kaspersky

Kaspersky Network Security Threat Data Feeds for PaloAlto NGFW

Version 2.0

kaspersky

Introduction

Network security controls – Next Generation Firewalls (NGFW), as a rule, possess the functionality of filtering DNS/Web traffic using external dynamic lists of IoCs.

Kaspersky offer dynamic lists, specifically designed to be used in such security controls.

Kaspersky Network Security Threat Data Feeds

Dynamic lists of IoCs from Kaspersky for network security controls are based on Kaspersky Threat Intelligence Data Feeds and contain regularly updated lists of IoCs of various types (IP addresses and domains). Using those lists it is possible to monitor/block user access to dangerous network resources.

The following lists of indicators are available:

Name	Type	Description	URI	Update frequency
Dangerous IPs	IP	List of dangerous IP addresses	https://tip.kaspersky.com/api/feeds/dangerous_ips	20
Malicious URLs	URL	List of malicious domains	https://tip.kaspersky.com/api/feeds/malicious_domains	20
Phishing URLs	URL	List of phishing domains	https://tip.kaspersky.com/api/feeds/phishing_domains	20
Botnet CnC URLs	URL	List of botnet C&C domains	https://tip.kaspersky.com/api/feeds/botnet_domains	60

In order to download the lists above (including direct downloading into network security controls) you will need an API token for Kaspersky Threat Intelligence Portal: https://tip.kaspersky.com/Help/Doc_data/en-US/ManagingAPItoken.htm (after clicking the link, close the authorization window that appears to proceed to the help page). You may request it in your account on Kaspersky Threat Intelligence Portal. After that make sure your token is configured for downloading dynamic lists of IoCs for network security controls (ask your Technical Manager or send the request to intelligence@kaspersky.com).

You may test downloading the lists using cURL utility (below is the syntax for Linux):

curl -v -u api_token:<YOUR API TOKEN> https://tip.kaspersky.com/api/feeds/dangerous_ips?limit=100

kaspersky

Configuring Kaspersky Network Security Threat Data Feeds in PaloAlto NGFW

PaloAlto NGFW supports external dynamic lists of IoCs available as updatable plain text files via HTTP/HTTPs.

After import into PaloAlto NGFW IoCs can be used in traffic filtering policies.

For more information please refer to the documentation: docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list

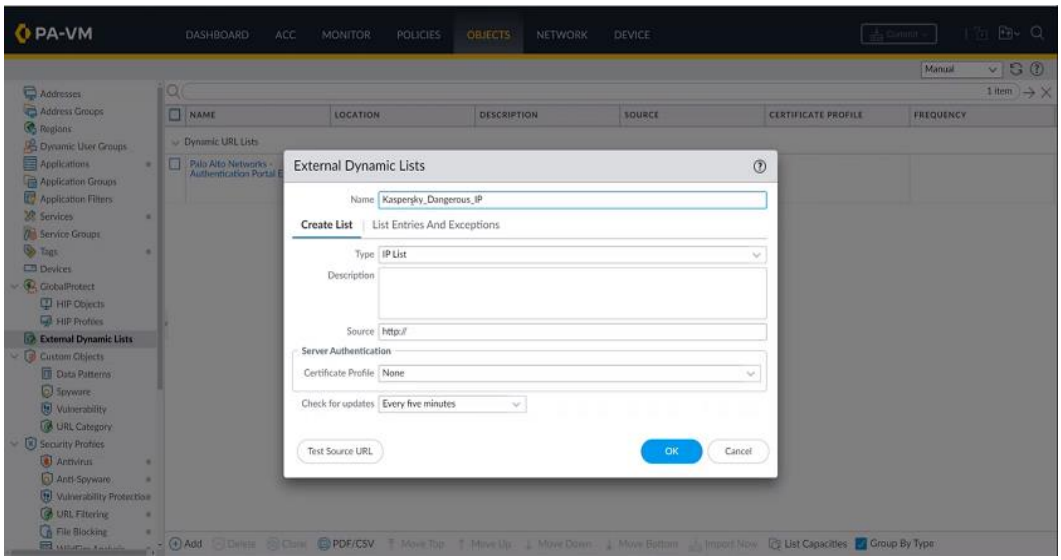
In order to import a dynamic list of IoCs from Kaspersky into PaloAlto NGFW follow the steps:

