



datainnovations.com

Technical Webinar for IM

General Knowledge **and common issues**

Overview

High level discussion of webinar

- Instrument Manager™ (IM) and InterSystems Caché®
- How to apply Microsoft Patches
 - Data Innovations MS patch testing
- Security Keys
 - Hardkey vs. Softkey
 - Changing from Hardkey to Softkey
- Upgrading IM
 - Common tasks
 - Executing IM Core upgrade
 - Existing hardware
 - New hardware
 - How to apply Patches to Instrument Manager
 - Thin Client
 - Shadow systems

Shutdown of IM

Process to Shut down IM and Caché

- What needs to be done prior to **ALL** of the below steps?
 - IM **MUST** be shut down **PRIOR** to any changes to the core software version, any of the OS patching, or any OS reboot.
 - Full documentation for shutdown located in Getting Started Setup Guide → Maintaining Instrument Manager → Instrument Manager → Shutting down Instrument Manager
 - Shutdown steps, in brief.
 1. If you have a Shadow System, perform steps i. and ii. first.
 - i. On the Shadow Right click on the Caché Cube, choose Stop Caché.
 - ii. Choose Shut Down, click OK
 2. On the Primary, Log into IM
 3. If you have Thin Clients licensed, Perform Steps a) and b)
 - a) Have users log off of all Thin Clients
 - b) System menu → Status Of Instrument Manager Sessions
 - c) Highlight and choose End Task for each remaining TC session on that screen
 4. From the System menu → Shut Down → Yes
 5. Once IM has closed, Right click on Caché Cube, choose Stop Caché.
 6. Choose Shut Down, click OK 
 7. Once the Caché has stopped (the Cube is Gray ), Caché is off and you may continue with the steps for your required update

Windows Updates

How to apply Windows Updates

Microsoft OS Patches

Overview

- Microsoft releases a Security bulletin monthly that summarizes what OS patches are released that month.
- Data Innovations will review these released patches within 4 weeks of the summary bulletin to determine if a patch will conflict or negatively impact the functionality of our applications. (IM and JRN)
- Upon completion of the patch review, information related to the Bulletin will be distributed as follows:
 - A notification will be sent out in the Tips & Tricks listserv
 - An entry will be added into the DI Knowledge Base
- You are responsible for your own internal validation, testing, application, and management of OS patches.

Microsoft OS Patches

Data Innovations Testing process

- Data Innovations tests **all** the classified as ‘Critical’ or ‘Important’ Microsoft patches as provided by Windows Update for the **two** most frequently used versions of Windows that have been validated for the **two** most current Enhancement versions.
 - This means that we do not test any optional patches
 - If you are on an older version of IM/Windows, we are not testing these older versions against new Microsoft Patches
 - Even though we test additional updates, only the updates outlined in that month’s Microsoft Security Bulletin are posted to the Customer Web Portal Knowledge Base.
 - Details on what Operating systems and IM versions were tested are outlined in the Knowledge base article

Microsoft OS Patches

Pictures

Follow-up Links

[Email Updates Form](#)

[Data Innovations Website](#)

[Customer Web Portal](#)

Data Innovations Microsoft Security Updates Notification

Data Innovations has downloaded, installed, and tested all Important Microsoft Security updates published January 12, 2016.

For details on the updates, go to the Microsoft Technet website: <https://technet.microsoft.com/en-us/library/security/ms16-jan.aspx>

No Instrument Manager functionality has been affected.

To install the Windows Updates, please follow the steps

▷ Security Advisories and Bulletins

▷ Security Bulletin Summaries

▲ 2016

MS16-FEB

MS16-JAN

Microsoft Security Bulletin Summary for January 2016

Published: January 12, 2016 | Updated: January 19, 2016

Version: 1.3

This bulletin summary lists security bulletins released for January 2016.

For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit [Microsoft Technical Security Notifications](#).

