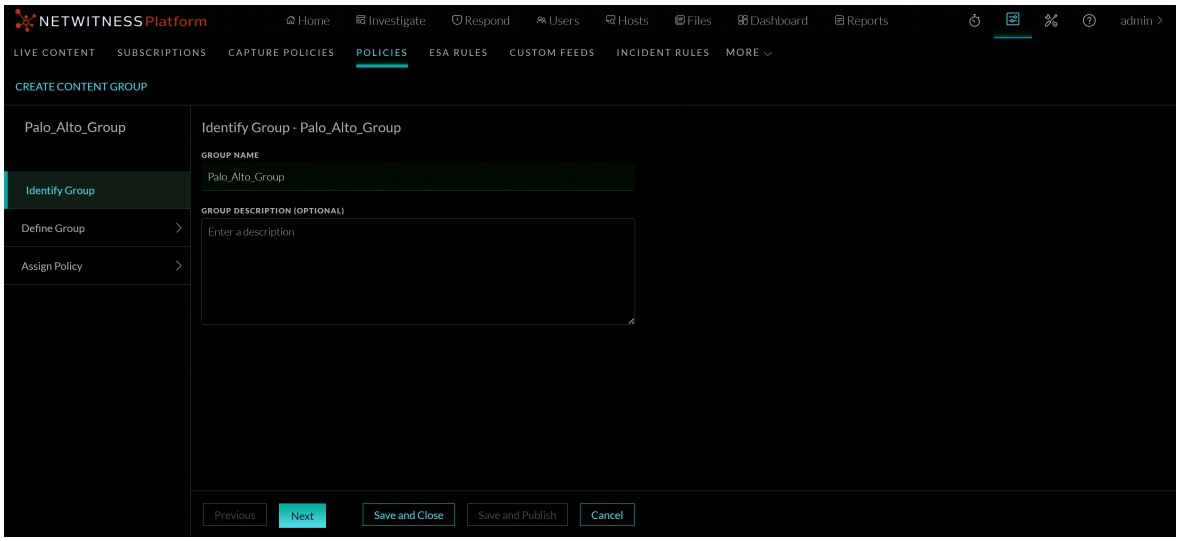


9. Click **Next**.

10. If there are no unassigned groups available, click + Create Group to save the policy and redirect you to the **Create Content Group** screen.

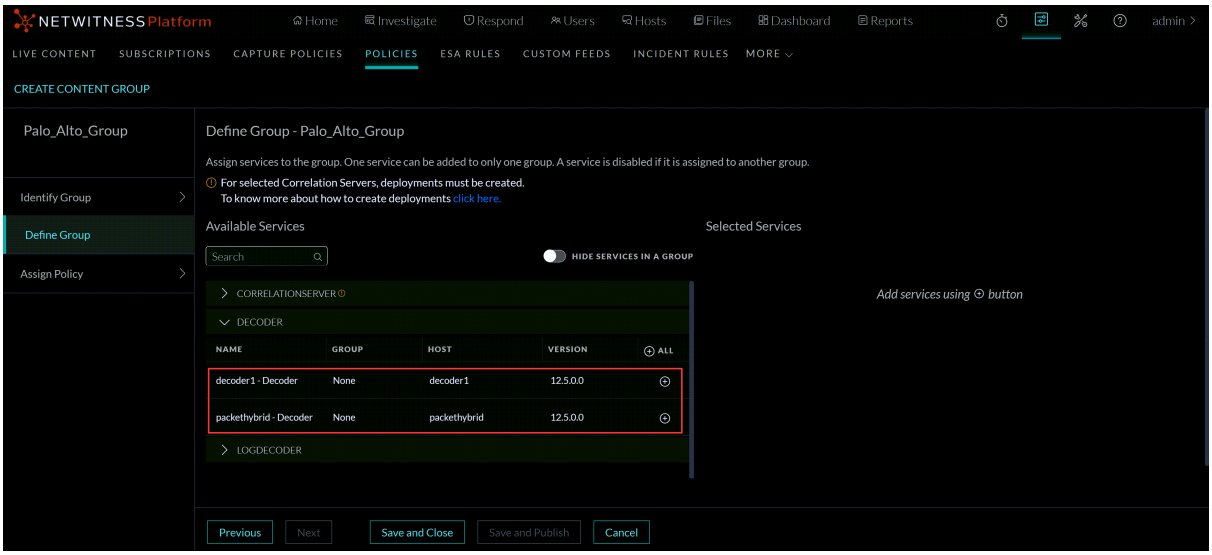
11. In the New Group panel, do the following:

    - Enter the name of the group.
    - (Optional) Enter the description for the group.



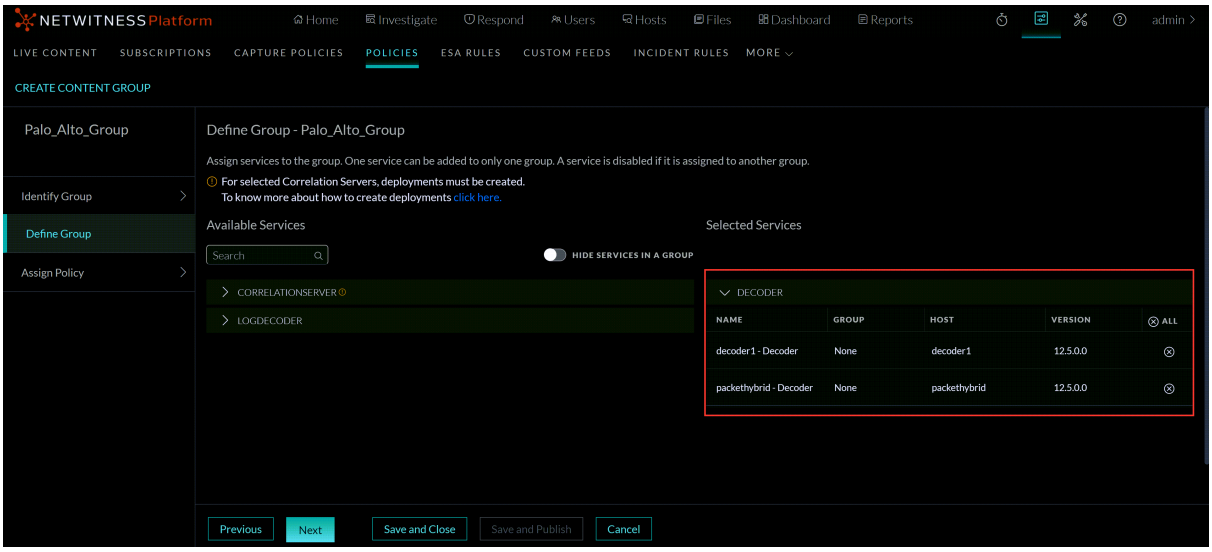
12. Click **Next**.

13. In the **Define Group**, click + to assign services to the group.

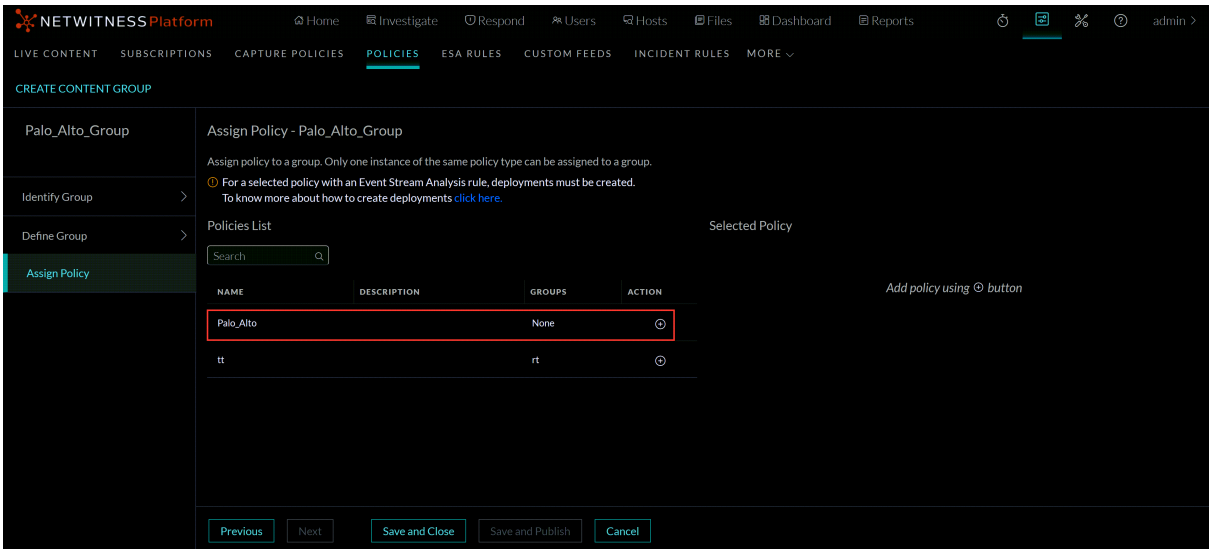


Note:
- A service is disabled if it is assigned to another group.
- A service is disabled if it is not managed by Policy-based Centralized Content Management.

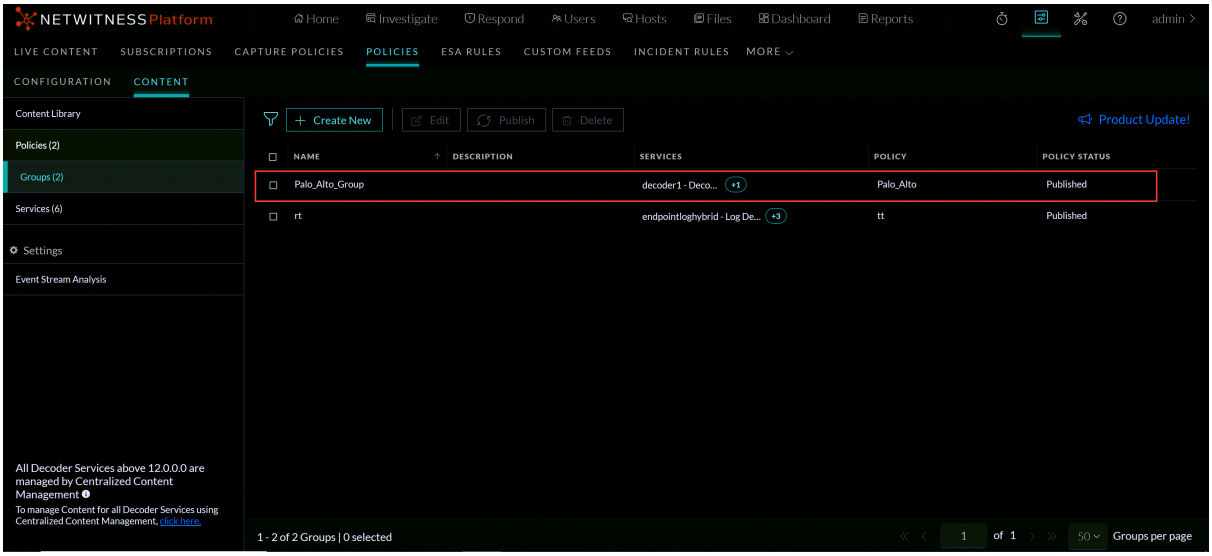
14. Click **Next**.



