Kanguru Defender Self Service Password Management

Quick Start Guide

For Defender Drives

NOTICES AND INFORMATION

Please be aware of the following points before using your Kanguru Defender flash drive

Kanguru Solutions will not be held responsible for any illegal use of this product nor any losses incurred while using this product. The user is solely responsible for the copyright laws, and is fully responsible for any illegal actions taken.

Customer Service

To obtain service or technical support for your system, please contact Kanguru Solutions Technical Support Department at 508-376-4245, or visit www.Kanguru.com for web support.

Legal notice

In no event shall Kanguru Solutions' liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential software, or its documentation. Kanguru Solutions offers no refunds for its products. Kanguru Solutions makes no warranty or representation, expressed, implied, or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Kanguru Solutions reserves the right to revise or update its products, software, or documentation without obligation to notify any individual or entity.

Export Law Compliance

Regardless of any disclosure made to Kanguru Solutions pertaining to the ultimate destination of the specific Kanguru product, you warrant that you will not export, directly or indirectly, any Kanguru product without first obtaining the approval of Kanguru Solutions and the appropriate export license from the Department of Commerce or other agency of the United States Government. Kanguru Solutions has a wide range of products and each product family has different license requirements relative to exports.

Defragmenting Flash Memory Warning

Do not attempt to defragment your Kanguru Defender Flash Drive. Flash memory does not need to be defragmented and does not gain any performance by doing so. Defragmenting your flash drive can actually degrade the flash memory which may reduce the drive's total capacity and lifespan.

Table of Contents

1. Overview

In the event that a Kanguru Defender drive's login password is forgotten, the Self Service Password Management feature (referred to throughout this document as SSPM) allows the device user to reset their password and regain access to the data on their drive.

The SSPM feature is free if your device is being managed by KRMC Cloud. Otherwise a SSPM license key is required. Activating SSPM requires an internet connection. You will not be able to use SSPM until you have registered an email address.

This guide was created for users who would like to setup the Self Service Password Management feature. The process for setting up SSPM is different for managed and unmanaged drives. Please refer to the appropriate section depending on whether you are using KRMC Cloud to manage your Defender drive.

Additional Documentation

For Product Compatibility matrix and general information about SSPM, please refer the Kanguru Knowledge Base article at https://kanguru.zendesk.com/entries/95393867

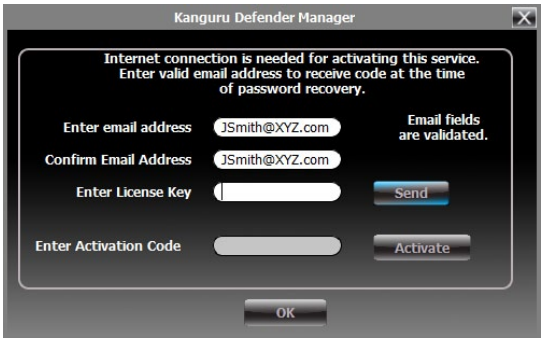
2. Enabling SSPM on Unmanaged Defender Drives

SSPM can be enabled on unmanaged Defender drives during the Setup Wizard.

When you reach the Password setup window:

1. Select the **Enable Service option** and then click on the **Apply button**.
   Note: If you want SSPM but have not purchased an SSPM license, or if you do not have internet access, you can select 'I will set this up later' and then click on the **Next button**. Skip the remaining steps and refer to section 4. Activating SSPM on page 12 for instructions on completing SSPM setup.

2. Next you'll need to register an email address where a password reset link can be sent in case you forget your login password. Enter your email in the corresponding fields.



3. Enter your SSPM license key in the 'Enter License Key' field and then click on the **Send button**. Your SSPM license key should have been e-mailed to you when you purchased your SSPM subscription. Contact Kanguru if you did not receive your SSPM license.

4. An email containing your activation code will be sent to the email address you entered above for verification. Enter the activation code into the 'Enter Activation Code' field and then click on the **Activate button**. The activation code field is case sensitive. Please enter your activation code exactly as it appears in the email that you received from Kanguru.

5. Click on the **OK button** to close the window. Then click on the **Next button** and complete the Setup Wizard.

3. Enabling SSPM on Managed Defender Drives

If you are using KRMC Cloud to manage your Defender drives, then you have three methods for enabling SSPR on your managed drives.

- Enable through global auto-provisioning settings
- Create a global action
- Create a device specific action

3.1 Defining SSPM Behavior

The KRMC Cloud administrator has three options to choose from for defining SSPM behavior on their managed Defender drives:

- **Enable and Force Setup**
  Enable the SSPM feature on the drive and activate it immediately by requiring the user to provide an e-mail address.

