Identiv Connected Physical Access Manager version 3.1.0(0.3.8) Release Notes

The Identiv Connected Physical Access Manager (ICPAM) version 3.1.0(0.3.8) software integrates with the Identiv EM-100 Controller. Together with the Identiv uTrust TS reader line, the ICPAM solution offers a complete premises access management system combining strong authentication with Identiv secure credentials at the door. The system includes support for legacy systems, enabling a mixed-environment of Mx-1, Mx-4, Mx8 controllers, EM-100 edge controllers and Cisco Physical Access Gateways (CIAC-GW-K9).

This document contains important information about ICPAM software version 3.1.0(0.3.8) released November 16, 2017, including an overview of release scope, policy and procedures, and exclusions and an explanation of resolved issues and caveats.

IMPORTANT INSTALLATION NOTES for deployments with Mx Controllers:

- ICPAM 3.0.1 and later requires SNIB3 firmware 2.01.0025 or later.
- Once the SNIB3 firmware has been updated, the Mx controller 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.
- Assigning two or more access policies to a credential for at least one of the doors in a specific Mx controller, or adding a start and/or end of validity to a credential consumes additional space in the controller. Capacity can be reduced to up to half of the maximum, in the most complex cases.

- If the capacity is exceeded, the Mx controller memory can be expanded by adding the appropriate Memory Expansion Board. Please see Page 17 of the ICPAM Ordering Guide for more information.
- After installing or upgrading to ICPAM v3.1.0(0.3.8), the Command and Control Module (CCM) **MUST** have the firmware upgraded to version 7.5.70.26 to maintain proper functionality with ICPAM.
- Please refer to the ICPAM 3.1 New Features Guide Page 3 for instructions on how to update the CCM firmware.

Table of Contents

Scope of ICPAM 3.1.0 - Features

This release adds:

- Support for Input Module for EM-100 PoE Network Controller
- Support for Hirsch Mx-1 PoE+ Network Controller
- Unified Credential Template
- High-Density Data Cabinet Solution
- Driver level Lockdown for Mx and EM-100 Controllers
- Mx CCM Firmware download via ICPAM Software

Upgrade Paths

The following upgrade paths to ICPAM v3.1.0(0.3.8) are supported:

- ICPAM 3.0.0(0.3.12) to ICPAM 3.1.0(0.3.8)
- ICPAM 3.0.0(0.3.12) + any 3.0.0 HOTFIX to ICPAM 3.1.0(0.3.8)
- ICPAM 3.0.1(0.3.13) to ICPAM 3.1.0(0.3.8)
- ICPAM 3.0.1(0.3.13) + any 3.0.1 HOTFIX to ICPAM 3.1.0(0.3.8)

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, 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	● ICPAM 3.0.0(0.3.12) ● ICPAM 3.0.0(0.3.12) hotfixes ● ICPAM 3.0.1(0.3.13) ● ICPAM 3.0.1(0.3.13) hotfixes
Physical access controllers and/or controller modules	● Identiv Mx Controllers: Mx-4, Mx8, and controllers must contain SNIB-3 boards. ○ Firmware Release: 2.01.0011 or later is required on all Identiv Mx-4 and Mx-8, controllers. These controllers will ship with SNIB-3 boards and v2.01.0011 firmware from the factory.

	● Identiv EM-100 Controllers: Firmware Release 3.5.1, 3.5.2 or 3.6.0 is required. ● 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.)

Unified Credential Templates

Unified Credential Templates are designed to simplify the way in which credential formats are specified in ICPAM. From ICPAM 3.1 and onward, the format only needs to be specified once in the client and there is no need for vff files or other mechanisms to define credential formats for Gateways, EM-100s, or Mx controllers.

Unified Credential Templates will be created during the upgrade process and associated with the credentials previously associated with the Virtual Credential Template being converted.

It is important to understand the conversion process so that your existing Virtual Credential Templates are complete enough for an accurate conversion.

