



Quick Start Guide

Table of contents

04 Purpose of this guide

04 Installation instructions

- Installing Key Manager Plus in a Windows environment
- Installing Key Manager Plus in a Linux environment

06 Basic configurations

- Mail server configuration
- Proxy server configuration
- Update the Key Manager Plus server's SSL certificate using the web console
- Configure an SSH key management policy

11 Getting started with SSL certificate management

- Discover and consolidate SSL certificates
- Create self-signed certificates
- Request and manage certificates from third-party certificate authorities
- Centralize deployment of certificates to their corresponding servers
- Scan and eliminate configuration vulnerabilities post deployment

16 Getting started with SSH key management

- Discover SSH resources in your network
- Establish connection, enumerate users, and import keys
- Generate and deploy new keys
- Perform and track key management operations from a centralized interface
- Manage SSH keys, resources, and users in bulk

21 Advanced configurations

- RESTful API support
- Active Directory and RADIUS authenticator integration
- Disaster recovery
- Privacy settings
- Scheduled tasks
- Auditing and reports

Contact information

Purpose of this guide

This guide will help you install Key Manager Plus and carry out the configurations necessary to get the application running. Starting with setup and mandatory configurations, and moving on to advanced features and additional resources, this guide will enhance your understanding of Key Manager Plus.

If you have any questions, feel free to write to us at keymanagerplus-support@manageengine.com.

If you want an elaborate walk-through of Key Manager Plus' features, schedule a [personalized demo](#) with our experts. We'll get in touch with you right away.

Installation instructions

Key Manager Plus consists of the following components:

- Key Manager Plus server
- PostgreSQL 9.2.4 bundled with Key Manager Plus, which runs as a separate process. It accepts connections only from the host in which it is running and is not visible externally.

Installing Key Manager Plus in a Windows environment:

- Log in as an administrator, download Key Manager Plus, and execute **ManageEngine_KeyManagerPlus.exe**.

- Choose an installation directory. By default, Key Manager Plus will be installed in **C:/ManageEngine/KeyManager** (which is generally referred to as “**KeyManagerPlus_Home**” in the product documentation).
- In the final step, you’ll see two checkboxes—one for viewing the ReadMe file and the other for starting the server immediately after installation. If you choose to start the server immediately, it will get started in the background.
- If you choose to start the server after installation, you can start it from **Start > Programs > ManageEngine Key Manager Plus**. Make sure you run the program as an administrator. You can perform other actions such as stopping the server or uninstalling the product directly from the Start menu.
- Once you install Key Manager Plus, a tray icon appears in the far right end of the taskbar. You can also use the tray icon to start or stop the Key Manager Plus service, open the application web console, and view startup logs or startup options.
- You can also start Key Manager Plus as a background service. Open the run command window and type “services.msc”. Choose **ManageEngine Key Manager Plus** from the list of services displayed and click the start button in the left pane.

Installing Key Manager Plus in a Linux environment:

- Download **ManageEngine_KeyManagerPlus.bin** for Linux.
- In the Linux terminal window, assign executable permission by typing the following command: “**chmod a+x <file-name>**”.

- Execute the following command: “./<file_name>”.
- If you are installing Key Manager Plus on a headless server, execute the following command: “./<file_name> -console”.
- Follow the on-screen instructions.
- Key Manager Plus will be installed on your machine in the desired location.

Note:

During installation, be sure to install Key Manager Plus from a normal user account and not the root account. Using root accounts to install the application will result in improper extraction of the PGSQL database.

Refer to the detailed explanation in the [user guide](#) for further information on launching Key Manager Plus in your environment and connecting to the web interface.

Basic configurations

Mail server configuration

After installing Key Manager Plus, configure your mail server so that the application can communicate with the users directly without an external mail client. To configure your mail server:

- Navigate to **Settings ---> General Settings ---> Mail Server**.
- Provide your SMTP server details, such as server name, port number, username, password, sender, and reply-to email addresses.

- Check the configuration by sending a test email, and save the configuration.

Key Manager Plus users are notified about various key and certificate management operations, such as certificate export, digital key export, schedules, policy enforcements, and reports, only through email. So it's important to make sure all the details are provided correctly.

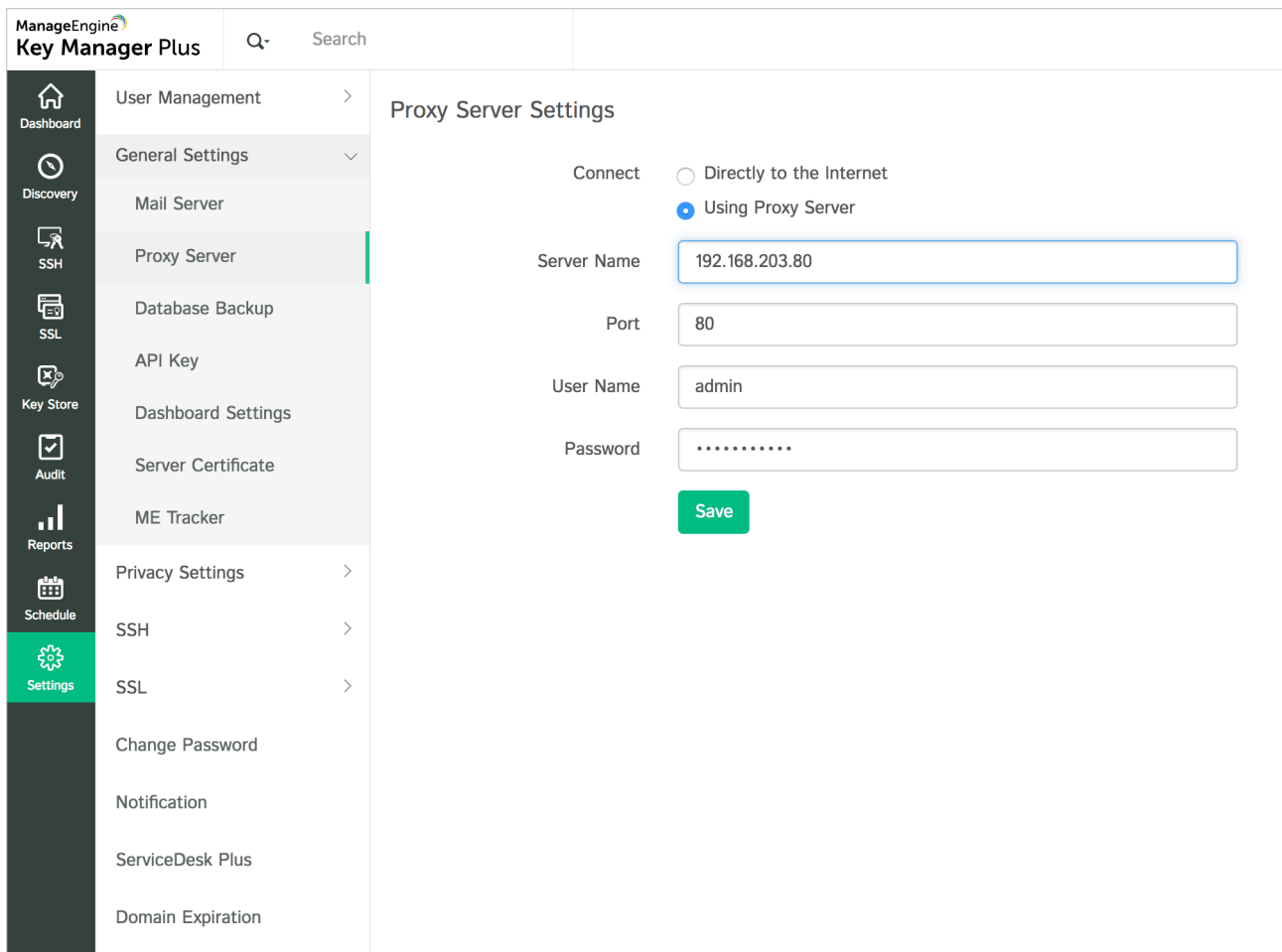
The screenshot shows the ManageEngine Key Manager Plus interface. The left sidebar contains a navigation menu with the following items: Dashboard, Discovery, SSH, SSL, Key Store, Audit, Reports, Schedule, Settings (highlighted in green), and Change Password. The main content area is titled "Mail Server Settings" and contains the following fields and controls:

- SMTP Server:
- Port:
- Requires authentication
- User Name:
- Password:
- From/Sender Address:
- To Address:
- Buttons:

Proxy server configuration

After configuring the mail server, you have to specify how you want to connect to the internet. Key Manager Plus provides you with two options—either a direct connection or using a proxy.

Switch to **Settings** ---> **General Settings** ---> **Proxy Server** in the Key Manager Plus user interface. If you're using a proxy server to connect to the internet, provide the server name, port number, username, and password, and save the configuration.



The screenshot displays the ManageEngine Key Manager Plus web console. The left sidebar contains a navigation menu with the following items: Dashboard, Discovery, SSH, SSL, Key Store, Audit, Reports, Schedule, Settings (highlighted in green), Change Password, Notification, ServiceDesk Plus, and Domain Expiration. The main content area is titled "Proxy Server Settings" and includes the following configuration options:

- Connect:** Radio buttons for "Directly to the Internet" (unselected) and "Using Proxy Server" (selected).
- Server Name:** Text input field containing "192.168.203.80".
- Port:** Text input field containing "80".
- User Name:** Text input field containing "admin".
- Password:** Password input field with masked characters ".....".

A green "Save" button is located below the password field.

Update the Key Manager Plus server's SSL certificate using the web console

Key Manager Plus runs as an HTTPS service. It requires an SSL certificate bearing the common name as the name of its host—for users to be able to connect with it via the web console. By default, during the first-time startup, Key Manager Plus uses the certificate issued for the domain `demo.keymanagerplus.com` that comes bundled along with the product.

However, this certificate will not be trusted within your environment and will cause browsers to throw security errors when users access the application. To avoid security errors, you have to update your own certificate so that it will be trusted within your environment.

To update your server certificate for Key Manager Plus:

- Navigate to **Settings** ---> **General Settings** ---> **Server Certificate**.
- Browse and upload the required certificate file from your system. Alternatively, you can choose a certificate present in Key Manager Plus' certificate repository by clicking on **Existing Certificate**.
- Specify the port in which the application is running and save the configuration.

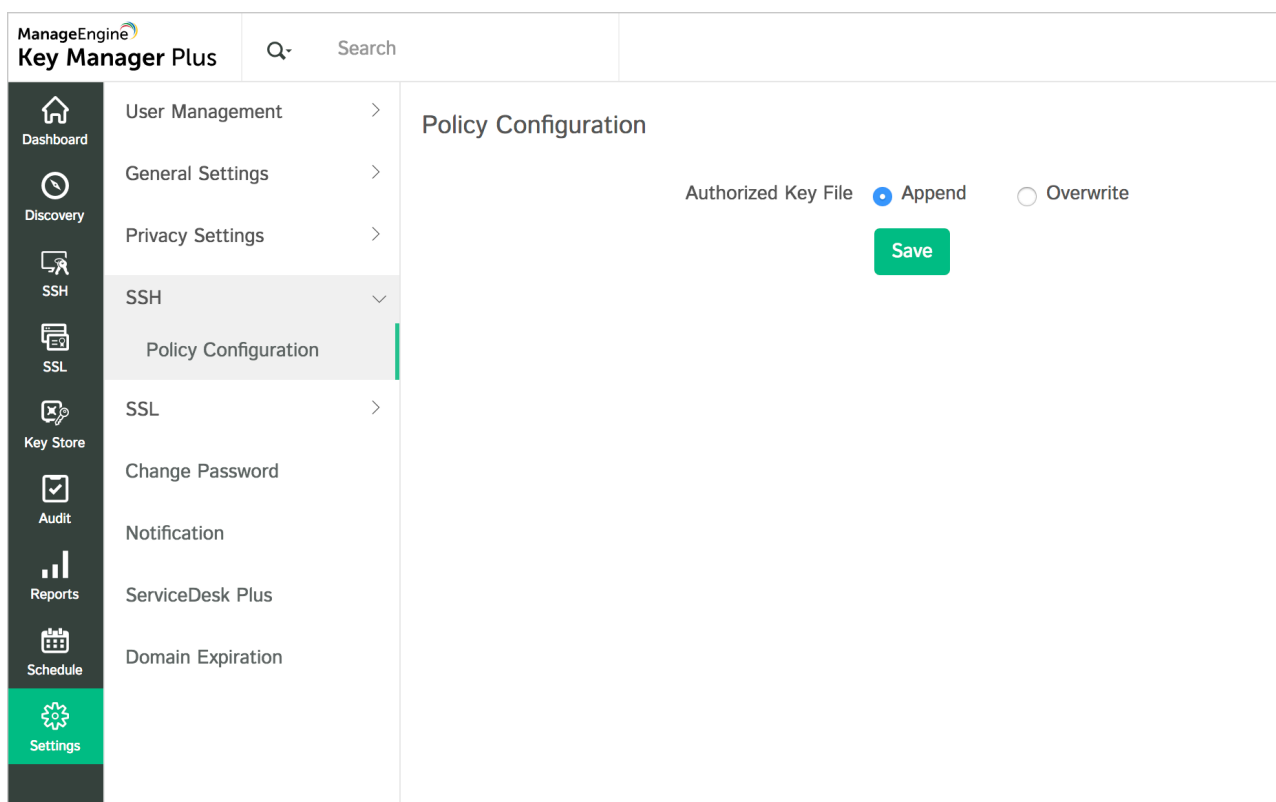
The screenshot shows the 'Server Certificate' configuration page in the Key Manager Plus interface. The left sidebar contains a navigation menu with 'Settings' highlighted. The main content area has a search bar at the top and a 'Server Certificate' section. In this section, there is a 'Select Certificate' label, a 'Browse' button, and an 'Existing Certificate' link. Below this, a note specifies the file format: '(File format should be .cer/.crt/.pfx/.p12/.pkcs12/.pem/.der/.jks/.keystore)'. There is also a 'Server Port' input field with the value '8080' and a green 'Save' button. A help box at the bottom contains a 'Help' icon and a bullet point: 'Key Manager Plus server has to be restarted for the new certificate to take effect'.

