# Migration of Cisco Physical Access Manager to the Identiv Connected Physical Access Manager

The following upgrade path from Cisco Physical Access Manager (CPAM) to Identiv Connected Physical Access Manager (ICPAM) 3.x is supported:

- CPAM 1.5.3 to ICPAM 3.x

This procedure assumes that your Cisco Gateways are already running firmware version 1.5.3, which is the required firmware version for ICPAM 2.1.0 and above.

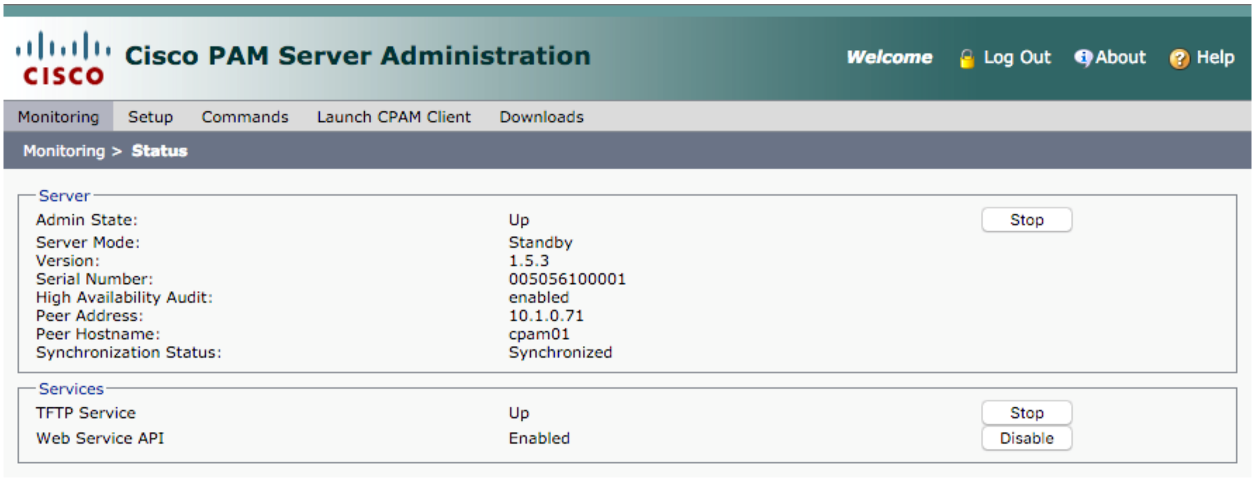
Note: This procedure only supports migrating from CPAM running v1.5.3 versions, older versions need to be upgraded to v1.5.3 before migrating to ICPAM 3.x. Systems with older versions can be upgraded to 1.5.3 by using 1.5.3 upgrade bin file from Cisco. However versions prior to CPAM 1.5.3 utilized a 32 bit operating system and database when upgrading using the Cisco provided .BIN upgrade file for 1.5.3 from a previous version it does not upgrade either the operating system or the database to their newer 64 bit versions. It is recommended to upgrade to 1.5.3 from those versions then perform a backup of the configuration and restore it to a fresh 1.5.3 install to take advantage of the performance upgrades provided by the 64 bit operating system and database prior to upgrading to ICPAM 3.x.

Regardless of the version you are migrating from, it is recommended that you verify your CPAM installation is stable and functional before you proceed with the migration. Do not proceed with the migration until you have verified that your current CPAM installation is functional and working properly.

After you have verified your system is functioning properly, you must complete the **Pre-Upgrade Assessment Checklist** and return it to Identiv Technical Support. The Pre-Upgrade Assessment Checklist is available on the Identiv ICPAM Support page at the following web address: http://files.identiv.com/products/physical-access/icpam/ICPAMCustomerPre-UpgradeAssessmentChecklist.pdf

Once you have completed the Pre-Upgrade Assessment Checklist and returned it to Identiv Technical Support, they will provide you with the .BIN file required for the upgrade to ICPAM 3.x. The process of using the BIN file to upgrade is explained on page four of this guide, under the section *Upgrade the Active Server*.

1. Stop the CPAM services through the CPAM Web Console
   a. If CPAM HA is installed and configured, stop the ***Standby*** server from the *Monitoring* > *Status* page by clicking the ***Stop*** button

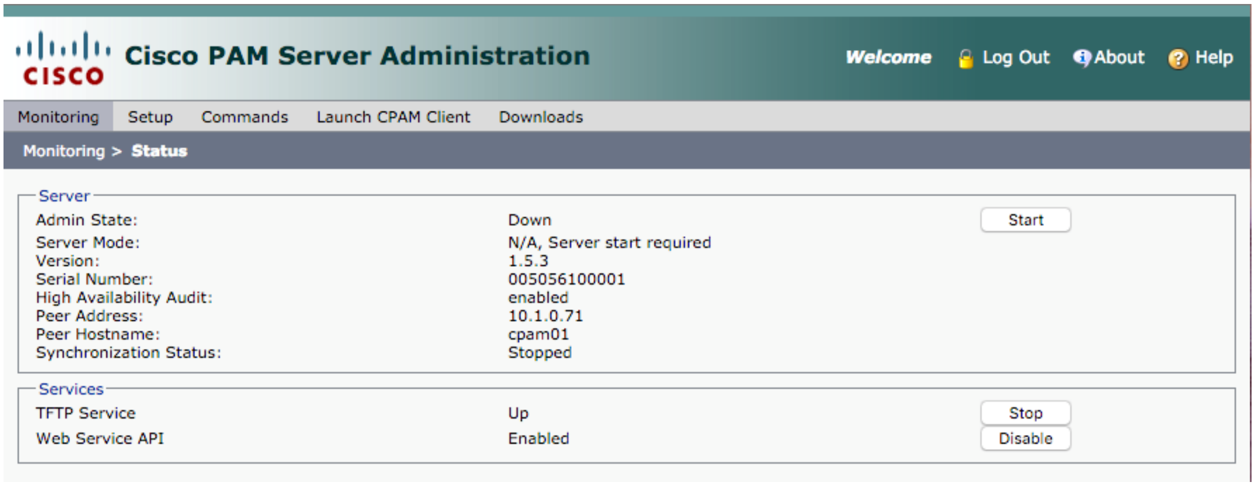


Server

| | |
|---|---|
| Admin State: | Up |
| Server Mode: | Standby |
| Version: | 1.5.3 |
| Serial Number: | 005056100001 |
| High Availability Audit: | enabled |
| Peer Address: | 10.1.0.71 |
| Peer Hostname: | cpam01 |
| Synchronization Status: | Synchronized |

