Panda SIEMFeeder

Infrastructure Guide de Panda SIEMFeeder

Author: Panda Security

Version: 3.10.00

Date: 4/10/2025

Legal Notice.

Registered Trademarks.

Contact Information.

Corporate Headquarters:

Panda Security

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 Spain.

https://www.pandasecurity.com/en/office-locator/

About the Panda SIEMFeeder Infrastructure Guide

To get the latest version of the documentation in PDF format, go to:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-EN.pdf

Download the Panda SIEMFeeder Software

To get the Panda SIEMFeeder installation package, go to: **https://www.pandasecurity.com/en-us/support/card?id=950031**

Panda SIEMFeeder Events Guide

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeederAD-EventDescriptionGuide-EN.pdf

Panda Adaptive Defense 360 and Panda Adaptive Defense Administration Guides

Administration guides for Aether products:

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSE360oAP-guide-EN.pdf

https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/latest/ADAPTIVEDEFENSEoAP-guide-EN.pdf

Panda Partner Center Administration Guide

You can find the latest version of this guide at:

http://documents.managedprotection.pandasecurity.com/AdvancedGuide/PARTNERCENTER- Manual-EN.pdf

For more information about a specific topic, see the product online help at:

https://documents.managedprotection.pandasecurity.com/Help/v77000/Partners/en-us/Content/index.htm

Technical Support

Panda Security provides global support services aimed at responding to specific questions regarding the operation of the company products. The technical support team also generates documentation that covers technical aspects of our products. This documentation is available in the eKnowledge Base portal.

To access specific information about the product, go to:

https://www.pandasecurity.com/en/support/siemfeeder/

Panda SIEMFeeder Infrastructure Guide Survey

Rate this guide and send us suggestions and requests for future versions of our documentation:

https://es.surveymonkey.com/r/feedbackSIEMFeederInfManEN

Contents

Chapter 2

Preface

This guide provides the information and procedures necessary to implement the Panda SIEMFeeder and Panda SIEMFeeder for Partners services.

Chapter Contents

Intended Audience

This document is intended for:

- Technical staff responsible for managing the IT systems of companies that have contracted the Panda SIEMFeeder service.
- Technical staff of the managed security service provider (MSSP) that has contracted the Panda Panda SIEMFeeder for Partners service.

Compatible Security Products

Panda SIEMFeeder and Panda SIEMFeeder for Partners require that one of these products be installed on protected computers:

- Panda Adaptive Defense (compatible with Panda SIEMFeeder and Panda SIEMFeeder for Partners)
- Panda Adaptive Defense 360 (compatible with Panda SIEMFeeder and Panda SIEMFeeder for Partners)

All the procedures and instructions in this guide apply equally to all of the aforementioned products. Also, the term "Panda Adaptive Defense" is used generically to refer to all of those products, because there is no difference among them with regard to the service.

Document Structure

The information in this guide is divided into three sections, each of which is intended for different areas/technical profiles within the IT department of a company or MSSP:

- **Architecture information** (chapters 2 and 3): Intended for systems architects who need to have global visibility into the service to assess the impact of any changes made to the organization IT infrastructure and generate management and recovery procedures.
- **Service requirements information** (chapter 4): Intended for system administrators who need to provision the resources needed for the service to work correctly.
- **Service deployment information** (chapters 5 and 6): Intended for IT security specialists who configure the network access required to enable integration of the service into the company or the MSSP SIEM server.

Icons

This document uses these icons:

Explanations and additional information, such as an alternate method for performing a certain task.

Suggestions and recommendations.

See other chapters or sections in the guide for more information.

Chapter 3

Panda SIEMFeeder Architecture

Panda SIEMFeeder is the Panda service that delivers information and knowledge generated by the Panda Adaptive Defense products to customer SIEM platforms.

Panda SIEMFeeder enables you to:

- Uncover unknown threats, advanced malware (Advanced Persistent Threats), and targeted attacks.
- Gain in-depth visibility of the activity of processes that run across the network structures of an organization.

For more information about the equivalent solution to Panda SIEMFeeder for security service providers (Panda SIEMFeeder for Partners) see ***Panda SIEMFeeder for Partners Architecture*** *en la página* ***17****.*

Chapter Contents

Service Objectives

Panda SIEMFeeder acts as a link between the protection software installed on your company computers and the SIEM server of your company. Information flow generated by Panda

SIEMFeeder:

1. Panda Adaptive Defense continuous monitoring sends the Panda cloud the telemetry generated by the applications run on a customer systems.
2. Panda SIEMFeeder enriches the activity data with security intelligence generated by Panda.
3. Panda Importer retrieves the enriched information from the Microsoft Azure infrastructure assigned to you, and sends it directly to your SIEM server or to one of the supported platforms (Kafka and Syslog) for leverage.

Monitored Activity Enrichment

Panda Adaptive Defense monitors the actions taken by the processes run on user computers. These actions are sent to the Panda cloud platform, where they are analyzed using machine learning techniques on a big data infrastructure to extract security intelligence. This information enables Panda to classify each and every process run by your users with 99.999% accuracy.

Panda SIEMFeeder gathers information about the events monitored by Panda Adaptive Defense and the security data generated, creating a single data flow compatible with your SIEM server.

Panda SIEMFeeder does not make any changes to the settings of a monitored computer or network. The service operates within the Panda infrastructure, receiving data automatically from each workstation and server on your IT network. This data is normalized, enriched, and sent to your SIEM server for leverage.

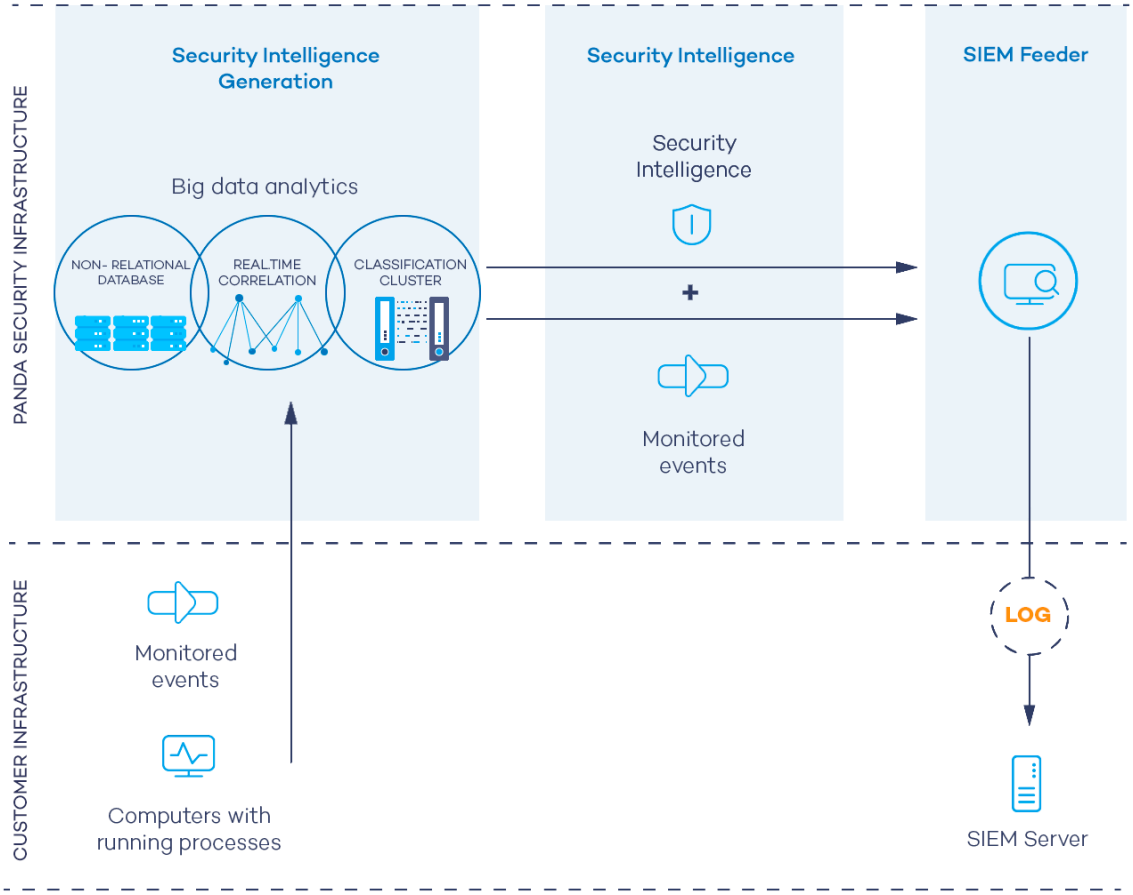

Figure 3.1: Information flow generated by Panda Adaptive Defense and Panda SIEMFeeder

Benefits of the Service

Panda SIEMFeeder delivers information about the activity of processes run on your IT network. With the security information provided, you can:

- **View the evolution of the malware detected on the network**: Whether it was run or not, the infection vector, and the actions taken by processes. With this information, you can make decisions to take remediation actions and adjust security policies.
- **View the actions run by each process** regardless of its classification: This enables you to detect suspicious activities of programs run. Panda SIEMFeeder compiles data that can be used to reach conclusions about their potential risk.
- **View attempts to access confidential corporate information**: This prevents data leakage and theft. Panda SIEMFeeder shows the Office files, databases, and other repositories of confidential information accessed by malware.
- **View the network connections made by processes**: This identifies suspicious or potentially risky destinations used to exfiltrate data.

- **Find all executed programs**: This is useful for programs with known vulnerabilities installed on user computers, to design software update plans and adjust security policies.

General Architecture

The Panda SIEMFeeder service consists of these components:

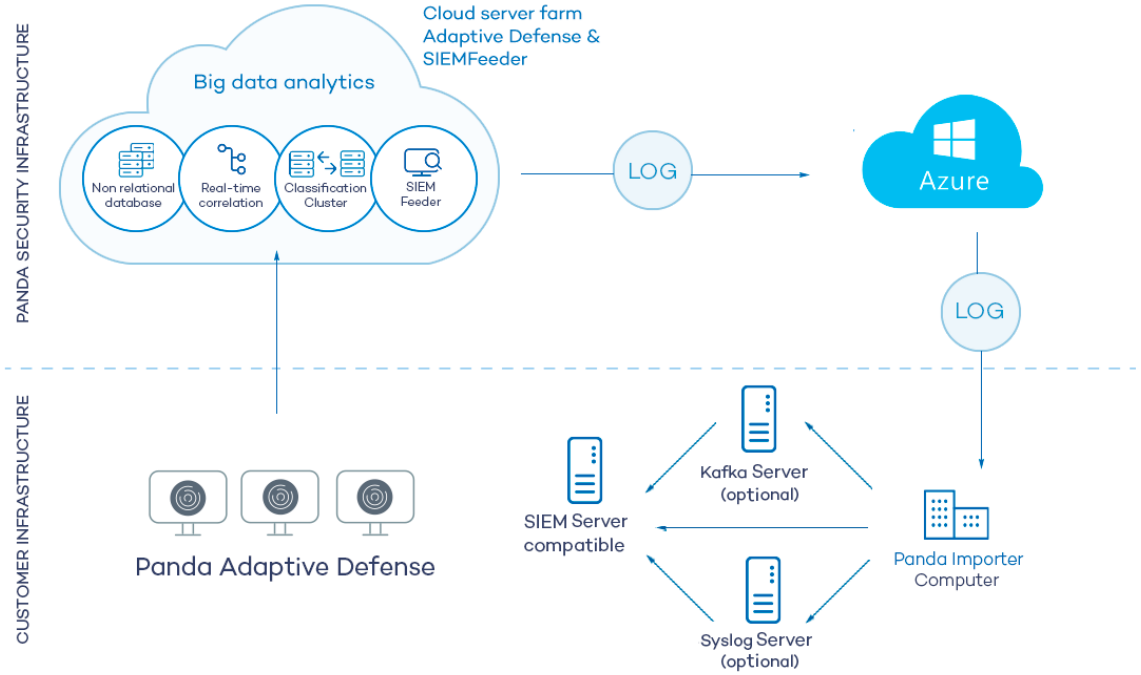

Figure 3.2: Logical diagram of the components that make up Panda SIEMFeeder and their relationships

The figure shows these items:

- **Computers on the network:** Computers on the network that are protected by Panda Adaptive Defense or Panda Adaptive Defense 360.
- Panda **cloud infrastructure**: The Panda cloud infrastructure stores data from the processes that run and analyzes the data to extract security intelligence.
- Panda SIEMFeeder **service:** The Panda SIEMFeeder service collects events and security data and encapsulates the data in the form of log files to send them to the Microsoft Azure platform.
- **Microsoft Azure infrastructure**: Azure is a cloud computing platform that receives log files from the Panda SIEMFeeder service and stores them temporarily before they are downloaded by Panda Importer.
- **Panda Importer computer**: A computer on the customer network that runs Panda Importer and downloads the available log files from the Azure infrastructure.
- **Kafka server (optional)**: A computer on the customer network that manages the queue of log files it receives from Panda Importer and sends them to the company SIEM server.

