ICPAM 3.1 New Feature User Guide

November 2017



Contents

Introduction	3
Updating Mx Controller's CCM Firmware	3
Work Flow	3
Upload CCM Image to the ICPAM Server	3
Download CCM Image to the Mx Controller	4
Verifying the CCM Image	
Unified Credential Template	
Work Flow	6
Data Needed to Define a Credential Template	6
Credential Template Module UI	7
Predefined Credential Templates	7
Explicit Facility Code for the EM-100 Controller	12
Mx-1 Controller	
Adding a New Mx-1 Controller	13
Adding Expansion Boards to an Existing Controller	17
Adding an Exit Reader to an Existing Door	
IT Rack Template for an Mx-8 Controller	
Configuring an Mx-8 Controller as an IT Rack Controller	
Adding Expansion Boards to an Existing Mx-8 IT Rack Controller	
Lockdown support for Mx and EM-100 Controllers	
Lockdown on Mx Controllers	
How it works on Mx Controllers	
Activating Lockdown mode	
Deactivating Lockdown mode	
Lockdown on EM-100 controllers	
How it works on EM-100 controllers	
Activating Lockdown mode	
Deactivating Lockdown mode	
EM-100 Input Module	28



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

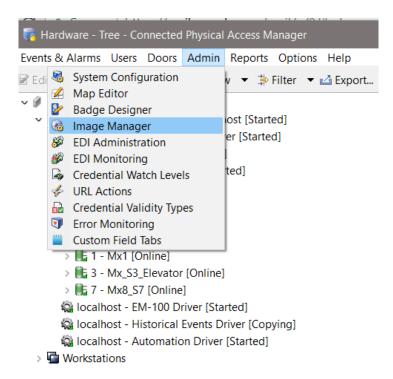
ICPAM 3.1 now supports Mx Controller Command & Control Module (CCM) firmware updates via the ICPAM software client. Updating the CCM firmware ensures optimal operating conditions and allows for support of the latest features in ICPAM. It is HIGHLY REOMMENDED to upload the latest version of CCM firmware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



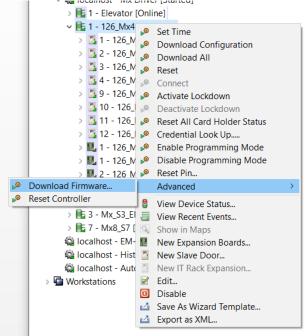
🛜 Image Manager - Conn	ected Physic	al Access Man	lager			-		\times
Events & Alarms Users D	oors Admi	n Reports (Options Hel	p				
TFTP server: 10.151.40.102	Default							
Local:				Remote:				
C:\ < C:\ccmupgradede	ev\ccmimag	es\ccm7_5_70_	_25ccm 🐼					1
Name	Size	Date		Name	Size	Date		
🗎 ccm7_5_70_12ccm	524288	Thu Jan 0						
📄 ccm7_5_70_23ccm	524288	Mon Oct						
ccm7_5_70_25ccm	524288	Wed Oct						
			Upload	Download				
Alarms: 68 active					c	pamadmin	- Test_102	2

• 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
 - o 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

Download Firn	nware		×
Image Type:		ССМ	
Image name:			Browse
TFTP server:	10.151.40.1	02	
Path:			
[ОК	Cancel	

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"

Download Firmware	Enabled: Yes				
Image Type: O SNIB O CC Image name:	Browse	151.40.5 23:0f:00:	-		
Path:	Image List				×
ОК	File Name ccm7_5_70_25ccm		Image Name CCM171011	Version 7.5.70(25)	
	ccm7_5_70_23ccm		CCM171009	7.5.70(23)	
	ccm7_5_70_26ccm		CCM171012	7.5.70(26)	
		OK	Cancel		
	version date. re	,			

- 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.

I - 126_Mx4M [Downloading Firmware]

- > 3 1 126_Mx4M Door 1 Reader 1 [Downloading Firmware]
- > 3 2 126_Mx4M Door 2 Reader 1 [Downloading Firmware]
- > 3 126_Mx4M Door 3 Reader 1 [Downloading Firmware]
- > 3 4 126_Mx4M Door 4 Reader 1 [Downloading Firmware]
- > 3 126_Mx4M Door 1 Reader 2 [Downloading Firmware]
- > 3 10 126_Mx4M Door 2 Reader 2 [Downloading Firmware]
- I1 126_Mx4M Door 3 Reader 2 [Downloading Firmware]
- 3 12 126_Mx4M Door 4 Reader 2 [Downloading Firmware]
- > III 1 126_Mx4M Expansion Inputs [Downloading Firmware]
- > 1 126_Mx4M Onboard Outputs [Downloading Firmware]
- J La 2 126_Mx4M Expansion Outputs [Downloading Firmware]



• 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".