Microsoft also provides information to help customers prioritize monthly security updates with any non-security updates that are being released on the same day as the monthly security updates. Please see

On this page

[Executive Summaries](#)

[Exploitability Index](#)

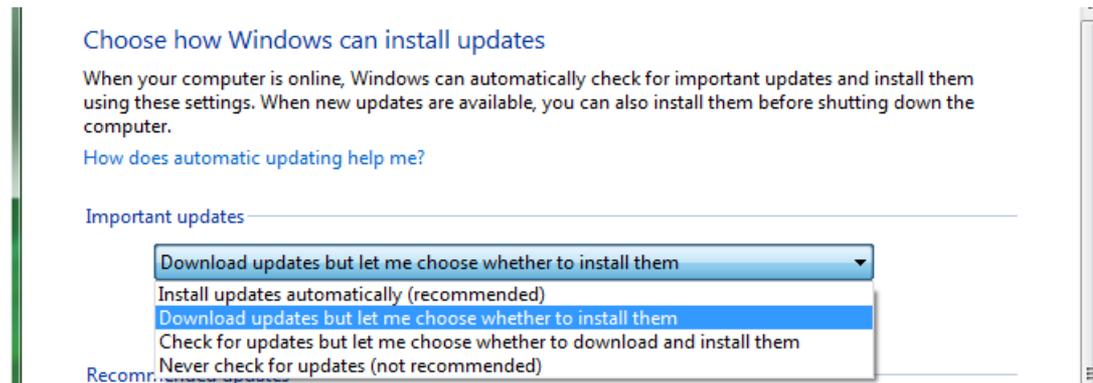
- Known Issues
- Microsoft Patch Review
 - 2015
 - 2016
 - 01-MS16-JAN**
 - Archive

Title:	MS16-001
Description:	Cumulative Security Update for Internet Explorer (3124903)
Symptom:	Testing Completed
Resolution:	Testing completed. Date: 29 Jan 2016. Test cases executed and Instrument Manager functionality not impacted. For 8.13.04 Testing was done on Windows 7 - 64 - Bit Professional and Windows Server 2008 R2. For 8.14.01 Testing was done on Windows 7 - 64 - Bit Professional and Windows Server 2012 R2.

Microsoft OS Patches

Patch Setup

- Frequently OS patches require a reboot.
- Please remember that IM/Caché need to be stopped **BEFORE** restarting the OS or applying the patches.
- As such, patches **cannot** be applied automatically via a patch management tool or by the Windows Update.
- The Windows recommended 'Install Automatically' **must be disabled**. Instead use any user controlled option.



Microsoft OS Patches

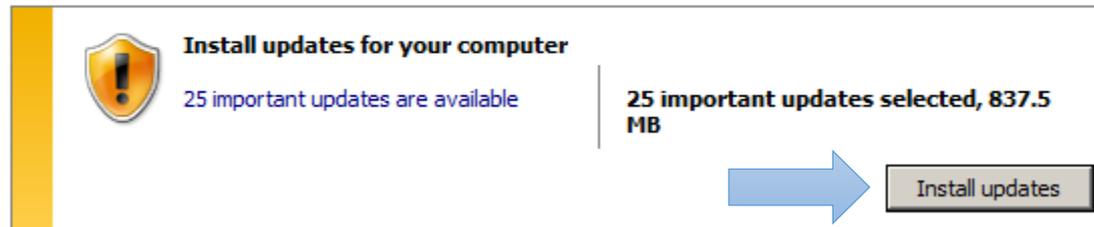
How to apply patches?

1. Stop IM/Caché per process above.
2. From the Windows Task bar, double click on the Install Update icon.



3. Choose Install updates.

Windows Update



4. Once completed, restart Windows
 - Remember to Start the Primary before you start the Shadow (if applicable).
5. Once Caché has started, log into IM and start your connections.

Questions?

Security Key

- Hard vs Soft keys
- Replacement

Security Key

What is a Security Key?

The use of Instrument Manager requires that a valid Security Key be connected to the Primary IM server at all times.

Keys are tied to your license number to determine validity

There are currently three different types of Hard keys:

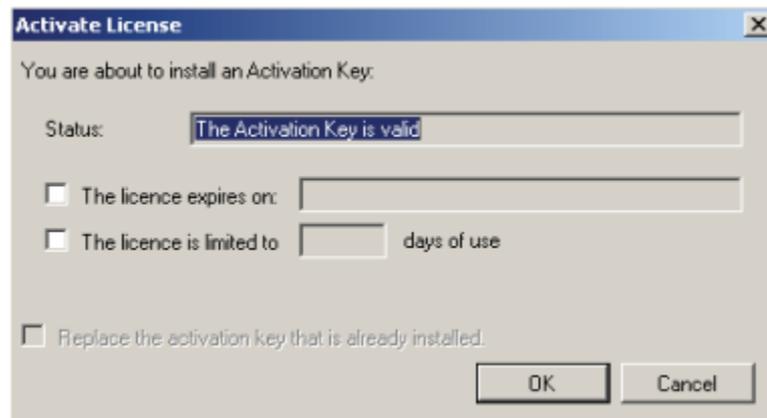


USB



Parallel

And one Software Security Key.