Services

| | |
|---|---|
| TFTP Service | Up |
| Web Service API | Enabled |



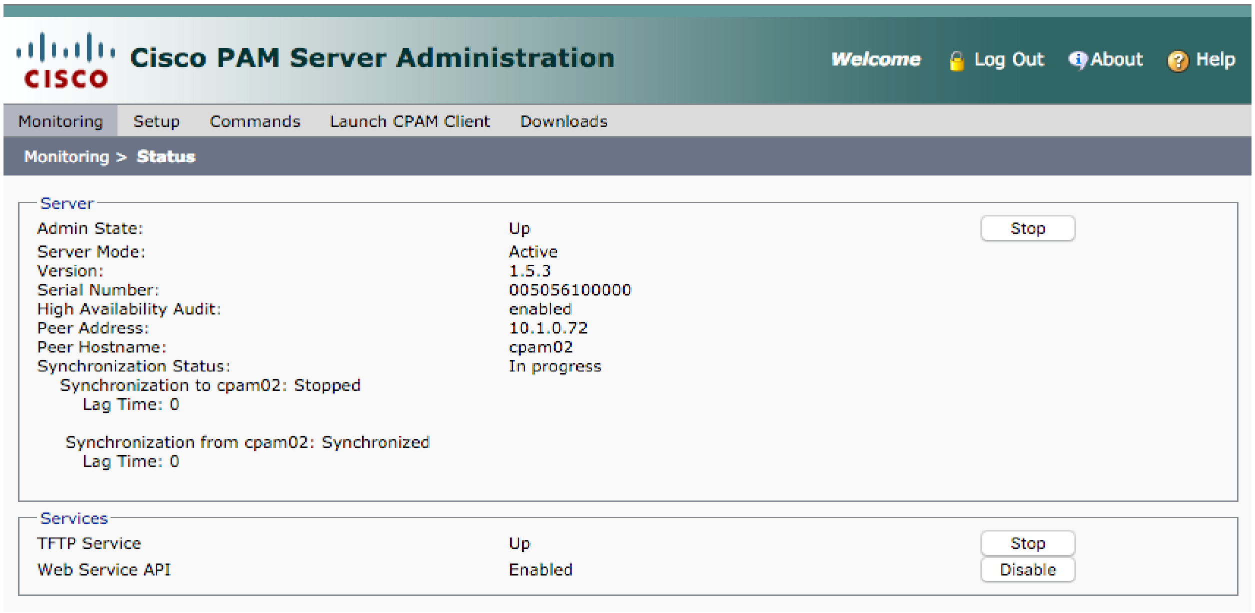
Server

| | |
|---|---|
| Admin State: | Down |
| Server Mode: | N/A, Server start required |
| Version: | 1.5.3 |
| Serial Number: | 005056100001 |
| High Availability Audit: | enabled |
| Peer Address: | 10.1.0.71 |
| Peer Hostname: | cpam01 |
| Synchronization Status: | Stopped |

Services

| | |
|---|---|
| TFTP Service | Up |
| Web Service API | Enabled |

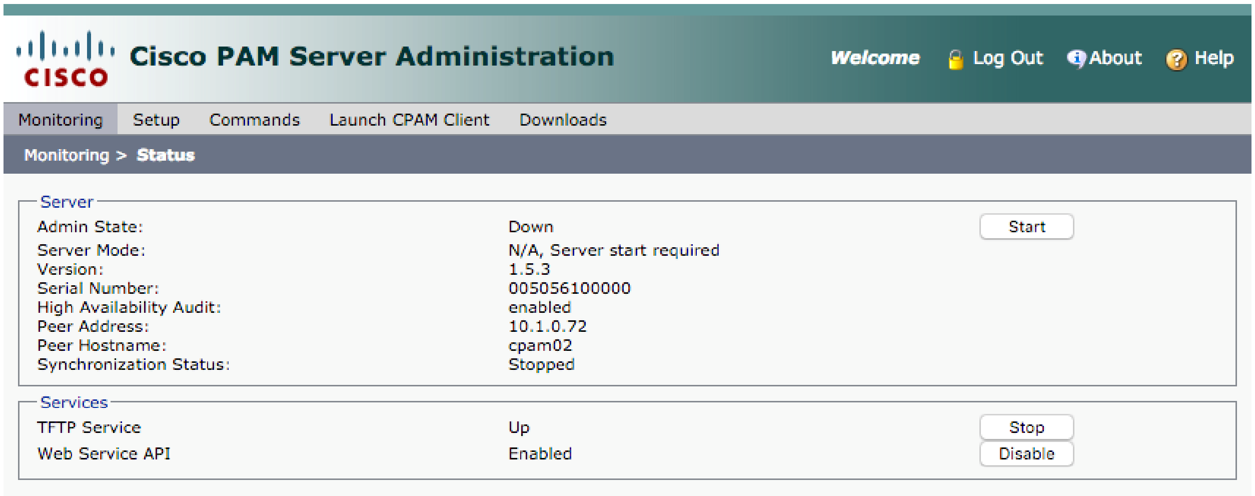
   b. Stop the CPAM services on the ***Active*** server from the *Monitoring* > *Status* page



```
Server
Admin State:                    Up
Server Mode:                    Active
Version:                        1.5.3
Serial Number:                  005056100000
High Availability Audit:        enabled
Peer Address:                   10.1.0.72
Peer Hostname:                  cpam02
Synchronization Status:         In progress
    Synchronization to cpam02: Stopped
        Lag Time: 0

    Synchronization from cpam02: Synchronized
        Lag Time: 0

Services
TFTP Service                    Up
Web Service API                 Enabled
```



```
Server
Admin State:                    Down
Server Mode:                    N/A, Server start required
Version:                        1.5.3
Serial Number:                  005056100000
High Availability Audit:        enabled
Peer Address:                   10.1.0.72
Peer Hostname:                  cpam02
Synchronization Status:         Stopped

Services
TFTP Service                    Up
Web Service API                 Enabled
```