Location:
✓ Extended Status
IP Address: 10.151.40.55
MAC Address: 00:23:0f:00:0c:8f
Host name:
Controller ID: 1
Controller type: DTM64_MSP
Application version: 7.5.70_26
CCM BIOS version: 7.5.66
SNIB3 firmware: 02.02.0011
OS: 01.04.3917
Driver: 01.05.0002

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
 - o Define reader properties for MX controllers
- Download the configuration to the controllers

Data Needed to Define a Credential Template

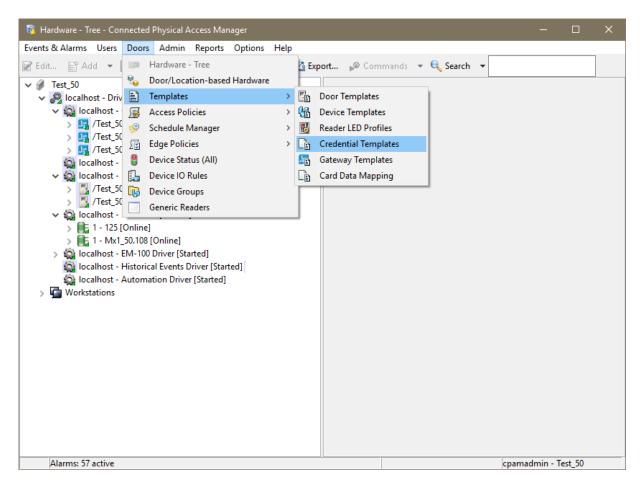
Before defining a credential template, the following data should be collected from the card vendor,

- 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



🐻 Cr	redential Templates - Conr	nected Physical Access N	Nanager	—	□ X
Events	s & Alarms Users Doors	s Admin Reports (Options Help		
🛃 Edi	it 📑 Add 🗶 Delete	📓 Report 🐙 Col	umns 🔍 Search 🔻		
N	lame	Primary Credential	Secondary Credential		
E 20	6BitWiegandCT	Standard Wiegand 26			
B 20	6BitWiegandKeypadCT	Standard Wiegand 26	Keypad		
Ē 31	7BitWiegandHID_H10302	Wiegand 37			
B 31	7BitWiegandHID_H10304	Wiegand 37 H10304			
Гр Н	HD_CORP_1000_35	Wiegand 35			
🔓 н	HD_CORP_1000_48	Wiegand 48			
Co K	leyPad_BCD4	KeyPad_BCD4			
			7 items	cpamadı	min - Test_50

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

• Total number of bits

o 26

- Total number of fields in the format (for example, facility code, badge number or company id)
 - o 2(Card ID, Facility code)
- Bit details for each field (start position, end position, etc,)
 - \circ 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
 - o Two parity bits,
 - bit position 0, Bit-Ranges 1-12, even parity
 - o 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:

🌇 Add - Credential Tem	plate			\times
🔚 Save and Close 📓 R	eport			
General Primary Data	General	26DimAGeneral		_
Secondary Data Custom		26BitWiegand Wiegand	 	~
		Fixed Keypad Magstripe Wiegand		
		Wiegand-Keypad		

Then select Primary Data tab

🌇 Add - Credential Ten	iplate	×
🔚 Save and Close 🗐 R	eport	
General	Primary Data	
Primary Data		
Secondary Data Custom	Name: Standard 26Bit	
Custom	Type: Wiegand Data	
	Length in bits: 26	
	Card ID Facility Site Other Parity Sentinel	
	Number of bits: 16	
	Encoding: Binary ~	
	Out bits: 0	
	Compliment data	
	Most significant bit order	
	Bit ranges	
	Edit Add Delete	
	Begin Bit End Bit	
	9 24	



General Primary Data Secondary Data Custom	Primary Data Name: Standard 2 Type: Wiegand D			Position: 0 Bit ranges Edit	Add Delete
	Length in bits: 26 Card ID Facility	5	Parity Sentinel	Begin Bit	End Bit
	Edit Add Delete Parity Type Position Bit Ranges			C R Bit Position	0K Cancel X
				Begin bit: 1 End bit: 12 OK	Cancel

