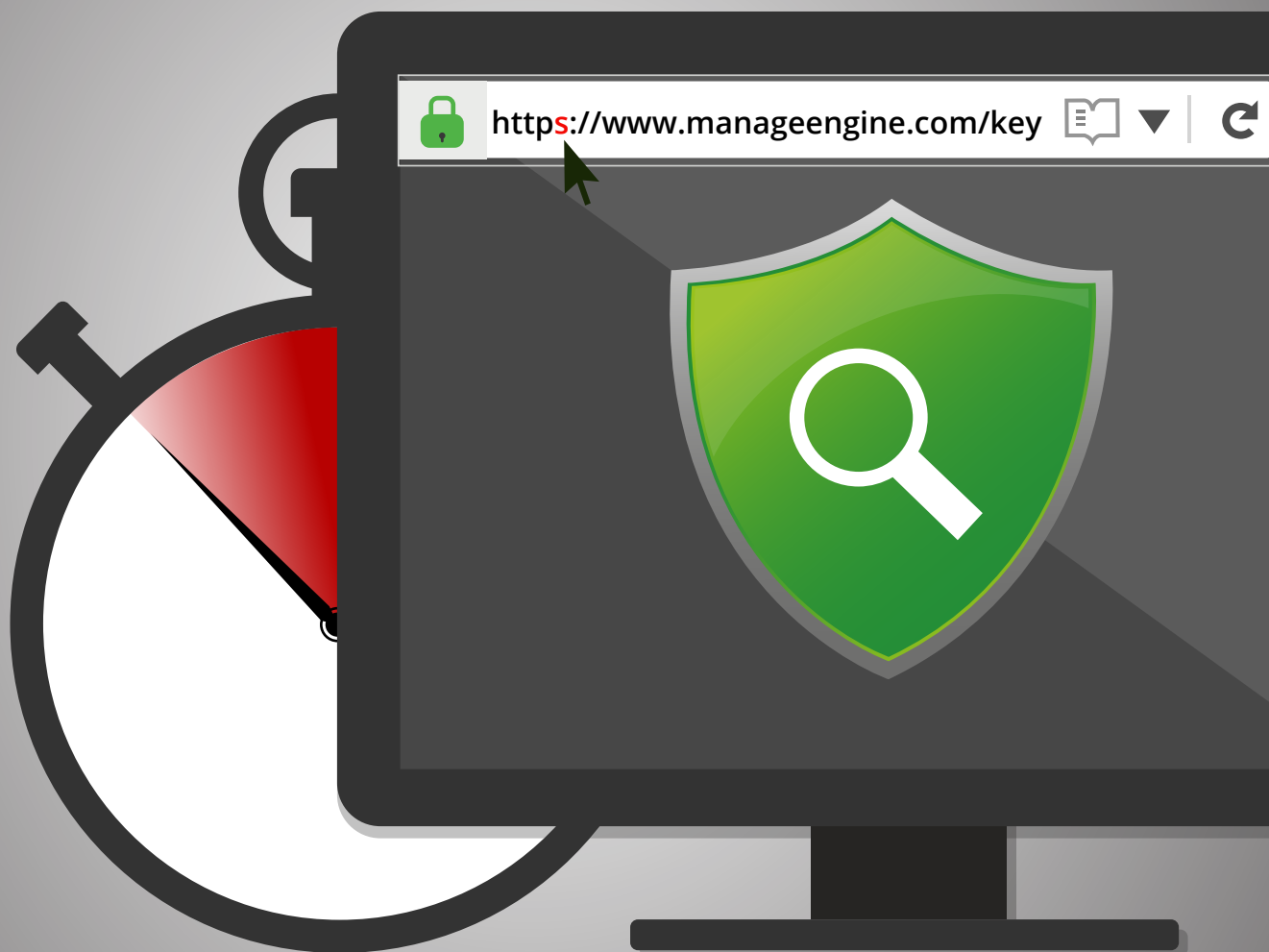


SHA-1 is now obsolete!

