



RPC2™ Communications Module

MCT Mass Configuration and Firmware Update

Installer/User Guide

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures. For additional assistance, visit <https://www.VertivCo.com/en-us/support/>.

TABLE OF CONTENTS

1 Overview	1
1.1 Minimum Requirements	1
1.2 Using the Tool	1
1.2.1 Agent/Devices tab	2
1.2.2 Configuration tab	5
1.2.3 Firmware tab	6
1.2.4 Tasks tab	7

1 OVERVIEW

The Mass Configuration Tool (MCT) is a software tool designed to manage configuration for and apply firmware updates to several Emerson Network Power RPC2™ network interface cards and communications modules in parallel. The MCT enables you to push a configuration from an RPC2 module to other RPC2 modules, or from a Liebert® RPC-1000™ module to other RPC2 modules, saving hours of configuration time for devices subsequently added to your network.

Major features include:

- Pull configuration from RPC-1000 and provision or clone to RPC2
- Pull configuration from RPC2 and provision and clone to RPC2
- Single firmware update to RPC-1000
- Mass firmware updates to RPC2s
- Reboot or reset devices to factory defaults
- Maintain configuration and firmware update history in the local database
- Store network card configurations and firmware files to local folders

NOTE: You cannot push a configuration from an RPC2 module to an RPC-1000 module. The RPC-1000 modules can be firmware updated only one unit at a time.

As a supplement to the RPC2™ Communications Module User Manual, this guide describes how to access and navigate the tool. Prior to using this tool, see the RPC2™ Communications Module User Manual for instructions to install and operate the RPC2 Communications Module.

1.1 Minimum Requirements

The following are the minimum requirements to use the tool:

- RPC2 Communications Module firmware upgraded to version 9.0.0.5 or later
- 1 GHz or faster 32-bit (x86) or 64-bit (x64) processor
- Microsoft® Windows™ 7 or later
- Java™ version 8 or later
- Network access using SNMPv1v2, HTTP/HTTPS protocols over TCP/IP networks for client/host communications

1.2 Using the Tool

The MCT file is available at <https://www.vertivco.com/en-us/support/software-download/it-management/mph2-managed-rack-pdu-software-downloads/>.

To download the MCT:

1. Download the zip file to a folder on your computer.
2. Extract the files from the folder.
3. Double-click the MCT.bat file to open the application.

The main page of the web user interface (UI) has four tabs which are used to discover devices, map configurations, upgrade the firmware and manage tasks.

Figure 1.1 Mass Configuration Tool Example



Table 1.1 Mass Configuration Tool Description

NUMBER	NAME	DESCRIPTION
1	Agent/Devices	Discover, manage and pull configurations from devices
2	Configuration	Create mappings of configurations used for tasks
3	Firmware	Retrieve firmware update files used for tasks
4	Tasks	Create and run tasks to manage configuration push and firmware update to one or more devices
5	Help	Opens the Mass Configuration Tool User Guide
6	Status light	Flashes when a process is running

NOTE: Network performance, configuration size and number of parallel tasks running can influence the time for configuration pull and tasks to complete.

1.2.1 Agent/Devices tab

From the Agent/Devices tab, you can discover devices, view a list of discovered communications modules saved in the database, force a reboot or reset to factory default or retrieve their configurations and configure SNMP settings and update usernames and passwords for RPC-1000 communications modules.

Before you add devices to the MCT, only the Discover button is enabled. When devices are discovered and added to the MCT database, you must click on the name of the device to select it before the buttons for actionable processes become enabled. For example, you must click on a device to select it for the Settings button to be enabled.

When a device is busy with an operation, buttons for conflicting operations are disabled until the current operation is complete.

You can also abort an upload or any other action task at any point during its process. The Abort feature is only available after a process is in progress. When a process starts, the Abort button is enabled. Otherwise, the Abort button remains disabled. After devices are discovered, they can be accessed individually for configuration.

To discover devices:

NOTE: The time to complete the discovery process depends on the size of the IP address range.

1. From the Agent/Devices tab, click *Discover*.
2. For a range of IP addresses, select the IPV4 Range radio button and enter the start IP address and end IP address.

-or-

For a single device, select either the IPV4 Single or IPV6 radio button and enter the IP address.

3. Select the Use SNMPv1v2 radio button in the SNMPv1v2 Community section and enter strings for the Read Only Access and Read/Write Access fields.