Configure an SSH key management policy

If you are going to use the SSH module, the next step is to configure your SSH key management policy. Key Manager Plus provides you with two options—**append** and **overwrite**. The former appends the keys generated using Key Manager Plus to the target servers' `authorized_keys` files. The latter deletes the keys present in the `authorized_keys` file of the target server first, then deploys the keys generated from Key Manager Plus, paving the way for a fresh start.

To choose your SSH policy:

- Navigate to **Settings** ---> **SSH** ---> **Policy Configuration**.
- Choose a policy—**append** or **overwrite**—depending on your requirements, and save the configuration.



The screenshot displays the ManageEngine Key Manager Plus web interface. The top navigation bar includes the logo, a search bar, and the text 'ManageEngine Key Manager Plus'. A left sidebar contains a menu with icons and labels for various sections: Dashboard, Discovery, SSH, SSL, Key Store, Audit, Reports, Schedule, and Settings (highlighted in green). The main content area is titled 'Policy Configuration' and features two radio buttons for 'Authorized Key File': 'Append' (selected) and 'Overwrite'. A green 'Save' button is positioned below the radio buttons.

Getting started with SSL certificate management

SSL certificate management begins with discovering all the SSL certificates across your network and consolidating them in a secure, centralized repository. Listed below are the various stages involved in certificate life cycle management.

Discover and consolidate SSL certificates

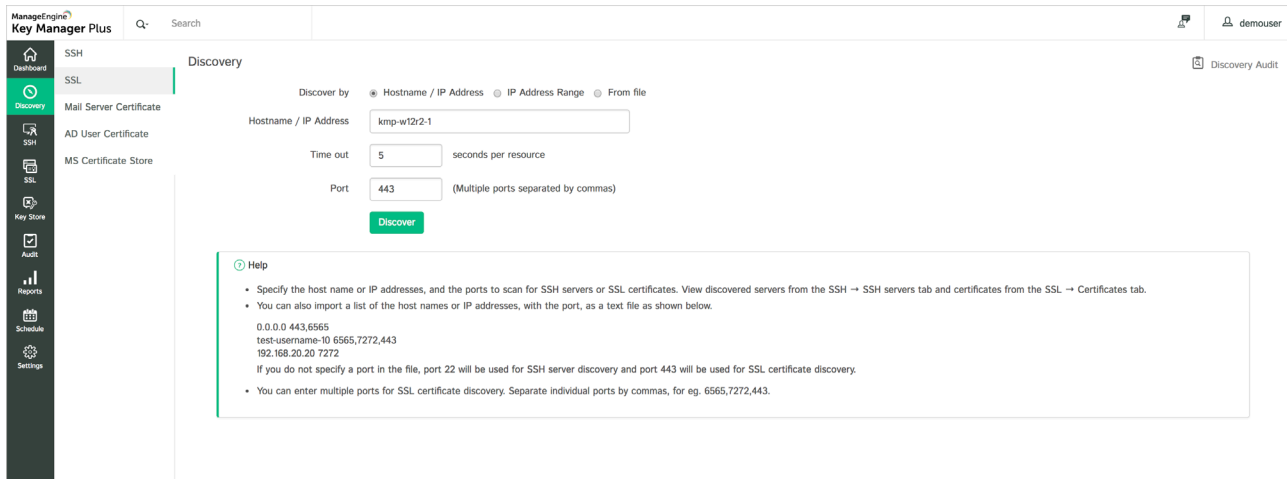
Key Manager Plus comes with a built-in certificate discovery tool that enables you to discover all SSL certificates across your network and consolidate them in Key Manager Plus' centralized repository. Similar to SSH key discovery, certificates can be discovered whenever necessary or through scheduled tasks.

Additionally, Key Manager Plus provides separate and dedicated discovery options for certificates mapped to user accounts in Active Directory, certificates present in the MS Certificate Store, certificates issued by your local or in-house certificate authorities, and certificates used by SMTP servers within your environment.

Navigate to **Discovery --> SSL** to begin discovering SSL certificates across your network. Provide the host name from which the certificates are to be discovered and specify the port number. You can simultaneously discover certificates from many resources by specifying the IP address range or by uploading a text file containing a list of resources.

You can specifically discover certificates mapped to Active Directory user accounts using the **Discovery --> AD User Certificate** option and certificates issued by your local certificate authority using the **Discovery --> MS Certificate Store** option.

Refer to [this](#) section of the help documentation for a detailed explanation of certificate discovery.



Create self-signed certificates

You can create self-signed certificates for in-house applications and deploy them to target servers using Key Manager Plus. The built-in CSR generator expedites the process and the certificate is available for use typically within minutes. Click the Create option under the SSL tab to generate self-signed certificates from Key Manager Plus.

Refer to [this](#) section of the help document for a detailed explanation on creating self-signed certificates.

Key Manager Plus also allows you to sign locally-generated certificate requests using a custom root certificate authority or from a Microsoft Certificate Authority that's installed within your network.

To learn more about certificate signing, click [here](#).

