Version: 1.0.0

Notices and Information

Kanguru Solutions will not be held responsible for any illegal use of this product nor any losses incurred while using this product. The user himself is 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.

End User License Agreement

This legal document is an agreement between you, the end user (“Licensee”), and Kanguru Solutions, a division of Interactive Media Corporation (“Licensor”).
By and using this software, you are consenting to be bound by the terms of this agreement, which includes the disclaimer of warranty.
This agreement constitutes the complete agreement between you and licensor. If you do not agree to the terms of this agreement, cease to use the product immediately.

DISCLAIMER OF WARRANTIES
The software as a service is provided on an “AS IS” basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose, and non-infringement. The entire risk as to the results and performance of the software is assumed by you, the Licensee. If the software is defective, you, and not Licensor or any distributor, agent or employee of Licensor assumes the entire cost of all necessary servicing, repair, or correction.

LIMITATION OF DAMAGES
In no event shall Licensor, or anyone else who has been involved in the creation, distribution, or delivery of this product be liable for any direct, indirect, special, punitive, exemplary, consequential or incidental damages (including but not limited to damages for loss of business profits, business interruption, loss of business information, and the like) arising out of the use or inability to use such product even if Licensor has been advised of the possibility of such damages.
Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

COPYRIGHT RESTRICTIONS
This software and any accompanying materials are copyrighted. Unauthorized copying of this software or of any of the textual materials accompanying it is expressly forbidden.
You may not modify, adapt, translate, reverse engineer, decompile, disassemble (except to the extent applicable laws specifically prohibit such restriction), or create derivative works based on the software.

EXPORT RESTRICTIONS
You agree that you will not export the software to any country, person or entity subject to U.S. export restrictions.

ENTIRE AGREEMENT
This written End User License Agreement is the exclusive agreement between you and Licensor concerning the software as a service and supersedes any and all prior oral or written agreements, negotiations or other dealings between us concerning the software. This License Agreement may be modified only by a writing signed by you and Licensor.
This agreement is subject to the laws and jurisdiction of the courts of the Commonwealth of Massachusetts, USA. If a court of competent jurisdiction invalidates one or more of the terms of this contract, the surviving terms continue in force. This License Agreement is effective upon the use of the software as a service.

Contents

Contents

Contents

Contents

Introduction

1

Thank you for using the KRMC On-Premise. KRMC On-Premise is a revolutionary product that places a complete USB security policy into your hands, giving you the ability to remotely manage USB flash drives from anywhere in the world. KRMC On-Premise was designed to work specifically with the following iStorage Kanguru security drives:

Current

- Defender 3000
- Defender Elite 300
- Defender Elite 30
- Defender Bio-Elite30
- Defender Bio-Elite30 Life Planner Edition
- Defender HDD/SSD 35
- Defender HDD/SSD 350

- **Legacy**
- Defender V2
- Defender Basic+
- Defender Elite
- Defender DualTrust
- Defender 2000
- Defender Elite200
- Defender HDD/SSD
- Defender HDD/SSD300

The devices mentioned above communicate through a secure, encrypted tunnel to ensure that your information is protected. For more information regarding the communication protocols used by KRMC On-Premise, please contact: Sales@Kanguru.com.

KRMC On-Premise has an array of features that give administrators the ability to manage their iStorage Kanguru secure USB flash drives and hard drives. Below is a list of some of the features in KRMC On-Premise:

- Remote Data Deletion
- Self-Service Password Management (SSPM)
- Remote Device Disable/Enable
- Remote Password Management
- Administrator Level Auditing of Actions and Events
- Ability to Create Groups Consisting of Multiple Devices
- Configurable Offline Settings
- Remote Re-Provisioning of Devices for Security Policy Enforcement and Compliance
- IP Address and Hostname Device Usage Tracking
- Logging of All Account Actions and Events
- Organized Asset Management System
- Remote Messaging to Devices
- License Management for KRMC On-Premise and Endpoint Protection by BitDefender.
- Ability to Create Schedule-Based Actions

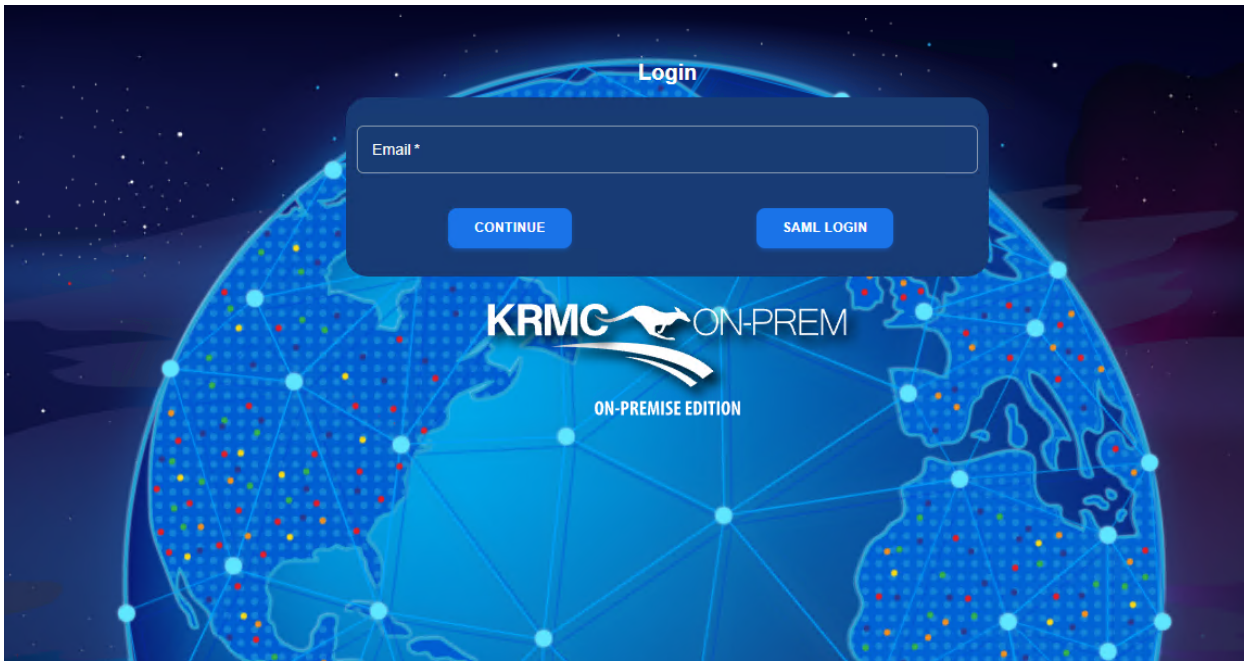
Installation of KRMC

2

The KRMC On-Premise Virtual Appliance has been pre-loaded and pre-configured with all the necessary software applications required to run. Installing KRMC On-Premise is as simple as running the virtual machine in a hypervisor. Currently KRMC On-Premise is able to be launched within the following environments.

Host system Requirements:

- Single-core processor or better
- 250GB Storage
- 4GB RAM or higher



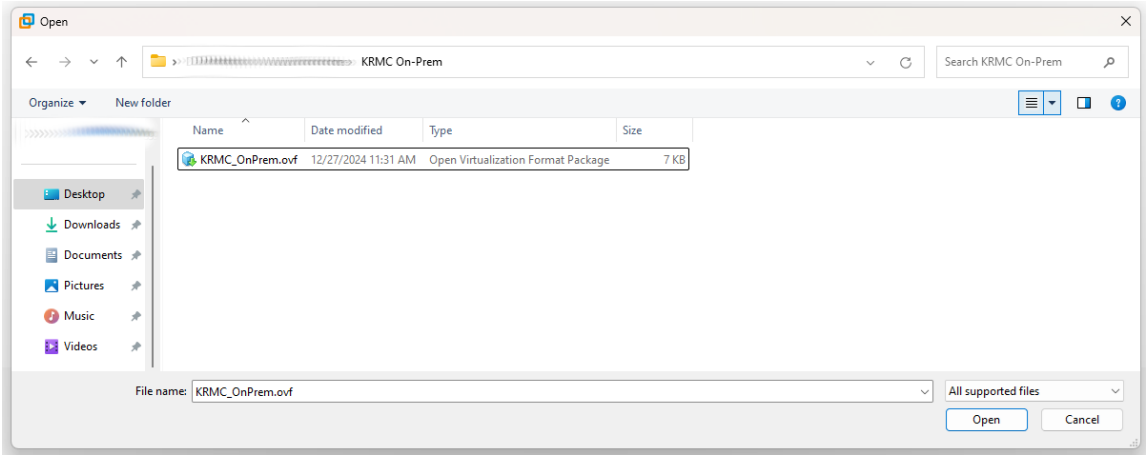
KRMC with VMware

The KRMC On-Premise Virtual Appliance has been pre-loaded and pre-configured with all the necessary software applications required to run. Installing KRMC On-Premise is as simple as running the virtual machine in a hypervisor.

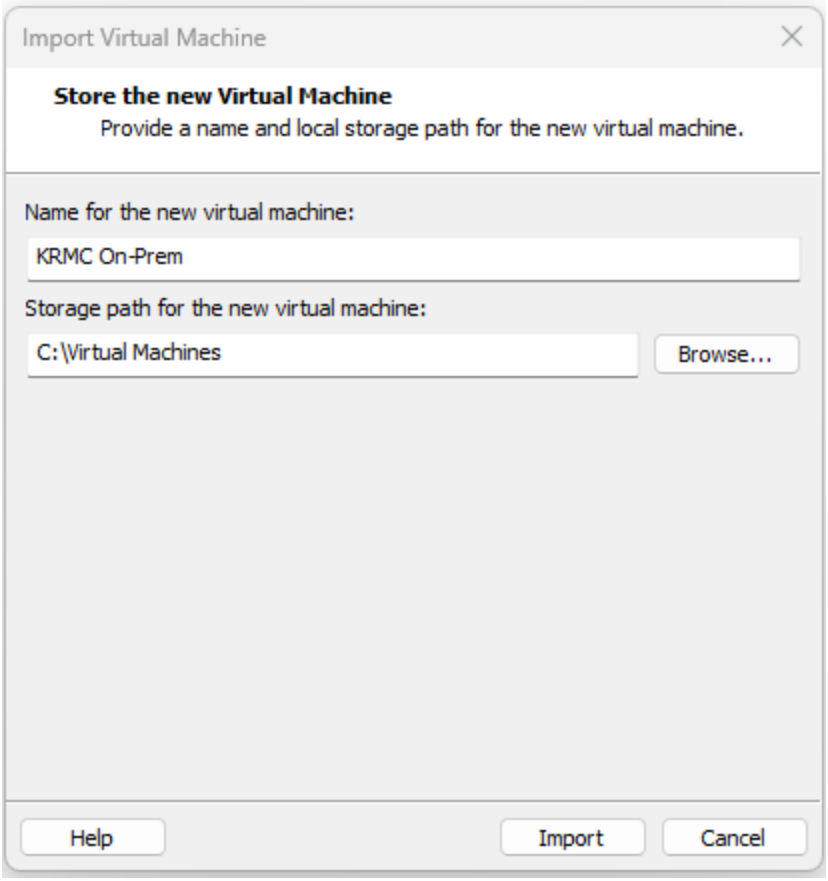
To setup KRMC On-Premise on VMware:

1. Unzip the KRMC On-Premise file and save the contents to a local drive on the host machine.
2. Launch a VMware hypervisor. In this example we will be using VMware Workstation. Your actual experience may vary depending on which VMware hypervisor you use.
3. From VMware Workstation Home page select "Open a Virtual Machine".

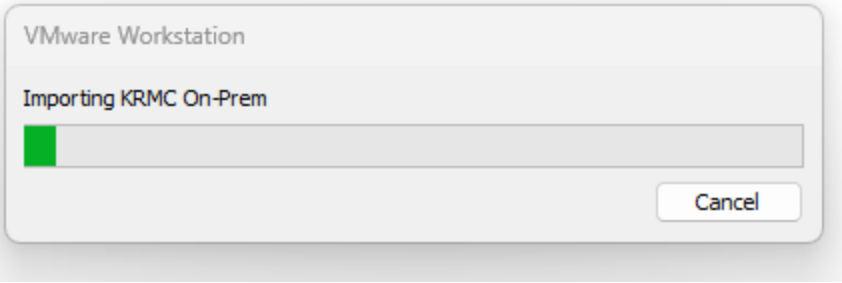
4. A pop-up window should appear now. Use this window to navigate to the location you extracted the files in Step 1. Once there select the file "KRMC_OnPrem.ovf" and select "Open" at the bottom right of the display.



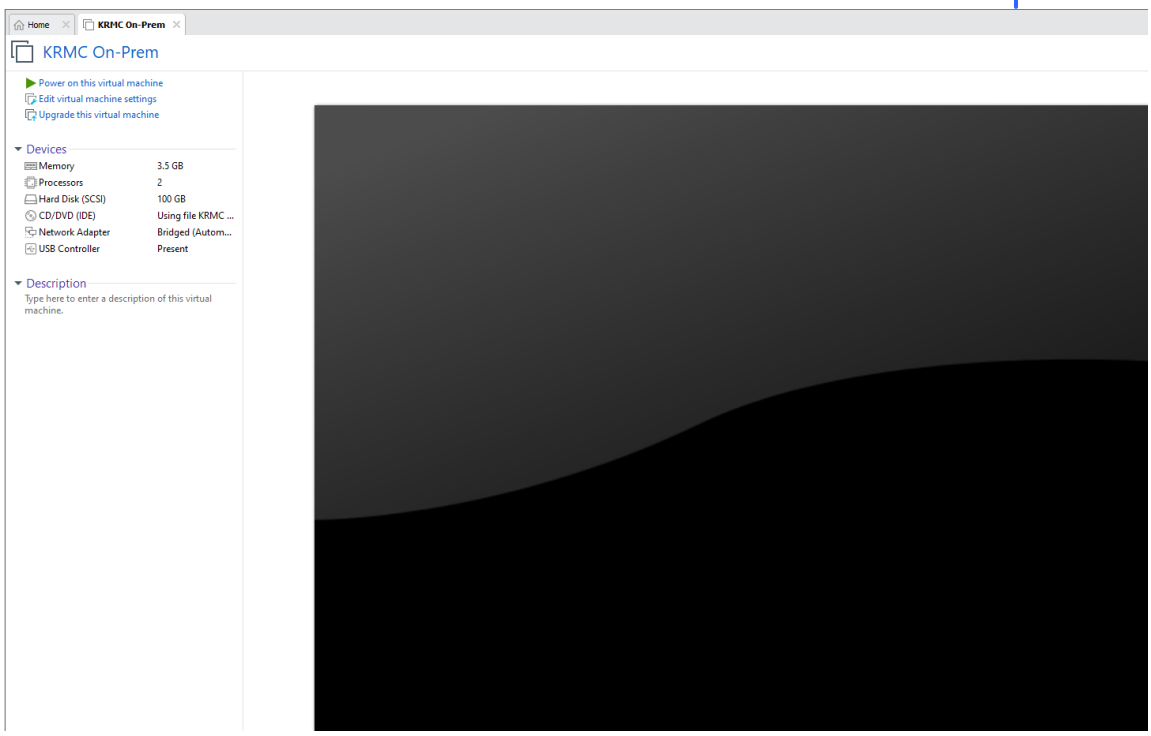
5. You will need to create a name for the KRMC On-Premise VM as well as a path for the appliance to be stored. In this example I have named the VM "KRMC On-Premise" and have chosen the location "C:\Virtual Machines" for the VM to be stored. After completing this information, you can now select "Import".



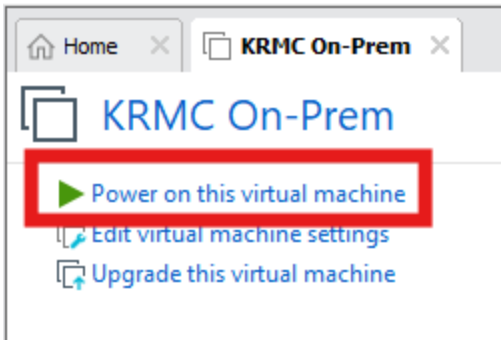
6. When you select "Import" you should receive a pop-up window showing the progress of the KRMC import. This may take a few minutes to complete.



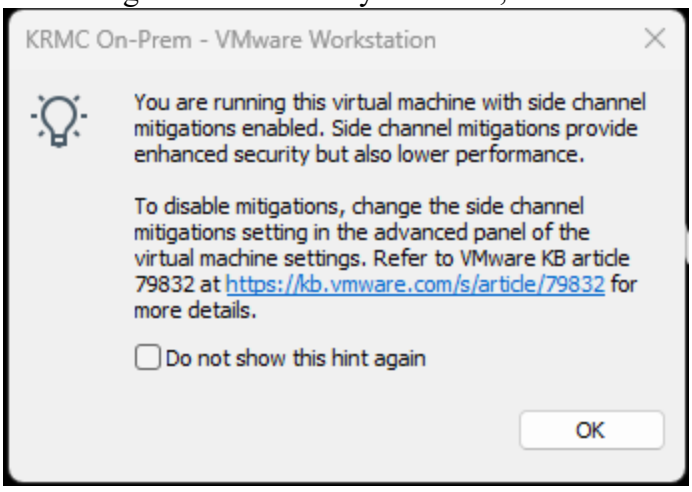
7. After the virtual machine has been imported, it will appear in the library. We would recommend verifying that the "Network Adapter" meets your network requirements. If it does not, you will need to alter the "Network Adapter" settings by double clicking it. For my example we are using the VM set as "Bridged" however yours may be different depending on your environment.



8. To start the KRMC On-Premise VM you will need to select "Power on this virtual machine" located at the top left of the display.



9. When the virtual machine starts, you may receive a message stating the virtual machine is running with side channel mitigations enabled. If you see this, select "OK" to proceed.



10. Once KRMC boot you will be brought to the KRMC VM Main Menu 69. If this is your first time using KRMC, you will be able to follow the steps under Setting up KRMC for first time 22.

Congratulations! Open a browser and navigate to the IP address displayed in the top of the Main Menu to access your KRMC.

Installation of KRMC

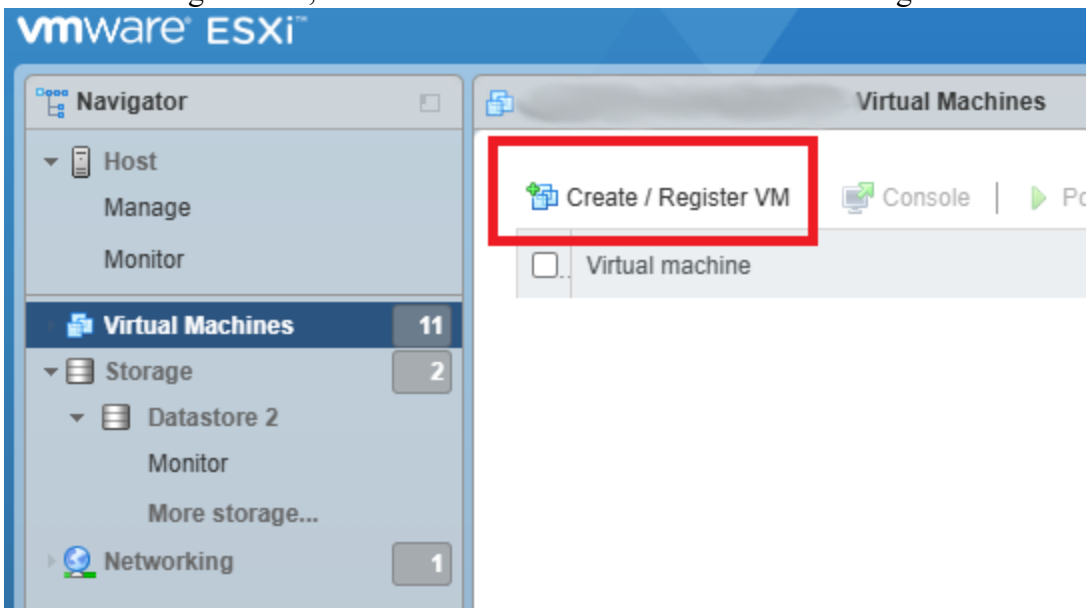
2

KRMC with ESXi

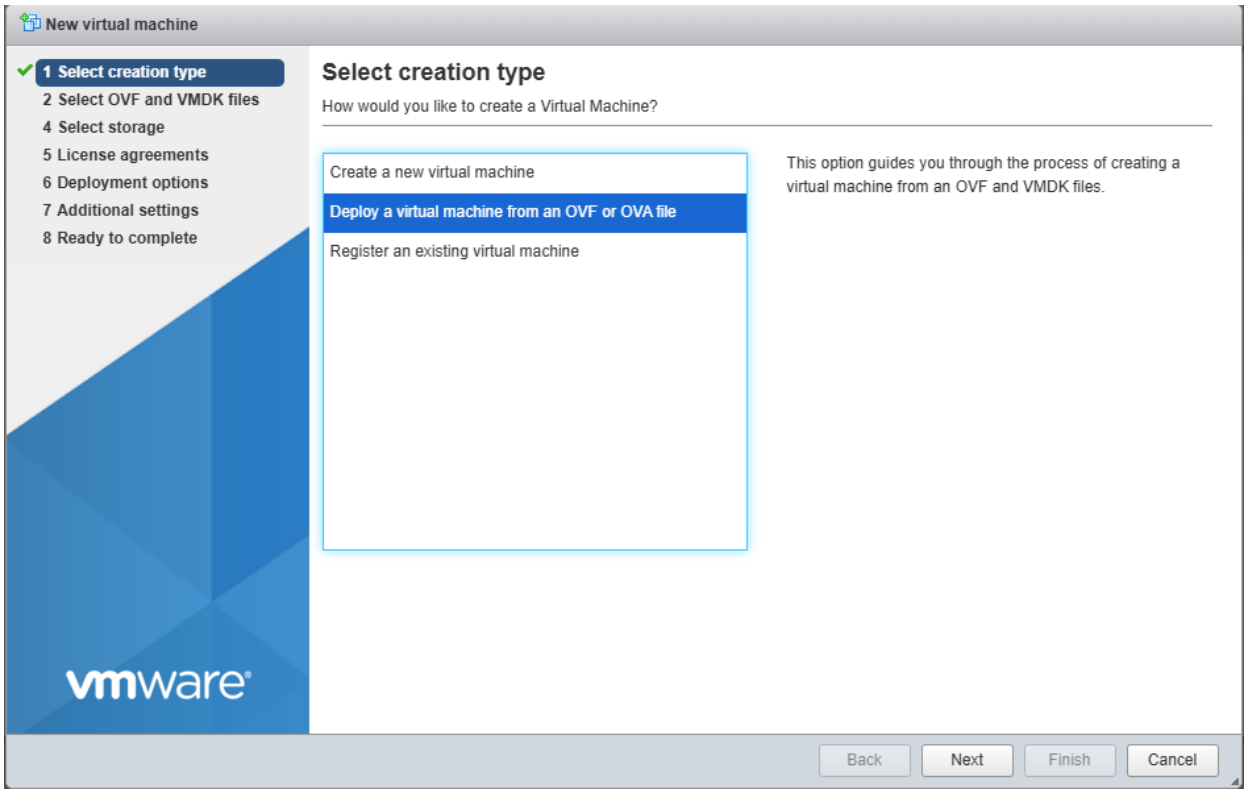
The KRMC On-Premise Virtual Appliance has been pre-loaded and pre-configured with all the necessary software applications required to run. Installing KRMC On-Premise is as simple as running the virtual machine in a hypervisor.

To setup KRMC On-Premise on ESXi:

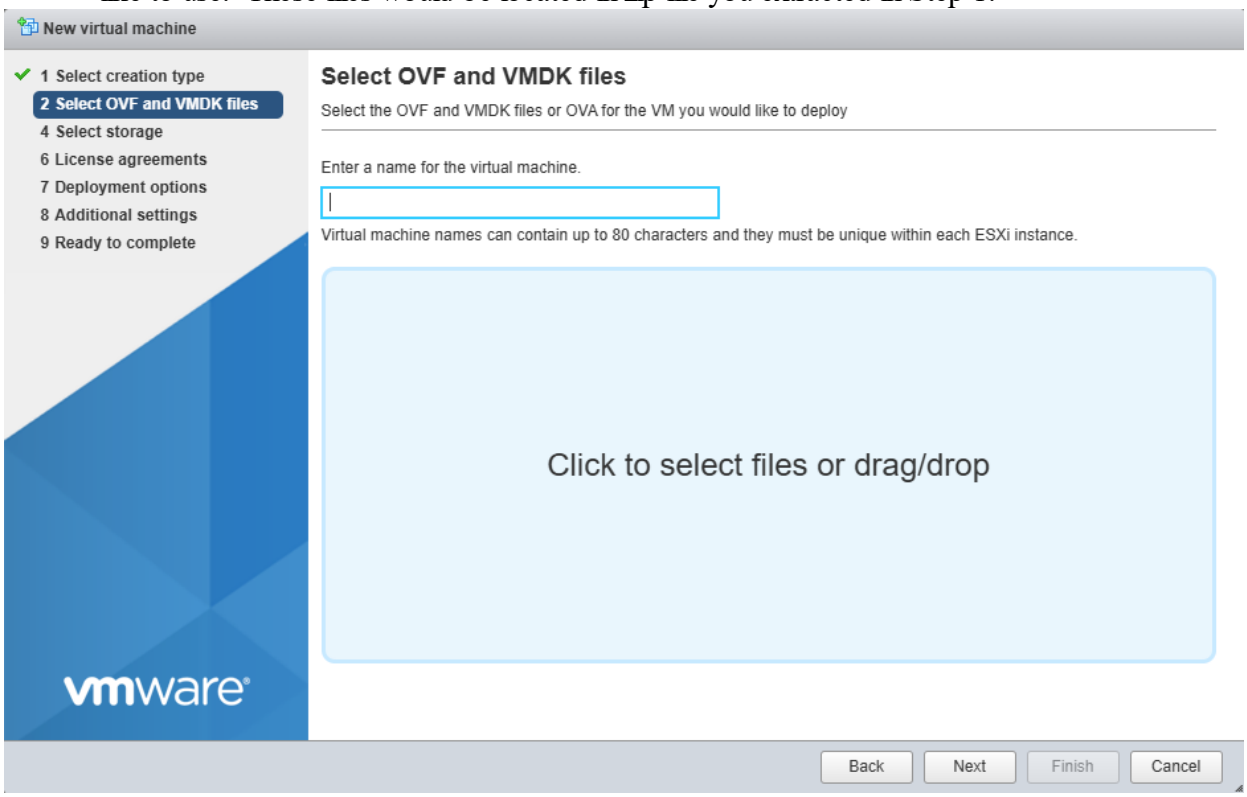
1. Unzip the KRMC On-Premise file and save the contents to a local drive on the host machine.
2. Log into your ESXi portal. In this example we will be using ESXi 7. Your actual experience may vary depending on which ESXi hypervisor you use.
3. From the navigation bar, select Virtual Machines then select "Create / Register VM".



4. A New Virtual Machine wizard should appear now. Select "Deploy a virtual machine from an OVF or OVA file" then select "Next".

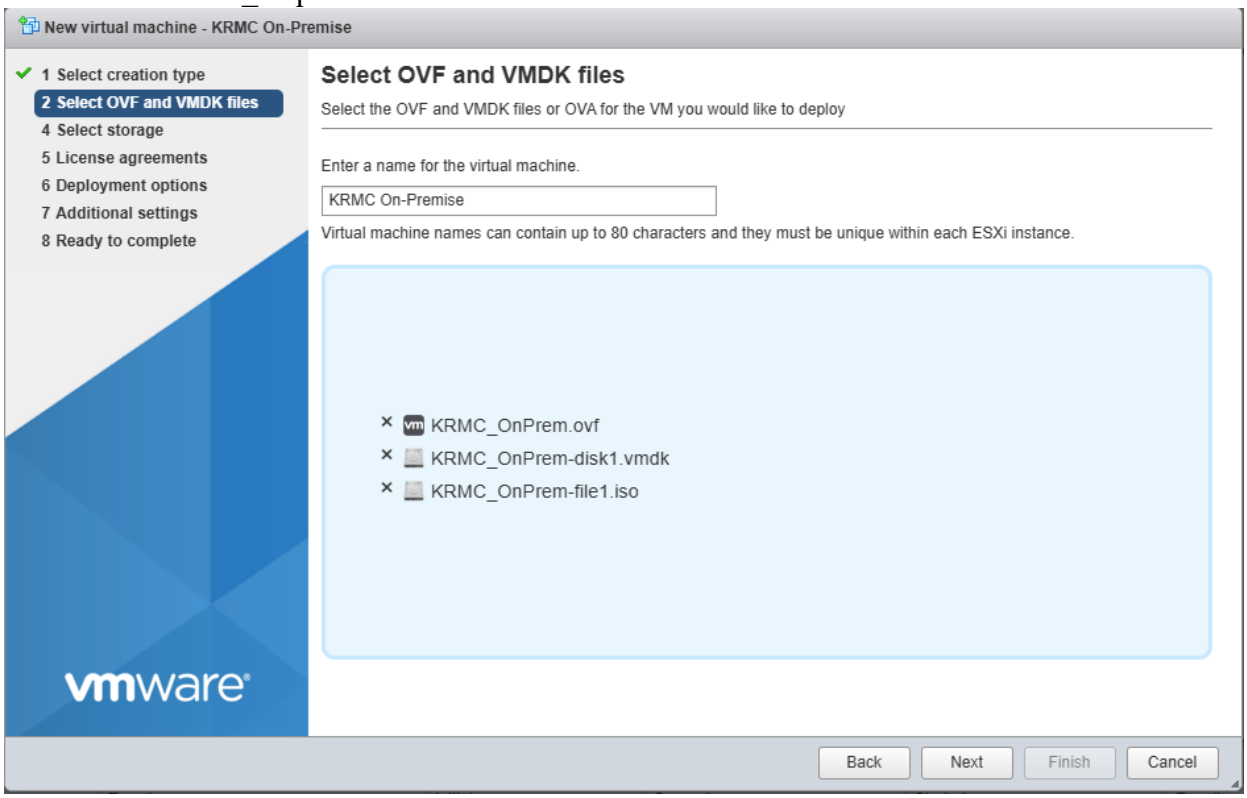


5. You will now be asked to enter a name for you virtual machine as well as select files you would like to use. These files would be located in zip file you extracted in Step 1.

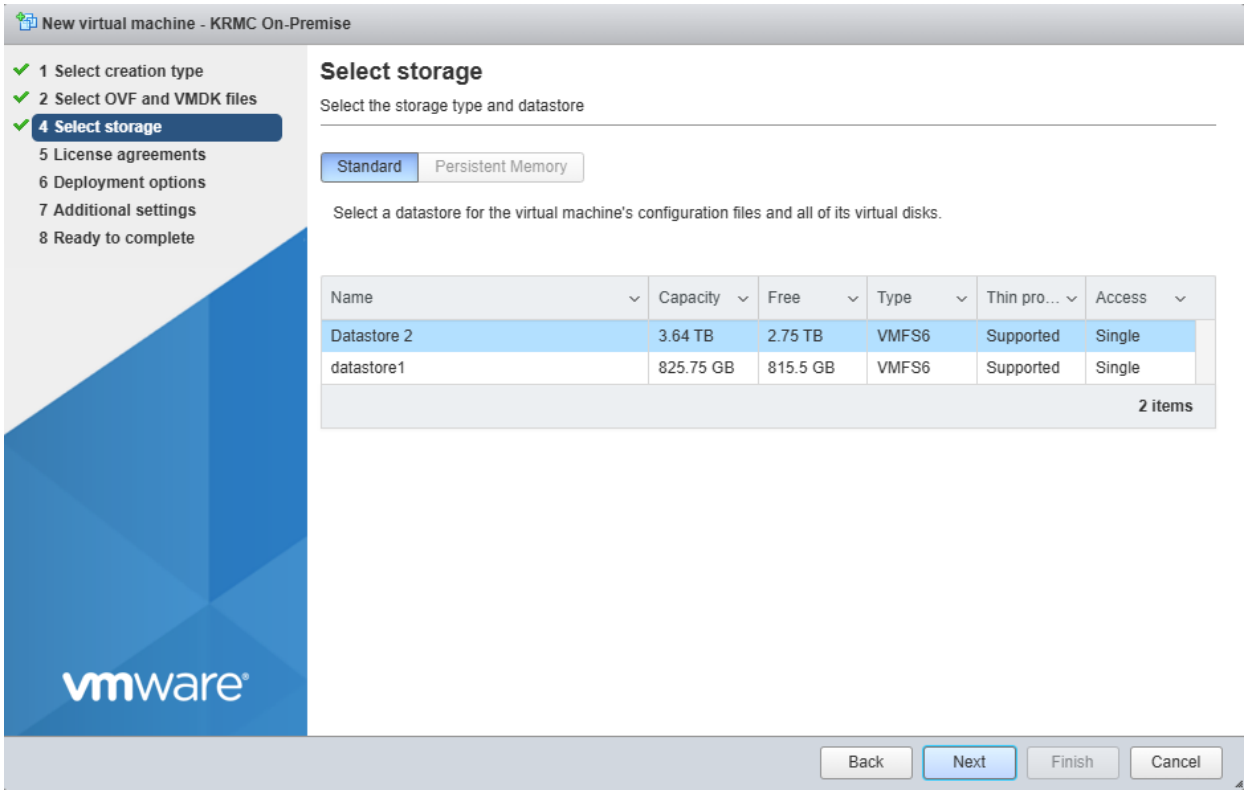


6. Next you will need to select the files from Step 1 to upload. After uploading them, you will select "Next". You will need to upload the following files:
   a. KRMC_OnPrem.ovf

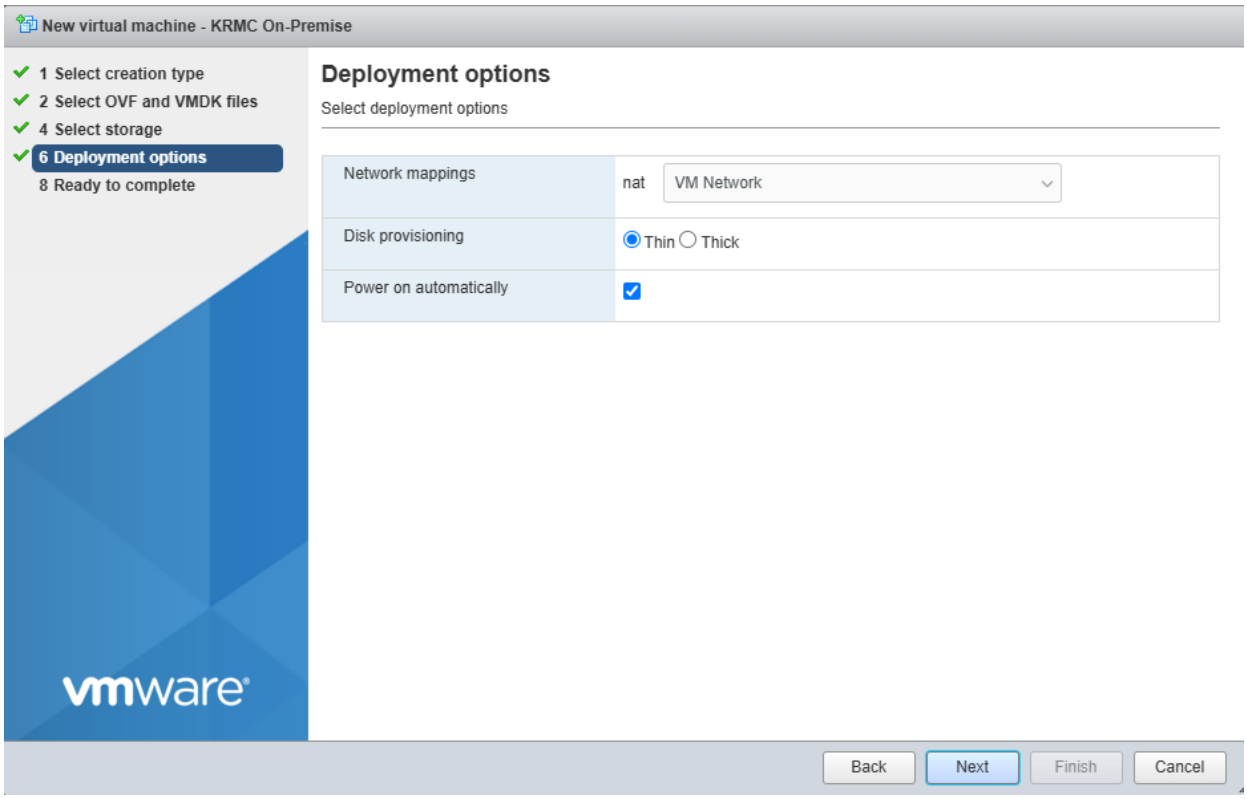
b. KRMC_OnPrem-disk1.vmdk
c. KRMC_Onprem-file1.iso



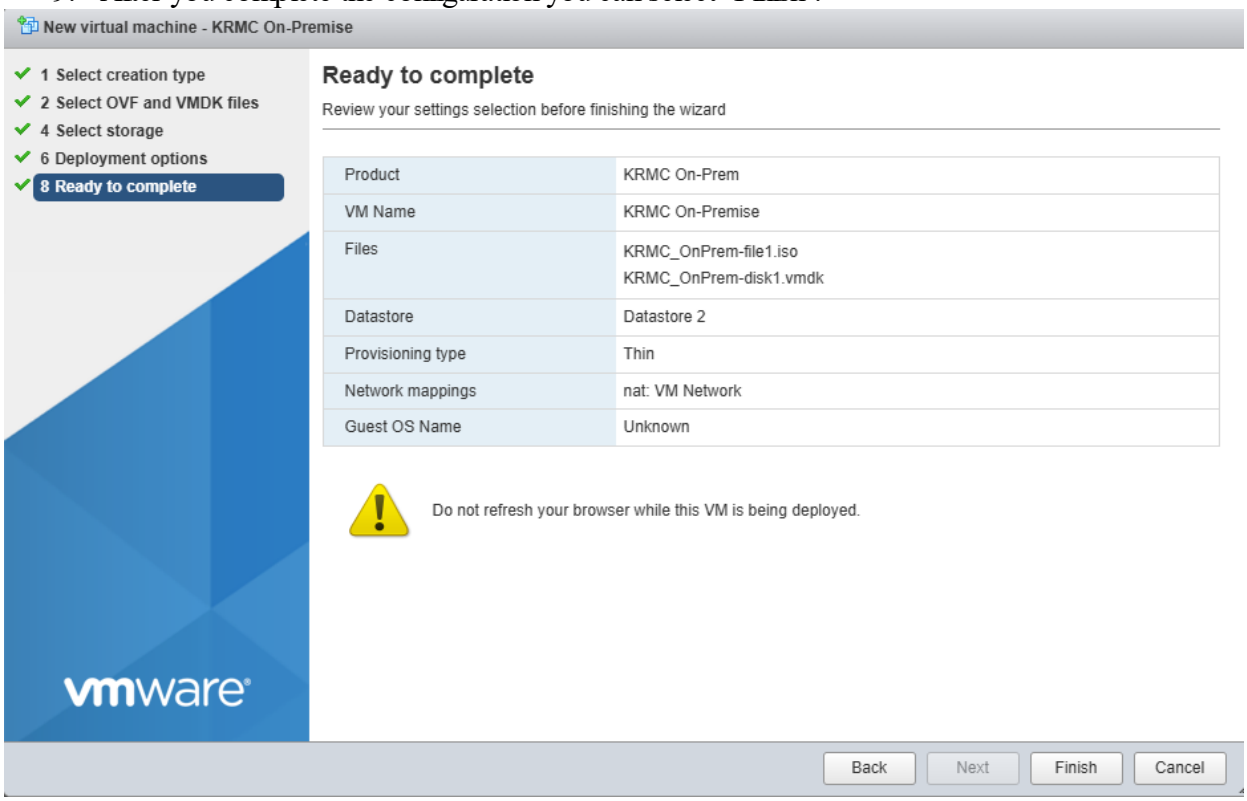
7. Select the datastore for KRMC to be stored and click "Next".



8. You can edit the Deployment options as you see fit. In this example we are leaving them with the default settings.

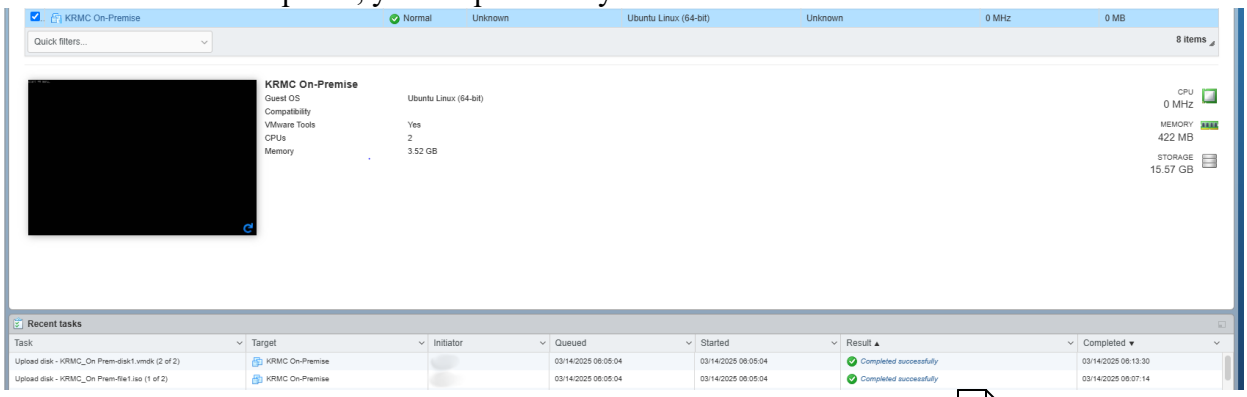


9. After you complete the configuration you can select "Finish".



10. ESXi will now attempt to create the KRMC virtual appliance based on the information and files provided. This may take a few minutes to complete however once it is completed you will this

KRMC virtual appliance located under your list of virtual machines. After this appears and the creation is completed, you can power on your KRMC VM and wait for it to boot.



11. Once KRMC boot you will be brought to the KRMC VM Main Menu 69. If this is your first time using KRMC, you will be able to follow the steps under Setting up KRMC for first time 22.

Congratulations! Open a browser and navigate to the IP address displayed in the top of the Main Menu to access your KRMC.

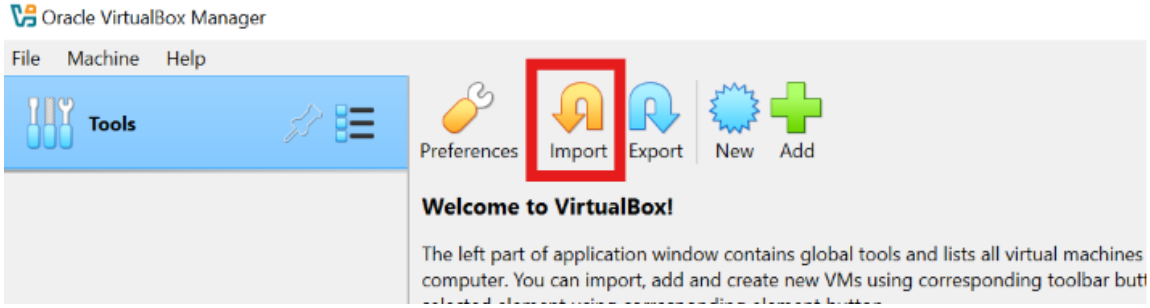
Installation of KRMC 2

KRMC with VirtualBox

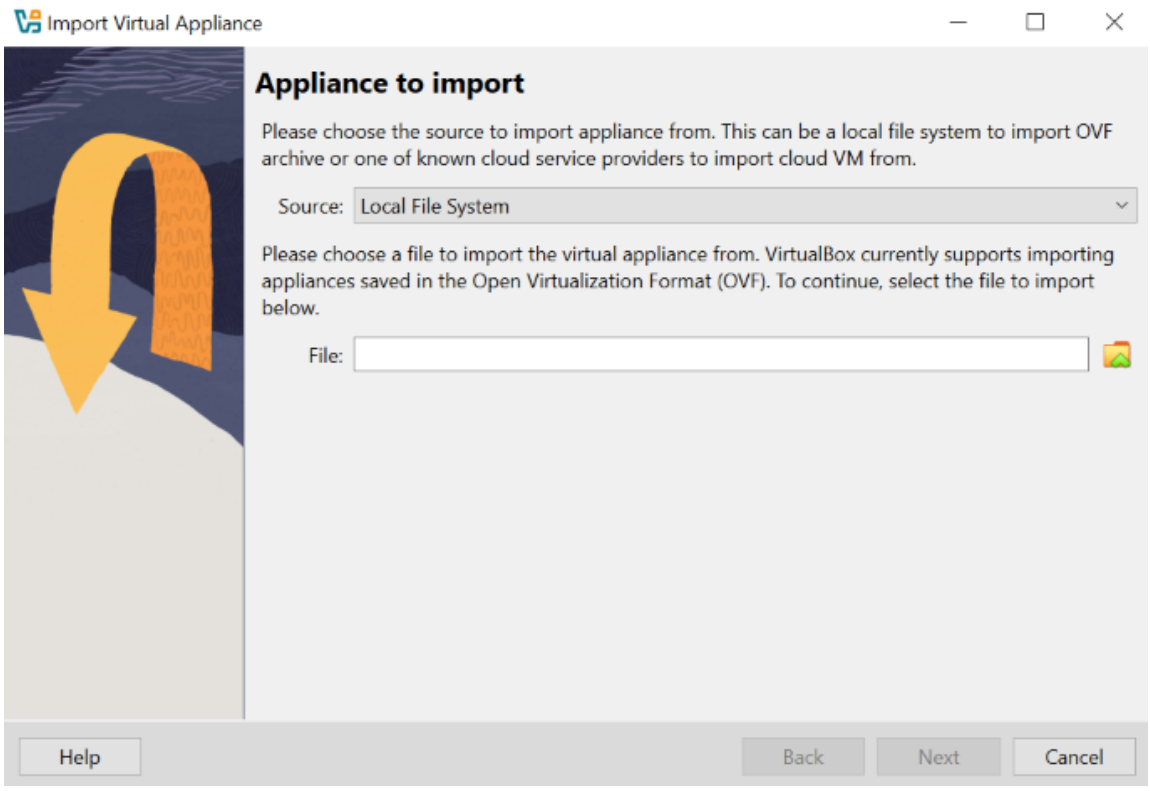
The KRMC On-Premise Virtual Appliance has been pre-loaded and pre-configured with all the necessary software applications required to run. Installing KRMC On-Premise is as simple as running the virtual machine in a hypervisor.

To setup KRMC On-Premise on VirtualBox:

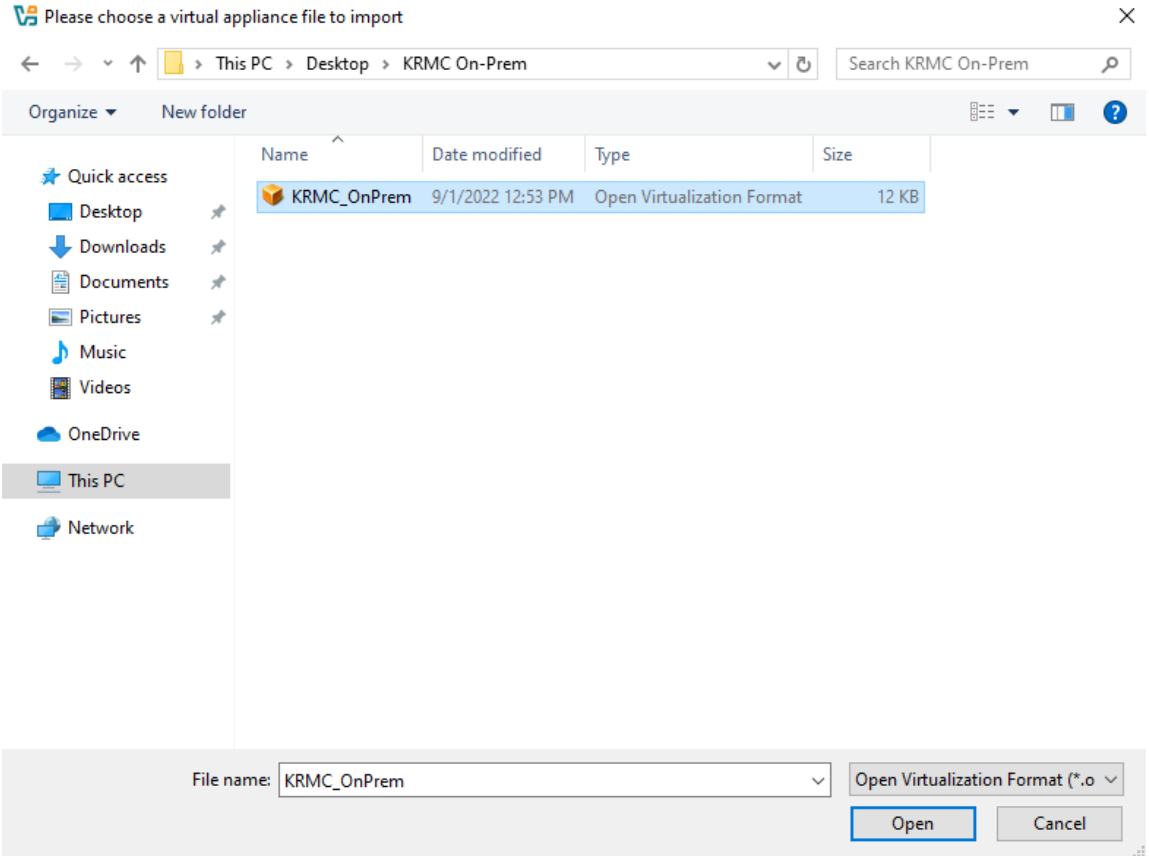
1. Unzip the KRMC On-Premise file and save the contents to a local drive on the host machine.
2. Launch a VirtualBox hypervisor.
3. From the VirtualBox Manager, select "Import".



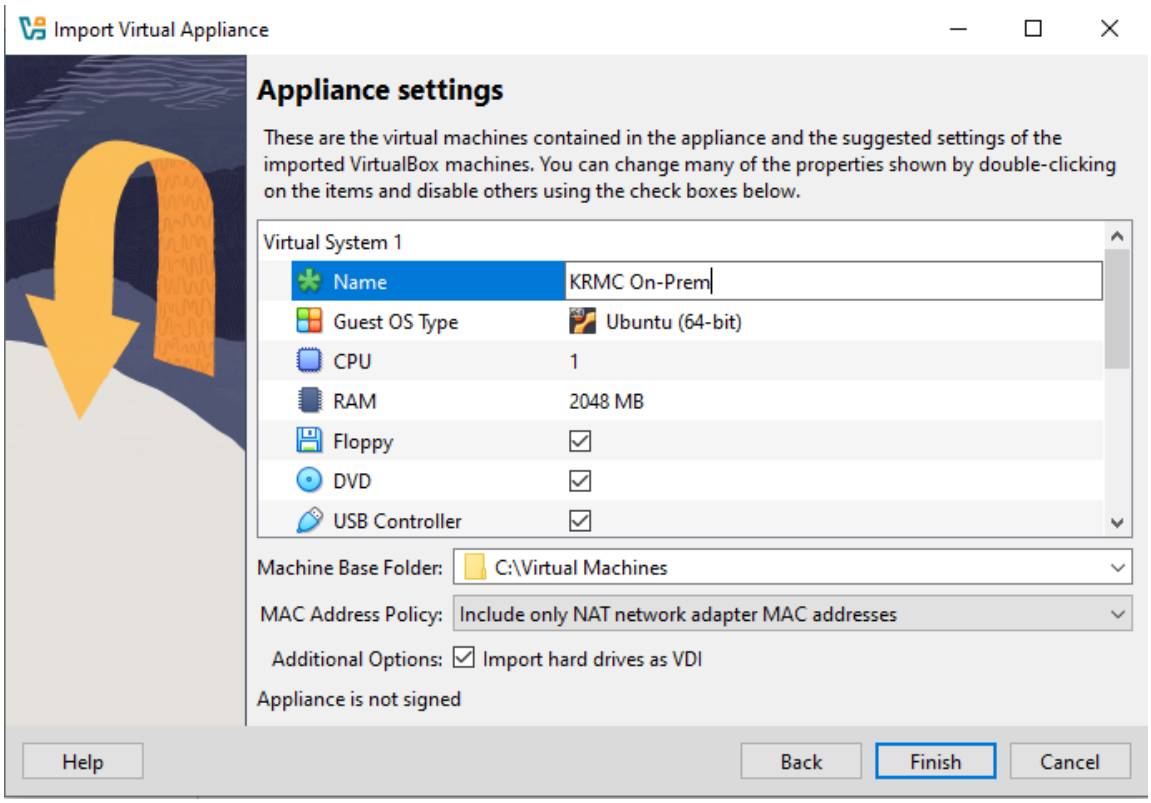
4. The "Import Virtual Appliance" window will appear. From here you will need to choose the "KRMC_OnPrem.ovf" file that you extracted in Step 1. You can accomplish this by either entering the path of the file in the space provided or by selecting the file icon to the right of this field.



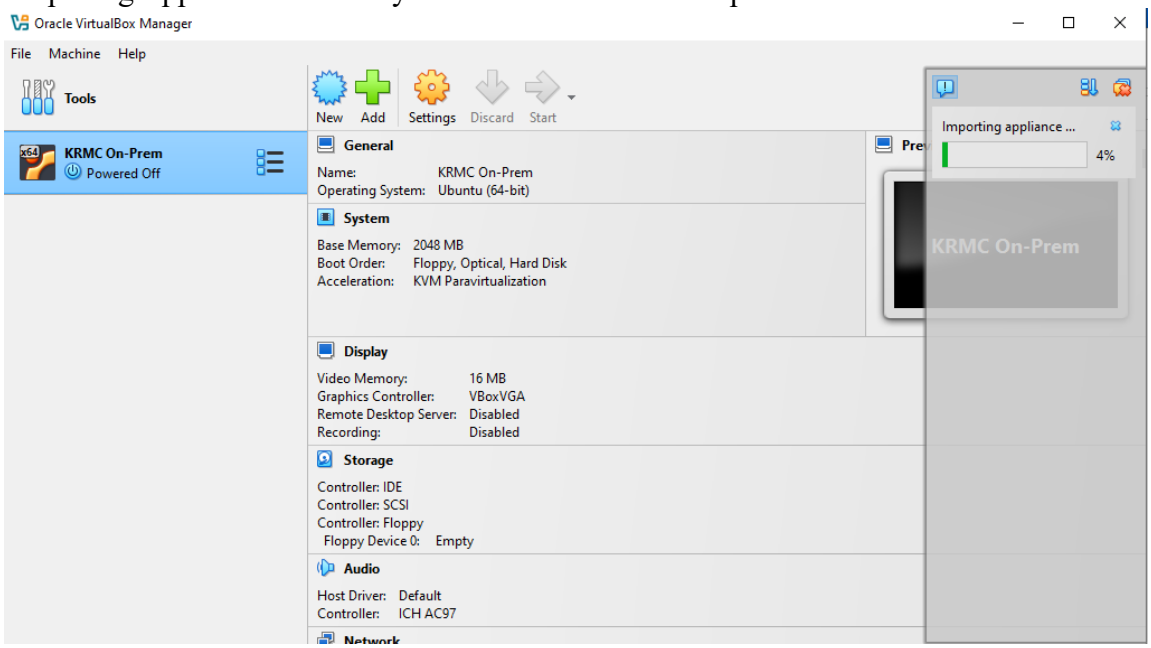
5. If you selected the file icon, a pop-up will appear so you can navigate to the location you extracted the files to in Step 1. Once there select the file "KRMC_OnPrem.ovf" and select "Open" at the bottom right of the display.



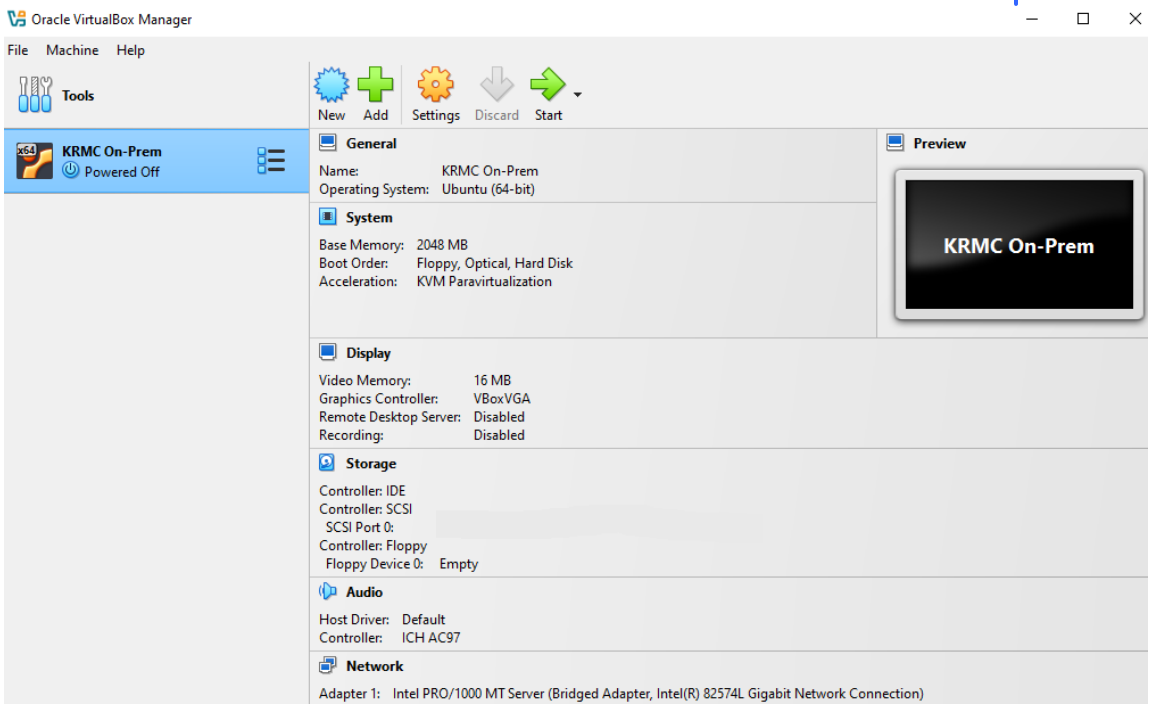
6. After the "KRMC_OnPrem.ovf" file has been selected, you should see the file path displaying for you after a few seconds. You will need to select "Next" to continue
7. You will need to create a name for the KRMC On-Premise VM as well as a path for the appliance to be stored. In this example I have named the VM "KRMC On-Premise" and have chosen the location "C:\Virtual Machines" for the VM to be stored. After completing this information, you can now select "Finish".



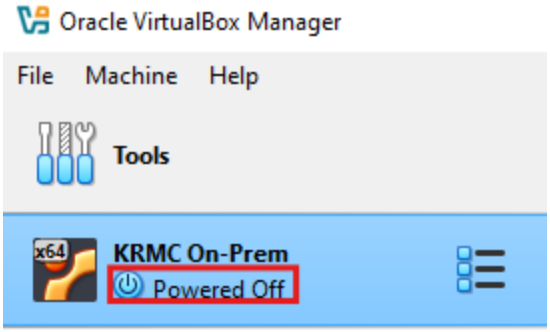
8. When you select "Finish" you see the pop-up will close and a right side bar will appear stating "Importing Appliance". This may take a few minutes to complete.



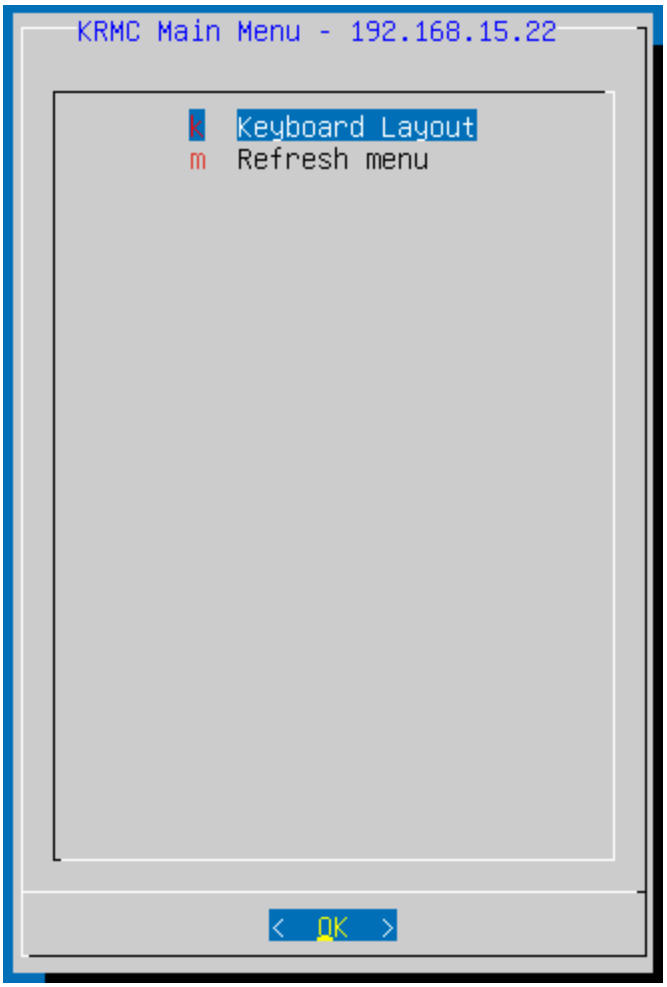
9. After the virtual machine has been imported, it will appear in the library. We would recommend verifying that the "Network" meets your network requirements. If it does not, you will need to alter the "Network" settings by double clicking it. For my example we are using the VM set as "Bridged" however yours may be different depending on your environment.



10. To start the KRMC On-Premise VM you will need to double click "Powered Off" located at the top left of the display.



11. Once KRMC boot you will be brought to the KRMC VM Main Menu 69. If this is your first time using KRMC, you will be able to follow the steps under Setting up KRMC for first time 22.



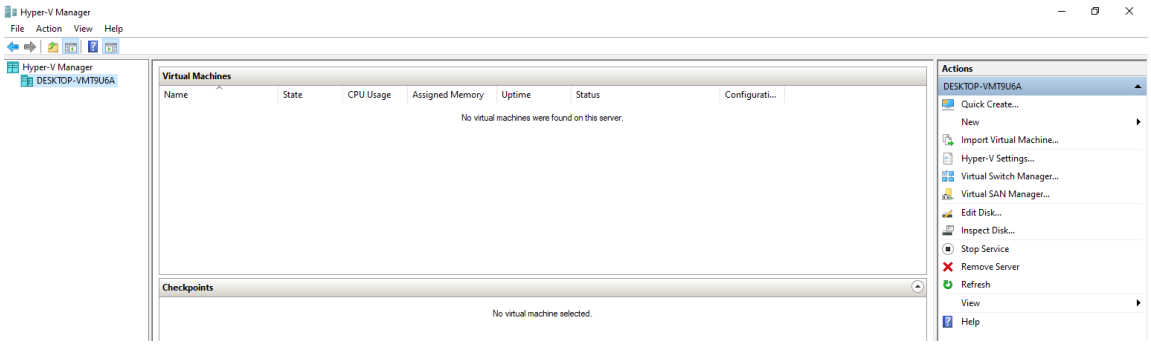
Congratulations! Open a browser and navigate to the IP address displayed in the top of the Main Menu to access your KRMC.

KRMC with Hyper-V

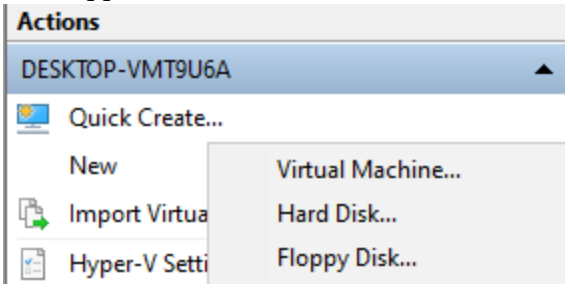
The KRMC On-Premise Virtual Appliance has been pre-loaded and pre-configured with all the necessary software applications required to run. Installing KRMC On-Premise is as simple as running the virtual machine in a hypervisor.

To setup KRMC On-Premise on Hyper-V:

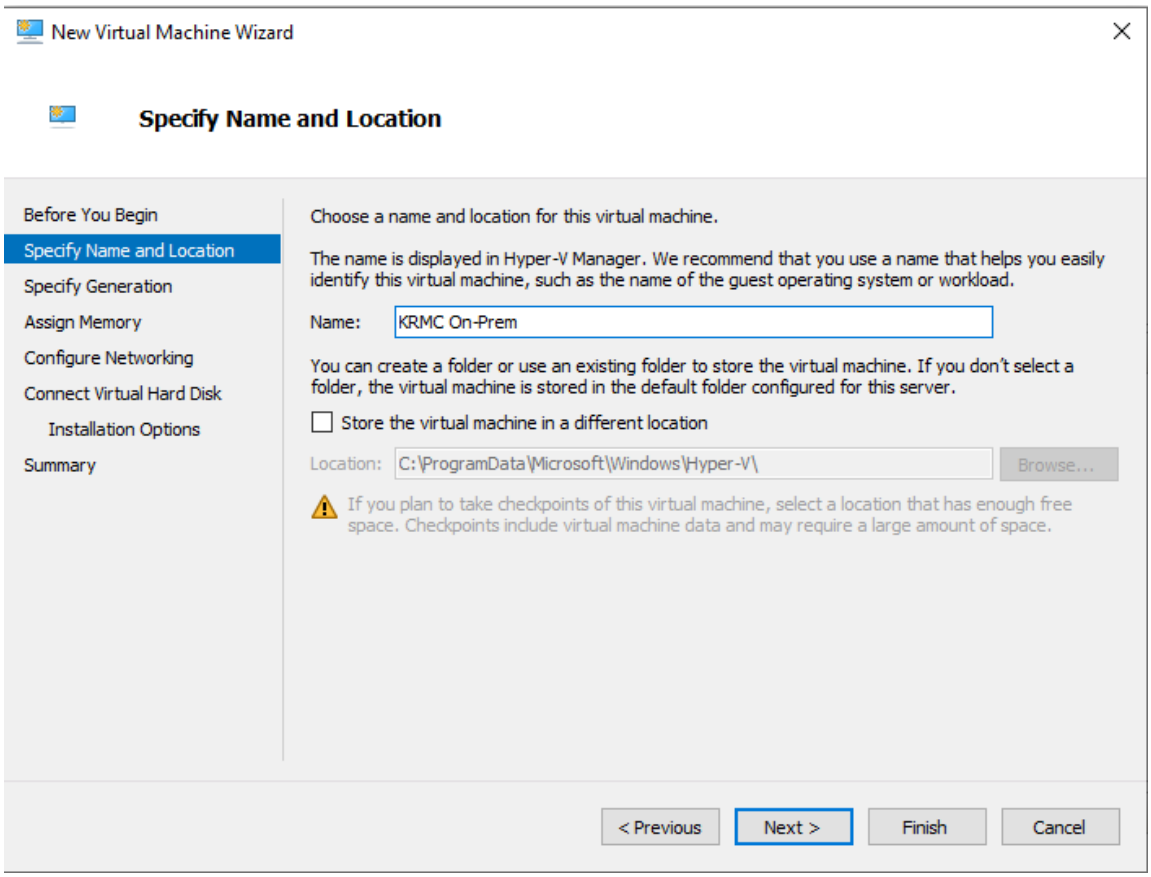
1. Unzip the KRMC On-Premise file and save the contents to a local drive on the host machine.
2. Launch Hyper-V Manager.
3. From Hyper-V Manager main page, locate “Actions” on the right side of the screen and select “New”



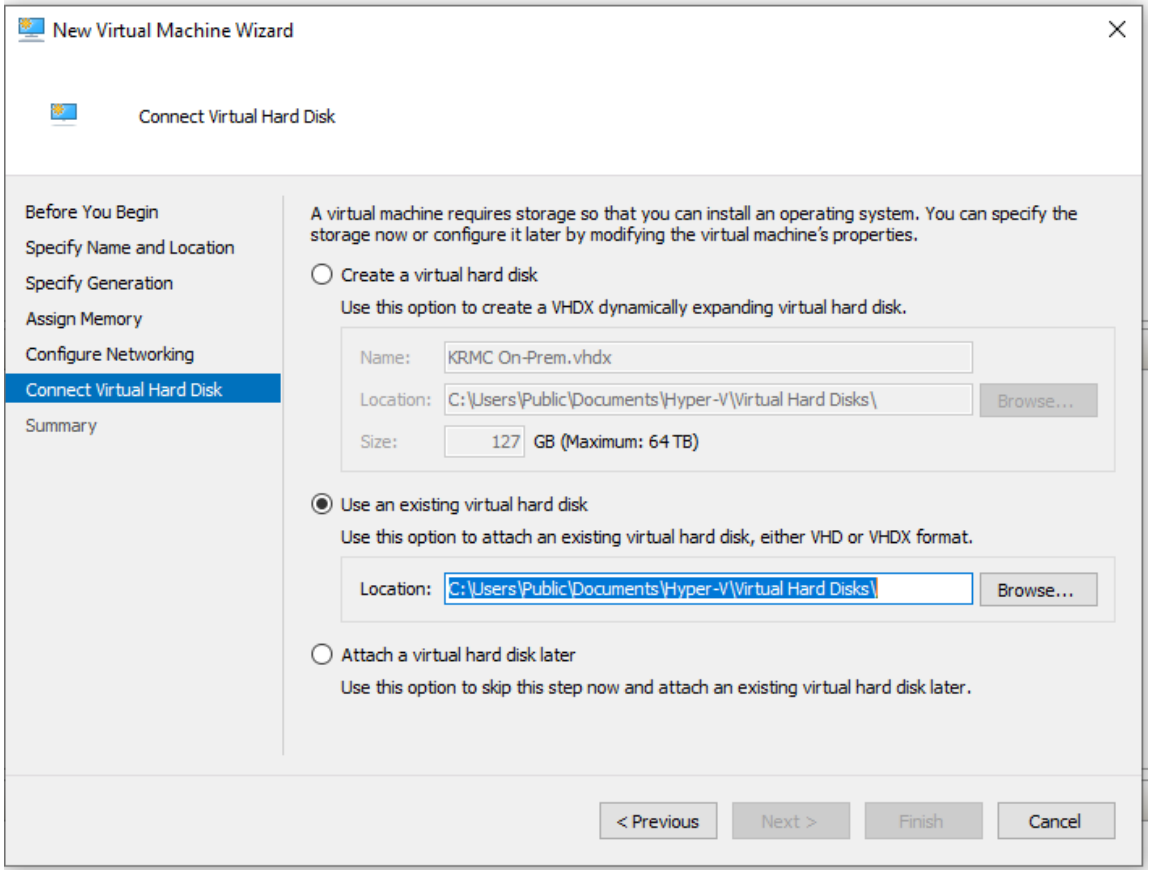
4. On the drop-down menu that appears, select “Virtual Machine”.



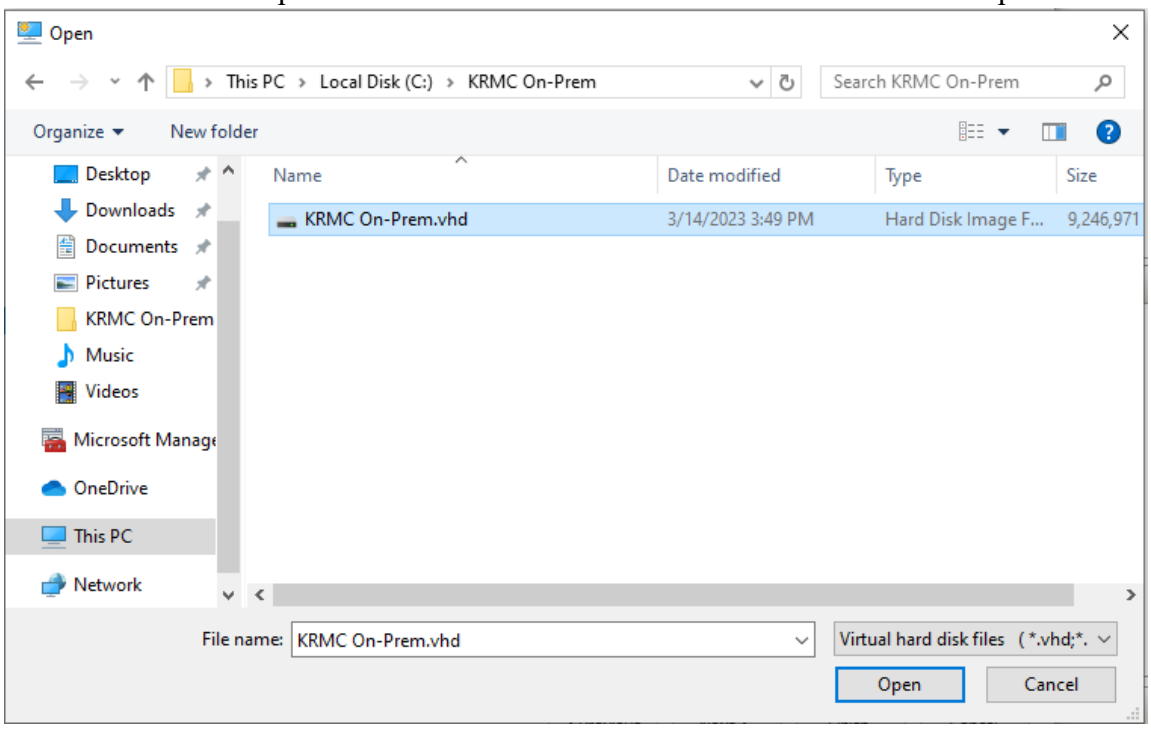
5. A pop-up window should appear now. Use this window to name your virtual machine. In this case we named it “KRMC On-Premise”.



