

# **FIELD TECH NOTES**

## **Azure Security Center - Manual Integration**

Patrick Glynn  
CE, AMER

### **Introduction**

This guide will walk the reader through the process of adding existing Palo Alto Networks firewalls to the Azure Security Center (ASC). It is possible to deploy a firewall based upon the recommendations by ASC which already has the necessary integration configured; however, due to limitations in Azure, this can only be used for new deployments. This document can be used in cases where existing firewalls need to be added to ASC. Note that the concepts herein should be applicable to Panorama.

Azure Security Center is a security management system that facilitates securing on-premises and cloud-based resources by providing a central location for log/alert collection and processing.



# Expected Outcome

This guide will walk the reader through the following configurations.

- Creating an Azure Log Analytics Workspace
- Gathering integration information for the syslog host
- Building a Linux host to forward logs to Log Analytics
- Configure a custom log format on the Firewall

# Prerequisites

## Before You Begin

This guide assumes prior knowledge of and access to the Azure console. The guide also assumes prior knowledge of the Palo Alto Networks VM-Series firewall.

The reader should now login into the Azure console and navigate to the desired Resource Group.

# Log Analytics Workspace

## Overview

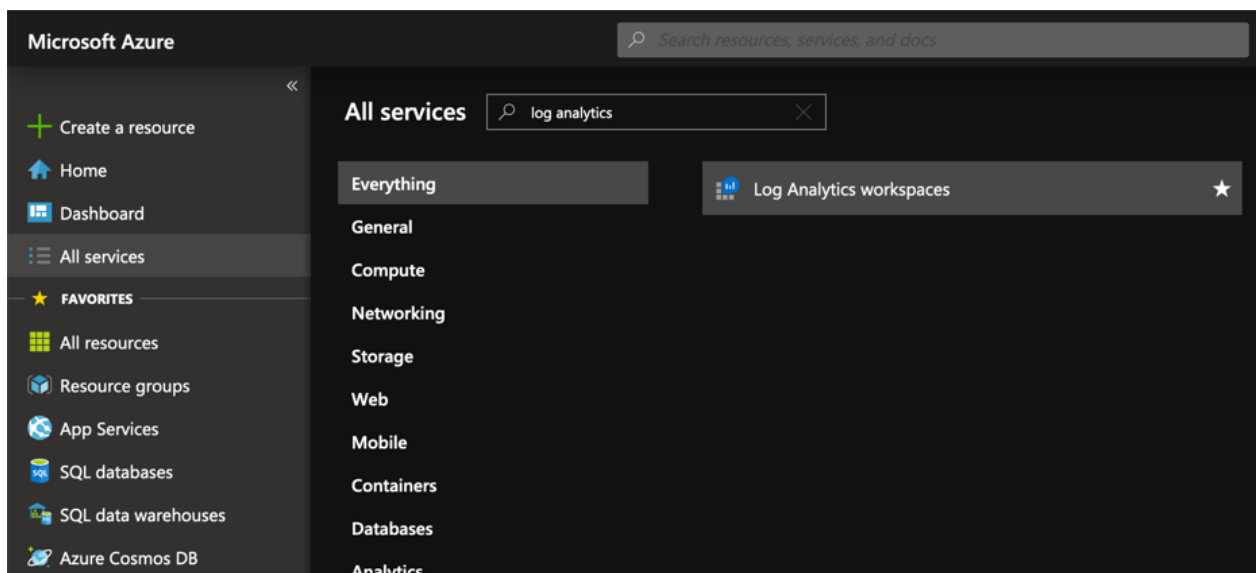
The guide will walk through the creation of a Log Analytics Workspace. The Log Analytics Workspace serves as the location to which the firewall logs are written prior to processing by ASC.

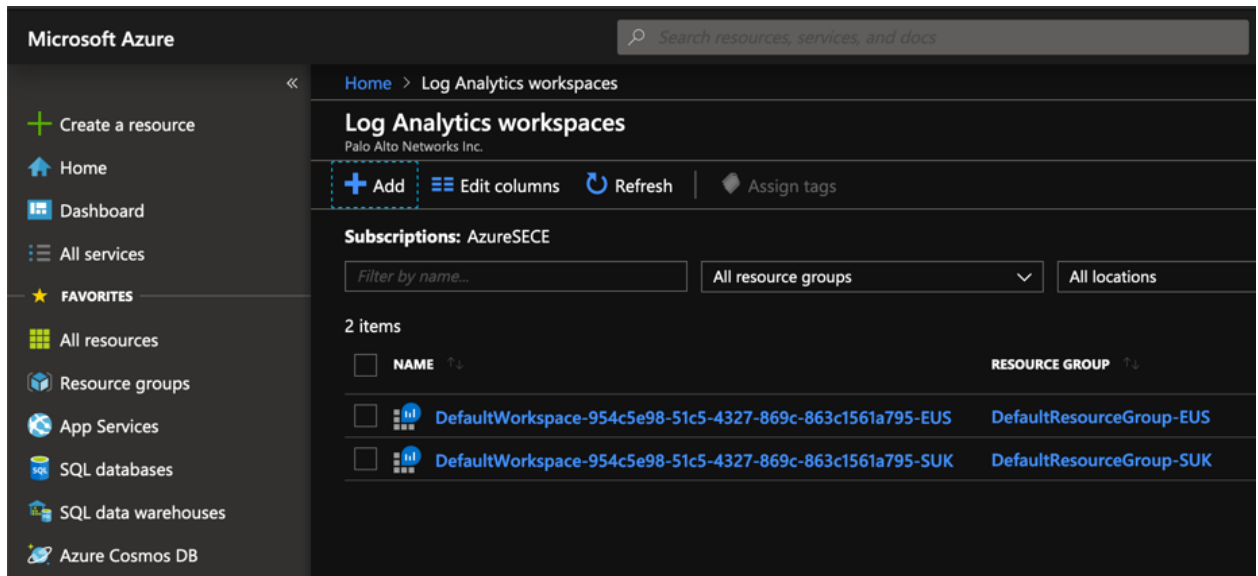
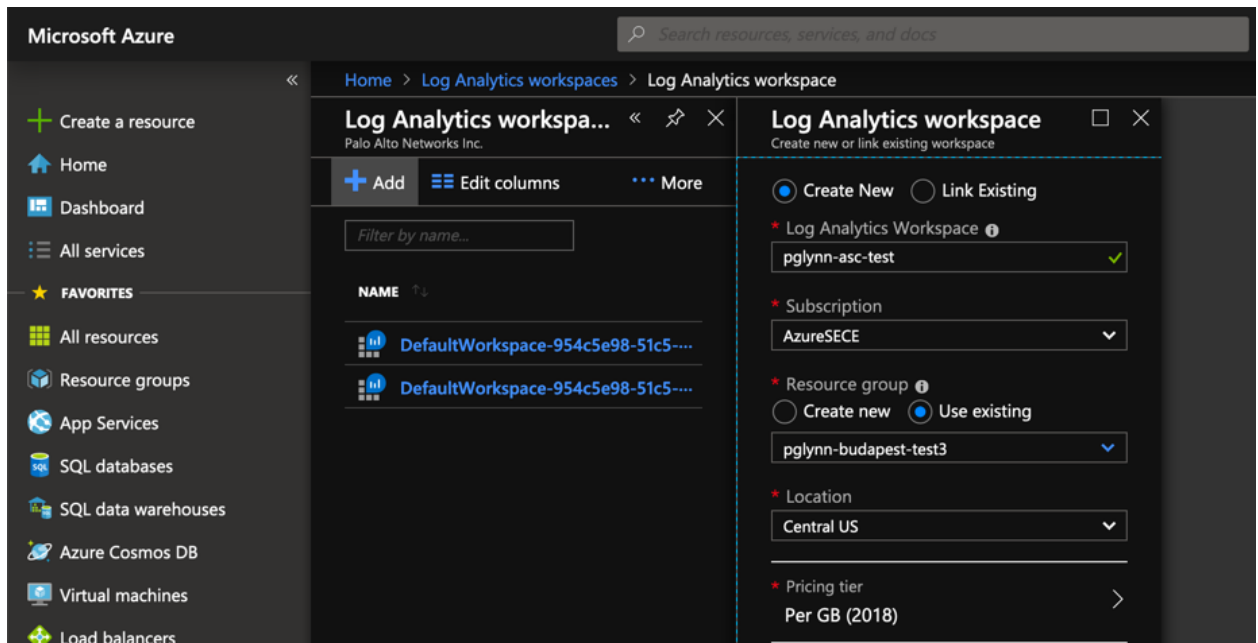
## Process Flow

