IDENTIV

Identiv Connected Physical Access Manager version 3.0.0(Hotfix 07/14/2017) Release Notes

The Identiv Connected Physical Access Manager (ICPAM) version 3.0.0(0.3.12) 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 panel controllers, EM-100 edge controllers and Cisco Physical Access Gateways (CIAC-GW-K9).

This document contains important information about the hotfix dated July 14, 2017 for ICPAM software version 3.0.0(0.3.12) released Dec 23, 2016, including an overview of release scope, and an explanation of resolved issues.

To access the most current version of the ICPAM Hotfix, please complete and submit the ICPAM Software Request form and select the version for 3.0.

INSTALLATION DISCLAIMER: After applying the Hotfix to the ICPAM Server, Reinstall ALL ICPAM Clients.

Table of Contents

Scope of 3.0 Hotfix - Features

Scope of 3.0 Hotfix 07/14/2017 Release - Features

This hotfix adds:
- Trigger alarm for breach of max of 100 (or new max) access policies per badge for a gateway during cred download

Scope of 3.0 Hotfix 04/13/2017 Release - Features

No features have been added in this iteration of the hotfix

Scope of 3.0 Hotfix 03/15/2017 Release - Features

No features have been added in this iteration of the hotfix

Scope of 3.0 Hotfix 02/22/2017 Release - Features

This hotfix adds:
- Mx hardware wizard models to allow deploying Mx-4 and Mx-8 as elevator controllers

- The ability to set the IP address of Mx controllers from within the wizard when using the "Discover" capability
- Online help update for the Mx Driver
- Usability enhancements around the Mx Driver

Upgrade Paths

This hotfix only applies to ICPAM 3.0.0(0.3.12) or ICPAM 3.0.0(0.3.12) with and prior hotfix applied.

Hotfix 07/14/2017 Deployment

1. Go to web admin console > monitoring > click stop on the server
2. ftp/winscp the hotfix-ICPAM-3.0.0_07142017.zip to the ICPAM server as cpamadmin user. For scp:
   a. `scp hotfix-ICPAM-3.0.0_07142017.zip cpamadmin@<your server IP address>:.`
3. ssh to server as cpamadmin
   a. `ssh cpamadmin@<your server IP address>`

4. `cd /home/cpamadmin`
5. `sudo su`
6. `service immortal stop`
7. `unzip ./hotfix-ICPAM-3.0.0_07142017.zip`
8. `cd patch07142017`
9. `sh ./hotfix-ICPAM-3.0.0_07142017.sh`
10.   `service immortal start`

11. Wait for start process to complete

12.   `exit`
13.   `exit`

14. Go to web admin console. Note you may have to wait from 5 to 30 seconds for the web admin console to restart.
15. Select Monitoring > Status, confirm the Server Mode is Down and click Start.
16. Reinstall *all* ICPAM clients by downloading a new version from the web admin console under Downloads > Identiv CPAM Client (JRE required)"

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

Resolved Issues

Resolved Issues - 02/22/2017 Hotfix

The following issue resolutions are included with ICPAM version 3.0.0(0.3.12).

Identifier	Title
ICPAM-1079	When configuring an Mx controller for the first time, connecting goes to Unlicensed state
ICPAM-1108	WS API call getAllBadgesByPerson missing Access Policy data after upgrade

ICPAM-1114	8 access policy limiting being hit due to no AP filtering per controller
ICPAM-1124	WS API call enrollBadge fails to populate credential template in badge after upgrade to 2.2(0.3.12)

Resolved Issues - 03/15/2017 Hotfix

ICPAM-980	Mx-Controller is executing schedules based on timezone of server rather than controller
ICPAM-1179	Events from Mx controllers not visible in monitoring when location is set in device objects of hardware tree
ICPAM-1185	Database connections note freed under certain Mx Driver scenarios leading to connection starvation

Resolved Issues - 04/13/2017 Hotfix

ICPAM-1172	Cisco licenses ignored after hotfix
ICPAM-1247, ICPAM-1248	Download configuration fails if more than 8 access policies is associated with a single Mx controller or an Mx device group is associated with more than one access policy
ICPAM-1249	Badges download after deactivation
ICPAM-1250	Duplicate PIN associated with badge is incorrectly denied access

Resolved Issues - 07/14/2017 Hotfix

ICPAM-1330	Door deny access on every door
ICPAM-1332	Support Cisco IP phone door commands for MX