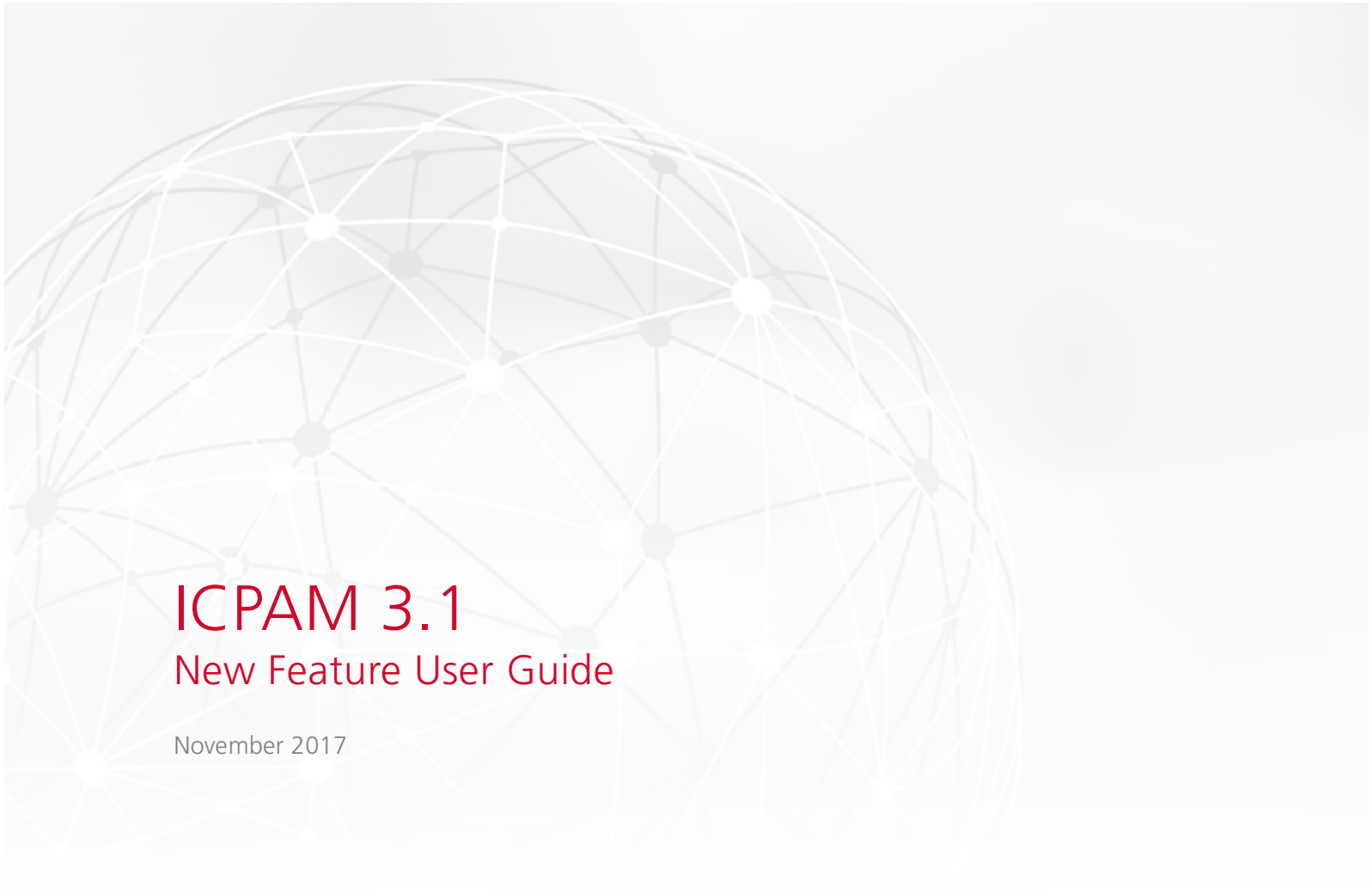


ICPAM 3.1

New Feature User Guide

November 2017

IDENTIV

Contents

Introduction

This document explains configuring the following new features implemented in ICPAM 3.1.

- Updating Mx Controller's CCM Firmware.
- Unified Credential Template.
- Adding an Mx-1 controller.
- Adding and Configuring an Mx-8 controller as an IT Rack controller.
- Lockdown feature for Mx and EM-100 controllers.
- Configuring an External Input Module (EIM) when adding an EM-100 controller.

Updating Mx Controller's CCM Firmware

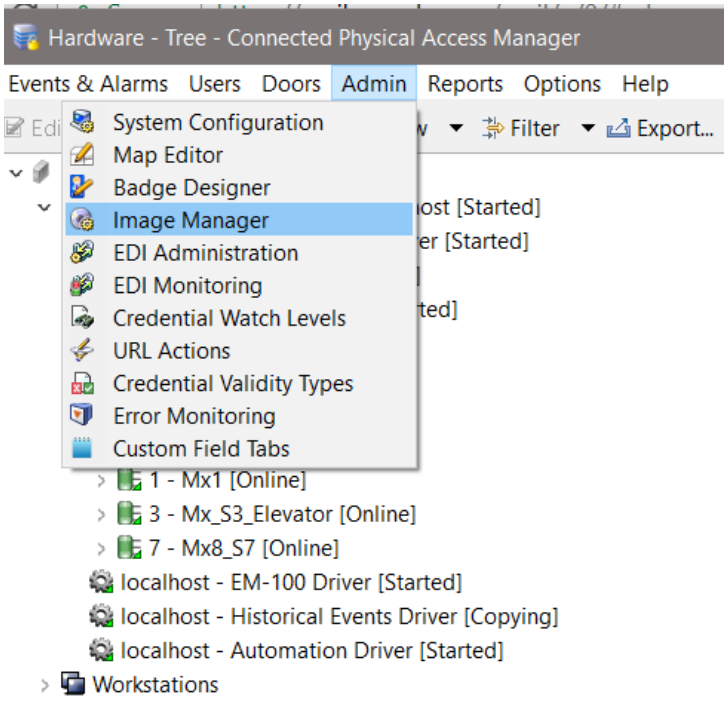
ICPAM 3.1 now supports Mx Controller Command & Control Module (CCM) firmware updates via the ICPAM software client. Updating the CCM firmware ensures optimal operating conditions and allows for support of the latest features in ICPAM. It is HIGHLY REOMMENDED to upload the latest version of CCM firmware to all Mx controllers in a production system.

Work Flow

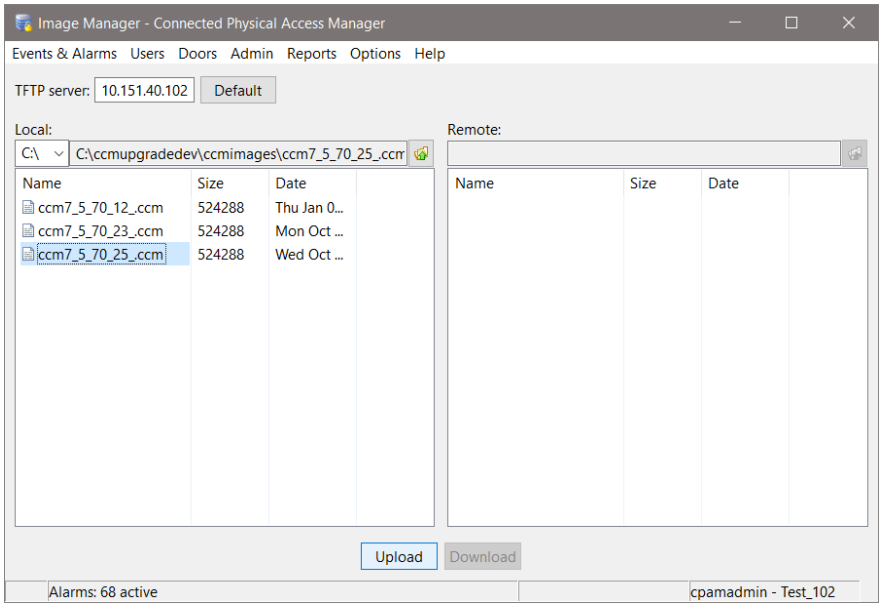
- Upload the CCM image to ICPAM server via Image Manager Module
- Download the CCM image to Controller from ICPAM server

Upload CCM Image to the ICPAM Server

- Upload CCM image to ICPAM server using Image Manager Module
    - To launch Image Manger, Select "Admin" → "Image Manager"



- In the Image Manager, browse to local folder that has CCM image. Then upload the CCM image to the ICPAM server

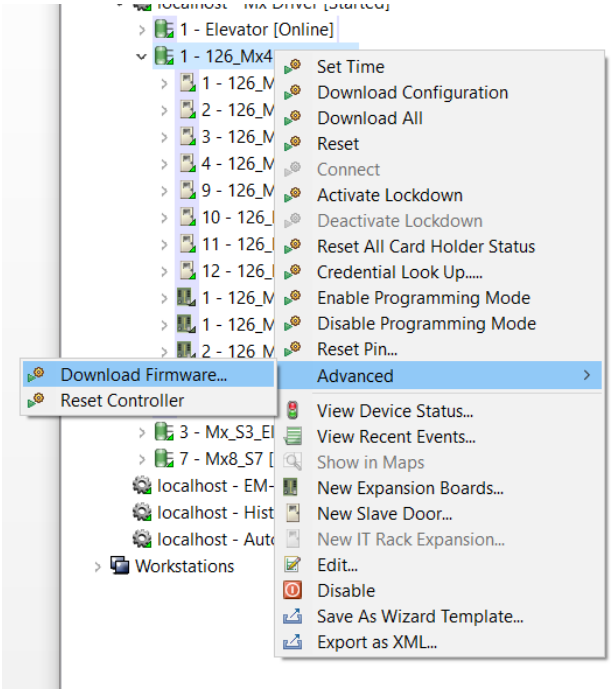


- Select the CCM image and click "Upload." A file successfully uploaded message will appear once completed

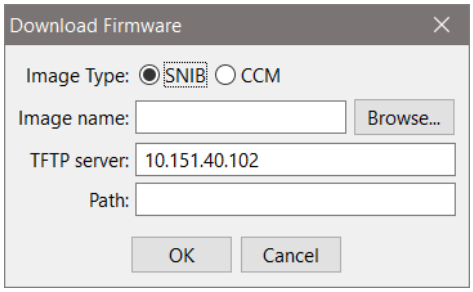
Download CCM Image to the Mx Controller

With the CCM file successfully uploaded to the ICPAM server, the firmware needs to be pushed to EACH Mx Controller individually.

- Download CCM firmware to the Mx Controller
    - Right click on the desired Mx Controller in the Hardware tree, Select "Advanced" → "Download Firmware"

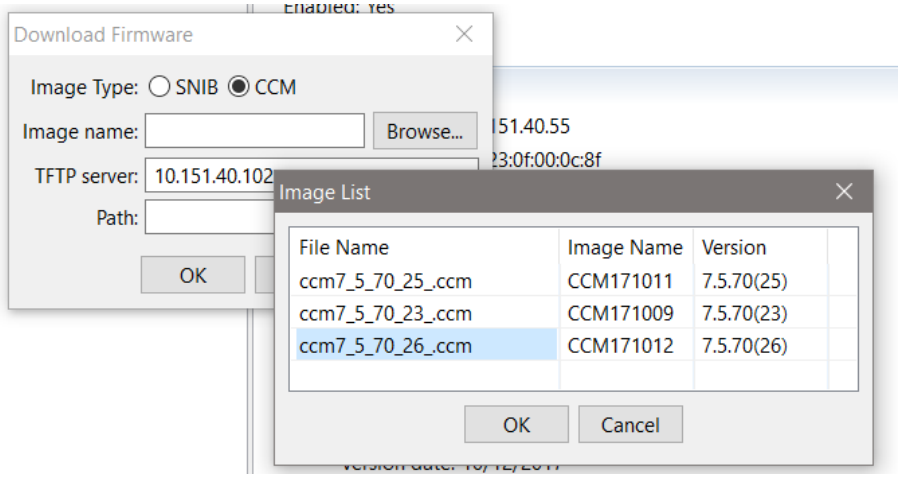


- A dialog box will appear asking to select the CCM firmware image uploaded to the ICPAM server

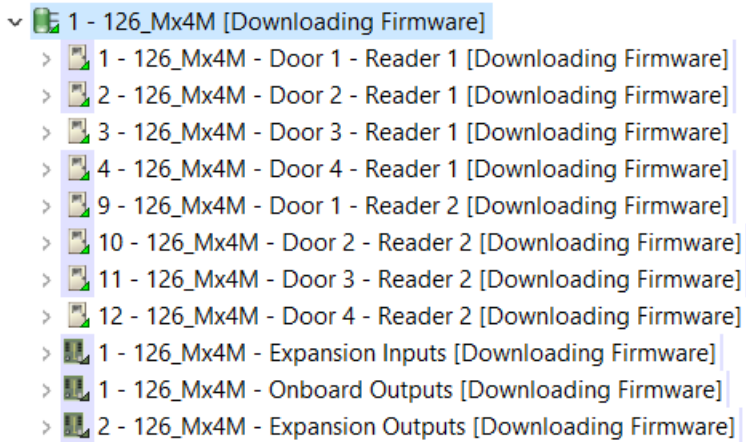


IMPORTANT NOTE: Make sure the CCM image downloaded is compatible with ICPAM. Failure to do so may lead to improper operation from the controller.