1. Open **Device > Setup > Services > Service Route Configuration > Customize** and edit the service **External Dynamic Lists.**

2. Select **Objects > External Dynamic Lists.**

3. Select action **Add** and specify the name of the list in the **Name** field – e.g. Kaspersky Dangerous IP.

4. Select the appropriate list **Type**. For lists with *Domain* type it is possible to set the additional option **Automatically expand to include subdomains.**



5. In the field **Source** specify the URL of the list – e.g. https://tip.kaspersky.com/api/feeds/malicious_domains?limit=130000

limit – the threshold on the number of IoCs actually being downloaded. This parameter is optional, if you do not specify it, all available IoCs will be downloaded. The actual number of downloaded IoCs can be less than the specified value, it depends on the number of available IoCs of certain type.

Full list size can exceed the threshold allowed by your PaloAlto NGFW (thresholds vary among PaloAlto NGFW models). It is recommended to set the limit according to the recommended value for your PaloAlto NGFW.

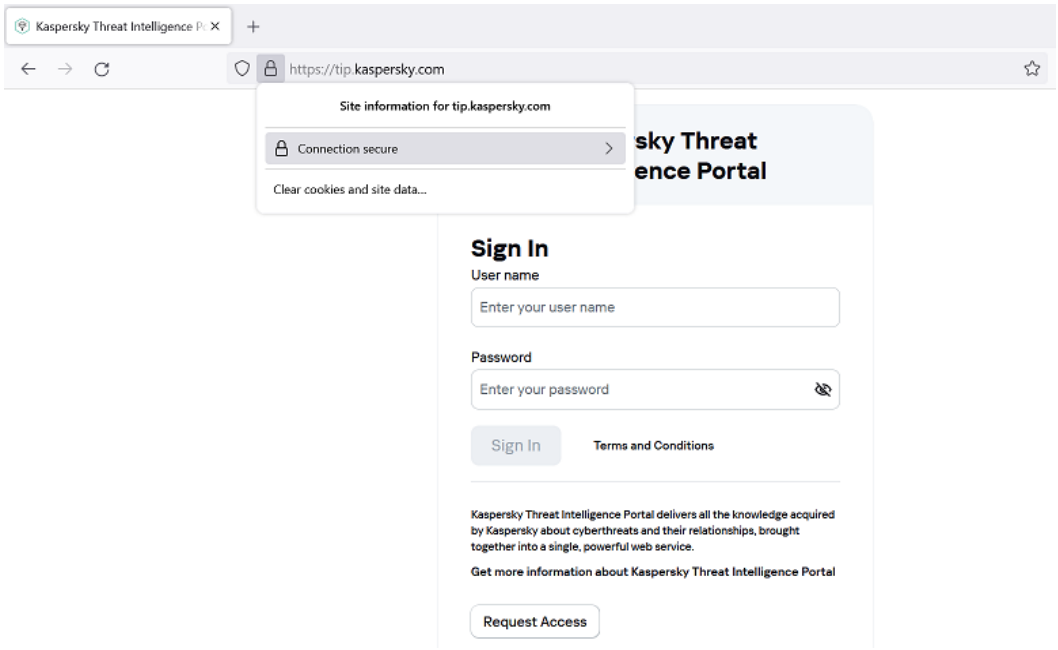
The full API specification for downloading dynamic lists of IoCs is available on Kaspersky Threat Intelligence Portal online documentation:https://tip.kaspersky.com/Help/api/?specId=tip-feeds-api (after clicking the link, close the authorization window that appears to proceed to the help page).

