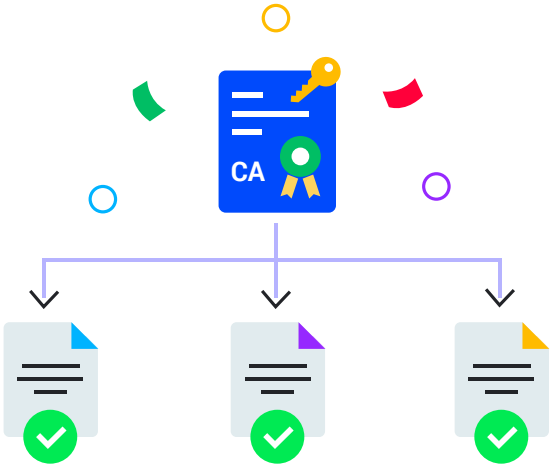
What's new in Key Manager Plus 5610

Implement a custom root CA to sign locally generated certificate requests in bulk.

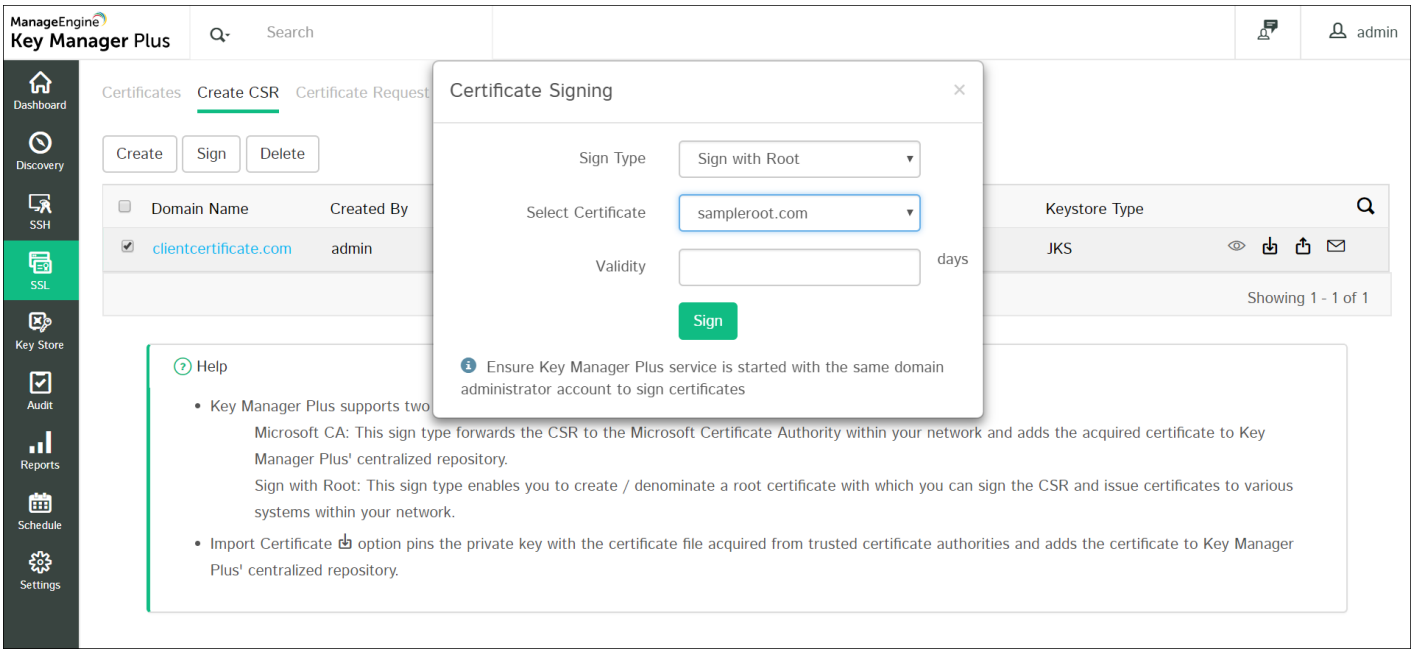


Often, organizations are forced to purchase and deploy trusted third-party CA certificates for their internal applications to avoid service interruptions caused by browser security warnings.

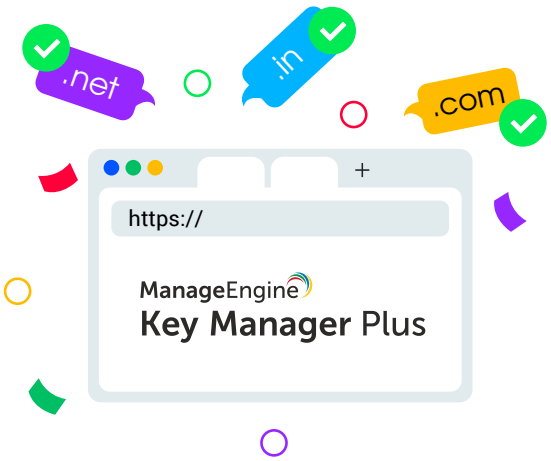
With the introduction of custom root CA signing, admins can effortlessly sign locally generated certificate requests using a custom root CA, and instantly deploy them to target systems in bulk from Key Manager Plus. The whole process is only a few simple steps, which saves a great deal of time for administrators.