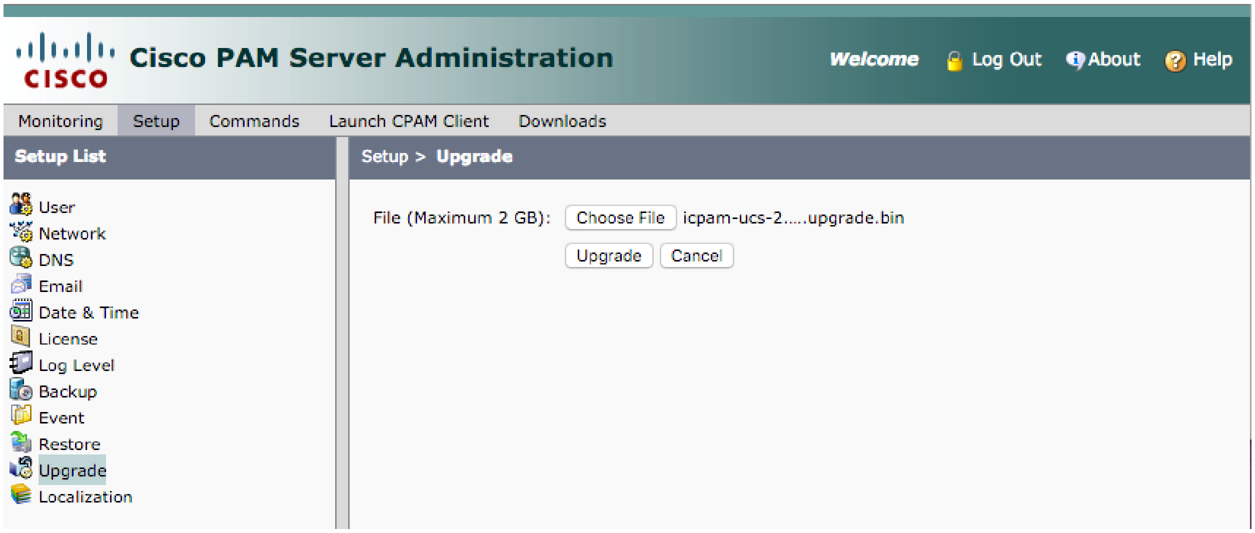
✎ Note Perform the upgrade procedures on the server that was Active before stopping services first

2. Once the services are stopped run a manual backup
    a. On the server that was ***Active*** click on the ***Setup*** tab at the top of the CPAM Web Console then select ***Backup*** from the left menu
    b. If ***Automatic backup*** is selected uncheck the box then click on the ***Manual*** tab
    c. Enter a password for the backup and select ***Configuration Only*** check box then click the ***Backup Now*** button
    d. Once the backup is completed click on the backup hyperlink and download the backup to your PC
    e. If you disabled automatic backups re-enable them before proceeding

3. If you are running CPAM in a virtual appliance on VMware it is highly recommended to snapshot before upgrading.

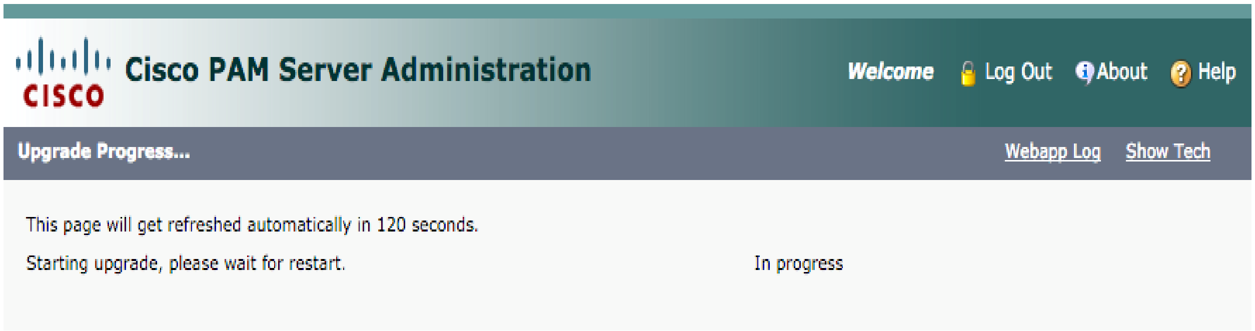
   a. If you are performing a snapshot it is recommended to shut down the server first as the snapshot will complete faster
   b. Once your snapshot is complete boot CPAM server up and log into the CPAM Web Console and ensure the services are still stopped

4. Upgrade the ***Active*** server
   a. From the CPAM Web Console for the ***Active*** server click on the ***Setup*** tab and ***Upgrade*** from the menu on the left
   b. In the right pane click the ***Choose File*** button and browse for the upgrade BIN file you downloaded from Identiv after completing the process mentioned on page one