15. In the Assign Policies, click + to assign policies to a group. You can assign only one policy to any particular group.



16. Click **Save and Publish** to save and publish the settings.



IMPORTANT: Ensure that you always publish the policy after adding the **Palo Alto Prisma Integration** plugin to the policy to deploy the plugin to the Decoder service.

Note: You can also publish a policy from the **Policy Details** screen. For more information on publishing a policy from the **Policy Details** screen, refer to the View a Policy topic.

For more information on Policies, see Manage Policies.

For more information on Groups, see Manage Groups.

Next, go to the policy details view and perform the Palo Alto Prisma Integration settings.

Task 3. Configure Palo Alto Prisma Integration from Policy Details View

Administrators can configure the Palo Alto Prisma Integration to capture the network data from the decoder service within a policy, which sends the data to NetWitness. The data is then processed by NetWitness so that it can provide a comprehensive view of network traffic and malicious activity. Analysts can use this data to monitor network traffic, identify threats, and investigate any malicious behavior.

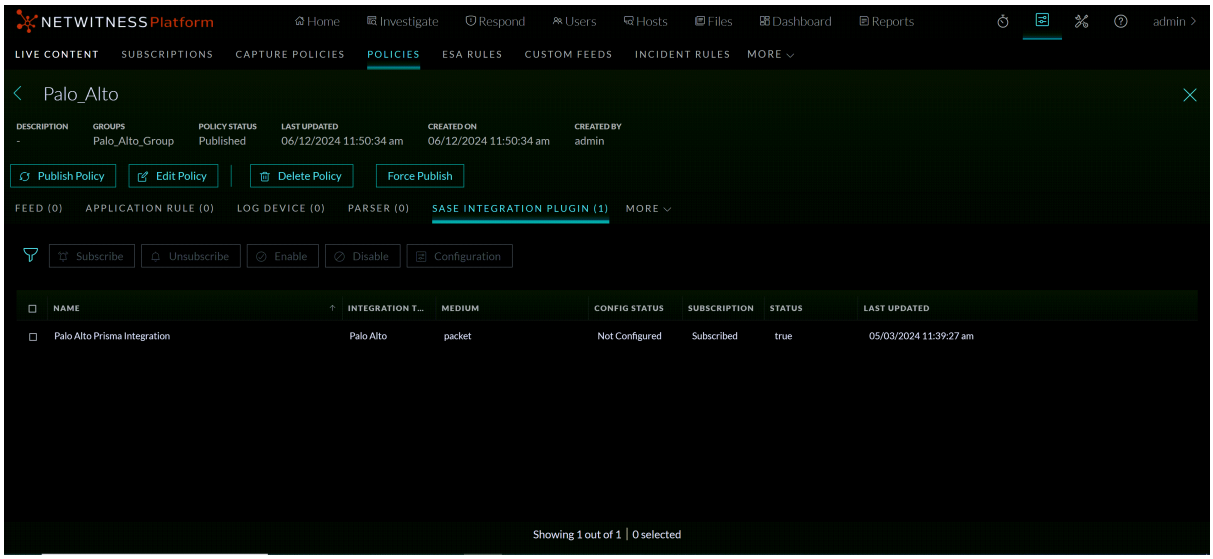
Prerequisites

Before you begin configuring the Palo Alto Prisma Integration, ensure that you have the following details:

- Ensure there is a policy created with the Palo Alto Prisma Integration plugin, and the policy is associated with the group that has a Decoder service configured, and the policy is published.
- You must have the Private Key (.pem file), optional Bucket Authentication (.JSON file), GCP bucket names, local GCP project ID, and Pub/Sub Subscription ID available for configuration.

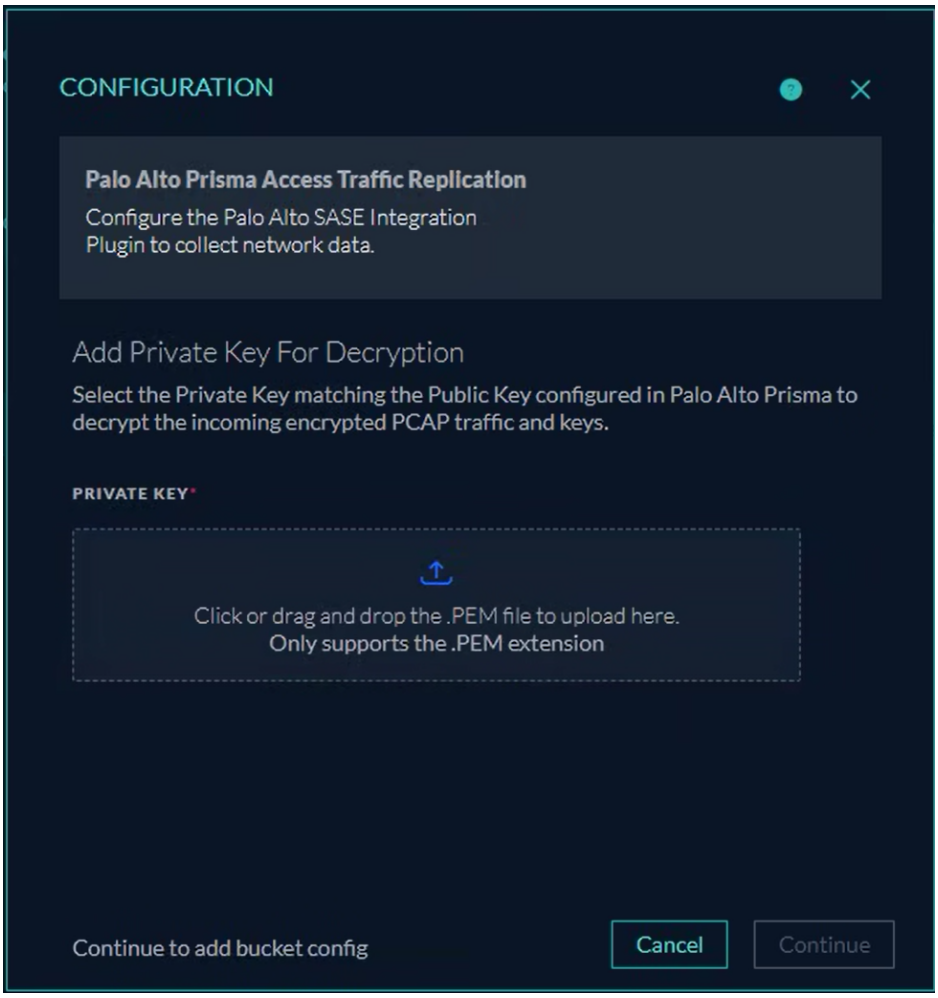
To Configure the Palo Alto Prisma Integration

1. Go to  **(Configure)** > **Policies**.
2. In the policies panel, click **Content**.
3. In the left panel, click **Policies**.
4. Do one of the following:
   a. Click the policy name containing the Palo Alto Prisma plugin type to view the policy details.
   b. Click a row to view details about the selected policy and click **View Details**.
5. Click **More** > **SASE Integration Plugin** tab.



IMPORTANT: The **Configuration** button will be disabled when the policy status is **Unpublished**, **Failed**, or **N/A**. For more information, see Filter Policies.

6. Select the **Palo Alto Prisma Integration** plugin type and click **Configuration**.
   The Configuration dialog is displayed.

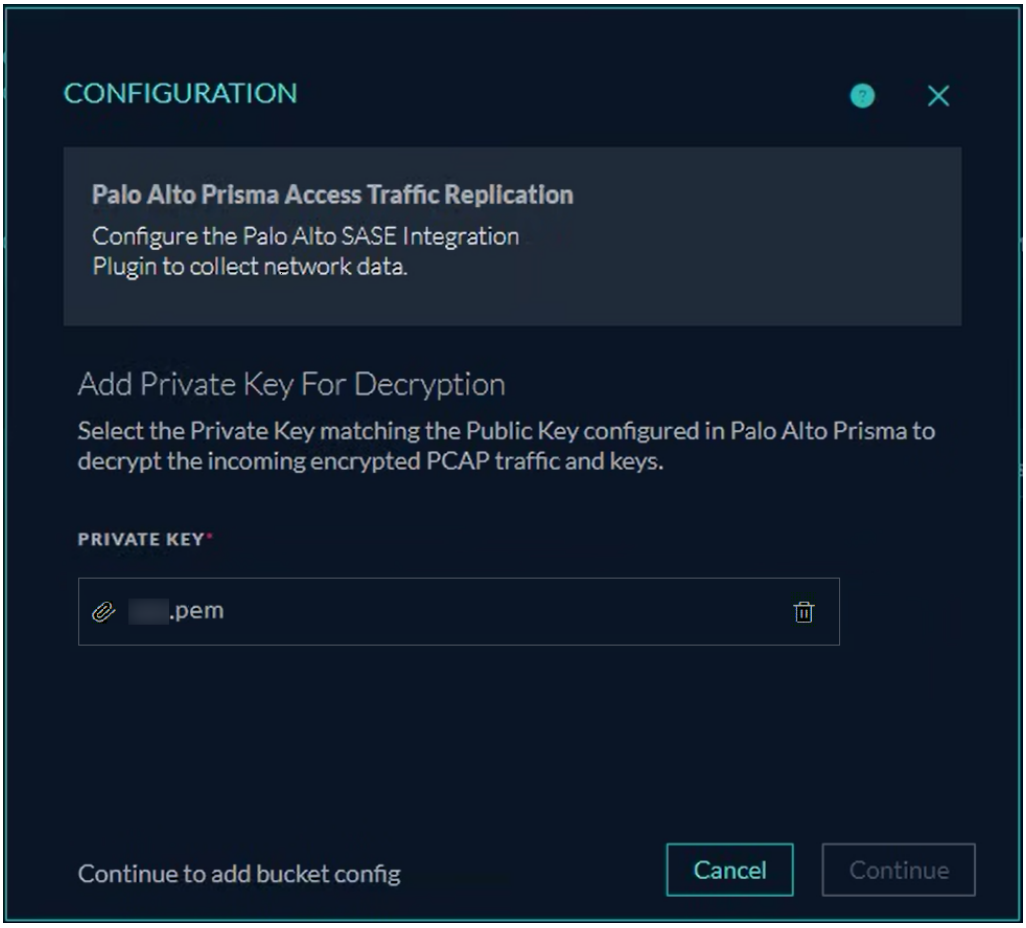


7. In the **Add Private Key for Decryption** section, do the following:
   a. In the **Private Key** area, click or drag and drop the (.pem) file to upload.
   b. Click **Continue** to add the bucket configuration.

