Emergency Update Required

PAN-OS Root & Default Certificate Expiration

Nitish Tiwari

November 2023

What is Changing in Emergency Update?

On December 31, 2023,

- The root certificate and default certificate for Palo Alto Networks firewalls and appliances running PAN-OS software will expire.
- If you do not renew your certificates before they expire, your firewalls and Panorama appliances will no longer establish new connections to Palo Alto Networks cloud services.
- Which will impact network traffic and potentially cause a network outage when existing connections terminate and attempt to reconnect due to network changes, configuration changes, or unforeseen events.

The root certificate will expire December 31 14:47:47 2023 GMT
The device certificate will expire December 31 20:14:14 2023 GMT

Palo Alto Customers who have Firewalls or Panorama used for any of the below following services will be impacted:

1. **Scenario 1**
   - Data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list)
   - URL PAN-DB private cloud (M-Series)
   - WildFire private cloud appliance (WF500/B)

1. **Scenario 2**
   - WildFire/Advanced WildFire Public Cloud
   - URL/Advanced URL Filtering
   - DNS Security
   - ThreatVault
   - AutoFocus

Target Upgrade Versions:

Current PAN-OS Version	Upgrade Target Version
8.1	8.1.21-h2 8.1.25-h1 or greater
9.0	9.0.16-h5 or greater
9.1	9.1.11-h4 9.1.12-h6 9.1.13-h4 9.1.14-h7 9.1.16-h3 9.1.17 or greater
10.0	10.0.8-h10 10.0.11-h3 10.0.12-h3 or greater
10.1	10.1.3-h2 10.1.5-h3 10.1.6-h7 10.1.8-h6 10.1.9-h3 10.1.10 or greater
10.2	10.2.3-h9 10.2.4 or greater
11.0	11.0.0-h1 11.0.1-h2 11.0.2 or greater
11.1	11.1.0 or greater

Note:

- All hotfix releases have been published for Firewalls, Panorama, WF500/B, and URL Pan-DB private cloud (M-series) appliances.
- For WF500/B and URL Pan-DB private cloud (M-series) appliances specifically, please use the following hotfix releases:

8.1.25-h2,
9.0.16-h6,
9.1.16-h4,
10.0.12-h4,
10.1.11-h3,
10.2.7-h1,
11.0.3-h1,
11.1.0-h1

Action Required
Scenario 1

Scenario 1 Required Steps

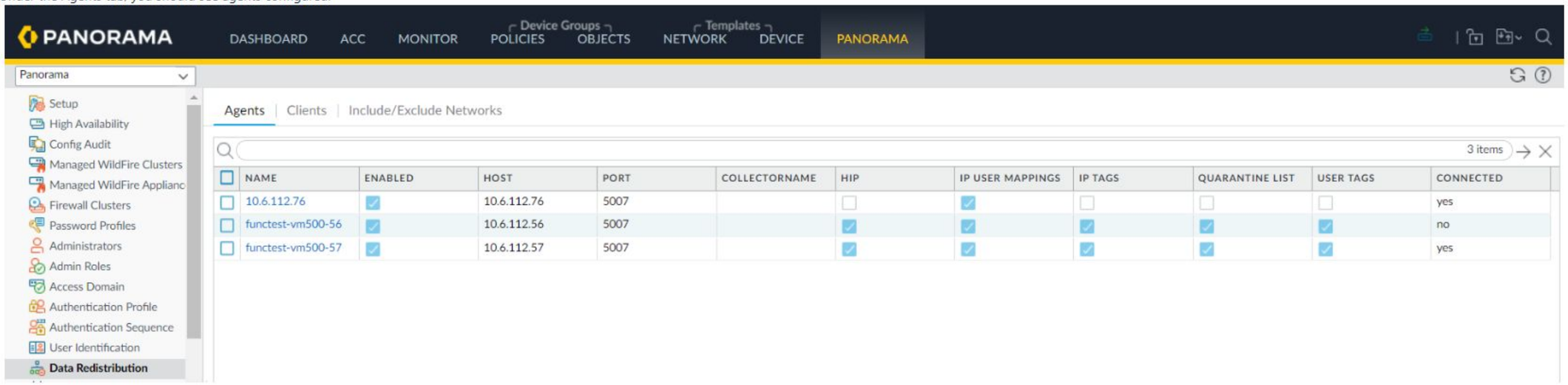
➔ If you are a customer with **Data redistribution** (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list) you will need to take one of the following two actions:

- (1a) upgrade your affected firewalls, and Panorama (Management and Log Collector modes),
- (1b) deploy Custom Certificates to your affected firewalls, and Panorama (Management and Log Collector modes).