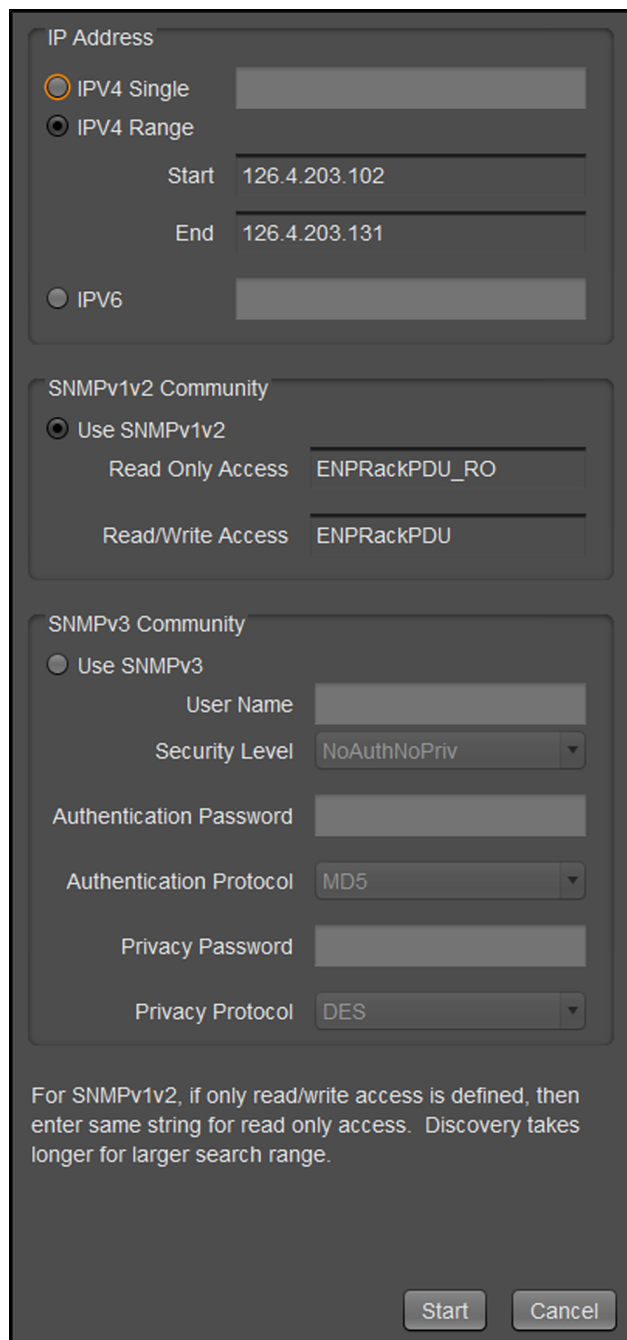
-or-

Select the Use SNMPv3 radio button in the SNMPv3 Community section, enter strings for the User Name, Authentication Password and Privacy Password fields, and make the appropriate selection from the Security Level, Authentication Protocol and Privacy Protocol drop-down lists.

NOTE: The discovery process only finds RPC-1000 and RPC2 devices if the SNMP community strings are properly assigned, correct SNMP protocol is used and agents/devices are connected to the network and operational.

4. Click *Start* to search for devices, then click *OK* in the Discovery Status window.

Figure 1.2 Agent/Devices Discovery Dialog



The dialog box is titled "Agent/Devices Discovery Dialog". It contains three main sections for configuration:

- IP Address:**
 - ☐ IPv4 Single: A text field for a single IP address.
 - ☒ IPv4 Range:
 - Start: 126.4.203.102
 - End: 126.4.203.131
 - ☐ IPv6: A text field for an IPv6 address.
- SNMPv1v2 Community:**
 - ☒ Use SNMPv1v2:
 - Read Only Access: ENPRackPDU_RO
 - Read/Write Access: ENPRackPDU
- SNMPv3 Community:**
 - ☐ Use SNMPv3:
 - User Name: [Text Field]
 - Security Level: NoAuthNoPriv (Dropdown)
 - Authentication Password: [Text Field]
 - Authentication Protocol: MD5 (Dropdown)
 - Privacy Password: [Text Field]
 - Privacy Protocol: DES (Dropdown)

At the bottom, there is a note: "For SNMPv1v2, if only read/write access is defined, then enter same string for read only access. Discovery takes longer for larger search range." Below the note are "Start" and "Cancel" buttons.

To delete devices:

1. From the Agent/Devices tab, select one or more devices.
2. Click *Delete*, then click *OK* in the warning dialog.

NOTE: If the device is deleted, any configuration files, mapping and tasks associated with it are deleted.

To reboot the device:

1. From the Agent/Devices tab, select one or more devices.

2. Click *Reboot*, then click *OK* in the warning dialog.

To restore factory defaults for a device:

1. From the Agent/Devices tab, select one or more devices.
2. Click *Reset Factory Defaults*, then click *OK* in the warning dialog.

To upload device configurations:

1. From the Agent/Devices tab, select one or more devices.
2. Click *Retrieve Configuration*, click *OK* to confirm you want to retrieve the device's configuration and click *OK* to acknowledge the saved file's location.

NOTE: The device status changes from Ready to Busy while the configuration is retrieved.

3. Click *OK* after the configuration process is complete.

To delete a device configuration:

1. From the Agent/Devices tab, select one or more devices.
2. Click *Delete Configuration File*, then click *OK* in the warning dialog.

To abort a process:

After the Abort button becomes enabled, indicating the process is in progress, click *Abort* from the Agent/Devices tab, and click *OK* in the warning window.