   The Private Key (.pem file) is used to decrypt the AES key, which is used to decrypt the PCAPs.

> **Note:**
> • Private keys must have a valid private key format extension (.pem).
> • The size of the Private Key (.pem file) must not exceed 8 MB.

> **IMPORTANT:** You only need to upload the private key once when configuring the bucket for the first time. For subsequent bucket configurations, the private key is not required. When you click on the **Configuration** option, you will be taken directly to the **Add Bucket Configuration** screen.

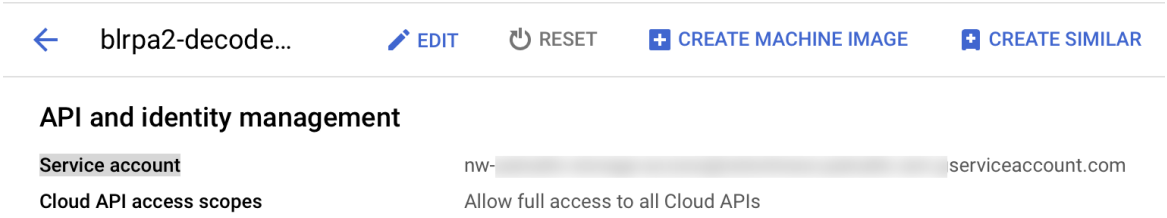


8. In the **Add Bucket Configuration** section, do the following:
   a. Select the decoder service from the **Decoder** drop-down list.

      Note: A bucket can only be configured with one decoder at a time.

   b. Enter the Google Cloud Project ID which is a user-defined unique identifier for a Google Cloud project.
   c. Enter the Publish/Subscribe (Pub/Sub) Subscription ID. The Subscription ID is specific to a Pub/Sub subscription within a project. Each subscription allows users to receive messages from a specific Pub/Sub topic, effectively linking the subscription to that topic.
   d. Enter the GCP bucket name from which the decoder needs to fetch the data. For example, **us-east-gcp-bucket**.
   e. (Optional) In the **Bucket Authentication** area, click or drag and drop the (.JSON) file to upload. Bucket Authentication is used to authenticate access to a bucket in GCP.

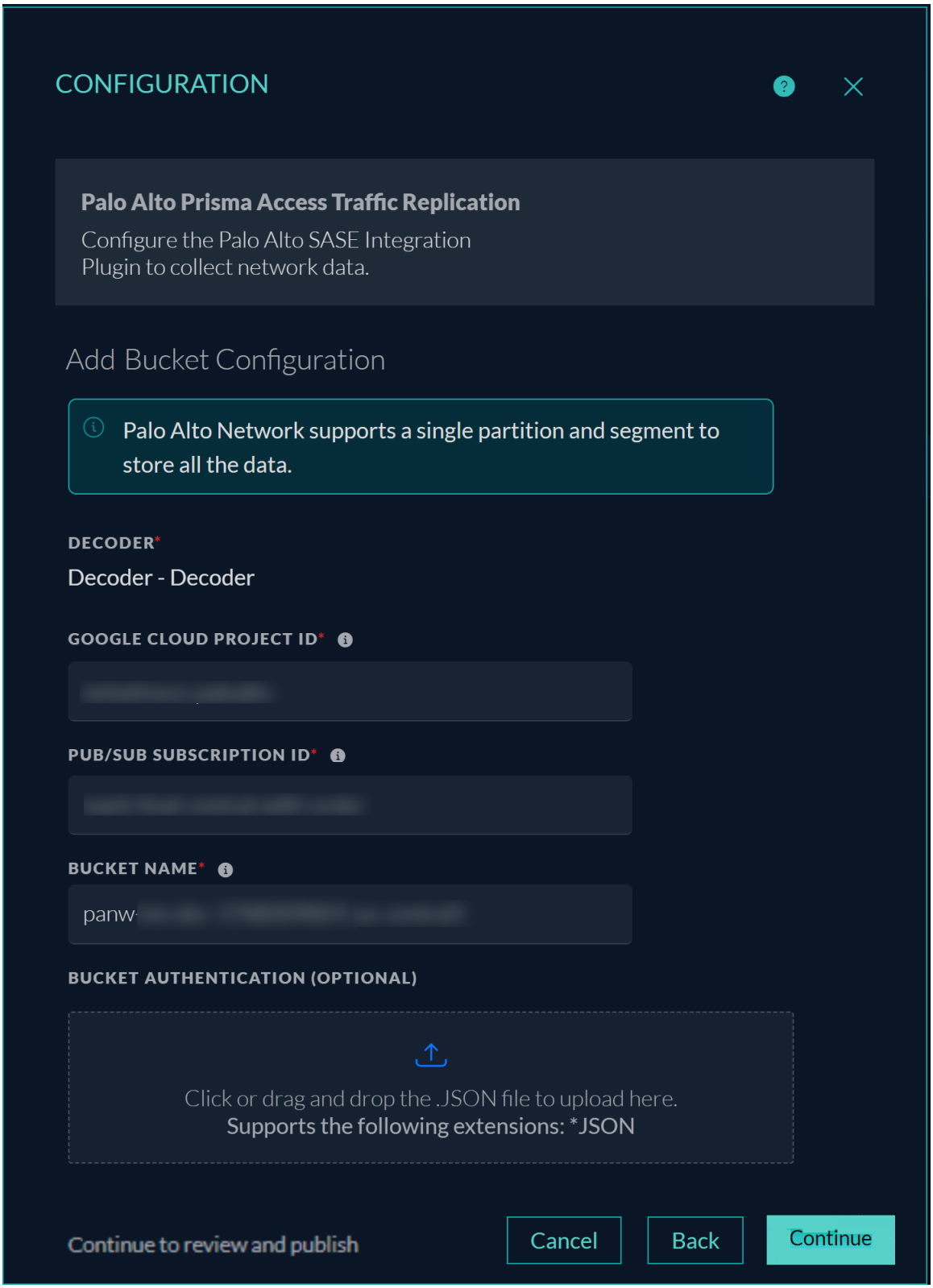
      (Optional) Service account can be attached directly to the Decoder VM housing the integration.



Note:
• Bucket names must be more than two characters and can only contain lowercase letters, numeric characters, dashes (-), underscores (_), and dots (.). Spaces are not allowed.
• The Bucket Authentication must have a valid bucket authentication key format extension (.JSON).
• The size of the Bucket Authentication (.JSON file) must not exceed 8 MB.

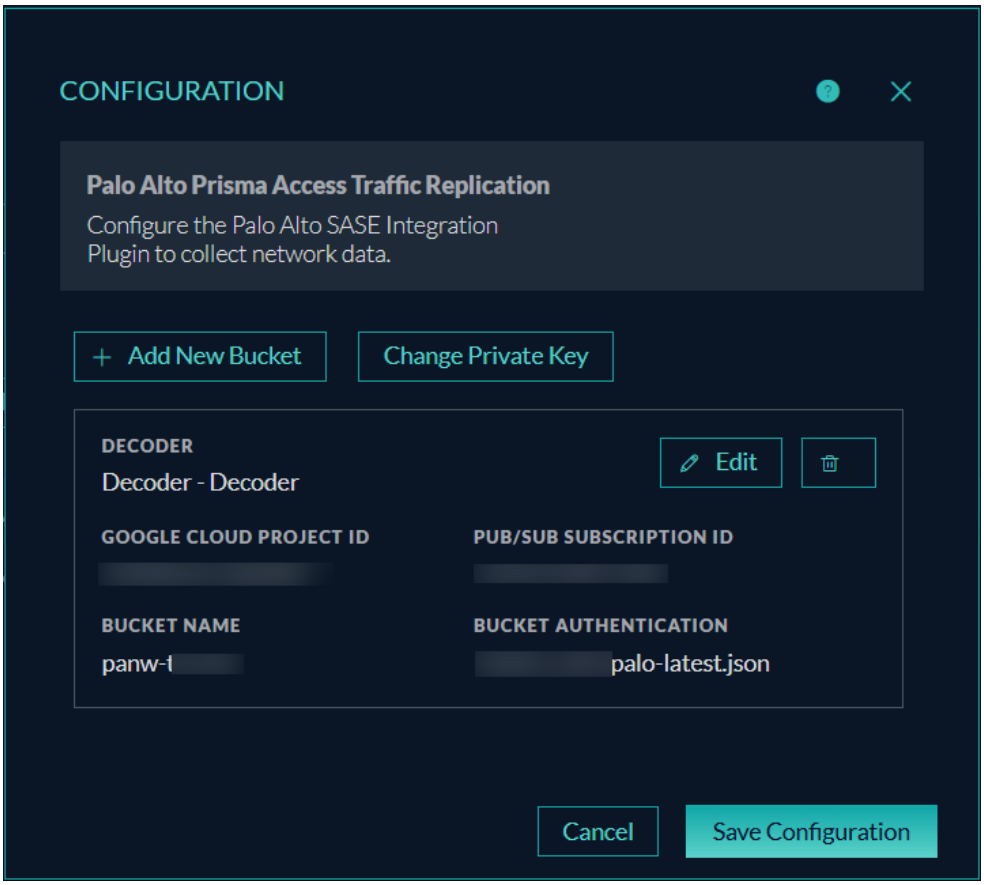
Note:
By default, the values for partition.total is 1, and partition.segment is 0. It will be pushed to the Decoder along with the changes in the Configuration modal. You can view these values in the **Decoder Explore** page.

f. Click **Continue**.