Here's a quick summary:

- Create a custom root CA
- Generate a certificate signing request (CSR)
- Sign the CSR using the custom root CA
- Deploy the signed certificate to target systems from Key Manager Plus

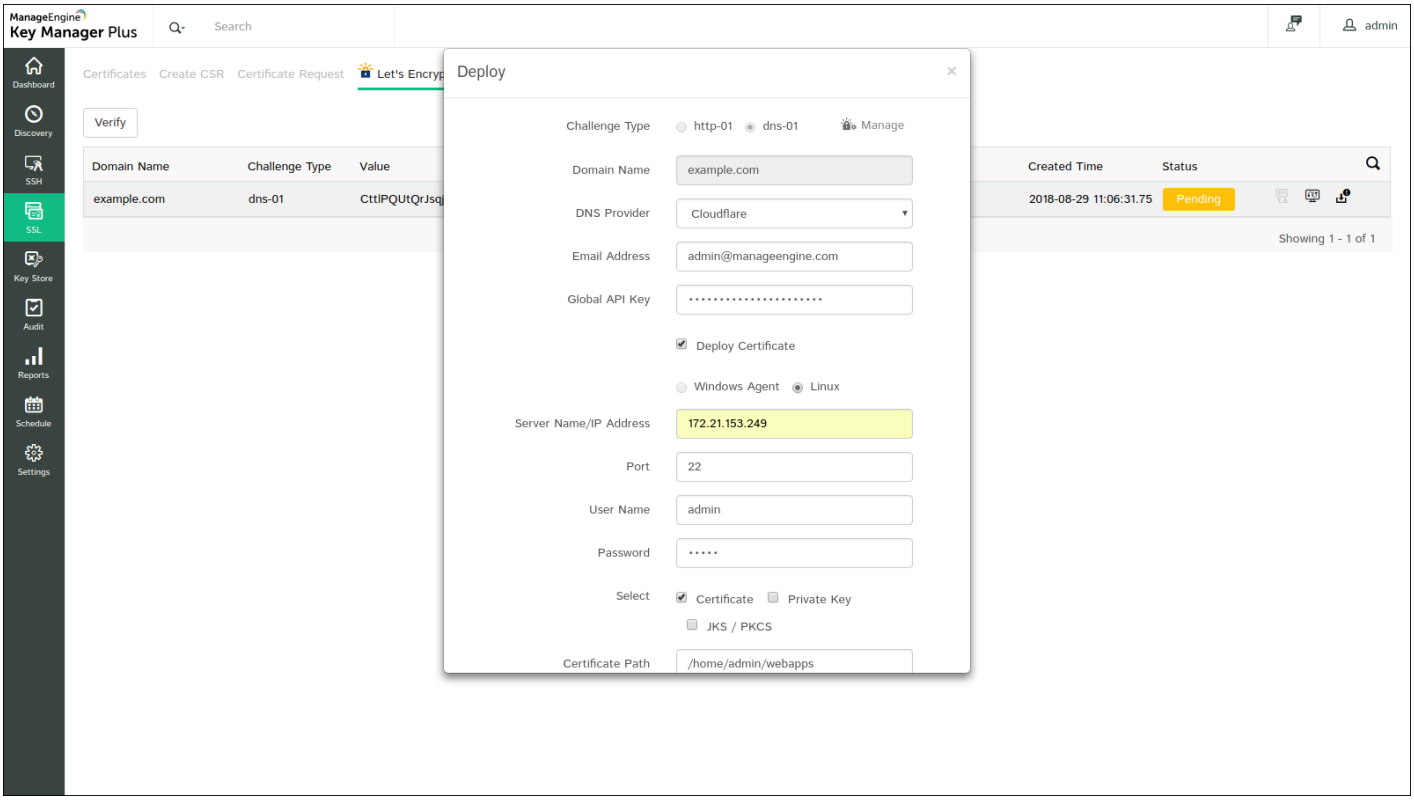


Keep close tabs on your expiring domains.

