

Chapter 1: Centralizing Logs

Logging and Reporting Settings ?

Log Storage | Log Export and Reporting | Pre-Defined Reports | Log Collector Status

Log Storage Quota

	Quota(%)	Quota(GB/MB)	Max Days			
Traffic	29	4.56 GB	[1 - 2000]	Traffic Summary	7	1.10 GB [1 - 2000]
Threat	15	2.36 GB	[1 - 2000]	Threat Summary	2	321.94 MB [1 - 2000]
Config	4	643.88 MB	[1 - 2000]	GTP and Tunnel Summary	1	160.97 MB [1 - 2000]
System	4	643.88 MB	[1 - 2000]	SCTP Summary	0	0.00 MB [1 - 2000]
Alarm	3	482.91 MB	[1 - 2000]	URL Summary	2	321.94 MB [1 - 2000]
App Stats	4	643.88 MB	[1 - 2000]	Decryption Summary	1	160.97 MB [1 - 2000]
HIP Match	3	482.91 MB	[1 - 2000]	Hourly Traffic Summary	3	482.91 MB [1 - 2000]
GlobalProtect	1	160.97 MB	[1 - 2000]	Hourly Threat Summary	1	160.97 MB [1 - 2000]
App Pcaps	1	160.97 MB	[1 - 2000]	Hourly GTP and Tunnel Summary	0.75	120.73 MB [1 - 2000]
Extended Threat Pcaps	1	160.97 MB	[1 - 2000]	Hourly SCTP Summary	0	0.00 MB [1 - 2000]
Debug Filter Pcaps	1	160.97 MB	[1 - 2000]	Hourly URL Summary	1	160.97 MB [1 - 2000]
IP-Tag	1	160.97 MB	[1 - 2000]	Hourly Decryption Summary	0	0.00 MB [1 - 2000]
User-ID	1	160.97 MB	[1 - 2000]	Daily Traffic Summary	1	160.97 MB [1 - 2000]
HIP Reports	1	160.97 MB	[1 - 2000]	Daily Threat Summary	1	160.97 MB [1 - 2000]
Data Filtering Captures	1	160.97 MB	[1 - 2000]	Daily GTP and Tunnel Summary	0.75	120.73 MB [1 - 2000]
GTP and Tunnel	2	321.94 MB	[1 - 2000]	Daily SCTP Summary	0	0.00 MB [1 - 2000]
SCTP	0	0.00 MB	[1 - 2000]	Daily URL Summary	1	160.97 MB [1 - 2000]
Authentication	1	160.97 MB	[1 - 2000]	Daily Decryption Summary	0	0.00 MB [1 - 2000]
Decryption	1	160.97 MB	[1 - 2000]	Weekly Traffic Summary	1	160.97 MB [1 - 2000]
				Weekly Threat Summary	1	160.97 MB [1 - 2000]
				Weekly GTP and Tunnel Summary	0.75	120.73 MB [1 - 2000]
				Weekly SCTP Summary	0	0.00 MB [1 - 2000]
				Weekly URL Summary	0.75	120.73 MB [1 - 2000]

Edit settings - overmind.10 (pano) (ESXi 5.5 virtual machine)

Virtual Hardware | VM Options

➤ Add hard disk
➤ Add network adapter
➤ Add other device

CPU	8	i
Memory	16384	MB
Hard disk 1	81	GB
Hard disk 2	2	TB
Maximum Size	920.83 TB	
Type	Thin provisioned	
Disk File	[datastore1] pano.10/pano.10_1.vmdk	
Shares	Normal	1000
Limit - IOPs	Unlimited	

Save
Cancel

Panorama Settings



Panorama Servers 192.168.27.10

Enable pushing device monitoring data to Panorama

Receive Timeout for Connection to Panorama (sec) 240

Send Timeout for Connection to Panorama (sec) 240

Retry Count for SSL Send to Panorama 25

Enable automated commit recovery

Number of attempts to check for Panorama connectivity on automated commit recovery 1

Interval between retries (sec) on automated commit recovery 10

Collector Group



General | Monitoring | Device Log Forwarding | Collector Log Forwarding | Log Ingestion

Name CollectorGroup

Log Storage Total: 423.10 GB, Free: 20.31 GB

Min Retention Period (days) [1 - 2000]

Collector Group Members

Search 1 item → ×

- COLLECTORS ^
 - Panorama()
 - Collector()
- + Add - Delete

- Enable log redundancy across collectors
- Forward to all collectors in the preference list
- Enable secure inter LC Communication

OK

Cancel

Collector Group



General | Monitoring | **Device Log Forwarding** | Collector Log Forwarding | Log Ingestion

Log Forwarding Preferences

1 item → ×

<input type="checkbox"/>	DEVICES	COLLECTORS
<input type="checkbox"/>	PANgurus	Panorama Collector
<input type="checkbox"/>	RemotelAB	Collector Panorama

+ Add - Delete

OK

Cancel

SNMP Trap Server Profile



Name

Version V2c V3

NAME	SNMP MANAGER	COMMUNITY
SNMP server	192.168.27.162	notifications

SNMP Trap Server Profile



+ Add - Delete

Name

Enter the IP address:

Version V2c V3

NAME	SNMP MANAGER	USER	ENGINEID	AUTH PASSWORD	PRIV PASSWORD
snmp server	192.168.27.161	notify		*****	*****

+ Add - Delete

Enter the IP address or FQDN of the SNMP Manager

OK

Cancel

Syslog Server Profile



Name

Servers | Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
syslog server	192.168.27.14	SSL	6514	BSD	LOG_USER

+ Add - Delete

Enter the IP address or FQDN of the Syslog server

UDP
TCP
SSL

BSD
IETF

LOG_USER
LOG_LOCAL0
LOG_LOCAL1
LOG_LOCAL2
LOG_LOCAL3
LOG_LOCAL4
LOG_LOCAL5
LOG_LOCAL6
LOG_LOCAL7

OK

Syslog Server Profile



Name

Edit Log Format



Servers | Custom Log Format

LOG TYPE	CUSTOM F
Config	Default
System	Default
Threat	Default
Traffic	\$action \$app \$bytes_received \$bytes_sent \$src \$dst \$doort \$elapsed \$receive_time
URL	Default
Data	Default
WildFire	Default

Escaping
 Escaped Characters
 Escape Character

Fields
 nfrans
nssai_sd
nssai_sst
nthreats
nurlcount
outbound_if
packets
parent_session_id
parent_start_time
pkts_received
pkts_sent
pod_name
pod_namespace
policy_id
proto
receive_time
repeatcnt
rule
rule_uuid
s_decrypted
s_encrypted
sdwan_cluster
sdwan_cluster_type

Traffic Log Format

```
$action $app $bytes_received $bytes_sent $src $dst $doort $elapsed $receive_time
```

Enter the log format above. Click on the field names in the left panel to include them in the log format.

Restore default

OK

Cancel

Email Server Profile



Name

Email Display Name

From

To

Additional Recipient

Email Gateway

Type Unauthenticated SMTP SMTP over TLS

Port

TLS Version 1.2 1.1

Authentication Method

Certificate Profile

Username

Password

Confirm Password

Test Connection

OK

Cancel

HTTP Server Profile



Name

Tag Registration

The server(s) should have User-ID agent running in order for tag registration to work

Servers

Payload Format

Payload Format



LOG TYPE	FORMAT
Config	Default
System	Default
Threat	ServiceNov
Traffic	ServiceNov
URL	ServiceNov
Data	Default
WildFire	Default
Tunnel	Default
Authentication	Default
User-ID	Default
HIP Match	Default
Globalprotect	Default
Iptag	Default
Decryption	Default

Pre-defined Formats

Name

URI Format

ServiceNow Security Incident

HEADERS	VALUE
content-type	text/xml

PARAMETERS	VALUE
------------	-------

```
receive_time:$receive_time, serial:$serial,
type:$type, subtype:$subtype,
config_ver:$config_ver,
time_generated:$time_generated, source:$src,
destination:$dst, nat_source:$natsrc,
nat_destination:$natdst, rule:$rule,
source_user:$srcuser,
destination_user:$dstuser, app:$app,
vsys:$vsys, from:$from, to:$to,
inbound_if:$inbound_if,
outbound_if:$outbound_if, logset:$logset,
time_received:$time_received,
sessionid:$sessionid, repeatcnt:$repeatcnt,
sport:$sport, dport:$dport, natport:$natport,
natdport:$natdport, flags:$flags, proto:$proto,
action:$action, misc:$misc, threatid:$threatid,
category:$category, severity:$severity,
direction:$direction, seqno:$seqno,
actionflags:$actionflags, srcip:$srcip
```

Send Test Log

OK

Cancel

HTTP Server Profile



Name

Tag Registration

The server(s) should have User-ID agent running in order for tag registration to work

Servers

1 item → ×

<input type="checkbox"/>	NAME	ADDRESS	PROTOC...	PORT	TLS VERSION	CERTIFIC... PROFILE	HTTP METHOD	USERNA...	PASSWO...
<input checked="" type="checkbox"/>	UIDagent	192.168...	HTTPS	443	1.2	None	GET	httpuser	*****
			HTTP		1.2				
			HTTPS		1.1				
					1.0				

+ Add - Delete Test Server Connection

OK

Cancel

Ethernet Interface



Interface Name

Comment

Interface Type

Netflow Profile

Config | IPv4 | IPv6 | SD-WAN | Advanced

Assign Interface To

Virtual Router

Security Zone

OK

Cancel

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK

- SSH Service Profile
- Response Pages
- Log Settings**
- Server Profiles
 - SNMP Trap
 - Syslog
 - Email
 - HTTP
 - Netflow
 - RADIUS
 - TACACS+
 - LDAP
 - Kerberos
 - SAML Identity Provider
 - Multi Factor Authentication
- Local User Database
 - Users
 - User Groups
- Scheduled Log Export
- Software
- GlobalProtect Client
- Dynamic Updates
- Plugins
- VM-Series
- Licenses
- Support
- Master Key and Diagnostics
- Policy Recommendation

System

<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA
<input type="checkbox"/>	all system logs		All Logs	<input checked="" type="checkbox"/>

+ Add - Delete Clone PDF/CSV

Configuration

<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA
<input type="checkbox"/>	all configuration		All Logs	<input checked="" type="checkbox"/>

+ Add - Delete Clone PDF/CSV

User-ID

<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP
<input type="checkbox"/>	all user-ID		All Logs	<input checked="" type="checkbox"/>	

+ Add - Delete Clone PDF/CSV

HIP Match

<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA	SNMP TRAP
--------------------------	------	-------------	--------	----------	-----------

+ Add - Delete Clone PDF/CSV

GlobalProtect

<input type="checkbox"/>	NAME	DESCRIPTION	FILTER	PANORAMA
--------------------------	------	-------------	--------	----------

+ Add - Delete Clone PDF/CSV

reaper | Logout | Last Login Time: 12/04/2020 21:15:28 | Session Expire Time: 01/04/2020 21:25:58

Log Settings - System ?

Name:

Filter:

Description:

Forward Method

Panorama

<input type="checkbox"/> SNMP ^ <input checked="" type="checkbox"/> SNMPv3 <input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> EMAIL ^ <input checked="" type="checkbox"/> email <input type="checkbox"/> Add <input type="checkbox"/> Delete
<input type="checkbox"/> SYSLOG ^ <input checked="" type="checkbox"/> syslog <input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> HTTP ^ <input type="checkbox"/> Add <input type="checkbox"/> Delete

Log Settings - System

Name:

Filter:

Description: All Logs
 (severity eq critical)
 (severity eq high)
 (severity eq informational)
 (severity eq low)
 (severity eq medium)

Forward Method: SNMP Filter Builder

Create Filter

Create Filter | View Filtered Logs

Connector	Attribute	Operator	Value
and	Description	equal	informational
or	Event	not equal	low
	Object	greater than or equal	medium
	Receive Time	less than or equal	high
	Severity		critical
	Time Generated		
	Type		

Negate + Add

OK Cancel

Log Forwarding Profile

Name:

Description:

3 items → ×

<input type="checkbox"/>	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
<input type="checkbox"/>	all traffic to panorama	traffic	All Logs	• Panorama	
<input type="checkbox"/>	all threat to panorama	threat	All Logs	• Panorama	
<input type="checkbox"/>	all url to panorama	url	All Logs	• Panorama	

+ Add - Delete 🔄 Clone

OK Cancel

Log Forwarding Profile Match List



Name alert to security

Description

Log Type threat

Filter (severity eq critical)

Forward Method

Panorama

<input type="checkbox"/> SNMP ^	<input type="checkbox"/> EMAIL ^
	<input type="checkbox"/> email
<input type="checkbox"/> SYSLOG ^	<input type="checkbox"/> HTTP ^
<input type="checkbox"/> syslog	
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete

Built-in Actions

Quarantine

<input type="checkbox"/> NAME	TYPE
<input type="checkbox"/> Add <input type="checkbox"/> Delete	

OK

Cancel

Security Policy Rule



General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	any	quarantine
<input type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> SOURCE ADDRESS ^	<input type="checkbox"/> SOURCE USER ^	<input type="checkbox"/> SOURCE DEVICE ^
<input type="checkbox"/> GP			
<input type="checkbox"/> trust			
<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete	<input type="checkbox"/> Add <input type="checkbox"/> Delete

Negate

OK

Cancel

Action ?

Name: tagging 🔖

Tagging

Target: Source Address 👉

Action: Destination Address

Registration: Source Address

Timeout (min): User

Tags: X-Forwarded-For Address

Action ?

Name: tagging 🔖

Tagging

Target: Source Address ▼

Action: Add Tag Remove Tag

Registration: Local User-ID 👉

Timeout (min): Local User-ID

Tags: Panorama User-ID
Remote User-ID

Action ?

Name: tagging 🔖

Tagging

Target: Source Address ▼

Action: Add Tag Remove Tag

Registration: Local User-ID ▼

Timeout (min): 240

Tags: Blocked × ▼

OK Cancel

OK Cancel

Dynamic User Group ?

Name: dynamic users 🔖

Description:

Match: 'Blocked'

+ Add Match Criteria

Tags: Blocked × ▼

OK Cancel

Address Group ? 📄

Name: blocked addresses 🔖

Description:

Type: Dynamic ▼

Match: 'Blocked'

+ Add Match Criteria

Tags: Blocked × ▼

OK Cancel

Logs

- Traffic
- Threat
- URL Filtering
- WildFire Submissions
- Data Filtering
- HIP Match
- GlobalProtect
- IP-Tag**
- User-ID
- Decryption
- Tunnel Inspection
- Configuration

	RECEIVE TIME	VIRTUAL SYSTEM	IP-ADDRESS	IP SUBNET/RANGE	TAG	EVENT	TIMEOUT	SOURCE NAME	SOURCE TYPE
	12/16 22:06:00	vsys1	05.58		Blocking	register	0	XMLAPI	xml-api
	12/16 22:03:46	vsys1	35.35		Blocking	register	0	XMLAPI	xml-api
	12/16 21:58:42	vsys1	3.150		Blocking	register	0	XMLAPI	xml-api
	12/16 21:55:52	vsys1	66.248		Blocking	register	0	XMLAPI	xml-api
	12/16 21:45:16	vsys1	68.222		Blocking	register	0	XMLAPI	xml-api
	12/16 21:39:01	vsys1	67.5		Blocking	register	0	XMLAPI	xml-api
	12/16 21:30:04	vsys1	7.234		Blocking	register	0	XMLAPI	xml-api

PANgurus | DASHBOARD | ACC | MONITOR | POLICIES | **OBJECTS** | NETWORK | DEVICE | Commit

1 item

NAME	LOCATION	MEMBERS COUNT	ADDRESSES	TAGS
<input checked="" type="checkbox"/> Dynamic Blocking		dynamic	more...	

Click for details: Dynamic Blocking

Address Groups - Dynamic Blocking

527 items

ADDRESS	TYPE	ACTION
183	registered-ip	Unregister Tags
.246	registered-ip	Unregister Tags
.158	registered-ip	Unregister Tags
.65	registered-ip	Unregister Tags
.118	registered-ip	Unregister Tags
.173	registered-ip	Unregister Tags
5.108	registered-ip	Unregister Tags
15	registered-ip	Unregister Tags
?	registered-ip	Unregister Tags
3.112	registered-ip	Unregister Tags
2.254	registered-ip	Unregister Tags
2.185	registered-ip	Unregister Tags
8.208	registered-ip	Unregister Tags
2.222	registered-ip	Unregister Tags
1.127	registered-ip	Unregister Tags

Page 1 of 3 | Displaying 1 - 200 / 527

Tasks | Language | paloalto

Close

Security Policy Rule



General | Source | Destination | Application | Service/URL Category | **Actions** | Usage

Action Setting

Action: Allow

Send ICMP Unreachable

Log Setting

Log at Session Start

Log at Session End

Log Forwarding: default

Profile Setting

Profile Type: Group

Group Profile: default

Other Settings

Schedule: None

QoS Marking: None

Disable Server Response Inspection

OK
Cancel

PANORAMA

DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICES

Panorama Device Group All

Logs

- Traffic**
- Threat
- URL Filtering
- WildFire Submissions
- Data Filtering
- HIP Match
- GlobalProtect
- IP-Tag
- User-ID
- Decryption
- Tunnel Inspection
- Configuration
- System
- Authentication
- Unified

	GENERATE TIME	START TIME	RECEIVE TIME	TYPE	FROM ZONE	TO ZONE
	12/18 13:38:13	2020/12/18 13:38:08	2020/12/18 21:26:59	end	outside	LAN
	12/18 13:38:13	2020/12/18 13:38:08	2020/12/18 21:26:59	end	outside	LAN
	12/18 13:38:06	2020/12/18 13:37:51	2020/12/18 21:26:59	end	LAN	outside
	12/18 13:38:05	2020/12/18 13:37:49	2020/12/18 21:26:59	end	LAN	outside
	12/18 13:38:03	2020/12/18 13:37:51	2020/12/18 21:26:59	end	LAN	outside
	12/18 13:38:02	2020/12/18 13:37:46	2020/12/18 21:26:59	end	LAN	outside
	12/18 13:38:01	2020/12/18 13:37:56	2020/12/18 21:26:52	drop	prisma	untrust


```
top - 01:35:49 up 1 day, 22:20, 1 user, load average: 2.30, 2.62, 2.74
Tasks: 146 total, 4 running, 141 sleeping, 0 stopped, 1 zombie
%Cpu0  :  6.3 us,  5.9 sy,  6.6 ni, 81.2 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
%Cpu1  :100.0 us,  0.0 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
%Cpu2  :100.0 us,  0.0 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
%Cpu3  :  8.9 us,  4.0 sy,  3.0 ni, 82.8 id,  0.0 wa,  0.0 hi,  1.3 si,  0.0 st
KiB Mem : 4119684 total, 374860 free, 1890600 used, 1854224 buff/cache
KiB Swap: 4097968 total, 4087960 free, 10008 used. 1687028 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
4959	root	20	0	91288	37828	9968	R	100.0	0.9	2772:43	pan_task
4961	root	20	0	66608	12856	9776	R	99.7	0.3	2773:05	pan_task
3096	root	0	-20	202292	38024	6672	S	5.9	0.9	17:35.09	masterd_apps
3116	root	15	-5	121516	9704	3808	S	5.9	0.2	36:01.46	sysd
5404	root	20	0	528236	59904	7608	S	0.7	1.5	20:33.87	dnsproxyd
3285	root	20	0	1022616	12800	5684	S	0.3	0.3	1:25.75	sysdagent
3290	root	30	10	198380	18704	6356	S	0.3	0.5	15:47.09	python
3591	nobody	20	0	44244	5364	1344	S	0.3	0.1	7:28.24	redis-server
3596	nobody	20	0	41684	2032	1172	S	0.3	0.0	7:19.29	redis-server
4943	root	20	0	71380	10000	7196	S	0.3	0.2	1:53.10	sdwand
4945	root	20	0	58160	9416	6756	S	0.3	0.2	7:17.89	pan_dha
5383	root	20	0	130836	26568	3308	S	0.3	0.6	19:15.40	identityclient
8155	reaper	20	0	4228	1636	1128	R	0.3	0.0	0:00.13	top

```
reaper@PANgurus> request log-collector-forwarding status

Log Collector Preference List
Forward to all: No
Serial Number: 0007 IP Address: 192.168.27.10 IPV6 Address: unknown

-----
Type           Last Log Created      Last Log Fwded      Last Seq Num Fwded  Last Seq Num Acked  Total Logs Fwded
-----
> CMS 0
    Not Sending to CMS 0
> CMS 1
    Not Sending to CMS 1

>Log Collector
'Log Collection log forwarding agent' is active and connected to 192.168.27.10

DNS :
    Successfully resolved FQDN (), IP (192.168.27.10)
    success
    2020/12/21 00:36:42

Registration :
    registration request sent
    success
    2020/12/21 00:36:45

SSL :
    ssl channel established to (192.168.27.10)
    success
    2020/12/21 00:36:44

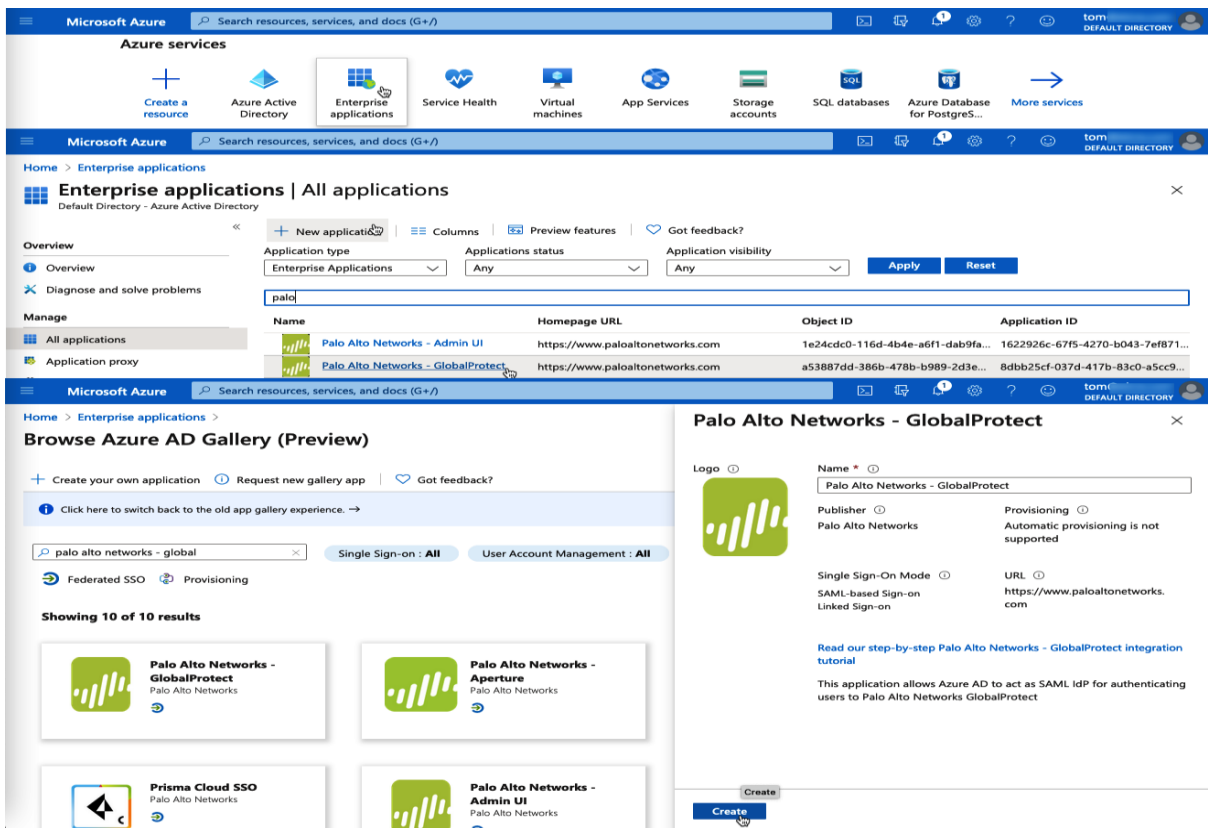
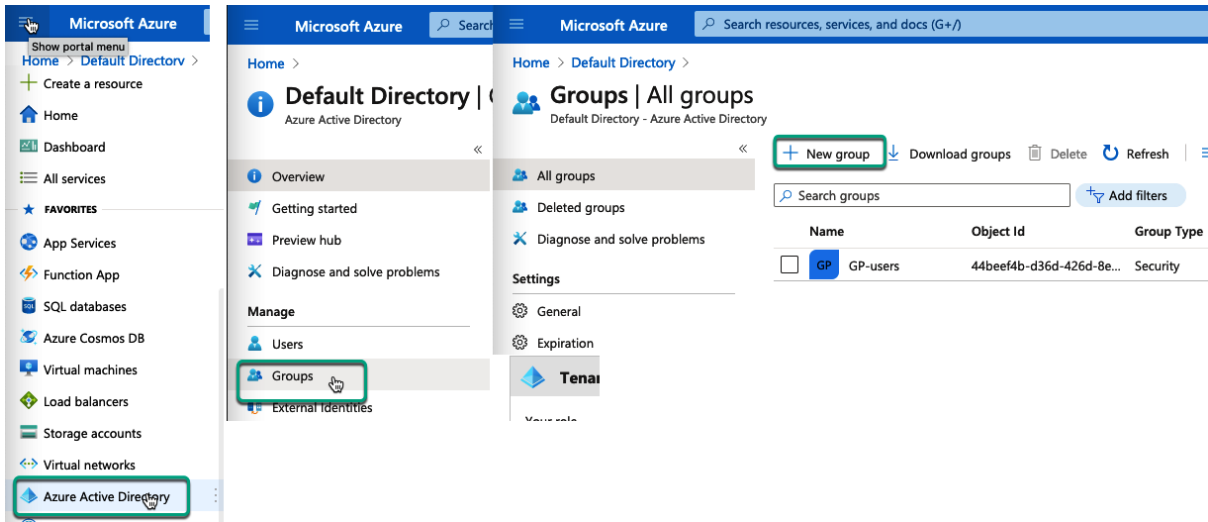
Status :
    Connection successful
    success
    2020/12/21 00:36:45