Security Key

What happens when the key is removed/missing/invalid?

Periodically QMGR will check on the Security Key validity, as will all connections when they first start.

- If the key is missing or invalid, the QMGR connections will enter a **Connecting** state, stop processing data, post an error about the missing key, and keep checking periodically for the key.
- When the key is detected as valid while QMGR is in **Connecting** state, QMGR will immediately transition back **ON** and resume processing data.

Connections will still continue processing in new data and sending data that QMGR has already processed if they were running prior to when the key became invalid/missing.

If the connections are stopped, they will not start again while the key is invalid/missing. Attempting to start the connection will post an error and the connection will stay in the OFF state.

Security Key

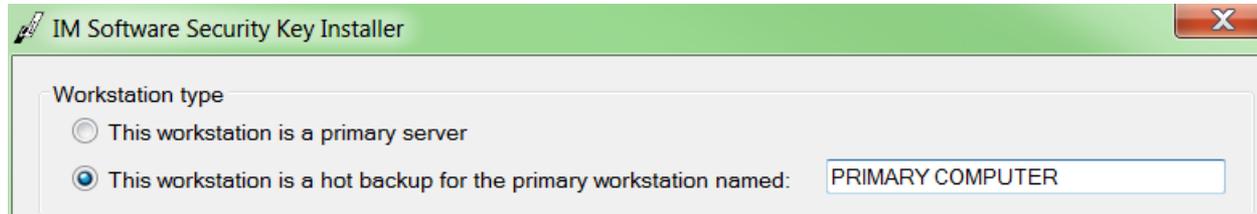
What happens when the key is removed/missing/invalid?

- If the key becomes damaged or somehow unusable, the system will not be able to function without running the security key bypass from the **IM Security Key Utility.exe** located in the Instrument Manager folder on the Primary server.
- The bypass will give you 7 days of operation without a valid key.
- The day you run the key counts as day 1, no matter what time you run the key. (It doesn't matter if its 00:00:01 or 23:59:59)
 - This means if you run it any time on Monday, the key will expire the following Sunday at 23:59:59.
- During this time you need to contact Support for a replacement key, ship the broken key back **with a tracking number**, and have the new key arrive.
 - **DO NOT WAIT!** 7 days can go really quick.
 - Contact Support Immediately if you have a suspect key.

Security Key

How does a Software Key work with the Shadow?

- When you generate the Workstation ID for the Shadow system, you must identify the Computer Name of the Primary System.



- The Shadow will generate its Workstation ID based on the Computer Name of the Primary System and the system configuration of the Shadow system.
 - This is so that the key will be valid, but not allow the connections to start until a fail over and you change the computer name of the Shadow to be the computer name of the Primary.
- The idea is that the Computer Name controls when the connections will start and know the key is valid to run.

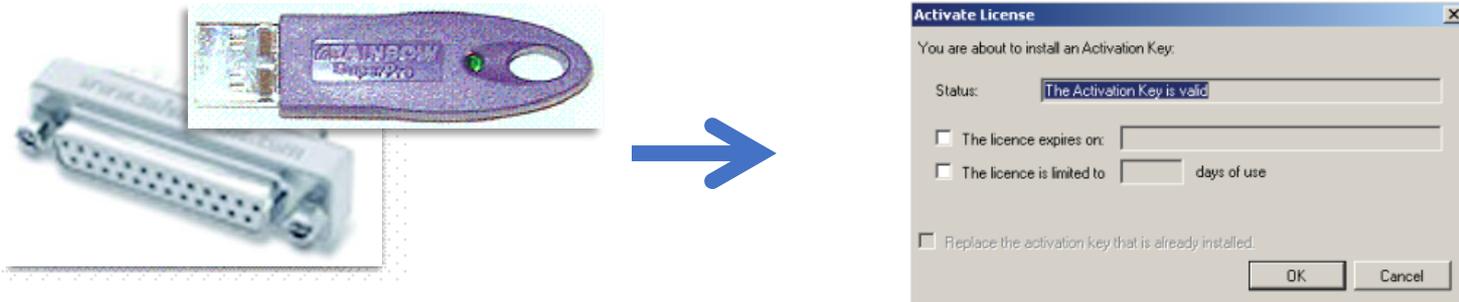
Security Key

Why would you need a different key?

The white 25 Pin key was used for many years, but is dependent on a Parallel port being available on the hardware. Often newer computer hardware no longer have parallel ports, which requires a transition to a USB Key.