For Virtual Credential Templates, the following are the possible combinations and the source material used for the conversion in each scenario:

Source Virtual Credential Template	**Preferred Source Template**
Gateway credential template only	Gateway cred template. Format will be propagated to EM-100 and Mx cred templates. * **
Mx credential template only	Mx cred template. Format will be propagated to GW and EM-100 cred templates. ***
EM-100 credential template only	EM-100 cred template. Format will be propagated to GW and Mx cred templates.
Gateway and EM-100 credential template	Gateway cred template Format will override EM-100 and be propagated to an Mx cred template. * **

EM-100 and Mx credential template	EM-100 cred template Format will override Mx cred template and be propagated to a Gateway cred template.
Gateway and Mx credential template	Gateway cred template Format will override the Mx cred template and be propagated to an EM-100 cred template. * **
Gateway, EM-100, and Mx credential template	Gateway cred template Format will override the Mx cred template and EM-100 cred template. * **

* Note: Some customers have received custom Mx card format patches in the past. Though this will no longer be required, it is important to ensure that you manually create a Gateway Credential Template for each custom Mx Credential Template you have inuse to ensure the upgrade process understands the format.

** Note: It has often been found in customer deployments that Gateway Credential Templates have been defined to ignore card parity information. The Mx controller requires the parity definition to be completed. If Mx controllers have been deployed or are planned to be deployed, existing Gateway Credential Templates that are missing parity information will need to be modified to include the parity information. Please note that this may require contacting your card supplier for parity details.

*** Note: If the Mx credential template is the only source, only 26 bit, 35 bit Corp 1000, 37 bit Open, and 37 bit Managed will be converted.

Exclusions

- 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 obtain software, documents, and tools, do the following:

- Download ICPAM software:
  Go to the following URL: https://support.identiv.com/icpam/
  Click **Software Request**.
  Register user to enable access to software download link.

  Registered Partners can access the Cisco Partner Portal and go to the ICPAM Software Downloads page.

- ICPAM 3.1 New Features Guide, ICPAM v3.0.1 User Guide and ICPAM v3.0 Installation Guide: Go to the following URL:
  https://support.identiv.com/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 https://support.identiv.com/icpam/ or contact us support_icpam@identiv.com

EM-100 Installation Notice

When applying any *hardware* changes to EM-100 network controllers, a FULL reboot is required to have the change apply and maintain complete functionality.

New Features

New Features in ICPAM 3.1.0(0.3.8)

The following features are included with ICPAM version 3.1.0(0.3.8).

Identifier	Title
ICPAM-71	Unify Credential Template - Dynamic generation of EM-100 vff's from common credential template format
ICPAM-224	EM-100: Input Expansion Module support for EM-100 PoE Controller
ICPAM-366	EM-100: Bulk and location based EM-100 controller Firmware Upgrades
ICPAM-530	VMWARE Tools in ICPAM OVA & BIN
ICPAM-536	EM-100: Lockdown with privileged badges allowed
ICPAM-643	EM-100: Driver allows Credential Lookup via Right Click
ICPAM-678	Add additional Cisco Gateway credential templates: HID Corp 1000 48bit, 35D/HID Corp 1000 35bit, 37D/H10302
ICPAM-1048	EM-100: Support Triggering the AUX EM-100 output with anyone of the Input Module inputs (excluding tamper)
ICPAM-1049	EM-100: Allow user to choose the typing for any of the 4 inputs on the Input Module
ICPAM-1110	Dynamic specification of Mx match code and EM-100 vff from common credential template format
ICPAM-1132	Mx: Lockdown with privileged badges allowed
ICPAM-1134	Mx: CCM Firmware delivery and download capability through ICPAM
ICPAM-1136	EM-100: Add additional EM-100 credential templates: 26D/H10301 HID 26bit, HID Corp 1000 48bit, 35D/HID Corp 1000 35bit, 37D/H10302
ICPAM-1231	EM-100: Allow adding an Input Module via the Hardware tree to an existing controller

ICPAM-1298	Mx: Data Center Rack Solution for Mx
ICPAM-1347	MX: Add support for Hirsch Mx-1 PoE+ Controller
ICPAM-1366	MX: Raise an alarm when we exceed the capacity of the controller upon download
ICPAM-1403	EM-100: Driver level lockdown and lift lift lockdown support
ICPAM-1422	Reset all configurations and credentials using commands

Resolved Issues and Caveats

Caveats

Resolutions for these issues are currently being investigated and will be scheduled for a future release unless specified:

Identifier	Title
CSCuv50557	Advanced Gateway options not seen in single screen badge wizard.
CSCuo83272	CPAM MySQL bin files occupying the entire space when Standby is absent.
CSCul35210	CPAM Client does respond when viewing Sanity Report, “Badges - Added (or changed) since the most recent download”.
CSCul62691	CreateTEC API allows pushing to parallel location objects for a profileUser.
ICPAM-98	In Access Level, Cisco doors don't disappear from left when moved to right col
ICPAM-120	Enable missing from Access Policies right-click / context menu on a disabled Access Policy. Work around: Edit access policy and check enabled. Web Admin
ICPAM-162	Badge Add / Edit UI control is localizing to Access Levels and Access Level Groups. Should be "Access Policies" and "Access Policy Groups".

ICPAM-233	Client allows attempted downloading of more than the limit of 8 Access Policies to a single EM-100 and prevents download completion. Workaround: do not exceed limit of 8 Access Policies
ICPAM-262	HA – Shared IP goes to standby mode
ICPAM-268	CSCuv50557: Advanced options not seen in single screen badge wizard
ICPAM-356	EM-100 controller may go offline on rare occasions when left disconnected from ICPAM server for long periods. Work around: Connect to problem controller's web console, Click Basic Settings menu item, without changing any settings, click Save, click Submit. Controller should come online and should remain so.
ICPAM-396	GUI: Command and Monitoring Tabs do not work in some browsers Workaround: Use MS IE and add ICPAM server URL to compatibility list.
ICPAM-400	Door/Location - Door/location module allows the same entry by assigning location manually
ICPAM-437	A badge that is attached to an expired access policy is granted access
ICPAM-443	Running a report with customized Variable Parameters throws an error
ICPAM-482	Location info is not inherited to the door upon selecting the checkbox "Inherit location from parent"
ICPAM-484	All Doors report does not display status for EM doors
ICPAM-491	Backup version x allows restore to ICPAM version y and corrupts installation
ICPAM-495	Duplicate card caused by cred # + format and then raw form entered
ICPAM-596	Virtual Credential Template Add/Edit dialogue has incorrect label. Refers to "Badge Format"
ICPAM-598	AdModCardRecord fails with -1001 Duplicate unique ID when no card DB has ever been downloaded to a previously used EM-100

ICPAM-826	Authenticate Credentials on Gateways
ICPAM-881	Cannot support more than 7 levels of locations for Cisco VSM cameras
ICPAM-1497	After CCM upgrade on a slave controller, the master controller needs to be reconnected to bring that slave controller online, or Mx-Driver restart required
ICPAM-1537	While download all at the Mx driver level in a master / slave setup, the slaves do not start download until master is completed but throws an event stating that the download failed for slave(s)

Resolved Issues

The following issue resolutions are included with ICPAM version 3.1.0(0.3.8).

Identifier	Title
ICPAM-123	Heap dumps are currently dumped to an inappropriately size constrained mysql folder in the server
ICPAM-383	EM-100 Saving wizard fails with client error
ICPAM-405	Authenticate badge on EM-100
ICPAM-646	Leverage Cisco schedule across Mx and EM-100 controllers
ICPAM-816	No message for download completion for Download Configuration and Download All commands
ICPAM-911	Integrate badge expiration with MX after CCM change.
ICPAM-1106	CSCuw86208 Unable to create /db/cpamadmin-heap.hprof: Permission Denied
ICPAM-1234	Creating a URL Action via Doors>Edge Policy>Add, allows creating a URL Action with no Condition
ICPAM-1296	Controller loses credentials in database cleanup after large number of credentials downloaded
ICPAM-1332	Trigger alarm for breach of max of 100 (or new max) access policies per badge for a gateway during cred download

ICPAM-1445	Fix Mx Discovery on Subnet Broadcasting
ICPAM-1464	Door held open is not working if access policy is created using device group
ICPAM-1479	Add Credential Template UI Issue while save and close
ICPAM-1480	Connection leak Issue in getAllBadgeTypeIds and getBadgeByCardNum API
ICPAM-1482	NullPointerException thrown while adding credential template if facility code definition found with no facility code in custom tab