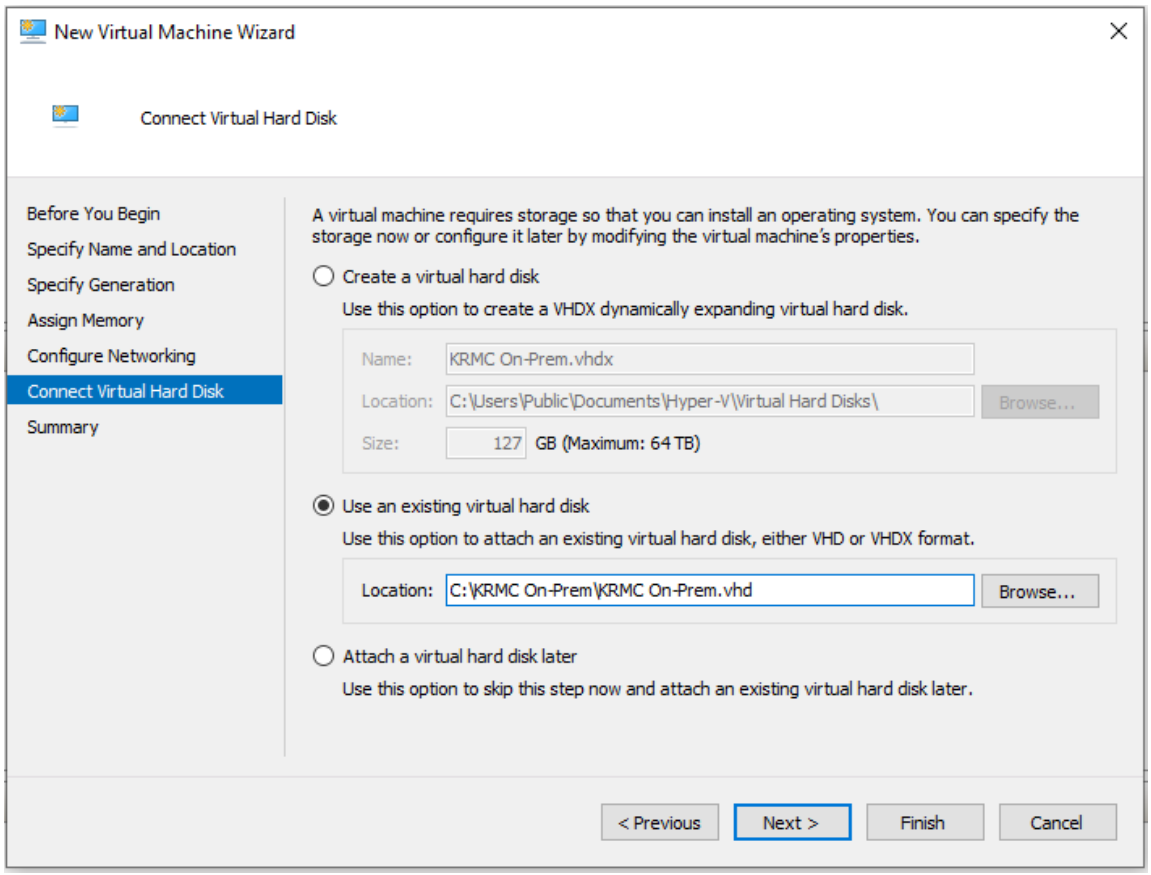
6. After naming the virtual machine, you can select "Connect Virtual Hard Disk" from the left side navigation. Select the option "Use an existing virtual hard disk" then select "Browse…".



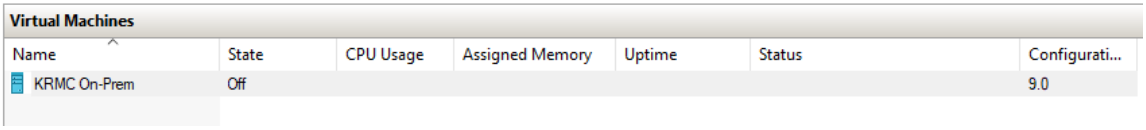
7. A File Explorer window will now appear and you need to navigate to the location you extracted the file in Step 1. Select the file "KRMC On-Premise.vhd" and select "Open".



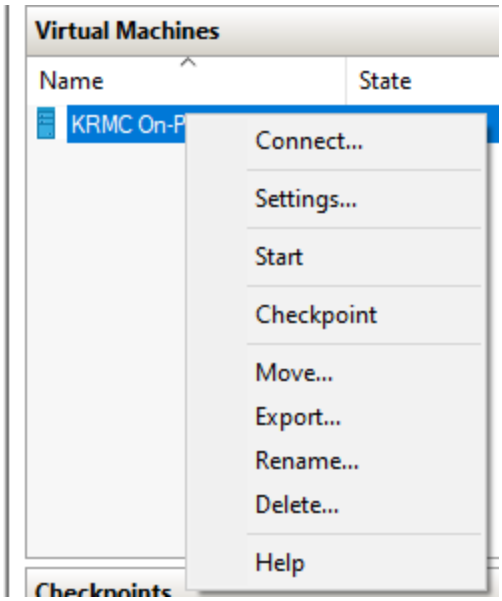
8. After your VHD file appears, select "Finish".



9. The virtual machine will be created and this may take a few minutes. Once the import has been completed, you will see this appear on you Hyper-V manager main window.



10. To start the KRMC On-Premise VM you will need to right click onto the virtual machine and select "Start".



11. Once KRMC boot you will be brought to the KRMC VM Main Menu 69. If this is your first time using KRMC, you will be able to follow the steps under Setting up KRMC for first time 22.

Congratulations! Open a browser and navigate to the IP address displayed in the top of the Main Menu to access your KRMC.

Setting up KRMC for the first time 3

KRMC On-Premise has been designed to streamline the setup process for first time use. In only 14 steps your server will be fully accessible and ready to be used.
The default credentials required to complete the setup are as follows:

Email	root
Password	krmc

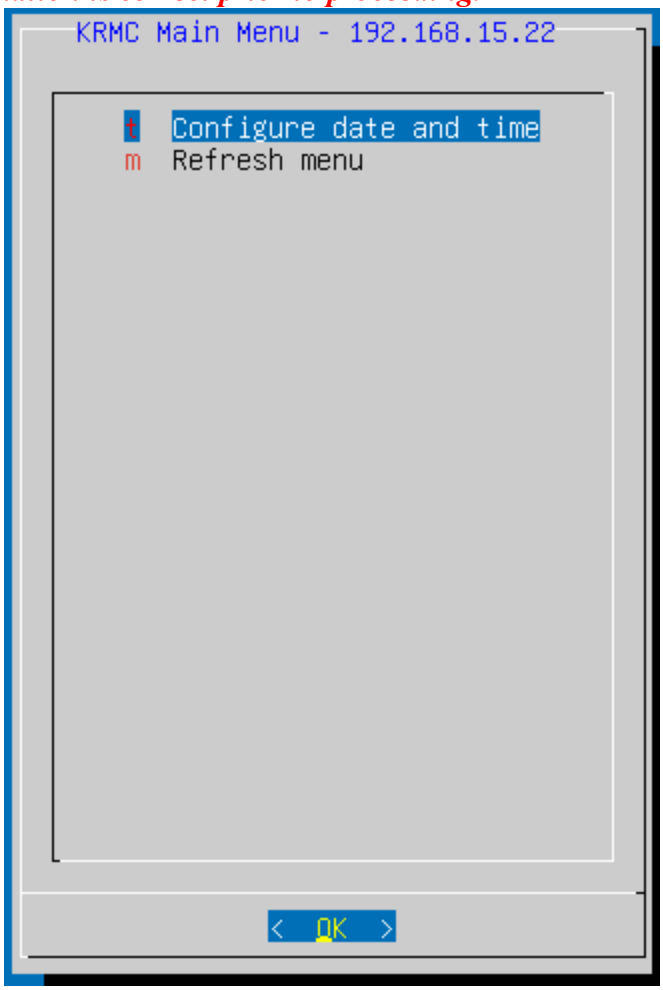
To proceed with these steps, make sure you have completed Installation of KRMC 2.

Note: *Steps 1 – 4 described here require configure options on the KRMC 9 VM menu. For information on these option, please refer to* *KRMC On-Premise Virtual Console* 69.

1. After installing and powering on your KRMC server in your choice of hypervisor, you will be brought to the setup menu for the **KRMC On-Premise Virtual Console**. Use the **Up** and **Down** arrows until you see Keyboard Layout 96 is selected and press **ENT**. The **Keyboard Layout** can be altered after the setup is completed as well.

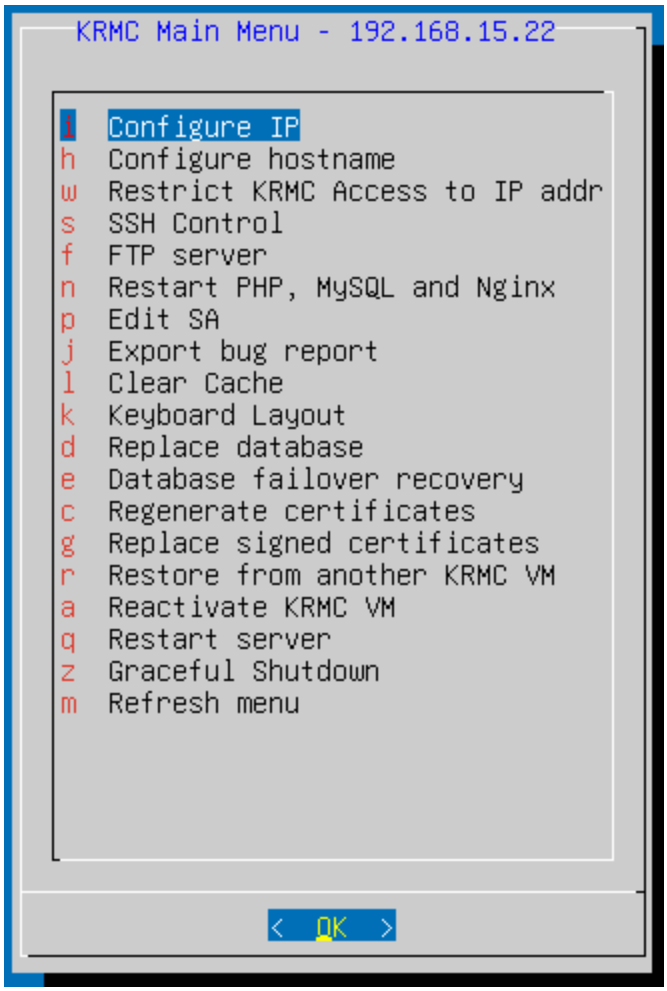
2. Once you have completed **Keyboard Layout**, you will find the next option on the **KRMC On-Premise Virtual Console** to be completed is Configure date and time 71. Use the **Up** and **Down** arrows until you see **Configure date and time** is selected and press **ENT**. ***The***

option Configure date and time is unable to be altered after this point. Please make sure the information is correct prior to proceeding.

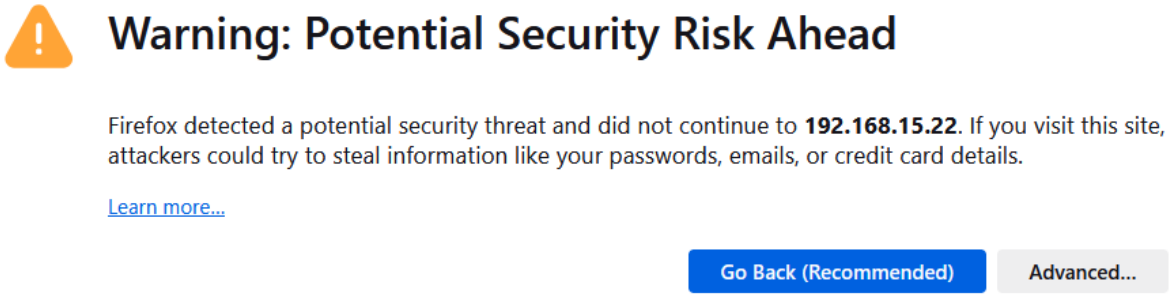


3. Once you have completed **Configure date and time**, you will find the next option on the **KRMC On-Premise Virtual Console** to be completed is Generate certificates 74. Use the **Up** and **Down** arrows until you see **Generate certificates** is selected and press **ENT**. If you are looking to use your own signed certificate, refer to Replace signed certificates 105. If you need to generate a new self-signed certificate for any reason, refer to Regenerate Certificates 103.

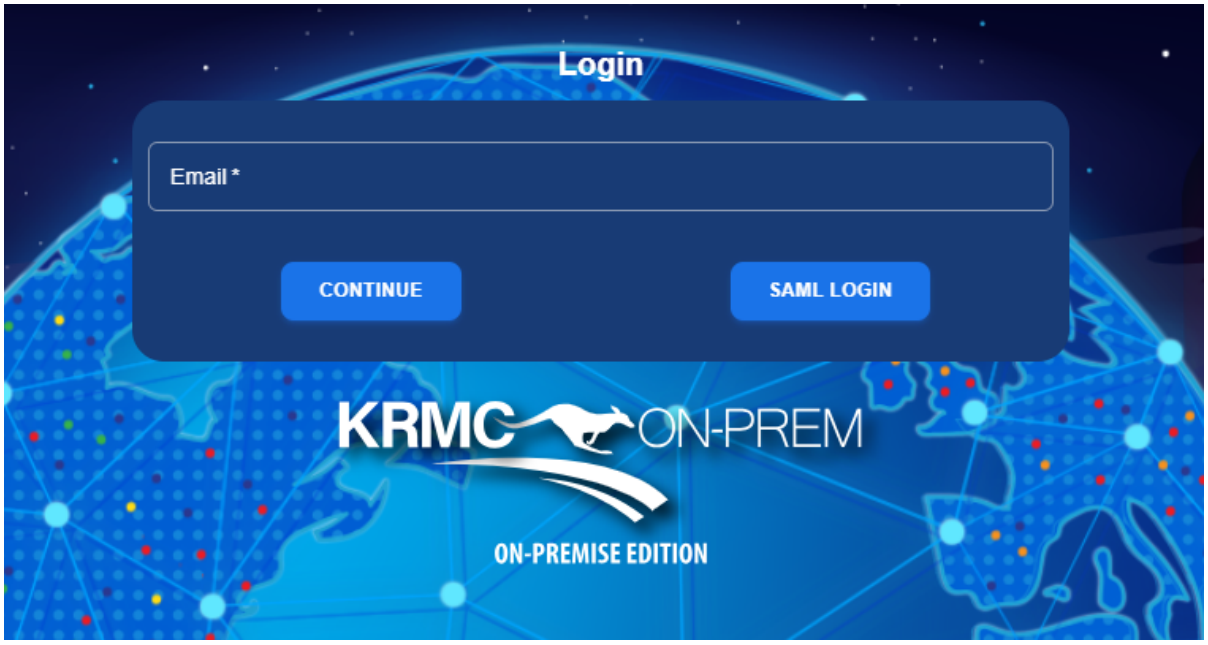
4. Your configuration of the **KRMC On-Premise Virtual Console** is now complete. If you would like to alter the IP address or Hostname, you can using Configure IP 76 and Configure Hostname 79 however it is not required. Additionally, if you are looking to migrate information from either KRMC 8 or a different version of KRMC 9, you can use Restore from another KRMC VM 107.



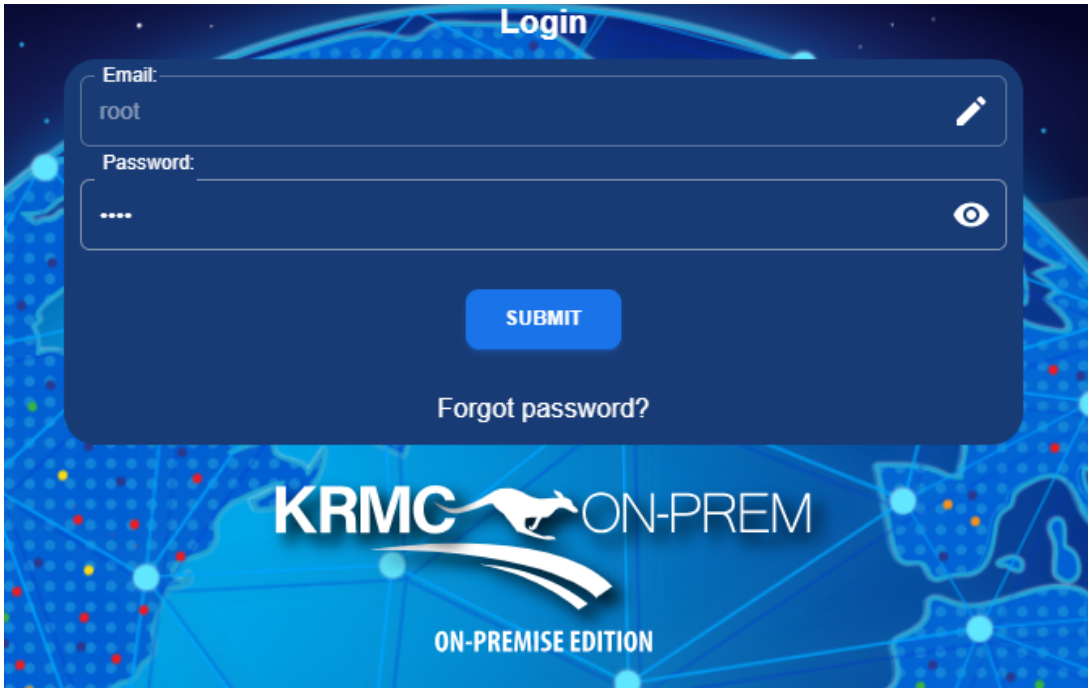
5. After completing the setup configuration on the **KRMC On-Premise Virtual Console**, you can now configure the web browser interface. At the top of your KRMC On-Premise Virtual Console menu you will find your IP address for the server. Open a browser and in the address bar navigate to https://<KRMC IP Address>. Since you are by default using a self-signed certificate, you will receive a message stating that there is a security risk (message will differ based on the browser). If you see this, select the option to advance/proceed to the site.



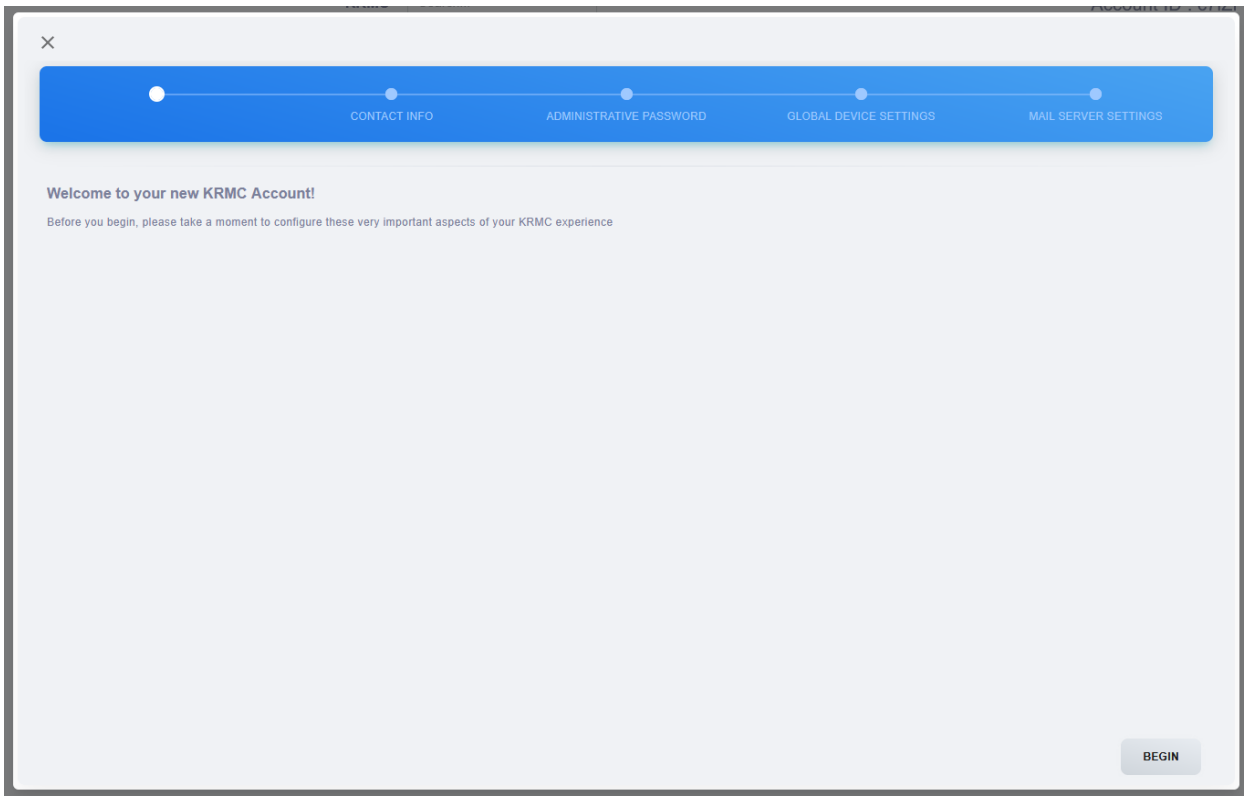
6. After proceeding beyond the security message, you will be brought to the Login screen for KRMC On-Premise (KRMC On-Prem). In the Email field, enter the default username root and select **Continue**.



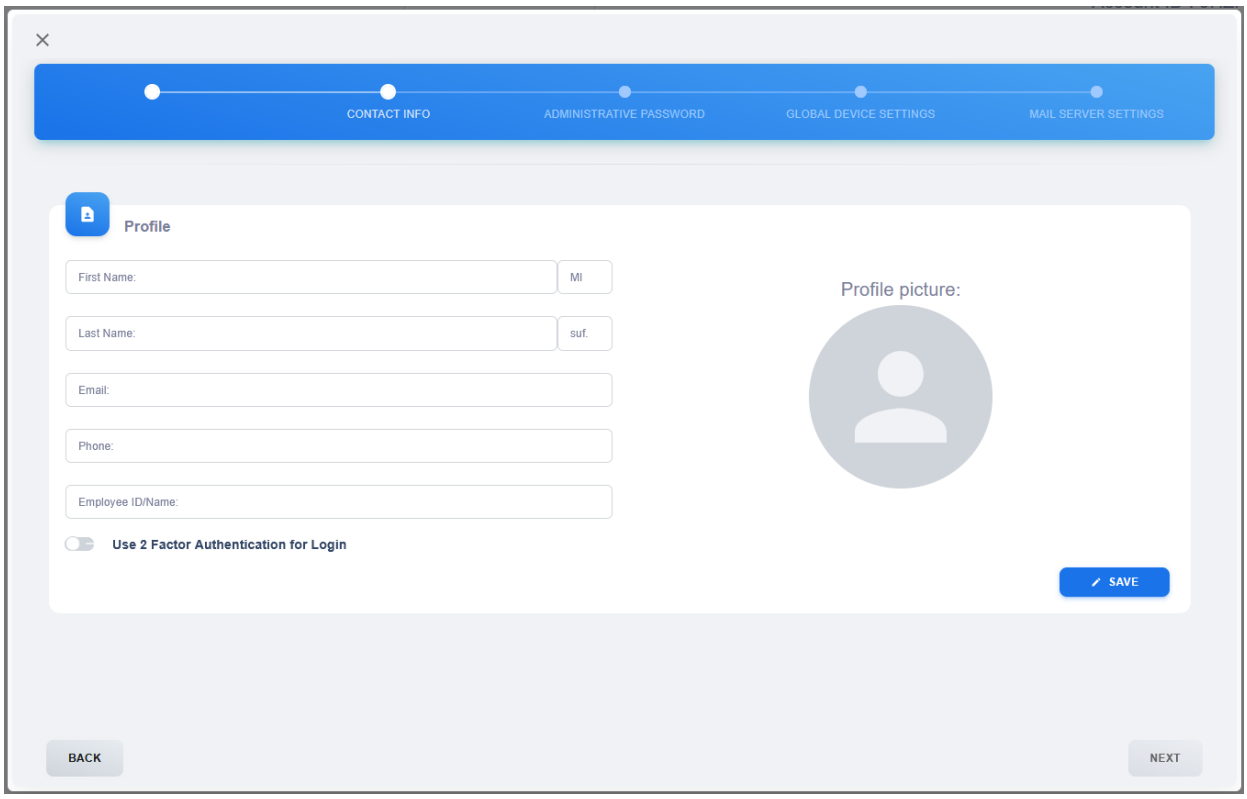
7. In the Password field, enter the default password krmc and select **Submit**.



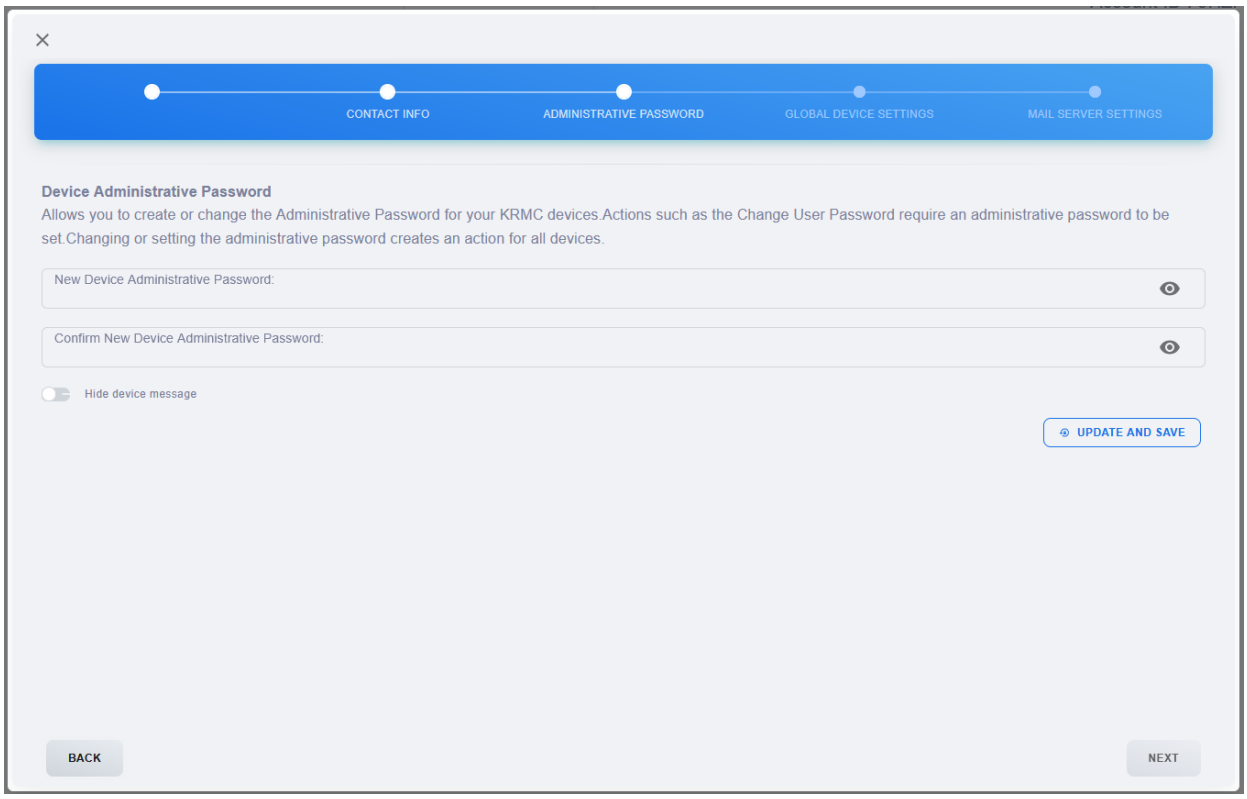
8. In selecting **Submit**, you will be greeted with the Welcome Screen. Click on the **BEGIN** button to proceed with initial setup and configuration. ***Note:*** *If at any point your click outside of the pop-up and the pop-up closes, it will re-open once you navigate to any page of KRMC.*



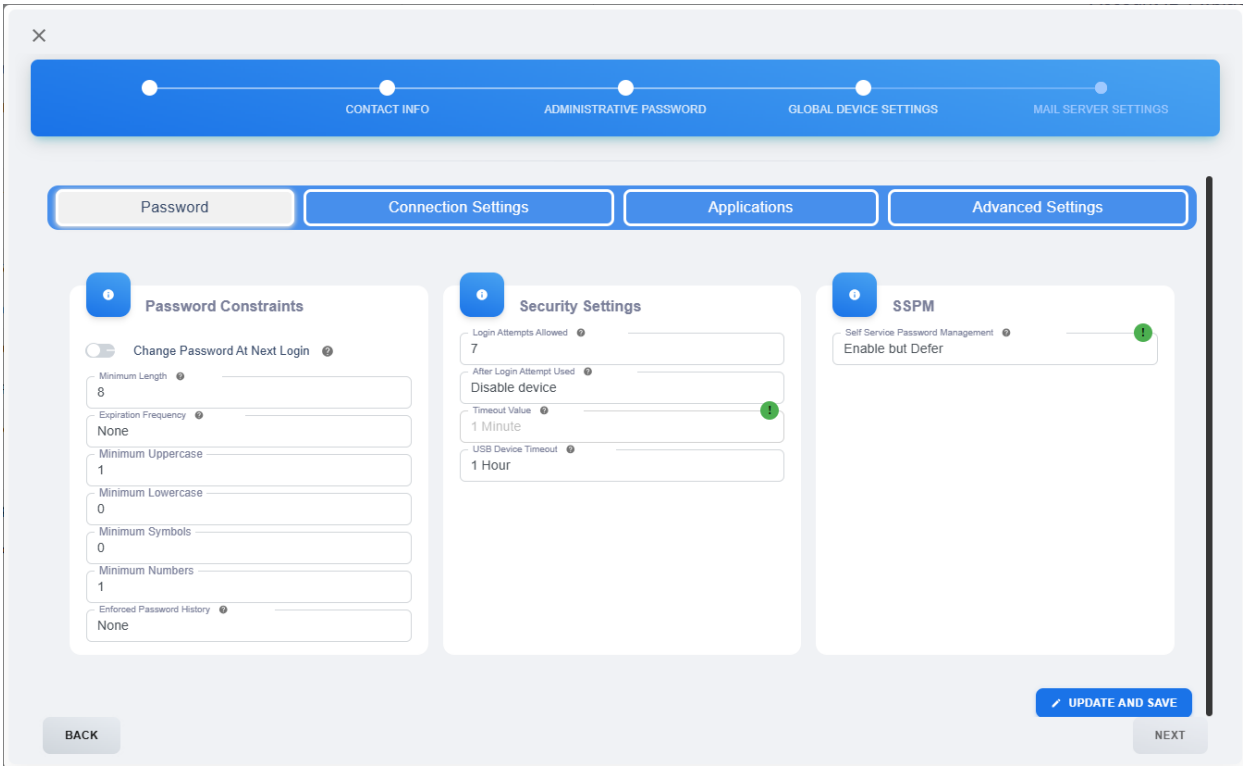
9. The first configuration page is Contact Info. This contact information is for the Super Administrator (SA) of your KRMC server. We only require the Email address field to be completed however do recommend completing the First Name and Last Name fields as well. The email address you enter will be the new SA login username.



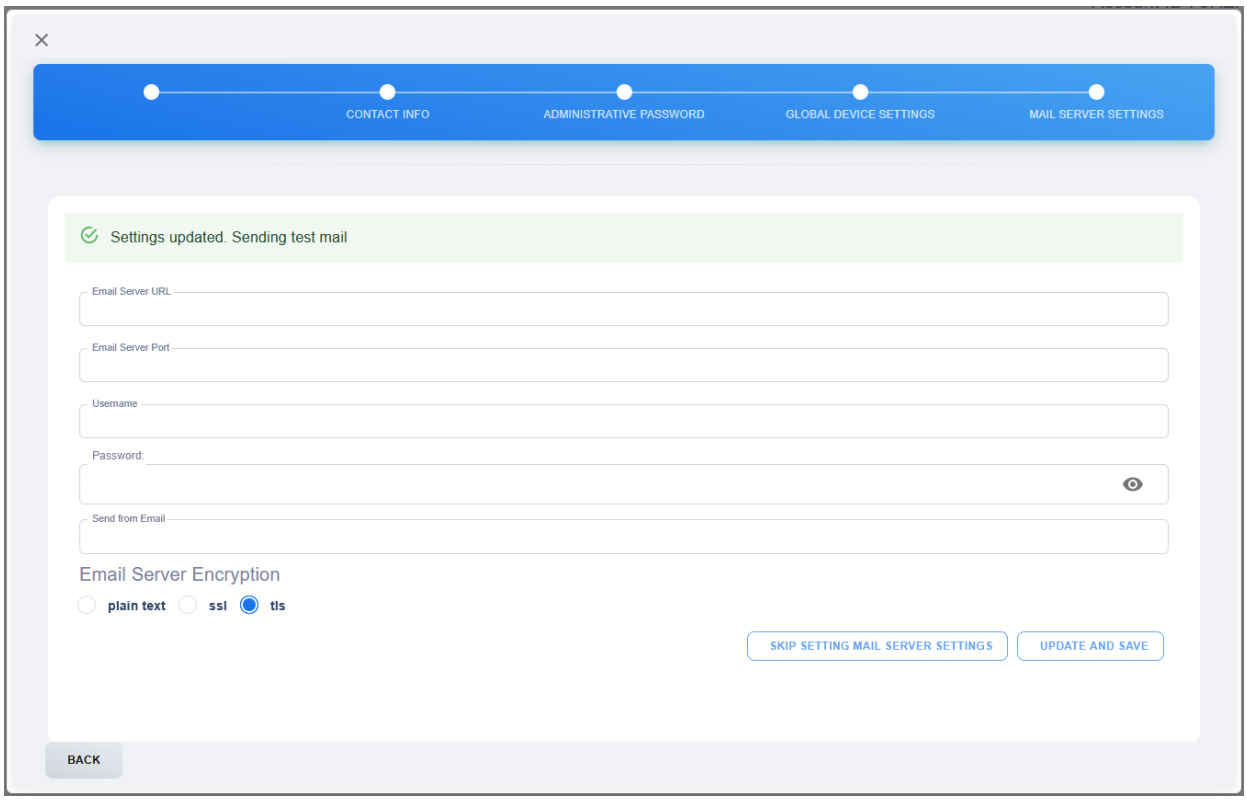
10. On the next screen you will be prompted to create an Administrative Password. The Administrative Password must conform to the default security parameters. Enter and then re-enter an Administrative Password and then click on the **Update and Save** button. The option "Hide Device Message" is disabled by default. If you enable this, no newly registered drive will receive a visible message stating that the device Administrative Password has been received.
***Note**: The password must be a minimum of 8 characters, with at least 1 upper case letter and 1 number.*



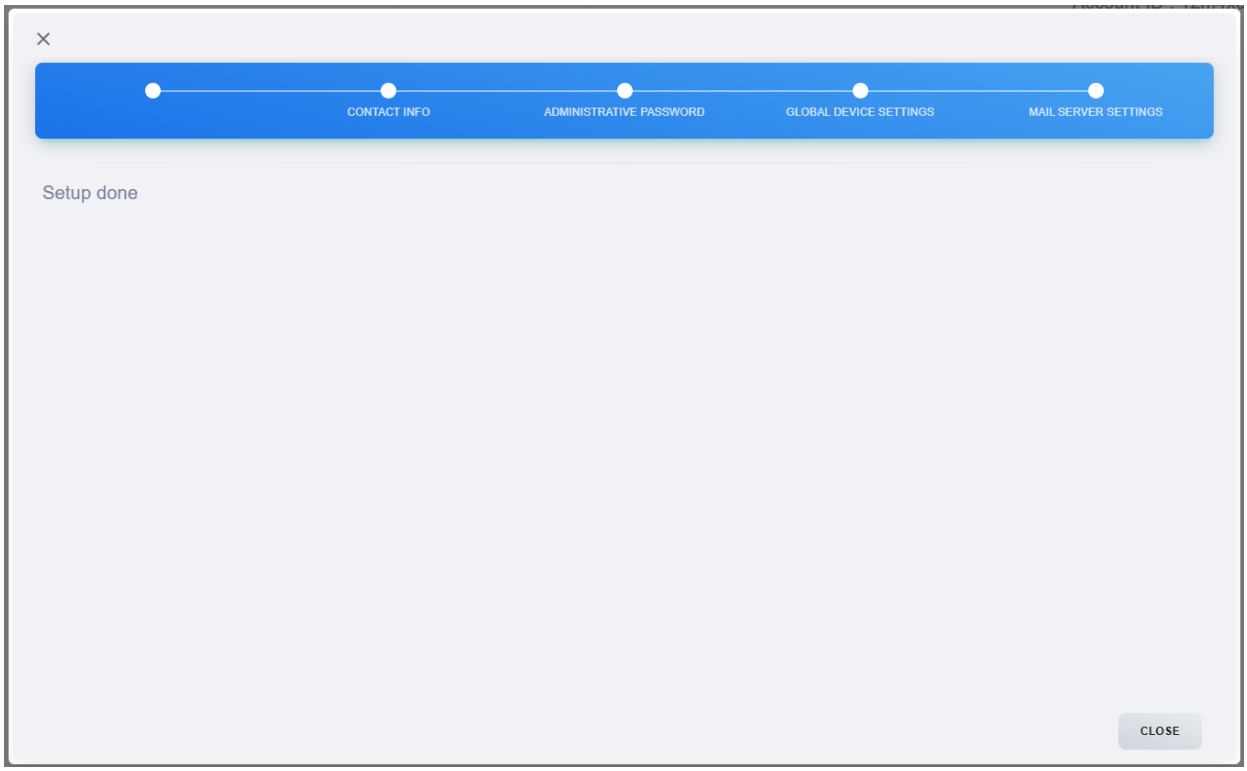
11. Next, you need to define a Global Device Settings and then click on the **Update and Save** button. All managed drives registered with KRMC On-Premise will be automatically configured with these security policy settings. The SA is able to alter this at a later point by navigating to Settings 170 and selecting Global Device Settings 171.



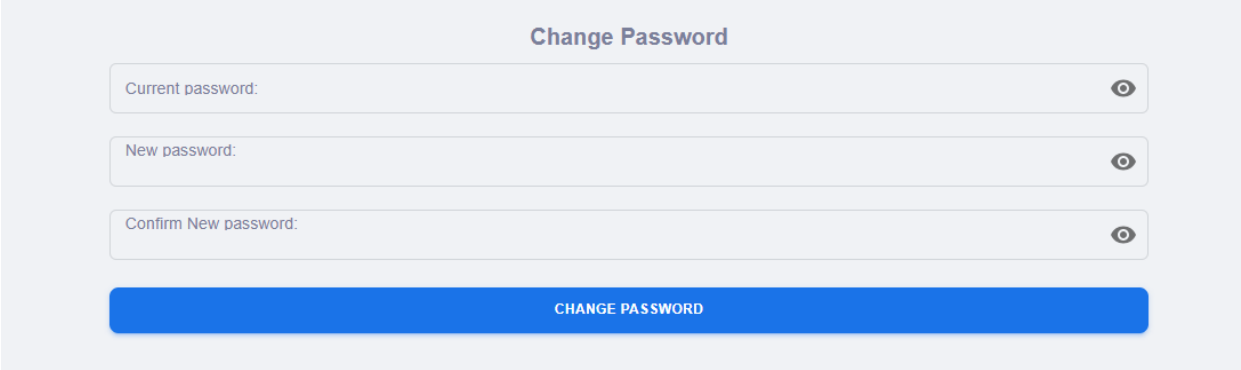
12. You will now need to configure **Mail Server** Settings if you would like. If configured, you are able to use feature such as Self-Service Password Management (SSPM), KRMC Forgot Password, and Two Factor Authentication (2FA). If you choose not to configure the email settings, you can select "**Skip Setting Mail Server Settings**". The SA is able to alter this at a later point by navigating to Settings 170 and selecting Mail Server 194. ***Note:*** *If configuring this, the server will attempt to send a test email using the credentials provided. If the server if unable to complete the request you can either skip to the time being or try again.*



13. Once the setup configuration is completed, you can select **Close**.



14. The last step in the configuration is to change the default password for the SA. The password must be a minimum of 8 characters, with at least 1 upper case letter and 1 number. In completing this step, the root user and default password are deactivated.



Congratulations! You have completed the setup of KRMC On-Premise and you are now able to start managing your encrypted devices.

Provisioning Drives to KRMC

4

KRMC On-Premise provides system administrators a secure platform for managing their fleet of Defender drives remotely. You MUST configure and register each of your Defender drives in order for them to communicate with your KRMC On-Premise server.

The steps to enable KRMC On-Premise functionality and to register your devices will vary depending on which method you use to configure KRMC On-Premise during the initial setup process:

- KRMC On-Premise configured using the On-Premise Provisioning Tool.
- KRMC On-Premise configured using Kanguru's Local Administrator tool (UKLA).

Important! *Both methods require network connection to your KRMC On-Premise server. The PC being used for drive provisioning MUST have a clear network connection to KRMC On-Premise server. If you are behind a firewall or connect to the internet through a proxy, you may experience connectivity issues which will lead to errors.*

Regardless of which method you are using, you will need your KRMC On-Premise server address in order to register your devices with your KRMC On-Premise server. You can locate this address on your KRMC On-Premise Virtual Machine.

Provisioning Drives to KRMC 4

On-Premise Provisioning Tool

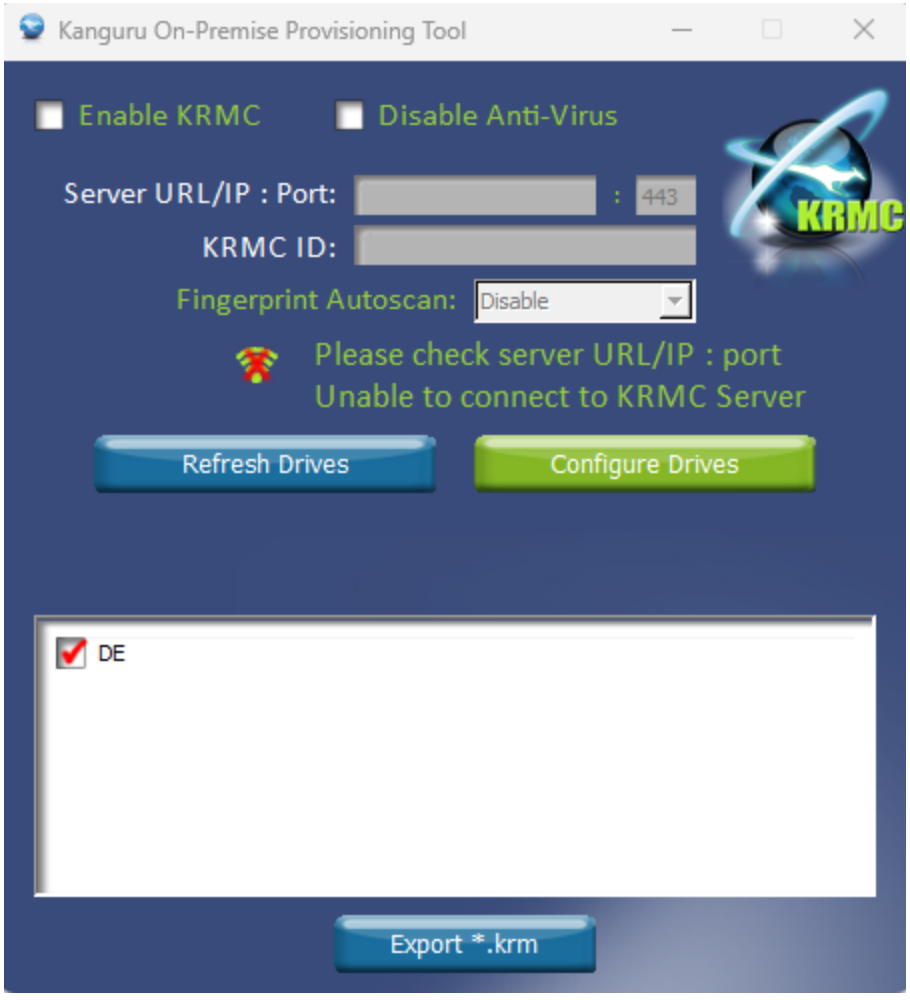
The On-Premise Provisioning Tool allows you to to enable KRMC On-Premise and/or to disable on-board endpoint protection. The On-Premise Provisioning Tool must be used to configure devices before they are provided to the end user for use.

The following drive models are supported by the On-Premise Provisioning Tool: Defender 3000, DefenderElite300, Defender Elite30, Defender BioElte30.

Note: *If KRMC On-Premise was previously disabled on the device through the Defender Manager Setup Wizard, you will need to reset the device before using it with the On-Premise Provisioning Tool.*

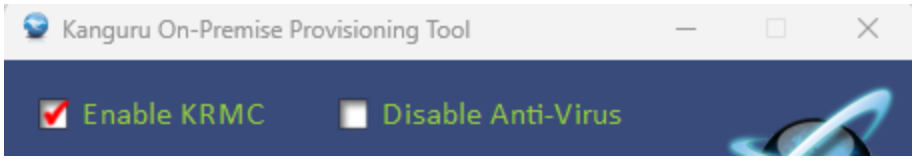
1. Connect your Defender devices to your computer and launch the On-Premise Provisioning Tool. Any connected Defender devices will appear with two drive letters in the bottom half of the window.

Note: *If no devices appear in the On-Premise Provisioning Tool window, make sure your drives are connected and then click on the refresh drives button.*

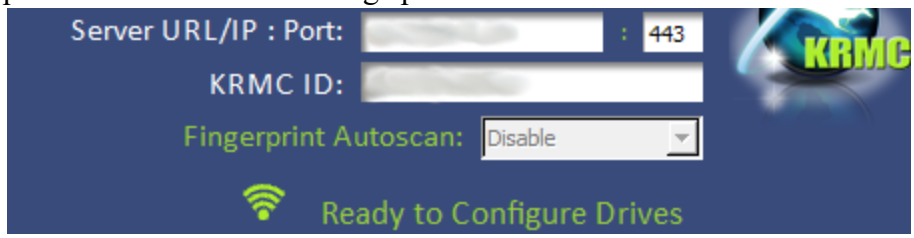


2. Select the checkbox next to “Enable KRMC”.

Note: *If you want to disable onboard Endpoint Protection, select "Disable Endpoint Protection".*



3. The fields for "Server URL/IP:Port" and "KRMC ID" become active. Fill in these fields with the appropriate information. If the device that you are provisioning is a BioElite30 model, then you have the option to Enable or Disable Fingerprint Autoscan.

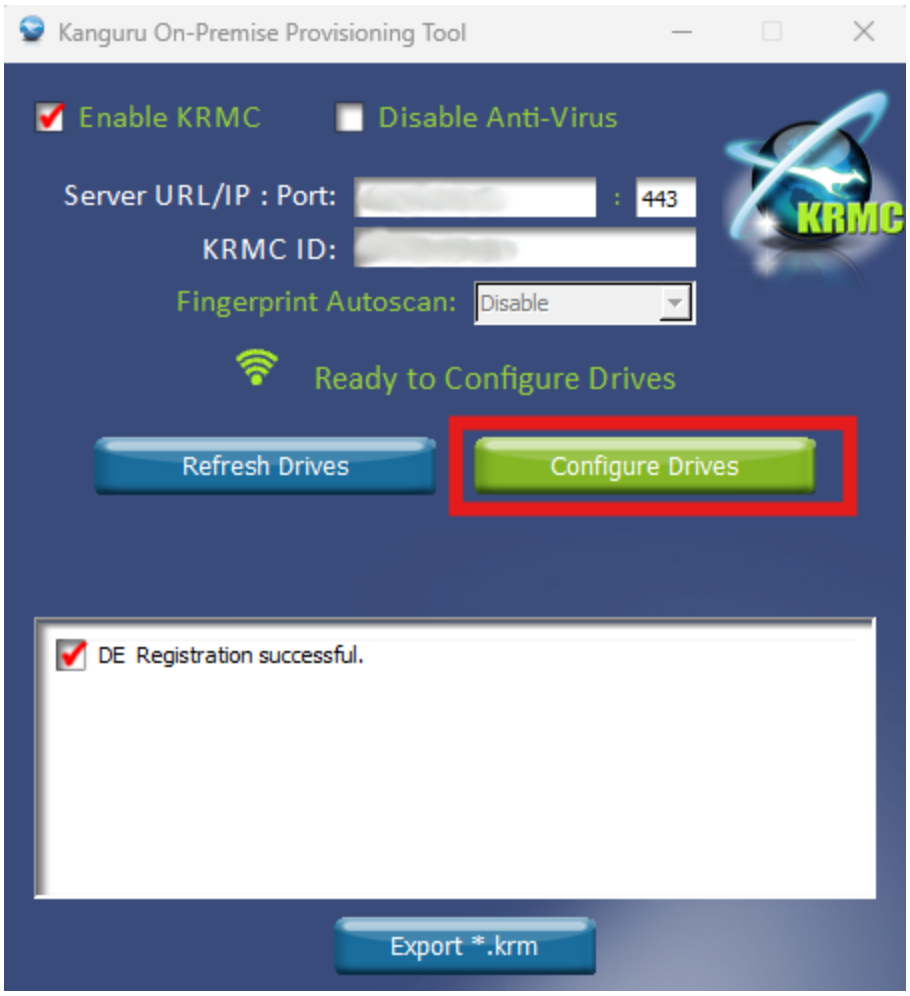


Server URL/IP : Port	This is the URL or IP address of the KRMC On-Premise server. The port cannot be changed and remains as 443.
KRMC ID	The KRMC ID (also known as Account ID) can be located at the top right hand corner of KRMC once you log into KRMC.
Fingerprint Autoscan	Disabled - The device user will be required to run KDMBio to access the secure storage partition. Since KDMBio is always needed in this configuration, the drive will only work on a supported PC or Mac. This is typically recommended for devices being managed by KRMC On-Premise.
	Enabled - The device user will be able to access the drive's secure partition using only their fingerprint. They will not need to run KDM in this configuration and their BioElite30 device will run on any OS.

4. Click on the Configure drives button. If everything is configured correctly then you will receive a message stating, "Register succeeded."

Provisioning Drives to KRMC

4



KRMC On-Premise has now been enabled on the device and the device has been registered with your KRMC On-Premise account.

If you would like to keep a record of the drives that you have imported, you can use the option Export *.krm. This would be useful if you need to manually import a drive(s) back into your KRMC server. The .KRM file contains the following information:

- Device Name
- Device Administrator
- Administrator Contact Information
- Employee ID/Name
- Additional device info

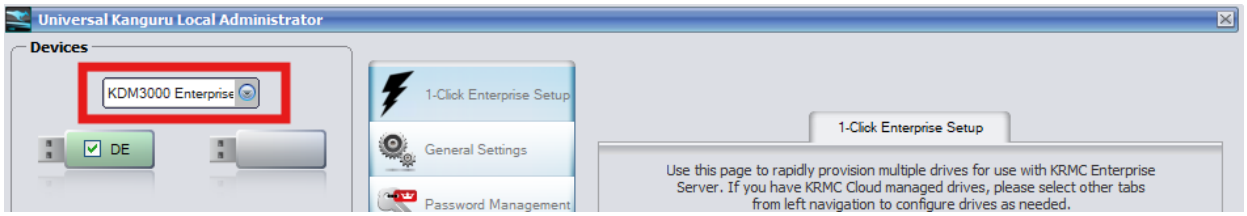
Provisioning Drives to KRMC

4

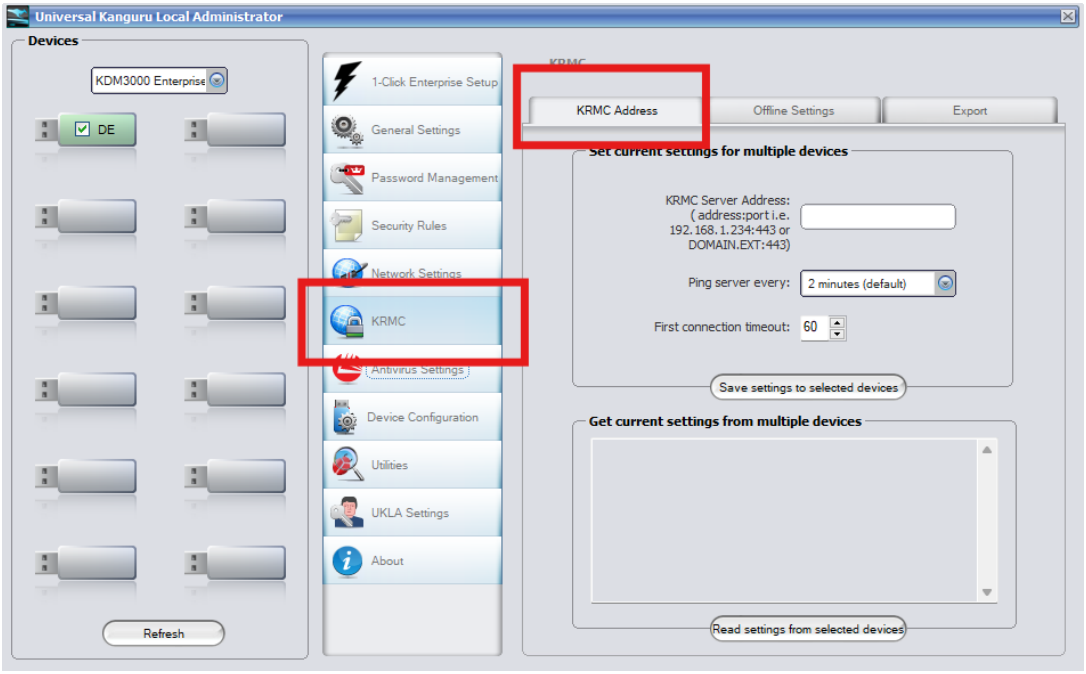
Devices Configured Using UKLA

This section only applies if your are looking to register your drives to KRMC On-Premise using the Universal Kanguru Local Administrator (UKLA) application.

1. Connect your devices to your computer and launch UKLA. ***Note:*** *All connected Defender devices should be the same model (e.g., Elite30, Elite300, 3000). Although UKLA is capable of configuring multiple devices simultaneously, it is unable to configure more than one model type at a time. For example, it is possible to configure five Defender Elite 300s and then configure five Defender 3000s afterwards, but you cannot configure five Defender Elite 300s and five Defender 3000s at the same time.*
2. Once you have logged into UKLA, select the device model type from drop-down menu located at the top of the Device Grid. ***Note:*** *Make sure you select the "Enterprise/On-Premise" version, and not "Cloud/Hosted".*



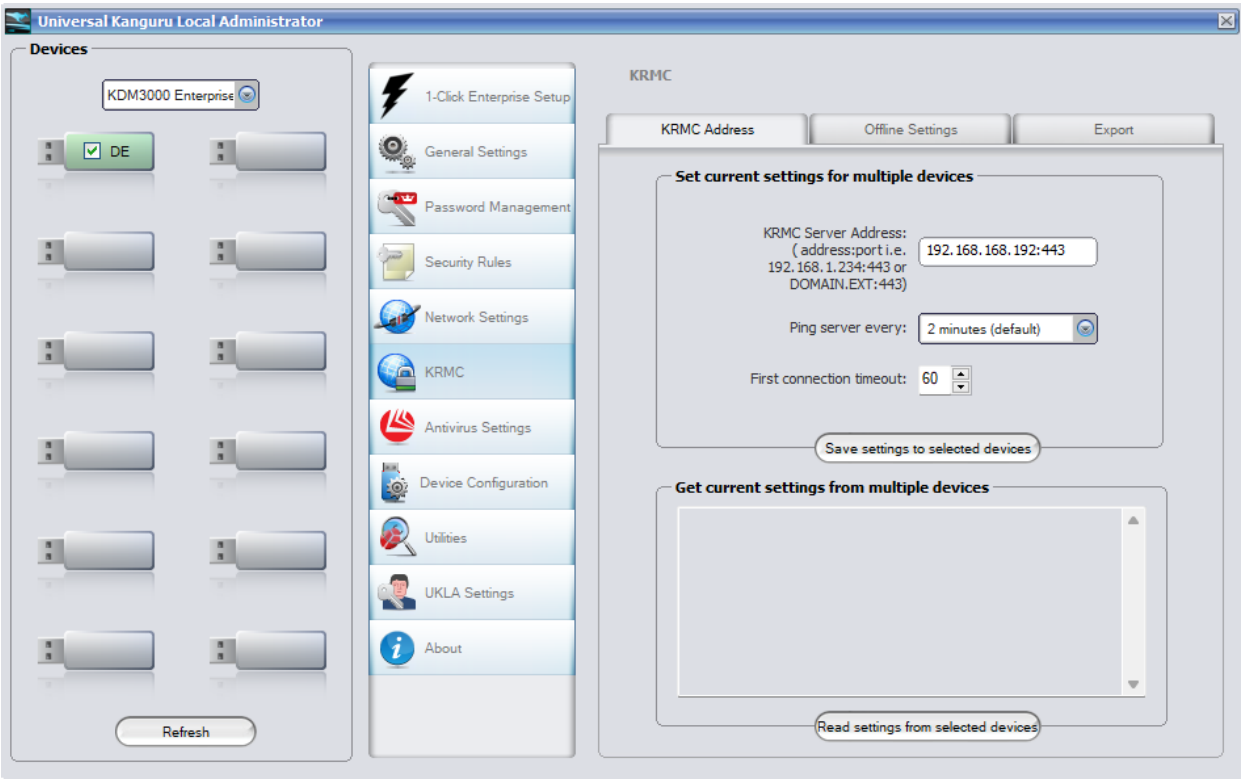
3. Click on **KRMC** in the navigation menu on the left and verify you are on the **KRMC Address** tab.



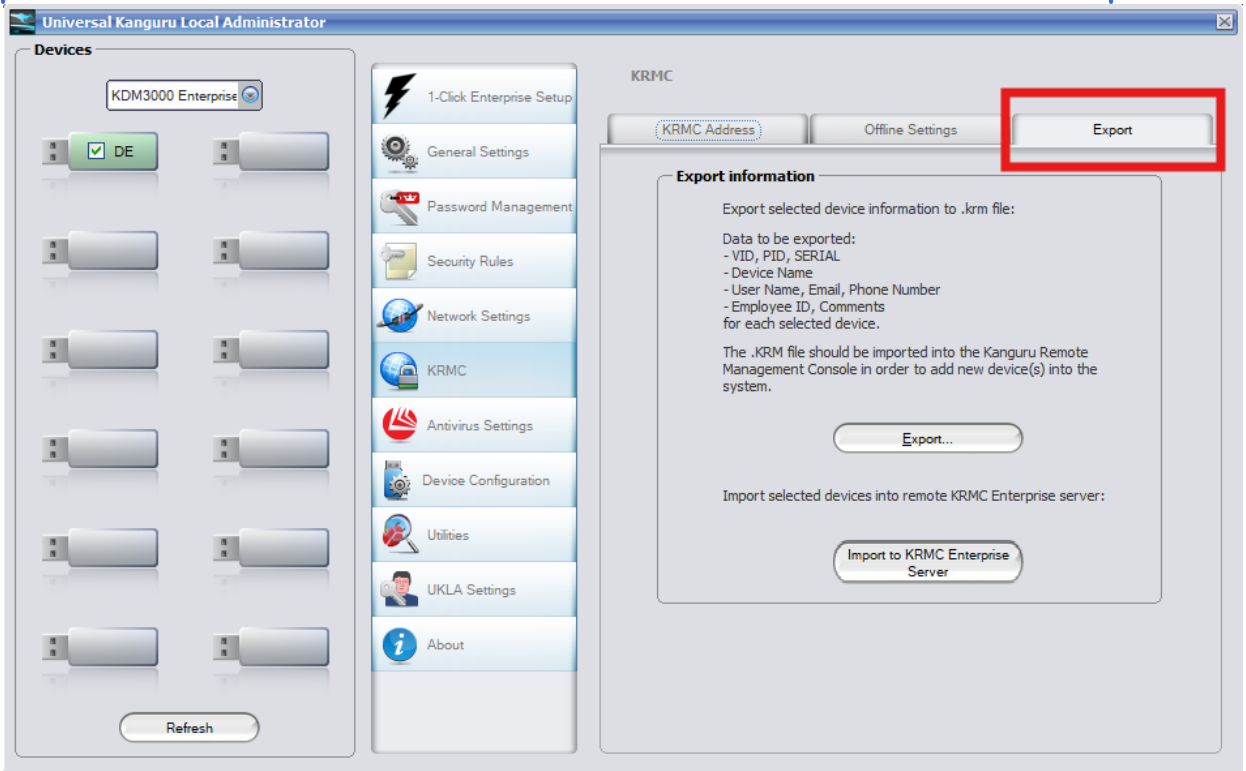
4. Complete the fields provided and once completed, select **Save Settings to Selected Devices**.

KRMC Server Address	The server address must be entered in one of the following formats: IP:Port or Hostname:Port

	IP:Port - Enter the IP address of the server that KRMC was installed on, and then the server-specified port that allows the device to communicate with the KRMC server (e.g. 192.168.1.1:443)
	Hostname:Port - Enter the domain name, and then the server-specified port that allows the device to communicate with the KRMC server (e.g. kanguru.com:443)
Ping server every	The ping time is how often the device will attempt to communicate with the server and receive new commands. A device configured to ping the server every "time KDM starts" will only check the server for new commands when the user logs into the device. The default and recommended time period if 2 minutes.
First connection timeout	When a device user logs into their device, the device will automatically attempt to connect to the KRMC server. If the KRMC server is unavailable, the device will continuously attempt to connect to the KRMC server for the time specified here. Once the specified time expires, KDM will start and the device will operate in offline mode.



5. After the settings have been saved, you can not import the drive(s) into your KRMC On-Premise server. Navigate to the **Export** tab. You will be presented with two options: Export and Import to KRMC On-Premise/Enterprise Server.



6. Using Export option:

After you have finished configuring your device(s), you can export the device information to a .KRM (Kanguru Resource Management) file.

The .KRM file contains the following information:

- Device Name
- Device Administrator
- Administrator Contact Information
- Employee ID/Name
- Additional device info

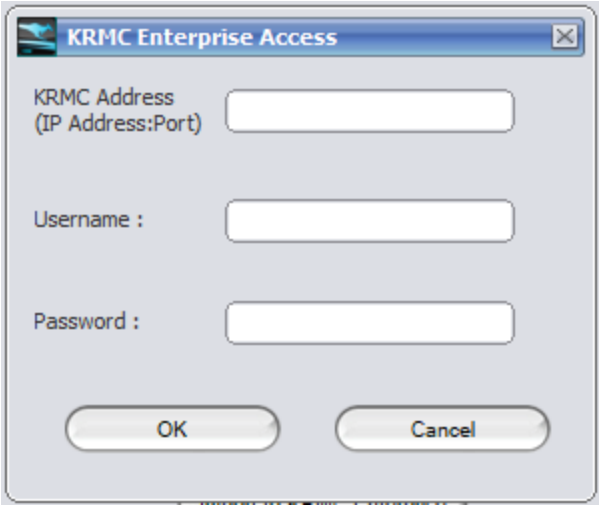
The .KRM file will be imported to KRMC by a KRMC Super Administrator to register the devices with the system.

To export device information:

i. Select the devices you want to export from the Device Grid.
ii. Click on the Export button.
iii. Select a filename and a destination where you want to save the file to.
iv. Click on the save button.

7. Using Import to KRMC On-Premise/Enterprise Server option:
   Instead of exporting your devices to a .KRM file and then manually importing the .KRM file through KRMC, you can instantly import your devices directly to your KRMC Enterprise server from KLA. This facilitates the entire device import process.
   To import the device information directly to the KRMC Enterprise server:
   i. Select the devices you want to export from the Device Grid.
   ii. Click on the Import to KRMC On-Premise/Enterprise server button.

   iii. The KRMC Enterprise Access window appears.



iv. Enter the information required for your KRMC On-Premise server. The Username and Password must be KRMC Super Admin login credentials.
v. Click on the OK button to import your selected devices to KRMC On-Premise.

Your devices have now been configured and registered for use with your KRMC On-Premise account. Repeat these instructions for each Defender model type in your possession, until all devices have been registered with your KRMC On-Premise account.

Getting to Know KRMC On-Prem 5

KRMC On-Premise is a web-based Software as a Service (SaaS) application that provides administrative tools in a single, centrally managed console. It allows you to manage, monitor, and provision your USB devices. Its intuitive design simplifies the workflow for an administrator, making it easy to take advantage of the array of tools and available options. There are a large amount of options, settings, and features to KRMC so here are some basic items to get started with:

Logging into KRMC with SAML 43	KRMC Advanced and Premium accounts have the ability to utilize SAML for logging into KRMC. If utilizing this feature, you can follow these steps to show how that process will work.
Two Factor Authentication 44	Security is always a top priority and as such we recommend utilizing Two Factor Authentication. We currently provide steps for how to utilize 2FA with Email or Google Authenticator.
Navigation Menu 52	This is a breakdown of the navigation options available on KRMC.
Account Activity Icons 54	Every account as access to activity icons granting access to different features. Some of these include changing account password, logging out of KRMC, customizing the dashboard.
Admins, Auditors, and Groups 62	A breakdown of the different types of accounts that are available on KRMC and how to create them.
License Assignment 68	A base description on how licenses are assigned and how to manually assign licenses.

Logging into KRMC Hosted with SAML

Active Directory (AD) based Single Sign On (SSO) using Security Assertion Markup Language(SAML) provides KRMC On-Premise administrators an alternative sign-on option for login. If setup for the account, an administrator wishing to login to KRMC On-Premise will be redirected to the SSO URL for authentication using their own SAML supported AD service. Once the administrator authenticates into their AD service, they will be redirected back to KRMC On-Premise in a 'logged-in' state, where they can continue to use KRMC On-Premise features as usual.

Benefits of using AD based login:

- Productivity savings for administrators – no additional passwords to remember for KRMC On-Premise. The KRMC On-Premise login now ties seamlessly with SSO.
- Administrators are authenticated using the company's trusted internal AD services, enabling higher customer trust in the KRMC On-Premise ecosystem overall.
- Near instant privilege revocation in case a KRMC On-Premise Administrator is terminated as an employee. KRMC On-Premise will refresh the account state with the customer's AD server every 30 minutes.

SAML in KRMC On-Premise is located on the Settings 170 page under the section Server Settings 182.

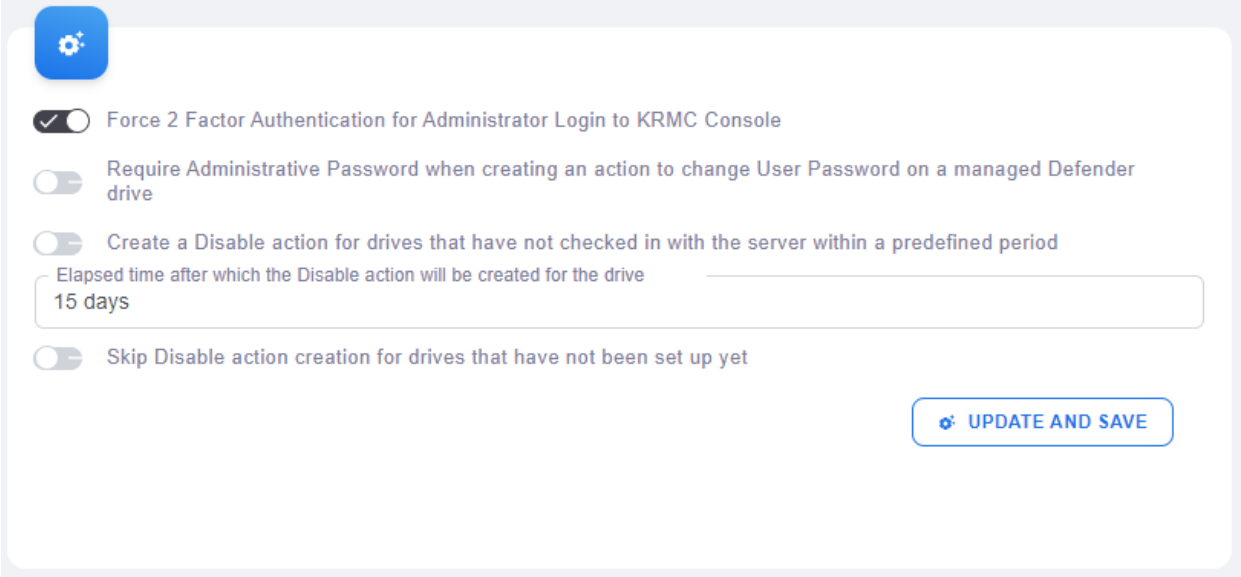
Two Factor Authentication

Two Factor Authentication (2FA) is a feature that extends an additional layer of security which prevents unauthorized administrators and auditors from logging into KRMC On-Premise. At this time KRMC On-Premise supports 2FA in forms of email and Google Authenticator. ***Note:** 2FA using email is only available if you have configured* Mail Server 194.

2FA can be enabled on all KRMC On-Premise accounts or individual ones based on your preferences.

For steps on how to enable 2FA email for individual accounts, please click HERE 47.
For steps on how to enable 2FA Google Authenticator for individual accounts, please click HERE 49.

- To force 2FA for all administrators on your account you will need to navigate to Settings 170 and selecting Administrative Settings 181 and enable "Force 2 Factor Authentication for Administrator Login to KRMC On-Premise Console" and select the **Update and SAVE** button.



- You will receive an email with a verification code that will need to be entered into the designated field on KRMC On-Premise.

Hello [redacted],

Please use code **324144** to verify that Two-Factor Authentication will work well for you. This code will expire in 30 minutes.

Using two factor authentication protects your users by preventing unauthorized logins into your KRMC account. Thank you for doing your bit in keeping KRMC secure.

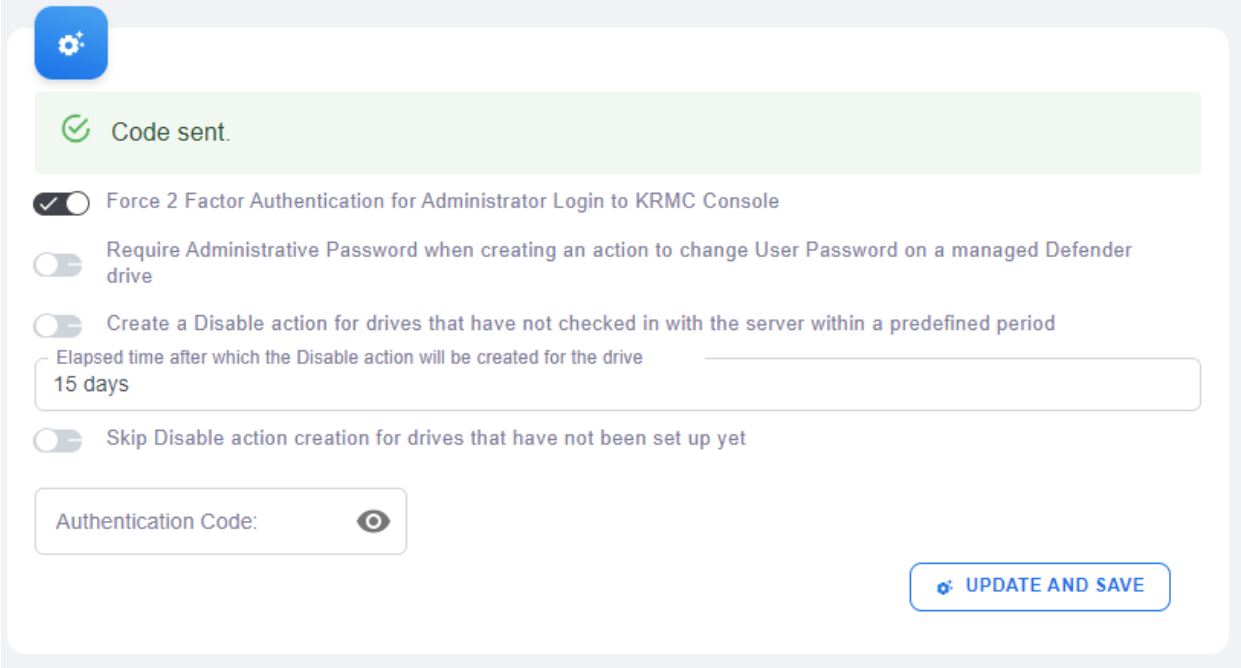
Warm Regards,
Team Kanguru.

Kanguru Solutions
1360 Main Street
Millis, MA 02054

1-888-KANGURU
www.kanguru.com

KANGURU™
Secure. Anytime. Anywhere.

- After the code has been entered, select the **VERIFY** button. You will know that the 2FA setup has been completed as you will receive a message on KRMC On-Premise stating "Administrative Settings Updates" and the Authentication Code field will be blank.



- You will then receive an email stating that 2FA has been enabled on your account.

Hello [redacted]

This is just a courtesy notification that the Super Administrator for your KRMC account [redacted] has activated Two-Factor authentication for your KRMC account. You will now receive on this email address a time limited code for logging into KRMC each time you log in.

Sincerely,
Your Kanguru Support Team.

Kanguru Solutions
1360 Main Street
Millis, MA 02054

1-888-KANGURU
www.kanguru.com

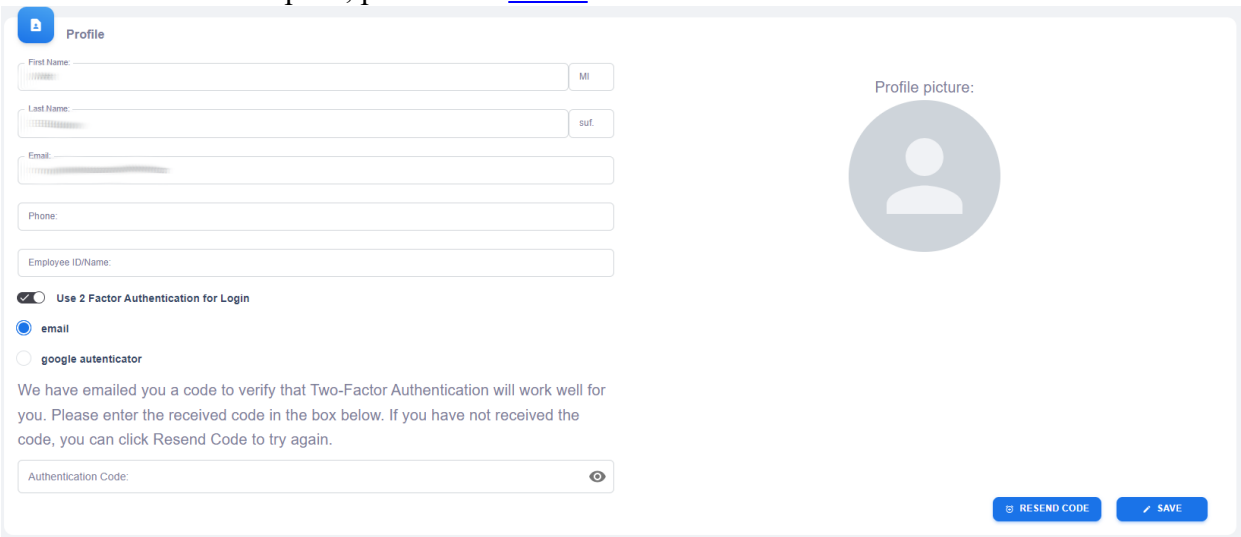
KANGURU™
Secure. Anytime. Anywhere.

For logging into KRMC On-Premise when 2FA is enable, please click HERE[50].

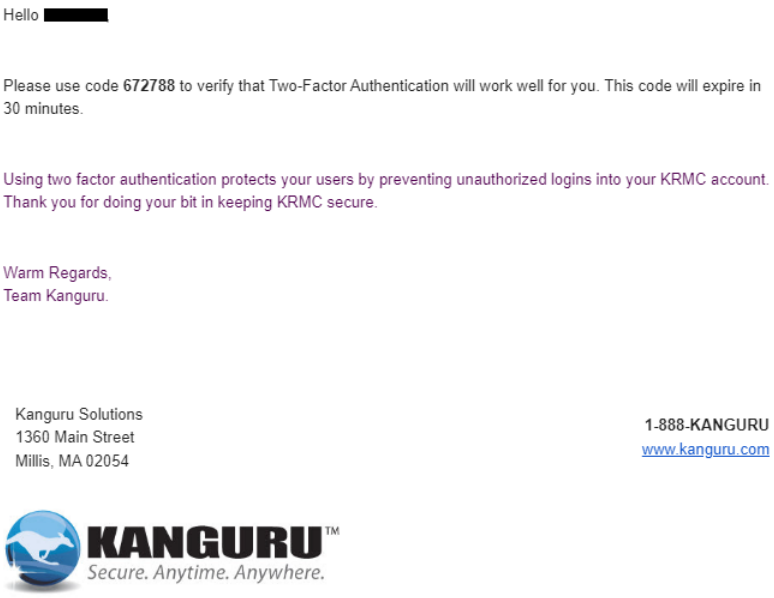
Enable 2FA EMail

Enabling Two Factor Authentication (2FA) for the email authentication method can be performed on the currently logged in account, Super Administrator (SA), or Regular Administrator (RA) if the RA has the permissions "Can Create and Edit Administrators" and "Can Create and Edit Auditors" located under Edit Admin Information 145. ***Note:*** *2FA using email is only available if you have configured* *Mail Server* 194.

