ManageEngine
Key Manager Plus

Security and Privacy Specifications

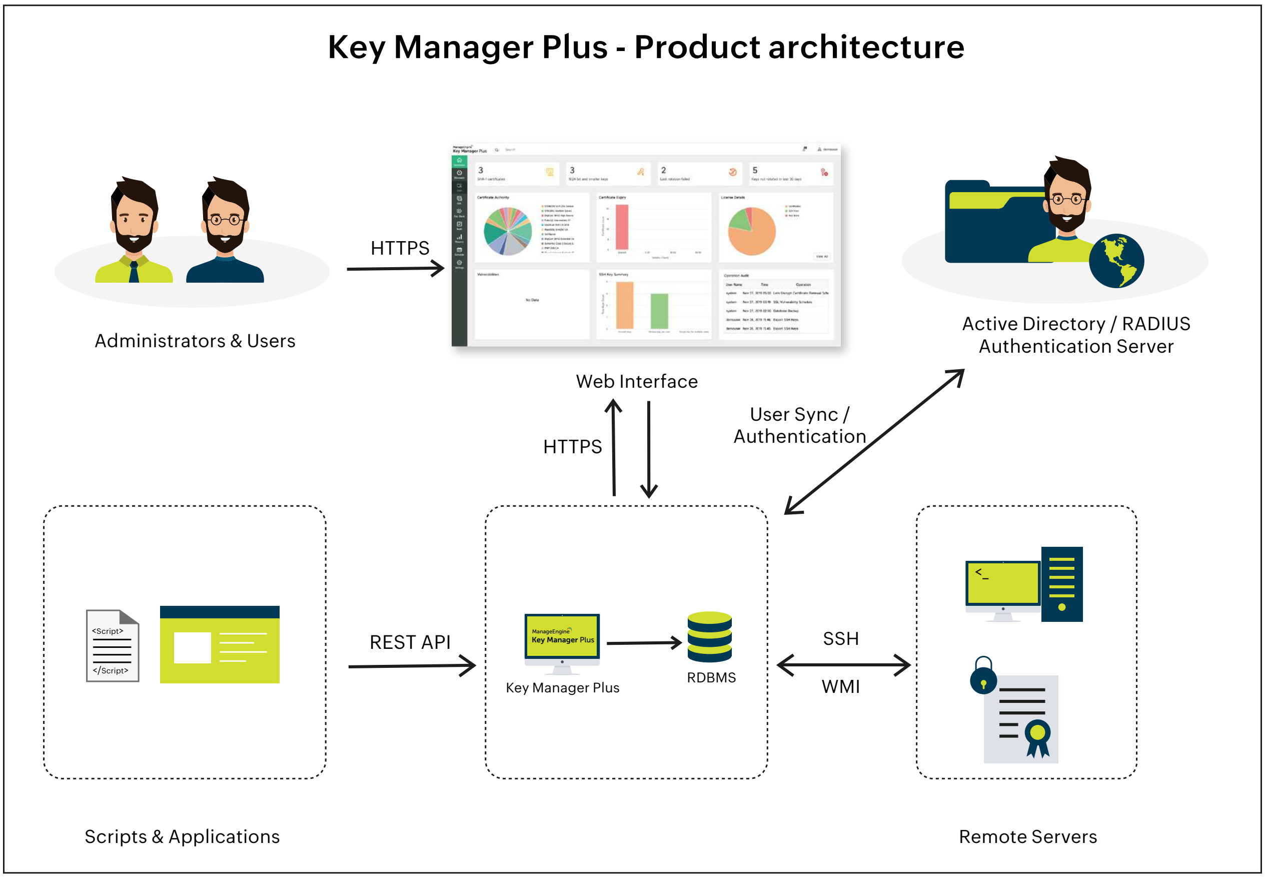
www.keymanagerplus.com

Overview

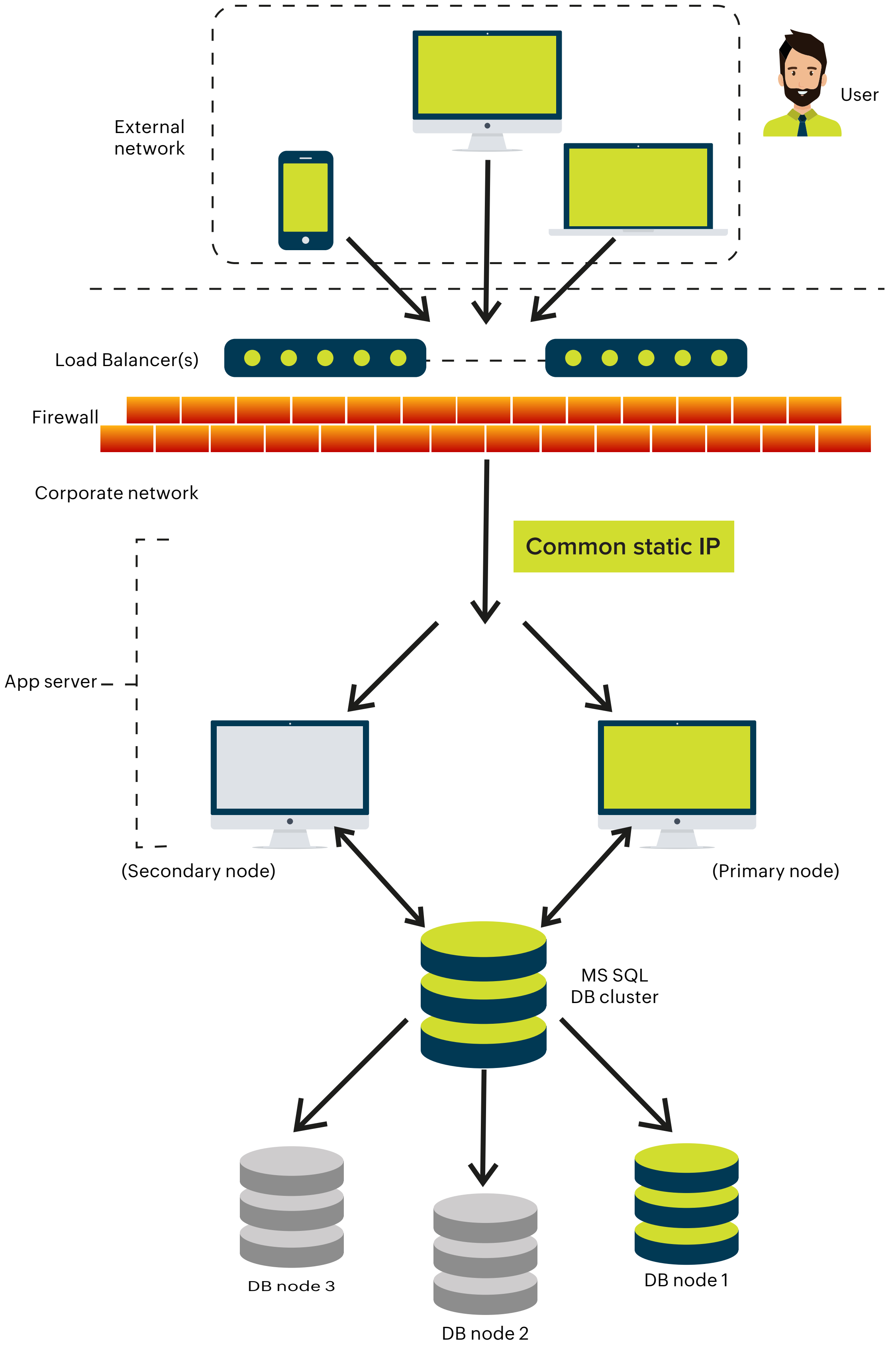
Key Manager Plus stores and manages digital keys that grant access to various critical assets within your organization. The growing transition towards password-less authentication has increased businesses' dependency on digital keys to authenticate users into privileged assets within their network. A secure, central, and streamlined key management mechanism is therefore vital to prevent rampant proliferation of keys, which when unmonitored, could result in privilege abuse and eventually a breach of sensitive data.

For this reason, Key Manager Plus comes with a range of security and privacy checks tightly woven into its architectural design, that spans across various stages of the product workflow right from installation, user authentication, access control, to data transmission and storage. This document provides an overview of the security and privacy specifications in Key Manager Plus.

(**Note:** This document outlines the security and privacy settings specific to Key Manager Plus only. To read about ManageEngine's overall security policy, go to www.manageengine.com/security.html