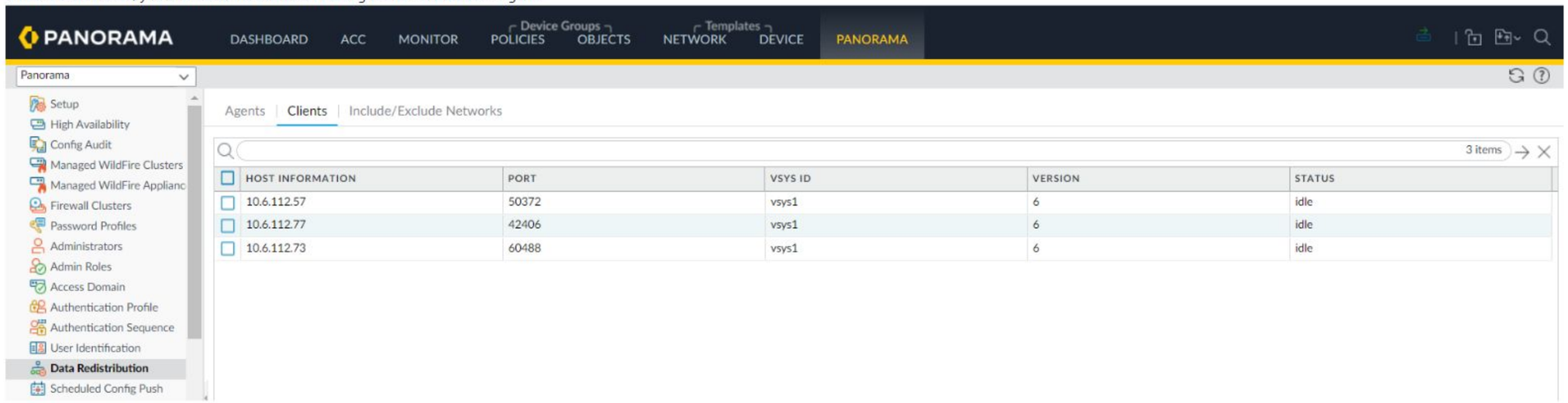
➔ If you are a customer with **URL PAN-DB private cloud** (M-Series), or **WildFire private cloud appliance** (WF500/B), you will need to take the following action:

- (1a) upgrade your affected firewalls, WF-500s, M-Series, and Panorama (Management and Log Collector modes).

- **Panorama PAN-OS 10.0+**
  - Go to Panorama → Data Redistribution
    - Under the Agents tab, you should see agents configured.



    - Under the Clients tab, you will see all the clients connecting to the Redistribution Agent.



- admin@PA-M200-Panorama-9> **show redistribution service status**

```
Redistribution info:
        Redistribution service:          up
        listening port:                  5007
        SSL config:                      Default certificates
        back pressure is:                off
        number of clients:               3
```