6. You will need to download pem files of public keys of trust chain for tip.kaspersky.com, except for the end node.

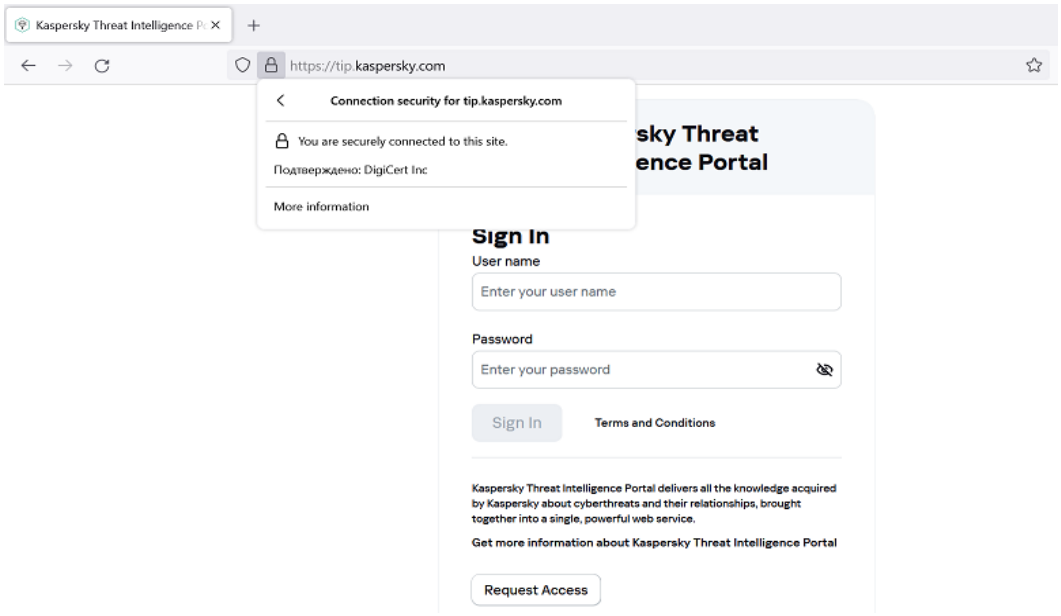
Below is the procedure for obtaining pem files of certificates using Firefox Browser 123.0 as an example:

1) Proceed to https://tip.kaspersky.com. You will be asked for the client's certificate. You may refuse or choose any available certificate, since no authorization is required for getting information about chain of trust.

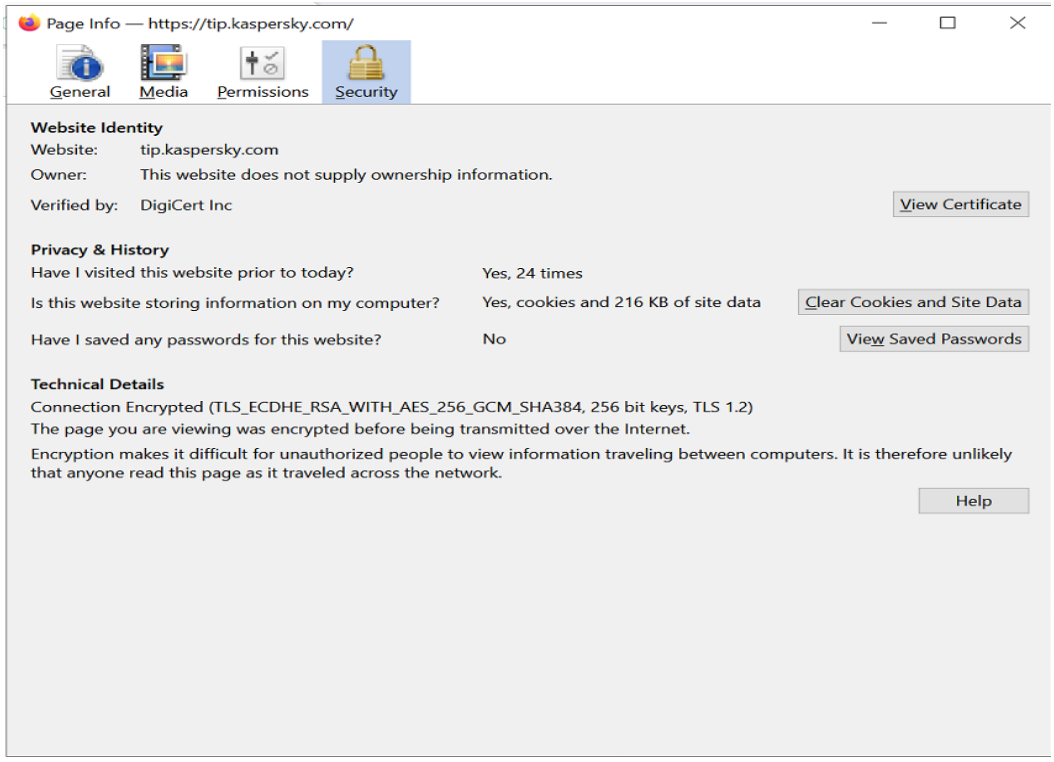
2) Click on the ‘lock’ symbol next to the browser address line. Information about TLS connection to the site will be displayed:



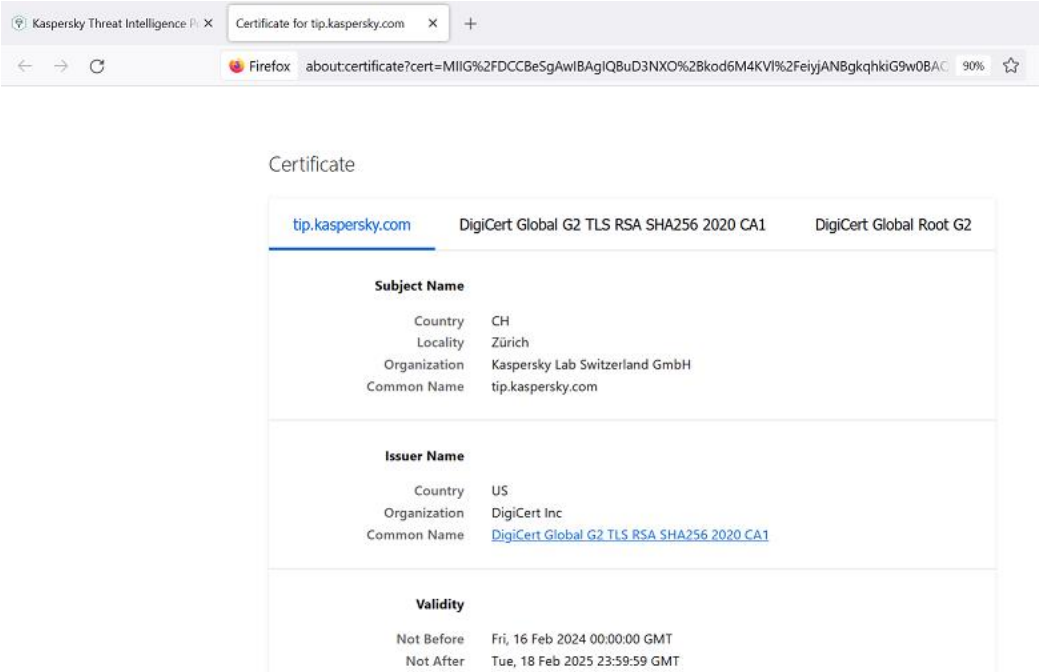
3) Click on **Connection secure**. Additional information about connection will be displayed:



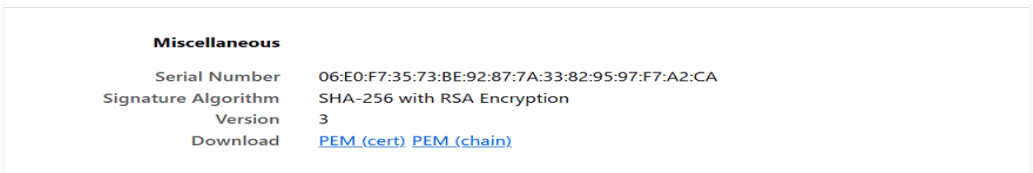
4) Click on **More information**. The **Page Info - https://tip.kaspersky.com** window will open:



5) Click on **View Certificate**. The browser will display a tab with information about chain of certificates:

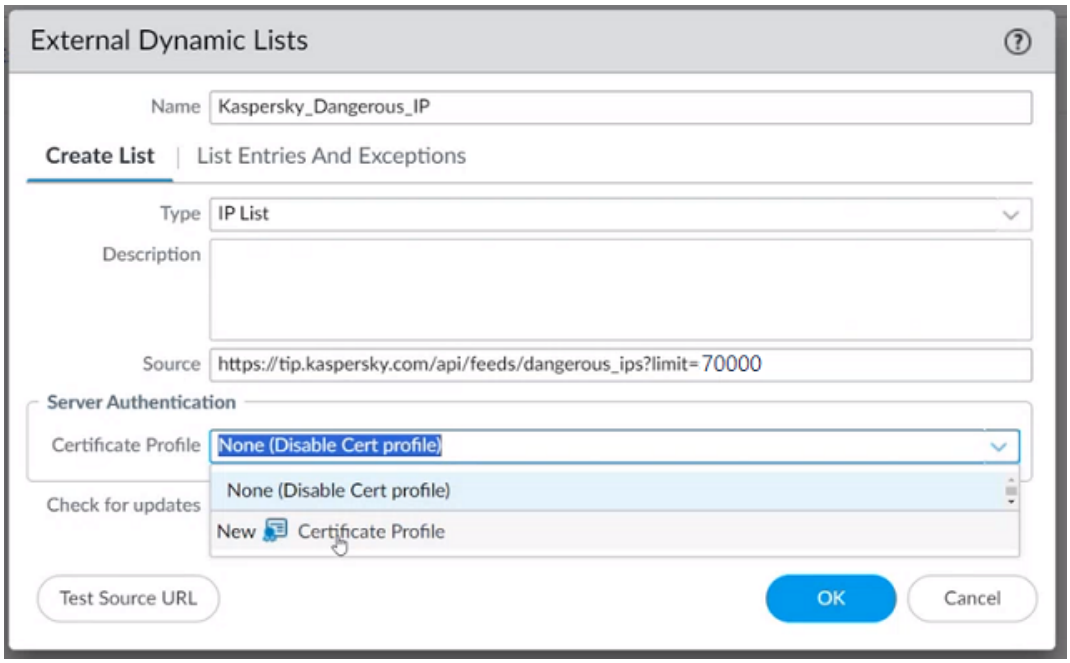


6) For Certificate Authority (root certificate) and Intermediate certification authority download pem files of certificates. To do this, on all tabs except for **tip.kaspersky.com**, find **Miscellaneous** and select PEM (cert) in the **Download** field:

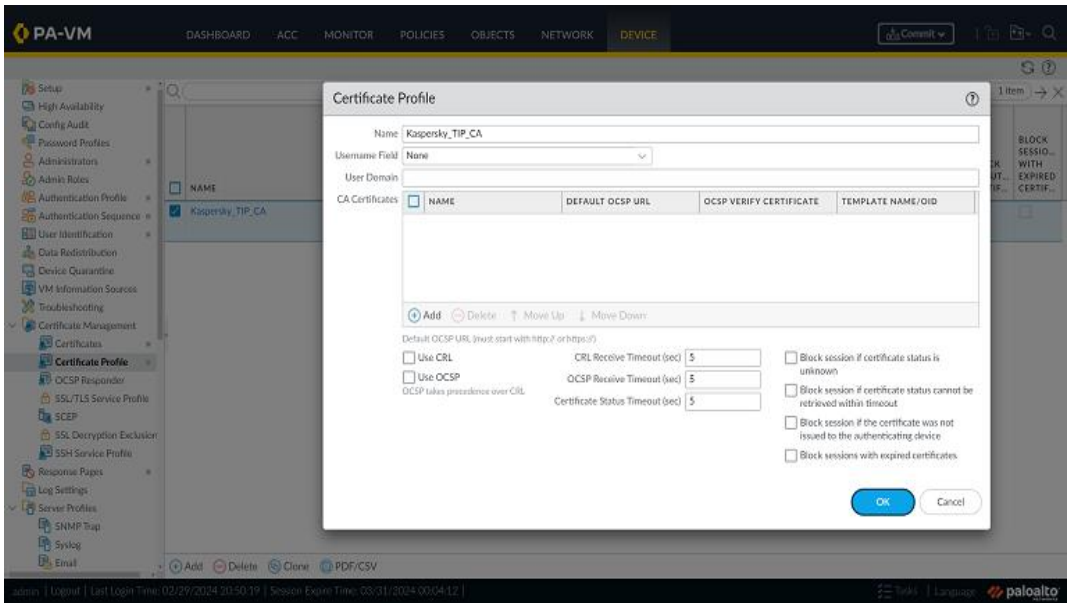


In our example, two files will be downloaded: **tip-kaspersky-com.pem** and **tip-kaspersky-com(1).pem**.