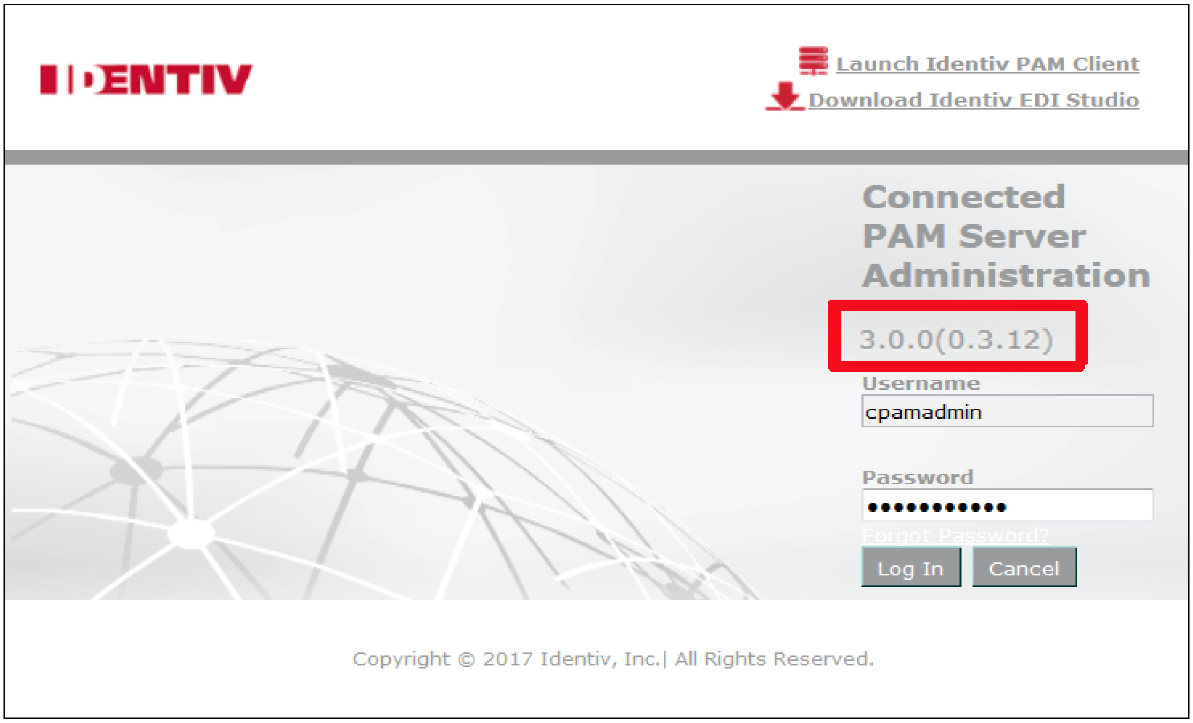
File (Maximum 2 GB): icpam-ucs-2.....upgrade.bin

   c. Once you have selected the upgrade file click the ***Upgrade*** button
   d. The upgrade process time depends on a number of items including but not limited to database size, server speed and capacity, available disk space, etc.
   e. After the file uploads you should see a series of statuses and you will be asked to log back in



This page will get refreshed automatically in 120 seconds.

Starting upgrade, please wait for restart. In progress


IDENTIV
Launch Identiv PAM Client
Download Identiv EDI Studio
Connected PAM Server Administration

3.0.0(0.3.12)

Username: cpamadmin

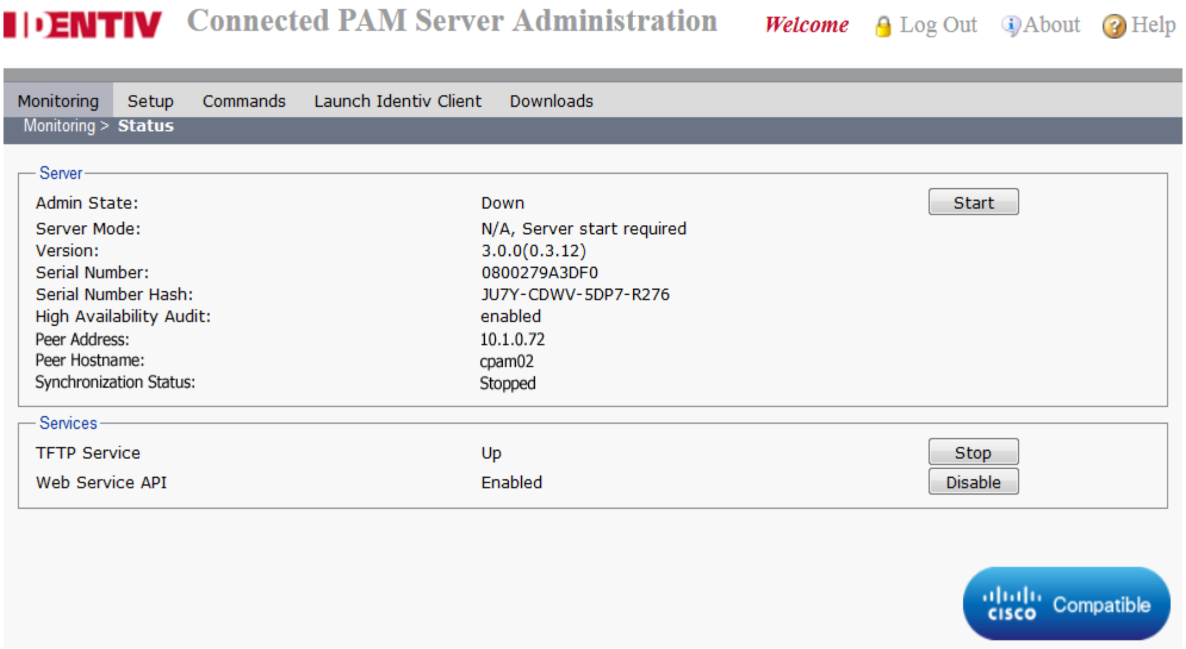
Password: ●●●●●●●●●●●

Forgot Password?
Log In
Cancel

Copyright © 2017 Identiv, Inc.| All Rights Reserved.