TCP :
    tcp connection established
    success
    2020/12/21 00:36:42

Connect-Agent-Status :
    DNS resolution success for (IP: 192.168.27.10)
    success
    2020/12/21 00:36:32

config 2020/12/21 00:17:41 2020/12/21 00:37:55 3241 3241 4
system 2020/12/21 22:10:53 2020/12/21 22:11:11 24693947 24693947 13383
threat 2020/12/21 22:11:47 2020/12/21 22:11:52 7335620 7335606 293082
traffic 2020/12/21 22:11:47 2020/12/21 22:11:52 83644996 83644987 499747
```

Chapter 2: Configuring Advanced GlobalProtect Features



Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications > Palo Alto Networks - GlobalProtect

Palo Alto Networks - GlobalProtect | Users and groups

Enterprise Application

Overview
Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups**
- Single sign-on

« + Add user/group Edit Remove Update Credentials

i The application will appear on the Access Panel for assigned users. Set 'visible to

First 100 shown, to search all users & groups, enter a display name.

Display Name	Object Type
<input type="checkbox"/> TP tom piens	User

Microsoft Azure Search resources, services, and docs (G+)

Home > Enterprise applications > Palo Alto Networks - GlobalProtect

Palo Alto Networks - GlobalProtect | Single sign-on

Enterprise Application

« Select a single sign-on method [Help me decide](#)

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on**
- Provisioning

Disabled

Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Palo Alto Networks - GlobalProtect | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators (Preview)
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Self-service
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-ins
 - Usage & insights (Preview)
 - Audit logs
 - Provisioning logs (Preview)
 - Access reviews

Upload metadata file Change single sign-on mode Test this application Got feedback?
Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Palo Alto Networks - GlobalProtect.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	https://gp.pangurus.com:443/SAML20/SP
Reply URL (Assertion Consumer Service URL)	https://gp.pangurus.com/SAML20/SP/ACS
Sign on URL	https://gp.pangurus.com
Relay State	Optional
Logout Url	Optional

2 User Attributes & Claims [Edit](#)

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
username	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Signing Certificate [Edit](#)

Status	Active
Thumbprint	9FAD2FC8FC99487DA1BA2679D7D317A709B6544A
Expiration	1/4/2024, 1:17:49 AM
Notification Email	tom@elcre.com
App Federation Metadata Url	https://login.microsoftonline.com/dce79451-5259-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

3 SAML Signing Certificate [Edit](#)

Status	Active
Thumbprint	9FAD2FC8FC99487DA1BA2679D7D317A709B6544A
Expiration	1/4/2024, 1:17:49 AM
Notification Email	tom@elcre.com
App Federation Metadata Url	https://login.microsoftonline.com/dce79451-5259-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Palo Alto Networks - GlobalProtect

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/dce79451-5259-...
Azure AD Identifier	https://sts.windows.net/dce79451-5259-4e34-926-...
Logout URL	https://login.microsoftonline.com/common/wsfed-...

[View step-by-step instructions](#)

SAML Identity Provider Server Profile Import



Profile Name

Administrator Use Only

Identity Provider Configuration

Identity Provider Metadata [Browse...](#)

Validate Identity Provider Certificate

Validate Metadata Signature

Maximum Clock Skew (sec)

OK

Cancel

SAML Identity Provider Server Profile



Profile Name

Administrator Use Only

Identity Provider Configuration

Identity Provider ID

Identity Provider Certificate

Select the certificate that IDP uses to sign SAML messages

Identity Provider SSO URL

Identity Provider SLO URL

SAML HTTP Binding for SSO Requests to IDP Post Redirect

SAML HTTP Binding for SLO Requests to IDP Post Redirect

Validate Identity Provider Certificate

Sign SAML Message to IDP

Maximum Clock Skew (seconds)

OK

Cancel

Authentication Profile ?

Name 📄

Authentication | Factors | **Advanced**

Type

IdP Server Profile

Certificate for Signing Requests Select the certificate to sign SAML messages to IDP

Enable Single Logout

Certificate Profile

User Attributes in SAML Messages from IDP

Username Attribute

User Group Attribute

Admin Role Attribute

Access Domain Attribute

Home > Enterprise applications > Palo Alto Networks - GlobalProtect >

Palo Alto Networks - GlobalProtect | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage**
- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

User Attributes & Claims ✎ Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
username	user.userprincipalname
Unique User Identifier	user.userprincipalname

Authentication Profile ?

Name 📄

Authentication | Factors | **Advanced**

Allow List

<input type="checkbox"/>	ALLOW LIST ^
<input type="checkbox"/>	all

GlobalProtect Portal Configuration

General

Authentication

Portal Data Collection

Agent

Clientless VPN

Satellite

Server Authentication: SSL/TLS Service Profile: **gp**

Client Authentication

<input type="checkbox"/>	NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICA...
<input checked="" type="checkbox"/>	SAML	Browser	SAML SSO	<input type="checkbox"/>	Username	Password	Enter login credentials	No
<input type="checkbox"/>	Idap	Any	pangurus	<input type="checkbox"/>	Username	Password	Enter login credentials	No

Client Authentication

Name: SAML

OS: **Browser**

Authentication Profile: **Browser**

GlobalProtect App Login Screen: Chrome

Username Label: iOS

Password Label: IoT

Authentication Message: Mac

Allow Authentication with User Credentials OR Client Certificate:

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

OK Cancel

GlobalProtect Portal

Sign in to your account

https://gp.pangurus.com/global-protect/login.esp

https://login.microsoftonline.com/dce79451-5259

paloalto NETWORKS

GlobalProtect Portal

Username

Password

LOG IN

Microsoft

Sign in

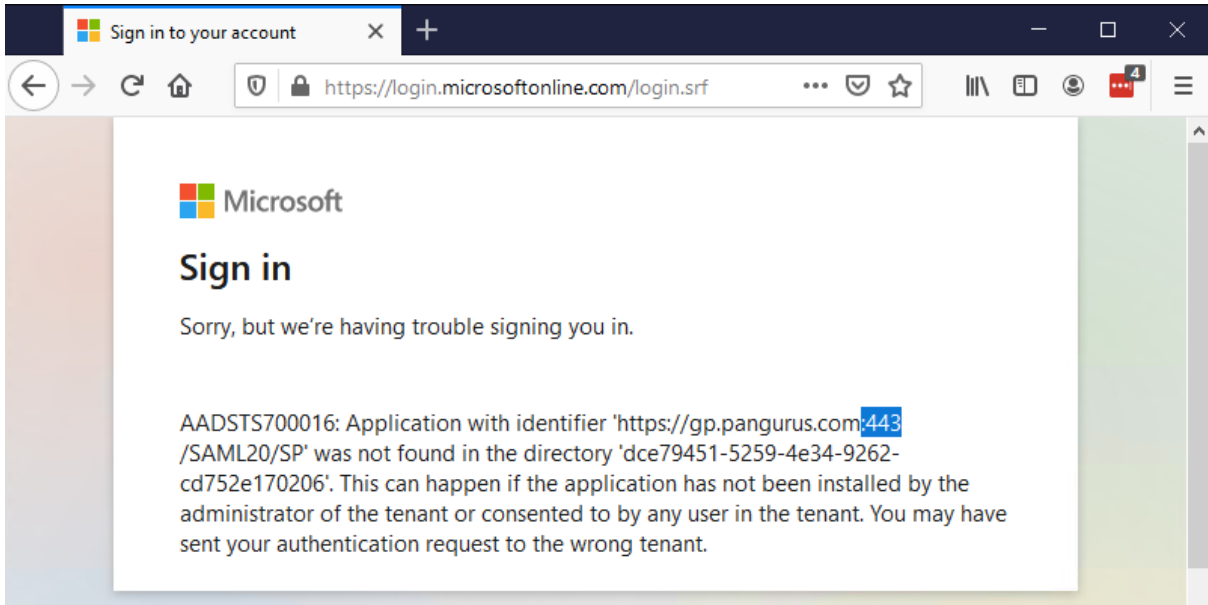
reaper@pangurus.com

Can't access your account?

Sign-in options

Next

Terms of use Privacy & cookies



GlobalProtect Gateway Configuration ?

General

Authentication

Agent

Satellite

Server Authentication

SSL/TLS Service Profile:

Client Authentication

<input type="checkbox"/>	NAME	OS	AUTHENTICAT... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC... MESSAGE	ALLOW AUTHENTIC... WITH USER CREDENTIALS OR CLIENT CERTIFICATE
<input checked="" type="checkbox"/>	SAML	Any	SAML SSO	<input type="checkbox"/>	Username	Password	Enter login credentials	No

Certificate Profile:

Block login for quarantined devices

Configs



Authentication | Config Selection Criteria | Internal | External | **App** | HIP Data Collection

App Configurations

Connect Method	Pre-logout (Always On) ▼
GlobalProtect App Config Refresh Interval (hours)	User-logout (Always On)
Allow User to Disable GlobalProtect App	Pre-logout (Always On)
Allow User to Uninstall GlobalProtect App (Windows Only)	On-demand (Manual user initi...)
Allow User to Upgrade GlobalProtect App	Pre-logout then On-demand
Allow User to Sign Out from GlobalProtect App	Allow with Prompt
Use Single Sign-on (Windows)	Yes
Use Single Sign-on (macOS)	No
Clear Single Sign-On Credentials on Logout (Windows Only)	Yes

Welcome Page None ▼

Disable GlobalProtect App

Passcode

Confirm Passcode

Max Times User Can Disable

Disable Timeout (min)

Uninstall GlobalProtect App

Uninstall Password

Confirm Uninstall Password

Mobile Security Manager Settings

Mobile Security Manager

Enrollment Port

OK

Cancel

GlobalProtect Portal Configuration



General

Authentication

Portal Data Collection

Agent

Clients

Satellite

Configs



Authentication | Config Selection Criteria | Internal | External | **App** | HIP Data Collection

Name

Client Certificate None ▼

The selected client certificate including its private key will be installed on client machines.

Save User Credentials Yes ▼

Authentication Override

Generate cookie for authentication override

Accept cookie for authentication override

Cookie Lifetime Days

Certificate to Encrypt/Decrypt Cookie gp-pangurus-cert ▼

GlobalProtect Gateway Configuration



General

Authentication

Agent

Satellite

Tunnel Settings | **Client Settings** | Client IP Pool | Network Services | Connection Settings | Video Traffic | HIP Notification

1 item → ×

CONFIGS	USERS	OS	Source Address			INCLUDE ACCESS ROUTE
			REGION	IP ADDRESS	IP POOL	
<input type="checkbox"/>	clientsettings	any	any		192.168.27.53-192.168.27.60	192.168.27.0/24

Configs



Config Selection Criteria | **Authentication Override** | IP Pools | Split Tunnel | Network Services

Generate cookie for authentication override

Accept cookie for authentication override

Cookie Lifetime Hours

Certificate to Encrypt/Decrypt Cookie gp-pangurus-cert ▼

OK

Cancel

GlobalProtect Gateway Configuration ?

General | Tunnel Settings | **Client Settings** | Client IP Pool | Network Services | Connection Settings | Video Traffic | HIP Notification

Authentication

Agent

Satellite

2 items → ×

	CONFIGS	USERS	OS	Source Address		INCLUDE ACCESS ROUTE
				REGION	IP ADDRESS	
<input checked="" type="checkbox"/>	prelogon client	pre-logon	any			192.168.27.53-19... 192.168.27.0/24
<input type="checkbox"/>	client	any	any			192.168.27.50-19... 192.168.27.0/24

Configs ?

Config Selection Criteria | Authentication Override | IP Pools | Split Tunnel | Network Services

Name: prelogon client

Config Selection Criteria

pre-logon	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE USER ^	<input type="checkbox"/> OS ^

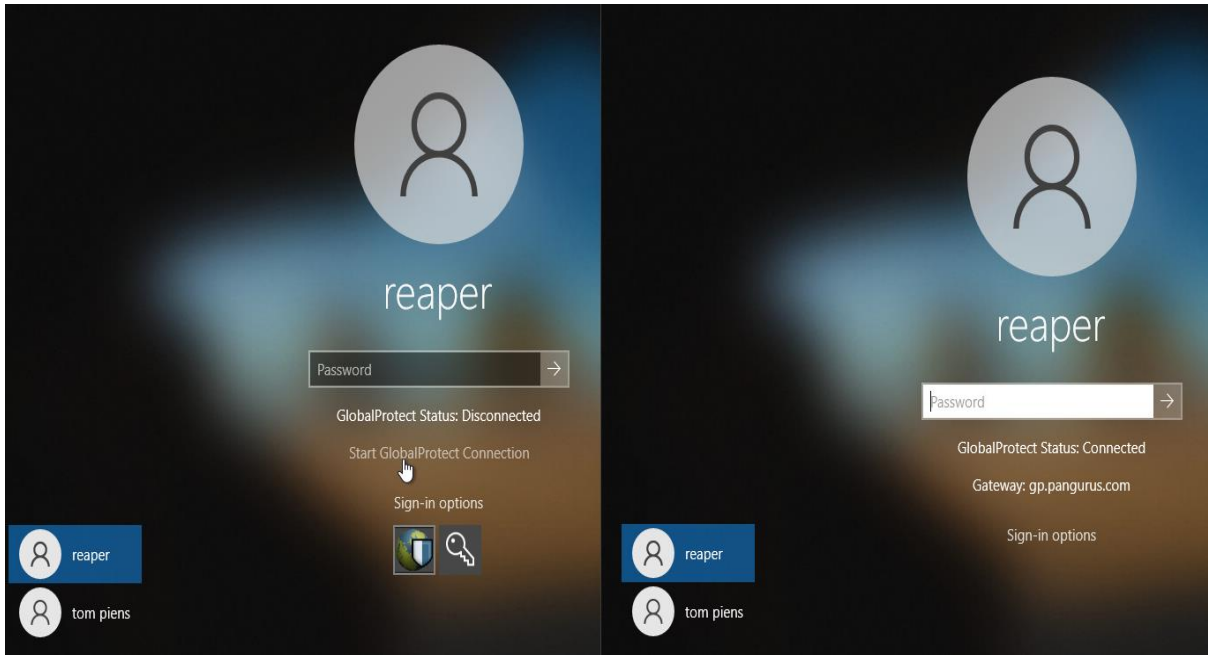
+ Add - Delete

Registry Editor - □ ×

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup

Name	Type	Data
(Default)	REG_SZ	(value not set)
Installfolder	REG_SZ	C:\Program Files\Palo Alto Networks\GlobalProtect
Portal	REG_SZ	gp.pangurus.com
Prelogon	REG_SZ	1
ProductCode	REG_SZ	{717E7B2D-F4DF-4707-8024-E346F2E64F4F}
Version	REG_SZ	1.0.0.1
use-sso	REG_SZ	yes
ShowPreLogonButton	REG_SZ	yes



PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** Commit ?

Device Certificates | Default Trusted Certificate Authorities

Search: pki 1/9

<input type="checkbox"/>	NAME	EXPIRES	SUBJECT	ISSUER	CA	K...	USAGE
<input type="checkbox"/>	▼ pangurusPKI-rootCA	Nov 30 22:30:36 2030...	DC = com, DC = pangurus, C...	DC = com, DC = pa...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted Root CA Certif...
<input type="checkbox"/>	PKI-OCSP	Jan 25 23:00:35 2021 ...	CN = HIVE.pangurus.com	DC = com, DC = pa...	<input type="checkbox"/>	<input type="checkbox"/>	

Certificate information ?

Name: pangurusPKI-rootCA

Subject: /DC=com/DC=pangurus/CN=pangurus-HIVE-CA

Issuer: /DC=com/DC=pangurus/CN=pangurus-HIVE-CA

Not Valid Before: Nov 30 22:20:37 2020 GMT

Not Valid After: Nov 30 22:30:36 2030 GMT

Algorithm: RSA

Certificate Authority

Forward Trust Certificate

Forward Untrust Certificate

Trusted Root CA

Revoke
OK
Cancel

Delete Revoke Renew Import Generate Export Certificate Import HA Key Export HA Key PDF/CSV

Generate Certificate



Certificate Type Local SCEP

Certificate Name

Common Name

IP or FQDN to appear on the certificate

Signed By

Certificate Authority

Block Private Key Export

OCSP Responder

Cryptographic Settings

Algorithm

Number of Bits

Digest

Expiration (days)

Certificate Attributes

<input type="checkbox"/>	TYPE	VALUE
<input type="checkbox"/>	Country = "C" from "Subject" field	BE
<input type="checkbox"/>	Host Name = "DNS" from Subject Alternative Name (SAN) field	selfsigned.pangurus.com

Generate

Cancel

Certificate Profile



Name

Username Field

User Domain

CA Certificates

<input type="checkbox"/>	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
<input type="checkbox"/>	pangurusPKI-rootCA	http://hive.pangurus.com/ocsp	PKI-OCSP	

Default OCSP URL (must start with http:// or https://)

Use CRL

CRL Receive Timeout (sec)

Use OCSP

OCSP Receive Timeout (sec)

OCSP takes precedence over CRL

Certificate Status Timeout (sec)

Block session if certificate status is unknown

Block session if certificate status cannot be retrieved within timeout

Block session if the certificate was not issued to the authenticating device

Block sessions with expired certificates

OK

Cancel

GlobalProtect Gateway Configuration



General

Authentication

Agent

Satellite

Server Authentication

SSL/TLS Service Profile

Client Authentication

<input type="checkbox"/>	NAME	OS	AUTHENTICAT... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC... MESSAGE	ALLOW AUTHENTIC... WITH USER CREDENTIALS OR CLIENT CERTIFICATE
<input type="checkbox"/>	auth	Any	pangurus	<input type="checkbox"/>	Username	Password	Enter login credentials	No

+ Add - Delete ↺ Clone ↑ Move Up ↓ Move Down

Certificate Profile

Block login for quarantined devices

OK Cancel

GlobalProtect Gateway Configuration



General

Authentication

Agent

Satellite

Tunnel Settings | **Client Settings** | Client IP Pool | Network Services | Connection Settings | Video Traffic | HIP Notification

2 items → ×

<input type="checkbox"/>	CONFIGS	USERS	OS	Source Address		IP POOL	INCLUDE ACCESS ROUTE
				REGION	IP ADDRESS		
<input type="checkbox"/>	prelogon client	pre-logon	any			192.168.27.53-192.168.27.55	192.168.27.0/24
<input type="checkbox"/>	regular users	any	any			192.168.27.50-192.168.27.52	192.168.27.0/24

Configs



Config Selection Criteria | Authentication Override | IP Pools | Split Tunnel | Network Services

Name

Config Selection Criteria

+ Add

<input type="text" value="pre-logon"/>	<input checked="" type="checkbox"/> Any
any	<input type="checkbox"/> OS ^
pre-logon	
select	

+ Add - Delete

GlobalProtect Portal Configuration ?

- General
- Authentication**
- Portal Data Collection
- Agent
- Clientless VPN
- Satellite

Server Authentication

SSL/TLS Service Profile:

Client Authentication

<input type="checkbox"/>	NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICA...
<input type="checkbox"/>	ldap	Any	pangurus	<input type="checkbox"/>	Username	Password	Enter login credentials	No

Certificate Profile:

GlobalProtect Portal Configuration ?

- General
- Authentication
- Portal Data Collection
- Agent**
- Clientless VPN
- Satellite

Agent

<input type="checkbox"/>	CONFIGS	USER/USER GROUP	OS	EXTERNAL GATEWAYS	CLIENT CERTIFICATE
<input type="checkbox"/>	prelogon agent	pre-logon	any	prelogon.pangurus.com	
<input type="checkbox"/>	agent	any	any	gp.pangurus.com	

Configs ?

App Configurations

Connect Method	<input type="text" value="Pre-logon (Always On)"/>
GlobalProtect App Config Refresh Interval (hours)	<input type="text" value="User-logon (Always On)"/> <input type="text" value="Pre-logon (Always On)"/>
Allow User to Disable GlobalProtect App	<input type="text" value="On-demand (Manual user initi...)"/> <input type="text" value="Pre-logon then On-demand"/>
Allow User to Uninstall GlobalProtect App (Windows Only)	
Allow User to Upgrade GlobalProtect App	<input type="text" value="Allow with Prompt"/>

Welcome Page:

Disable GlobalProtect App

Passcode:
 Confirm Passcode:
 Max Times User Can Disable:
 Disable Timeout (min):

Uninstall GlobalProtect App

Generate Certificate

Certificate Type Local SCEP

Certificate Name

Common Name
IP or FQDN to appear on the certificate

Signed By
 Certificate Authority
 Block Private Key Export

OCSP Responder

Cryptographic Settings

Algorithm
Number of Bits
Digest
Expiration (days)

Certificate Attributes

<input type="checkbox"/>	TYPE	VALUE

Generate Certificate

Certificate Type Local SCEP

Certificate Name

Common Name
IP or FQDN to appear on the certificate

Signed By
 Certificate Authority
 Block Private Key Export

OCSP Responder

Cryptographic Settings

Algorithm
Number of Bits
Digest
Expiration (days)

Certificate Attributes

<input type="checkbox"/>	TYPE	VALUE

Microsoft Active Directory Certificate Services -- pangurus-HIVE-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:
[Request a certificate](#)
[View the status of a pending certificate request](#)
[Download a CA certificate, certificate chain, or CRL](#)

Microsoft Active Directory Certificate Services -- pangurus-HIVE-CA Home

Request a Certificate

Select the certificate type:
[User Certificate](#)

Or, submit an [advanced certificate request](#).

Microsoft Active Directory Certificate Services -- pangurus-HIVE-CA Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
aIyO3/nzFbGwu1HFQjXTRMkd5CMigXTff/Gg/6mg
27J12XQRKF5gX409SgLo0SUmFw4u7x4EIfA0i6G
mytr57dW0/n5oh6luVh2RG8Q82wLoVjBIip4iP
/vKzsZyJHr53ZVlKDMzygOutJ/hNc0BjfgrofW==
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Additional Attributes:

Attributes:

Microsoft Active Directory Certificate Services -- pangurus-HIVE-CA Home

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** Commit

Device Certificates | Default Trusted Certificate Authority

Import Certificate

Certificate Type: Local SCEP

Certificate Name: Pre-logout-MachineCet

Certificate File: C:\fakepath\certnewplmc.cer Browse...

File Format: Base64 Encoded Certificate (PEM)

Private key resides on Hardware Security Module
 Import Private Key
 Block Private Key Export