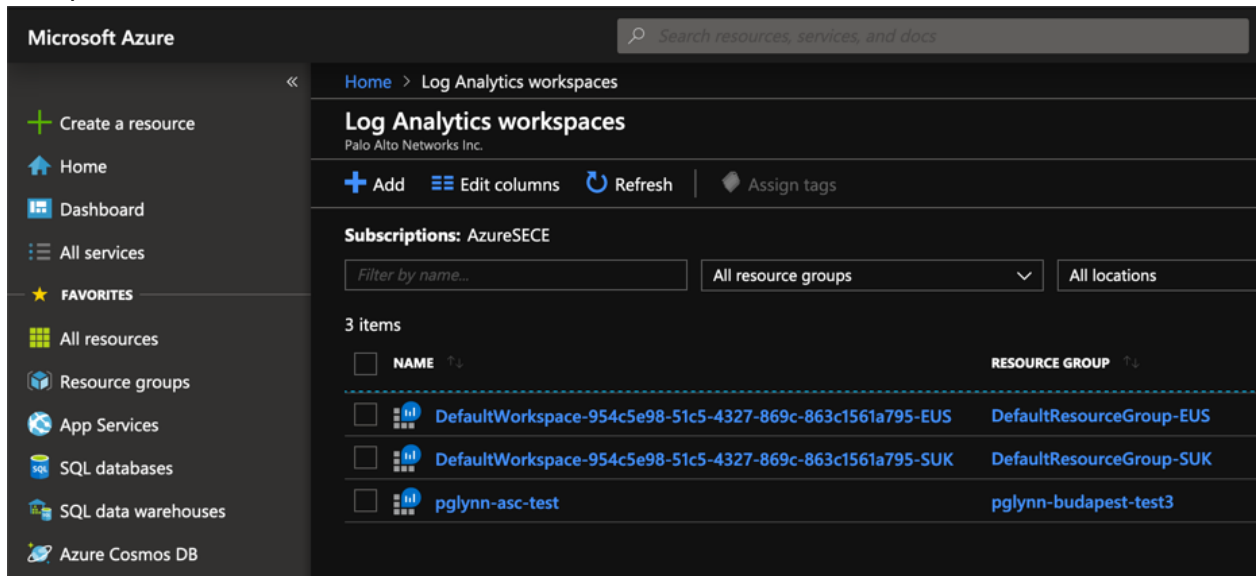
### Procedure 1: [Log Analytics Workspace Creation](#)

**Step 1** In the Azure console, open the target Resource Group.

**Step 2** Create a new Log Analytics Workspace



**Step 3** Click “Add”**Step 4** Specify the relevant parameters and click “OK”.

**Step 5** Complete.

The screenshot shows the Microsoft Azure portal interface. On the left is a navigation sidebar with options like 'Create a resource', 'Home', 'Dashboard', 'All services', and a 'FAVORITES' section. The main content area is titled 'Log Analytics workspaces' and shows a list of 3 items. The items are listed in a table with columns for 'NAME' and 'RESOURCE GROUP'. The items are 'DefaultWorkspace-954c5e98-51c5-4327-869c-863c1561a795-EUS', 'DefaultWorkspace-954c5e98-51c5-4327-869c-863c1561a795-SUK', and 'pglynn-asc-test'.

Microsoft Azure

Search resources, services, and docs

Home > Log Analytics workspaces

### Log Analytics workspaces

Palo Alto Networks Inc.

+ Add Edit columns Refresh Assign tags

Subscriptions: AzureSECE

Filter by name... All resource groups All locations

3 items

	NAME	RESOURCE GROUP
<input type="checkbox"/>	DefaultWorkspace-954c5e98-51c5-4327-869c-863c1561a795-EUS	DefaultResourceGroup-EUS
<input type="checkbox"/>	DefaultWorkspace-954c5e98-51c5-4327-869c-863c1561a795-SUK	DefaultResourceGroup-SUK
<input type="checkbox"/>	pglynn-asc-test	pglynn-budapest-test3

# Gather Information

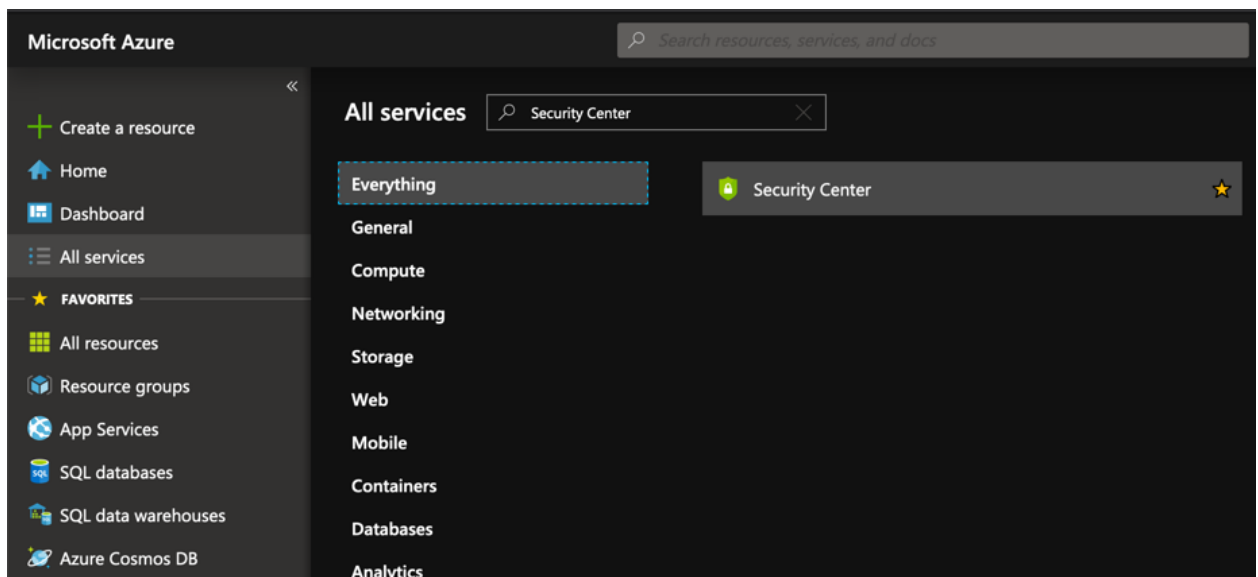
## Overview

Only authenticated systems are permitted to send logs to the Log Analytics Workspace. Prior to the deployment/configuration of the syslog receiver, it is necessary to gather the authentication information from ASC.

## Process Flow

### Procedure 2: [Information Gathering](#)

**Step 1** In the Azure console, open Security Center.



**Step 2** Select “Compute & apps” and then click “+ Add Computers”.

Home > Security Center - Compute & apps

## Security Center - Compute & apps

Showing subscription 'AzureSECE'

Search (Ctrl+/)

**+ Add Computers**

**GENERAL**

- Overview
- Getting started
- Events
- Search

**POLICY & COMPLIANCE**

- Coverage
- Secure score
- Regulatory compliance
- Security policy

**RESOURCE SECURITY HYGIENE**

- Recommendations
- Compute & apps

**Overview**

VMs and Computers

VM scale sets


Search recommendations


RECOMMENDATION	SECURE S...	FAILED RESOURCES
Install a vulnerability assessment solution on your ...	+30	13 of 180 virt...
Resolve monitoring agent health issues on your m...	+20	91 of 180 virt...
Web Application should only be accessible over H...	+20	1 of 1 web ap...
Function App should only be accessible over HTTPS	+20	1 of 1 functio...
Install endpoint protection solution on virtual mac...	+15	9 of 180 virtu...
Apply disk encryption on your virtual machines	+10	179 of 180 vir...