- **Syslog server (optional)**: A computer on the customer network that collects the log files it receives from Panda Importer and sends them to the company SIEM server.
- **SIEM server**: A customer server that receives the data that Panda Importer downloads and generates dashboards that help detect suspicious processes that can pose a security threat.
- **Local and perimeter firewalls**: Firewalls protect inbound and outbound data traffic between the computer that runs Panda Importer and the Azure infrastructure.

Benefits of the Azure Platform

Panda SIEMFeeder generates log files asynchronously and stores them temporarily until Panda Importer collects and integrates them in your SIEM system. To do that, it uses cloud-based services hosted on the Azure platform. These services have these characteristics:

- **Cloud-based storage**: High availability service, meaning the service is available 24 hours a day, from anywhere in the world. Maximum amount of data that the Azure platform retains is 80 GB for each customer. Maximum number of days that the Azure platform retains log files is seven days.
- **Encrypted communications**: The information exchanged between the Panda Importer computer and the Azure platform is encrypted with the SSL cryptographic protocol.
- **Authenticated communications**: To manage authentication and authorization processes, Panda Importer uses two independent tokens to negotiate the shared key required to access the Panda SIEMFeeder platform. Each token has a different expiration time to ensure data access confidentiality.

*For more information, see **Appendix 2: Security Architecture** en la página **61***

- **Compressed communications**: The Azure platform stores data in a compressed file format to reduce bandwidth usage when data is downloaded.
- **Push-based data delivery mechanism**: To facilitate firewall configuration, connections to the Azure infrastructure are outbound from your network. After Panda Importer establishes a communication channel, Azure sends all new log files available on the platform using push messages.

Information Flow

1. Panda Adaptive Defense constantly monitors and collects process activity. These actions are sent to the Panda cloud platform.
2. This data is enriched with security intelligence in the Panda cloud and placed in the Microsoft Azure infrastructure, where it is temporarily stored.

3. Panda Importer, which runs on a server on your network, downloads the generated log files from Azure, managing them in different ways based on its settings:
    1. Stores log files in a folder that the SIEM server of your organization can connect to, managing the volume of files so as not to exceed the limit set by you.
    2. Sends log files to an Apache Kafka queue server, where the files are sent to the SIEM server of the organization.
    3. Sends log files to a syslog server, where the files are sent to the SIEM server of the organization.
4. The SIEM server imports the log files and analyzes them periodically to incorporate the information into its repository and generate dashboards.

Chapter 4

Panda SIEMFeeder for Partners Architecture

Panda SIEMFeeder for Partners is the Panda service for partners that delivers information and knowledge generated by the Panda Adaptive Defense products installed on your customer computers to your SIEM platform.

Panda SIEMFeeder for Partners enables you to:

- Uncover unknown threats, advanced malware (Advanced Persistent Threats), and targeted attacks.
- Gain in-depth visibility of the activity of processes that run across the network structures of an organization.

Chapter Contents

Service Objectives

Panda SIEMFeeder for Partners acts as a link between the protection software installed on your customer computers and the SIEM server of your company. Information flow generated by Panda SIEMFeeder:

1. Panda Adaptive Defense continuous monitoring sends the Panda cloud the telemetry generated by the applications run on your customer computers.

2. Panda SIEMFeeder for Partners enriches the activity data with security intelligence generated by Panda.
3. Panda Importer retrieves the enriched information from the Microsoft Azure infrastructure assigned to you, and sends it directly to your SIEM server or to one of the supported platforms (Kafka and Syslog) for leverage.

Monitored Activity Enrichment

Panda Adaptive Defense monitors the actions executed by processes on your customer computers. These actions are sent to the Panda cloud platform, where they are analyzed using machine learning techniques on a big data infrastructure to extract advanced security intelligence. This information enables Panda to classify each and every process run on your customer computers with 99.999% accuracy.

Panda SIEMFeeder for Partners gathers information about the events monitored by Panda Adaptive Defense and the security data generated, creating a single data flow compatible with your SIEM server.

Panda SIEMFeeder for Partners does not make any changes to the settings of your customer computers. The service operates within the Panda infrastructure, receiving data automatically from each workstation and server on your customer IT networks. This data is normalized, enriched, and sent to your SIEM server for leverage.

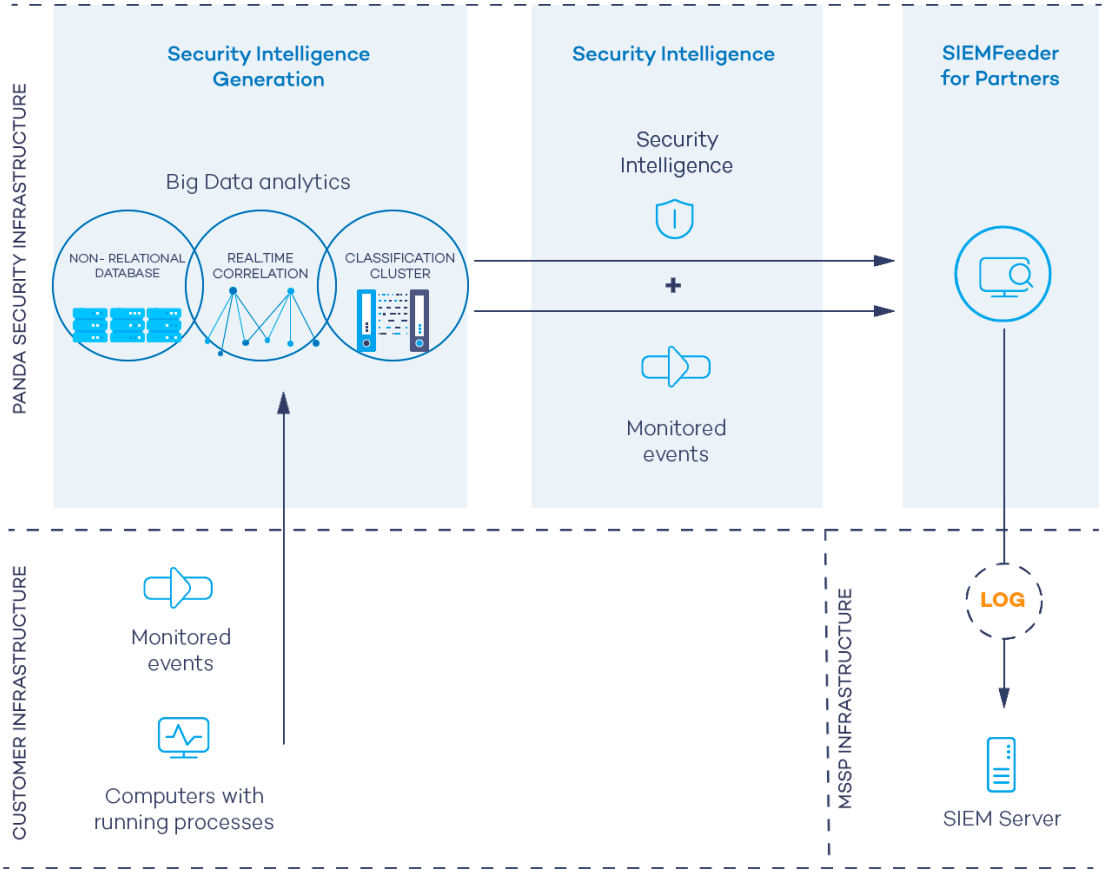

Figure 4.1: Information flow generated by Panda Adaptive Defense and Panda SIEMFeeder

Benefits of the Service

Panda SIEMFeeder for Partners delivers information about the activity of processes run on your customer IT networks. With the security information provided, you can:

- **View details of the malware detected on your customer IT networks**, and see whether it was run or not, the infection vector, and the actions taken by processes. With this information, you can make decisions to take remediation actions and adjust security policies for the organizations you manage.
- **View the actions run by each process** regardless of its classification: This enables you to detect suspicious activities of programs run. Panda SIEMFeeder for Partners compiles data that can be used to reach conclusions about their potential risk.
- **View access by processes to your customer confidential information**, preventing data leakage and theft. Panda SIEMFeeder shows the Office files, databases, and other repositories of confidential information accessed by malware.
- **View the network connections made by processes**: This identifies suspicious or potentially risky destinations used to exfiltrate data.

- **Find all executed programs**: This is useful for programs with known vulnerabilities installed on user computers, to design software update plans and adjust security policies for the organizations you manage.
- **Apply centralized settings through Panda Partner Center**: This enables you to push out settings to all your customers simultaneously.
- **Install the service easily and securely**: Configure the telemetry download service only once and add new customers without having to deploy or install any additional components. Additionally, Panda SIEMFeeder for Partners ensures safe downloads through secure TLS (Transport Layer Security) connections from the Panda cloud.
- **Keep storage costs down**: Filter required events before they reach your infrastructure, minimizing bandwidth usage and storage costs.

Architecture

The Panda SIEMFeeder for Partners service consists of these components:

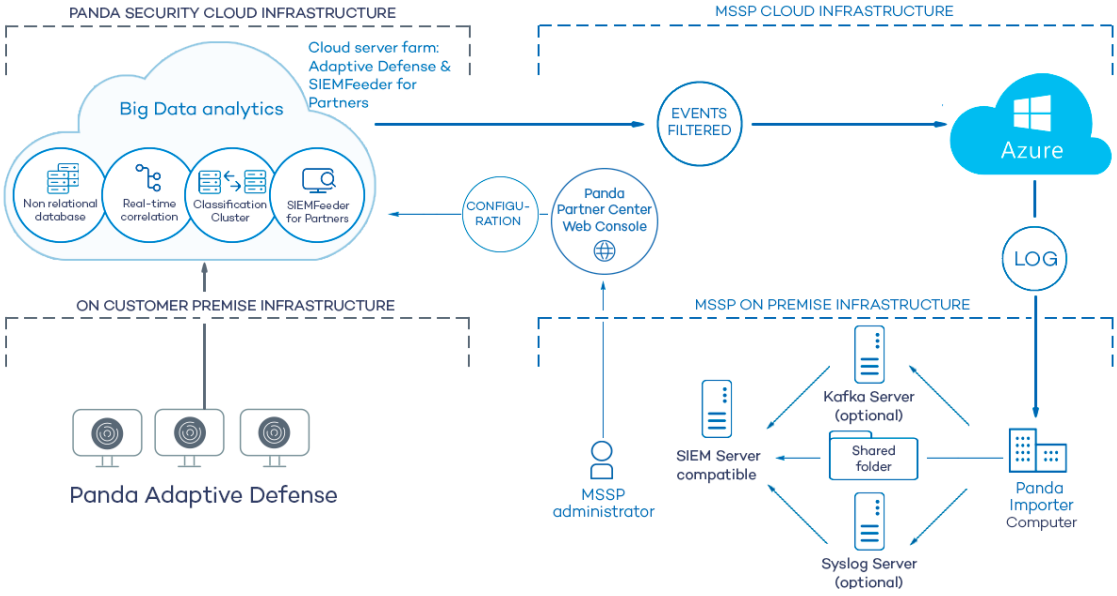

Figure 4.2: Logical diagram of the components that make up Panda SIEMFeeder for Partners and their relationships

The figure shows these items:

- **Computers on the customer network**: Computers on the customer network that are protected by Panda Adaptive Defense or Panda Adaptive Defense 360.
- **Panda cloud infrastructure**: The **Panda** cloud infrastructure stores data from the processes that run and analyzes the data to extract security intelligence.
- **Panda SIEMFeeder for Partners service**: The **Panda SIEMFeeder for Partners** service collects events and security data and encapsulates the data in the form of log files to send them to the Microsoft Azure platform.