- **Enable but Allow User to Setup Later**
  Enable the SSPM feature on the drive but allow the user to provide their e-mail address at a later time. **Note:** Simply enabling SSPM does not allow the device user to reset their password. SSPM must be activated by providing a valid e-mail address.

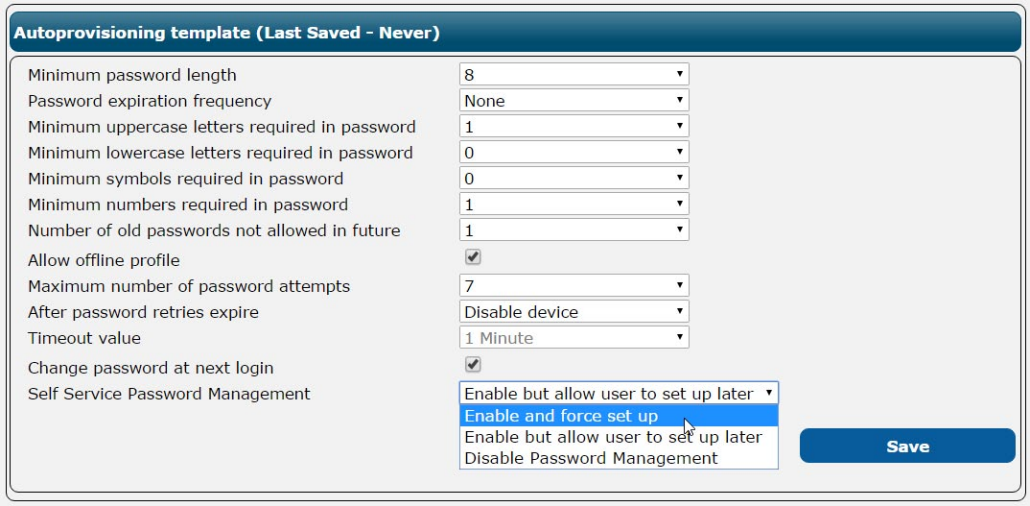
- **Disable Password Reset**
  Disable SSPM entirely. The 'Forgot Password' button will not be available on the Defender's login window.

3.2 Enabling SSPM through Global Auto-Provisioning Settings

Setting up the relevant option in the Global Settings. By choosing this option, any Defender drive with a supported version will automatically download the configured settings as configured by the administrator at the time of set up.

1. After logging into your KRMC Cloud account, click on the **Settings menu** and then select **Global Settings**.

2. The Autoprovision template appears. The Self Service Password Management setting is the last option in the list. Choose your preferred behavior from the dropdown menu.



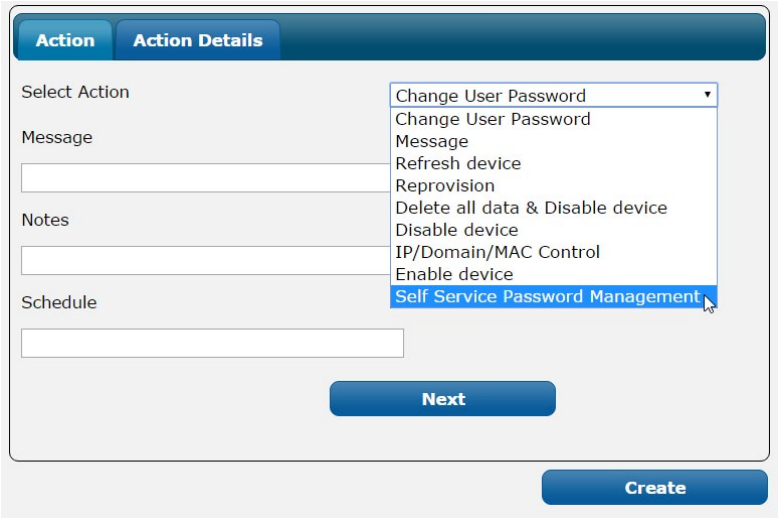
3. Click on the **Save button**.

3.3 Creating a Global SSPM Enable Action

Creating a Global SSPM action will configure SSPM on all managed Defender drives with supported client versions. A global remote action is created in KRMC for all drives managed by the administrator's account. When the managed drives communicate with KRMC, the relevant action will be executed on each drive.