- Select "CCM" and click *Browse* to access the "Image List"



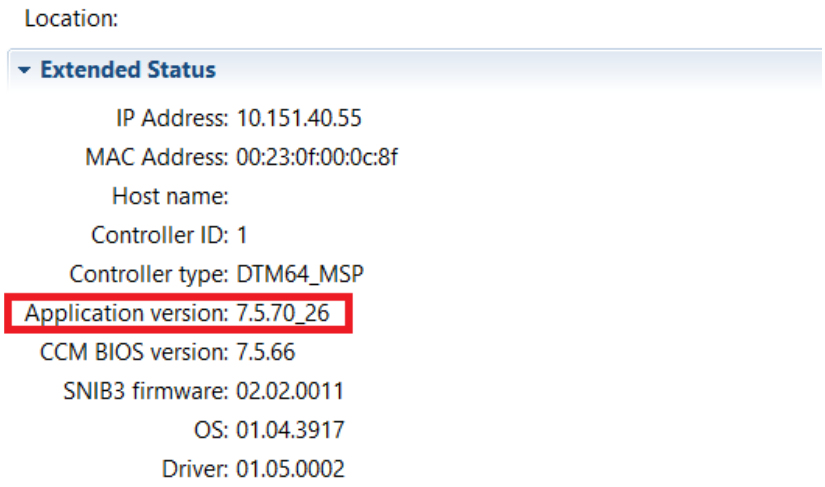
- Select the desired CCM image from the list and click *OK*. Confirm the CCM image selected and server information is correct and click *OK* to begin the upgrade process.
- During the image download, the controller will be in "Downloading Firmware" state.



- Once the download is completed, the Mx controller will go offline while completing the upgrade process. The controller will automatically restart and will come back online after the upgrade is successful.

Verifying the CCM Image

To verify the CCM firmware version, select the updated controller from the hardware tree and check the "Extended Status".



Unified Credential Template

In order for badges to function with ICPAM controllers, a credential template needs to be defined. This document explains how to define credential templates and associate them with a badge. When an access control card is presented to a reader, the reader reads a set of bits. The reader needs to know how to interpret the bits, how to validate the data, and how to extract relevant card information. Credential Templates specify the card data format for a reader.

Work Flow

- Get the badge format details from the Vendor
- Define Credential Template based on the badge format
- Associate credential Template to badge.
- Configure controller specific detail
  - Define facility code for EM-100 controllers
  - Define reader properties for MX controllers
- Download the configuration to the controllers

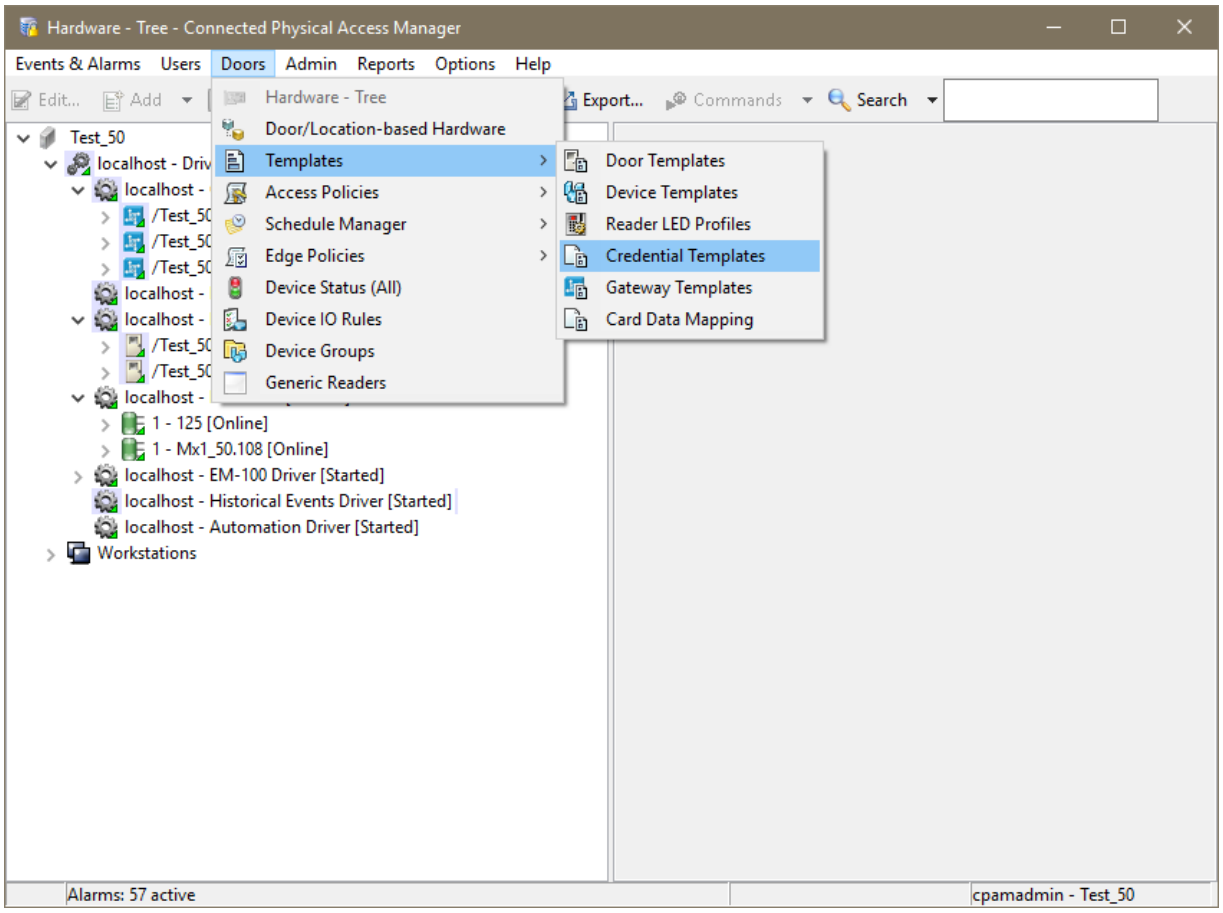
Data Needed to Define a Credential Template

Before defining a credential template, the following data should be collected from the card vendor,

- Total number of bits
- Total number of fields in the format (for example, facility code, badge number or company id)
- Bit details for each field (start position, end position, etc.)
- Parity bit positions, its nature (odd or even) and bit positions (bit ranges) that are needed to derive the parity bit value (odd or even)

Credential Template Module UI

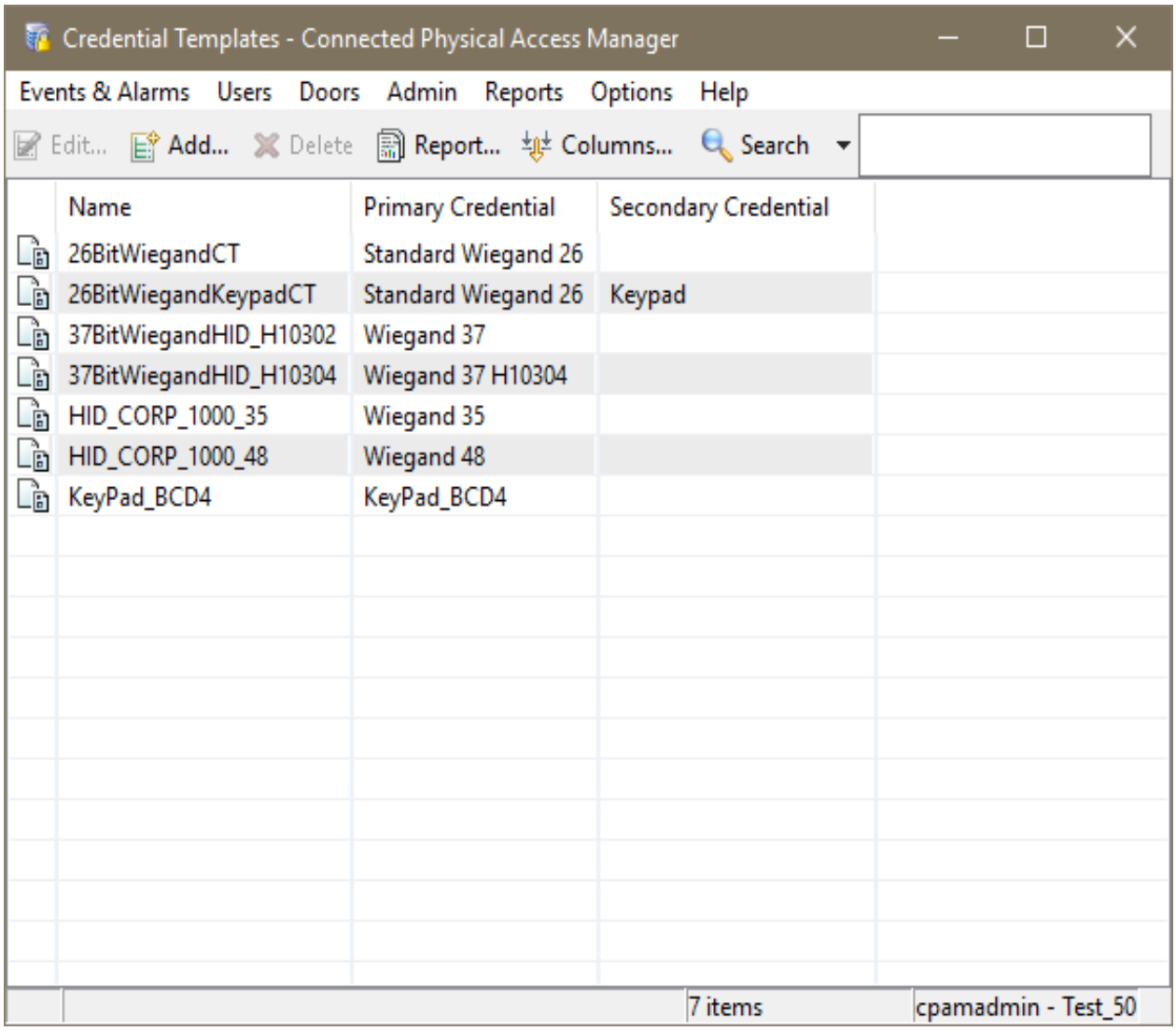
The Credential Templates module is used to define credential templates.



Predefined Credential Templates

In the Credential Templates module, commonly used credential templates are available by default,

- 26BitWiegandCT- Standard 26 bit Wiegand format with parity
- 26BitWiegandKeypadCT
- 37BitWiegandHID_H10302 - 37Bit Open format
- 37BitWiegandHID_H10304 - 37Bit Managed format
- HID_CORP_1000_35 - HID_Corp 35 Bit
- HID_CORP_1000_48 - HID_Corp 48 Bit

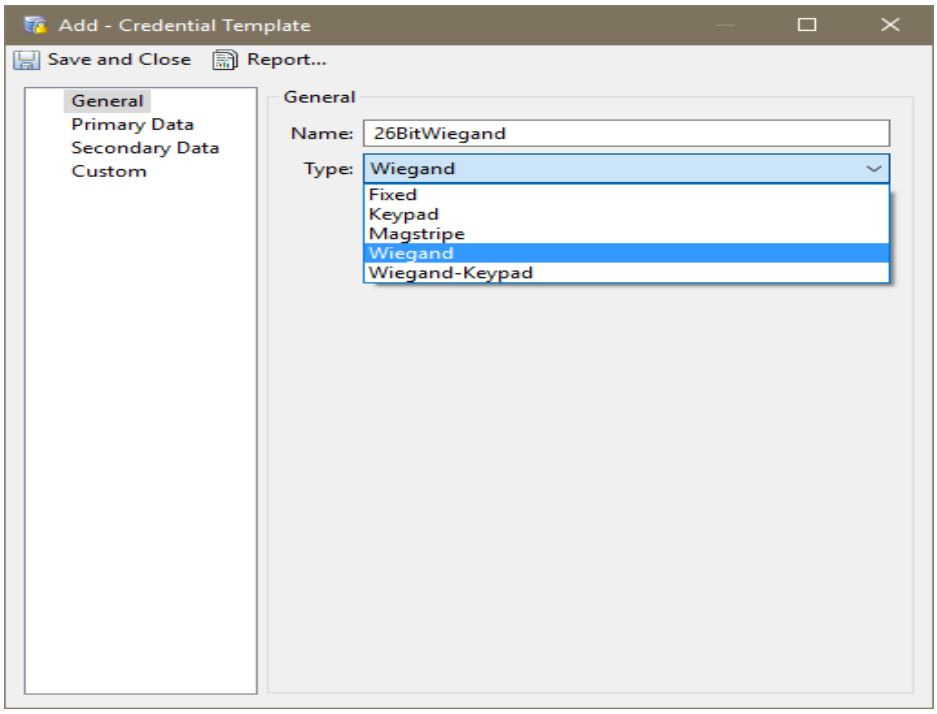


Here is an example of defining a Credential template for a 26-Bit standard Wiegand card:

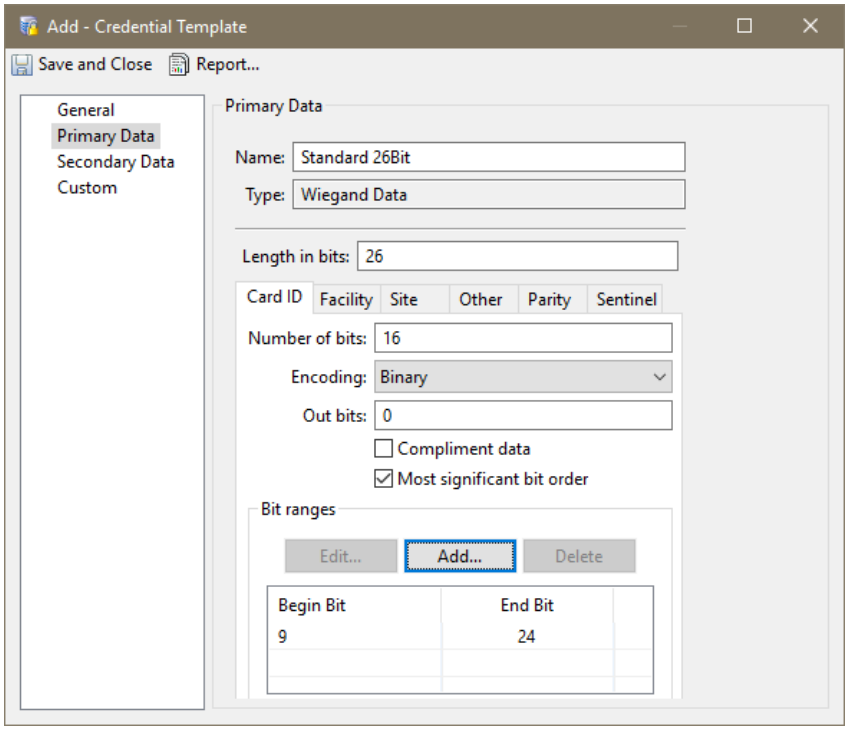
- Total number of bits
  - 26
- Total number of fields in the format (for example, facility code, badge number or company id)
  - 2(Card ID, Facility code)
- Bit details for each field (start position, end position, etc,)
  - Card ID-> total bits 16, start bit 9 and end bit 24
  - Facility Code --> total bits 8, start bit 1 and end bit 8
- Parity bit positions, its nature (odd or even) and bit positions that are needed to derive the parity
  - Two parity bits,
  - bit position 0, Bit-Ranges 1-12, even parity
  - bit position 25 Bit-Ranges 13-24, odd parity

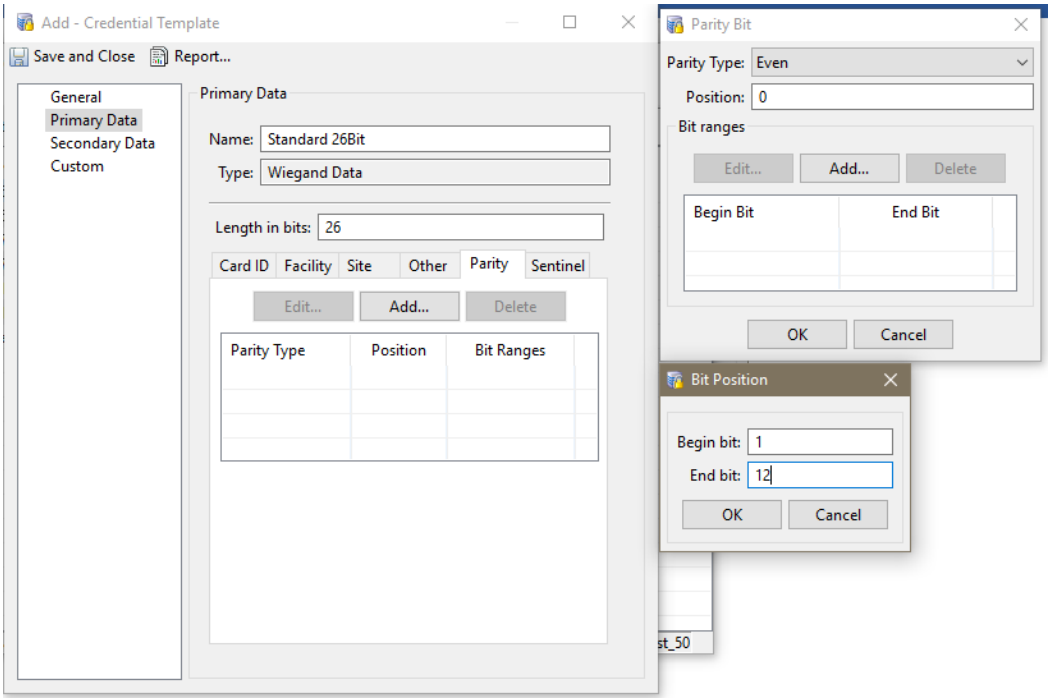
Note: If you are using a custom format, all the above details need to be collected from the card manufacturer to create a credential template.

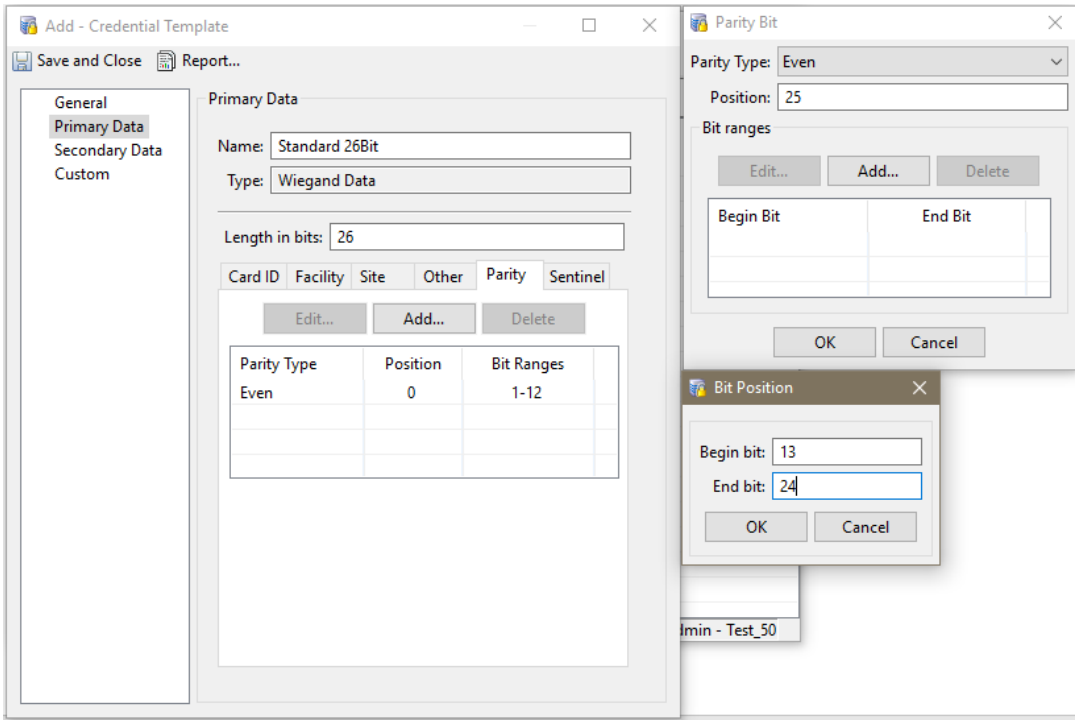
UI flow to create the above format:

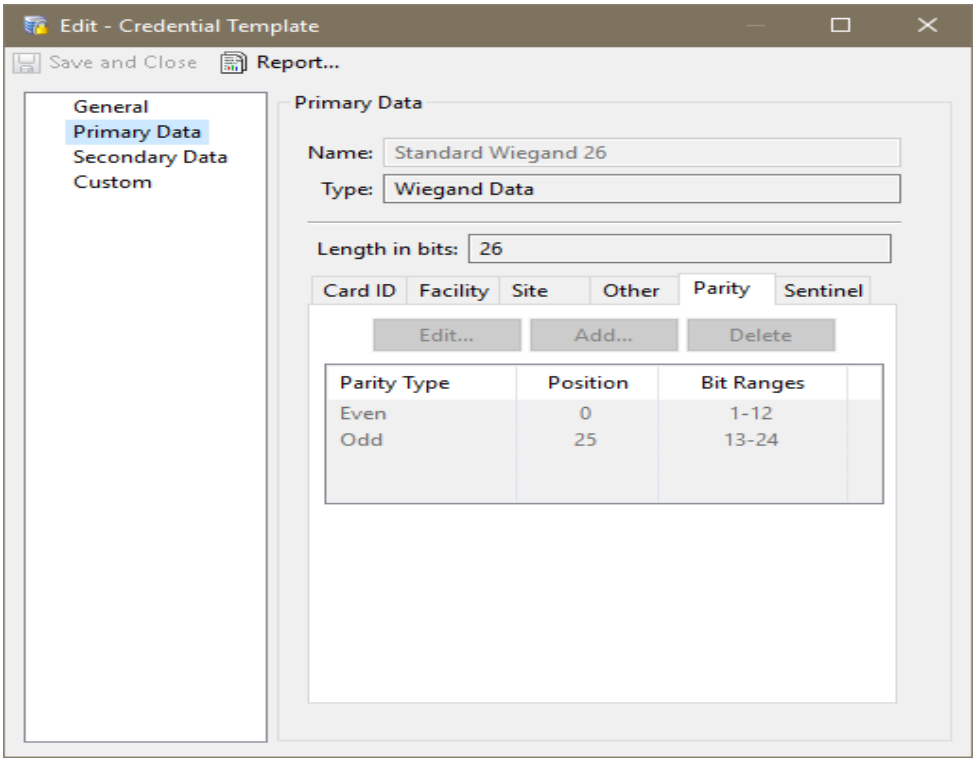


Then select Primary Data tab

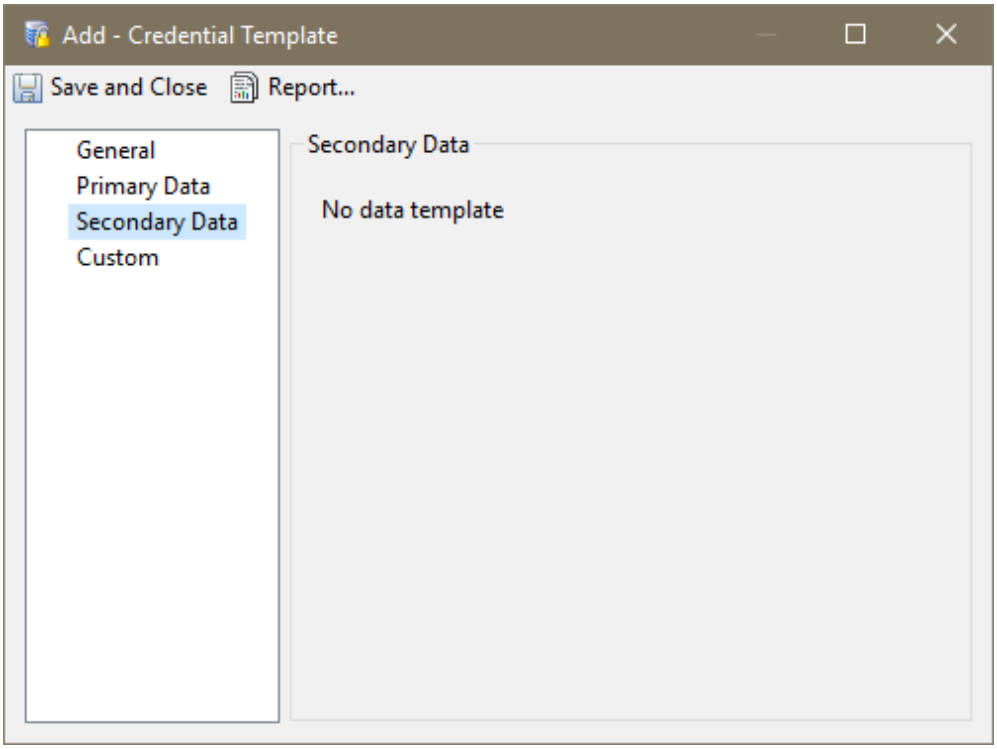



Add - Credential Template
Save and Close
Report...
General
Primary Data
Secondary Data
Custom
Primary Data
Name: Standard 26Bit
Type: Wiegand Data
Length in bits: 26
Card ID
Facility
Site
Other
Parity
Sentinel
Edit...
Add...
Delete
Parity Type
Position
Bit Ranges
Parity Bit
Parity Type: Even
Position: 0
Bit ranges
Edit...
Add...
Delete
Begin Bit
End Bit
OK
Cancel
Bit Position
Begin bit: 1
End bit: 12
OK
Cancel


Add - Credential Template
Save and Close
Report...
General
Primary Data
Secondary Data
Custom
Primary Data
Name: Standard 26Bit
Type: Wiegand Data
Length in bits: 26
Card ID
Facility
Site
Other
Parity
Sentinel
Edit...
Add...
Delete
Parity Type
Position
Bit Ranges
Even
0
1-12
Parity Bit
Parity Type: Even
Position: 25
Bit ranges
Edit...
Add...
Delete
Begin Bit
End Bit
OK
Cancel
Bit Position
Begin bit: 13
End bit: 24
OK
Cancel

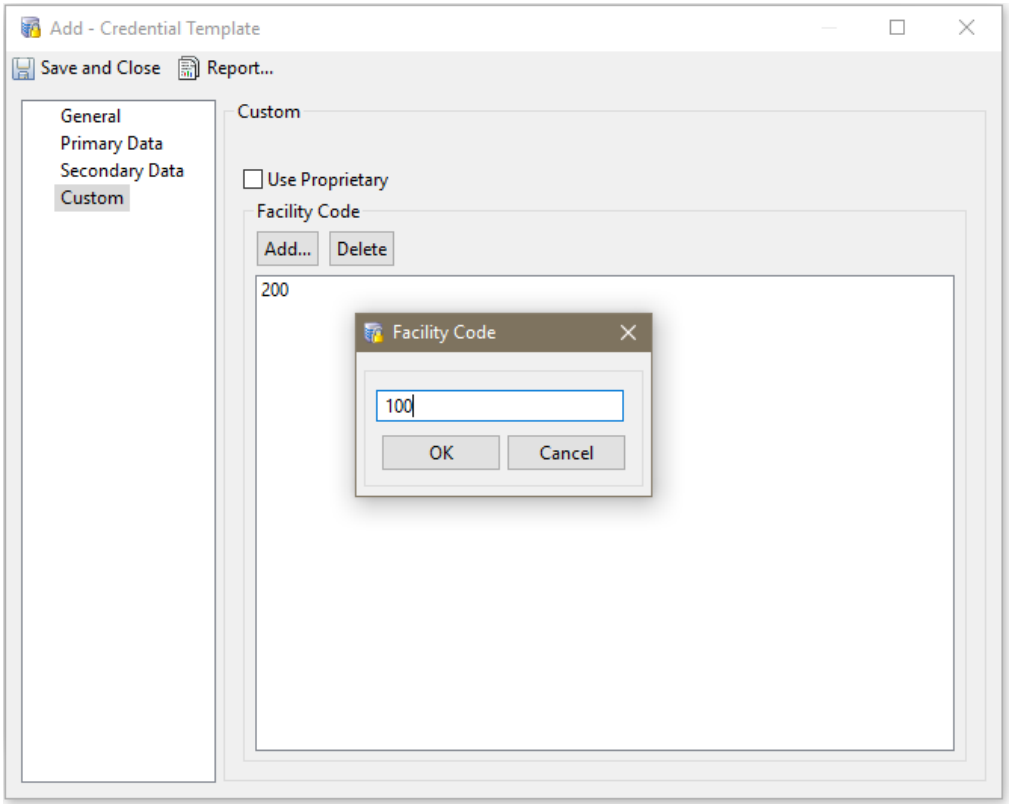


Secondary Data will be empty for a standard 26Bit credential template



Explicit Facility Code for the EM-100 Controller

The EM-100 controller requires an explicit facility code to be specified in the credential template.