General Primary Data Secondary Data Custom	Primary Data Name: Standard 26 Type: Wiegand Da			Position: 25 Bit ranges Edit	Add Delete
	Length in bits: 26 Card ID Facility		Parity Sentinel	Begin Bit	End Bit
	Edit Parity Type Even	Add Position 0	Delete Bit Ranges 1-12	OK	Cancel
				Begin bit: 13 End bit: 24	Cancel
				lmin - Test_50	



General Primary Data Secondary Data Custom	Primary Data Name: Standard Wiegand 26 Type: Wiegand Data Length in bits: 26					
	Card ID	Facility	Site	Other	Parity	Sentinel
		Edit	A	Add	Del	ete
	Parity	Туре	Pos	ition	Bit Rar	nges
	Even Odd			0	1-12 13-2	

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

n Add - Credential Tem	plate		×
Save and Close 📓 R	eport		
General Primary Data Secondary Data Custom	Secondary Data No data 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.

🔞 Add - Credential Ten	nplate		\times
🔚 Save and Close 📓 F	Report		
General Primary Data Secondary Data Custom	Custom Use Proprietary Facility Code Add, Delete 200 Image: Code Image: Cod		

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.

new Mx Control	ler	
Controller Enter configuration	on values	
Enter configuration		
Parent controller:		•
Panel address:	1	
IP address:	192.168.5.242	
MAC address:	00:23:0f:00:07:29	
IP port:	10001	
Subnet mask:	255.255.254.0	
Default gateway:	192.168.4.1	
Retry:	3	
Time Zone:		•
	Secure Connection	
	Discover Mx Information	
Mx info:	192.168.5.242 (Administration Building)	 Discover
	< <u>B</u> ack <u>N</u> ext > <u>F</u> inish	Cancel

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



🐻 New N	1x Controller					Х
Choose	Template					
Choose a	template for new hardwa	re.				
Template:	Hirsch Mx-1					~
		< Back	Next >	Finish	Cancel	

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

🐻 New	Mx Controller					×
Device	Name					
Enter th	e device name.					
News	Mx1-Controller					
	Append device model to n	ame				
		< Back	Next >	Finish	Cancel	

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.



🐻 New Mx Controller			×
Door 1			1
Enter configuration values	5		
			_
Name:	Mx1-Controller - Mx-1 IP - Door 1 - Reader 1	 	
Number:	1		
Access mode:	Card Only		\sim
Door contact supervision:	Normally Closed		~
	< Back Next > Finish	Cancel	

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.

new Mx Controller			\Box \times
Expansion Input/Output			
Check the configuration values			
AEB (1 to 8)	REB (1 to 8)		
AEB (9 to 16)	REB (9 to 16)		
AEB (17 to 24)	REB (17 to 24)		
AEB (25 to 32)	REB (25 to 32)		
	REB (33 to 40)		
	REB (41 to 48)		
	REB (49 to 56)		
	REB (57 to 64)		
	< Back Next > Finis	sh	Cancel



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.

V 🎇 localhost - Mx Driver [Started]	
I - Mx1-Controller - Mx-1 IP [Unknown]	1
> 🗾 1 - Mx1-Controller - Mx-1 IP - Door 1 - Reader 1 [Ui	ſ
> III 1 - Mx1-Controller - Onboard Inputs [Unknown]	A
> III 2 - Mx1-Controller - Expansion Inputs [Unknown]	
> III 1 - Mx1-Controller - Onboard Outputs [Unknown]	En
> 🌉 2 - Mx1-Controller - Expansion Outputs [Unknown]	Lo

Type: Mx Controller Model: Mx-1 IP Parent: Mx Driver Address: 1 inabled: Yes

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".