- admin@PA-M200-Panorama-9> **show redistribution agent state all**

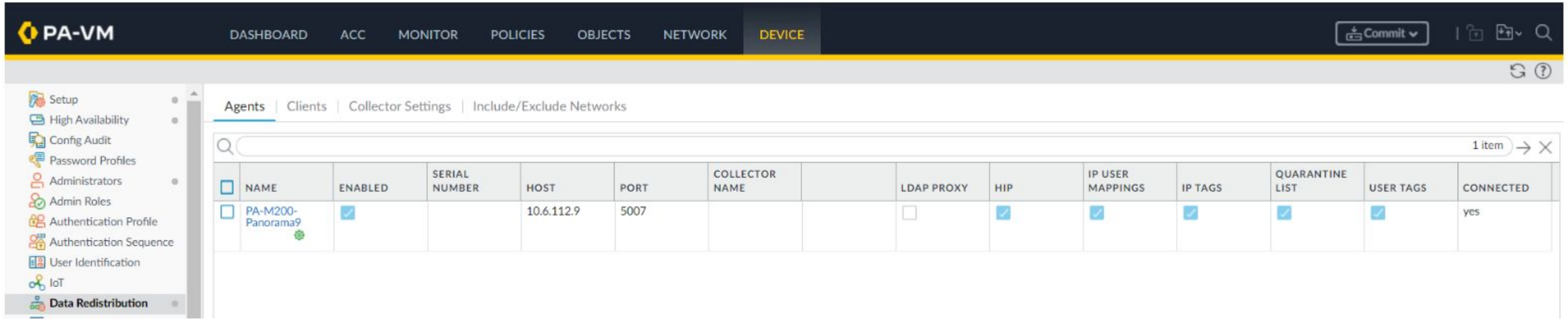
```
Agent: 10.6.112.76(vsys: vsys1) Host: 10.6.112.76(10.6.112.76):5007
        Status                                  : conn:idle
        Version                                 : 0x6
        SSL config:                             : Default certificates
        num of connection tried                 : 1
        num of connection succeeded             : 1
        num of connection failed                : 0
        num of status msgs sent                 : 191416
        num of status reply msgs rcvd           : 191416
        num of request of ip mapping msgs sent  : 0
        num of request of all ip mapping msgs sent : 1
        num of user ip mapping msgs rcvd        : 0
        num of user_id_command msgs rcvd        : 0
        num of hip update msgs rcvd             : 0
        num of hip report get messages sent     : 0
        num of hip report get msgs rcvd         : 0
        num of iptag post msgs rcvd             : 0
        num of usertag post msgs rcvd           : 0
        num of all quarantine msgs sent         : 0
        num of quarantine msgs rcvd             : 0
        Last heard(seconds ago)                 : 1
```

admin@PA-M200-Panorama-9> **show redistribution service client all**

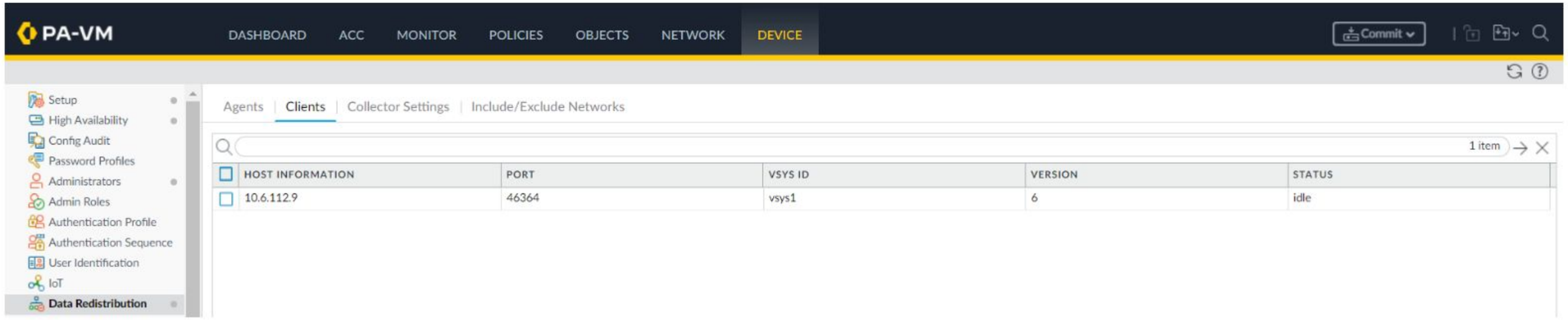
Device ID	Vsys-ID	Version	Status	Redistribution
10.6.112.57/50372	1	6	idle	**ITUHQ**
10.6.112.77/42406	1	6	idle	I
10.6.112.73/60488	1	6	idle	ITU

Redistribution: 'I': IP User Mapping
Redistribution: 'T': IP Tag
Redistribution: 'U': User Tag
Redistribution: 'H': HIP Report
Redistribution: 'Q': Quarantine

- **Firewall PAN-OS 10.0+**
  - Got to Device → Data Redistribution
    - Under the Agents tab, you should see agents configured.



    - Under the Clients tab, you will see all the clients connecting to the Redistribution Agent.