- **MSSP Microsoft Azure infrastructure**: Azure is a cloud computing platform that receives logs from the Panda SIEMFeeder for Partners service and stores them temporarily before they are downloaded by Panda Importer.
- **Panda Importer computer**: A computer on the MSSP network that runs Panda Importer and downloads the available logs from the Azure infrastructure.
- **Kafka server (optional)**: A computer on the MSSP network that manages the queue of logs it receives from Panda Importer and sends them to the SIEM server.
- **Syslog server (optional)**: A computer on the MSSP network that collects the logs it receives from Panda Importer and sends them to the SIEM server
- **Shared folder (optional)**: A storage system on the MSSP network where Panda Importer deposits the logs in the absence of more advanced resources, such as a syslog or Kafka server.
- **SIEM server**: An MSSP server that receives the data that Panda Importer downloads and generates dashboards that help detect suspicious processes that can pose a security threat to the MSSP customers.
- **Local and perimeter firewalls**: Firewalls protect inbound and outbound data traffic between the computer that runs Panda Importer and the Azure infrastructure.
- **Panda Partner Center Console**: Enables the MSSP to activate the Panda SIEMFeeder for Partners service for customers and configure it to receive only selected events.

Benefits of the Azure Platform

Panda SIEMFeeder for Partners generates logs asynchronously and stores them temporarily until they are collected and integrated in a SIEM server. To do that, it uses cloud-based services hosted on the Azure platform. These services have these characteristics:

- **Cloud-based storage**: High availability service, meaning the service is available 24 hours a day, from anywhere in the world. Maximum amount of data that the Azure platform retains is 80 GB. Maximum number of days that the Azure platform retains log files is seven days.
- **Encrypted communications**: The information exchanged between the MSSP Panda Importer computer and the Azure platform is encrypted with the SSL cryptographic protocol.
- **Authenticated communications**: To manage authentication and authorization processes, Panda Importer uses two independent tokens to negotiate the shared key required to access the Panda SIEMFeeder for Partners platform. Each token has a different expiration time to ensure data access confidentiality.

*For more information, see **Appendix 2: Security Architecture** en la página **61***

- **Compressed communications**: The Azure platform stores data in a compressed file format to reduce bandwidth usage when data is downloaded.
- **Push-based data delivery mechanism**: To facilitate firewall configuration, connections to the Azure infrastructure are outbound from your network. After you establish a communication channel, Azure sends all new log files available on the platform using push messages.

Information Flow

1. Panda Adaptive Defense constantly monitors and collects process activity. These actions are sent to the Panda cloud platform.
2. This data is enriched with security intelligence in the Panda cloud and placed in the Microsoft Azure infrastructure, where it is temporarily stored.
3. Panda Importer, which runs on a server on your network, downloads the generated log files from Azure, managing them in different ways based on its settings:
    1. Stores log files in a folder that the SIEM server of your organization can connect to, managing the volume of files so as not to exceed the limit set by you.
    2. Sends log files to an Apache Kafka queue server, where the files are sent to the SIEM server of the organization.
    3. Sends log files to a syslog server, where the files are sent to the SIEM server of the organization.
4. The SIEM server imports the log files and analyzes them periodically to incorporate the information into its repository and generate dashboards.

Service Provider General Operations

1. Checks that the subscription to the Panda SIEMFeeder for Partners service is active in Panda Partner Center. See **Product and License Management**. If your subscription has expired or you are not a Panda SIEMFeeder for Partners, customer, contact your assigned Panda sales representative.
2. Checks the connectivity of the items shown in figure **Architecture**, especially with respect to communication between Panda Importer and Azure. See **Firewall Configuration** en la página **27**.
3. Checks the deployment and installation requirements. See **Deployment and Integration Requirements** en la página **26**.
4. Installs Panda Importer on your IT infrastructure. See **Install and Configure Panda Importer on Windows Systems** en la página **33** or **Install and Configure Panda Importer on Linux Systems** en la página **45**.

5. Creates a Panda SIEMFeeder for Partners setting profile in Panda Partner Center detailing the groups of events to be sent to the Azure platform. See **Panda SIEMFeeder for Partners Settings**.

6. Associates the newly created settings profile with customers. See **Assigning and Sending Settings**. Depending on the **Enable real-time communication** option selected in the security product console for each customer, the settings profile is assigned either immediately or with a maximum delay of 10 minutes. See **Configuring Real- time Communication** in the administration guide of the product contracted by the customer.

After all steps have been completed, your customer computers start sending information which is temporarily stored on the Azure platform until the Panda Importer computer downloads it.

Chapter 5

Deployment and Integration Requirements

To use the Panda SIEMFeeder and Panda SIEMFeeder for Partners services, make sure your environment meets these requirements:

- Licenses and user Information
- Deployment and operation
- Integration into the existing IT infrastructure

Chapter Contents

Licenses and Required Information

Both Panda SIEMFeeder and Panda SIEMFeeder for Partners require the customer ID sent in the welcome email and the details of a user of the management console of the security product contracted by the organization and compatible with the service:

- Panda Adaptive Defense (compatible with Panda SIEMFeeder and Panda SIEMFeeder for Partners)
- Panda Adaptive Defense 360 (compatible with Panda SIEMFeeder and Panda SIEMFeeder for Partners)

Panda SIEMFeeder

- The email address and password of a user of your Panda Adaptive Defense 360 or Panda Adaptive Defense console with the Full Control role.
- An email account managed by an administrator. This is used to send notifications about the service status.
- The customer ID included in the welcome email you receive when the **Panda Adaptive Defense** service is provisioned.

Panda SIEMFeeder for Partners

- The email address and password of a user of the MSSP Panda Adaptive Defense or Panda Adaptive Defense 360 console with the Full Control role.
- The customer ID included in the welcome email that is sent to the MSSP technician when the **Panda Adaptive Defense** service is provisioned.
- An email account managed by the administrator. This is used to send notifications about the service status.

Deployment and Integration Requirements

- A network of user computers protected by Panda Adaptive Defense.
- Active Panda SIEMFeeder or Panda SIEMFeeder for Partners licenses.
- A computer with Panda Importer installed. See **Panda Importer Computer**.
- Valid firewall settings. See **Firewall Configuration**.
- Valid proxy server settings. See **Proxy Server Configuration**.
- Enough bandwidth to receive the Panda Importer data. See **Bandwidth Sizing**.

Panda Importer Computer

A computer that meets these requirements:

- Processor: 1 GHz or faster.
- RAM: 512 MB minimum.

- Free disk space: Enough space to store the log data that Panda Importer imports. On average, Panda Importer uses 1 MB of storage space for each computer, for each hour. By default, logs are sent in LEEF format.

To receive logs in CEF format in Panda SIEMFeeder, send an email message with your request to panda.ad_siemfeeder@watchguard.com.
To receive logs in CEF format in Panda SIEMFeeder for Partners, access Panda Partner Center and change the assigned settings. See ***Panda SIEMFeeder for Partners Settings****.*

- Panda Importer must be configured correctly. For more information, see **Install and Configure Panda Importer on Windows Systems** en la página **33** or **Install and Configure Panda Importer on Linux Systems** en la página **45**.
- You need the access information specified in section **Licenses and Required Information**.
- An NTP server is required for computer time synchronization.

Firewall Configuration

For Panda Importer to download log files from Microsoft Azure, any firewall on the computer that runs Panda Importer must allow these network settings:

- Allow this URL: **https://auth.pandasecurity.com**.
- Allow this URL: **https://storage.accesscontrolmngr.pandasecurity.com**.
- Allow this URL: **sb:// pac100siemfeeder.servicebus.windows.net**.
- **Communication source**: Panda Importer computer.
- **Communication target**: Azure platform.
- **Connection type**: Outbound from the user network.
- **Layer 3 (transport) protocol**: Transport Layer Security (TLS) 1.2.
- **Layer 4 (application) protocol**: HTTPS (port 443), Amqp (ports 5671 and 5672), AmqpWebSockets (port 443).

Proxy Server Configuration

If the computer that hosts Panda Importer uses a proxy server to access the Panda cloud, the proxy server must use WebSockets to enable access. Panda Importer uses the Amqp WebSockets protocol and not Amqp.

Bandwidth

For each hour of use, Panda Importer generates an average of 500 KB of compressed data, stored in the GZIP format.

The required bandwidth depends on the number of computers monitored on the network and the maximum of the allowable delay. You can configure two thresholds:

- **Minimum threshold**: The minimum bandwidth to receive all logs without loss of files, due to expiration of the log retention period. For more information, see **Service Availability** The log generation rate depends on multiple factors (computer activity, the role of the computer within the organization, and so on). With a low bandwidth value, the service uses non-work hours to receive the log files that Panda Importer generates while in peak hours.

A low bandwidth value leads to delays for when Event Importer receives log files and prevents the receiving and processing of logs in real time by the SIEM server of the organization.

- **Maximum threshold**: The bandwidth required to download all log files as they generate.

Data Leverage Requirements

To leverage the delivered data, install and configure a SIEM server compatible with any of the supported log formats.

Supported SIEM servers

SIEM products that are compatible with the Panda SIEMFeeder or Panda SIEMFeeder for Partners service are those that support the Common Event Format (CEF) developed by ArcSight or the Log Event Extended Format (LEEF) developed by QRadar.

Logs are sent in one of the two formats: CEF or LEEF. Here is a partial list of SIEM servers that are compatible with these two formats:

- AlienVault Unified Security Management (USM)
- Fortinet (AccelOps) FortiSIEM
- Hewlett Packard Enterprise (HPE) ArcSight
- IBM QRadar Security Intelligence Platform
- Intel Security McAfee Enterprise Security Manager (ESM)
- LogRhythm

- SolarWinds Log & Event Manager (LEM)
- Splunk Security Intelligence Platform

SIEM Server Configuration

For the SIEM server to obtain the log files, you configure a storage channel in the Panda Importer application to indicate where Panda Importer sends the log files that it receives. The SIEM server can obtain files from these storage locations:

- Local folder where the Panda Importer computer stores the received logs.
- Apache Kafka queue server that collects the logs sent by Panda Importer.
- Syslog server that collects the logs sent by Panda Importer.

*For a complete description of the received data, see **Panda SIEMFeeder Event Guide**.*

Characteristics of Log Files

- Each log file has a maximum size of 256 KB in compressed format.
- Panda Importer stores log files to the configured storage location.
- Each log file has a name in the form of **yyyymmdd-hhmm-(xxxxxx)**, where:
  - **yyyy**: Year created.
  - **mm**: Month created.
  - **dd**: Day created.
  - **hh**: Time created (hours).
  - **mm**: Time created (minutes).
  - **–(xxxxxx)**: If Panda Importer creates more than one log file within the same minute, it assigns an index number to additional log files.