Make your migration to SHA-2 seamless with Key Manager Plus.

A step-by-step migration guide to SHA-2 signed SSL certificates.



SHA-1 (Secure Hash Algorithm 1) is simply not secure. It can lead to system downtime, errors, and security threats. Therefore, all organizations need to migrate to SHA-2 signed certificates before January 1, 2017. This document provides step-by-step instructions to identify all SHA-1 certificates in your organization and migrate to SHA-2 using ManageEngine Key Manager Plus.

Overview

The Secure Socket Layer (SSL) protocol has become the de facto standard for securely transmitting sensitive information over the internet. However, its reliability depends on underlying cryptographic hash algorithms. The majority of SSL certificates in use today have been signed using SHA-1, which is susceptible to collision attacks. This vulnerability will make it easy for hackers to spoof browsers with forged signatures.

The National Institute of Standards and Technology (NIST) has banned the use of SHA-1 for new certificates, and browser companies have announced that they will stop accepting SHA-1 certificates starting January 1, 2017. Soon, websites that use SHA-1 certificates will stop functioning or start throwing errors. So, organizations should switch all their certificates from SHA-1 to SHA-2 immediately.

Why SHA-1 to SHA-2 migration is important for your business?

Despite being unsafe, SHA-1 is the most widely used hash algorithm. Using SHA-1 presents the following threats:

- It is increasingly vulnerable to real-world forgery attacks, putting your company's security at stake.
- All the trusted certificate authorities (CAs) have already announced that they will stop issuing SHA-1 certificates starting January 2016.
- Today, all leading browsers display "secure but with minor errors" (🔒⚠️) warnings for websites that have SHA-1 certificates expiring between January 2016 and December 2016. This risks the reputation of your organization.
- Leading browsers including Chrome and Firefox display "affirmatively insecure" (🔒❌) errors for websites using SHA-1 certificates expiring after December 31, 2016.
- Likewise, Microsoft will stop accepting all SHA-1 certificates starting January 1, 2017, and is even planning to accelerate the deprecation timeline.

SHA-2 adoption: The challenges

Switching to the secure SHA-2 hashing algorithm is easier said than done. But with Key Manager Plus, a web-based key management solution, it doesn't have to be. Key Manager Plus helps you consolidate, control, manage, monitor, and audit the entire life cycle of SSL certificates. This migration guide breaks down your migration plan step by step. But here's a quick overview:

- Get a list of all SSL certificates in use.
- Identify and isolate the certificates that have been signed with SHA-1.
- Get in touch with the certificate issuing authority, submit a fresh certificate signing request, and get a new certificate signed with SHA-2.
- Deploy the new certificate to your respective sites to ensure security.
- Keep track of the use and expiration of the newly deployed certificate.

This is a lot to do manually, especially when it's so easy to make mistakes. Key Manager Plus expedites this migration process so all it takes is the following four steps.

1. Discover every SHA-1 certificate in your organization

In order to migrate all SHA-1 certificates, you have to identify them first. Key Manager Plus can discover all SHA-1 certificates in your network with a single click.

- In Key Manager Plus, go to the Discovery tab.
- Click on the **SSL** button.
- Specify the host name and click **Discover**.

This will display all the SSL certificates in your network. Once you have complete visibility of your SSL environment, it's easy to identify all certificates signed with SHA-1.