1. Once logged into KRMC On-Premise, you will need to navigate to Edit Profile which is located at the top right of the screen under the Account Icon.
2. Make sure the option "Use 2 Factor Authentication for Login" is selected, then select email. ***Note****: If 2FA is being forced on all KRMC On-Premise accounts, you will be unable to disable this option but you can switch the option between Email and Google Authenticator.* For more information on this option, please click HERE 44.



3. You will receive an email with a verification code that will need to be entered into the designated field on KRMC On-Premise.



Hello [redacted]

Please use code **672788** to verify that Two-Factor Authentication will work well for you. This code will expire in 30 minutes.

Using two factor authentication protects your users by preventing unauthorized logins into your KRMC account. Thank you for doing your bit in keeping KRMC secure.

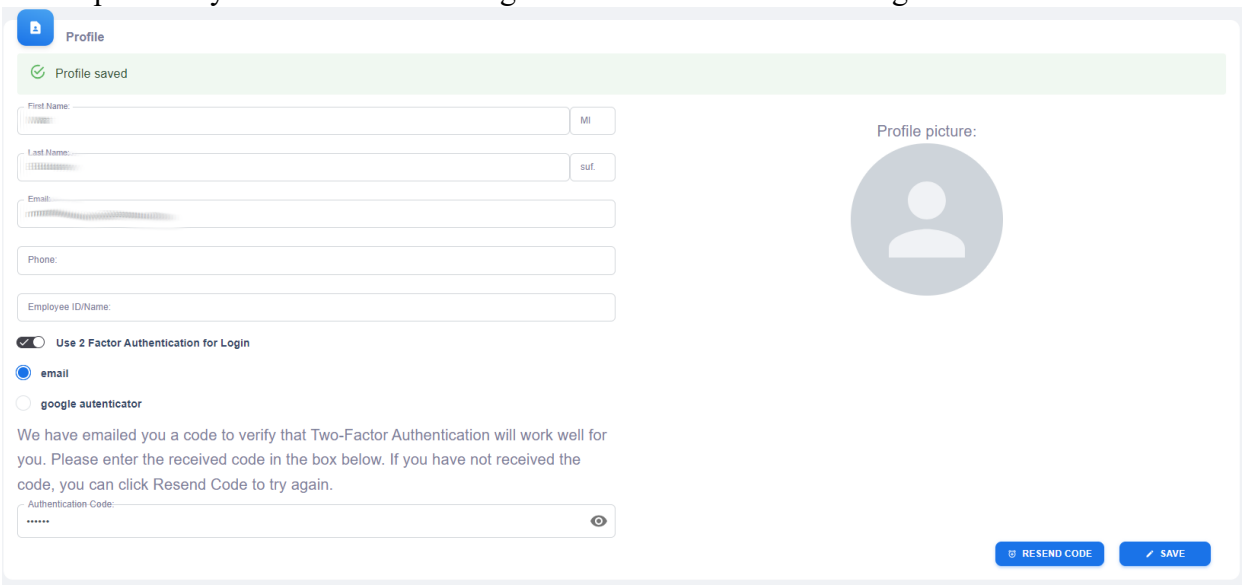
Warm Regards,
Team Kanguru.

Kanguru Solutions
1360 Main Street
Millis, MA 02054

1-888-KANGURU
www.kanguru.com

KANGURU™
Secure. Anytime. Anywhere.

4. After entering the code, click on the **SAVE** button.You will know that the 2FA setup has been completed as you will receive a message on KRMC On-Premise stating "Profile Saved".

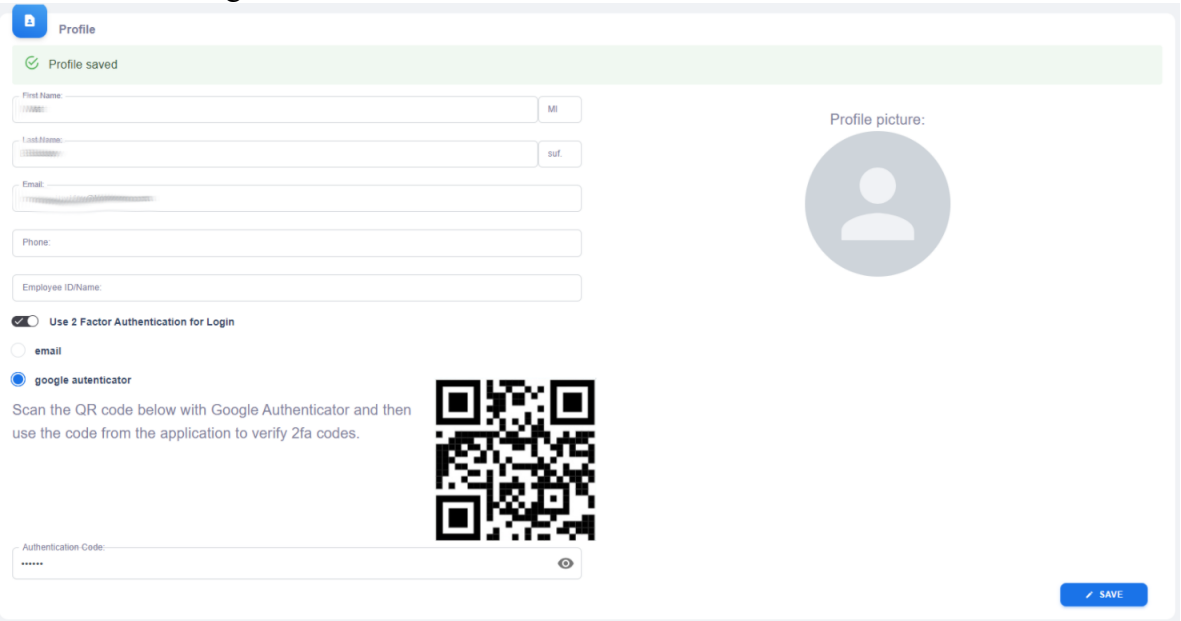


For logging into KRMC On-Premise when 2FA is enable, please click HERE 50.

Enable 2FA Google Authenticator

Enabling Two Factor Authentication (2FA) for the Google Authenticator can only be performed on the currently logged in account.

1. Once logged into KRMC On-Premise, you will need to navigate to Edit Profile which is located at the top right of the screen under the Account Icon.
2. Make sure the option "Use 2 Factor Authentication for Login" is selected, then select Google Authenticator, and press the **SAVE** button. ***Note**: If 2FA is being forced on all KRMC On-Premise accounts, you will be unable to disable this option but you can switch the option between Email and Google Authenticator.* For more information on this option, please click HERE 44.
3. You will need to open your Google Authenticator Application on your Smart Device to scan the QR code presented to you. and enter the code provided. After entering the code, click on the **SAVE** button.
4. You will know that the 2FA setup has been completed as you will receive a message on KRMC On-Premise stating "Profile Saved".



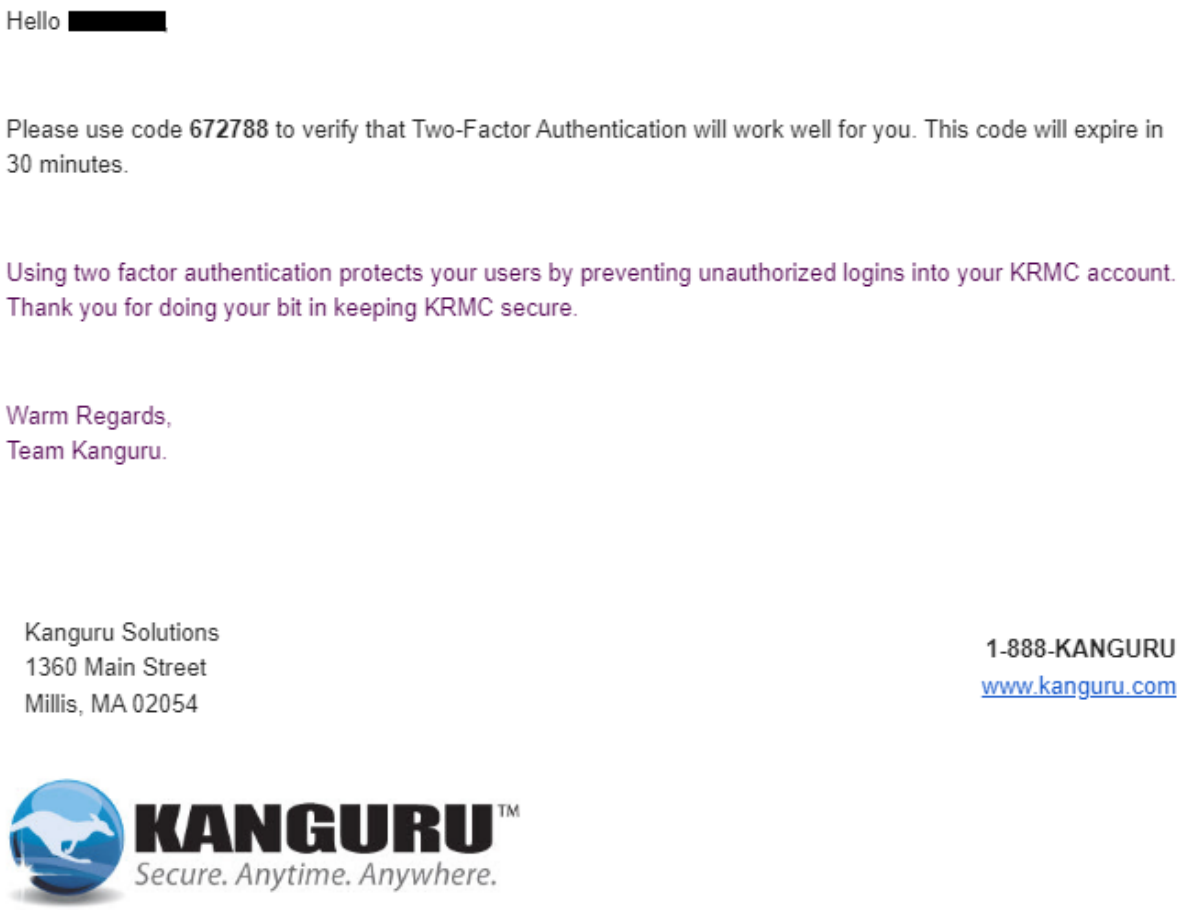
For logging into KRMC On-Premise when 2FA is enable, please click HERE 50.

Logging in with Two Factor Authentication

Two factor authentication (2FA) is a feature that extends an additional layer of security which prevents unauthorized users from logging into KRMC On-Premise. At this time KRMC On-Premise supports 2FA in forms of email and Google Authenticator. For more information on 2FA, please click HERE 44.

When 2FA has been enabled, after signing into KRMC On-Premise with your password (or sign in with SAML), you are directed to an authentication page based on the method of 2FA selected for that account.

If utilizing the email form of 2FA, an authentication code is automatically generated and sent by email to the administrator. ***Note:*** *2FA using email is only available if you have configured* *Mail Server* 194.



Hello [redacted]

Please use code **672788** to verify that Two-Factor Authentication will work well for you. This code will expire in 30 minutes.

Using two factor authentication protects your users by preventing unauthorized logins into your KRMC account. Thank you for doing your bit in keeping KRMC secure.

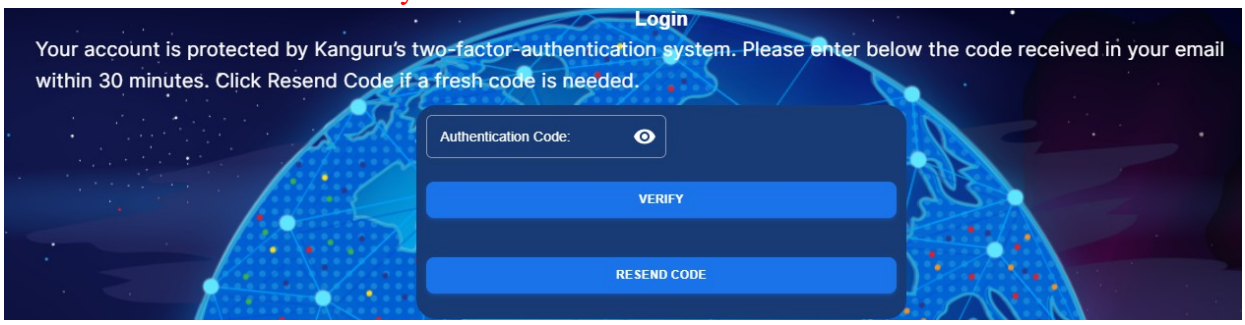
Warm Regards,
Team Kanguru.

Kanguru Solutions
1360 Main Street
Millis, MA 02054

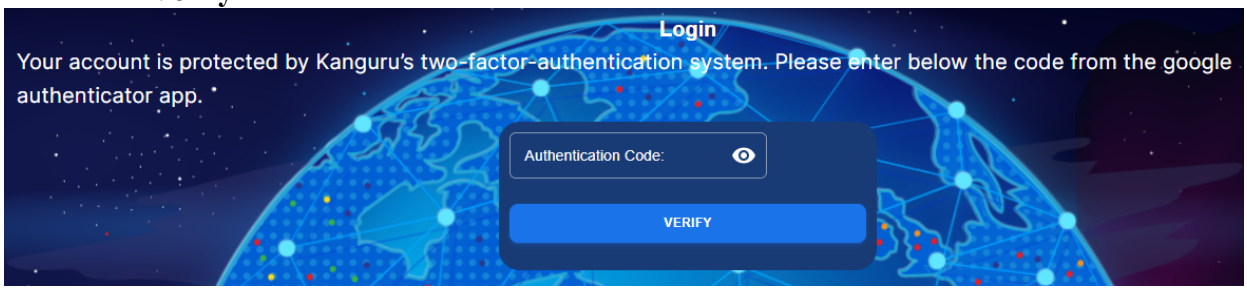
1-888-KANGURU
www.kanguru.com

KANGURU™
Secure. Anytime. Anywhere.

The administrator must copy the authentication code from the email into the 'Authentication Code' field and then click on the **Verify** button. **Note:** Authentication codes are only valid for 30 minutes after they have been generated. If your code has expired, then click the Resend Code button and a fresh authentication code will be sent by email.



If you are utilizing the Google Authenticator form of 2FA, you will need to open your Google Authenticator Application on your Smart Device and enter the code provided. After entering the code, click on the **Verify** button.



Once the authentication code has been validated, the administrator will be logged into the web console.

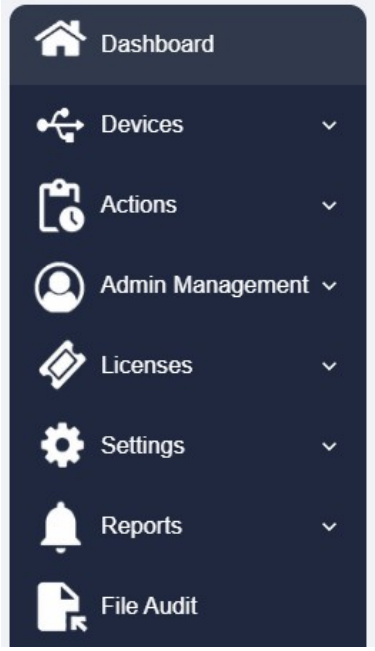
Getting to Know KRMC On-Prem 5

Navigation Menu

The **Navigation Menu** is located on the left-side of every page. Initially, the Navigation Menu only displays icons. When you hover your mouse over the area, the menu will expand revealing the full context. This can change to always show the expanded navigation menu by selecting the an option in either Account Settings 60 or Server Settings 182,

There is a total of eight main pages in KRMC On-Premise that are accessible through the Navigation Menu on the left. These main pages are listed and detailed below. Each main page listed also has series of sub-pages to assist in navigating to the page you are looking to access. The first sub-page is the page that you will be brought to when you select the main page.

Dashboard 114	An account overview which provides access to account information and a series of charts and lists.
Devices 117	A list of devices that are registered to this account. You can manage devices, create remote actions, and update security settings.
Actions 138	A list of pending, successful, and failed actions that occurred on devices. You can also create global actions from this page.
Admin Management 143	A list of current admins, auditors, and groups. You can add additional accounts and groups on this page, as well as modify existing permissions or settings.
Licenses 164	A quick snapshot of your licenses' status. Your order history is also listed here.
Settings 170	Configure a global device settings, administrative settings, and server settings.
Reports 201	Event and usage reports along with messages sent to the account.
File Auditing 204	Data is sent to KRMC containing file actions that occur such as Deletion, Creation, Read, and Write for files stored on your drive(s).


Dashboard
Devices
Actions
Admin Management
Licenses
Settings
Reports
File Audit

Account Activity Icons

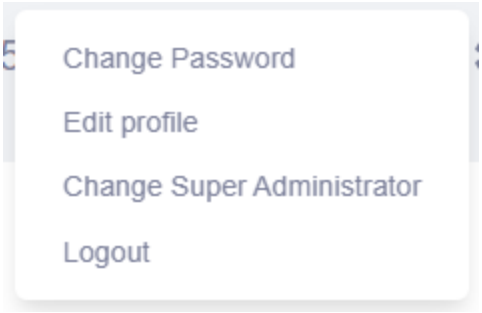
Located at the top right of every page on KRMC are the Account Activity Icons. These icons provide you access to specific features and functions regardless of the page you are on for ease of use. One of the key items is the Account ID. As this ID is required to register any device to your account, you will now be able to easily locate and copy it. Here is a full list of the icons that are available for you.

Account ID	The account-level Account ID used to register devices to this account.
Account Notifications	All events that occur on the account appear within Account Notifications. You will be informed of a new event occurring with a number inside a red notification bubble next to the icon. A full list of the events can be located on the Events 202 page located under Reports 201.
Account Messages	These are messages to the account. Commonly regarding news about products, important updates to KRMC, and more. You will be informed of a new messages with a number inside a red notification bubble next to the icon. A full list of the messages can be located on the Message 203 page located under Reports 201.
Account Icon 55	Access account information such as editing your profile, changing your password, and logging out of KRMC.
Account Settings 60	The theme of the server can be changed, you can auto-hide or show the navigation menu, and edit the dashboard.

Account Icon

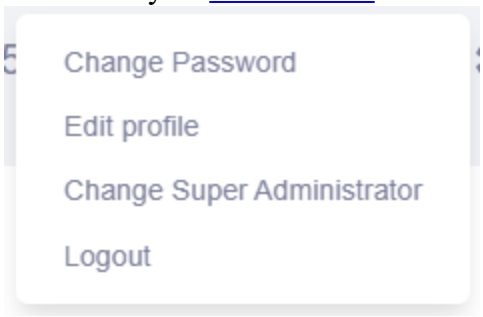
The **Account Icon** provides access to many features for ease of use and convenience as well as personalize your account slightly.

Change Password 56	Within this menu you are required to enter your current password, then you are free to change your password.
Edit Profile 57	Items such as name, email, and phone number are able to be entered or added. Additionally, you can add in a profile image and alter your two factor authentication settings.
Change Super Administrator 58	This is available for the Super Administrator (SA) account only. This setting allows you as the SA to move the SA permissions to a different account.
Logout 59	This logs you out of the KRMC account.

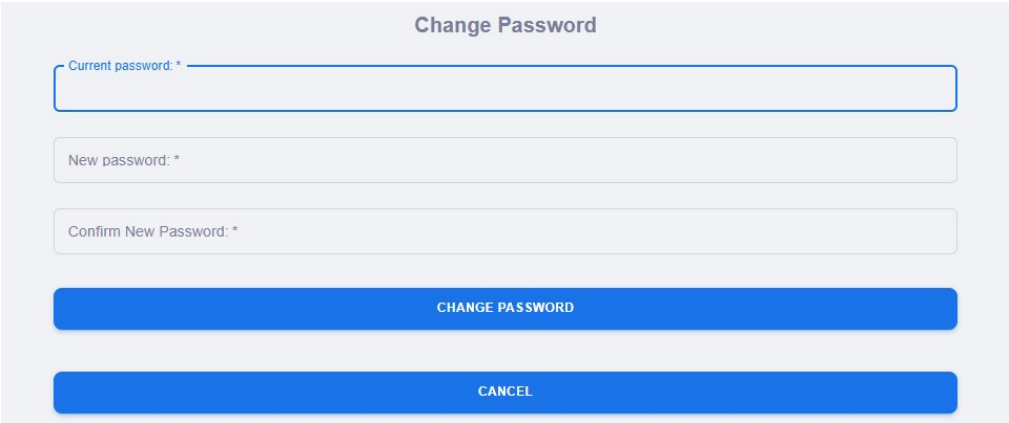


Change Password

Your account password is a vital part of KRMC as without it, you are not able to gain access to the service. If for any reason you need to change your password after you log into KRMC, you can be selecting **Change Password** located under your Account Icon 55.

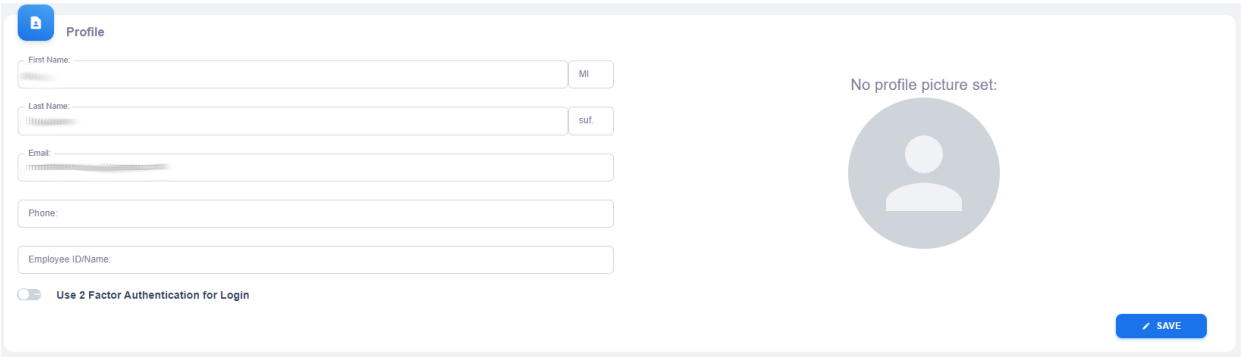


This will redirect you to the Change Password page. Enter the required password information and then click the **Change password** button. After changing your password, you will be brought back to the page you were previously on and you will need to enter the new password when you next attempt to log into KRMC.



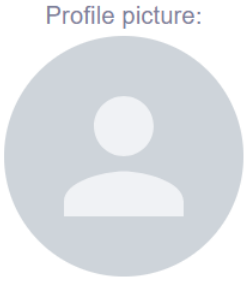
Edit Profile

Edit Profile provides the ability to customize your Admin or Auditor account on KRMC. Using this menu you are able to change/insert Name, Email, Phone, or Employee ID/Name information as you see fit. Any changes that are made will not be saved until you select the **SAVE** button.

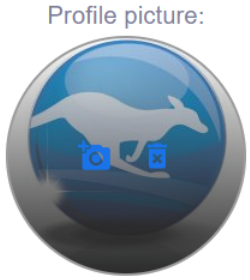


Additionally, you are able to add, remove, or edit the two factor authentication settings on your account. For more information on Two Factor Authentication, click HERE 44.

Lastly, KRMC offers the ability to add a profile picture. The image must be in the format of PNG, JPEG, JPG and cannot exceed 15MB in size. To change or add a profile image, click on the Profile Picture icon. In selecting this, you should be displayed a file navigation popup allowing you to navigate through your computer for an image you would like to use.



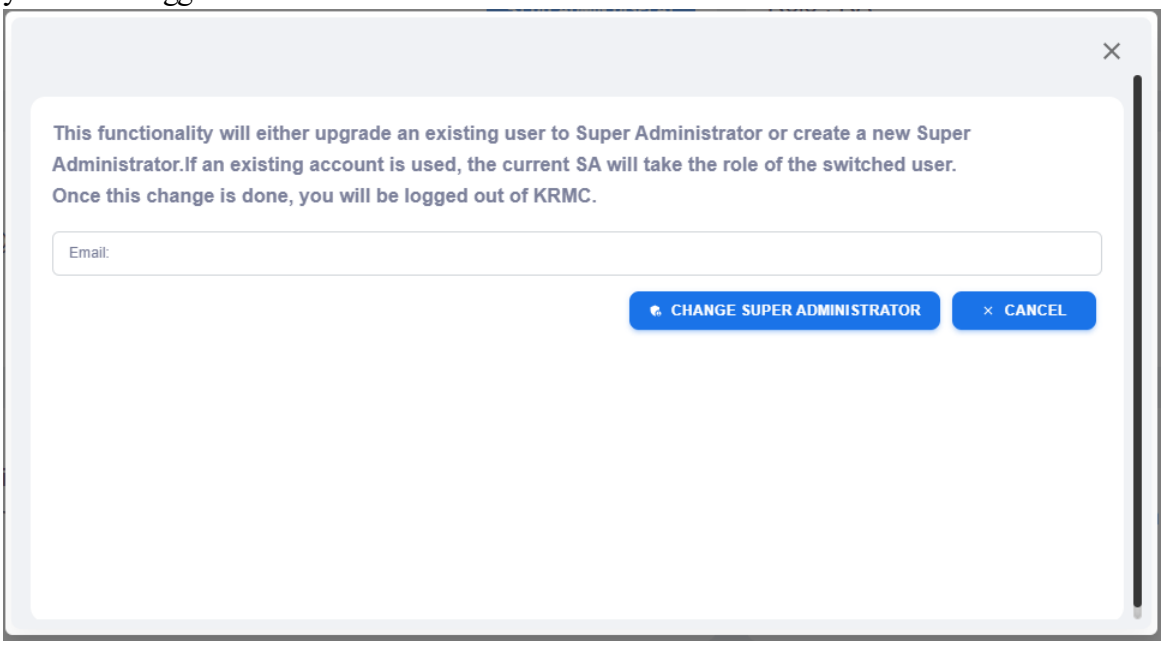
If at any point you want to change or fully remove your profile picture, you can click either the change profile picture or delete profile picture icons that appear when you hover your mouse over your picture.



Change Super Administrator

KRMC only has one Super Administrator (SA) account. With that said, there are options available if needed to change the account that is considered the SA account. ***Note:*** *You must be logged in as the SA in order to change the SA.* A full list of methods to change your SA can be located under Change Super Administrator 151 located under Admin Management 143 and Admins 144 however here is one method.

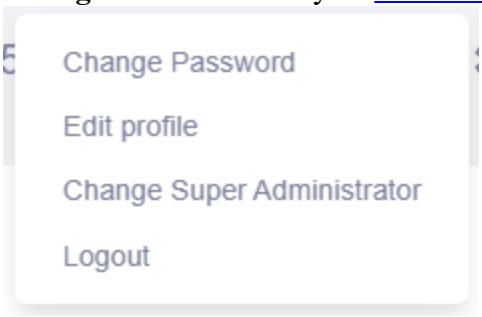
1. Located under the Account Icon 55 you can select **Change Super Administrator**.
2. Once you select this option you will be presented with a display stating "This functionality will either upgrade an existing user to Super Administrator or create a new Super Administrator. If an existing account is used, the current SA will take the role of the switched user. Once this change is done, you will be logged out of KRMC.".



3. You will need to add the email address that you would like to use as the new SA. ***Note:*** *If you are choosing a new account to be the SA, the new account will use the same account password as the original SA. This password can be changed with a password reset if you would like*.

Log Out of KRMC

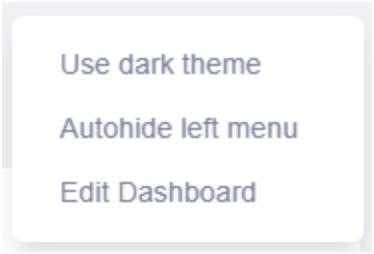
For security reasons, you should always log out of KRMC once you have completed your work on it. To accomplish this, you can select **Logout** located under your Account Icon 55.



Account Settings

Account Settings provides the ability to alter the look and feel of your KRMC experience. The three options provided within this are available for all KRMC On-Premise accounts regardless of account level.

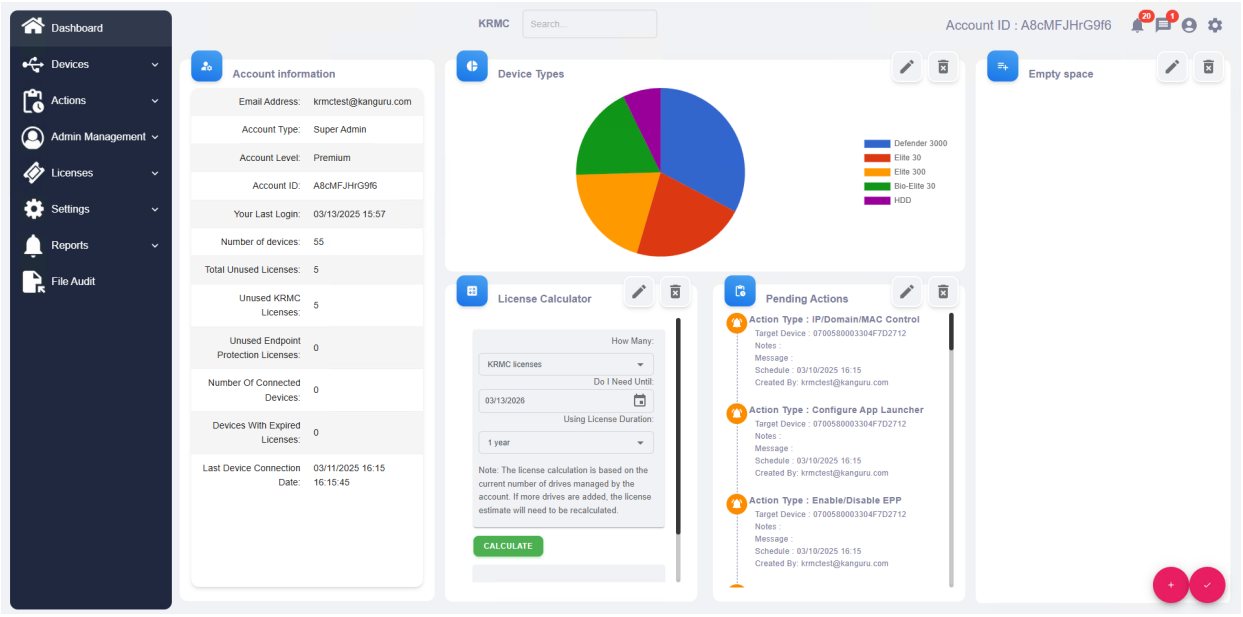
Use Dark/Light Theme	KRMC On-Premise provides the ability to alter the visual theme between a Light or Dark mode. For more information on this, please refer to Light or Dark Mode 188 located under Server Settings 182.
Autohide/Show Full Left Menu Always	Initially, the Navigation Menu only displays icons. When you hover your mouse over the area, the menu will expand revealing the full context. This can change to always show the expanded navigation menu. For more information on the Navigation Menu 52 please refer to Getting to Know KRMC On-Premise 42.
Edit Dashboard 61	The Dashboard is designed to be customizable to make your account overview as easy as possible. To accomplish this, you are able to change what is shown on you're your Dashboard.



Edit Dashboard

The Dashboard is designed to be customizable to make your account overview as easy as possible. To accomplish this, you are able to change what is shown on you're your Dashboard. After selecting Edit Dashboard you will be brought to an editable version of your Dashboard. There are a series of icons in this mode to assist you in editing this page. ***Note:*** *the box Account Information is not able to be moved from the Left side of the screen*.

Edit 	This allows you to choose from a list of options on what to display in this box.
Delete 	Deleting a box removes the content from that box. All remaining boxes will shift over to cover the newly emptied space.
Add Extra Box 	This adds a new blank box for you to add information to. If you leave the box blank, it will not appear after you exit the editing mode.
Finish Editing 	This saves all changes made within this mode.



Getting to Know KRMC On-Prem 5

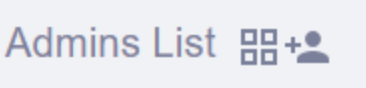
Admins, Auditors, and Groups

To make organization and management simpler KRMC On-Premise offers the ability to create several different account types and groups. Each of these account types and groups provide different permission levels and abilities.

Super Administrator	The Super Administrator (Super Admin/SA) has the highest-level access. The SA has authorization in KRMC On-Premise to manage all aspects of KRMC On-Premise in terms of devices, admins, groups and settings. There is only one SA per KRMC On-Premise company account.
	For steps on how to change the SA account, please click HERE 151.
Administrators	Administrators (Regular Administrators/RA) have the second-highest access level, just below the SA. RAs have the authority in KRMC On-Premise to manage only Groups assigned to them by the SA. RAs are also restricted to the actions that they can perform for said manageable items.
	For steps on how to create an admin, please click HERE 63.
	For steps on how to edit or delete an admin, please click HERE 145.
	For steps on how to edit permissions for an admin, please click HERE 147.
	For steps on how to edit the display options available to the admin, please click HERE 150.
Auditor	These read only accounts are allowed to view all devices and users within KRMC On-Premise, but their actions are limited solely to exporting logs and reports.
	For steps on how to create an auditor, please click HERE 65.
	For steps on how to export logs, please click HERE 131.
Groups	Groups allow you to organize multiple drives and users within heading such as a department. Groups can have their own Account ID allowing them to register drives directly to their Group account on KRMC On-Premise. Once drives are assigned to a Group, the SA or RAs administrating the group are able to search for drives for and send actions to the drive(s) on the account.
	For steps on how to create a group, please click HERE 67.
	For steps on how to edit groups, please click HERE 160.
	For steps on how to send actions to the drive(s) in the group, please click HERE 163.
	For steps on how to create group settings, please click HERE 162.

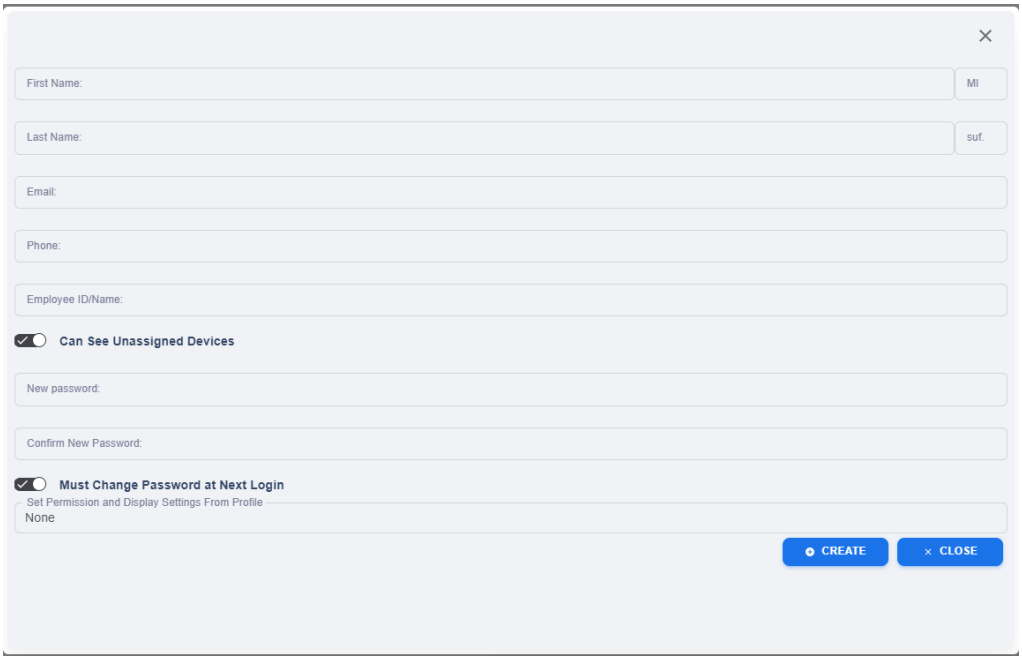
Create New Admin

When you are on the Admins or Auditor pages you should notice at the top left side of the screen a person icon with a plus sign (on Groups it is just a circle with a plus sign).



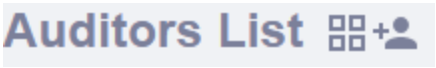
Create Admin
Click on the icon to reveal the Create Admin menu. The Create Admin menu allows you to easily create a new admin without navigating away from the current page.

First Name	The admin's first name
Last Name	The admin's last name
MI	The admin's middle initial
Suf.	The admin's suffix
Email	The admin's email
Phone	The admin's phone number
Employee ID/Name	The admin's employee ID
Can see unassigned devices	When enabled allows the administrator to view any unassigned devices. If disabled the administrator will only see devices assigned to them.
New Password	You are able to create a password for the new Admin account. After creating the password, you would then need to confirm the new password.
Must Change Password at Next Login	When this is enabled, your Admin will be asked to change their account password the next time they log into KRMC.
Set Permission and Display Settings From Profile	This feature allows you to copy the settings from another administrator to this new administrator account. This provides a simple way to assign permissions and display settings for multiple administrators. To use this feature you must have an account (other then the SA account) that has both Admin Permissions and Admin Display settings saved. Once those settings have been saved, refresh your browser and you should be able to see the admin appearing in the list to choose.


First Name:
MI
Last Name:
suf.
Email:
Phone:
Employee ID/Name:
Can See Unassigned Devices
New password:
Confirm New Password:
Must Change Password at Next Login
Set Permission and Display Settings From Profile
None
CREATE
CLOSE

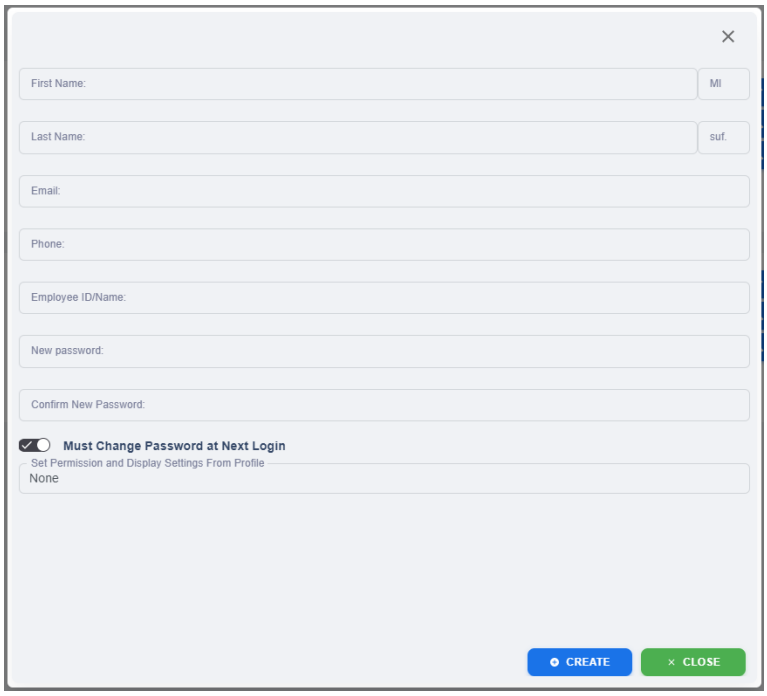
Create New Auditor

When you are on the Admins or Auditor pages you should notice at the top left side of the screen a person icon with a plus sign (on Groups it is just a circle with a plus sign).



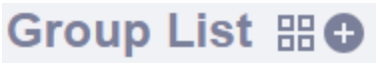
Create Auditor
Click on either the Create User or Create Admin icon to reveal the Create User/Admin menu. Once selected, choose Auditor which allows you to easily create a new Auditor without navigating away from the current page.

First Name	The auditor's first name
Last Name	The auditor's last name
MI	The auditor's middle initial
Suf.	The auditor's suffix
Email	The auditor's email
Phone	The auditor's phone number
Employee ID/Name	The auditor's employee ID
New Password	You are able to create a password for the new Auditor account. After creating the password, you would then need to confirm the new password.
Must Change Password at Next Login	When this is enabled, your Auditor will be asked to change their account password the next time they log into KRMC.
Set Permission and Display Settings From Profile	This feature allows you to copy the settings from another account to this new account. This provides a simple way to assign permissions and display settings for multiple. To use this feature you must have an account (other then the SA account) that has both Admin Permissions and Admin Display settings saved. Once those settings have been saved, refresh your browser and you should be able to see the admin appearing in the list to choose.


First Name:
MI
Last Name:
suf.
Email:
Phone:
Employee ID/Name:
New password:
Confirm New Password:
Must Change Password at Next Login
Set Permission and Display Settings From Profile
None
CREATE
CLOSE

Create New Group

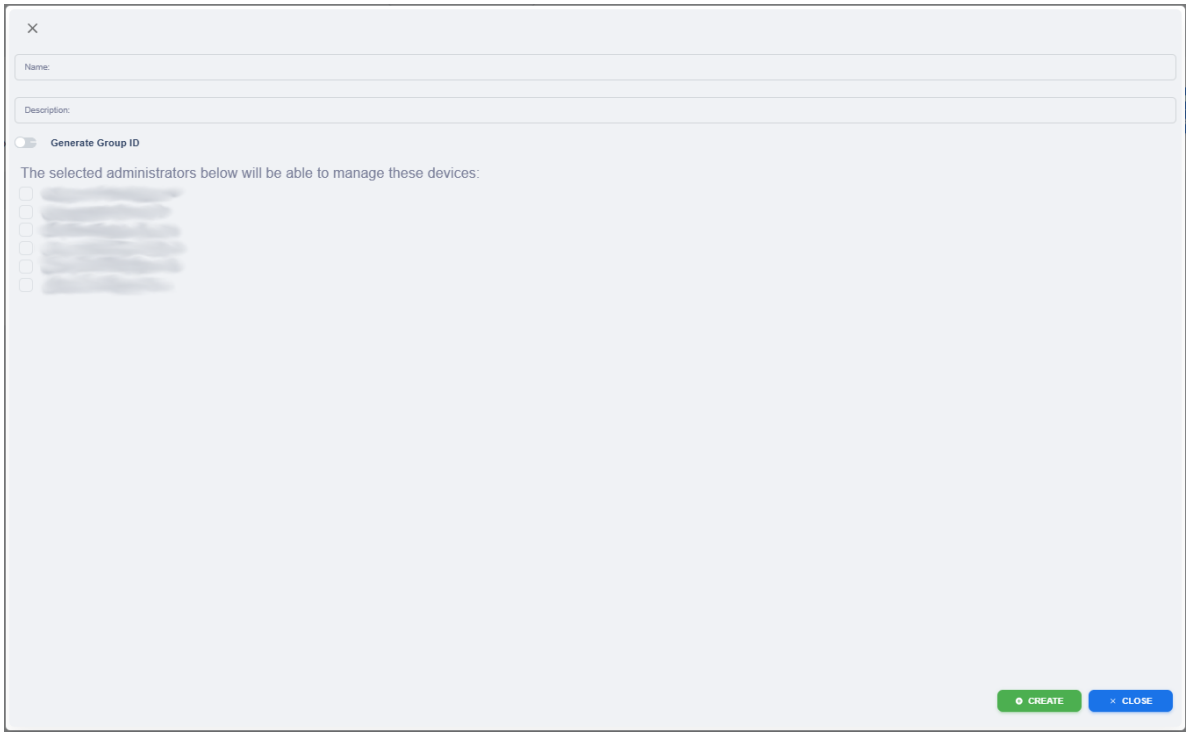
When you are on the Groups page you should notice at the top left side of the screen a circle with a plus icon (on the Admins or Auditor pages it will be person icon with a plus sign).



Create Group

The Create New Group menu allows you to easily create a group without navigating away from the current page.

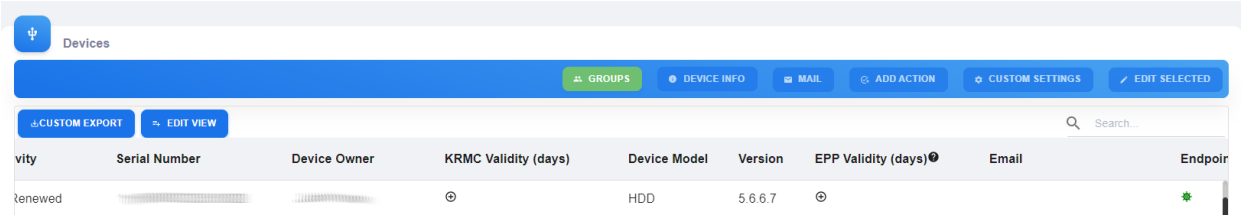
Name	The Group's name, e.g., "Sales Department"
Description	A short description of the group. e.g., "Northeast Territory"
Generate Group ID	The Group ID allows you to assign Defender drives directly to a group.
The selected administrator below will be able to manage these devices	Allows you to add administrators to the group. Administrators assigned to this group will be able to manage all devices associated with the group.



License Assignment

KRMC and Endpoint Protection licenses are applied automatically to devices based on which drives communicated with KRMC recently. The licenses are assigned to drives that require one at the time of the order. KRMC regularly checks drive validity to confirm that all drives have valid licenses if available in your license pool. If a drive does not have a valid license and you have licenses available in your license pool, you can manually assign a license in the Active 118 list.

To perform this, you will need to make sure you have both the KRMC and EEP validity columns appearing (Edit View 133 will assist with this). Once appearing to you, you can now select the Plus Icon associated with your drive(s) that you are looking to manually assist a license to.



KRMC On-Premise Virtual Console 6

The KRMC On Premise virtual appliance main menu provides a series of options for you to configure your server as you would like.
Navigation within the KRMC menu is as follows:

- Press the UP or down key to navigate the menu items
- Press the tab key to switch between fields
- Press the ENT key to confirm an action
- Press the Spacebar to select an option
- Press the ESC key to cancel an action

The KRMC menu consists of the following options:
Note: *If you are setting up KRMC for the first time you may not see all menu options. Please refer to Setting up KRMC for first time 22.*

Configure date and time 71	Configure date and time allows you to change the time zone, date and time and at the server location
Generate Certificates 74	Generate Certificates creates a self-signed certificate which is used to ensure secure communication between the KRMC server and any computers accessing it remotely. Make sure that you set the correct date and time before generating certificates as the Configure Data and Time menu will not be available after you generate the certificates.
Configure IP 76	Allows you to set or change an IP address for your server. Your options are Static or DHCP
Configure hostname 79	This allows you to set or change the hostname for your KRMC server.
Restrict KRMC Access to IP address 80	You can restrict access to the KRMC web console by IP. There are 4 options for restricting access: Regular expression, Multiple regular expressions, IP List, All
SSH Control 84	SSH Control allows you to stop or start SSH. SSH is not running by default but can be enabled which allows for remote connections.
FTP Server 86	You can configure KRMC to automatically save the last 7 database backup files on an FTP server by entering your FTP server location and credentials.
Restart PHP, MySQL, and Nginx 88	This can be done if you are experiencing any issues with the KRMC web portal not behaving correctly (e.g. pages not loading, information not appearing, etc.).
Edit SA 89	If your SA is unable to gain access to KRMC for any reason, you are able to use this option to change general login information for the account.
Export bug report 91	Export bug report provides the ability to download all of the KRMC server logs so they can be provided to support. These logs are essential to troubleshoot certain issues being experienced. These logs are also available to be downloaded by navigating to Settings 170 then Helpful Info 200. Please note that all logs are provided in the ZIP file format.

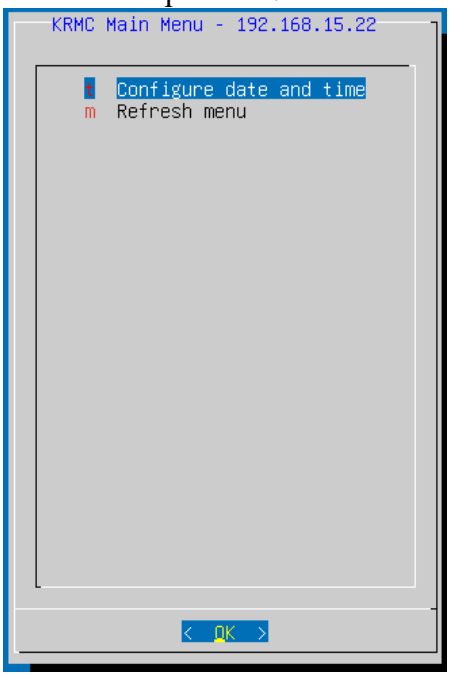
Clear Cache 95	Clear Cache allows you to clear the web server cache, which can resolve any problems using the KRMC web interface
Keyboard Layout 96	This allows you to change the keyboard layout for the options within the KRMC VM menu.
Replace database 97	If you are upgrading from a legacy version of KRMC (such as KRMC 5, KRMC 6, or KRMC 7) you can use this option to migrate your database over to the new KRMC server.
Database failover recovery 99	If your KRMC database get corrupted for any reason, you can attempt to recover the database using a backup file either locally stored on the VM or located on your FTP.
Regenerate certificates 103	Regenerate Certificates allows you to create a new self-signed certificate for your KRMC server. This option is useful your current certificate expired or if you would like to remake the self-signed certificate.
Replace signed certificates 105	This allows you to replace the self-signed certificate with your own signed certificate.
Restore from another KRMC VM 107	If you are restoring an existing KRMC virtual appliance, you must import the certificates and database from the existing KRMC to maintain your data and access.
Reactivate KRMC VM 109	When migrating from an old KRMC VM to a new one, the old KRMC VM is deactivated during the migration. You are able to reactivate the old KRMC VM in the event that something goes wrong with the new KRMC VM.
Restart server 111	Gracefully restart the KRMC virtual appliance. This will allow the system to complete any queued data transfers, pending tasks and/or processes before shutting down and restarting the KRMC VM.
Graceful shutdown 112	A graceful shutdown will allow the system to complete any queued data transfers, pending tasks and/ or processes before shutting down the KRMC VM.
Refresh menu 113	Refresh the KRMC Main Menu to update the menu display.

Configure date and time

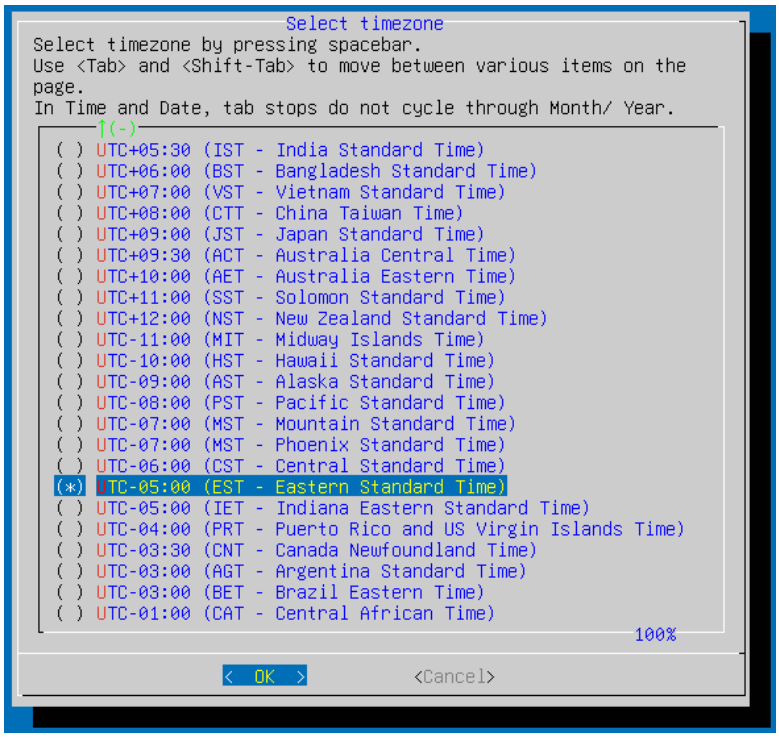
Configure date and time allows you to change the time zone, date and time and at the server location. This is the second set in Setting up KRMC for the first time 22. By default, the appliance should be able to select the correct information from your hypervisor application so this should be just a verification. This is not able to be altered after this point so please verify the information is correct prior to finalizing these settings.

To configure the date and time:

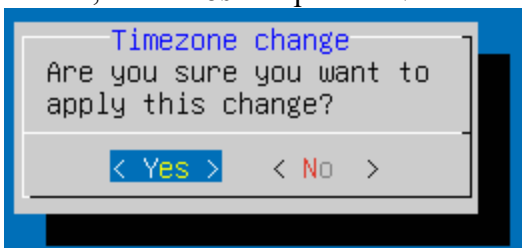
1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Configure date and time** is selected and press **ENT**.



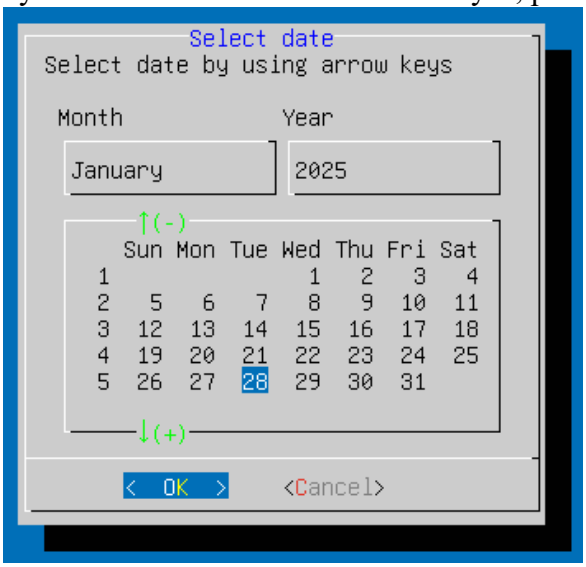
2. A time zone window will appear to you. You will need to use the **Up** or **Down** arrows to navigate the options available. Once you have located the correct time zone for you, press the **Spacebar** to select the time zone.



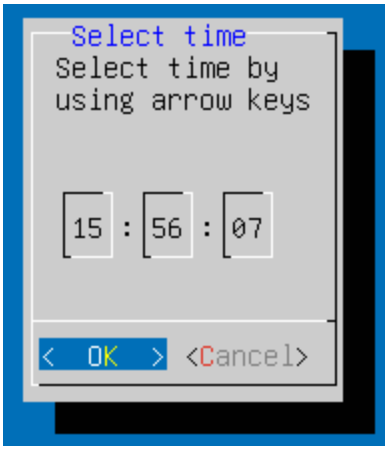
3. Press **ENT** to continue and you will be displayed with a message asking you to confirm your selection. If you wish to proceed, select **Yes** and press **ENT**.



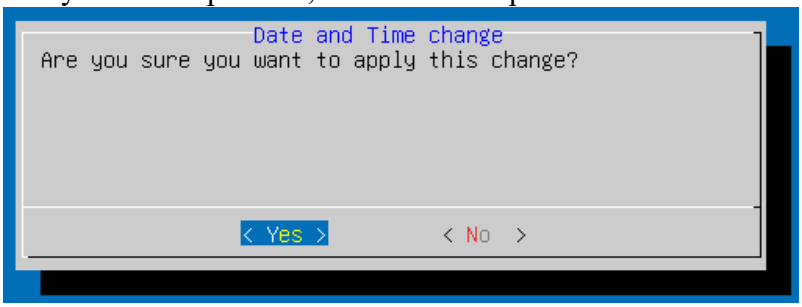
4. After confirming the time zone, a calendar will appear to you so you can select your current date. Once again, you will need to use the **Up**, **Down**, **Left**, and **Right** arrows to navigate the options available. Once you have located the correct date for you, press **ENT**.



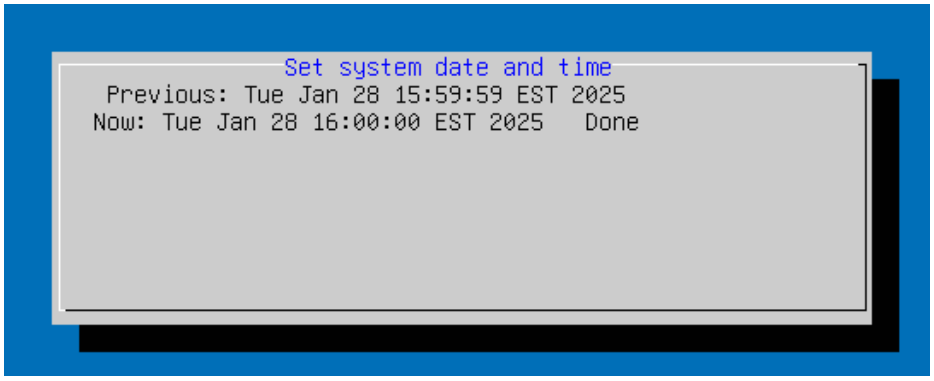
5. After selecting your date, you will be brought to a 24-hour clock for you to enter your current time. you will need to use the **Up**, **Down**, **Left**, and **Right** arrows to navigate the options available and change them as needed. Once you have set your server to the correct time, press **ENT**.



6. You will lastly be brought to a window asking you to confirm you want to apply the changes you have made. If you wish to proceed, select **Yes** and press **ENT**.



7. After confirming your selection, you will have a quick display showing the original settings and the new settings. This should last only a few seconds, then you will be brought back to the KRMC On-Premise Virtual Console.



Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

KRMC On-Premise Virtual Console 6

Generate Certificates

Generate Certificates creates a self-signed certificate which is used to ensure secure communication between the KRMC server and any computers accessing it remotely. This is the third set in Setting up KRMC for the first time 22.

If you are looking to apply your own signed certificate, you will need to first generate a signed certificate using the steps below then you can follow the steps on Replace signed certificates 105.

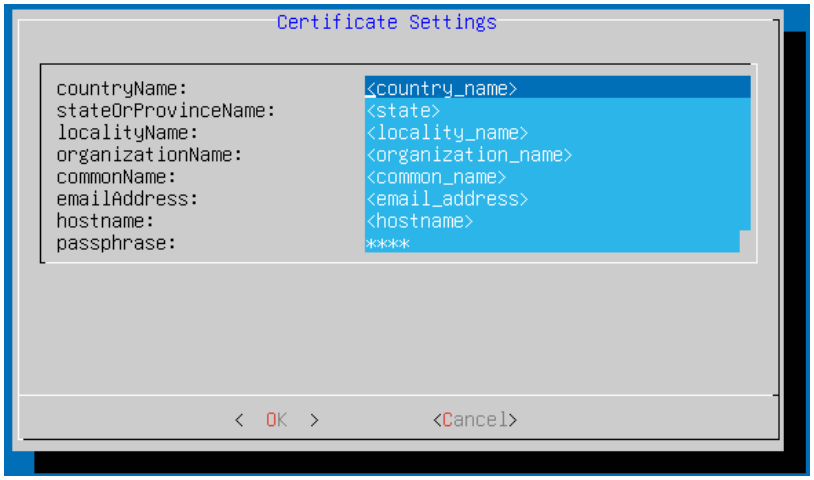
To Generate certificates:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Generate Certificates** is selected and press **ENT**.

2. After pressing **ENT** will be brought to the Certificate Settings Window. You will need to complete each field in order to proceed. Use the **Up**, **Down**, **Left**, and **Right** arrows to navigate between the options as well as **Backspace** or **Delete** to remove any default content that is displayed. ***Note**: All fields require at least 2-characters to be entered.*

CountryName	The country where the organization or individual is legally located.
StateOrProvinceName	The state or province where the organization or individual is legally located.
localityName	The city or town where the organization or individual is legally located.
organizationName	The company/organization name.
commonName	A field that identifies the domain name or entity the certificate is issued to, typically matching the website's domain name.
emailAddress	The email address of the administrator configuring your KRMC certificate.

hostname	The domain name or subdomain for which the certificate is issued.
passphrase	The password that you are setting on your KRMC certificate. This must be more then four characters in length.



3. After completing all of the required fields you can press **ENT** to continue. You will have a display showing the server certificate and client certificate has been replaced as well as the Nginx server has restarted. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.

Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press* ***ESC*** *on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

Configure IP

Configure IP allows you to set the network interface to either Static IP or DHCP. If you choose DHCP, the server will automatically assign an IP address to your KRMC Enterprise sever. If you choose Static, you will need to manually enter in the IP address, netmask, gateway and DNS information for your KRMC On-Premise server.

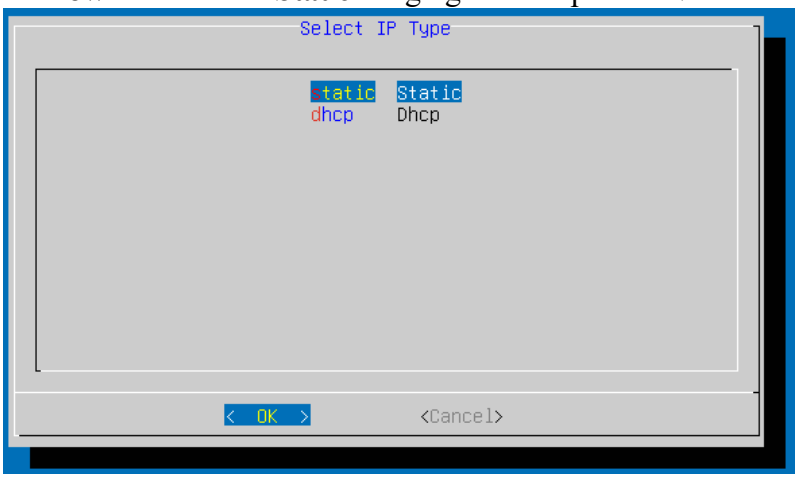
The server network interface will need to be restarted in order to apply any changes to the IP address.

Note: *The* ***Configure IP*** *option is not available until after you have completed* *Generate Certificate* 74.

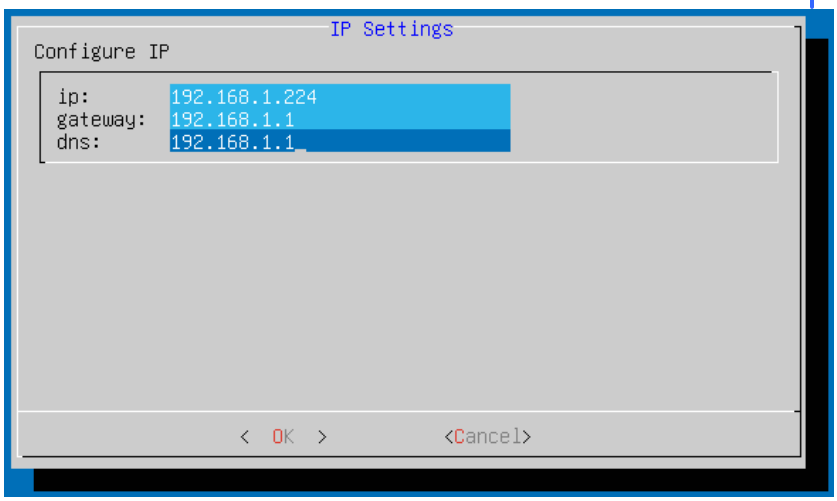
To configure the IP address:

1. From the **KRMC On-Premise Virtual Console** 69, use the **Up** or **Down** arrows until you see **Configure IP** is selected and press **ENT**.

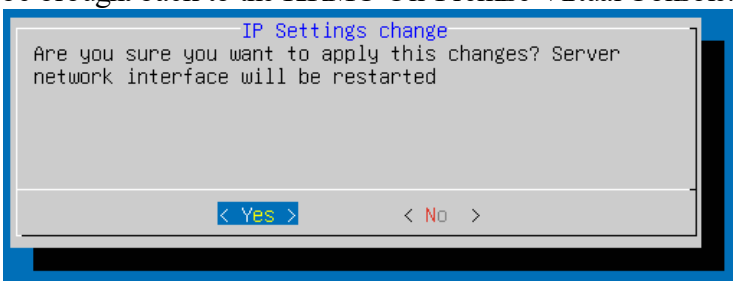
2. You will have two options to choose how to proceed.
3. To set a **Static** address:
   a. Press the **Up** and **Down** arrows until **Static** is highlighted and press **ENT**.



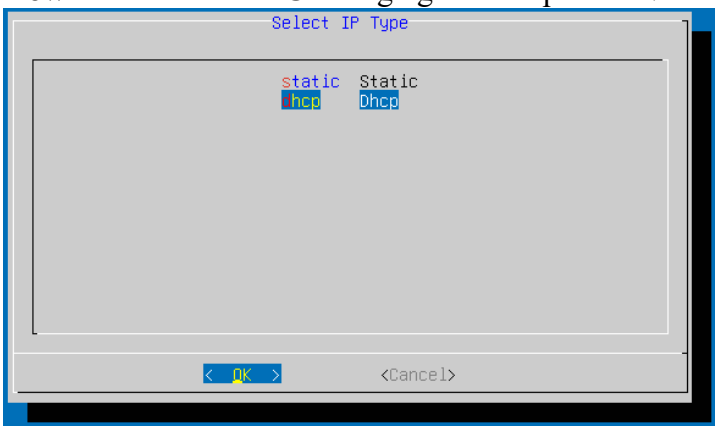
   b. Upon selecting static, you will be brought to a page where you will need to complete the fields provided. The fields required to be completed are: IP Address, Gateway, and DNS. You can use the **Up**, **Down**, **Left**, and **Right** arrows as well as your keypad to enter the requested information.



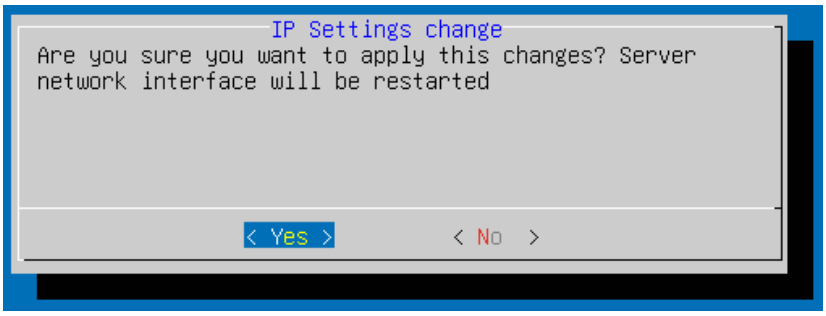
c. After completing the fields, you can press **ENT**. You will have a display showing asking you to confirm you would like to apply the changes made. If you would like to proceed, select **YES** and press **ENT**. After selecting **YES**, the screen will remain here as it attempts to apply the networking configuration you have configured. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



4. To set a **DHCP** address:
   a. Press the **Up** and **Down** arrows until **DHCP** is highlighted and press **ENT**.



   b. After pressing **ENT**. You will have a display showing asking you to confirm you would like to apply the changes made. If you would like to proceed, select **YES** and press **ENT**. After selecting **YES**, the screen will remain here as it attempts to apply the networking configuration you have configured. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press* ***ESC*** *on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

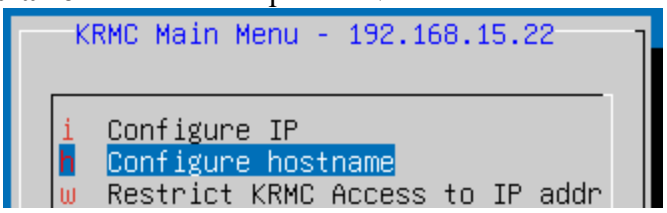
Configure hostname

Configure hostname allows you to update the hostname if required. The server network interface will need to be restarted in order to apply any changes to the hostname.

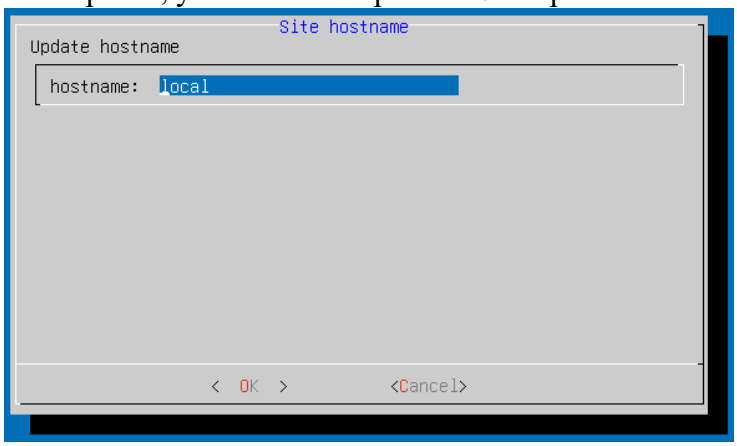
***Note**: The **Configure Hostname** option is not available until after you have completed* *Generate Certificate* 74.

To configure hostname:

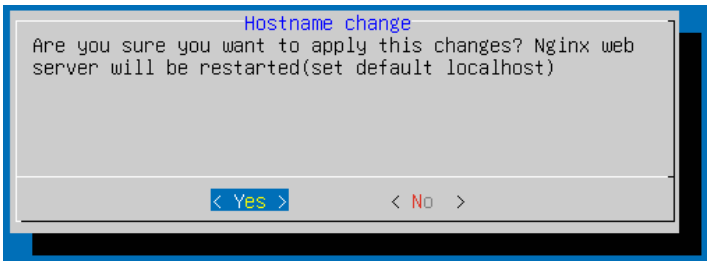
1. From the **KRMC On-Premise Virtual Console** 69, use the **Up** or **Down** arrows until you see **Configure hostname** is selected and press **ENT**.



2. After entering Configure hostname, you will need to enter the new hostname for your server. Once this has been completed, you will need to press **ENT** to proceed.



3. You will have a display showing asking you to confirm you would like to apply the changes made. If you would like to proceed, select **YES** and press **ENT**. After selecting **YES**, the screen will remain here as it attempts to apply the hostname configuration you have configured. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

Restrict KRMC Access to IP address

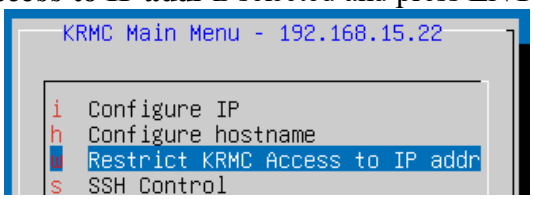
Restrict KRMC Access to IP address allows you as the administrator to dictate the location of your administrators must be in order to log into and gain access to the KRMC web console. Please note that while you will not be able to log into the console if your IP address does not meet the conditions implemented, you will still be able to navigate to the login screen itself. You can restrict access to the KRMC web console by IP. There are 4 options for restricting access:

Regular expression	Enter a single IP range that will be allowed access (e.g. 192.168.1.0-192.168.1.50). All other IPs outside of this range will be blocked.
Multiple regular expressions	Enter multiple IP ranges, separated by a semicolon, that will be allowed access (e.g. 192.168.1.0-192.168.1.50;10.10.10.1-10.10.10.10). Any IP outside of these ranges will be blocked. There is no limit to the number of IP ranges that can be specified.
IP List	Enter multiple IPs, separated by a semicolon, that will be allowed access (e.g. 192.168.1.0;10.10.10.1). All other IPs outside of these specific IPs will be blocked.
All	Allow all IPs access to the KRMC web console. ***Note:*** *This is the default setting.*

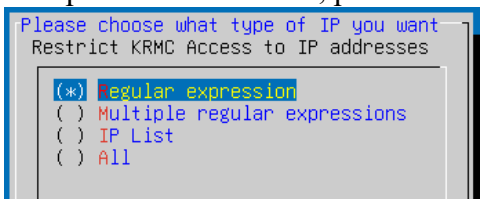
Note: *The* ***Restrict KRMC Access to IP address*** *option is not available until after you have completed* *Generate Certificate* 74.

To restrict KRMC access to IP address:

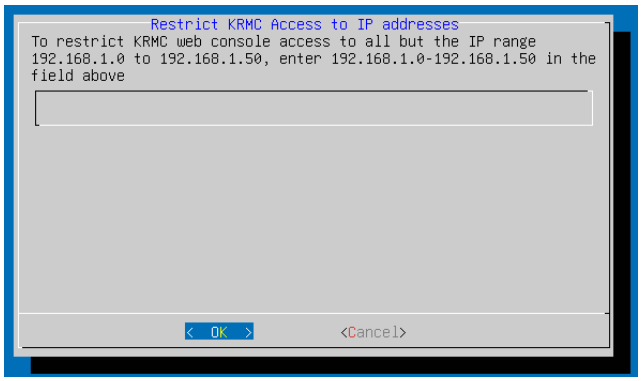
1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Restrict KRMC Access to IP addr** is selected and press **ENT**.



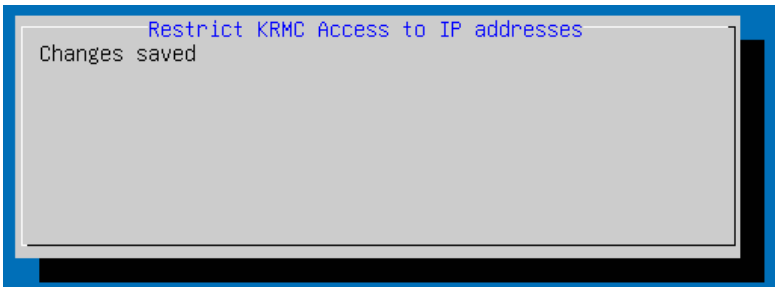
2. You will have four options to choose how to proceed.
3. To set a **Regular expressions**:
   a. Press the **Up** and **Down** arrows until **Regular expression** is selected and press the **Spacebar** to select the option. After selected, press **ENT**.



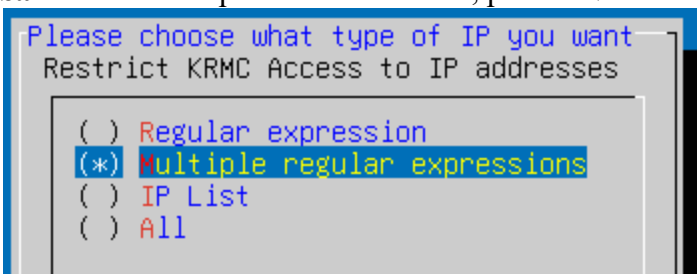
   b. Upon selecting Regular expression, you will be brought to a screen where you will need to complete the filed that is provided.



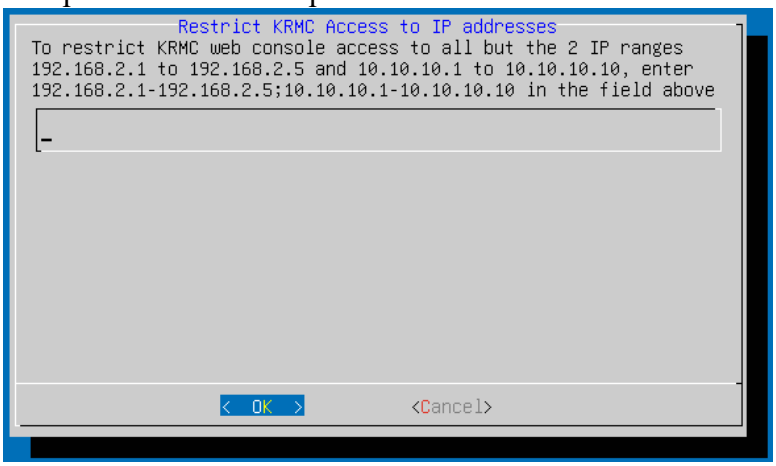
c. After entering the range in which you are looking to restrict access to, press **ENT**. You will receive a message stating that the changes you have requested have been saved. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



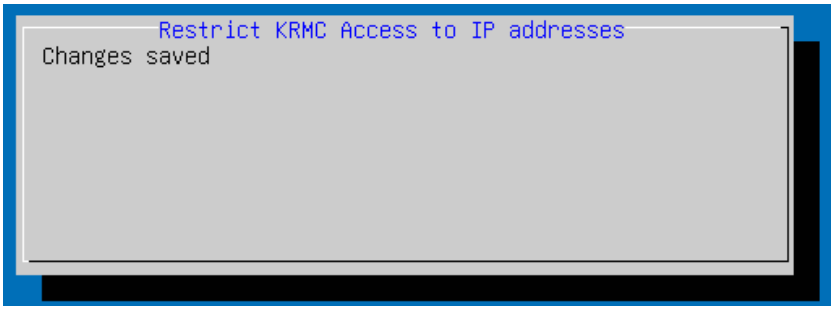
4. To set **Multiple regular expressions**
   a. Press the **Up** and **Down** arrows until **Multiple regular expression** is selected and press the **Spacebar** to select the option. After selected, press **ENT**.