Panda Importer Computer Sizing Recommendations

Bandwidth Sizing

- Calculate the bandwidth required based on the number of monitored user computers (500 KB per computer/hour).

- Use the value calculated in the previous point to configure QoS rules on your organization router that connects the Panda Importer computer to the Internet. Monitor your bandwidth usage.at all times.
- Compare the date the log files were received on the Panda Importer computer to the date the events were generated to find out whether there are delays in receiving data. The generation date for log files is provided by the operating system. The generation date for each event is part of the log file internal information schema. For a detailed description of the fields included in log files, see **Panda SIEMFeeder Event Guide**.
- If the difference between the event receipt and generation dates increases gradually over time, check the received data flow.
- If the data flow is using all bandwidth reserved by the QoS rule, Panda SIEMFeeder is generating a number of log files too large for the bandwidth allocated to the Panda Importer computer. If, after seven days (a full week to include periods of lower activity), the above mentioned difference does not decrease, or the organization requires a shorter event receipt time, increase the bandwidth allocated to the service by the QoS rule.
- If the bandwidth allocated to the service is not completely used, but the difference between the log receipt date and the event generation date increases, there is a bottleneck in the Panda Importer computer hardware. See **Panda Importer Computer Hardware Sizing Recommendations**.

Panda Importer Computer Hardware Sizing Recommendations

If the difference between the log receipt date and the event generation date increases gradually over time, but the bandwidth allocated to the service is not completely used by the received data flow, it is very likely that there is a bottleneck in the Panda Importer computer hardware.

Because Panda Importer is a program that retrieves messages from a queue-type structure, its CPU and RAM requirements are relatively low. In complex networks, with a large number of monitored computers, the main reason for slow download speeds is usually a bottleneck in the storage system of the computer that runs Panda Importer. Follow this advice to determine the source of bottlenecks and resolve them. To see CPU and hard disk performance stats, you must start the Windows Task Manager with Panda Importer running in command-line or service mode.

- **High CPU usage with free cores**: Panda Importer is a single-thread application, that is, it uses only one of the cores of the processor installed on the server. If the Windows Task Manager reports a sustained CPU usage of more than 80% on one core, you can run multiple instances of Panda Importer with different delivery target folders. A conservative recommendation is to run one instance of Panda Importer for each core on the computer. For more information, see **Configure Multiple Panda Importer Instances** en la página **38**.
- **High CPU usage without free cores**: If the Windows Task Manager reports a sustained CPU usage of more than 80% on all cores, install Panda Importer to a more powerful computer or

upgrade to a more powerful CPU.

- **High bandwidth consumption from the storage system**: If the Windows Task Manager reports high bandwidth usage for hard disk access, it is advisable to upgrade one or all of the storage components:
    - Replace mechanical disk drives with solid state drives (SSD).
    - Install a RAID–0 system or equivalent that allows data to be written to several drives at a time.
    - Replace the data bus interface with a more up-to-date version (SATA, eSATA, SAS, etc.).

Service Availability

Panda SIEMFeeder is available 24/7. Any service interruption is notified by email to the administrator account provided during the registration process.

To prevent data loss in the event of connectivity failure, unavailability of the customer Panda Importer computer, or any other error, Panda retains the log files generated and not delivered to the customer for these time periods:

- **Maximum number of days that log files are kept on the Azure platform**: Seven days
- **Maximum amount of data kept on the Azure platform**: 80 GB for each customer.

Chapter 6

Install and Configure Panda Importer on Windows Systems

Panda Importer is an application that downloads the events logged by Panda Adaptive Defense and Panda Adaptive Defense 360 from the Azure platform. These events are stored in log files which, based on the settings that you configure, Panda Importer decompresses and saves to a local or remote folder, or sends to a compatible server (Apache Kafka or syslog).

Chapter Contents

Installation Requirements

Required Information

For the information required by Panda Importer, see **Licenses and Required Information** en la página **25**.

Operating System and Required Libraries

Make sure the computer that will run the Panda Importer program meets these requirements:

- Panda Importer **requires Microsoft .NET Framework 4.6.2 or higher**: If an earlier version is installed, go to **https://www.microsoft.com/es- es/download/details.aspx?id=49981** to download the appropriate version. Panda Importer is compatible with .NET Framework up to version 4.8.
- **Supported operating systems**: Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7 SP 1, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2 SP1.

Required Permissions

You can run Panda Importer from the command line or unattended as a Windows service:

- When you run Panda Importer as a service, it runs under the `local system` computer account and must have administrator permissions to run correctly.
- When you run Panda Importer from the command line, it does not require any specific permissions, other than write access to the folder that you configure to store the logs that Panda Importer downloads.

Firewall Configuration

For Panda Importer to download log files from Microsoft Azure, any firewall on the computer that runs Panda Importer must allow these network settings:

- Allow this URL: **https://auth.pandasecurity.com**.
- Allow this URL: **https://storage.accesscontrolmngr.pandasecurity.com**.
- Allow this URL: **sb:// pac100siemfeeder.servicebus.windows.net**
- **Communication source**: Panda Importer computer.
- **Communication target**: Azure infrastructure.
- **Connection type**: Outbound from the user network.
- **Layer 3 (transport) protocol**: Transport Layer Security (TLS) 1.2.
- **Layer 4 (application) protocol**: HTTPS (port 443), Amqp (ports 5671 and 5672), Amqp WebSockets (port 443).

NTP Server

To download the log files stored on the Azure platform, an authentication process that involves the generation of a token must complete. To improve security, this token has an expiration date. The system time of both communication endpoints must be the same. Panda Importer must use a time

service (for example, the Windows Time Service) to synchronize with the time from an NTP server. For more information, go to **https://docs.microsoft.com/es-es/windows-server/networking/windows-time-service/accurate-time**.

Installation and Configuration

For more information about error messages that can occur during installation, see ***Appendix 1: Troubleshooting*** *en la página* ***59****.*

To install and configure Panda Importer:

1. Download and decompress the `.zip` file that contains the installer. See **Download the Install Package**.
2. Indicate the connection method supported by the IT infrastructure that will host the Panda Importer computer: direct connection or through a corporate proxy. See **Configure the Connection Method**.
3. Enter the credentials of the account used to access the service. See **Enter the Access Credentials**.
4. Specify the platform where your Panda security products reside. See **Configure the Platform to Use**.
5. Select the method to store and forward received log files. See **Configure Log Storage and Forwarding Method**.
6. Update the `configuration.json` file with the new installation settings. See **Update the configuration.json File**.
7. Configure how Panda Importer must run: as a service or from the command line. See **Configure the Execution Mode**.

Download the Install Package

Download the `.ZIP` package for the Windows version of Panda Importer from **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA**. Unpack it to a folder on your computer. The package contains these main files:

- `EventsFeederImporter.Host.exe`: Downloads the log files that contain the events that occur on the customer computers. It stores them on the computer hard disk or forwards them to another computer, depending on the settings you configure.
- `EventsFeederImporter.ConfigAssistant.exe`: Starts the configuration wizard that contains the parameters to configure Panda Importer.

- `Configuration.json`: Contains the program settings. All personal data is stored obfuscated to prevent security leaks.

Configuration

This section describes the steps to generate the configuration file required to run a single Panda Importer instance in command-line or service mode and connect to the Azure platform to download log files.

To configure Panda Importer, run the `EventsFeederImporter. ConfigAssistant.exe` program in command-line mode. Type **Y** when prompted: **Do you want to change the configuration settings? [Yes/No]**. Panda Importer generates a new configuration file that overrides the existing file, then launches the configuration wizard.

*To install Panda Importer as a service, run `EventsFeederImporter.ConfigAssistant.exe` with administrator permissions. Right-click the file and select **Run as Administrator**.*

Configure the Connection Method

Panda Importer uses the configured proxy server to connect to the Azure platform assigned to the user. It is not used to connect to other resources such as a file server, an Apache Kafka server, or a syslog server.

If the Panda Importer computer is behind a proxy server:

- Type **Y** to answer the question **Is Event Importer behind a proxy server? [Yes/No]**.
- Panda Importer prompts you to enter the proxy server IP address, as well as the user name and password if the proxy server requires authentication.

The password must be a string of alphanumeric characters, spaces, and symbols, except for: ":", "/", "?", "#", "[", "]", "@", "!", "$", "&", "'", "(", ")", "", "+", ";", "=", ",".*

Configure the Platform to Use

Configure the Panda Adaptive Defense platform: **Select your platform: [C]urrent or [W]G Endpoint Security**:

- **C (Current)**: Type **C** if the account used belongs to the Panda platform.
- **W (WatchGuard)**: Type **W** if the account used belongs to the WatchGuard platform.

Enter the Access Credentials

- Enter the email address of the user account used to access the Panda Adaptive Defense console.
- Enter the password. If the account has 2FA enabled, enter the 6-digit OTP code immediately after the password, without any blank spaces.
- Enter the Customer ID specified in the welcome email. After you enter it, Panda Importer generates a new access token it uses to access the Azure platform and download the generated log files.

To check whether the access account has 2FA enabled, go to the Panda Adaptive Defense management console:

- If your security provider is Panda Security, click **https://www.pandacloudsecurity.com/PandaLogin/**. Enter your credentials. The management console opens.
- If your security provider is WatchGuard:
    - Go to **https://www.watchguard.com/**. Click the **Log In** button in the upper-right corner of the page.
    - Enter your WatchGuard credentials. The **Support Center** page opens.
    - Select **My WatchGuard**. A drop-down list appears.
    - Select **Manage Panda Products**. A page opens that shows all the services you have contracted.
    - Click the tile for the product you want to access. The management console opens.
- Click the account name in the upper-right corner of the page. A drop-down list appears.
- Select **Set up my profile**. The **Panda Account** page opens. This page indicates whether 2FA is enabled or not.

For more information about how to enable 2FA, go to ***http://documents.managedprotection.pandasecurity.com/Help/PandaCloud/es-es/#t=001.htm***

Configure Log Storage and Forwarding Method

For more information about how to choose the method to store and forward downloaded logs, see **Configure Log Storage and Forwarding Method**.

Configure the Execution Mode

Panda Importer can run as a service or in command-line mode. At the command prompt, type **Y** or **N** to configure the execution mode: **Do you want to register Event Importer as a Windows service? [Yes/No]**.

- **Y:** Registers Panda Importer as a Windows service. The user who started the installation process must have administrator permissions.

*Type **Y** only if you are going to install and run a single Panda Importer instance as a service on the computer. In all other cases, type **N**. See **Configure Multiple Panda Importer Instances**.*

- **N**: Runs one or multiple instances from the command line or runs multiple Panda Importer instances as a service. See **Configure Multiple Panda Importer Instances**.

Update the `configuration.json` File

After the Panda Importer configuration wizard completes, Panda Importer updates the `configuration.json` file and begins to download log files stored on the Microsoft Azure platform.

The `configuration.json` contains this data:

- Information about the customer for which log files are downloaded.
- Information about the method used to forward and store log files.
- Information about the execution mode (command line or service).

Configure Multiple Panda Importer Instances

You must configure multiple instances of Panda Importer in these cases:

- If the computer that hosts Panda Importer reports low system resources as described in section **Panda Importer Computer Sizing Recommendations** en la página **29**. We recommend that you install one or more additional instances of the program and run them concurrently.
- If you require that a single computer with Panda Importer installed download log files for

more than one customer simultaneously, but you are not using Panda SIEMFeeder for Partners.

To download log files for multiple customers and centralize all downloads through a single Panda Importer instance, use Panda SIEMFeeder for Partners. See ***Architecture*** *en la página* ***20****.*

Multiple Instances of Panda Importer in Command-Line Mode

- Download the latest version of Panda Importer from **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA**. For each customer for which you want to download log files, decompress the file contents to a separate folder.
- To install Panda Importer in command- line mode, configure each instance of the application independently by following the steps described in **Configuration**.
- Run each instance of the application separately.

