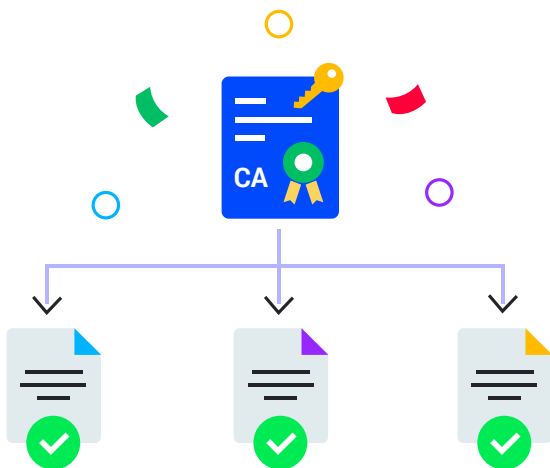


What's new in Key Manager Plus 5610

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

The screenshot shows the ManageEngine Key Manager Plus interface. A 'Certificate Signing' dialog box is open, displaying the following options:

- Sign Type: Sign with Root
- Select Certificate: sampleroot.com
- Validity: [] days

A 'Sign' button is visible. The background shows the 'Certificates' section with a table listing certificates:

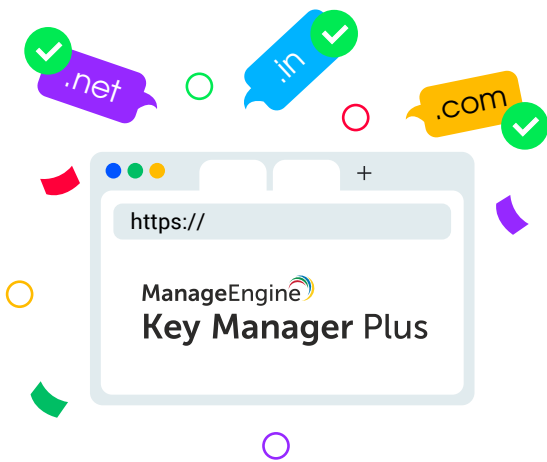
Domain Name	Created By
clientcertificate.com	admin

Below the table, there is a 'Help' section with the following text:

Ensure Key Manager Plus service is started with the same domain administrator account to sign certificates

- Key Manager Plus supports two...
Microsoft CA: This sign type forwards the CSR to the Microsoft Certificate Authority within your network and adds the acquired certificate to Key Manager Plus' centralized repository.
Sign with Root: This sign type enables you to create / denominate a root certificate with which you can sign the CSR and issue certificates to various systems within your network.
- Import Certificate [] option pins the private key with the certificate file acquired from trusted certificate authorities and adds the certificate to Key Manager Plus' centralized repository.

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.

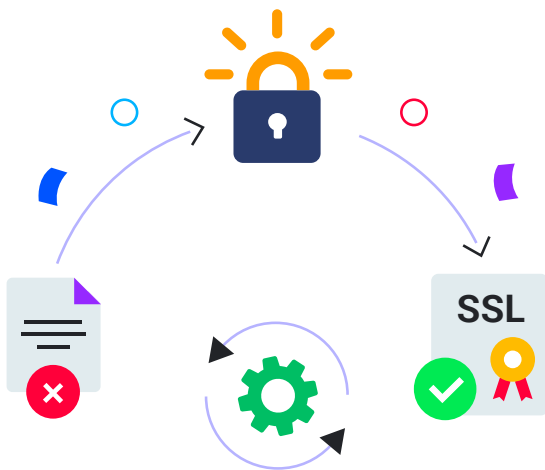
Key Manager Plus keeps admins informed about domain expiration through effective in-product and email notifications. Furthermore, its built-in domain lookup tool provides users the option to search for and obtain information about any registered domain on the internet such as ownership details, expiration 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.

A screenshot of the ManageEngine Key Manager Plus web interface. The interface includes a sidebar with navigation options like Dashboard, Discovery, SSH, SSL, Key Store, Audit, Reports, Schedule, and Settings. The main content area shows a 'Verify' button and a table with columns for Domain Name, Challenge Type, and Value. A 'Deploy' dialog box is open in the foreground, containing the following fields and options:

- Challenge Type: http-01 dns-01 Manage
- Domain Name:
- DNS Provider:
- Email Address:
- Global API Key:
- Deploy Certificate
- Windows Agent Linux
- Server Name/IP Address:
- Port:
- User Name:
- Password:
- Select: Certificate Private Key
- JKS / PKCS
- Certificate Path:

In the background, a table shows a certificate entry with 'Created Time' 2018-08-29 11:06:31.75 and 'Status' Pending.

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.

Common Name	DNS Name	Algorithm	Domain Expiration	Description
*.google.ie	maa03s21-in-f3.1e100.net	NA	Nov 11, 2027	
*.zillow.com	server-54-192-11-191.lhr3.r	NA	Jul 11, 2027	
*.google.com.pe	maa03s21-in-f67.1e100.net	NA	Feb 27, 2021	
*.shutterstock.com	www.nj02.shutterstock.co	NA	Jun 13, 2019	
discordapp.com	104.16.59.5	NA	Sep 30, 2018	
*.google.com.ng	maa03s21-in-f3.1e100.net	GlobalSign Organizat...	Apr 1, 2019	216 2048 SHA256
*.google.com.vn	maa03s21-in-f67.1e100.net	TeleSec ServerPass...	Jan 24, 2019	149 2048 SHA256
*.ntd.tv	104.16.195.240	DigiCert Global CA G2	Mar 29, 2019	213 2048 SHA256
www.walmart.com	161.170.232.170		Sep 24, 2019	
*.gmx.net	redir-bs.web.de		Dec 8, 2018	
www.amazon.es	52.95.116.112		NA	