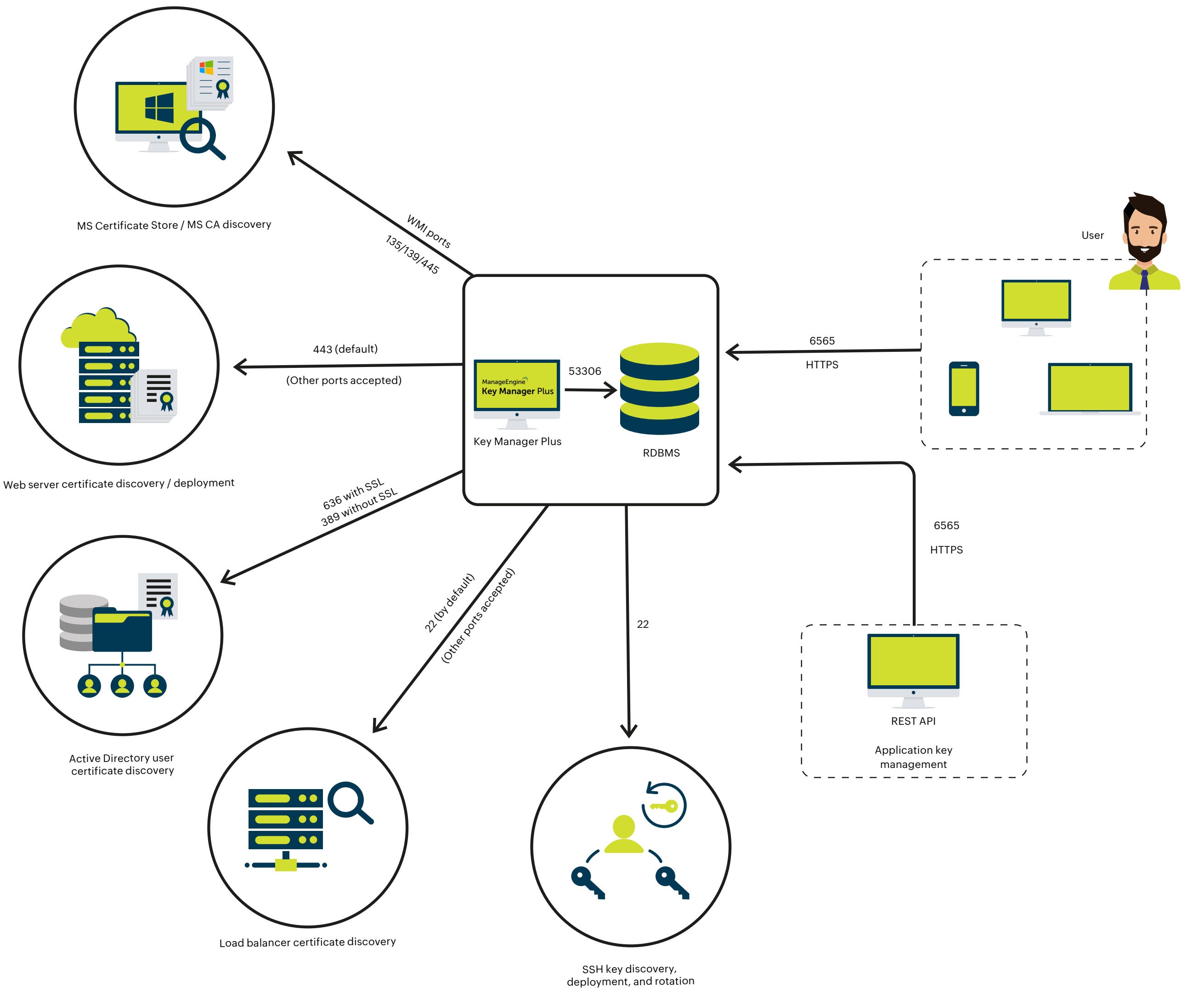


Key Manager Plus - Failover Architecture



(**Note:** Failover service available only for Windows installations of Key Manager Plus with MS SQL cluster as the backend database.)

Key Manager Plus - Data flow diagram


MS Certificate Store / MS CA discovery
WMI ports
135/139/445
User
443 (default)
(Other ports accepted)
6565
HTTPS
53306
ManageEngine
Key Manager Plus
Key Manager Plus
RDBMS
Web server certificate discovery / deployment
636 with SSL
389 without SSL
6565
HTTPS
22 (by default)
(Other ports accepted)
22
REST API
Application key management
Active Directory user certificate discovery
Load balancer certificate discovery
SSH key discovery, deployment, and rotation

Security specifications in Key Manager Plus	
1. Vaulting mechanism: Secure by Design	• AES-256 encryption • Dual encryption - at the application level and the database level • Master encryption key and encrypted data cannot reside together
2. Authentication and authorization	• Integration with identity stores like Microsoft Active Directory, any LDAP compliant directory service, and RADIUS • Unique accounts and strong local authentication
3. Industry-recommended key generation standards	• NIST-recommended encryption algorithms • Additional passphrase for keys
4. Data Security and Integrity	• **At rest** • Dual AES-256 encryption • **In transmission** • Secure, encrypted communication • between the client machine and application server • Secure, encrypted communication between the application server and RDBMS • Secure, encrypted communication between the primary and secondary Key Manager Plus server instances • HTTPS connections for inter-app communications with SSL/TLS certificate-based verification • Protection against SQL injection, cross-site scripting, buffer overflow, and other attacks

5. Access control measures	• Role-based access control mechanism • Automated SSH key rotation
6. Secure remote access and file transfer	• Remote SSH sessions from any HTML5 compatible browser • All connections are tunnelled through the Key Manager Plus server • No direct connectivity between the client machine and remote host • Secure, encrypted file transfer over SCP • Non-availability of remote host credentials in client machines
7. Audit, accountability control, and real time audit	• All operations audit • Real-time alerts for various events like certificate expiration, key rotation • Provisions to raise SNMP traps and Syslog messages • Video recording availability for remote SSH sessions
8. Availability mechanisms	• Failover Service
9. Disaster recovery	• Scheduled database backup • System failure and recovery

Privacy settings in Key Manager Plus

- Provision to purge audit trails
- Password protection for file exports
- Controls for personal data exposure in reports
- Provisions to manage non-user email addresses
- Options to disable product activity tracker

Security at various levels

Vaulting mechanism: Secure by design

- Key Manager Plus uses AES-256 encryption (the strongest known encryption that the US government has approved) to store all sensitive information.
- The application-level encryption key, which is also called the master key, is uniquely generated for every installation.
- The master key cannot be stored inside Key Manager Plus to prevent residing of the encryption key and encrypted data together in the same place.
- The recommended setup is to store the key in a physically separate server or device and ensure that it is available to the server during application start-up. Subsequently, the key is held only in the server memory and never written anywhere.
- The Key Manager Plus database is also encrypted through a separate key, which can either be stored in Key Manager Plus or any other secured location that is accessible by the application server.

Authentication and authorization

- Key Manager Plus readily integrates with third-party identity stores like Microsoft Active Directory, all LDAP compliant directory services, and RADIUS allowing administrators to import users from the respective identity stores. Users will be uniquely identified through their respective accounts in the identity store.
- Besides integration with identity stores, Key Manager Plus also comes with a local authentication mechanism allowing unique accounts to be created for individual users. Furthermore, only the administrator is given privileges to create user accounts, thereby ensuring access to the application is legitimate.