Multiple Instances of Panda Importer in Service Mode

Complete the steps in this procedure with administrator permissions.

To run multiple instances of Panda Importer in service mode, you must first run each instance of the application in command-line mode. You then manually register each Panda Importer instance as a service.

- This example uses the folders `c:\users\customer1` and `c:\users\customer2`.
- Complete the steps in the previous section, **Multiple Instances of Panda Importer in Command-Line Mode**.
- Press the keyboard shortcut `control + C` to stop each instance that runs.
- To register Panda Importer as a service, give each instance a different name and use the parameters `servicename`, `description` , and `displayname`.

```
PS C:\> cd c:\users\customer1
PS C:\users\customer1> EventsFeederImporter.Host.exe install
-servicename:ServiceCustomer1
```

```
-description: ServiceCustomer1
-displayname: ServiceCustomer1
PS C:\> cd c:\users\customer2
PS C:\users\customer2> EventsFeederImporter.Host.exe install
-servicename:ServiceCustomer2
-description: ServiceCustomer2
-displayname: ServiceCustomer2
```

- To start each instance of Panda Importer:

```
PS C:\> cd c:\users\customer1
PS C:\users\customer1> EventsFeederImporter.Host.exe start
-servicename:ServiceCustomer1
PS C:\> cd c:\users\customer2
PS C:\users\customer2> EventsFeederImporter.Host.exe start
-servicename:ServiceCustomer2
```

Configure Log Storage and Forwarding

Panda Importer provides several methods to store or forward event log files. Network architecture, available resources, and volume of event log files that Panda Importer receives from the Microsoft Azure platform can help you to decide the method to use:

- Save log files to a local or remote folder.
- Send log files to an Apache Kafka server.
- Send log Files to a syslog server

To select the storage method, type **Y** when Panda Importer shows the question **Event Importer enables you to send received events simultaneously to various channels. Do you want to change the current channel configuration? [Yes/No]** in the configuration wizard. This deletes the existing storage and forwarding settings (if any) and generates new settings.

Save Log Files to a Local or Remote Folder

- On the computer that runs Panda Importer, or on a shared drive or resource, create a folder to store the log files.

- To run multiple instances of Panda Importer, create a separate folder for each instance. Otherwise, some log files might be lost during collection and storage.
- Type **F** when this message appears: **Select where you want to deliver received events**: **[F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Enter the full folder path for each instance of Panda Importer.
- Enter the extensions of the files the events received from Panda Importer will be saved to.
- To complete configuration of this delivery method, type **N** when prompted: **Do you want to configure another delivery channel? [Yes/No]**.

Send Log Files to an Apache Kafka Server

- Type **K** when this message appears: **Select where you want to deliver received events**: **[F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Enter the IP address or domain name of the Kafka server and the listening port, separated by a colon.
- Enter the name of the queue/topic that log files will be sent to on the Kafka server.
- Enter the communication protocol to use to send log files to the Kafka server:
    - **None**: Type **N** to use the unencrypted format.
    - **SSL**: Type **S** to use SSL encryption.
    - **SASL_SSL**: Type **A** to use SASL/SSL encryption.
    - **SASL_PLAINTEXT**: Type **T** to use SASL/PLAIN text encryption.
- If the chosen communication protocol encrypts data, you must enter the path of the file that contains the certificate issued by the CA configured on the Kafka server.
- To complete configuration of this delivery method, type **N** when prompted: **Do you want to configure another delivery channel**? **[Yes/No]**.

Send Log Files to a Syslog Server

- Type **S** when this message appears: **Select where you want to deliver received events**: **[F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Select the message format configured on the syslog server for the received log files: **RFC [5]424** or **RFC[3]164**.
- Enter the IP address or domain name of the syslog server and the listening port, separated by a colon.
- Select the transport protocol configured on the syslog server for the received log files: **[T]CP** or **[U]DP**.

To make sure the syslog server receives all the log files that Panda Importer sends, we recommend use of the TCP transport protocol on both ends of the communication. Otherwise, in overload situations, the UDP protocol might lose log files unexpectedly.

- Select the cryptographic protocol to use to encrypt communications between the syslog server and Panda Importer: **[N]one** or **TLS 1.[2]**.
- Select the end-of-message marker that the syslog server configures for the received log files: **[C]R**, **[L]F**, or **C[R]LF**.

If the transport protocol is UDP, no end-of-line marker is used.
*If the transport protocol is TCP or TLS, a **null** end-of-line marker is used.*

- If the communication protocol chosen encrypts data, indicate the location of the certificate issued by the CA configured on the syslog server:
  - **[F]ile**: CA certificate is in a separate file.
  - **[C]ert Store**: CA certificate found in the local certificate store on the computer where Panda Importer runs, in the Trusted People certificates branch (Windows only).
- To complete configuration of this delivery method, type **N** when prompted: **Do you want to configure another delivery channel**? **[Yes/No]**.

Download Log Files to Multiple Locations

Panda Importer can simultaneously download log files to multiple locations. When a location updates, Panda Importer removes a log entry from the download queue on the Azure platform.

If errors occur while log collection takes place, different locations might have a different number of logs at completion of the process.

To download log files to multiple locations, Panda Importer uses a *channels* method, where the channel contains information about the storage type it uses and other configuration settings for Panda Importer to import log files.

To configure Panda Importer:

1. Install Panda Importer as described in section **Configuration**.
2. Stop Panda Importer as described in section **Start and Stop Panda Importer**.

3. In the `configuration.json` file, add a delivery channel:

```
"Channels": [{ channel 1 parameters} , {channel 2 parameters}, …]
```

4. For each channel, indicate the storage type used to store logs and its associated settings.

This is an example of a `configuration.json` file that implements two channels. The first channel saves log files to the `Log1` folder, and the second channel saves log files to the `Log2` folder.

```
"Channels": [{
"Type": "LocalDisk",
"Name": "LD1",
"Configuration": {
"fullPath":
"D:\\\\SIEMFeeder\\\\PandaEventFeederImporter 1.0.3 Pro\\\\Log1",
"filesSplitFormat": "1m",
"filesSizeLimitInBytes": 102400,
"directoryMaxSizeInMb": 1024
}
}, {
"Type": "LocalDisk",
"Name": "LD2",
"Configuration";{
"fullPath:
"D:\\\\SIEMFeeder\\\\EventFeederImporter 1.0.3 Pro\\\\Log2",
"fileSplitFormat":"1m",
"filesSizeLimitInBytes": 102400,
"directoryMaxSizeInMb": 1024
}
},]
```

Start and Stop Panda Importer

In Command-line Mode

- To start Panda Importer, double-click the `EventsFeederImporter.Host.exe` file or run it from the command line.
- To stop Panda Importer, at the command prompt, press the keyboard shortcut `Control + C`.

In Service Mode

- The service is automatically configured to start when the operating system boots. To start the Panda Importer service after a manual stop, access the Services snap-in in the operating system Microsoft Management Console (MMC) and find the `EventsFeederImporter` service (this is the default name used by the installation wizard provided you did not register the service manually). Right-click the service and select **Start**.
- To stop the Panda Importer service, access the Services snap-in in the operating system Microsoft Management Console (MMC) and find the `EventsFeederImporter` service. Right-click the service and select **Stop**.

Chapter 7

Install and Configure Panda Importer on Linux Systems

Panda Importer is an application that downloads the events logged by Panda Adaptive Defense and Panda Adaptive Defense 360 from the Azure platform. These events are stored in log files which, based on the settings that you configure, Panda Importer decompresses and saves to a local or remote folder, or sends to a compatible server (Apache Kafka or syslog).

Chapter Contents

Installation Requirements

Required Information

For the information required by Panda Importer, see **Licenses and Required Information** en la página **25**.

Operating System and Required Libraries

Although Panda Importer is compatible with all Linux platforms that support .NET Framework 8.0, Panda Security certifies and supports these distributions:

- Ubuntu 24.04 LTS
- Red Hat Enterprise Linux 9.5

The install package contains everything Panda SIEMFeeder requires.

For more information about distributions that support .NET Framework 8.0, see **.NET 8.0 - Supported OS Versions**.

Required Permissions

You can run Panda Importer from the command line or unattended as a system daemon:

- When you run Panda Importer in daemon mode, it runs under a user account. Panda Importer requires `root` permissions for configuration.
- When you run Panda Importer in command-line mode as an administrator, it does not require any specific permissions, other than write access to the folder you configure to store the logs that Panda Importer downloads

Firewall Configuration

For Panda Importer to download log files from Microsoft Azure, any firewall on the computer that runs Panda Importer must allow these network settings:

- Allow this URL: **https://auth.pandasecurity.com**.
- Allow this URL: **https://storage.accesscontrolmngr.pandasecurity.com**.
- Allow this URL: **sb:// pac100siemfeeder.servicebus.windows.net**
- **Communication source**: Panda Importer computer.
- **Communication target**: Azure platform.
- **Connection type**: Outbound from the user network.
- **Layer 3 (transport) protocol**: Transport Layer Security (TLS) 1.2.
- **Layer 4 (application) protocol**: HTTPS (port 443), Amqp (ports 5671 and 5672), Amqp WebSockets (port 443).

NTP Server

To download the log files stored on the Azure platform, an authentication process that involves the generation of a token must complete. To improve security, this token has an expiration date. The system time of both communication endpoints must be the same. Panda Importer uses the `ntpd`

daemon (or equivalent) to synchronize with the time from an NTP server. For more information, go to **https://www.ntppool.org/en/use.html**.

Installation and Configuration

> *For more information about error messages that can occur during installation, see* ***Appendix 1: Troubleshooting*** *en la página* ***59****.*

To install and configure Panda Importer:

1. Download and decompress the `.gz` file that contains the installer. See **Download the Install Package**.
2. If required, modify the execution attribute of files.
3. Indicate the connection method supported by the IT infrastructure that will host the Panda Importer computer: direct connection or through a corporate proxy. See **Configure the Connection Method**.
4. Enter the credentials of the account used to access the service. See **Enter the Access Credentials**.
5. Specify the platform where your Panda security products reside. See **Configure the Platform to Use**.
6. Select the method to store and forward received log files. See **Configure Log Storage and Forwarding**.
7. Update the `configuration.json` file with the new installation settings. See **Update the Configuration.json File**.
8. (Optional) Configure Panda Importer to run as a daemon. See **Configure Panda Importer to Run as a Daemon**.

Download the Install Package

Download the `.GZ` package for the Linux version of Panda Importer from **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA**. Unpack it to a folder on your computer. The `EventsFeederImporter x.x Pro.zip` package contains these main files:

- `EventsFeederImporter.Multiplatform.Host`: Downloads the log files that contain the events that occur on user computers. It stores them on the computer hard disk or forwards them to another computer, depending on the settings you configure.

- `EventsFeederImporter.Multiplatform.ConfigAssistant`: Starts the configuration wizard that contains the parameters to configure Panda Importer.
- `Configuration.json`: Contains the program settings. All personal data is stored obfuscated to prevent security leaks.

Modify the Execution Attribute of Files

For a Linux distribution to run an application, you must first turn on the execute bit of the file. At the command prompt, type:

```
$ sudo chmod a+x /#_SAMPLEFOLDER_
SiemFeeder#/EventsFeederImporter.Multiplatform.Host
$ sudo chmod a+x /#_SAMPLEFOLDER_
SiemFeeder#/EventsFeederImporter.Multiplatform.ConfigAssistant
```

The variable `/#_SAMPLEFOLDER_SiemFeeder#/` is the full path to the folder where the uncompressed package resides on your computer.

Configuration

This section describes the steps to generate the configuration file required to run a single Panda Importer instance in command-line mode and connect to the Azure platform to download log files.