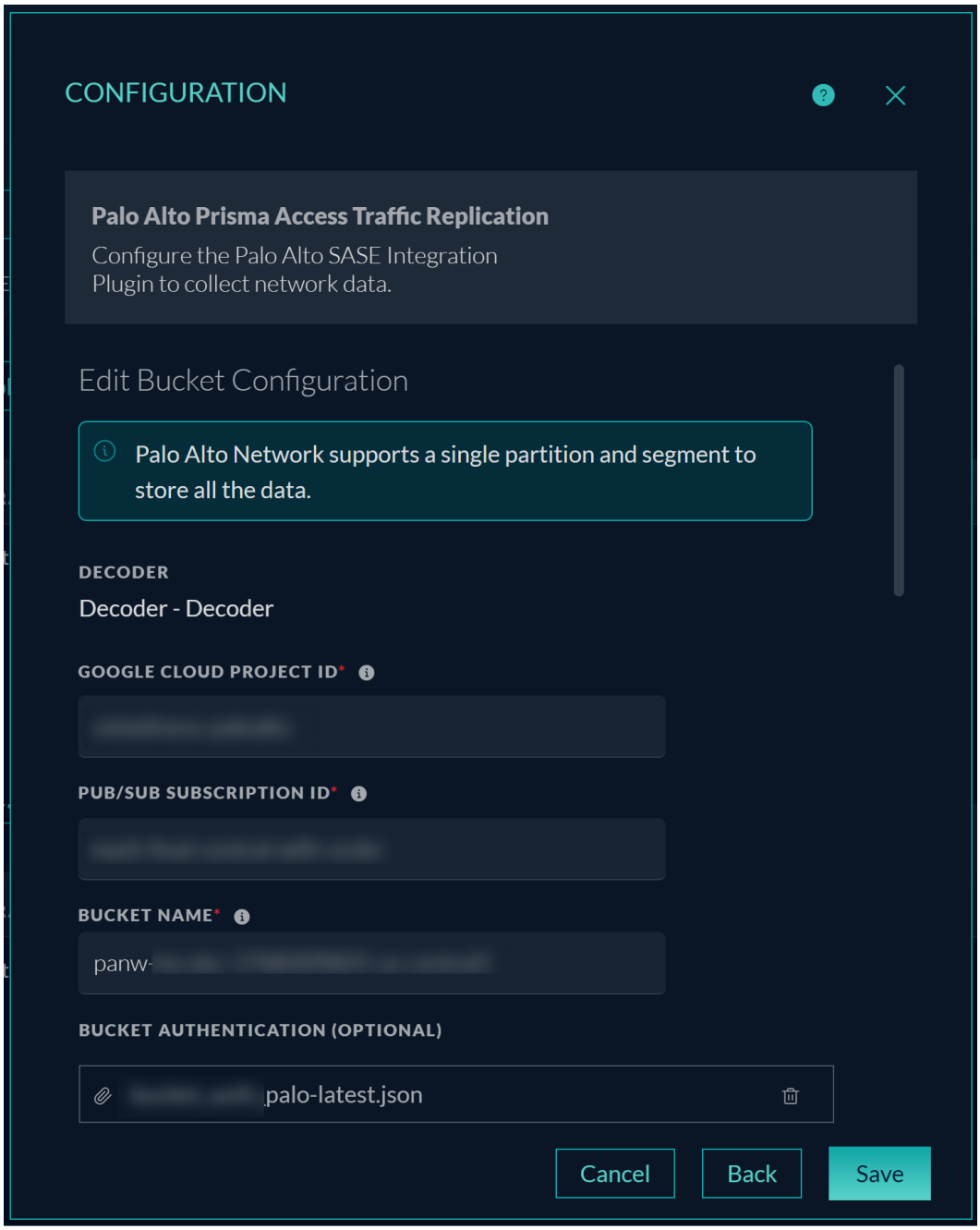
9. Click + **Add New Bucket** to add new buckets, which navigates to the **Add Bucket Configuration** section. Follow **step 8** to configure the bucket details.

Note: You can configure the number of buckets based on the total number of decoders added to the particular policy.

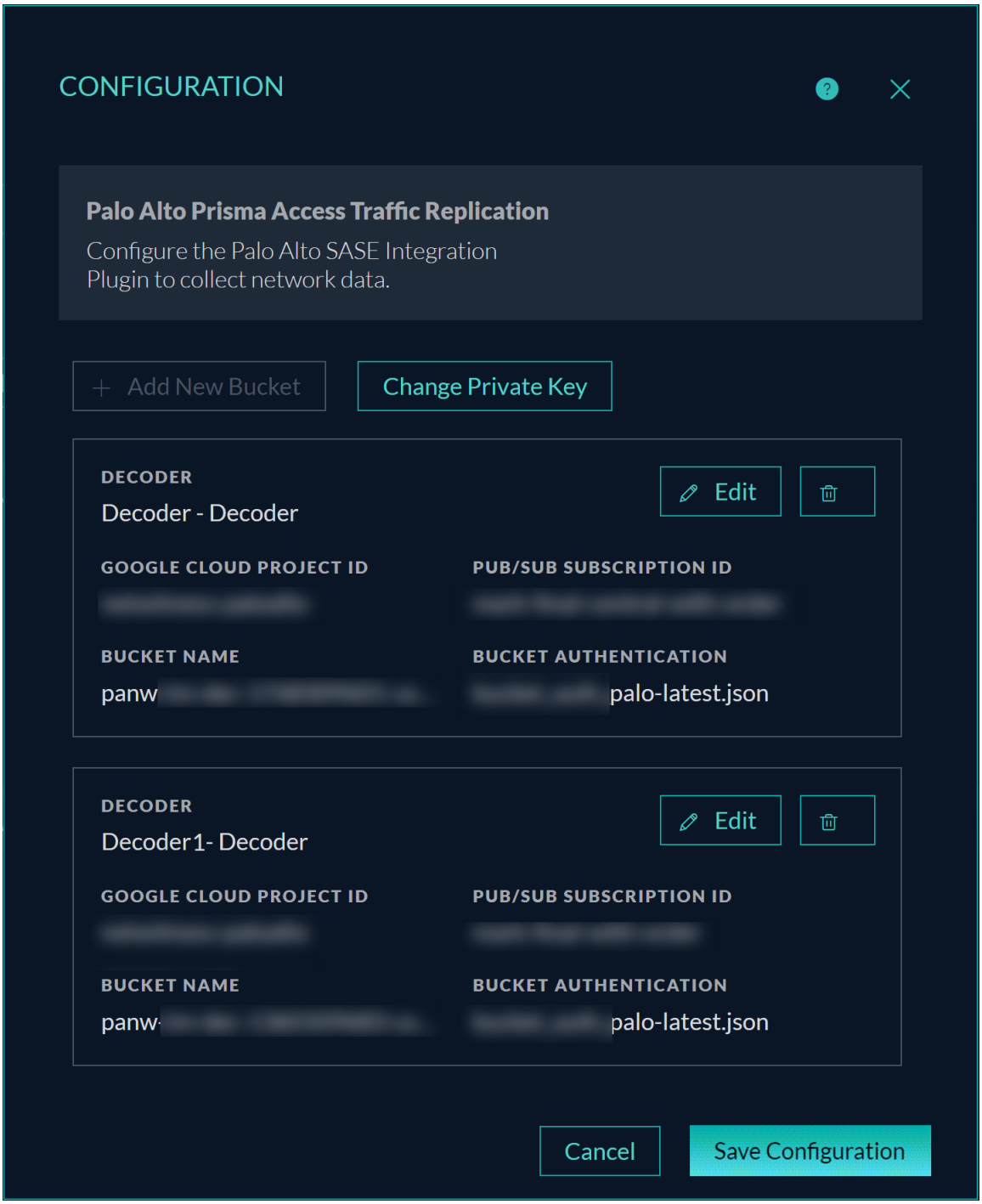


10. (Optional) Click **Change Private Key** to change the private key. It navigates you to the **Add Private Key for Decryption** section, click and then upload a new private key (.pem file) and click **Save**.
11. If you want to modify the existing bucket configuration, perform the following steps:
    - Click **Edit** will navigate to the **Edit Bucket Configuration** Section.
    - Modify the details and click **Save**.

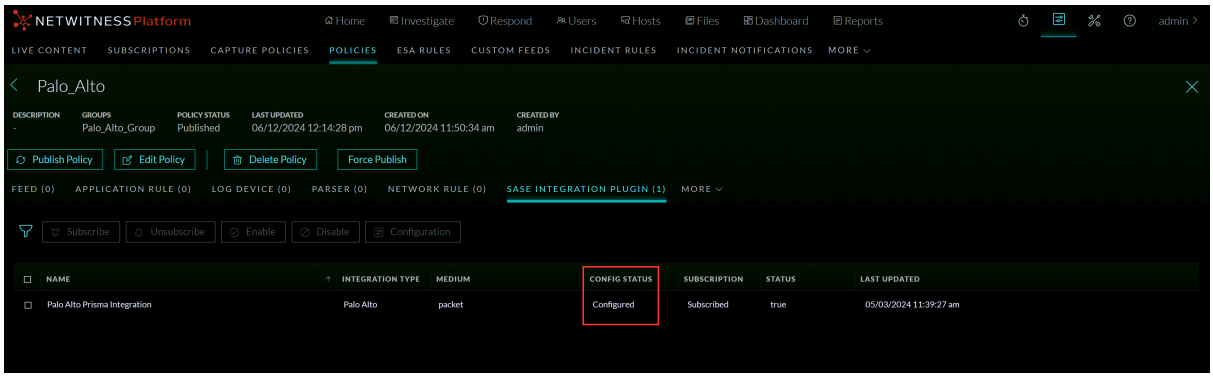
    Note: You cannot edit or change the decoder for a bucket configuration. If you need to change the decoder, you must delete the existing bucket configuration and add a new one.



12. Click **(Delete)** to remove the bucket configuration permanently.
13. Review the bucket configuration details and click **Save Configuration**.

