



Identiv Connected Physical Access Manager Version 3.2.0(0.3.4) Release Notes

The Identiv Connected Physical Access Manager (ICPAM) version 3.2.0 (0.3.4) software integrates with the Identiv EM-100, Mx-1, Mx-4, Mx-8 Controllers. 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 3.2.0(0.3.4) released April 6th, 2018 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.
- **If upgrading from ICPAM 3.0.1(0.3.8) to ICPAM v3.2.0(0.3.4), 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.*
 - *The latest version of CCM Firmware can be found in the [Cisco Partner Portal](#) under **ICPAM Downloads***

Table of Contents

[Identiv Connected Physical Access Manager version 3.2.0\(0.3.4\)Release Notes](#)

[Upgrade Paths](#)

[Policies and Procedures](#)

[Minimum System Requirements](#)

[Implementation Notes](#)

[Exclusions](#)

[Obtaining Software, Documentation and Related Information](#)

[Software Images and Other Tools](#)

[Related Documentation](#)

[Support and Service Requests](#)

[EM-100 Installation Notice](#)

[Resolved Issues](#)

[Resolved Issues](#)

Upgrade Paths

The following upgrade paths to ICPAM v3.2.0(0.3.4) are supported:

- ICPAM 3.0.1(0.3.13) to ICPAM 3.2.0(0.3.4)
- ICPAM 3.0.1(0.3.13) + 3.0.1 HOTFIX to ICPAM 3.2.0(0.3.4)
- ICPAM 3.1.0(0.3.8) to ICPAM 3.2.0(0.3.4)

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	<ul style="list-style-type: none"> ● 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 must be disabled. ● User account with administrative privileges.
Workstation hardware requirements	<ul style="list-style-type: none"> ● Modern Intel or AMD multi-core processor. ● 4GB RAM or more. ● 250MB hard disk space available for the application.
Server hardware requirements	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● ICPAM 3.0.1(0.3.13) ● ICPAM 3.1.0(0.3.8)
Cisco VSM (If Applicable)	<ul style="list-style-type: none"> ● VSM 7.x Only (up to VSM 7.9)
Physical access controllers and/or controller modules	<ul style="list-style-type: none"> ● Identiv Mx Controllers: Mx-1, Mx-4, Mx-8. Mx-4 and Mx-8 controllers must contain SNIB-3 boards. <ul style="list-style-type: none"> ○ SNIB-3 Firmware Release: 2.01.0025 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. To upgrade older firmware versions on Mx Controllers, see the SNIB FW Update Walkthrough for instructions. ● CCMx Firmware version 7.5.61 or later. To upgrade older CCM firmware versions, see Page 3 of the ICPAM 3.1 New Feature User Guide for instructions. ● Identiv EM-100 Controllers: Firmware Release 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

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.)

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 v3.1 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.

Resolved Issues

Resolved Issues

The following issue resolutions are included with ICPAM version 3.2.0(0.3.4).

Identifier	Title
CIS-4	Review why EM-100 holidays always have time ranges of 00:00-23:59
CIS-5	Fix the issue when getAllAcDevices API call returns 0 devices
CIS-7	API assignScheduleToDoor changes the in-schedule and out-of-schedule door mode
CIS-8	API getAllAcDevices does not return any devices regardless of the filter passed
CIS-9	HereIAm tolerance has no effect regarding network latency
CIS-10	API applyScheduleToDoor only applies to GW.DOORs and fails for HV.DOOR and HH.DOOR devices

CIS-12	Resolved an issue that returns EM-100 License error in UI - Unlicensed
CIS-16	Improve stability of HA
CIS-17	Resolve the issue when API needs an endpoint to determine the schedule assigned for door mode
CIS-18	Include completed EM-100 per-controller credential download DB connection efficiency fix
CIS-23	Support same MAC/serial lookup behavior in EM-100's as is exhibited with Gateways
CIS-26	ICPAM Web API EnrollBadge and EnrollPerson not saving custom user fields
CIS-56	Badges fail to download to MX panel in specific instances
CIS-63	Badges changes during controller offline mode are not downloaded when comes back online
CIS-66	Add Door status support for MX Controller Doors
CIS-71	Resolve an issue on Unified Credential Template when updating ICPAM version with particular information fields missing data