ManageEngine
Key Manager Plus

Search

Download

demouser

Discovery

Select ☐ SSH ☒ SSL

Discover by ☒ Hostname / IP Address ☐ IP Address Range ☐ From file

Hostname / IP Address

Time out seconds per resource

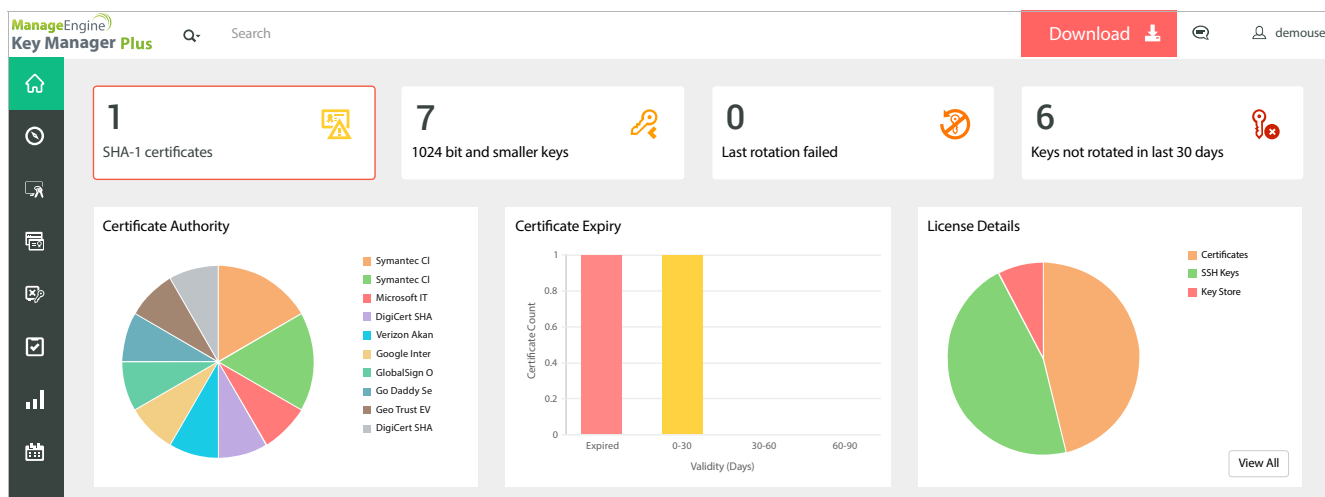
Port (Multiple ports separated by commas)

Discover

2. Isolate the SHA-1 certificates

Key Manager Plus' central repository tells you how many SSL certificates you have in total. All you have to do is go to **SSL**, and then **Certificates**. Click on a certificate to view more details.