Key File: Browse...

Passphrase:

Confirm Passphrase:

OK Cancel 1 / 12

NAME	EXPIRE	ISSUER	VALIDITY	CA	KEY	USAGE
▼ pangurusPKI-rootCA	Nov 30 22:30:36 2030 GMT	DC = com, DC = pangurus, CN = pangurus...	DC = com, DC = pangurus, C...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted Root CA Certificate
PKI-OCSP	Jan 25 23:00:35 2021 GMT	CN = HIVE.pangurus.com	DC = com, DC = pangurus, C...	<input type="checkbox"/>	<input type="checkbox"/>	
prelogin	Jan 12 22:25:05 2022 GMT	DC = com, DC = pangurus, CN = Users, C...	DC = com, DC = pangurus, C...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Pre-logout-MachineCet	Jan 13 23:16:14 2022 GMT	DC = com, DC = pangurus, CN = Users, C...	DC = com, DC = pangurus, C...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Delete Revoke Renew Import Generate Export Certificate Import HA Key Export HA Key PDF/CSV

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** Commit

Device Certificates | Default Trusted Certificate Authority

Export Certificate - Pre-logout-MachineCet

File Format: Encrypted Private Key and Certificate (PKCS12)

Passphrase:

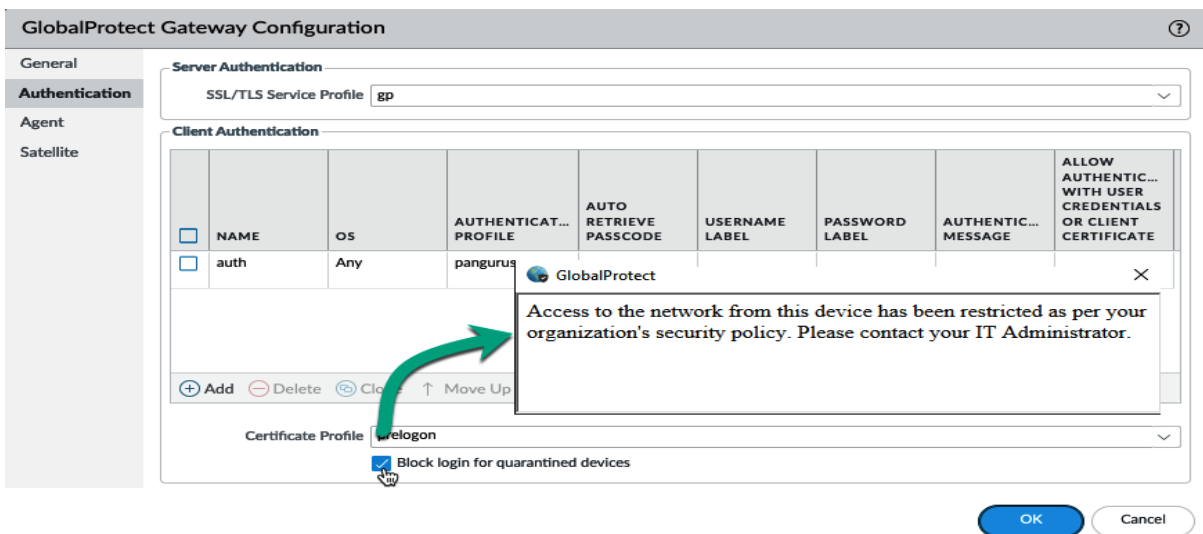
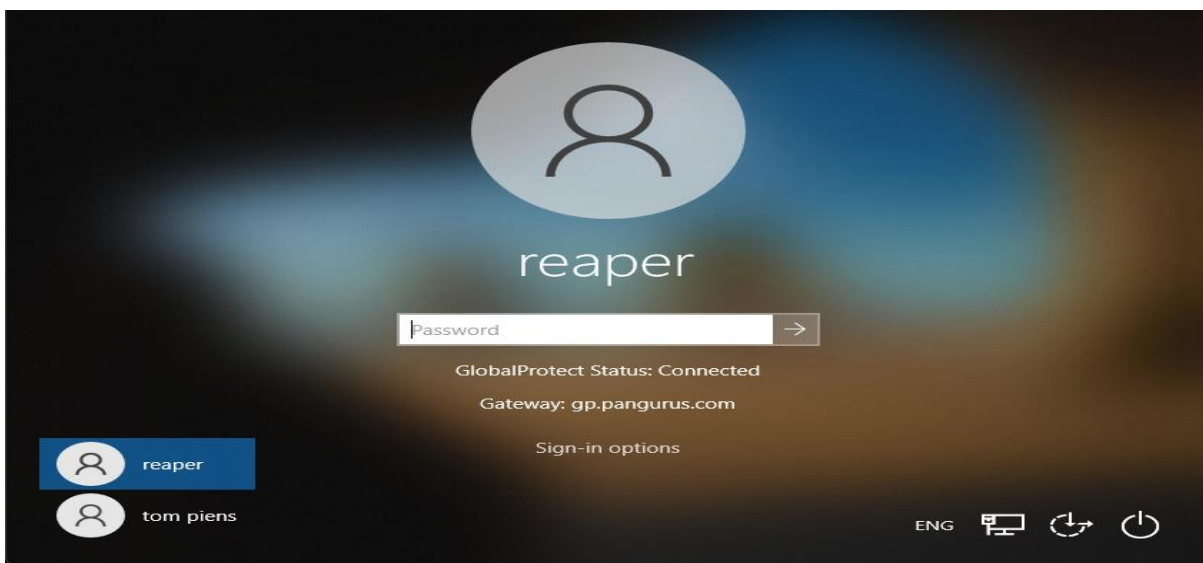
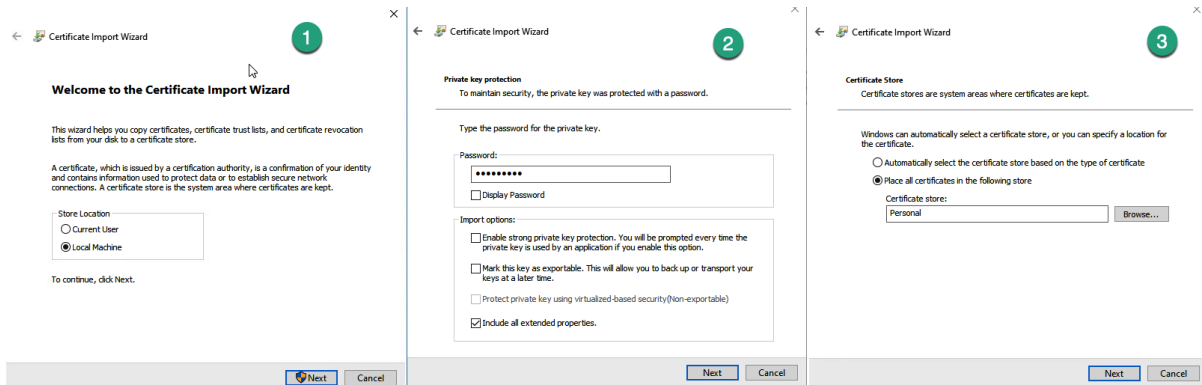
Confirm Passphrase:

OK Cancel 12 items

NAME	EXPIRE	ISSUER	VALIDITY	CA	KEY	USAGE
▼ pangurusPKI-rootCA	Nov 30	C = pangurus, C...	C = pangurus, C...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Trusted Root CA Certificate
PKI-OCSP	Jan 25	C = pangurus, C...	C = pangurus, C...	<input type="checkbox"/>	<input type="checkbox"/>	
prelogin	Jan 12	C = pangurus, C...	C = pangurus, C...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Pre-logout-MachineCet	Jan 13 23:16:14 2022 GMT	DC = com, DC = pangurus, CN = Users, C...	DC = com, DC = pangurus, C...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Delete Revoke Renew Import Generate Export Certificate Import HA Key Export HA Key PDF/CSV

reaper | Logout | Last Login Time: 01/13/2021 22:13:19 | Session Expire Time: 02/12/2021 22:14:57 Tasks Language **palco**



NAME	Source			Destination		APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS	HIT COUNT
	ZONE	USER	DEVICE	ZONE	ADDRESS						
25	vpn in Quarantine	any	quarantine	any		dns ssl web-bro...	application-default	Allow	URL Filtering Profile: Quarantine		-
26	vpn in Quarantine drop	any	quarantine	any			application-default	Drop			-
27	vpn in prelogon	pre-logon	any	ActiveDirectory		Domain...	application-default	Allow			-
28	vpn in	pangurus/pangurus pangurus/vpn users reaper	any	192.168.27.0/24		dns ms-ds-s... ms-rdp splunk ssh ssl vnc more...	application-default	Allow	Log Forwarding Profile setting: Quarantine		36657

URL Filtering Profile

Name Quarantine

Description

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

74 items → ×

<input type="checkbox"/>	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Pre-defined Categories			
<input type="checkbox"/>	abortion	override	allow
<input type="checkbox"/>	abused-drugs	override	allow
<input type="checkbox"/>	adult	override	allow
<input type="checkbox"/>	alcohol-and-tobacco	override	allow
<input type="checkbox"/>	auctions	override	allow
<input type="checkbox"/>	business-and-economy	override	allow

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

OK

Cancel

Log Forwarding Profile

Name Quarantine

Description

1 item → ×

<input type="checkbox"/>	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS ^
<input type="checkbox"/>	quarantine user	threat	(severity geq high)	Email • SecTeam-email	• quarantine

+ Add - Delete Clone

OK

Cancel

PANgurus DASHBOARD ACC MONITOR

URL Filtering Continue And Override Page

2 items → ×

LOCATION

Predefined

Shared

Import File

Import File: C:\fakepath\override.txt [Browse...](#)

Destination: shared

[OK](#) [Cancel](#)

[Close](#)

Delete Import

https://192.168.27.2/# Login Time: 01/14/2021 01:04:41 | Session Expire Time: 02/13/2021 22:41:42

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

1 item → ×

HOST ID	REASON	TIME STAMP	SOURCE DEVICE/APP	SERIAL NUMBER	USER NAME
<input checked="" type="checkbox"/>	Auto-Quarantine	2021/01/15 00:48:29	192.168.27.115		reaper

[Add](#) [Delete](#) [PDF/CSV](#)

reaper | Logout | Last Login Time: 01/14/2021 01:04:41 | Session Expire Time: 02/13/2021 22:41:42 ⚠

javascript:Pan_base.redirectToLogout("14")

PANgurus DASHBOARD ACC **MONITOR** POLICIES OBJECTS NETWORK DEVICE

Logs ((status eq failure))

RECEIVE TIME	PORTAL/GATE...	STATUS	STAGE	EVENT	SOURCE USER	PUBLIC IPV4	AUTH METHOD	ERROR
01/15 00:53:49	gateway	failure	login	quarantined	reaper	192.168.27.2...		Device is quarantined
01/14 22:23:47	portal	failure	before-login	clientlessvpn-prelogin		65.154.226.1...		Client cert not present
01/14 22:22:44	portal	failure	before-login	clientlessvpn-prelogin		205.169.39.44		Client cert not present
01/14 22:14:17	gateway	failure	before-login	gateway-prelogin		192.168.27.1...		Client cert not present
01/14 22:14:16	portal	failure	before-login	portal-prelogin		192.168.27.1...		Client cert not present
01/14 01:02:40	portal	failure	login	portal-auth	reaper	192.168.27.2...	Cookie	Cookie expired
01/13 22:42:10	portal	failure	login	portal-auth	pre-logout	192.168.27.2...	Cookie	Cookie expired
01/13 22:39:27	portal	failure	login	portal-auth	pre-logout	192.168.27.2...	Cookie	Cookie expired
01/13 22:26:20	portal	failure	login	portal-auth	pre-logout	192.168.27.2...	Cookie	Cookie expired
01/13 22:12:58	portal	failure	login	portal-auth	pre-logout	192.168.27.2...	Cookie	Cookie expired
01/13 22:12:56	portal	failure	login	portal-auth	pre-logout	192.168.27.2...	Cookie	Cookie expired
01/13 22:10:57	gateway	failure	login	gateway-register	pangurus/reaper	192.168.27.2...		Existing user session found
01/13 01:17:49	gateway	failure	before-login	gateway-prelogin		192.168.27.2...		Client cert not present

PANgurus DASHBOARD ACC **MONITOR** POLICIES OBJECTS NETWORK DEVICE

Logs ((subtype eq auth))

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
01/14 01:07:11	auth	Informational	auth-success		Certificate validated for user 'pre-logout'. From: 192.168.27.204.
01/14 01:04:41	auth	Informational	auth-success		authenticated for user 'reaper'. From: 192.168.27.116.
01/14 01:02:56	auth	Informational	auth-success		Certificate validated for user 'pre-logout'. From: 192.168.27.204.
01/14 01:02:41	auth	Informational	auth-success	pangurus	authenticated for user 'reaper'. auth profile 'pangurus', vsys 'vsys1', server profile 'pangurus', server address '192.168.27.7', From: 192.168.27.204.
01/14 00:45:55	auth	Informational	auth-success		Certificate validated for user 'pre-logout'. From: 192.168.27.204.
01/13 23:06:29	auth	Informational	auth-success		Certificate validated for user 'pre-logout'. From: 192.168.27.204.

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE Commit

1 item → ×

NAME	LOCATION	INTERFACE	IP	SSL/TLS SERVICE PROFILE	AUTHENTIC... PROFILE	CERTIFICATE PROFILE	INFO
portal		loopback	192.168.27.3	gp	pangurus	prelogon	Current Users

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE Commit

1 item → ×

NAME	LOCATION	LOCAL INTERFACE	LOCAL IP	TUNNEL	MAX USER	INFO
gateway		loopback	192.168.27.3	tunnel		Remote Users

User Information - gateway

Current User | Previous User

1 item → ×

DOMAIN	USER	PRIMARY USERNAME	COMPUT...	CLIENT	PRIVATE IP	PUBLIC IP	SOURCE REGION	TUN... TYPE	LOGIN AT	LIFETI... (S)	LOGO...
pangurus	reaper	pangurus\r...	DESKTOP-QOBLVMD	Microsoft Windows 10 Pro , 64-bit	192.168.27.51	192.168.27....	home	IPSec	Jan 15 23:13:17	25920...	

Refresh PDF/CSV

Close

GlobalProtect Settings ×

General Connection Host Profile **Troubleshooting** Notification

If you're having trouble with GlobalProtect, please contact your system administrator. They might need to see the GlobalProtect logs in order to troubleshoot the problem.

Collect Logs

Network Configurations
 Routing Table
 Sockets
 Logs

Log: PanGP Service Start

PanGP Service
PanGP Agent

Logging Level: Debug

Chapter 3: Setting up Site-to-Site VPNs and Large-Scale VPNs

IKE Crypto Profile

Name: phase1

DH GROUP

- group19
- group20
- group2

AUTHENTICATION

- sha512
- sha256
- non-auth
- md5
- sha1
- sha256
- sha384
- sha512

ENCRYPTION

- aes-256-cbc
- des
- 3des
- aes-128-cbc
- aes-192-cbc
- aes-256-cbc
- aes-128-gcm
- aes-256-gcm

Timers: Minimum lifetime = 3 mins

IKEv2 Authentication: Multiple

OK Cancel

IKE Crypto Profile

Name: phase1

DH GROUP

- group19
- group1
- group2
- group5
- group14
- group18
- group20
- sha1

ENCRYPTION

- aes-256-cbc

Timers: Key Lifetime: Hours, 8. Minimum lifetime = 3 mins

IKEv2 Authentication: Multiple

OK Cancel

IKE Gateway

General | Advanced Options

Name: ReaperGW

Version: IKEv2 preferred mode

Address Type: IPv4 IPv6

Interface: ethernet1/1

Local IP Address: IP Address, 198.51.100.2/24

Peer IP Address Type: IP FQDN Dynamic

Peer Address: 198.51.100.1

Authentication: Pre-Shared Key Certificate

Pre-shared Key: ●●●●●●

Confirm Pre-shared Key: ●●●●●●

Local Identification: None

Peer Identification: None

Comment: None

- FQDN (hostname)
- IP address
- KEYID (binary format ID string in HEX)
- User FQDN (email address)

OK Cancel

Authentication Pre-Shared Key Certificate

Local Certificate

Local Identification

Peer Identification

Peer ID Check Exact Wildcard

Permit peer identification and certificate payload identification mismatch

Certificate Profile

Enable strict validation of peer's extended key use

Comment

IKE Gateway

IKE Gateway



General | **Advanced Options**

Common Options

- Enable Passive Mode
- Enable NAT Traversal

IKEv1 | IKEv2

Exchange Mode

IKE Crypto Profile

Enable Fragmentation

Dead Peer Detection

Interval

Retry

General | **Advanced Options**

Common Options

- Enable Passive Mode
- Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile

Strict Cookie Validation

Liveness Check

Interval (sec)

OK

Cancel

OK

Cancel

IPSec Crypto Profile

Name: Suite-B-GCM-256

IPSec Protocol: ESP

Encryption	Authentication
<input type="checkbox"/> ENCRYPTION	ESP
<input type="checkbox"/> aes-256-gcm	AH

Buttons: + Add, - Delete, ↑ Move Up, ↓ Move Down

AUTHENTICATION

<input checked="" type="checkbox"/> none
md5 (below 80-bit strength)
none
sha1 (NIST rating 128-bit strength)
sha256 (NIST rating 256-bit strength)
sha384 (NIST rating over 256-bit strength)
sha512 (NIST rating over 256-bit strength)

Buttons: + Add, - Delete, ↑ Move Up, ↓ Move Down

DH Group: group20

Lifetime: Hours, 1

Minimum lifetime = 3 mins

Enable

Lifesize: MB, [1 - 65535]

Recommended lifesize is 100MB or greater

Buttons: OK, Cancel

IPSec Crypto Profile

Name: Suite-B-GCM-256

IPSec Protocol: ESP

Encryption
<input checked="" type="checkbox"/> aes-256-gcm
des
3des
aes-128-cbc
aes-192-cbc
aes-256-cbc
aes-128-gcm
aes-256-gcm
null

Buttons: + Add, - Delete, ↑ Move Up, ↓ Move Down

DH Group: group20

Lifetime: no-pfs, group1, group2, group5, group14, group19, group20

Enable

Lifesize: []

Buttons: OK, Cancel

Tunnel Interface

Interface Name: tunnel . 4

Comment: []

Netflow Profile: None

Config | IPv4 | IPv6 | Advanced

Assign Interface To

Virtual Router: default

Security Zone: VPN

Buttons: OK, Cancel

IPSec Tunnel ?

General | Proxy IDs

Name ?

Tunnel Interface

Type Auto Key Manual Key GlobalProtect Satellite

Address Type IPv4 IPv6

IKE Gateway

IPSec Crypto Profile

Show Advanced Options

Enable Replay Protection

Copy ToS Header

Add GRE Encapsulation

Tunnel Monitor

Destination IP

Profile

Comment

IPSec Tunnel ?

General | Proxy IDs

IPv4 | IPv6

<input type="checkbox"/>	PROXY ID	LOCAL	REMOTE	PROTOCOL
--------------------------	----------	-------	--------	----------

IPSec Tunnel ?

General | Proxy IDs

IPv4 | IPv6

<input type="checkbox"/>	PROXY ID	LOCAL	REMOTE	PROTOCOL
<input type="checkbox"/>	ID1	10.0.0.0/24	192.168.27.0/24	any
<input type="checkbox"/>	ID2	10.10.10.0/24	192.168.27.0/24	any

Virtual Router - default

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

	NAME	DESTINATION	INTERFA...	Next Hop		ADMIN DISTAN...	ME...	BFD	ROUTE TABLE
				TYPE	VALUE				
<input type="checkbox"/>	dg	0.0.0.0/0	ethernet...	ip-address	198.51...	default	10	None	unicast
<input type="checkbox"/>	10.0.0.0-8-GP	10.0.0.0/8		next-vr	vr1	default	11	None	unicast
<input type="checkbox"/>	10.0.0.0-8-prisma	10.0.0.0/8		next-vr	vr2	default	10	None	unicast
<input checked="" type="checkbox"/>	vpn LAB	192.168.27.0/24	tunnel.4			30	10	None	unicast

Virtual Router - Static Route - IPv4

Name

Destination

Interface

Next Hop

Admin Distance

Metric

Route Table

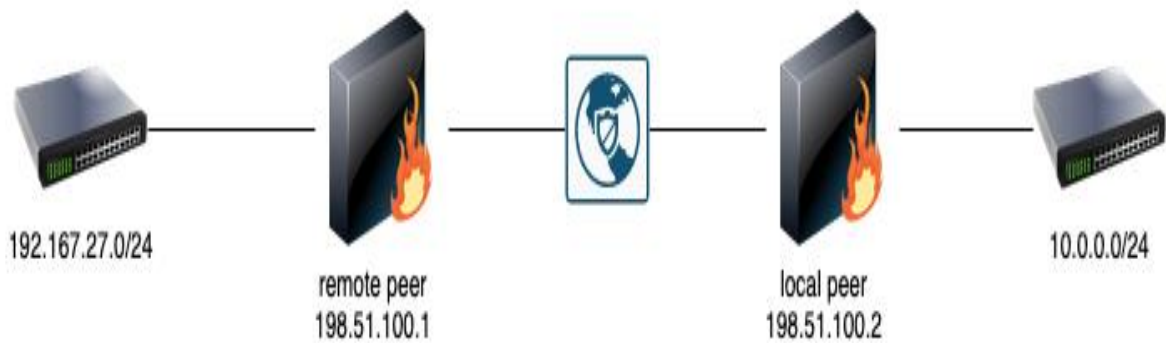
BFD Profile

Path Monitoring

Failure Condition Any All

Preemptive Hold Time (min)

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
<p><input type="button" value="+ Add"/> <input type="button" value="- Delete"/></p>						



IKE Gateway IKE Gateway ?

General | **Advanced Options**

Name: ReaperGW

Version: IKEv2 preferred mode

Address Type: IPv4 IPv6

Interface: ethernet1/1

Local IP Address: 198.51.100.2/24

Peer IP Address Type: IP FQDN Dynamic

Peer Address: 198.51.100.1

Authentication: Pre-Shared Key Certificate

Pre-shared Key: ●●●●●●

Confirm Pre-shared Key: ●●●●●●

Local Identification: None

Peer Identification: None

Comment:

General | **Advanced Options**

Common Options

Enable Passive Mode

Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile: Suite-B-GCM-128

Strict Cookie Validation

Liveness Check

Interval (sec):

OK **Cancel**

OK **Cancel**

PSec Tunnel IPSec Tunnel ?

General | **Proxy IDs**

Name: ReaperTunnel

Tunnel Interface: tunnel.4

Type: Auto Key Manual Key

Address Type: IPv4 IPv6

IKE Gateway: ReaperGW

Sec Crypto Profile: Suite-B-GCM-128

Show Advanced Options

Enable Replay Protection

Copy ToS Header

Add GRE Encapsulation

Tunnel Monitor

Destination IP:

Profile: None

Comment:

General | **Proxy IDs**

IPv4 | **IPv6**

<input type="checkbox"/>	PROXY ID	LOCAL	REMOTE	PROTOCOL
<input type="checkbox"/>	ProxyID1	10.0.0.0/24	192.168.27.0/24	any

OK **Cancel**

IKE Gateway ?

General | **Advanced Options**

Name:

Version:

Address Type: IPv4 IPv6

Interface:

Local IP Address:

Peer IP Address Type: IP FQDN Dynamic

Peer Address:

Authentication: Pre-Shared Key Certificate

Pre-shared Key:

Confirm Pre-shared Key:

Local Identification:

Peer Identification:

Comment:

General | **Advanced Options**

Common Options

Enable Passive Mode

Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile:

Strict Cookie Validation

Liveness Check

Interval (sec):

IPSec Tunnel ?

General | **Proxy IDs**

Name:

Tunnel Interface:

Type: Auto Key Manual Key

Address Type: IPv4 IPv6

IKE Gateway:

IPSec Crypto Profile:

Show Advanced Options

Enable Replay Protection

Copy ToS Header

Add GRE Encapsulation

Tunnel Monitor

Destination IP:




Profile:

Comment:

General | **Proxy IDs**

IPv4 | IPv6

<input type="checkbox"/>	PROXY ID	LOCAL	REMOTE	PROTOCOL
<input type="checkbox"/>	ProxyID1	10.0.0.0/24	192.168.27.0/24	any

	NAME	STATUS	TYPE	IKE Gateway/Satellite				Tunnel Interface				
				INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTER...	VIRTUAL ROUTER	VIR... SYS...	SE... ZO...	S... C...
	ReaperTunnel	 Tunnel Info	Auto Key	ethernet1/1	198.51.100.2/24	198.51.100.1	 IKE Info	tunnel.4	default (Show Routes)	vsys1	VPN	

Q (subtype eq vpn) and (receive_time geq '2021/01/26 23:17:34')

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
01/26 23:41:11	vpn	informat...	ike-nego-p1-delete	ReaperGW	IKE phase-1 SA is deleted SA: 198.51.100.2[500]-198.51.100.1[500] cookie:20af4534796f0f71:0000000000000000.
01/26 23:41:11	vpn	informat...	ike-nego-p1-fail	ReaperGW	IKE phase-1 negotiation is failed as initiator, main mode. Failed SA: 198.51.100.2[500]-198.51.100.1[500] cookie:20af4534796f0f71:0000000000000000. Due to timeout.
01/26 23:40:38	vpn	informat...	ike-nego-p1-start	ReaperGW	IKE phase-1 negotiation is started as initiator, main mode. Initiated SA: 198.51.100.2[500]-198.51.100.1[500] cookie:20af4534796f0f71:0000000000000000.
01/26 23:40:38	vpn	informat...	ikev2-nego-use-v1	ReaperGW	IKEv1 is used in IKEv2 preferred mode.
01/26 23:40:38	vpn	informat...	ike-generic-event		IKE_SA_INIT retransmission failed for gateway ReaperGW SN 2, trying IKEv1.
01/26 23:38:22	vpn	informat...	ikev2-nego-ike-start	ReaperGW	IKEv2 IKE SA negotiation is started as initiator, non-rekey. Initiated SA: 198.51.100.2[500]-198.51.100.1[500] SPI:75dc0c769c7978cf:0000000000000000.

Q (subtype eq vpn) and (receive_time geq '2021/01/26 23:41:34')

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
01/26 23:57:02	vpn	informat...	ike-nego-p1-delete	ReaperGW	IKE phase-1 SA is deleted SA: 198.51.100.2[500]-198.51.100.1[500] cookie:0d2c50104c952c72:92601de302f9d953.
01/26 23:57:02	vpn	informat...	ike-nego-p1-fail-common	ReaperGW	IKE phase-1 negotiation is failed. no suitable proposal found in peer's SA payload.
01/26 23:57:02	vpn	informat...	ikev2-nego-use-v1	ReaperGW	IKEv1 is used in IKEv2 preferred mode.
01/26 23:57:02	vpn	informat...	ike-nego-p1-start	ReaperGW	IKE phase-1 negotiation is started as responder, main mode. Initiated SA: 198.51.100.2[500]-198.51.100.1[500] cookie:0d2c50104c952c72:92601de302f9d953.