**Step 3** Click the previously-created workspace name.

Home > Security Center - Compute & apps > Onboard servers to Security Center

## Onboard servers to Security Center


 Refresh

 Onboard servers to Security Center

To onboard servers to Security Center:

1. Select or create a workspace in which to store the data.  
[Create New Workspace](#)
2. Select **Upgrade** to set the workspace's pricing tier to Standard and start your free 30-day trial. ⓘ
3. Select **Add Servers** to view instructions on how to install the Microsoft Monitoring Agent. [Learn more>](#)
4. After onboarding, you can monitor the machines under [Compute and apps>](#)

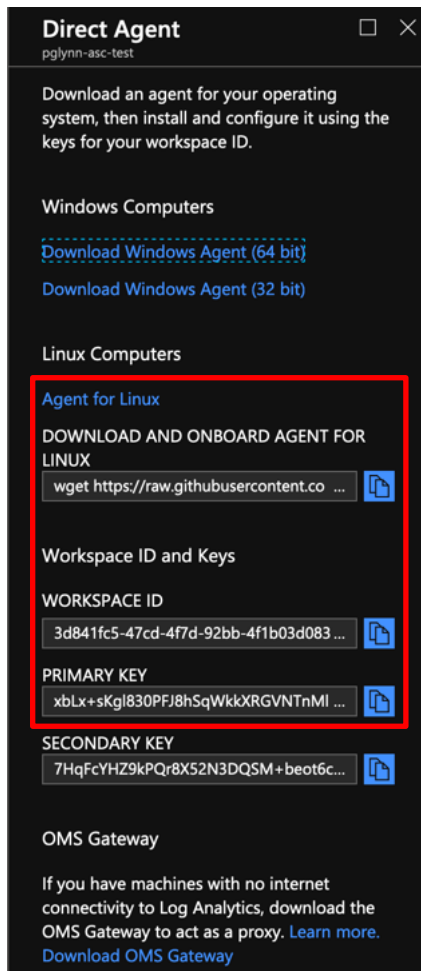
You may see only workspaces in subscriptions for which you have permission. To get tenant-wide visibility follow these [instructions](#).

WORKSPACE NAME	COVERAGE	VMS & SERVERS
 pglynn-asc-test	Standard	1

Azure Security Center Standard will be applied \$15/node/month. [Pricing details>](#)



**Step 4** Make a note of the Workspace ID and Primary Key, then download the relevant agent.



**Step 5** Download the desired Linux agent version from GitHub (1.10.0-1 for 64-bit Linux variants in this case).

Code Issues 84 Pull requests 22 Projects 0 Wiki Insights

Releases Tags

Latest release

OMSAgent\_v1.10....  
3ce6775

## OMS Agent for Linux GA v1.10.0-1

aliabuckner released this 5 days ago · 9 commits to master since this release

### MD5

EDC43B0AADAD5E37C844DB31A5112356	omsagent-1.10.0-1.universal.x64.sh
1CB68180016AD2CABF27FC7B5D2A5463	omsagent-1.10.0-1.universal.x86.sh

### SHA256

82C228BF1367254DAFAB0C8D0B4B5B3F83CB3635D8298DFE320BD309957E71CB	omsagent-1.10.0-1.universal.x64.sh
53D23970C13B3D79F95D1A1D4CD9315F3358B5095FE8760DF709982931061ED2	omsagent-1.10.0-1.universal.x86.sh

[License](#)

[Documentation](#)

# Build a Linux Host

## Overview

For extant firewalls, traffic logs must be sent through an intermediary system to Log Analytics. In this example, a Linux host is deployed and configured to be that intermediary system. As noted earlier, multiple Linux variants or Windows systems may be used.

## Process Flow

### Procedure 3: [Deploy/configure a Linux Host](#)

The guide moves on to deploy a syslog receiver into the Resource Group. In order to forward logs from the firewall to ASC, a syslog receiver must be used to take in the firewall logs and forward them to the Log Analytics Workspace.

In this example, an Ubuntu server (16.0.4 LTS) is used but other Linux variants as well as Microsoft Windows are also supported.

The host is deployed into the subnet containing the management interface of the firewall; however, it can be deployed into a separate Resource Group/VNet/subnet provided the firewall can send syslog messages to the host.

**Step 1** In the Azure console, deploy a Linux server to act as the syslog receiver/log forwarder.

The screenshot shows the Microsoft Azure portal interface for creating a virtual machine. The breadcrumb trail is: Home > Resource groups > pglynn-asctest > Get Started > Ubuntu Server > Create a virtual machine. The page title is 'Create a virtual machine'. A green banner indicates 'Validation passed'. The 'Review + create' tab is active, showing the following details:

- PRODUCT DETAILS**
  - Ubuntu Server by Canonical. Pricing not available for this offering. Links: Terms of use | Privacy policy.
  - Standard D2s v3 by Microsoft. Subscription credits apply. Price: 0.1100 USD/hr. Link: Pricing for other VM sizes.
- TERMS**

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.
- BASICS**

Subscription	AzureSECE
Resource group	pglynn-asctest
Virtual machine name	pglynn-oms-agent
Region	Central US
Availability options	No infrastructure redundancy required
Authentication type	SSH public key

**Step 2** Upload the agent to the Linux host.

**Step 3** Connect to the Linux host and execute the command “sudo su –” to become the root user.

**Step 4** Navigate to the directory /etc/rsyslog.d/

**Step 5** Edit the file “security-config-omsagent.conf”

```

1. root@pglynn-oms-agent: /etc/rsyslog.d (ssh)
pglynn@pglynn-oms-agent: ~$ sudo su -
root@pglynn-oms-agent: ~# cd /etc/rsyslog.d/
root@pglynn-oms-agent: /etc/rsyslog.d# vi security-config-omsagent.conf

```

**Step 6** Insert the following text into the file:

```
#OMS_facility = local4

local4.debug @127.0.0.1:25226
```

**Step 7** Save the file. This example assumes rsyslogd is in use. If syslog-ng or another syslog service is in use, refer to documentation for that service for configuration details. The desired result is for syslog messages received on the local4 syslog facility to be resent to localhost on port 25226.

**Step 8** Edit the file “/etc/rsyslog.conf” and enable syslog reception on UDP/514.

```

1. root@pglynn-oms-agent: ~ (ssh)
# /etc/rsyslog.conf Configuration file for rsyslog.
#
# For more information see
# /usr/share/doc/rsyslog-doc/html/rsyslog_conf.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
#### MODULES ####
#####

module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

"/etc/rsyslog.conf" 61L, 1371C 19,1 Top

```

This example assumes rsyslogd is in use. If syslog-ng or another syslog service is in use, refer to documentation for that service for configuration details. The desired result is for the syslog daemon to receive logs from external hosts on UDP port 514 (or whichever port is desired).

**Step 9** Install the auditd package.

```

1. root@pglynn-oms-agent: /var/tmp (ssh)
root@pglynn-oms-agent: /var/tmp# apt-get install auditd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libauparseo
Suggested packages:
  audispd-plugins
The following NEW packages will be installed:
  auditd libauparseo
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 228 kB of archives.
After this operation, 737 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://azure.archive.ubuntu.com/ubuntu xenial-updates/main amd64 libaupars
eo amd64 1:2.4.5-1ubuntu2.1 [35.5 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu xenial-updates/main amd64 auditd am
d64 1:2.4.5-1ubuntu2.1 [192 kB]
Fetched 228 kB in 0s (1,493 kB/s)
Selecting previously unselected package libauparseo:amd64.
(Reading database ... 53440 files and directories currently installed.)
Preparing to unpack .../libauparseo_1%3a2.4.5-1ubuntu2.1_amd64.deb ...
Unpacking libauparseo:amd64 (1:2.4.5-1ubuntu2.1) ...
Selecting previously unselected package auditd.
Preparing to unpack .../auditd_1%3a2.4.5-1ubuntu2.1_amd64.deb ...