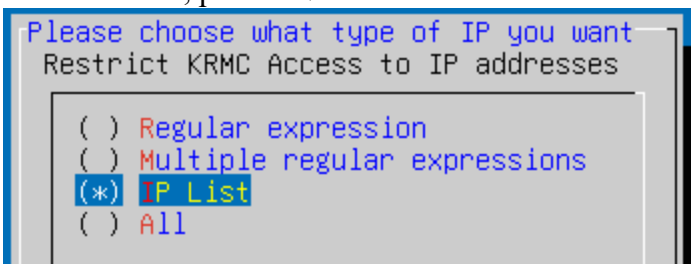
   b. Upon selecting Multiple regular expressions, you will be brought to a screen where you will need to complete the filed that is provided.



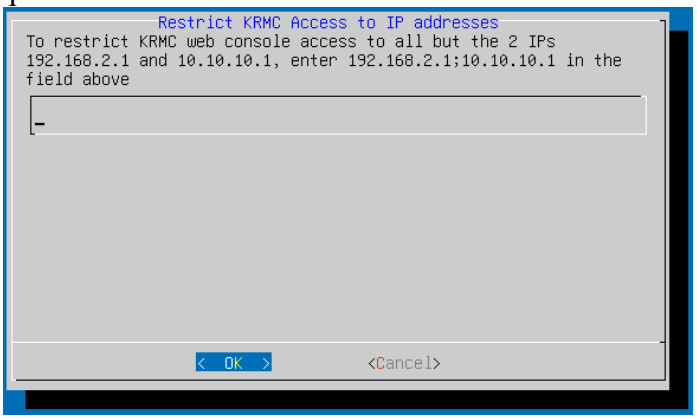
c. After entering the range in which you are looking to restrict access to, press **ENT**. You will receive a message stating that the changes you have requested have been saved. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



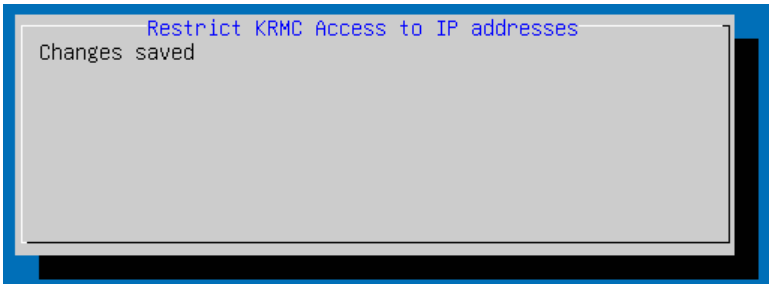
5. To set **IP List**
   a. Press the **Up** and **Down** arrows until **IP List** is selected and press the **Spacebar** to select the option. After selected, press **ENT**.



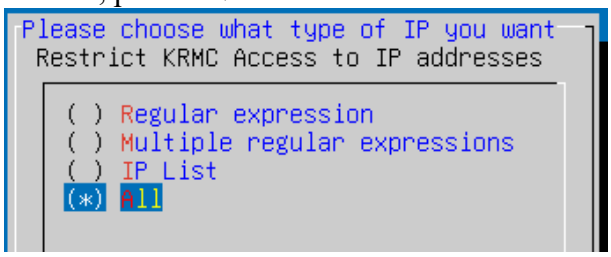
   b. Upon selecting IP List, you will be brought to a screen where you will need to complete the filed that is provided.



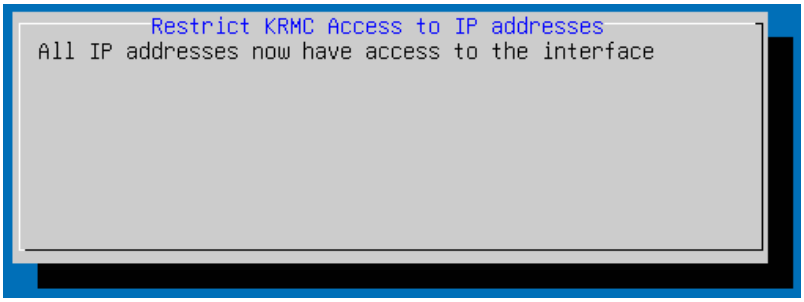
   c. After entering the IP addresses in which you are looking to restrict access to, press **ENT**. You will receive a message stating that the changes you have requested have been saved. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



6. To set **All**
   a. Press the **Up** and **Down** arrows until **All** is selected and press the **Spacebar** to select the option. After selected, press **ENT**.



   b. You will receive a message stating that All Ip address now have access to the interface. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console



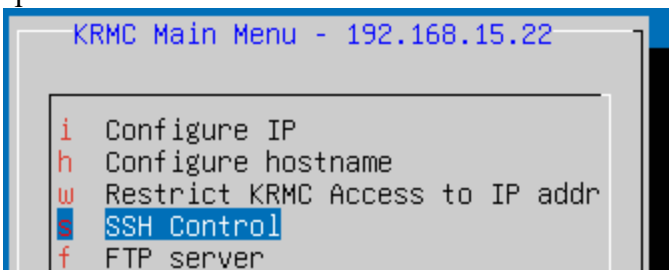
***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved*

SSH Control

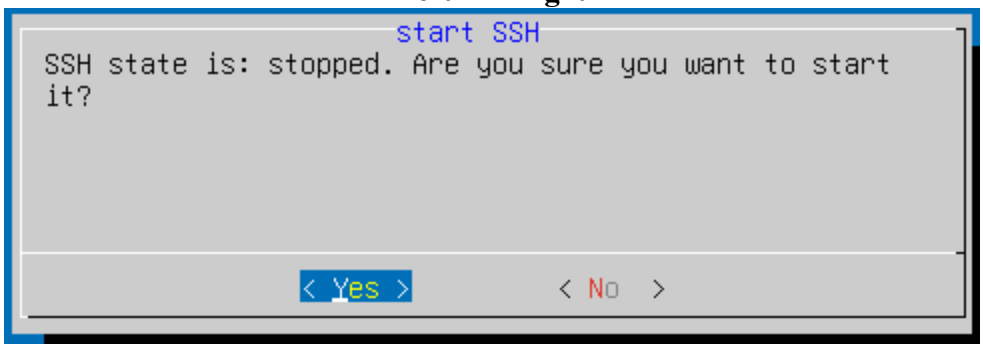
SSH Control allows you to stop or start SSH. SSH is not running by default but can be enabled which allows for remote connections with Technical Support during a scheduled remote session. The port configured for this is the default port 22. This port cannot be changed/altered.

To configure SSH:

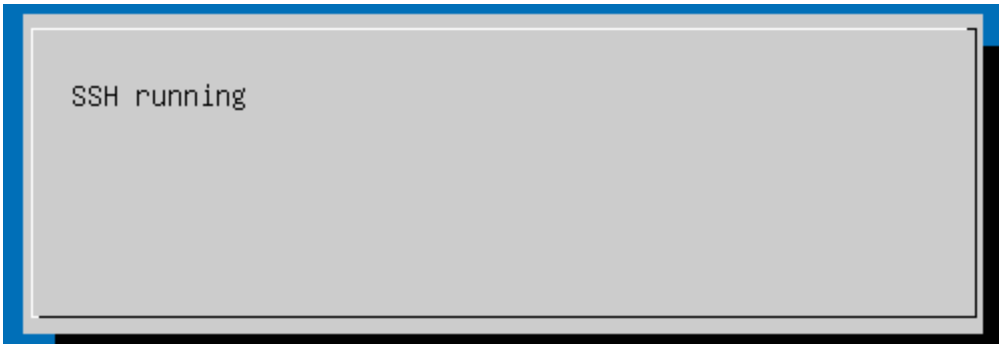
1. From the KRMC On-Premise Virtual Console 69, use the Up or Down arrows until you see SSH is selected and press ENT.



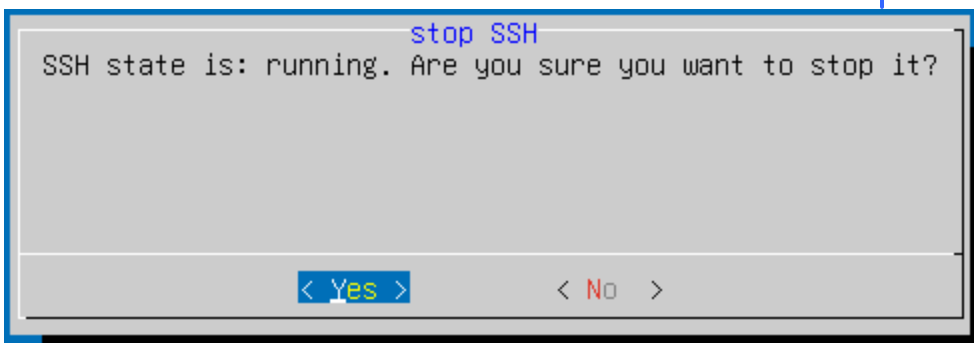
2. If SSH is currently disabled (the default setting):
   a. Upon pressing **ENT** you will receive a message stating SSH state is stopped. Are you sure you want to start it?". You can use the **Left** and **Right** arrow to choose either Yes or No.



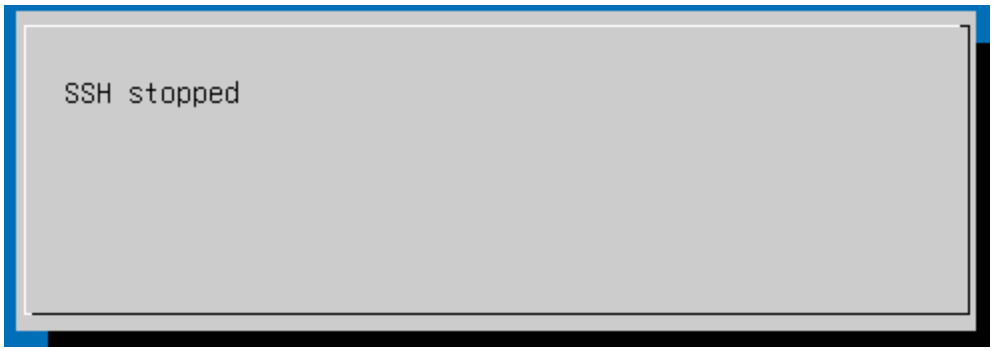
   b. If you select **Yes** and press **ENT**, a message stating "SSH running" will appear. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console



3. If SSH is currently enabled:
   a. Upon pressing **ENT** you will receive a message stating SSH state is running. Are you sure you want to stop it?". You can use the **Left** and **Right** arrow to choose either Yes or No.



b. If you select **Yes** and press **ENT**, a message stating "SSH running" will appear. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console



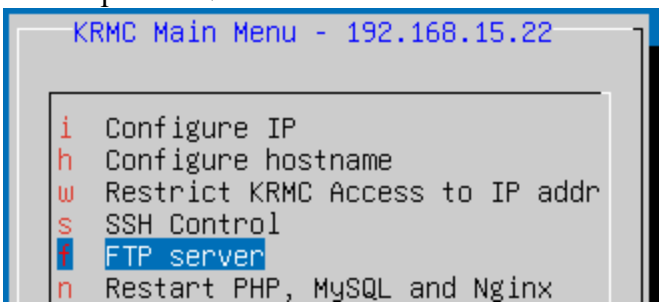
***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

FTP Server

Using FTP server, you can configure KRMC to automatically save the last 7 database backup files on an FTP server within your network.

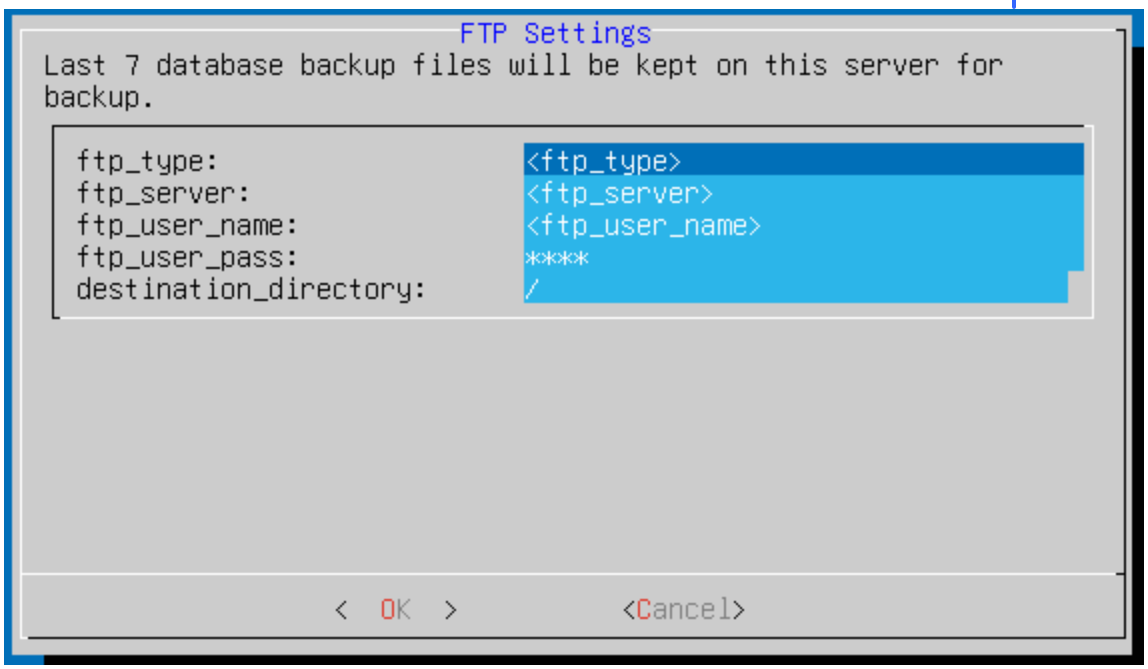
To connect to an FTP server:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **FTP server** is selected and press **ENT**.



2. Upon pressing **ENT**, you will be presented with a series of fields that need to be completed. Use the **Up**, **Down**, **Left**, and **Right arrows** to navigate between the options as well as **Backspace** or **Delete** to remove any default content that is displayed.

ftp_type	This is the type of FTP that you are looking to connect KRMC to. An example would be: FTP, SFTP, FTPS.
ftp_server	The IP address or server name with the port number.
ftp_user_name	The username you are looking to access the FTP with. This will be stored on the server and will be the login that KRMC will always use to gain access.
ftp_user_pass	The password you are looking to access the FTP with. This will be stored on the server and will be the login that KRMC will always use to gain access.
destination_directory	The directory that the database will be stored within your FTP server.



3. After you complete the fields, press **ENT**. You will receive a message stating "Changes saved". This may last a minute or two but then you will be brought back to the **KRMC On-Premise Virtual Console**.

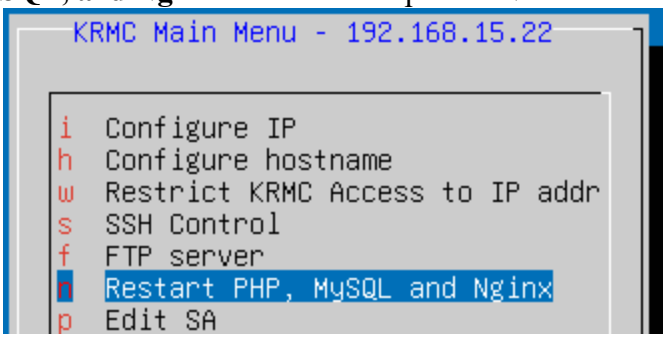
***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

Restart PHP, MySQL, and Nginx

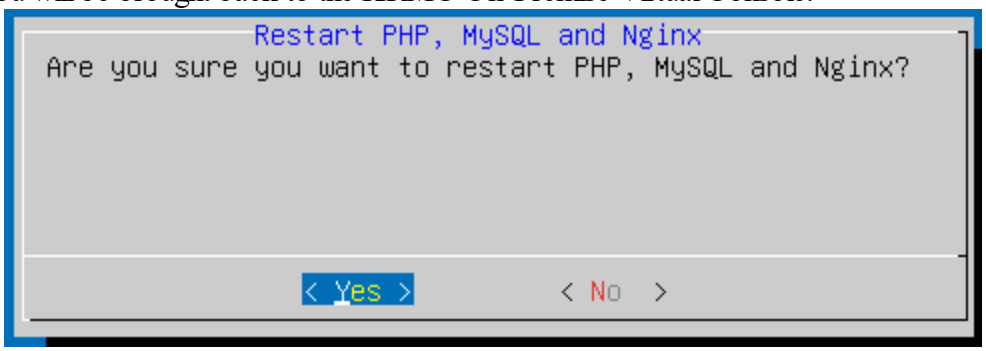
Restart PHP, MySQL and Nginx services allows you to attempt to correct any issues you are experiencing any issues with the KRMC web interface (e.g. pages not loading, information not appearing, etc.). We strongly recommend contacting support if this does not grant access back to KRMC once completed.

To Restart PHP, MYSQL, and Nginx:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Restart PHP, MYSQL, and Nginx** is selected and press **ENT**.



2. You will have a display showing asking you to confirm you would like to restart the services. If you would like to proceed, select **YES** and press **ENT**. After selecting **YES**, the screen will remain here as it attempts to restart the mentioned services. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



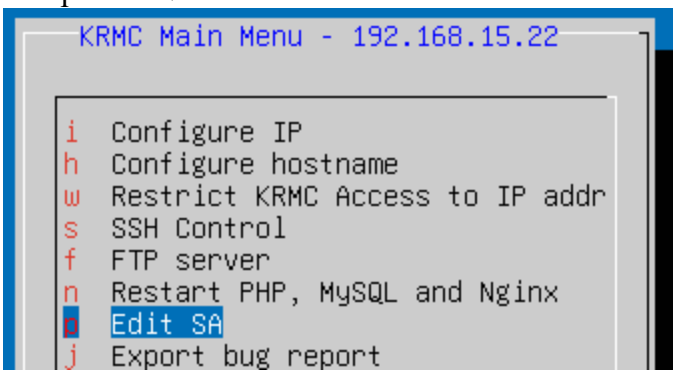
***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

Edit SA

Edit SA is a troubleshooting option within the KRMC On-Premise Virtual Console 69 which allows you to alter the Super Administrator (SA) account information. This should only be used in the cases where the SA is unable to gain access to the account and other steps like "Forgot Password" are not granting access.

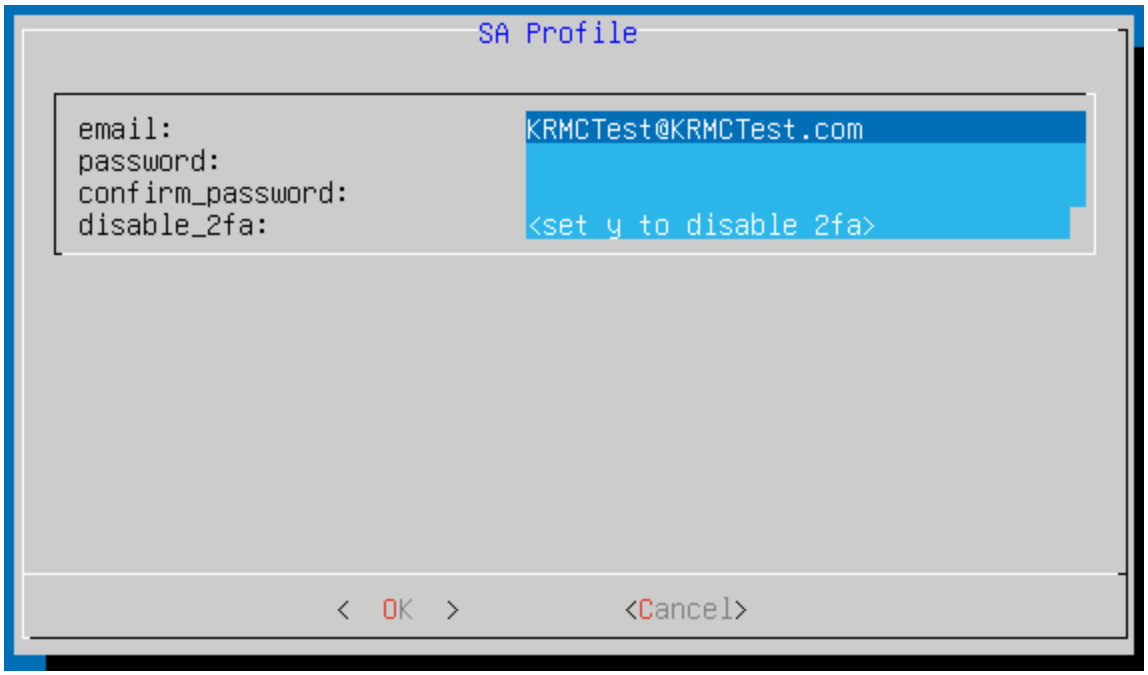
To Edit SA:

1. From the **KRMC On-Premise Virtual Console**, use the **Up** or **Down** arrows until you see **Edit SA** is selected and press **ENT**.

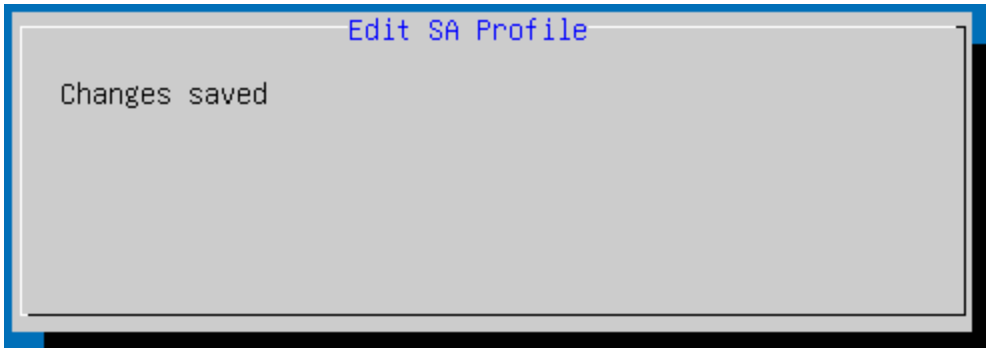


2. Once you press **ENT**, you will be able to see the SA account that you will be altering along with three additional fields for you to alter.

email	This will display the current email address of the SA. If this is changed here, the current SA will be converted to a Regular Administrator (RA) and will maintain the same password as before. Additionally, you are able to convert and RA to an SA by using this method if needed. In performing this the orginal SA will be converted to an RA and the RA will be converted to the SA. If you are able to gain access to the KRMC web browers we recommend performing this change instead in the menu option Administrative Management 143 under Admins 144 and Change Super Administrator 151.
password	This will alter the password to the email account displayed.
confirm_password	This is the confirmation of the above password.
disable_2fa	If you are looking to disable 2FA as the feature is not working properly for you, clear the contents and inster Y. If you are not looking to alter the 2FA setting, clear the contents and insert N.



3. After making your changes to the SA account, press **ENT**. You will receive a message stating "Changes Saved". This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

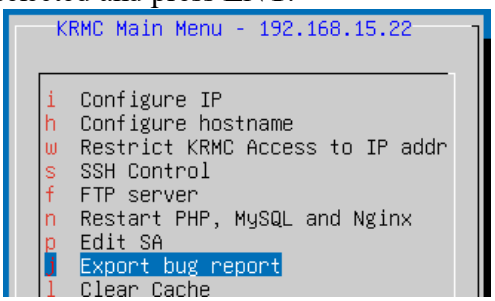
Export bug report

Export bug report provides the ability to download all of the KRMC server logs so they can be provided to support. These logs are essential to troubleshoot certain issues being experienced. These logs are also available to be downloaded by navigating to Settings 170 then Helpful Info 200. Please note that all logs are provided in the ZIP file format. By using Export bug report, you are able to choose from three options:

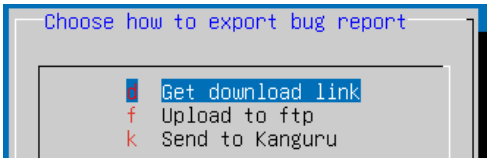
Get download link	This provides you a URL that you can use to download the logs via use of a browser.
Upload to ftp	If you have an FTP server available, you can connect your KRMC server to it for your server logs to be uploaded to. If you already configured your KRMC server with FTP settings using the option FTP Server 86 on the KRMC On-Premise Virtual Console 69, your previously entered configuration will display to you. If you have not configured the FTP settings previously, you will need to complete the information in the fields provided.
Send to Kanguru	If your KRMC server is on a network that can communicate with our servers, you can choose to upload the your bug report directly to our servers. You are provided a field to describe the issue you are experiencing along with the logs.

To Export bug report:

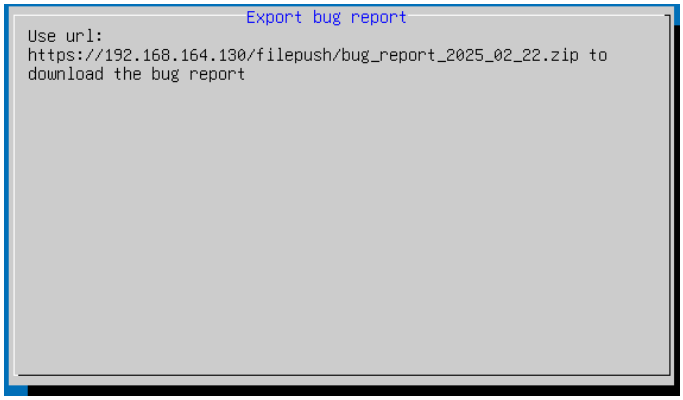
1. From the **KRMC On-Premise Virtual Console**, use the **Up** or **Down** arrows until you see **Export bug report** is selected and press **ENT**.



2. You will have three options to choose how to proceed:
3. To export using Get download link:
   a. Press the **Up** and **Down** arrows until **Get download link** is selected and press **ENT**.

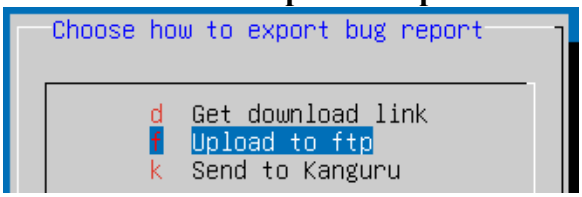


   b. A message will appear on your screen showing you a URL that will need to be entered into your browser to download the logs. The URL will only display for 30 seconds so we would recommend taking a screenshot of the URL so you will not be rushed in entering into your browser. The URL will follow the following format: https://<serveraddress>/filepush/bug_report_<year>_<month>_<day>.zip.



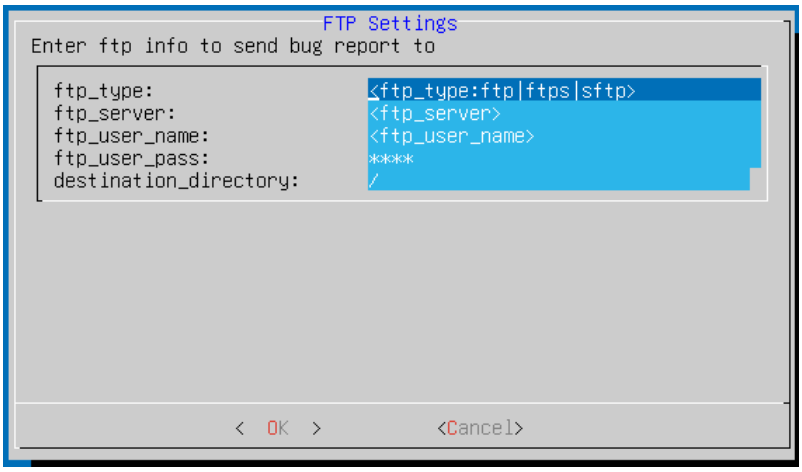
c. After the URL has displayed for 30 seconds, you will be brought back to the KRMC On-Premise Virtual Console.

4. To export using **Upload to ftp**:
   a. Press the **Up** and **Down** arrows until **Upload to ftp** is selected and press **ENT**.

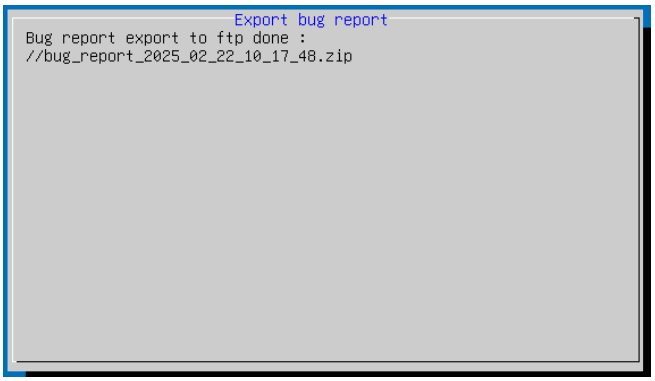


   b. You will be presented with a series of fields that need to be completed. Use the **Up**, **Down**, **Left**, and **Right** arrows to navigate between the options as well as **Backspace** or **Delete** to remove any default content that is displayed.

ftp_type	This is the type of FTP that you are looking to connect KRMC to. An example would be: FTP, SFTP, FTPS.
ftp_server	The IP address or server name with the port number.
ftp_user_name	The username you are looking to access the FTP with. This will be stored on the server and will be the login that KRMC will always use to gain access.
ftp_user_pass	The password you are looking to access the FTP with. This will be stored on the server and will be the login that KRMC will always use to gain access.
destination_directory	The directory that the database will be stored within your FTP server.

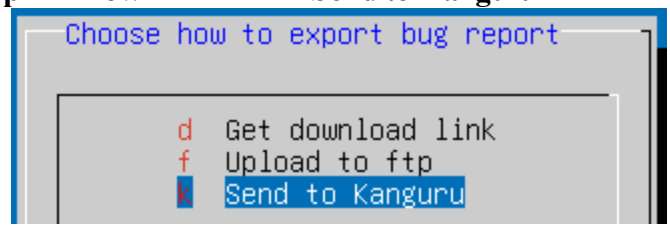


c. After you complete the fields, press **ENT**. You will receive a message stating that bug report has been completed and will provide the report name for you to look for.

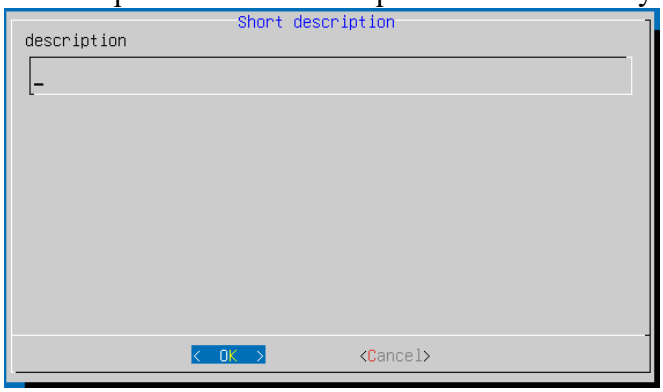


d. After this message has displayed for 30 seconds, you will be brought back to the KRMC On-Premise Virtual Console.

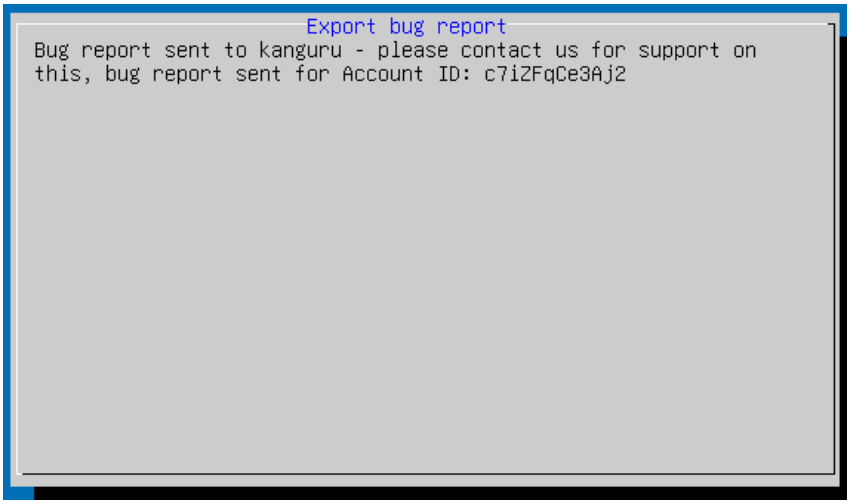
5. To export using **Send to Kanguru**:
   a. Press the **Up** and **Down** arrows until **Send to Kanguru** is selected and press **ENT**.



   b. You will be asked to provide a short description of the issue that you are experiencing.



c. After you complete your description and press **ENT**, you will receive a message stating that the bug report has been sent to support and you will be asked to contact support for assistance with this.



d. After this message has displayed for 30 seconds, you will be brought back to the KRMC On-Premise Virtual Console.

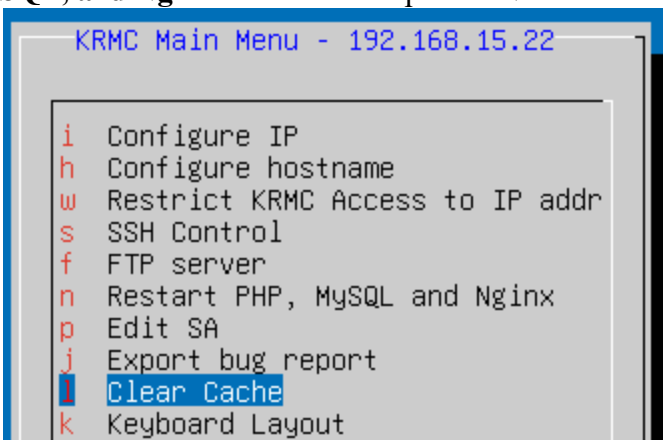
***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

Clear Cache

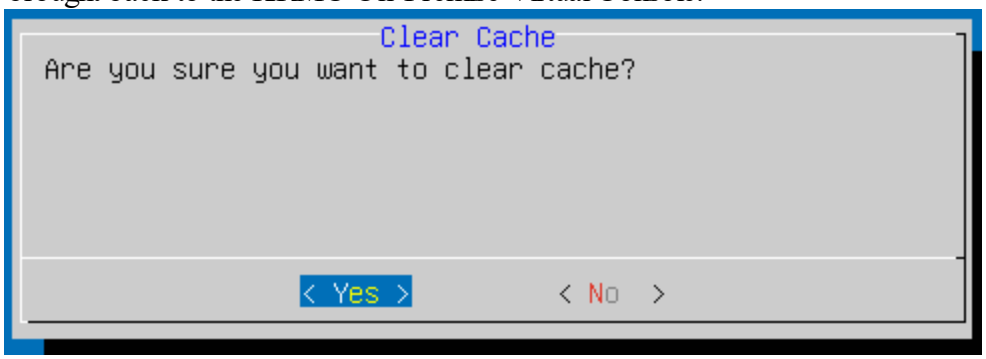
Clear Cache allows you to clear the web server cache, which can resolve any problems using the KRMC web interface (e.g. pages not loading, information not appearing, etc.). We strongly recommend contacting support if this does not grant access back to KRMC once completed.

To Clear Cache:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Restart PHP, MYSQL, and Nginx** is selected and press **ENT**.



2. You will have a display showing asking you to confirm you would like to clear the cache. If you would like to proceed, select **YES** and press **ENT**. After selecting **YES**, the screen will remain here as it attempts to clear the server cache. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.



***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

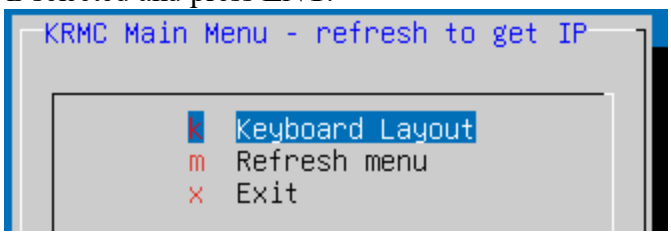
Keyboard Layout

Keyboard Layout allows you as the administrator to select the basic layout of the keyboard that you are using for navigation and settings for the KRMC On-Premise Virtual Console 69. This is the first step in Setting up KRMC for the first time 22 however can also be altered at any point after the setup is complete. The options available in this section are as follows:

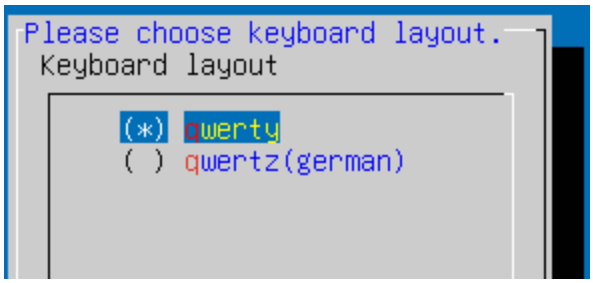
qwerty	This is the standard US keyboard layout and follows the top six letters (left to right) in the order of qwerty. This is the default option.
qwertz	This is an alternative keyboard layout commonly used with German keyboard layouts and follows the top six letters (left to right) in the order of qwertz.

To configure the Keyboard Layout:

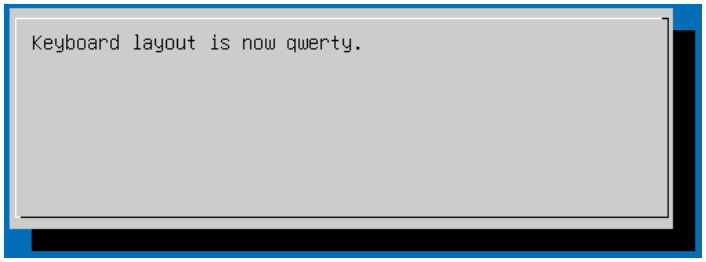
1. From the **KRMC On-Premise Virtual Console**, use the **Up** or **Down** arrows until you see **Keyboard Layout** is selected and press **ENT**.



2. You will have two options to choose from. Press the **Up** and **Down** arrows until the option you wish to select is highlighted and press the **Spacebar** to select the option. After selected, press **ENT**.



3. You will receive a message stating that the changes you have requested have been saved. This may last a minute or two but then you will be brought back to the **KRMC On-Premise Virtual Console**.



***Note**: If at any point you do not want to proceed with the confirmation of the settings, you can press ESC on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

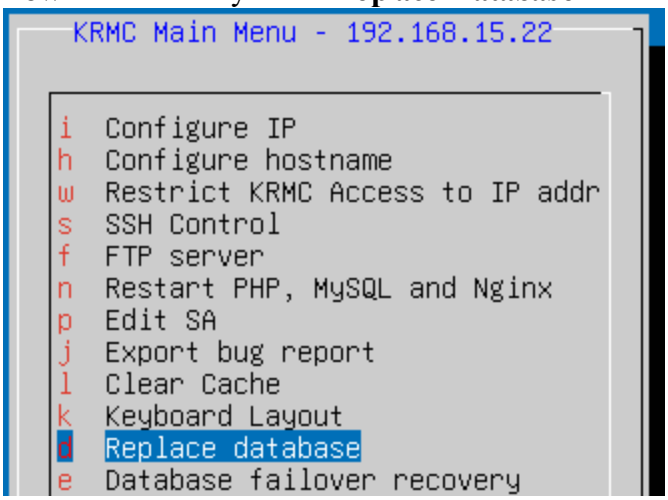
Replace database

Replace database allows you to migrate your previous installation of KRMC 5, 6, or 7 to the new KRMC 9 server. This process will require access to both the original KRMC 5, 6, or 7 server as well as the new KRMC 9 server instance. For steps on how to perform this, refer to Migrate from KRMC 5, 6, or 7 219.

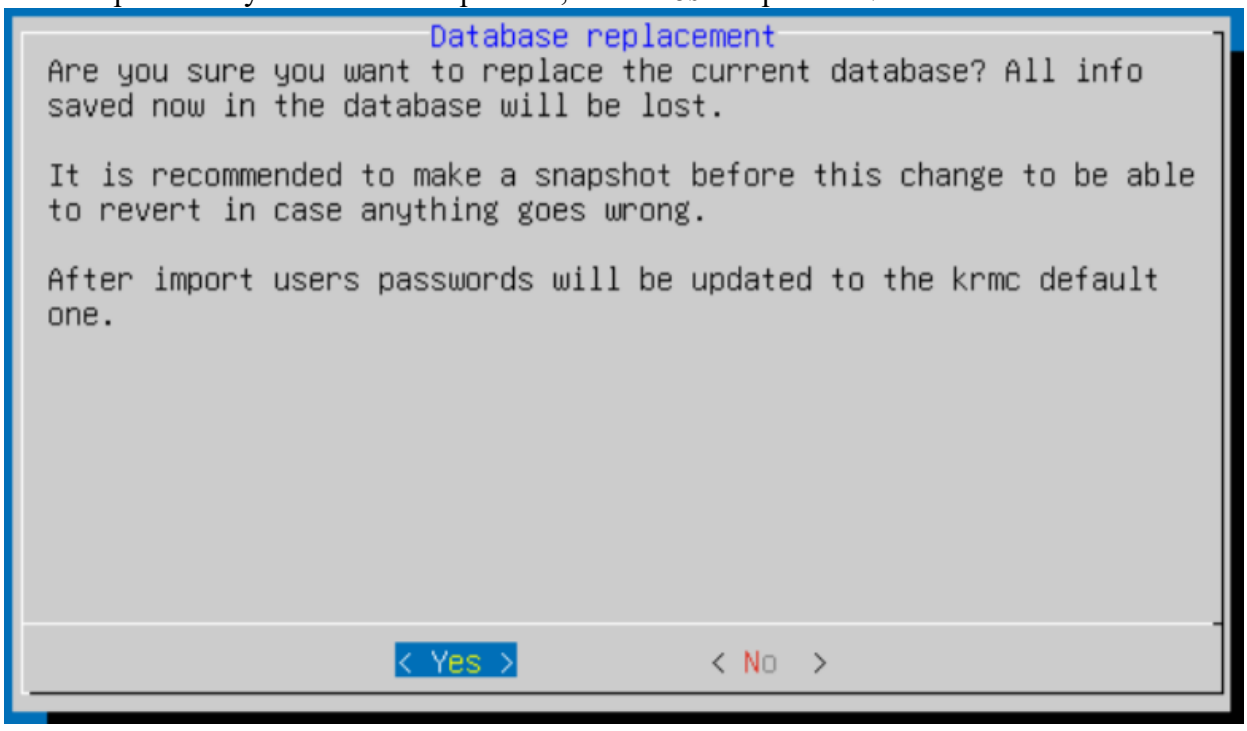
If you are looking to migrate from a KRMC 8 server or different instance of KRMC 9 to a new version, refer to Migrate from a different KRMC VM 216.

To access Replace Database:

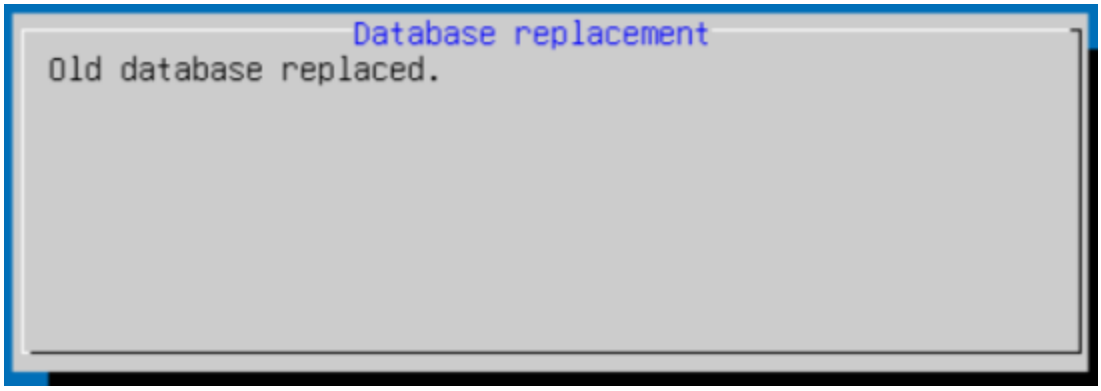
1. Use the **Up** and **Down** arrows until you see **Replace Database** is selected and press **ENT**



2. You will receive a message asking if you are sure you would like to proceed with this database replaced. If you would like to proceed, select **Yes** and press **ENT**.



3. This process may take a few minutes however after this is completed you will receive a message stating "**Old database replaced**". Once this appears, you will be brought back to the **KRMC On-Premise Virtual Console**.



Note: *The 1024bit certificates that are used in KRMC versions 5, 6, and 7 are not compatible with KRMC 9. Due to this, we recommend you have the KDM application on your drives fully updated before performing any migration like this. The latest version of KDM are able to request new certificates allowing the drives to maintain their communication with KRMC.*

Database failover recovery

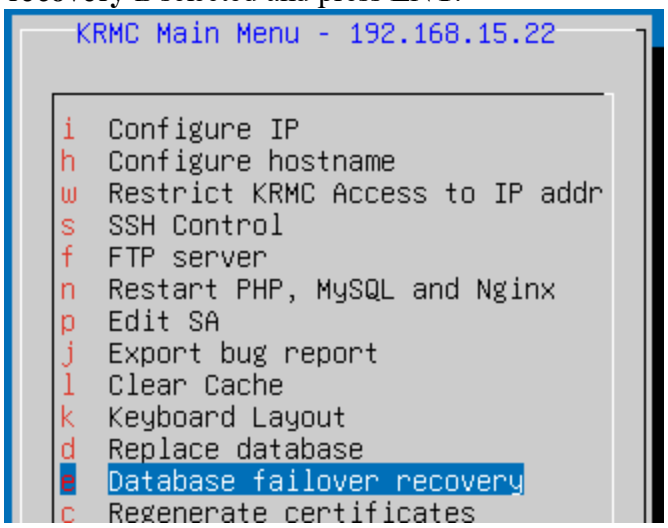
Database failover recovery allows you to restore your database in the case database corruption occurs. We recommend contacting support prior to performing the steps here as well as making a snapshot of your KRMC 9 server.

There are two locations your database backup can be located:

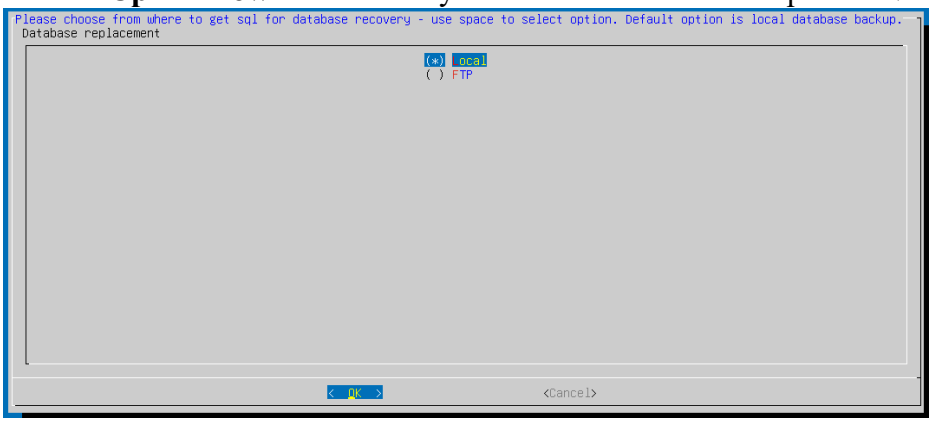
Local	The KRMC virtual appliance automatically saves up to 7 backup database files locally. These backups are performed once every 24hrs. After 7 backups are performed, the next backup replaces the oldest and that pattern continues to repeat.
FTP	If you have configured your FTP server 86 settings, you will receive database backups once every 24hrs on your FTP that you would be able to use for this recovery.

To perform a database failover recovery:

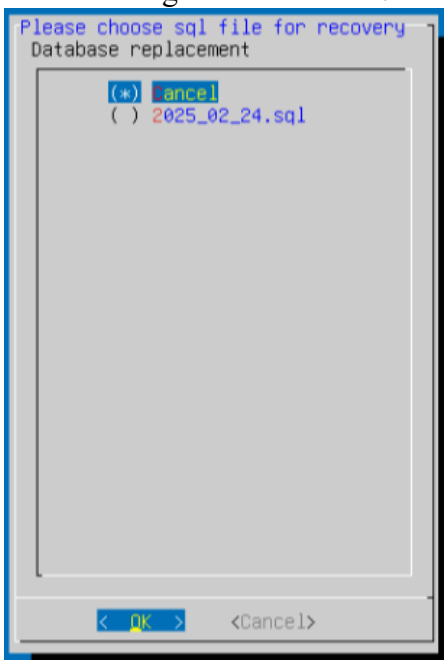
1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Database failover recovery** is selected and press **ENT**.



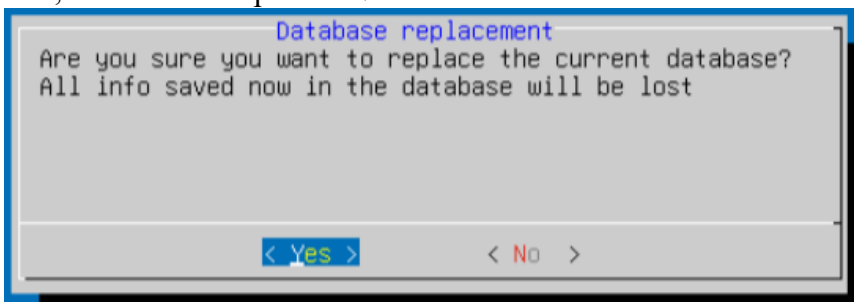
2. To use **Local**
   a. Press the **Up** and **Down** arrows until you see local is selected and press **ENT**.



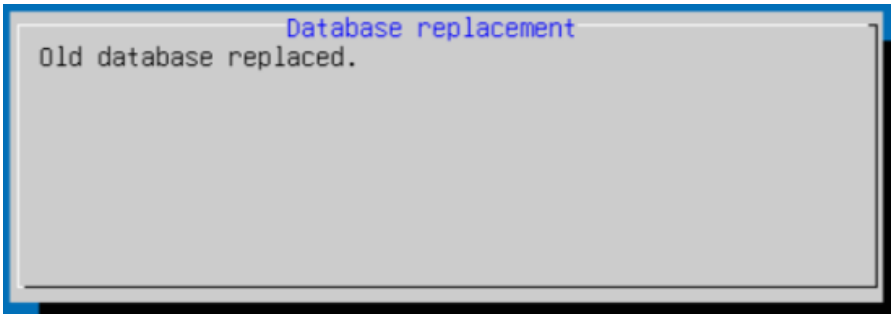
b. You will be displayed a list of backups that you will be able to choose from. Use the **Up** and **Down** arrows to navigate through the list of backups and press the **Spacebar** when you see the backup you are looking to use. Press **ENT** to continue.



c. You will receive a pop-up stating "**Are you sure you want to replace the current database? All info saved now in the database will be lost**.". If you would like to proceed, select Yes and press **ENT**.

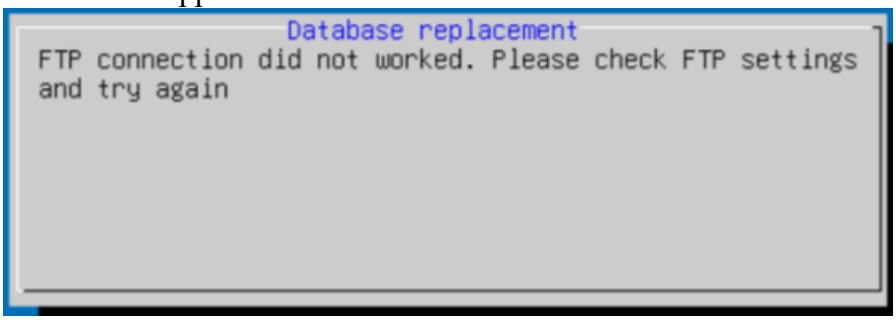


d. After a process that may take a few minutes, you will receive a message stating "**Old database replaced**". Once this appears, you will be brought back to the **KRMC On-Premise Virtual Console**.

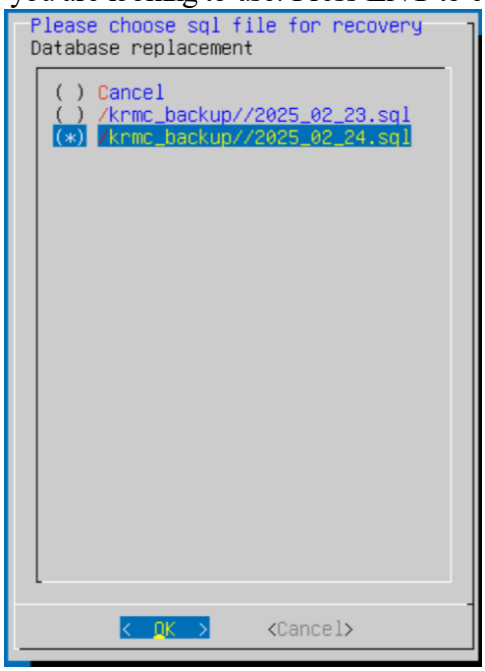


3. To use FTP
   a. Press the **Up** and **Down** arrows until you see ftp is selected and press **ENT**.

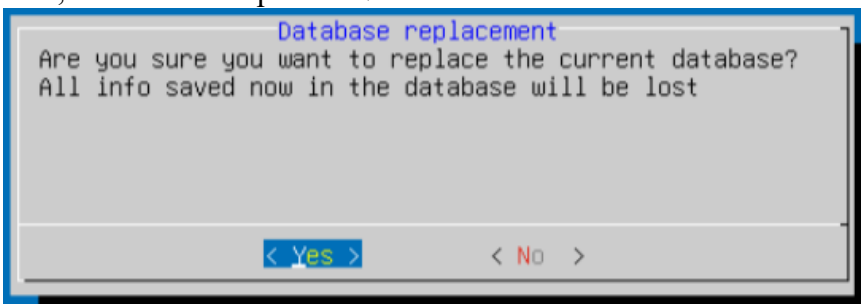
b. If you have not configured the FTP settings or the FTP server if not able to be reached you will receive the message "FTP connection did not work. Please check FTP settings and try again". If you did configure your FTP settings and confirmed it is able to be accessed, please contact support.



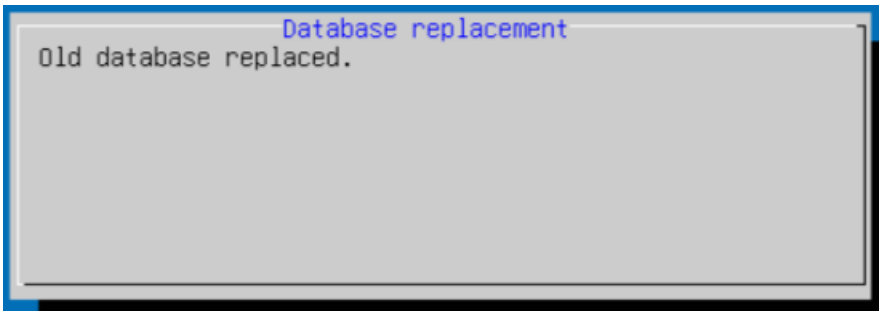
c. You will be displayed a list of backups that you will be able to choose from. Use the **Up** and **Down** arrows to navigate through the list of backups and press the **Spacebar** when you see the backup you are looking to use. Press **ENT** to continue.



d. You will receive a pop-up stating "**Are you sure you want to replace the current database? All info saved now in the database will be lost**.". If you would like to proceed, select Yes and press **ENT**.



e. After a process that may take a few minutes, you will receive a message stating "**Old database replaced**". Once this appears, you will be brought back to the **KRMC On-Premise Virtual Console**.



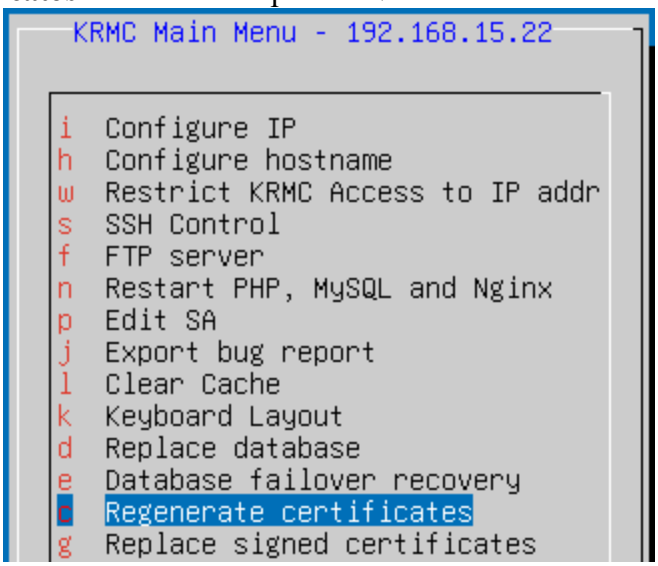
Regenerate Certificates

Regenerate Certificates allows you to create a new self-signed certificate for your KRMC server. This option is useful your current certificate expired or if you would like to remake the self-signed certificate.

If you are looking to apply your own signed certificate, you will need to first generate a signed certificate using the steps below then you can follow the steps on Replace signed certificates 105.

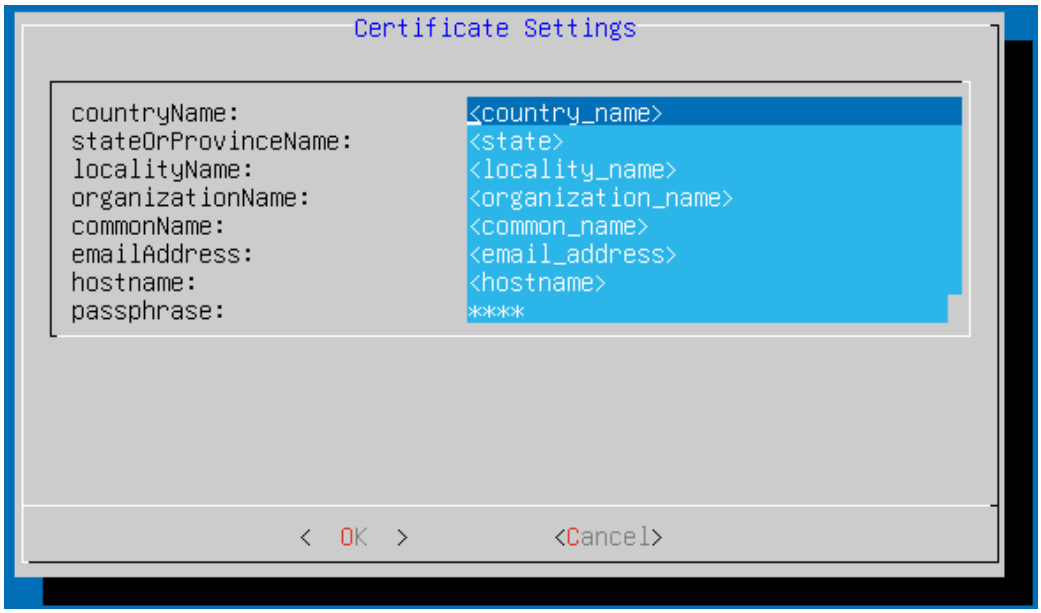
To Regenerate certificates:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Regenerate Certificates** is selected and press **ENT**.



2. After pressing **ENT** will be brought to the Certificate Settings Window. You will need to complete each field in order to proceed. Use the **Up**, **Down**, **Left**, and **Right** arrows to navigate between the options as well as **Backspace** or **Delete** to remove any default content that is displayed. ***Note**: All fields require at least 2-characters to be entered.*

CountryName	The country where the organization or individual is legally located.
StateOrProvinceName	The state or province where the organization or individual is legally located.
localityName	The city or town where the organization or individual is legally located.
organizationName	The company/organization name.
commonName	A field that identifies the domain name or entity the certificate is issued to, typically matching the website's domain name.
emailAddress	The email address of the administrator configuring your KRMC certificate.
hostname	The domain name or subdomain for which the certificate is issued.
passphrase	The password that you are setting on your KRMC certificate. This must be more then four characters in length.



3. After completing all of the required fields you can press **ENT** to continue. You will have a display showing the server certificate and client certificate has been replaced as well as the Nginx server has restarted. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.

Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press* ***ESC*** *on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

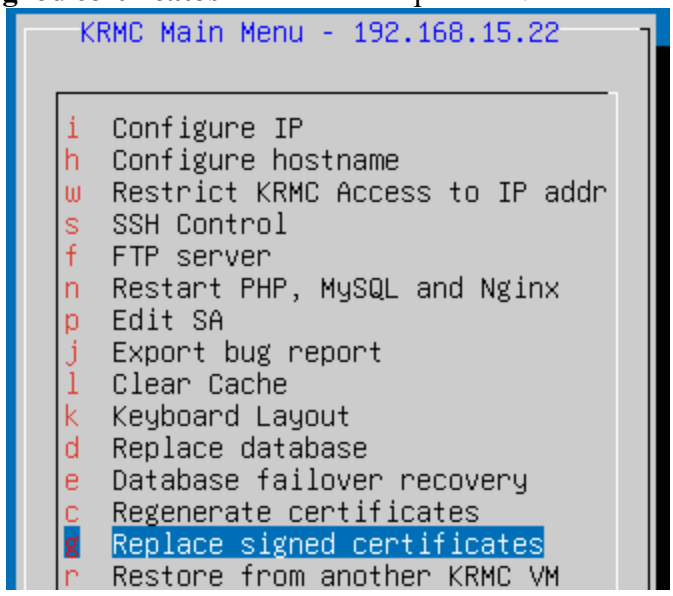
Replace signed certificates

KRMC On-Premise provides the ability to replace the self-signed certificate that you generate during your initial configuration of KRMC with your own signed certificate. For steps on how to perform this, refer to Steps to Import a Signed Certificate 224.

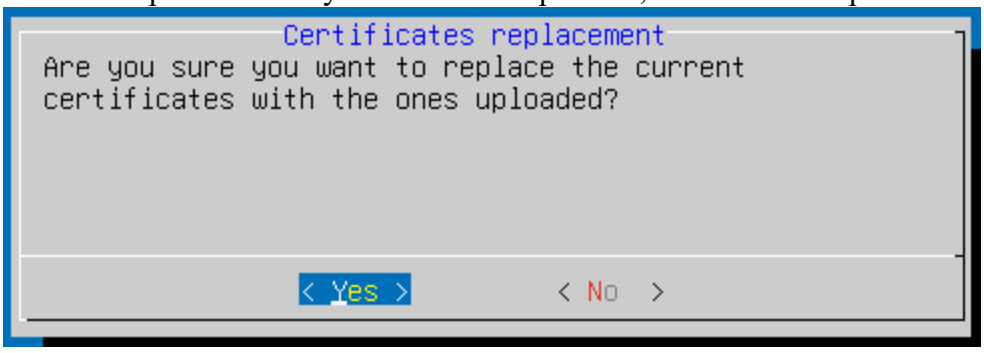
Note: *Before making any certificate changes we* ***strongly recommend*** *you make a snapshot/backup of your KRMC VM.*

To access Replace Signed Certificate:

1. Go to the KRMC On-Premise Virtual Console 69 and use the **Up** and **Down** arrows until you see **Replace signed certificates** is selected and press **ENT**.



2. You will receive a message asking "Are you sure you want to replace the current certificates with the ones uploaded?". If you would like to proceed, select **YES** and press **ENT**.



3. You will be notified that the certificate and key have been copied. Additionally, Nginx will have restarted. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.

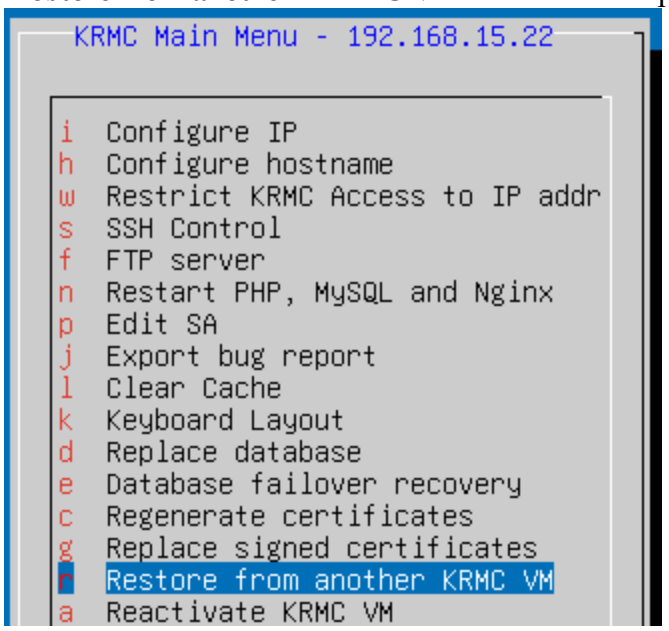
Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press* ***ESC*** *on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

Restore from another KRMC VM

If you currently have a KRMC 8 or KRMC 9 VM currently in your environment and you are looking to upgrade, we have provided a method for migrating your data from one KRMC instance to another using Restore from another KRMC VM. For steps on how to perform this, refer to Migrate from a different KRMC VM 216.

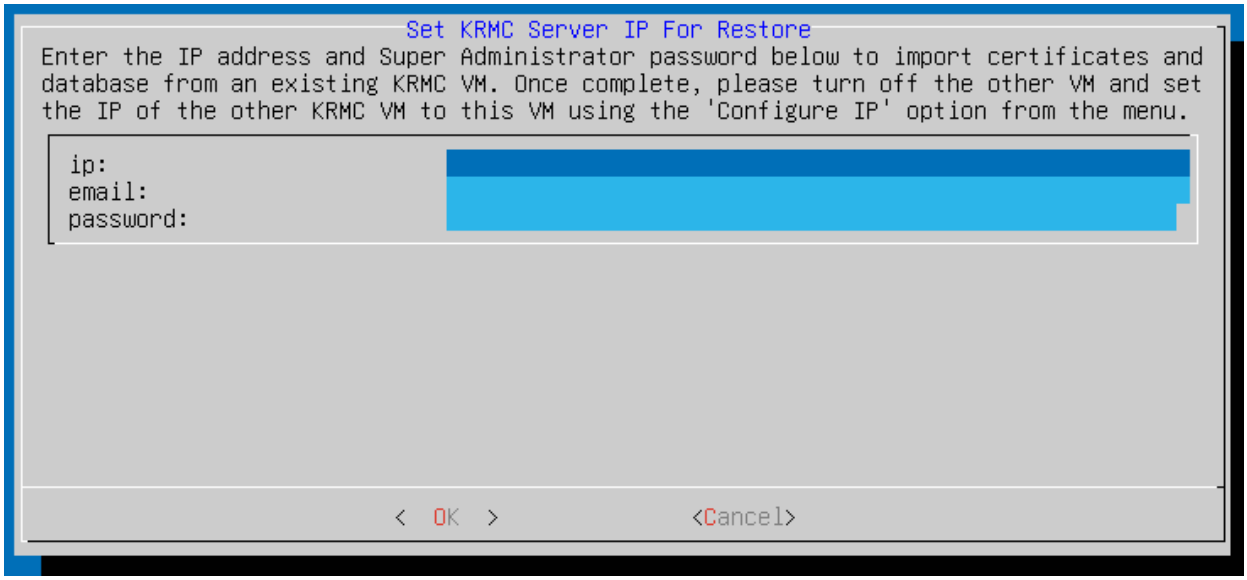
To access Restore from another KRMC VM:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Restore from another KRMC VM** is selected and press **ENT**.



2. A pop-up will appear with three fields that will need to be completed. After completing the fields, press **ENT**.

ip	The IP address of the first instance of KRMC (the KRMC server you are looking to pull data from).
email	The email address of the Super Administrator (SA) of the first instance of KRMC (the KRMC server you are looking to pull data from).
password	The password of the Super Administrator (SA) of the first instance of KRMC (the KRMC server you are looking to pull data from).

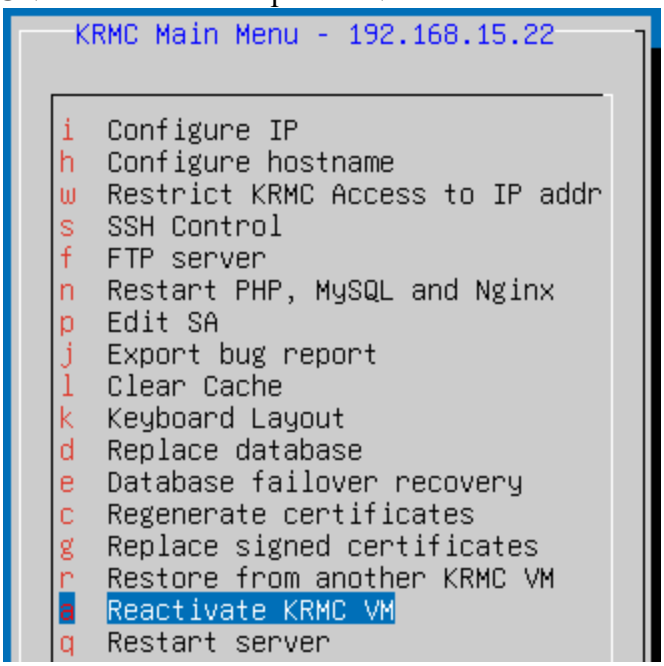

Set KRMC Server IP For Restore
Enter the IP address and Super Administrator password below to import certificates and database from an existing KRMC VM. Once complete, please turn off the other VM and set the IP of the other KRMC VM to this VM using the 'Configure IP' option from the menu.
ip:
email:
password:
< OK >
<Cancel>

Reactivate KRMC VM

After you perform the steps in Restore from another KRMC VM, the original KRMC VM instance will no longer be able to be accessed. Any attempts to access this version of KRMC using a browser will result with a messaged stating "Stopped". If there was an issue with the migration process and you need to gain access back to this instance of KRMC, you will need to use the option Reactivate KRMC VM.

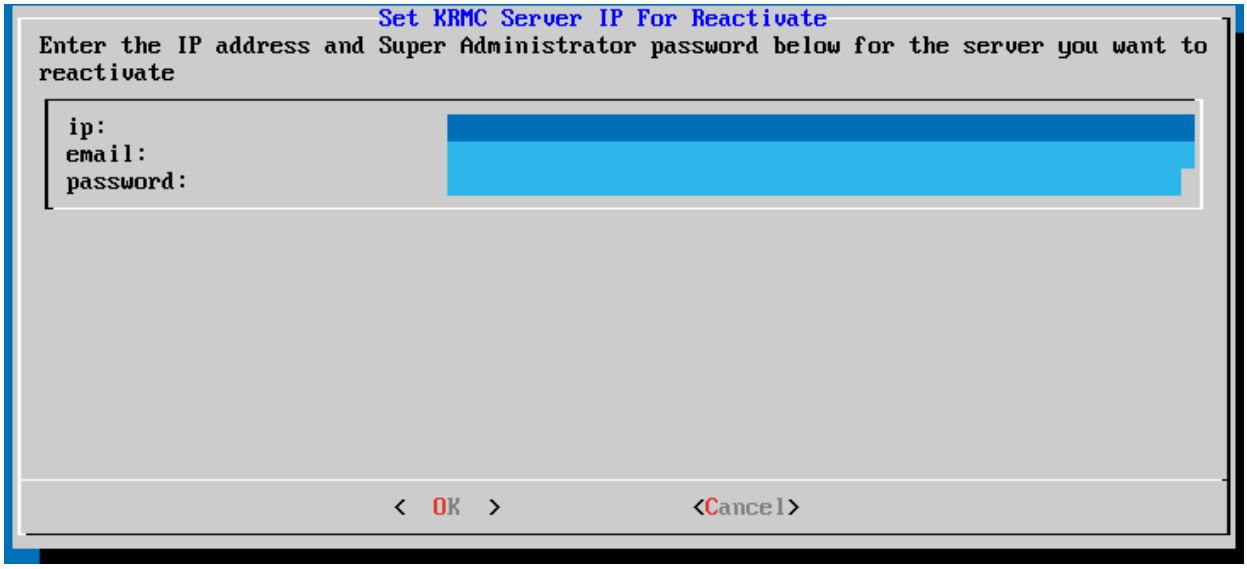
To Reactive the KRMC VM:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Reactivate KRMC VM** is selected and press **ENT**.

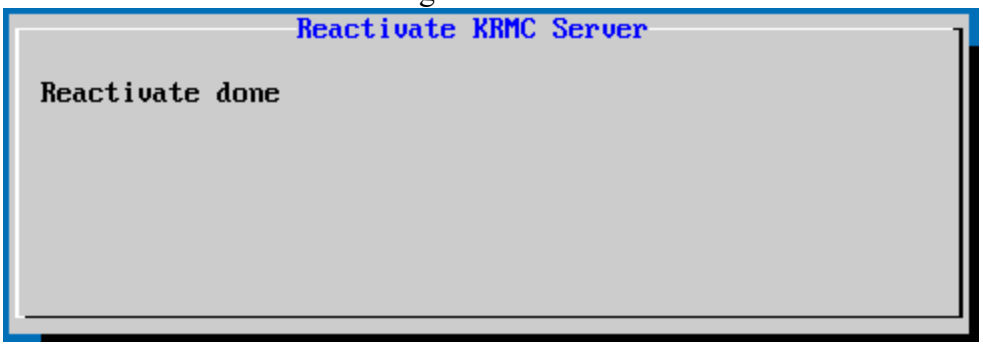


2. A pop-up will appear with three fields that will need to be completed. After completing the fields, press **ENT**.

ip	The IP address of the first instance of KRMC (the KRMC server you are looking to pull data from).
email	The email address of the Super Administrator (SA) of the first instance of KRMC (the KRMC server you are looking to pull data from).
password	The password of the Super Administrator (SA) of the first instance of KRMC (the KRMC server you are looking to pull data from).



3. You will receive a message stating "Reactivate done". This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console. You will now be able to gain access to this instance of KRMC again.



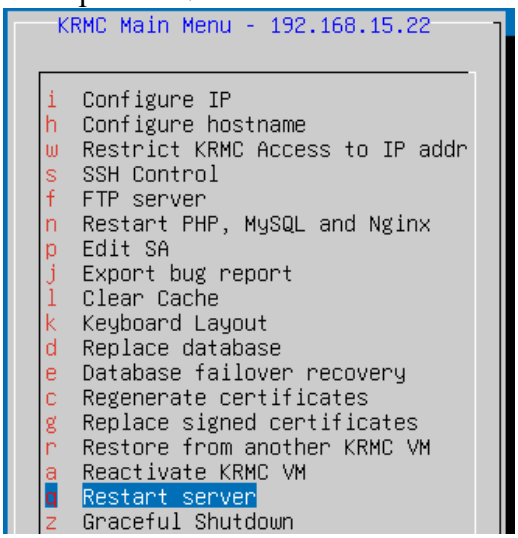
Restart server

Restart Server gracefully restart the KRMC virtual appliance. This will allow the system to complete any queued data transfers, pending tasks and/or processes before shutting down and restarting the KRMC VM.