Detailed (1a) Steps:

Upgrade your impacted firewalls, WF-500, M-Series, and Panorama

➔ If you do not have Custom Certificates installed, you must upgrade all of your firewalls, WF-500s, M-Series, and Panoramas (Management and Log Collector modes) that participate in **data redistribution** (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list), **URL PAN-DB private cloud** (M-Series), and/or **WildFire private cloud** (WF500/B) to one of the PAN-OS versions in the Target Upgrade Version table above on Slide-4.

➔ Customers must upgrade their WF-500/B appliance to the releases mentioned below:

- Released: 8.1.25-h2, 9.0.16-h6, 9.1.16-h4, 10.0.12-h4, 10.1.11-h3, 10.2.7-h1, 11.0.3-h1, 11.1.0-h1

➔ Customers must upgrade their URL PAN-DB private cloud (M-Series) appliances to the releases mentioned below:

- Released: 8.1.25-h2, 9.0.16-h6, 9.1.16-h4, 10.0.12-h4, 10.1.11-h3, 10.2.7-h1, 11.0.3-h1, 11.1.0-h1

Detailed (1b) Steps:

Data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list):

If all firewalls and Panorama on your network are running PAN-OS version 10.0 or above, you can switch to Custom Certificates for data redistribution instead of default device and root certificates. To know more about Customer Certificate: Link

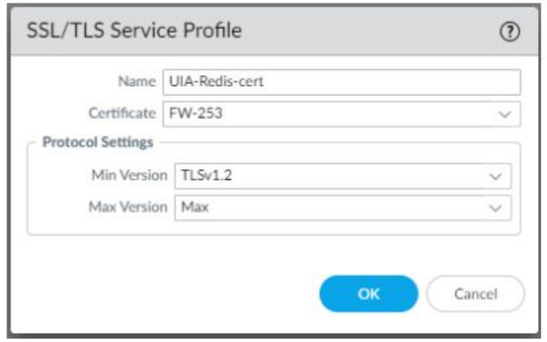
Important:

- ➔ You must switch to custom certificates on the data redistribution agent and client for secure server and client communications.
- ➔ If you use data redistribution between firewalls and Prisma Access, you must also apply a hotfix or upgrade your impacted firewalls. You do not need to make changes to Prisma Access–you need only upgrade your firewalls to a targeted upgrade version.

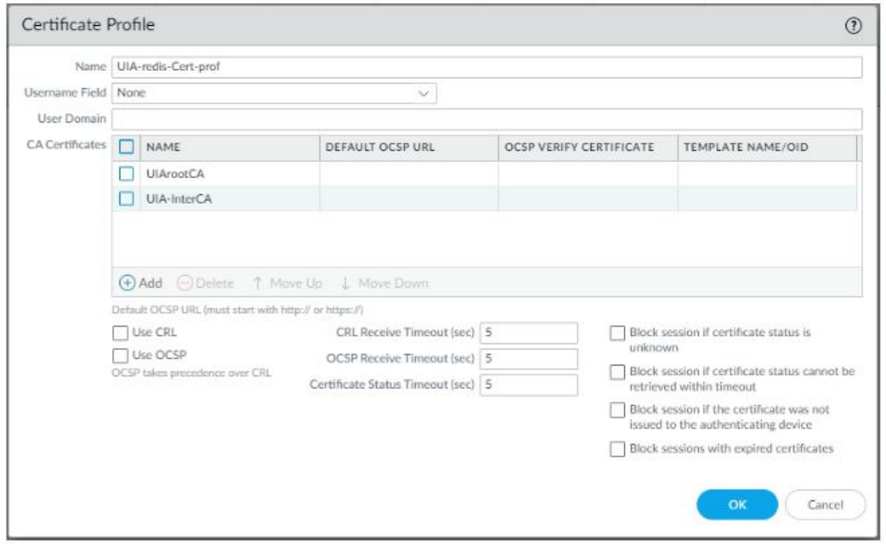
WildFire private cloud (WF500/B): Custom Certificates are not an option.

URL PAN-DB private cloud (M-Series): Custom Certificates are not an option.

