**:BOS3.0 Installation Steps :**

**Pre-Requisite:**

Below are required files before proceeding BOS3.0 installation:

*Files are available on,*

*S: Drive : S:\HO\Dept\IS\USit\QA Team\BOS 3.0*

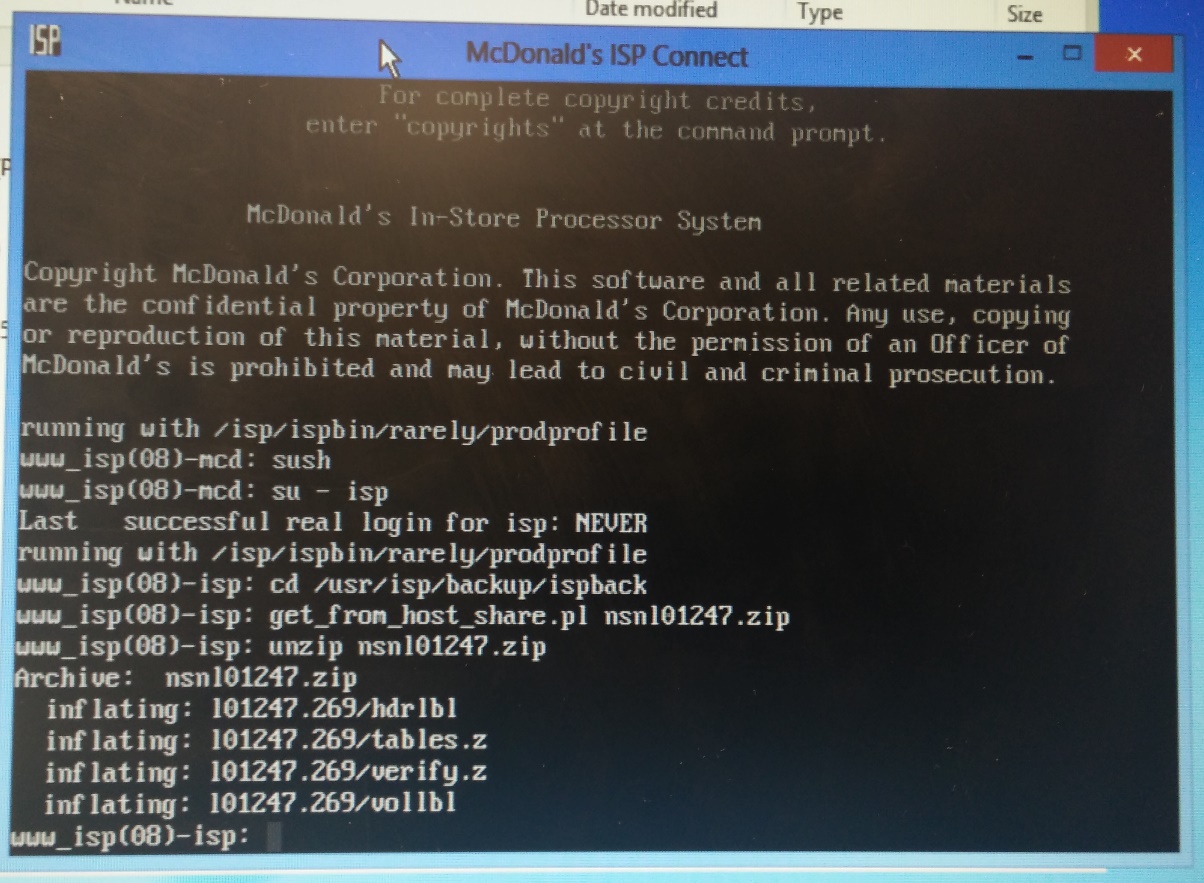
***SharePoint****:* [*https://spo.mcd.com/sites/us\_natl\_it\_rest\_sol\_qa/team/QA%20Library/BOS3.0*](https://spo.mcd.com/sites/us_natl_it_rest_sol_qa/team/QA%20Library/BOS3.0)