The screenshot shows the 'Create Certificate' form in the ManageEngine Key Manager Plus interface. The form is titled 'Create Certificate' and is located under the 'Certificates' menu. The form fields are as follows:

Field	Value
Common Name	example.com
SAN	example.com
Organization Unit	ManageEngine
Organization	Zoho Corporation
Location	Chennai
State	Tamil Nadu
Country	IN
Key Algorithm	RSA
Key Size	4096
Signature Algorithm	SHA256
Keystore Type	JKS
Validity	100 days
Store Password

Below the form fields, there is a checkbox labeled 'Generate root certificate' which is currently unchecked. At the bottom of the form, there are two buttons: 'Create' (highlighted in green) and 'Cancel'.

Request and manage certificates from third-party certificate authorities

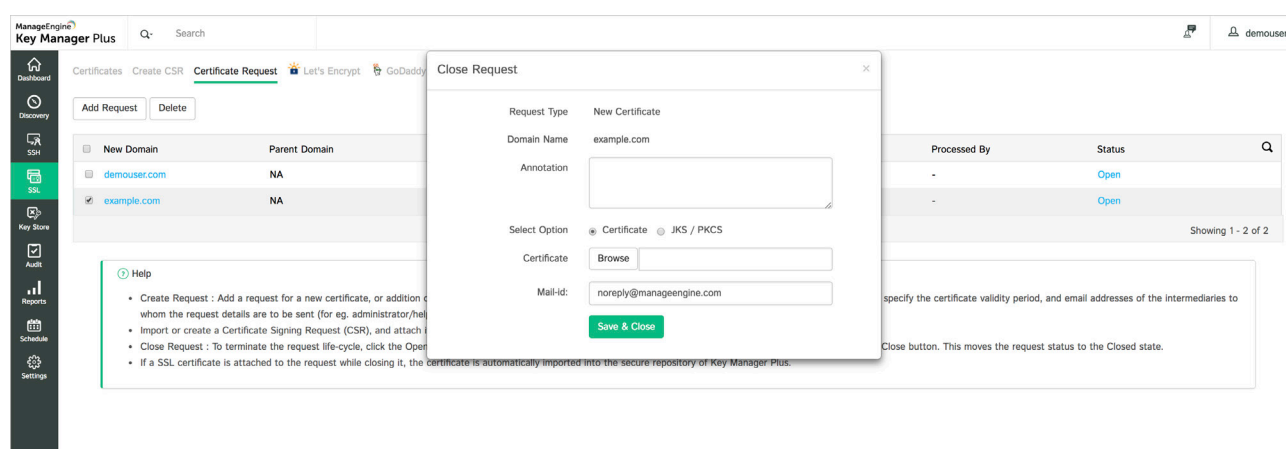
Key Manager Plus enables you to request and acquire SSL certificates from trusted third-party certificate authorities for public-facing websites and deploy them to target servers through a smooth certificate request workflow. You can either acquire certificates for a completely new domain or request more sub-domains for an existing certificate. The certificate request workflow consists of the following stages:

- Adding a certificate request
- Closing a request

The status of each certificate request is emailed to you as well as the user who initiated it.

In addition, Key Manager Plus is integrated with trusted third-party certificate authorities, such as Let's Encrypt CA and GoDaddy CA, that help you achieve end-to-end management of certificate life cycles directly from Key Manager Plus' interface.

For more details on certificate request workflow, refer to [this](#) section of our help documentation.



Centralize deployment of certificates to their corresponding servers

SSL certificates, after being acquired from trusted certificate authorities, need to be deployed onto their corresponding web servers. Key Manager Plus provides a centralized approach to certificate deployment, making it easy for you to keep track of the servers on which certificates are deployed, as well as usage and expiration details—all from a unified interface.

To deploy a certificate to an endpoint server, choose the certificate under the **SSL tab**, and click **Deploy** from the top menu.

Refer to our [help documentation](#) for detailed, server-specific instructions on certificate deployment.

The screenshot displays the Key Manager Plus interface. A 'Certificate Deployment' dialog box is open, showing the following configuration:

- Server Type: Windows
- Deployment Type: Single
- Server Name: 192.168.123.80
- User Name: admin
- Password: [Redacted]
- Path: C:\mycert
- Select: Certificate, JKS / PKCS
- Certificate File Name: demo.keymanagerplus.com

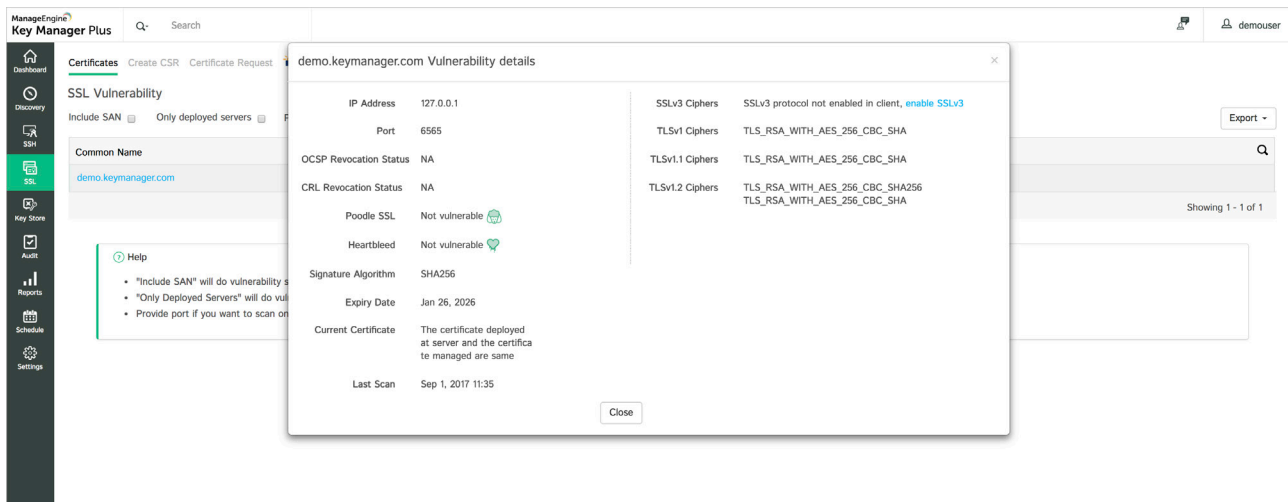
The background shows a table of certificates with the following columns: Common Name, DNS Name, Signature Algorithm, Domain Expiration, and Description. The table lists various certificates, including those for 'demo.keymanagerplus.com' and 'local.adcommunity.manageengine.jp'.