Important Note: The unified credential feature hides importing VFF (Virtual File Format) files and auto generates the VFF behind the scenes based on the facility code. Multiple facility codes can be entered in this UI and in the server VFF file. After each facility code is created, it will be pushed to the controller when the "Apply Configuration Command" is issued from the controller.

Note for MX Controllers: For MX controllers, reader protocol must be "Hex Pass-Through". The unified credential feature will generate a hex code based on the credential template and its associated badge number and facility code. Thus simplifying the credential configuration.

Mx-1 Controller

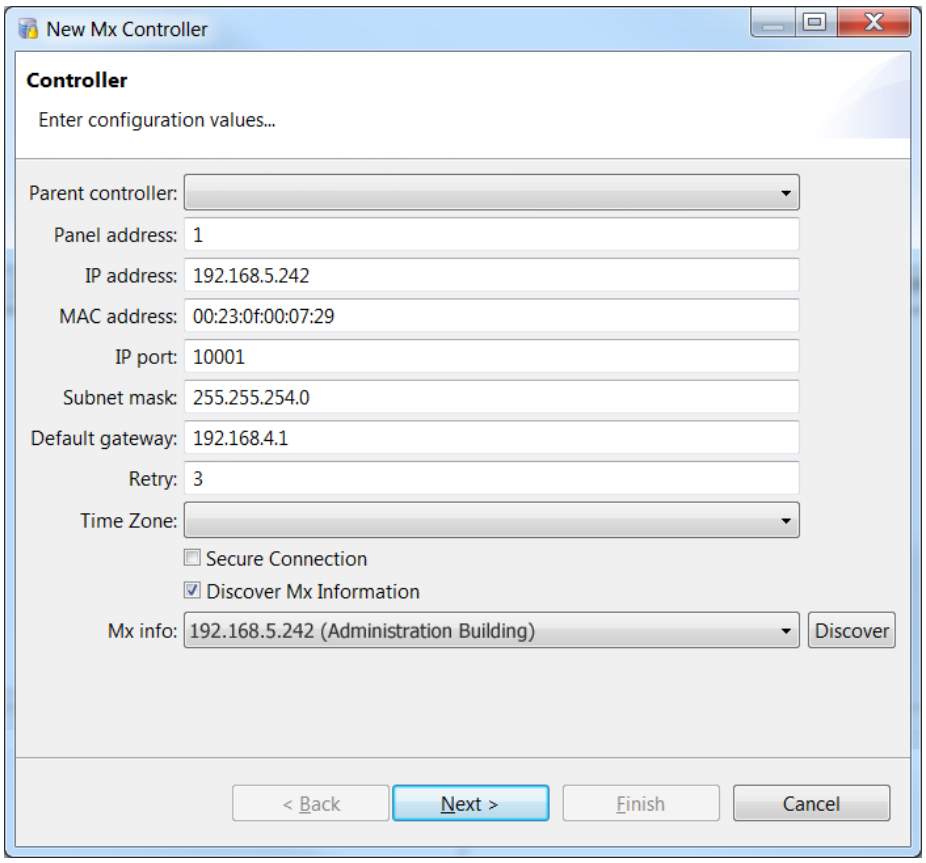
The Hirsch Mx-1 Controller manages a single fully supervised door for controlled entry and exit. The Entry reader and optional Exit reader, both support card and PIN options. Like other Hirsch controllers (such as the Mx-4 or Mx-8) the Mx-1 can be connected and configured for expansion boards (such as the AEB and REB).

Adding a New Mx-1 Controller

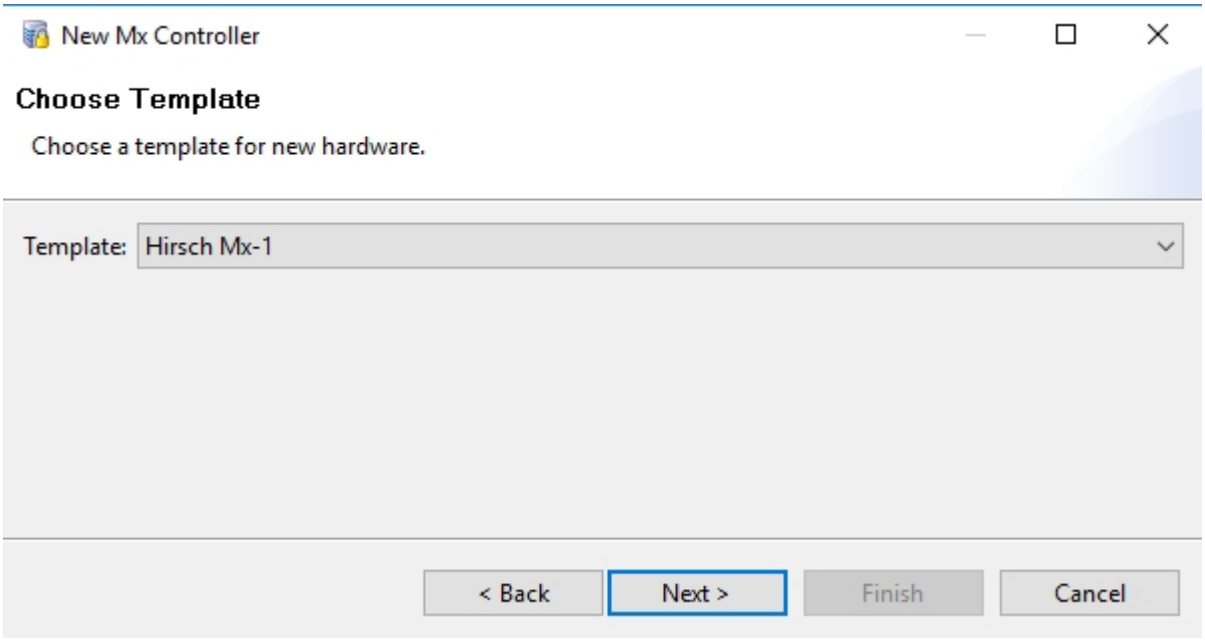
Step 1: Open the Hardware module.
Step 2: Right-click "Mx Driver" and select "New Mx Controller Wizard"

This will launch a Wizard for configuring a new Mx controller.

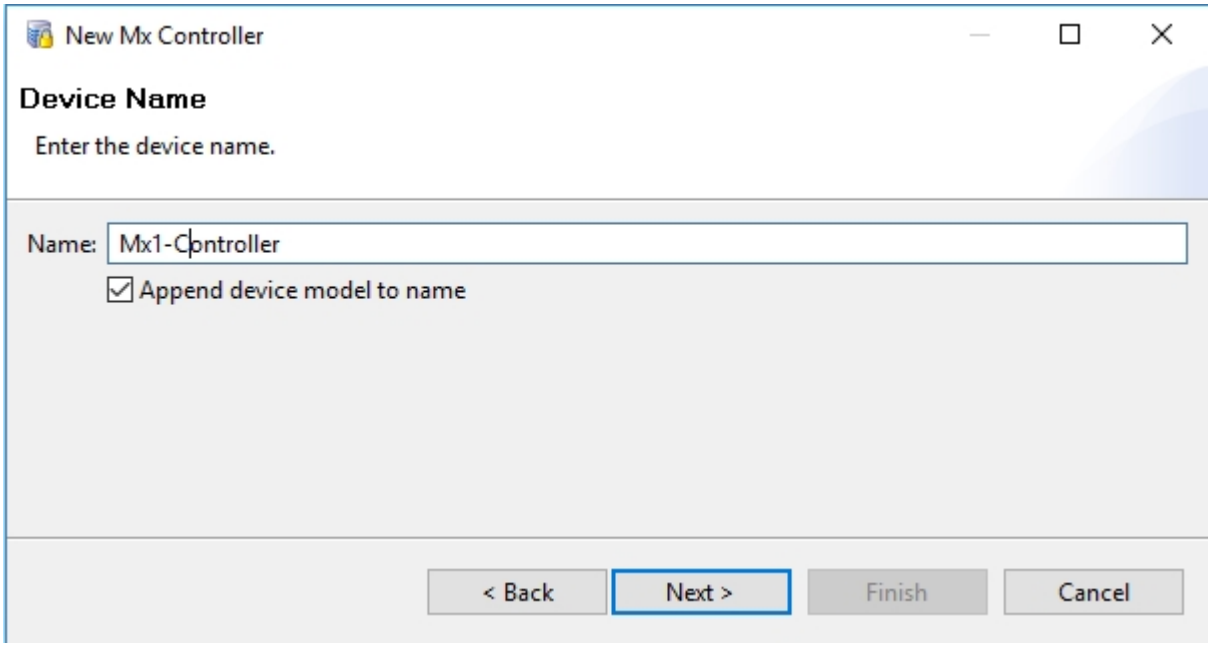
Step 3: Specify the configuration values for the Mx-1 controller on the first page, and then click the Next button.



Step 4: On the Choose Template page, select "Hirsch Mx-1" from the template drop-down list, then click Next.

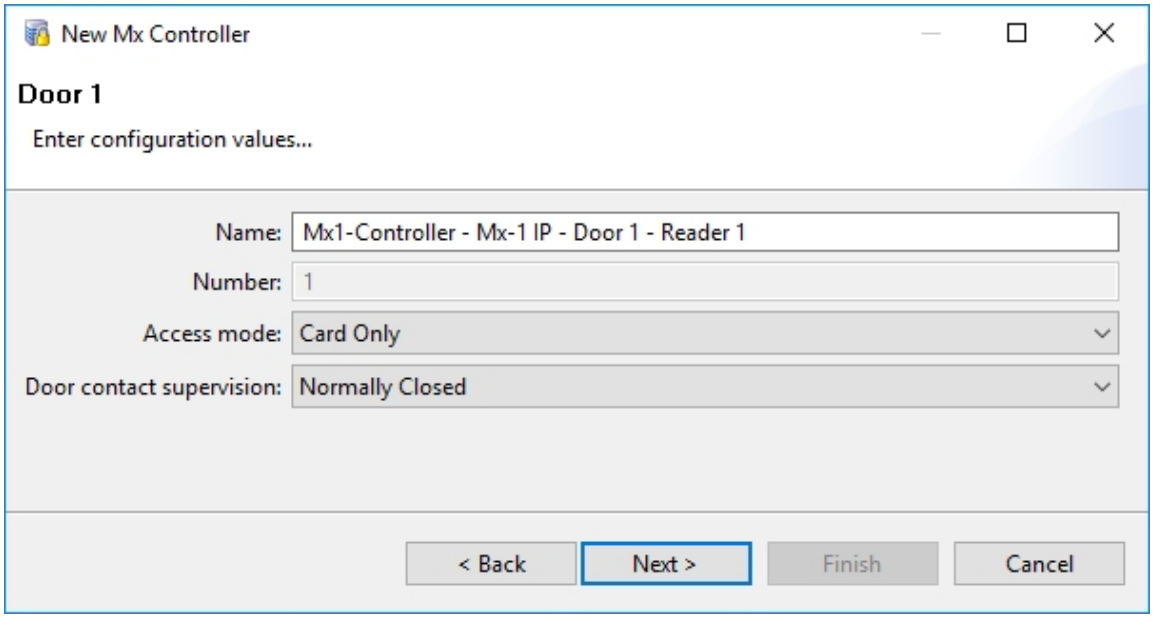


Step 5: Type a unique Name and Description for you Mx-1 controller, then click Next.