1. Domainparms
2. BOS2.2 Store Data
3. Config File
4. Public Key
5. Step2-MSI

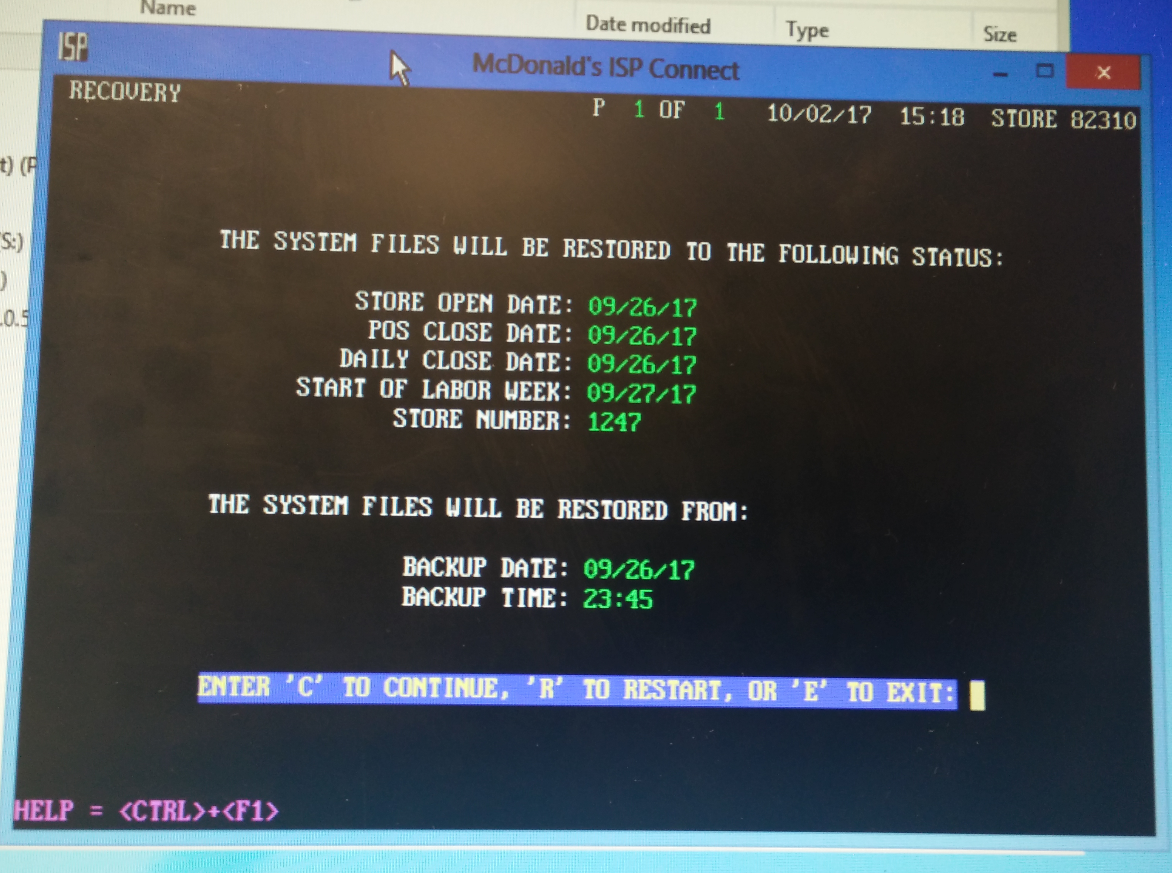
**Lab should be on 10.116.x.y subnet.**

**Steps:**

1. Restage the BOS to the latest BOS 2.2 build 13 (110602.13)
2. Set QA flag.
3. Recover the data (nsnl01247).
   * **Following are the steps for the recovery:**
     1. Copy the zip file (such as nsnl01247.zip) to C:\ISPCONFIG
     2. Go to F8 session (Press Alt + F8)
     3. Login: mcd
     4. Password: Use MCD password for the month
     5. At the prompt enter **sush –c “su – isp”** to become super user.
     6. Enter **cd /usr/isp/backup/ispback**
     7. Enter **get\_from\_host\_share.pl nsnl01247.zip**
     8. Enter **unzip nsnl01247.zip** (Zip files will be unzipped for example as l01247.269)



* + 1. Keep any backup CD in BOS server and enter “Recovery” in ISP. It will recover the data from the file that we have unzipped.



1. Now run “Internet Setup” (say no to reboot here) and “Store ID” to match the current Store Number, which requires a reboot. After it comes up, it should have the correct store number and network IPs, double check the network IPs under Control Panel.