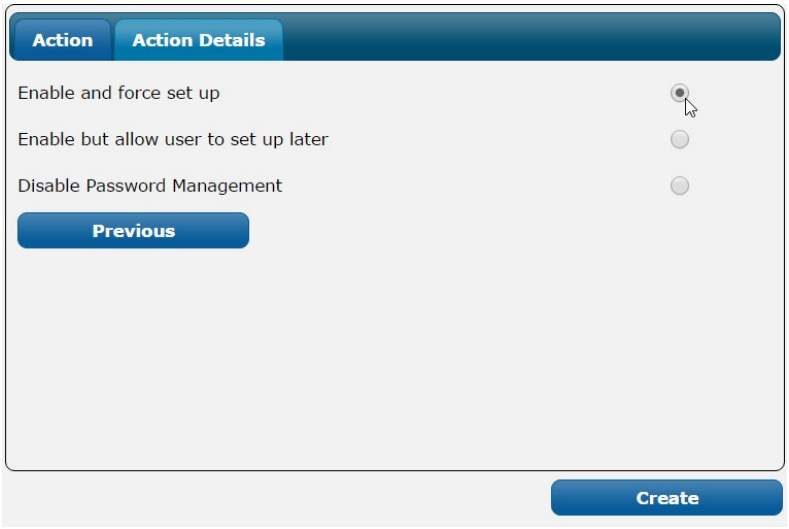
1. After logging into your KRMC Cloud account, click on the **Action menu** and then select **Create Global Action**.

2. The Global Action screen appears. Select **Self Service Password** from the Select Action dropdown menu.



3. Provide a message, note (both optional) and schedule the a date and time for the action to occur. Then click on the **Next Button**.

4. The Action Details screen appears. Configure the SSPM behavior by clicking on the radio button that corresponds to your preferred option.



5. Click on the **Create button**.

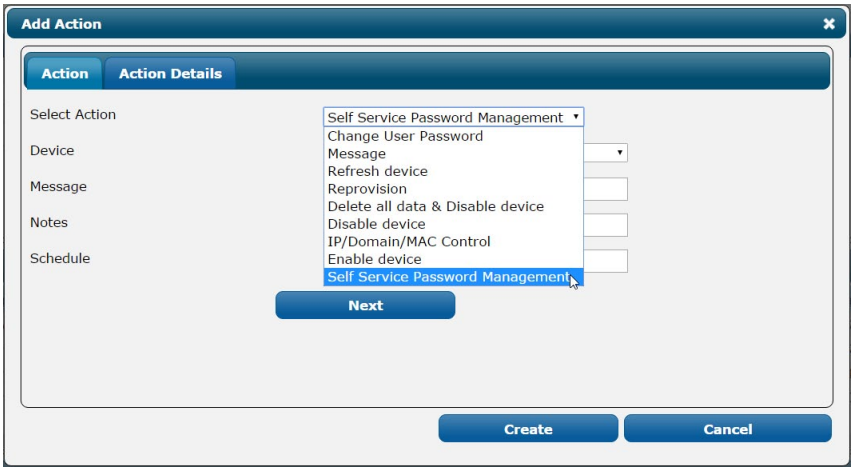
3.4 Creating a Drive Specific SSPM Enable Action

Creating an individual SSPM action for a managed Defender drive will only enable SSPM for that particular device.

1. After logging into your KRMC Cloud account, click on the **Device menu** and then select **Device List**.

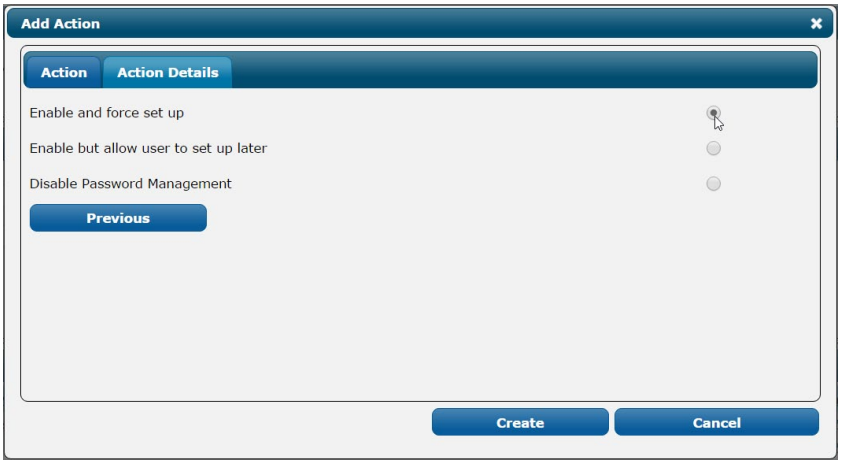
2. In the table showing the device list, click on the **Add Action button** located under the Action column for the managed Defender drive that you want to create a Self Service Password Reset action for.