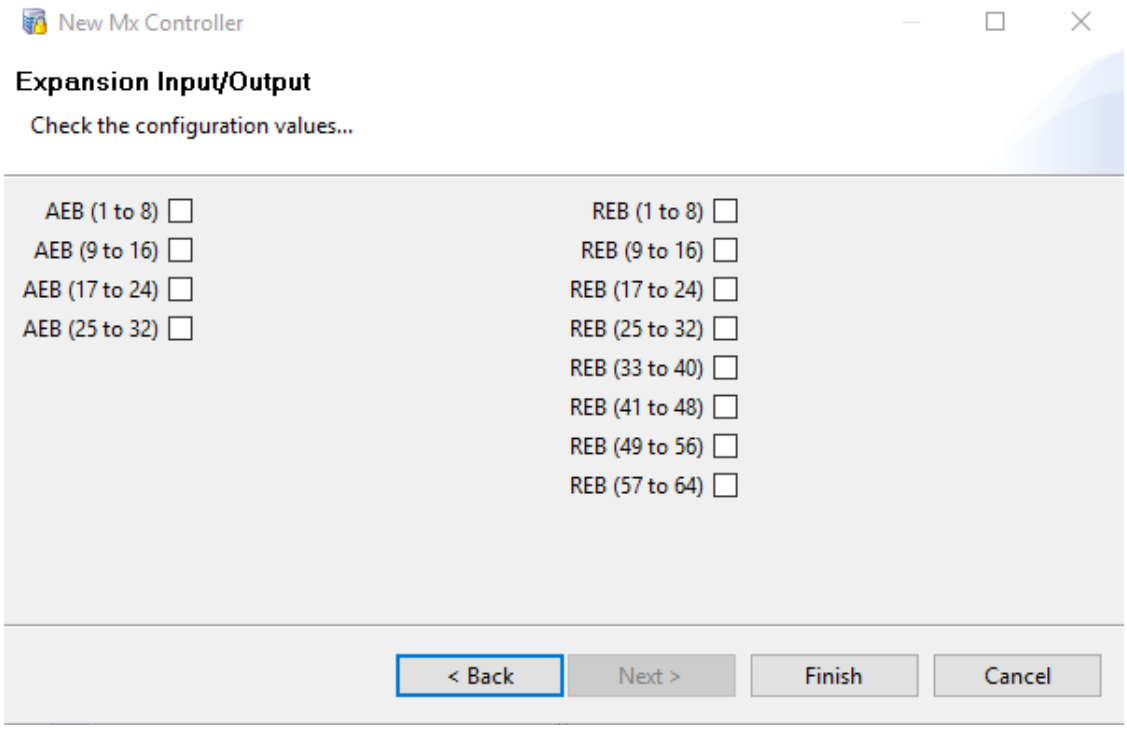
Step 6: On the resulting Door configuration page,

- Enter a unique and descriptive Name for this door. (The door's reader is set to 1, and cannot be changed.)
- If necessary, change the Door contact supervision value.
- Click the Next button.

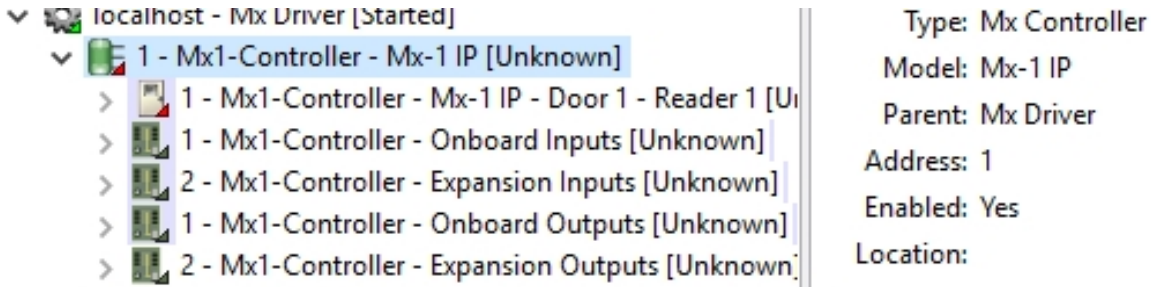


Step 7: On the resulting Expansion Input/Output page:

- If your Mx-1 controller does <u>not</u> contain any Alarm or Relay Expansion boards, then click on the Finish button.
- Otherwise, select the checkbox next to each Expansion board that is installed in the controller, then click on the Finish button.

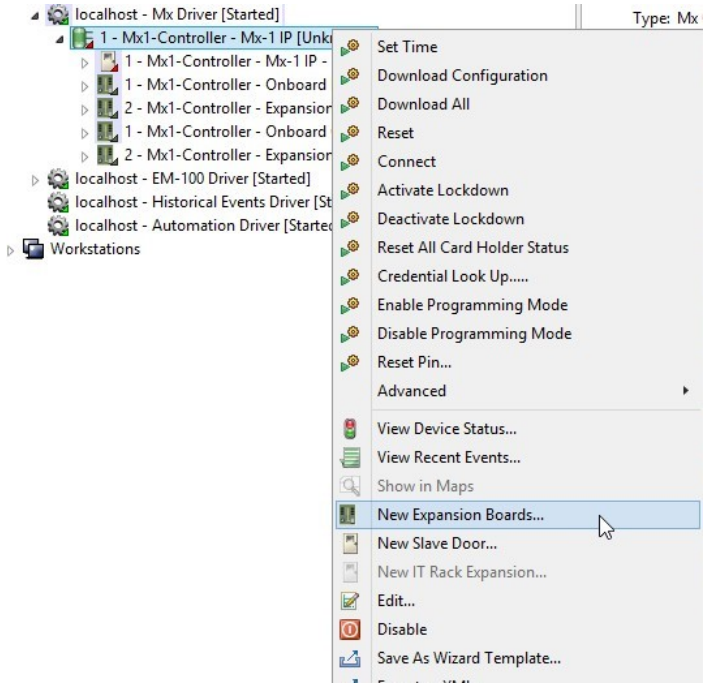


Step 8: In the Hardware module, the newly created Mx-1 controller and its components will be listed with the state of "Unknown". Right-click on the controller, and select "Connect" to connect to the Mx-1 controller.

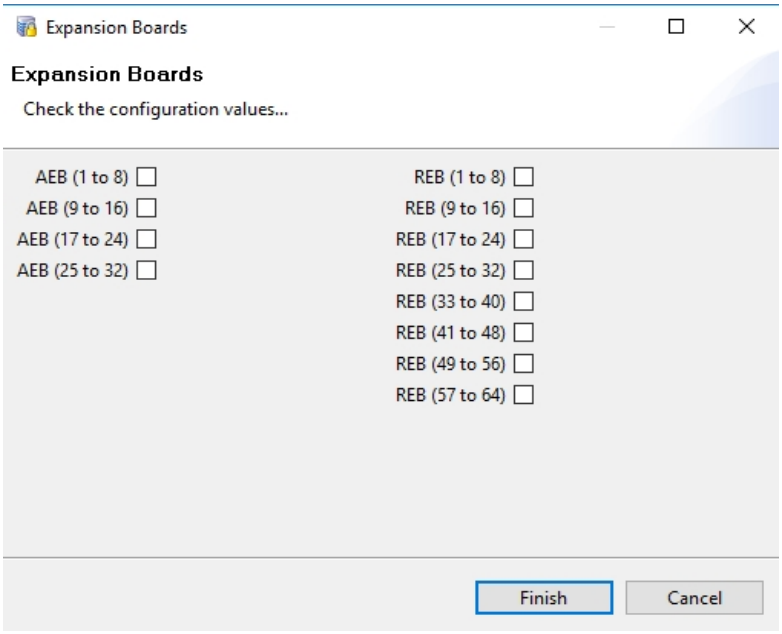


Adding Expansion Boards to an Existing Controller

If a controller was created without specifying any expansion boards, you can add expansion boards later by right-clicking on the controller and select "New Expansion Boards".



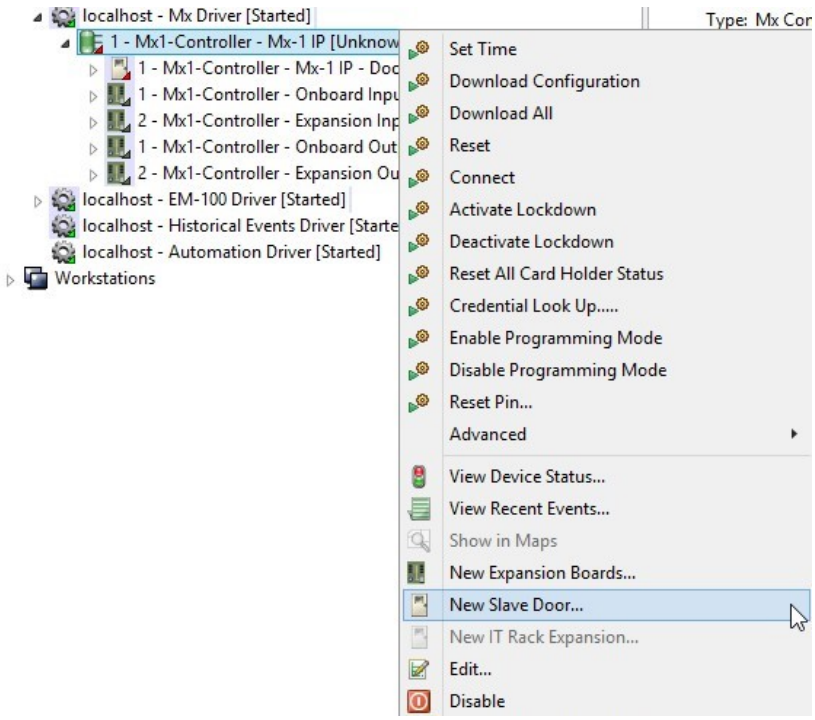
The resulting dialog looks like this:



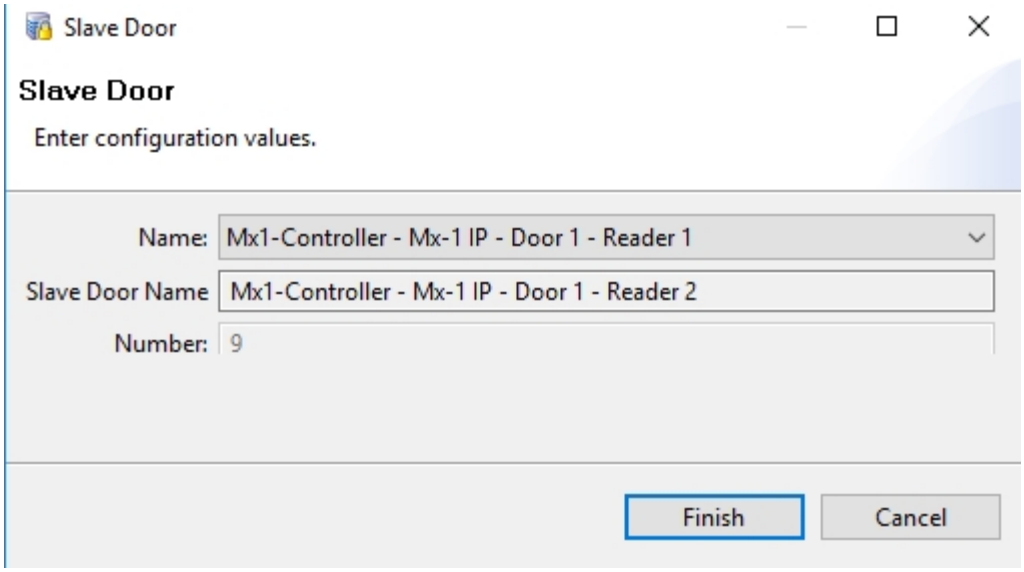
Adding an Exit Reader to an Existing Door

If a controller was created without an exit reader, you can add one later by right-clicking on the controller and selecting "New Slave Door".

(The functionality is the same as other Mx Controllers.)



The resulting dialog looks like this:



The door/reader Number is set to the required value of 9.

IT Rack Template for an Mx-8 Controller

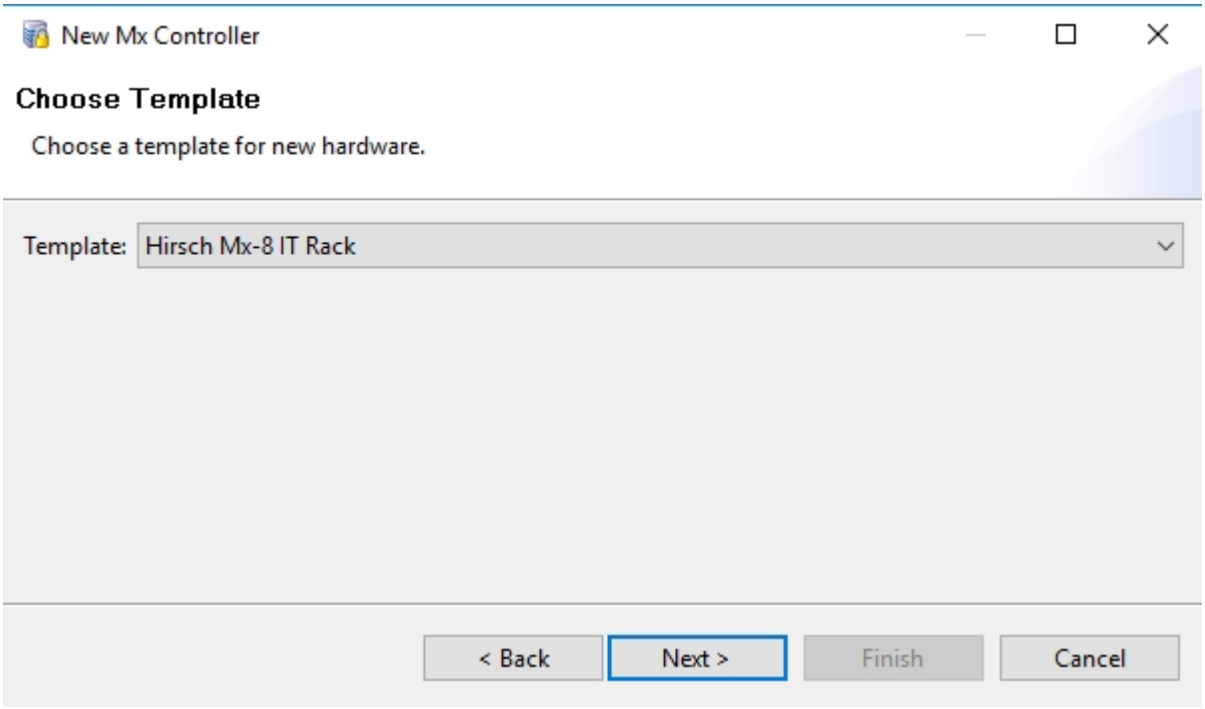
This template configures an Mx-8 controller as an IT Rack controller, for a data center needing access control to individual data racks.