To view the community strings:

From the Agent/Devices tab, click *Settings*.

NOTE: Valid login credentials are necessary to download a configuration and update the firmware on an RPC-1000.

To change the username and password for an RPC-1000 communications module:

1. From the Agent/Devices tab, select one or more devices and click *Settings*.
2. Enter the username.
3. Enter and confirm the password, then click *Save*.

NOTE: The RPC2 module does not require authorization.

1.2.2 Configuration tab

From the Configuration tab, you can create, view and edit mappings that are used to push configuration settings. Each mapping defines a communications module as the source and one or more modules as the targets. The source configuration settings can either be provisioned to or cloned on the target. With the provisioning feature, you can pick individual elements from a configuration to push to a target device, however provisioning does not push user-customized labels to target devices. If you want to push an entire configuration including labels from a source to a target, you can use the clone feature.

When provisioning device configurations such as PDU, branch and receptacle configurations, the source and target models and array configuration must be identical.

To create a configuration mapping:

1. From the Configuration tab, click *Add* and enter a unique mapping name that describes the Source to Target device relationship.
2. Click *Save*.
3. Click *Select* in the Source section, select the system name of the preferred source device and click *Save*.
4. Click *Configure* in the Target section.
5. Select the Provision radio button and enable the checkboxes next to the sets to be pushed.

-or-

Select the Clone radio button.

6. Select the system name of the preferred target device from the Target ID list and click *Save*.

NOTE: If the mapping is modified or deleted, a task using it will be affected or deleted, respectively.

To edit a mapping name:

1. From the Configuration tab, select the mapping name from the Configuration Name list and click *Edit Name*.
2. In the Name field, enter the updated name and click *Save*.

To delete a mapping:

1. From the Configuration tab, select the mapping name from the Configuration Name list.
2. Click *Delete*, then click *OK*.

1.2.3 Firmware tab

From the Firmware tab, you can view a list of uploaded RPC communications module firmware files. Before a firmware file can be uploaded, you must download it from the Vertiv website. After it is downloaded, load the individual firmware files into the tool.

To add firmware update files to the tool:

1. From the Firmware tab, click *Add*.
2. Click *Browse File* or enter the path and name where the previously downloaded firmware update file is located.

NOTE: The firmware file must have an .epm extension.

3. Click *OK*.
4. (Optional) In the Upload Firmware window, enter a description of the firmware update file in the Notes field.
5. Click *Upload*.

To delete firmware files from the tool:

1. From the Firmware tab, select the firmware file.
2. Click *Delete*, then click *OK*.

1.2.4 Tasks tab

Tasks can be created to push configuration settings from a source device to target devices after a configuration mapping is created. Tasks can also be created to upgrade firmware on single or multiple devices. Make sure the settings or firmware updates apply for all mapped targets in your local or remote data center.

NOTE: If a system name is changed by a configuration update or another client, delete and rediscover the affected RPC. In addition, if devices undergo configuration changes, they should be deleted from the Agent/Devices tab and rediscovered so the MCT database is updated accordingly.

To add a configuration task:

1. From the Tasks tab, click *Add Configuration*.
2. Enter the configuration task name in the Add Configuration window.
3. Select the applicable configuration mapping and click *Save*.

To edit a configuration task:

1. From the Tasks tab, select the configuration task name and click *Edit*.
2. Enter the updated name and/or select the correct configuration mapping and click *Save*.

The entire firmware file must be programmed to the device and must be complete before accessing the device or changing the configuration. If timeouts occur while adding firmware update files, limit the task from 10 to 20 modules.

NOTE: Downgrading firmware is not recommended because it resets the configuration to factory default settings.

To add a firmware task:

1. From the Tasks tab, click *Add Firmware*.
2. Enter the firmware task name in the Add Firmware window.
3. Select the drop-down list and click the applicable firmware file.
4. Click *Add*, select the applicable target devices and click *OK*.

-or-

Select the applicable devices from the Device ID list and click *Delete*.

5. Click *Save*.

To edit a firmware task:

1. From the Tasks tab, select the firmware task name and click *Edit*.
2. Enter the updated task name in the Edit Firmware Task window.
3. From the drop-down list, select the applicable firmware update file.
4. Click *Add* and select the applicable target devices.

-or-

Select the applicable devices from the Device ID list and click *Delete*.

5. Click *Save*.

To run a task:

1. From the Task tab, select the task and click *Run*.

NOTE: The device status changes from Ready to Busy while the task runs, and from Busy to Completed successfully when the task is complete.

2. (Optional) Click *Completed successfully* for a comprehensive report dialog with the individual status of each device impacted by the task.

NOTE: After certain types of a configuration push or a firmware update is complete, the device automatically reboots. During the reboot process, the agent does not communicate.

To delete a task:

NOTE: Deleting a task does not delete the associated firmware files or configuration mappings.

1. From the Task tab, select the task and click *Delete*.
2. Click *OK*.

