Password Manager Pro masterclass

webinar Q&A
July 26, 2018

1. Should the PMP server be available on the internet to use Let's Encrypt?

Yes, it should have internet connectivity as the server needs to contact Let's encrypt for certificate creation or renewal.

2. Is the KMP agent same as the PMP agent? If not, will it be merged to avoid double deployment?

They are not the same; both the agents work as separate entities. However, we will forward this requirement to the development team to analyze the feasibility to merge them in the future versions.

3. For SSH key rotation, how can we deploy the public key to one user and the private key to another user automatically?

PMP only deploys the public key to the user and retains the private key within the web client/data base. During the public key deployment, PMP appends the authorized_key file in the target endpoint.

4. Does PMP replace the authorized keys file? Can that file be customized from PMP?

PMP does not replace the existing authorized key file. There are two options during the key deployment:

Append and **Overwrite.**

Append replaces only the key that was previously deployed by PMP and rest all remains the same.

Overwrite clears the authorized_key file and adds the new public key.

5. Is it possible to use the credentials stored in PMP to log on to KMP without having to enter the passwords manually?

We have plans to implement this option in one of our immediate releases.

6. Can a host be dissociated from a key without deleting the key?

Yes. Using the dissociate option in PMP, you can very well dissociate the key without deleting it.

7. Do you use python to connect to networking devices? If yes, can we export your scripts and modify them to do custom scripts on your server or a different network management station?

We use SSH and SSH scripts that can be modified.
Please contact us at passwordmanagerpro-support@manageengine.com for further details.

8. How to renew the existing certificates from Let's encrypt?

To manually renew certificates issued by Let's Encrypt, select the required certificates from 'Let's Encrypt' tab and click 'Renew' from the top menu. You then have to complete the Let's Encrypt challenge verification process, which proves your continued ownership of your domain. Once you have completed the challenge, the selected certificate is renewed. Save the certificate in order to replace the old version with the current certificate in the certificate repository.

Key Manager Plus also facilitates automatic renewal of SSL certificates through automatic domain validation, provided you already have configured agent mapping. In this case, the certificates are rotated automatically after every 75 days and an email notification is sent to the account-holder's email address.

Below is the help document link on Let's Encrypt Renewal,

Let's Encrypt Help document.

(**NOTE:** Currently, if you already have an expiring Let's Encrypt certificate which is not acquired through the Key Manager Plus interface, it's not possible to carry out the renewal operation from Key Manager Plus. However, you can always manage such certificates using Key Manager Plus by manually importing them into KMP's certificate repository.)

9. I wanted to know whether I can track the expiry of SSL certificates with same common name that have been derived from different CAs. As far as I can see, Key Manager doesn't allow me to upload 2 different certificates with the same name.

When the certificates are imported with the same common name, then they will be added to the certificate history section.

We differentiate the certificate names based on the common name as one entry in the certificates tab and display all the deployed servers in the UI. As KMP is licensed based on the number of certificates, we have designed it this way so that customers do not end up spending the licence keys for a same certificate.

If this is a different certificate, you have to manually move it to the certificate repository list by following the below steps. Once moved into the certificate repository list, the new cert file will be counted for licencing.

1. Navigate to the Certificates tab and click on the “certificate history” present on the right hand corner.
2. In Certificate history window, Click on “Certificate Settings” icon and select Manage Certificate to move the correct cert file to the certificate list.
3. In case, if there are two certificates in the certificate history section and if you’d like to make only one particular certificate visible in the certificate repository page, then select the option “set as current certificate” by clicking on the “Certificate settings” icon.

10. While doing SSL Discovery from a file, is there any way to indicate a range of IP addresses, or a subnet in the file? Anything short of listing out 1000’s of IP addresses or host names within a network?

To discover the certificates by providing a range of IP address, please follow the below steps:

1. Go to the Discovery Tab in the GUI.
2. Click on the SSL tab.
3. Select the radio button option “IP Address Range”.
4. Specify the IP range and port and click on the “Discover” button to discover all the SSL certificates available in the servers falling under the range.

Use the “From File” option to discover certificates from multiple IP addresses over different networks.

(**Note:** The file to be imported must be a text file containing the hostname or IP addresses of individual servers listed one below another, with each followed by its respective port(s) separated by a space.

Eg: 0.0.0.0 22
test-username-10 6565
192.168.20.20 7272)