**Ad Join:**

1. IF Lab is already in NAR Domain skip to E\*REST Step.
2. Navigate to c:\ispconfig folder on BOS server. Check if ‘domainparms’ file for NAR domain exists on this folder. If not,
   * Copy “Domainparms” file from S:\HO\Dept\IS\USit\QA Team\BOS 3.0 and keep in c: \ispconfig in BOS server.
   * Create POS\_Close flag on C:\ispconfig folder to consume the domainparms file.
   * System should be rebooted and apply the changes
   * After reboot verify that domain should change to “nar.na.mcdrest”

**E\*REST:**

1. Next step is to check make the store as eRest:
2. Enter command ‘E\*REST’ on ISP F8 session to validate if the store is already E\*Rest activated, If Store is not erest activated use the following commands to make it erest activated:
3. E\*Rest Activation
4. Press Alt+F8 to go to the Unix section
5. Login : mcd
6. Password: Enter monthly password
7. Enter: Sush
8. Enter: Su – isp
9. Enter: isp\_crypt –o –e ERA
10. Enter: isp\_crypt –m –e ERA
11. Navigate to F1 session and Type ‘E\*Rest’ and verify that it says E\*Restraurant is active, if it Prompts to ‘Activate the E\*Labor and E\*HR Modules (Y/N)?’ respond with ‘Y’. It will prompt to Enter ‘Yes’ or ‘ No’ : Say ‘YES’ and Hit enter.

***Processing the eREST112 file on the ISP : We will skip this step during this installation.***

***We can process this file later. I will update this section once we receive eREST file and process at onsite lab.***

1. *Login to BOS with User as “ support” and Password “newpos6”*
2. *Place the “er\_mdm\_12089\_2012-12-06.tar.Z “file in \\10.0.0.24\ccard location on BOS.*

*(Common file for all the stores, copy from flash drive)*

1. *Go to F8 session on the ISP and run the commands as below:*
2. *Press Alt+F8 at same time ( Unix section should be displayed)*
3. *Login : mcd*
4. *Password: Enter monthly password*
5. *Sush*
6. *Su – isp*
7. *Run the command on F8 session on ISP :*

*zcat /usr/ccard/tmp/er\_mdm\_12089\_2012-12-06.tar.Z | tar xvf – ( After Z space | space tar xvf space -)*

1. *File should be processed*
2. *If user wants to go back then press Alt+ F1 at same time*

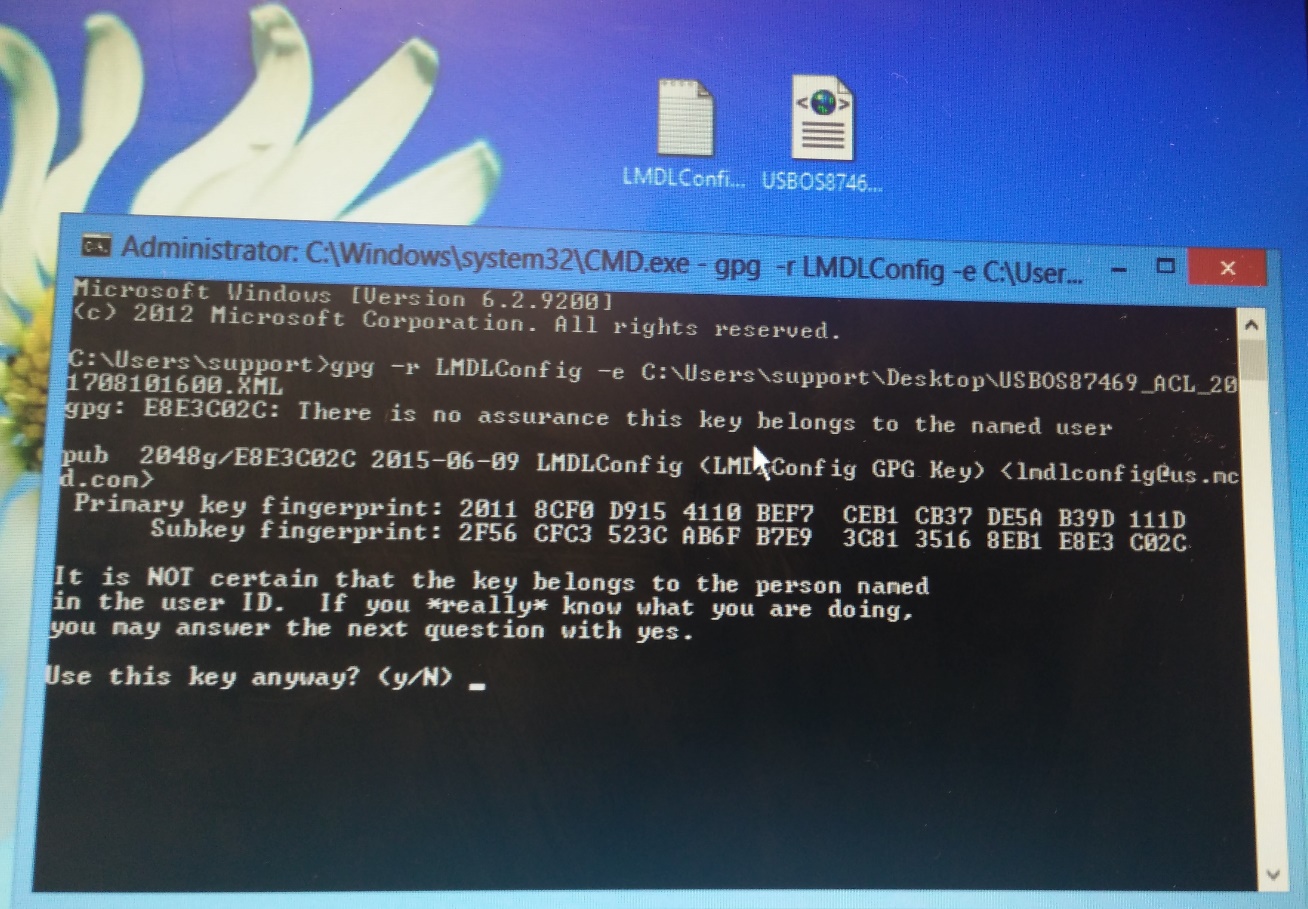
*Note: If already processed above file earlier then no need to process same file once again, we can skip this file process and directly we will process eREST file which I have mentioned in below steps for eREST file.*