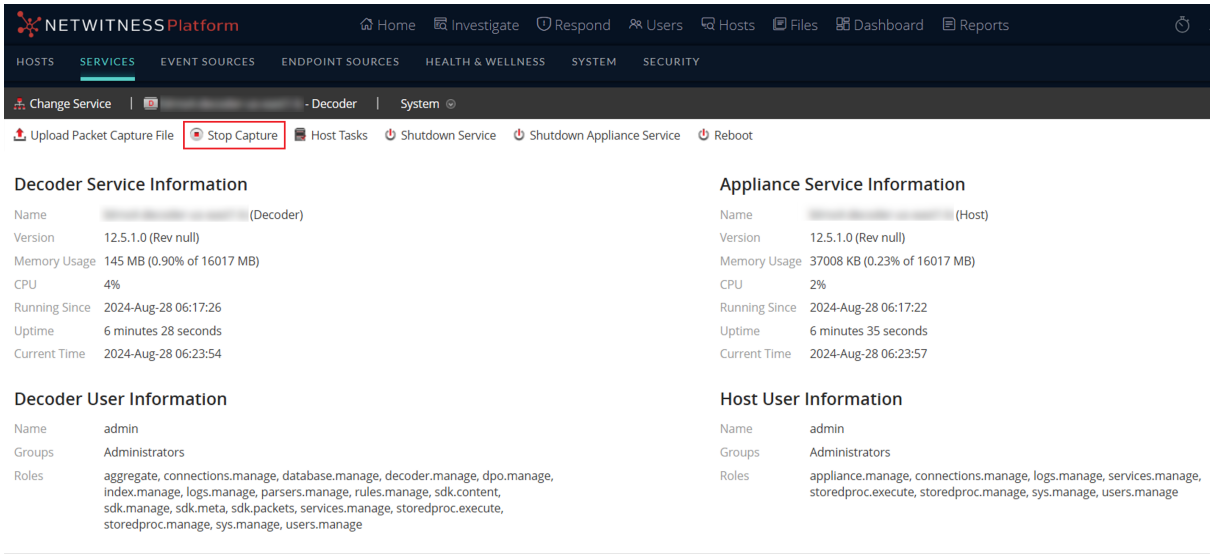


To verify if the configuration was completed successfully, ensure that the **Config Status** column displays **Configured** for the Palo Alto Prisma Integration.



14. Restart the Decoder service. Go to the **Services** view, select the Decoder service, and click  > **Restart**.
15. A Confirmation dialog request is displayed. To restart the service, click **Yes**.
16. (Optional) Navigate to the System view of the Decoder service and check if the Decoder is capturing the data.

    This option ensures the decoder has already started capturing the packets.



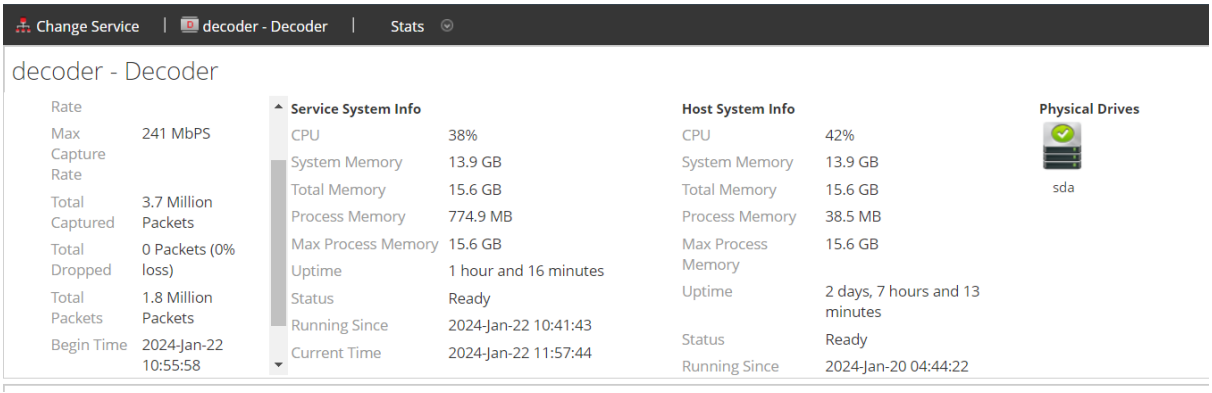
Task 4. Verify Palo Alto Prisma Events Received at Decoder

You can analyze the Palo Alto Prisma events that have been received by the Decoder and verify their accuracy.

To verify the Palo Alto Prisma Events Received at Decoder

1. Log in to the NetWitness Platform.
2. Go to  **(Admin)** > **Services**.

3. Select the **Packet Decoder** service and click  > **View** > **Stats**.
4. Under the **Key Stats** section, check the values for **Capture Rate**, **Max Capture Rate**, **Total Captured** , **Total Dropped**, and **Total Packets** for the decoder service.



Task 5. Verify Events Meta from Palo Alto Prisma in Investigate View

To verify Palo Alto Prisma events, you must first aggregate the Decoder service into the Concentrator and then go to the **Investigate** > **Events** page to view the Palo Alto Prisma events.

- Add the Decoder Service in the Concentrator
- Verify from the Investigate > Events View

Add the Decoder Service in the Concentrator

1. Log in to the NetWitness Platform.
2. Go to  **(Admin)** > **Services**.
3. In the **Services** list, select the **Concentrator** service.
4. Click  > **View** > **Config**.

   The Services Config View of the Concentrator is displayed.
5. Select the **Sources** tab.
6. Click  and select Available Services.

   The Available Services dialog is displayed.
7. Select the **Decoder** service and click **OK**.

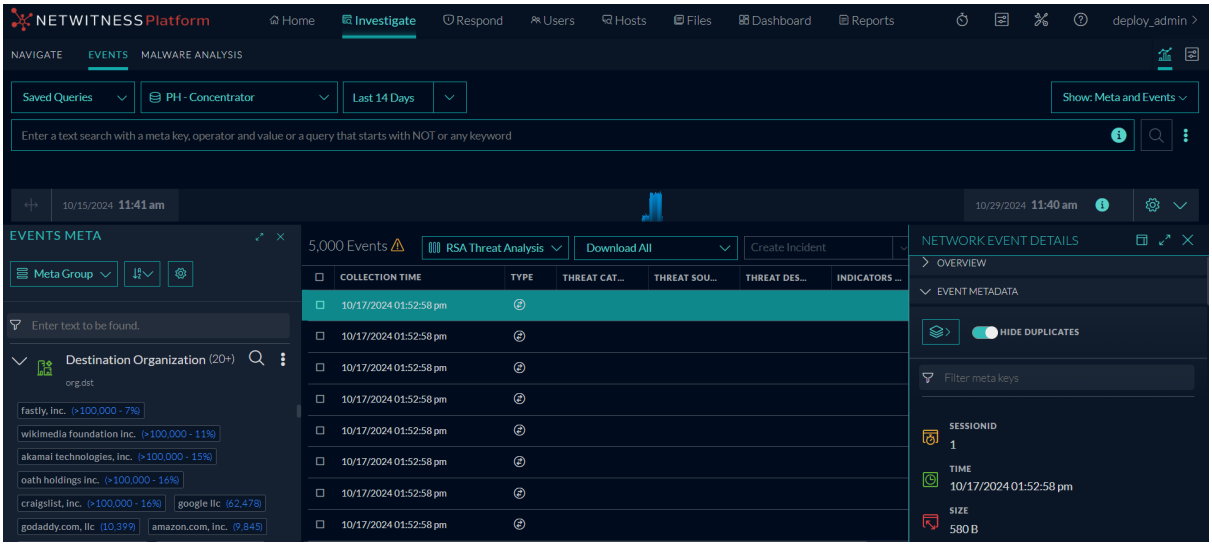
   The service authentication dialog box is displayed.

Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

8. Enter the Username and Password for the service.
9. Click **OK**.
10. Click **Apply**.

Verify from the Investigate > Events View

1. Go to **Investigate** > **Events**.
2. Select the **Concentrator** Service from the **Services** selection drop-down list.
3. Click  to load the Palo Alto Prisma events data.



Deploy Palo Alto Prisma Integration using NwConsole

This topic describes how to deploy the Palo Alto Prisma Integration using the NwConsole for users who are not utilizing the Centralized Configuration Management.

Prerequisites

Before you begin configuring the Palo Alto Prisma Integration, ensure that you have the following details:

- The NetWitness Platform (Admin Server and Packet Decoder Host) is on version 12.4 or later.
- The Decoder services are **not** managed by CCM. If CCM manages it, you can disable CCM for the particular decoder service. For more information, see topic Enable or Disable CCM for Individual Decoder Services.
- You must have the Private Key (.pem file), optional Bucket Authentication (.JSON file), GCP bucket names, local GCP project ID, and Pub/Sub Subscription ID available for configuration:
  - The Private Key (.pem file) is used to decrypt the AES key, which is used to decrypt the PCAPs. For more general information on managing and using the Private Key, please refer to Palo Alto's **Traffic Replication in Prisma Access** documentation https://docs.paloaltonetworks.com/prisma-access/administration/prisma-access-advanced-deployments/mobile-user-globalprotect-advanced-deployments/traffic-mirroring#traffic-mirroring-and-pcap-support-in-prisma-access.
  - The optional Bucket Authentication Key (.JSON file) is used to authenticate access to a bucket in GCP. Creating a Bucket Authentication Key (.JSON file) is a two-step process:
    - Create a service account in GCP with **Storage Object Viewer (roles/storage.objectViewer)**. For more information, see topic Create service accounts.
    - Create a service account key in GCP. For more information, see Create and delete service account keys.

Create Google Cloud Pub/Sub Subscription

The Subscription ID is unique to each Pub/Sub subscription within a project. Each subscription enables users to receive messages from a designated Pub/Sub topic, creating a direct link between the subscription and its corresponding topic. This setup allows for efficient message delivery, ensuring users can manage and retrieve relevant information in real-time.

To create a subscription, use the gcloud tool available on the SASE head nodes.

```
gcloud pubsub subscriptions create <SUBSCRIPTION ID> --topic-
project=<PAN GCP PROJECT ID> --topic=<PAN GCP PUB/SUB TOPIC ID> --
message-filter='attributes.bucketId="<PAN GCS BUCKET>"' --enable-
message-ordering

Created subscription [projects/<LOCAL GCP PROJECT
ID>/subscriptions/<SUBSCRIPTION ID>].
```

`--topic-project` is the home project of the topic, where all subscriptions will be received.

`--topic` is the topic ID.

`--message-filter` is the subscription filtering criteria based on the message payload. In this case, it retrieves messages containing an attribute that specifies a particular bucket ID, which is required for the integration plugin.

`--enable-message-ordering` ensures that subscription messages from the topic, which share the same ordering key (in this case, the GCS bucket of interest), are **ordered/delivered** in the same order they were published. If message ordering is not enabled, it may result in disruptions or breaks in the continuity of the incoming session data.

Any policies specific to custom messages, such as retention, must be determined by the customer according to their needs.

Note: Files in the PAN GCS bucket will have a retention period of three days.

Configure Permissions for Google Cloud Platform

By setting these permissions, the service account will have the necessary access to perform its functions effectively within the Google Cloud Platform (GCP) infrastructure.