Note: *It is recommended to use the KRMC virtual appliance's Restart server instead of the virtual machine software's Restart Guest function.*

To Restart server:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Restart Server** is selected and press **ENT**.



2. You will be asked to confirm you would like to restart the server. Select **Yes**, then press **ENT**.

3. After you press **ENT**, you will see your server startup prompts. This could take a minute or two to complete and once successful you will be brought back to the **KRMC On-Premise Virtual Console**.

Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

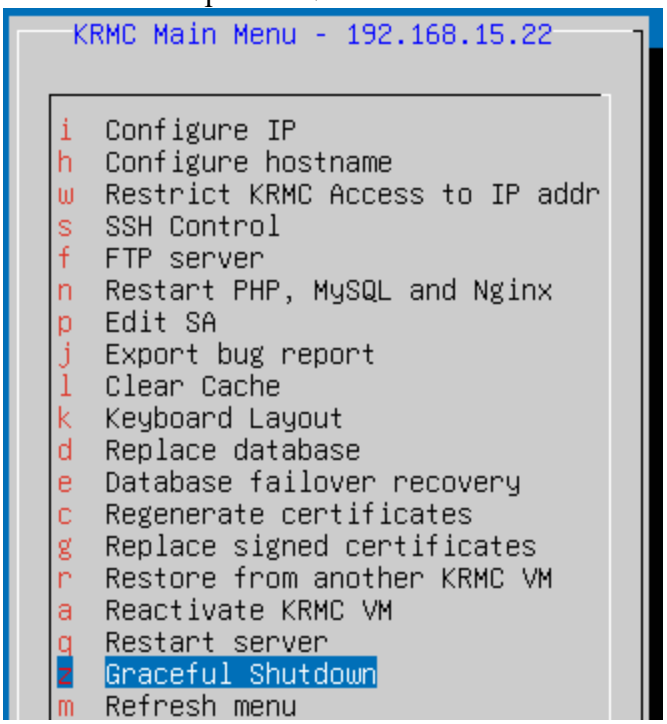
Graceful shutdown

A graceful shutdown will allow the system to complete any queued data transfers, pending tasks and/or processes before shutting down the KRMC VM.

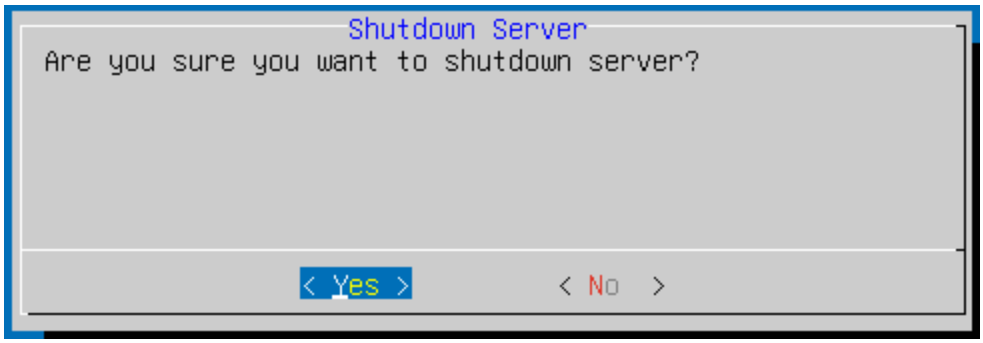
Note: *It is recommended to use the KRMC virtual appliance's Graceful shutdown instead of the virtual machine software's Shutdown Guest function.*

To Gracefully shutdown:

1. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see **Graceful Shutdown** is selected and press **ENT**.



2. You will be asked to confirm you would like to shut down the server. Select **Yes**, then press **ENT**.



3. After you press **ENT**, you will see your server will start to shutdown. Typically this takes only a few seconds to complete.

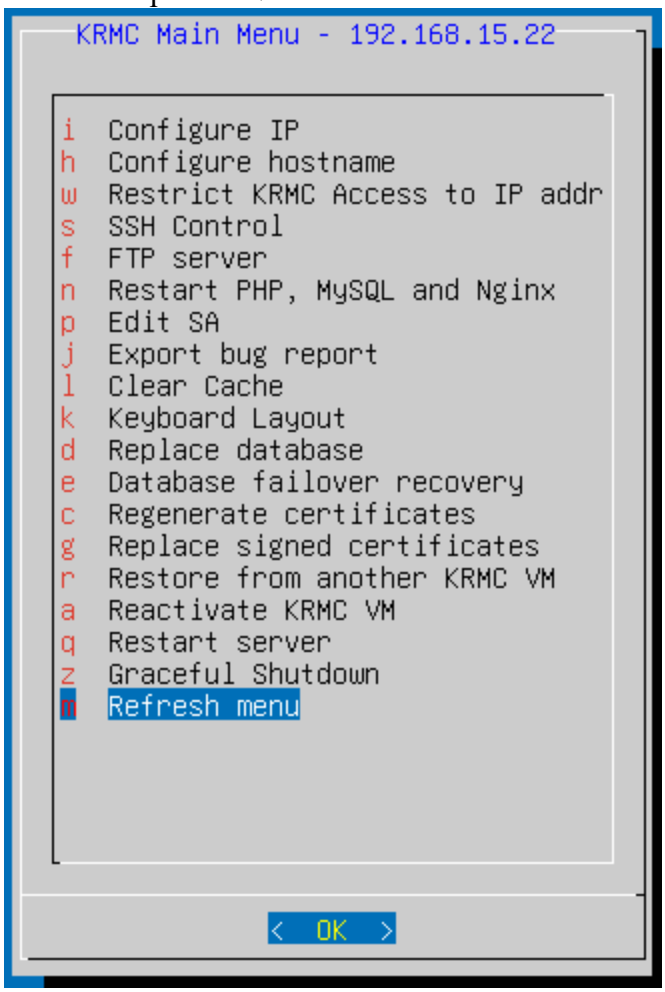
Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press **ESC** on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*

Refresh menu

Refresh menu will refresh the KRMC On-Premise Virtual Console menu display. This is helpful if you make changes to the IP address using Configure IP and the changes are not displayed at the top of the menu.

To Refresh the menu:

1. From the KRMC On-Premise Virtual Console, use the **Up** or **Down** arrows until you see **Refresh Menu** is selected and press **ENT**.



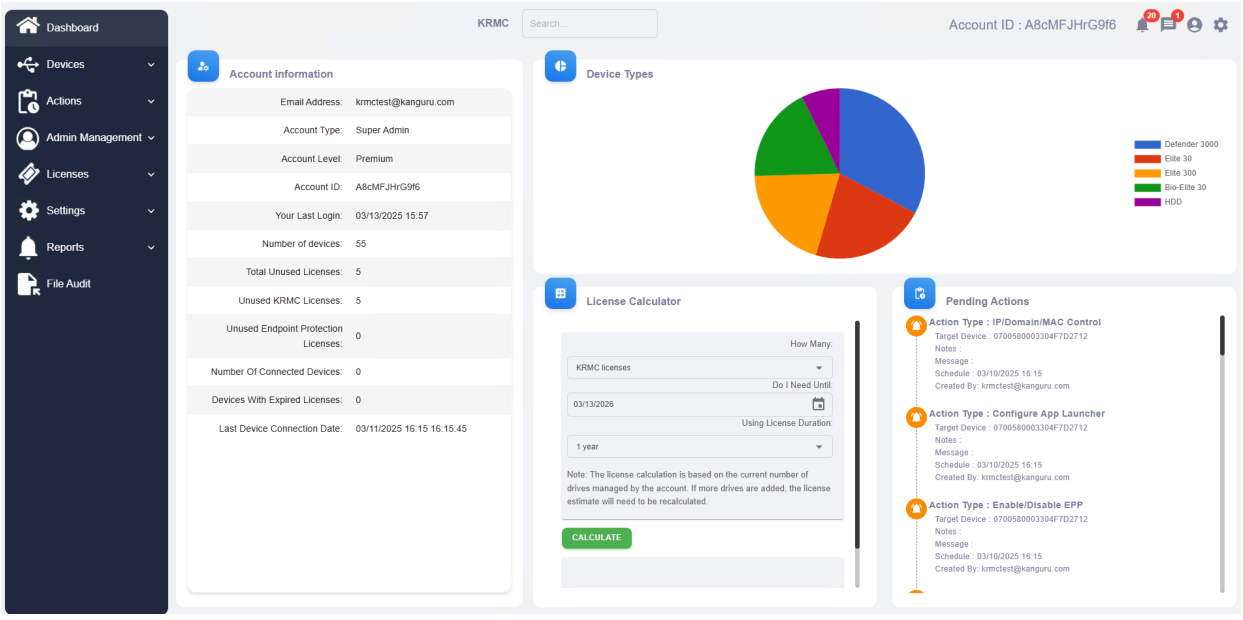
2. After a second or two the display should refresh and you will find that the top menu option will be highlighted instead Refresh Menu. When this occurs, the refresh is completed.

Dashboard

7

When you login to KRMC On-Premise, you are automatically directed to the KRMC On-Premise dashboard. The KRMC On-Premise dashboard page provides you with a system overview displaying information such as notifications from iStorage Kanguru, the time of your last login, your devices, your licenses, and of any successful, pending or failed actions, etc. The Dashboard is customizable so what is displayed may appear different then what is in the image below. With that said, the default Dashboard view consists of the following:

Account Information 115	The general information regarding your KRMC On-Premise account will appear such as your Account ID, Account Type, and Usable Licenses.
Device Types	This chart shows the drive breakdown of all drives types that are on your KRMC account. You are able to hover over each section to obtain the exact number.
License Calculator 165	The License Calculator allows you to determine how many licenses would be required to manage all drives currently on your account. For more information on this tool, please refer to the License Summary 165 page.
Pending Actions	This shows all pending actions on your KRMC account.



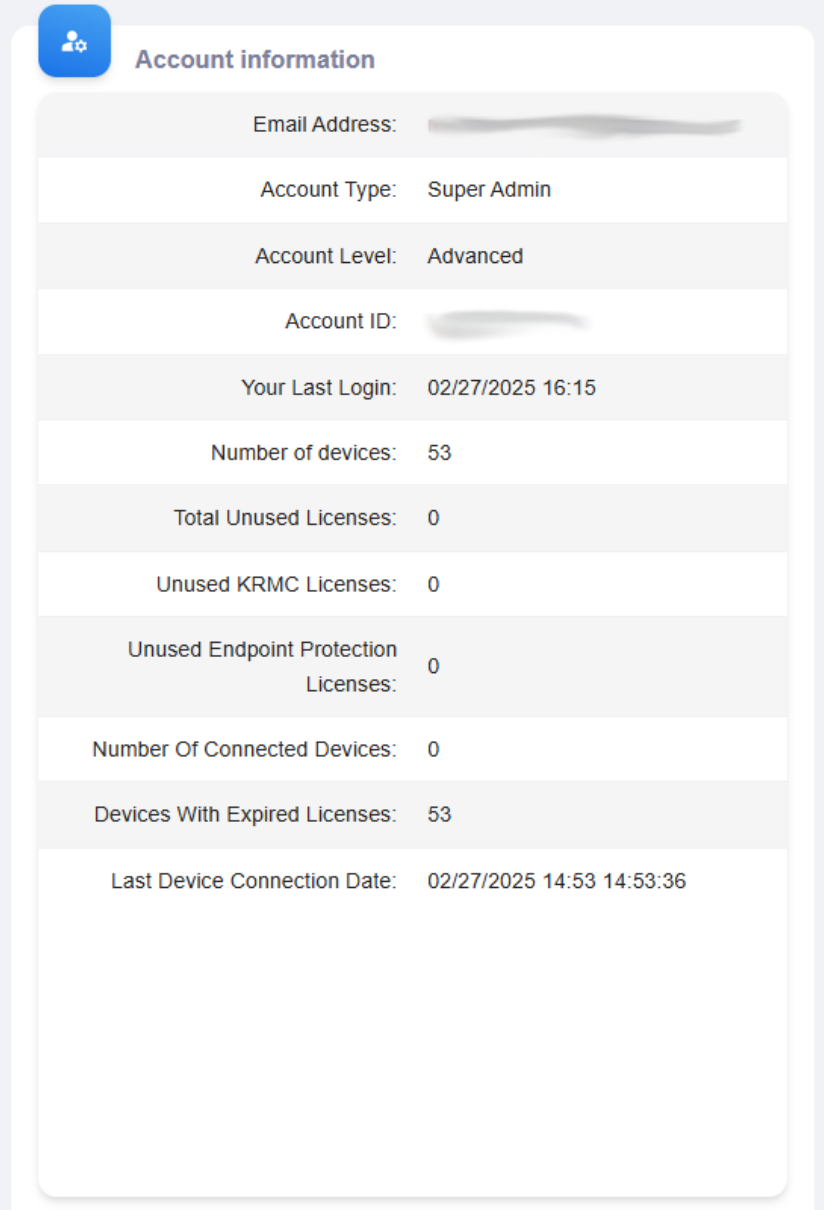
Dashboard

7

Account Information

Account Summary displays an overview of your KRMC On-Premise account. It contains the following information:

Email Address	The email address of the account that is currently logged into KRMC.
Account Type	The status of the KRMC account. This includes: Super Administrator, Regular Administrator, and Auditor. For more information on the different account types, please refer to Admins, Auditors, and Groups 62.
Account Level	This indicates if the account is Advanced, or Premium.
Account ID	The account-level Account ID used to register devices to this account.
Your Last Login	The date that the current Administrator last logged into the console.
Number of Devices	The total number of devices registered with this account.
Total Unused Licenses	The total number of KRMC and Endpoint Protection licenses available that can be assigned to a device.
Unused KRMC Licenses	The Number of KRMC licenses available that can be assigned to a device.
Unused Endpoint Protection Licenses	The Number of Endpoint Protection licenses available that can be assigned to a device.
Number of Connected Devices	The number of devices that are currently being used and communicating back to the server. ***Note**: Devices running in offline mode will not report this information.*
Devices with Expired Licenses	The number of devices that currently have expired licenses. Devices with expired licenses will not be able to receive remote actions from the KRMC On-Premise server. It is strongly recommended to assign a new license to any device with an expired license.
Last Device Connection Date	The most recent date that a device communicated with the KRMC On-Premise server.

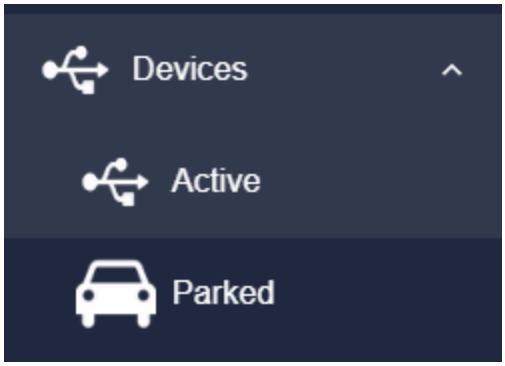

Account information
Email Address:
Account Type: Super Admin
Account Level: Advanced
Account ID:
Your Last Login: 02/27/2025 16:15
Number of devices: 53
Total Unused Licenses: 0
Unused KRMC Licenses: 0
Unused Endpoint Protection Licenses: 0
Number Of Connected Devices: 0
Devices With Expired Licenses: 53
Last Device Connection Date: 02/27/2025 14:53 14:53:36

Device Page

8

The **Devices Page** provides you with options for viewing and managing your Defender devices. You can navigate to the Active or Parked options by clicking on the icons or options on the navigation bar.

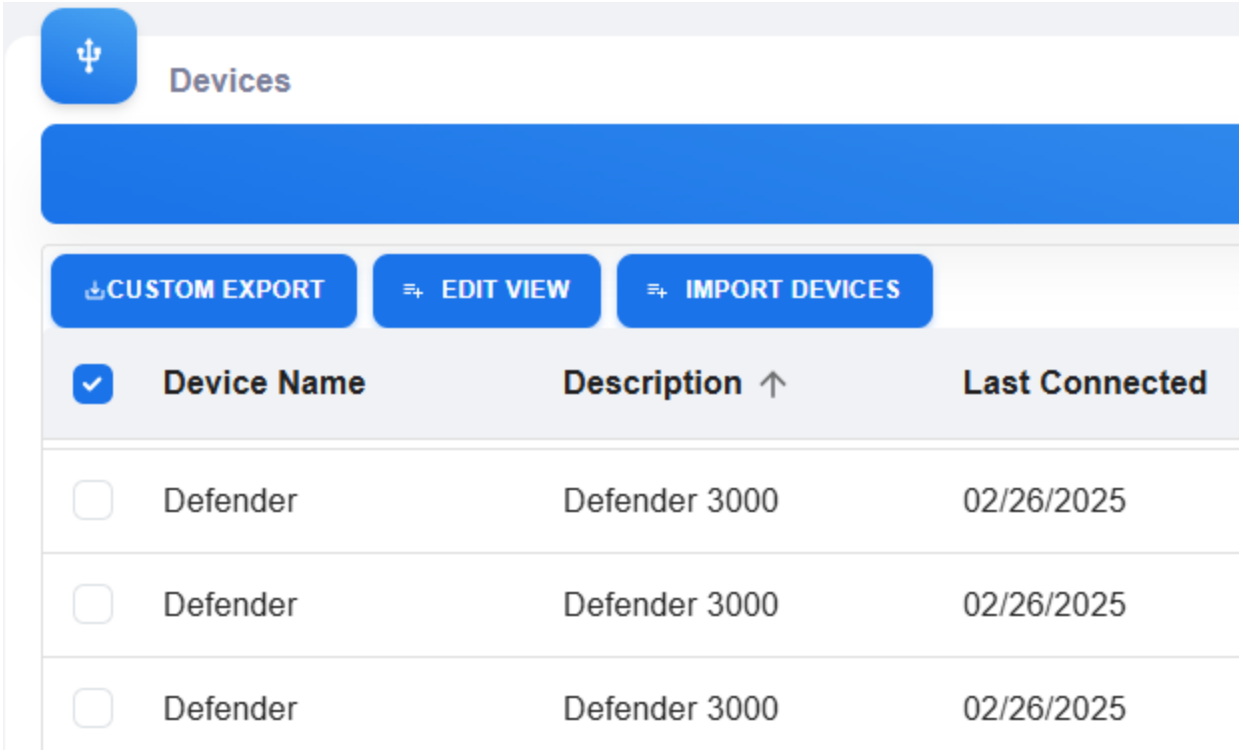
Active 118	Displays all active devices on your KRMC account. You are able to send actions to selected devices, change device contact information, export the device list, etc. ***Note:*** *No Parked or Deleted devices appear in this list.*
Parked 136	Displays all drives that have been parked on your KRMC account. You are able to make the drives active again, export the device list, and more.



Device Page 8

Active

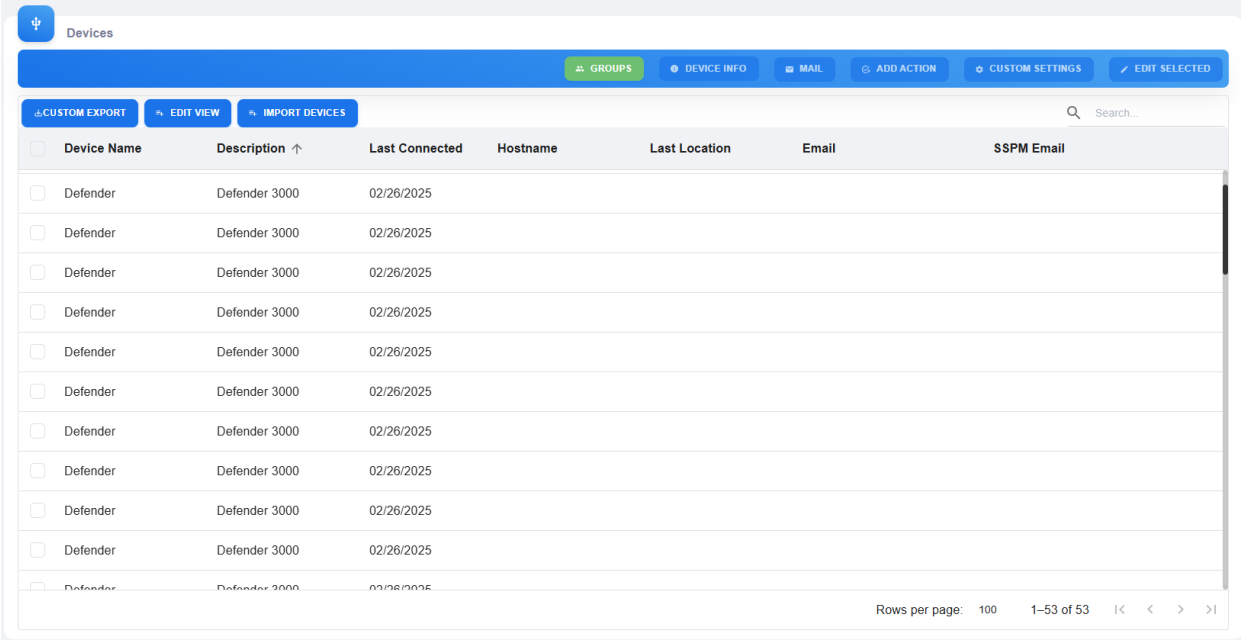
The **Active** device page provides you with options for viewing and managing your Defender devices. A device can be selected by using the checkbox on the left side column. If you are looking to select multiple devices you can either check the boxes next to each device or select the checkbox on the title bar.



Groups 120	Allows the KRMC account to view all devices within the selected group.
Device Info 121	KRMC accounts are able to view device history and previously requested SSPM codes. ***Note:*** *This option is not available when multiple devices are selected.*
Mail 122	You can send an email from KRMC to the selected device(s).
Add Action 124	KRMC accounts with permissions are able to send remote actions to the selected device(s).
Custom Settings 125	Devices are able to have settings customized if required. These settings would differ from those set from the Global Device Settings or Group Provisioning Profile.
Edit Selected 126	The contact information and general device information is able to be changed.
Custom Export 131	KRMC with the correct permissions are able to export the Device list for auditing purposes.
Edit View 133	Provides the ability to change which columns are displayed on your Device list.
Import Devices 135	Allows you to manually import devices into your KRMC server.

Device Page

8



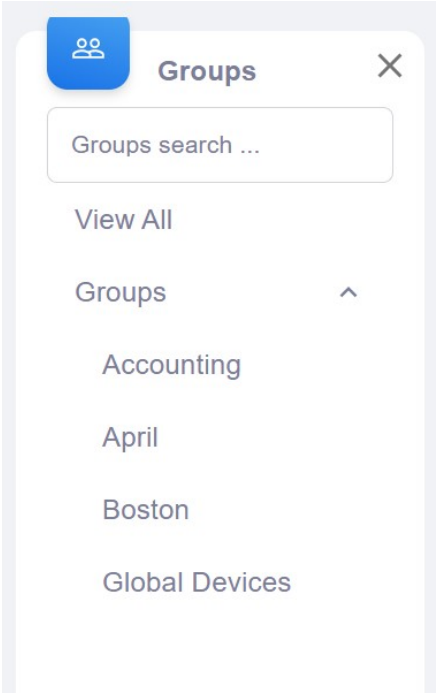
Device Page

8

Groups

Groups, can provide the Super Administrator (SA) with increased control over permissions, requirements, and customizations with their drives. If your KRMC account has groups, you can sort your device list by selecting a group using the Groups button. ***Note:*** *SA and Administrators can view all devices and groups if they have the permission "Can See All Devices" located under Advanced Account Abilities. For more information on Admin permissions, please look at* *Edit Admin Permissions* 147.

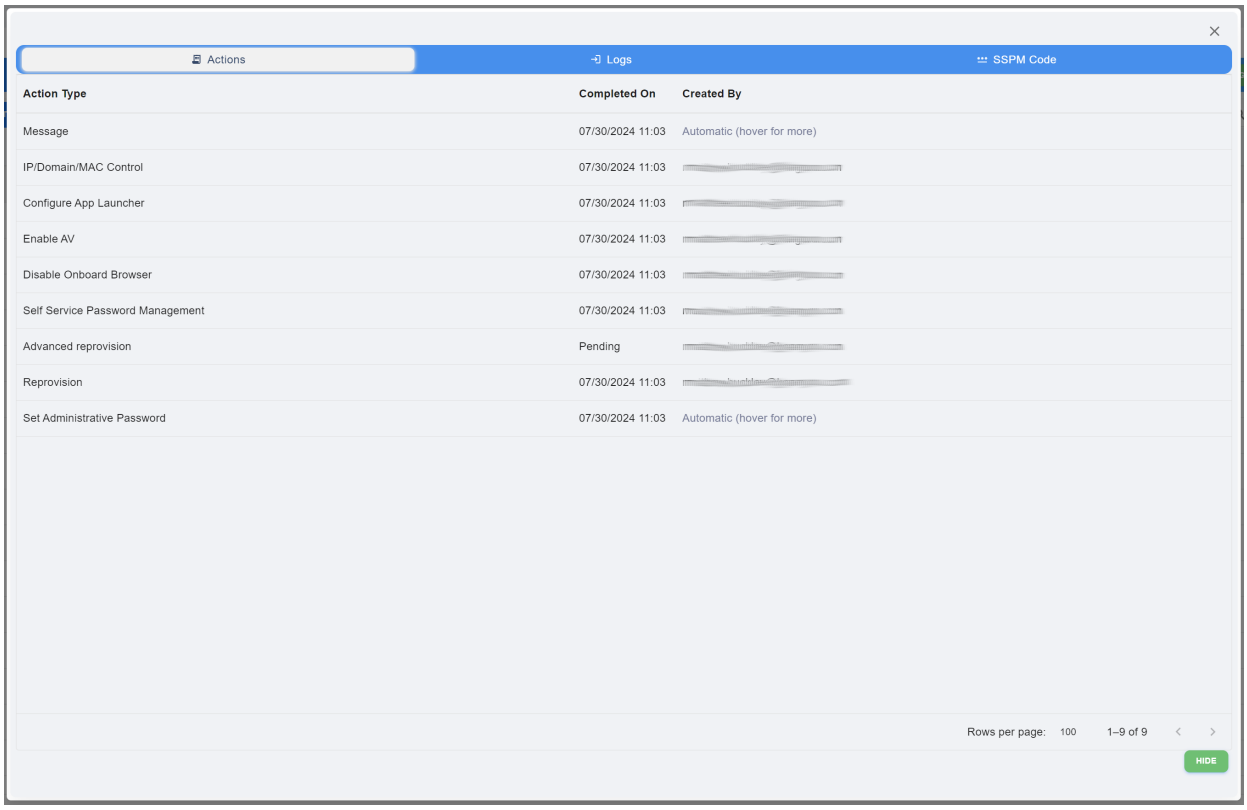
View All	Displays all devices registered with this KRMC On-Premise account in the Device List.
Group	Displays a list of all devices assigned to that group in the Device List. If your account does have any groups, you can select the title "Groups" which will display all groups which can then be selected.



Device Info

Device Info provides basic information for each device in a three tab popup. ***Note:*** *This option is not available when multiple devices are selected.*

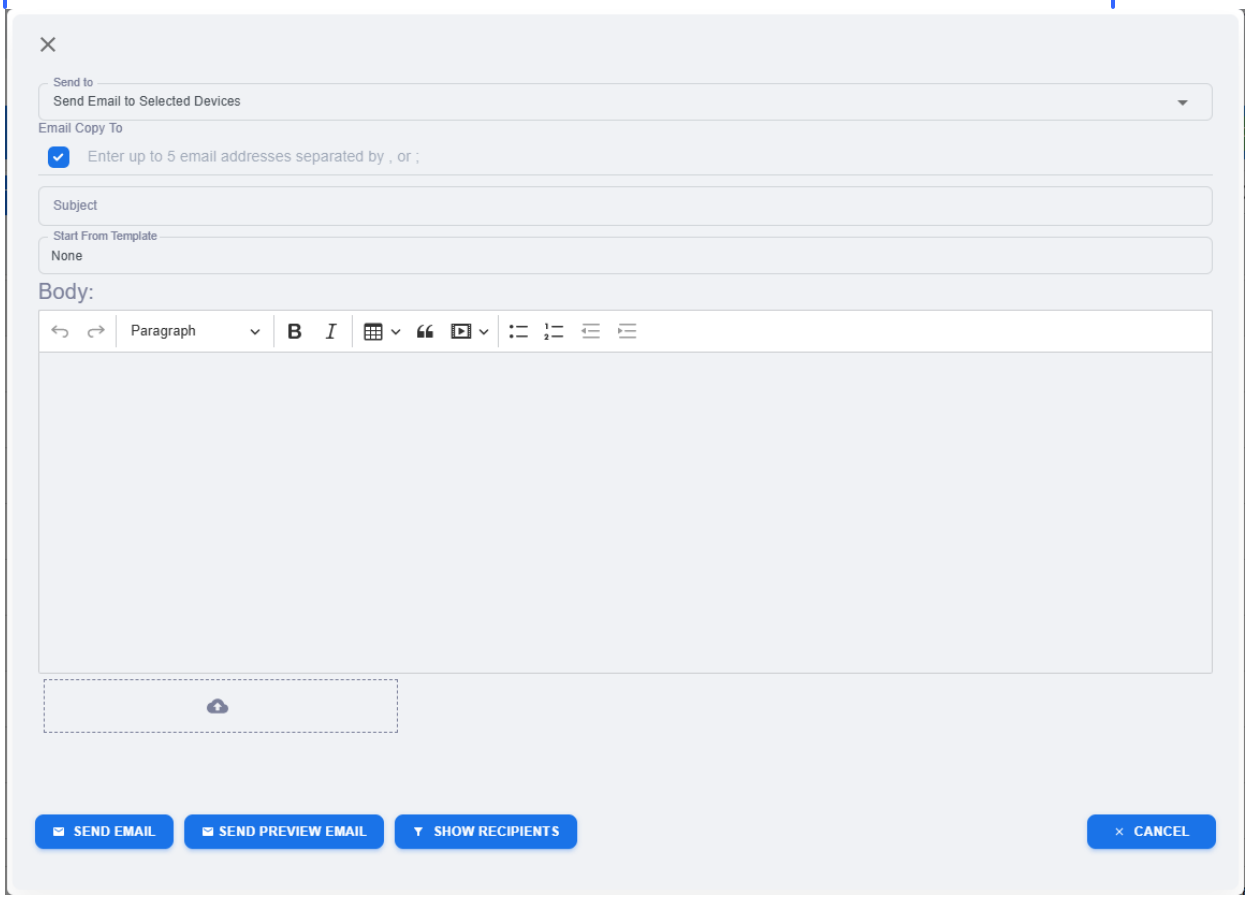
Actions	This tab provides a list of the action history for the device. You are able to see the action types, when the action was completed on (if it is still pending, it will be indicated as such), and which admin created the action for the device. If the action was an automatic action, it is response to settings provided through Global Device settings or Group Provisioning Profile.
Logs	This tab tracks all login attempts on your drive. ***Note:*** *This only tracks instances where the drive is able to communicate with KRMC and does not contain a record for any offline login attempts.*
SSPM Codes	This tab provides the most recent SSPM code issued to the drive as well as the current status of SSPM on the drive. If an end user is unable to receive the SSPM emails, we highly recommend checking email settings to determine if emails are being caught by the SPAM filters. If still no emails are coming through, the admin will be able to provide the user the code from this location.



Mail

Clicking the **Mail** button will open the Send Email window. Here you can send notification emails to KRMC On-Premise device user(s) and up to five CC'd addresses. Note: This is only available if you configured your Mail Server 194 on KRMC On-Premise.

Send To	Email recipients are limited to end user email addresses found in either Contact Information associated with a registered KRMC On-Premise device, or an SSPM email ID.
All users with contact info	This will send to all email addresses listed as Contact Info for a registered KRMC On-Premise device.
All users with SSPM email updated in system	This will send to all associated Self Service Password Management email addresses.
Send Email to Selected Devices	This will send to the email address listed in the Contact Info for a selected device.
Email Copy To	CC up to five additional email recipients. Copy email addresses do not need to be associated with a KRMC On-Premise device or SSPM.
Subject	The subject of the email that is being sent.
Start From Template	If you have created your own email templates 192, you can use this feature to select one of those templates to send to the selected users.
Body	The main content of an email message, which is where the sender writes their actual message, including text, images, links, and any other information intended for the recipient to read.
Upload a File	This allows you to attach a file to the email you are sending. The max file size allowed for this is 10MB Supported file formats include: DOC, DOCX, EPUB, ZIP, GZIP, JSON, PDF, TXT, JPG,, PNG, PSD, EPS.
Send Preview Email	Sends a preview email to the Admin that is currently logged into KRMC and drafting the email.
Send Email	Sends the email to all recipients.
Show Recipients	Shows a list of all the selected recipients (both email address and drive serial number).
Cancel	The actions creation is canceled.


Send to
Send Email to Selected Devices
Email Copy To
Enter up to 5 email addresses separated by , or ;
Subject
Start From Template
None
Body:
Paragraph
SEND EMAIL
SEND PREVIEW EMAIL
SHOW RECIPIENTS
CANCEL

Add Action

Add Action allows you to create an action that is executed on the selected drive managed by your account. If you are looking to send this action to multiple drives, you can select the drives using the checkbox on the left side of the device list. The actions available to the Regular Administrator (RA) is dependent on their permissions as defined under Edit Admin Permissions 147. For a full list and description of actions available, please refer to Remote Action List 206.

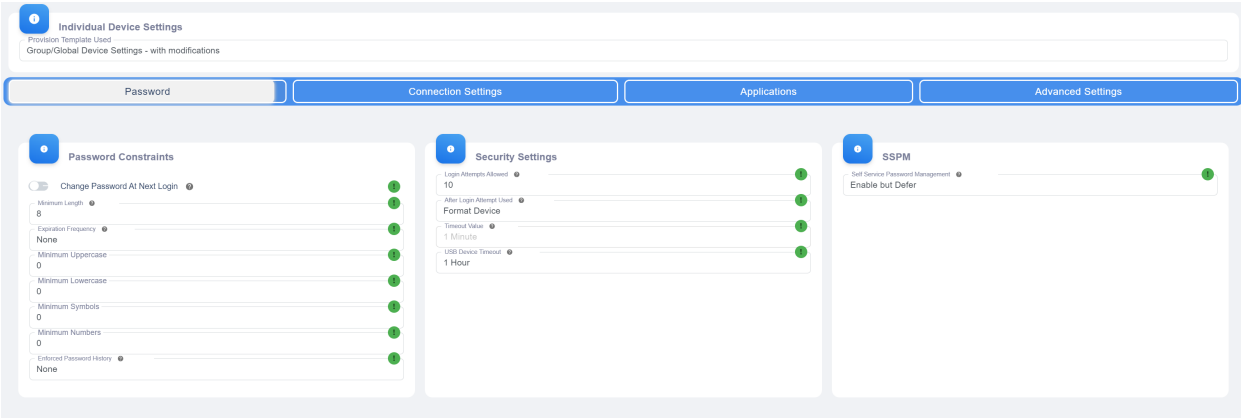
If you are looking to send an action to all devices, please look at Global Actions 142.

The default fields that will be available for you are as follow:

Select Action	This allows you to select the action that you are trying to send to all devices within this group. ***Note:*** *Depending on the action selected, the fields below may change.*
Message	A message is something that is displayed to the end user once the actions is received by the device.
Notes	This is an internal note about the action. This is not displayed to the end user.
Run this action on specific date and time	By default, a new action is scheduled to execute the next time the device is seen by the KRMC On-Premise server. If you want to delay the action until later, you can select Run this action on specific date and time and set a future date and time when the action can be executed. ***Note:*** *A scheduled action may not occur at the exact date and time set here. The action will be executed the next time the device communicates with KRMC On-Premise after the scheduled date and time.*
Create	This creates the action based on the options selected above.
Cancel	The actions creation is canceled.

Custom Settings

Custom Settings provides each drive the ability to have a security profile that is different then that set by the Global Device settings or the Group Provisioning Profile. In general it is not recommended to alter individual drive settings as it may lead to confusion with your predefined settings however if needed you can. An example of this being useful would be if an employee would need to use your device offline for an extended period of time. If you hover your mouse over the red icon, you will be shown what the setting was prior to the change. For more information on the settings and options available within this option, please refer to Global Device Settings 171.



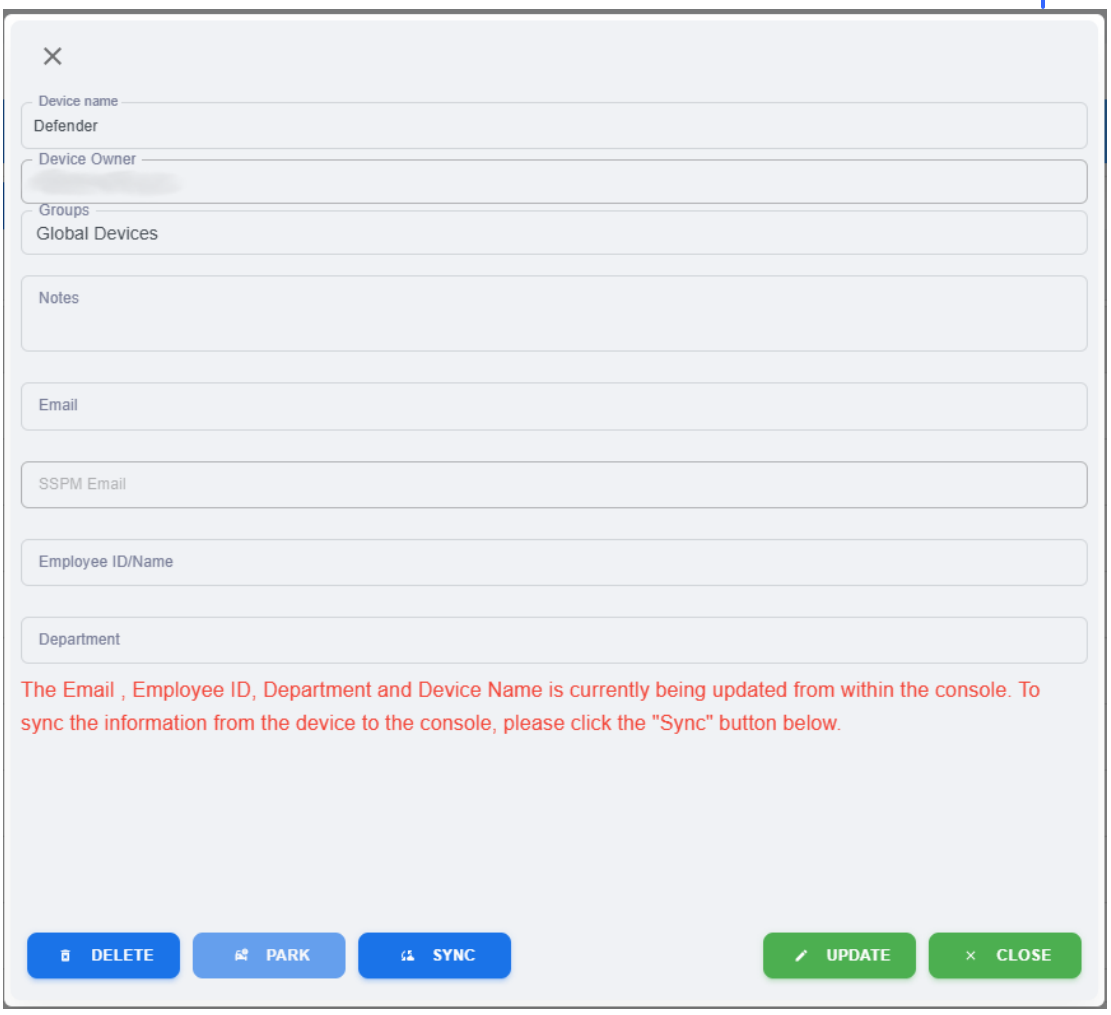
Device Page

8

Edit Selected

Edit Selected allows the Super Administrator (as well as other administrators with the ability to manage the selected device) the ability to change basic information on the device within KRMC. The options available to be altered are as follows:

Device Name	This is the name that the device will appear as on KRMC.
Device Owner	This is the owner of the device. This is the name of the Super Administrator (SA) account on KRMC.
Groups	This will display the current group that the device is assigned to. You can use this field to change the device to another group if you would like.
Notes	This is an internal note section about this device.
Email	The email address that is to be associated with this device.
SSPM Email	The Self-Service Password Management (SSPM) email address that has been registered for this device.
Employee ID/Name	The employee ID number for the user that the device has been assigned to.
Department	The department that the device will be utilized in.
Delete 128	This will delete a selected device from your KRMC account.
Park 129	Parking a device will convert a device to a deactivated state where no licenses are consumed but the device is still on your KRMC to be brought back at a later date.
Sync	This synchronizes the current contact information on the drives to display on this interface. This is based on the last time the device was logged into. ***Note:*** *If you have updated the information but the device has not connected since that point, clicking Sync will result in your changes being lost.*
Update	This updates all the device settings with the new information you have inserted into these fields.
Close	Closes the display regardless of whether information has been updated or not.


Device name
Defender
Device Owner
Groups
Global Devices
Notes
Email
SSPM Email
Employee ID/Name
Department
The Email , Employee ID, Department and Device Name is currently being updated from within the console. To sync the information from the device to the console, please click the "Sync" button below.
DELETE
PARK
SYNC
UPDATE
CLOSE

Delete Device

When a device is deleted from KRMC On-Premise, it will no longer be remotely manageable, and all actions and logs associated with the device will also be deleted. Any KRMC On-Premise license assigned to the drive will also be lost.

Deleting a device is only recommended if you are certain that the device will not need to be managed in the future. Some situations where you would want delete a device from KRMC On-Premise include:

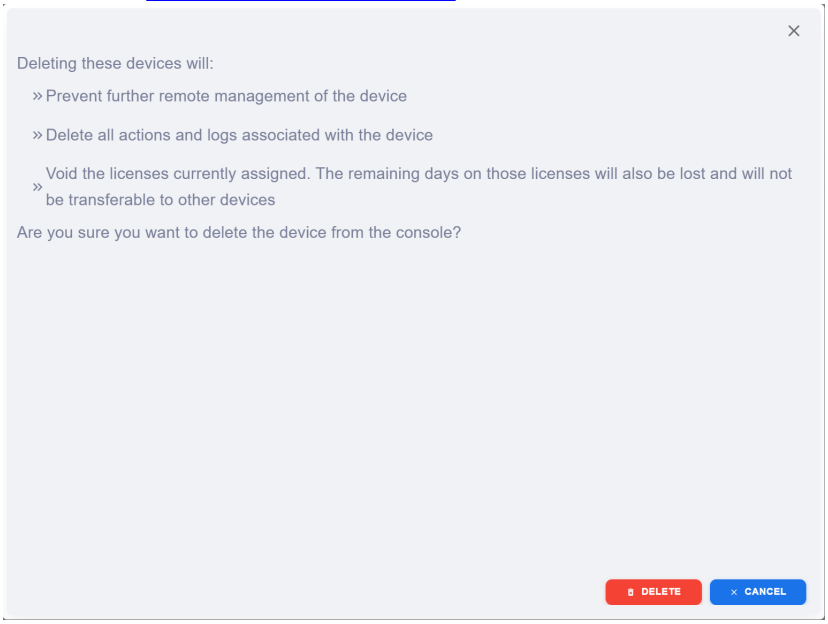
- A device is no longer functional and cannot or will not be repaired.
- A device is being decommissioned due to age
- A device is permanently lost.

If there is any possibility that the device will be managed in the future then you should **Park** the device instead of deleting it. **Parking** a device only temporarily places the device in an inactive state, allowing it to be reactivated and managed by KRMC On-Premise at a later time.

Clicking the **Delete Device** button will display the Delete Device dialogue in the Device Activity list.

- Click the **Delete** button to confirm removing the device and close the Device Activity List
- Click the **Cancel** button to keep the device registered with KRMC On-Premise and return to the Device Activity List.

Note: *SA and Administrators can delete drives if they have the permission "Can Delete Drives from KRMC" located under Advanced Account Abilities. For more information on Admin permissions, please look at* *Edit Admin Permissions* 147.



Park

Devices that have not been seen by the KRMC On-Premise server for at least 18 months can be **Parked**. Parking a device will temporarily exclude it from normal KRMC On-Premise activity without removing the device from the account. When a device is parked from KRMC On-Premise it will not be assigned new licenses, nor will it be remotely manageable but all actions and logs associated with the device will be retained. Any licenses assigned to the drive when it is parked will be lost. Parking a device requires the consumption of one parking license. Devices in this state are moved to the parked list within the Device Page. Parking a device is recommended if there is a possibility that the device will be managed again in the future.

If there is no possibility that the device will be managed in the future then you should consider deleting the device instead of parking it.

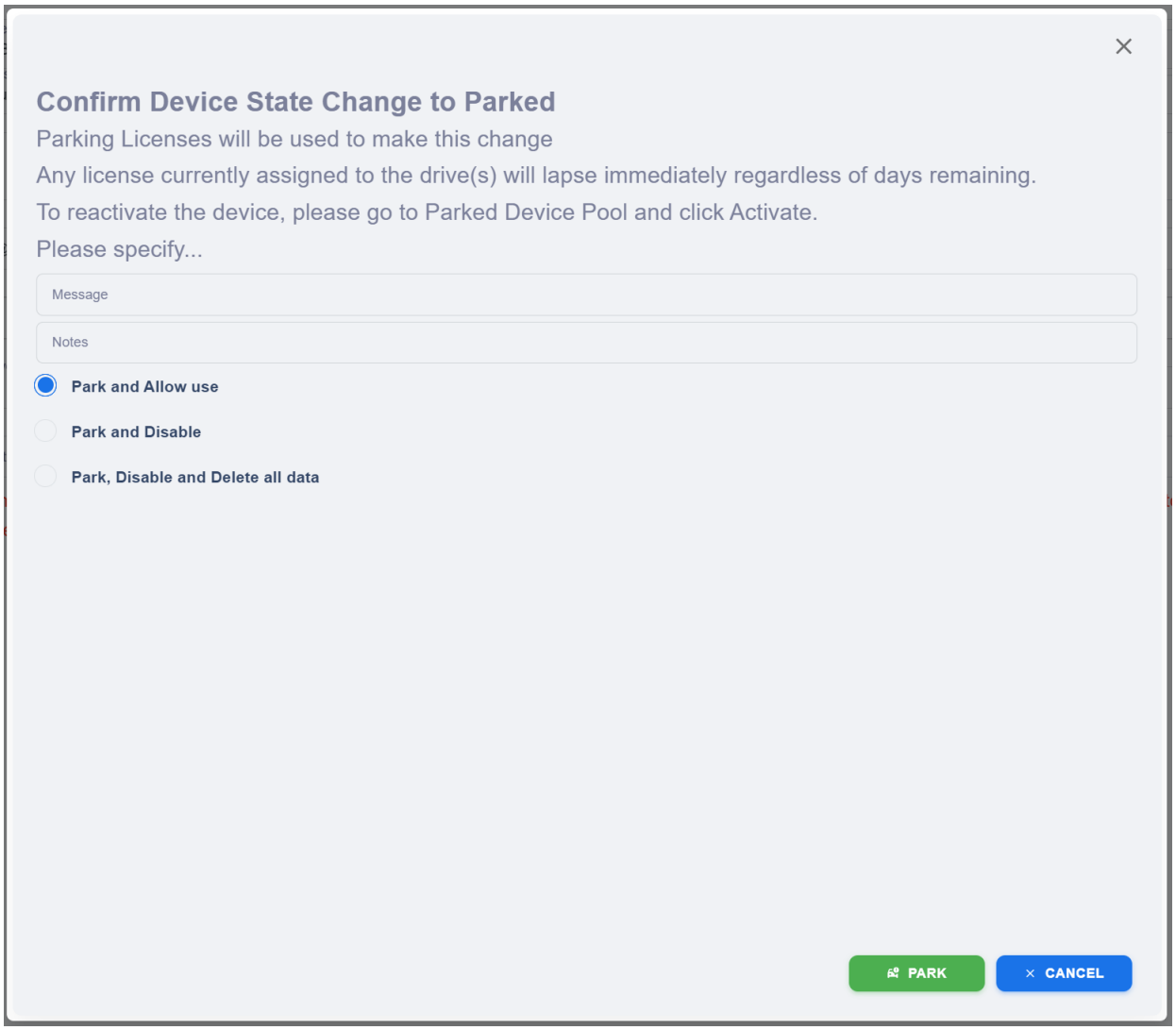
Caution! *If you want to park a device but you need to verify the device's serial number,* ***DO NOT*** *run KDM to find the serial number. Running KDM could make the device seen by the KRMC On-Premise server, in which case the device will no longer be valid for parking. Please use the Serial Number Display Tool to obtain the serial number. The Serial Number Display Tool can be downloaded HERE.*

Clicking the **Park** button will display the Park Device dialogue in the Device Activity list.

You can specify how you want the parked device to behave:

Park and Allow Use	Parks the device from KRMC On-Premise but allows the user to continue using the device as normal.
Park and Disable	Parks the device from KRMC On-Premise and prevents the device from being used. The device user is not able to login to a disabled device.
Park, Disable and Delete all data	Parks the devices from KRMC On-Premise, deletes all data from the device and prevents the device from being used.
Park	Parks the device from KRMC On-Premise using the settings selected above.
Cancel	The park action is canceled.

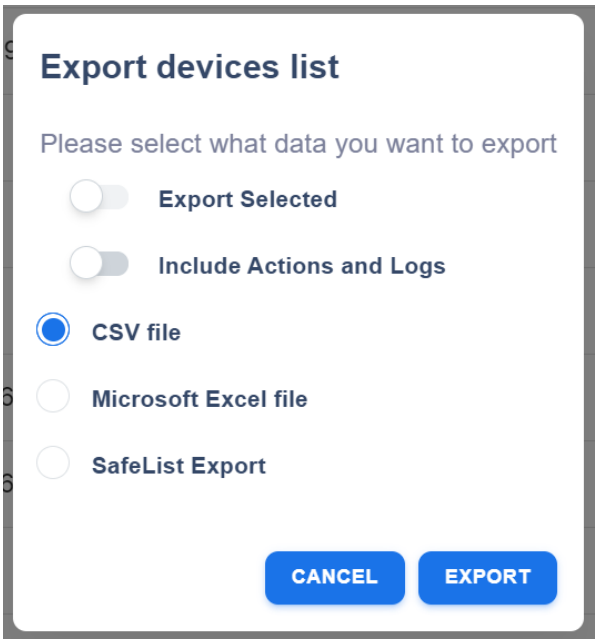
Note: *SA and Administrators can park drives if they have the permission "Can Park Drives from KRMC" located under Advanced Account Abilities. For more information on Admin permissions, please look at Edit Admin Permissions* 147.


Confirm Device State Change to Parked
Parking Licenses will be used to make this change
Any license currently assigned to the drive(s) will lapse immediately regardless of days remaining.
To reactivate the device, please go to Parked Device Pool and click Activate.
Please specify...
Message
Notes
Park and Allow use
Park and Disable
Park, Disable and Delete all data
PARK
CANCEL

Custom Export

Within the Active device page, all accounts have the ability to export all or selected devices along with all actions and device logs.

Selected	The default setting is to export all devices located on this page. Regular Administrators (RA) will be able to export only the drives that they have the permissions to manage. The option "Selected" limits the export to only the drives that have been selected using the checkboxes next to each drive. ***Note: An** RA can export all devices on the KRMC account if they have the permission "Can See All Drives" located under Advanced Account Abilities. For more information on Admin permissions, please look at* *Edit Admin Permissions* 147.
CSV File	The exported file will be exported in a CSV file format.
Microsoft Excel File	The exported file will be exported in a XLSX file format.
SafeList Export	The exported file will be exported in a CSV file format however the drives Vendor ID (VID) and Product ID (PID) have been altered to fit common device and endpoint control applications (such as CrowdStrike).
Include Actions and Logs	The export will include all actions for all devices exported along with the Device Logs which consist of the successful and failed login attempts on the devices. If you export using the Microsoft Excel File format, the export will only consist of one file with multiple pages. If you export using the CSV or SafeList format, the export will be in the form of a ZIP file containing: Device Logs, Devices, Pending Device Actions, Successful Device Actions, and Failed Device Actions. ***Note**: If there are fields with no data, they will not be included in the export. For example, if your account does not have any Failed Device Actions, your export will not contain a Failed Device Actions page or file.* If not selected, the export will only include information within the Device Page
Export	The exported file will be generated based on the information selected in the window.
Cancel	The export action will be ended.


Export devices list
Please select what data you want to export
Export Selected
Include Actions and Logs
CSV file
Microsoft Excel file
SafeList Export
CANCEL
EXPORT

Device Page

8

Edit View

The Device List displays a list of devices belonging to the KRMC account or Group selected. ***Note:*** *A Regular Administrator (RA) can see all devices on the KRMC account if they have the permission "Can See All Drives" located under Advanced Account Abilities. For more information on Admin permissions, please look at* *Edit Admin Permissions* 147. The drives are displayed in a series of columns containing all information that iStorage Kanguru gathers regarding the drives and their usage to make managing them as simple as possible. To better customize the appearance to fit your needs, you can use the option Edit View.

Columns that are shown by default are as follows:

Device Name	The name of the device assigned by UKLA, device setup, or KRMC On-Premise.
Description	A description of the device. The default description is the device's name.
Last Connected	This is the date and time the server last communicated with this Defender device.
Hostname	The name of the machine the device was last connected to.
Last Location	The geographical location of the computer that the device was last connected to. The geographical location is an approximate location of the drive. The actual location may differ.
Email	The email address of the User that the drive belongs to.
SSPM Email	The Self-Service Password Management (SSPM) email address the User entered into the drive.

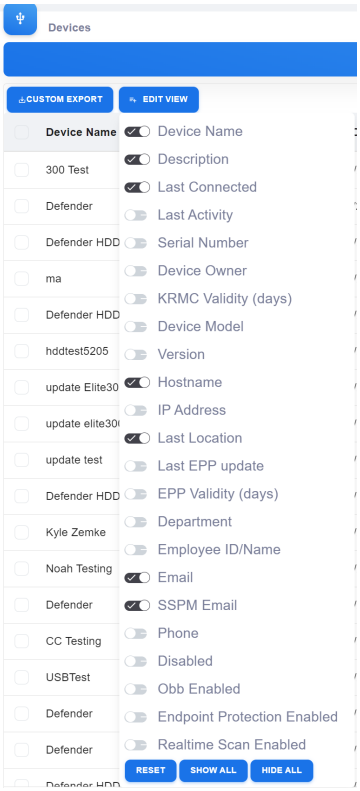
Additional columns available are as follows:

Device Owner	The Super Administrator (SA) that the device is assigned to.
Device Model	This displays the model of the Defender device.
Version	The client version that the device last reported it was running.
Last Activity	The last time the device communicated with KRMC On-Premise.
Serial Number	The serial number of the physical device.
KRMC On-Premise Validity (days)	The number of days remaining on the device's KRMC On-Premise license.
KRMC On-Premise Validity (date)	The date the device's KRMC On-Premise license will expire.
IP Address	The IP address of the machine the device was last connected to.
Last EPP Update	The date the drive was last updated with Endpoint Protection definitions.
EPP Validity (days)	The number of days remaining on the device's Endpoint Protection license.

EPP Validity (date)	The date the device's Endpoint Protection license
Department	The department that the drive or drive's user belongs to.
Employee ID/Name	The name and employee ID of the end user that the drive is assigned to.
Phone	The phone number of the User or Administrator that the drive belongs to.
Disabled	Displays whether the device is currently disabled.
Endpoint Protection Enabled	The current state of the Endpoint Protection application on the drive.
Realtime Scan Enabled	This current state of the Real-Time Scanning setting on the Endpoint Protection application on the drive.
File Audit	This is the current state of the file auditing status on the drive.

Along with the column options, you also have three option:

Reset	This resets your column selection to the KRMC defaults.
Show All	This displays all columns in KRMC.
Hide All	This hides all columns on KRMC.



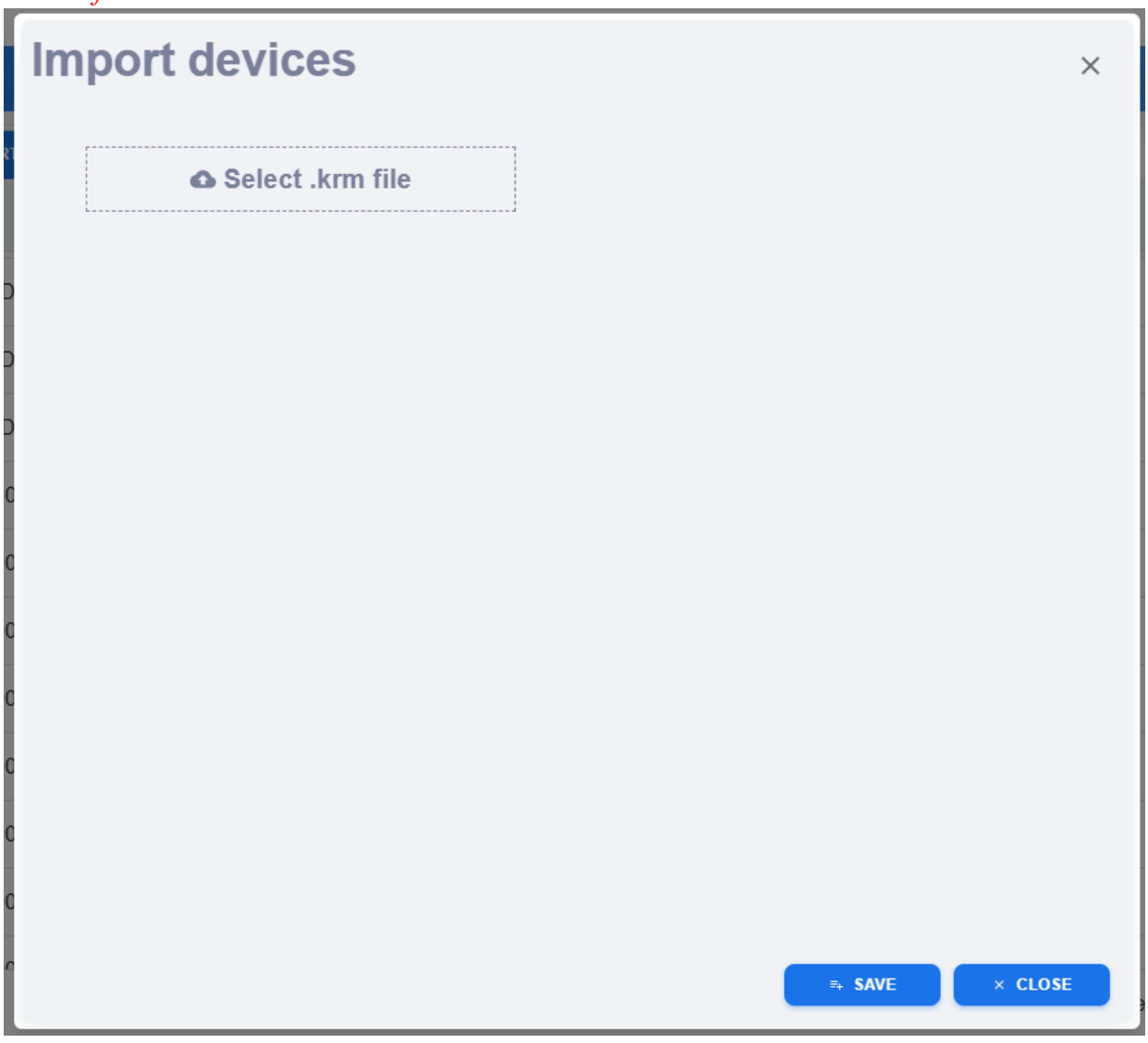
Device Page

8

Import Devices

KRMC provides the ability to manually import devices into the server if preferred. You will require a KRM file provided by either UKLA (Devices Configured Using UKLA)or the On-Premise Provisioning tool (On-Premise Provisioning Tool). When you select Import Devices a pop-up will appear. You will need to select the option "Select .krm file" which will open a window for you to choose file you are looking to import.

Note: *Importing the same drive multiple times cannot occur. If your KRM file contains multiple drives and some are already imported, KRMC will only import the drives that are not already on the server. If for any reason you need to import a drive multiple times, the drive must first be deleted from KRMC.*



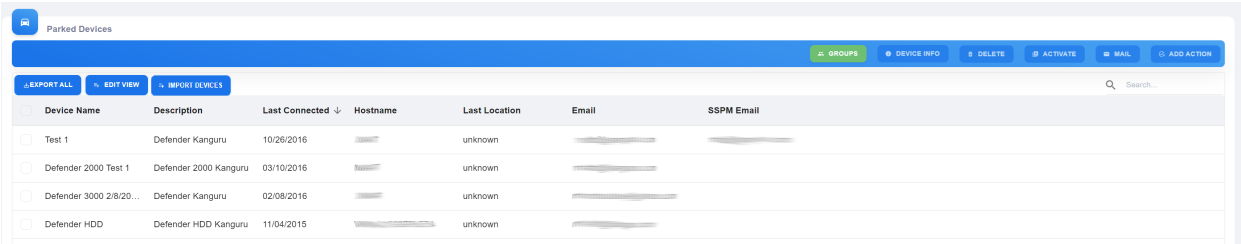
Device Page

8

Parked

The **Parked** device page provides you with options for viewing all devices that you have parked on KRMC. For information on how to park a drive and the feature, please click HERE 129. Within this page you can select a device using the checkbox on the left side column. If you are looking to select multiple devices you can either check the boxes next to each device or select the checkbox on the title bar. In selecting a device, you gain access to multiple options.

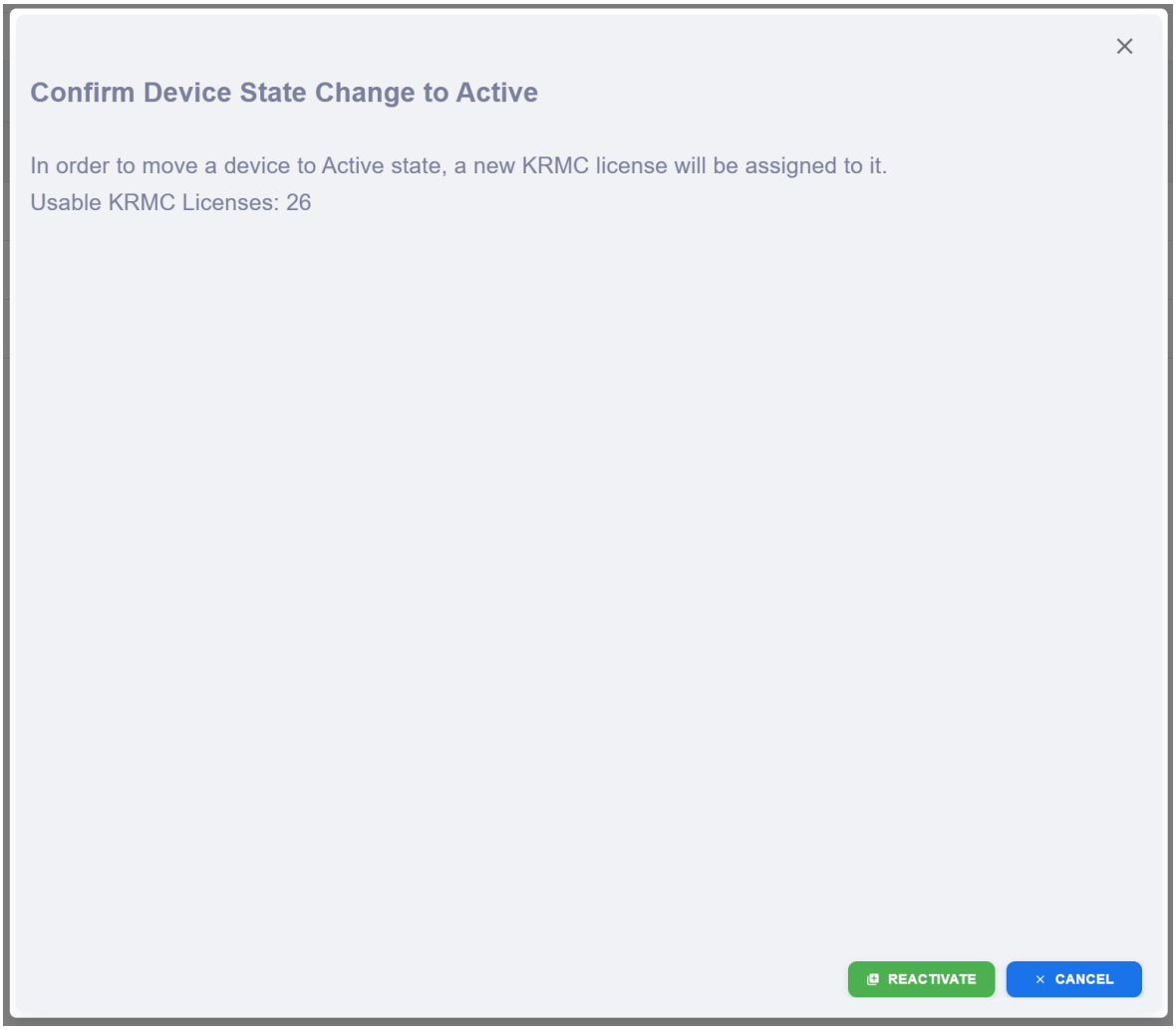
Groups	Allows the KRMC account to view all devices within the selected group. For more information on how to use Groups in the Device pages, please refer to the Groups section on Active Devices located HERE 120.
Device Info	KRMC accounts are able to view device history and previously requested SSPM codes. For more information on Device Info, please refer to the Device Info section on Active Devices located HERE 121. ***Note:*** *This option is not available when multiple devices are selected.*
Delete	Deletes the selected device(s) from KRMC. For more information on deleting devices from KRMC, please refer to the Delete section on Active Devices located HERE 128.
Activate 137	Provides you the ability to bring a device back into the active list to be managed.
Mail	You can send an email from KRMC to the selected device(s). For more information on the Mail feature, please refer to the Mail section on Active Devices located HERE 122.
Add Action	KRMC accounts with permissions are able to send remote actions to the selected device(s). For devices within Parked, there are limited actions available for the devices. These actions are limited to Enable, Disable, and Disable and delete all data. For more information on actions in general, please refer to the Add Action section on Active Devices located HERE 124 .
Custom Export	KRMC with the correct permissions are able to export the Device list for auditing purposes. For information on the export feature, please refer to the Custom Export section on Active Devices located HERE 131.
Edit View	Provides the ability to change which columns are displayed on your Device list. For information on the Edit View feature, please refer to the Edit View section on Active Devices located HERE 133.



Activate Parked Drive

When selecting a parked device from the Parked Device List, there is an option to activate a the selected device(s). This option requires the consumption of one KRMC On-Premise license per drive you are looking to activate. In activating a device, it becomes able to be managed (able to receive remote actions).

Reactivate	Actives the device so it is able to managed once again. This will require a KRMC license that is currently not assigned to any drive.
Cancel	The activation process is canceled.



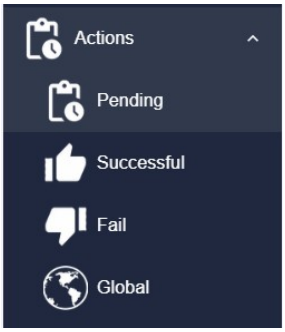
Actions Page

9

The **Actions Page** allows the currently logged in Administrator to review the history of actions sent to devices they own. From here you can view a list of all pending actions, successful actions, and failed actions, and also create a global action that will be sent to every device that you manage.

To switch between each view, click on one of the tabs located at the top of the page:

Pending Actions 139	Allows you to view information on all pending actions within the KRMC On-Premise account
Successful Actions 140	Allows you to view information on all pending actions within the KRMC On-Premise account
Failed Actions 141	Allows you to view information on all pending actions within the KRMC On-Premise account
Create Global Actions 142	Allows the creation of actions to be sent to all devices within the KRMC On-Premise account.



Within each view you will see these default columns along with more:

Action Type	The type of action to be executed.
Target Device	The device that the action will occur on.
Serial Number	The serial number of the drive that the action was created for.
Notes	Internal facing notes provided at the time the action was created.
Message	The message that will be displayed to the device user when the action is executed.
Created At	The date and time the action was created.
Schedule	The earliest date that the action is set to occur.
Created By	The Administrator that originally created the action. ***Note**: Automatic Actions are system generated actions for enabling specific end user features like Creating Admin Password, Custom Settings (Reprovision), Self-Service Password Management (SSPM) related actions. Although these are not created explicitly by an admin, server-side changes by the admin may trigger these management actions on your managed drives.*

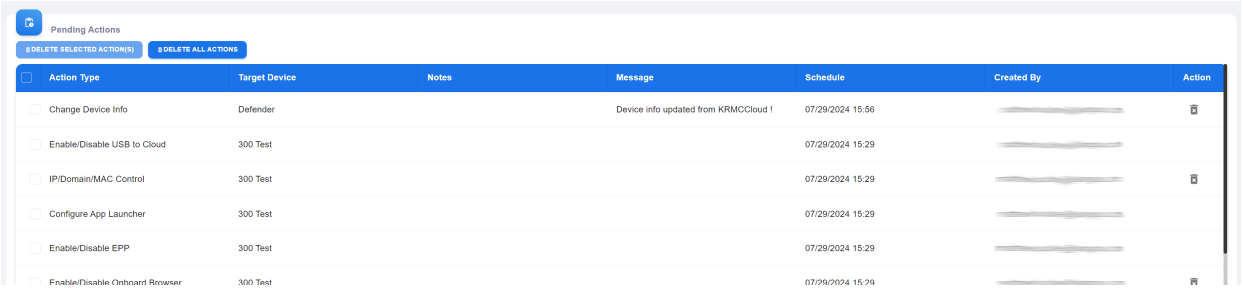
Actions Page

9

Pending Actions

Pending Actions contains a list of actions that are currently waiting to be executed. Once a drive communicates with KRMC On-Premise, it will receive any actions that are scheduled on the pending list. Once received, the device will execute the action.

Action Type	The type of action to be executed.
Target Device	The device that the action will occur on.
Serial Number	The device serial number that the action was created for.
Notes	Internal facing notes provided at the time the action was created.
Message	The message that will be displayed to the device user when the action is executed.
Created At	The date and time an action was created.
Schedule	The earliest date that the action is set to occur.
Created By	The Administrator that originally created the action. ***Note**: Automatic Actions are system generated actions for enabling specific end user features like Creating Admin Password, Custom Settings (Reprovision), Self-Service Password Management (SSPM) related actions. Although these are not created explicitly by an admin, server-side changes by the admin may trigger these management actions on your managed drives.*
Action	You can delete a pending action by clicking on the delete action icon located in the Action column, removing it from the pending actions queue and preventing it from being executed.



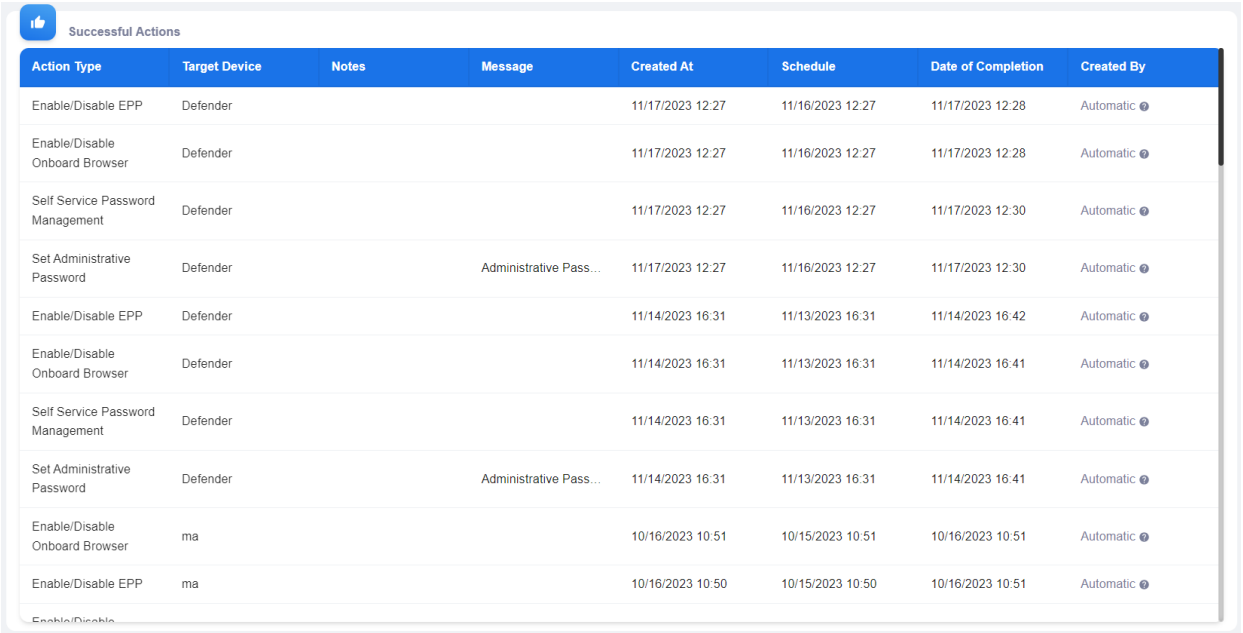
You can delete all pending actions for every device assigned to you by clicking on the **Delete All Actions**. You can delete selected actions by using the check box on the left side of each action then select **Delete Selected Actions**. ***Note**: Some actions are critical to a device's operation and manageability and cannot be deleted.*

Actions Page 9

Successful Actions

Successful Actions contains a list of actions that were successfully executed on the target device. Actions on this page cannot be deleted. There is an additional Date of Completion column in Successful Actions that records the date and time that the action was executed.

Action Type	The type of action to be executed.
Target Device	The device that the action will occur on.
Serial Number	The device serial number that the action was created for.
Notes	Internal facing notes provided at the time the action was created.
Message	The message that will be displayed to the device user when the action is executed.
Created At	The date and time an action was created.
Schedule	The earliest date that the action is set to occur.
Date of Completion	The date and time an action was reported as completed to KRMC On-Premise.
Created By	The Administrator that originally created the action. ***Note**: Automatic Actions are system generated actions for enabling specific end user features like Creating Admin Password, Custom Settings (Reprovision), Self-Service Password Management (SSPM) related actions. Although these are not created explicitly by an admin, server-side changes by the admin may trigger these management actions on your managed drives.*



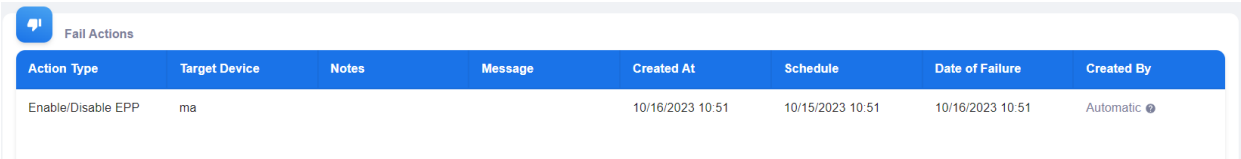
Actions Page

9

Failed Actions

Failed Actions contains a list of actions that have failed. A common reason for why an action fails is if a device has an expired license, or if an incorrect administrative password was used when attempting to run a Change User Password action. There is an additional Date of Failure column in the Failed Actions that displays the date and time when the action failed.

