Recommendations for Help Desk or KRMC Administrators
How to Upload Accurate User Contact Information When Registering Kanguru Defender Devices with KRMC

It is helpful for KRMC administrators to have company email addresses for their device users. This allows administrators to contact users by email and request that they plug in their devices to get updates and security settings. The following are recommendations for how to register your devices to KRMC and make sure that you have accurate user contact information associated with each device. A few scenarios are presented, so follow the guidelines for the scenario that best matches your situation.

A single device is registered to KRMC and given immediately to the user:

1) Use our provisioning tool (found at https://kanguru.zendesk.com/hc/en-us/sections/206384187-Cloud-Provisioning-Tool to register your device to KRMC. (The provisioning tool instructions are also pasted at the end of this document.)

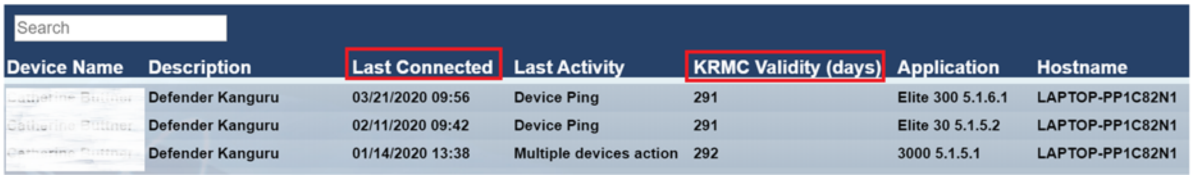
2) Immediately after registering the device, disconnect it.

3) **a)** Give the device to the user and request that the user plug it into an internet-connected machine and go through the setup process immediately. During the setup process, current versions of KDM will require users to enter their contact information. Users should enter their first and last name, company email address, company phone number, and register their email for self-service password management (SSPM), if that feature has been enabled by the Super Administrator of the account. *(For SSPM, Kanguru highly recommends choosing "Enable and Force" in the "Global Provision Profile" tab of the KRMC "Settings" page.)* The user contact information should then populate in your device list within KRMC.

Note: if the user delays this setup process, the device will appear in your account but you will not have contact information for this user. You want to avoid having this happen.

-- OR --

b) The Super Administrator (SA) can enter the contact information for the user (if you know who the user will be) by logging into KRMC and going to the "Devices" page. The device will likely show up at the top of your device list, but if it doesn't, you could locate the registered device by clicking on the "Last Connected" or "KRMC Validity (days)" columns. Clicking on "Last Connected" one or two times should bring the most recently connected device to the top of the list, and clicking on "KRMC Validity (days)" should allow you to find the device with the newest license.



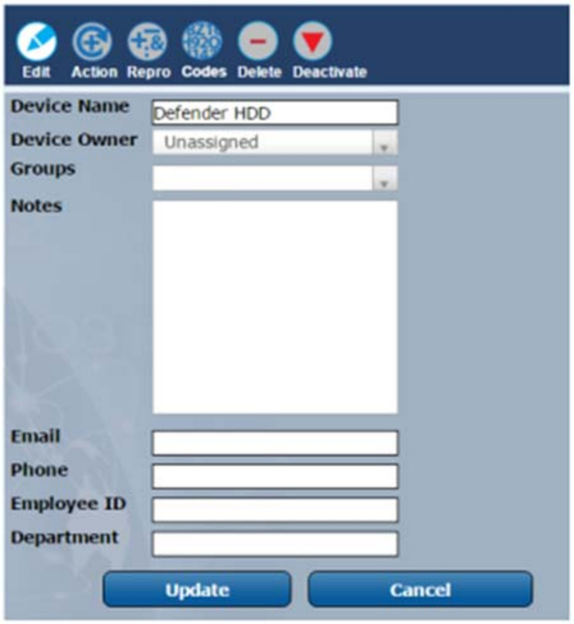
Device Name	Description	Last Connected	Last Activity	KRMC Validity (days)	Application	Hostname
[redacted]	Defender Kanguru	03/21/2020 09:56	Device Ping	291	Elite 300 5.1.6.1	LAPTOP-PP1C82N1
[redacted]	Defender Kanguru	02/11/2020 09:42	Device Ping	291	Elite 30 5.1.5.2	LAPTOP-PP1C82N1
[redacted]	Defender Kanguru	01/14/2020 13:38	Multiple devices action	292	3000 5.1.5.1	LAPTOP-PP1C82N1

Once the device is located, click on it, and look for the "Edit" button on the right side of the split screen. Enter the user's first and last name in the field for "Device Name," as well as the user's email address and phone number in the lower fields (see screenshot below).