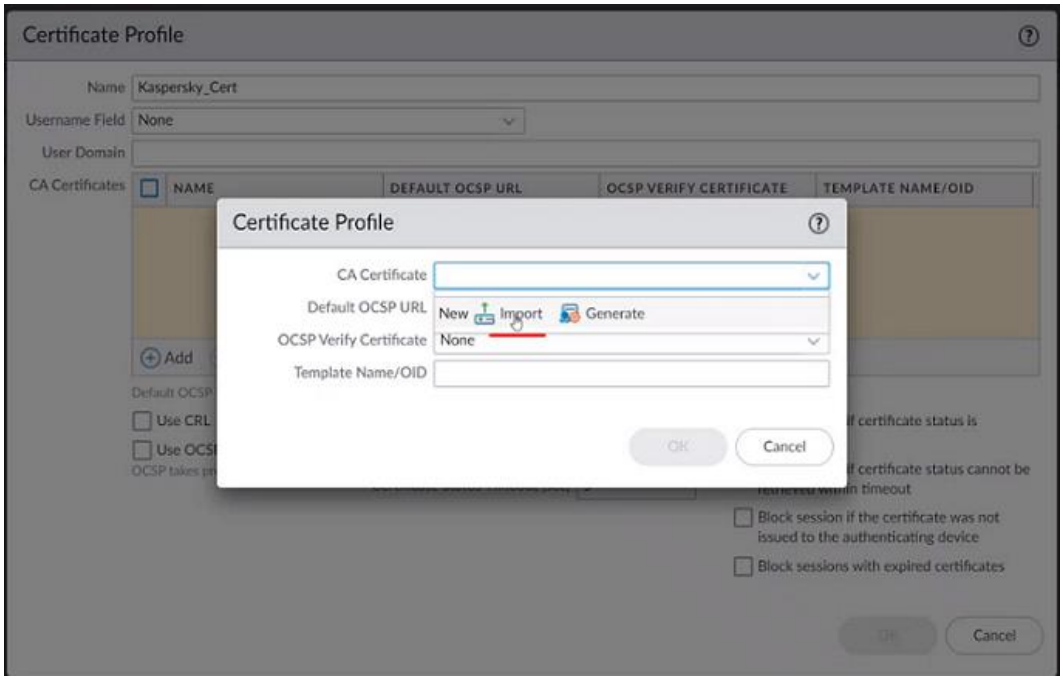
7) You will need to create a certificate profile for connecting to HTTPS server. To do this, select **New Certificate Profile**:



A window for creating certificate profile will open. Fill in the **Name** field and import the trust chain certificates obtained earlier. To do this, click **Add** in the **CA Certificates** section.



8) In the window that opens, select **Import**:



9) In the certificate import window, fill in the following:

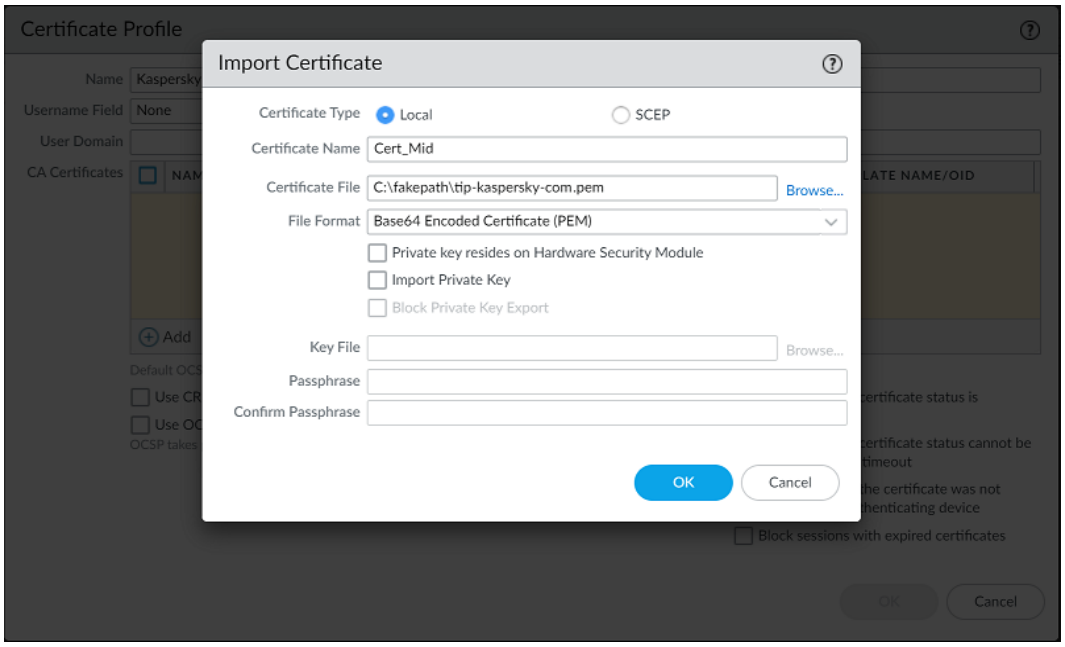
Certificate Name = (any name, in the example below - "Cert_Mid")

Certificate Type = Local

Certificate File = select pem file of certificate public key for chain of trust.

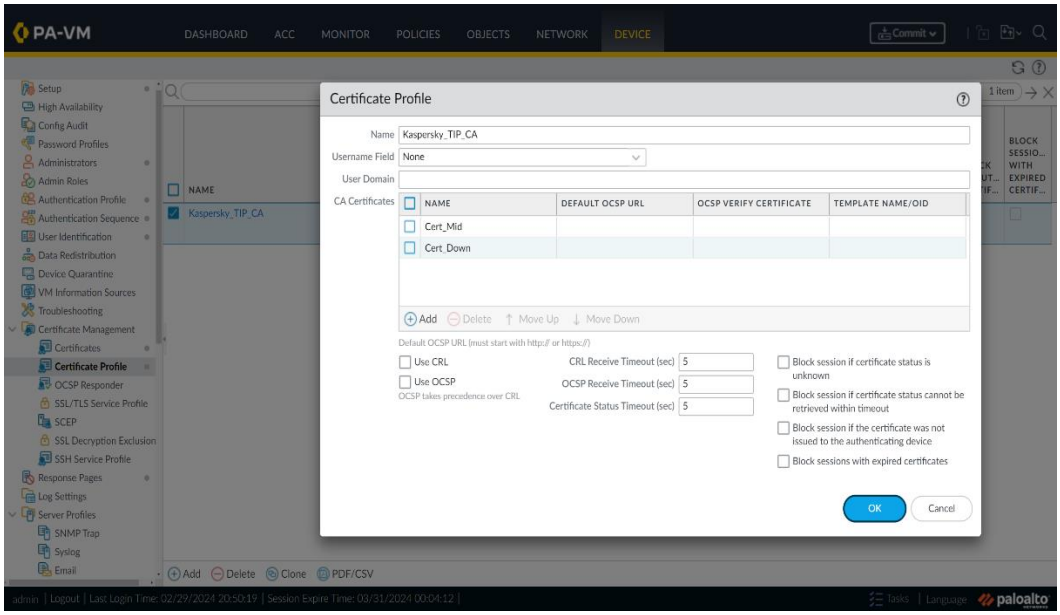
Other fields should be unchanged.

Click **OK**.



The above step should be performed twice – for root CA and intermediate CA trust chain certificates.