To configure Panda Importer, run the `EventsFeederImporter.Multiplatform.ConfigAssistant` program. Type **Y** when prompted: **Do you want to change the configuration settings? [Yes/No]**. Panda Importer generates a new configuration file that overrides the existing file, then launches the configuration wizard.

Configure the Connection Method

Panda Importer uses the configured proxy server to connect to the Azure platform assigned to the user. It is not used to connect to other resources such as a file server, an Apache Kafka server, or a syslog server.

If the Panda Importer computer is behind a proxy server:

- Type **Y** when prompted: **Is Event Importer behind a proxy server? [Yes/No]**.
- Panda Importer prompts you to enter the proxy server IP address, as well as the user name and password if the proxy server requires authentication.

The password must be a string of alphanumeric characters, spaces, and symbols, except for: ":", "/", "?", "#", "[", "]", "@", "!", "$", "&", "'", "(", ")", "", "+", ";" , "=", ",".*

Configure the Platform to Use

Configure the Panda Adaptive Defense platform: **Select your platform: [C]urrent or [W]G Endpoint Security**:

- **C (Current)**: Type **C** if the account used belongs to the Panda platform.
- **W (WatchGuard)**: Type **W** if the account used belongs to the WatchGuard platform.

Enter the Access Credentials

- Enter the email address of the user account used to access the Panda Adaptive Defense console.
- Enter the password. If the account has 2FA enabled, enter the 6-digit OTP code immediately after the password, without any blank spaces.
- Enter the Customer ID specified in the welcome email. After you enter it, Panda Importer generates a new access token it uses to access the Azure platform and download the generated log files.

To check whether the access account has 2FA enabled, go to the Panda Adaptive Defense management console:

- If your security provider is Panda Security, click **https://www.pandacloudsecurity.com/PandaLogin/**. Enter your credentials. The management console opens.
- If your security provider is WatchGuard:
    - Go to **https://www.watchguard.com/**. Click the **Log In** button in the upper-right corner of the page.
    - Enter your WatchGuard credentials. The **Support Center** page opens.
    - Select **My WatchGuard**. A drop-down list appears.
    - Select **Manage Panda Products**. A page opens that shows all the services you have contracted.
    - Click the tile for the product you want to access. The management console opens.
- Click the account name in the upper-right corner of the page. A drop-down list appears.
- Select **Set up my profile**. The Panda Account page opens. This page indicates whether 2FA is enabled or not.

For more information about how to enable 2FA, go to ***http://documents.managedprotection.pandasecurity.com/Help/PandaCloud/es-es/#t=001.htm***

Configure Log Storage and Forwarding Method

For more information about how to choose the method to store and forward downloaded logs, see **Configure Log Storage and Forwarding**.

Update the Configuration.json File

After you configure the log storage and forwarding method, Panda Importer updates the `configuration.json` file in the same folder with these data:

- Information about the customer for which log files are downloaded.
- Information about the method used to forward and store log files.
- Information about the Panda Importer execution mode (command line or service).

Configure Panda Importer to Run as a Daemon

Panda Importer can run automatically as a background process at system startup. In this case, it does not show any messages on screen:

- Type **N**, when prompted: **Do you want to start the Event Importer process? (This is not necessary when Event Importer runs as a daemon.)**.
- Edit the `siemfeeder.service` file included in the .GZ package. At the `ExecStart` line, type the path to the folder that contains the `EventsFeederImporter.Multiplatform.Host` file. For example:

```
ExecStart="/home/panda/Desktop/SIEMFeeder 3.10
Linux/EventsFeederImporter.Multiplatform.Host"
```

- Copy the `siemfeeder.service` file to the system directory of your Linux distribution. In most cases, the path is:
  - Ubuntu: `/lib/systemd/system`
  - Red Hat `/usr/lib/systemd/system`
- If the computer has Security-Enhanced Linux (SELinux) enabled and a Red Hat Enterprise distribution installed, use the `selinux-checks.sh` script to configure the execution environment:

  - To enable execution permissions for the script, run the command: `chmod +x selinux-checks.sh`.
  - Run the command: `sudo #_PATH_#/selinux-checks.sh`. Make sure there are no spaces in the path where the script is located.
- To add the script to the system startup sequence, run the command: `sudo systemctl enable siemfeeder`.
- To start Panda SIEMFeeder, see **Start and Stop Panda Importer**.

Configure Multiple Panda Importer Instances

You must configure multiple instances of Panda Importer in these cases:

- If the computer that hosts Panda Importer reports low system resources as described in section **Panda Importer Computer Hardware Sizing Recommendations** en la página **30**. We recommend that you install one or more additional instances of the program and run them concurrently.
- If you require that a single computer with Panda Importer installed download log files for more than one customer simultaneously, but you are not using Panda SIEMFeeder for Partners.

> ⚠ *To download log files for multiple customers and centralize all downloads through a single Panda Importer instance, use Panda SIEMFeeder for Partners. See **Panda SIEMFeeder for Partners Architecture** en la página **17**.*

Multiple Instances of Panda Importer in Command-Line Mode

- Download the latest version of Panda Importer from **https://techsearch.pandasecurity.com/pandakbview?id=kA16S000000byzwSAA**. For each customer for which you want to download log files, decompress the file contents to a separate folder.
- To install Panda Importer in command- line mode, configure each instance of the application independently by following the steps described in **Configuration**.
- Run each instance of the application separately.

Configure Log Storage and Forwarding

Panda Importer provides several methods to store or forward event log files. Network architecture, available resources, and volume of event log files that Panda Importer receives from the Microsoft

Azure platform can help you to decide the method to use:

- Save log files to a local or remote folder.
- Send log files to an Apache Kafka server.
- Send log files to a syslog server.

To select the storage method, type **Y** when Panda Importer shows the question **Event Importer enables you to send received events simultaneously to various channels. Do you want to change the current channel configuration? [Yes/No]** in the configuration wizard. This deletes the existing storage and forwarding settings (if any) and generates new settings.

Save Log Files to a Local or Remote Folder

Make sure that Panda SIEMFeeder has write permissions on the local or remote folder where it downloads log files.

- On the computer that runs Panda Importer, or on a shared drive or resource, create a folder to store the log files.
- To run multiple instances of Panda Importer, create a separate folder for each instance. Otherwise, some log files might be lost during collection and storage.
- Type **F** when this message appears: **Select where you want to deliver received events**: **[F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Enter the full folder path for each instance of Panda Importer.
- Enter the extensions of the files the events received from Panda Importer will be saved to.
- To complete configuration of this delivery method, type **N** when prompted: **Do you want to configure another delivery channel? [Yes/No]**.

Send Log Files to an Apache Kafka Server

- Type **K** when this message appears: **Select where you want to deliver received events**: **[F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Enter the IP address or domain name of the Kafka server and the listening port, separated by a colon.
- Enter the name of the queue/topic that log files will be sent to on the Kafka server.
- Enter the communication protocol to use to send log files to the Kafka server:
    - **None**: Type **N** to use the unencrypted format.
    - **SSL**: Type **S** to use SSL encryption.

  - **SASL_SSL**: Type **A** to use SASL/SSL encryption.
  - **SASL_PLAINTEXT**: Type **T** to use SASL/PLAIN text encryption.
- (Optional) If the chosen communication protocol encrypts data, you must enter the path of the file that contains the certificate issued by the CA configured on the Kafka server.
- To complete configuration of this delivery method, type **N** when prompted: **Do you want to configure another delivery channel**? **[Yes/No]**.

Send Log Files to a Syslog Server

- Type **S** when this message appears: **Select where you want to deliver received events**: **[F]ile on disk, [K]afka topic/queue, or [S]yslog server**.
- Select the message format configured on the syslog server for the received log files: **RFC [5]424** or **RFC[3]164**.
- Enter the IP address or domain name of the syslog server and the listening port, separated by a colon.
- Select the transport protocol configured on the syslog server for the received log files: **[T]CP** or **[U]DP**.

To make sure the syslog server receives all the log files that Panda SIEMFeeder sends, we recommend use of the TCP transport protocol on both ends of the communication.

- Select the cryptographic protocol to use to encrypt communications between the syslog server and Panda Importer (TLS 1.2 supports only the TCP transport protocol): **[N]one** or **TLS 1.[2]**.
- Select the end-of-message marker that the syslog server configures for the received log files: **[C]R**, **[L]F**, or **C[R]LF**.

If the transport protocol you selected is UDP, no end-of-message marker is used.
If the transport protocol you selected is TCP, Panda SIEMFeeder uses the end-of-message marker you select.

- If the communication protocol chosen encrypts data, indicate the location of the certificate issued by the CA configured on the syslog server.
- To complete configuration of this delivery method, type **N** when prompted: **Do you want to configure another delivery channel**? **[Yes/No]**.

Download Log Files to Multiple Locations

Panda Importer can simultaneously download log files to multiple locations. When a location updates, Panda Importer removes a log entry from the download queue on the Azure platform.

If errors occur while log collection takes place, different locations might have a different number of logs at completion of the process.

To download log files to multiple locations, Panda Importer uses a *channels* method, where the channel contains information about the storage type it uses and other configuration settings for Panda Importer to import log files.

To configure Panda Importer:

1. Install Panda Importer as described in section **Configuration**.
2. Stop Panda Importer as described in section **Start and Stop Panda Importer**.
3. In the `configuration.json` file, add a delivery channel:

```
"Channels": [{ channel 1 parameters} , {channel 2 parameters}, …]
```

4. For each channel, indicate the storage type used to store logs and its associated settings.

This is an example of a `configuration.json` file that implements two channels. The first channel saves log files to the `Log1` folder, and the second channel saves log files to the `Log2` folder.

```
“Channels”: [{
“Type”: “LocalDisk”,
“Name”: “LD1”,
“Configuration”: {
“fullPath”:
“D:\\\\SIEMFeeder\\\\EventFeederImporter 1.0.3 Pro\\\\Log1”,
“filesSplitFormat”: “1m”,
“filesSizeLimitInBytes”: 102400,
“directoryMaxSizeInMb”: 1024
}
}, {
“Type”: “LocalDisk”,
```

```
"Name": "LD2",
"Configuration";{
"fullPath:
"D:\\\\SIEMFeeder\\\\EventFeederImporter 1.0.3 Pro\\\\Log2",
"fileSplitFormat":"1m",
"filesSizeLimitInBytes": 102400,
"directoryMaxSizeInMb": 1024
}
},]
```

Start and Stop Panda Importer

In Command-line Mode

- To start Panda Importer, double-click the `EventsFeederImporter.Multiplatform.Host` file or run it from the command line.
- To stop Panda Importer when it runs in command-line mode, press the keyboard shortcut `control + c`.

In Daemon Mode

- To start Panda Importer, from the command line, type the command `sudo service siemfeeder start`
- To stop Panda Importer, from the command line, type the command `sudo service siemfeeder stop`
- To get the status of Panda Importer, from the command line, type the command `systemctl status siemfeeder.service`

Modify Panda SIEMFeeder Settings

Panda SIEMFeeder stores the execution parameters you configure in the `configuration.json` file. This file is located in the same folder where Panda Importer resides.

After the installation and execution processes are complete, you can regenerate the configuration file to change some of its parameters, or edit it manually.

Regenerate the Configuration File with the Wizard

- If running, stop the Panda SIEMFeeder process. See **Start and Stop Panda Importer** en la página **44** (Windows) or **Start and Stop Panda Importer** en la página **55** (Linux).
- Run from the command line or double- click the `EventsFeederImporter.ConfigAssistant.exe` program on Windows computers or `EventsFeederImporter.Multiplatform.ConfigAssistant` on Linux computers.
- Type **Y**, when prompted: **Do you want to change the configuration settings? [Yes/No]**
- Complete the configuration wizard.
- Start Panda Importer. See **Start and Stop Panda Importer** en la página **44** (Windows) or **Start and Stop Panda Importer** en la página **55** (Linux).

