Identiv Connected Physical Access Manager (ICPAM) version 2.2 Release Notes

The Identiv Connected Physical Access Manager (ICPAM) v2.2(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 both EM-100 Controllers and Cisco Physical Access Gateways (CIAC-GW-K9).

This document contains important information about the ICPAM software version 2.2, including an overview of release scope, policy and procedures, minimum system requirements, reference documentation, exclusions and an explanation of resolved issues and caveats.

NOTE: Upgrade to ICPAM v2.2 is mandatory for CPAM customers planning to deploy EM-100 Controllers, or deploy a mixed environment consisting of EM-100 Controllers and Cisco Physical Access Gateways, and recommended for existing ICPAM 2.1.0(0.3.x) deployments.

Table of Contents

Scope of Release - Features

EM-100 Controller Support
ICPAM 2.2 supports management of Identiv EM-100 Controllers, while simultaneously providing continued support for Cisco Physical Access Gateways.

EM-100 AES encryption is supported in this release and must be enabled in both the controller and ICPAM configuration.

Steps to enable:
Configure the EM-100 controller by using a browser to logon to the controller. In Advanced Settings, ensure the "Encrypt Host Communication" checkbox is checked (encrypt) and a random seed number specified in the "Encryption Key Seed Value" field at the bottom of the page. Click "Submit" to save the changes, and "Save" to confirm them.

When adding the EM-100 controller to ICPAM in the hardware tree, ensure the "Use encryption" checkbox is checked in the "Configuration" tab, and the same seed number provided to the controller is entered into the "Encryption seed" field. Click "Save and Close".

This release supports up to 2000 controllers. This number may vary based on hardware configuration, network quality and configuration.

EM-100 Exit Reader and Anti-Passback Support

ICPAM 2.2 introduces support for an exit reader on EM-100's to support tracking/reporting on badge-out events as well as enforcing anti-passback (APB) policies. APB modes support soft (grant access but record event/alarm on violation), hard (deny access on violation), timed (deny access until badge times out of APB zone), and soft timed (grant access but record event/alarm on violation until badge times out of APB zone).

Exit reader expansion modules can be added to existing deployed EM-100 doors, and a virtual "slave door" added to represent the second reader in APB scenarios.

New doors to be deployed with an second exit reader can be added with a built-in "Single door, Two readers" EM-100 template.

Upgrades
In-place upgrades from existing customer deployments of CPAM 1.5.3 are supported. No need to make configuration changes or replace current UCS, gateway, or desktop hardware, and operating systems that meet recommended minimum system requirements. Cisco Physical Access Gateways must be upgraded to v1.5.3 firmware prior to upgrade.

Continued Integration
ICPAM integrates with Cisco Video Surveillance Manager (VSM) to provide total access, single point of security, any distance from the door.

Workflow Changes
Virtual Credential Templates have been introduced in ICPAM to enable support for controller-type-specific credential templates. A Virtual Credential Template groups together controller-type-specific credential templates and virtual credential templates are bound to badges.

The filter option in the various list dialogues is disabled by default. If needed, this option can be re-enabled via User Profiles.

Upgrade Paths

Upgrade is mandatory for customers deploying EM-100 Controllers, or an environment consisting of EM-100 Controllers and Cisco Physical Access Gateways.

The following upgrade paths to ICPAM 2.2 are supported:

- CPAM 1.5.3 to ICPAM 2.2(0.3.8)
- ICPAM 2.1.0 to ICPAM 2.2(0.3.8)
- ICPAM 2.1.1 to ICPAM 2.2(0.3.8)

Note:
System configuration checks are performed as part of the upgrade process. If a conflict is detected, the upgrade process will gracefully exit, leaving the system in its original state. The following conditions will prevent upgrade:

- CPAM version earlier than v1.5.3
- A VSM 6.x driver installed present

Customers using older CPAM versions (1.5.2 and below) will need to first upgrade to 1.5.3 then to 2.2. Reference Cisco 1.5.3 release notes for further upgrade details.

Additional upgrade instructions for ICPAM can be found in the ICPAM installation guide accessible at: http://www.identiv.com/support-icpam

For reference the Cisco v1.5.3 release notes can be found at http://www.cisco.com/c/en/us/td/docs/security/physical_security/access_control/release_notes/1_5_3/cpac_rn_1_5_3final.html

Cisco CPAM install and upgrade document can be found with the Cisco Physical Access Manager Documentation at: http://www.cisco.com/en/US/products/ps9688/tsd_products_support_series_home.html

Identiv CPAM 2.2 supports Cisco Physical Access Gateways with the 1.5.3 version of firmware. Future iterations of ICPAM will no longer implicitly require Gateway firmware to be upgraded. See the Cisco Physical Access Gateway User Guide for instructions to upgrade older firmware versions to 1.5.3.

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	• Fresh installation or CPAM 1.5.3, ICPAM 2.1.0, or ICPAM 2.1.1
Physical access controllers and/or controller modules	• Identiv EM-100 Controllers: Firmware Release 3.5.1 is required on all Identiv EM-100 controllers. The EM-100 will ship with FW version 3.5.1 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

- 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.)

- Two Door policies is not supported for EM-100 Doors

- 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 v2.2 User Guide and ICPAM v2.2 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

Cisco CPAM Physical Access Gateway documentation:

- http://www.cisco.com/en/US/products/ps9687/tsd_products_support_series_home.html

Support and Service Requests

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

Resolved Issues and Caveats

Caveats

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

Additional descriptions, status, or workaround information can be found using the Bug Search Tool.

Identifier	Title
CSCuv50557	Advanced Gateway options not seen in single screen badge wizard.
CSCuo83272	CPAM MySQL bin files occupying the entire space when Stand-By 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-233	Client allows attempted downloading of more than the limit of 8 Access Policies to a single EM-100 and prevents download completion. Work-around: do not exceed limit of 8 Access Policies
ICPAM-262	HA – Shared IP goes to standby mode
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-491	Backup version x allows restore to ICPAM version y and corrupts installation
ICPAM-598	AdModCardRecord fails with -1001 Duplicate unique ID when no card DB has ever been downloaded

ICPAM-484	All Doors report does not display status for EM doors
ICPAM-482	Location info is not inherited to the door upon selecting the checkbox "Inherit location from parent"
ICPAM-443	Running a report with customized Variable Parameters throws an error
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-396	GUI: Command and Monitoring Tabs do not work in some browsers Work around: 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-268	CSCuv50557: Advanced options not seen in single screen badge wizard
ICPAM-437	A badge that is attached to an expired access policy is granted access
ICPAM-596	Virtual Credential Template Add/Edit dialogue has incorrect label. Refers to "Badge Format"
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-495	Duplicate card caused by cred # + format and then raw form entered

Resolved Issues

The following issue resolutions are included with ICPAM version 2.2(0.3.8).

Identifier	Title
CSCux00201	Access Policy restriction not happening based on Profiles
ICPAM-129	After upgrade the filter option is not displayed. Work around: After upgrade, go to Profiles and enable filter option for each required module.
CSCuw61388	Blank schedule is created when we try to create schedule through API.
CSCuw55423	Error while executing "createTimeEntry" in WS API.
ICPAM-312	Abrupt shutdown of ICPAM leaves Web Admin Console blocked in archive page of setup wizard
ICPAM-239	EM-100 controller goes to Error/Unlicensed state
ICPAM-386	Some AD Fields not being pulled in EDI Job + Disabled Users in AD not Getting Disabled in ICPAM
ICPAM-381	CPAM : Unable to login to CPAM webadmin , System Isn't Ready