When moving from a Physical Server to a Virtual server, the Hardware Key cannot be attached to the virtual machine without problems. This requires a Software Security Key to be issued.



Security Key

Key changes

- For all Key changes, please contact Data Innovations to initiate the process. (Or your system specific support)
 - Support
 - NorthAmerica-Support@DataInnovations.com
 - 802-658-1955
 - Sales
 - NorthAmerica-Sales@DataInnovations.com
 - 802-658-2850
- Support will be able to assist you with troubleshooting a failed key or starting the process for a Key replacement.
- If you have consulting time, please work with your assigned consultant on key replacement. They will be able to request replacement/swap and install the key.

Questions?

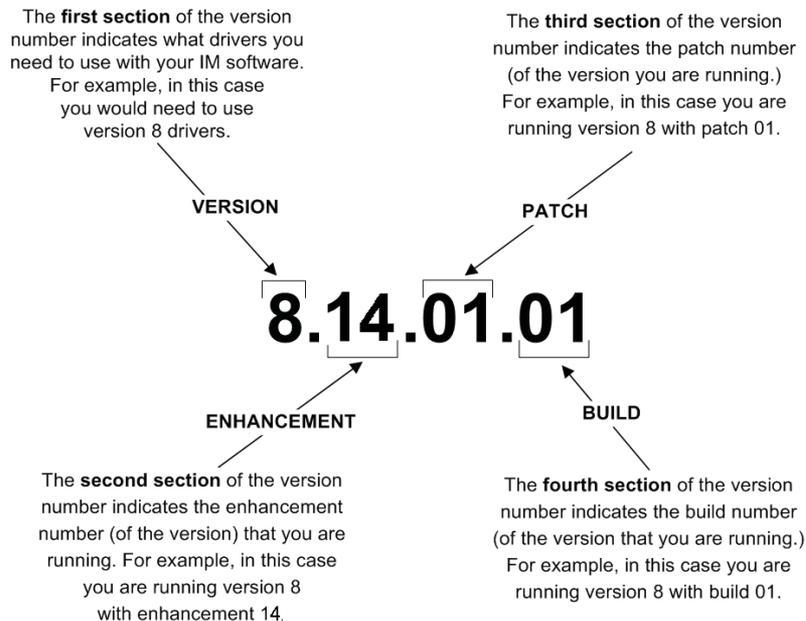
Instrument Manager Upgrades

- Core Enhancement vs. Patch upgrades
- Shadowing and Thin Client considerations
- New hardware

Upgrading IM

Understanding version numbers

- Each Instrument Manager (IM) software application has a version number. The version number is used to keep track of features and changes to the IM software application.
- The version is made up of four sections as explained below.



- The version number displays in IM's **About** box, which is accessible by clicking on the **Help** menu and then choosing **About Instrument Manager**.

Upgrading IM

Documentation and suggestions

- This outline is the abbreviated steps for Upgrading IM Thin Clients and Primary/Shadow Systems, additional detail within the IM User's Guide: Upgrade Manual.
- These steps apply to all instances of IM and Caché. The steps must also be followed for the Primary, Shadow, Thin Clients and Test Systems. (As applicable)
- It is **STRONGLY** recommended to use an **IM Test System** to test and validate the new version of the core application, Rules, and any updated drivers **BEFORE** scheduling downtime to perform the upgrade.
- Problems that may arise **might not** be solvable within your scheduled downtime window.

Upgrading IM

Starting the process

- If you are directly supported by Data Innovations LLC, you can contact either Support or Sales for the upgraded license files and Installation Media for a newer Core version.
- The upgraded license files and media are available at no cost to directly supported customers.
- In order to process the upgrade, Sales or Support will need the following information:
 1. Name, Phone Number, and Email address of requestor
 2. Shipping address, and attention if appropriate
 3. License Number(s) and the associated version(s) in place
 4. What version you are requesting? (“Latest version” is fine.)
 5. Does your server meet the new version minimum specifications?
 6. Do we need to replace the Security Key or Swap to a Soft Key?
- Upgrade Installation Services are available with a cost. Please contact Sales for a quote or more information.

