Identiv Connected Physical Access Manager (ICPAM) version 3.0.1(0.3.13) Release Notes

The Identiv Connected Physical Access Manager (ICPAM) version 3.0.1(0.3.13) software integrates with the Identiv EM-100 Controller, Mx-Controllers and Cisco Physical Access Gateways (CIAC-GW-K9).
This document contains important information about the ICPAM software version 3.0.1(0.3.13) released June 20, 2017, including an overview of release scope, policy and procedures, and exclusions and an explanation of resolved issues and caveats.

IMPORTANT INSTALLATION NOTES:

- After installing or upgrading to ICPAM v3.0.1(0.3.13), the Secure Network Interface Board (SNIB3) **MUST** have the firmware upgraded to version 2.01.0025 to maintain proper functionality with ICPAM.
- Once the SNIB firmware has been updated, the Mx panel requires a *FULL Factory* Reset, by pressing the Blue button above the 28V DC Power Supply connection
- In addition, after the firmware has been updated, all Mx Controllers need to have all data re-downloaded to ensure proper functionality.
- **If the number of credentials exceeds 2000 users with multiple access policies, ALL Mx Controllers will REQUIRE a memory expansion board. Please see Page 17 of the ICPAM Ordering Guide for more information.**

Table of Contents

Scope of Release - Features

Mx Controller URL Triggers
This release provides URL trigger support for Mx-4, Mx-8 and M64N. In addition, significant stability measures for the Mx series of controllers have been introduced, as well as more detailed access denied events to better identify the badge.

Upgrade Paths

This release is strongly recommended for all customers deploying Mx Controllers, EM-100 Controllers and/or Cisco Physical Access Gateways.

The following upgrade paths to ICPAM 3.0.1(0.3.13) supported:

- CPAM 1.5.3(0.3.6) to ICPAM 3.0.1(0.3.13)
- ICPAM 2.2.0(0.3.12) to ICPAM 3.0.1(0.3.13)
- ICPAM 2.2.0(0.3.12) + any 2.2.0 HOTFIX to ICPAM 3.0.1(0.3.13)
- ICPAM 3.0.0(0.3.12) to ICPAM 3.0.1(0.3.13)
- ICPAM 3.0.0(0.3.12) + any 3.0.0 HOTFIX to ICPAM 3.0.1(0.3.13)

Policies and Procedures

This section provides general policies and procedures regarding installation and service-related issues for this release.

Minimum System Requirements

Requirement	Description
Workstation software requirements	• Windows 7 or Windows 8 and Internet explorer versions 8-11. • 32 bit Java runtime environment 1.6 (release 27) or 1.7 (release 79) for both installation and normal use. • Auto-update of the Java runtime environment disabled • User account with administrative privileges.
Workstation hardware requirements	• Modern Intel or AMD multi-core processor. • 4GB RAM or more. • 250MB hard disk space available for the application.
Server hardware requirements	• ICPAM server includes at least 16GB of RAM memory, 4 virtual processors, and sufficient hard drive capacity to accommodate the database and software (500GB). Actual capacity needed will vary with event archival strategy, user count, controller count, event rates, etc.
ICPAM appliance software requirements	• CPAM 1.5.3(0.3.6) • ICPAM 2.2.0(0.3.8) • ICPAM 2.2.0(0.3.12) • ICPAM 3.0.0(0.3.12)
Physical access controllers and/or controller modules	• Identiv Mx Controllers: Mx-4, Mx8, and M64 controllers must contain SNIB-3 boards. ○ Firmware Release: 1.07 or 2.01.0011 is required on all Identiv Mx-4, Mx-8, and M64 controllers. These controllers will ship with SNIB-3 boards and v2.01.0011 firmware

	from the factory. • Identiv EM-100 Controllers: Firmware Release 3.5.2 or 3.6.0 is required on all Identiv EM-100 controllers. The EM-100 will ship with FW version 3.6.0 from the factory. • Cisco Physical Access Gateways: Firmware Release 1.5.3 is required on all physical access gateway modules. Some older physical access gateways may need an upgrade. To upgrade older firmware versions on physical access gateways to 1.5.3, see the Cisco Physical Access Gateway User Guide for instructions.