a 🎡 localhost - Mx Driver [Started]			Type: Mx
 Coalhost - Mx Driver [Started] 1 - Mx1-Controller - Mx-1 IP [Unk 1 - Mx1-Controller - Mx-1 IP - 1 - Mx1-Controller - Onboard 2 - Mx1-Controller - Expansion 1 - Mx1-Controller - Expansion 2 - Mx1-Controller - Expansion 2 - Mx1-Controller - Expansion 2 - Mx1-Controller - Expansion 3 - Controller - Expansion 3 - Controller - Expansion 3 - Controller - Expansion 4 - Mx1-Controller - Expansion 4 - Mx1-Controller - Expansion 5 - Mx1-Controller - Expansion 6 - Mx1-Controller - Expansion 6 - Mx1-Controller - Expansion 7 - Mx1-Controller - Expansion 8 - Mx1-Controller - Expansion 9 - Mx1-Controller - Expansion 9 - Mx1-Controller - Expansion 		Set Time Download Configuration Download All Reset Connect Activate Lockdown Deactivate Lockdown Reset All Card Holder Status Credential Look Up Enable Programming Mode Disable Programming Mode Reset Pin Advanced View Device Status View Recent Events	Type: Mx
		Show in Maps New Expansion Boards	
	P1.		9
	[M]		
		New IT Rack Expansion Edit	
	0	Disable	
		Save As Wizard Template	



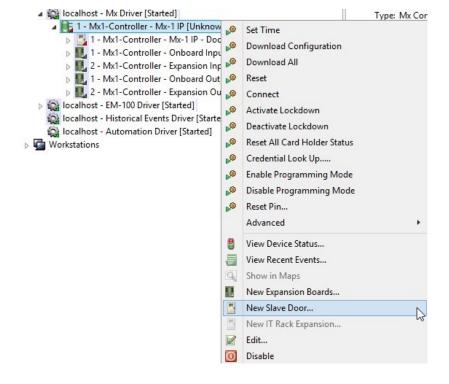
The resulting dialog looks like this:

🐻 Expansion Boards			×
Expansion Boards			
Check the configuration values			
AEB (1 to 8)	REB (1 to 8)		
AEB (9 to 16)	REB (9 to 16)		
AEB (17 to 24)	REB (17 to 24)		
AEB (25 to 32)	REB (25 to 32)		
	REB (33 to 40)		
	REB (41 to 48)		
	REB (49 to 56)		
	REB (57 to 64)		
	Finish	Canc	el

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:

🐻 Slave Door		_		\times
Slave Door				
Enter configuration	on values.			
Name:	Mx1-Controller - Mx-1 IP - Door 1 - Reader 1			~
Slave Door Name	Mx1-Controller - Mx-1 IP - Door 1 - Reader 2			
Number:	9			
	Finish		Cance	el

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.



🐻 New M	x Controller						×
Choose 7	Femplate						
Choose a	template for new hardwa	ire.					
Template:	Hirsch Mx-8 IT Rack						~
		< Back	Next >	Fini	sh	Cance	ł

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

IT Rack Reader and Doors			×
Device Name			
Enter the device name.			
Name: IT-RACK			
Append device model to name			
< <u>B</u> ack <u>N</u> ext >	<u>F</u> inish	Cance	el



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.

🐻 IT Rack Reade	r and Doors				-		×
IT Rack Door	1						
Enter configurati	on values						
Rack Door Name	IT Rack Door 1						
	Number at end of label	will increme	ent per door				
Number:	1						
Reader Protocol	Wiegand						\sim
		< <u>B</u> ack	<u>N</u> ext >	<u>F</u> inish		Cance	

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.



🐻 IT Rack Reader and Doors	· ·	C		×
IT Rack Expansion Check the configuration values				
AEB8/REB8 (9 to 16) 🗹 AEB8/REB8 (17 to 24) 🗹				
< Back Next > Finis	;h	C	Cancel	