3. The Add Action window appears. Select **Self Service Password Management** from the Select Action dropdown menu.



4. Provide a message, note (both optional) and schedule the a date and time for the action to occur. Then click on the **Next Button**.

5. The Action Details screen appears. Configure the SSPM behavior by clicking on the radio button that corresponds to your preferred option.



6. Click on the **Create button**.

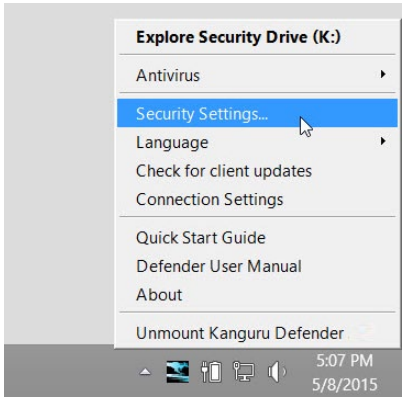
4. Activating SSPM

If SSPM was enabled on your drive but was not activated, then you will need to activate SSPM before you can reset your password.

To activate the SSPM functionality:

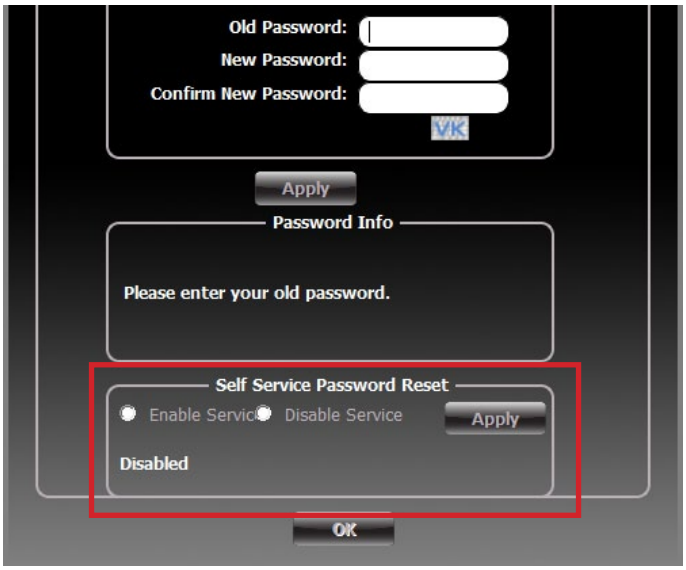
1. Click on the **KDM icon**  located in the task bar and then click on '**Security Settings…'** from the popup menu.

   Note: Linux users must right-click on the **KDM icon** in the task bar.

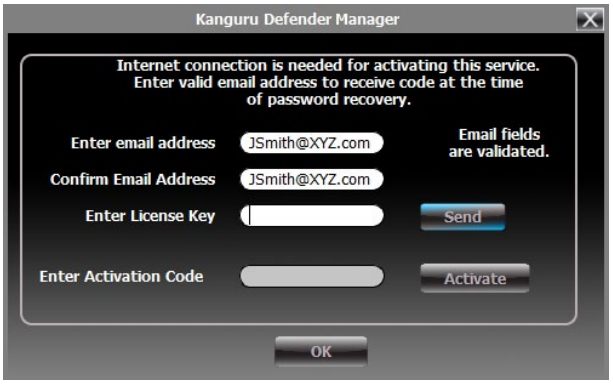


2. The 'Password Settings' window opens.

3. Select the **Enable Service option** and then click on the **Apply button**.
   Note: This section is not available if you have already enabled SSPM during the setup wizard.



4. Next you'll need to designate an email address where you can have a password reset link sent to, in case you forget your login password. Enter your email in the corresponding fields.



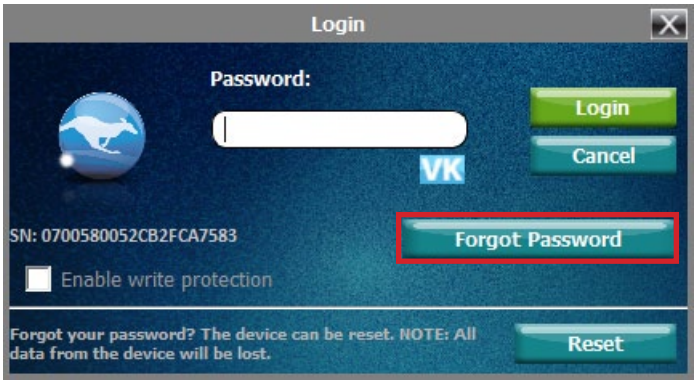
5. Enter your SSPM license key in the 'Enter License Key' field and then click on the **Send button**. Your SSPM license key should have been emailed to you when you purchased your SSPM subscription. Contact Kanguru if you did not receive an email with your SSPM license.