Implementation Notes

- General
    - Conditional Support for JRE 1.7 (release 79): The updated security settings in JRE 1.7 (release 79) may interfere with the normal functioning of the ICPAM client. The security settings in the Java control panel settings must be set to Medium: [Control panel -> Java (32-bit) -> Select **Medium** and select **OK**] to allow the installation of the ICPAM client. Users may face issues while performing functions with third party devices like badge printers or image capture devices. In such situations, Java runtime environment 1.6 (release 45) is recommended.
    - VMware: An ICPAM server runs as a Linux Virtual Appliance on VMware vSphere 5.x or 6.x (Other virtualization products, such as Oracle VirtualBox, Microsoft Hyper-V, Xen, etc. are not supported.)
    - The addition of module licenses to a server will require a restart of the controller driver via the Hardware Tree
- EM-100 Controllers
    - Two Door policies are not supported for EM-100 Doors
    - Each EM-100 controller is limited to being included in 8 access policies per credential (i.e. the same door and same credential can only appear in up to 8 redundant access policies)

- Mx Controllers
  - Non-door outputs for Mx controllers may only be actuated by global I/O
  - Only Wiegand and MATCH reader connectivity are supported initially
  - Master Mx controllers (connected via ethernet) must be address 1
- Cisco Gateway Controllers
  - Gateway doors are no longer added through the Locations/Doors module, only through the Logical Driver. Once doors are created, go to Locations/Doors and drag the unassigned doors into the relevant location, or alternatively, set the locations while adding doors or by editing the doors.

Exclusions

- VSM 6.x is not supported with ICPAM v2.1.0 or later; VSM 7.x will continue to be supported. Existing CPAM 1.5.x installations integrated with VSM 6.x will need to migrate to VSM 7.x before upgrading to ICPAM.

- JRE 1.8 is unsupported and is known to cause issues with Cisco VSM video playback in the ICPAM client and with the ICPAM map display.

Obtaining Software, Documentation and Related Information

Software Images and Other Tools

To access the self-service portal and obtain software, documents, and tools, do the following:

- Download ICPAM software:
  Go to the following URL: http://www.identiv.com/support-icpam
  Click the **Registration and Downloads** tab.
  Register user to enable access to software download link.

- Download Credential Template VFF files:
  Go to the following URL: http://www.identiv.com/icpam-credential-templates
  Select the applicable template zip files for your credential format.
  Click the link to download.

- ICPAM v3.0 User Guide and ICPAM v3.0 Installation Guide:
  Go to the following URL: http://www.identiv.com/support-icpam
  Click the ICPAM documents tab and select the guide.

Related Documentation

To obtain data sheets and other important information go to:

Identiv Connected Physical Access Manager documentation:

- For general product information: http://www.identiv.com/icpam
- For links to access Technical Data Sheets and product information: http://www.identiv.com/support-icpam

Support and Service Requests

To contact ICPAM support, go to the following link and submit your request via web http://www.identiv.com/support-icpam or contact us support_icpam@identiv.com

Enhancements & Resolved Issues

Enhancements & Resolved Issues

The following issue resolutions are included with ICPAM version 3.0.1(0.3.13).

Identifier	Title
ICPAM-823	Disabling Mx lock, door contact, or REX does not prevent usage at door
ICPAM-980	Mx controller using server time zone for evaluating schedules under some conditions
ICPAM-1079	When configuring an Mx controller for the first time, controller shows an Unlicensed state in the Hardware Tree
ICPAM-1108	Web Service API call getAllBadgesByPerson missing Access Policy data after upgrade
ICPAM-1114	8 access policy limit being hit due to no access policy filtering per controller
ICPAM-1124	Web Service API call enrollBadge fails to populate credential template in badge after upgrade to 2.2(0.3.12)

ICPAM-1129	Need to disable slave door configuration if Mx-4 or Mx-8 is configured as an elevator
ICPAM-1141	Unable to add expansion output boards during Mx controller creation
ICPAM-1157	EM-100 controller stops working if door is not associated with access policy
ICPAM-1172	Cisco licenses ignored after 3.0 hotfix
ICPAM-1179	Mx schedule driven door events not visible on setup
ICPAM-1205	Changed default setting for Mx Door Contact > Line Module to REX/door contact/tamper
ICPAM-1217	Mx input state events not visible on setup
ICPAM-1185	Database connections not freed under certain Mx Driver scenarios leading to connection starvation
ICPAM-1324	Badge numbers is now reported in access denied events if downloaded to the controller
ICPAM-1237	Changed default tamper times of reader to be more practical
ICPAM-1238	Mx door lockout time label should indicate "min" not "sec"
ICPAM-1247	Error if Mx Controller associated with more than 8 access policy
ICPAM-1248	Duplicate access zone ID created if a Mx door(s) of a controller are associated with more than one access policy for the controller
ICPAM-1249	Inactive badge pushed to Mx controller
ICPAM-1250	Bypass code conflict check is missing (If badge has duplicate PIN)
ICPAM-1265	Unable to create an Mx slave door when we have a controller that was created in 3.0.0(0.3.12)
ICPAM-1276	Mx controller fails during download where a badge has a card number is greater than 4,294,967,296 with valid access level
ICPAM-1278	Badge capacity in Extended Status not displaying correctly after memory board installation

ICPAM-1328	Unexpected log off from Mx controllers can interrupt very large credential downloads