Action Type	The type of action to be executed.
Target Device	The device that the action will occur on.
Serial Number	The device serial number that the action was created for.
Notes	Internal facing notes provided at the time the action was created.
Message	The message that will be displayed to the device user when the action is executed.
Created At	The date and time an action was created.
Schedule	The earliest date that the action is set to occur.
Date of Failure	The date and time an action was reported as failed.
Created By	The Administrator that originally created the action. ***Note**: Automatic Actions are system generated actions for enabling specific end user features like Creating Admin Password, Custom Settings (Reprovision), Self-Service Password Management (SSPM) related actions. Although these are not created explicitly by an admin, server-side changes by the admin may trigger these management actions on your managed drives.*



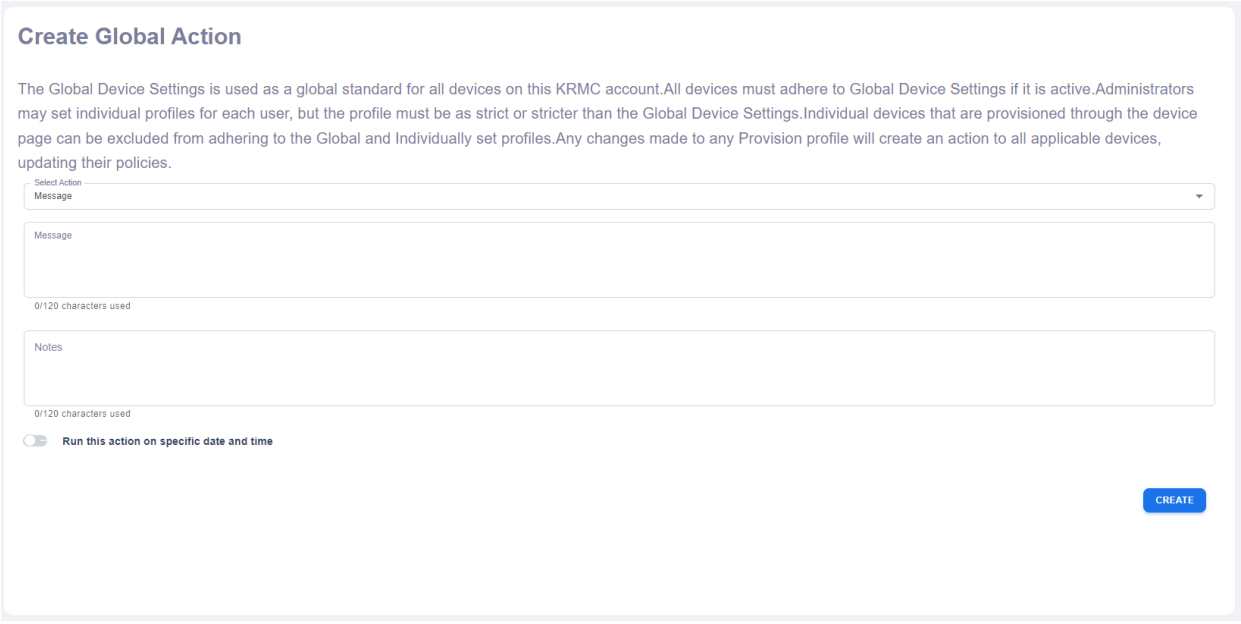
Actions Page 9

Global Actions

Create Global Action allows you to create an action that is executed on all devices managed by your account. Creating a global action creates individual pending actions for every device that you manage. The actions available to the Regular Administrator (RA) is dependent on their permissions as defined under Edit Admin Permissions 147. For a full list and description of actions available, please refer to Remote Action List 206.

The default fields that will be available for you are as follow:

Select Action	This allows you to select the action that you are trying to send to all devices within this group. Note: Depending on the action selected, the fields below may change.
Message	A message is something that is displayed to the end user once the actions is received by the device.
Notes	This is an internal note about the action. This is not displayed to the end user.
Run this action on specific date and time	By default, a new action is scheduled to execute the next time the device is seen by the KRMC On-Premise server. If you want to delay the action until later, you can select Run this action on specific date and time and set a future date and time when the action can be executed. ***Note:*** *A scheduled action may not occur at the exact date and time set here. The action will be executed the next time the device communicates with KRMC On-Premise after the scheduled date and time.*
Create	This creates the action based on the options selected above.



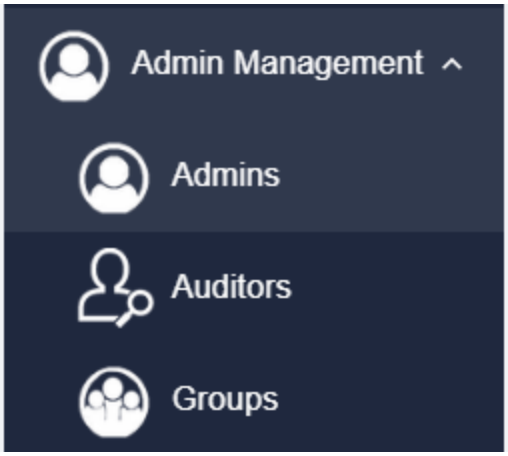
Admin Management Page

10

The **Admin Management Page** allows you to view and edit Administrator, Auditors, and Groups created by your Super Administrator (SA) account.

To view the different accounts in each level, click on one of the options in the navigation bar:

Admins 144	Allows you to view all administrators on the KRMC On-Premise company account and edit information, permissions, and restrictions.
Auditors 153	Allows you to view and edit all auditor accounts on KRMC On-Premise.
Groups 159	Allows you to view all groups within KRMC On-Premise. You are able to edit information within the group and send actions to all drives associated with it.



On the pages: Admins, Auditors, and Groups there are options at the top left of the section to change the view of the page as well as add a new Admin/Auditor/Group.

The default viewing method is a more visual based display designed to make navigation and understanding easier. The second mode is more of a list-based mode. This is less visually impactful and displays all the information in a more traditional KRMC based format. If you would like to learn how to set the default visual method, please click HERE 189.

For steps on how to create an Admin, please click HERE 63.
For steps on how to create an Auditor, please click HERE 65.
For steps on how to create a Group, please click HERE 67.

Admin Management Page 10

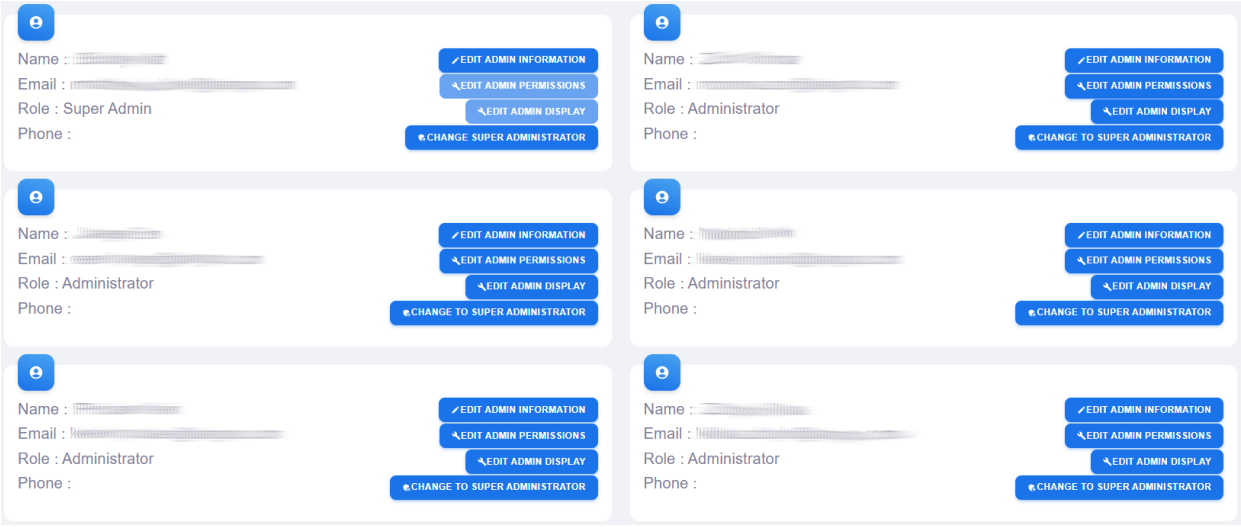
Admins

The **Admins** list provides a list of Administrator. For more information on Administrators, please click HERE 62. ***Note**: The Super Administrator (SA) and Regular Administrators (RA) are able to view all administrators. RAs are able to view themselves and any group(s) that they are assigned.*

Each Administrator account has the following actions available:

Edit Admin Information 145	Allows the administrators the ability to edit general information about their account such as Name, Email, and Phone Number. The SA and Administrators with permission have the ability to perform other actions as well such as enable/disable an account or assign a group to the account.
Edit Admin Permissions 147	The SA and Administrators with permission have the ability to add or remove permissions that an RA has on the platform.
Edit Admin Display 150	The SA and Administrators with permission have the ability to add or remove pages on KRMC that an RA has access to. Additionally, you are able to indicate which page should be the first page seen by the account when logged in.
Change Super Administrator 151	This is only available for the SA account. This allows the SA to change the SA on their account to a different email or RA.
Change to Super Administrator 151	This is only available for the RA account(s). This allows the SA or RA to change the SA on their account to a specific RA account.

Clicking on any of these action buttons will display the selected information in the area to the right.



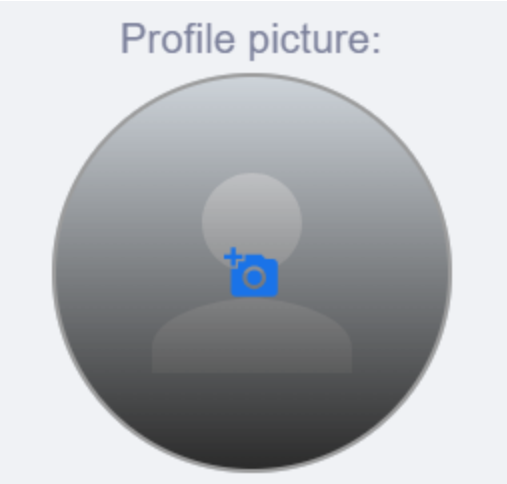
Admin Management Page

10

Edit Admin Information

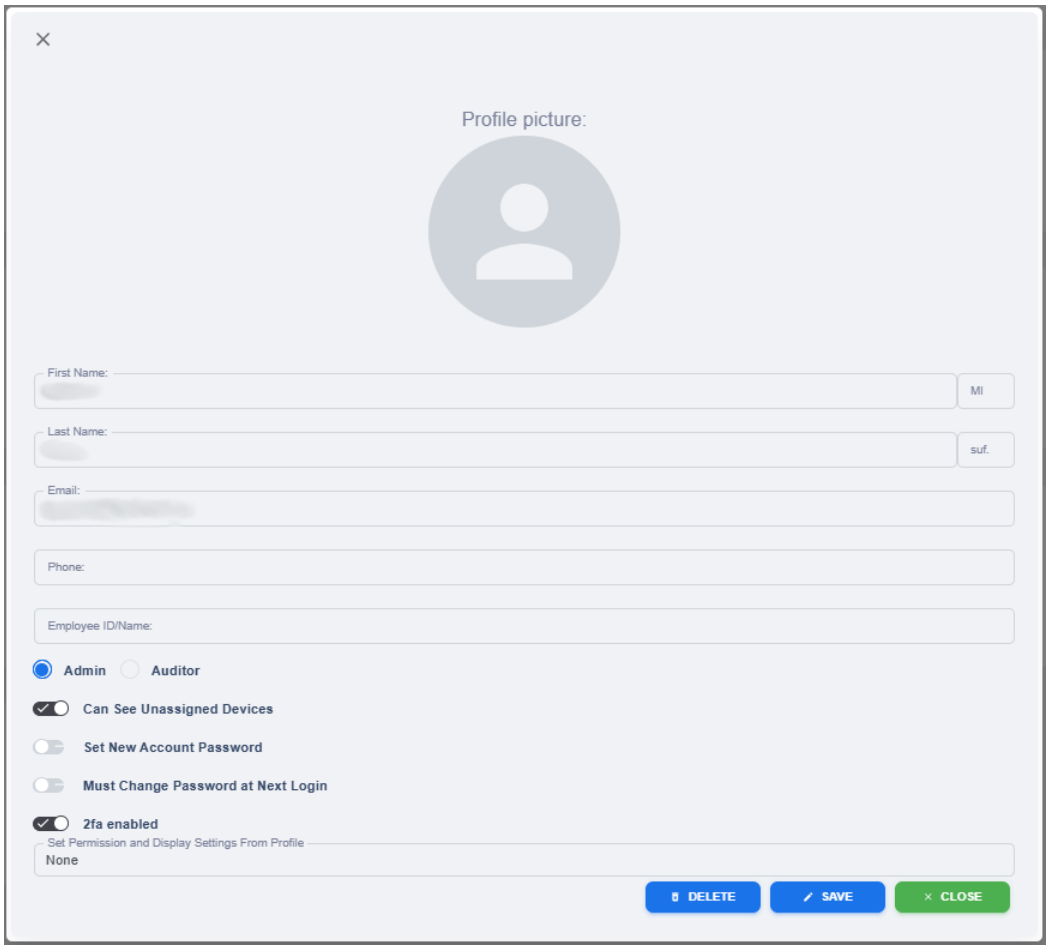
Edit Admin Information allows you to change information such as name or email address of the selected administrator. Additionally, you are able to add a profile picture for the administrator and change whether the selected account is an Admin or is changed to an Auditor. You are able to alter many of these items for your own account by selecting Edit Profile 57 at the top right side of your screen.

To change the profile picture, you will need to select the image and left click. From here, a window will appear allowing you to choose from an image located on your computer. ***Note:*** *You may need to refresh your browser for the image to appear after selected.*



First Name	The admin's first name
Last Name	The admin's last name
MI	The admin's middle initial
Suf.	The admin's suffix
Email	The admin's email
Phone	The admin's phone number
Employee ID/Name	The admin's employee ID
Admin/Auditor	This allows you to switch the account role between an Admin or an Auditor.
Can see unassigned devices	When enabled allows the administrator to view any unassigned devices. If disabled the administrator will only see devices assigned to them.
Set New Password	You are able to create a password for the new Admin account. After creating the password, you would then need to confirm the new password.
Must Change Password at Next Login	When this is enabled, your Admin will be asked to change their account password the next time they log into KRMC.
2fa Enable	Enable or Disable 2fa on the account.

Set Permission and Display Settings From Profile	This feature allows you to copy the settings from another administrator to this new administrator account. This provides a simple way to assign permissions and display settings for multiple administrators. To use this feature you must have an account (other then the SA account) that has both Admin Permissions and Admin Display settings saved. Once those settings have been saved, refresh your browser and you should be able to see the admin appearing in the list to choose.
Save	Saves all changes made within this menu.
Delete	Deletes the account from KRMC On-Premise. ***Note:*** *Deleted accounts cannot be retrieved after deleted.*
Close	The window closes.



Edit Admin Permissions

Edit Admin Permissions allows you to change the permissions for any account on KRMC. KRMC provides the ability to alter most settings within the console providing you the ability to make accounts function the way you want. ***Note:*** *If you are looking to use the feature "Set Permissions and Display Settings From Profile", you must set the permissions in this section as well as Edit Admin Display for at least one Regular Administrator (RA) before use.*

Account Access

Account Enabled	The Account is enabled and able to be accessed. ***Note:*** *The option will change automatically if "Account Disabled" is selected.*
Account Disabled	The Account is disabled and unable to be accessed. ***Note:*** *The option will change automatically if "Account Enabled" is selected.*

Account Permissions

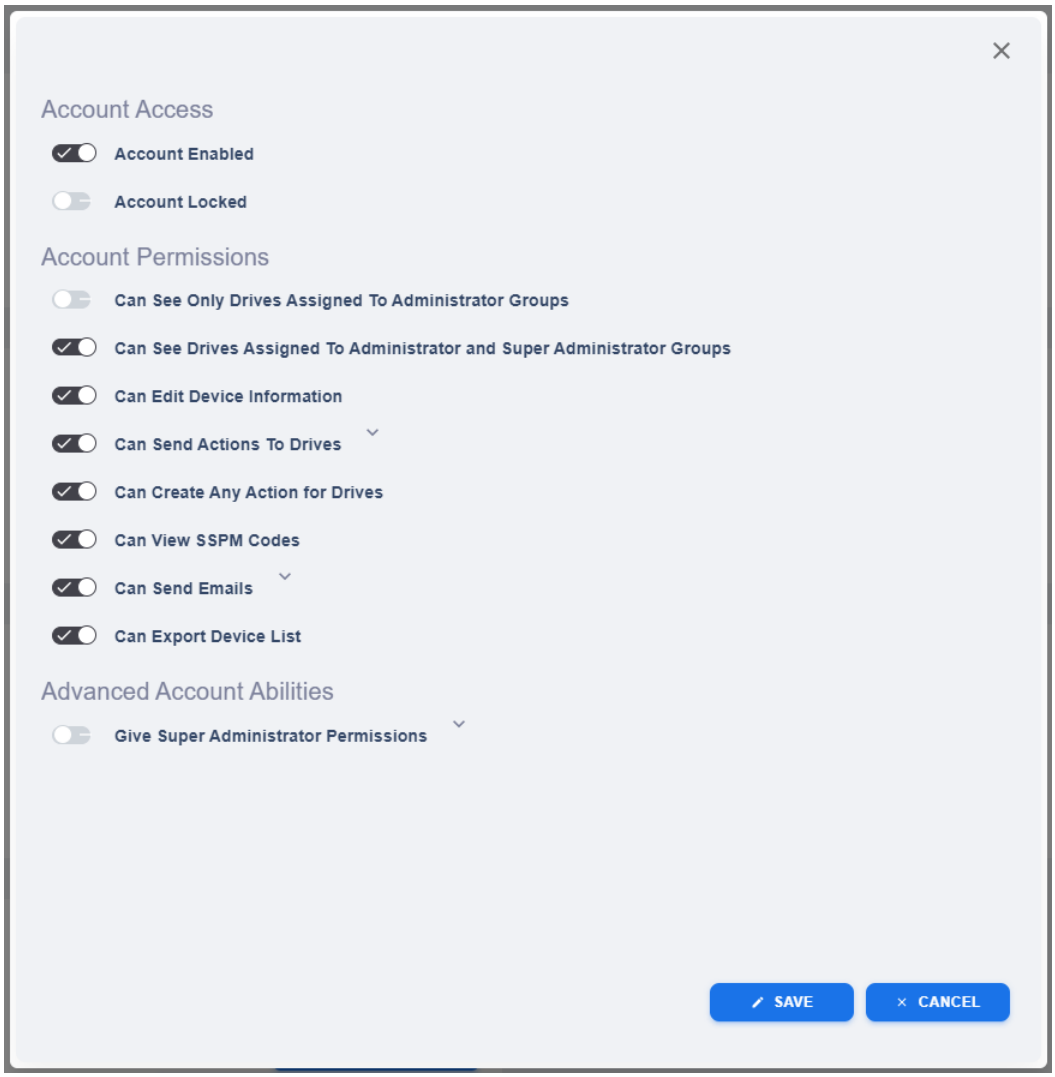
Can See Only Drives Assigned to Administrator Groups	The administrator account is only able to see drives that has been assigned to a group the account is added to. This will provide a limited access to drives. ***Note:*** *The option will change automatically if "Can See Drives Assigned to Administrator and Super Administrator Groups" is selected.*
Can See Drives Assigned to Administrator and Super Administrator Groups	The administrator account is only able to see drives that has been assigned to a group the account is added to. This will provide a limited access to drives. ***Note:*** *The option will change automatically if "Can See Only Drives Assigned to Administrator Groups" is selected.*
Can Edit Device Information	The administrator account can edit device information for drives that the administrator is able to manage.
Can Send Actions to Drives	The administrator account can send actions to drives that the administrator is able to manage. You can use the drop-down to select and unselect actions that the admin is able to perform. ***Note:*** *You are not able to unselect action types if the permission "Can Create Any Action For Drives" is selected.*
Can View SSPM Codes	The administrator account can view the most recent SSPM code sent for a drive that the administrator is able to manage.
Can Send Emails	The administrator account can send emails to the users of the drives that the administrator is able to manage. Additionally, it can be selected whether the account can use either KRMC email services, Custom SMTP services, or both.

Can Export Device List	The administrator account can export the device list. ***Note:*** *This will only contain the information for drives that the administrator is able to manage.*

Advanced Account Abilities

Give Super Administrator Permissions	This setting when enabled, provides the ability to use any/all of the options below. In previous version of KRMC, this was called the Global Device Administrator. It is highly recommended that you only provide access to those accounts that need them as this can limit the SA's ability to control the account.
Can See All Drives	The administrator account can see all drives on the KRMC account without limitations of what groups drives are in.
Can Send Actions to All Drives	The administrator account can send any action to all drives on the KRMC account without limitations of what groups drives are in.
Can Create Any Global Action for Drives	The administrator account can send any action to all drives on the KRMC account as a Global Action without limitations of what groups drives are in.
Can Park Drives	The administrator account can park eligible drives on the KRMC account.
Can Activate Park Drives	The administrator account can activate parked drives on the KRMC account. Note: A valid KRMC license is required for a drive to be moved to Active from Parked.
Can Delete Drives from KRMC	The administrator account can delete any drive from KRMC account.
Can Create and Edit Administrators	The administrator account is able to create and edit other administrator accounts (not including the SA account).
Can Create and Edit Auditors	The administrator account is able to create and edit auditor accounts.
Can Create and Edit Groups	The administrator account is able to create and edit groups. This includes which drives are assigned to a group and provisioning settings.
Can Edit SAML Settings	The administrator account edit the SAML settings on the KRMC account.
Can Edit SSPM Email Domain Allowlist	The administrator account can edit the SSPM and Contact allowlist settings on the KRMC account.
Can Edit Event Export	The administrator account edit the Event Export (SIEM) settings on the KRMC account.
Can Edit AD Service Integration Sync	The administrator account edit the AD Integration Device Disable setting on the KRMC account.
Can Edit Email Templates	The administrator account is able to edit the templates used for the email services.
Can Manage File Audit Notifications	The administrator account edit the File Audit View settings on the KRMC account.
Can Manage Server Certificates	The administrator account can import a signed certificate.

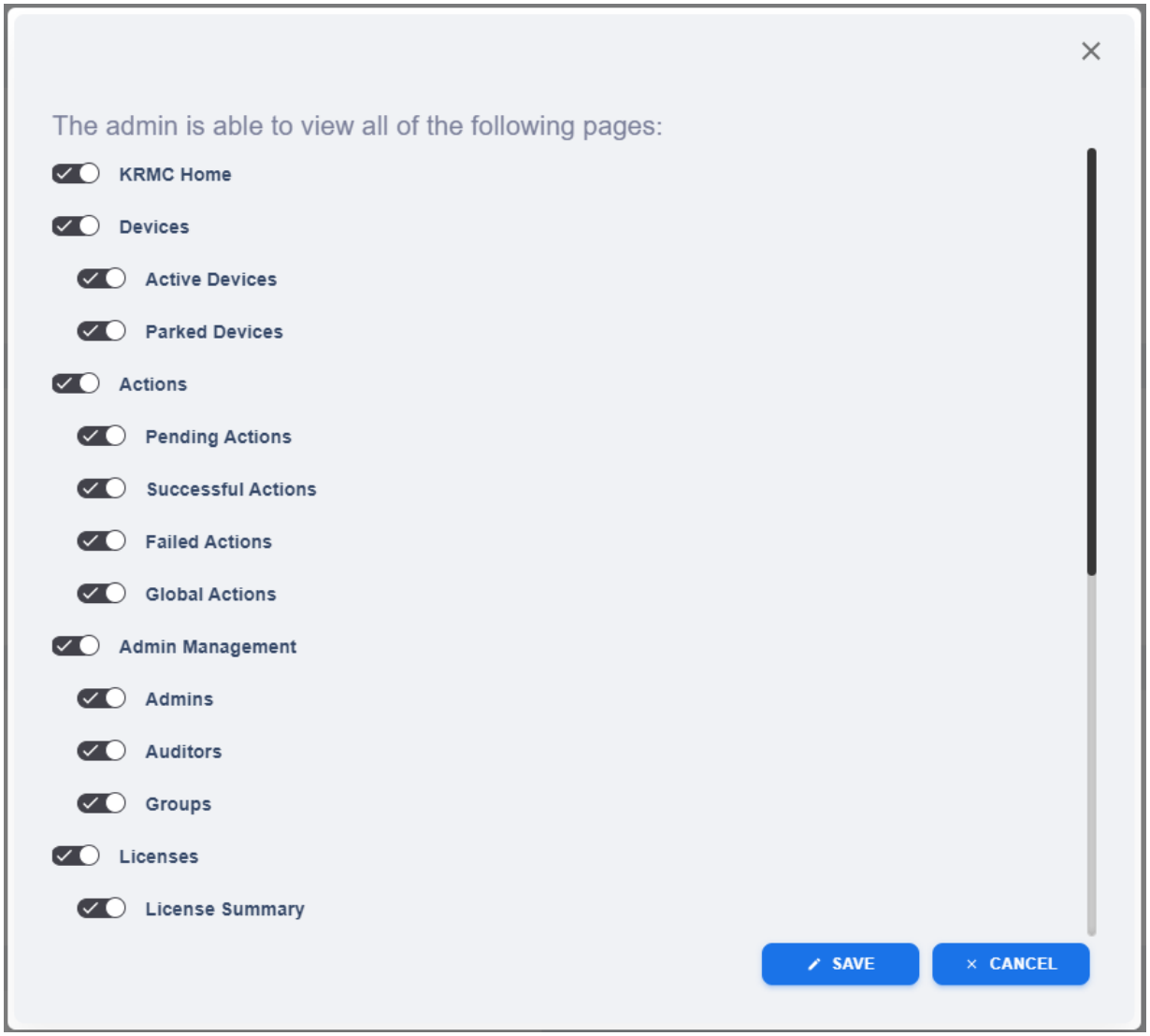
Can Import Database File	The administrator account is able to import the database from a KRMC 5, 6, or 7 server.
Can Do Server Update	The administrator account is able to perform server updates.
Can Manage EPP Settings	The administrator account is able to alter the EPP settings located under EPP Connection Settings.
Can Change Server License Tier	The administrator account is able to convert the KRMC server account type between Advanced and Premium.



Admin Management Page 10

Edit Admin Display

Edit Admin Display allows you to change what pages are viewable for your Regular Administrators (RAs). In addition to choosing which pages are viewable to your RAs, you can also choose which page your RAs see when they first log into KRMC. ***Note:*** *If you are looking to use the feature "Set Permissions and Display Settings From Profile", you must set the permissions in this section as well as Edit Admin Permission for at least one Regular Administrator (RA) before use.*

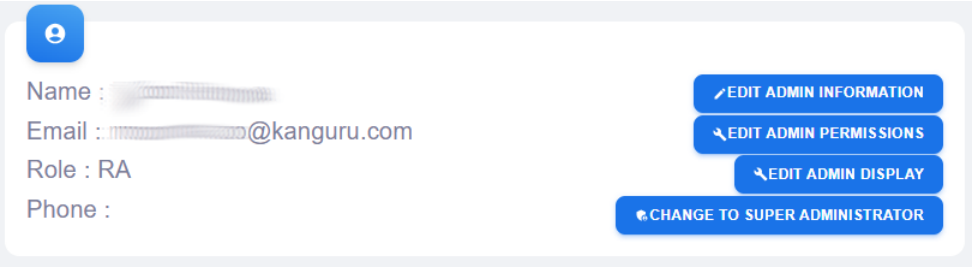


Change Super Administrator

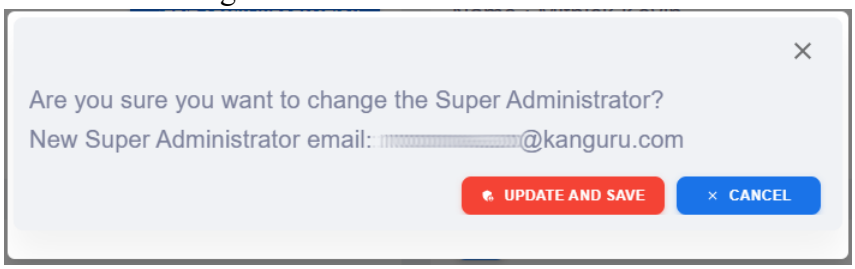
KRMC only has one Super Administrator (SA) account. With that said, there are options available if needed to change the account that is considered the SA account. ***Note:*** *You must be logged in as the SA in order to change the SA.*

Method 1: Change to Super Administrator

1. If you have a Regular Administrator (RA) that you are looking to prompt to the SA level, you can select the option "Change to Super Administrator" that is associated for that RA account.

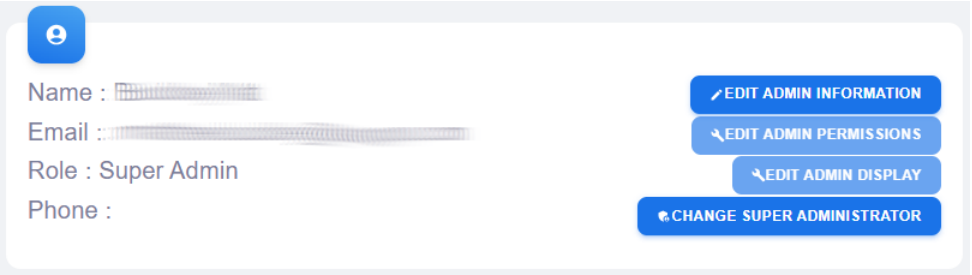


2. Once selected, you will receive a popup asking for you to confirm that you would like to make this RA the new SA. If you select "Update and Save", your RA account will be converted to be the new SA and the original SA will be converted to be an RA.

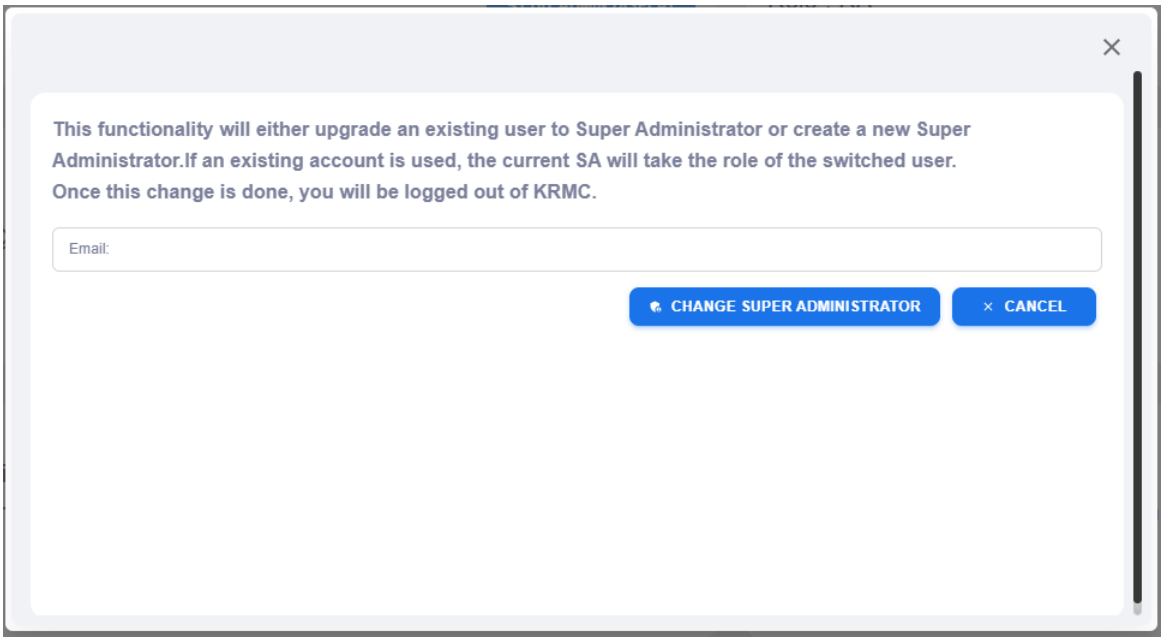


Method 2: Change Super Administrator

1. If you are looking to change the SA account to an email currently not associated with an RA or Auditor account, you can use the option "Change Super Administrator" that is associated with your SA account.

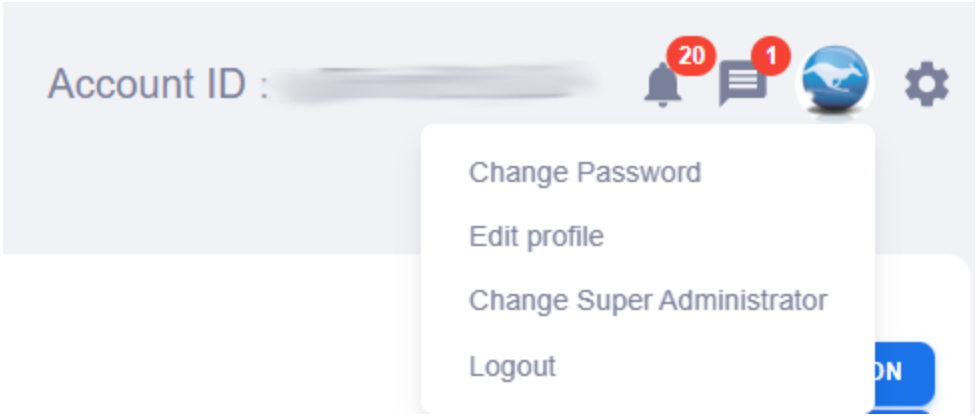


2. Once you select this option you will be presented with a display stating "This functionality will either upgrade an existing user to Super Administrator or create a new Super Administrator. If an existing account is used, the current SA will take the role of the switched user. Once this change is done, you will be logged out of KRMC.".



3. You will need to add the email address that you would like to use as the new SA. ***Note:*** *If you are choosing a new account to be the SA, the new account will use the same account password as the original SA. This password can be changed with a password reset if you would like*.

Note: *You can also use Method 2 by selecting you Account Icon* 55 *at the top right of the screen and select "Change Super Administrator".*



Method 3: Edit Admin Information

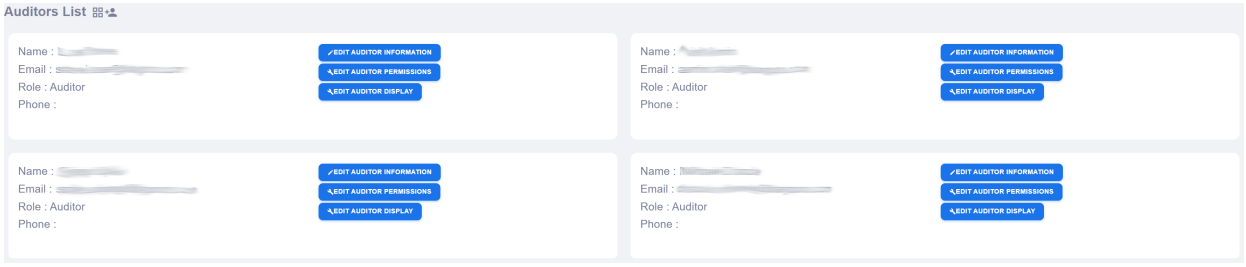
1. If you are logged into KRMC as the SA you can use the option Edit Admin Information on the SA account to change the account first name, last name, and email address. ***Note:*** *Using this method is not recommended if you are looking to use an email address associated with a different account. If you are looking to perform that, we would recommend either Method 1 or Method 2*.

Auditors

The **Auditors** list displays a list of Auditors created in KRMC On-Premise. Auditors are allowed (by default) to view all devices, groups, and events within KRMC On-Premise. The Auditor account actions are limited solely to exporting logs and reports. For more information on Auditors, please click HERE 62.

Each Auditor account has the following actions available:

Edit Auditor Information 145	Allows the administrators the ability to edit general information about the auditor account such as Name, Email, and Phone Number. The SA and Administrators with permission have the ability to perform other actions as well such as enable/disable an account or assign a group to the account.
Edit Auditor Permissions 147	The SA and Administrators with permission have the ability to add or remove permissions that the auditor has on the platform.
Edit Auditor Display 150	The SA and Administrators with permission have the ability to add or remove pages on KRMC that the auditor has access to. Additionally, you are able to indicate which page should be the first page seen by the account when logged in.

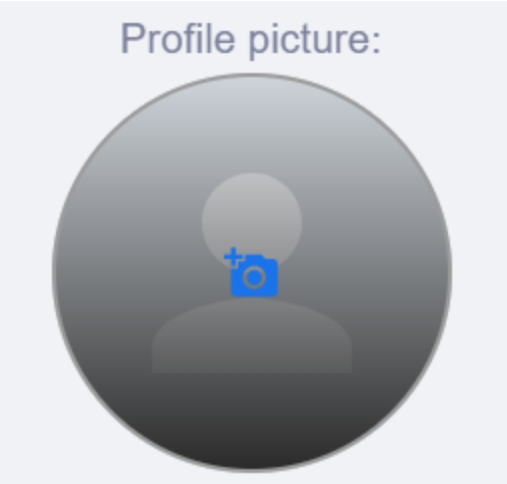


Admin Management Page 10

Edit Auditor Information

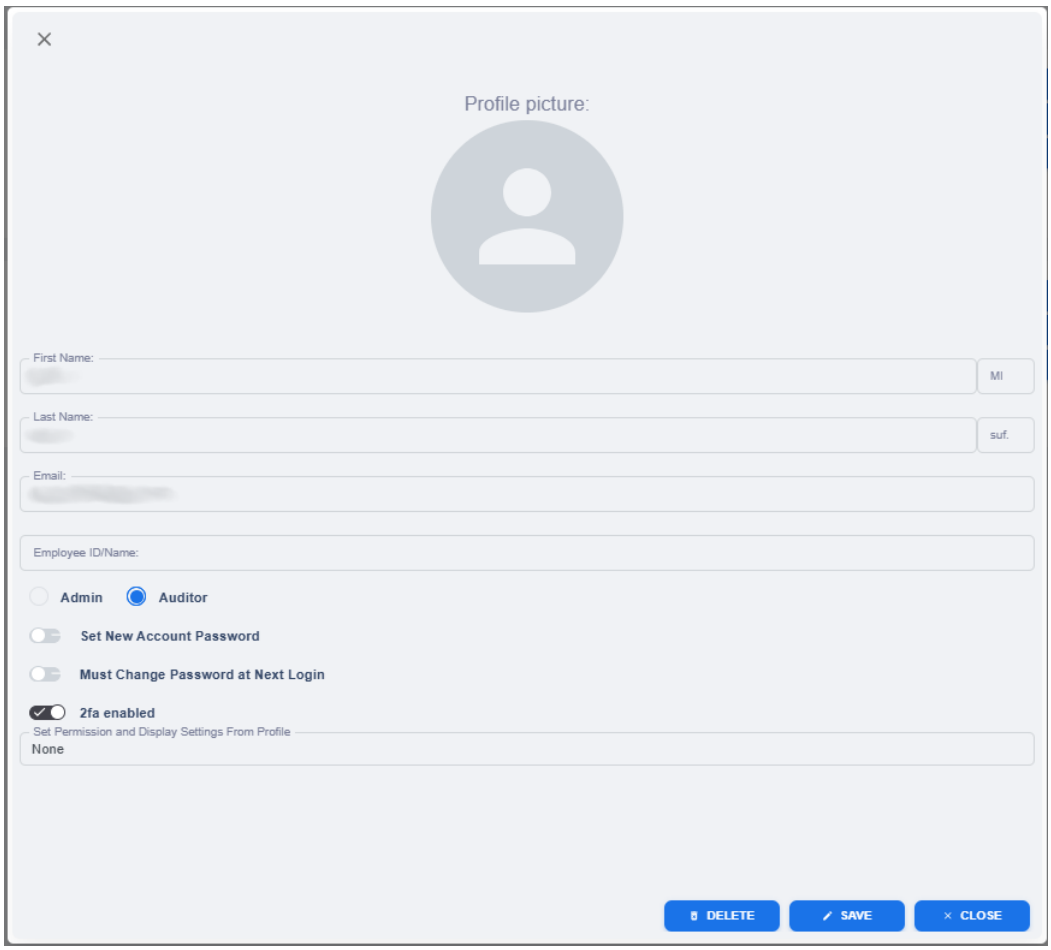
Edit Auditor Information allows you to change information such as name or email address of the selected auditor. Additionally, you are able to add a profile picture for the auditor and change whether the selected account is an auditor or is changed to an admin. You are able to alter many of these items for your own account by selecting Edit Profile 57 at the top right side of your screen. HERE.

To change the profile picture, you will need to select the image and left click. From here, a window will appear allowing you to choose from an image located on your computer. ***Note:*** *You may need to refresh your browser for the image to appear after selected.*



First Name	The auditor's first name
Last Name	The auditor's last name
MI	The auditor's middle initial
Suf.	The auditor's suffix
Email	The auditor's email
Phone	The auditor's phone number
Employee ID/Name	The auditor's employee ID
Admin/Auditor	This allows you to switch the account role between an Admin or an Auditor.
Set New Password	You are able to create a password for the new auditor account. After creating the password, you would then need to confirm the new password.
Must Change Password at Next Login	When this is enabled, your auditor will be asked to change their account password the next time they log into KRMC.
2fa Enable	Enable or Disable 2fa on the account.
Set Permission and Display Settings From Profile	This feature allows you to copy the settings from another auditor to this new auditor account. This provides a simple way to assign permissions and display settings for multiple administrators. To use this feature you must have an account that has both auditor Permissions and auditor Display settings saved.

	Once those settings have been saved, refresh your browser and you should be able to see the auditor appearing in the list to choose.
Save	Saves all changes made within this menu.
Delete	Deletes the account from KRMC On-Premise. ***Note:*** *Deleted accounts cannot be retrieved after deleted.*
Close	The window closes.



Admin Management Page 10

Edit Auditor Permissions

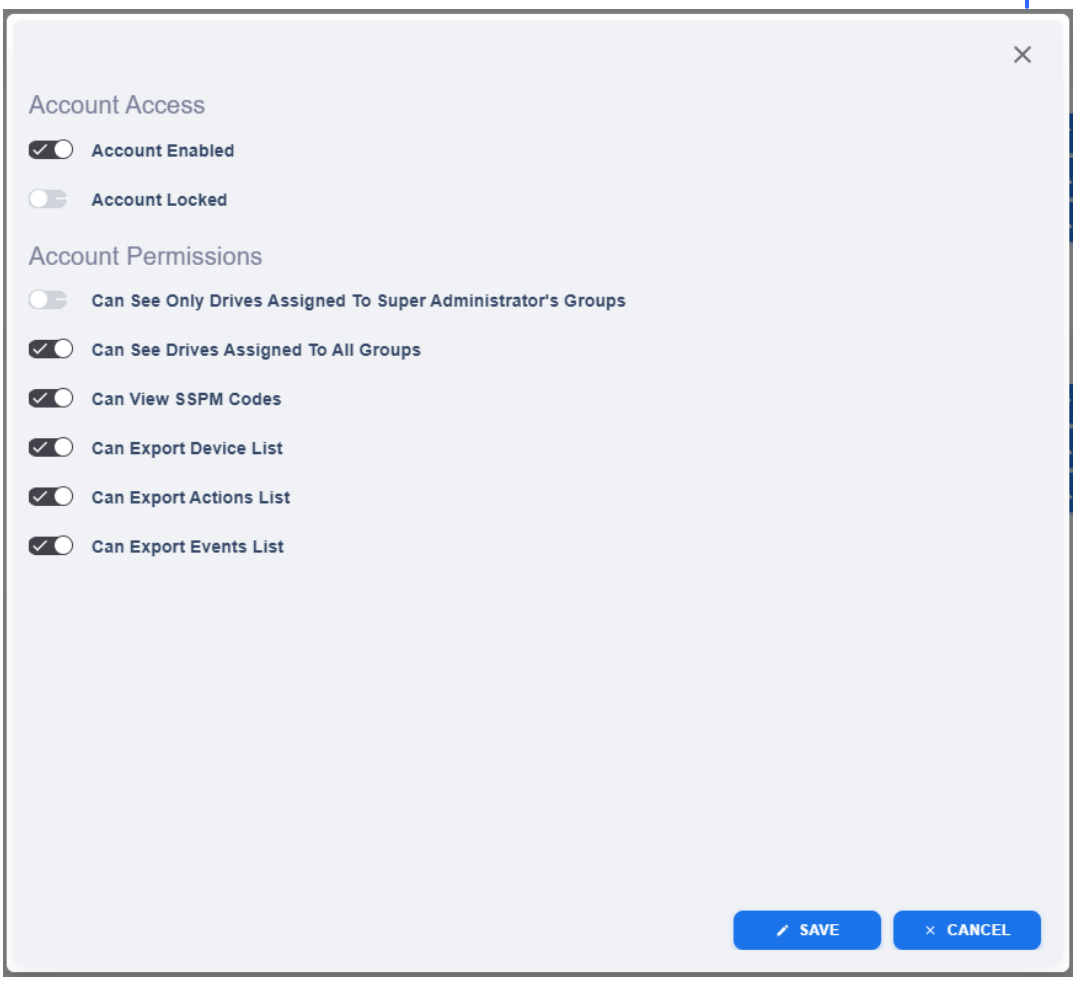
Edit Auditor Permissions allows you to change the permissions for any account on KRMC. KRMC provides the ability to alter most settings within the console providing you the ability to make accounts function the way you want. ***Note:*** *If you are looking to use the feature "Set Permissions and Display Settings From Profile", you must set the permissions in this section as well as Edit Admin Display for at least one auditor before use.*

Account Access

Account Enabled	The Account is enabled and able to be accessed. ***Note:*** *The option will change automatically if "Account Disabled" is selected.*
Account Disabled	The Account is disabled and unable to be accessed. ***Note:*** *The option will change automatically if "Account Enabled" is selected.*

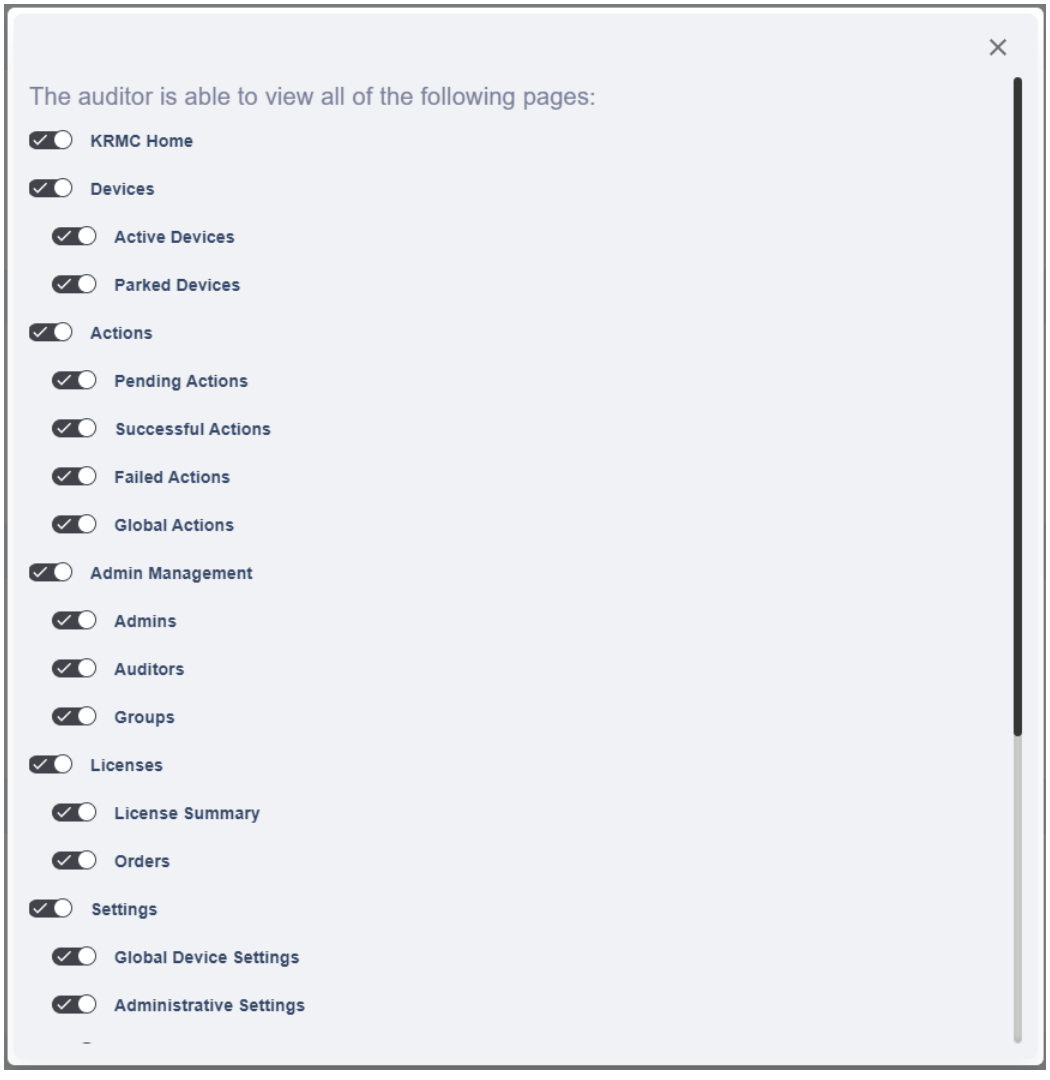
Account Permissions

Can See Only Drives Assigned to Super Administrator Groups	The auditor account is only able to see drives that has been assigned to the Super Administrator group. ***Note:*** *The option will change automatically if "Can See Drives Assigned To All Groups" is selected.*
Can See Drives Assigned to All Groups	The auditor account is only able to see all drives on the KRMC On-Premise account. ***Note:*** *The option will change automatically if "Can See Only Drives Assigned to Super Administrator Groups" is selected.*
Can View SSPM Codes	The auditor account can view the most recent SSPM code sent for a drive that is on KRMC
Can Export Device List	The auditor account can export the device list. ***Note:*** *This will only contain the information for drives that the auditor is able to see based on the setting "Can See Drives Assigned To All Groups".*
Can Export Action List	The auditor account can export the action list. ***Note:*** *This will only contain the information for drives that the auditor is able to see based on the setting "Can See Drives Assigned To All Groups".*
Can Export Event List	The auditor account can export the event list. ***Note:*** *This will only contain the information for drives that the auditor is able to see based on the setting "Can See Drives Assigned To All Groups".*


Account Access
Account Enabled
Account Locked
Account Permissions
Can See Only Drives Assigned To Super Administrator's Groups
Can See Drives Assigned To All Groups
Can View SSPM Codes
Can Export Device List
Can Export Actions List
Can Export Events List
SAVE
CANCEL

Edit Auditor Display

Edit Auditor Display allows you to change what pages are viewable for your auditor. In addition to choosing which pages are viewable to your auditor, you can also choose which page your auditor see when they first log into KRMC. ***Note:*** *If you are looking to use the feature "Set Permissions and Display Settings From Profile", you must set the permissions in this section as well as Edit Admin Permission for at least one auditor before use.*



Admin Management Page

10

Groups

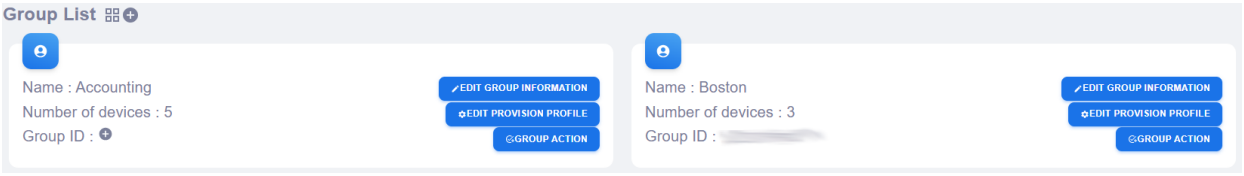
The **Groups** list on KRMC, displays all groups on your account. Groups, can provide the Super Administrator (SA) with increased control over permissions, requirements, and customizations with their drives. This can occur by specifying which Regular Administrators (RA) are allowed to manage the drives. Additionally, it provides the ability to give each group alternative settings to the SA Global Device Settings (as long as the settings are strict if not stricter then the SA Global Device Settings). For more information on Groups, please click HERE 62.

Each Group is listed with the following information:

Group Name	It is recommended to create a descriptive name for your Groups to make them easily recognizable.
Number of Devices	The number of devices assigned to this Group.
Group ID	This is an optional item that if generated allows drives to be registered directly to the group. If the group does not have a Group ID, the SA (or RA with the correct permissions) can select the plus icon to generate an ID.

In addition to the information provided on the groups, there are three management features also available.

Edit Group Information 160	Edit group allows you to modify the group name, description, generate a Group ID, administrators, and drives associated with the group.
Edit Provision Profile 162	Allows you configure default settings sent to all drives within the Group. These settings must be as strong if not stronger then the settings on the Global Device Profile set by the SA.
Group Action 163	Add group action provides the ability to send all devices on within this group an action.

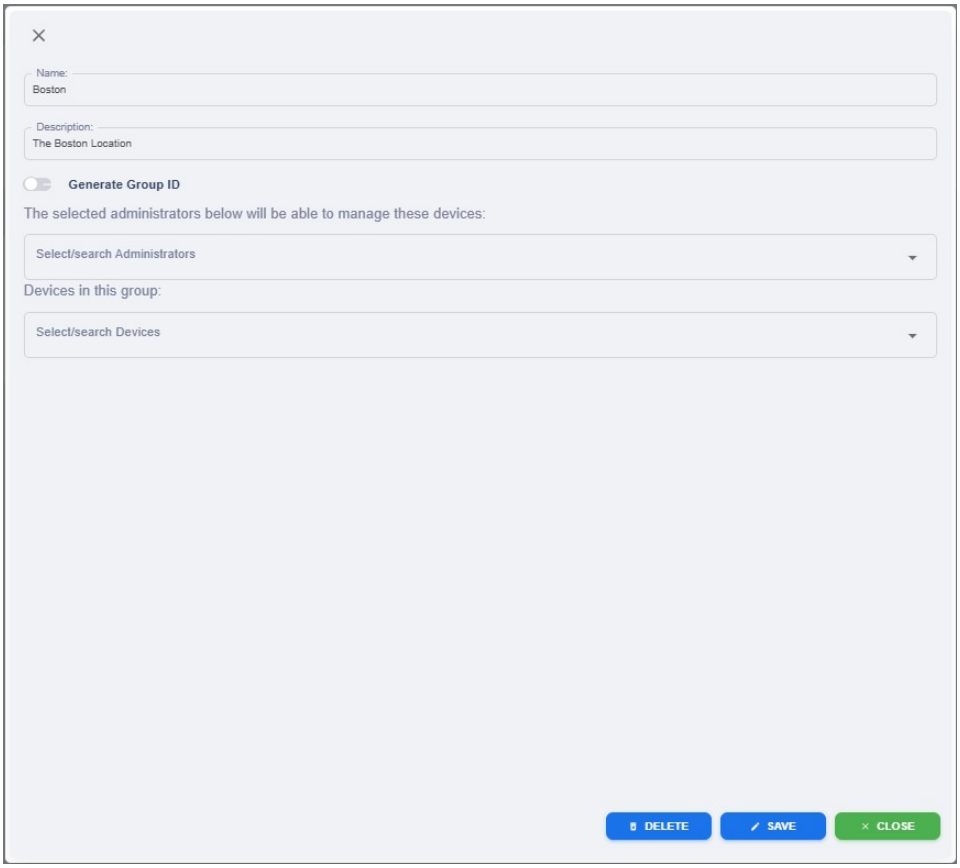


Edit Group Information

Super Administrators (SA) and Regular Administrators (RA) with access can change a Group's information by clicking the **Edit Group Information** button.

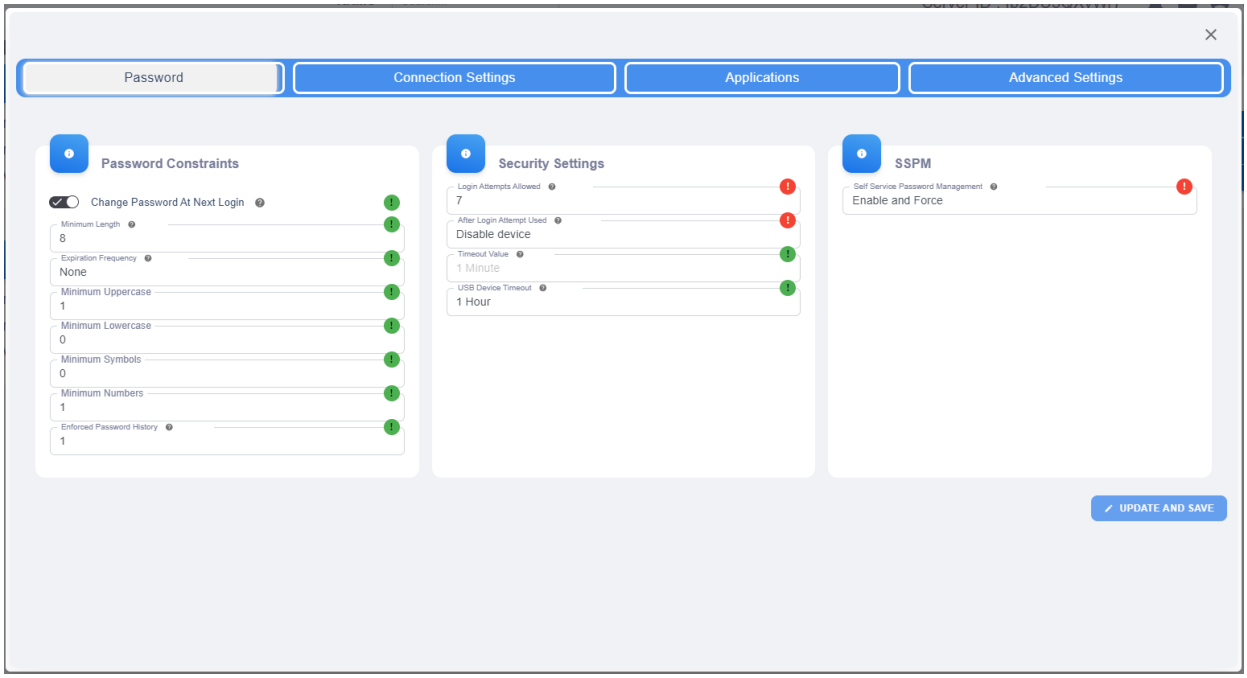
Edit Group Information change modify the following:

Name	The name of the group that is displayed both on the groups page but as well on the Device List.
Description	The description of the group. This is not visible anywhere except for Group Edit Information.
Generate Group ID	If your group does not already have a Group ID generated, you can enable this option and select Save. This will automatically generate a Group ID for this group. If your group already has a Group ID, this option will not be able to be toggled. ***Note:*** *Group IDs are not able to be deleted after being generated.*
Select/Search Administrators	You are able to select as many or as few RA accounts you would like to manage these drives. If no RA is selected, the drives in this group will only be able to managed by the SA or by an RA with the Advanced Account Ability of "Can See All Drives". For more information on Advanced Account Abilities, please click HERE 147.
Select/Search Administrators	This allows you to select which drives are in your group. ***Note:*** *Drives are only allowed to be in one group.*
Save	Saves all changes made within this menu.
Delete	Deletes the group from KRMC On-Premise. ***Note:*** *Deleted groups cannot be retrieved after deleted.*
Close	The window closes.


Name:
Boston
Description:
The Boston Location
Generate Group ID
The selected administrators below will be able to manage these devices:
Select/search Administrators
Devices in this group:
Select/search Devices
DELETE
SAVE
CLOSE

Edit Provision Profile

Edit Provisioning Profile provides each group the ability to have a security profile that is used as the standard configuration for all devices registered within this this group. These profiles must meet the minimum requirements set by the Global Device Settings. When a change is made to a setting within the Global Device Settings, the green icon to the right of each option will turn red. If you hover your mouse over the red icon, you will be shown what the setting was prior to the change. For more information on the settings and options available within this option, please refer to Global Device Settings 171.

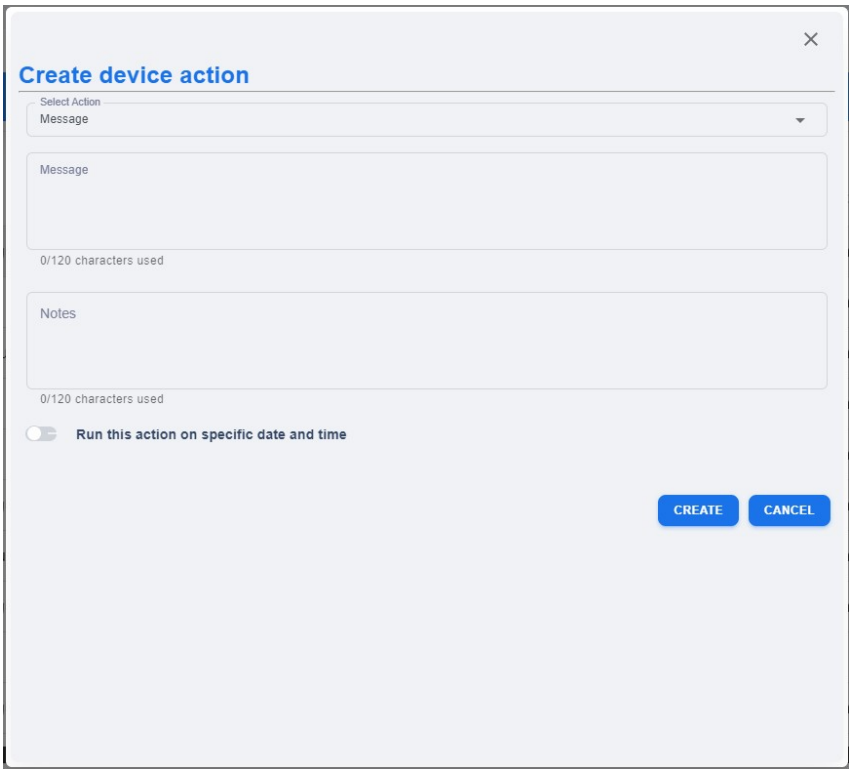


Group Action

Group Action will send an action to all drives within the group. The actions available to the Regular Administrator (RA) is dependent on their permissions as defined under Edit Admin Permissions 147. For a full list and description of actions available, please refer to Remote Action List 206.

The default fields that will be available for you are as follow:

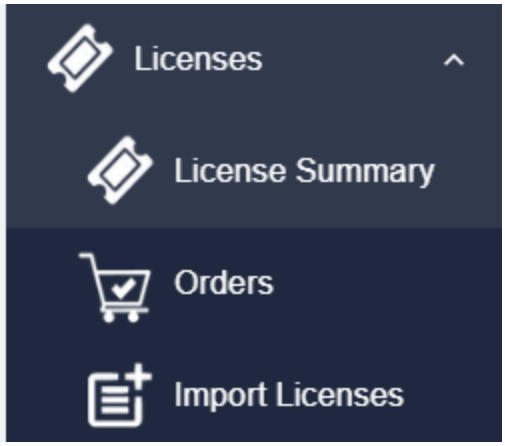
Select Action	This allows you to select the action that you are trying to send to all devices within this group. Note: Depending on the action selected, the fields below may change.
Message	A message is something that is displayed to the end user once the actions is received by the device.
Notes	This is an internal note about the action. This is not displayed to the end user.
Run this action on specific date and time	By default, a new action is scheduled to execute the next time the device is seen by the KRMC On-Premise server. If you want to delay the action until later, you can select Run this action on specific date and time and set a future date and time when the action can be executed. ***Note:*** *A scheduled action may not occur at the exact date and time set here. The action will be executed the next time the device communicates with KRMC On-Premise after the scheduled date and time.*
Create	This creates the action based on the options selected above.
Cancel	The actions creation is canceled.



Licenses Page 11

The **Licenses Page** allows you to view and manage your KRMC On-Premise device licenses. You can navigate to the various options by clicking on the icons or options on the navigation bar.

License Summary 165	The **License Summary** page displays a low-level overview of the current status of any KRMC On-Premise, Endpoint, and Parking licenses for devices registered with this KRMC On-Premise account.
Orders 167	Allows you to manage your license purchases directly from the web console.
Import Licenses 168	KRMC On-Premise licenses will be automatically sent to your server if EPP Connection Settings 198 have been configured. However if your server does not have this configured, the licenses will need to manually be imported into your server.



Licenses Page

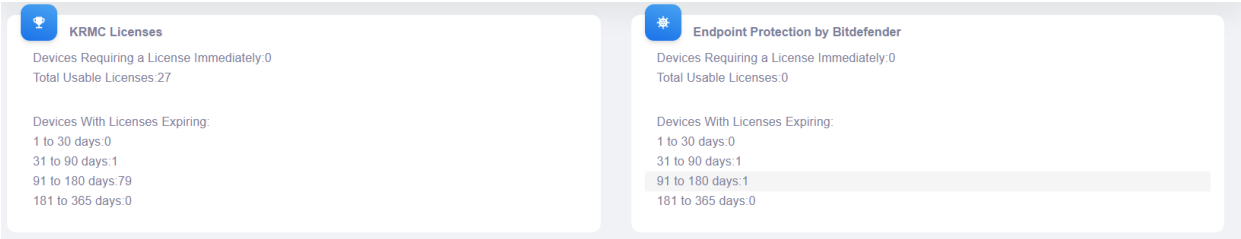
11

License Summary

The **License Summary** page displays a low-level overview of the current status of any KRMC On-Premise, Endpoint, and Parking licenses for devices registered with this KRMC On-Premise account.

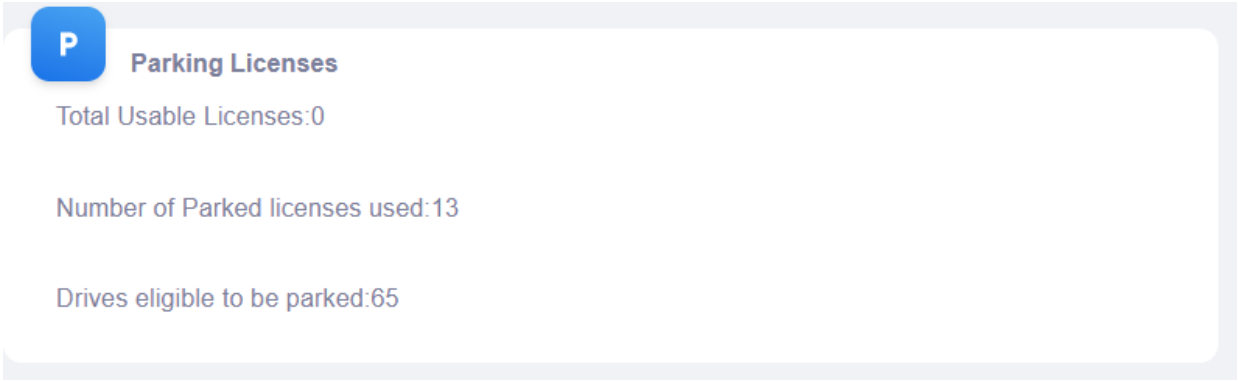
For KRMC Licenses and Endpoint Protection Licenses, you are provided the following breakdown:

Devices Requiring a License immediately	The number of devices which currently do not have a valid license.
Total Usable Licenses	The number of licenses available to be assigned to devices. These licenses are currently not assigned to any device.
Devices With Licenses Expiring	This information can be used to help determine when you need to purchase more licenses. It is good practice to always have enough licenses available to replace any licenses set to expire within 30 days.

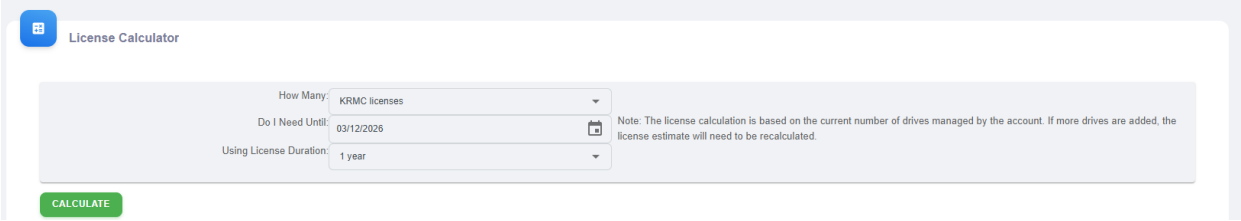


For Parking Licenses, you are provided the following breakdown:

Total Usable Licenses	The number of licenses available to be assigned to devices. These licenses are currently not assigned to any device.
Number of Parked Licenses Used	The total number of parked licenses that have been used on this KRMC On-Premise account.
Devices eligible to be parked	This is the total number of active drives (drives that have not been deleted or parked) that are eligible to be parked at this time. Drives that are considered eligible to be parked are drives that have not communicated with KRMC in 18 months or more.



You can easily figure out the number of licenses you will need to purchase in the future by entering a time frame into the license calculator located at the bottom of the License Summary page and then clicking the **Calculate** button.



Important! *Newly imported KRMC On-Premise and Endpoint Protection Licenses are automatically assigned to the most recently used (communicated with KRMC On-Premise) active device without a valid license. KRMC Licenses cannot be manually assigned to specific devices.*

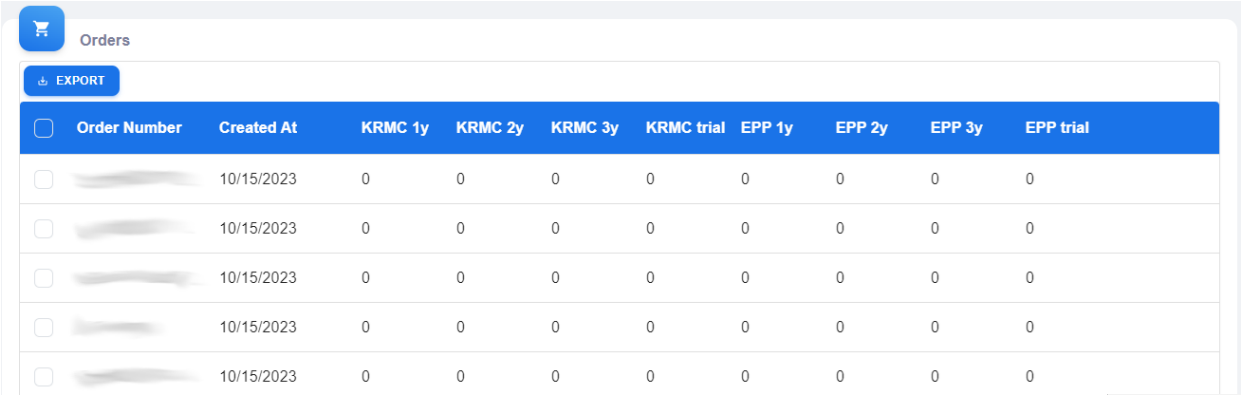
Licenses Page

11

Orders

The **Orders** page will allow you to view any orders that were processed on your account and displays the number of each license purchased with that order. ***Important!*** *Newly purchased KRMC On-Premise and AV Licenses are automatically assigned to the most recently used (communicated with KRMC On-Premise) active device without a valid license. KRMC Licenses cannot be manually assigned to specific devices.*

All orders displayed on this page are able to be exported either by selecting the check box next to specific orders and selecting "Export" or if you want full order list exported, then simply selecting "Export" with no check boxes selected. All exports on this page are in CSV format.

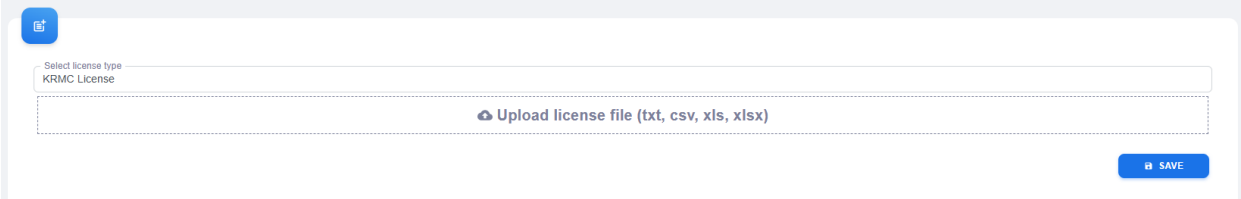


Licenses Page 11

Import Licenses

KRMC On-Premise licenses will be automatically sent to your server if EPP Connection Settings 198 have been configured. However if your server does not have this configured, the licenses will need to manually be imported into your server. There are four options within your Import Licenses:

KRMC Licenses	Licenses that allow KRMC On-Premise configured drives to communicate with the KRMC. If a device does not have a valid license, no actions will be received by the device.
EPP Licenses	Licenses that allow KRMC On-Premise configured drives to download new virus definitions and run onboard endpoint protection scans.
Parking Licenses	Parking Licenses allow a device to be parked temporarily in a suspended state. Click HERE 129 for more information on parking drives.
Premium Upgrade	This allows you to change your server Account Level between Advanced and Premium.



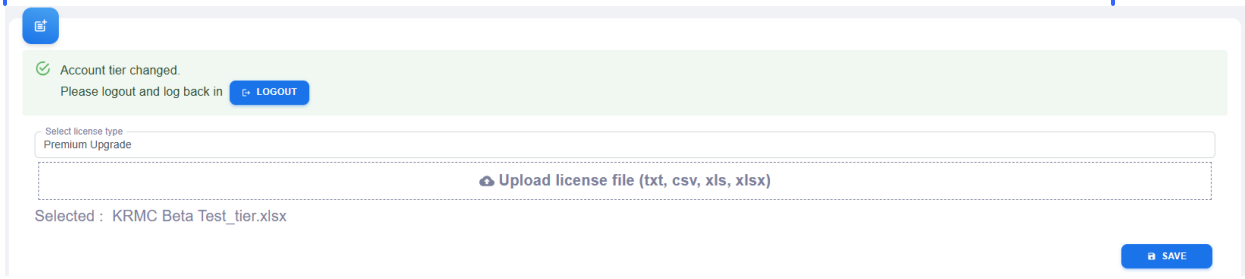
To add more licenses to your KRMC:

1. Select the license type that you are importing. The default selection is "**KRMC License**" however selecting that will display a dropdown menu that you can select between the available options.
2. Click on the "**Upload License File (txt, csv, xls, xlsx)**" browse button.
3. Navigate to and select the license file that you received from in your email when the order was placed. Click on the open button.
4. Click on the **Save** button to import the licenses into KRMC.

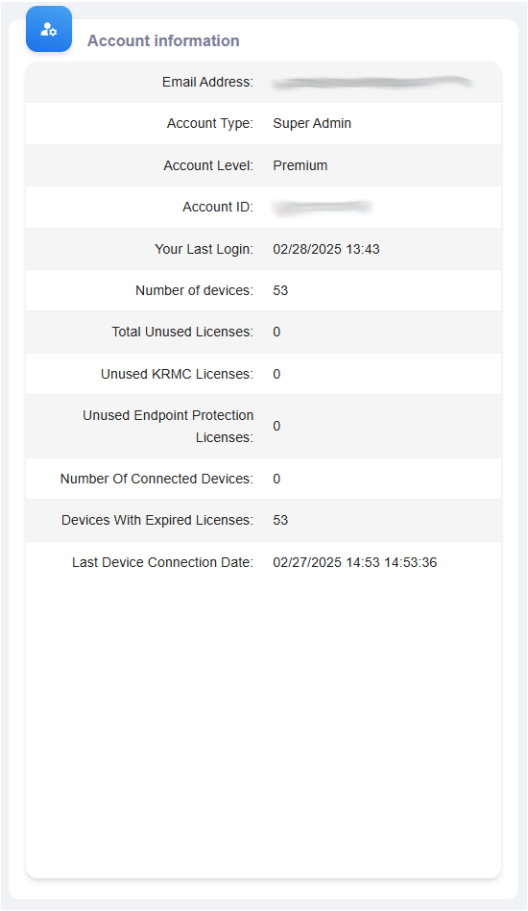
If you are changing Account Level, before selecting the KRMC licenses you are looking to import into your server you will need to perform an additional step. In order to perform the steps below, you will need to provide your Account ID 115.