Upgrading IM

Starting the process – Core Enhancement vs. Patch Upgrades

- Patch upgrades
 - **Do not** require new license files.
 - Generally **Do not** convert the contents of the Databases
 - Are almost always the **same version** of Caché
 - **Cannot** upgrade Enhancement versions (8.13→8.14)
 - **Cannot** be used to create a standalone install on new hardware
 - Available via Customer Web Portal
- Enhancement Upgrades
 - **Require** new license files.
 - **Can require** conversion of the contents of the Databases
 - Are almost always **different versions** of Caché
 - **Can** be used to apply Maintenance Releases. (8.14.01→8.14.10)
 - **Can** be used create a standalone install on new hardware
 - Available via request from Data innovations.
- No cost to direct customers to obtain either upgrade as long as there is a valid Maintenance and Support agreement.

Upgrading IM

Core & Enhancement upgrade – Preparation for upgrade

- For all Core upgrades, it is recommended that you perform the following before you start the upgrade:
 1. Appropriately release all samples held for verification
 2. Ensure that the hardware can support your security key and meets the minimum specifications for the new version
 3. Ensure that there is sufficient free space for the upgrade
 4. Ensure that the installation files are local to the system
 5. Log into Windows as Local Administrator
 6. Complete a backup of critical files.
 7. Any required communications trace data is saved to disk
 8. No other applications running on the system
 9. Appropriately shut down IM and Caché **before** the upgrade

Upgrading IM

Core & Enhancement upgrade – Same/Existing hardware

- Upgrading IM on the same hardware is fairly simple with few concerns. (This assumes that you are upgrading from 8.06+)
 1. Run the Setup.exe from the installation folder.
 2. Agree to EULA and when prompted if this is an upgrade, click Yes.
 3. Once completed, Caché should automatically start.
 4. Perform the Caché Memory Tuning settings as outlined in the Troubleshooting guide.
 5. Put the updated license files in the appropriate directories
 6. Restart Caché. If IM can be opened, Shut down IM first
 7. IM is now operational, but the upgrade is not complete.
 - Purge will be running a conversion (as required) that will take time depending on the size of your databases.
 8. An entry in the System Log is posted when the conversion is complete.
- Total upgrade time from start to operational, around 30 minutes to an hour. The background conversion depends entirely on how much data you are saving and can take up to several hours.

Upgrading IM

Core & Enhancement upgrade – New hardware (Only 8.06+)

- Upgrading onto new hardware often will take longer to perform the upgrade, as you must copy the Databases from the existing hardware.
- You must follow all the steps outlined in the Upgrade Manual to ensure the upgrade completes successfully. Failure to do so can cause failures and system instability.
- Additional Preparation steps for new hardware:
 - The newer version of Instrument Manager and Caché must be installed on the new hardware. (IM/Caché should be off)
 - Note: The config does not need to be loaded on the new system.
 - License files need to be loaded and ready beforehand.
 - Load all drivers that will be in use on the new system into the C:\Instrument Manager\Drivers\ directory and load into IM.
 - Performance tuning for the New hardware system should be done **prior** to the upgrade.
 - You must be able to copy the Database files from the old system to the new system. (These files can be fairly large.)

Upgrading IM

Core & Enhancement upgrade – New hardware

1. Make note of the IM version on the old system by looking at the file properties of the Instrument Manager.exe.
 - A. Do this by right-clicking on the Instrument Manager.exe file
 - B. Selecting file properties
 - C. Click on the Version tab
 - D. Copy the File Version that is displayed at the top of the Version tab.
 2. Make note of the IP address and Computer Name of the old system.
 3. Copy only the following database files (Caché.dat) from the old system to the new system Instrument Manager folder:
 - C:\Instrument Manager\databases\Globals
 - C:\Instrument Manager\databases\Drivers
 - C:\Instrument Manager\databases\MA
 - C:\Instrument Manager\databases\SEL
 - C:\Instrument Manager\databases\Archive
 - C:\Instrument Manager\databases\Temp2
- This can take a significant amount of time based on the file size!

Upgrading IM

Core & Enhancement upgrade – New hardware

4. Once the Databases are in place on the new system, there is a registry key that needs to be set with the version obtained in **Step 1**.