```

**Step 10** Navigate to the directory where the agent software was uploaded.

```

1. root@pglynn-oms-agent: /var/tmp (ssh)
pglynn@pglynn-oms-agent: ~$ sudo su -
root@pglynn-oms-agent: ~# cd /etc/rsyslog.d/
root@pglynn-oms-agent: /etc/rsyslog.d# vi security-config-omsagent.conf
root@pglynn-oms-agent: /etc/rsyslog.d# cd /var/tmp
-su: cd: /var/tmp: No such file or directory
root@pglynn-oms-agent: /etc/rsyslog.d# cd /var/tmp
root@pglynn-oms-agent: /var/tmp# ls
cloud-init
omsagent-1.10.0-1.universal.x64.sh
systemd-private-4d627da548144e3a8261b066d97ca874-systemd-timesyned.service-OIi3Q
3
root@pglynn-oms-agent: /var/tmp# █

```

**Step 11** Set the file to executable with the command “chmod +x <file\_name>”.

```

1. root@pglynn-oms-agent: /var/tmp (ssh)
pglynn@pglynn-oms-agent: ~$ sudo su -
root@pglynn-oms-agent: ~# cd /etc/rsyslog.d/
root@pglynn-oms-agent: /etc/rsyslog.d# vi security-config-omsagent.conf
root@pglynn-oms-agent: /etc/rsyslog.d# cd /var/tmp
-su: cd: /var/tmp: No such file or directory
root@pglynn-oms-agent: /etc/rsyslog.d# cd /var/tmp
root@pglynn-oms-agent: /var/tmp# ls
cloud-init
omsagent-1.10.0-1.universal.x64.sh
systemd-private-4d627da548144e3a8261b066d97ca874-systemd-timesyned.service-OIi3Q
3
root@pglynn-oms-agent: /var/tmp# chmod +x omsagent-1.10.0-1.universal.x64.sh
root@pglynn-oms-agent: /var/tmp# ls
cloud-init
omsagent-1.10.0-1.universal.x64.sh
systemd-private-4d627da548144e3a8261b066d97ca874-systemd-timesyned.service-OIi3Q
3
root@pglynn-oms-agent: /var/tmp# █

```

- Step 12** Usage help can be viewed by issuing the command “omsagent-<version>.universal.x64.sh – help”. The Options of interest are “-w id” and “-s key”. These allow automatic onboarding of the agent to Security Center.

```
1.root@pglynn-oms-agent: /var/tmp (ssh)
usage: omsagent-1.10.0-1.universal.x64.sh [OPTIONS]
Options:
  --extract           Extract contents and exit.
  --force            Force upgrade (override version checks).
  --install          Install the package from the system.
  --purge           Uninstall the package and remove all related data.
  --remove          Uninstall the package from the system.
  --restart-deps    Reconfigure and restart dependent service(s).
  --source-references Show source code reference hashes.
  --upgrade         Upgrade the package in the system.
  --enable-opsmgr   Enable port 1270 for usage with opsmgr.
  --version         Version of this shell bundle.
  --version-check   Check versions already installed to see if upgradab
le.
  --debug           use shell debug mode.
  -w id, --id id    Use workspace ID <id> for automatic onboarding.
  -s key, --shared key Use <key> as the shared key for automatic onboardin
g.
  -d dmn, --domain dmn Use <dmn> as the OMS domain for onboarding. Optiona
l.
  -p conf, --proxy conf Use <conf> as the proxy configuration.
                        ex: -p [protocol://][user:password@]proxyhost[:port]
```

- Step 13** Run the installation using the Workspace ID and Primary Key information noted earlier:

```
omsagent-1.10.0-1.universal.x64.sh --install -w <Workspace ID> -s
<Primary Key>
```

```
1.root@pglynn-oms-agent: /var/tmp (ssh)
root@pglynn-oms-agent: /var/tmp# ./omsagent-1.10.0-1.universal.x64.sh --install -
w 3d841fc5-47cd-4f7d-92bb-4f1b03d083c2 -s xBLx+sKgl83oPFJ8hSqWkkXRGVNTnMl mXD1Tsi
vGu56frwuTXf4UVlW4TK55uJegOXbAQZok4nxLSv1a2ZoX5g==
Checking host architecture ...
Extracting...
----- Installing package: omi (omi-1.6.0-0.ulinux.x64) -----
Selecting previously unselected package omi.
(Reading database ... 53498 files and directories currently installed.)
Preparing to unpack 100/omi-1.6.0-0.ulinux.x64.deb ...
Creating omiusers group ...
sent invalidate(passwd) request, exiting
sent invalidate(group) request, exiting
sent invalidate(group) request, exiting
Creating omi_group ...
sent invalidate(passwd) request, exiting
sent invalidate(group) request, exiting
sent invalidate(group) request, exiting
Creating omi service account ...
sent invalidate(passwd) request, exiting
sent invalidate(group) request, exiting
sent invalidate(passwd) request, exiting
sent invalidate(group) request, exiting
Unpacking omi (1.6.0.0) ...
Setting up omi (1.6.0.0) ...
Generating a 2048 bit RSA private key
```

Change to the directory “/etc/opt/microsoft/omsagent/<Workspace ID>/conf/omsagent.d” and edit the file “security\_events.conf”. Populate it with the following text (ensure that the “format” directive is on a single line):

```
<source>
type syslog
port 25226
bind 127.0.0.1
```

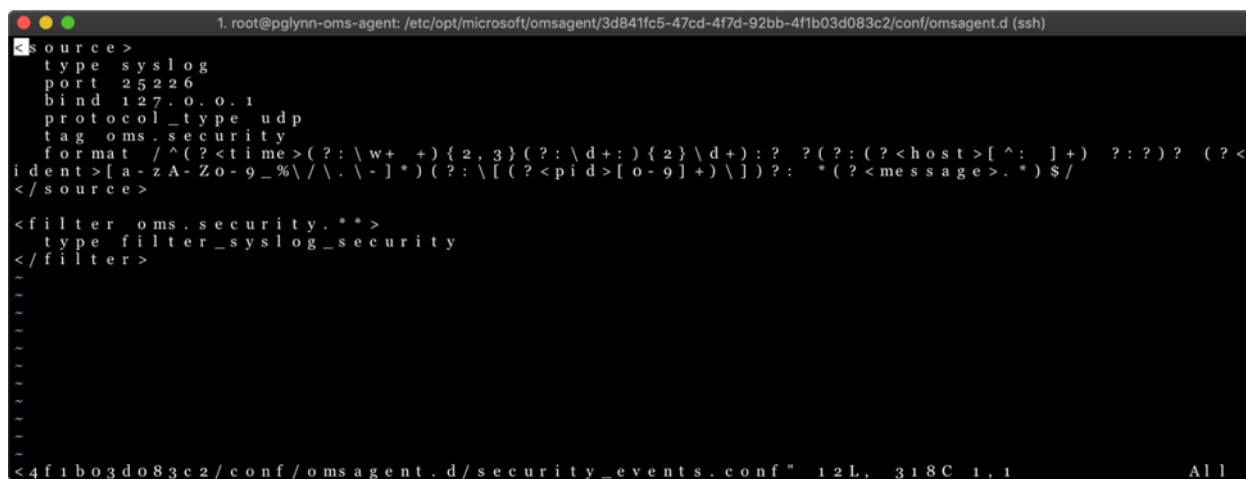
```

protocol_type udp
tag oms.security
format /^(?<time>(?:\w+ ){2,3}(?:\d+:){2}\d+):? ?(?: (?<host>[^\: ]+)
?:?)? (?<ident>[a-zA-Z0-9_%\./\.-]*) (?:\[ (?<pid>[0-9]+\)\])?:
*(?<message>.*)$/
</source>
<filter oms.security.**>
type filter_syslog_security
</filter>

```

N.B. – The file may also be downloaded from the MS GitHub Repository for upload to the Linux host:

[https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/conf/omsagent.d/security\\_events.conf](https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/conf/omsagent.d/security_events.conf)



```

1. root@pglynn-oms-agent: /etc/opt/microsoft/omsagent/3d841fc5-47cd-4f7d-92bb-4f1b03d083c2/conf/omsagent.d (ssh)
source >
type syslog
port 25226
bind 127.0.0.1
protocol_type udp
tag oms.security
format /^(?<time>(?:\w+ ){2,3}(?:\d+:){2}\d+):? ?(?: (?<host>[^\: ]+)
?:?)? (?<ident>[a-zA-Z0-9_%\./\.-]*) (?:\[ (?<pid>[0-9]+\)\])?:
*(?<message>.*)$/
</source>
<filter oms.security.**>
type filter_syslog_security
</filter>
<4f1b03d083c2/conf/omsagent.d/security_events.conf" 12L, 318C 1,1 All