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

n Hardware - Tree - Connected Physical Access Manager	- 0	×
vents & Alarms Users Doors Admin Reports Options Help		
	t @ Community - P County -	_
🖁 Edit 🖹 Add 🔻 🔟 Disable 🛯 View 🔻 🍰 Filter 💌 🛃 Expo	π 🔊 Commands 👻 🔍 Search 👻	
✓ Q localhost - Mx Driver [Started]		
I - IT-RACK - Mx-8 Rack [Unknown]		
1 - IT-RACK - IT Rack Reader 1 [Unknown]		
> 3 1 - IT-RACK - IT Rack Door 1 [Unknown]		
> 2 - IT-RACK - IT Rack Door 2 [Unknown]		
> 🗾 3 - IT-RACK - IT Rack Door 3 [Unknown]		
> 3 4 - IT-RACK - IT Rack Door 4 [Unknown]		
> 5 - IT-RACK - IT Rack Door 5 [Unknown]		
> 🛃 6 - IT-RACK - IT Rack Door 6 [Unknown]		
> 3 - IT-RACK - IT Rack Door 7 [Unknown]		
> 3 - IT-RACK - IT Rack Door 8 [Unknown]		
> 3 9 - IT-RACK - IT Rack Door 9 [Unknown]		
> 3 10 - IT-RACK - IT Rack Door 10 [Unknown]		
> 11 - IT-RACK - IT Rack Door 11 [Unknown]		
> 🛃 12 - IT-RACK - IT Rack Door 12 [Unknown]		
> 🛃 13 - IT-RACK - IT Rack Door 13 [Unknown]		
> 🛃 14 - IT-RACK - IT Rack Door 14 [Unknown]		
> 15 - IT-RACK - IT Rack Door 15 [Unknown]		
> 💁 16 - IT-RACK - IT Rack Door 16 [Unknown]		
> 🛃 17 - IT-RACK - IT Rack Door 17 [Unknown]		
> 🗾 18 - IT-RACK - IT Rack Door 18 [Unknown]		
> 19 - IT-RACK - IT Rack Door 19 [Unknown]		
> 🛃 20 - IT-RACK - IT Rack Door 20 [Unknown]		
> 🛃 21 - IT-RACK - IT Rack Door 21 [Unknown]		
> 22 - IT-RACK - IT Rack Door 22 [Unknown]		
> 23 - IT-RACK - IT Rack Door 23 [Unknown]		
> 🗾 24 - IT-RACK - IT Rack Door 24 [Unknown] 🗸		
Alarms: 19 active	cpamadmin - ICPAM_42	

- 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".



🗸 🔛 localhost - Mx Driver [Started] 🚽		II
> 1 - IT Rack2 - Mx-8 Rack [Un	>	Set Time
> 🕕 1 - IT-RACK - Mx-8 Rack [Un	\$	Download Configuration
> 🎡 localhost - EM-100 Driver [Starte	0	Download All
localhost - Historical Events Driv	0	Reset
- Automation Driver [3	0	Connect
workstations	0	Activate Lockdown
	-	
	\$	Deactivate Lockdown
	»	Reset All Card Holder Status
	\$	Credential Look Up
	\$	Enable Programming Mode
		Disable Programming Mode
		Reset Pin
	-	Advanced >
	8	View Device Status
		View Recent Events
	9	Show in Maps
		New Expansion Boards
	μ.	New Slave Door
	-	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.

	n IT Rack Expansion			×
	IT Rack Expansion			
	Check the configuration values			
i	AEB8/REB8 (9 to 16)			
	AEB8/REB8 (17 to 24)			
		Finish	Cance	I

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.

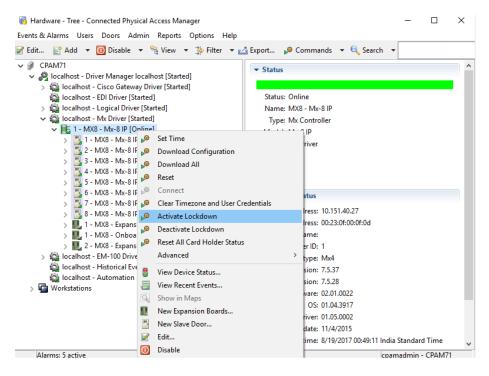
Lockdown on Mx Controllers

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).

🐻 Add - Badge				×
Save and Close Report				
General	Advanced Mx			
Access Levels Access Level Groups	Duress digit:	9		•
Advanced Advanced Gateway		Enable PIN-only access (requires PIN to be unique)		
Advanced EM-100		Enable Prive only access (requires Prive to be unique) Enable Card or Pin		
Advanced Mx HSPD-12	On Expiration			
Audit Records		O Disable		
Recent Events	Threat Authority:	90	Limit 0 to	o 99
	Threat Level:		Limit 0 to	o 99
		✓ Lockdown		

• 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.