1. *Login to BOS with User as “ support” and Password “newpos6”*
2. *Place the erest112 file in \\10.0.0.24\ccard location on BOS. ( File should be like this format “EREST2MCD\_0000055\_0000020822.dat “ ) and for eREST file we need to send mail to Alta team (*[*mcdsupport@altametrics.com*](mailto:mcdsupport@altametrics.com)*;* [*alta\_mcd\_timekeeping@altametrics.com*](mailto:alta_mcd_timekeeping@altametrics.com) *)*
3. *Go to F8 session on the ISP and run the commands as below:*
4. *Press Alt+F8 at same time ( Unix section should be displayed)*
5. *Login : mcd*
6. *Password: Enter monthly password*
7. *Sush*
8. *Su – isp*
9. *load\_tmprecv.sh EREST2MCD\_0000055\_0000020822.dat ( Enter load\_tmprecv.sh and then enter eREST file name which we are received from “Alta” team, file name should be different for each store)*
10. *Enter Yes and then press enter button*
11. *eREST file should be processed.*

**Process Config File:**

1. Next Step is to process Config file. Config file is available at location: S:\HO\Dept\IS\USit\QA Team\BOS 3.0\Config file\USBOS87469\_ACL\_201708101600.xml. (This file is decrypted), Copy this file to BOS desktop.
2. For encrypting the config file, change the store ID (NSN filed in file) to match the current store, then run the following command to encrypt it, goto command prompt:

gpg –r LMDLConfig -e USBOS87469\_ACL\_201708101600.XML (drag and drop this file from desktop)

