ManageEngine
Key Manager Plus

# DATASHEET

**Web-based SSH key and SSL certificate management solution for enterprises.**

## What does it do?

ManageEngine Key Manager Plus is a web-based key and certificate management solution that helps enterprises discover, consolidate, create, deploy, audit, and track the life cycles of SSH (Secure Socket Shell) keys and SSL/TLS (Secure Sockets Layer/Transport Layer Security) certificates. It provides complete visibility and control over the SSH and SSL environments and helps administrators take total control of digital identities to preempt breaches and compliance issues.

## Why is it important?

Safeguarding data in transit has always been a big challenge for IT security administrators. SSH keys help organizations ensure security in remote administrative access and data transfer, but they also present some unique challenges.

Usually, SSH keys are left unmonitored and unmanaged, making organizations vulnerable to cyberattacks. In the absence of an automated system, getting the list of all the keys in use, finding and restricting access privileges, and ensuring periodic rotation is a herculean task.

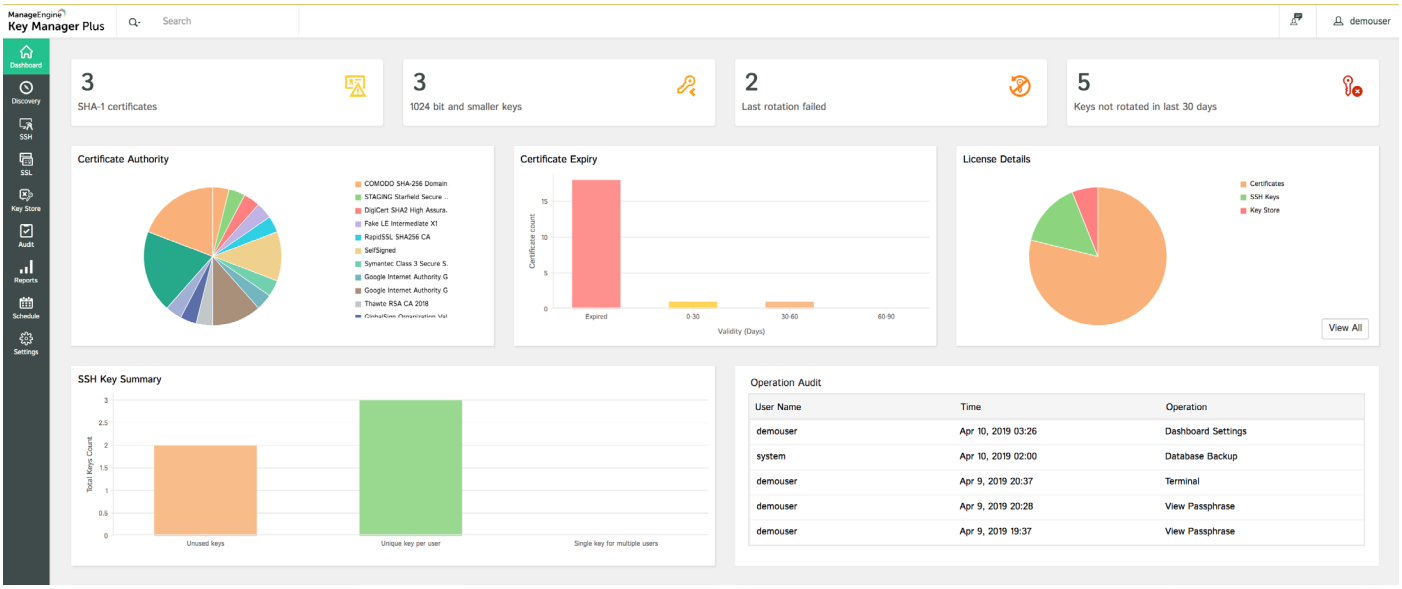
Similarly, managing an SSL/TLS environment can be daunting, especially when organizations use a large number of SSL certificates issued by different certificate authorities with different validity periods. SSL certificates, when left unmanaged can expire unexpectedly, or rogue/invalid SSL certificates could be used. Both scenarios can lead to service downtimes or display error messages that hurt your brand credibility, and in extreme cases, result in security breaches.

Therefore, enterprises need a solution that can centralize and automate the management of these digital identities and thwart misuse of privileges caused by inappropriate usage keys and certificates.

# Benefits

- Gain complete visibility of all SSH keys and SSL certificates present in your organization, and achieve centralized control.
- Remove existing public key-user trust relationships, and generate new key pairs. Deploy the new public keys to users in bulk, and enforce periodic rotation directly from Key Manager Plus.
- Acquire SSL certificates from trusted certificate authorities for your public websites through a hassle-free certificate request workflow.
- Achieve end-to-end certificate life cycle management through centralized deployment, vulnerability scans, and recurring notifications when certificates are about to expire.
- Get instant access to tamper-proof, real time audit trails and comprehensive reports on all operations performed around key and certificate management.

Centralized dashboard providing at-a-glance view of overall SSL/SSH related operations.



# Salient features

## SSL certificate management

### SSL/TLS certificate discovery
Discover all SSL/TLS certificates deployed in your network and add them to a secure, centralized inventory.

### Certificate request workflow
Generate CSRs instantly; request and acquire public CA certificates through a hassle-free certificate request workflow.