Configuring an Mx-8 Controller as an IT Rack Controller

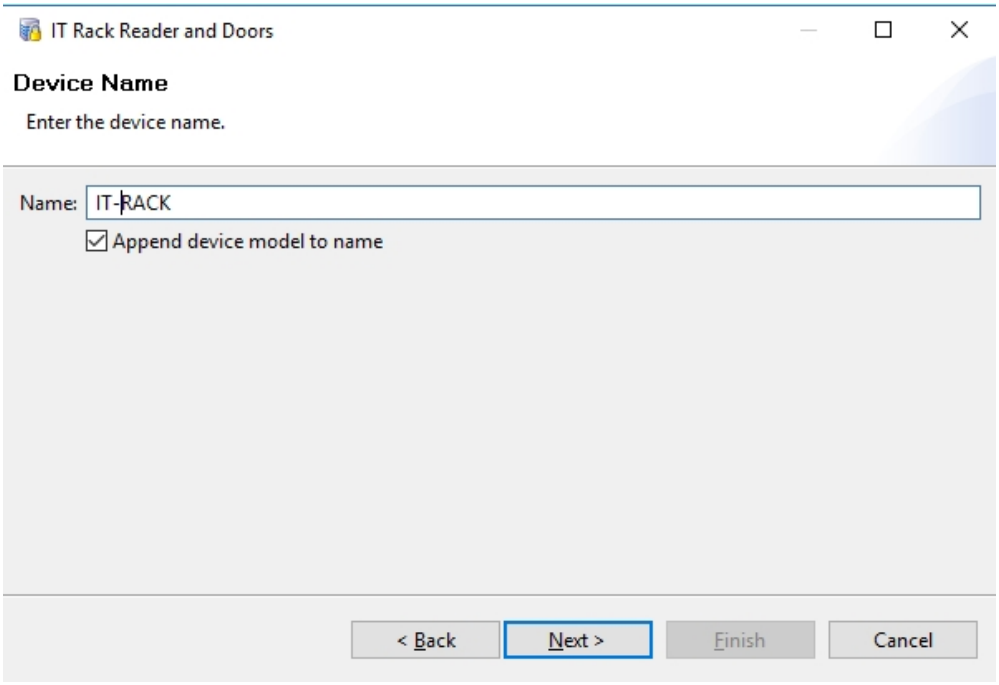
Step 1: Open the Hardware module.
Step 2: Right-click "Mx Driver" and select "New Mx Controller Wizard"

This will launch a Wizard for configuring a new Mx Controller.

Step 3: On the Choose Template page, select "Hirsch Mx-8 IT Rack" from the template drop-down list, and then click the Next button.

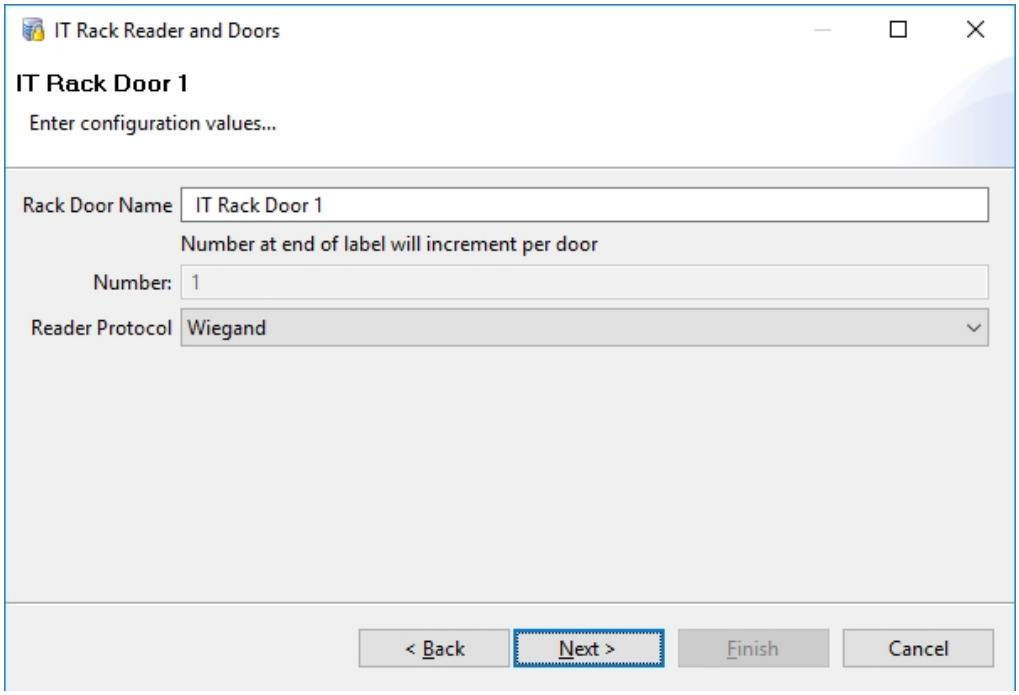


Step 4: Type a unique and descriptive name for the controller, and then click the Next button.



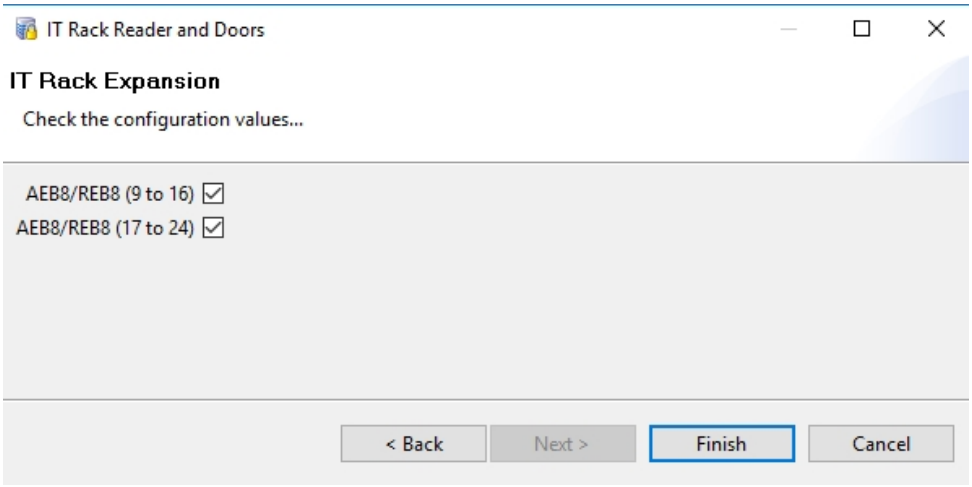
Step 5: On the resulting page:

- Decide on a naming convention (e.g. IT Rack HR Dept Door 1) and stick to it for all doors.
- Reader number is set to 1 and cannot be changed. (This number will incrementally increase by one for the other doors.)
- Adjust the Reader Protocol if necessary, then click the Next button.

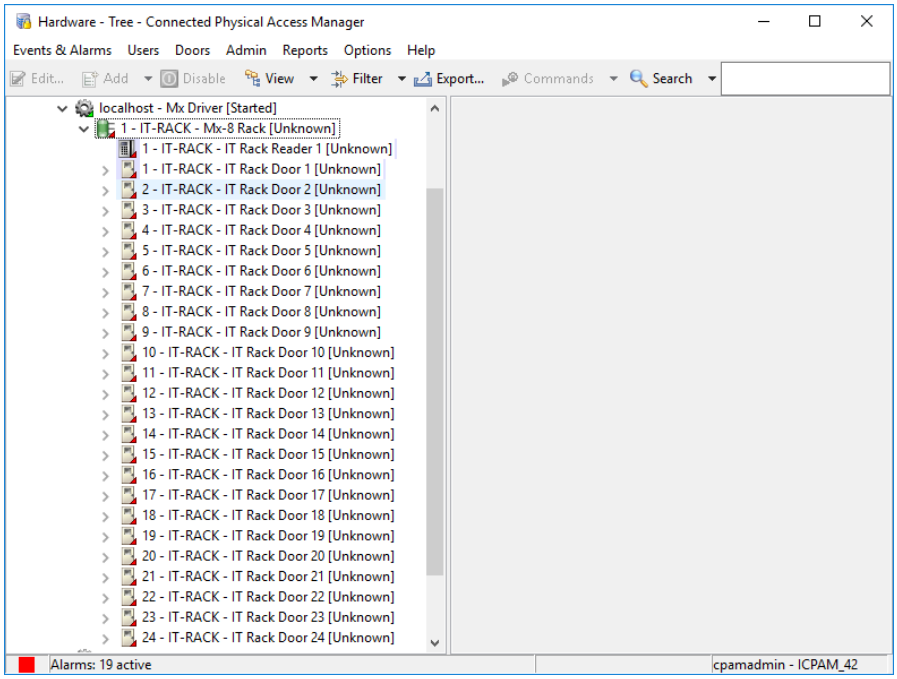


Step 6: On the resulting page:

- If you Mx-8 controller does not contain any Alarm or Relay Expansion boards, then click the Finish button.
- Otherwise, select the checkbox next to each Expansion board that is installed in the controller, then click on the Finish button.



The new IT Rack controller (with 24 doors in this example) now appears in the Hardware Tree.

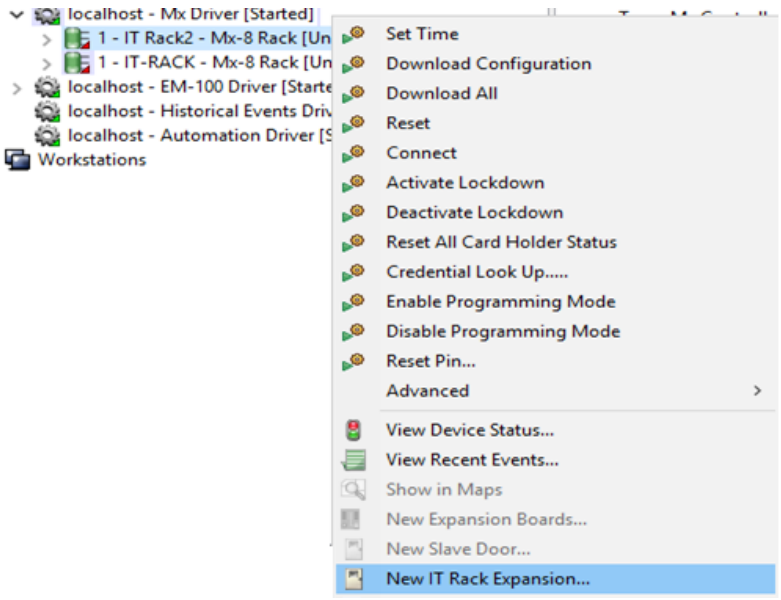


- It contains one reader which is common to all rack doors in a controller
- Each rack door contains an input and a relay

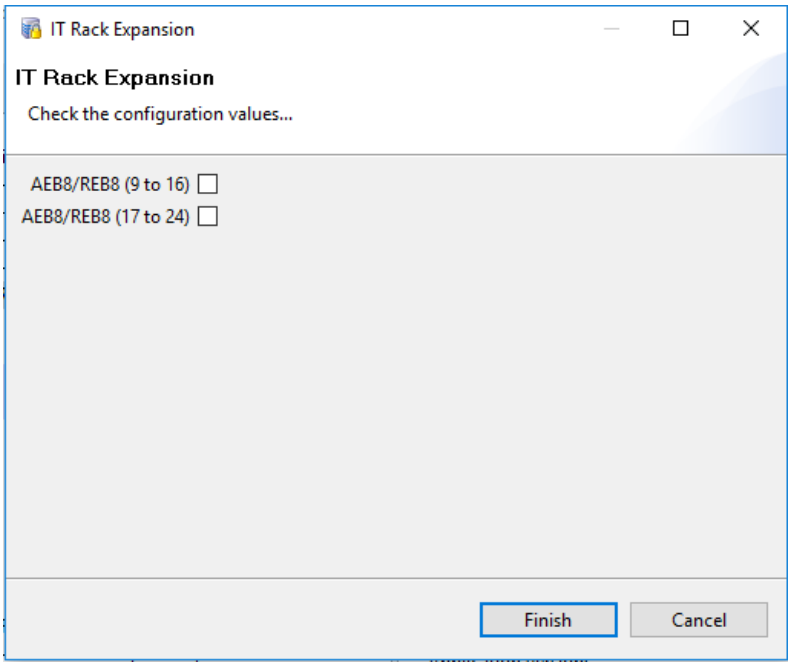
Adding Expansion Boards to an Existing Mx-8 IT Rack Controller

Any Mx-8 controller using the "IT Rack" template which was created with 8 doors, can be expanded later (up to 24 doors).

Right-click on the controller and select "New IT Rack Expansion".



On the resulting dialog, select the checkbox for each Expansion board that is installed in the controller, then click on the Finish button.



Lockdown support for Mx and EM-100 Controllers

In ICPAM 3.1, we are supporting the Lockdown feature for both Mx and EM-100 controllers. Lockdown is used in an emergency situation to grant access only to a few privileged users and to

restrict access to all the other users. This topic explains how to enable the Lockdown feature for both Mx and EM-100 controllers.