Manually Modify Panda SIEMFeeder Settings

The `configuration.json` file uses the JSON syntax.

- If running, stop Panda SIEMFeeder. See **Start and Stop Panda Importer** en la página **44** (Windows) or **Start and Stop Panda Importer** en la página **55** (Linux).
- Open the `configuration.json` file with a text editor.
- For more information about supported parameters, see **Parameters Related to Event Log File Download** en la página **56** and **Parameters Related to the Execution Log** en la página **57**
- Run Panda SIEMFeeder. See **Start and Stop Panda Importer** en la página **44** (Windows) or **Start and Stop Panda Importer** en la página **55** (Linux).

Parameters Related to Event Log File Download

These parameters decide how Panda Importer generates event log files:

- **fullPath**: Absolute path to the log folder.
- **fileSizeLimitInBytes**: Maximum size of the log files.
- **directoryMaxSizeInMB**: Maximum size of the content in the folder that stores the log files. When Panda Importer reaches the maximum size, it deletes 10 percent of the oldest files.
- **fileSplitFormat**: Rotation interval of the log files. The file name contains the year (yyyy), month (MM), day (dd), hour (HH), and minute (mm) of when Panda Importer creates the file.
    - "**1h**" or empty: yyyyMMdd-HH format. Generates a file every hour.
    - "**1m**": yyyyMMdd-HHmm format. Generates a file every minute.
    - "**5m**": yyyyMMdd-HHmm format. Generates a file every 5 minutes.
    - "**10m**": yyyyMMdd-HHmm format. Generates a file every 10 minutes.
    - "**15m**": yyyyMMdd-HHmm format. Generates a file every 15 minutes.
    - "**30m**": yyyyMMdd-HHmm format. Generates a file every 30 minutes.
- **Channels**: Indicates the characteristics of the channel used to download log files.
- **Type**: Storage type used in the channel.
- **Name**: Channel name.
- **Configuration**: Channel settings (**fullPath**, **fileSplitFormat**, **fileSizeLimitInBytes**, **directoryMaxSizeInMb**).
- **MessageFormat**: Format of the messages sent to the syslog server.
    - **0**: RFC5424
    - **1**: RFC3164
- **MessageDelimiter**: Delimiter character for the messages sent to the syslog server:
    - **13**: CR
    - **10**: LF
    - **1310**: CRLF
- **IterationCount**: Internal message counter used to make a pause in sending messages to the syslog server.
- **IterationMs**: Pause in milliseconds that is made when **IterationCount** messages are sent to the syslog server.
- **MaxBufferSize**: Maximum size in bytes of the messages sent to the syslog server.

Parameters Related to the Execution Log

Panda Importer saves all operations it executes to text files. It stores the text files in the `log` folder of the application.

For more information about error messages that Panda Importer might show, see ***Appendix 1: Troubleshooting*** *en la página* ***59***

These parameters decide how Panda Importer generates the text files.

- **LogsPath**: Absolute or relative path and file name. Make sure to escape the backlash character ("\"). For example `.\\log\\log.txt`.
- **LogFileSizeLimitKBytes**: Rotates the log file when it reaches a certain size in kilobytes, adds the suffix "-SequenceNumber". For example `log-3.txt`.
- **LogRetainedFileCountLimit**: Indicates the maximum number of files that Panda Importer stores on the storage device. Panda Importer deletes the oldest file when it reaches this number.
- **Interval**: Rotation interval of the log files:
  - **0**: No rotation. The file name is the same as the name the **LogsPath** parameter defines.
  - **1**: File rotates every year. The suffix for the name defined in **LogsPath** is LognameYear (YYYY). For example `log2021.txt`.
  - **2**: File rotates every month. The suffix for the name defined in **LogsPath** is LognameYearMonth(YYYYMM). For example `log202107.txt`
  - **3**: File rotates every day. The suffix for the name defined in **LogsPath** is LognameYearMonthDay(YYYYMMDD). For example `log20210722.txt`
  - **4**: File rotates every hour. The suffix for the name defined in **LogsPath** is LognameYearMonthDayHour(YYYYMMDDhh). For example `log2021072210.txt`
  - **5**: File rotates every minute. The suffix for the name defined in **LogsPath** is LognameYearMonthDayHourMinute (YYYYMMDDhhmm). For example `log202107221055.txt`

Chapter 8

Appendix 1: Troubleshooting

These are common types of errors you might encounter, and the solutions that most often resolve them.

Symptom / Error	Cause	Solution
.NET Framework initialization error	Panda Importer cannot find .NET Framework 4.6.1 or later on the administrator computer.	Make sure .NET Framework 4.6.1 is installed. To download it, go to **https://www.microsoft.com/es-es/download/details.aspx?id=49981**.
invalid_redirect_uri **unrecognized_client_id** **unsupported_scope**	Customer ID not recognized.	Make sure the customer is correctly registered in the Panda SIEMFeeder service. Make sure the email address used to log in to the Panda Adaptive Defense management console is correctly entered in Panda Importer.
unrecognized_client_secret **unsupported_grant_type** **invalid_grant**	Customer password not recognized.	Make sure the Panda account used to access the Panda SIEMFeeder service has the Full Control role assigned. Run Panda Importer. To re-enter the password, type **Y** when prompted **Do**

Symptom / Error	Cause	Solution
		you want to change the configuration settings? Make sure the computer where Panda Importer runs uses NTP or a similar service for time synchronization. Make sure the Windows Time Service is running.
unauthorized_client **unsupported_response_type** **invalid_scope** **access_denied** **invalid_request**	The authentication information is correct, but there is a problem downloading data.	Contact Panda Technical Support.
temporarily_unavailable **server_error**	The Panda SIEMFeeder service is temporarily unavailable due to technical issues.	Run Panda Importer again after a few minutes. Check the email account used to register the service. If the error persists, an email message is sent to the administrator, explaining the reasons for the service stop and the available options.

Common types of errors and solutions

Chapter 9

Appendix 2: Security Architecture

This chapter deals with the AAA (Authentication, Authorization, and Access) security architecture implemented in Panda SIEMFeeder as well as the encryption of all communications between the Panda Importer software and all other components that make up the service.

Chapter Contents

AAA Security Architecture Overview

Security Architecture Components

This figure shows the components that authenticate customers and grant them access to the Azure platform resources required to download the log files that contain the information collected from the organization IT network.

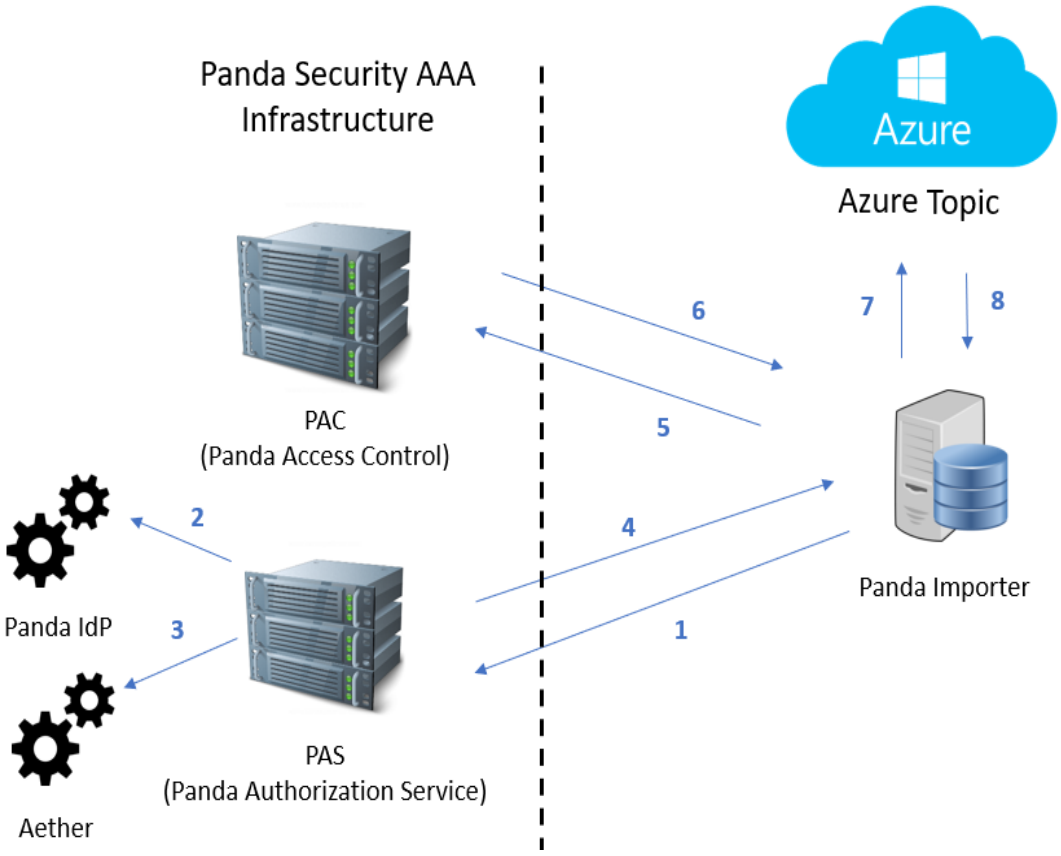

Figure 9.1: AAA security architecture overview

- **Panda Importerr**: A program provided by Panda that collects the log files stored on the Azure platform.
- **Azure topic**: A queue-type resource generated on the Azure platform. It stores the log files received from Panda with the information collected from the organization IT network.
- **PAS** (Panda **Authorization Service**): A service that authenticates and authorizes access to the Azure topic. It receives, from Panda Importer, the credentials assigned to the customer after they contract the service, and returns to it an access token and a refresh token.
- **PAC** (**Panda Access Control**): A service that enables Panda Importer to access the Azure topic provisioned to the customer. It receives the refresh token from Panda Importer and returns a shared access signature (SAS) key.
- **Panda IdP (Identity Provider)**: A service that authenticates the credentials sent.
- **Panda**: A service that authorizes access to Panda SIEMFeeder.

Initial Message Exchange

To access the Panda SIEMFeeder service securely, an initial message exchange must take place between the Panda Importer computer and Panda SIEMFeeder. This exchange must take place successfully; otherwise, Panda Importer cannot access the information published in the Azure topic.

The image below shows the message flow exchanged the first time Panda Importer runs. This message flow must occur every time the user is removed from the system or is unassigned the Full Control role assigned through the Panda security product management console.

1. Panda Importer sends the credentials (email address and password) assigned to the customer.
2. Authentication phase: The CAS service connects to the Panda IdP service to validate the credentials.
3. Authorization phase: The CAS service connects to the Panda service to check whether the customer has access to the Panda SIEMFeeder service.

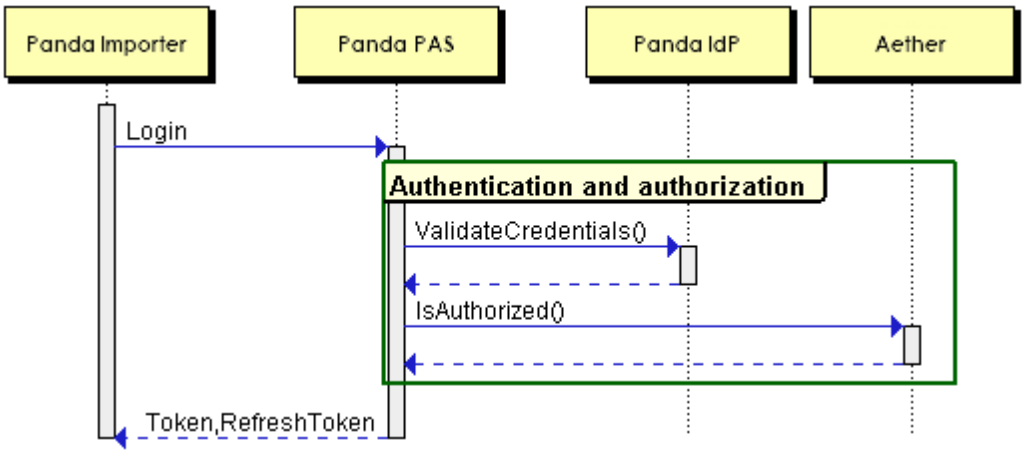

Figure 9.2: Steps 1 to 4 of the initial message exchange

1. The CAS service generates and delivers an access token and a refresh token to Panda Importer.
2. Panda Importer sends the refresh token to the CAC service.
3. Access phase: The CAC service generates a shared access signature (SAS) key.
4. Access to the topic: Panda Importer accesses the assigned topic using the SAS key.
5. Panda Importer receives the log files from the subscribed topic.