🌇 Hardware - Tree - Connected Physical Access Manager

Events & Alarms Users Doors A	dmin Reports Options Help					
📝 Edit 📑 Add 🔻 🚺 Disable	💌 🐏 View 💌 🚔 Filter 💌 🖻	🐴 Export 💕	🛛 Commands 🔻 🔍 Search 👻			
CPAM71 Gradhost - Driver Manager Ag localhost - Cisco Gatew Gradhost - EDI Driver [S Goalhost - Logical Driv Glacalhost - Logical Driv Glacalhost - Mx Driver [S	vay Driver [Started] tarted] er [Started]		Online MX8 - Mx-8 IP Mx Controller			
 ↓ 1 - MX8 - MX-81 ↓ 1 - MX8 - MX ↓ 2 - MX8 - MX ↓ 3 - MX8 - MX 	 Download Configuration Download All 		Их-8 IP Их Driver les			
 4 - MX8 - MX + 5 - MX8 - MX + 6 - MX8 - MX + 7 - MX8 - MX + 	Connect Clear Timezone and User Creder	ntials	es 1 Status Address: 10.151.40.27			
 3 8 - MX8 - MX 3 1 - MX8 - Exp 3 1 - MX8 - Exp 3 1 - MX8 - On 3 2 - MX8 - Exp 4 - MX8 - Exp 4 - MX8 - Exp 5 - MX8 - Exp 	Deactivate Lockdown	>	Address: 00:23:0f:00:0f:0d st name: troller ID: 1			
View	View Recent Events Show in Maps		iller type: Mx4 version: 7.5.37 version: 7.5.28 irmware: 02.01.0022			
	New Slave Door Edit		OS: 01.04.3917 Driver: 01.05.0002 ion date: 11/4/2015 ate/time: 8/19/2017 00:51:27 India Standard Time			
Alarms: 5 active	Delete		cpamadmin - CPAM71			

– 🗆 ×

• 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).

🐻 Add - Badge			×	ł
🔡 Save and Close 📓 Report	t			ł
-	t Advanced Mx Duress digit: 9 Enable PIN-only access (requires PIN to be unique) Enable Card or Pin On Expiration Disable Threat Authority: Lockdown Lockdown	Limit 0	¢ 10 99	



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

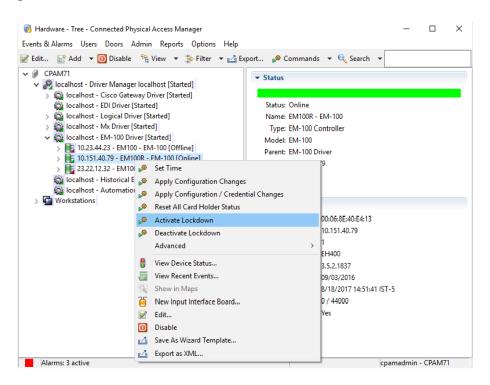
- To enable access for a badge during Lockdown mode:
 - In the Badge module, select the Lockdown checkbox on the "Advanced EM-100" page.

🐻 Add - Badge	-	-	\times
Save and Close Report General Access Levels Access Level Groups Advanced Advanced Gateway Advanced EM-100 Advanced Mx HSPD-12 Audit Records	Advanced EM-100 Enable PIN-only access (requires PIN to be unique) Allow PIN commands C Lockdown	-	×
Audit Records Recent Events			



• To select Lockdown mode, right click on a controller and select the "Activate Lockdown" command.

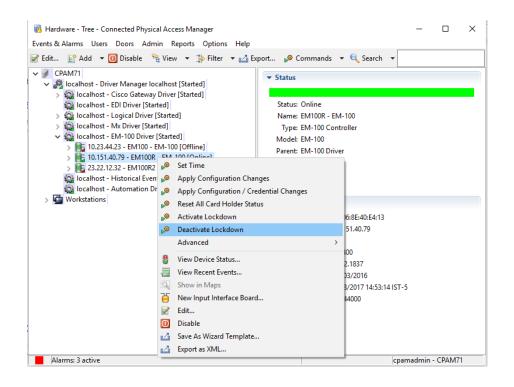
- Only Lockdown field enabled badges will be downloaded to the controller, limiting access to a few privileged users.



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.



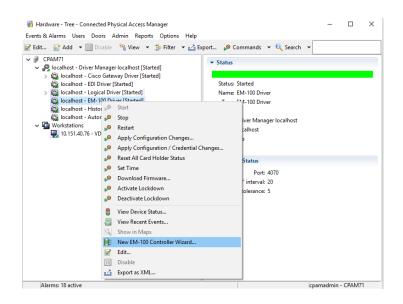


EM-100 Input Module

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.



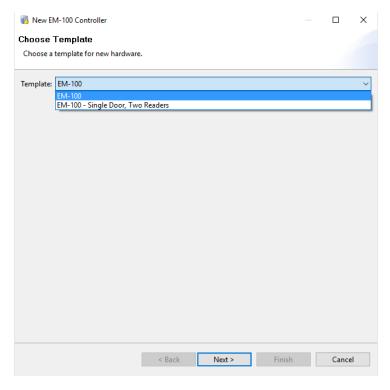


Step 2: On the resulting Choose Template page, either:

• 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).