Scan and eliminate configuration vulnerabilities post deployment

SSL certificates need to be periodically scanned post deployment to ensure there aren't any configuration vulnerabilities. Key Manager Plus scans all SSL certificates in its repository and flags certificates that are prone to any vulnerability. This way, you're kept informed of any insecure certificate or server configurations so you can take steps to remediate them.

Key Manager Plus provides a **Scan Vulnerabilities** option for every certificate in its repository (under the **SSL** tab) which helps you scan certificates on demand and discover any vulnerabilities or insecure ciphers associated with the configuration.

For more details on how to perform a vulnerability scan across your network using Key Manager Plus, click [here](#).



Getting started with SSH key management

After configuring the basic settings, the next step toward SSH key management is to discover all the SSH resources in your network and import the existing keys. Once the keys are imported, you can perform a bulk key rotation and rotate all the keys. You can also delete all the existing keys and replace them with new key pairs generated from Key Manager Plus for a fresh start.

Once you have updated the keys on your SSH resources, you can perform various key management operations, such as launching a remote SSH connection, rotating keys, and carrying out a secure file transfer, directly from Key Manager Plus. Let's quickly run through each stage involved in SSH key management.

Discover SSH resources in your network

Discovering SSH resources is the first step to managing SSH keys in your network. You can discover resources anytime or based on scheduled tasks. The discovery options are pretty flexible—you can discover resources either individually or in bulk.

Refer to the [help documentation](#) on our website for a step-by-step explanation of the resource discovery procedure.

- Discovering resources on demand
- Discovering resources automatically through schedules

Note:

1. Before performing resource discovery, make sure the Key Manager Plus server can access the resources you're interested in.

2. By default, Key Manager Plus uses port 22 for SSH communications. So make sure port 22 is open in the target server(s).

The screenshot shows the Key Manager Plus Discovery interface. The left sidebar contains navigation options: Dashboard, SSH, SSL, Mail Server Certificate, AD User Certificate, MS Certificate Store, Key Store, Audit, Reports, Schedule, and Settings. The main content area is titled 'Discovery' and features a 'Discover by' section with three radio buttons: 'Hostname / IP Address' (selected), 'IP Address Range', and 'From file'. Below this, there are input fields for 'Hostname / IP Address' (containing 'kmp-w12r2-1'), 'Time out' (5 seconds per resource), 'Port' (22), and a 'Landing Server' dropdown menu. A green 'Discover' button is positioned below the input fields. A 'Help' section is visible at the bottom, providing instructions on how to specify hostnames, ports, and file formats for discovery.

Establish a connection, enumerate users, and import keys

After discovering the resources, you have to establish a connection between the discovered resources and Key Manager Plus to begin SSH key import and management. You can establish a connection with a discovered resource by providing the credentials of any user account associated with the resource.

Once connected, Key Manager Plus automatically enumerates all the user accounts present in the resource. They can be viewed under **SSH --> SSH Users**. Among the discovered accounts, provide the user credentials for the accounts with SSH keys you'd like to manage. Alternatively, if you provided the root credentials for a resource after discovery while establishing a connection, you get key management privileges for all the user accounts associated with the resource.

Once the user credentials are updated, Key Manager Plus automatically fetches the SSH keys from those accounts, and lists them under **Discovered Keys**. You then have to import the keys that you wish to manage into Key Manager Plus' centralized repository (**SSH --> SSH Keys**) by clicking **Import**.

Refer to the [help documentation](#) on our website for a step-by-step explanation on connection establishment, user enumeration, and importing SSH keys.

- [Establishing a connection with the discovered resources](#)
- [User enumeration](#)
- [Import SSH keys](#)

The screenshot shows the Key Manager Plus interface. The top navigation bar includes the logo, a search bar, and the user name 'demouser'. The left sidebar contains navigation icons for Dashboard, Discovery, SSH, Key Store, Audit, Reports, Schedule, and Settings. The main content area is titled 'Discovered Keys' and features an 'Import' button and an 'Export' dropdown. Below these is a table with the following data:

Resource Name	User Name	Discovered Keys
test_server_1	test	id_rsa
test_server_1	testuser	id_rsa
test_server_1	siva	id_rsa

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and 'Showing 1 - 3 of 3'. Below the table is a 'Help' section with the following text:

Discovered Keys are the SSH private keys available in the discovered SSH server's user accounts. Provide access to the relevant user accounts, to manage the discovered keys using Key Manager Plus.

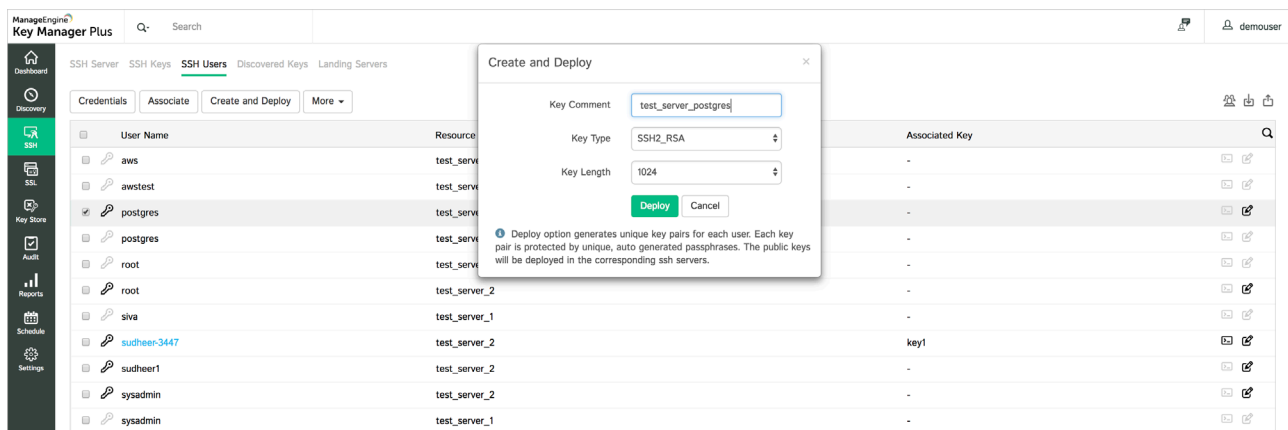
- You can import the keys by clicking the Import button. You will be prompted for a passphrase, wherever applicable.
- The imported keys can be managed from the SSH → SSH keys tab.

Generate and deploy new keys

Key Manager Plus helps you generate new key pairs and deploy them to endpoint servers. The **Create** option under the **SSH Keys** tab allows you to generate fresh key pairs from Key Manager Plus. You can then associate the key with specific user accounts using the **Associate** option in the top menu.