To properly configure permissions for the service account used by the plugin, you need to grant the following access and permissions:

1. **GCS Bucket and Pub/Sub Topic Read Access**
   - Managed by **PAN** (Palo Alto Networks).
   - **GCS Bucket Read Access**: Required to retrieve new packets from the GCS bucket.
   - **Pub/Sub Topic Read Access**: It is necessary to subscribe to the Pub/Sub topic for real-time message processing.
2. **Pub/Sub Admin Role**
   - The service account must be assigned the "**Pub/Sub Admin Role**", which grants full permissions (pubsub.*) for managing topics and subscriptions.
   - This role is essential to onboard subscriptions locally within the GCP environment that hosts the NetWitness instance.
3. **Cloud API Access for Attached Service Accounts**
   - If the service account is directly attached to Decoder **VM**, it must be granted **full access to Cloud APIs** to ensure seamless communication with other GCP resources.

Deploy Palo Alto Prisma Integration

You must perform the following tasks to deploy the Palo Alto Prisma Integration on NetWitness Platform.

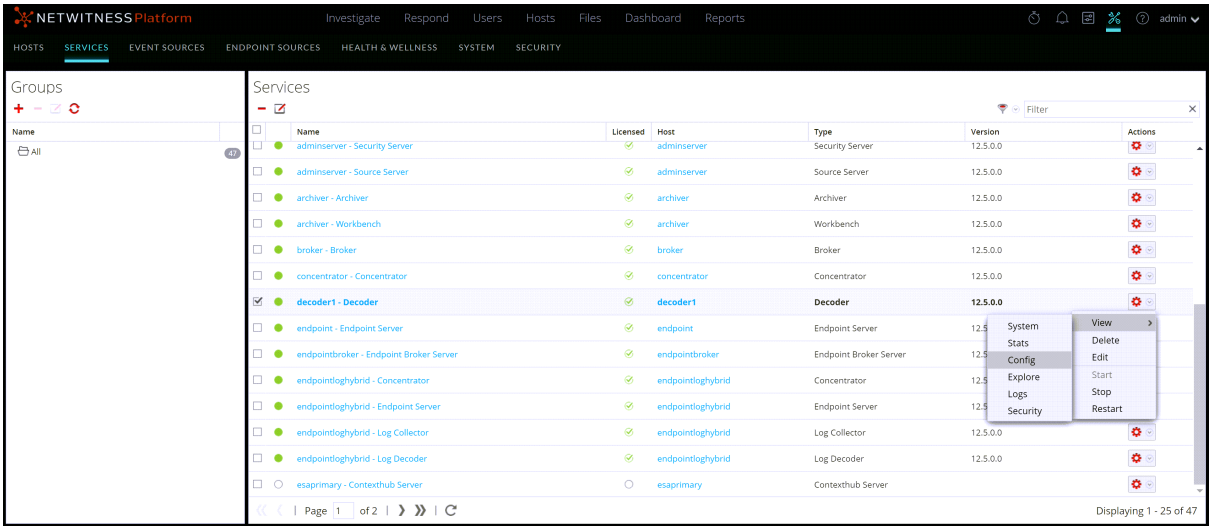
- Task 1. Map Network Adapter in Decoder for Palo Alto Prisma Integration
- Task 2. Deploy the Palo Alto Prisma Integration Plugin on Decoder
- Task 3. Verify Palo Alto Prisma Events Received at Decoder
- Task 4. Verify Events Meta from Palo Alto Prisma in Investigate View

Task 1. Map Network Adapter in Decoder for Palo Alto Prisma Integration

You must select a network adapter **(pcap_stream,Pcap File Streamer)** and enable **Capture Autostart** option through which the Decoder captures packets and processes the data.

To Map the Network Adapter in Decoder for Palo Alto Prisma Integration

1. Log in to the NetWitness Platform.
2. Go to  **(Admin)** > **Services**.
3. Select the **Packet Decoder** service and click  > **View** > **Config**.

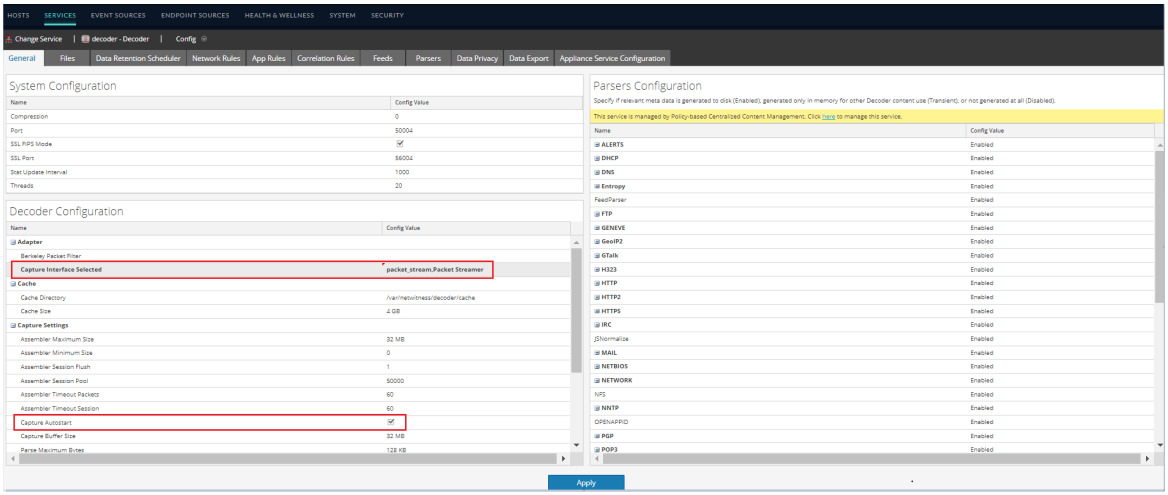


The Configure view for the Decoder service is displayed with the **General** tab open.

4. Under the **Decoder Configuration** section, do the following:
   a. Set the **Capture Interface Selected** to **pcap_stream,Pcap File Streamer** network adapter. (Applicable for 12.4 and 12.4.1)

      Set the **Capture Interface Selected** to **packet_stream,Packet Streamer** network adapter. (Applicable for 12.4.2 and above versions)

b. Enable the optional **Capture Autostart** option.



5. Click **Apply** to save the changes.

Task 2. Deploy the Palo Alto Prisma Integration Plugin on Decoder

You can search for the SASE integration Plugin from the Live Content view and deploy it on the decoder services using NWconsole.

Prerequisites

- Ensure that the **Palo Alto Prisma Integration** content type is available in the Live Content view.
- You must have the Private Key (.pem file), optional Bucket Authentication (.JSON file), GCP bucket names, local GCP project ID, and Pub/Sub Subscription ID available for configuration.

Supported Hosts

- Packet Decoder
- Packet Hybrid

To deploy Palo Alto Prisma Integration Plugin on Decoder

1. Log in to the NetWitness Platform.
2. Go to **(Configure)** > **Live Content**.
3. Select the **SASE Integration Plugin** from the **Resource Types** drop-down list in the Search Criteria panel.

   Note: To narrow the results further, you can use the different options available in the Search Criteria panel.

4. Click **Search**.

The available SASE Integration plugins are displayed.

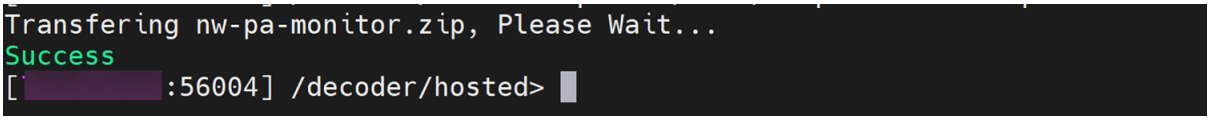
5. In the **Matching Resources** panel, select **Show Results** > **Grid**.
6. Select the **Palo Alto Prisma Integration** plugin checkbox and click **Package** > **Create**.

   The resource bundle gets downloaded to your local system.
7. Extract the resource bundle to view the **nw-pa-monitor.zip** package.
8. SSH to the Packet Decoder host.
9. Create a directory by running the following command:

   `mkdir /opt/paloalto`
10. Copy the **nw-pa-monitor.zip** package, optional **Bucket Authentication Key** (.Json) file, and **Bucket Private Key** (.pem) file to the newly created `/opt/paloalto` directory.
11. Connect to the NwConsole utility with the following command: `NwConsole`
12. Log in to the Decoder service using the following command, entering the password when prompted.

    ```
    > login localhost:56004:ssl admin netwitness
    Successfully logged in to localhost:56004 as session 1561
    ```
13. Navigate to the following directory: `cd /decoder/hosted`
14. Run the following command to install the plugin:

    `upload /opt/paloalto/nw-pa-monitor.zip`

    Note: When the installation is completed, ensure that a success message appears.
15. Navigate to the Paloalto directory: `cd /etc/netwitness/ng/hosted/paloalto`
16. Run the following command to create an instance:

    `sh configure-pa-instance.sh`
17. Enter the values in the following fields:
    - **Instance name**: Enter the instance name. Only alpha-numeric characters are allowed, and spaces are not allowed. For example, `paloalto`.
    - **Bucket name**: Enter a valid GCP bucket name. For example, `panw-tm-dec-632773000-us-east4`

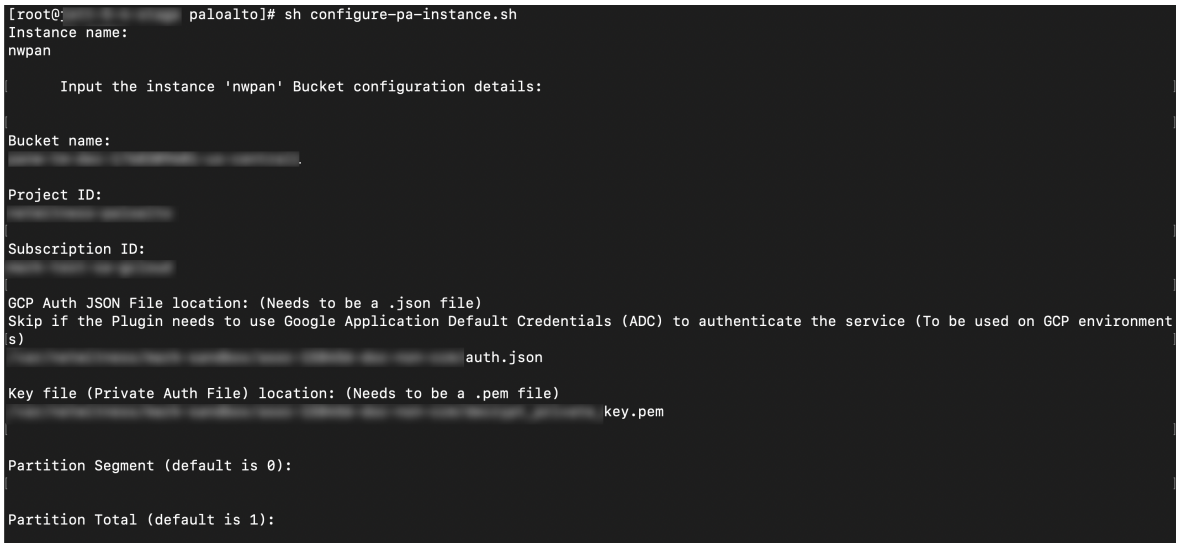
      Note: Bucket names can only contain lowercase letters, numeric characters, dashes (-), underscores (_), and dots (.). Spaces are not allowed.
    - **Project ID**: Enter the local GCP project ID that houses the NetWitness instance and Pub/Sub subscription.
    - **Subscription ID**: Enter Pub/Sub Subscription ID created for the PAN topic.