```

2021-01-27 00:13:34.424 +0100 [DEBG]: processing isakmp packet
2021-01-27 00:13:34.424 +0100 [DEBG]: ==
2021-01-27 00:13:34.424 +0100 [DEBG]: 124 bytes message received from 198.51.100.1
2021-01-27 00:13:34.424 +0100 [DEBG]: chk packet c771bell:20 size 124, rcp 0, NF rc -1
2021-01-27 00:13:34.425 +0100 [DEBG]: PH1 state changed: 0 to 0 sp1_set_next_state
2021-01-27 00:13:34.425 +0100 [DEBG]: PH1 state changed: 0 to 1 sp1_set_next_state
2021-01-27 00:13:34.425 +0100 [DEBG]: new cookie:
6b6e61e532f24a
2021-01-27 00:13:34.425 +0100 [PNTF]: { 2: } : ==> PHASE-1 NEGOTIATION STARTED AS RESPONDER, MAIN MODE <==>
===== Initiated SA: 198.51.100.2[500]-198.51.100.1[500] cookie:cf36
36226328f7023b:6b6e61e532f24a <=====
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : begin.
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : seen nptype=1(sa)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : seen nptype=13(vid)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : seen nptype=13(vid)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : succeed.
2021-01-27 00:13:34.425 +0100 [INFO]: { 2: } : received Vendor ID: DPD
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : remote supports DPD
2021-01-27 00:13:34.425 +0100 [INFO]: { 2: } : received Vendor ID: PANOS - the new generation of firewall
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : total SA len=52
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : begin.
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : seen nptype=2(prop)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : succeed.
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : proposal #1 len=44
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : begin.
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : seen nptype=3(trns)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : succeed.
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : transform #1 len=36
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Life Type, flag=0x8000, lrv=seconds
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Life Duration, flag=0x8000, lrv=28800
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Encryption Algorithm, flag=0x8000, lrv=AES
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : encryption(aes)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Key Length, flag=0x8000, lrv=128
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Authentication Method, flag=0x8000, lrv=PSK
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Hash Algorithm, flag=0x8000, lrv=SHA256
2021-01-27 00:13:34.425 +0100 [DEBG]: hash(sha256)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Group Description, flag=0x8000, lrv=DH19
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : dh(eep256)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : pair 1:
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : 0x7fac402180: next=(nil) tnext=(nil)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : proposal #1: 1 transform
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : prop#1, prot-id=ISAKMP, spi-size=0, #trns=1
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : trns#1, trns-id=IKE
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Life Type, flag=0x8000, lrv=seconds
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Life Duration, flag=0x8000, lrv=28800
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Encryption Algorithm, flag=0x8000, lrv=AES
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Key Length, flag=0x8000, lrv=128
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Authentication Method, flag=0x8000, lrv=PSK
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Hash Algorithm, flag=0x8000, lrv=SHA256
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Group Description, flag=0x8000, lrv=DH19
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : Compared: DB:Peer
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : (lifetime = 28800:28800)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : (lifetime = 0:0)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : enctype = AES:AES
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : (encklen = 192:128)
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : hashtype = SHA256:SHA256
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : authmethod = PSK:PSK
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : dh_group = DH19:DH19
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Life Type, flag=0x8000, lrv=seconds
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Life Duration, flag=0x8000, lrv=28800
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Encryption Algorithm, flag=0x8000, lrv=AES
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Key Length, flag=0x8000, lrv=128
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Authentication Method, flag=0x8000, lrv=PSK
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Hash Algorithm, flag=0x8000, lrv=SHA256
2021-01-27 00:13:34.425 +0100 [DEBG]: { 2: } : type=Group Description, flag=0x8000, lrv=DH19
2021-01-27 00:13:34.425 +0100 [PERR]: { 2: } : no suitable proposal found.
2021-01-27 00:13:34.425 +0100 [PERR]: { 2: } : 198.51.100.2[500] - 198.51.100.1[500]:(nil) failed to get valid p
proposal
2021-01-27 00:13:34.425 +0100 [PERR]: { 2: } : failed to process packet.
2021-01-27 00:13:34.425 +0100 [INFO]: { 2: } : ==> PHASE-1 SA DELETED <=====
===== Deleted SA: 198.51.100.2[500]-198.51.100.1[500] cookie:cf36
36226328f7023b:6b6e61e532f24a <=====

```

🔍 (subtype eq vpn) and (receive_time geq '2021/01/27 00:41:32') →

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
01/27 00:55:46	vpn	informat...	ike-send-notify	ReaperGW	IKE protocol notification message sent: NO-PROPOSAL-CHOSEN (14).
01/27 00:55:46	vpn	informat...	ike-nego-p2-proposal-bad	ReaperTunnel:Pr...	IKE phase-2 negotiation failed when processing SA payload. no suitable proposal found in peer's SA payload.
01/27 00:55:46	vpn	informat...	ike-nego-p2-start	198.51.100.1[50...	IKE phase-2 negotiation is started as responder, quick mode. Initiated SA: 198.51.100.2[500]-198.51.100.1[500] message id:0x6040CA45.
01/27 00:55:38	vpn	informat...	ike-send-notify	ReaperGW	IKE protocol notification message sent: NO-PROPOSAL-CHOSEN (14).
01/27 00:55:38	vpn	informat...	ike-nego-p2-proposal-bad	ReaperTunnel:Pr...	IKE phase-2 negotiation failed when processing SA payload. no suitable proposal found in peer's SA payload.
01/27 00:55:38	vpn	informat...	ike-nego-p2-start	198.51.100.1[50...	IKE phase-2 negotiation is started as responder, quick mode. Initiated SA: 198.51.100.2[500]-198.51.100.1[500] message id:0x6040CA45.

IKE Gateway/Satellite							Tunnel Interface				
NAME	STATUS	TYPE	INTERFACE	LOCAL IP	PEER ADDRESS	STATUS	INTERFACE	VIRTUAL ROUTER	VIRTU... SYSTE...	SEC... ZONE	STA...
ReaperTunnel		Auto Key	ethernet1/1	198.51.100.2/24	198.51.100.1		tunnel4	default (Show Routes)	vsys1	VPN	

(subtype eq vpn) and (receive_time geq '2021/01/27 00:41:32')

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
01/27 01:18:11	vpn	informat...	ike-nego-p2-proxy-id-bad	ReaperGW	IKE phase-2 negotiation failed when processing proxy ID. cannot find matching phase-2 tunnel for received proxy ID. received local id: 10.0.0.0/24 type IPv4_subnet protocol 0 port 0, received remote id: 192.168.27.0/24 type IPv4_subnet protocol 0 port 0.
01/27 01:18:11	vpn	informat...	ike-nego-p2-start	198.51.100.1[50...	IKE phase-2 negotiation is started as responder, quick mode. Initiated SA: 198.51.100.2[500]-198.51.100.1[500] message id:0xBAA77FAB.
01/27 01:18:08	vpn	informat...	ike-nego-p2-proxy-id-bad	ReaperGW	IKE phase-2 negotiation failed when processing proxy ID. cannot find matching phase-2 tunnel for received proxy ID. received local id: 10.0.0.0/24 type IPv4_subnet protocol 0 port 0, received remote id: 192.168.27.0/24 type IPv4_subnet protocol 0 port 0.
01/27 01:18:08	vpn	informat...	ike-nego-p2-start	198.51.100.1[50...	IKE phase-2 negotiation is started as responder, quick mode. Initiated SA: 198.51.100.2[500]-198.51.100.1[500] message id:0xBAA77FAB.



IKE Gateway

General | Advanced Options

Name: ReaperGW

Version: IKEv2 preferred mode

Address Type: IPv4 IPv6

Interface: ethernet1/1

Local IP Address: 198.51.100.2/24

Peer IP Address Type: IP FQDN Dynamic

Authentication: Pre-Shared Key Certificate

Pre-shared Key: ●●●●●●

Confirm Pre-shared Key: ●●●●●●

Local Identification: None

Peer Identification: FQDN (hostname) remote.pangurus.lab

Comment: None

FQDN (hostname)
 IP address
 KEYID (binary format ID string in HEX)
 User FQDN (email address)

OK Cancel

IKE Gateway
IKE Gateway ?

General | **Advanced Options**

Common Options

Enable Passive Mode
 Enable NAT Traversal

IKEv1 | IKEv2

Exchange Mode: aggressive

IKE Crypto Profile: Suite-B-GCM-128

Dead Peer Detection

Interval: 5
Retry: 5

General | **Advanced Options**

Common Options

Enable Passive Mode
 Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile: Suite-B-GCM-128
 Strict Cookie Validation

Liveness Check

Interval (sec): 5

OK
Cancel

GlobalProtect Portal Configuration
GlobalProtect Portal Configuration ?

General

Authentication

Portal Data Collection

Agent

Clientless VPN

Satellite

Satellite

	NAME	CONFIGURATI... REFRESH INTERVAL (HOURS)	SATELLITE HOSTNAME	SERIAL NUMBER	EXTERNAL GATEWAYS	ROUTING PRIORITY
<input type="checkbox"/>	satellites	24	unknown	007051000120...	satellite	1

+ Add
 - Delete
 ↑ Move Up
 ↓ Move Down

TRUSTED ROOT CA ^

pangurusPKI-rootCA

+ Add
 - Delete

Client Certificate: Local SCEP

Issuing Certificate: pangurusCA

OCSF Responder: ocsf-hive

Validity Period (days): 7

Certificate Renewal Period (days): 3

OK
Cancel

GlobalProtect Satellite
GlobalProtect Satellite ?

General | **Devices** | Enrollment User/User Group | Gateways

Name: satellites

Configuration Refresh Interval (hours): 24

GlobalProtect Satellite

1 Item

	SERIAL NUMBER	SATELLITE HOSTNAME
<input checked="" type="checkbox"/>	00:	unknown

GlobalProtect Satellite

1 Item

GlobalProtect Satellite

1 Item

GlobalProtect Satellite

1 Item

	GATEWAYS	ADDRESS	ROUTING PRIORITY
<input type="checkbox"/>	satellite	satellite.pangurus.com	1

+ Add
 - Delete

OK
Cancel

GlobalProtect Gateway Configuration



- General
- Authentication
- Agent
- Satellite**

Tunnel Settings | Network Settings | Route Filter

Tunnel Configuration

Tunnel Interface:

Replay attack detection

Copy TOS

Configuration Refresh Interval (Hours):

Tunnel Monitoring

IPv4 Destination Address:

IPv6 Destination Address:

Tunnel Monitor Profile:

Crypto Profiles

IPSec Crypto Profile:

OK Cancel

GlobalProtect Gateway Configuration



- General
- Authentication
- Agent
- Satellite**

Tunnel Settings | **Network Settings** | Route Filter

Inheritance Source:

[Check inheritance source status](#)

Primary DNS:

Secondary DNS:

Inherit DNS Suffixes

DNS Suffix:

IP POOL	ACCESS ROUTE
<input type="checkbox"/> 10.0.0.0-10.0.0.100	<input type="checkbox"/> 192.168.27.0/24
<input type="button" value="+ Add"/> <input type="button" value="- Delete"/> <input type="button" value="↑ Move Up"/> <input type="button" value="↓ Move Down"/>	<input type="button" value="+ Add"/> <input type="button" value="- Delete"/>

These IPs will be added to the firewall's routing table

These routes will be added to the client's routing table

OK Cancel

GlobalProtect Gateway Configuration



- General
- Authentication
- Agent
- Satellite**

Tunnel Settings | Network Settings | **Route Filter**

Routing Updates

Accept published routes

🔍 1 item → ✕

PERMITTED SUBNETS

172.16.0.0/12

OK

Cancel

IPSec Tunnel



General | Advanced

Name

Tunnel Interface

Type Auto Key Manual Key GlobalProtect Satellite

Portal Address

IPv6 preferred for portal registration

Interface

IPv4 Address

IPv6 Address

Comment

OK

Cancel

IPSec Tunnel ?

General | **Advanced**

Publish all static and connected routes to Gateway

Routes Published to GlobalProtect Gateways

0 items → ×

SUBNET

⊕ Add
⊖ Delete

External Certificate Authority

Local Certificate PANgurusCA ▼

Certificate Profile pangurus ▼

OK
Cancel

GlobalProtect Gateway Status ? ☰

Name satellite	IPv4 Address 198.51.100.3
Location vsys1	IPv6 Address
Interface loopback.5	Tunnel IPv4 172.16.0.1
Tunnel Interface tunnel.5	Tunnel IPv6

Active Satellites | Inactive Satellites

SATELLITE ^	STATUS	PUBLIC IP	TUNNEL IP	ROUTE SHARING	LOGO...
PA-VM2 <small>(Serial No. 067051000120304)</small>	Active <small>Established: Feb.03 21:55:46</small>	198.51.100.2, :: <small>Connected: 198.51.100.2</small>	172.16.0.100 <small>::</small>	Satellite Routes: 10.0.0/24, 10.10.10.0/24	

GlobalProtect Satellite Configuration and Runtime Status ? ☰

GlobalProtect Satellite Name satellite Interface ethernet1/1 Tunnel Interface tunnel.5 Local IP 198.51.100.2 Local IPv6	GlobalProtect Portal Address gp.pangurus.com Connected IP 198.51.100.3 Status Connection initializing - 02/03/2021 16:54:58 (reconnect to portal)
---	---

	GATEWAY ^	STATUS	PRIORI...	GATEWAY ADDRESS	TUNNEL MONITOR
☑	gp	Active 02/03/2021 21:55:46 <small>Established</small>	1	gp.pangurus.com <small>Connected: 198.51.100.3</small>	Interval: 0 sec Threshold: 0
	Name	VALUE	ACCESS ROUTES	DENIED ROUTES	DUPLICATE SUBNETS
	Gateway Tunnel	172.16.0.1 0:0:0:0:0:0	192.168.27.0/24 192.168.27.7/32		
	Local Tunnel	172.16.0.100			
	Prefer Ipv6	no			

Reconnect to GW | Refresh GW Config

Refresh
Close

GlobalProtect

IP-Tag

User-ID

Decryption

Tunnel Inspection

Configuration

System

Alarms

Authentication

Unified

(subtype eq satd) and (severity eq critical)

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
02/03 00:53:03	satd	critical	satd-gateway-connect-failed	Satellite	GlobalProtect Satellite connection to gateway failed. Satellite failed to connect to Gateway gp.pangurus.com due to certificate was not trusted. subject=/CN=gp.pangurus.com; issuer=/C=AT/O=ZeroSSL/CN=ZeroSSL RSA Domain Secure Site CA; not before=Dec 28 00:00:00 2020 GMT; not after=Mar 28 23:59:59 2021 GMT;
02/02 23:57:15	satd	critical	satd-portal-connect-failed	Satellite	GlobalProtect Satellite connection to portal failed. Satellite failed to connect to Portal 198.51.100.3 due to certificate common name does not match the configured hostname on the satellite. subject=/CN=gp.pangurus.com; issuer=/C=AT/O=ZeroSSL/CN=ZeroSSL RSA Domain Secure Site CA; not before=Dec 28 00:00:00 2020 GMT; not after=Mar 28 23:59:59 2021 GMT;

GlobalProtect Portal Configuration ?

General

Authentication

Portal Data Collection

Agent

Clientless VPN

Satellite

Satellite

<input type="checkbox"/>	NAME	CONFIGURATI... REFRESH INTERVAL (HOURS)	SATELLITE HOSTNAME	SERIAL NUMBER	EXTERNAL GATEWAYS	ROUTING PRIORITY
<input type="checkbox"/>	satellites	24	PA-VM2	007051000120...	satellite	1

TRUSTED ROOT CA ^

pangurusPKI-rootCA

comodoCA

Client Certificate Local SCEP

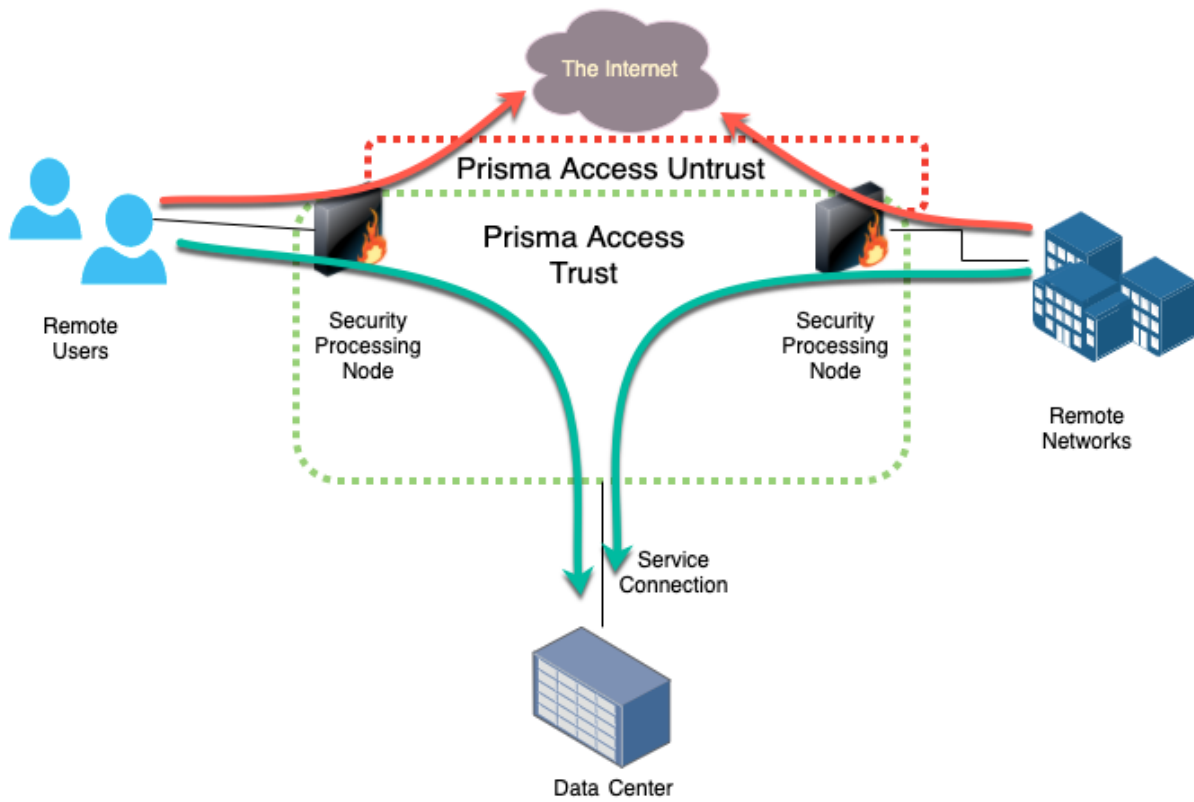
Issuing Certificate

OCSP Responder

Validity Period (days)

Certificate Renewal Period (days)

Chapter 4: Configuring Prisma Access



Management | Operations | Services | Interfaces | Telemetry | Content-ID | Wi

Time Zone Europe/Brussels
 Locale en
 Time Thu Apr 29 1:15:27 CEST 2021

Management | Operations | **Services** | Interfaces | Telemetry | Content-ID | Wil

Services

Update Server updates.paloaltonetworks.com
 Verify Update Server Identity
 DNS Servers
 Primary DNS Server 192.168.27.7
 Secondary DNS Server 1.1.1.1
 Minimum FQDN Refresh Time (sec) 30
 FQDN Stale Entry Timeout (min) 1440
 Proxy Server
 Primary NTP Server Address ntp.belnet.be
 Primary NTP Server Authentication Type None
 Secondary NTP Server Address time.nist.gov
 Secondary NTP Server Authentication Type None

Management | Operations | Services | Interfaces | **Telemetry** | Content-ID | Wil

Telemetry

Threat Prevention
 Device Health and Performance
 Product Usage
 Telemetry Region Europe
 Certificate Status Device Certificate does not exist
[View details for installing the certificate](#)

PANORAMA DASHBOARD ACC MONITOR Device Groups POLICIES OBJECTS Templates NETWORK DEVICE PANORAMA Commit

Panorama 5 items

FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS	RELEASE NOTE URL
cloud_services-1.6.0-h1	1.6.0-h1	2020/05/23 19:34:21	4M	✓		Install Delete	
cloud_services-1.8.0	1.8.0	2020/11/16 15:28:51	6M	✓	✓	Remove Config Uninstall	

Successfully Completed Setup.



Setup Complete

Recommended Next Steps

Copy One-time Password

42594416f11594b5

Valid before 9:22:59 AM



Install Cloud Services Plugin



Assign Role-based Access Control



Associate Directory-Sync Service



Configure Data Lake Quota



Manage App Instances



Current Account: [Account Name]

Cloud Services

Activate Cloud Services Auth-Code **Generate OTP** Filter By: Auth Code

Export To CSV **Generate One Time Password** [X]

Auth Code	S
[Redacted]	[Redacted]

Device Type: Generate OTP for Panorama

The OTP provides users the password to input into the Cloud Services. This is a required step to enable secure use of the cloud services. This password is only valid for 10 minutes. If the time has expired before you have use this password, please generate a new password.