Industry-recommended key generation standards

- Key Manager Plus comes with NIST-recommended digital signature algorithms and key lengths, that allows creation and deployment of digital keys across your organization with strict adherence to industry standards.

- Key Manager Plus also provides passphrase encryption for private keys, which adds an additional layer of security by preventing unauthorized access in the unlikely event of a key compromise.
- Moreover, only the administrator user is entitled with the privileges to create keys, which ensures that the keys are not strewn across multiple endpoints and that access control is streamlined and centralized.
- Key Manager Plus comes with robust SSH key policies to replace existing key-user associations across your network with associations created via Key Manager Plus providing greater visibility and central control.

Data security and Integrity

Encryption at rest

- Key Manager Plus is designed as a web application with a web server for business logic and RDBMS for data store.
- Upon applying appropriate initialization vectors and other standard good practices around encryption, the first-level encryption key with AES-256 algorithm is generated in the web server.
- The encrypted data is then pushed to the RDBMS for storage by using SQL queries. Here, Key Manager Plus encrypts the data with built-in AES functions of RDBMS for dual layers of encryption.
- The video recorded remote SSH sessions are also encrypted before storage and can be played only through proprietary player because the data is stored in the proprietary format.

Encryption in transit

- All data transmission between the client interface and Key Manager Plus server are encrypted and takes place through HTTPS. The SSL/TLS certificate needed for server-client communication can be created and managed using Key Manager Plus itself.
- All data transmission between Key Manager Plus and the RDBMS occur over SSL/TLS.

- Key Manager Plus allows agents to be deployed to endpoints that can connect to the server. The communication is always one way, that is, the agent always initiates the connection. Therefore, only the server needs to be available for the agents, eliminating the need to punch firewall holes or creating VPN paths for the server to reach all agents. The agent periodically pings the server through HTTPS to check whether any operation is pending for execution. The agent will then carry out the tasks and after completing them, will notify the server back with the results.
- Communication between the primary and secondary Key Manager Plus server instances (that are mapped to a common MS-SQL cluster) is encrypted and occurs over HTTPS.
- Key Manager Plus facilitates application-to-application key and certificate management by exposing a web API which other applications can leverage and connect via HTTPS. The application's identity is verified by forcing it to issue a valid SSL certificate, matching the auth token details that has already been created and stored in Key Manager Plus.
- Key Manager Plus thoroughly validates all inputs in the GUI. Usage of special characters and HTML code are filtered, and the application is guarded against common attacks like SQL injections, cross-site scripting, buffer overflow, and other attacks.

Access control measures

- All data access in Key Manager Plus is subjected to the role-based access control mechanism. Users can see and access only those accounts that are assigned to them by the application administrator.
- All access to keys and certificates and all operations performed in any resource are captured in audit trails, ensuring accountability for all users and actions.
- Key Manager Plus facilitates automatic SSH key rotation at periodic time intervals via scheduled task creation to reduce risks of key compromise and unauthorized access to critical assets. Administrators can custom alerts for failed key rotations and for keys that have not been rotated in a long time.

Secure remote access and file transfer

- Key Manager Plus allows users to launch highly secure, reliable, and completely emulated SSH terminal sessions from any HTML5-compatible browser without the need for an additional plug-in or agent software.
- Remote connections to endpoints are tunneled through the Key Manager Plus server, requiring no direct connectivity between the user device and the remote host.
- Key Manager Plus facilitates secure, encrypted transfer of files between users' local machines and the remote host over SCP, ensuring the authenticity and confidentiality of data in transit.
- Besides superior reliability, the tunneled connectivity also provides extreme security, as the credentials (passwords or keys) needed to establish remote sessions don't need to be available on users' local machines.

Audit, accountability control, and real-time alerts

- Every operation and scheduled task carried out by users is audited. The audit logs are stored in the same database and are tamper-proof, ensuring non-repudiation.
- Key Manager Plus provides real-time alerts and notifications for various key- and certificate-related events, including access, certificate expiration, and key rotation. This enables administrators to take prompt corrective action.
- The audit module that captures all user and system operations also allows administrators to configure what events need to be sent to SIEM systems. The event alerts can either be sent as syslog messages or SNMP traps.
- All operations performed by users during remote terminal sessions are video recorded and securely stored. The recordings can later be watched on demand or used for forensic analysis.

Availability mechanisms

Failover service

The failover service in Key Manager Plus, which is aimed at ensuring uninterrupted access to keys and certificates, functions with redundant (two) Key Manager Plus server instances mapped to a common MS SQL cluster.

One instance will be the primary instance to which all users stay connected, and the other instance will act as secondary or standby server. The administrators and users can connect to the primary or secondary instance to access the GUI console via a desktop browser.

At any point in time, data in both the primary and secondary server instances will be in sync with one another. The data replication happens through a secure, encrypted channel.

Disaster recovery

Scheduled database backup

- Key Manager Plus allows administrators to configure scheduled database backups from within the product.
- All sensitive data in the backup file is stored in encrypted form in a .zip file in the application installation directory or in the destination directory configured by the admin.
- The backup copy will not have the encryption master key because Key Manager Plus does not allow both the encryption key and the encrypted data to reside together. Unless someone presents the encryption key, sensitive data cannot be deciphered from the backup copy.
- While a database backup operation is in progress, no configuration change can be performed in Key Manager Plus.