IMPORTANT: Bucket Authentication is optional if you have already configured GCP default credentials.

- **Bucket Auth File Location**: Specify the path where the Bucket Authentication Key (.json) file is kept. For example, `/opt/paloalto/bucket_auth_key.json`. The Bucket Authentication Key (.JSON file) is used to authenticate access to a bucket in GCP.

  Note: Bucket Authentication file is optional, if the customer chooses to not include this file, just press Enter when the Bucket auth file location is prompted by the script. The Bucket Authentication must have a valid bucket authentication key format extension (.JSON). The size of the Bucket Authentication (.JSON file) must not exceed 8 MB.

- **Key file (Private Auth File) Location**: Specify the path where the Bucket Private Key (.pem) file is kept. For example, `/opt/paloalto/bucket_priv_key.pem`. The Private Key (.pem file) is used to decrypt the AES key, which is used to decrypt the PCAPs.
- **Partition Segment**: Enter '0' or leave it blank, as the integration currently supports only one segment.
- **Partition Total**: Enter '1' or leave it blank, as the integration currently supports only one segment.



18. Type **yes** to use the Trusted authentication mechanism to log in to NwConsole; if you type no, you need to specify decoder credentials (username and password).

    Note: NetWitness recommends that you use a trusted authentication mechanism for communication with the decoder service, where the option is enabled by default.

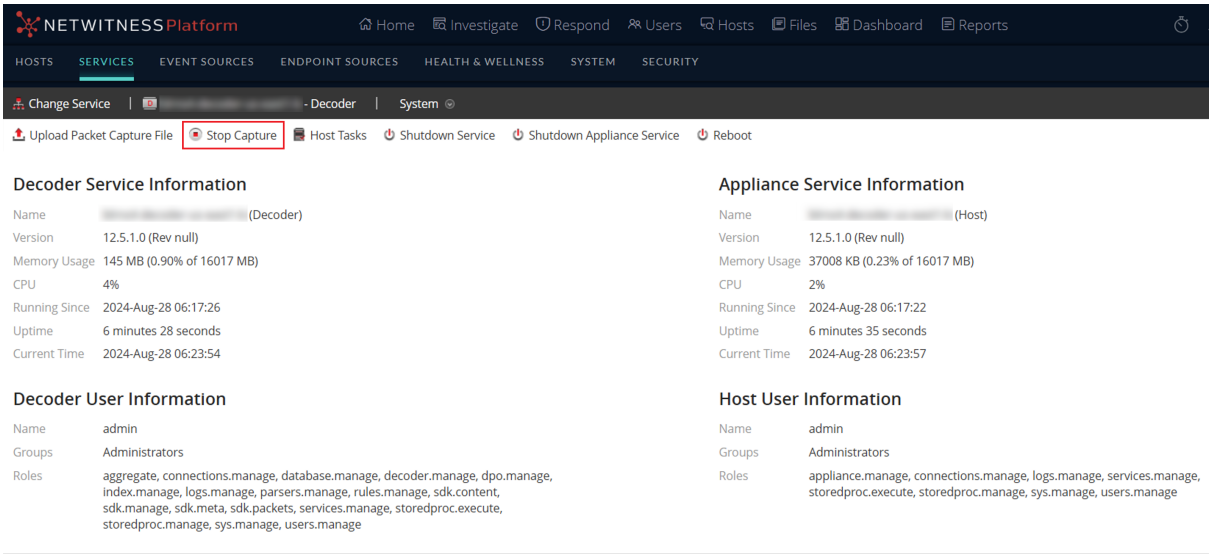
19. Type **yes** to enable the instance.

```
Do you want to use Trusted Authentication to login to NwConsole? :
Type 'yes' to use Trusted Authentication or type 'no' to use Credentials [By default, Trusted Authentication will be used] :
yes

You have selected Trusted Authentication.

Using default cert and key .pem files for Trusted Authentication..

     Login Successful

Instance 'nwpan' created
Adding GCP configuration to the instance 'nwpan' ...

Configured the Palo Alto integration instance 'nwpan'

Do you wish to enable the instance 'nwpan' right now?
Please enter 'yes' to enable the instance or 'no' to disable the instance
yes
Instance 'nwpan' enabled!

Configuration of instance creation has been completed
```

The instance is now configured successfully.

20. Restart the Decoder service. Go to the **Services** view, select the Decoder service, and click  > **Restart**.
21. A Confirmation dialog request is displayed. To restart the service, click **Yes**.
22. (Optional) Navigate to the System view of the Decoder service and check if the Decoder is capturing the data.

    This option ensures the decoder has already started capturing the packets. To view the packets in the Decoder, perform Task 3. Verify Palo Alto Prisma Events Received at Decoder

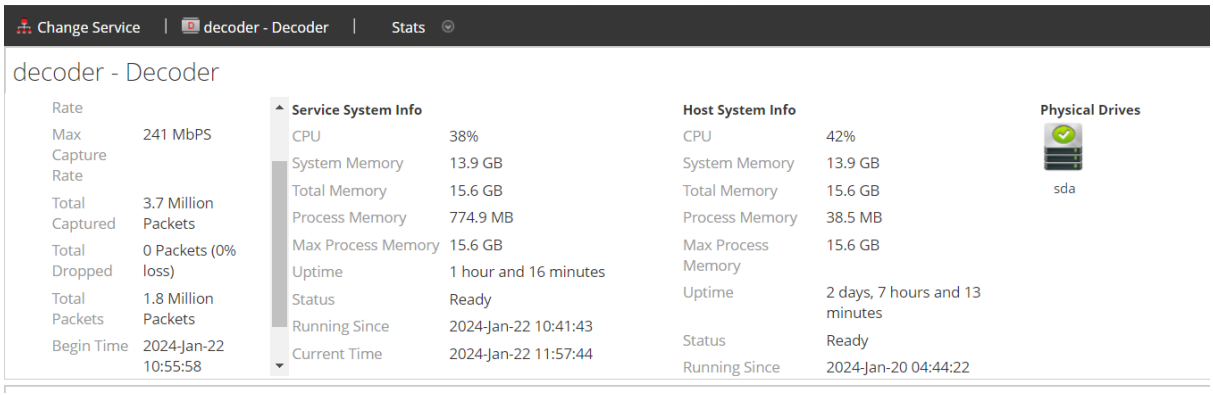


Task 3. Verify Palo Alto Prisma Events Received at Decoder

You can analyze the Palo Alto Prisma events that have been received by the Decoder and verify their accuracy.

To verify the Palo Alto Prisma Events Received at Decoder

1. Log in to the NetWitness Platform.
2. Go to **(Admin)** > **Services**.
3. Select the **Packet Decoder** service and click > **View** > **Stats**.
4. Under the **Key Stats** section, check the values for **Capture Rate**, **Max Capture Rate**, **Total Dropped**, and **Total Captured packets** for the decoder service.



Task 4. Verify Events Meta from Palo Alto Prisma in Investigate View

To verify Palo Alto Prsima events, you must first aggregate the Decoder service into the Concentrator and then go to the **Investigate** > **Events** page to view the Palo Alto Prisma events.

- Add the Decoder Service in the Concentrator
- Verify from the Investigate > Events View

Add the Decoder Service in the Concentrator

1. Log in to the NetWitness Platform.
2. Go to **(Admin)** > **Services**.
3. In the **Services** list, select the **Concentrator** service.
4. Click > **View** > **Config**.

   The Services Config View of the Concentrator is displayed.
5. Select the **Sources** tab.
6. Click + and select Available Services.

   The Available Services dialog is displayed.
7. Select the **Decoder** service and click **OK**.

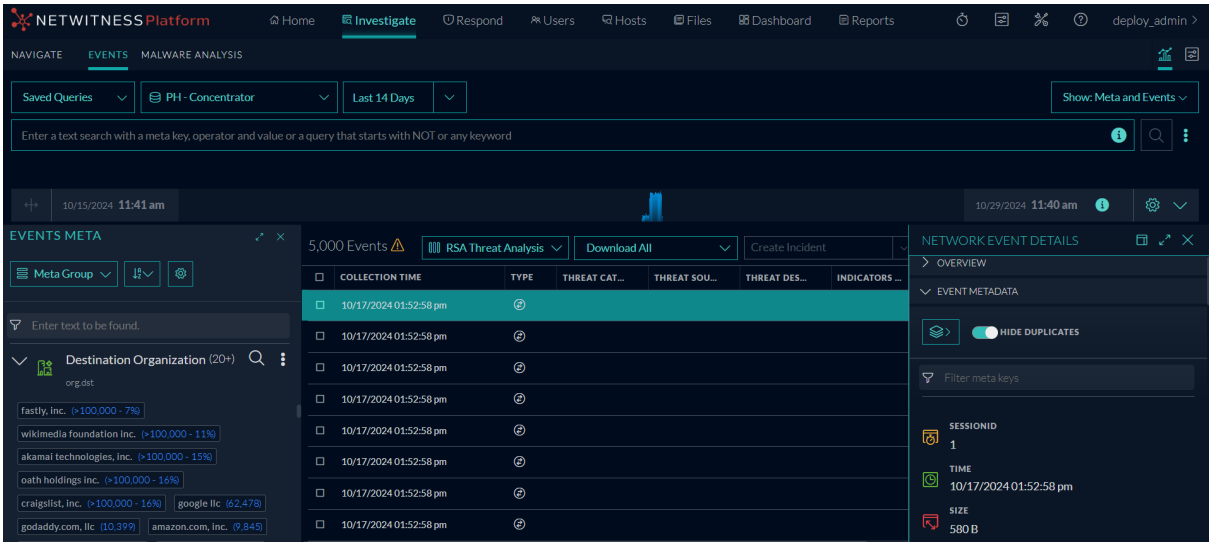
The service authentication dialog box is displayed.