```

**Step 14** Reboot the Linux host to start/restart all services.

## Configure the firewall

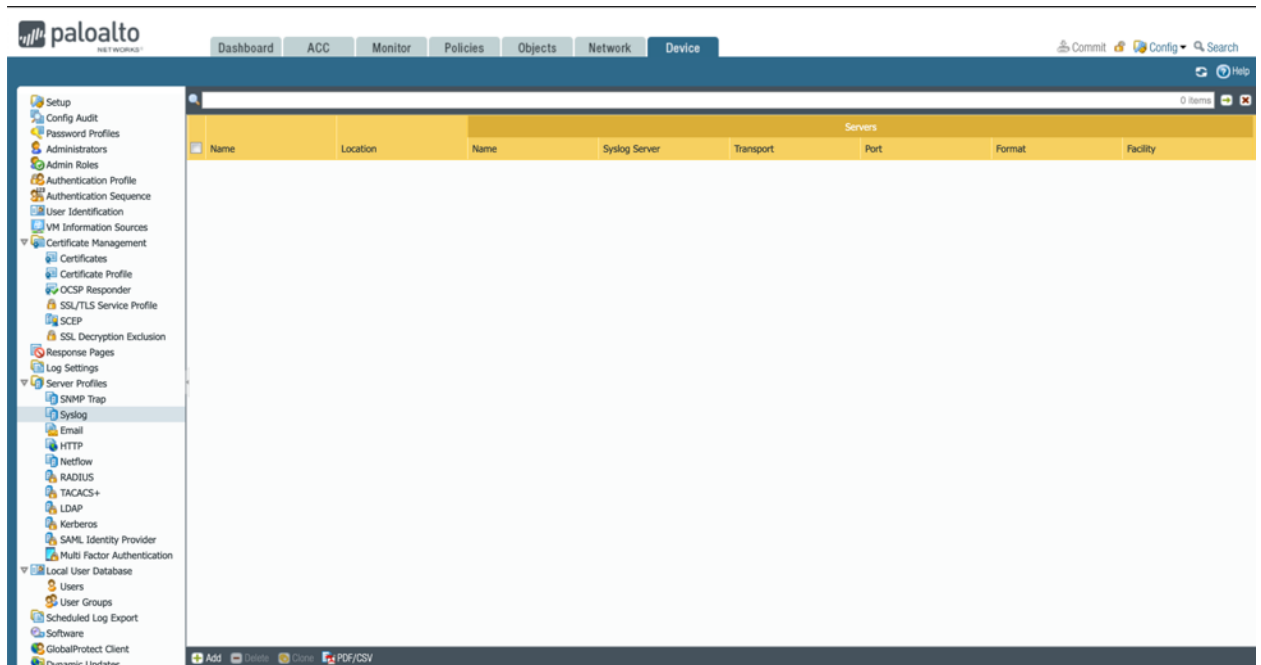
### Overview

At this stage, the firewall is configured to send traffic to the syslog server and on to Log Analytics.

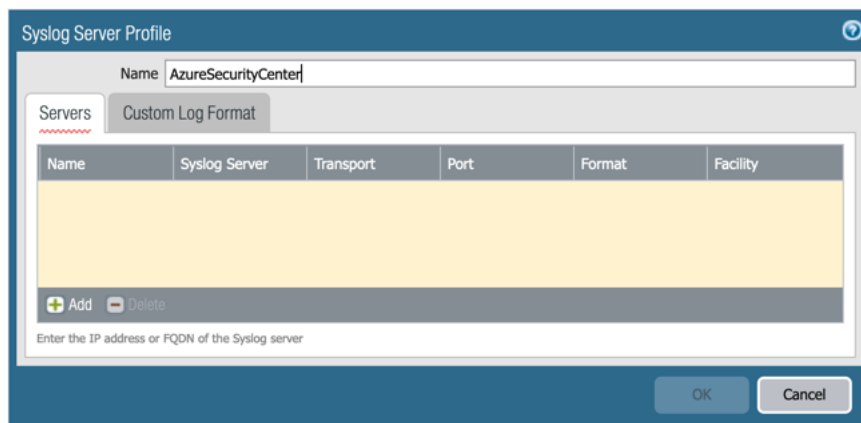
### Process Flow

#### Procedure 4: Configure the firewall

**Step 1** Login to the Firewall and navigate to the Device Tab > Server Profiles > Syslog.



**Step 2** Click “Add” and specify a Name for the profile.



**Step 3** Under Servers, click “Add”. Specify:

- Name (freeform text)
- Internal IP of the Linux host
- Transport (UDP default)
- Port (514 default)
- Facility (LOG\_LOCAL4)



**Syslog Server Profile**

Name:

Servers: **Custom Log Format**

Name	Syslog Server	Transport	Port	Format	Facility
SecurityCenter	10.5.0.5	UDP	514	BSD	LOG_LOCAL4

Enter the IP address or FQDN of the Syslog server

**Step 4** Click on the “Custom Log Format” tab.

**Syslog Server Profile**

Name:

Servers: **Custom Log Format**

Log Type	Custom Format
Config	Default
System	Default
Threat	CEF:0 Palo Alto Networks PAN-OS \$sender_sw_version \$subtype \$type \$number-of-severity rt=\$cef-formatted-receive_time deviceExternalId=\$serial src=\$src dst=\$dst sourceTranslatedAddress=\$natsrc destinationTranslatedAddress=\$natdst cs1Label=Rule cs1=\$rule suser=\$srcuser duser=\$dstuser app=\$app cs3Label=Virtual System cs3=\$vsys cs4Label=Source Zone cs4=\$from cs5Label=Destination Zone cs5=\$to deviceInboundInterface=\$inbound_if deviceOutboundInterface=\$outbound_if cs6Label=LogProfile cs6=\$logset cn1Label=SessionID cn1=\$sessionid cnt=\$repeatcnt spt=\$sport dpt=\$dport sourceTranslatedPort=\$natport destinationTranslatedPort=\$natdport flexString1Label=Flags flexString1=\$flags proto=\$proto act=\$action request=\$misc cs2Label=URL Category cs2=\$category flexString2Label=Direction flexString2=\$direction PanOSActionFlags=\$actionflags externalId=\$seono

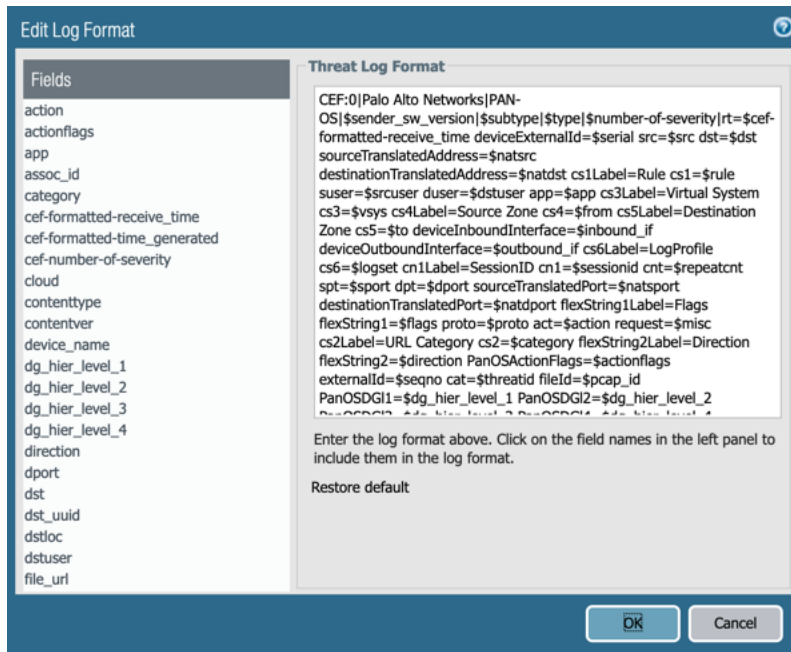
☐ **Escaping**

Escaped Characters:

Escape Character:

**Step 5** Click on the log type “Threat” to create a custom format for the logs and paste in the CEF format described in the section CEF-style Log Formats in the following link:

<https://docs.paloaltonetworks.com/resources/cef>

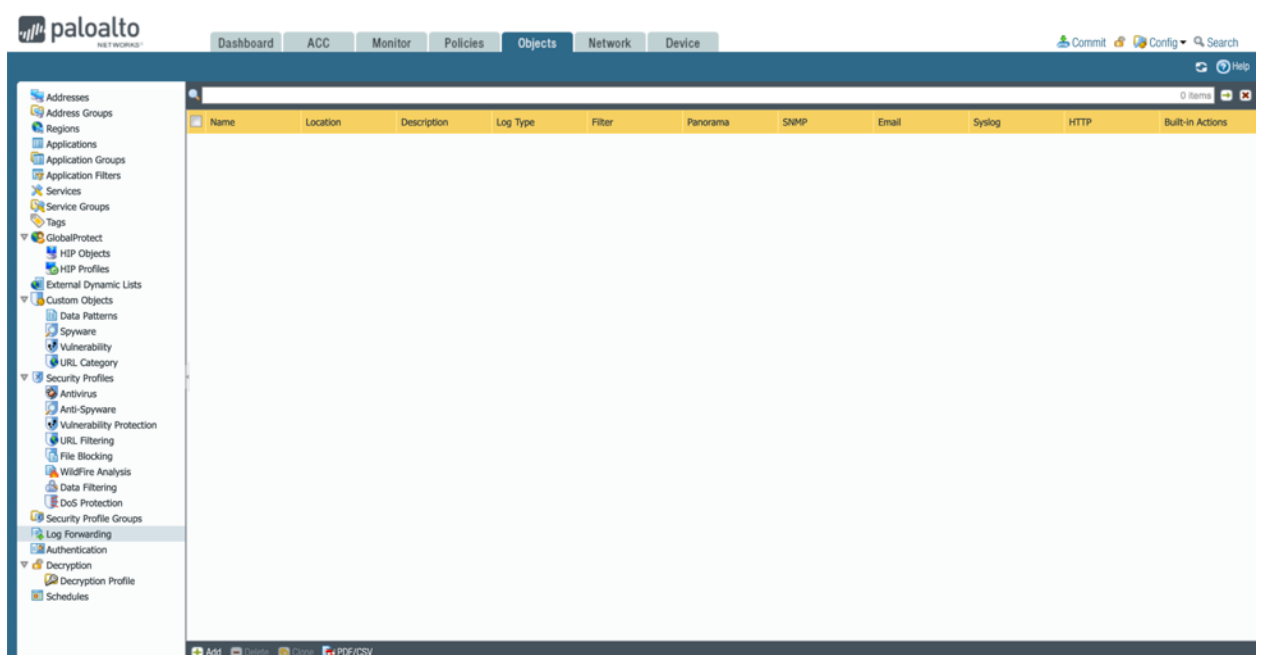


N.B. – Copy/paste actions occasionally result in spurious characters or spaces being inadvertently included. This may result in logs not showing up in the Log Analytics Database of having incorrectly-populated fields.

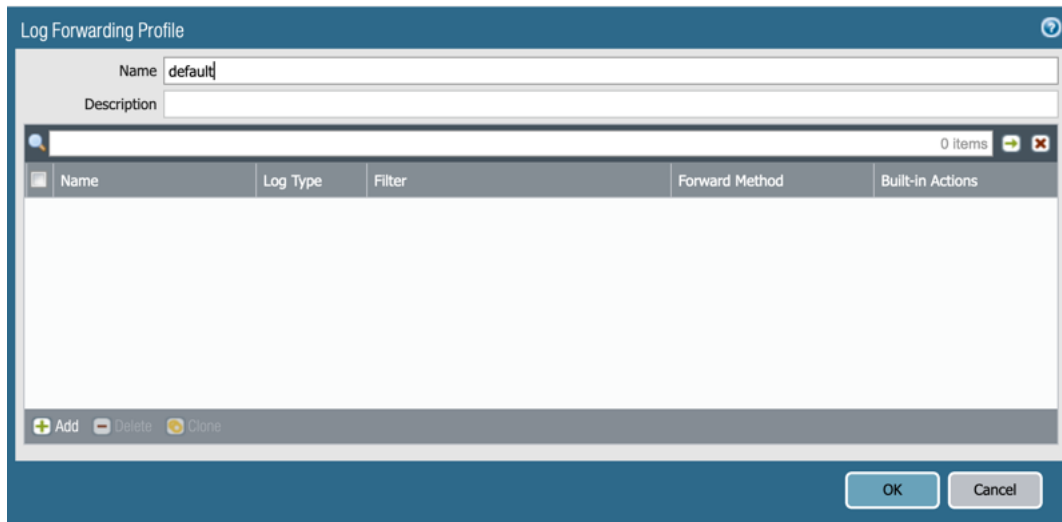
Click “OK” when done.

**Step 6** Repeat the previous two steps as necessary for the other logs (e.g. Traffic, Wildfire, URL, System, Config, etc.).

**Step 7** Navigate to the Objects Tab > Log Forwarding.



**Step 8** Click “Add” and specify a name.



The screenshot shows the "Log Forwarding Profile" configuration window. At the top, there are two text input fields: "Name" (containing "default") and "Description". Below these is a table with the following columns: "Name", "Log Type", "Filter", "Forward Method", and "Built-in Actions". The table is currently empty, with "0 items" displayed in the top right corner. At the bottom left of the table area, there are three buttons: "Add", "Delete", and "Clone". At the bottom right of the window, there are "OK" and "Cancel" buttons.

N.B. – If the profile is named “default”, it will automatically show up as the default log forwarding profile in each new rule created. It can also be created on Panorama and be pushed to the firewall(s) as well as be added to an existing log forwarding profile.

**Step 9** Click “Add” and specify:

- Name (Free form text)
- Log Type
- The previously-created Syslog profile

**Log Forwarding Profile Match List**

Name: SecurityCenter-Threat

Description:

Log Type: threat

Filter: All Logs

**Forward Method**

☐ Panorama

SNMP	Email
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete
<input type="checkbox"/> Syslog <input type="checkbox"/> AzureSecurityCenter	<input type="checkbox"/> HTTP
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete

**Built-in Actions**

Name	Type
<input type="checkbox"/> Add <input type="checkbox"/> Delete	

OK Cancel

**Step 10** Click “OK” when done. Repeat as required for other log types.

**Log Forwarding Profile**

Name: default

Description:

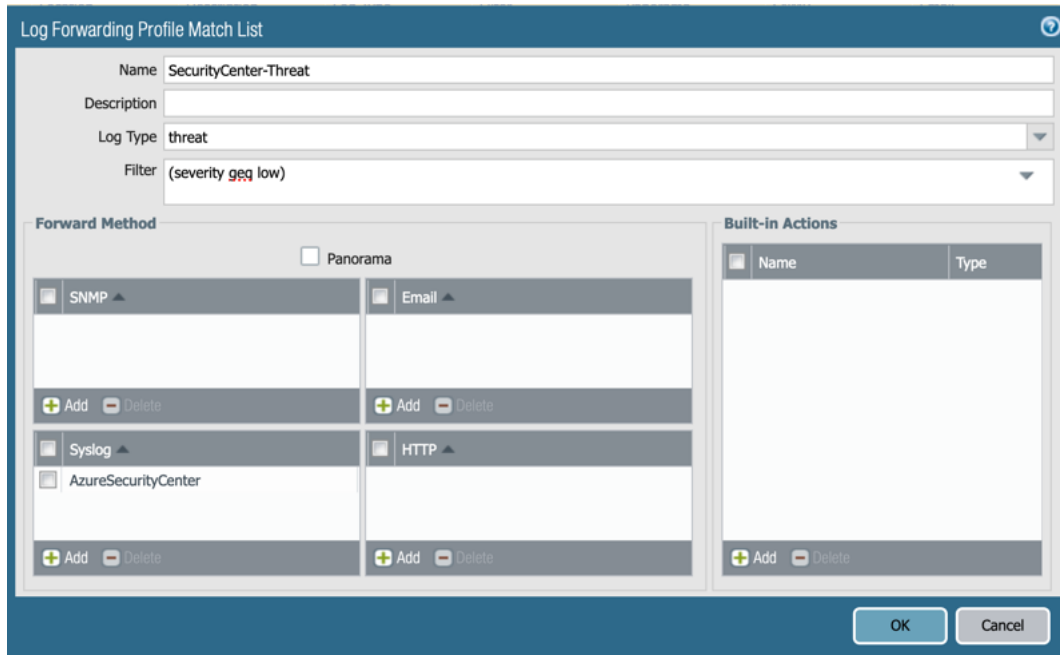
2 items

Name	Log Type	Filter	Forward Method	Built-in Actions
<input checked="" type="checkbox"/> SecurityCenter-Threat	threat	All Logs	SysLog • AzureSecurityCenter	
<input type="checkbox"/> SecurityCenter-WildFire	wildfire	All Logs	SysLog • AzureSecurityCenter	