🐻 New EM-100 C	ontroller					×
Controller						
Enter configuration	on values.					
Host / IP address:	10.151.40.79					
MAC address:						
Calendar:						\sim
Time Zone:						\sim
	🗹 Enable Input Mo	dule				
					-	
		< Back	Next >	Finish	Cance	

Step 4: On the resulting page:

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



🐻 New EM-100 C	ontroller				_		×
Interface Board Enter configuratio		out Type)					
Number:	2						
Input supervision:	Normally closed,	no EOL					~
		< Back	Next >	Finish		Cance	

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".)

🔞 New EM-100 Controlle	r			×
Door 1				
Enter configuration value	s.			
Nama	EM100 - EM -100_Door			
Access mode:				~
Door contact supervision				~
	Normally closed, no EOL			~
Keypad type:	•			~
Reypoortype:	[no keypool			-
	< Back Next > Fit	nish	Cancel	



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

Weiter Weiter Image: Constant of the second s	Hardware - Tree - Connected Physical Access Manager		_		×
CPAM71 Iocalhost - Driver Manager localhost [Started] Iocalhost - Cisco Gateway Driver [Started] Iocalhost - Logical Driver [Started] Iocalhost - Logical Driver [Started] Iocalhost - EM-100 Doror [Secure] Card Only] Iocalhost - EM-100 Doror [Secure] Card Only] Iocalhost - Bthrup - Generic Input 1 Armed Inactive] Iocalhost - EM100 - Integrated(EM-100EIM) [Online] Iocalhost - EM100 - IEM_2 - Generic Input 1 [Armed Inactive] Iocalhost - Historical Events Driver [Started] Ioc	Events & Alarms Users Doors Admin Reports Options Help				
 Jocalhost - Driver Manager Jocalhost [Started] Jocalhost - Cisco Gateway Driver [Started] Jocalhost - EDJ Driver [Started] Jocalhost - EM-100 Driver [Started] Jocalhost - EM-100 Driver [Started] Jocalhost - EM-100 - Integrated(EM-100) [Online] Jocalhost - EM-100 - Integrated(EM-100) [Online] Jocalhost - EM-100 - Tamper Switch [Armed Inactive] Jocalhost - EM100 - Integrated(EM-100EIM) [Online] Jocalhost - EM100 - Integrated(EM-100EIM) [Online] Jocalhost - Historical Events Driver [Started] Jocalhost - Automation Driver [Started] Jocalhost - Automati	📝 Edit 🖹 Add 🔻 🚺 Disable 🛯 View 🔻 🍰 Filter 🔻 🛃 Exp	ort 🎤 Commands 🔻 🔍 Search 🔻			
Alarme: 18 active	 Incalhost - Driver Manager localhost [Started] Iocalhost - Cisco Gateway Driver [Started] Iocalhost - EDI Driver [Started] Iocalhost - Logical Driver [Started] Iocalhost - EM-100 Driver [Started] Iocalhost - EM-100 Driver [Started] Iocalhost - EM-100 - EM-100 [Online] I - EM100 - Integrated(EM-100) [Online] I - EM100 - EM-100_Door [Secure Card Only] I - EM100 - Tamper Switch [Armed Inactive] S - EM100 - Nattery Monitor [Armed Active] S - EM100 - Output 2 [Off] I - EM100 - Integrated(EM-100EIM) [Online] I - EM100 - EIM_2 - Generic Input 1 [Armed Inactive] Z - EM100 - EIM_2 - Generic Input 2 [Armed Inactive] S - EM100 - EIM_2 - Generic Input 3 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] I - EM100 - EIM_2 - Generic Input 4 [Armed Inactive] 	Status: Online Name: EM100 - EM-100 Type: EM-100 Controller Model: EM-100 Parent: EM-100 Driver Address: 10.151.40.79 Enabled: Yes Location: Extended Status MAC address: 00:06:8E:40:E4:13 Host / IP address: 10.151.40.79 Controller ID: 3 Controller ID: 3 Controller type: EH400 Application version: 3.5.2.1837 Version date: 09/03/2016 Date/time: 10/10/2017 14:01:11 Cards loaded: 550 / 44000	IST-5		
	Alarms: 18 active	c	pamadmin	- CPAM71	1