This method would be beneficial if there are likely to be delays between issuing the device and the user setting up the device. The user can still edit the contact information during the setup process, but this allows the SA to know who the user is if there is a delay in the user setup process.

figure 1. Edit Device Info

*Clicking the **Edit Device button** will open the Edit Device menu. From here you can change the device's name, assign the device to an owner or group, and add internal notes about the device.*



Device Name: Defender HDD
Device Owner: Unassigned
Groups:
Notes:
Email:
Phone:
Employee ID:
Department:

For devices that have been registered to KRMC but there is no contact information for the users:

If you have a small number of devices like this, you may be able to determine the user by going to the "Devices" page, and looking at the "hostname," "Employee ID," or other fields associated with each device. *Note: you can select the columns that are displayed on the "Devices" page by clicking the "Edit Columns" option in the upper right corner of the dark blue banner.* If you can determine who the user is, click on the device to create the split screen, then enter the user's contact information, as shown in Figure 1 above.

--OR--

If you have a large number of devices like this, this may require a mass email to all employees requesting a response from those who were issued a Defender security device, either a flash drive or a hard drive. From the responses, the user association can begin. (**First time setup requires an active KRMC license so be sure all expired licenses are brought to current before this step**). If a response is that a user does have the device, request that they connect it to an internet-connected system and go through the setup process. Also request that they connect it on a monthly basis so that updates and security settings can be received in accordance with company guidelines. After users go through the setup process, their contact information will populate in KRMC in association with the devices they have. This will allow for ongoing user communication and better auditing of devices within the organization.

For devices in inventory and not yet registered to KRMC:

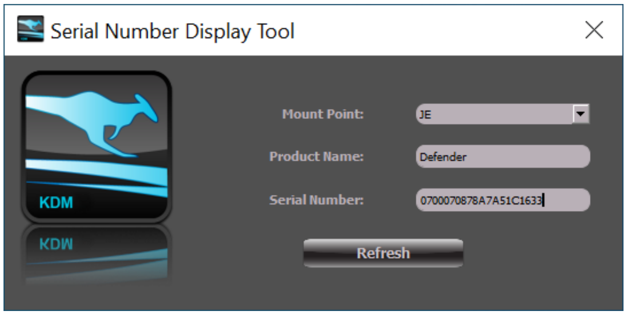
Follow the instructions listed on page 1 for steps 1, 2, and 3a or 3b. Although it is possible to register 8 devices at one time using a standard USB hub, if users do not go through the setup process immediately, their contact information will not populate in your device list. Therefore, we highly recommend registering devices one at a time with KRMC, as outlined in step 3b.

For devices in inventory and already registered to KRMC and for devices that are pre-registered by Kanguru as part of your order:

Before issuing the device to the user, this requires an extra step in order to match the serial number of the device to the serial number already listed in KRMC. Select the device that will be issued to a user and connect it without running the application "Kanguru Defender Manager (KDM)" because that would require a complete setup of the device, which is what the user will be doing. The Super Administrator should do the following, with the device connected:

1) Go to Kanguru.com → Support → Technical Support → Visit Tech Support → Software Downloads. To be sure the device is running the latest KDM version, download and run the KDM updater for the model of device that you have. (The model name should be engraved on the unit.)

2) Leave the device plugged in after the update, and browse to the DVD-CD-ROM partition for the device. Within the files, you will see a SNTool.exe file. Running this utility will tell you the serial number from the device. Be sure to pull down the Mount Point and select "JE", or whatever returns you the Product Name "Defender," in order to obtain the correct information. Also, be sure only one Defender device is connected to assure a proper match between the serial number and device.


Serial Number Display Tool

Mount Point: JE

Product Name: Defender

Serial Number: 0700070878A7A51C1633

3) If you find that the SNTool is not available from the DVD-RW-CD-Rom partition on the device, you can get it from Kanguru's technical support site. Go to Kanguru.com → Support → Technical Support → Visit Tech Support → Software Downloads → Serial Number Display Tool. The tool can be retained on the desktop for future use.

4) Copy the device serial number to your clipboard.

5) Log into KRMC, navigate to the "Devices" page, and search by pasting that serial number into the search bar. The device will be found immediately and you can edit the information to add the user's name, email address, and phone number (as in step 3b on page 1) before issuance.

   NOTE: A device's serial number is displayed when a user runs KDM. However, the SNTool can also be run to determine the serial number in the case where the user cannot log in or the administrator cannot determine the serial number by looking at other criteria within KRMC. Note that even if a device is disabled, it should show up as being connected in KRMC and the administrator should be able to identify it.