System failure and recovery

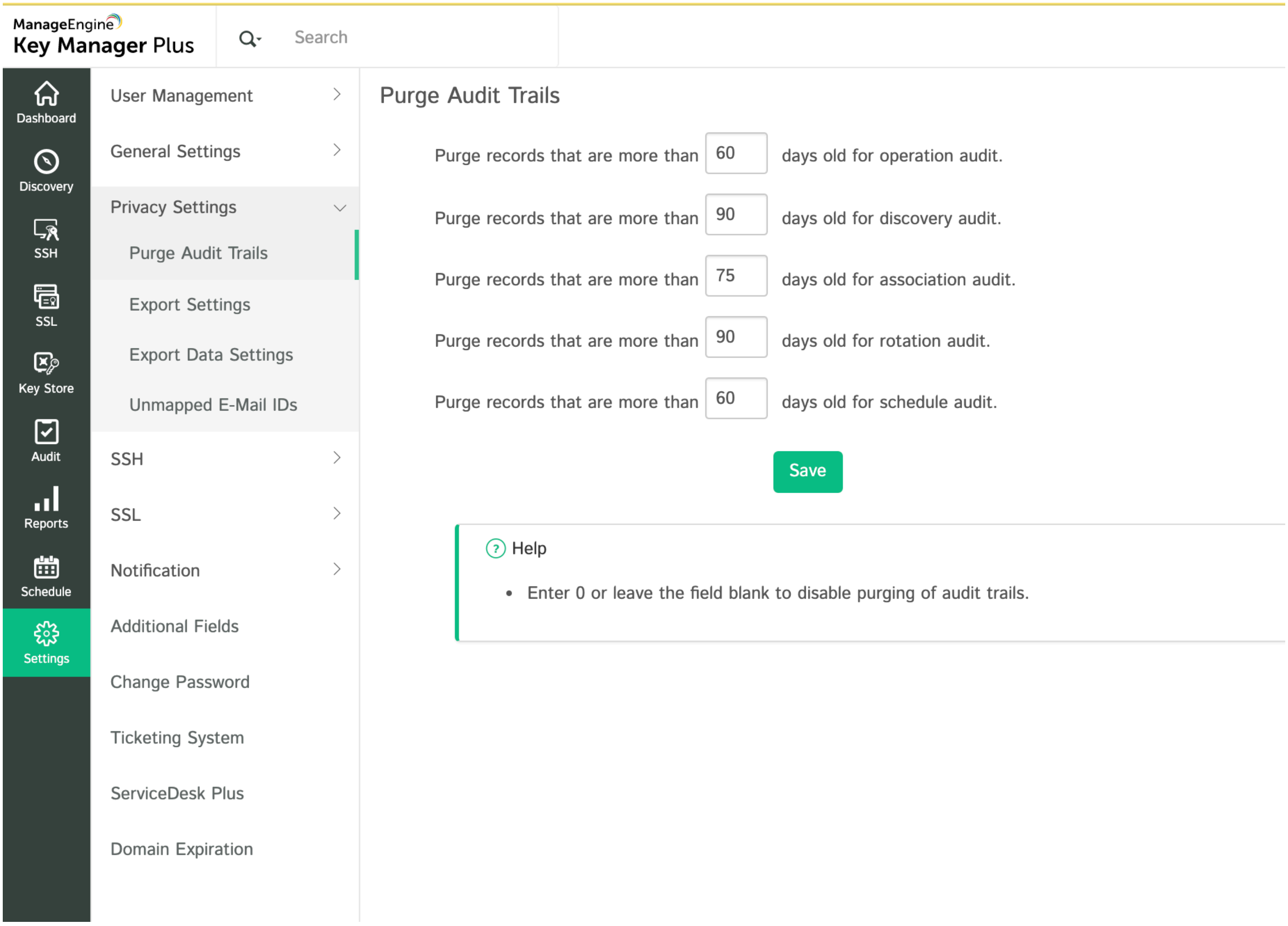
- In the event of a disaster or data loss, users can quickly make a fresh install of the same version of Key Manager Plus and restore the backed-up data to the database.

- Stop the Key Manager Plus server before trying to restore the data. If restoration is attempted while the server is running, it might lead to data corruption.
- Disaster recovery for Key Manager Plus with MS SQL Server as the back-end database can be performed only with the corresponding master key initially used for encryption upon installation.

Privacy settings in Key Manager Plus

Provision to purge audit trails

Key Manager Plus provides administrators with the option to purge old audit trails operation-wise, typically those that contain sensitive information and are no longer required for the purposes for which they were originally captured.



Purge Audit Trails

Purge records that are more than 60 days old for operation audit.

Purge records that are more than 90 days old for discovery audit.

Purge records that are more than 75 days old for association audit.

Purge records that are more than 90 days old for rotation audit.

Purge records that are more than 60 days old for schedule audit.