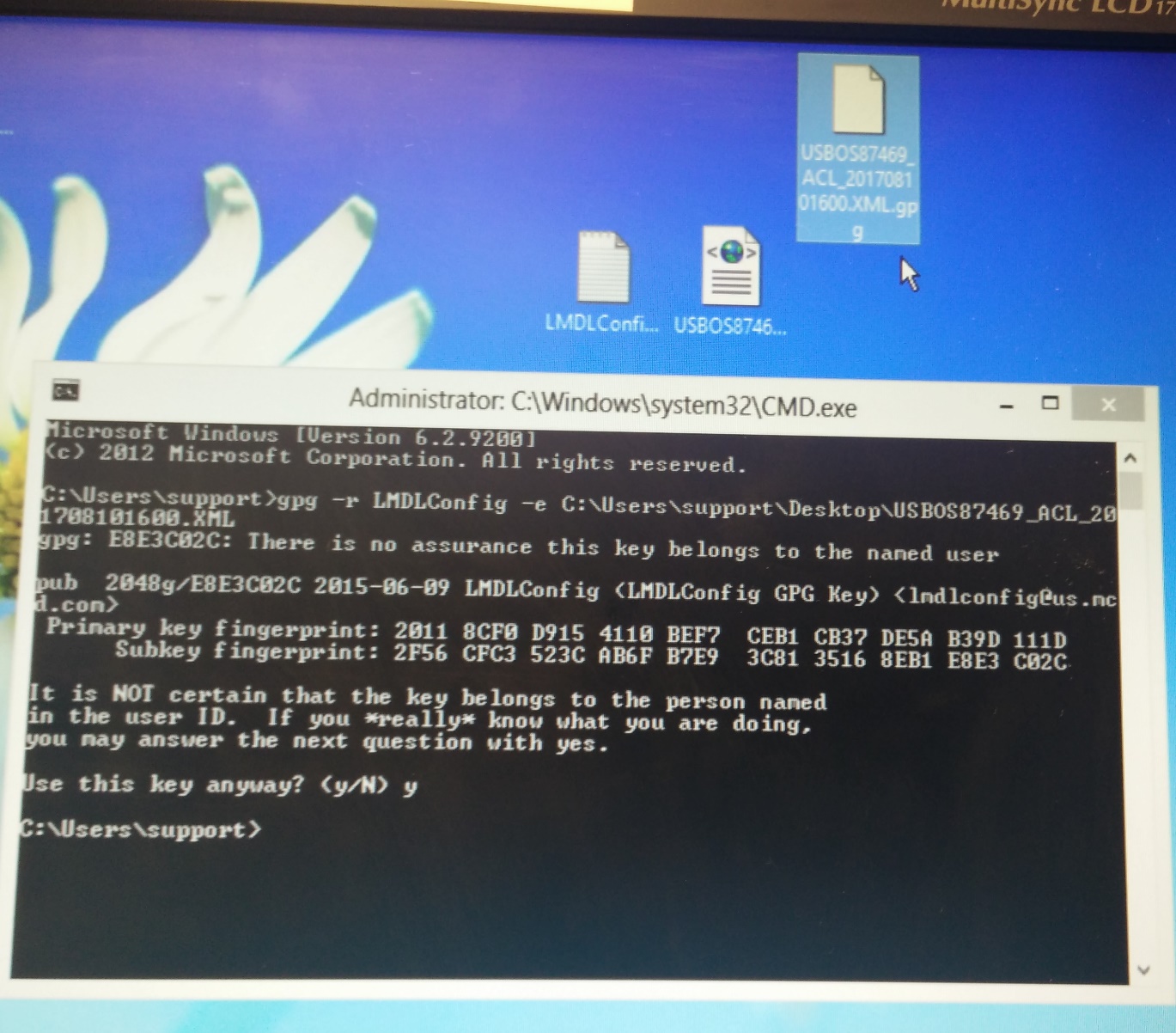


1. If it does not work and says, “Public key not found”. Need to import the public key (copy it onto the desktop) using the following command:

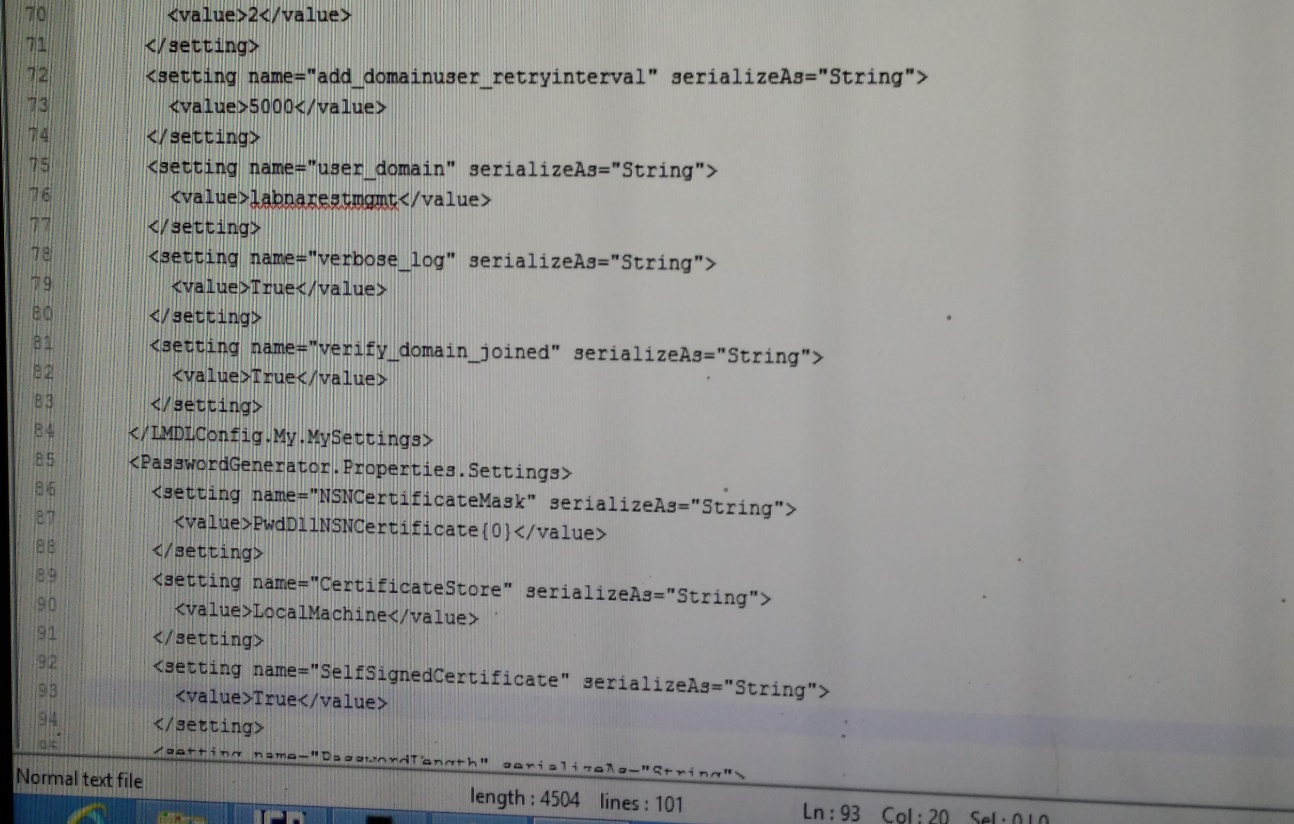
gpg --import <public key> (drag and drop this file from desktop)