☐ Add ☐ Delete ☐ Clone

OK Cancel

N.B. – By default, logs of severity “Low”, “Medium”, “High” and “Critical” are displayed in Security Center. Filters can be used to limit the logs that are sent. This can be used to send “interesting” logs and filter out low value ones (e.g. low level).



**Log Forwarding Profile Match List**

Name: SecurityCenter-Threat

Description:

Log Type: threat

Filter: (severity ~~999~~ low)

**Forward Method**

☐ Panorama

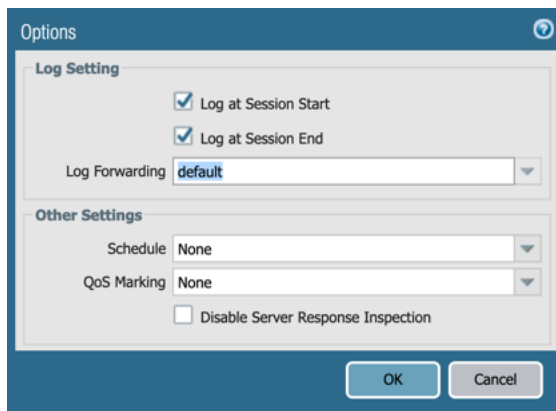
SNMP	Email
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete
<input type="checkbox"/> Syslog	<input type="checkbox"/> HTTP
<input type="checkbox"/> AzureSecurityCenter	
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete

**Built-in Actions**

Name	Type
<input type="checkbox"/> Add <input type="checkbox"/> Delete	

OK Cancel

**Step 11** Attach the Log Forwarding profile to the target rules and commit when done.



**Options**

**Log Setting**

☒ Log at Session Start

☒ Log at Session End

Log Forwarding: default

**Other Settings**

Schedule: None

QoS Marking: None

☐ Disable Server Response Inspection

OK Cancel

## Verification

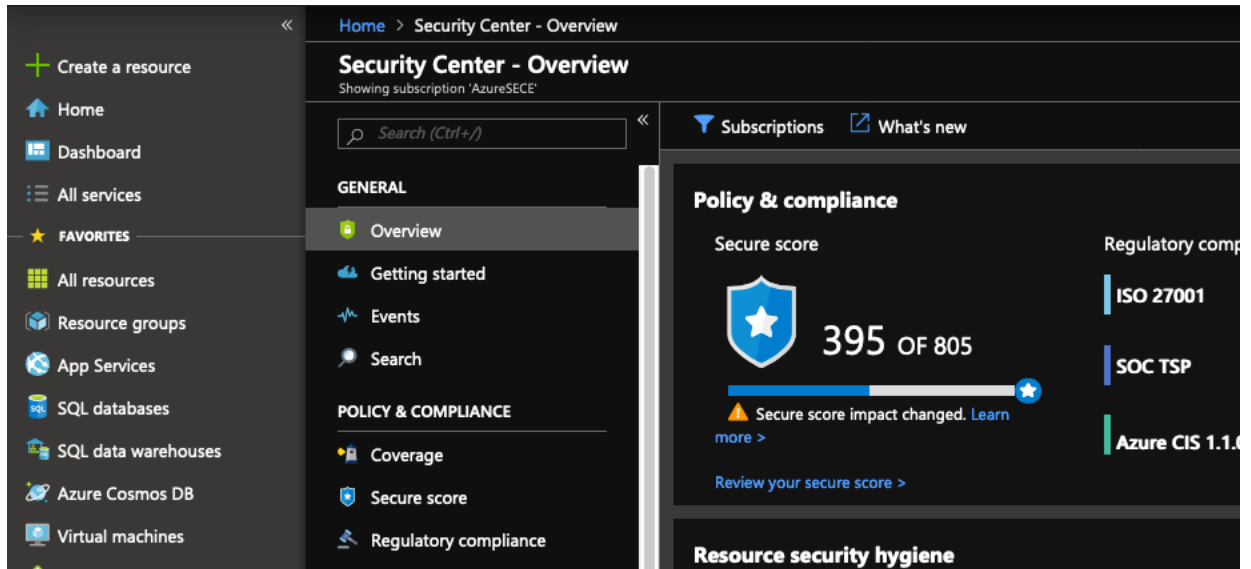
### Overview

At this stage, the firewall should be sending traffic to Log Analytics although it may take some time for them to show up in the Azure console. Confirmation may be had by looking at the events in ASC.