(Notice the version number now reflects 3.0.0)

f. Once the upgrade is completed it will take you to ICPAM Server Log In screen. Enter your password and click Log In



Server

Admin State: Down

Server Mode: N/A, Server start required

Version: 3.0.0(0.3.12)

Serial Number: 0800279A3DF0

Serial Number Hash: JU7Y-CDWV-5DP7-R276

High Availability Audit: enabled

Peer Address: 10.1.0.72

Peer Hostname: cpam02

Synchronization Status: Stopped

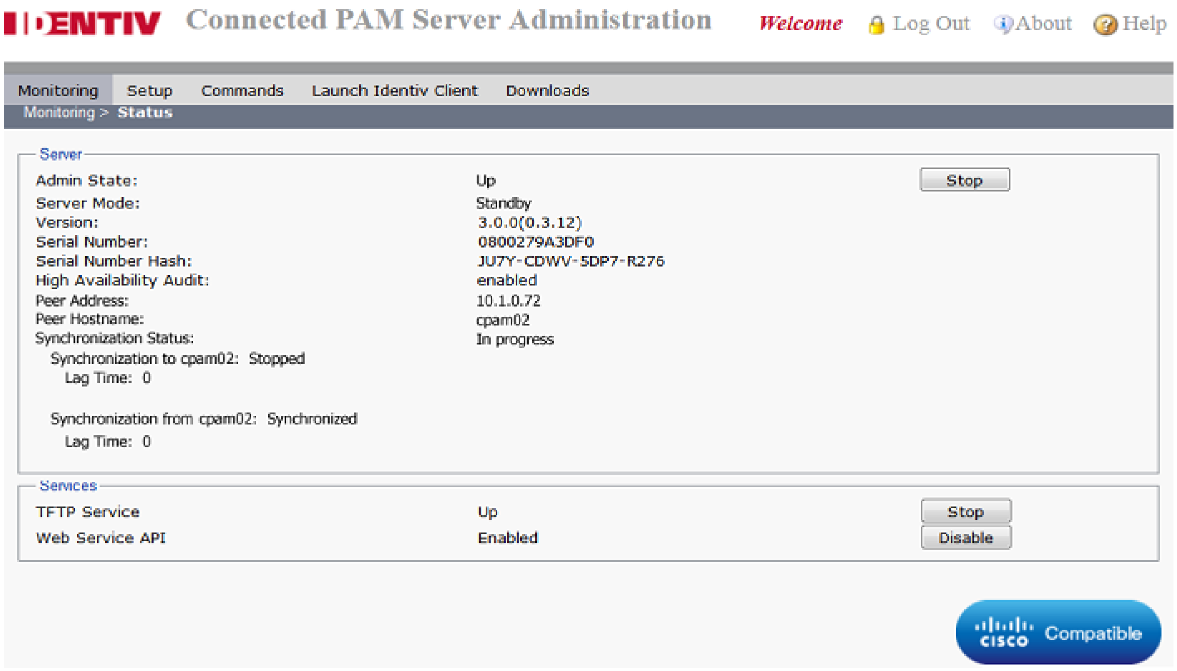
Services

TFTP Service Up

Web Service API Enabled

g. Click the ***Start*** button on the *Monitoring > Status* page

h. Once the ***Start*** button has changed to ***Stop*** the ICPAM services have started



Server

Admin State: Up

Server Mode: Standby

Version: 3.0.0(0.3.12)

Serial Number: 0800279A3DF0

Serial Number Hash: JU7Y-CDWV-5DP7-R276

High Availability Audit: enabled

Peer Address: 10.1.0.72

Peer Hostname: cpam02

Synchronization Status: In progress

Synchronization to cpam02: Stopped
Lag Time: 0

Synchronization from cpam02: Synchronized
Lag Time: 0

Services

TFTP Service Up

Web Service API Enabled

5. Install the ICPAM Desktop Client
    a. Click on the ***Downloads*** tab at the top of the ICPAM Web Console
    b. Click on the ***Identiv PAM Client (JRE required)*** link
    c. Run the client once it is downloaded and follow the prompts

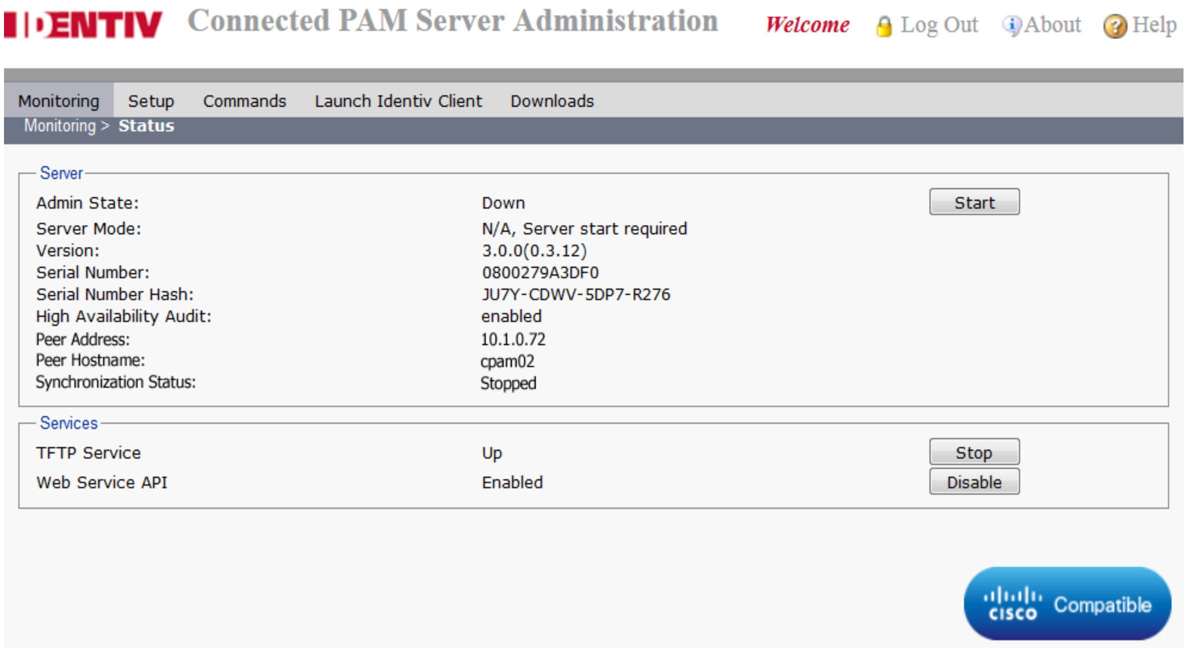
   i. If you are running Windows and cannot install to the Program Files directory you may have a permissions problem
   ii. To work around you can create a directory outside of Program Files and install to that folder (i.e. c:\Identiv\ICPAM 3.0.0\)