To upgrade your Account Level:

1. In the "**Select License Type**" field, select "**Premium Upgrade**".
2. Click on the "**Upload License File (txt, csv, xls, xlsx)**" browse button.
3. Navigate to and select the license file that you received from in your email when the order was placed. Click on the open button. This file name will end with "**_tier.xlsx**".
4. By clicking the **Save** button, you will be informed of the change as well as told that you will need to logout of KRMC.



5. Once you log back into KRMC, you will notice that your **Account Level** will display the new **Account Level Premium**.



6. Navigate back to **Import Licenses** and this time select **KRMC Licenses**.
7. Click on the "**Upload License File (txt, csv, xls, xlsx)**" browse button.
8. Navigate to and select the license file that you received from in your email when the order was placed. Click on the open button.
9. Click on the **Save** button to import the licenses into KRMC.

Settings Page 12

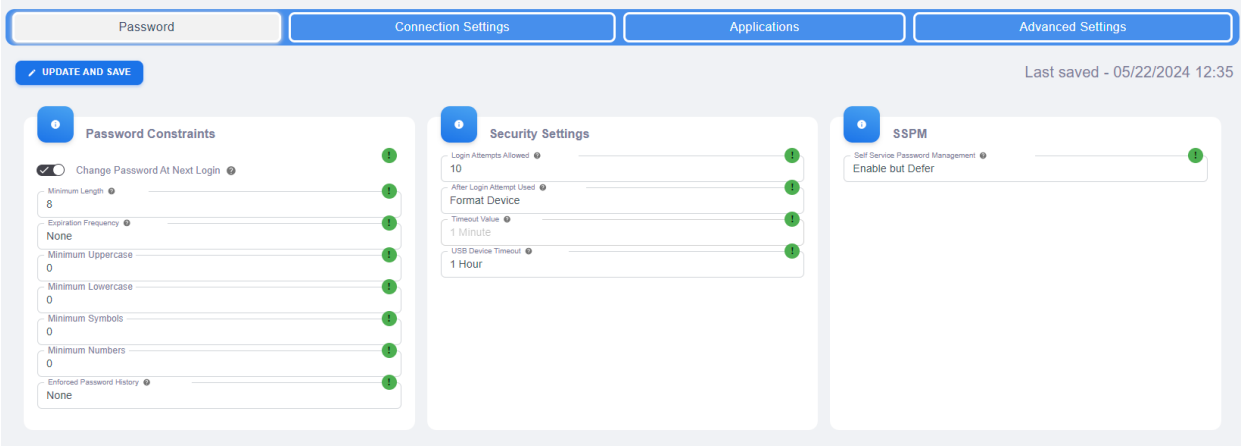
The **Settings Page** provides you with options for viewing and configuring KRMC On-Premise system settings. You can navigate to the various settings by clicking on the icons or options on the navigation bar.

Global Device Settings 171	Allows you configure default settings sent to all drives on your KRMC On-Premise account.
Notifications 178	Allows you to change what and how events are displayed within the events bar.
Administrative Settings 181	Allows you the ability to change the Administrative Password for KRMC On-Premise as well as enable additional features such as 2FA.
Server Settings 182	Allows you to alter general settings within the server such as date and time, date format, etc.
Email Templates 192	Automatic emails utilize a template which have the ability to be edited as the Admin would like or even have new ones created.
Mail Server 194	Mail Server provides the ability to configure/edit the email setting stored in your KRMC server. With no email settings stored in KRMC, you will not have access to Self-Service Password Management (SSPM), KRMC Forgot Password, and Two Factor Authentication (2FA).
Import Signed Certificate 195	KRMC On-Premise provides the ability to replace the self-signed certificate that you generate during your initial configuration of KRMC with your own signed certificate.
Import Database 196	KRMC On-Premise provides the ability to migrate your data from a previous KRMC 5, 6, or 7 installation to this new version of KRMC.
Update Server 197	iStorage Kanguru will provide updates to KRMC On-Premise regularly. When these occur, you can use Update Server to download an install the updates.
EPP Connection Settings 198	The EPP Connection Settings allows you to configure the internet settings that will allow KRMC to connect to the Kanguru Central Server and upload anti-virus definition updates which can then be pushed down to the drives. It also allows you to manually upload EPP definition files on offline servers to keep the device's onboard BitDefender Endpoint Protection software up to date.
Helpful Info 200	Displays iStorage Kanguru Support contact information as well provides access to the User Guide and the Provisioning Tool.
Release Notes	Displays the most recent release notes for the version of KRMC On-Premise.

Global Device Settings

The **Global Device Settings** are available to the Super Administrator (SA). It is a security profile that is used as the standard configuration for all devices registered within this KRMC On-Premise account. Additionally, you have the ability to have groups and each group can have their own device settings profile.

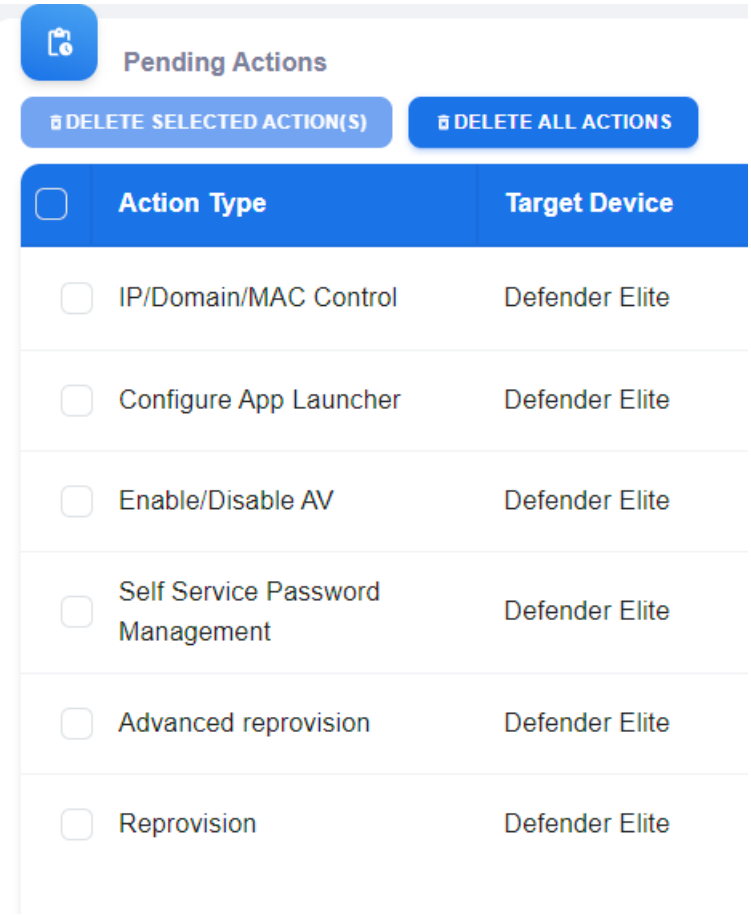
KRMC On-Premise devices must adhere to the Global/Group Device Setting. Administrators may configure separate device settings for individual devices and Groups, but these profiles must meet the minimum requirements set by the Global Device Settings. When a change is made to a setting within the Global Device Settings, the green icon to the right of each option will turn red. If you hover your mouse over the red icon, you will be shown what the setting was prior to the change.



Any changes made to the Global Device Settings will create the following actions all applicable devices:

Reprovision	This is a combination of Password Constraints and Security Settings located under the Password tab and Offline Access located under the Connection Settings tab on the Global Device Setting. The Reprovision action will provide the values for items such as minimum number of characters in a password.
Advanced Reprovision	This is the Advanced Settings options located under the Advanced Settings tab on the Global Device Setting. Additionally, Proxy Settings located under the Connection Settings tab on the Global Device Settings are within this action. The Advanced Reprovision action will provide the state that the settings should be in as well as if it is enabled then which settings to alter.
Self Service Password Management	The SSPM setting is located under the Password tab on the Global Device Setting. The Self Service Password Management action will provide the state that the application should be in.
Enable/Disable EPP	This setting is located under the Application tab on the Global Device Setting. The Enable/Disable Endpoint Protection (EPP) action will provide the state that the application should be in as well as if it is enabled then which option for Realtime Scanning should be selected.
Configure App Launcher	This setting is located under the Advanced Settings tab on the Global Device Setting. The Configure App Launcher action will provide the state

	that the setting should be in as well as if it is enabled then the name of the application that the services to use.
IP/Domain/Mac Control	This setting is located under the Connection Settings tab on the Global Device Setting. The IP/Domain/Mac Control action will provide the state that the setting should be in as well as if it is enabled then which settings to utilize moving forward.



Click on the **Update and Save** button to update the security policies for each device the next time they are seen by the KRMC On-Premise server.

If a device is in a group other then the default SA group, no actions will be sent to those devices. If the new Global Device Settings minimum requirements cause groups to no longer be in compliance, Groups will need to have their settings changed manually.

There are four tabs/sections within the Global Device Settings containing different settings in each. Here is a breakdown of the settings that are in section.

Password

Password Constraints	**Change Password at Next Login** - If selected, the user will have to change their password the next time they successfully login to their device.
	Password Length (8 - 15 characters) – The mandatory minimum number of characters a password must contain to be valid.
	Expiration Frequency (none, 30, 60, 90, 180, 360 days) – How often the system will force the user to change their user password.
	Minimum Uppercase/Lowercase/symbols/Numbers (0 - 5) – The minimum number of upper- and lower-case letters, symbols and digits a valid password must contain.
	Enforced Password History (none, 1 - 10) - The number of previously used passwords that may not be accepted as your current password. A higher number discourages users from alternating between several common passwords.
Security Settings	**Login Attempts Allowed (3 – 15 attempts)** - The number of times a user can incorrectly enter their password when attempting to login to the drive. A warning message will appear to inform the user when they have one attempt remaining.
	Format Device - The device will automatically format itself if the user exceeds the number of allowed password retries. This will erase all admin settings and user data stored on the device and reset the device to the factory default settings.
	Timeout - The device will automatically activate a timeout period if the user exceeds the number of allowed password retries. The user will have to wait for the timeout period to pass before they are allowed to attempt entering a password again.
	Disable Device - The device will become disabled if the user exceeds the number of allowed password retries. The device user will be unable to login to their device or access the device's secure partition again until it is enabled by an 'Enable Device' remote action.
	Timeout Value (1 Min, 2 Min, 5 Min, 10 Min, 30 Min) - How long the timeout period is. If the user exceeds the set number of password retries, the user will have to wait this long before they are allowed to enter a password again.
	USB Timeout (30 Min, 1 hr, 2 hr, 4 hr, No timeout) - This allows the admin the ability to set an idle timeout period where by if the device is not used for a specific period of time, then the drive will auto-unmount. ***Note**: The default setting is 1-hour.*
SSPM	The Self-Service Password Management feature allows the user to reset their own login password for a managed Defender device. Users must register an email address so that a password reset e-mail can be sent to the user.
	Enable and Force - Enable SSPM and force the user to register an e-mail the next time they use their device.

	Enable But Defer - Enable SSPM but allow the user to register an e-mail at a later time.
	Disable - Disable SSPM, preventing users from resetting the password on their device. If the user forgets their password, the only method of recovery is for the device administrator to create a 'Change User Password' action for the device.

Connection Settings

Access Control Settings	Create a list of IP Ranges or Domains or MAC addresses that you will either allow or restrict your devices to access KRMC On-Premise from. You can include multiple IP Ranges, Domains, or Mac addresses to the list.
	Enable Access Control - Check this box to enable IP/Domain/Mac control.
	Functionality - Select whether IP/Domain/Mac control will allow or deny certain IP ranges, Domains, or Mac addresses.
	Allow all Except (blocklist) - When selected, all devices will be allowed to access KRMC On-Premise unless it is located under any of the IP ranges, Domains, or Mac addresses listed.
	Deny all Except (safelist) - When selected, only devices that are located under any of the IP ranges, Domains, or Mac addresses listed will be able to access KRMC On-Premise.
	Control based - Select whether you want IP/Domain/Mac Control to be based on IP Range, Domain or MAC Address.
	IP Range - If you are looking to add an IP Range, enter the information into the fields provided. After entering the information select the "ADD" button directly underneath. After selecting "ADD" your range will appear under allowing you to add additional IP ranges if you would like. If you choose to remove the range, you can use the "DELETE" button that appears for you.
	Domain List - If you are looking to add a Domain, enter the information into the fields provided. After entering the information select the "ADD" button directly underneath. After selecting "ADD" your range will appear under allowing you to add additional domains if you would like. If you choose to remove the range, you can use the "DELETE" button that appears for you.
	Mac List - If you are looking to add a Mac address, enter the information into the fields provided. After entering the information select the "ADD" button directly underneath. After selecting "ADD" your range will appear under allowing you to add additional Mac addresses if

	you would like. If you choose to remove the range, you can use the "DELETE" button that appears for you.
Proxy Settings	**Enable Proxy Settings** - Check this box to enable Proxy settings.
	Proxy Address - This location you will enter the IP address or Proxy server name that you will be using.
	Proxy Type - Select from the drop-down the proxy type that is to be used. Our devices support HTTP, SOCKS4, and SOCKS5
	Proxy Username - If you Proxy service requires the usage of a username, you can enter it here. If your Proxy service does not require any username, then this can be left blank. ***Note**: This username will be sent to all drives.*
	Proxy password - If you Proxy service requires the usage of a password, you can enter it here. If your Proxy service does not require any password, then this can be left blank. ***Note:** This password will be sent to all drives.*
Offline Access	**Allow offline access (Unlimited, 1-100 Logins)** - If unselected, the device user will not be able to login to access the device's secure partition if the computer the device is connected to does not have internet access. When selected, the device user will be able to access the device's secure partition when there is no internet access. The number of logins on computers without internet access can be set as 1 login up to 100 logins. If "Unlimited" is selected, the device user will always be able to login to the device, regardless of internet access.

Applications

Endpoint Protection powered by Bitdefender	**Enable/Disable Endpoint Protection** – This option allows you to enable or disable the Endpoint Protection on the Defender device. ***Note**: This can only be set for user devices running KDM client version 5.6.6.2 and later.* If you Enable Endpoint Protection, you are then able to determine how the real-time scan works.
	Enable Real-Time Scan – Real-Time Scanning is enabled however the user scan disabled this at their choosing.
	Disable Real-Time Scan - Real-Time Scanning is disabled and the user is unable to enable it.
	Force Real-Time Scan - Real-Time Scanning is enabled and the user is unable to disable it.

Advanced Settings

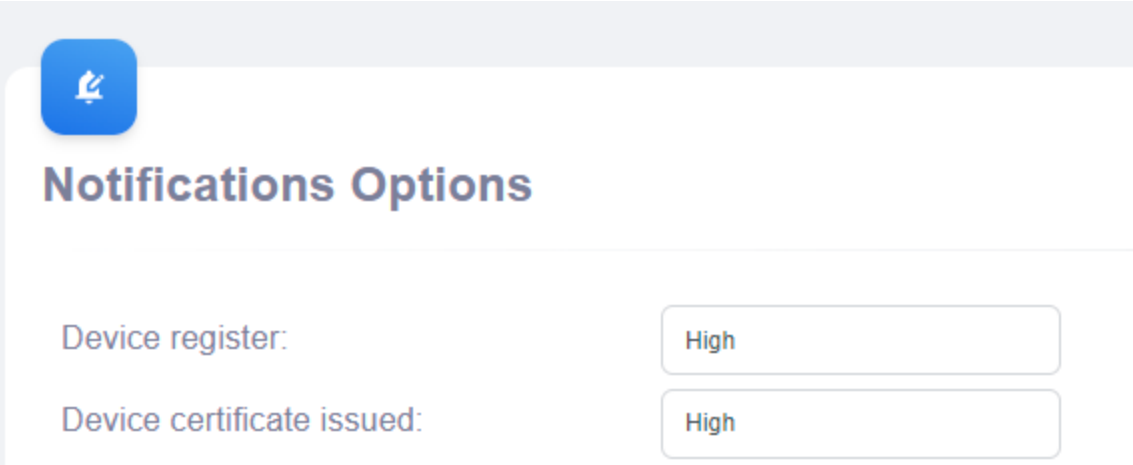
Advanced Settings	**Enable Advanced Settings** - This setting allows you to enable one or more of these settings under Advanced Settings. If this setting is disabled, no setting enabled within this section will be enabled.
	Allow Force Unmount - Enable this feature to allows you to unmount devices even if an application is still accessing data on the secure partition.
	Suppress pop up messages and warnings - Enable this feature to prevent any device messages that do not require any user interaction from being displayed, i.e. pop-up messages that only have an 'OK' button. Pop-up messages that require user input will still be displayed. Additionally, this feature to prevent the warning message that usually shows when a drive is improperly disconnected from being displayed.
	Unmount security partition at user logoff - When selected, the secure partition will automatically unmount when the user logs off the computer the device is connected to.
	Unmount security partition at hibernate / sleep - When selected, the secure partition will automatically unmount if the computer the device is connected to enters hibernate or sleep mode.
	Enable Write Protection (Defender 2000/3000 devices) - The Defender 2000 and 3000 devices do not have a physical write protect switch option but rather a software write protect option. Enabling this setting will turn on the write protect feature, making the Defender 2000 and 3000 a read-only device. The device user will not have the ability to turn the write protect feature off.
	Disable Logging - The Defender drive keeps a track of its internal working in encrypted log files on the user's computer. These logs do not store any user data like files/folders, are never sent automatically to iStorage Kanguru, and contain only internal information related to the KDM application. This action helps you enable/disable the drive's logging feature. ***Note:*** *that disabling drive logs might inhibit our ability to help you troubleshoot technical issues.*
	Show Contact Information - The Customer Info section allows you to configure whether the device user's contact information is displayed when logging into their Defender device. By default, no information is shown. Enable show customer info to allow contact information to be displayed when logging in to the device. You have two options for information that can be displayed.
	Show limited customer info at KDM client login screen - The user's name and telephone number are displayed.
	Show full customer info at KDM client login screen - The user's name, telephone number, e-mail and department information are displayed.
	Show Reset to Factory button at KDM Login Screen - The client application login screen has a button for resetting the device to the factory

	default settings. You can choose whether or not the end user will have this option available
	Panic Mode - A device operating in Panic Mode must be seen by the server in the designated time period. If the device is not seen by the KRMC server during this time, the device will be identified as lost and the next time it is accessed, a specified action will occur. The application will be able to be disabled, disabled and have all data removed, or have all data removed and the user will need to set the device up once again.
Device App Launcher	**Configure App Launcher -** This section is where you can configure a device to auto-execute an application stored on the device. The Auto Run feature will execute every time the device's end user successfully logs into their drive and mounts the device's secure partition. If the file name is entered incorrectly or if the file does not exist on the drive, the end user will receive the following error message: "The process set for auto acquisition failed to start. File not found."

Settings Page 12

Notifications

The **Notification** page determines which events appear within Events 202 as well as if you receive any email notifications.



There are three status options for event types:

Off	Events that have been set to Off will not be displayed within the Events page.
On	Events that have been set to On will be displayed within the Events page.
High	Events that have been set to High will be displayed within the Events page. Additionally, email notifications can occur to select email addresses.

Event Descriptions

Device Register	A new device has been registered with your KRMC Server
Device Certificate Issued	A Device has been issued a new certificate for communication with KRMC.
Device Command Executed	An action has been received by the device.
Admin Created a New Command	The admin has created a new action for a device.
Admin Canceled a Command	The admin has deleted an action for a device before it was received by the device.
Failed KRMC Login	There was a failed login attempt on the KRMC account.
Group Created	A group was created.
Group Deleted	A group was deleted.
Action Run on Group	An action was created for all drives in a group.
Devices Added to Group	A device has been added to a group.
Devices Removed from Group	A device has been removed from a group.
Successful KRMC Login	An Administrator successfully logs in to KRMC On-Premise.
Multiple devices action	A new remote action is created for multiple devices.
Successful KRMC Logout	An Administrator successfully logs out of KRMC On-Premise.

Device State Change	The status of a device changes between Active and Disabled.
Send Mail	An admin sends an email to a device user using KRMC On-Premise.
Admin Created	An Administrator has been created.
Auditor Created	An Auditor has been created.
Admin Deleted	An Administrator has been deleted.
Auditor Deleted	An Auditor has been deleted.
Admin Permission Updated	Permissions for an Administrator has been changed.
Auditor Permission Updated	The display options for an Administrator has been changed.
Admin Display Updated	Permissions for an Auditor has been changed.
Auditor Display Updated	The display options for an Auditor has been changed.
Admin Updated	An Administrator has been edited.
Auditor Updated	An Auditor has been edited.
Group Updated	A group has been edited.
Global Settings Updated	The Global Device Settings have been updated. The new settings will appear in Info.
Group Device Settings Updated	The Group Device Settings have been updated. The new settings will appear in Info.
SA Changed	The Super Administrator (SA) for the KRMC On-Premise account has been changed.
Export	Information from KRMC On-Premise has been exported.
Device Deleted	A device has been deleted from the KRMC On-Premise account.
Device Settings Updated	The settings to a drive have been edited.
Device Updated	The application on a drive has been updated to the latest version.
Delete All Actions	All pending actions for a drive(s) has been deleted.
AD Disable : The drive was disabled because the owner's account in Active Directory was disabled	A drive is disabled due to an Active Directory disable action.
New File Audit Info	A new file has been logged within File Auditing.
Server Settings Changed	Any changes within Server Settings, Administrative Settings, and Notification Settings.
Mail Server Settings Failed	The Mail Server setting have failed to be properly configured.
License Import	Licenses have been imported into KRMC.
Tier Update	The KRMC Account Level has changed from Advanced to Premium.

The Super Administrator (SA) is also able to have automatic e-mail alerts sent to up to five email addresses with triggers.

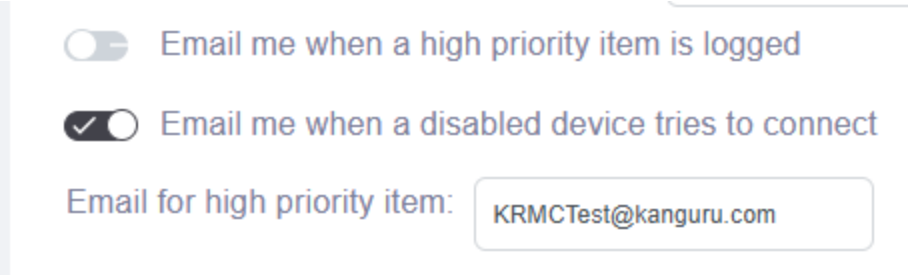
E-Mail Triggers

- Email Me When a High Priority Item is Logged

- Email me when a disabled device tries to connect

To enable email feature:

1) Select any/all email trigger options.
2) Navigate to “Email for high priority item” and select the field provided.
3) Enter an email address in the field provided. If you are looking to have multiple email addresses added, separate each one with a semicolon “;”.
4) Select the Update and Save located at the bottom right of the screen.



Settings Page

12

Administrative Settings

Administrative Settings allows you to change the Administrative Password. The Administrative Password is a system-wide password that is required when creating security sensitive actions like Change User Password. Click on the save button to create or change the Administrative Password. Creating or changing the Administrative Password will create a new action for all devices registered with this KRMC On-Premise account. ***Note**: If "Hide Device Message" is enabled, the users will not receive any notification from the Defender that the action was received.*

Force 2 Factor Authentication for Administrators logging into KRMC On-Premise.

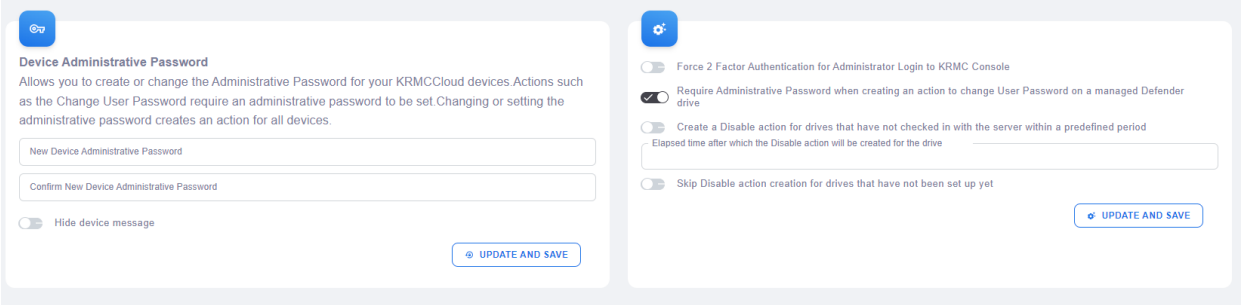
- When enabled, all current admins will be required to log in to KRMC On-Premise using both their login password as well as an authentication code delivered by e-mail or with Google Authenticator. Any new administrators created while this option is enabled will also be required to login with 2FA. The default 2FA methodology setup utilizing this option is e-mail however if you want to change this to Google Authenticator for individual accounts, please click HERE[49].
- ***Important!** If you disable "Force 2 Factor Authentication" from the **Administrative Settings Tab**, it will only prevent new administrators who are created after this option is disabled from having to use 2FA during login by default. Any administrators that previously had to login with 2FA will still have to do so. To disable the requirement for an administrator to login using 2FA, it must be manually disabled for the individual administrators.*

Require Administrative Password when creating an action to Change User Password on a managed Defender drive.

- When enabled, all administrators with permissions to perform a Change User Password action will be required to enter the Administrative Password before the action can be sent to the user.
- ***Note**: This will require all administrators to know that the Administrative Password is as it will not be unique per administrator.*

Create a Disable action for drives that have not checked in with the server within a predefined period.

- When enabled, after a predefined period of time elapses since the Defender has last communicated with KRMC On-Premise a disable action will be automatically generated for the device. Users receive two emails during this process with the first being 10-day prior to the event occurring and the second being 1-day before the event occurring.
- ***Note**: If you have drives that have not completed the setup process yet and the SA chooses, these drives can be skipped for this disable feature.*



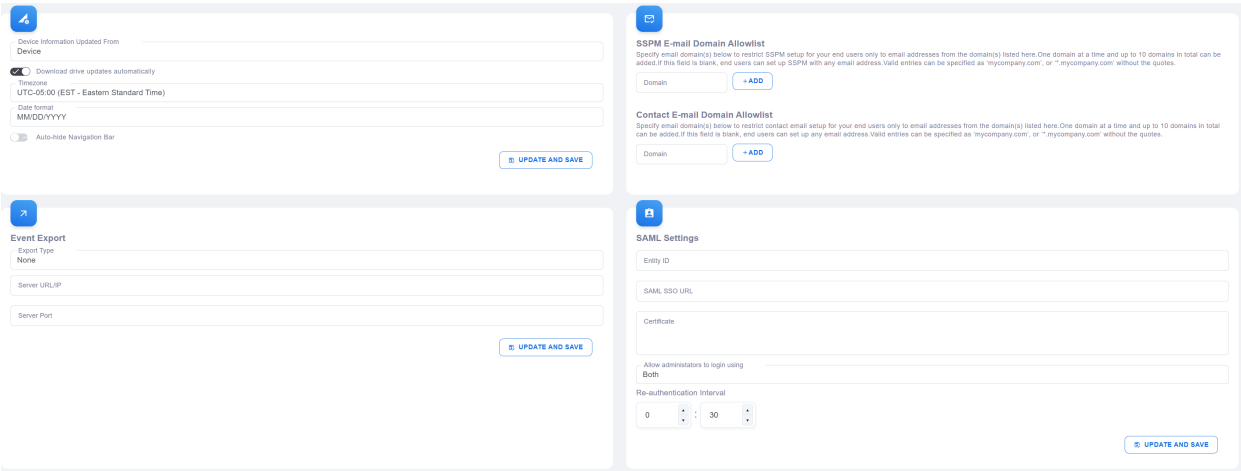
Settings Page

12

Server Settings

The **Server Settings** page allows you to view and change some server level settings.

General Server Settings 183	Settings such as date and time formats and whether updates are pushed to your drives are located within General Server Settings.
E-mail Domain Allowlist 184	KRMC On-Premise administrators can specify email domain(s) to restrict email addresses used for both SSPM and Contact information from the domain(s) listed.
Event Export 185	KRMC On-Premise events can be sent to a log server of your choosing.
SAML Settings 187	Setting that allows you to log into KRMC On-Premise using SSO.
Light or Dark Mode 188	This allows you to set the visual theme of KRMC On-Premise between a light or dark theme.
Data Visualization Mode 189	This alters the default view of data within KRMC On-Premise from a more graphical view to a more standard list based view.
AD Integration Device Disable 190	AD Integration syncs disabled users with Defender drives based on email address. If a user in Active Directory is disabled, any drive that matches their email address will be disabled.
File Audit 191	This allows you to set which File Auditing events appear within the File Auditing section.



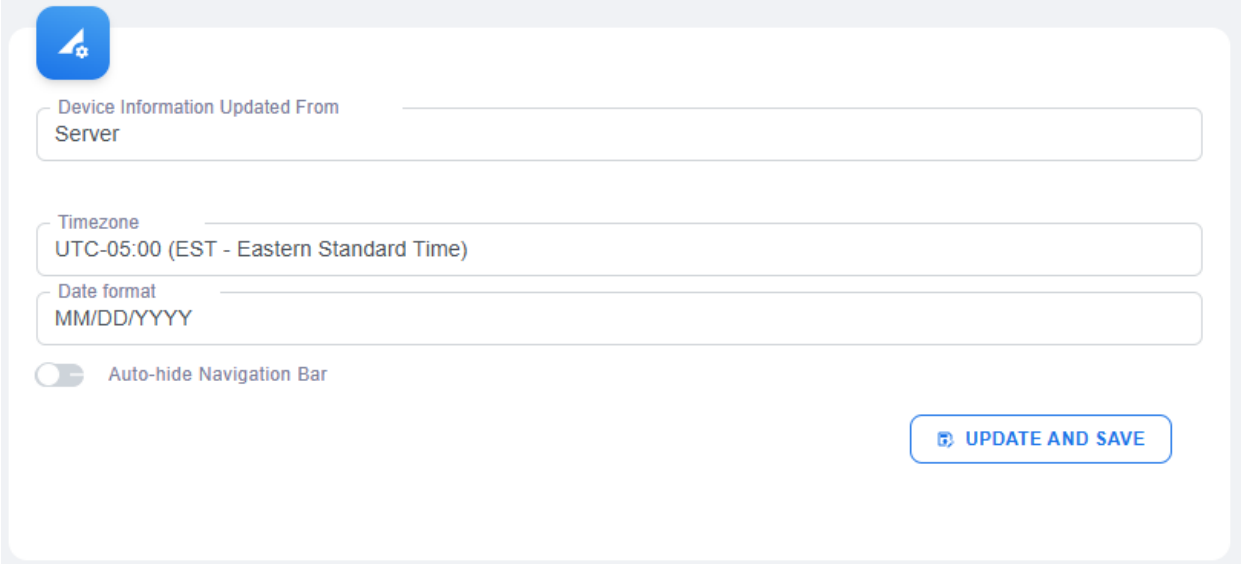
Settings Page

12

General Server Settings

KRMC On-Premise provides the ability to alter general settings on the account such as Date and Time formats. Here is a full list of the settings available.

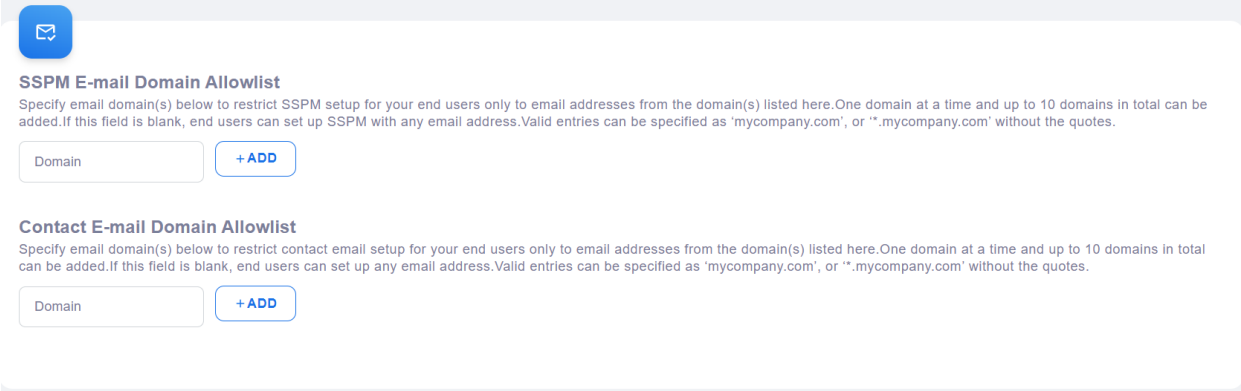
Device Information Updated From	Select how device information is synched with KRMC.	
	Device	Information is read from the device and updated in KRMC. Any changes to device information made directly through the device will override information saved in KRMC.
	Server	Information is read from KRMC and updated to the device. Any changes made to device information in KRMC will override the information saved on the device.
Time zone	Set the Time zone that you want your KRMC account set in. All your scheduled actions and events will occur and be recorded based on the Time zone that your KRMC account is set to. If you change your timezone to a different one, only events after that change will be represented in that new timezone.	
Date Format	Set the Date format that you want your KRMC account set in. All your scheduled actions and events will occur and be recorded based on the Date format that your KRMC account is set to.	
Navigation Bar Auto-Hide	This sets the state of the left side navigation bar to either Auto-Hide or remain showing. This setting will also be set from the top of the navigation bar.	



E-mail Domain Allowlist

Self Service Password Management (SSPM) is an optional feature available on most Defender devices. SSPM is an automated email service that provides device users with a secure method for resetting a device's password remotely, without any intervention from a KRMC On-Premise administrator.

KRMC On-Premise administrators can specify email domain(s) to restrict SSPM setup and or the user contact email address to an email address from the domain(s) listed. allowlisted domains can be added one at a time, up to 10 domains in total. Valid entries can be specified as 'mycompany.com', or '*.mycompany.com' without the quotes. ***Important!*** *If no domains are specified, then end users will be able to use any email address.*

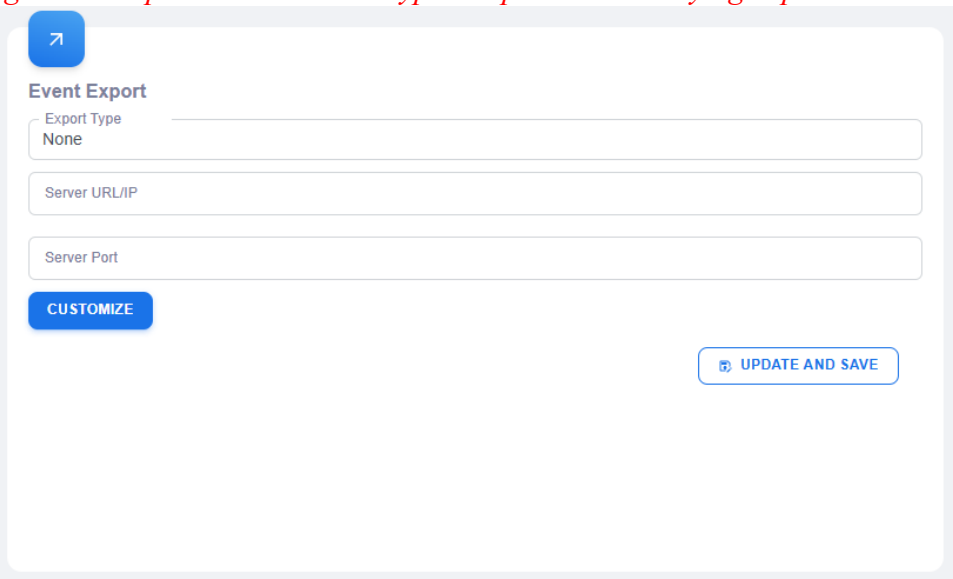


Note*: Defender Devices being registered for SSPM require a minimum version of KDM v5.1.3.4 or later. Defender HDDs and SSDs are currently not supported.*

Event Export (SIEM)

KRMC On-Premise Premium accounts have the ability to export events recorded by KRMC On-Premise to a customer's SIEM server in real time. Exporting to Splunk, Graylog, and to a generic Syslog server is supported in the current KRMC On-Premise release. Events that are exported to such a server are located within the Notification 178 options located under the Setting Page 170.

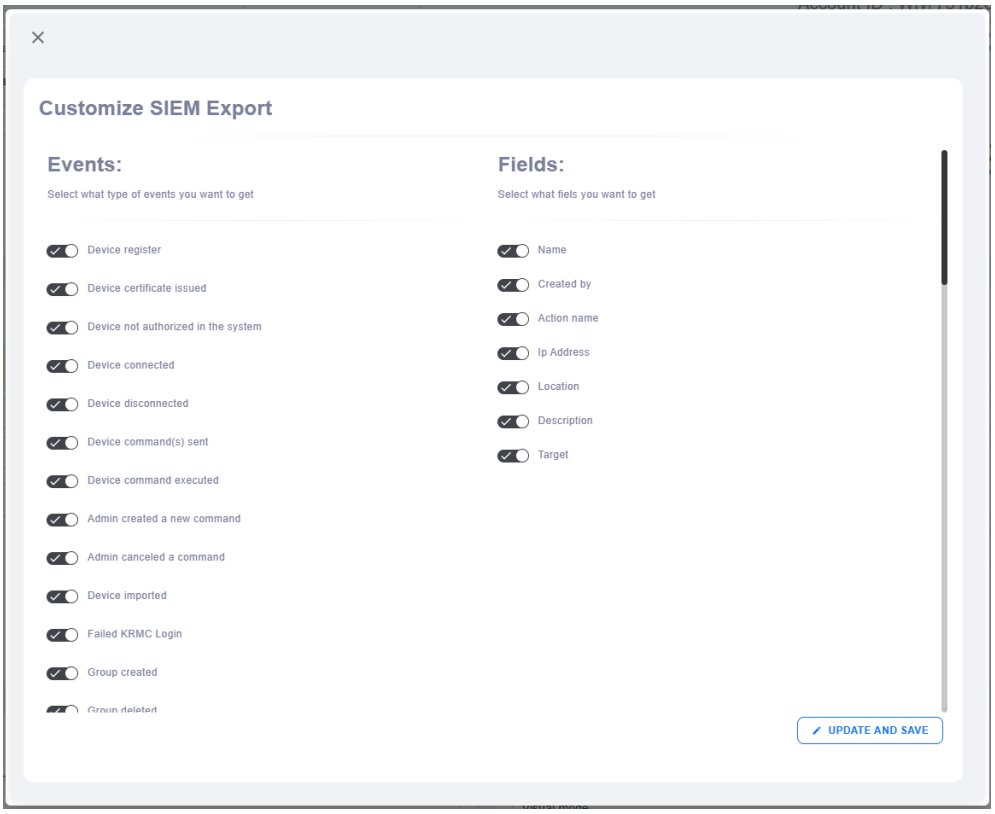
***Note**: Syslog server exports will be unencrypted. Splunk and Graylog exports will be encrypted.*



The option Customize allows you to choose which events are sent to your configured SIEM server as well as what fields are sent such as Name and Created By.

Settings Page

12



SAML Settings

If you are using Active Directory (AD) based Single Sign On (SSO) using Security Assertion Markup Language (SAML), KRMC On-Premise administrators can use this option to sign-in to their KRMC On-Premise account. SAML Settings must be configured and saved to allow administrators to login using the SSO URL for authentication through their own SAML supported AD service.

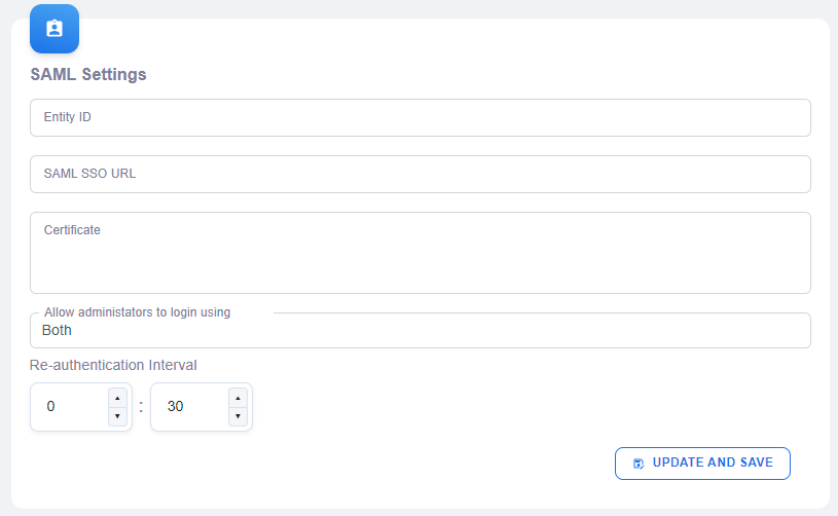
You can choose to **Allow administrators to login using** KRMC, SAML only, or Both. This setting allows you to choose how administrators on KRMC On-Premise are able to log into KRMC On-Premise.

KRMC On-Premise Only	Requires admins to utilize their KRMC On-Premise login credentials and does not utilize SAML. All attempts to utilize SAML will result in the login failing.
AD Federation SAML Only	Requires all Regular Administrators (RA) to only login utilizing SAML. All attempts to utilize standard KRMC On-Premise login will fail.
Both	Allows the administrator the ability to choose which login type they would like to use. ***Note:*** *The SA will always be able to use both regardless of which option is selected.*

The following links show how to perform the steps for KRMC Hosted however will work for KRMC On-Premise with two corrections:

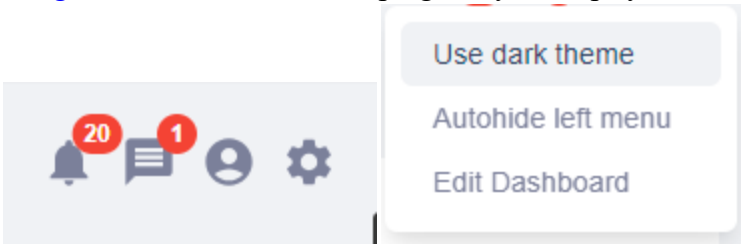
- SSO URL - https://<KRMC_IP_Address>/app.php/saml_login
- Entity IP - https://<KRMC_IP_Address>

For steps on how to connect KRMC On-Premise to your OKTA, please click HERE.
For steps on how to connect KRMC On-Premise to your Microsoft Azure, please click HERE.
For steps on how to connect KRMC On-Premise to your Microsoft Active Directory Federation Services, please click HERE.

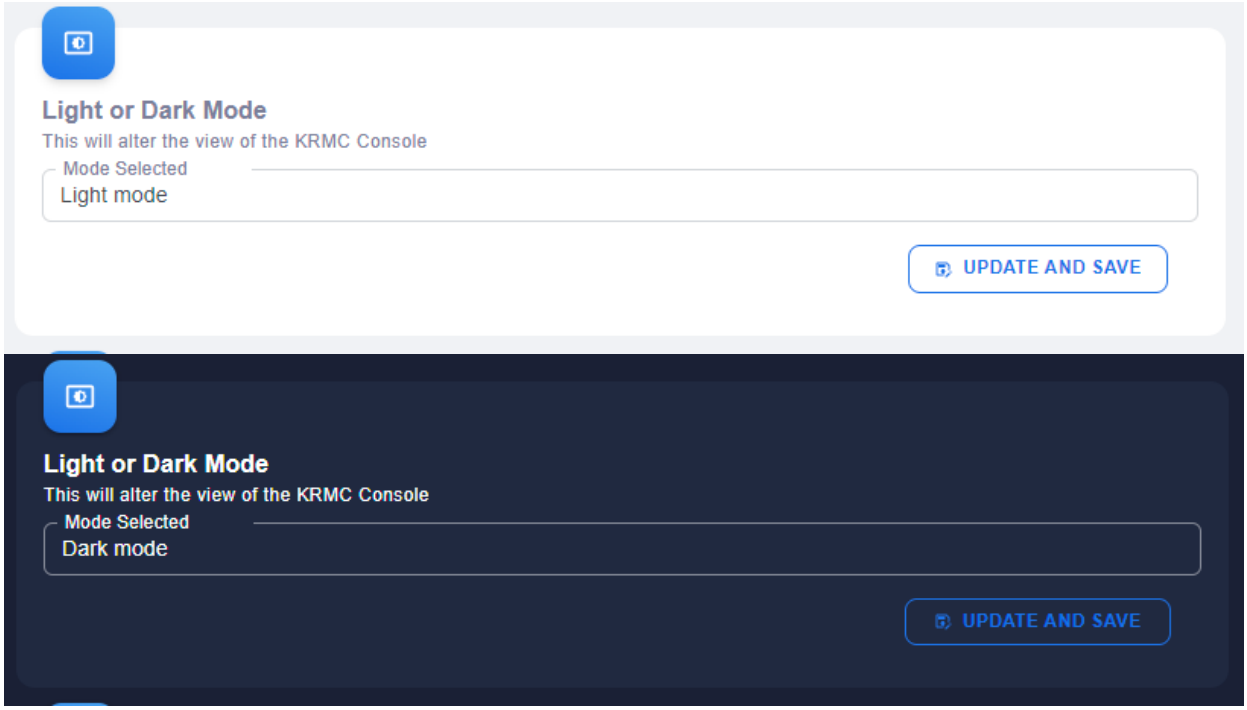


Light or Dark Mode

KRMC On-Premise provides the ability to alter the visual theme between a Light or Dark mode. To alter the theme you can either use the option located in Server Settings or by using the option located within the Account Settings icon located at the top right of your display.



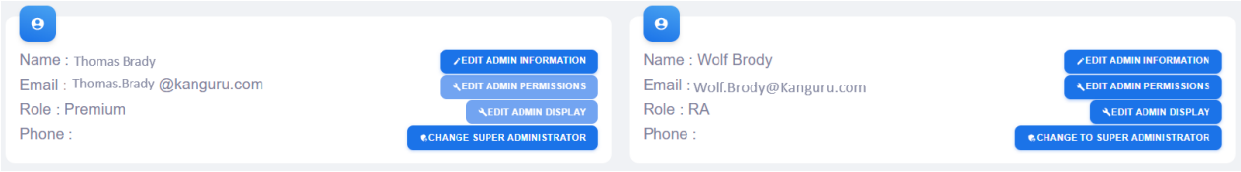
Note: *This setting will only impact your account and will not impact the appearance for your secondary administrators or auditors.*



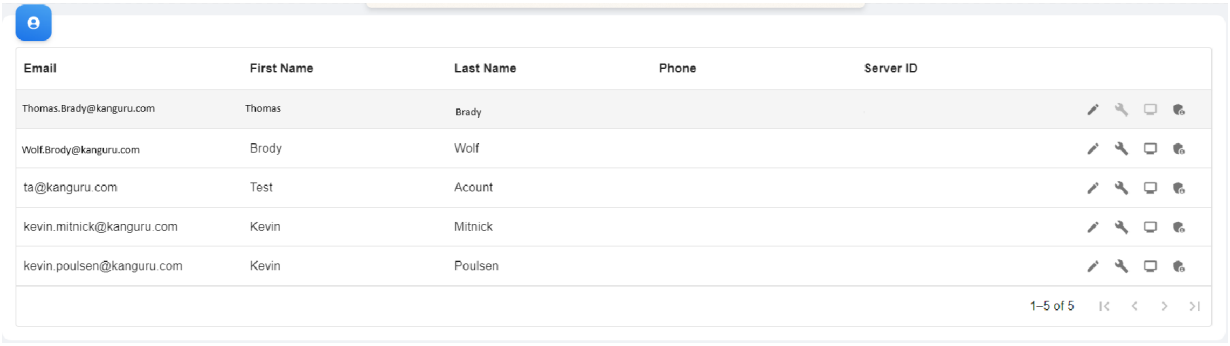
Data Visualization Mode

KRMC On-Premise provides the ability to alter the method in which data is displayed by default on Admin Management 143. There are two visualization options:

Visual Mode: This mode as seen below is more visual based to make understanding and navigation simplified.



List Mode: This mode as seen below is less visually impactful and displays all content in a more traditional list format.

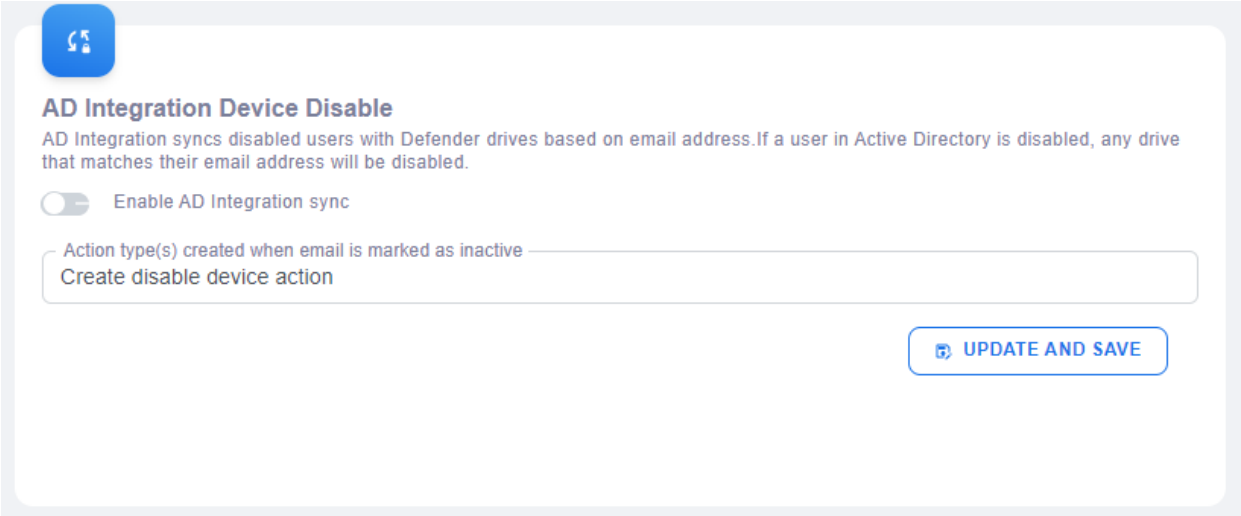


AD Integration Device Disable

KRMC On-Premise Premium accounts have the ability to utilize the AD Integration Device Disable feature. AD Integration syncs disabled users with Defender drives based on email address. If a user in Active Directory is disabled, any drive that matches their email address will have a Disable action automatically created for it. For steps on how to install and setup Kanguru Active Directory Service (KADService), refer to Kanguru Active Directory Setup 211.

There are two options:

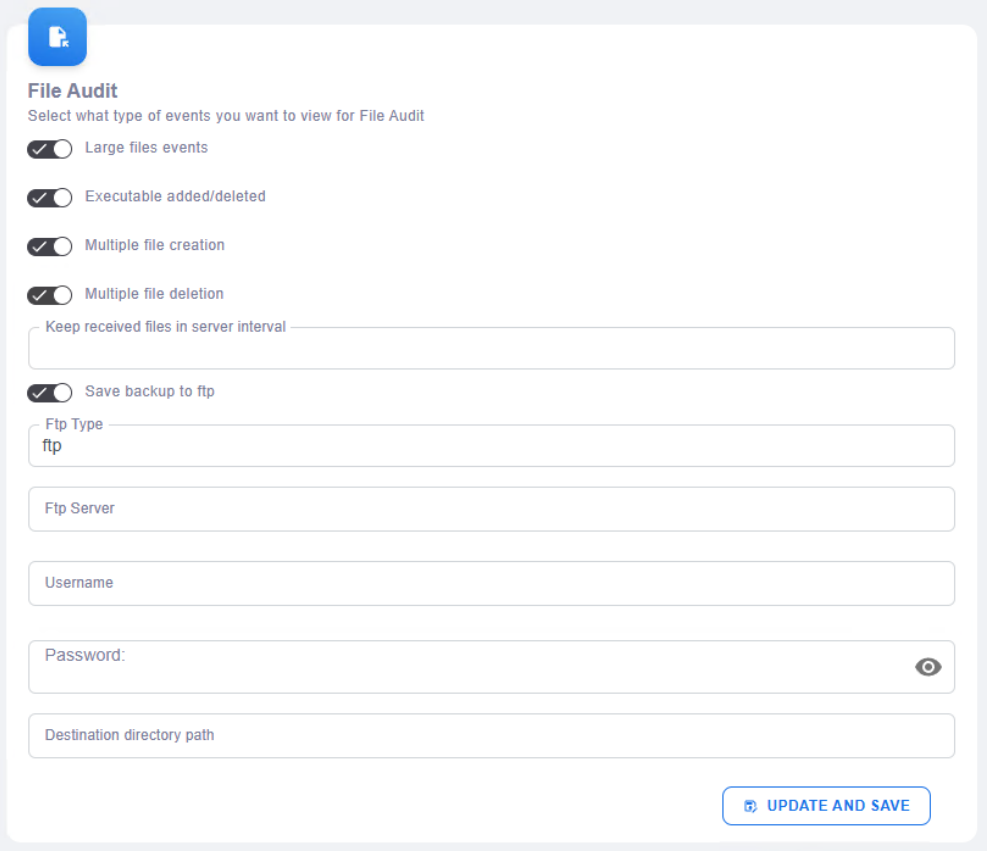
- Create Disable Device Action
- Create Disable Device and Reset For New User Action



File Audit

KRMC On-Premise Premium accounts have the ability to utilize the File Auditing feature. When this feature is used, KRMC will receive file monitoring updates from active Defender devices reporting file modifications. For more information on File Auditing, click HERE 204. This setting provides you the ability to selecting which events you want to view within the File Auditing Page on KRMC. ***Note:*** *File Auditing is only available with Premium KRMC On-Premise accounts and on devices with KDM version of 5.6.7.5 or newer.*

Large file events	Any file 1gb or larger will trigger an event being recorded within Events.
Executable added/deleted	An executable file being added or removed from the device will trigger an event being recorded within Events.
Multiple file creation	If multiple files are added to the device, this trigger an event being recorded within Events.
Multiple file deletion	If multiple files are removed to the device, this trigger an event being recorded within Events.
Keep received fines in server interval	To save space on your server, you are able to dictate how long File Audit results remain on your server. The default setting is 30-days.
Save backup to FTP	You are able to offload your File Audit results to an FTP server if you would like. If you select this, you will need to complete the fields provided to connect to the FTP server.



Settings Page 12

Email Templates

KRMC On-Premise provides the ability to create and edit email templates for use using the Email 122 feature. Pre-existing email templates are sent automatically when an action triggers it. For instance, if an administrator/auditor has failed its login multiple times, its account will then be locked. At that point, the Account Reactivation email template will be automatically sent to the account email. ***Note:*** *This is only available if you have configured Mail Server* 194.

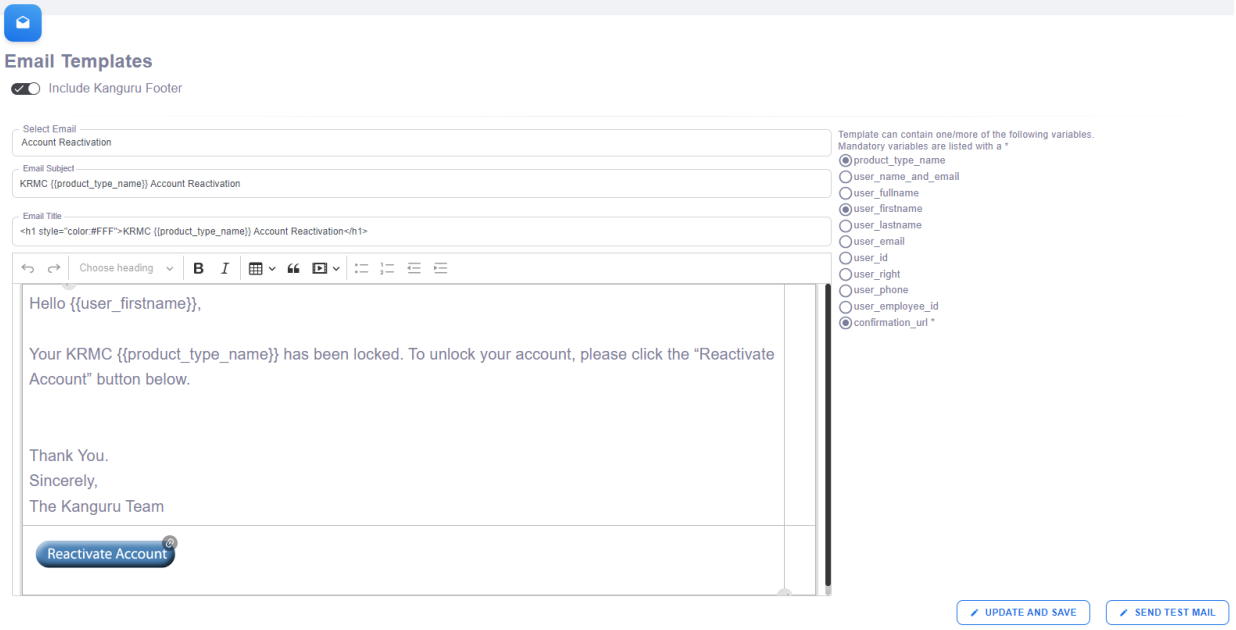
The the ability to access this for Regular Administrator (RA) is dependent on their permissions as defined under Edit Admin Permissions 147.

You also have the ability to create email templates. Manually generated templates are unable to be triggered to be automatically sent however if you select one or multiple devices in the Devices 117, you will be able to select that newly created email template.

Automatic Email Triggers provide the ability to edit not only the body of the email but also allows you to utilize the following variables:

- product_type_name
- user_name_and_email
- user_fullname
- user_firstname
- user_lastname
- user_email
- user_id
- user_right
- user_phone
- user_employee_id
- confirmation_url *

Select Email	Allows you to select which email template you would like to alter. Additionally, you can select "Create New" to generate a new email template.
Email Subject	Allows you to alter the subject line for the email.
Email Title	Provides the ability to alter the look of the template using HTML.
Email Body	Shows all the content in the email itself allowing you to make changes as you see fit.


Email Templates
Include Kanguru Footer
Select Email
Account Reactivation
Email Subject
KRMC {{product_type_name}} Account Reactivation
Email Title
<h1 style="color:#FFF">KRMC {{product_type_name}} Account Reactivation</h1>
Choose heading
Hello {{user_firstname}},
Your KRMC {{product_type_name}} has been locked. To unlock your account, please click the "Reactivate Account" button below.
Thank You.
Sincerely,
The Kanguru Team
Reactivate Account
Template can contain one/more of the following variables. Mandatory variables are listed with a *
product_type_name
user_name_and_email
user_fullname
user_firstname
user_lastname
user_email
user_id
user_right
user_phone
user_employee_id
confirmation_url *
UPDATE AND SAVE
SEND TEST MAIL

Settings Page 12

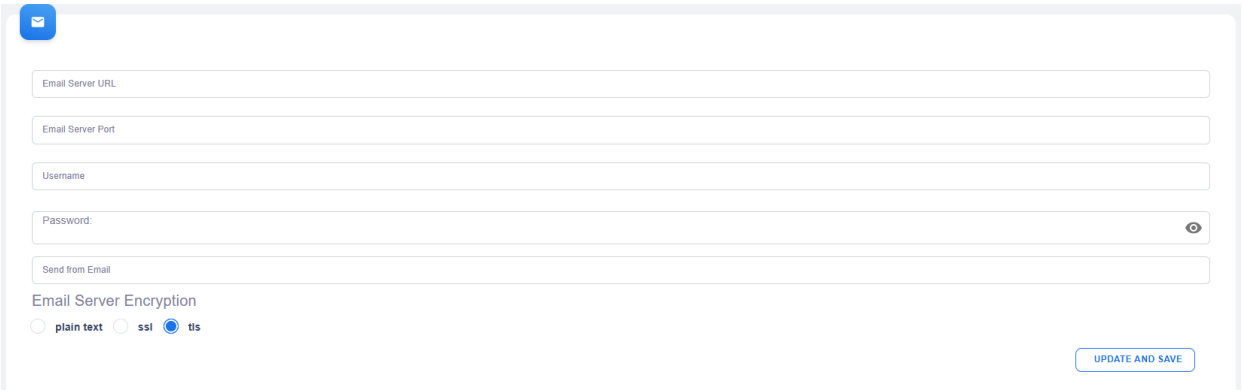
Mail Server

Mail Server provides the ability to configure/edit the email setting stored in your KRMC server. With no email settings stored in KRMC, you will not have access to Self-Service Password Management (SSPM), KRMC Forgot Password, and Two Factor Authentication (2FA).

The the ability to access this for Regular Administrator (RA) is dependent on their permissions as defined under Edit Admin Permissions 147.

There are 6 fields that need to be completed to configure the Mail Server:

Email Server URL	The URL for your email server.
Email Server Port	The port your email server uses.
Username	A username to gain access to your email server.
Password	The password to the username.
Send from Email	The email address you are looking to send emails from. This can be different then your username added for access to the email server.
Email Server Encryption	This is the type of encryption your email server uses. We support plain text, SSL, and TLS.



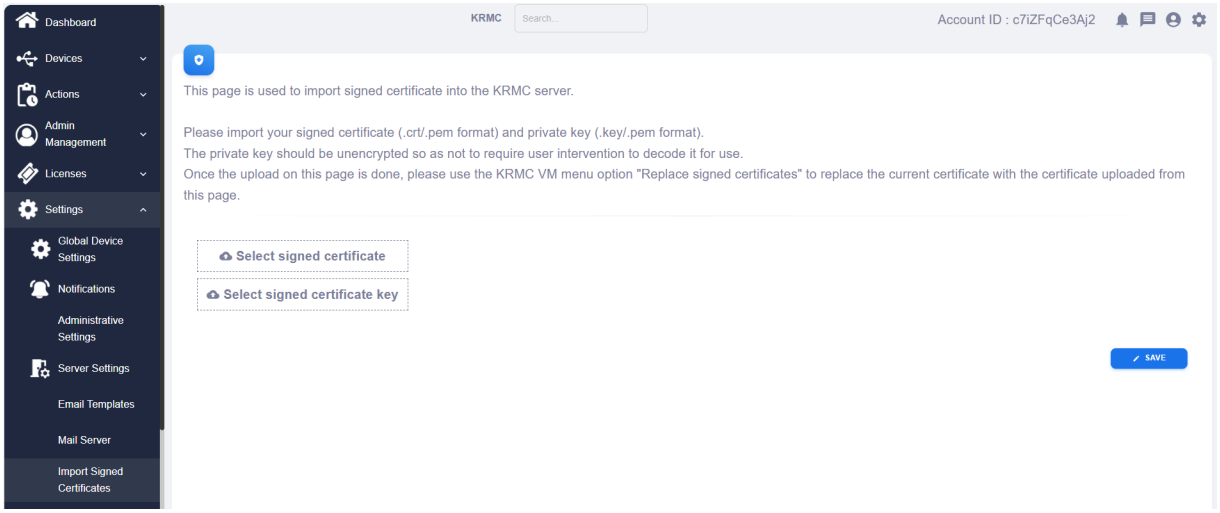
Import Signed Certificate

KRMC On-Premise provides the ability to replace the self-signed certificate that you generate during your initial configuration of KRMC with your own signed certificate. For steps on how to perform this, refer to Steps to Import a Signed Certificate 224.

Import Signed Certificate allows you the ability to load a certificate and the private key into KRMC so you can apply it at a later point.

The the ability to access this for Regular Administrator (RA) is dependent on their permissions as defined under Edit Admin Permissions 147.

*Note: Before making any certificate changes we **strongly recommend** you make a snapshot/backup of your KRMC VM.*

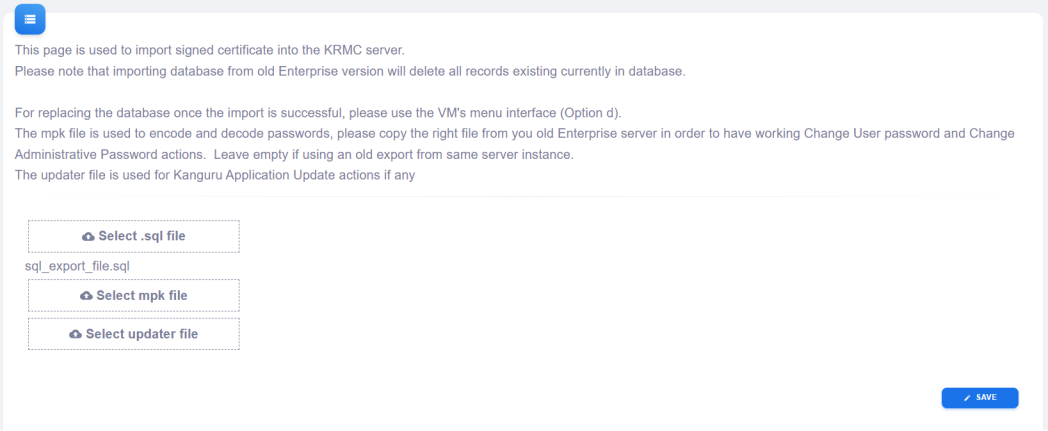


Import Database

KRMC On-Premise provides the ability to migrate your data from a previous KRMC 5, 6, or 7 installation to this new version of KRMC. ***Note:*** *performing this will remove all data that was previously stored on this instance of KRMC*. For steps on how to perform this, refer to Migrate from KRMC 5, 6, or 7 219.

Import Database allows you the ability to load your database and mpk file from your older KRMC 5, 6, or 7 server into this KRMC so you can apply it at a later point.

Note: *Before making any database changes we* ***strongly recommend*** *you make a snapshot/backup of your KRMC VM.*



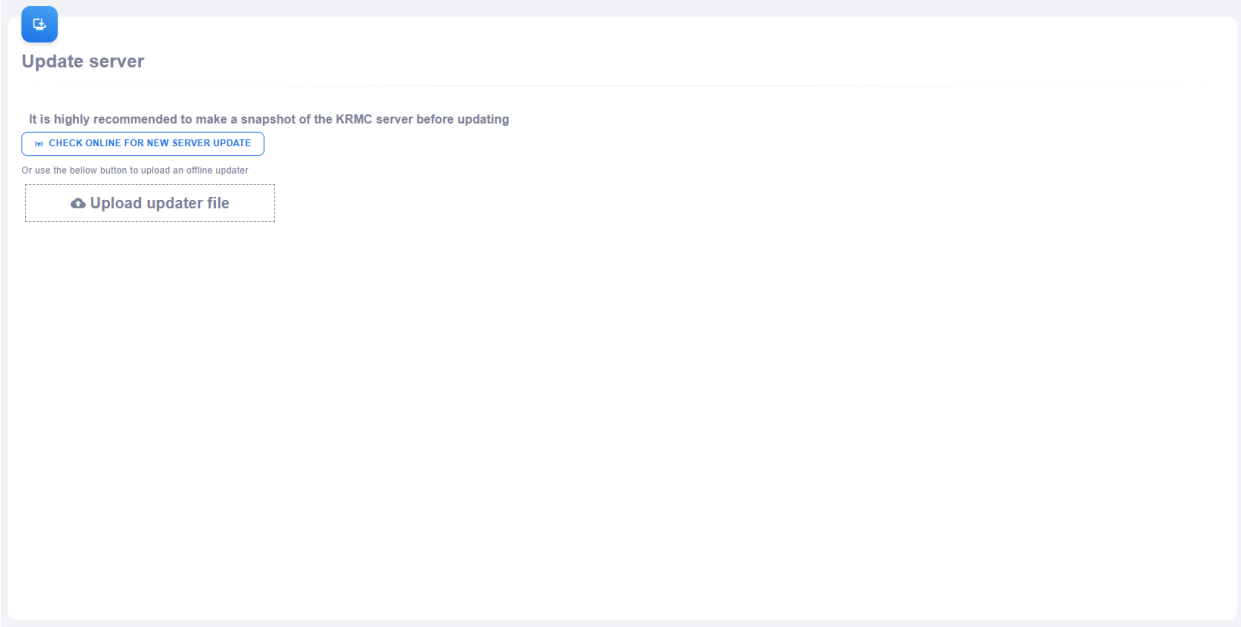
Update Server

iStorage Kanguru will provide updates to KRMC On-Premise regularly. When these occur, you can use Update Server to download an install the updates.

Note: *Before attempting any updates, we* ***strongly recommend*** *you make a snapshot/backup of your KRMC VM.*

If you are on an air gapped network and cannot communicate with iStorage Kanguru servers, you have the ability to manually upload an updater into the server.

Note: *Larger updates may require a new KRMC VM. In those cases, you can use the steps* *Migrate from a different KRMC VM* 216 *to migrate over.*



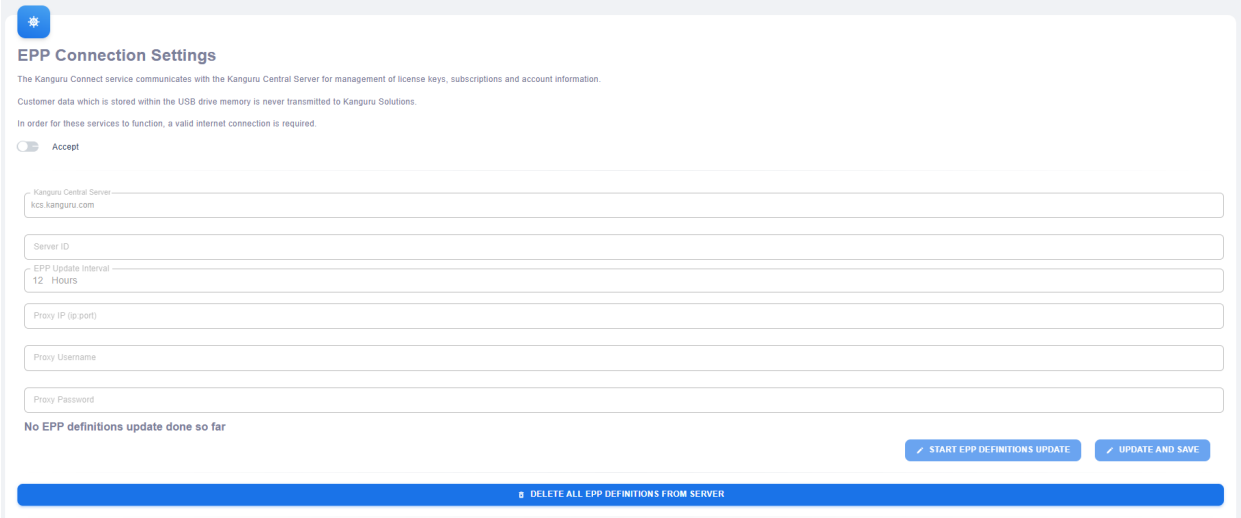
Settings Page 12

EPP Connection Settings

The EPP Connection Settings allows you to configure the internet settings that will allow KRMC to connect to the Kanguru Central Server and upload EPP definition updates which can then be pushed down to the drives. It also allows you to manually upload EPP definition files on offline servers to keep the device's onboard BitDefender Endpoint Protection software up to date.

Before you can configure the server settings, please read the important message regarding the information that Kanguru Centeral Server collects, confirm that you agree to the terms and then click on the accept button. After you have accepted, you can click the Update EPP definitions now button to immediately download the latest EPP definitions. Fill out the fields with the information for your network and then click on the save button. In addition to receiving EPP definitions automatically, by accepting the connection you will also receive licenses automatically and no longer need to manually import them into your server.

Kanguru Central Server	This is the URL your KRMC server will attempt to communicate with. The default setting should be kcs.kanguru.com.
Server ID	This is provided by iStorage Kanguru during your installation of KRMC.
EPP Update Interval	The time interval in which the server attempts to download new EPP definitions. The options are 3-hours, 6-hours, 12-hours, and 24-hours.
Proxy IP	The IP address of your proxy server if one is needed for communication with iStorage Kanguru servers.
Proxy Username	A username to gain access to your proxy server.
Proxy Password	The password to the username.

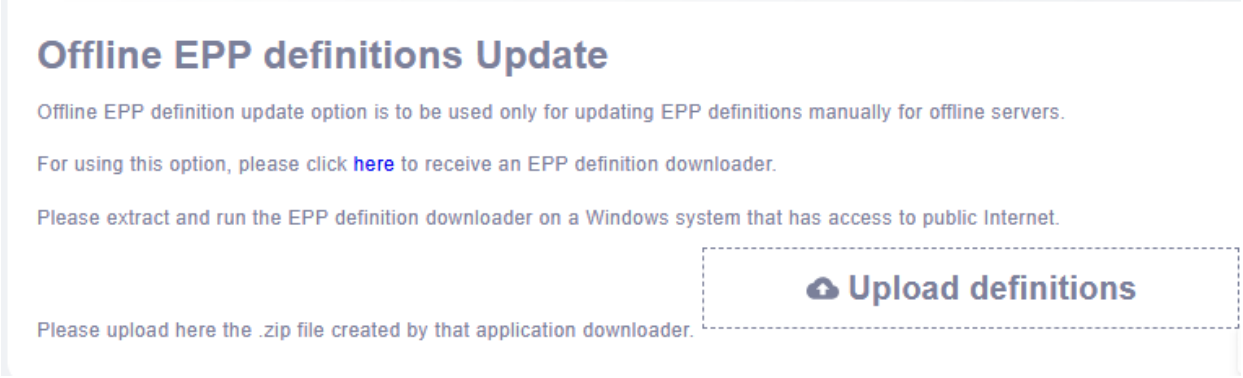


Note: *If you experience issues with the EPP definitions, you can select* ***Delete All EPP Definitions from Server****.*

Offline EPP definitions update KRMC servers running on a closed network are not able to communicate with the Kanguru Central Server to automatically receive EPP definition updates. In order to keep your BitDefender EPP definitions up-to-date, you must manually upload the definitions to your KRMC server.

Important! You MUST keep EPP Definitions up-to-date in order for EPP protection to be effective.

1. Click on where it says "click here" to download the EPP Definition Downloader tool
2. Once the download is completed, run the EPP Definition Downloader tool to obtain an EPP Definitions file.
3. Once you have obtained the EPP Definition File, click on Choose file and select the EPP Definitions file.
4. Click the Upload definitions button to import the latest EPP definitions to your KRMC server.

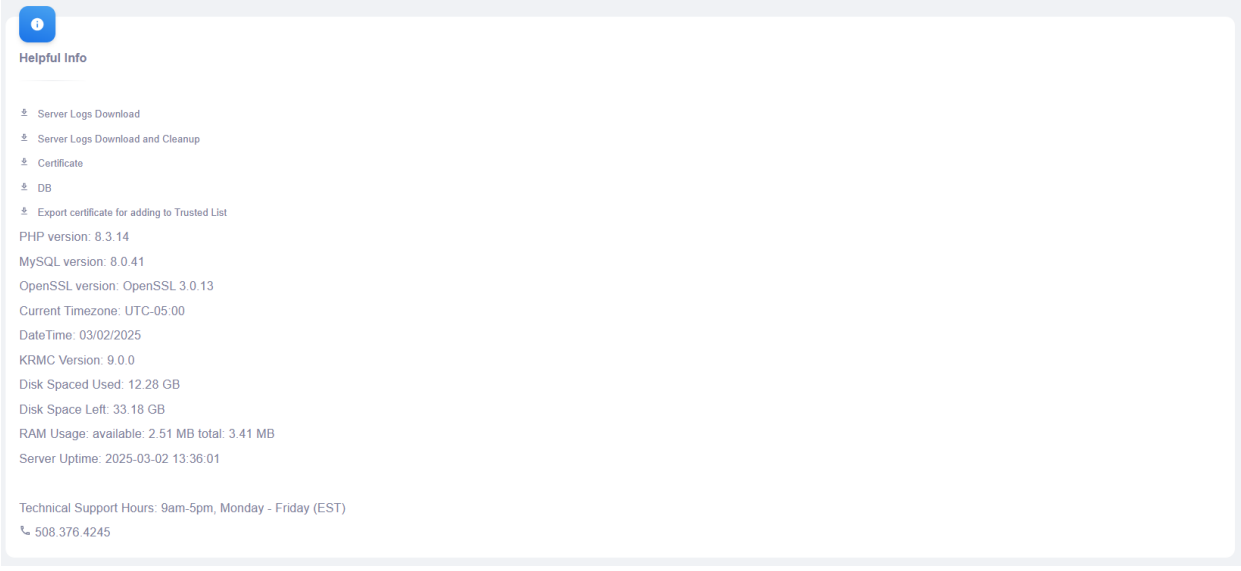


Settings Page 12

Helpful Info

The **Helpful Info** page provides general information for your KRMC On-Premise server.