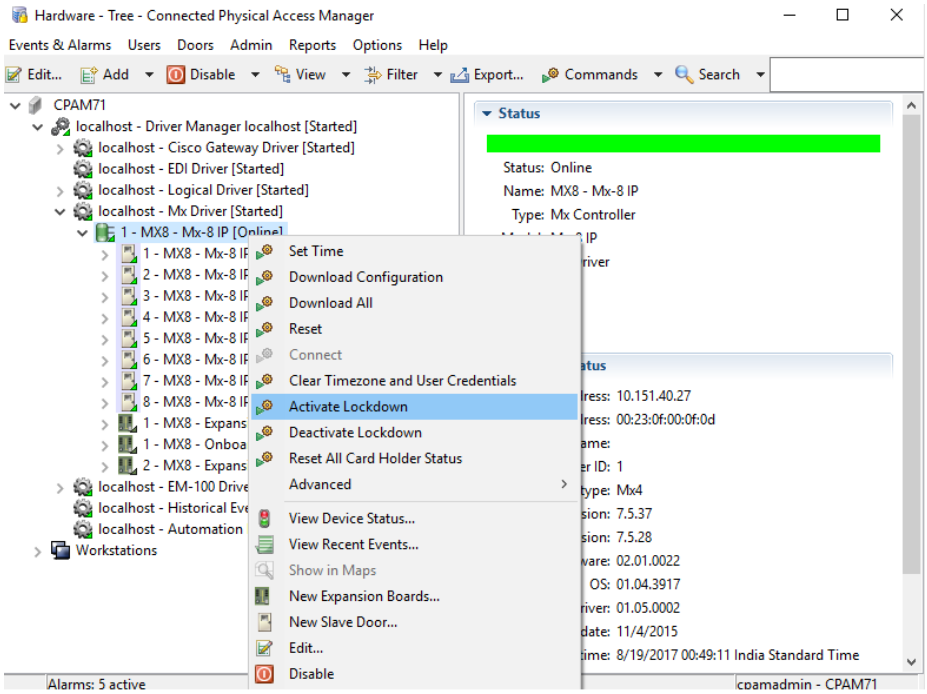
Lockdown on Mx Controllers

How it works on Mx Controllers

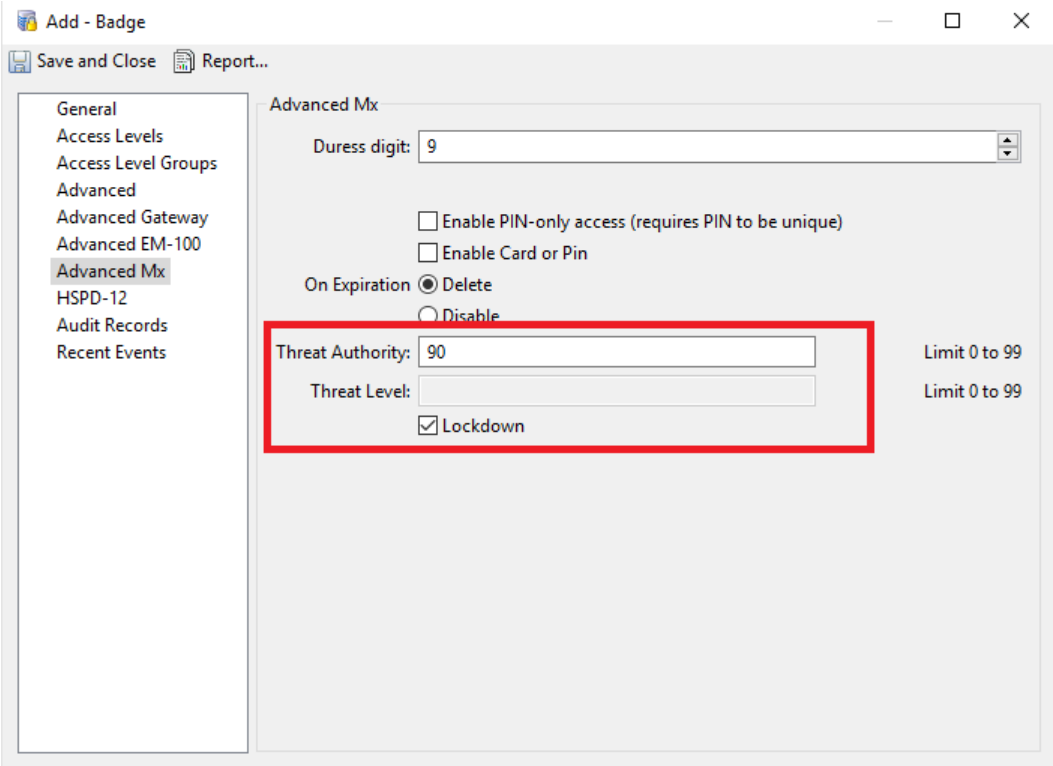
- Activate the lockdown mode by right-clicking on an Mx controller and selecting the "Activate Lockdown" command.
- By executing this command, the threat level is set to 90 on the controller.
- Select the Lockdown checkbox in the Badge module on the "Advanced Mx" page.
- By selecting the Lockdown option in the Badge module, threat authority 90 is set to the badge.
- During the credential download process, all the credentials will be pushed to the controller.
- During Lockdown mode, only Lockdown "enabled" badges will be granted access.
- To deactivate the Lockdown mode, right-click on the controller and select the "De-activate Lockdown" command.
- By executing this command, the threat level is set to 0 on the controller.
- After the Lockdown mode is deactivated, all the badges will again grant access according to their access policies.

Activating Lockdown mode

- Lockdown mode is triggered via a device command.
- To activate Lockdown mode, right-click on a controller and select the "Activate Lockdown" command.
  - Threat level 90 is set on the controller.



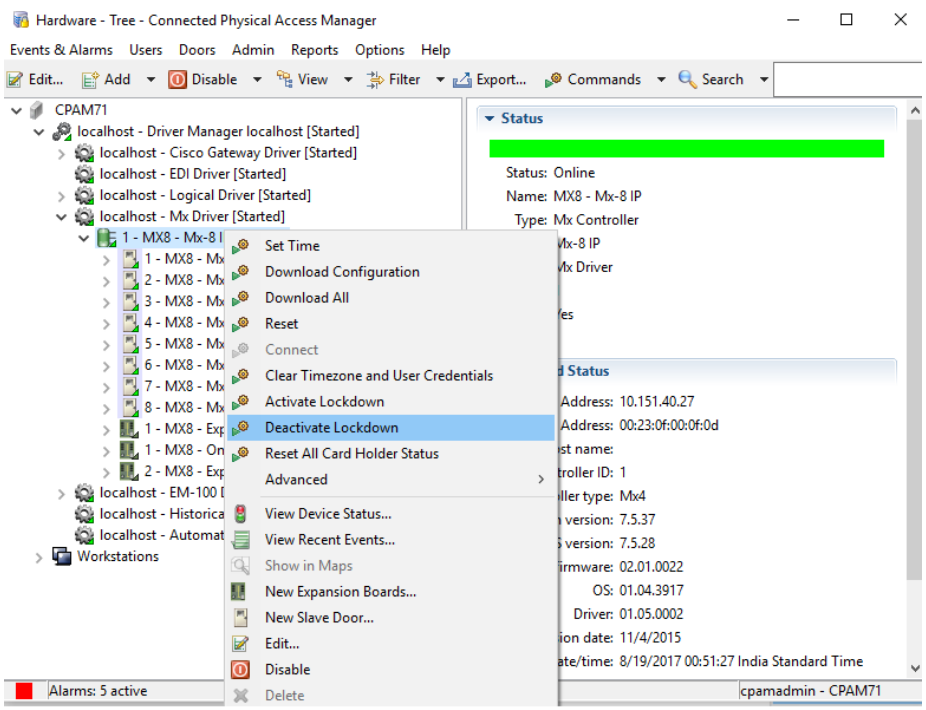
- To enable access for a badge during Lockdown mode:
  - In the Badge module, select the Lockdown checkbox on the Advanced Mx page.
  - Threat authority value 90 is set to the badge (so this badge can obtain access even during Lockdown mode).



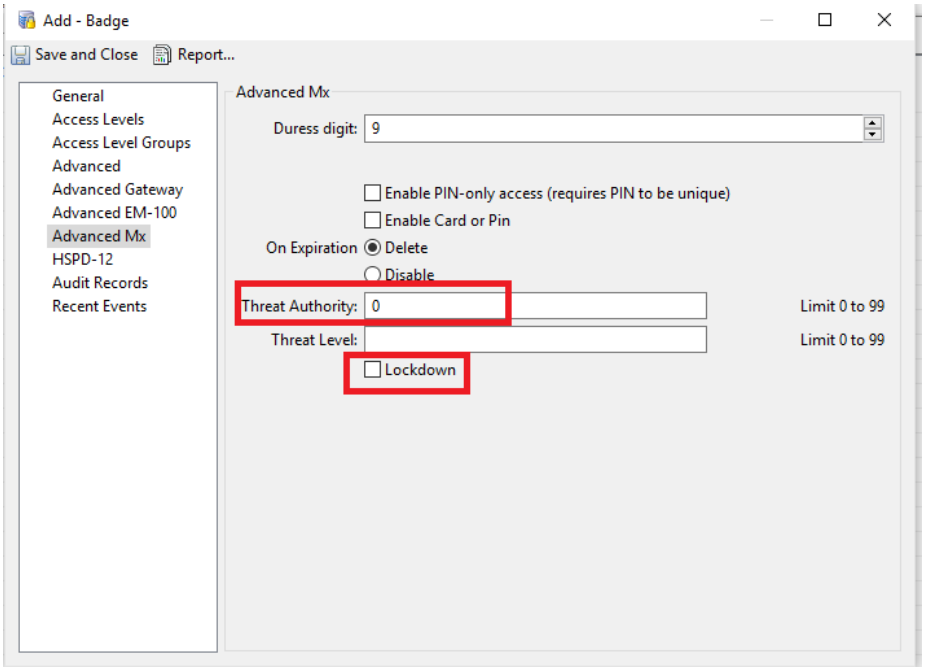
- During the Lockdown state, when a "Download All" command is executed, all the badges will be downloaded but only Lockdown-enabled badges with Threat Authority 90 (or greater) will be granted access to the controller's doors.

Deactivating Lockdown mode

- To deactivate Lockdown mode, right-click on a controller and select the "Deactivate Lockdown" command.
  - The default Threat level of 0 is set on the controller.
  - Now all the badges with threat authority 0 (or greater) can have access to the controller's doors.



- When the Lockdown option is unchecked (on the "Advanced Mx" page in the Badge module), the Threat Authority is automatically set to 0 (default value).



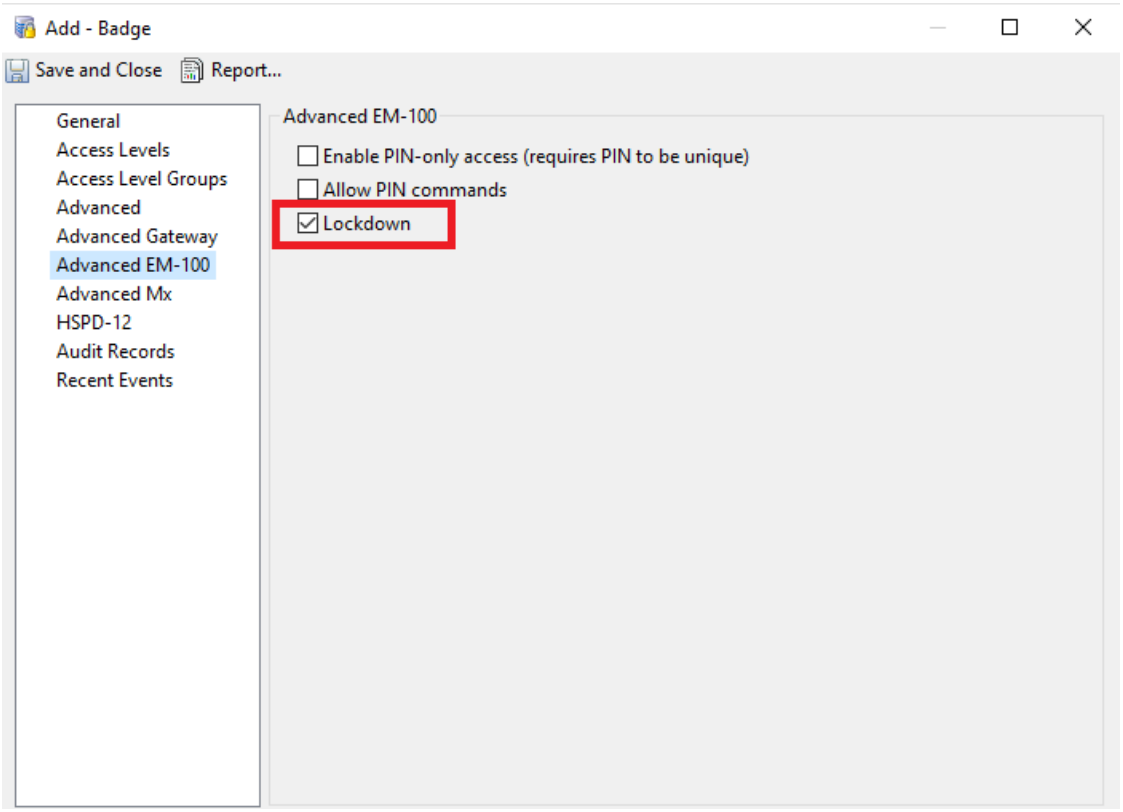
Lockdown on EM-100 controllers

How it works on EM-100 controllers

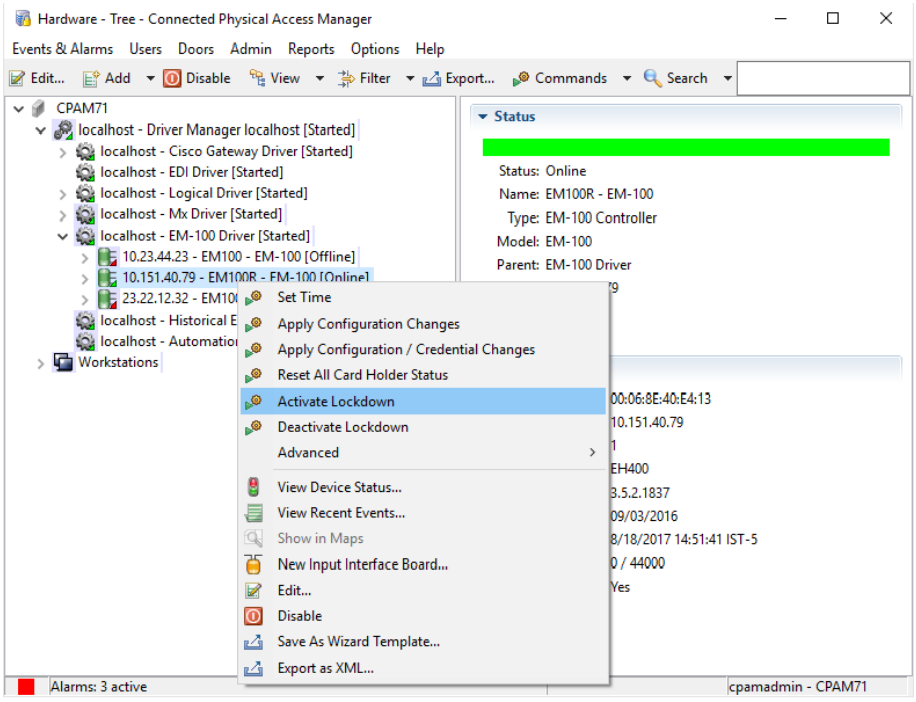
- Select the Lockdown checkbox in the Badge module on the "Advanced EM-100" page.
- To activate the Lockdown mode, right-click on the controller and select the "Activate Lockdown" command.
- By executing this command, only Lockdown field enabled badges will be downloaded to the controller.
- To deactivate the Lockdown mode, right-click on the controller and select the "De-activate Lockdown" command.
- By executing this command, all the badges wil be downloaded to the controller.