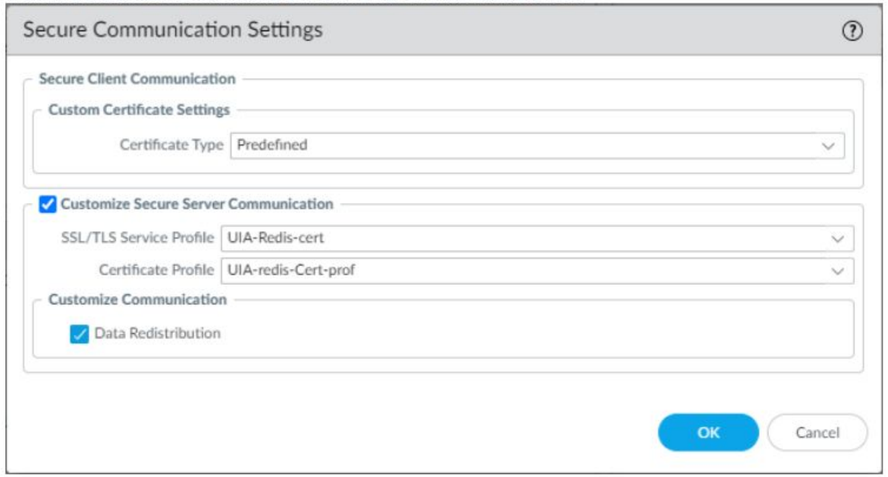
- Once you have imported or generated the certificates, go to **Device → Certificate Management → SSL/TLS Profile**
- Click Add, provide a name for the object, select the appropriate certificate, and then select the min and max TLS versions.



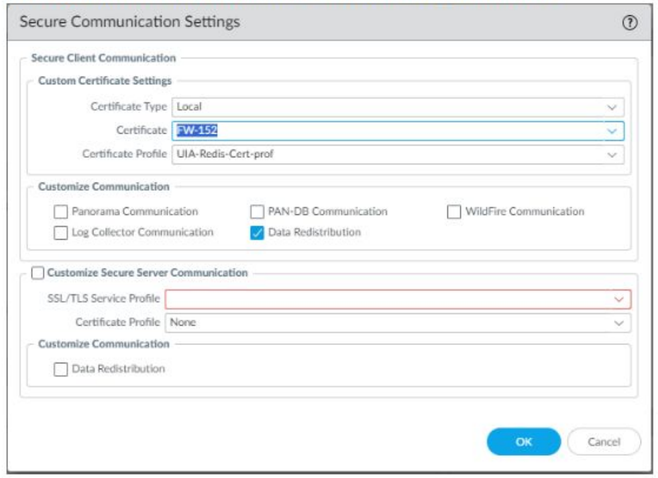
- Then Go to **Device → Certificate Management → Certificate Profile**
- Then click **Add** and Name the certificate profile, then click Add again under CA Certificates and add all CA Certificates that signed leaf certificate.



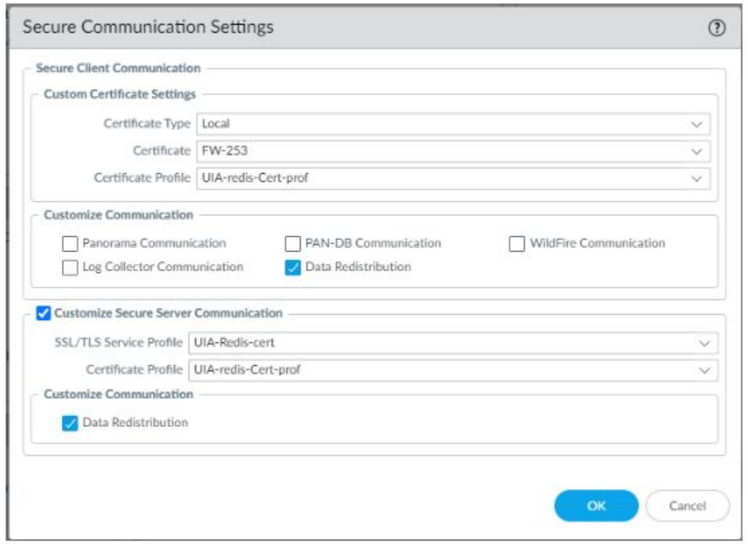
- Go to **Device → Setup → Secure Communication Settings**
  - Click on the gear in the top right corner to edit Secure Communication Settings
  - If configuring the firewall or Panorama as a server only for Data Distribution
    - Check the box for **Customize Secure Server Communication**, then select the correct SSL/TLS Service Profile and the Certificate Profile.
    - Under the **Customize Communication**, check the box for **Data Redistribution**



  - If configuring the firewall or Panorama as a client only for Data Redistribution
    - Under **Secure Client Communication → Custom Certificate Settings**, select the **Certificate Type** as **Local**, and select the appropriate **Certificate** and **Certificate Profile.**
      - Under **Customize Communication**, check the box on **Data Redistribution**.