Select OTP Type: Logging Service

Panorama: 0007

Password: `afe7beed2c3f8252bdd48200e7b137472f4fe1bfc31299af9246677e27c2b26cde338f115f069458bb89d38e9`

Expires On: 12/2/2020 5:11:42 AM

Copy to Clipboard **Generate OTP** Close

PANORAMA DASHBOARD ACC MONITOR **PANORAMA** Commit Manual

Panorama Status

Verify Account

Your account needs to be verified. Get your one-time password from the Customer Support Portal and enter it below. Note: you must be superuser on the CSP.

One-time Password:

OK Cancel

Your account needs to be verified.

Verify

admin | Logout | Last Login Time: 11/19/2020 04:49:11 | Session Expire Time: 12/19/2020 06:25:45 Tasks | Language paloalto

Service Setup | Service Connction | Traffic Steering

Settings

Internal Domain List | Cortex Data Lake | Advanced

Service Infrastructure

Infrastructure Subnet: 172.31.0.0/16

Infrastructure BGP AS: 65534

Internal Domain List

DOMAIN NAMES	PRIMARY DNS	SECONDARY DNS
mydomain.com	192.168.10.7	

Cortex Data Lake Theater: europe (europe)

Advanced

Routing Preference: Default

HIP Redistribution

Enable HIP Redistribution

Commit and Push

Doing a commit will overwrite the Panorama running configuration with the commit scope.

Commit All Changes Commit Changes Made By:(1) admin

COMMIT SCOPE	LOCATION TYPE
Service_Conn_Device_Group	Device Groups
PrimaryDevices	Device Groups
Service_Conn_Template	Templates
PrimaryStack	Template Stacks
Service_Conn_Template_Stack	Template Stacks
service-connections	Cloud Services

Preview Changes Change Summary Validate Commit Group By Location Type

PUSH SCOPE	LOCATION TYPE	ENTITIES
Service_Conn_Device_Group	Prisma Access	

Push Scope Selection

Device Groups | Templates | Collector Groups | WildFire Appliances and Clusters | **Prisma Access**

Service Setup

Commit And Push | Cancel

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICES PANORAMA

Panorama | Template: Service_Conn_Template | View by: Device | Mode: Multi VSYS; Normal Mode; VPN

IKE Gateway

General | Advanced Options

Common Options

- Enable Passive Mode
- Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile: Phase1 Strict Cookie V

Liveness Check
Interval (sec): 5

Name: ServiceConnection-DC1
Version: IKEv2 preferred mode
Peer IP Address Type: IP Dynamic
Authentication: Pre-Shared Key Certificate
Pre-shared Key: [Redacted]
Confirm Pre-shared Key: [Redacted]
Local Identification: FQDN (hostname) cloud.prisma.lab
Peer Identification: FQDN (hostname) fw.prisma.lab
Comment: [Empty]

OK **Cancel**

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICES PANORAMA

Panorama | Template: Service_Conn_Template | View by: Device

IPSec Tunnel

General | Proxy IDs

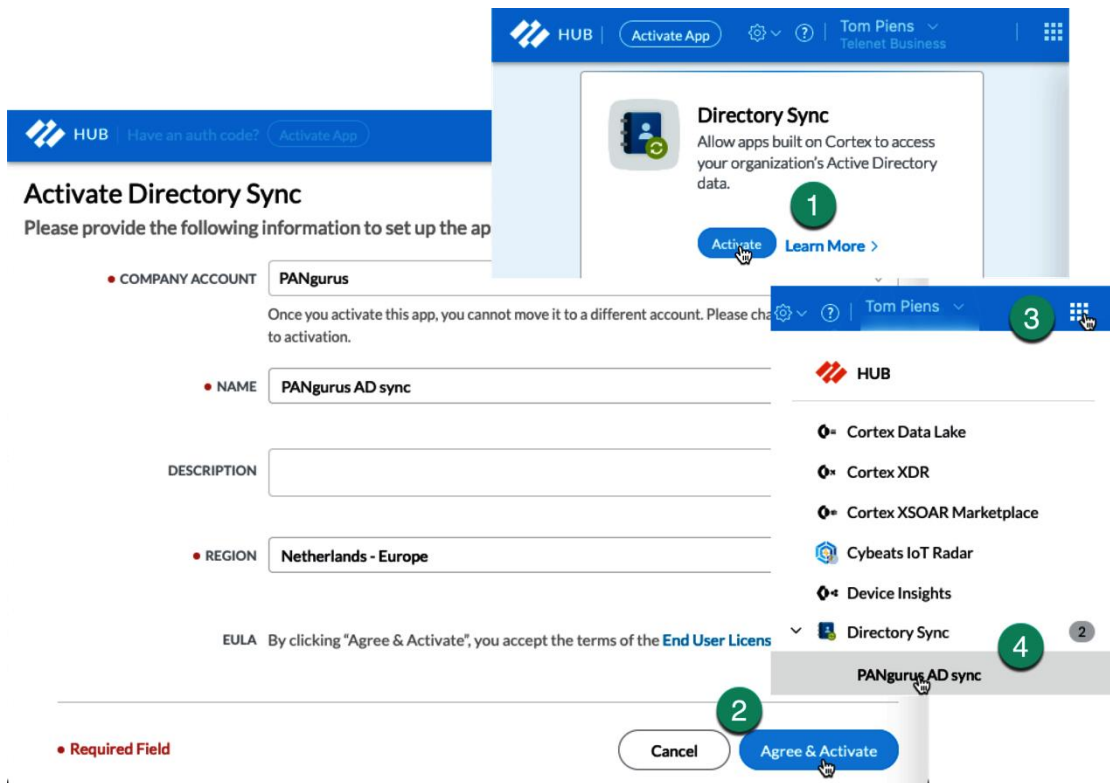
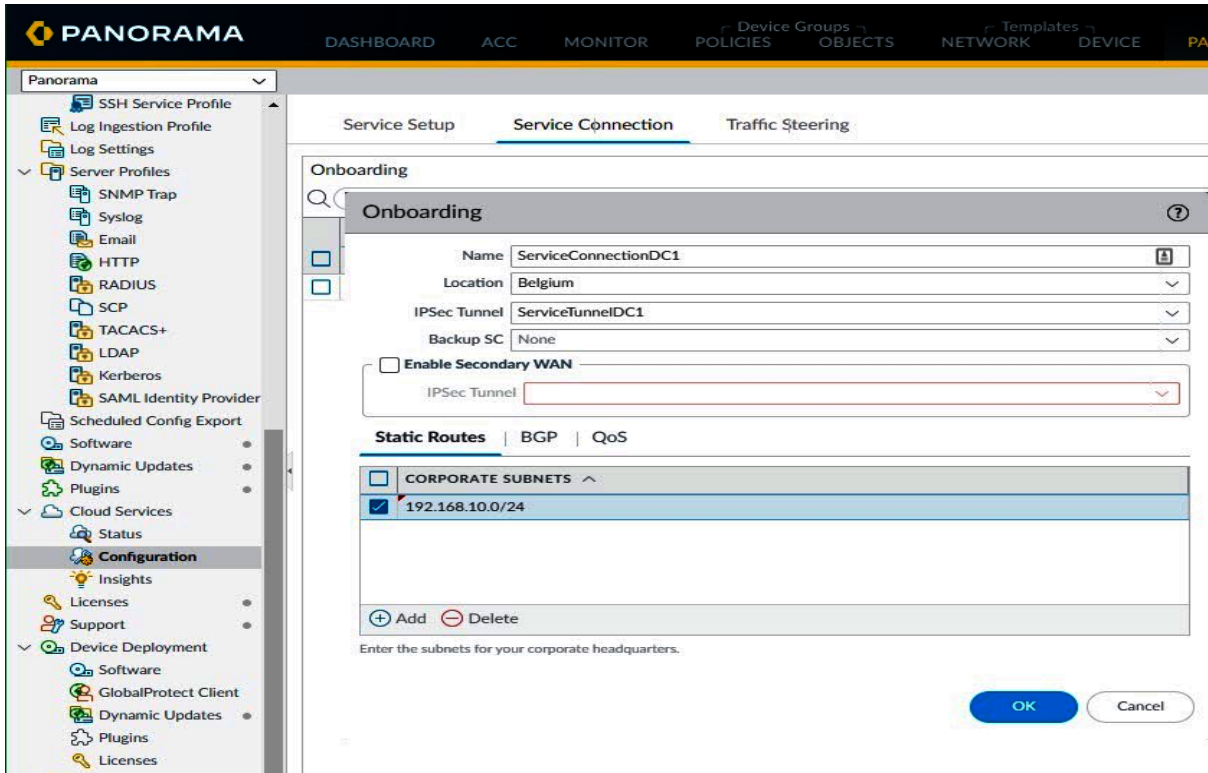
Name: ServiceTunnelDC1
Type: Auto Key
IKE Gateway: ServiceConnection-DC1
IPSec Crypto Profile: phase2

Enable Replay Protection
 Copy ToS Header
 Add GRE Encapsulation

Tunnel Monitor

Destination IP: 192.168.10.1
Proxy ID: None
Comment: [Empty]

OK **Cancel**





Set Up Directory

Configure an on-premises Active Directory or Azure Active Directory for this Directory Sync instance.



On-Premises

Install and configure a Directory Sync agent to collect user, group, and device attributes from your Active Directory.



Azure Active Directory

Grant permissions for Directory Sync to access your Azure Active Directory and collect user, group, and device attributes.

Set Up

Set Up



Configure Directory Sync for Active Directory

Download and install the Directory Sync agent on a Windows server to allow Palo Alto Directory.

1

Download

Download the latest version of the Directory Sync agent.

Download Agent

2

Generate Certificate

Generate a certificate to authenticate the agent with the Directory Sync service.

Get Certificate

3

Install

Install the agent on a Windows server and configure it to communicate with your Act

Get Started



cert.p12

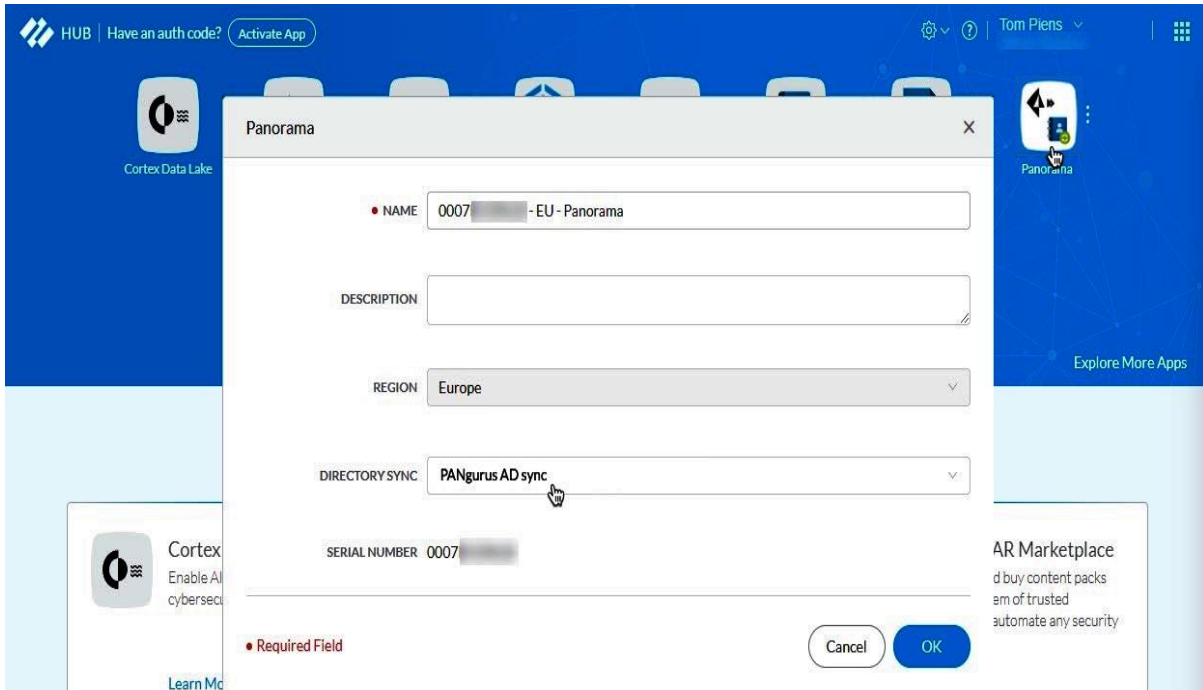
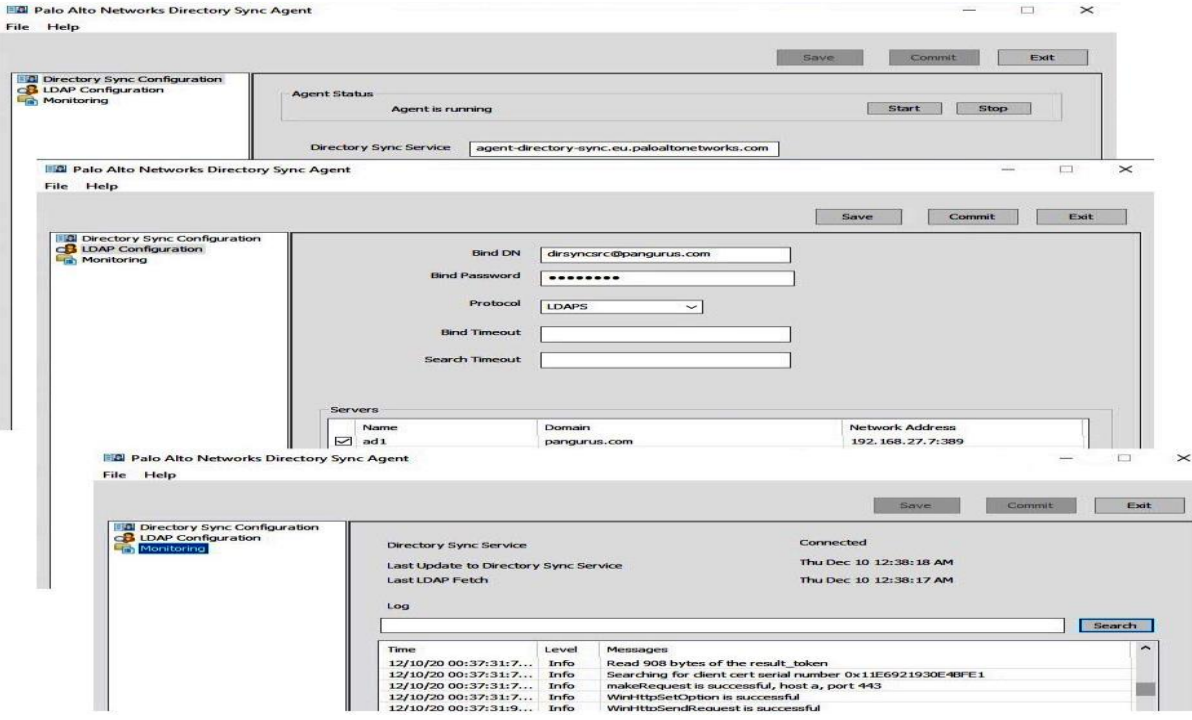
[Open file](#)



DalInstall-1.6.0.msi

[Open file](#)





PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE** PANORAMA

Panorama **Template** Service_Conn_Template View by Device Mode Multi VSYS; Normal Mode; VPN Enabled

Location vsys1

User Mapping | Connection Security | Terminal Server Agents | **Group Mapping Settings** | Authentication Portal Settings

NAME	ENABLED	SERVER PROFILE	UPDATE INTERVAL (SEC)
<input type="checkbox"/> group mapping	<input checked="" type="checkbox"/>	service-connection-LDAP	default

Panorama **Template** Service_Conn_Template View by Device Mode Multi VSYS; Normal Mode; VPN Enabled

NAME	LOCATION	SERVERS	OTHERS
<input type="checkbox"/> service-connection-LDAP	Shared	Name: AD1 LDAP Server: 192.168.27.7 Port: 389	Type: active-directory SSL: <input checked="" type="checkbox"/>

Service Setup **Mobile Users** Remote Networks Service Connection Traffic Steering Enable Multitenancy

Settings

Template Stack Mobile_User_Template_Stack
Mobile_User_Template

Parent Device Group PrimaryDevices
Mobile_User_Device_Group

Zone Mapping

Trusted Zones (Not Configured)

Untrusted Zones prisma-trust, prisma-untrust

Zone Mapping

UNTRUSTED ZONES	TRUSTED ZONES
prisma-trust	
prisma-untrust	

Service Setup **Onboarding**

General | Locations | IP Pools | Network Services | Manual Gateway Locations

Portal Name Type Use Default Domain Use Company Domain

Portal Hostname mylab
This FQDN will be published to public domain name servers.

Client Authentication

Authentication Profile **service-connection-LDAP**

Authentication Override Certificate **Use Auto Generated CA and Certificate**

Select the certificate for encrypting and decrypting the secure cookie to authentication gateways user login. The selected certificate including the private key will be authentication configuration can be changed in Mobile_User_Template: Net

Internal Host Detection

IP Address 192.168.10.1

Hostname labfirewall.mydomain.com

Onboarding

General | **Locations** | IP Pools | Network Services | Manual Gateway Locations

- < All Europe locations
Your subscription allows you to use up to 5
Prisma Access locations for Mobile Users



Onboarding



General | Locations | **IP Pools** | Network Services | Manual Gateway Locations

Search: 1 item → ×

<input type="checkbox"/>	REGION	IP POOL
<input type="checkbox"/>	Africa, Europe & Middle East	172.16.0.0/19

Warning

The IP pools you provided are only for emea. Without a worldwide IP pool, the mobile user infrastructure will be deployed to the configured regions only.

+ Add - Delete

You have added 5 locations.

Do you want to proceed?

OK

Cancel

Yes

No

1 item → ×

	REGION	Internal Domains			Public Domains	
		PRIMARY DNS	SECONDARY DNS	DOMAIN LIST	PRIMARY DNS	SECONDARY DNS
<input checked="" type="checkbox"/>	Africa, Europe & Middle East	192.168.10.5		mydomain.com	Use Cloud Default	Use Cloud Default

+ Add - Delete

For a domain entry in the Internal Domains list, enter as *-<domain>. For example *.acme.com.
 For a domain entry in the DNS Suffix Search list, enter as <domain>. For example, acme.com

WINS Configuration

Select this to provide a region-specific Primary and Secondary WINS server configuration.

OK Cancel

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE PANORAMA

Device Groups Templates

Panorama Template: Mobile_User_Template View by Device Mode: Multi VSYS; Normal Mode; VPN Enabled

NAME	LOCATION	IP	SSL/TLS SERVICE PROFILE	AUTHENTICATION PROFILE
GlobalProtect_Portal	vsys1		-	LDAP

IPSec Tunnels GRE Tunnels GlobalProtect Portals Gateways

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS **NETWORK** DEVICE PANORAMA

Device Groups Templates

Panorama Template: Mobile_User_Template View by Device Mode: Multi VSYS; Normal Mode; VPN Enabled

NAME	LOCATION	TUNNEL	MAX USE
GlobalProtect_External_Gateway	vsys1	-	

IPSec Tunnels GRE Tunnels GlobalProtect Portals Gateways

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Panorama Template Remote_Network_Template View by Device Mode Multi

Zones

- Routing
 - Logical Routers
 - Routing Profiles
 - BGP
- IPSec Tunnels
- GRE Tunnels

CONNECTION NAME

- prisma-RN-trust
- prisma-RN-untrust

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA

Panorama Template Remote_Network_Template View by Device Mode Multi VSYS; Normal Mode; VPN Enabled

IKE Gateway

General | **Advanced Options**

Name: RemoteNetwork-BE

Version: IKEV2 preferred mode

Peer IP Address Type: IP Dynamic

Authentication: Pre-Shared Key Certificate

Pre-shared Key: *****

Confirm Pre-shared Key: *****

Local Identification: FQDN (hostname) cloudRN.prisma.lab

Peer Identification: FQDN (hostname) BE.prisma.lab

Comment:

Advanced Options

Common Options

- Enable Passive Mode
- Enable NAT Traversal

IKEv1 | **IKEv2**

Exchange Mode: auto

IKE Crypto Profile: phase1

Enable Fragmentation

Dead Peer Detection

Interval: 5

Retry: 5

Advanced Options

Common Options

- Enable Passive Mode
- Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile: phase1

Strict Cookie Validation

Liveness Check

Interval (sec): 5

OK

IPSec Tunnel ?

General | **Proxy IDs**

Name: RemoteTunnelBE

Type: Auto Key

IKE Gateway: RemoteNetwork-BE

IPSec Crypto Profile: phase2

- Enable Replay Protection
- Copy ToS Header
- Add GRE Encapsulation

Tunnel Monitor

Destination IP: 192.168.27.1

Proxy ID: None

Comment:

OK Cancel

Bandwidth Allocation

Allocated Total : 0 / 200 Mbps
Click each bandwidth allocation to edit bandwidth allocated to com

Bandwidth Allocation (Mbps)	Compute Location
0	Canada Central
0	US Northwest
0	US Southeast
0	US Southwest
0	US Central
0	US East
0	South America East
0	Europe Central
0	Europe North
200	Belgium
0	Europe West

Onboarding

Name: RemoteNetworks

ECMP Load Balancing: None

Location: Belgium
Your subscription allows you to use up to 5 Prisma Access locations.

IPSec Termination Node: belgium-daffodil

IPSec Tunnel: RemoteTunnelBE

Enable Secondary WAN

IPSec Tunnel:

Static Routes | BGP

BRANCH IP SUBNETS ^

192.168.27.0/24

Service Setup | Mobile Users | **Remote Networks** | Service Connection | Traffic Steering | Enable Multitenancy

Settings

Template Stack: Remote_Network_Template_Stack

Parent Device Group: Remote_Network_Template

Secondary Devices: Remote_Network_Device_Group

Overlapped Subnets:

Zone Mapping

Trusted Zones: prisma-RN-trust

Untrusted Zones: prisma-RN-untrust

Bandwidth Allocation

Allocated Bandwidth: 200/200Mbps

Onboarding

CONNECTION NAME	LOCATION	Prisma Access			Links		Remote Networks		
		IPSEC TERMINATION NODE	ECMP	INBOUND ACCESS	IPSEC TUNNEL	PEER IP ADDRESS	SUBNETS	BGP PRIMARY	BGP SECONDARY
RemoteNetworks	Belgium	belgium-daffodil	Disabled	Disabled	RemoteTunnelBE (Primary)	dynamic	192.168.27.0/24	Disabled	Disabled

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA

Commit Manual

Panorama

Status | Monitor | **Network Details**

Service Infrastructure Service Connection Remote Networks Mobile Users

1 item

NAME	SERVICE IP ADDRESS	USER-ID AGENT ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET	EBGP ROUTER	BRANCH AS AND ROUTER
ServiceConnectionDC1	208.127.60.119	172.31.0.1	dynamic	192.168.10.0/24	172.31.0.1	

Export to CSV

admin | Logout | Last Login Time: 12/11/2020 08:53:08 | Session Expire Time: 01/10/2020 09:46:15

PANORAMA DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE PANORAMA

Commit Manual

Panorama

Status | Monitor | **Network Details**

Service Infrastructure Service Connection Remote Networks Mobile Users

1 item

NAME	SERVICE IP ADDRESS	LOCAL IP ADDRESS	STATIC SUBNET	Secure Inbound Apps		EBGP ROUTER	BRANCH AS AND ROUTER
				APP NAME / PUBLIC ADDRESS / PRIVATE ADDRESS:PORT			
RemoteNetworks	208.127.60.125	dynamic	192.168.27.0/24			172.31.0.11	

Export to CSV

admin | Logout | Last Login Time: 12/11/2020 08:53:08 | Session Expire Time: 01/10/2020 09:46:15

IKE Gateway

General | **Advanced Options**

Common Options

Enable Passive Mode
 Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile: phase1

Strict Cookie Validation

Liveness Check
Interval (sec): 5

OK Cancel

General | Advanced Options

Name: Prisma-RN-Uplink
Version: IKEv2 preferred mode
Address Type: IPv4 IPv6
Interface: ethernet1/1
Local IP Address: 198.51.100.2/24
Peer IP Address Type: IP FQDN Dynamic
Peer Address: 208.127.60.125
Authentication: Pre-Shared Key Certificate
Pre-shared Key:
Confirm Pre-shared Key:
Local Identification: FQDN (hostname) | BE.prisma.lab
Peer Identification: FQDN (hostname) | cloudRN.prisma.lab
Comment:

OK Cancel

IPSec Tunnel

General | Proxy IDs

Name: Prisma-SC-tunnel
Tunnel Interface: tunnel10
Type: Auto Key Manual Key
Address Type: IPv4 IPv6
IKE Gateway: Prisma-SC-Uplink
IPSec Crypto Profile: phase2
 Show Advanced Options
 Enable Replay Protection
 Copy ToS Header
 Add GRE Encapsulation

Tunnel Monitor
Destination IP:
Profile: None
Comment:

Virtual Router - VR

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

4 items → X

NAME	DESTINATION	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE
			TYPE	VALUE				
<input type="checkbox"/> DG	0.0.0.0/0	ethernet1/1	ip-address	10.0.73.254	default	10	None	unicast
<input type="checkbox"/> prisma-infrastructure	172.31.0.0/24	tunnel10			default	10	None	unicast
<input type="checkbox"/> prisma-GP	172.16.0.0/19	tunnel10			default	10	None	unicast
<input type="checkbox"/> prisma-RN	192.168.27.0...	tunnel10			default	10	None	unicast

+ Add - Delete Clone

OK Cancel

IKE Gateway

General | **Advanced Options**

Name: Prisma-SC-Uplink
 Version: IKEv2 preferred mode
 Address Type: IPv4 IPv6
 Interface: ethernet1/1
 Local IP Address: 10.0.73.54/24
 Peer IP Address Type: IP FQDN Dynamic
 Peer Address: 208.127.60.119
 Authentication: Pre-Shared Key Certificate
 Pre-shared Key: [REDACTED]
 Confirm Pre-shared Key: [REDACTED]
 Local Identification: FQDN (hostname) | fw.prisma.lab
 Peer Identification: FQDN (hostname) | cloud.prisma.lab
 Comment: [REDACTED]

Advanced Options

Common Options

Enable Passive Mode
 Enable NAT Traversal

IKEv1 | **IKEv2**

IKE Crypto Profile: phase1
 Strict Cookie Validation

Liveness Check
 Interval (sec): 5

OK Cancel

IPSec Tunnel

General | **Proxy IDs**

Name: Prisma-RN-tunnel
 Tunnel Interface: tunnel3
 Type: Auto Key Manual Ke
 Address Type: IPv4 IPv6
 IKE Gateway: Prisma-RN-Uplink
 IPSec Crypto Profile: phase2
 Show Advanced Options
 Enable Replay Protection
 Copy ToS Header
 Add GRE Encapsulation

Tunnel Monitor
 Destination IP: [REDACTED]
 Profile: None
 Comment: [REDACTED]

Virtual Router - default

Static Routes

IPv4 | **IPv6**

NAME	DESTINATION	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	ROUTE TABLE
			TYPE	VALUE			
dg	0.0.0.0/0	vlan	ip-address	192.168.27.1	default	10	unicast
Prisma-SC	192.168.10.0...	tunnel3			default	10	unicast
prisma-infrastr...	172.31.0.0/24	tunnel3			default	10	unicast
prisma-GP	172.16.0.0/19	tunnel3			default	10	unicast

4 items → ×

⊕ Add ⊖ Delete 🔄 Clone

OK Cancel

Configuration

Instance: [REDACTED] - EU - Cortex Data Lake | Region: Europe

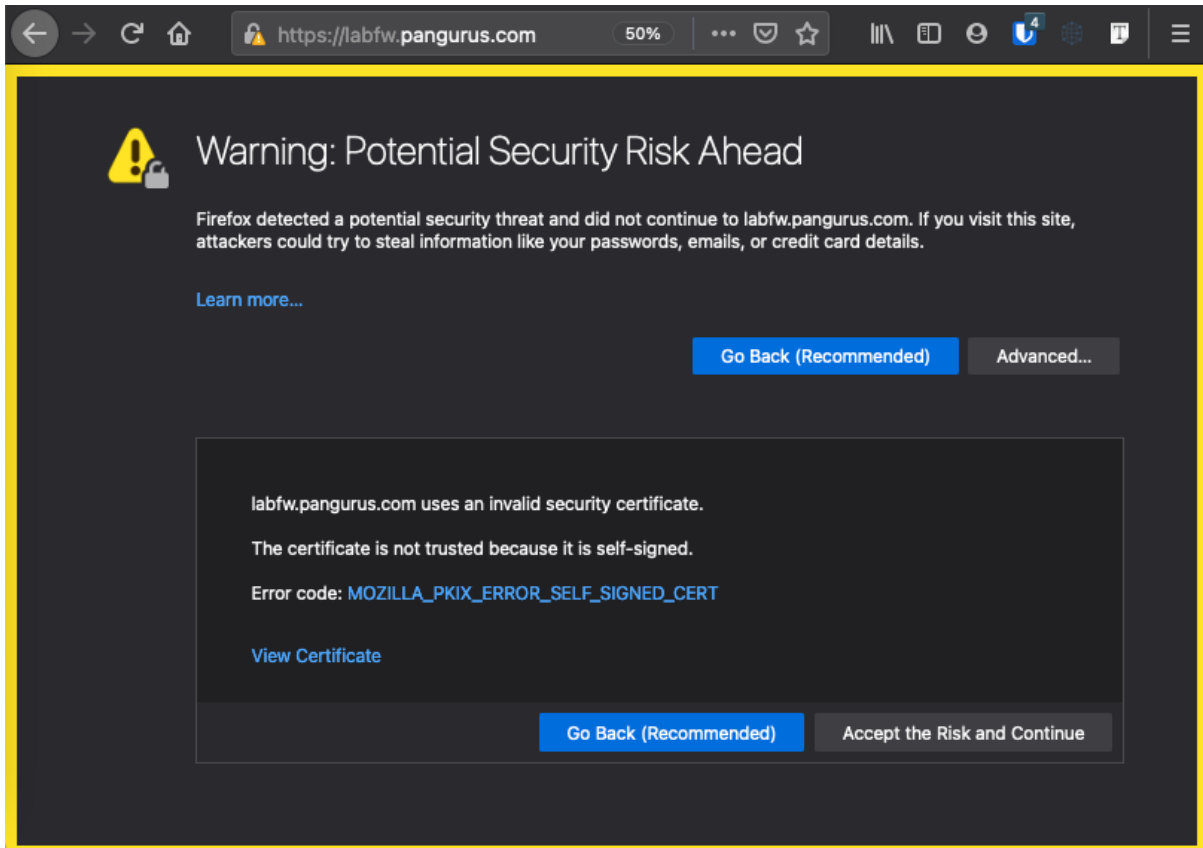
5 TB

TOTAL STORAGE
 5 TB Allocated
 0 MB Unallocated

Firewall Logs: 4.9 TB

LOG TYPE	QUOTA (%)	ALLOCATED SIZE
Cortex XDR		-
alert	Empty or [0-100]	-
Endpoint Data	Empty or [0-100]	-
Common Logs		102.4 GB
config	1%	51.2 GB
system	1%	51.2 GB
Firewall Logs		4.9 TB
decryption	1%	51.2 GB
globalprotect	2%	102.4 GB
threat	10%	51.2 GB
traffic	70%	3.5 TB

Chapter 5: Enabling Features to Improve Your Security Posture



Generate Certificate

Certificate Type: Local SCEP

Certificate Name: Management-cert

Common Name: labfw.pangurus.com

Signed By: External Authority (CSR) (IP or FQDN to appear on the certificate)

Certificate Authority

Block Private Key Export

OCSP Responder: [Empty]

Cryptographic Settings

Algorithm: Elliptic Curve DSA

Number of Bits: 256

Digest: sha256

Expiration (days): 365

Certificate Attributes

TYPE	VALUE
IP = "IP Address" from Subject Alternative Name (SAN) field	192.168.27.11
Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailA...	security@pangurus.com

+ Add - Delete

Generate Cancel

Welcome

Use this Web site to request a certificate. You can verify your identity to the CA depending upon the type of certificate you request.

You can also use this Web site to view the status of a pending certificate request, or to view the revocation list (CRL), or to view the status of a pending certificate request.

For more information about Active Directory Certificate Services, click [Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Request a Certificate

Select the certificate type:

[User Certificate](#)



Or, submit an [advanced certificate request](#).

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBITCBxwIBADBDMRswGQYDVQDExJ3VyaXR5Qm9udj5w
hkiG9w0BCQEFXNLY3VyaXR5Qm9udj5wLmNv
SM49AwEHA0IABFSBSdUgC20drgabpsSVfdZrIV9
JzXe3q1RcQRawv4MUNItHHRmIXD5TVZAomgIjAg
A1UdEQQIMAaHBMCoGswCgYIKoZIzj0EAwIDSQA...
```