Alternatively, you can also generate key pairs and simultaneously deploy them to various user accounts in one go using the **Create and Deploy** option under the **SSH Users** tab. Key Manager Plus also provides a graphical map of key-user relationships that helps you effectively track the distribution and usage of SSH keys within your network.

For detailed information on SSH key creation and deployment, refer to the [help documentation](#) on our website.



The screenshot displays the Key Manager Plus interface. The 'SSH Users' tab is active, showing a list of users and their associated resources. A 'Create and Deploy' dialog box is open, allowing for the generation and deployment of SSH keys. The dialog box contains the following fields and options:

- Key Comment: test_server_postgres
- Key Type: SSH2_RSA
- Key Length: 1024
- Buttons: Deploy, Cancel

A note below the dialog box states: "Deploy option generates unique key pairs for each user. Each key pair is protected by unique, auto generated passphrases. The public keys will be deployed in the corresponding ssh servers."

User Name	Resource	Associated Key
aws	test_server_1	-
awstest	test_server_1	-
postgres	test_server_1	-
postgres	test_server_2	-
root	test_server_1	-
root	test_server_2	-
siva	test_server_1	-
sudheer-3447	test_server_2	key1
sudheer1	test_server_2	-
sysadmin	test_server_2	-
sysadmin	test_server_1	-

Perform and track key management operations from a centralized interface

Once SSH keys are associated with their user accounts, you can perform a wide range of key management operations, and monitor key usage and activities centrally from Key Manager Plus. Here's a quick summary of the operations that can be performed using Key Manager Plus.

Key rotation:

You can configure Key Manager Plus to rotate all SSH keys associated with user accounts. This can be done either manually on demand or by creating scheduled tasks.

Push keys to remote user accounts:

You can push the private key, public key, or both to target endpoints from Key Manager Plus.

Edit authorized_keys files:

You can fetch the authorized_keys files from various user accounts, edit their contents, and deploy them back from Key Manager Plus.

Secure file transfer:

Key Manager Plus allows you to securely transfer files from your system to target user accounts using the Secure Copy Protocol (SCP).

Launch terminal connections:

You can launch secure SSH connections to remote servers within your network and record the session for audits.

For a detailed explanation of all the key management operations you can perform using Key Manager Plus, refer to the [help documentation](#) on our website.

Manage SSH keys, resources, and users in bulk

Key Manager Plus provides you with the option to categorize SSH resources, keys, and users into specific groups depending on various criteria. Click on the resource group, key group, or user group icon in the corresponding tabs for bulk organization. Once the SSH resources, keys, and users are categorized, you can perform key management operations in bulk, similar to working with a single resource.

Refer to the [help documentation](#) for more details on bulk management.

Advanced configurations

RESTful API support

Key Manager Plus provides an open API repository which allows various applications and processes across your network to integrate with the Key Manager Plus server and retrieve SSH key and SSL certificate-related information to be used in other applications or databases. To use the Key Manager Plus API in another application, generate and provide the API key from the Key Manager Plus web interface for authentication.

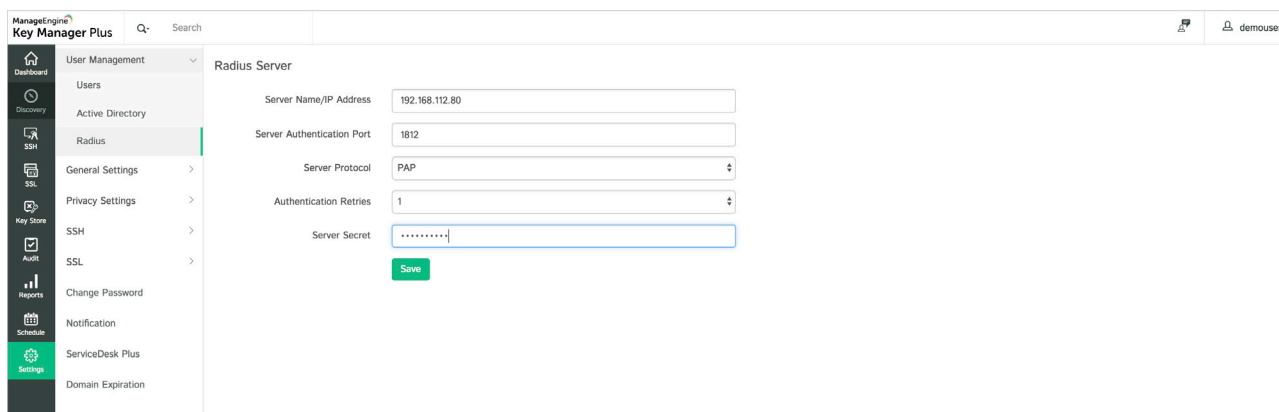
For more details on configuring the key management API, refer to [this](#) section of the help documentation.

Active Directory and RADIUS authenticator integration

Key Manager Plus integrates with Microsoft Active Directory (AD) and RADIUS authenticator, allowing users to access Key Manager Plus using their AD or RADIUS credentials.

To integrate with AD and import all AD users into Key Manager Plus, navigate to **Settings ---> User Management ---> Active Directory**. Provide your domain details and server credentials, and then choose the required users or user groups. Once the selected users are imported into Key Manager Plus, they can log in to the application using their AD credentials.

To integrate with RADIUS authenticator, navigate to **Settings ---> User Management ---> RADIUS**. Configure the server details and enable RADIUS authentication. Once the initial configuration is done, you'll have to add RADIUS users manually using the **Add User** option under **User Management ---> Users**. Once added, the users can access Key Manager Plus with their RADIUS credentials.



The screenshot displays the 'Radius Server' configuration page in the Key Manager Plus interface. The left sidebar contains a navigation menu with options like Dashboard, User Management, Active Directory, Radius, General Settings, Privacy Settings, SSH, SSL, Change Password, Notification, ServiceDesk Plus, and Domain Expiration. The main content area is titled 'Radius Server' and includes the following fields:

- Server Name/IP Address: 192.168.112.80
- Server Authentication Port: 1812
- Server Protocol: PAP
- Authentication Retries: 1
- Server Secret: [masked]

A green 'Save' button is located at the bottom of the configuration form.

Refer to the detailed instructions in our [help documentation](#) for more information on integrating with AD and RADIUS authenticator.

Disaster recovery

Key Manager Plus provides a disaster recovery configuration that allows you to recover data in the event of a disaster or data loss. Using this option, you can schedule [database backups](#) from Key Manager Plus and restore the data through scripts.