d. Once the ICPAM Desktop Client is installed login and test your system to ensure your system is functioning properly.

Note ICPAM 3.0.0 Desktop Client requires Java JRE 1.7 or 1.6, do not use JRE 1.8

6. Perform post upgrade backup
   a. From the ICPAM Web Console of the ***Active*** server click on ***Setup*** on the top and ***Backup*** from the left menu
      i. There is no need to stop the ICPAM services
   b. If ***Automatic backup*** is selected uncheck the box then click on the ***Manual*** tab
   c. Enter a password for the backup and select ***Configuration Only*** check box then click the ***Backup Now*** button
   d. Once the backup is completed click on the backup hyperlink and download the backup to your PC
   e. If you disabled automatic backups re-enable them before proceeding

7. Upgrade Standby server
   a. If you have HA setup on your CPAM server repeat the above steps on the ***Standby*** server after you have successfully completed the upgrade and testing of the ***Active*** server
   b. Once the server has been upgraded the *Monitoring* > *Status* page should show services stopped



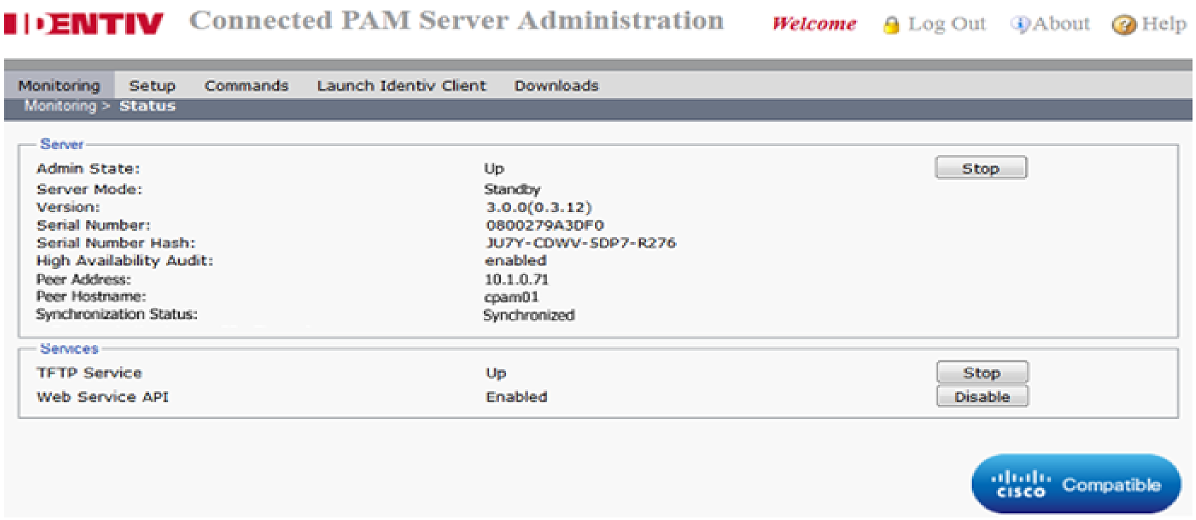
Server

| | | |
|---|---|---|
| Admin State: | Down | Start |
| Server Mode: | N/A, Server start required | |
| Version: | 3.0.0(0.3.12) | |
| Serial Number: | 0800279A3DF0 | |
| Serial Number Hash: | JU7Y-CDWV-5DP7-R276 | |
| High Availability Audit: | enabled | |
| Peer Address: | 10.1.0.72 | |
| Peer Hostname: | cpam02 | |
| Synchronization Status: | Stopped | |

Services

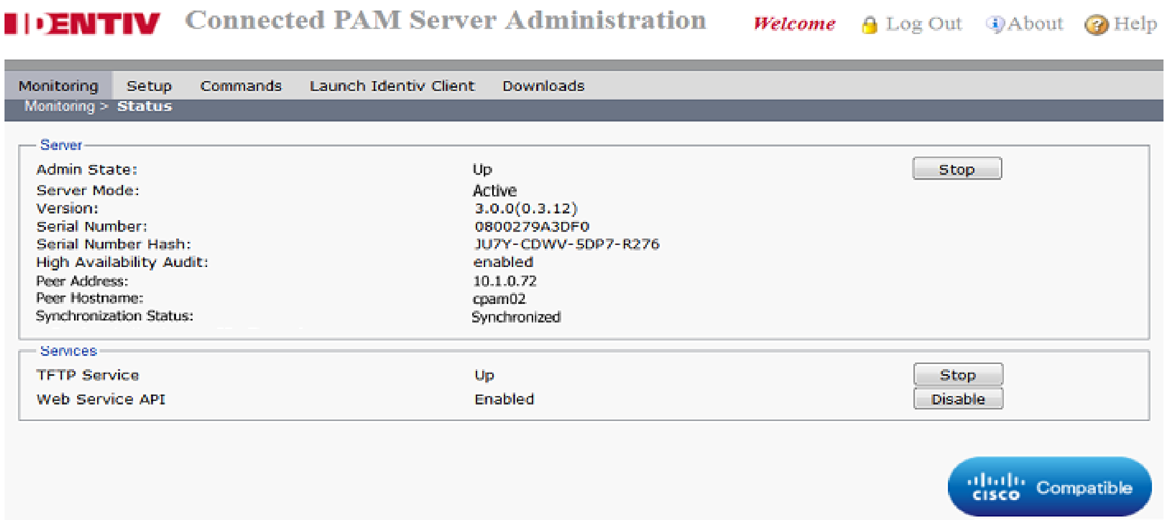
| | | |
|---|---|---|
| TFTP Service | Up | Stop |
| Web Service API | Enabled | Disable |