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

- [Download certificate](#)
- [Download certificate chain](#)



Certificate Template:

Web Server 3

Additional Attributes:

Attributes:



Submit

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Device Certificates | Default Trusted Certificate Authorities

NAME	SUBJECT
√ PANgurusCA	CN = rootca.pangur...
connect	CN = connect.pangu...
Testcert...	CN = test.pangurus....
untrustcert	CN = untrusted.pan...
Management-cert	labfw.pangurus.com

Import Certificate

Certificate Type: Local SCEP

Certificate Name: Management-cert

Certificate File: C:\fakepath\certnew.cer Browse...

File Format: Base64 Encoded Certificate (PEM)

Private key resides on Hardware Security Module

Import Private Key

Block Private Key Export

Key File: C:\fakepath\certnew.cer Browse...

Passphrase:

Confirm Passphrase:

OK Cancel

Delete Revoke Renew Import Generate Export Certificate Import HA Key Export HA Key PDF/CSV

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

- Setup
- High Availability
- Config Audit
- Password Profiles
- Administrators
- Admin Roles
- Authentication Profile
- Authentication Sequence
- User Identification
- Data Redistribution
- Device Quarantine
- VM Information Sources
- Troubleshooting
- Certificate Management
 - Certificates
 - Certificate Profile
 - OCSP Responder
 - SSL/TLS Service Profile**

NAME	LOCATION	CERTIF
SSL/TLS Service Profile		connec

SSL/TLS Service Profile ?

Name:

Certificate:

Protocol Settings

Min Version:

Max Version:

PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Management | Operations | Services | Interfaces | Telemetry | Content-ID | WildFire | Session | HSM

General Settings ?

General Settings ?

Hostname:

Domain:

Accept DHCP server provided Hostname

Accept DHCP server provided Domain

Login Banner:

Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile:

Time Zone:

Locale:

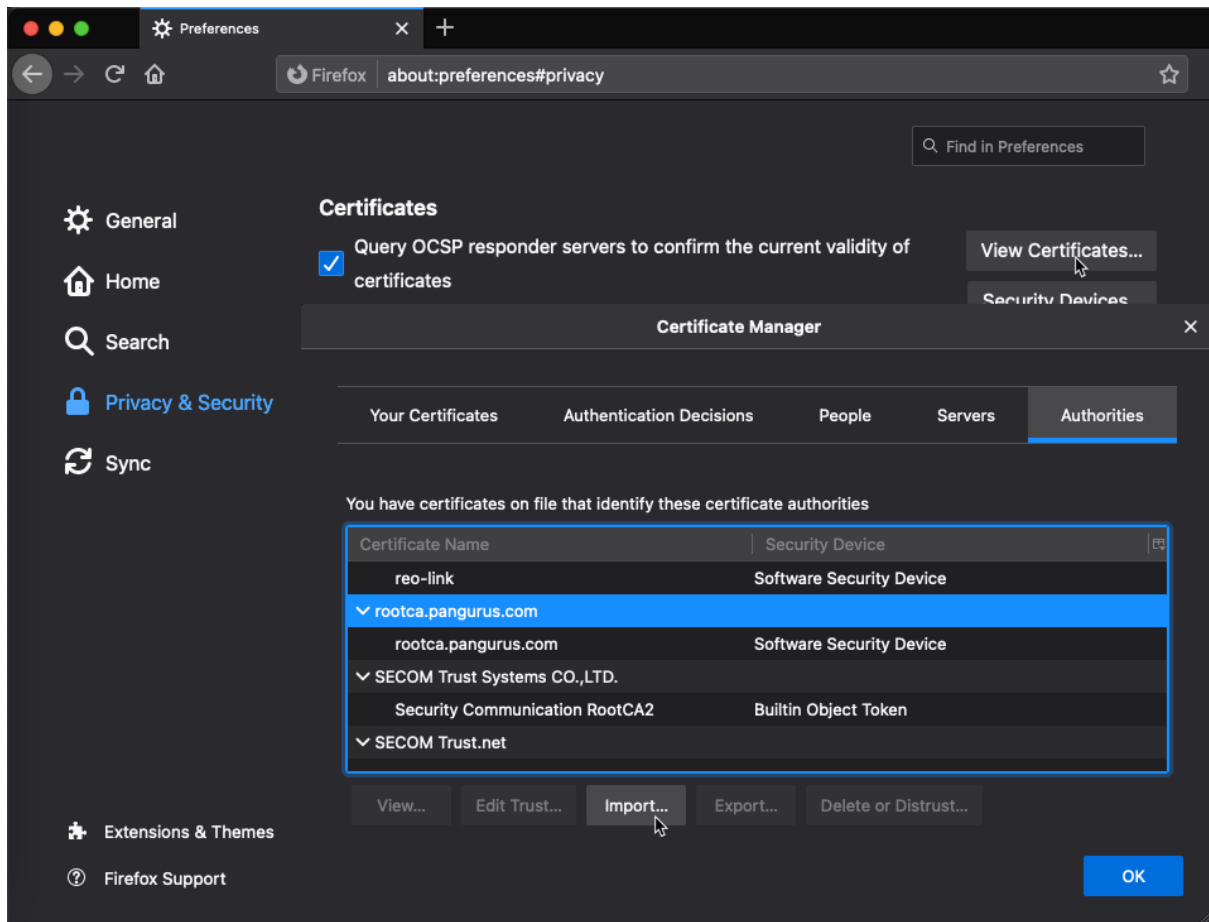
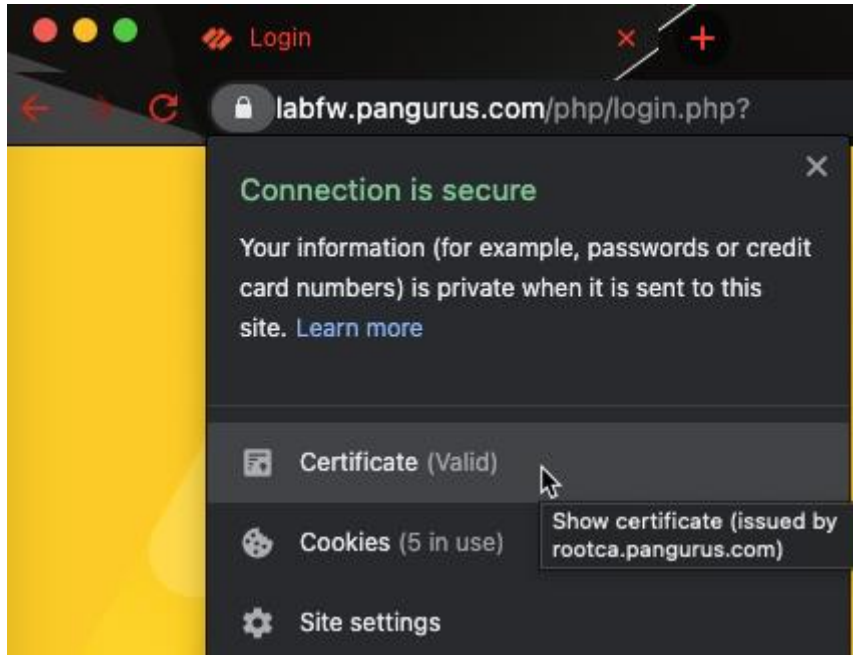
Panorama Settings

En

R

Number of

Interval bet



Minimum Password Complexity ?

Enabled

Password Format Requirements

Minimum Length	8
Minimum Uppercase Letters	1
Minimum Lowercase Letters	1
Minimum Numeric Letters	1
Minimum Special Characters	1
Block Repeated Characters	2
<input type="checkbox"/> Block Username Inclusion (including reversed)	

Functionality Requirements

New Password Differs By Characters	5
<input type="checkbox"/> Require Password Change on First Login	
Prevent Password Reuse Limit	15
Block Password Change Period (days)	0
Required Password Change Period (days)	180
Expiration Warning Period (days)	14
Post Expiration Admin Login Count	1
Post Expiration Grace Period (days)	7

Functionality requirements can be overridden by password profiles

OK Cancel

Administrator ?

Name	EXT-bryan
Authentication Profile	None
<input type="checkbox"/> Use only client certificate authentication (Web)	
Password	••••••••
Confirm Password	••••••••
Password Requirements	
- Minimum Password Length (Count) 8	
<input type="checkbox"/> Use Public Key Authentication (SSH)	
Administrator Type	<input type="radio"/> Dynamic <input checked="" type="radio"/> Role Based
Profile	auditadmin
Password Profile	consultant

Password Profiles ?

Name	consultant
Required Password Change Period (days)	30
Expiration Warning Period (days)	5
Post Expiration Admin Login Count	0
Post Expiration Grace Period (days)	0

OK Cancel

OK Cancel

Admin Role Profile (Read Only)

Name

Description

Web UI | XML API | Command Line | REST API

- Licenses
- Support
- Master Key and Diagnostics
- Policy Recommendation
- Operations
- Privacy
- Validate
- Save
 - Partial Save
 - Save For Other Admins
- Commit
 - Device
 - Commit For Other Admins
- Tasks
- Global
 - System Alarms

Legend: Enable Read Only Disable

Admin Role Profile (Read Only)

Name

Description

Web UI | XML API | Command Line | REST API

- Dashboard
- ACC
- Monitor
 - Logs
 - Traffic
 - Threat
 - URL Filtering
 - WildFire Submissions
 - Data Filtering
 - HIP Match
 - GlobalProtect
 - IP-Tag
 - User-ID
 - Decryption
 - Tunnel Inspection
 - Configuration

Legend: Enable Read Only Disable

Admin Role Profile ?

Name

Description

Web UI | XML API | Command Line | REST API

- Network
 - Interfaces
 - Zones
 - VLANs
 - Virtual Wires
 - Virtual Routers
 - IPSec Tunnels
 - GRE Tunnels
 - DHCP
 - DNS Proxy
 - GlobalProtect
 - QoS
 - LLDP
- Network Profiles
 - GlobalProtect IPSec Crypto
 - IKE Gateways

Legend: Enable Read Only Disable

OK

Cancel

Admin Role Profile ?

Name

Description

Web UI | XML API | Command Line | REST API

- SD-WAN Interface Profile
- Device
- Operations
- Privacy
 - Show Full IP Addresses
 - Show Username In Logs And Reports
 - View PCAP Files
- Validate
- Save
 - Partial Save
 - Save For Other Admins
- Commit
 - Device
 - Commit For Other Admins
- Tasks
- Global

Legend: Enable Read Only Disable

Admin Role Profile ?

Name

Description

Web UI | **XML API** | Command Line | REST API

- Report
- Log
- Configuration
- Operational Requests
- Commit
- User-ID Agent
- IoT Agent
- Export
- Import

Legend: Enable Read Only Disable

Admin Role Profile

Name

Description

Web UI | XML API | **Command Line** | REST API

- None
- None
- superuser
- superreader
- deviceadmin
- devicereader

Admin Role Profile

Name

Description

Web UI | XML API | Command Line | **REST API**

- Objects
- Policies
- Network
 - Aggregate Ethernet Interfaces
 - Ethernet Interfaces
 - VLAN Interfaces
 - Loopback Interfaces
 - Tunnel Interfaces
 - Zones
 - VLANs
 - Virtual Wires
 - Virtual Routers
 - Logical Routers
 - BGP Routing Profiles
 - IPSec Tunnels
 - GRE Tunnels

Legend: Enable Read Only Disable

General Settings



Hostname

Domain

Accept DHCP server provided Hostname

Accept DHCP server provided Domain

Login Banner **WARNING! Access to this device is restricted to those individuals with specific Permissions. If you are not an authorized user, disconnect now. Any attempts to gain unauthorized access will be logged and**

Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile

Time Zone

Locale

Date

Time

Latitude

Longitude

Automatically Acquire Commit Lock

Certificate Expiration Check

Use Hypervisor Assigned MAC Addresses

GTP Security

SCTP Security

Advanced Routing

Tunnel Acceleration

OK

Cancel

Authentication Settings



Authentication Profile

Authentication profile to use for non-local admins. Only RADIUS, TACACS+ and SAML methods are supported.

Authentication Profile(Non-UI)

Authentication Profile to use for non-UI like CLI and API.

Certificate Profile

Idle Timeout (min)

API Key Lifetime (min)

API Keys Last Expired [Expire All API Keys](#)

Failed Attempts

Lockout Time (min)

Max Session Count (number)

Max Session Time (min)

OK

Cancel

Management Interface Settings

IP Type Static DHCP Client

IP Address
 Netmask
 Default Gateway
 IPv6 Address/Prefix Length
 Default IPv6 Gateway
 Speed
 MTU

Administrative Management Services

HTTP HTTPS
 Telnet SSH

Network Services

HTTP OCSP Ping
 SNMP User-ID
 User-ID Syslog Listener-SSL User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES	DESCRIPTION
<input type="checkbox"/> 192.168.27.0/24	

Interface Management Profile

Name

Administrative Management Services

HTTP HTTPS
 Telnet SSH

Network Services

Ping
 HTTP OCSP
 SNMP
 Response Pages
 User-ID
 User-ID Syslog Listener-SSL
 User-ID Syslog Listener-UDP

PERMITTED IP ADDRESSES
192.168.27.0/24
10.0.0.5

Ex. IPv4 192.168.1.1 or 192.168.1.0/24 or IPv6 2001:db8:123:1::1 or 2001:db8:123:1::/64

Local User Database

- Users
- User Groups
- Scheduled Log Export
- Software
- GlobalProtect Client
- Dynamic Updates
- Plugins
- VM-Series
- Licenses
- Support
- Master Key and Diagnostics**

Policy Recommendation

- IoT
- SaaS

Master Key

Stored on HSM

Lifetime

Time for Reminder

Auto Renew With Same Master Key **Disabled**

FIPS CC mode

SAML Identity Provider

Multi Factor Authentication

Local User Database

- Users
- User Groups
- Scheduled Log Export
- Software
- GlobalProtect Client
- Dynamic Updates
- Plugins
- VM-Series
- Licenses
- Support
- Master Key and Diagnostics

Master Key

Stored on HSM

Lifetime

Time for Reminder

Auto Renew With Same Master Key

Start-time for Scheduled Self-test

Cryptographic Algorithms

Software

Run Cryptographic Algorithm Self-test

Run Software Integrity Self-test

Master Key



Master Key

Current Master Key

New Master Key

Confirm New Master Key

Lifetime Days Hours

Ranges from 1 hour to 18250 days.

Time for Reminder Days Hours

Ranges from 1 hour to 365 days.

You must configure a new master key before the current key expires. If the master key expires, the firewall automatically reboots in Maintenance mode. You must then reset the firewall to Factory Default Settings.

Auto Renew Master Key

Auto Renew With Same Master Key Days Hours

Ranges from 1 hour to 730 days.

OK

Cancel

URL Filtering Profile



Name

Description

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

76 items

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Custom URL Categories		
<input type="checkbox"/> custom category *	allow	allow
<input type="checkbox"/> risky sites *	block	block
External Dynamic URL Lists		
<input checked="" type="checkbox"/> MineMeld URLfeed +	alert	block
Pre-defined Categories		

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

OK

Cancel

Anti-Spyware Profile



Name

Description

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions

DNS Policies

10 items

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
External Dynamic Lists			
<input checked="" type="checkbox"/> MineMeld domainfeed	medium	slow	disable
Palo Alto Networks Content			
<input type="checkbox"/> default-paloalto-dns			disable
DNS Security			

DNS Sinkhole Settings

Sinkhole IPv4

Sinkhole IPv6

OK

Cancel

External Dynamic Lists ?

Name:

Create List | **List Entries And Exceptions**

Type: **IP List**

Description: **Predefined IP List**

Source: **Domain List**

Server Authentication: **URL List**

Certificate Profile: **None**

Check for updates: **Daily** at **03:00**

External Dynamic Lists ?

Name:

Create List | **List Entries And Exceptions**

List Entries 1116 items

LIST ENTRIES
<input type="checkbox"/> 113.201.51.0-113.201.51.255
<input type="checkbox"/> 116.79.0.0-116.79.255.255
<input type="checkbox"/> 119.227.224.0-119.227.255.255
<input type="checkbox"/> 120.128.128.0-120.128.191.255
<input type="checkbox"/> 120.128.192.0-120.128.255.255
<input type="checkbox"/> 120.129.0.0-120.129.127.255
<input type="checkbox"/> 120.129.128.0-120.129.255.255

Manual Exceptions 0 items

LIST ENTRIES

MINEMELD DASHBOARD **NODES** CONFIG LOGS ADMIN SYSTEM

NAME	STATUS	INDICATORS	AGED OUT	PROCESSED	PROCESSED
wWhiteListIPv4	MINER STARTED	0	3	TX: 4	PROCESSED: 0 TX: 3
inboundfeedhc	OUTPUT STARTED	1114	0	ADDED: 529 REMOVED: 461	RX: 16137 PROCESSED: 16137 TX: 0
inboundfeedic	OUTPUT STARTED	0	0	ADDED: 0 REMOVED: 0	RX: 16137 PROCESSED: 0 TX: 0
inboundfeedmc	OUTPUT STARTED	0	0	ADDED: 0 REMOVED: 0	RX: 16137 PROCESSED: 0 TX: 0

MINEMELD DASHBOARD **NODES** CONFIG LOGS ADMIN SYSTEM

inboundfeedhc NODE LOGS

STATUS

CLASS: minemeld.ft.redis.RedisSet

PROTOTYPE: stdlib.feedHCGreen

STATE: **STARTED**

FEED BASE URL: https://192.168.27.171/feeds/inboundfeedhc

TAGS:

INDICATORS: 1114

OUTPUT: **DISABLED**

INPUTS: inboundagggregator

MINEMELD DASHBOARD * NODES CONFIG LOGS ADMIN SYSTEM

COMMIT REVERT LOAD IMPORT EXPORT

Search:

NAME	TYPE	PROTOTYPE	INPUTS	OUTPUT
dshield_blocklist	MINER	dshield.block	None	ENABLED
spamhaus_DROP	MINER	spamhaus.DROP	None	ENABLED
spamhaus_EDROP	MINER	spamhaus.EDROP	None	ENABLED
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic	None	ENABLED
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundaggregator	DISABLED
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundaggregator	DISABLED
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundaggregator	DISABLED
inboundaggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wlWhiteListIPv4	ENABLED

enable expert mode add node

1 2 3

MINEMELD DASHBOARD * NODES CO

ADD NODE

NAME

PROTOTYPE

INPUTS

- MINER
- openphish.feed**

OK CANCEL

ADD NODE

NAME: phishinging-feeds-URL

PROTOTYPE: aggregatorURL

INPUTS:

- PROCESSOR
- stdlib.aggregatorURL

OK CANCEL

ADD NODE

NAME: phishinging-feeds-URL

PROTOTYPE: stdlib.aggregatorURL

INPUTS:

- Select input nodes...
- MINER
- cofense
- openphish-miner

ADD NODE

NAME: phishingfeed

PROTOTYPE: feed

INPUTS:

- stdlib.feedLCRedWithValue
- stdlib.feedLCWithValue
- stdlib.feedMCGreen
- stdlib.feedMCGreenWithValue
- stdlib.feedMCRedWithValue
- stdlib.feedMCWithValue
- stdlib.feedRedWithValue
- stdlib.taxiiDataFeed

ADD NODE

NAME: phishingfeed

PROTOTYPE: stdlib.feedMCGreen

INPUTS:

- MINER
- openphish-miner
- PROCESSOR
- phishinging-feeds-URL

PROTOTYPES

Show 50 entries

Search: openphish

NAME	TYPE	INDICATORS	DESCRIPTION
M openphish.feed <small>MINEMELD CORE TEAM</small>	MINER	URL	<p>EXPERIMENTAL</p> <p>openphish OpenPhish launched in June 2014 as a result of a three-year research on phishing detection</p> <p>openphish.feed The free feed</p> <p>TAGS: OSINT</p> <p>ShareLevelGreen ConfidenceMedium</p>

Showing 1 to 1 of 1 entries (filtered from 268 total entries)

MINEMELD DASHBOARD NODES CONFIG

ENGINE STATUS: STOPPING

COMMIT REVERT LOAD IMPORT

Restarting engine, could take minutes. Check [SYSTEM](#)

COMMIT SUCCESSFUL

NAME	TYPE	PROTOTYPE	INPUTS
cofense	MINER	cofense.Intelligence	None

MINEMELD DASHBOARD NODES CONFIG LOGS ADMIN SYSTEM

ADD INDICATOR

Show All entries Search: phi

NAME	TYPE	STATE	INDICATORS	ADD/REM/AO	UPDATES	WITHDRAWS
openphish-miner	MINER	STARTED	1643	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 1643	RX: 0 PROCESSED: 0 TX: 0
phishing-feed	OUTPUT	STARTED	1643	ADDED: 1643 REMOVED: 0	RX: 1643 PROCESSED: 1643 TX: 0	RX: 0 PROCESSED: 0 TX: 0
phishinging-feeds-URL	PROCESSOR	STARTED	1643	ADDED: 0 REMOVED: 0	RX: 1643 PROCESSED: 1643 TX: 1643	RX: 0 PROCESSED: 0 TX: 0

Showing 1 to 3 of 3 entries (filtered from 13 total entries)

MINEMELD DASHBOARD NODES CONFIG LOGS ADMIN SYSTEM

phishing-feed NODE LOGS

STATUS

CLASS	minemeld.ft.redis.RedisSet	OUTPUT	DISABLED
PROTOTYPE	stdlib.feedMCGreen	INPUTS	phishinging-feeds-URL
STATE	STARTED		
FEED BASE URL	https://192.168.27.171/feeds/phishing-feed		
TAGS			
# INDICATORS	1643		

External Dynamic Lists ?

Name

Create List | List Entries And Exceptions

Type

Description

Source

Server Authentication

Certificate Profile

Check for updates

at

Chapter 6: Anti-Phishing with User Credential Detection

URL Filtering Profile ?

Name

Description

Categories | [URL Filtering Settings](#) | **[User Credential Detection](#)** | [HTTP Header Insertion](#) | [Inline ML](#)

User Credential Detection

Disabled ▼

- Disabled
- Use IP User Mapping
- Use Domain Credential Filter
- Use Group Mapping

Generate Certificate ?

Certificate Type Local SCEP

Certificate Name

Common Name
IP or FQDN to appear on the certificate

Signed By ▼

Certificate Authority

Block Private Key Export

OCSF Responder

^ Cryptographic Settings

Algorithm ▼

Number of Bits ▼

Digest ▼

Expiration (days)

Certificate Attributes

<input type="checkbox"/>	TYPE	VALUE
<input type="checkbox"/>	Host Name = "DNS" from Subject Alternative Name (SAN) field	decrypt.pangurus.com
<input type="checkbox"/>	Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailA...	decrypt@pangurus.com

+ Add - Delete

Generate Certificate ?

Certificate Type Local SCEP

Certificate Name

Common Name
IP or FQDN to appear on the certificate

Signed By

Certificate Authority
 Block Private Key Export

OCSF Responder

Cryptographic Settings

Algorithm

Number of Bits

Digest

Expiration (days)

Certificate Attributes

<input type="checkbox"/>	TYPE	VALUE
<input type="checkbox"/>	Email = "emailAddress" part of "Subject" CN filed (CN=CommonName/emailA...	helpdesk@pangurus.com

Device Certificates | Default Trusted Certificate Authorities

7 items → X

NAME	SUBJECT	ISSUER	CA	K...	EXPIRES	STA...	ALG...	USAGE
untrustcert	CN = untrustcert.pangurus.com	CN = untrustcert.pangurus.com	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 15 23:35:08 2022 GMT	valid	RSA	Forward Untrust Certif...
PANgurus HIVE	DC = com, DC = pangurus, CN = pan...	DC = com, DC = pangurus, CN = pa...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Nov 30 22:30:36 2030 GMT	valid	RSA	
Manageme...	DC = com, DC = pangurus, CN = Use...	DC = com, DC = pangurus, CN = pa...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 4 21:55:39 2022 GMT	valid	Ellipt...	
DecryptCert	CN = decrypt.pangurus.com, emailAd...	DC = com, DC = pangurus, CN = pa...	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mar 15 23:06:51 2023 GMT	valid	RSA	Forward Trust Certificate

Certificate information ?

Name

Subject

Issuer

Not Valid Before

Not Valid After

Algorithm

Certificate Authority

Forward Trust Certificate
 Forward Untrust Certificate
 Trusted Root CA

st Login Time: 03/15/2023

Tasks | Language | paloalto

Decryption Profile ?

