Identiv CPAM to ICPAM Migration
Frequently Asked Questions (FAQ)

Document Scope:

This document provides basic answers to frequently asked questions and/or provides guidance when addressing customer inquiries regarding a CPAM to ICPAM upgrade and product migration.

Table of Contents

General Information on CPAM and ICPAM Migration

How will my existing investment with CPAM hardware and software be protected?

Cisco has partnered with Identiv to protect your investment by providing migration options to the Identiv Connected Physical Access Manager (ICPAM). Customers are encouraged to migrate to ICPAM in order to receive important updates and continue expanding and extending their access control system. The ICPAM software will work with both the new EM-100 Controllers and existing Cisco Physical Access Gateways. The existing Cisco Physical Access Manager (CPAM) software (v1.5.3 and earlier) does not support new EM-100 controllers.

Cisco has announced their End-Of-Life (EOL) plan for the Cisco Physical Access Manager System. End-of-Sale (EOS) for the Cisco Physical Access Manager has been announced and orderability will be turned off on May 17, 2016. The following replacement products are available for order now:

Cisco Product ID (PID)	Replacement Product (PID)	Notes
CIAC-GW-K9	ICPAM-EM100-HW	Replacement product can be purchased through Cisco.
CIAC-PAME-EDI=	ICPAM-EAI=	
CIAC-PAME-HA=	ICPAM-HA=	

Cisco's End-of-Sale and End-of-Life announcement is published at:
http://www.cisco.com/c/en/us/products/collateral/physical-security/physical-access-manager/eos-eol-notice-c51-736268.html

What does the ICPAM upgrade cost?

Currently, there is no cost to upgrade from CPAM to the new ICPAM software as long as your existing software license covers the number of modules/doors deployed. To receive ICPAM technical support and access to new releases, however, customers should purchase support contracts directly from Identiv. Customers with no support package will fall under a per incident/call support plan. Further details can be found under the "Product Support" section of this document.

General Upgrade Questions:

What is the process for migration from CPAM to ICPAM?

Cisco and Identiv have partnered to provide a migration path to the Identiv Connected Physical Access Manager (ICPAM). Customers are encouraged to migrate to ICPAM in order to continue expanding and extending their access control system. The ICPAM software will work with both the new EM-100 Controllers and existing Cisco Physical Access Gateways. However, the existing Cisco Physical Access Manager (CPAM) software will not support new EM-100 controllers nor additional new hardware or software features released by Identiv.

Migration Request Process

The process used to plan and work with customers for the CPAM-to-ICPAM migration includes:

1. Submitting an Upgrade Request ticket to Identiv Technical Support. This is done by providing your customer and contact information by emailing Identiv Technical Support at: http://www.identiv.com/icpam-support
2. Completing the pre-assessment checklist and returning it to Identiv Technical Support.
   The checklist can be found at:
   http://files.identiv.com/products/physical-access/icpam/ICPAMCustomerPre-UpgradeAssessmentChecklist.pdf or http://support.identiv.com/icpam/
3. Technical Support will contact the customer to schedule an upgrade review. (This review may consist of running a script to assess your environment)

We ask customers to budget time before their desired upgrade date so that Identiv can work together to assess the scope of the migration and provide the proper support. The time and effort to upgrade will vary based on the following factors: database size (user/badge population size, number of doors, and the number of events not archived), the customer's CPAM version prior to upgrade, hardware performance, and integrations with other systems. Additional details can be found under the "Upgrade Paths and Tips" section of this document.

In some cases, the extent of the migration and previous customization may require partner or end-user training or utilization of Identiv Professional Services to ensure a successful experience.

Licenses

How are existing CPAM licenses handled after the upgrade?

Existing CPAM software licenses will be honored, however, if the number of modules/doors expand, you will need to review your coverage and, as needed, purchase additional ICPAM licenses. ICPAM software licenses are available based on the number of modules required (8, 16, 32, 128, 512 plus) Additionally, there are optional licenses available for purchase. Optional license purchase is applicable for end-users who require the following features and do not have a previously installed EDI and/or HA license.

Are my existing CPAM EDI and HA licenses transferable when I upgrade to ICPAM?

Yes. Previously installed EDI and HA licenses from Cisco with CPAM will remain effective after the upgrade to ICPAM without any specific action required. This is contingent on keeping the current MAC address of server, as the previous license is keyed to this address.

If I do not have an existing EDI and/or HA license, where can I purchase these?

Customers can purchase EDI and HA licenses through Cisco using the following PIDs:

Cisco Product ID (PID)	Description	Notes
ICPAM-EAI=	Enterprise Data Integration for database integration (LDAP/SQL)	Compatible with ICPAM only
ICPAM-HA=	ICPAM server High Availability	

These PIDs are compatible with ICPAM; they should NOT be used for installations that use CPAM.

Contact Identiv Inside Sales for further information at: sales@identiv.com or your Cisco sales representative.

How do controller licenses work in a mixed environment? Where do you see licenses in ICPAM?