The screenshot shows the 'Database Backup' configuration page in the ManageEngine Key Manager Plus interface. The left sidebar contains a navigation menu with options like User Management, General Settings, Mail Server, Proxy Server, Database Backup (selected), API Key, Dashboard Settings, Server Certificate, ME Tracker, Privacy Settings, SSH, SSL, Change Password, Notification, ServiceDesk Plus, and Domain Expiration. The main content area is titled 'Database Backup' and includes the following settings:

- Recurrence Type: Day Weekly Monthly
- Run backup every: 01 day(s)
- Backup Time: 02 : 00 [hh : min]
- Maintain latest: 5 backup(s) only
- Destination Directory: ../Backup
- Send Email Notification: admin@manageengine.com (Email addresses separated by commas)

A green 'Save' button is located at the bottom of the configuration area.

Privacy settings

Key Manager Plus provides a set of privacy options which you can customize according to your requirements to comply with the General Data Protection Regulation (GDPR). Here's the list of privacy settings [offered by Key Manager Plus](#):

- Provision to purge audit trails
- Password protection for exports
- Provision to control the exposure of personal data in reports
- Provision to manage non-user email addresses

The screenshot shows the 'Purge Audit Trails' configuration page in the ManageEngine Key Manager Plus interface. The left sidebar is similar to the previous screenshot, with 'Privacy Settings' expanded to show 'Purge Audit Trails' (selected), Export Settings, Export Data Settings, and Unmapped E-Mail IDs. The main content area is titled 'Purge Audit Trails' and includes the following settings:

- Purge records that are more than 100 days old for operation audit.
- Purge records that are more than 100 days old for discovery audit.
- Purge records that are more than 100 days old for association audit.
- Purge records that are more than 100 days old for rotation audit.
- Purge records that are more than 100 days old for schedule audit.

A green 'Save' button is located at the bottom of the configuration area. Below the configuration area, there is a 'Help' section with a note: "Enter 0 or leave the field blank to disable purging of audit trails."

Scheduled tasks

Key Manager Plus allows you to create scheduled tasks to automatically perform key and certificate management operations at periodic time intervals. The Add Schedule option under the Schedule tab in the Key Manager Plus web interface enables you to create schedules for key and certificate management operations, and specify the time interval and email to which notifications are to be sent. Key Manager Plus offers [eight types of schedules](#):

- Key rotation
- SSH discovery
- SSL discovery
- AD user certificate discovery
- SSL vulnerability
- Sync with CMDB
- SSL expiry
- Reports

ManageEngine
Key Manager Plus

Search

demouser

Feb 12, 2019 06:53:17

Add Schedule

Schedule Name: schedule_1

Schedule Type: Key Rotation

Select Keys: Specific keys Key Group User Group

Selected Keys: key2, key4

(Ctrl + Click for Multiple Selection)

Push private key file to remote user account
 Push public key file to remote user account
 Use keyname as filename

Recurrence Type: Hourly Daily Weekly Monthly Once only

Start Time: 6 : 55 [hh : min]

Start Date: 02/12/2019 [MM/DD/YY]

After Every: 1 Hour(s)

Send Email Notification: admin@manageengine.com
(Email addresses separated by commas)

Report Format: PDF CSV

Notify Key owners with rotation report

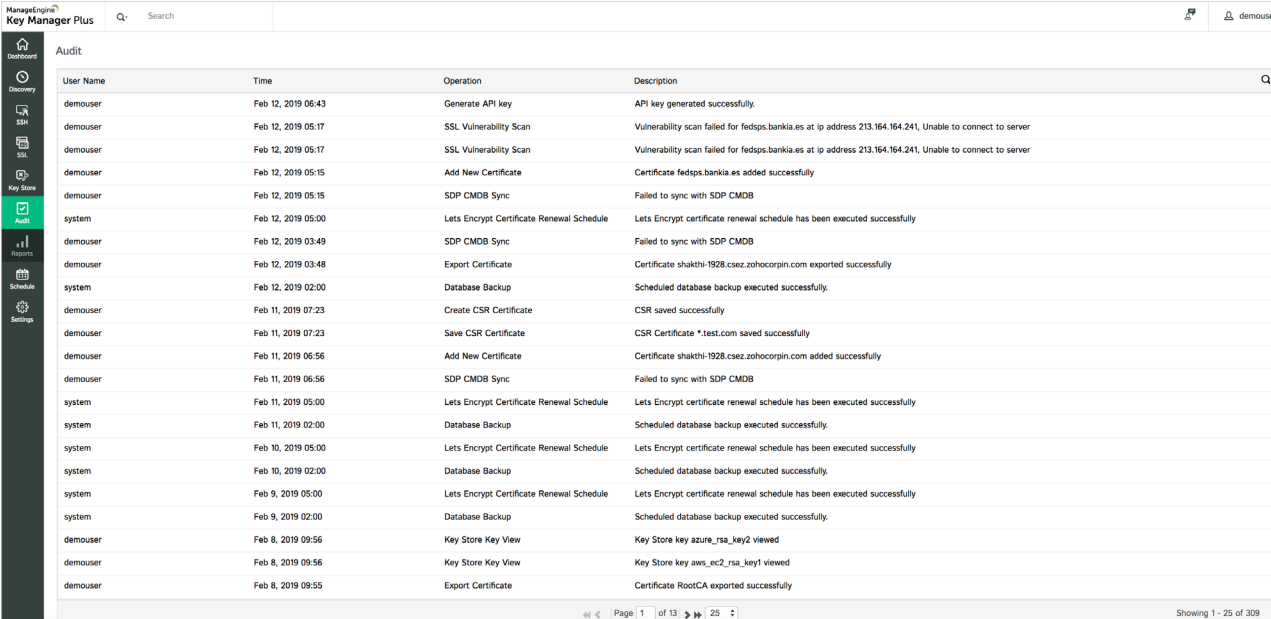
Save Cancel

For a detailed explanation of the scheduled tasks supported by Key Manager Plus and how they work, refer to [this](#) section of the help documentation.

Auditing and reports

[Key Manager Plus provides an efficient auditing mechanism](#) that captures all the product's operations. Users with the administrator role can view audit records pertaining to all users, while those with the operator role can view only those records associated with their activities in the product. The **Audit** tab in the web interface displays the audit trails. In addition, Key Manager Plus also captures operation-specific audit records (listed below) and displays them in their respective sections in the product interface.