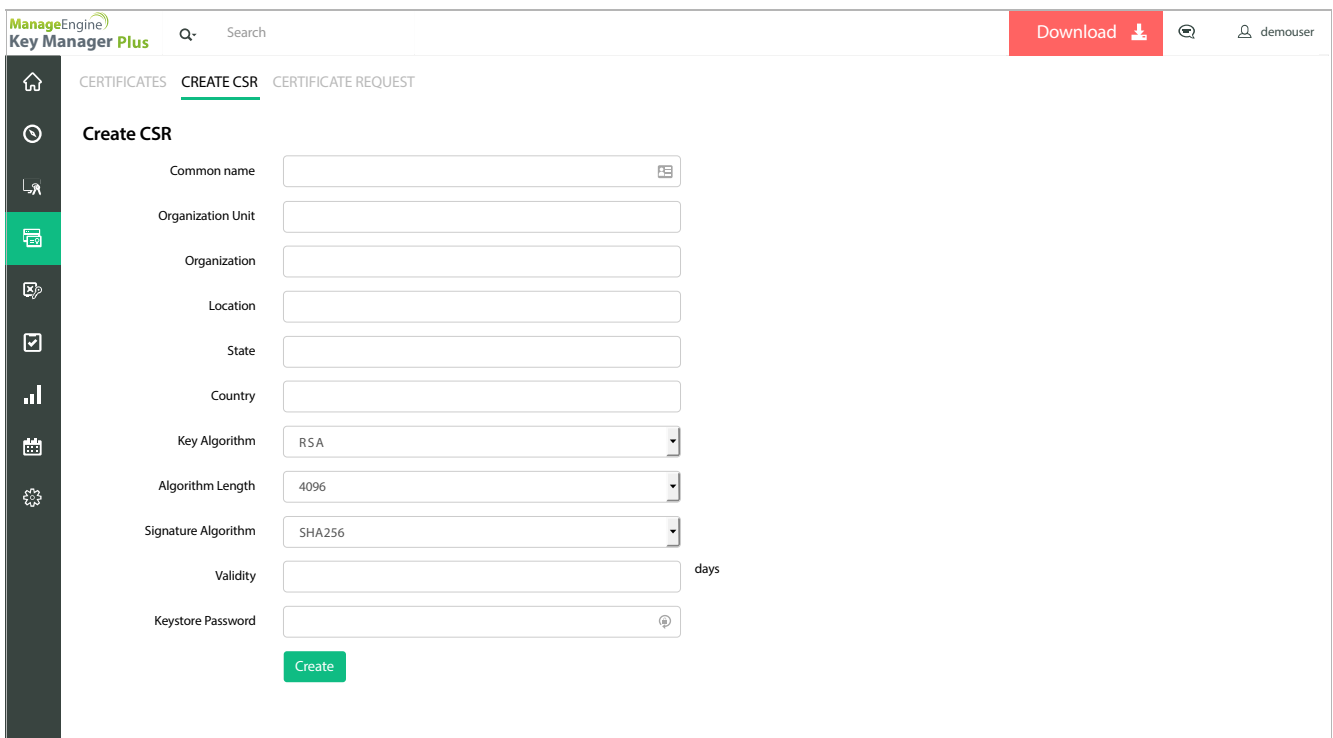
The **Dashboard** in the user interface also shows a consolidated count of SHA-1 certificates in use. Click on this count to view a table of all certificate details. This way, you can easily isolate all certificates signed with SHA-1.



3. Generate and centrally control new certificate signing requests

With Key Manager Plus, you can generate and centrally control certificate signing requests (CSR), which is how you obtain new SHA-2 certificates. To create a new CSR:

- Navigate to **SSL**, and then the **Create CSR** tab.
- Click the **Create** button.
- Enter your organization's name and certificate validity. Then, select the key algorithm and its length, the signature algorithm, and enter a keystore password.
- Click the **Create** button. You will be redirected to the certificate window where the contents of the CSR will display.
- You can then copy or export the contents to any required system or email it directly to the CA.



The screenshot shows the 'Create CSR' form in the ManageEngine Key Manager Plus interface. The form is titled 'Create CSR' and is located under the 'CERTIFICATES' tab. It contains the following fields and options:

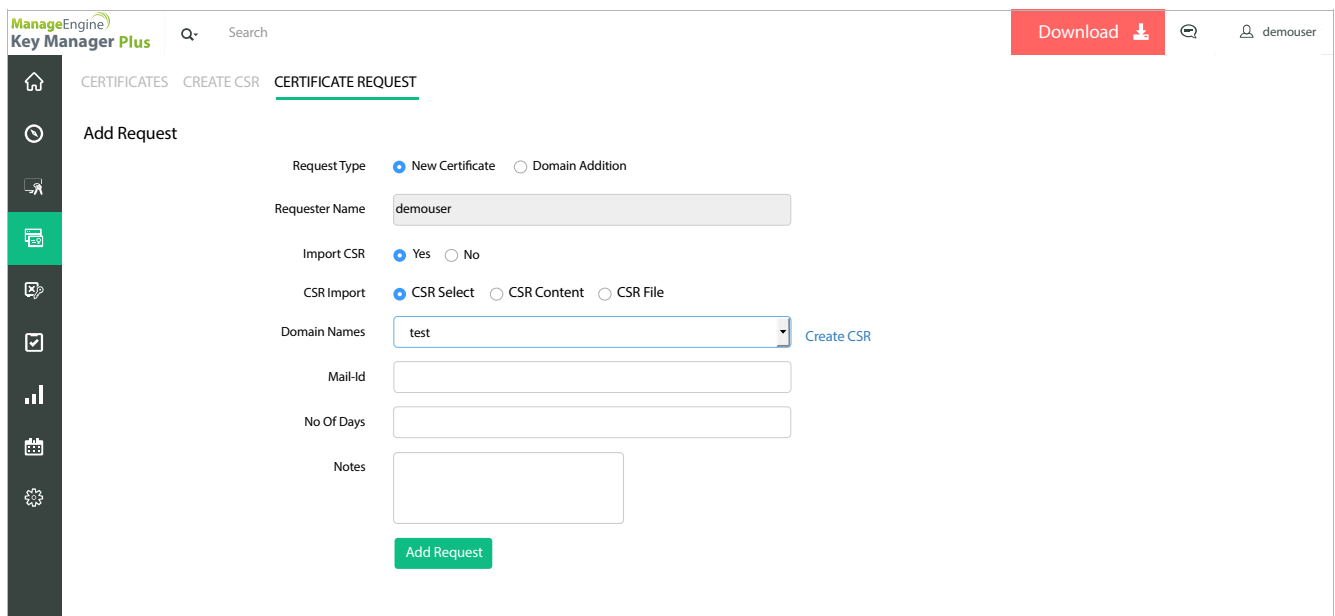
- Common name**: Text input field.
- Organization Unit**: Text input field.
- Organization**: Text input field.
- Location**: Text input field.
- State**: Text input field.
- Country**: Text input field.
- Key Algorithm**: Dropdown menu with 'RSA' selected.
- Algorithm Length**: Dropdown menu with '4096' selected.
- Signature Algorithm**: Dropdown menu with 'SHA256' selected.
- Validity**: Text input field with 'days' unit.
- Keystore Password**: Text input field with a password icon.
- Create**: Green button at the bottom.

The interface also includes a sidebar with navigation icons, a top navigation bar with 'CERTIFICATES', 'CREATE CSR', and 'CERTIFICATE REQUEST' tabs, and a top right bar with 'Download', 'demouser', and a search bar.

4. Import, deploy, and consolidate the new SHA-2 certificates

The *Certificate request* feature helps you track the whole process from CSR creation to the certificate authority. Navigate to **SSL, CERTIFICATE REQUEST**, and then **Add Request**.

- Attach the freshly created CSR to the certificate request and provide the certificate authority's email address.
- Click on **Add Request**.
- The request is automatically elevated to the **Open** state.
- Once you receive the new certificate, attach it to and close the request.
- The request then moves to the **Closed** state and the new certificate is added to Key Manager Plus' centralized repository.



The screenshot shows the 'Add Request' form in the ManageEngine Key Manager Plus interface. The form is titled 'Add Request' and is located under the 'CERTIFICATE REQUEST' tab. The form includes the following fields and options:

- Request Type:** Radio buttons for 'New Certificate' (selected) and 'Domain Addition'.
- Requester Name:** Text input field with the value 'demouser'.
- Import CSR:** Radio buttons for 'Yes' (selected) and 'No'.
- CSR Import:** Radio buttons for 'CSR Select' (selected), 'CSR Content', and 'CSR File'.
- Domain Names:** Text input field with the value 'test' and a 'Create CSR' button.
- Mail-Id:** Text input field.
- No Of Days:** Text input field.
- Notes:** Text area.
- Add Request:** Green button at the bottom.

The interface also features a sidebar with navigation icons, a top navigation bar with 'CERTIFICATES', 'CREATE CSR', and 'CERTIFICATE REQUEST' tabs, and a top right area with a 'Download' button and a user profile icon labeled 'demouser'.