Help

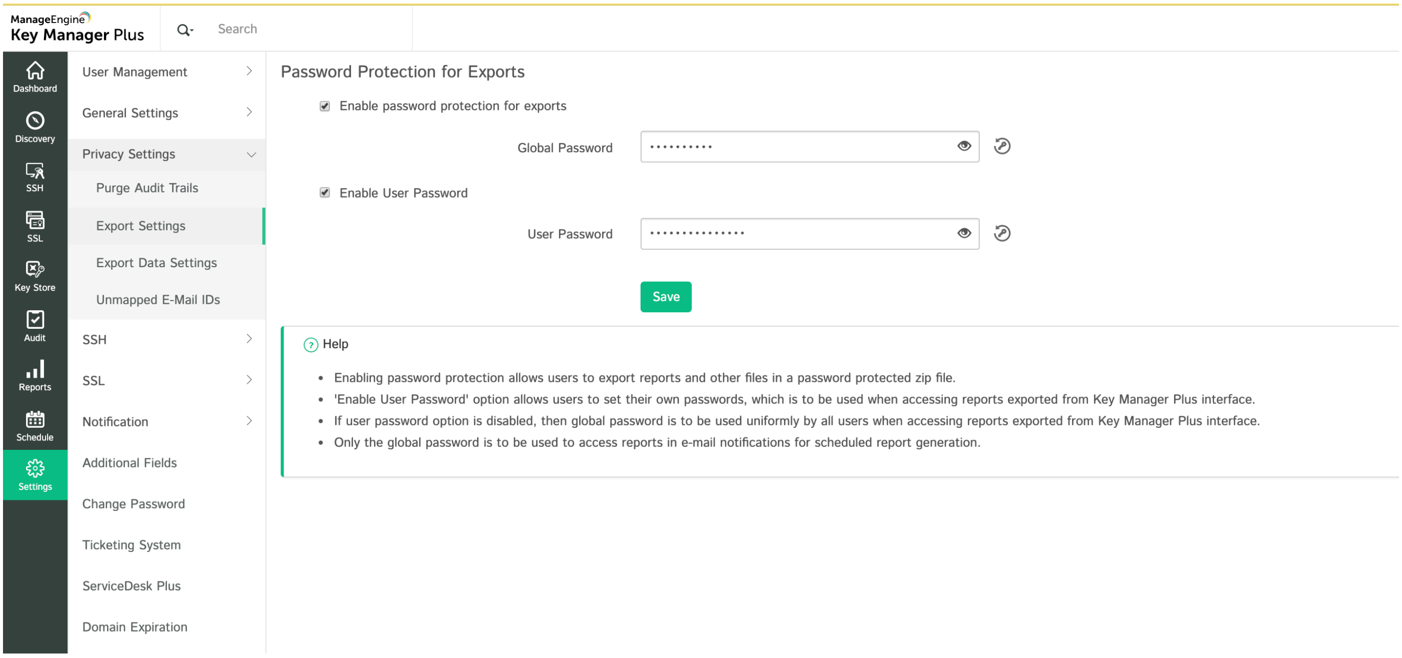
- Enter 0 or leave the field blank to disable purging of audit trails.

Password protection for file exports

Administrators can enable password protection for all files exported from Key Manager Plus. Key Manager Plus currently offers two levels of password protection for exports:

Global password: A uniform password applicable for all users when exporting files from Key Manager Plus.

User password: In addition to the global password, administrators can allow users to set their own separate passwords to be used when exporting files from Key Manager Plus.