- Discovery audit
- Key association audit
- Key rotation audit
- Schedule audit

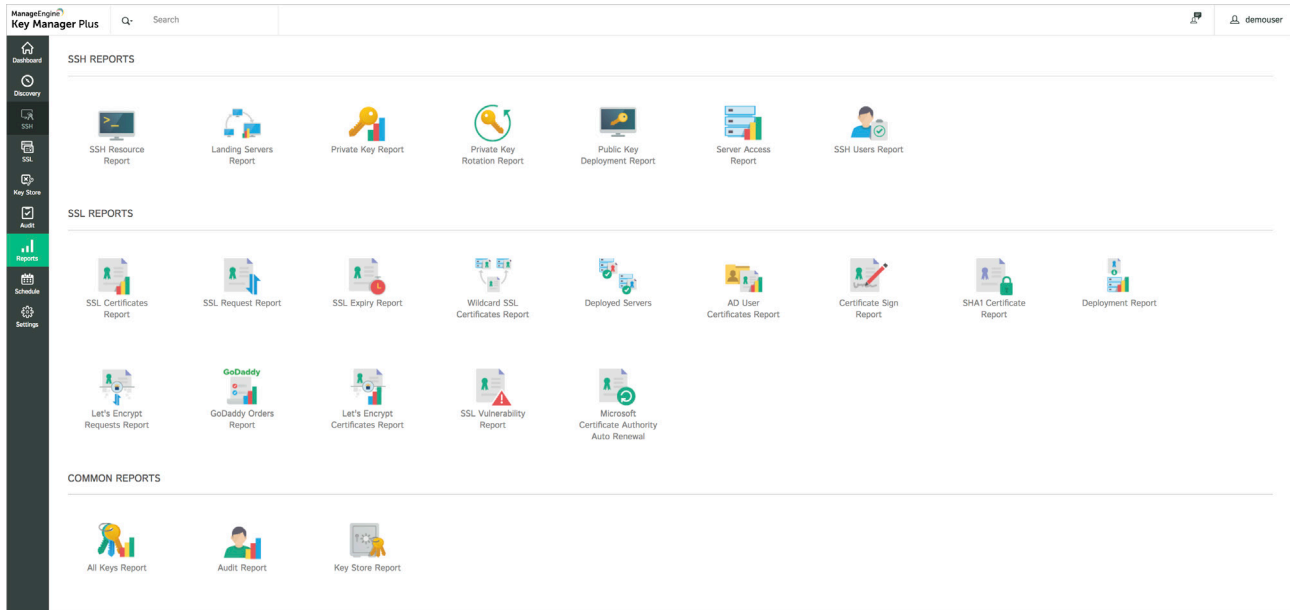


The screenshot shows the 'Audit' tab in the Key Manager Plus web interface. The table displays the following audit records:

User Name	Time	Operation	Description
demouser	Feb 12, 2019 06:43	Generate API key	API key generated successfully.
demouser	Feb 12, 2019 05:17	SSL Vulnerability Scan	Vulnerability scan failed for fedspz.bankia.es at ip address 213.164.164.241, Unable to connect to server
demouser	Feb 12, 2019 05:17	SSL Vulnerability Scan	Vulnerability scan failed for fedspz.bankia.es at ip address 213.164.164.241, Unable to connect to server
demouser	Feb 12, 2019 05:15	Add New Certificate	Certificate fedspz.bankia.es added successfully
demouser	Feb 12, 2019 05:15	SDP CMDB Sync	Failed to sync with SDP CMDB
system	Feb 12, 2019 05:00	Lets Encrypt Certificate Renewal Schedule	Lets Encrypt certificate renewal schedule has been executed successfully
demouser	Feb 12, 2019 03:49	SDP CMDB Sync	Failed to sync with SDP CMDB
demouser	Feb 12, 2019 03:48	Export Certificate	Certificate shakthi-1928.csez.zohocorpin.com exported successfully
system	Feb 12, 2019 02:00	Database Backup	Scheduled database backup executed successfully.
demouser	Feb 11, 2019 07:23	Create CSR Certificate	CSR saved successfully
demouser	Feb 11, 2019 07:23	Save CSR Certificate	CSR Certificate *.test.com saved successfully
demouser	Feb 11, 2019 06:56	Add New Certificate	Certificate shakthi-1928.csez.zohocorpin.com added successfully
demouser	Feb 11, 2019 06:56	SDP CMDB Sync	Failed to sync with SDP CMDB
system	Feb 11, 2019 05:00	Lets Encrypt Certificate Renewal Schedule	Lets Encrypt certificate renewal schedule has been executed successfully
system	Feb 11, 2019 02:00	Database Backup	Scheduled database backup executed successfully.
system	Feb 10, 2019 05:00	Lets Encrypt Certificate Renewal Schedule	Lets Encrypt certificate renewal schedule has been executed successfully
system	Feb 10, 2019 02:00	Database Backup	Scheduled database backup executed successfully.
system	Feb 9, 2019 05:00	Lets Encrypt Certificate Renewal Schedule	Lets Encrypt certificate renewal schedule has been executed successfully
system	Feb 9, 2019 02:00	Database Backup	Scheduled database backup executed successfully.
demouser	Feb 8, 2019 09:56	Key Store Key View	Key Store key azure_rsa_key2 viewed
demouser	Feb 8, 2019 09:56	Key Store Key View	Key Store key aws_ec2_rsa_key1 viewed
demouser	Feb 8, 2019 09:55	Export Certificate	Certificate RootCA exported successfully

Besides an auditing tool, Key Manager Plus also comes with a built-in reporting tool that categorizes all the audit data and renders it in a more readable format. The **Reports** tab in the web interface contains various types of reports related to key and certificate management operations with an option to export them as and when required.

For more details regarding the types of reports and configurations, refer to [this](#) section of the help documentation.



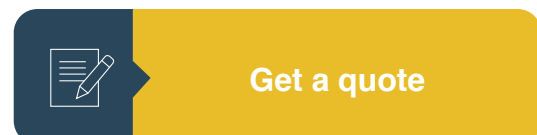
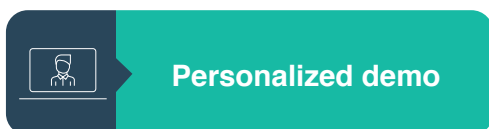
Contact information

If you need any assistance during installation, our technical support team is just an email or phone call away.

Email address: keymanagerplus-support@manageengine.com

Phone: +1-669-231-7079

Toll-free number: +1-888-720-9500



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

ManageEngine 
KeyManager Plus