c. Click the Start button to start the services on the Standby server



| | |
|---|---|
| Admin State: | Up |
| Server Mode: | Standby |
| Version: | 3.0.0(0.3.12) |
| Serial Number: | 0800279A3DF0 |
| Serial Number Hash: | JU7Y-CDWV-5DP7-R276 |
| High Availability Audit: | enabled |
| Peer Address: | 10.1.0.71 |
| Peer Hostname: | cpam01 |
| Synchronization Status: | Synchronized |
| TFTP Service | Up |
| Web Service API | Enabled |

d. Verify the server status on the ***Active*** server on the *Monitor* > *Status* page



| | |
|---|---|
| Admin State: | Up |
| Server Mode: | Active |
| Version: | 3.0.0(0.3.12) |
| Serial Number: | 0800279A3DF0 |
| Serial Number Hash: | JU7Y-CDWV-5DP7-R276 |
| High Availability Audit: | enabled |
| Peer Address: | 10.1.0.72 |
| Peer Hostname: | cpam02 |
| Synchronization Status: | Synchronized |
| TFTP Service | Up |
| Web Service API | Enabled |

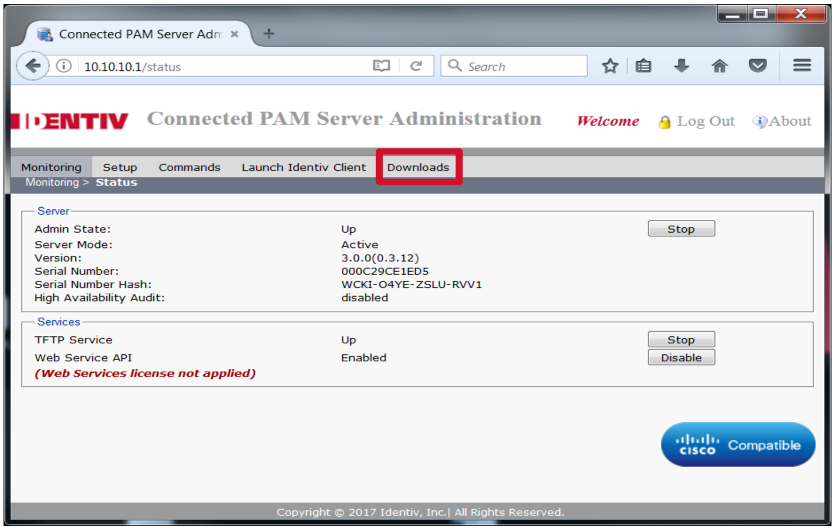
a. When *Synchronization Status* goes to ***Synchronized*** on both servers your migration is complete

Note Synchronization Status may take some time to fully synchronize depending on the size of your database.

## DOWNLOAD AND RE-INSTALL THE ICPAM CLIENT

Once the upgrade is complete and you have restarted the ICPAM Server, you will need to re-install the ICPAM Client. This can be done while you are still logged onto the ICPAM Server.

Click the **Downloads** Tab at the top of the ICPAM Server screen.



Server

| | |
|---|---|
| Admin State: | Up |
| Server Mode: | Active |
| Version: | 3.0.0(0.3.12) |
| Serial Number: | 000C29CE1ED5 |
| Serial Number Hash: | WCKI-O4YE-ZSLU-RVV1 |
| High Availability Audit: | disabled |

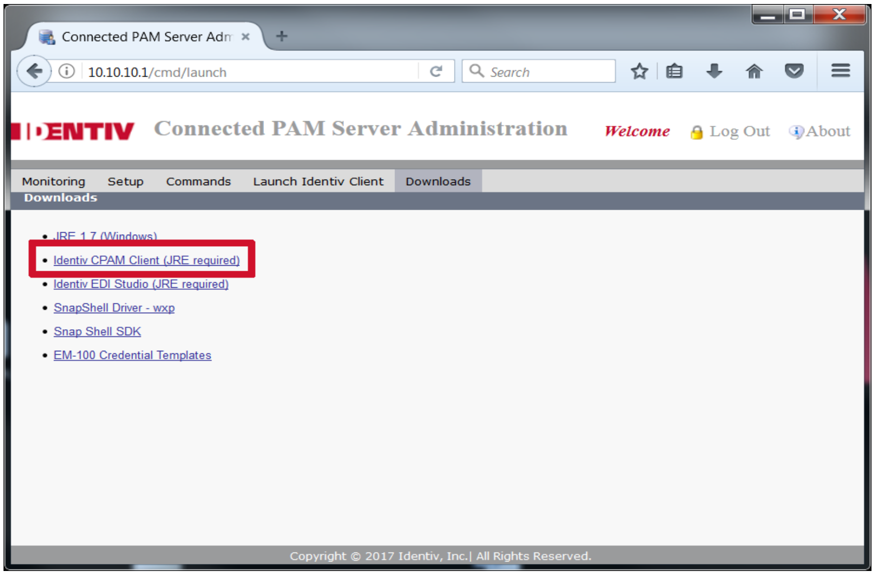
Services

| | |
|---|---|
| TFTP Service | Up |
| Web Service API | Enabled |

*(Web Services license not applied)*

Copyright © 2017 Identiv, Inc.| All Rights Reserved.