Password Protection for Exports

☑ Enable password protection for exports

Global Password: ••••••••••

☑ Enable User Password

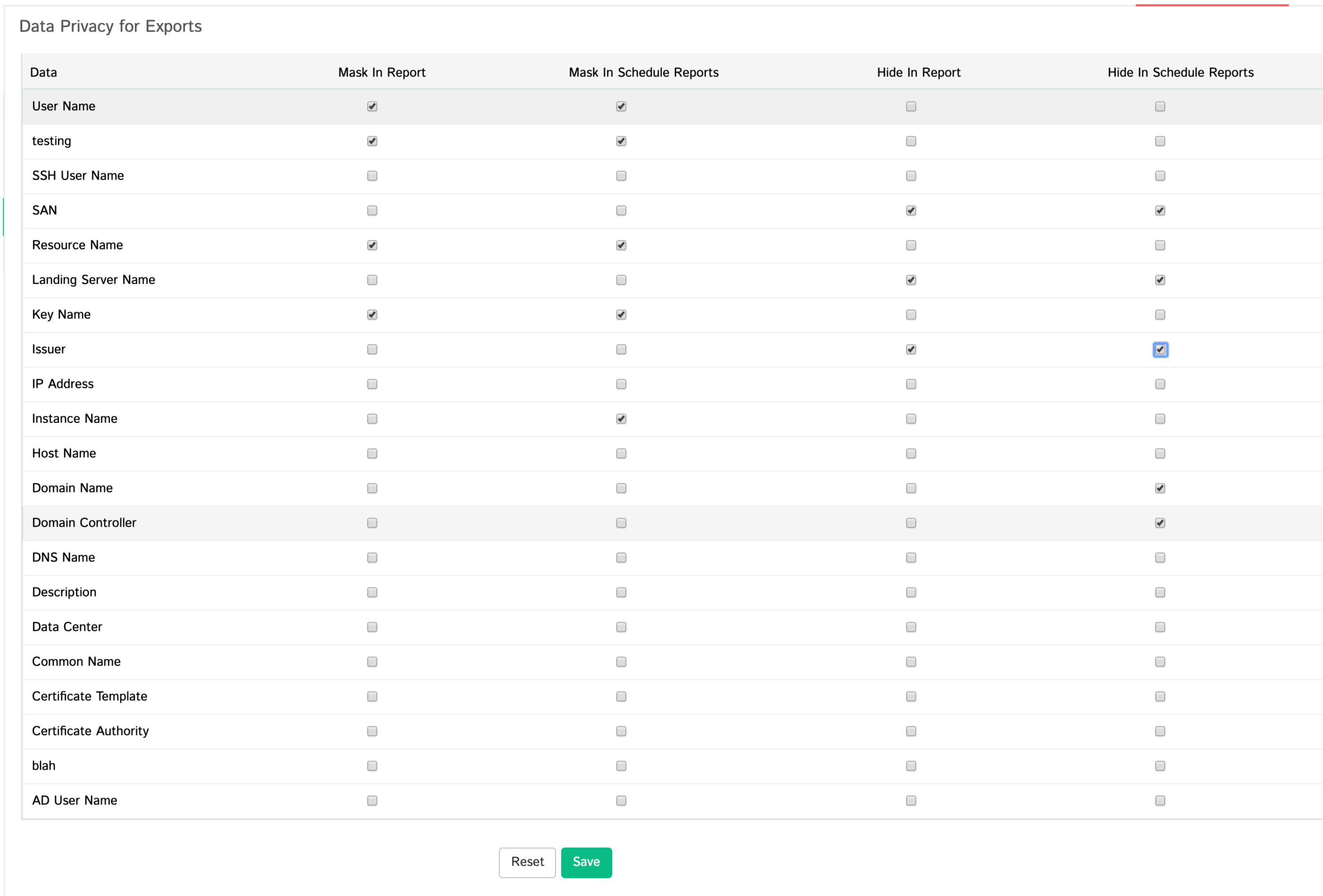
User Password: •••••••••••••••

Help

- Enabling password protection allows users to export reports and other files in a password protected zip file.
- 'Enable User Password' option allows users to set their own passwords, which is to be used when accessing reports exported from Key Manager Plus interface.
- If user password option is disabled, then global password is to be used uniformly by all users when accessing reports exported from Key Manager Plus interface.
- Only the global password is to be used to access reports in e-mail notifications for scheduled report generation.

Controls for personal data exposure in reports

Key Manager Plus includes provisions to control the extent to which personal data is exposed in canned reports. Administrators can choose to mask or hide certain personally identifiable information in reports exported from Key Manager Plus, including scheduled reports, and thereby can replace specific personal data with random characters or hide it entirely. Options are available to mask a range of personal data, such as usernames, host names, or IP addresses. To view the full list, click here.