I. Open regedit on the new system.

II. Browse to the **UpgradeVersion** key.

▪ The location of the key depends on your operating system:

• On a 32-bit operating system:

HKEY_LOCAL_MACHINE/SOFTWARE/Data Innovations/Instrument Manager

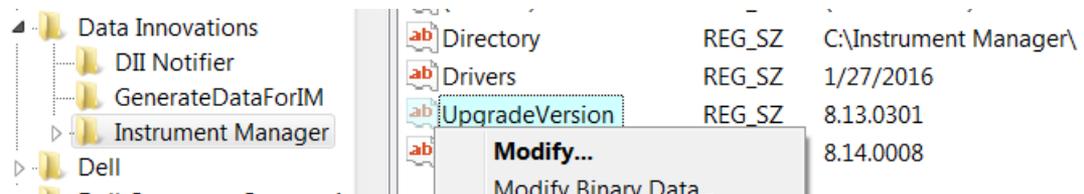
• On a 64-bit operating system:

HKEY_LOCAL_MACHINE/SOFTWARE/WOW6432Node/Data Innovations/Instrument Manager/

III. Modify the **UpgradeVersion** key to match OLD IM Version.

Example:

8.13.03 → 8.14.00



Upgrading IM

Core & Enhancement upgrade – New hardware

5. Replace Upgrade Database

- a. Copy the Caché.dat file from on the NEW system:
C:\Instrument Manager\Install Files\Databases\Upgrade\
b. Into the following path on the NEW system, replacing the existing Caché.dat file:
C:\Instrument Manager\Databases\Upgrade\

6. Shut Down the old hardware.

7. Change the Computer Name and IP address of the new hardware to match the old hardware. (This may require an OS reboot.)

8. Start Caché.

9. IM is now operational, but the upgrade is not complete.

- Purge will be running a conversion (as required) that will take time depending on the size of your databases.
- If you decided to update drivers during or after the upgrade and have not loaded the drivers prior to the DB copy, then you must load the drivers again after the upgrade.

10. An entry in the System Log is posted when the conversion is complete.

- Again, the Database copy from the old system to the new system will consume the greatest amount of time during the upgrade!

Upgrading IM

Upgrading Thin Clients

- Thin Clients must have the exact same version as is loaded on the Primary system that they are associated.
- Regardless of if you are applying a Patch or doing a Core upgrade of the IM system, the process for upgrading a Thin Client is the same.
 1. Ensure that IM has been upgraded on the Primary system.
 2. Ensure that the installation files are local to the Thin Client
 3. Run the Setup.exe from the installation folder.
 4. Agree to the EULA.
 5. When prompted if this is an upgrade, hit Yes.
 6. Upon completion, the Thin Client is upgraded and can be used for processing.
- Expected time to process per Thin Client: 5-10 minutes.

Upgrading IM

Upgrading a Shadow system – Report Server or Hot Backup

- Shadow systems must have the **exact same version** as is loaded on the Primary system that they are shadowing.
- You can upgrade the Shadow before or after the Primary, but you cannot start shadowing until both systems are on the same version.
- You should reconfigure Shadowing and re-sync the Primary and Shadow systems after the upgrade as outlined in the Hot Backup Users Guide.
- It is not advised to upgrade the Shadow, fail over to the Shadow, upgrade the Primary, then fail over back to the Primary. Doing this will cause data to be skipped/missed and won't reduce the downtime significantly.

Upgrading IM

Upgrading a Shadow system – Report Server or Hot Backup

- Regardless of if you are applying a Patch or doing a Core upgrade of the IM system, the process for upgrading a Shadow is the same.
 1. Run the Setup.exe from the installation folder.
 2. Agree to EULA and when prompted if this is an upgrade, hit Yes.
 3. Once completed, Caché should automatically start.
 4. Perform the Caché Memory Tuning settings as outlined in the Troubleshooting guide.
 5. Put the updated license files in the appropriate directories
 6. Restart Caché. If IM can be opened, Shut down IM first
 7. The Shadow is now upgraded, but not ready to shadow.
 8. After the Primary is Upgraded: Follow the steps in the Hot Backup Setup guide to re-sync and, if required, reconfigure the Shadow system to shadow.
- Expected time to Upgrade: 30 minutes + time to Re-Sync.
- Other than Step 8, all the Shadow Upgrade steps can be done regardless of the state of the Primary. (Down or during upgrade)

Upgrading IM

Final Steps

- If you're upgrading to 8.12 or higher, please take the time to update your Rules to use the newer rules engine instead of leaving your rules in "Legacy (Live)" mode.
 - The "Legacy (Live)" mode for rules do not benefit from the enhancements to the rules engine introduced in 8.12.
 - You are unable to edit anything in the "Legacy (Live)" rules set
- If you need to pause the SM Index conversion, say to load a global config, stop the Purge connection.
 - You should not leave Purge off for extended periods of time.
- Validation of the upgraded Version, Rules, Drivers, and System configuration is the responsibility of the site's system administrator.

Questions?

Last slide, please ask!