Then try Step : 9.

1. Answer ‘y’ to the message prompt and there will be an encrypted file ready to go on the desktop. (To verify that file is encrypted, open the file and you will not able to see any content within that file)



1. Rename the file that is created after encrypting, match it with your store ID and current date (like USBOS81247\_ACL\_201708101600.xml), so that it will be easy to identify and process. Have the encrypted Config file ready on the desktop.
2. Now run the ‘Launch MSI.bat’ (available under “S:\HO\Dept\IS\USit\QA Team\BOS 3.0\ISP - SS6.5 2016 BOS 2012 Release 3.0 - Build 110700.26D**\Step 2 – MSI”)**.
3. Open location C:\ISPCONFIG\RDM\TOISP folder and verify two tar files gets generated there after running the BOS 3.0 MSI, now copy the encrypted Config file from the desktop into the same TOISP folder. All these files will consumed after around 30-40 minutes.
   * If Files were not consumed,
     1. Make sure that lab is adjoined. ( Domain should be **nar.na.mcdrest**)
     2. Open windows explorer on BOS server.
     3. Navigate to C:\Program Files\McDonalds\LMDL\lmdl folder.
     4. Edit file LMDLConfig.exe.config.
     5. Change values for parameter ‘User\_Domain’ to ‘labnarestmgmt’
     6. Verbose\_log to ‘True’.
     7. ‘SelfSignedCertificate’ to ‘True’.



1. After these files consumed, there will be an upgrade ready flag created under /tmp directory. Goto ISP Alt+F8 session -> cd /tmp -> ls –la lmdl\*. This will show the flag UPG\_READY, which means that the store is ready for BOS 3.0 upgrade. Please find the screenshots for this step in the same folder where this doc is.
2. Now do “Store Opening” from ISP, for the BOS 3.0 upgrade to kick off. It will reboot the machine in between. After reboot wait for 10-15 min before login.
3. Once BOS 3.0 Upgrade is successfully performed. Need to use ISPADMIN (This application called as ISP Impersonate application) to log into ISP, and then press F9 on ISP window.
   * To Login to ISP :
     1. Click on Start.
     2. Type ‘ISPADMIN’ and Hit enter to launch it.
     3. Select any user and click on ‘Logon’ button. (There are chances that not all the users will work, as we did not processed eRESt file. Mostly above store user will work here. i.e users starting from ef / od / fe)
     4. Select ISP window and hit ‘F9’ button to login.

**To retrieve POS Users : (To login to Registers)**

Login to F8 session:

Login to super user: Sush

Enter: su - isp

Enter: cd $t

Enter : Idump -d tbemppxrf

Try combination of First 3 digits as user name and after Pipe symbol first 3 digits as password.