As previously noted, existing installed EDI and HA licenses from Cisco with CPAM will remain effective after the upgrade to ICPAM without any specific action required. This is contingent on keeping the current MAC address of server, as the previous license is keyed to this address. Similarly for controller licenses, existing licenses will be honored and be suitable for all types of hardware in your environment, however, if the number of modules/doors expand, you will need to review your coverage and, as needed, purchase additional ICPAM licenses. Controller licenses will appear side by side with feature licenses as they had for CPAM.

Why do my former CPAM Gateway controller licenses appear in the admin screens after upgrade?

Previously installed CPAM licenses will remain installed, applying to any types of hardware deployed.

What can I do if I have purchased, unused Cisco CPAM licenses?

Cisco will work directly with customers on appropriate adjustments should they have previously purchased, unused CPAM licenses. As each customer situation may be different and certain conditions will apply, please contact Cisco's CPAM product manager at ask-identiv@external.cisco.com

Supported Hardware

What controllers are supported by ICPAM?

ICPAM v2.x supports the current CPAM-compatible Cisco Physical Access Gateway with firmware v1.5.3 and the new EM-100 Controller.

Will my existing I/O modules be supported when I upgrade to ICPAM?

ICPAM v2.x supports the current CPAM-compatible Cisco I/O modules when paired with Cisco Physical Access Gateways.

Does ICPAM support Cisco Physical Access Control Gateways and EM-100 controllers together?

Yes. ICPAM v2.x will support both types of controllers deployed concurrently. However, do make sure your Cisco physical access gateway has the proper firmware version.

ICPAM v2.x only supports Gateways with firmware version 1.5.3. Details are outlined in release notes under the minimum system requirements section at: http://www.identiv.com/icpam-support#icpam-release-notes

Why do my Cisco Access Control Gateways show up in the hardware tree with a status of "mismatched"?

The controllers have an unsupported firmware. ICPAM v2.x only supports Gateways with firmware version 1.5.3. Details are outlined in release notes under the minimum system requirements section at: http://www.identiv.com/icpam-support#icpam-release-notes

What CPAM server hardware is supported by ICPAM?

New implementations of ICPAM v2.x will only be supported running as virtual machines on VMware vSphere 5.x or 6.x and will be provided to customers as an OVA (Open Virtual Appliance) file. Virtual appliances have the following minimum requirements of the VMWare host and its underlying physical hardware / resources:

- 4 vCPU 2.2 GHz or higher**
- 16GB of RAM
- 500GB of vDisk***

** Some environments may need additional CPU and RAM resources depending on the number of devices, I/O rules and/or number of transactions per hour.

*** The VMWare host disk should ideally be preallocated to the guest VM to avoid disk full conditions the VM OS is not capable of predicting as it approaches, and more generally disk full conditions should be avoided generally to ensure no data loss or DB corruption.

Identiv will support upgrades from CPAM v1.5.3 that are running bare metal with an existing CPAM implementation and configurations on supported platforms. Deployments over to ICPAM on any new UCS server must be done as virtual machine guests. (See VMWare vSphere requirements)

Several legacy platforms, including MSP and PAME servers have insufficient system resources to operate, are no longer supported and will require a hardware upgrade to move to ICPAM 2.x.

The following UCS models are recommended as server replacements:

Cisco Product ID (PID)	Replacement Cisco Server (PID)	Notes
Legacy platforms not supported on ICPAM: CIAC-PAME-1125-K9 CIVS-MSP-1RU	Recommended small 1RU servers: UCS-C220-M4L With VMWare vSphere Other options: Other Cisco UCS servers with VMWare vSPhere and meet minimum VM requirements	As each deployment and customer use case varies, consult with your Cisco specialist prior to selecting and ordering your new server hardware. Refer to minimum system requirements when selecting server options (e.g. 16GB RAM minimum, E5-2620 CPU or higher). **Must include and deploy on VMWare vSPhere.**

Cisco announced End-Of-Life (EOL) plan for the Cisco Physical Access Manager Appliance with an End-of-Sale (EOS) of Aug 16, 2011. Further details are published at: http://www.cisco.com/c/en/us/products/collateral/physical-security/physical-access-manager/end_of_life_notice_c51-649911.html

Cisco announced End-Of-Life (EOL) plan for the Cisco Physical Security Multiservices Platform, with an End-of-Sale (EOS) Jun 23, 2014. Further details are published at: http://www.cisco.com/c/en/us/products/collateral/physical-security/physical-security-multiservices-platform-series/eos-eol-notice-c51-730683.html

Functionality and Workflow

Workflow changes

The Workflow Changes section of each ICPAM version Release Notes provides details on workflow changes from past versions.
http://www.identiv.com/icpam-support#icpam-release-notes

Integration

Does ICPAM support most of the features of CPAM like integration with VSM, MAPS, EDI, Badge Design and Printing etc.?

ICPAM generally supports all the features and functionality of CPAM v1.5.3. If and when limitations or exceptions emerge, these are detailed in the Exclusions section of each ICPAM version Release Notes.

An example is ICPAM v2.x no longer supports Cisco Video Surveillance Manager v6.x integrations due to end-of-life of VSM 6.x.

Prior integrations with the CPAM v1.5.3 web services suite will remain compatible.