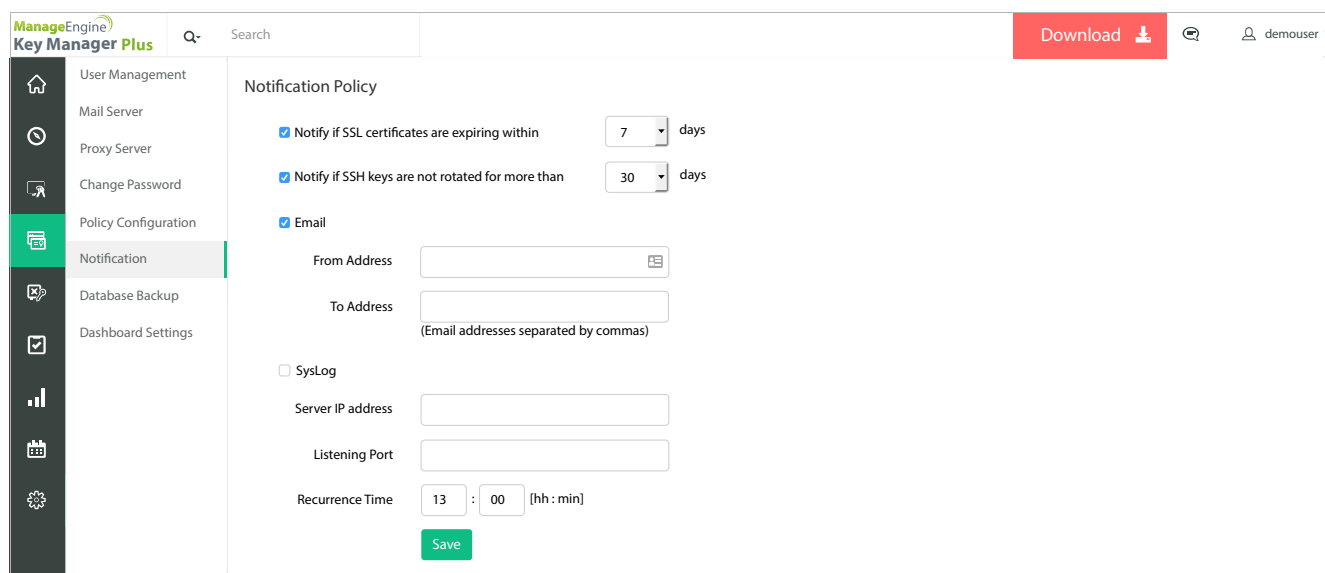
Key Manager Plus also comes with the following features to help you manage and control your SSL environment effectively after migration.

Track all certificate details

Key Manager Plus keeps track of new certificate details including the date of issue and expiration, certificate issuing authority, underlying encryption and signature algorithms, key length, and intermediate CA and certificates (if any).

Receive timely expiration alerts

Manually monitoring SSL certificate expiration dates is a lot of work. But improper monitoring just isn't worth the risk. Key Manager Plus solves this problem by providing timely alerts when the certificates are about to expire.



The screenshot shows the 'Notification Policy' configuration page in the Key Manager Plus interface. The left sidebar contains a navigation menu with options: User Management, Mail Server, Proxy Server, Change Password, Policy Configuration (highlighted), Notification (selected), Database Backup, and Dashboard Settings. The main content area is titled 'Notification Policy' and includes the following settings:

- ☒ Notify if SSL certificates are expiring within days
- ☒ Notify if SSH keys are not rotated for more than days
- ☒ Email
 - From Address:
 - To Address: (Email addresses separated by commas)
- ☐ SysLog
 - Server IP address:
 - Listening Port:
 - Recurrence Time: : [hh : min]

A green 'Save' button is located at the bottom of the configuration area. The top of the interface features the 'ManageEngine Key Manager Plus' logo, a search bar, a 'Download' button, and a user profile icon labeled 'demouser'.

Try Key Manager Plus now!

Need free consultation on SHA-2 migration?

If you need our support in migrating to SHA-2 (or) a personalized demo of Key Manager Plus, please write to us at keymanagerplus-support@manageengine.com. We'll get in touch with you immediately.