Activating Lockdown mode

- To enable access for a badge during Lockdown mode:
  - In the Badge module, select the Lockdown checkbox on the "Advanced EM-100" page.

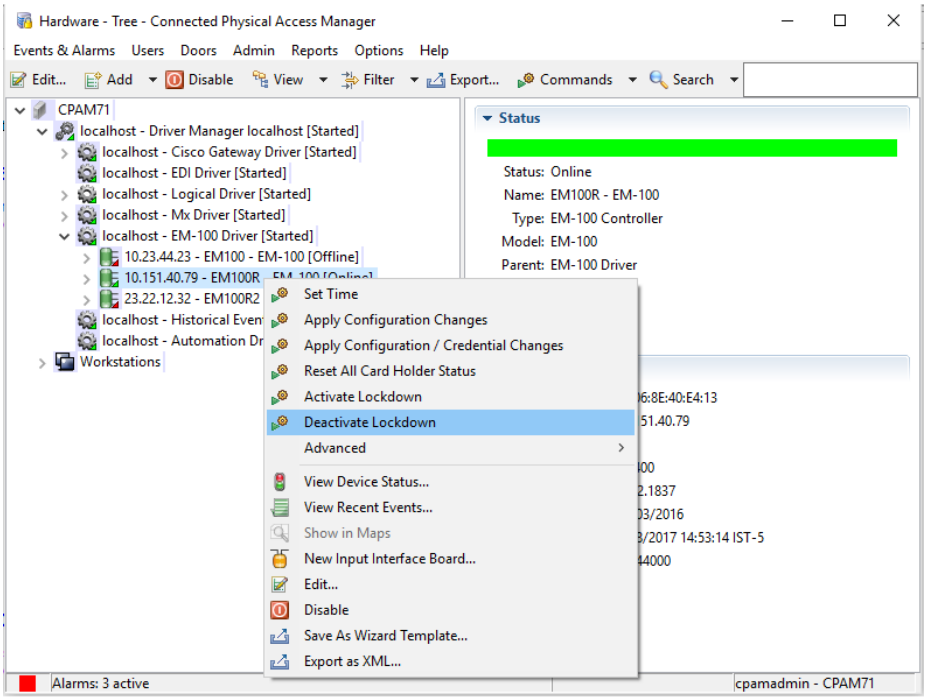


- To select Lockdown mode, right click on a controller and select the "Activate Lockdown" command.
  - Only Lockdown field enabled badges will be downloaded to the controller, limiting access to a few privileged users.



Deactivating Lockdown mode

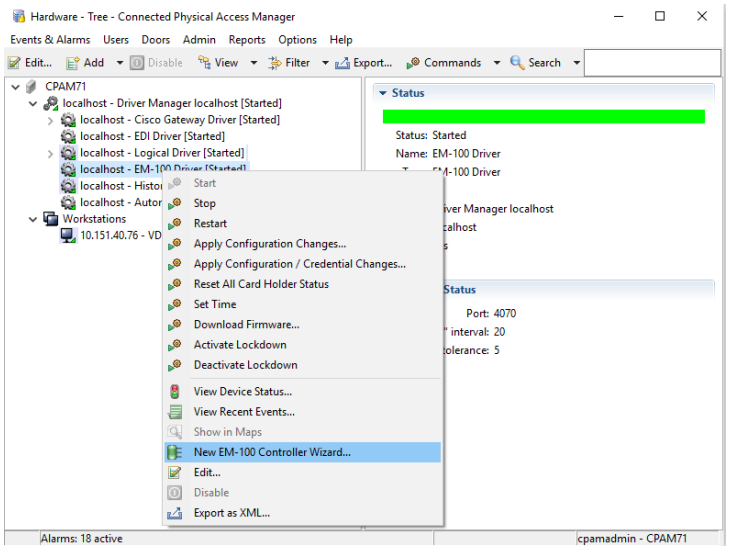
- To deactivate Lockdown mode, right-click on a controller and select the "Deactivate Lockdown" command. All the badges will be downloaded to the controller, restoring normal access for everyone.



EM-100 Input Module

In ICPAM 3.1, we support adding an input module for an EM-100 controller.

Step 1: In the Hardware Tree, right-click on the EM-100 driver and select the "New EM-100 Controller Wizard" command.

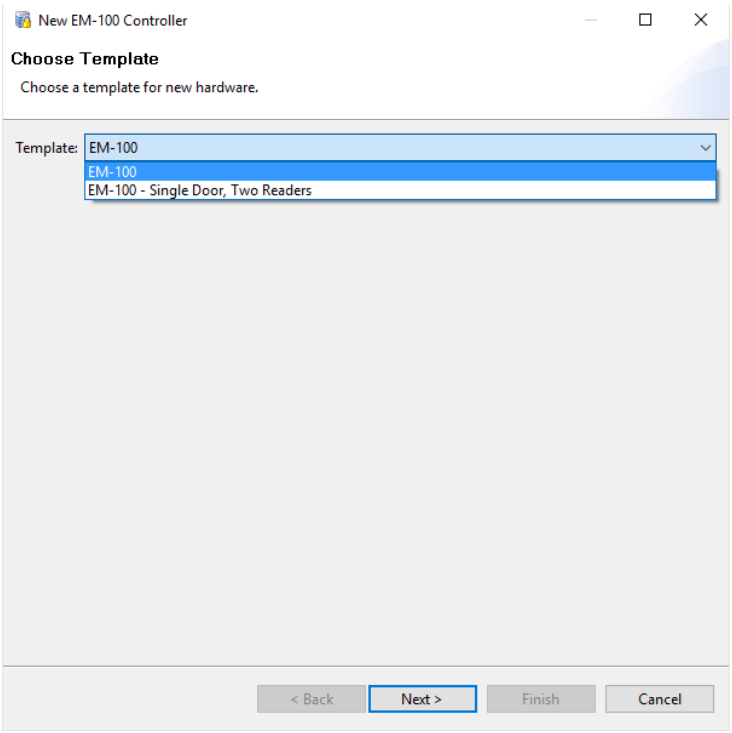


Step 2: On the resulting Choose Template page, either:

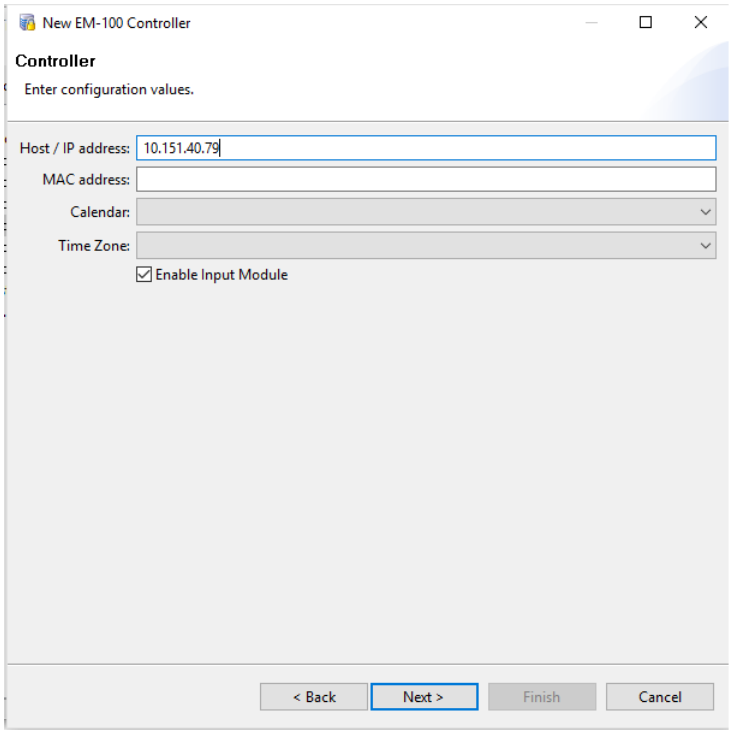
- Choose EM-100 for a standard "EM-100" controller with just an Entry reader.

Or:

- Choose "EM-100 – Single Door, Two Readers" for an enhanced EM-100 controller with an Exit reader Expansion Module.
- Click the Next button.

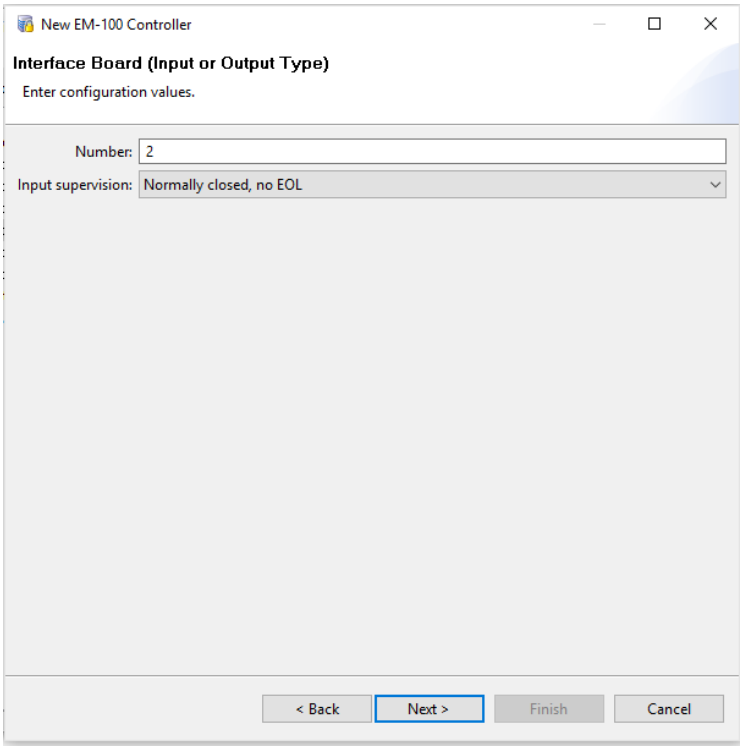


Step 3: On the resulting Controller page, select the "Enable Input Module" option to enable the EM-100 input module (and display the page where you can configure it).

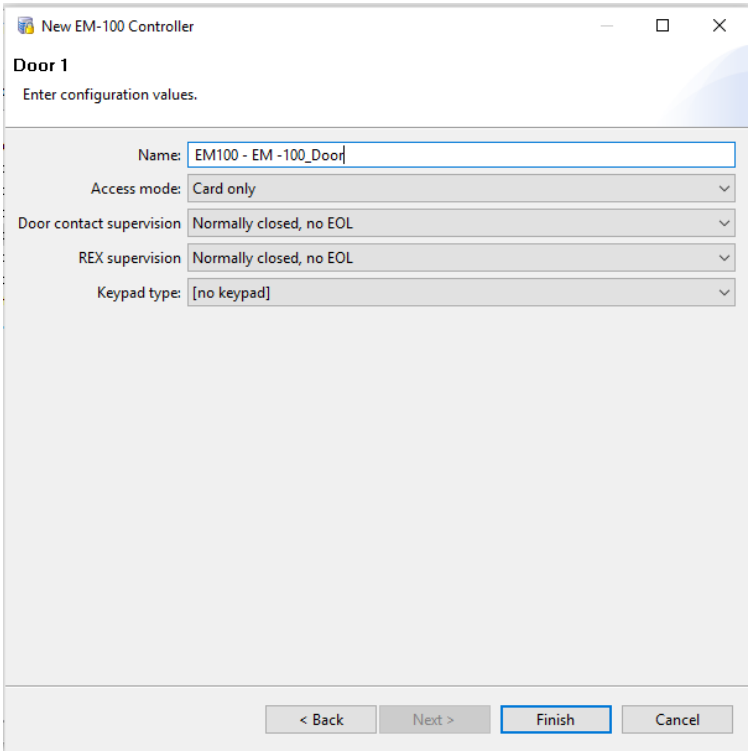


Step 4: On the resulting page:

- If necessary, select a different value from the Input supervision drop-down list.
- Click the Next button.



Step 5: On the resulting page, specify the appropriate door configuration values, and then click the Finish button. (For more information about the fields on this page, consult the ICPAM 3.1 User Guide under the section, "Adding an EM-100 Controller with an Exit Reader Expansion Module".)



After the EM-100 with input module has been created, it will appear in the Hardware Tree.