Identiv Connected Physical Access Manager version 3.0.1 (Hotfix 09/08/2017) Release Notes

The Identiv Connected Physical Access Manager (ICPAM) version 3.0.1(0.3.13) 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 September 8, 2017 for ICPAM software version 3.0.1(0.3.13) released June 20, 2017, including an overview of release scope, policy and procedures, and exclusions and an explanation of resolved issues and caveats.

Table of Contents

Scope of 3.0.1 Hotfix - Features

Scope of 3.0.1 Hotfix 8/8/2017 Release - Features

This hotfix adds:

- Support Cisco IP phone door commands for MX
- Raises an alarm when the access policy account exceeds the theoretical limit of a Cisco Gateway controller

Scope of 3.0.1 Hotfix 9/8/2017 Release - Features

This hotfix adds:

- Mx credential download filter

Upgrade Paths

This hotfix **ONLY** applies to ICPAM 3.0.1(0.3.13)

Hotfix Deployment

To apply Hotfixes to a current ICPAM deployment, please use the following steps:

Step 1: Stop the Standby Server (If applicable, Skip to Step 6 if no Standby Sever available)

a. Log on to the Standby appliance through the ICPAM Server Administration Utility.

b. Click the ***Monitoring*** tab and verify the Server Mode is Standby.

Step 2: On the Standby server, select the ***Setup*** tab, and then select Hotfix in the left pane.

Step 3: Click **Choose File** to locate and select the hotfix image to apply

Step 4: Click **Update** button

a. A message appears informing you that the update is starting and the Web page will refresh.

b. If the ICPAM Server Administration utility disconnects, a browser error message may show. Wait approximately five minutes for the server to restart, and then refresh your browser.

Step 5: Once complete, the **Hotfix Applied** version will display the latest Hotfix version.

Step 6: Stop the Active ICPAM server.

a. Log on to the Active appliance through the ICPAM Server Administration Utility.

b. Click the ***Monitoring*** tab and verify the Server Mode is Active

c. Click the **Stop** button to the right of the Admin State entry,

d. Verify that the Admin State is **Down**.

Step 7: On the Active server, select the ***Setup*** tab, and then select Hotfix in the left pane.

Step 8: Click **Choose File** to locate and select the hotfix image to apply

Step 9: Click **Update** button

a. A message appears informing you that the update is starting and the Web page will refresh.

b. If the ICPAM Server Administration utility disconnects, a browser error message may show. Wait approximately five minutes for the server to restart, and then refresh your browser.

Step 10: Once complete, the **Hotfix Applied** version will display the latest Hotfix version.

Step 11: Restart the Active ICPAM Server

a. Click the ***Monitoring*** tab

b. Click the **Start** button to the right of the Admin State entry

c. Verify that the Admin State is UP

Step 12: Reinstalling the ICPAM Client

a. After applying the Hotfix, it is **REQUIRED** to reinstall the ICPAM client.

b. Click the ***Downloads*** tab on the ICPAM Server Administration Utility.

c. Click the Identiv CPAM Client link.

d. Run the installer and follow the on-screen prompts.

Step 13: Restart the Standby ICPAM Server

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 only

Resolved Issues

Resolved Issues - 08/08/2017 Hotfix

The following issue resolutions are included with ICPAM version 3.0.1(0.3.13).

Identifier	Title
ICPAM-908	EM-100: Including any one holiday in a schedule, includes all holidays
ICPAM-1331	Support Cisco IP phone door commands for Mx controllers
ICPAM-1332	Trigger alarm for breach of max of 100 (or new max) access policies per badge for a gateway during cred download

Resolved Issues - 09/08/2017 Hotfix

The following issue resolutions are included with ICPAM version 3.0.1(0.3.13).

Identifier	Title
ICPAM-1439	Only Active Credentials with at least 1 access policy will be pushed and downloaded to Mx controllers