Note: The services with the Trust Model enabled must be added individually. You are prompted to provide a username and password for the selected service.

8. Enter the Username and Password for the service.
9. Click **OK**.
10. Click **Apply**.

Verify from the Investigate > Events View

1. Go to **Investigate** > **Events**.
2. Select the **Concentrator** Service from the **Services** selection drop-down list.
3. Click  to load the Palo Alto Prisma events metadata.



Remove Palo Alto Prisma Integration Plugin

If you have Palo Alto Prisma Integration plugin deployed on a policy and no longer want to use it, perform the following steps to delete it.

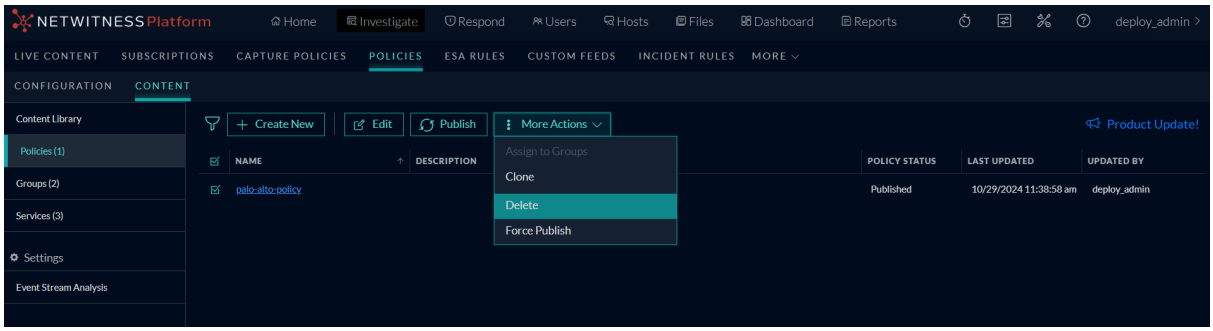
To remove the Palo Alto Prisma Integration completely, first delete the policy containing the plugin from **Policies** view, and then delete the plugin details on the Decoder host.

IMPORTANT: If you have deployed the plugin using CCM, you must perform steps **1** and **2** procedures. If you have deployed the plugin using NwConsole, you can proceed directly to step 2 and complete the procedure.

- Step 1: Remove the Policy containing Palo Alto Prisma Integration
- Step 2: Remove the Palo Alto Prisma Plugin Details from Decoder Host

Step 1: Remove the Policy containing Palo Alto Prisma Integration

1. Go to **(Configure) > Policies**.
2. In the policies panel, click **Content**.
3. Click **Policies**. The available policies are displayed.
4. Select one or more policies and in the **More Actions** drop-down list in the tool bar, click **Delete**.



The **Delete Policies** dialog is displayed.

5. To delete the deployed content from the group's services upon deleting the policy, select the option **Delete deployed content from the group's services on policy removal**.

Note: Removing the policy will delete only the Palo Alto Prisma Configuration details and not the plugin on the Decoder host.

6. Click **Delete** to permanently delete the selected policy.

Deletion will take immediate effect and the policy will no longer be available in any group.

Note:
- You can also delete a policy from the **Policy Details** view. For more information on deleting a policy from the **Policy Details** view, see View a Policy topic.
- The policy status changes to **Failed** if policy deletion fails for any particular reason.

Step 2: Remove the Palo Alto Prisma Plugin Details from Decoder Host

1. SSH to the Packet Decoder Host.
2. Run the following command to stop the Decoder service:

   ```
   systemctl stop nwdecoder
   ```

3. Navigate to the following path:

   ```
   /etc/netwitness/ng/hosted
   ```

4. Delete the **paloalto** folder.
5. Run the following command to start the Decoder service:

   ```
   systemctl start nwdecoder
   ```

6. Connect to the Decoder host by using the Decoder IP address and Port 50104 as follows:`<decoder-ip>:50104`
7. Navigate to the following path: `/decoder/hosted/paloalto`
8. Select the **delete** operation from the drop-down list and click **Send**.

The plugin details are removed from the decoder.

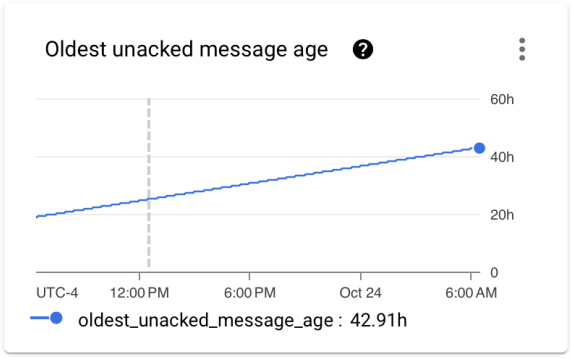
Troubleshooting NetWitness SASE Deployment

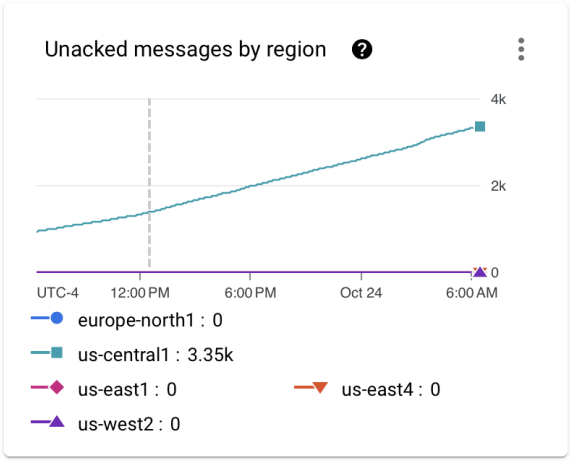
This table outlines potential issues and their corresponding solutions when deploying the NetWitness Platform SASE with Palo Alto Prisma.

Error/Problem	Possible Causes	Solutions
"GCS/Pub/Sub … authentication failed"	This error message appears when there are some authentication errors with the service account configured for the plugin	In this scenario, do the following: 1. If a credentials file is not used for explicit authentication, ensure the service account is attached to the VM with full access to Cloud APIs. 2. Confirm that the service account has been onboarded with read access to the relevant GCP resources.
"Error encountered when downloading file"	This error message appears when the plugin could not retrieve a file from the bucket.	In this scenario, do the following: 1. Check the log for a best-effort description of the error encountered. 2. Verify if the file still exists. In many cases, the file may have been deleted, as files are retained in the bucket for only 3 days. If the Pub/Sub message retention exceeds the file retention period, this could cause the error.
"Failed to process due to extraction error"	This error message appears if the plugin fails to unzip the ZIP file it received from the bucket.	During plugin recovery, inspect the staging folder for files that may contain invalid ZIP file content or headers, which is often caused by truncated downloads resulting from plugin crashes.
"Failed to process due to stream error"	This error message appears when the plugin could not stream processed packet data to the Decoder's streamer adapter.	In this scenario, do the following: 1. Investigate whether the packet data is invalid or corrupt. 2. Note that the default behavior of the Decoder is to drop and re-establish the connection when such exceptions occur. 3. Ensure that the plugin attempts to reconnect to the Decoder after a connection drop.

Error/Problem	Possible Causes	Solutions
"JSON decryption ran into an error"	This error message appears if the plugin could not decrypt the key data provided in the ZIP file in question.	Verify that the public-private keys are paired correctly.
Received message count is increasing, but not PCAP transferred	The plugin is receiving messages from the subscription, but the files are not being processed correctly.	• Identify any errors occurring during the processing of the PCAP files. • Check for issues with message payload processing, such as key mismatches or missing payloads, which may require attention from the Engineering team.
Unresolved Python modules	This error message appears if the plugin cannot resolve some code dependencies.	Verify if there was a packaging or build issue during the release that was preventing the module from being installed correctly. If so, escalate this matter with the NetWitness Support team.

Error/Problem	Possible Causes	Solutions
Files dropped when max_ queue_size is full	If the Decoder cannot process files from the bucket quickly enough as the downloaded queue increases, the queue can become full and the oldest file in the queue will be dropped and replaced with a newer one.	By default, the plugin will download at most 10 files every download "round" (`max_file_downloads`) and the plugin will manage a backlog of 50 downloaded files (`max_queue_size`). This warning appears when the configured max queue size is met or exceeded. This situation arises when the Decoder cannot offload/process files from the backlog fast enough as files are continuously downloaded from the bucket. • Config option `max_queue_sleep` can be used to control what happens on meeting the max queue size. • The option is disabled by default, which sets the oldest files in the queue to be removed and replaced with newer files that were just downloaded on previous download rounds. • If old files are replaced, the impact is greatest when there are high message backlogs from plugin downtime. During the recovery time following a plugin restart, many old files may be dropped and will not be processed by the Decoder. • When the plugin is not capturing, the subscription continues to retrieve messages from the PAN topic and retains messages according to the configured retention policies. • Instead of dropping the old files, the plugin can be configured to sleep until the backlog isn't full, delaying new file downloads from the bucket. Refer to the image below for an example of a subscription with a large backlog of messages.





Error/Problem	Possible Causes	Solutions
Disk usage advisory for `max_queue_size`	The `max_queue_size` impacts the disk space usage.	The default value of 50 unzipped file is 10 GB on disk at 200 MB per file in the staging directory under `/var/netwitness`, which should be configured based on the bandwidth for the staging and working directories. • Files from the bucket can be a variable size but will be at most 200 MB; the cutoff for a file is 200 MB in size or the last 5 minutes of traffic, whichever comes first. • The plugin uses staging and working folders located in the Decoder's data directory (`/var/netwitness/decoder/hosted/paloalto/%INSTANCE_NAME%/...`) • The staging area holds the downloaded unzipped ZIP files, while the working area holds the extracted packet data ready for streaming to the Decoder. • The maximum queue size can be configured at `max_queue_size` and adjusted to accommodate more downloaded files staged simultaneously. • The working disk locations can be adjusted in the `staging_folder` and `working_folder` if the default location in the data directory is not suitable. • If utilizing the Decoder's data directory, any minimum free space settings for the packet, meta, and session databases must be carefully considered while configuring the queue size and working locations. • Considering the variable sizes of the PCAP files, there are no size restrictions based on the disk footprint. Any guardrails must be enforced through the configurable queue and working area settings.