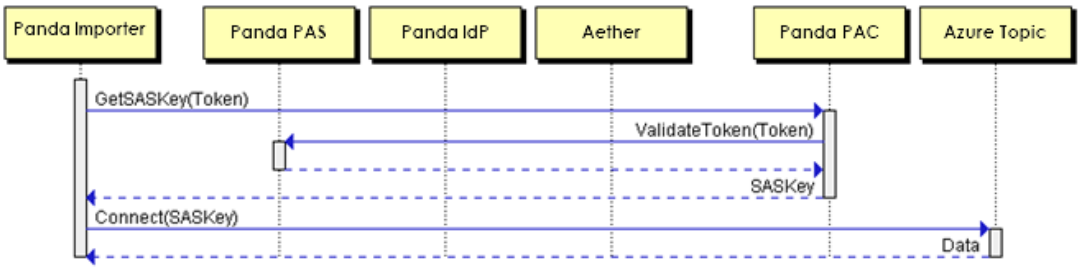

Figure 9.3: Steps 5 to 8 of the initial message exchange

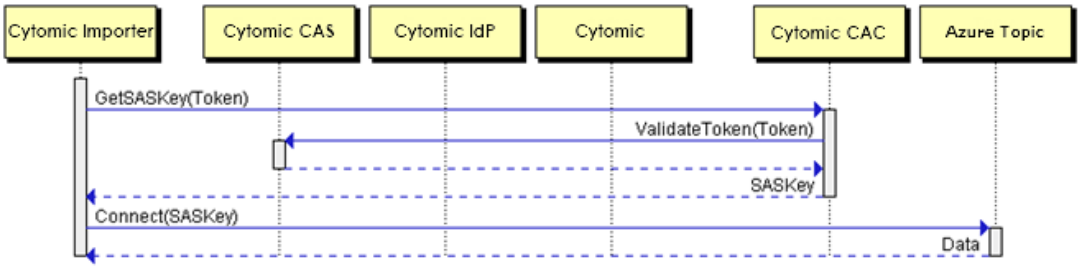

Figure 9.4: Steps 5 to 8 of the initial message exchange

Subsequent Message Exchange

Panda Importer uses the refresh token to obtain the SAS key. Both the token and the SAS key have an expiration time for security reasons. When the refresh token expires,Panda Importer generates this alternative message flow:

1. Panda Importer asks the CAS service for a new refresh token. To do this, it sends the access token that was assigned to it during the above-mentioned initial flow.
2. With the new refresh token, Panda Importer asks the CAC service for a new SAS key.
3. With the new SAS key, Panda Importer connects to the Azure topic and continues to collect log files.

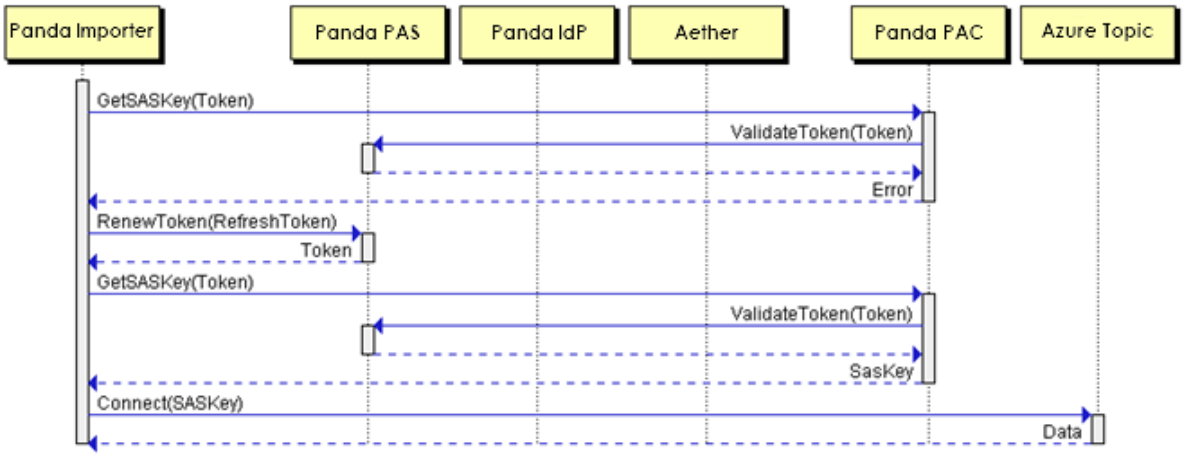

Figure 9.5: Message flow when the refresh token expires

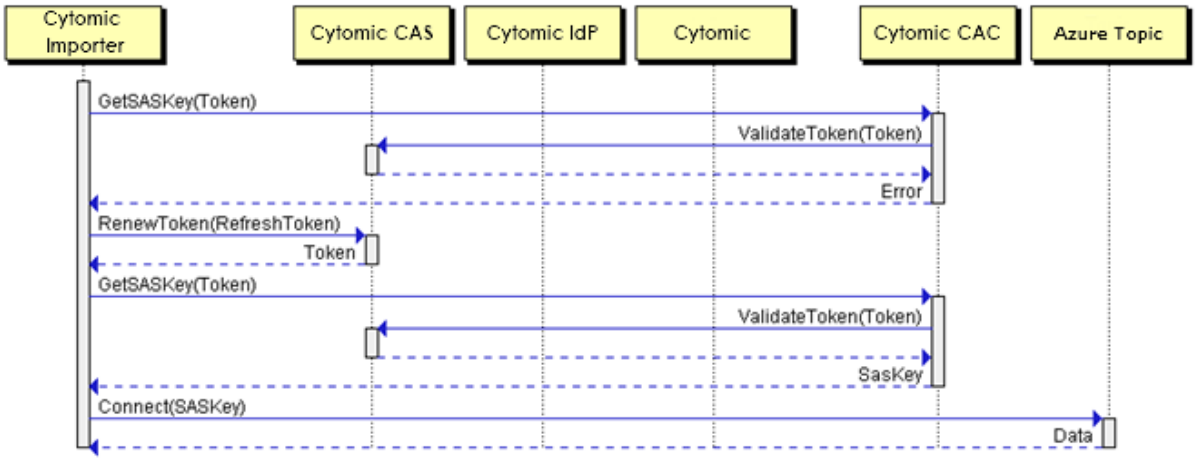

Figure 9.6: Message flow when the refresh token expires

Communication Characteristics

AAA Communication Encryption

All communications for requesting and sending tokens are encrypted with HTTPS protocol SSL SHA256 – G3.

Lifetime of the Tokens Assigned by Panda SIEMFeeder

- CAS refresh token: 14 days
- CAS access token: 20 minutes
- SAS key: 1 day

Panda Importer uses the refresh token to access the Azure topic. After the refresh token expires, a new access token is generated that contains the account details entered in the Panda Importer program. In addition to this, a new refresh token is also generated for Panda Importer to continue to access the Azure topic.

Even when the account used when configuring the service is no longer available or does not have the Full Control role assigned, the customer can continue to access the service, provided the refresh token has not expired (maximum lifetime: 14 days). When the refresh token expires, it is not possible to generate a new refresh token and access is denied.

Encrypted Communications for Log File Download

All communications established for downloading log files are encrypted with the TLS/SSL and SASL protocols.

Glossary

D

Domain

Windows network architecture where the management of shared resources, permissions, and users is centralized on a server called a Primary Domain Controller (PDC) or Active Directory (AD).

Domain Name System (DNS)

Service that translates domain names into different types of information, generally IP addresses.

E

Event

An action performed by a process on the user computer and monitored by Panda SIEMFeeder. Events are sent to the Panda cloud in real time as part of the telemetry. In the cloud, analysts, threat hunters, and automated machine learning processes analyze them in their context to determine whether they could be part of the Cyber Kill Chain (CKC) of a cyberattack. See Cyber Kill Chain (CKC).

F

Firewall

Technology that blocks the network traffic that matches certain patterns defined in rules created by the administrator. A firewall prevents or limits the communications established by the applications run on computers, reducing the attack surface.

Fully Qualified Domain Name (FQDN)

A domain name that specifies the exact location of a host in the tree hierarchy of the Domain Name System (DNS). It specifies all domain levels, including the top-level domain and the root zone.

I

Internet Protocol (IP)

Principal Internet communications protocol for sending and receiving datagrams generated on the underlying link level.

IP Address

Number that identifies a device network interface (usually a computer) logically and hierarchically on a network that uses the IP protocol.

L

Linux Distribution

Set of software packages and libraries that make up an operating system based on the Linux kernel.

M

Machine Learning

A branch of artificial intelligence whose objective is to develop technologies capable of predicting behaviors from unstructured data provided in the form of examples.

Malware

A term used to refer to all programs that contain malicious code (MALicious softWARE), whether a virus, a Trojan, a worm, or any other threat to the security and integrity of IT systems. Malware tries to infiltrate and damage computers, often without users knowing, for a variety of reasons.

N

Network Topology

Physical or logical map of nodes on a network to exchange data.

P

Panda SIEMFeeder Service

A module compatible with Panda SIEMFeeder that sends the telemetry generated by the processes run on the organization workstations and servers to the company SIEM server.

Port

Unique ID number assigned to a data channel opened by a process on a device through which data is exchanged (inbound/outbound) with an external source.

Protocol

A set of rules and specifications that enables two or more computers to communicate. One of the most commonly used protocols is TCP-IP.

Proxy

Software that acts as an intermediary for the communication between two computers: a client on an internal network (an intranet, for example) and a server on an extranet or the Internet.

Public Network

Networks in public places such as airports, cafés, etc. These networks require that you establish some limitations regarding computer visibility and usage, especially with regard to file, directory, and resource sharing.

S

Secure Sockets Layer (SSL)

Cryptographic protocol for the secure transmission of data over the Internet.

Security Information and Event Management (SIEM)

Software that provides storage and real-time analysis of the alerts generated by network devices.

SYN

Flag in the TOS (Type Of Service) field of TCP packets that identifies them as connection start packets.

T

Transmission Control Protocol (TCP)

The main transport-layer Internet protocol. It is aimed at IP packet exchange connections.

Transport Layer Security (TLS)

New version of protocol SSL 3.0.

Trusted Network

Networks in private places such as offices and households. Connected computers are generally visible to the other computers on the network, and you do not need to establish limitations on file, directory, and resource sharing.

U

User (Console)

Information set used by Panda SIEMFeeder to regulate administrator access to the web console and define the actions that administrators can take on the computers on the network.

User (Network)

A company employee who uses computing devices to do their job.

User Datagram Protocol (UDP)

A transport-layer protocol that is unreliable and unsuited for IP packet exchange connections.

W

Web Console

Tool to manage the Panda SIEMFeeder advanced security service. The console is accessible anywhere, anytime, through a supported Internet browser. The web console enables administrators to deploy the security software, push security settings, and view the protection status. It also provides access to a set of forensic analysis tools to assess the scope of security problems.