Name

SSL Decryption | No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | SSL Protocol Settings

Server Certificate Verification

- Block sessions with expired certificates
- Block sessions with untrusted issuers
- Block sessions with unknown certificate status
- Block sessions on certificate status check timeout
- Restrict certificate extensions [Details](#)
- Append certificate's CN value to SAN extension

Unsupported Mode Checks

- Block sessions with unsupported versions
- Block sessions with unsupported cipher suites
- Block sessions with client authentication

Failure Checks

- Block sessions if resources not available
- Block sessions if HSM not available
- Block downgrade on no resource

Client Extension

- Strip ALPN

Decryption Profile ?

Name

SSL Decryption | No Decryption | SSH Proxy

SSL Forward Proxy | SSL Inbound Inspection | **SSL Protocol Settings**

Protocol Versions

Min Version v

Max Version v

Key Exchange Algorithms

RSA DHE ECDHE

Encryption Algorithms

3DES AES128-CBC AES128-GCM CHACHA20-POLY1305

RC4 AES256-CBC AES256-GCM

Authentication Algorithms

MD5 SHA1 SHA256 SHA384

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

Decryption Profile ?

Name

SSL Decryption | **No Decryption** | SSH Proxy

Server Certificate Verification

- Block sessions with expired certificates
- Block sessions with untrusted issuers

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Check boxes to block those sessions instead.

Decryption Policy Rule



General | **Source** | Destination | Service/URL Category | Options

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	any	any
<input type="checkbox"/> SOURCE_ZONE ^	<input type="checkbox"/> SOURCE_ADDRESS ^	<input type="checkbox"/> SOURCE_USER ^	<input type="checkbox"/> SOURCE_DEVICE ^
<input type="checkbox"/> trust			

General | Source | **Destination** | Service/URL Category | Options

<input type="checkbox"/> Any	<input checked="" type="checkbox"/> Any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> DESTINATION_ZONE ^	<input type="checkbox"/> DESTINATION_ADDRESS ^	<input type="checkbox"/> DESTINATION_DEVICE ^
<input type="checkbox"/> untrust		

General | Source | Destination | **Service/URL Category** | Options

any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SERVICE ^	<input type="checkbox"/> URL_CATEGORY ^

General | Source | Destination | Service/URL Category | **Options**

Action No Decrypt Decrypt

Type SSL Forward Proxy

Decryption Profile decrypt

Log Settings

Log Successful SSL Handshake

Log Unsuccessful SSL Handshake

Log Forwarding default

OK Cancel

Palo Alto Networks User-ID Agent Setup



Server Monitor Account | Server Monitor | Client Probing | Cache | Syslog Filters | Ignore User List

Username pangurus\servitor

Domain's DNS Name pangurus.com

Password ●●●●●●

Confirm Password ●●●●●●

Kerberos Server Profile kerberos

OK Cancel

Palo Alto Networks User-ID Agent Setup



Server Monitor Account | **Server Monitor** | Client Probing | Cache | Syslog Filters | Ignore User List

Windows Server Monitoring

Enable Security Log

Server Log Monitor Frequency (sec)

Enable Session

Server Session Read Frequency (sec)

Novell eDirectory Monitoring

Novell eDirectory Query Interval (sec)

Syslog Listener Settings

Syslog Service Profile

OK

Cancel

Palo Alto Networks User-ID Agent Setup



Server Monitor Account | Server Monitor | **Client Probing** | Cache | Syslog Filters | Ignore User List

Enable Probing

Probe Interval (min)

OK

Cancel

Palo Alto Networks User-ID Agent Setup



Server Monitor Account | Server Monitor | Client Probing | **Cache** | Syslog Filters | Ignore User List

Enable User Identification Timeout

User Identification Timeout (min)

Allow matching usernames without domains

OK

Cancel

User Identification Monitored Server

Name:

Description:

Enabled

Type:

Transport Protocol:

Network Address:

User Identification Monitored Server

Name:

Description:

Enabled

Type:

Transport Protocol:

Network Address:

Palo Alto Networks User-ID Agent Setup

Domain's DNS Name: pangurus.com

Kerberos Server Profile: kerberos

Enable Security Log:

Server Log Monitor Frequency (sec): 2

Enable Session:

Server Session Read Frequency (sec): 10

Novell eDirectory Query Interval (sec): 30

Syslog Service Profile

Enable Probing:

Probe Interval (min): 20

Enable User Identification Timeout:

User Identification Timeout (min): 900

Allow matching usernames without domains:

Server Monitoring

<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input type="checkbox"/>	ActiveDirectory	<input checked="" type="checkbox"/>	Microsoft Active Directory	hive.pangurus.com	Connected

Zone

Name

Log Setting

Type

- INTERFACES ^
- ethernet1/2

User Identification ACL

Enable User Identification

INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

URL Filtering Profile ?

Name

Description

Categories | URL Filtering Settings | **User Credential Detection** | HTTP Header Insertion | Inline ML

User Credential Detection

Use IP User Mapping

Log Severity

Valid Username Detected Log Severity

URL Filtering Profile ?

Name

Description

Categories | URL Filtering Settings | **User Credential Detection** | HTTP Header Insertion | Inline ML

74 items

<input type="checkbox"/> CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
Custom URL Categories		
<input type="checkbox"/> updates *	allow	block
<input type="checkbox"/> corp sites *	allow	allow
Pre-defined Categories		
<input type="checkbox"/> auctions	allow	continue
<input type="checkbox"/> abortion	allow	block
<input type="checkbox"/> abused-drugs	block	block

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

NAME	Source		Destination		APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
	ZONE	USER	ZONE						
1 ssl	trust	any	untrust	any	application...	Allow			
2 intrazone-default	any	any	(intrazone)	any	any	Allow	URL Filtering Profile: URLfiltering		
3 interzone-default	any	any	any	any	any	Deny	none	none	

The screenshot shows a web browser window with two tabs. The active tab is titled 'Login' and shows the URL 'https://seattle.pangurus.com/php/login.php'. The page content includes a login form with a username field containing 'reaper', a password field with masked characters, and a 'Log In' button. A warning message at the bottom of the page reads: 'WARNING! Access to this device is restricted to specific Permissions. If you are not an authorized user, any attempts to gain unauthorized access will be blocked.' A second browser window is overlaid on top, displaying a security warning: 'Suspected Credential Phishing Detected'. The warning text states: 'Username and/or password submission to the page you are trying to access has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.' Below the warning, it lists: 'User: pangurus.com\reaper', 'URL: seattle.pangurus.com/php/login.php?', and 'Category: corp sites'.

LDAP Server Profile ?

Profile Name:

Administrator Use Only

Server List

NAME	LDAP SERVER	PORT
ldapsrvr	192.168.27.7	636

+ Add - Delete

Enter the IP address or FQDN of the LDAP server

Server Settings

Type:

Base DN:

Bind DN:

Password:

Confirm Password:

Bind Timeout:

Search Timeout:

Retry Interval:

Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

Group Mapping



Name

Server Profile | **User and Group Attributes** | Group Include List | Custom Group

Server Profile Update Interval

Domain Setting

User Domain

Group Objects

Search Filter

Object Class

User Objects

Search Filter

Object Class

- Enabled
- Fetch list of managed devices

OK

Cancel

Group Mapping



Name

Server Profile | **User and Group Attributes** | Group I

User Attributes

NAME	DIRECTORY ATTRIBUTE
Primary Username	sAMAccountName
E-Mail	mail
Alternate Username 1	userPrincipalName
Alternate Username 2	
Alternate Username 3	

Group Attributes

NAME	DIRECTORY ATTRIBUTE
Group Name	name
Group Member	member
E-Mail	mail

Group Mapping



Name

Server Profile | User and Group Attributes | **Group Include List** | Custom Group

Available Groups

-
- ×
- cn=enterprise admins
- cn=enterprise key admins
- cn=enterprise read-only domain controller
- cn=group policy creator owners
- cn=key admins
- cn=locals**
- cn=protected users
- cn=ras and ias servers
- cn=read-only domain controllers

Included Groups

cn=locals,cn=users,DC=pangurus,DC=com

OK

Cancel

URL Filtering Profile



Name URLfiltering

Description

Categories | URL Filtering Settings | **User Credential Detection** | HTTP Header Insertion | Inline ML

User Credential Detection

Use Group Mapping

Group Mapping Settings

GroupMapping

GroupMapping

Log Severity

Valid Username Detected Log Severity critical

OK

Cancel

facebook

Connect with friends and the world around you on Facebook.

tom

.....

Log In

[Forgot Password?](#)

Suspected Credential Phishing Detected

Username and/or password submission to the page you are trying to access has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: pangurus\reaper

URL: www.facebook.com/login/?privacy_mutation_token=eyJ0eXBIIjowLCJjcmVhdGlub90aW1IjoxNjE2MzYzNDM5LCJyWxcsc2I0ZV9pZCI6

Category: social-networking

facebook

Connect with friends and the world around you on Facebook.

reaper

.....

Log In

[Forgot Password?](#)

Suspected Credential Phishing Detected

Username and/or password submission to the page you are trying to access has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: pangurus\reaper

URL: www.facebook.com/login/?privacy_mutation_token=eyJ0eXBIIjowLCJjcmVhdGlub90aW1IjoxNjE2MzYzNDg5LCJyWxcsc2I0ZV9pZCI6

Category: social-networking

facebook

Connect with friends and the world around you on Facebook.

reaper@thisisreallynotmydomain.com

.....

Log In

[Forgot Password?](#)

Suspected Credential Phishing Detected

Username and/or password submission to the page you are trying to access has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: pangurus\reaper

URL: www.facebook.com/login/?privacy_mutation_token=eyJ0eXBIIjowLCJjcmVhdGlub90aW1IjoxNjE2MzYzNDg5LCJyWxcsc2I0ZV9pZCI6

Category: social-networking

Software Updates

Please Select:

User Identification Agent

Search

VERSION	RELEASE DATE	RELEASE NOTES	DOWNLOAD
10.0.3-10	03/01/2021	User_ID_Agent-10.0.3-RN.pdf	UaCredInstall64-10.0.3-10.msi

Palo Alto Networks User ID Agent Setup

Authentication Server Monitor Client Probing Cache Agent Service eDirectory Syslog Credentials

User name for Active Directory: servitor@PANGURUS.COM

Password: [REDACTED]

Palo Alto Networks User ID Agent Setup

Authentication Server Monitor Client Probing Cache Agent Service eDirectory Syslog Credentials

Windows Server Monitoring

Security Log Monitor Frequency (seconds): 1

Enable Security Log Monitor

Enable Server Session Read

Palo Alto Networks User ID Agent Setup

Authentication Server Monitor Client Probing Cache Agent Service eDirectory Syslog Credentials

Enable WMI Probing

Enable NetBIOS Probing

Probing Interval (minutes): 20

Palo Alto Networks User ID Agent Setup

Authentication Server Monitor Client Probing Cache Agent Service eDirectory Syslog Credentials

User-ID Service TCP Port: 5007

User-ID XML API TCP Port: 5006

Enable User-ID XML API

OK Cancel

Palo Alto Networks User ID Agent Setup



Authentication Server Monitor Client Probing Cache Agent Service eDirectory Syslog **Credentials**

Import from File

Import from UserID Credential Agent

Create credential filter for configured User Group DNS

OK Cancel

Palo Alto Networks User-ID Agent



File Help

Save Commit Exit

User Identification
Setup
Discovery
VM Information Sources
Monitoring
Logs
Server Certificate
MDM Integration
Setup
Mobile Devices

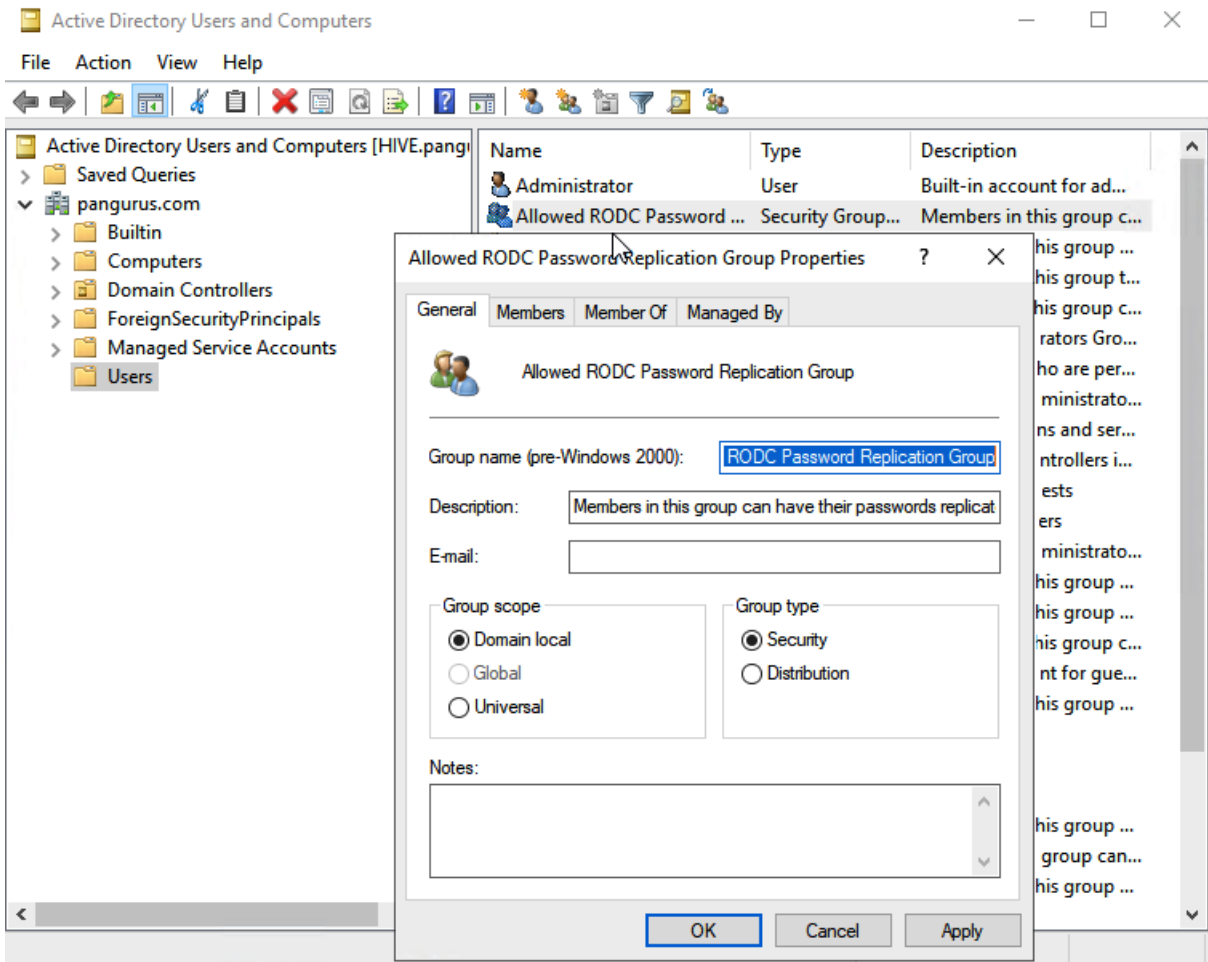
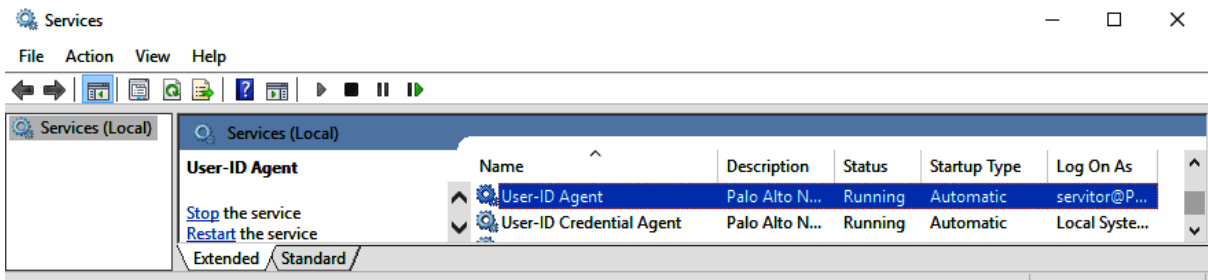
Servers

Name	Type	Network Address
<input type="checkbox"/> hive.pangurus.com	active-directory	192.168.27.7
<input type="checkbox"/> hive.pangurus.com	active-directory	10.0.0.7
<input type="checkbox"/> hive.pangurus.com	active-directory	192.168.0.2
<input type="checkbox"/> hive.pangurus.com	active-directory	192.168.1.2

Add Edit Delete **Auto Discover**

Include / Exclude list of configured networks

Name	Discovery	Network Address



Add a Data Redistribution Agent



Name

Enabled

Add an Agent Using Serial Number Host and Port

Host

LDAP Proxy

Port

Collector Name

Collector Pre-Shared Key

Confirm Collector Pre-Shared Key

Data type IP User Mappings HIP

IP Tags

Quarantine List

User Tags

OK

Cancel

URL Filtering Profile



Name

Description

Categories | URL Filtering Settings | **User Credential Detection** | HTTP Header Insertion | Inline ML

User Credential Detection

Use Domain Credential Filter

Log Severity

Valid Username Detected Log Severity

OK

Cancel

Suspected Credential Phishing Detected

Username and/or password submission to the page you are trying to access has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: pangurus\reaper
 URL: 192.168.27.13/php/login.php
 Category: private-ip-addresses

Same Username and Password as corporate

Same Username but different password

PANgurus DASHBOARD

General Information

Device Name	LABFW-scattle
MGT IP Address	192.168.27.13
MGT Netmask	255.255.255.0
MGT Default Gateway	192.168
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	
MGT IPv6 Default Gateway	
MGT MAC Address	
Model	
Serial #	
CPU ID	
UUID	
VM Cores	2

Logged In Admins

Admin	From	Client	Session Start	Idle For
reaper	192.168.27.108	Web	03/24 21:56:35	00:00:59s
reaper	192.168.27.233	Web	03/24 22:39:51	00:00:00s
paloalto	192.168.27.233	Web	03/24 22:36:40	00:01:44s
reaper	192.168.27.108	CLI	03/24 22:04:17	00:10:21s
paloalto	192.168.27.233	Web	03/24 22:27:33	00:07:57s
reaper	192.168.27.116	Web	03/24 21:50:06	00:25:39s

Config Logs

Command	Path
commit	
set	config paloalt
commit	
edit	vsys vs3 profiles URLfilt domain
commit	
move	vsys rule rules

Data Logs

No data available.

reaper Logout | Last Login Time: 03/24/2021 22:39:19 | Session Expire Time: 04/23/2021 23:39:51 | Tasks | Language

```
reaper@LABFW> show user credential-filter statistics
```

Configuration		Delete Pending		Last DP Pushed (sec)		Last change check (sec)
GM	BF	GM	BF	GM	BF	
No	Yes	No	No	88792	4551	37

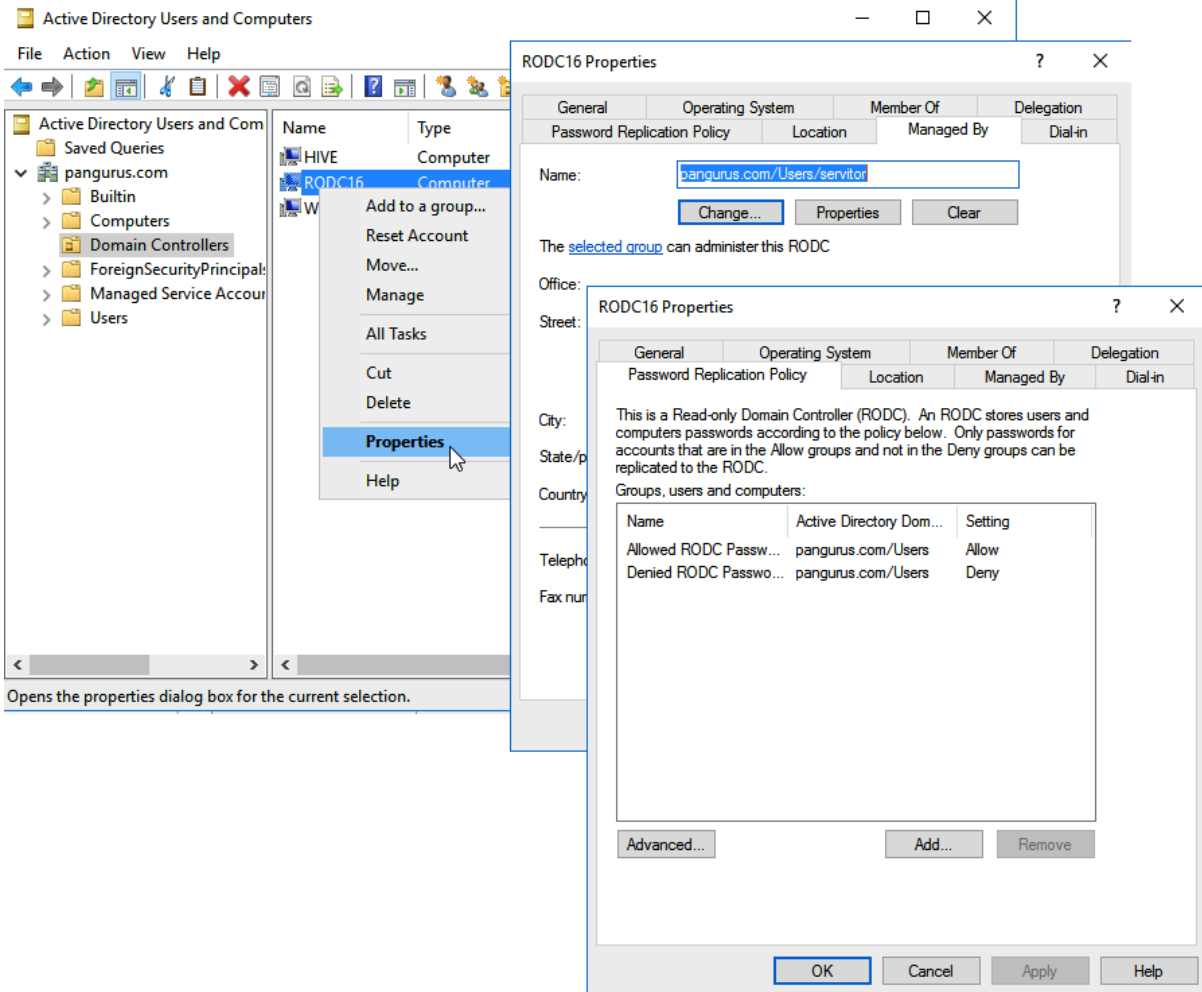
```
VSYS ID Group Mapping Domain Credential
```

VSYS ID	Group Mapping	Domain	Credential	Size (KB)	Digest
1	2	7	2	f4f28fe3485ba0aac3e6d57bda5540b4	

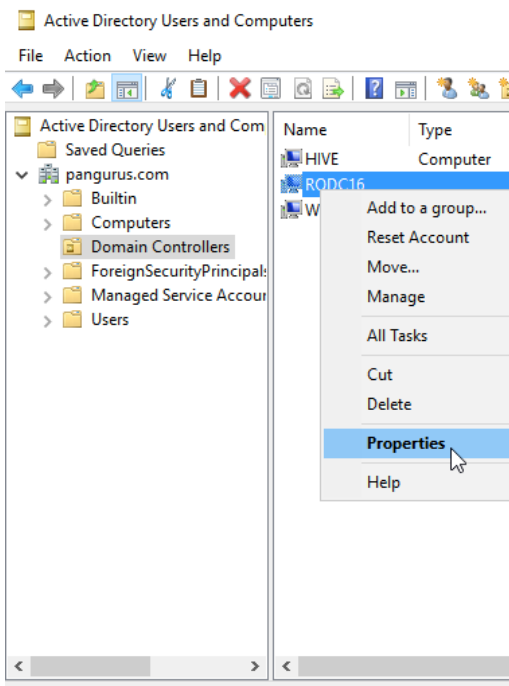

```

reaper@LABFW> show user user-id-agent state RODC
Agent: RODC(vsys: vsys1) Host: 192.168.27.9(192.168.27.9):5007
Status : conn:idle
Version : 0x5
SSL config : Default certificate
num of connection tried : 1
num of connection succeeded : 1
num of connection failed : 0
num of status msgs rcvd : 1161
num of request of status msgs sent : 1161
num of request of ip mapping msgs sent : 0
num of request of new ip mapping msgs sent : 0
num of request of all ip mapping msgs sent : 1
num of user ip mapping msgs rcvd : 16
num of ip msgs rcvd but failed to proc : 0
num of user ip mapping add entries rcvd : 22
num of user ip mapping del entries rcvd : 4
num of bloomfilter requests sent : 4
num of bloomfilter response received : 4
num of bloomfilter response failed to proc : 0
num of bloomfilter resize requests sent : 0
Last heard(seconds ago) : 4
Message State:
Job ID : 0
Sent messages : 1167
Rcvd messages : 1182
Rcvd rate(msgs/s) : 0
Rcvd peak rate(msgs/s) : 1
Lost messages : 0
Failed to send messages : 0
Failed to enqueue messages : 0
Queued sending msgs with priority 0 : 0
Queued sending msgs with priority 1 : 0
Queued rcvring msgs with priority 0 : 0
Credential Enforcement Status : In Sync
Last BF digest received(seconds ago) : 4
Last BF request sent(seconds ago) : 5129
Last BF updated(seconds ago) : 5129
Current BF digest : f4f28fe3485ba0aac3e6d57bda5540b4
reaper@LABFW>

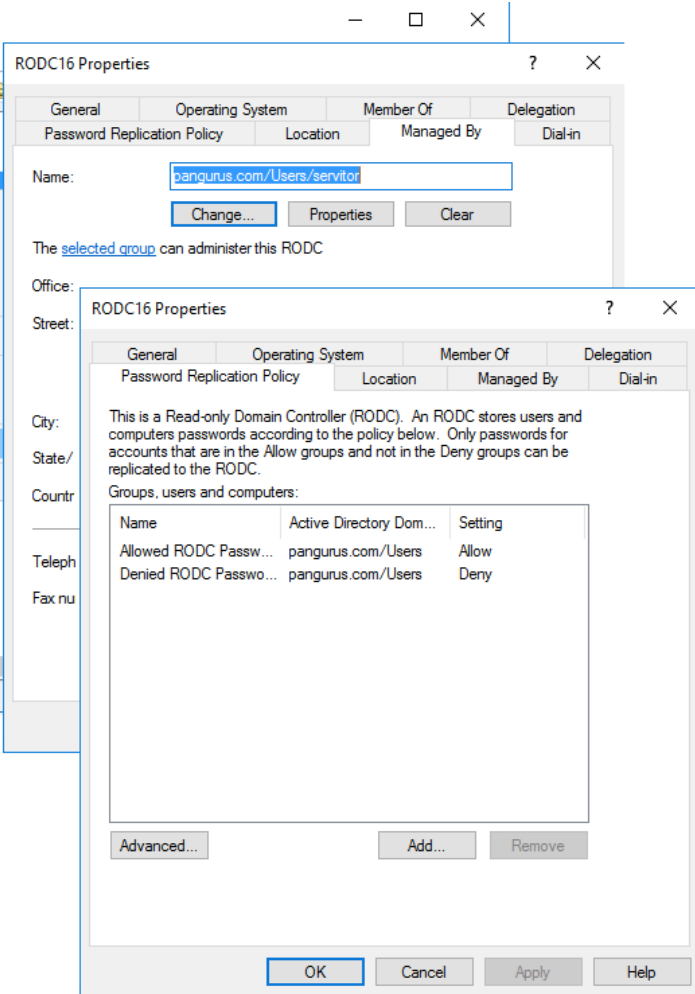
```



Opens the properties dialog box for the current selection.