### Centralized deployment
Centralize the deployment of newly acquired certificates to their respective end-servers.

### SSL vulnerability scan
Identify and remediate vulnerable SSL configurations and weak ciphers, and replace any revoked certificates.

### Active Directory integration
Readily integrate, import, and manage certificates mapped to user accounts in Active Directory.

### SHA-1 certificate flagging
Identify and replace certificates that use the obsolete SHA-1 hashing function.

### Expiration alerts
Eliminate service downtime by receiving customizable, recurring notifications on certificates that are about to expire.

## SSH key management

### SSH key discovery
Discover all SSH keys in your network and add them to a secure, centralized repository.

### Key creation and deployment
Create new SSH key pairs; associate them with users in bulk and deploy them to target systems.

### Periodic key rotation
Create scheduled tasks to rotate SSH keys automatically at periodic time intervals to avoid privilege misuse.

### Key-user mappings
Get a holistic view of key-user relationships across your organization through distinct mapping of individual keys with their respective user accounts.

### Remote SSH connections
Launch one-click SSH connections to remote systems.

### Disaster recovery
Schedule backups of your entire database at periodic intervals for disaster recovery purposes.

### Auditing and reports
Establish a tamper-proof auditing mechanism and get instant access to comprehensive reports on all user activities.

# Hardware requirements

The below table explains the minimum hardware capabilities that your Key Manager Plus application server needs to possess for successful installation and running.

| Organization Size | Processor | RAM | Hard Disk |
|---|---|---|---|
| Small<br>(Less than 500 keys*) | Dual Core / Core 2 Duo or above | 4 GB | • 300 MB for product<br>• 10 GB for database |
| Medium<br>(500 – 1000 keys*) | Quad Core or above | 8 GB | • 500 MB for product<br>• 20 GB for database |
| Large<br>(>1000 keys*) | Octa Core or above | 16 GB | • 1 GB for product<br>• 30 GB for database |

*The term 'keys' refers to the number of SSH private keys plus the number of SSL/TLS certificates plus any digital key managed using Key Manager Plus.

# Software requirements

## Operating Systems

### Windows

- Windows 10
- Windows 8
- Windows 7
- Windows Vista
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003
- Windows 2000 Server / Professional

### Linux

(Key Manager Plus usually works well with all the flavours of Linux)

- Ubuntu 9.x and above
- CentOS 4.4 & above
- Red Hat Linux 9.0
- Red Hat Enterprise Linux 5.3, 5.4, 5.5

**Note:** Key Manager Plus can also be run on the VMs of all the above operating systems.

### Supported Databases

- PostgreSQL 9.2.4 —comes bundled with the product.
- Supports MS SQL Server 2008 and above (SQL server should be installed in Windows 2008 Server or above).

### Supported Browsers

The HTML client requires one of the following browsers to be installed on the application server.

- IE 9 and above (on Windows)
- Chrome & Firefox (on Windows, Linux, and Mac)

## Prerequisite Software

There is no prerequisite software installation required to use Key Manager Plus. You just need to have the above mentioned hardware and software requirements plus an external mail server (SMTP server) to send email notifications to the users.

Apart from this, you need to have the following capabilities additionally if you are planning to utilize the SSH and SSL discovery operations in Key Manager Plus.

- A service account that has domain admin rights in the Key Manager Plus server and in the target systems that you would like to manage.
- Microsoft .NET framework.

# SSL Certificate Management

| Supported SSL Discovery | CA Integration |
|---|---|
| AD user certificates<br>Certificates in Microsoft Certificate Store<br>Certificates issued by Microsoft Certificate Authority<br>SMTP server certificates<br>Load balancer certificates<br>Certificates hosted in AWS—ACM & IAM<br>Self-signed certificates | Let's Encrypt<br>Microsoft CA<br>GoDaddy<br>Sectigo<br>Symantec<br>Thawte<br>GeoTrust<br>RapidSSL<br>DigiCert |

| Private Key Algorithm | Private Key Length (bit) | Signature Algorithm |
|---|---|---|
| RSA<br>DSA<br>EC | 1024<br>2048<br>4096 | SHA256<br>SHA384<br>SHA512 |

| Keystore Type | SSL Vulnerability Detection |
|---|---|
| JKS<br>PKCS12 | Certificate revocation status—CRL, OCSP<br>Heartbleed<br>POODLE<br>Weak cipher suites |

# SSH Key Management

| SSH Key Type | SSH Key Length (bit) | Signature Algorithm |
|---|---|---|
| RSA<br>DSA<br>ECDSA<br>ED25519 | 1024<br>2048<br>4096 | SHA256<br>SHA384<br>SHA512 |

## Other specifications

| Authentication Methods | Supported SSH, SSL/TLS Versions |
|---|---|
| Local (username and password)<br>Active Directory<br>RADIUS | SSH-2<br>SSL 3.0<br>TLS 1.0<br>TLS 1.1<br>TLS 1.2 |

*Key Manager Plus enables us to stay on top of SSL certificates for all of our websites. With Key Manager Plus, we're able to monitor which certificates are nearing expiration and roll out new certificates in a timely manner.*

**Ken Odibe**
Senior cloud infrastructure consultant,
Sapphire Systems

Schedule a personalized demo

Get a quote

Zoho Corporation
4141 Hacienda Drive,
Pleasanton, CA 94588
Phone: +1-925-924-9500

ManageEngine
Key Manager Plus