6. An email containing your activation code will be sent to the email address you entered above. Enter the activation code into the 'Enter Activation Code' field and then click on the **Activate button**.
   Note: The activation code field is case sensitive. You must enter your activation code exactly as it appears in the email that you received from Kanguru.

7. Click on the **OK button** to close the window. SSPM is now enabled.

5. Resetting Your Login Password

If you enabled Self Service Password Management functionality and completed the setup process then you will see a 'Forgot Password' button in the login window.



In the event that you forget your login password, you can use the Self Service Password Management feature to reset the login password and regain access to the secure partition.

To reset your Defender's login password:

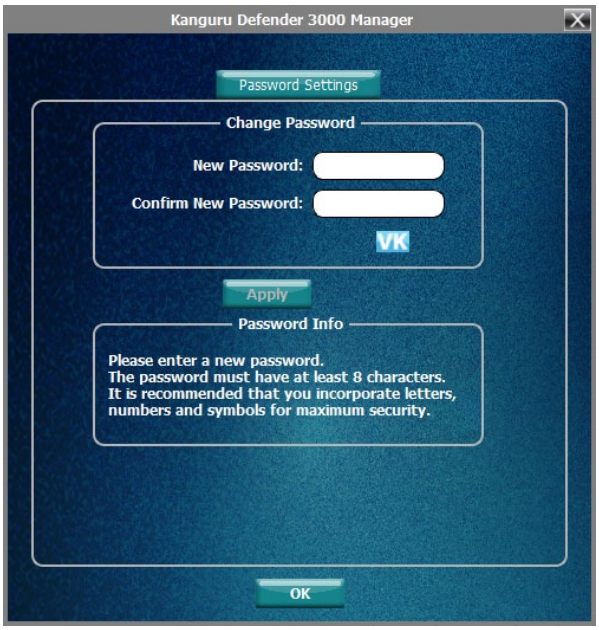
1. Click on the **Forgot Password button**.

2. An email is sent to the email address that you registered with SSPM and a code verification window appears.

3. Check your email for a message sent from *noreply-krmc@kanguru.com*. The email should be titled 'Self Service Password Management' and will contain a password management code.

4. Enter the password management code into the code verification window and then click on the **Verify code button**. The password management code is case sensitive. Make sure you input the password exactly as it appears in the e-mail that you received.

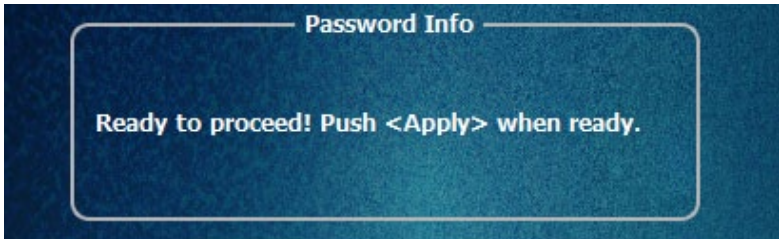
5. If the password management code is verified, the Change Password window appears.



6. Enter your new password in the 'New Password' field. You can enter your password using KDM's Virtual Keyboard by clicking the **VK button**.
   Note: For security reasons, it is recommended that you incorporate letters, numbers and symbols to achieve maximum security.

7. Enter the same password in the 'Confirm New Password' field for verification. If your passwords do not match or there is any other issue with the password which you have entered in the 'Change Password' area, an explanation will be visible in the 'Password Info' area.
   Note: The 'Password Info' area will inform you if there are any password requirements. It updates in real time. Disregard the messages in the 'Password Info' area until you have finished entering your password into both the 'New Password' and 'Confirm New Password' fields.

8. If the passwords you entered match, you will receive a "Ready to proceed!" message in the 'Password Info' area. Click on the **Apply button** to confirm your new password.



9. Click the **OK button** to return to the Login window.

You can now use your new password to login to KDM.

Kanguru Solutions
1360 Main Street
Millis, MA 02054
www.kanguru.com