Opens the properties dialog box for the current selection.



Chapter 7: Practical Troubleshooting

User Mapping | Connection Security | Terminal Server Agents | Group Mapping Settings | Authentication Portal Settings

Server Monitoring					
<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input type="checkbox"/>	hive.pangurus.com	<input checked="" type="checkbox"/>	Microsoft Active Directory	hive.pangurus.com	Connected

Agents | Clients | Collector Settings | Include/Exclude Networks

🔍 2 items → ×

<input type="checkbox"/>	NAME	ENABLED	HOST	PORT	LDAP PROXY	IP USER MAPPINGS	QUARANTI... LIST	USER TAGS	CONNECTED
<input type="checkbox"/>	AD	<input checked="" type="checkbox"/>	192.168.27.7	5007	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	yes
<input type="checkbox"/>	RODC	<input checked="" type="checkbox"/>	192.168.27.9	5007	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	no

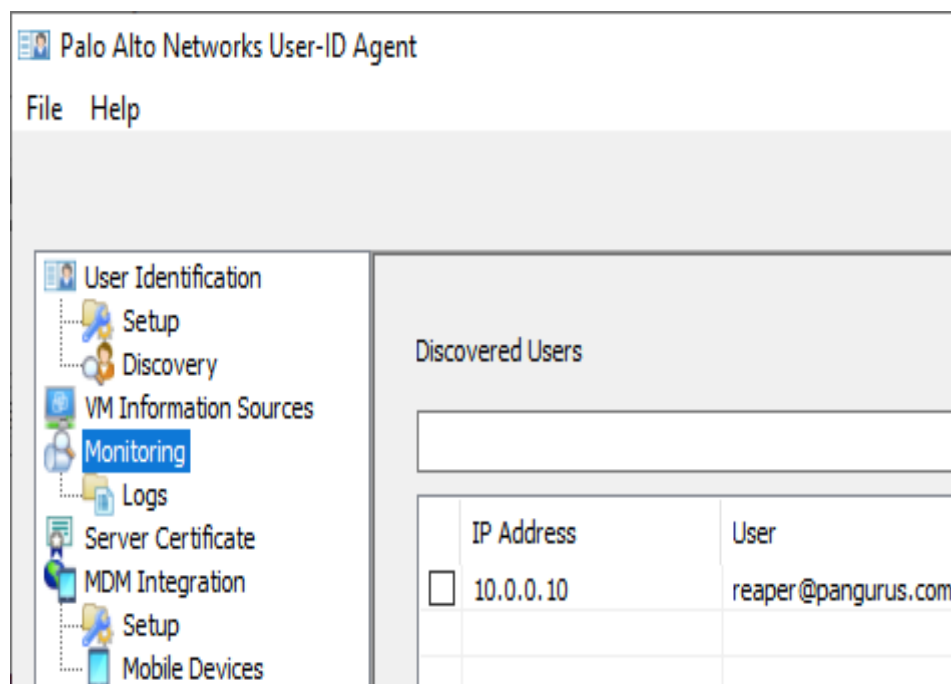
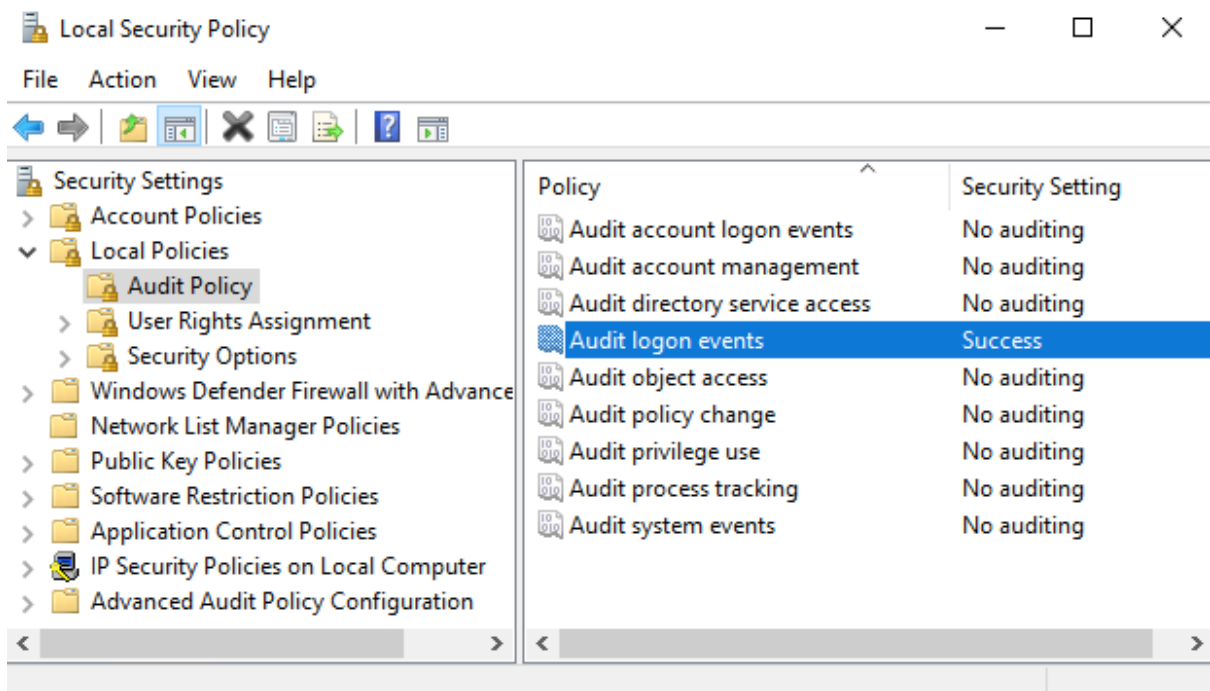
Server Monitoring					
<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input checked="" type="checkbox"/>	ActiveDirectory	<input checked="" type="checkbox"/>	Microsoft Active Directory	hive.pangurus.com	Kerberos error

Server Monitoring					
<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input type="checkbox"/>	ActiveDirectory	<input checked="" type="checkbox"/>	Microsoft Active Directory	hive.pangurus.com	Access denied

Server Monitoring					
<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input type="checkbox"/>	ActiveDirectory	<input checked="" type="checkbox"/>	Microsoft Active Directory	hive.pangurus.com	Not connected

Server Monitoring					
<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS	STATUS
<input type="checkbox"/>	ActiveDirectory	<input checked="" type="checkbox"/>	Microsoft Active Directory	hive.pangurus.com	Kerberos error

<input type="checkbox"/>	NAME	ENABLED	HOST	PORT	LDAP PROXY	IP USER MAPPINGS	QUARANTINE LIST	CONNECTED
<input type="checkbox"/>	RODC	<input checked="" type="checkbox"/>	192.168.27.9	5007	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	no
<input type="checkbox"/>	AD	<input checked="" type="checkbox"/>	192.168.27.7	5007	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	no



Zone

Name

Log Setting

Type

INTERFACES ^

ethernet1/2

+ Add - Delete

User Identification ACL

Enable User Identification

INCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will be identified.

EXCLUDE LIST ^

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

User Mapping
Connection Security

Enable User Identification

User Identification

Allow matching username

Server Monitoring

<input type="checkbox"/>	NAME	ENABLED
<input type="checkbox"/>	ActiveDirectory	<input checked="" type="checkbox"/>

+ Add - Delete Discover

Custom Include/Exclude Network Sequence

INCLUDE EXCLUDE NETWORK

LabNet

block 10-8

localnet

+ Add - Delete ↑ Move Up ↓ Move Down

Include/Exclude Networks

<input type="checkbox"/>	NAME	ENABLED	TYPE	NETWORK ADDRESS
<input type="checkbox"/>	block 10-8	<input checked="" type="checkbox"/>	Exclude	10.0.0.0/8
<input type="checkbox"/>	LabNet	<input checked="" type="checkbox"/>	Include	10.0.0.0/24
<input type="checkbox"/>	localnet	<input checked="" type="checkbox"/>	Include	192.168.27.0/24

+ Add - Delete Custom Include/Exclude Network Sequence

Save Commit Exit

- User Identification
 - Setup
 - Discovery
- VM Information Sources
- Monitoring
- Logs
- Server Certificate
- MDM Integration
 - Setup
- Mobile Devices

Servers

	Name	Type	Network Address
<input type="checkbox"/>	hive.pangurus.com	active-directory	192.168.27.7
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Add Edit Delete Auto Discover

Include / Exclude list of configured networks

	Name	Discovery	Network Address
<input checked="" type="checkbox"/>	block 10/8	Exclude	10.0.0.0/8
<input type="checkbox"/>	lab	Include	10.0.0.0/24
<input type="checkbox"/>			
<input type="checkbox"/>			

Add Edit De Move Up Move Down

Palo Alto Networks User-ID Agent Setup



Server Monitor Account | Server Monitor | Client Probing | Cache | Syslog Filters | **Ignore User List**

Search: 2 items → ×

<input type="checkbox"/>	IGNORE USER ^
<input type="checkbox"/>	adm_tom
<input type="checkbox"/>	svc_backup

+ Add - Delete

OK Cancel

Palo Alto Networks User-ID Agent Setup



Server Monitor Account | Server Monitor | **Client Probing** | Cache | Syslog Filters | Ignore User List

Enable Probing

Probe Interval (min)

Palo Alto Networks User ID Agent Setup



Authentication | Server Monitor | **Client Probing** | Cache | Agent Service | eDirectory | Syslog

Enable WMI Probing

Enable NetBIOS Probing

Probing Interval (minutes)

OK

Cancel

OK

Cancel

Palo Alto Networks User-ID Agent Setup



Server Monitor Account | Server Monitor | Client Probing | **Cache** | Syslog Filters | Ignore User List

Enable User Identification Timeout

User Identification Timeout (min)

Allow matching usernames without domains

Palo Alto Networks User ID Agent Setup



Authentication | Server Monitor | Client Probing | **Cache** | Agent Service | eDirectory | Syslog

Enable User Identification Timeout

User Identification Timeout (minutes)

OK

Cancel

OK

Cancel

LDAP Server Profile



Profile Name

Administrator Use Only

Server List

NAME	LDAP SERVER	PORT
ldapsrvr	192.168.27.7	636

Enter the IP address or FQDN of the LDAP server

Server Settings

Type

Base DN

Bind DN

Password

Confirm Password

Bind Timeout

Search Timeout

Retry Interval

Require SSL/TLS secured connection

Verify Server Certificate for SSL sessions

OK

Cancel

Group Mapping



Name

Server Profile | User and Group Attributes | Group Include List | Custom Group

Server Profile

Update Interval

Domain Setting

User Domain

Group Objects

Search Filter

Object Class

User Objects

Search Filter

Object Class

Enabled

Fetch list of managed devices

OK

Cancel

NAME	Original Packet						Translated Packet	
	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
hide-nat	trust lab	untrust	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	none
inbound 1	untrust	untrust	ethernet1/1	any	192.168.27.220	any	none	destination-translation address: 10.0.0.7
inbound static NAT	untrust	untrust	ethernet1/1	any	198.51.100.1	any	none	destination-translation address: 10.0.0.7

Source Translation ?

Translation Type:

Address Type:

Interface:

IP Address:

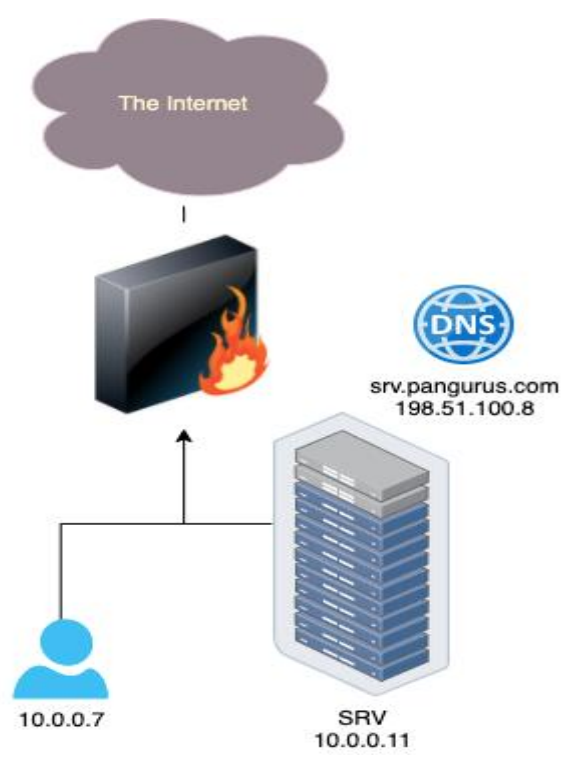
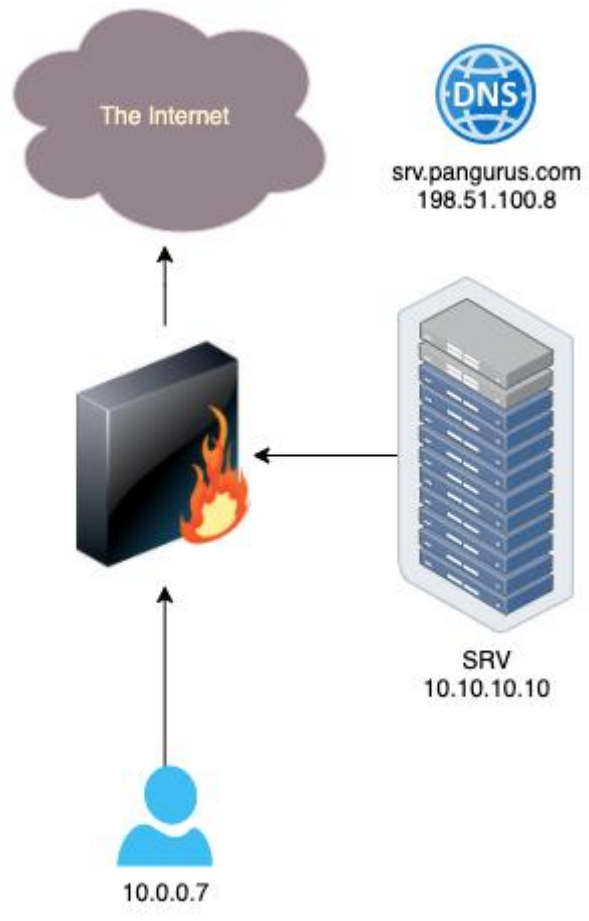
Source Translation ?

Translation Type:

Address Type:

- TRANSLATED ADDRESS ^
 - 192.168.27.220/32
 - 198.51.100.1/32
-

NAME	Original Packet						Translated Packet	
	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION TRANSLATION
1 hide-nat	trust lab	untrust	ethernet1/1	any	any	any	dynamic-ip-and-port ethernet1/1	none
2 inbound static NAT	untrust	untrust	ethernet1/1	any	198.51.100.7/24	any	none	destination-translation address: 10.0.0.7/24

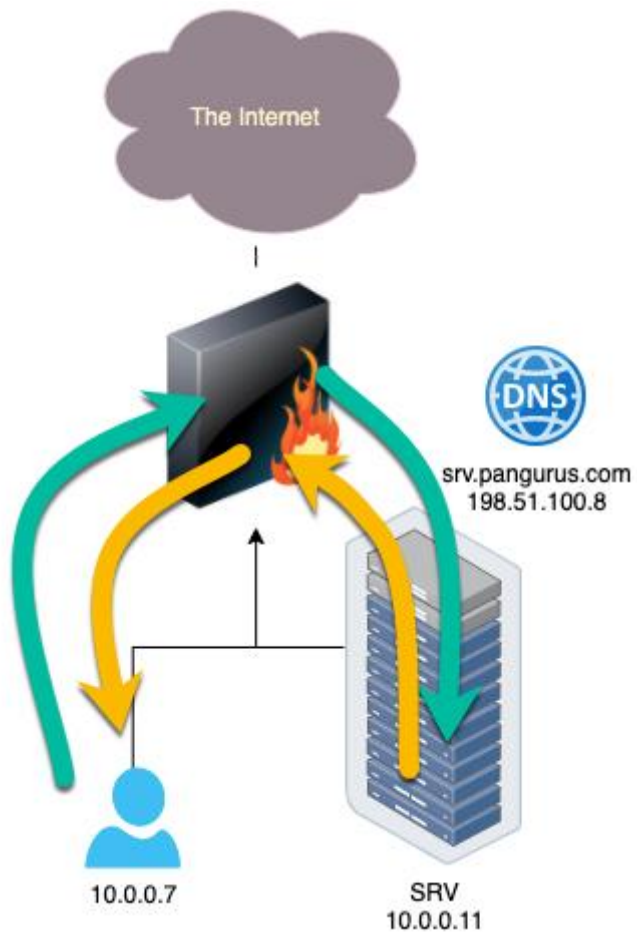


*Ethernet1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0...	10.0.0.7	198.51.100.8	TCP	66	53455 → 23 [SYN, ECN, CWR] Seq=0 Win=64240 Len=
2	0.0...	10.0.0.7	10.0.0.11	TCP	66	53455 → 23 [SYN, ECN, CWR] Seq=0 Win=64240 Len=
3	0.0...	10.0.0.11	10.0.0.7	TCP	60	23 → 53455 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
4	3.0...	10.0.0.7	198.51.100.8	TCP	66	[TCP Retransmission] 53455 → 23 [SYN, ECN, CWR]
5	3.0...	10.0.0.7	10.0.0.11	TCP	66	[TCP Retransmission] 53455 → 23 [SYN, ECN, CWR]
6	3.0...	10.0.0.11	10.0.0.7	TCP	60	23 → 53455 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



PANgurus DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK **DEVICE**

Support

Contact Click the contact link at right.

ExpiryDate July 24, 2021

Level Premium

Description 24 x 7 phone support; advanced replacement hardware service

[Activate support using authorization code](#)

Links

[Contact Us](#)

[Support Home](#)

[Manage Cases](#)

[Register Device](#)

Tech Support File

[Generate Tech Support File](#)

Last generated: 2021/04/30 00:56:11

[Download Tech Support File \(68.6M\)](#)

Stats Dump File

[Generate Stats Dump File](#)

Last generated: 2021/02/16 11:11:57

[Download Stats Dump File \(2.6K\)](#)

Core Files

No Core Files

Production Alerts

No Production Alerts

Application and Threat Alerts

No Application and Threat Alerts

reaper | Logout | Last Login Time: 04/28/2021 22:30:09 | Session Expire Time: 05/30/2021 00:34:09 | Tasks | Language **paloalto**

Account Management

Members

Create New User

Manage Users

Wildfire Users

Groups

Name	Email	Roles	Desc
Tom Piens	reaper@pangurus.com	Super User ASC User Bulk Registration CSSP User BPA User Domain Administrator Cloud Product	

Current Account: ▼

Quick Actions

Tools

PAN-DB URL Categorization

ASC Scorecard

ASC Scorecard 2.0

Best Practice Assessment

BEST PRACTICE ASSESSMENT (BPA) HISTORY

+ Generate New BPA

Search by Device Name, Serial Number, or TSF Name

DEVICE NAME	SERIAL NUMBER	MODEL/ PAN OS VERSION	DATE GENERATED (UTC+02:00)	TSF NAME/ DATE (UTC+02:00)
HOBO-PA1	00705100	PA-VM 9.1	2020-10-13 11:05	20201013_1100_techsupport.tgz 2020-10-13 03:59

Feedback

<input type="checkbox"/>	ZONE	DEVICE GROUP	CLASSIFICATION
<input type="checkbox"/>	internal3	vsys1	DMZ
<input type="checkbox"/>	internal	vsys1	Users
<input type="checkbox"/>	internal2	vsys1	DMZ
<input type="checkbox"/>	external	vsys1	Internet

- Perimeter
- Internet**
- DMZ
- 3rd Party/Vendor
- Internal Core
- Users
- IT Infrastructure
- Out-of-Band Management

If you need to review or edit your Architecture Classifications, please go BACK now.

Otherwise, you are now ready to generate your Best Practice Assessment Report.

Click on "Generate & Download Report" button to view your summary and download the detailed report.

Your current industry is selected by default. To compare your BPA results against a particular industry, please make a selection from the drop down below.

**Default industry is based on the Dun & Bradstreet database.*

High Technology ▼

Generate & Download Report

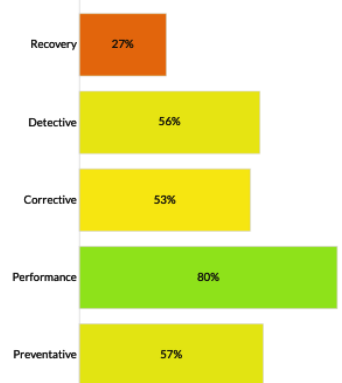
< [Best Practice Summary](#) Security Profile Adoption Application & User Control Adoption Logging & >

Capability & Control Category

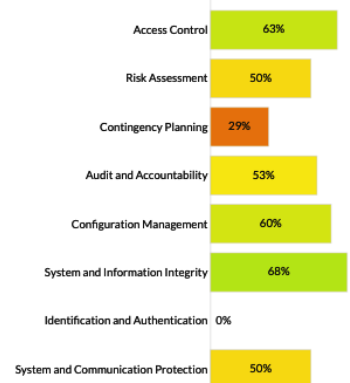
Class Summary

CIS Critical Security Controls

Capability Summary



Control Category Summary



Best Practice Checks - Strata - I -PA2 2021-04-26 v5.7.0

Feature	Location	Name	Check ID	Check Name	Message
Network > Zones	vsys1	internal	212	Enable Packet Buffer Protection	It is recommended to enable Packet Buffer Protection.
Network > Zones	vsys1	internal	60	Zone Protection Profile Applied to Zone	Zone should have a zone protection profile applied
Network > Zones	vsys1	internal2	212	Enable Packet Buffer Protection	It is recommended to enable Packet Buffer Protection.
Network > Zones	vsys1	internal2	60	Zone Protection Profile Applied to Zone	Zone should have a zone protection profile applied
Network > Zones	vsys1	internal3	212	Enable Packet Buffer Protection	It is recommended to enable Packet Buffer Protection.
Network > Zones	vsys1	internal3	60	Zone Protection Profile Applied to Zone	Zone should have a zone protection profile applied
Network > Zone Protection		ZP_external	85	Flood Protection	Flood Protection > ICMP / ICMPv6 / Other IP / UDP should be
Network > Zone Protection		ZP_external	87	Packet Based Attack Protection	IP Option Drop Malformed should be enabled. TCP Drop Mis
Network > IPsec Crypto		default	84	IPsec Crypto Profile Authentication	Recommended to only use SHA256 or higher for authenticat
Network > IPsec Crypto		default	83	IPsec Crypto Profile Encryption	Recommended to only use aes-128-gcm or aes-256-gcm for e
Network > Zones	vsys1	external	212	Enable Packet Buffer Protection	
Network > Zones	vsys1	external	60	Zone Protection Profile Applied to Zone	
Network > Zone Protection		ZP_external	86	Reconnaissance Protection	

paloalto STRATA ADOPTION HEATMAP BEST PRACTICE ASSESSMENT 47 DEVICE INFO

POLICIES

- Security
 - Security Rule Checks
 - Security Rulebase Checks 7**
 - Policy Based Forwarding
- Decryption
 - Decryption Rule Checks
 - Decryption Rulebase Checks 1
- Tunnel Inspection
- Application Override

Security Rulebase Device Group(s): vsys1

BEST PRACTICE CHECK ? New

- ✗ Interzone Deny Rule with Logging (Fail)

It is recommended to override the interzone-default rule with any Action except 'allow' and Log at Session End enabled.
- ✗ Intrazone Allow Rules with Logging (Fail)

It is recommended to override the intrazone-default rule with Action set to 'allow', Log at Session End enabled, and IPS capability enabled.