Is ICPAM compatible with PSOM or PSIM?

ICPAM supports these integrations. For further details on PSOM or PSIM, reference: http://www.cisco.com/c/dam/en/us/td/docs/security/physical_security/video_surveillance/psom/5_1/cpam_integration_guide/im_ac_cpam.pdf

Upgrade Paths and Tips

What version of CPAM software is upgradable to ICPAM?

Refer to ICPAM Release Notes, “Upgrade Path” for more details.
http://www.identiv.com/icpam-support#icpam-release-notes
The following upgrade paths from CPAM to ICPAM v2.2.0 are supported:

- CPAM 1.5.3 to ICPAM 2.2.0(0.3.8)
- ICPAM 2.1.0 to ICPAM 2.2.0(0.3.8)
- ICPAM 2.1.1 to ICPAM 2.2.0(0.3.8)

Note: For any new releases going forward, supported upgrade paths will be outlined in the ICPAM customer release notes.

What are the steps to upgrade from CPAM to ICPAM?

Details and screenshots can be found in the CPAM to ICPAM Technical Migration Guide at the following link: https://www.identiv.com/images/pdfs/ICPAMtechmigrationguide.pdf

Are there any system requirements/pre-reqs to be aware of?

A list of minimum system requirements are included in the release notes. The latest release notes can be found here: http://www.identiv.com/icpam-support#icpam-release-notes

Product Support

How will I continue to receive support for CPAM?

The Cisco Physical Access Gateway hardware and Cisco appliance server hardware will continue to be serviced by Cisco. Any RMA requests or service questions should be directed to Cisco's technical assistance center (TAC) per your existing process.

For CPAM software assistance, Identiv and Cisco have partnered to provide support. The method for contacting and initiating a support request for the Gateway or CPAM software has not changed; contact your Cisco support center per your current process.

How does Cisco's recent End-of-Sale and End-Of-Life announcement affect me?

Cisco TAC in partnership with Identiv will continue to provide support and bug fixes for CPAM per the EOL plan published at:

http://www.cisco.com/c/en/us/products/collateral/physical-security/physical-access-manager/eos-eol-notice-c51-736268.html

Once I upgrade, how will I receive support for ICPAM?

Identiv will provide support for both the EM-100 controllers and ICPAM software. Customers will have the choice of purchasing support contracts directly from Identiv to cover software or hardware support. Customers with no support package will fall under a per incident/call support plan. Details for support packages are referenced below.

Identiv Support Package

Identiv provides a support package for customers migrating from CPAM to ICPAM to provide continued technical support under ICPAM. These ICPAM support packages are purchased directly from Identiv. Consult with your Identiv Channel Sales Manager or email cisco@identiv.com for further details.

Identiv Support Product SKU	Product and Description	Products Covered
ICPAM-SAM-YRLY- ## ##: available to cover 1 to 1024 modules	Yearly Support and Maintenance for ICPAM - up to specified modules ICPAM yearly Software Support License for technical support, maintenance, new releases and updates	ICPAM software and Controller Firmware (EM-100, Gateway)

Additionally, the Hardware Maintenance Program, a hardware-only support package option, is available directly from Identiv. This provides annual access to significantly discounted replacement hardware for post-warranty hardware replacements.

Will my currently active Smartnet support contract through Cisco be transferable upon upgrade?

Customers will need to purchase a new support package directly from Identiv to cover their ICPAM software or EM-100 controller hardware as outlined in the previous section on “Identiv Support Package”. As an alternative, customers can choose to opt out of a support package, however, they will incur a per incident/call support charge and not be eligible for software or firmware updates.

Cisco will work directly with customers on adjustments or credits should they have a currently active Smartnet contract on the CPAM software. As each customer situation may be different, please contact your Cisco account manager to initiate this request.

Who do I contact if I have further questions?

Additional contact emails and links:
Support: Access our tech chat or submit an email at http://www.identiv.com/icpam-support
Inside Sales: sales@identiv.com
Product Roadmap and Other General Questions: cisco@identiv.com

Appendix A: Use Case Scenarios

The following are a few use case scenarios and how the migration plan might be addressed:

Customer has existing 32 licenses (CPAM), 10 doors, what is the effect of migrating to ICPAM?

- What about my licenses and how will this work? If I paid for licenses before, do I need to pay again?
    - Any existing licenses from a CPAM install will transfer in the upgrade to ICPAM
    - Any existing configured doors and gateways will continue to function as configured without any need for configuration changes.
- How do I add gateways?
    - In the ICPAM software, Gateways will continue to insert themselves into ICPAM once they have the server IP address in their configuration.
    - If you have DHCP option 150 setup for your security VLAN you can have the gateways insert themselves into ICPAM automatically without having to pre-configure the gateway.
- How will my mixed environment function?
    - EM-100 controllers are configured without the use of door templates and/or virtual device configuration; doors are configured directly on the hardware device.
    - Gateways in ICPAM v2.x will continue to function much the same as they had with CPAM v1.5.3 with a few exceptions. Most notably is the addition of virtual credential templates to help manage multiple types of credentials across multiple types of devices.