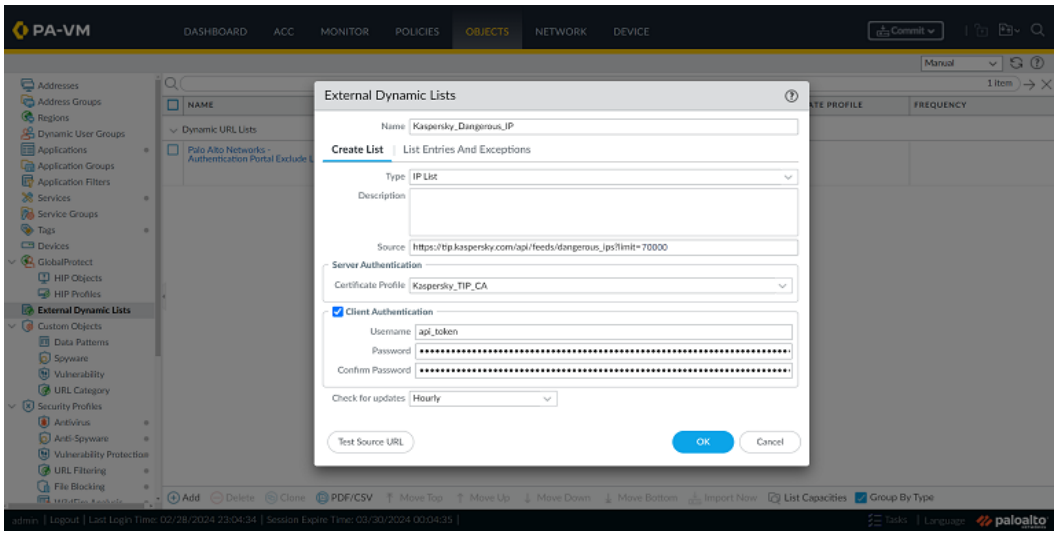
The **Test Source URL** button may not function in some PaloAlto versions. Thus, ignore the "Operation failed - URL access error" message, if appears.



10) Click **OK**.

7. Select **Client Authentication** and specify **Username** и **Password:**

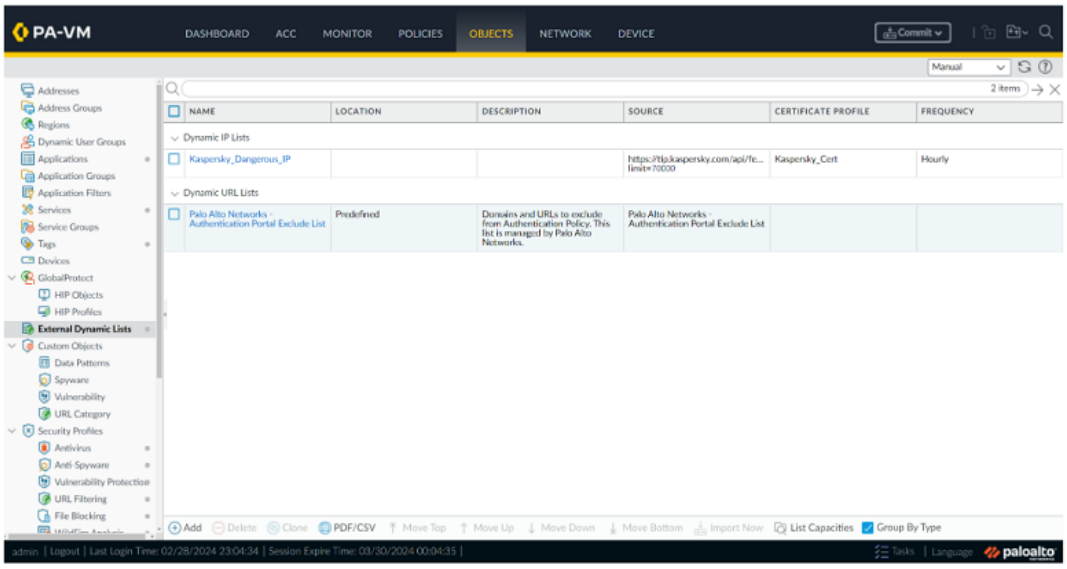
Username	api_token
Password	Your API token requested in your account on Kaspersky Threat Intelligence Portal



8. Set **Check for updates**, and specify the frequency of updates. Recommended values are described in the table of available lists above in this document.

9. Set **OK** to save settings and **Commit** for starting download of dynamic list of indicators.

A new list will appear in the dynamic IP lists: **Objects > External Dynamic Lists**.



In order to configure other dynamic lists of IoCs follow similar steps.

10. After applying the dynamic list in **Policies,** the entries will be displayed in **List Entries And Exceptions**.