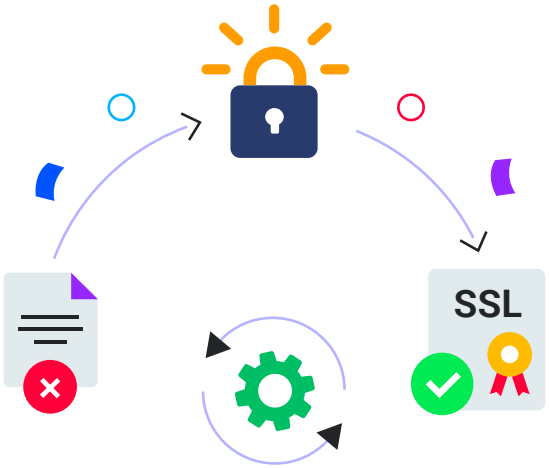


It's not uncommon for huge organizations to witness their domain names unexpectedly expire. That's because it's quite daunting for IT admins-who often juggle hundreds of domains to manually keep track of every domain that's about to expire and initiate a timely renewal. Expired domains pose a huge risk since they not only result in service interruption due to website outages, but also negatively impact the brand's credibility among visitors.

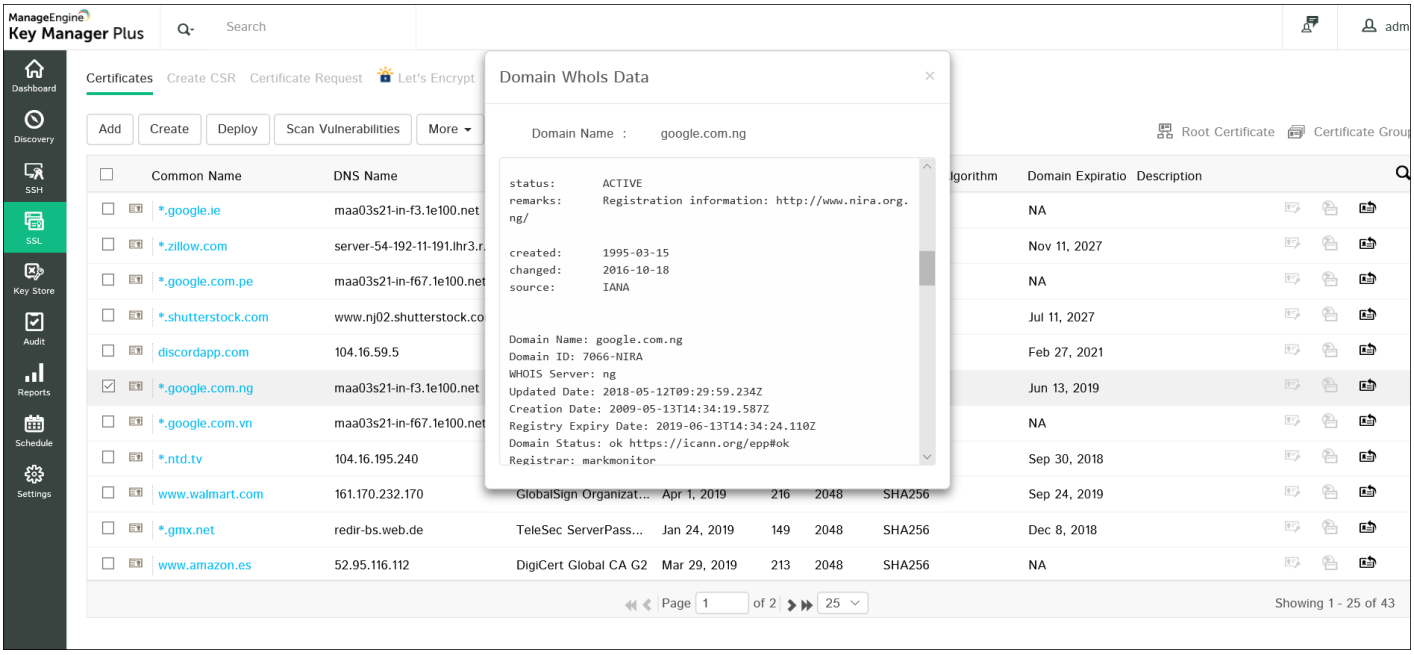
Key Manager Plus keeps admins informed about domain expiration through effective in-product and email notifications. Furthermore, its built-in domain lookup tool provides users the option to search for and obtain information about any registered domain on the internet such as ownership details, expiration date, IP address history, and more. This gives admins ample time to renew their domains well before expiration, saving them from the perils of domain ownership loss.



Accelerate renewal and deployment of Let's Encrypt certificates through automated domain verification.



When acquiring certificates from Let's Encrypt CA for public domains, administrators have to complete certain challenges to prove they own the domain. Key Manager Plus now facilitates automated verification of DNS-based challenges for domain validation when renewing certificates acquired from Let's Encrypt. With a few simple configurations, Key Manager Plus allows admins to completely automate certificate renewals, deploy new certificates to their corresponding end-servers, and achieve a complete end-to-end certificate management experience without any manual intervention.



4141 Hacienda Drive
Pleasanton,
California 94588, USA
Phone: +1-925-924-9500
Fax: +1-925-924-9600
Email: sales@manageengine.com

ManageEngine
KeyManager Plus