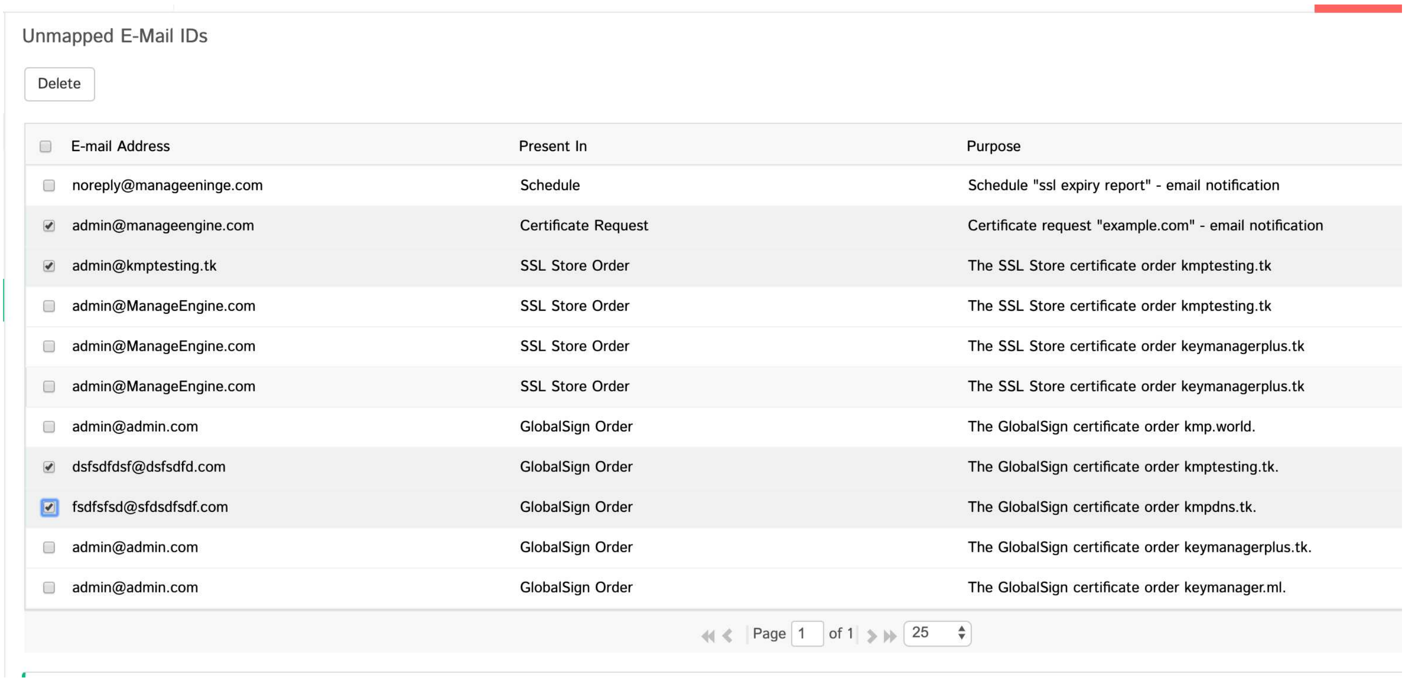


Data Privacy for Exports

Data	Mask In Report	Mask In Schedule Reports	Hide In Report	Hide In Schedule Reports
User Name	☑	☑	□	□
testing	☑	☑	□	□
SSH User Name	□	□	□	□
SAN	□	□	☑	☑
Resource Name	☑	☑	□	□
Landing Server Name	□	□	☑	☑
Key Name	☑	☑	□	□
Issuer	□	□	☑	☑
IP Address	□	□	□	□
Instance Name	□	☑	□	□
Host Name	□	□	□	□
Domain Name	□	□	□	☑
Domain Controller	□	□	□	☑
DNS Name	□	□	□	□
Description	□	□	□	□
Data Center	□	□	□	□
Common Name	□	□	□	□
Certificate Template	□	□	□	□
Certificate Authority	□	□	□	□
blah	□	□	□	□
AD User Name	□	□	□	□

Provisions to manage non-user email addresses

Administrators can configure email notifications about the completion of scheduled tasks, license expiration, and other important operations to be sent to users who do not have an individual account with Key Manager Plus. A complete list of all such external IDs are duly maintained in Key Manager Plus to assist authorized administrators in keeping track of the non-user email addresses stored in the application and deleting them if needed.



Unmapped E-Mail IDs

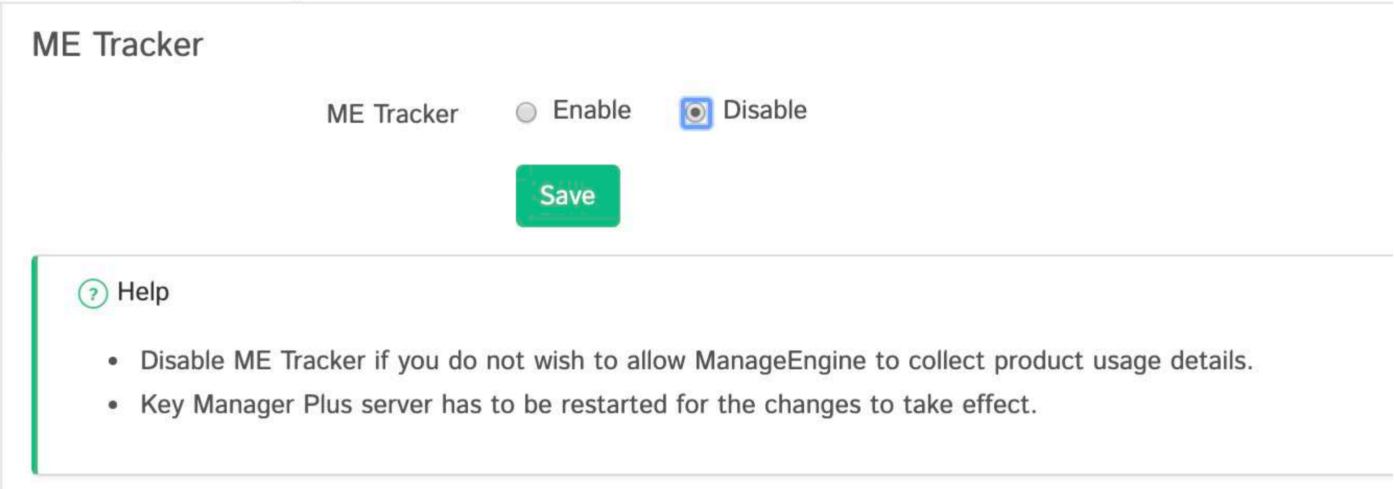
Delete

□	E-mail Address	Present In	Purpose
□	noreply@manageeninge.com	Schedule	Schedule "ssl expiry report" - email notification
☑	admin@manageengine.com	Certificate Request	Certificate request "example.com" - email notification
☑	admin@kmptesting.tk	SSL Store Order	The SSL Store certificate order kmptesting.tk
□	admin@ManageEngine.com	SSL Store Order	The SSL Store certificate order kmptesting.tk
□	admin@ManageEngine.com	SSL Store Order	The SSL Store certificate order keymanagerplus.tk
□	admin@ManageEngine.com	SSL Store Order	The SSL Store certificate order keymanagerplus.tk
□	admin@admin.com	GlobalSign Order	The GlobalSign certificate order kmp.world.
☑	dsfsdfdsf@dsfsdfd.com	GlobalSign Order	The GlobalSign certificate order kmptesting.tk.
☑	fsdfsfsd@sfdsdfsdf.com	GlobalSign Order	The GlobalSign certificate order kmpdns.tk.
□	admin@admin.com	GlobalSign Order	The GlobalSign certificate order keymanagerplus.tk.
□	admin@admin.com	GlobalSign Order	The GlobalSign certificate order keymanager.ml.

Page 1 of 1 25

Options to control product activity tracking

Application administrators have the option to disable ManageEngine tracker in the product, which prevents the insights on activities carried out within the product from being shared with ManageEngine.



ME Tracker

ME Tracker ○ Enable ● Disable

Save

Help

- Disable ME Tracker if you do not wish to allow ManageEngine to collect product usage details.
- Key Manager Plus server has to be restarted for the changes to take effect.

www.keymanagerplus.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.keymanagerplus.com

ManageEngine
Key Manager Plus