Server Logs Download	Allows you to download logs for troubleshooting. This is also able to be obtained by used Export Bug Report.
Server Logs Download and Cleanup	Allows you to download logs for troubleshooting then removes them from the server to save space.
Certificate	This downloads the complete certificate used by KRMC in the form of a zip file.
DB	Allows you to download the KRMC database.
Export certificate for adding to Trusted List	This exports the certificate in the for of .p12 file so it can be added to your trusted list.
PHP Version	Provides the current version of PHP on your server.
MySQL Version	Provides the current version of MySQL on your server.
OpenSSL Version	Provides the current version of OpenSSL on your server.
Current Timezone	The timezone selected for the server. It cannot be altered only viewed.
DateTime	The current date for the server. It cannot be altered only viewed.
KRMC Version	The current KRMC server version.
Disk Space Used	The total amount of disk space used on your KRMC VM.
Disk Space Left	The total amount of disk space remaining on your KRMC VM.
RAM Usage	The toal amount of RMA used and available on the KRMC VM.
Server Uptime	The date and time that your server was powered on.

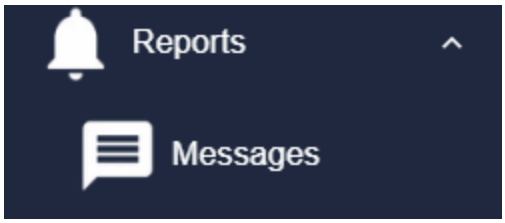


Reports

13

The **Reports** page provides access to all events on KRMC On-Premise and any messages that are sent from us. By selecting Reports you will be brought directly to the Events page on KRMC On-Premise.

Events 202	The Events page displays all events that occur within your KRMC On-Premise company account and is a good location to see all events that have occurred for the history of the KRMC On-Premise account.
Messages 203	The Messages page displays all messages from iStorage Kanguru to your KRMC On-Premise account. These messages range from important updates to KRMC On-Premise to iStorage Kanguru news.

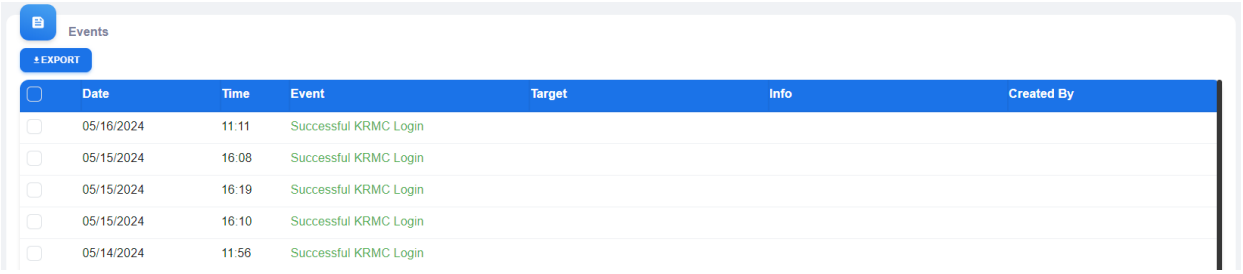


Reports 13

Events

The **Events page** displays all events that occur within your KRMC On-Premise company account. Information within Events includes:

Date	This is the date in which an event is reported. This date format will match the format on your account. For information on how to change this format, refer to Server Settings 182.
Time	This is the time in which an event is reported. This time will match the timezone on your account. The time reported on events cannot be altered. If you change your timezone to a different one, only events after that change will be represented in that new timezone. For information on how to change this format, refer to Server Settings 182.
Event	This will provide you the specific event itself such as Successful Login or Action Created.
Target	The Drive name(s) that the event occurred on will be displayed here. If an action is created for multiple drives, then the even in the list will display the drive names involved.
Info	Information regarding the event will appear here. Information such as setting changes on the server or or custom setting changes for the specific drives will be displayed within this location. If information within the display appears cutoff, you can move your mouse over it to display the remaining information.
Created By	This will provide you the specific account that created the event.



You can configure what type of events appear and how they show by using the options in the Notifications 178 page located under Settings.

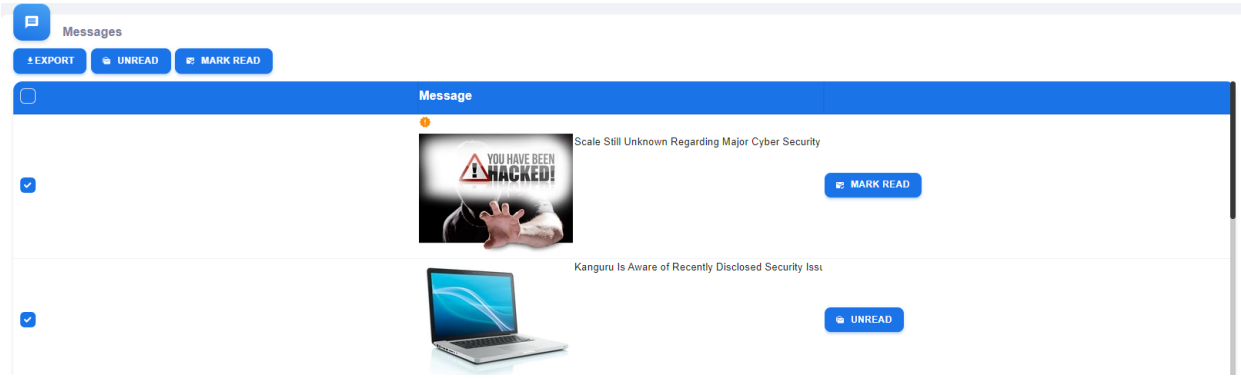
All events displayed on this page are able to be exported using the Export option at the top left of the page. If you want to export more then what is displayed on your screen, make sure to select the check box on the column title bar.You will be notified of new events once you log into KRMC On-Premise by looking at the top right of the screen. If the events icon has a red circle on it then there is an unread event waiting for you. The red circle should contain a number inside indicating how many unread events you currently have unseen. For more information on the icons at the top right of the screen, please refer to Account Activity Icons 54.

If you are looking to have all of your events exported to your SIEM server, please click HERE 182.

Messages

The **Messages** page displays all messages from iStorage Kanguru to your KRMC On-Premise server. ***Note:*** *This is only available to be received if you have configured* *EPP Connection Settings* 198. These messages range from important updates to KRMC On-Premise to iStorage Kanguru news. All messages displayed on this page are able to be exported using the Export option at the top left of the page. If you want to export more then what is displayed on your screen, make sure to select the check box on the column title bar.

Messages have two statuses in Read or Unread. If a message is unread there will be an indicator next to or on top of the message. Messages do not auto-mark turn to the unread status if you select the message and you will need to select the button "Mark Read" next to each message. If you want to undo marking a message as read or unread, you can use the button to the right of the message. Alternatively, you can use the check boxes to the left of each message to select one or more messages and mark as either "Unread" or "Mark Read".



You will be notified of new messages once you log into KRMC On-Premise by looking at the top right of the screen. If the Message icon has a red circle on it then there is an unread message waiting for you. The red circle should contain a number inside indicating how many unread messages you currently have waiting. For more information on the icons at the top right of the screen, please refer to Account Activity Icons 54.

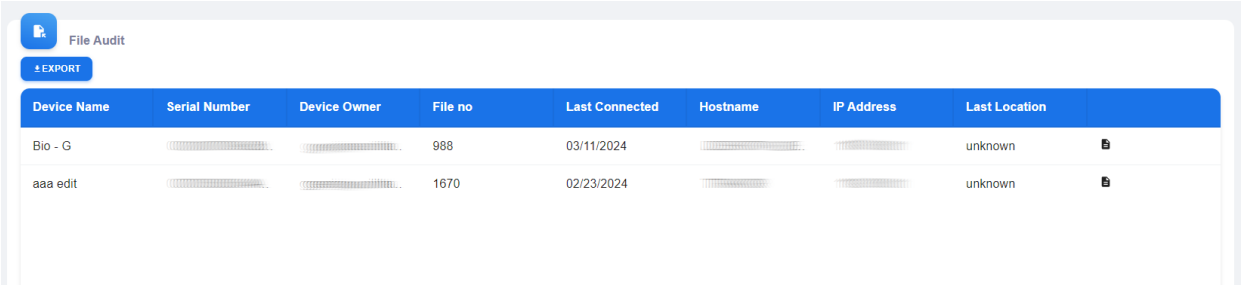
Note: *If you select the Message icon then click out of the windows, the indicator that tells you messages are waiting will disappear. This will reappear to you when you go to your next page.*

File Auditing 14

KRMC **File Auditing** works in conjunction with the registered devices on your KRMC account. Information regarding the files stored on your drives is sent to KRMC where it can then be viewed and exported as needed. ***Note:*** *File Auditing is only available with Premium KRMC On-Premise accounts and on devices with KDM version of 5.6.7.5 or newer.*

The File Auditing page contain general information regarding the device(s):

Device Name	The name of the device assigned by UKLA, device setup, or KRMC On-Premise.
Serial Number	The serial number of the physical device.
Device Owner	The Super Administrator (SA) that the device is assigned to.
File No	The number of files that has been reported for that device.
Last Connected	This is the date and time the server last communicated with this Defender device.
Hostname	The name of the machine the device was last connected to.
IP Address	The IP address of the machine the device was last connected to
Last Location	The geographical location of the computer that the device was last connected to. The geographical location is an approximate location of the drive. The actual location may differ.
File Icon	This allows you to look at the information gathered for the files reported for the device.
Export	Export will generate a CSV file with containing all of the information in the column displayed on this list for all devices.



If you click the File Icon associated with a device, a popup will appear providing all gathered information on the files on the devices. This includes:

Path	This is the file name and full storage path on the device.
Status	The status of the file is an action that has occurred. This includes Deletion, Creation, Read, and Write.
Size	This is the size of the file.
Fist Info	The first date in which the file was reported to KRMC as being on this device.
Last Info	This is the last/most recent date in which this file was reported to KRMC as being on this device.
Export	Export will generate a CSV file with containing all of the information in the column displayed on this list for all files.

Message	Send a notification message to be displayed on the device host's computer.	
IP / Domain / MAC Control	Create a list of IP Ranges or Domains or MAC addresses that you will either allow or restrict your devices to access KRMC from. You can include multiple IP Ranges, Domains, or Mac addresses to the list.	
	Enable Access Control	Check this box to enable IP/Domain/Mac control.
	Functionality	Select whether IP/Domain/Mac control will allow or deny certain IP ranges, Domains, or Mac addresses.
	Allow all Except (blacklist)	When selected, all devices will be allowed to access KRMC unless it is located under any of the IP ranges, Domains, or Mac addresses listed.
	Deny all Except (safelist)	When selected, only devices that are located under any of the IP ranges, Domains, or Mac addresses listed will be able to access KRMC.
	Control based	Select whether you want IP/Domain/Mac Control to be based on IP Range, Domain or MAC Address.
	New Values	Select whether you want the newly added IP Range, Domains, or Mac addresses to either append or overwrite the existing list of allowed or blocked IP Ranges/Domains/Mac addresses.
	Add IP Range, Add Domain, and Add MAC Address	Depending on whether control is based upon IP Range, Domain or MAC Address, this entry will be either 'Add IP Range', 'Add Domain', or 'Add MAC Address'.
	IP Range	Enter the start and end of the IP range that you wish to allow or deny.
Enable Device	Remotely enable a device that had been disabled by a 'Disable Device' remote action.	
Disable Device	Remotely disable a device. Administrator settings are not affected by this action. The device user will be unable to login to their device or access the device's secure partition again until it is enabled by an 'Enable Device' remote action.	
Delete All Data and Disable Device	Delete all the data stored on the device, and then disable the device. Administrator settings and stored data are not affected by this action. The device user will be unable to login to their device or access the device's	

	secure partition again until it is enabled by an 'Enable Device' remote action.	
Kanguru Application Update	Remotely upgrade the version of KDM application running on the device. You will need to upload a KDM Updater executable. ***Note:*** *Only one KDM update is able to be performed at a time. If your KRMC Console contains different Defender models, only perform this action on one model at a time.*	
Change User Password	Change the device's user password.	
	New Password	Enter the new user password for the device.
	Confirm Password	Enter the new user password again to confirm the password. This password must match the password entered in the New Password field.
	Administrative Password	Enter the KRMC Administrative Password.
	User Must Change Password on Next Login	When selected, the user will be forced to change their password after their next login.
Self-Service Password Management (SSPM)	Gives the Defender device user the ability to manually reset their Defender login password. In the event that the Defender login password is lost or forgotten, the user can reset their password without resetting the device and regain access to their data. If a device user forgets their password and self-service password management is enabled, all they need to do is click the 'Forgot Password' button at the Defender's login window and a password reset code will be sent to their designated email ID. Once they enter this reset code, they will be able to setup a new login password and access their data again.	
	Enable and Force	Enable the self-service password management feature on the drive and activate it immediately by requiring the user to provide an e-mail address where the password reset code can be sent.
	Enable but Defer	Enable the self-service password management feature on the drive but allow the user to provide their e-mail address at a later time. ***Note****: Simply enabling self-service password management 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 the self-service password management feature. The "Forgot Password" option will not be available on the Defender login window.

Enable / Disable drive logging	The Defender drive keeps a track of its internal working in encrypted log files on the user's computer. These logs do not store any user data like files/folders, are never sent automatically to iStorage Kanguru, and contain only internal information related to the KDM application. This action helps you enable/disable the drive's logging feature. ***Note:*** *that disabling drive logs might inhibit our ability to help you troubleshoot technical issues.*
Filepush	Remotely send a file to the device. The file will be downloaded to the device's secure partition the next time the device user logs in. Please remember that large files may take a long time to upload and download. ***Note****: The total amount of files sent cannot exceed 1GB in size.*
Reset for New User	This action is designed specifically for reprovisioning a managed Defender drive for a different end user. The Reset for New User action will delete all user data and contact information from the previous device owner, while retaining information critical to device management, i.e., Administrator Password, KRMC status, AV license info, proxy settings and access control restrictions. ***Note****: A Reset for New User action can only be created for devices running KDM client version 4.0.9.4 and later.*
Configure App Launcher	This section is where you can configure a device to auto-execute an application stored on the device. The Auto Run feature will execute every time the device's end user successfully logs into their drive and mounts the device's secure partition. If the file name is entered incorrectly or if the file does not exist on the drive, the end user will receive the following error message: "The process set for auto acquisition failed to start. File not found."
Enable / Disable Reset Autoscan Fingerprint	The Defender Bio-Elite 30 devices have the ability to be used in an OS agnostic state with the use of an Autoscan feature on the device. When Autoscan is enabled, the KDM application on the device does not need to be launched and instead the end user is able to simply connect the device to a system and scan their finger for access. Using this action, you can enable or disable this feature for any Bio-Elite 30 device. ***Note:*** *Changing the state of this feature will reset the device and all data will be removed.*
Enable / Disable USB to Cloud	This option allows you to enable or disable the USB to Cloud application on the Defender device. ***Note****: This action can only be created for devices running KDM client version 5.6.5.4 and later.* If USB to Cloud is enabled, you are then able to select which backup service you allow. Services that are compatible with USB to Cloud are as follows: Amazon S3, Baidu, Box, Dropbox, Google Drive, Mega, NAS (using WebDAV or DAS), OneDrive, OneDrive for Business, Sharefile by Citrix, Yandex Disk.
Enable / Disable Onboard Browser	This option allows you to enable or disable the On-Board Browser (OBB) application on the Defender device. ***Note****: This action can only*

	be created for devices running KDM client version 5.6.5.4 and later.	
Enable / Disable Reset Autoscan Fingerprint	Gives the Defender Bio-Elite 30 drives the ability to use or not use the Autoscan feature on the drives.	
	Enable Autoscan	When enabled, KDMBio only needs to be run once on a supported Windows PC or Mac to register at least one fingerprint. Afterwards, you will be able to access the secure storage partition using only a fingerprint scan. You will only need to run KDMBio to configure or manage EPP, KRMC, SSPM, or fingerprints.
	Disable Autoscan	When disabled, the device is running in standard mode. You will be required to run KDMBio to access the secure storage partition. Since KDMBio is always needed in this configuration, the drive will only work on a supported Windows PC or Mac. This is typically only recommended for devices managed using KRMC.
Enable / Disable EPP	This option allows you to enable or disable the Bit Defender End Point Protection (EPP) application on the Defender device. ***Note**: This action can only be created for devices running KDM client version 5.6.6.2 and later.* If you Enable EPP, you are then able to determine how the real-time scan works. You have three options:	
	Enable Real-Time Scan	Real-Time Scanning is enabled however the user scan disabled this at their choosing.
	Disable Real-Time Scan	Real-Time Scanning is disabled and the user is unable to enable it.
	Force Real-Time Scan	Real-Time Scanning is enabled and the user is unable to disable it.
Enable / Disable File Audit	Provides the ability to use the File Audit feature. ***Note:** File Auditing is only available with Premium KRMC On-Premise accounts and on devices with KDM version of 5.6.7.5 or newer.*	
	Enable File Audit	When enabled, the Defender device will start sending information to the KRMC account regarding the files stored on the device. This information can be seen on the File Audit page on KRMC.
	Disable File Audit	When disabled, no information on the files stored on the Defender device is sent to KRMC.
Full log Upload request File Audit	This action forces a full upload of all files on your Defender drives be sent to KRMC to be viewed with File Audit. ***Note:** File Auditing is only available with Premium KRMC On-Premise accounts and on devices with KDM version of 5.6.7.5 or newer.*	
Panic Mode	A device operating in Panic Mode must be seen by the server in the designated time period. If the device is not seen by the KRMC server	

	during this time, the device will be identified as lost and the next time it is accessed, a specified action will occur. The application will be able to be disabled, disabled and have all data removed, or have all data removed and the user will need to set the device up once again	
	Disable - data maintained	The device will be automatically disabled. All data and settings will remain and will need an enable action created for it prior to being able to be used once again.
	Disable and Delete all data	All device data is removed and the device reverts to the disabled state. An enable action will be required so the device can be used once again and the device will then need to be setup.
	Delete all data and revert to setup wizard	All device data is removed the device will need to be setup the next time the user attempts to use it.
	Panic Period	Defined period of time for the Panic Mode Setting.

Kanguru Active Directory Setup

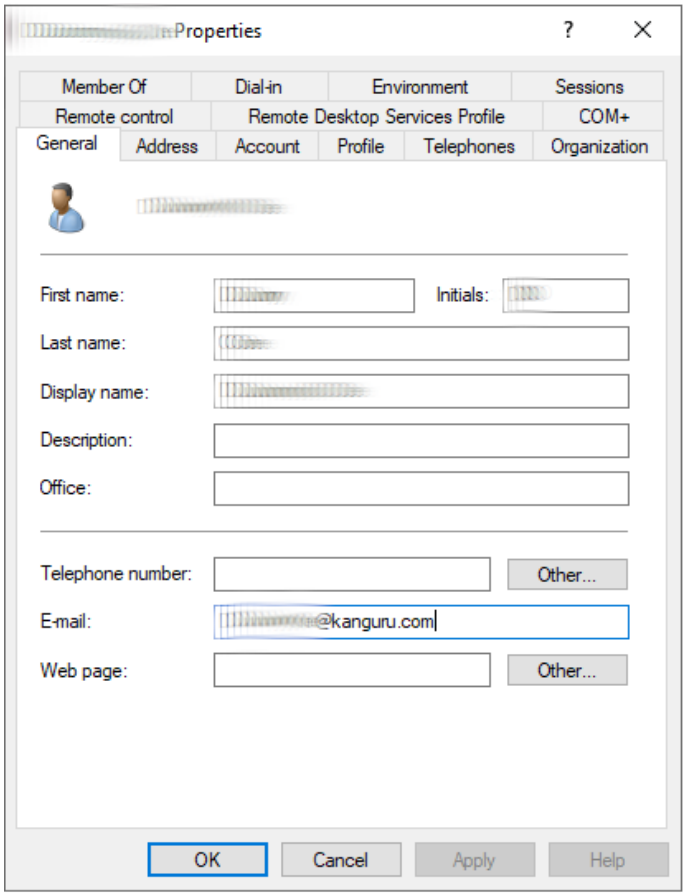
16

KRMC On-Premise Premium accounts have the ability to integrate their Active Directory (AD) accounts with KRMC. In performing this integration, you are able to sync the user accounts with the email addresses assigned to each of your drives on KRMC. If a user on your AD has been disabled, this service will indicate to KRMC of this change and any drive with that email address assigned to it will automatically have one of two actions generated for it.

The options available are as follows:

- Create Disable Device Action
- Create Disable Device and Reset for New User

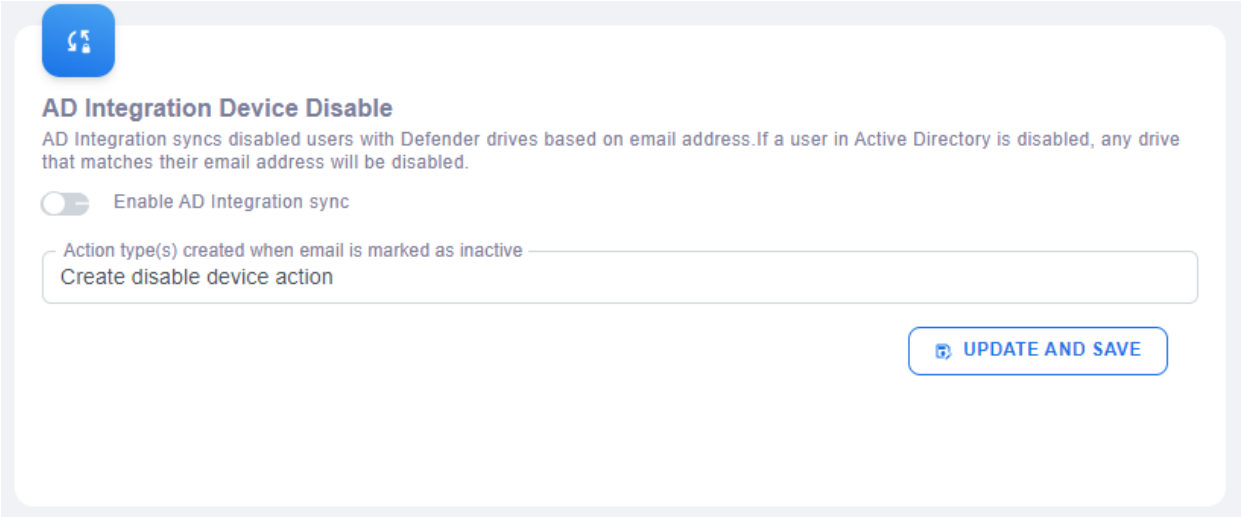
In order to use this feature you will need to ensure that each user on your AD has an email entered into their properties. Without this completed, our service will not be able to send the email address to KRMC if the account is disabled. Additionally, you will need to install the Kanguru AD Service (KADService) on a system on your Domain that will always be running. This requirement is so the service can continue to check for user updates at all designated times. KADService can be downloaded from our support site at: https://kanguru.zendesk.com/hc/en-us/articles/29413143106189.



Prepare your KRMC Account

Before installing the Kanguru AD Service (KADService), you need to turn on the setting to enable connection to KRMC.

1. Log into your KRMC account.
2. On the left-hand side, go to the navigation bar and click “Settings”.
3. Under the Settings panel, open your server settings by clicking “Server Settings”.
4. Navigate to the bottom of the page by scrolling to the section labeled “AD Integration Device Disable 190”.
5. Click the option to “Enable AD Integration sync”.
6. If you click on the “Action type(s) created when email is marked as inactive”, you will have 2 options to choose from.
   6.1. Create disable device action: Disable a device when its owner’s account is disabled in Active Directory.
   6.2. Create disable device and reset for new user: Disable the device and reset it for use by a new owner when the previous owner’s account is disable in Active Directory.
7. When you are satisfied with your choices, click the “Update and Save” button below the settings.



Prepare your domain connected Windows Workstation

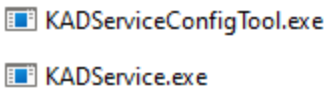
After KRMC is configured to listen for activity, we need to make sure all the software necessary is installed on your workstation.

You will need to install Visual C++ Redistributable, please install this application: https://aka.ms/vs/17/release/vc_redist.x64.exe

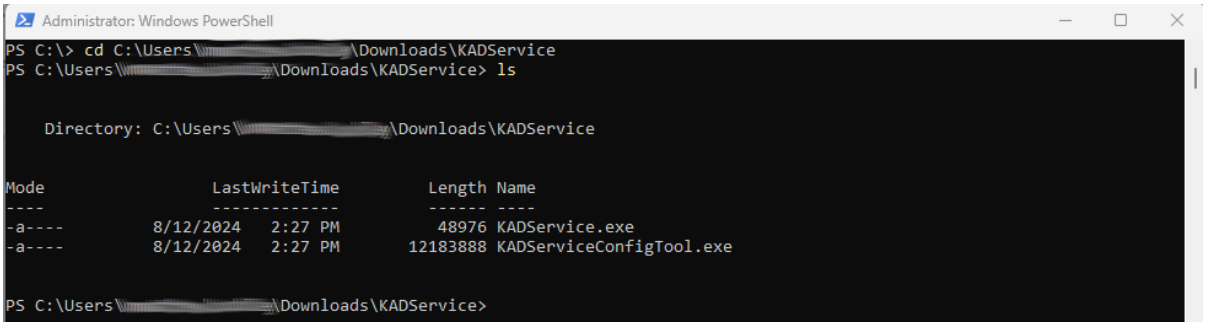
Installing the Service

iStorage Kanguru provides a Windows Service that needs to be installed to report disabled AD user's email addresses to KRMC. The information is sent encrypted and only email addresses are sent to KRMC. Once the event is processed, all information leaves the server and waits until it receives a new event after the set time configured.

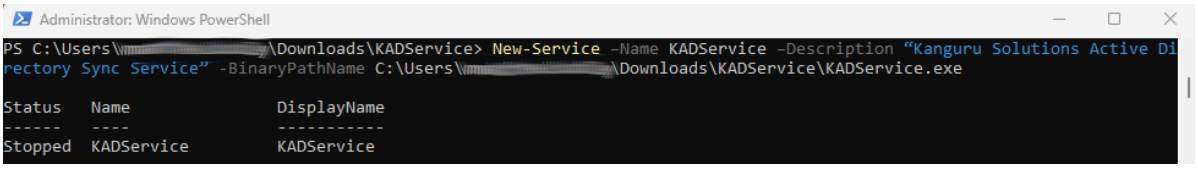
1. The service can be downloaded from our support site by clicking HERE.
2. Save the compressed folder as desired and unzip the folder.
3. Run a PowerShell terminal as Administrator.
4. Navigate to the directory of the Kanguru Service you recently decompressed.
5. Inside you will find "KADServiceConfigTool.exe" and "KADService.exe".



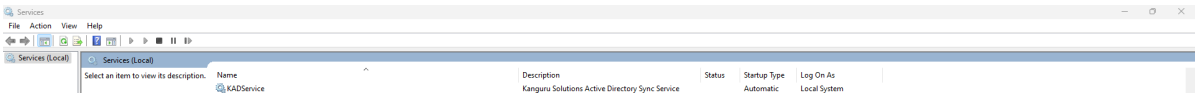
6. Using your PowerShell terminal, navigate to the KADService directory using a change directory command.
   a. For example: "cd C:\Users\<username>\Downloads\KADService"
   b. Or use "Set-Location -Path 'C:\Users\<username>\Downloads\KADService'"



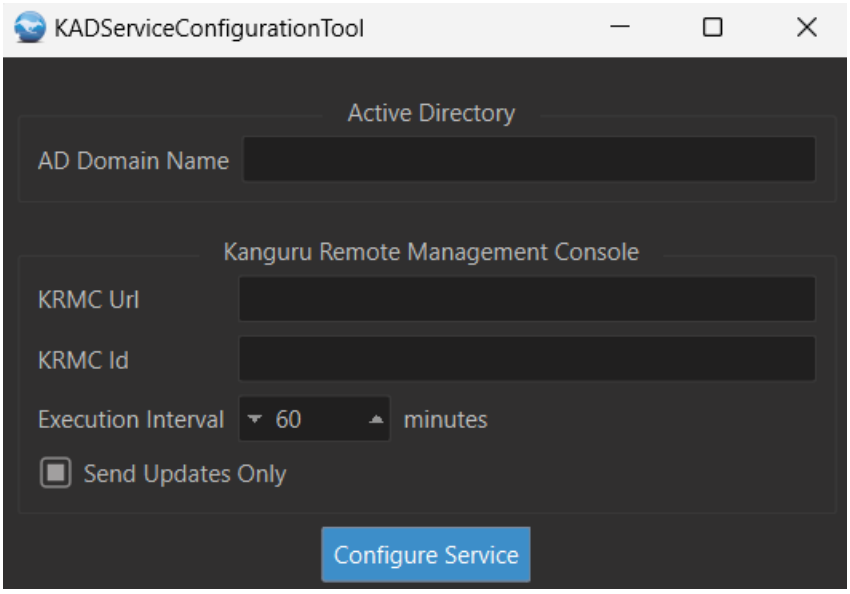
7. We are going to add the KADService.exe as a service on this computer by running the command "New-Service –Name KADService –Description "Kanguru Solutions Active Directory Sync Service" -BinaryPathName <path to KADService.exe>".



8. You should see an output that says the service named "KADService" is stopped, the means the service was successfully installed.
9. At this point you can see the service when you open the Service Management window in your OS.



10. Now we will configure the KADService using the KADServiceConfigTool
11. Navigate to the KADServiceConfigTool folder in your decompressed folder.
12. Double-click the executable KADServiceConfigTool.exe to launch the tool.

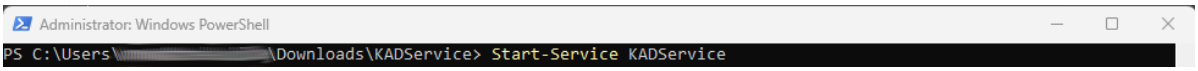


13. Once the configuration tool is open please input your Active Directory domain name into the corresponding field.

AD Domain Name	This is the name of your Domain for which you will be checking for updates.
KRMC URL	For KRMC On-Premise, the URL that you should enter is https://<KRMC_IP_Address>.
KRMC ID	This is the Account ID for your Super Administrator (SA) account. For information on how to locate your Account ID either refer to Account Activity Icons or Account Information.
Execution Interval	This is the number of minutes that the service will check for any changes that may have occurred. The default is set for 60 minutes (1-hour).
Send Updates Only	When selected, previous batches sent to KRMC are stored in system memory and only changes are sent to KRMC. This is useful if you are looking to quicker batches to be sent to KRMC however we commonly recommend not having this option selected.
Configure Service	This saves the configure settings entered here. You can change these settings at a later point by running KADServiceConfigTool.exe again.

14. Close the configuration tool window.

15. To start your service, you can run the PowerShell command “Start-Service KADService”, the resulting output should show the service is running.



Uninstalling the service

If you ever need to uninstall KADService, you can follow these steps:

1. Open up PowerShell as an Administrator.
2. If you have a newer version of PowerShell (version 6 or higher), you can use “Remove-Service KADService”
3. Otherwise, use “sc.exe delete KADService”
4. The service should now be uninstalled.

Getting Logs for Troubleshooting

The logs are located in C:\ProgramData\Kanguru\ADService\ , the logs files are unencrypted but do not contain any identifiable Active Directory information.

Migrate from a different KRMC VM 17

If you currently have a KRMC 8 or KRMC 9 VM currently in your environment and you are looking to upgrade, we have provided a method for migrating your data from one KRMC instance to another using Restore from another KRMC VM. To perform this migration, you will need to have two KRMC instances within your environment. The first instance would be your production server (the KRMC server currently being used). The second instance would be your new server that you are looking to migrate to.

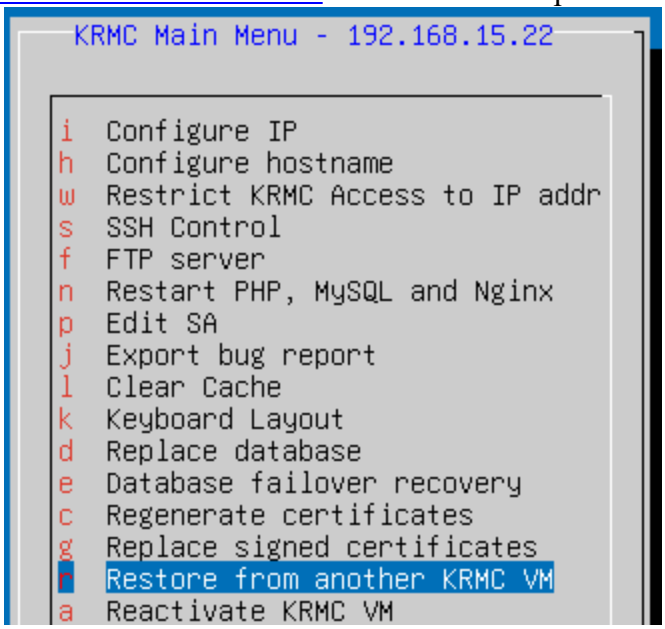
On the second instance of KRMC, please make sure you have completed the steps in the Installation of KRMC 2 as well as Setting up KRMC for the first time 22. Lastly, as always we recommend taking a snapshot of both of your KRMC instances.

Note: *Restore from another KRMC VM is only available if you are using an instance of KRMC 8 or KRMC 9. If you are using an older version of KRMC such as KRMC 5, 6, or 7, you will need to refer to Migrate from KRMC 5, 6,or 7 219.*

Note: *If migrating from KRMC 8 please use the Clear Cache option in the menu before performing these steps.*

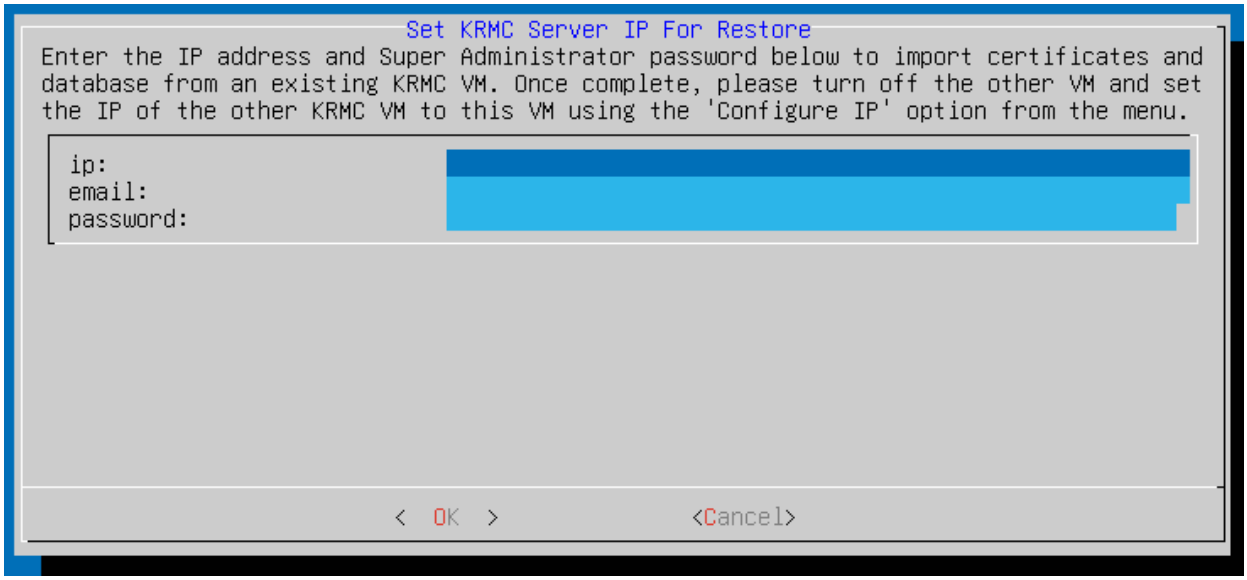
To perform a restore from another KRMC VM:

1. Steps to take on Second KRMC instance to start the migration:
   a. From the KRMC On-Premise Virtual Console 69, use the **Up** or **Down** arrows until you see Restore from another KRMC VM 107 is selected and press **ENT**.

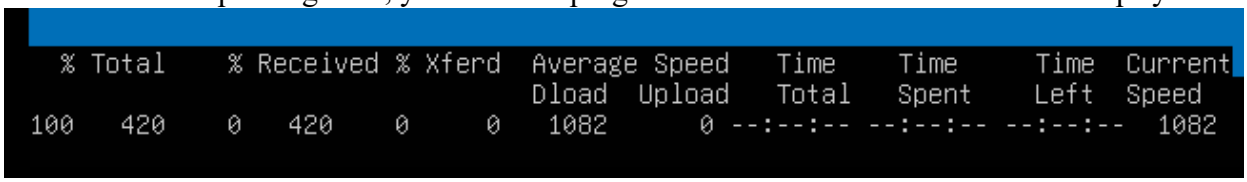


   b. A pop-up will appear with three fields that will need to be completed. After completing the fields, press **ENT**.

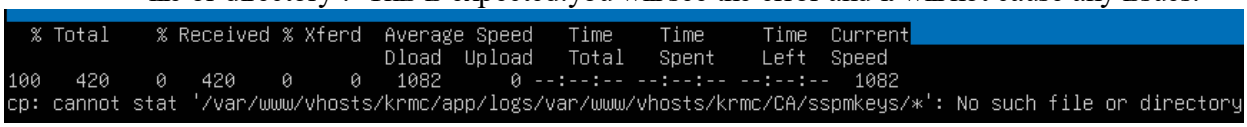
ip	The IP address of the first instance of KRMC (the KRMC server you are looking to pull data from).
email	The email address of the Super Administrator (SA) of the first instance of KRMC (the KRMC server you are looking to pull data from).
password	The password of the Super Administrator (SA) of the first instance of KRMC (the KRMC server you are looking to pull data from).



c. After pressing ENT, you will see a progress indicator at the bottom left of the display

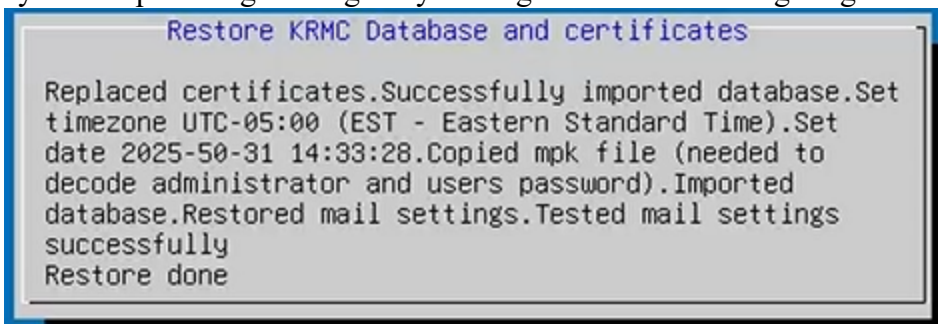


d. If you are upgrading from KRMC 8 to KRMC 9 you will see a message stating "No such file or directory". This is expected.you will see the error and it will not cause any issues.



e. This process may take a few minutes. The length depends on a number of factors however should not take more than 1-hour. If it does, please contact support.

f. When this is completed you will receive a message stating everything was successful. If you receive a message stating this was successful but that something went wrong. This message is due to the email settings not being carried over. The next time you log into KRMC, you will be asked to complete the email setup process. This is commonly resolved if you attempt the migration again by clearing the cache before migrating.



2. Steps to take on First KRMC instance after the migration:

Note: *After the migration steps listed above, this instance of KRMC will no longer be accessible using a web browser. If you need to gain access to this instance's web browser, refer to* *Reactivate KRMC VM* 109.

a. Note the IP address and if you configured the hostname of the server.
b. After noting that information, use Graceful shutdown 112 to power your KRMC server off.

3. Steps to take Second KRMC instance after the migration:
   a. With the first KRMC instance powered off, use Configure IP 76 to change the IP address to match the IP of the first KRMC instance.
   b. If your first KRMC instance also had a hostname configured, use Configure hostname 79 to match the hostname of the first KRMC instance.
   c. Lastly, if the first KRMC instance had a signed certificate, use Replace signed certificates 105 to import your signed certificate on the second KRMC instance.

Migrate from KRMC 5, 6, or 7

18

Replace database allows you to migrate your previous installation of KRMC 5, 6, or 7 to the new KRMC 9 server. This process will require access to both the original KRMC 5, 6, or 7 server as well as the new KRMC 9 server instance.

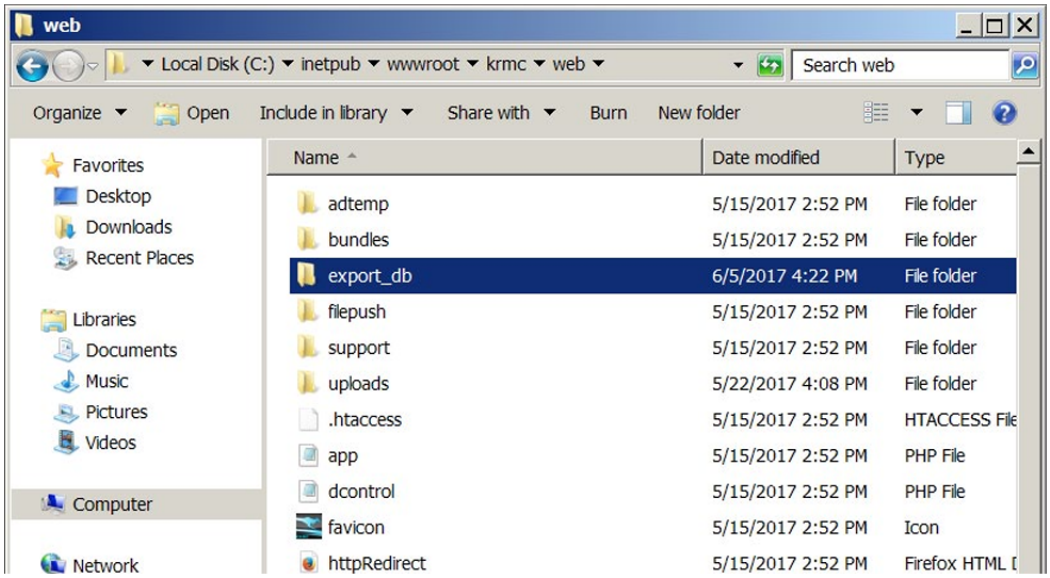
If you are looking to migrate from a KRMC 8 server or different instance of KRMC 9 to a new version, refer to Migrate from a different KRMC VM 216.

If you are looking to migrate from KRMC 5, 6 or 7 to KRMC 9 please make you have completed the Installation of KRMC 2 as well as Setting up KRMC for the first time 22. Lastly verify you have a snapshot made of your current KRMC 9 instance.

Additionally, KRMC 9 only supports subscription-based licenses with 1-, 2- or 3-years validity. If your current KRMC Enterprise licenses were purchased under the older licensing model (usually identified by licenses with over 60000 days validity), please get in touch with iStorage Kanguru Support prior to KRMC migration to convert your licenses to ensure that your new KRMC 9 server remains compatible with your licenses post-migration.

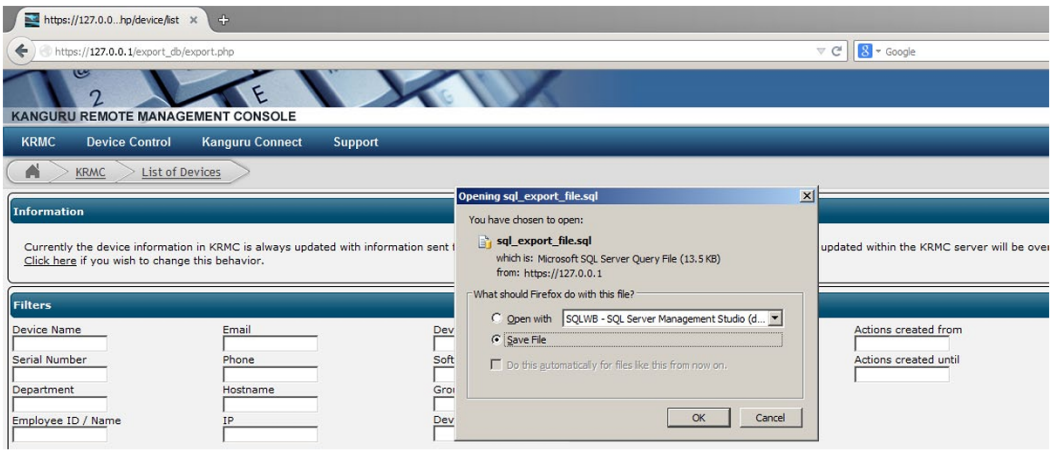
To migrate your existing KRMC 5, 6, or 7 information into KRMC 9:

1. Steps to take for the KRMC 5, 6, or 7 server:
   a. 1. Open a web browser and navigate to the following link to download the file "**export_db.zip**": https://kanguru.zendesk.com/hc/en-us/articles/115003674932-KRMC-8-Migration-Assistance. _
   b. Unzip the export_db.zip file and then copy the export_db file folder into the krmc project, located in the "**web**" folder at **C:\inetpub\wwwroot\krmc\web**.



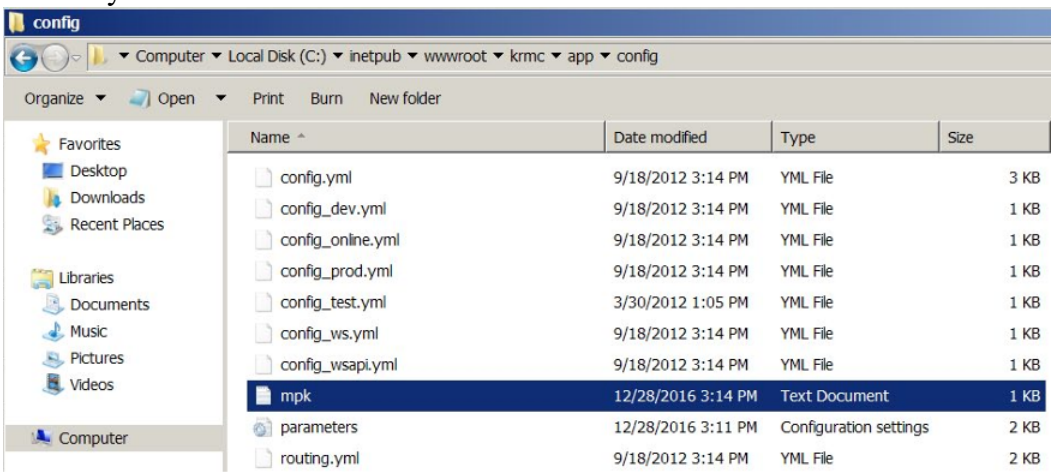
***Note:** You should not see another "export_db" file folder within this directory.*

   c. Open a web browser and navigate to **https://<current_krmc_ip>/export_db/export.php** where "<current_krmc_ip>" is the IP Address for the current KRMC. This will generate a sql file with data from the existing database. Save this file locally, as it will be used later.



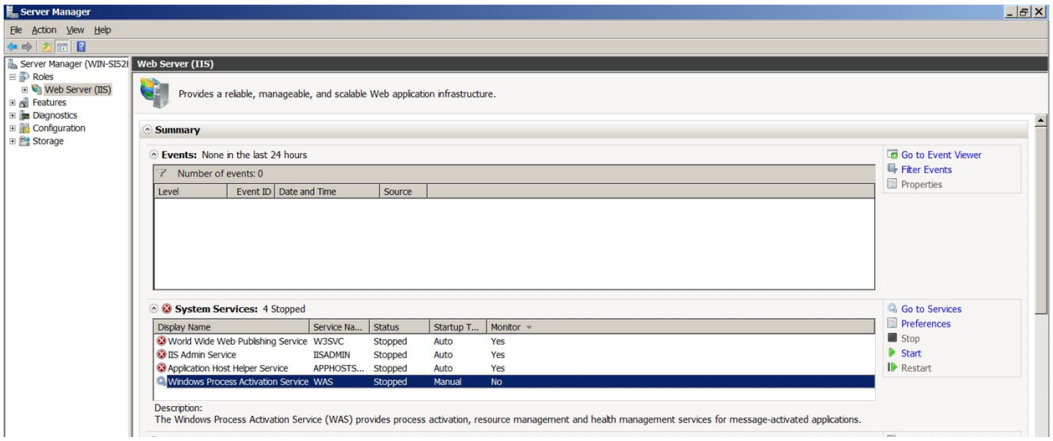
Note: *If you receive an error stating that your connection is not private, click on advanced and then click on Proceed to <current_krmc ip> (unsafe).*

d. Copy the **mpk.txt** file located at **C:\inetpub\wwwroot\krmc\app\config\mpk.txt** Save this file locally as it will be needed later.



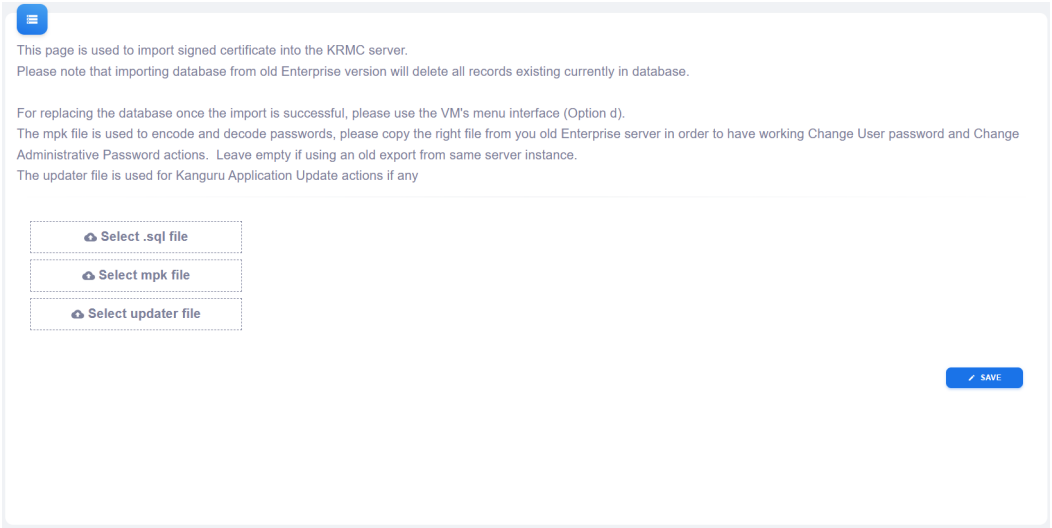
Note: *If there are any pending Client Upgrade actions in the current KRMC, then also copy and save the KdMUpdater.exe file located at C:\inetpub\wwwroot\krmc\web\uploads\upgrade*

e. Stop the IIS service, and if needed the Windows server, to ensure that the IP address of the server is available.

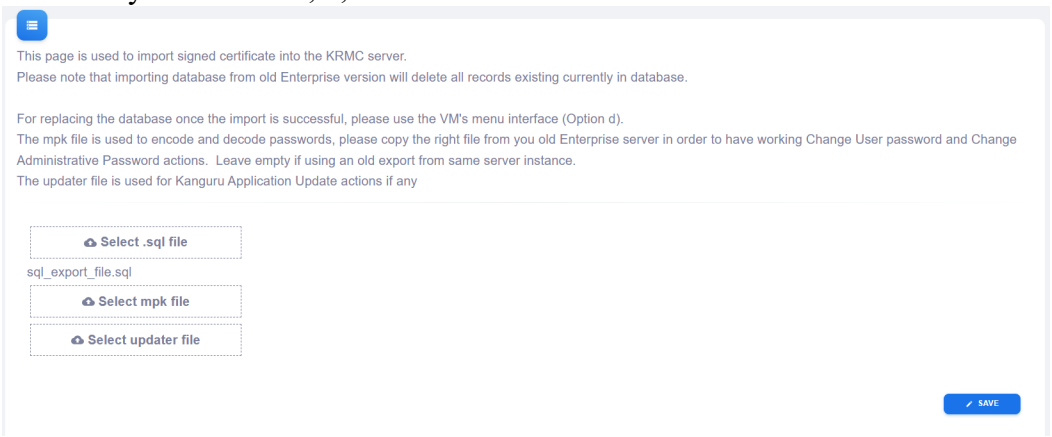


2. Steps to take on the KRMC 9 server browser interface:

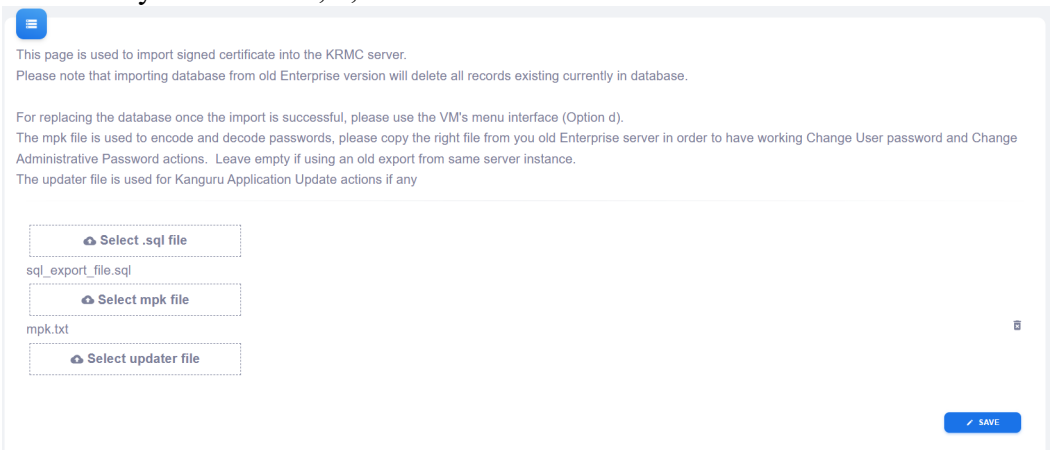
a. Log into KRMC 9 and navigate to the Settings Page 170. From here, select Import Database 196.



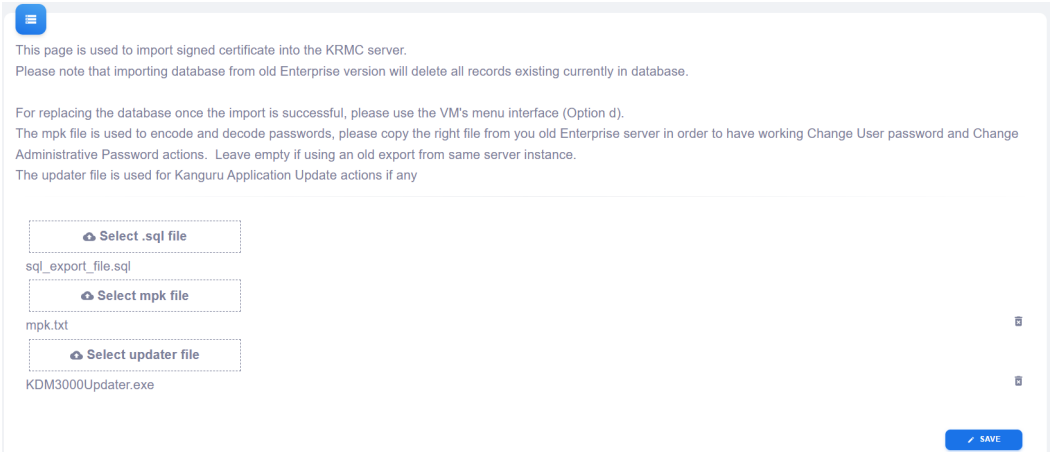
b. This page will allow you to import the files you obtained from your KRMC 5, 6, or 7 server. Select the option "**Select .sql file**" and a pop-up will appear so you can select the SQL file from your KRMC 5, 6, or 7 server.



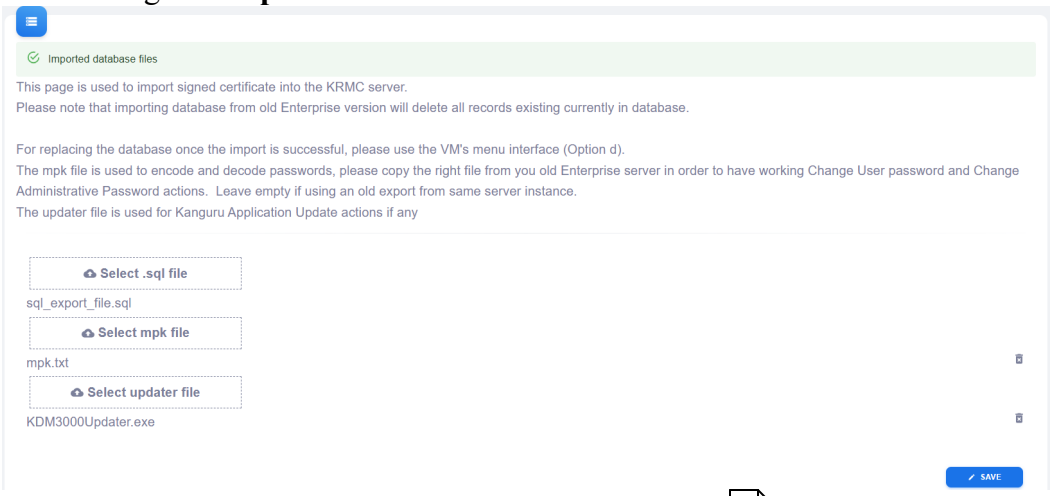
c. Next, select the option "**Select mpk file**" and a pop-up will appear so you can select the MPK file from your KRMC 5, 6, or 7 server.8.



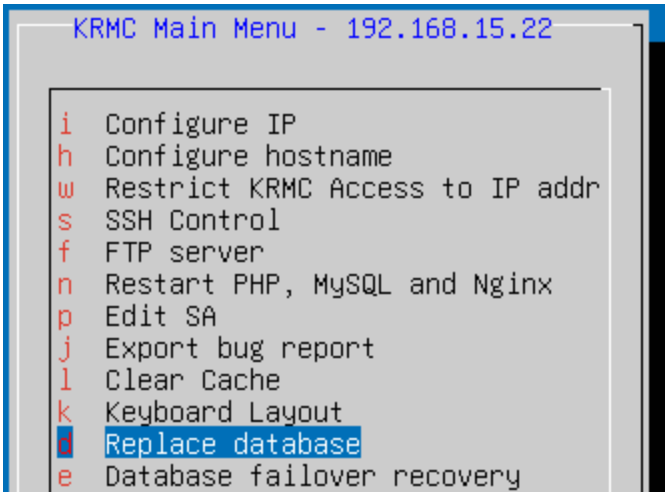
d. If you had KDM updates waiting, you will lastly, select the option "**Select updater file**" and a pop-up will appear so you can select the KDM updater file from your KRMC 5, 6, or 7 server.



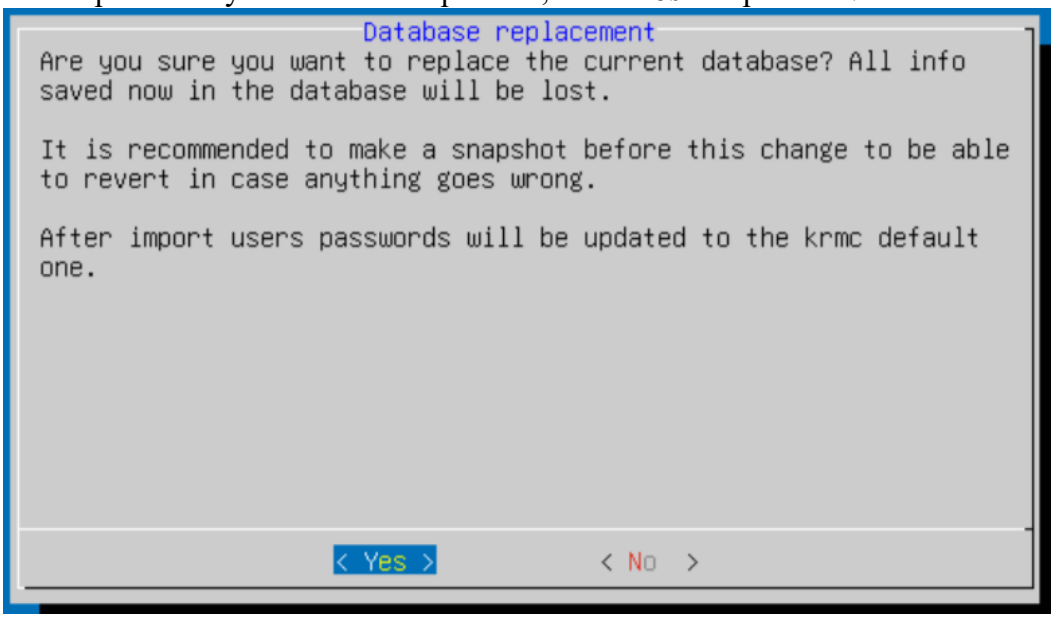
e. Once the files have been selected, select "**Save**" and after you few seconds you should be receive a message of "**Imported database files**".



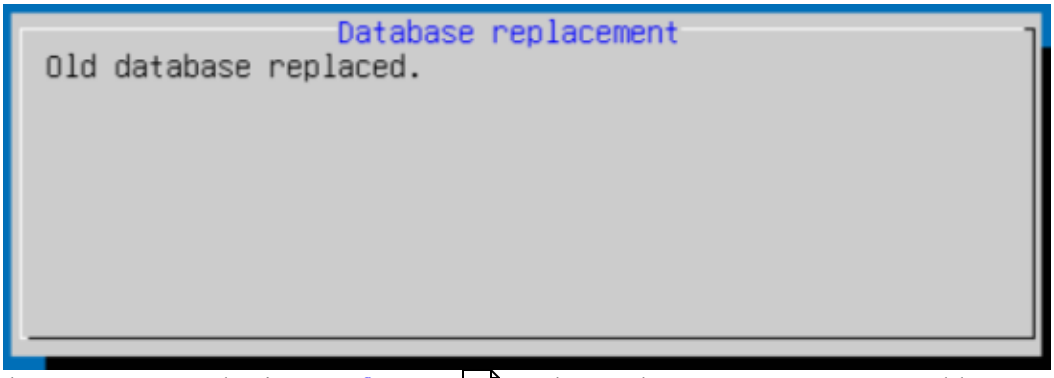
3. Steps to take on the KRMC 9 KRMC On-Premise Virtual Console 69:
   a. Use the **Up** and **Down** arrows until you see Replace Database 97 is selected and press **ENT**



b. You will receive a message asking if you are sure you would like to proceed with this database replaced. If you would like to proceed, select **Yes** and press **ENT**.



c. This process may take a few minutes however after this is completed you will receive a message stating "**Old database replaced**". Once this appears, you will be brought back to the **KRMC On-Premise Virtual Console**.



d. Lastly, we recommend using Configure IP 76 to change the KRMC 9 server IP address to the IP address of the previous KRMC 5, 6, or 7 server. This will assist with your drive communication with the server.

Note: *The 1024bit certificates that are used in KRMC versions 5, 6, and 7 are not compatible with KRMC 9. Due to this, we recommend you have the KDM application on your drives fully updated before performing any migration like this. The latest version of KDM are able to request new certificates allowing the drives to maintain their communication with KRMC.*

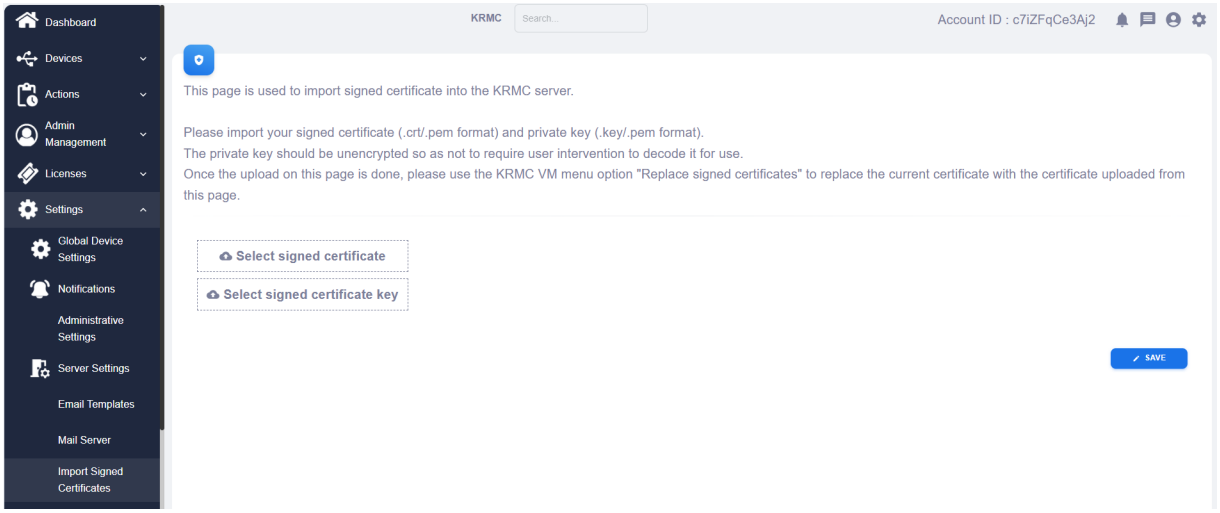
Steps to Import a Signed Certificate 19

KRMC On-Premise provides the ability to replace the self-signed certificate that you generate during your initial configuration of KRMC with your own signed certificate.

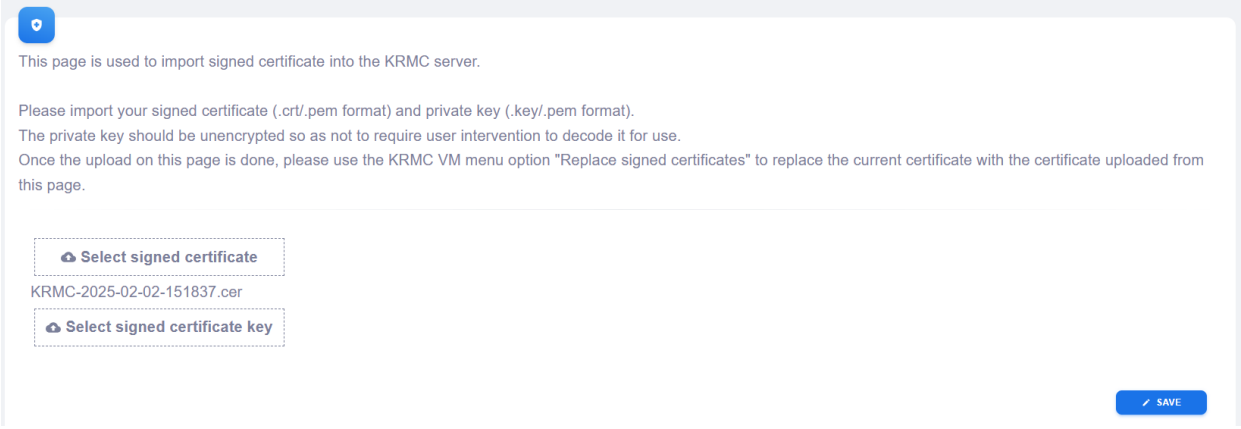
***Note:** Before making any certificate changes we **strongly recommend** you make a snapshot/backup of your KRMC VM.*

To import your own certificate and replace the self-signed certificate:

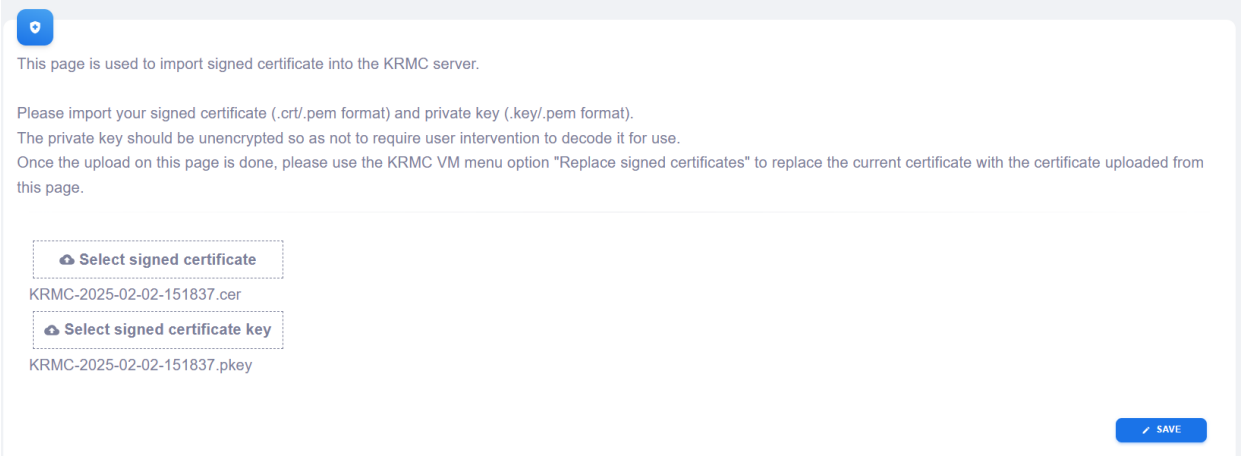
1. Log into KRMC and navigate to the Settings Page 170. From here, select Import Signed Certificates 195.



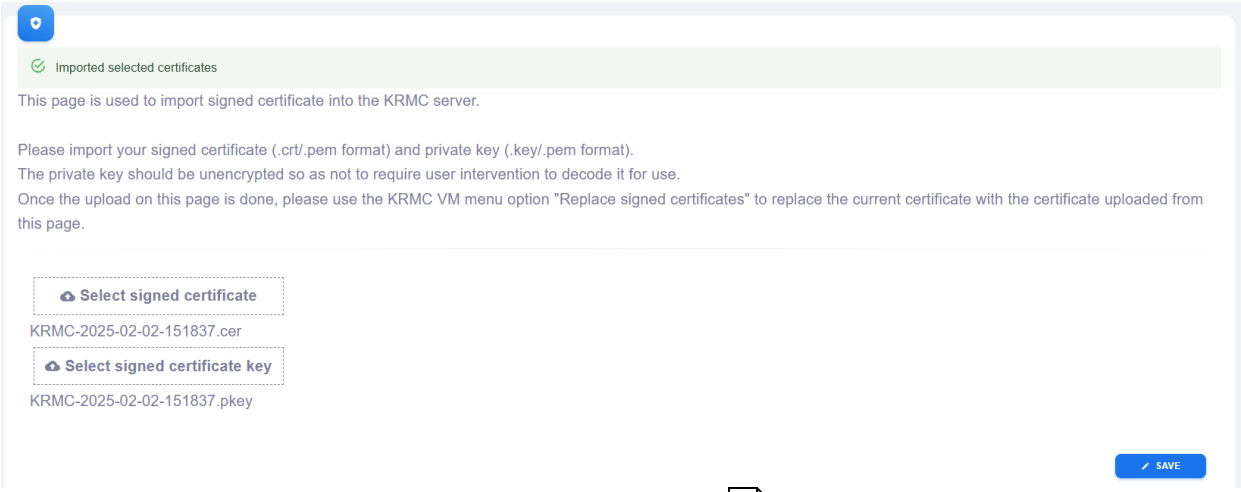
2. This page will allow you to import your own signed certificate and private key. Select the option **"Select signed certificate"** and a pop-up will appear so you can select your certificate.



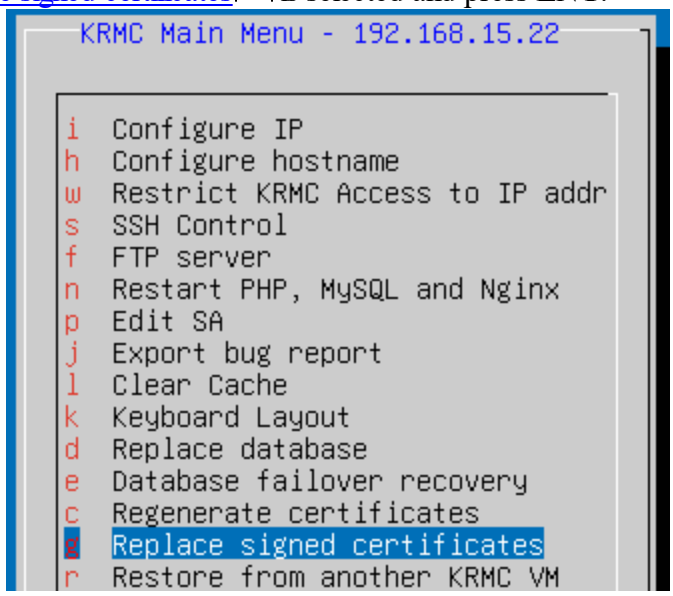
3. Next, select the option "**Select signed certificate key**" and a pop-up will appear so you can select your certificate key.



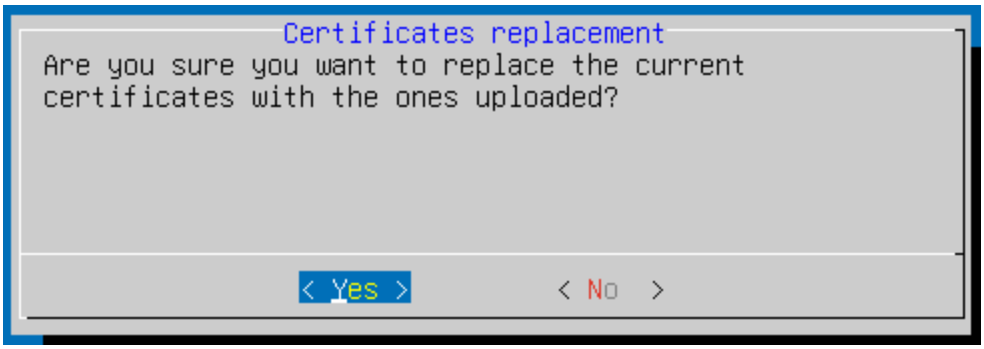
4. Once both files have been selected, press "**Save**". This will import the certificates into your KRMC VM.



5. Now go to the KRMC On-Premise Virtual Console 69 and use the **Up** and **Down** arrows until you see Replace signed certificates 105 is selected and press **ENT**.



6. You will receive a message asking "Are you sure you want to replace the current certificates with the ones uploaded?". If you would like to proceed, select **YES** and press **ENT**.



7. You will be notified that the certificate and key have been copied. Additionally, Nginx will have restarted. This may last a minute or two but then you will be brought back to the KRMC On-Premise Virtual Console.

Note: *If at any point you do not want to proceed with the confirmation of the settings, you can press* ***ESC*** *on your keyboard and you should be reverted back to the KRMC On-Premise Virtual Console with no settings saved.*