Devices Configured Using Kanguru Cloud Provisioning Tool

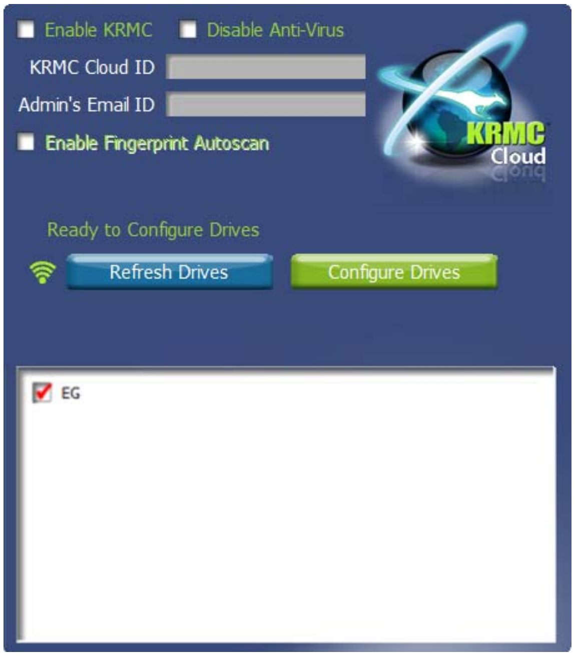
This section only applies if you are using the Kanguru Cloud Provisioning Tool to enable KRMC Cloud and/or to disable on-board anti-virus. The Kanguru Cloud Provisioning Tool must be used to configure devices before they are provided to the end user. This section does not apply to devices already registered with KRMC.

The following drive models are supported by the Cloud Provisioning Tool: Defender 3000, Defender Elite300, Defender Elite30, Defender BioElite30. If you are using a different drive model than the ones listed here, then you will not be able to use the Cloud Provisioning Tool and must use KLA to configure your drives.

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

To enable KRMC Cloud and register your Defender devices with your KRMC Cloud account using the Kanguru Cloud Provisioning Tool:

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



☐ Enable KRMC ☐ Disable Anti-Virus

KRMC Cloud ID

Admin's Email ID

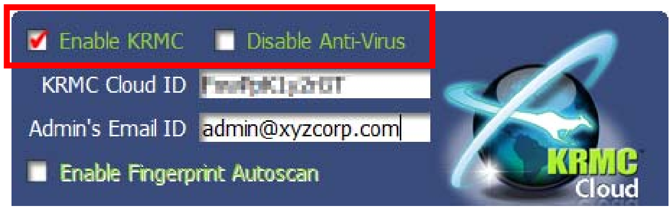
☐ Enable Fingerprint Autoscan

Ready to Configure Drives

☑ EG

Note: If no devices appear in the Kanguru Cloud 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 anti-virus on the selected devices, select the "Disable Anti-Virus" checkbox.



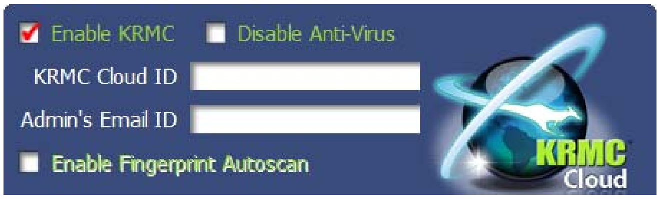
☑ Enable KRMC ☐ Disable Anti-Virus

KRMC Cloud ID [redacted]

Admin's Email ID admin@xyzcorp.com

☐ Enable Fingerprint Autoscan

3. The fields for "KRMC Cloud ID" and "Admin's Email ID" become active. Fill in these fields with the appropriate information.



☑ Enable KRMC ☐ Disable Anti-Virus

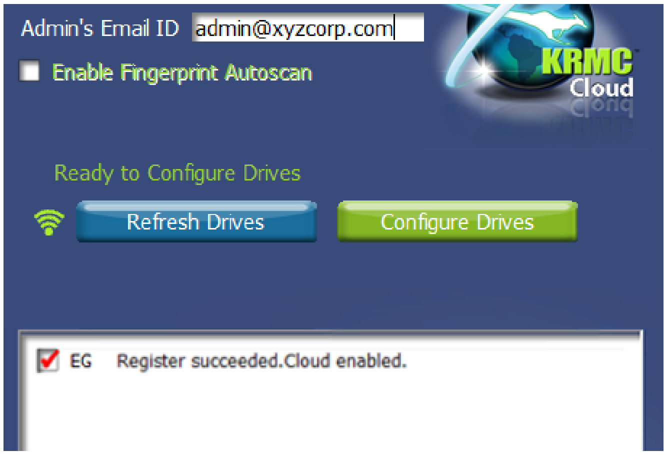
KRMC Cloud ID

Admin's Email ID

☐ Enable Fingerprint Autoscan

Note: If the device that you are provisioning is a BioElite30 model, then you have the option to select "Enable Fingerprint Autoscan". Selecting this option will configure the device so that 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. Cloud enabled."



Admin's Email ID admin@xyzcorp.com

☐ Enable Fingerprint Autoscan

Ready to Configure Drives

☑ EG Register succeeded.Cloud enabled.

Note: If you receive a status message stating, "unable to enable KRMC Cloud" then please reset the device(s) to the factory default settings and retry.

KRMC has now been enabled on the device and the device has been registered with your KRMC Cloud account.