Now double click the **Identiv CPAM Client** link to download the file, then use the downloaded file to re-install the ICPAM Client.



Downloads

- JRE 1.7 (Windows)
- Identiv CPAM Client (JRE required)
- Identiv EDI Studio (JRE required)
- SnapShell Driver - wxp
- Snap Shell SDK
- EM-100 Credential Templates

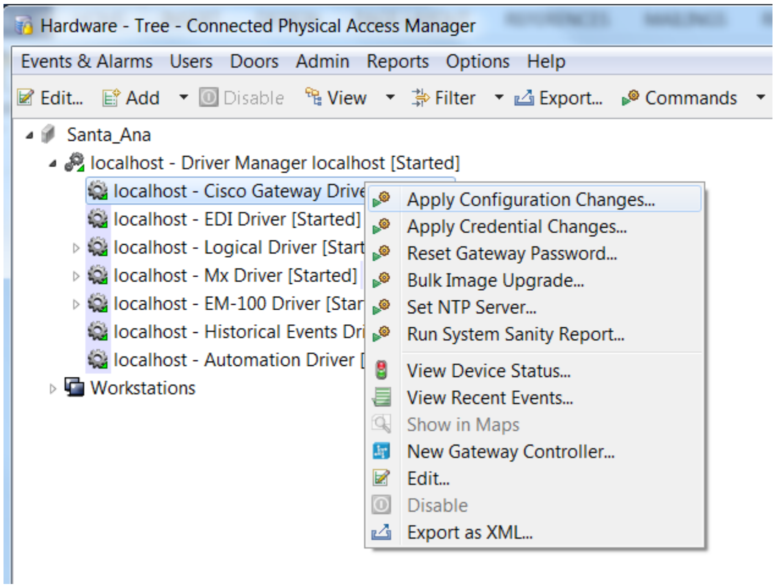
Copyright © 2017 Identiv, Inc.| All Rights Reserved.

NOTE: All machines that currently have the ICPAM Client will have to have the ICPAM Client re-installed.

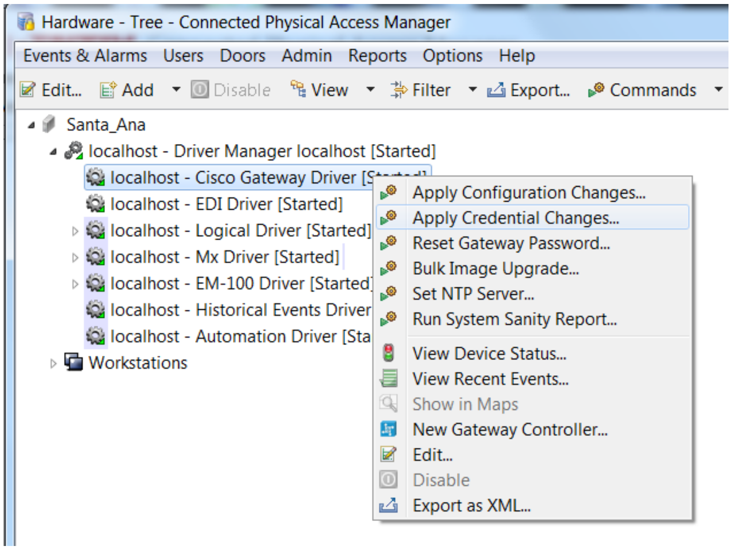
## CISCO GATEWAY DRIVER – APPLY CONFIGURATION and CREDENTIAL CHANGES

NOTE: If the following procedure is not performed after the upgrade is complete, all doors on your controller will remain locked and badges will not grant access. In addition, Access Polices will no longer work at any site.

1. Log on to the ICPAM Client.
    a. Open the Hardware Tree, and *right* click on **local host – Cisco Gateway Driver**.
    b. Select **Apply Configuration Changes...** (Depending on the size of you system, this may take several minutes.)


Hardware - Tree - Connected Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Edit...
Add
Disable
View
Filter
Export...
Commands
Santa_Ana
localhost - Driver Manager localhost [Started]
localhost - Cisco Gateway Drive
localhost - EDI Driver [Started]
localhost - Logical Driver [Start
localhost - Mx Driver [Started]
localhost - EM-100 Driver [Star
localhost - Historical Events Dri
localhost - Automation Driver [
Workstations
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...
Set NTP Server...
Run System Sanity Report...
View Device Status...
View Recent Events...
Show in Maps
New Gateway Controller...
Edit...
Disable
Export as XML...

2. *Right* click on **local host – Cisco Gateway Driver** again, and select **Apply Credential Changes...** (Depending on the size of you system, this may take several minutes.)


Hardware - Tree - Connected Physical Access Manager
Events & Alarms
Users
Doors
Admin
Reports
Options
Help
Edit...
Add
Disable
View
Filter
Export...
Commands
Santa_Ana
localhost - Driver Manager localhost [Started]
localhost - Cisco Gateway Driver [Started]
localhost - EDI Driver [Started]
localhost - Logical Driver [Started]
localhost - Mx Driver [Started]
localhost - EM-100 Driver [Started]
localhost - Historical Events Driver
localhost - Automation Driver [Sta
Workstations
Apply Configuration Changes...
Apply Credential Changes...
Reset Gateway Password...
Bulk Image Upgrade...
Set NTP Server...
Run System Sanity Report...
View Device Status...
View Recent Events...
Show in Maps
New Gateway Controller...
Edit...
Disable
Export as XML...