- If the firewall or Panorama is acting as a Redistribution Agent and Client for bi-directional Data Distribution, then Both settings need to be configured on both firewall and/or Panorama, with the appropriate server and client certificates.



Action Required
Scenario 2

Scenario 1 Required Steps

➔ If you are a customer with **WildFire public cloud**, **Advanced WildFire public cloud**, **URL Filtering**, **Advanced URL Filtering**, **DNS Security**, **Threat Vault**, or **AutoFocus**, you must perform one of the following three actions before your certificates expire on December 31, 2023:

- (2a) install a specific content update on your impacted firewalls and Panorama appliances OR
- (2b) upgrade your impacted firewalls and Panorama appliances OR
- (2c) enable device certificates on your impacted firewalls and Panorama appliances.

Detailed (2a) Steps:

Install a specific content update on your affected firewalls and Panorama appliances

➔ You must install the following content update version (**8776-8390 or later**) on your firewalls and Panorama.

- If you have automatic content configured, this update will be automatic
- If you manually update your content, please update your content to the content version above

Detailed (2b) Steps:

Upgrade your affected firewalls and Panorama

➔ Upgrade your firewall and Panorama to one of the PAN-OS versions in the Target Upgrade Versions **8776-8390 or later**

Detailed (2c) Steps:

Enable Device Certificate on your affected firewalls and Panorama

- ➔ If you have firewalls and Panorama appliances running PAN-OS 8.1, PAN-OS 9.0, or PAN-OS 9.1, we do not recommend that you use this option.
- ➔ If you have firewalls and Panorama appliances running PAN-OS 10.0.5, PAN-OS 10.1.10, PAN-OS 10.2.5, or PAN-OS 11.0.2 or any later versions or releases
- ➔ Steps to enable the device certificate are: Link

Impacts, If not upgraded

Impacts:

For Scenario 1:

- If you do not upgrade your impacted firewalls and Panorama appliances by December 31, 2023, your firewalls and Panorama appliances will no longer be able to establish new connections to **data redistribution** (User-ID, IP-tag, User-tag, GlobalProtect HIP, or quarantine list),
- **URL PAN-DB private cloud** (M-Series) appliances or **WildFire private cloud** (WF-500 or WF-500-B) appliances: If your existing connections terminate (such as when you make network or configuration changes or experience any unforeseen network events), you will experience an outage of the impacted services when they fail to reconnect due to expired certificates.

For Scenario 2:

If you do not complete the recommended actions above before December 31, 2023, your **WildFire public cloud, Advanced WildFire public cloud, URL Filtering, Advanced URL Filtering, DNS Security, Threat Vault, and AutoFocus** services will no longer be able to establish new connections after that date.

Common concerns / queries :

1. Config assistance

Please find the below document for your reference:
https://live.paloaltonetworks.com/t5/customer-advisories/emergency-update-required-pan-os-root-and-default-certificate/ta-p/564672

2. Functionality query

++ Production devices doesn't have userid, iptag, usertag, globalprotect, urlpandb private cloud so scenario 1 is not applicable Scenario 1 Data redistribution (User-ID, IP-tag, User-tag, GlobalProtect HIP, and/or quarantine list) URL PAN-DB private cloud (M-Series) WildFire private cloud appliance (WF500/B) Mitigation: Upgrade PAN-OS on your affected devices, OR Deploy custom certificates to replace the expiring certificates. ++ For scenario 2 we could resolve this by installing Content Update (8776-xxxx or later) Scenario 2 WildFire/Advanced WildFire Public Cloud URL/Advanced URL Filtering DNS Security ThreatVault Auto Focus

Global Customer Support - Palo Alto Networks

For any further technical assistance, please contact support numbers listed below:
https://www.paloaltonetworks.com/company/contact-support

Thank You

paloaltonetworks.com