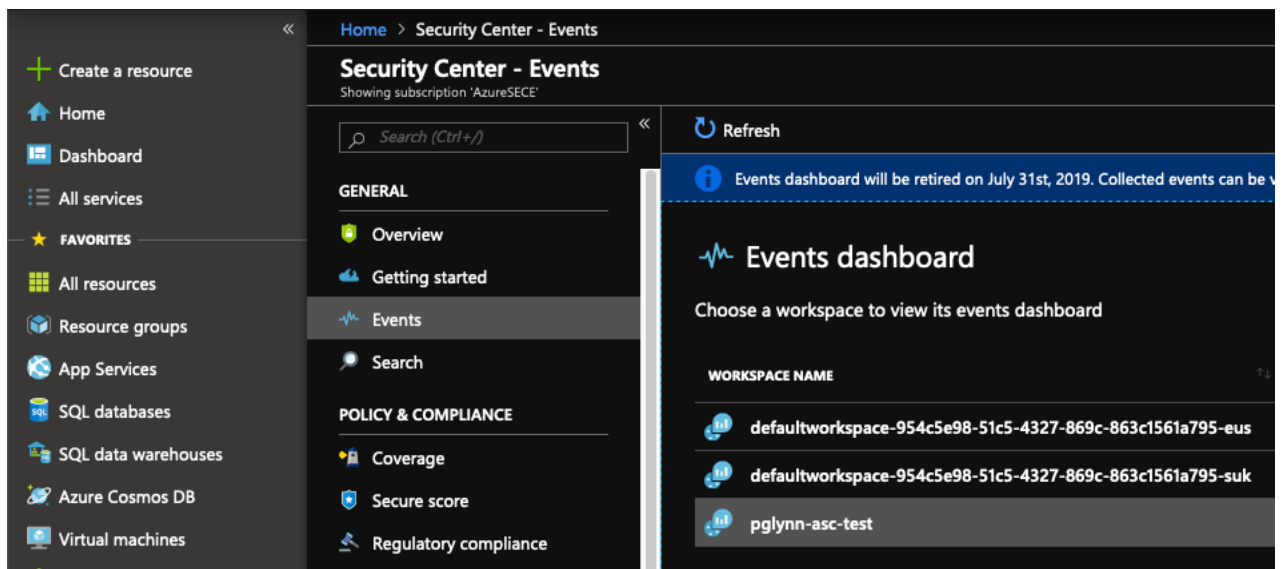
# Process Flow

## Procedure 5: Verify logs in ASC

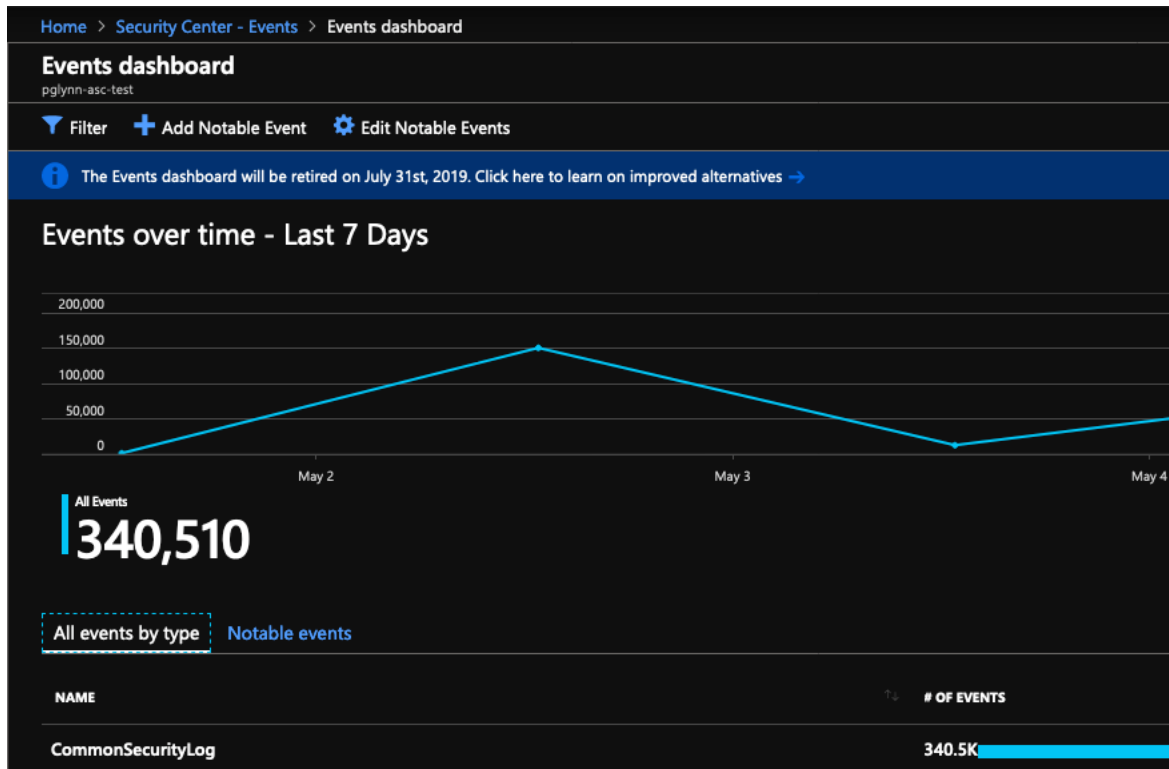
### Step 1 Launch Azure Security Center



### Step 2 Click on Events



### Step 3 Click on the Log Analytics Workspace name that was created earlier



**Step 4** The logs will show up in the CommonSecurityLog

Home > Security Center - Events > Events dashboard > Logs

## Logs

pglynn-asc-test

New Query 1\* +

pglynn-asc-test Run Time range: Custom

Schema Filter (preview) <<

Filter by name or type...

Collapse all

**Active**

- pglynn-asc-test
  - LogManagement
  - Security
    - CommonSecurityLog
    - LinuxAuditLog
    - ProtectionStatus
    - SecurityAlert
    - SecurityBaseline
    - SecurityBaselineSummary
    - SecurityDetection
    - SecurityEvent
    - SysmonEvent
    - Update

CommonSecurityLog

Completed. Showing partial results from the custom time range. ⓘ

TABLE CHART Columns ▾

Drag a column header and drop it here to group by that column

	TenantId	SourceSystem	TimeGenerated [UTC]
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:36.493
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:40.873
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:40.873
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:40.873
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:40.873
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:40.873
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:40.873
>	989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:40.873

**Step 5** Select an individual log to view the details:

The screenshot shows the Azure Security Center Logs interface. The breadcrumb navigation is: Home > Security Center - Events > Events dashboard > Logs. The workspace is 'pglynn-asc-test'. A query named 'New Query 1\*' is selected. The schema is 'CommonSecurityLog'. The interface shows a table of results with columns: TenantId, SourceSystem, and TimeGenerated [UTC]. The first row of data is expanded, showing details for a log entry.

TenantId	SourceSystem	TimeGenerated [UTC]
989ef0e0-9fb6-4728-9e7e-65b01355f195	OpsManager	2019-05-02T22:31:36.493

Expanded log entry details:

TenantId	989ef0e0-9fb6-4728-9e7e-65b01355f195
SourceSystem	OpsManager
TimeGenerated [UTC]	2019-05-02T22:31:36.493Z
ReceiptTime	May 02 2019 22:31:36 GMT
DeviceVendor	Palo Alto Networks
DeviceProduct	PAN-OS
DeviceEventClassID	end
LogSeverity	1
DeviceAction	allow
SimplifiedDeviceAction	allow
Computer	pan-fw
DestinationPort	443

# Troubleshooting

## Overview

Occasionally, the logs will fail to show up in ASC. When this happens, there are a number of places to start looking.

## Process Flow

After verifying that the firewall is correctly configured to send generated logs to the syslog receiver, check that the messages are arriving at the receiver and being properly processed.



## Procedure 6: Verify Logging

- Step 1** Login to the syslog receiver and verify that syslog messages are arriving from the firewall by performing a packet capture. The source IP address should match that of the firewall.

```
Last login: Thu May 2 12:56:48 2019 from 104.219.139.2
pglynn@pglynn-asc-oms:~$ sudo su -
root@pglynn-asc-oms:~# tcpdump -nti etho 'port 514'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on etho, link-type EN10MB (Ethernet), capture size 262144 bytes
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.error, length: 384
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 441
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 442
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 401
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 414
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 426
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 406
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 384
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 381
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 387
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 387
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 411
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 384
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 378
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 384
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 431
IP 10.5.0.4.49387 > 10.5.0.5.514: SYSLOG local4.info, length: 431
^C
17 packets captured
28 packets received by filter
11 packets dropped by kernel
root@pglynn-asc-oms:~#
```

- Step 2** Perform a packet capture on the loopback interface of the syslog receiver to ensure that the packets are being forwarded to the log processing service. The traffic should arrive on the port specified in the syslog configuration (25226 by default).

```
root@pglynn-asc-oms:~# tcpdump -nti lo 'port 25226'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1237
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1237
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1237
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1189
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1227
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1190
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1228
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1190
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1228
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1190
IP 127.0.0.1.47286 > 127.0.0.1.25226: UDP, length 1228
^
```

**Step 3** Review the agent log created on the syslog receiver. It is located at  
 /var/opt/microsoft/omsagent/< Workspace ID >/log/omsagent.log

The agent should create an entry at regular intervals for the heartbeat, when it matches (or fails to match) logs, and any other condition of interest.

```

root@pglynn-asc-oms:~# tail -100 /var/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
tag oms.update_run_progress.log
path /var/opt/microsoft/omsagent/log/urp.log
pos_file /var/opt/microsoft/omsagent/log/urp.log.pos
format json
</source>
<source>
  type exec
  tag heartbeat.output
  command echo > /dev/null
  format tsv
  keys severity, message
  run_interval 20m
</source>
<match oms.blob.**>
  type out_oms_blob
  log_level info
  num_threads 5
  omsadmin_conf_path /etc/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
  cert_path /etc/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
  key_path /etc/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
  buffer_chunk_limit 10m
  buffer_type file
  buffer_path /var/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
  buffer_queue_limit 10
  buffer_queue_full_action drop_oldest_chunk
  flush_interval 60s
  retry_limit 10
  retry_wait 30s
  max_retry_wait 9m
</match>
<match oms.** docker.**>
  type out_oms
  log_level info
  num_threads 5
  omsadmin_conf_path /etc/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
  cert_path /etc/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
  key_path /etc/opt/microsoft/omsagent/989ef0eo-9fb6-4728-9e7e-65b01355
  buffer_chunk_limit 5m
  buffer_type file

```