Linux on Z and Crypto Express Cards

Andy Hartman, Senior Consultant
andy.hartman@mainline.com
440.785.4890

The Technology Partner for Business Results

Mainline® INFORMATION SYSTEMS

Agenda

- What is Pervasive Encryption , CPACF and Crypto Express Cards
  - How to Implement Crypto Express Cards with Linux on z
    - Configure Crypto Express as an Accelerator
    - Configure z/VM to use the Crypto Express Cards
    - Configure Linux Guests to use the Crypto Express Cards
  - How to Measure Crypto Express Usage
    - From Linux
    - From the HMC
- Demo
  - Show processing offloaded by using the Crypto Cards
- Q&A

What Is Pervasive Encryption

- IBM Pervasive Encryption for Linux on IBM z covers several areas
- Data in Flight – SSL/TLS communications to and from the Linux system are encrypted
- Data at Rest – Partitions and File Systems can be encrypted so they cannot be used except when opened with the correct security key
- Secure Service Containers (SSC) - This allows a special LPAR to run that has been hardened and prevents access except through approved API's and secures data in flight , data at rest and provides for a secure boot process, signed images , encrypted dumps etc.
- There are several Hyper Protect offerings available that take advantage of the SSC technology

Crypto Express Cards And CPACF

- CPACF (CP Assist for Cryptographic Functions) are a set of instructions and a coprocessor on each IFL or GP processor used to process cryptographic requests
- No charge feature code 3863 is required to be activated
- Automatically virtualized and shared across all LPARs
- Scales as you grow, add more IFLs , you get more CPACF's
- Supports encryption and decryption using AES,TDES and DES for example as well as supporting SHA
- Provides very fast symmetric cryptographic functions
- Provides protected keys for encryption and decryption
- Provides the encryption and decryption of data at rest and z/VM encrypted paging

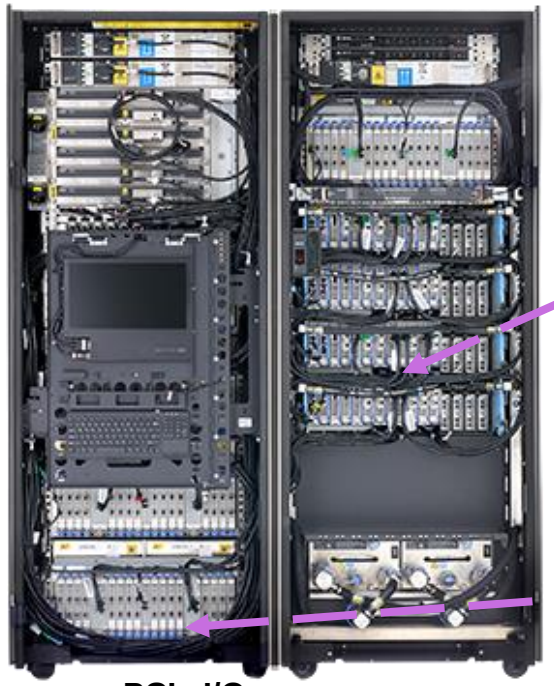
Crypto Express Cards And CPACF

- Crypto Express Cards are physical PCIe I/O cards that provide various cryptographic functions
- Up to 30 2 port cards can be configured on one z15 T01 / Minimum of 2 initially / 1 or more after initial order – Up to 20 2 port cards for a z15 T02 / Up to 16 1 port features can be supported on a z15/T01 or T02
- Each card supports either 40 or 85 domains depending on if it's installed on z15 T02 or z15 T01
- Domains are assigned to LPARs / All active LPARs must have unique domain assignments
- Crypto Express Cards provide offloading of certain cryptographic functions reducing CPU utilization
  - Secure IBM Common Cryptographic Architecture (CCA) coprocessor – provides FIPS 140-2 Level 4 certification – Used for secure key functions
  - Secure IBM Enterprise PKCS #11 Coprocessor – used to meet different industry requirements – Requires a TKE Workstation
  - Accelerator – used for public key and private key cryptography – Used in SSL/TLS processing

Crypto Express Cards And CPACF

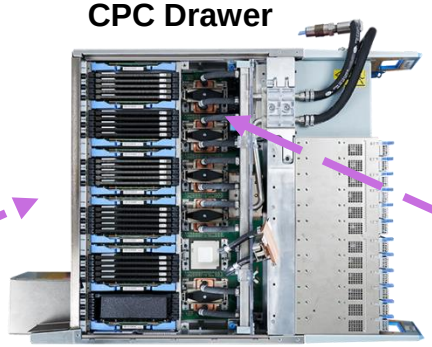
- Multiple cards may be required depending on your configuration
  - Performance
  - Multiple Accelerators and Coprocessors for redundancy or separation of workloads
  - When used as CCA coprocessors for encrypting data at rest domains need to be dedicated to a z/VM guests , Linux or KVM LPARs
- Crypto Express Cards provide hardware security module (HSM) which is a tamper resistant/responding repository for various types of master keys used for encryption and decryption
- Crypto express cards require that the Central Processor Assist for Cryptographic Function (CPACF) be enabled on your IBM z (this is a feature that is ordered with your system)

What are Crypto Express Cards

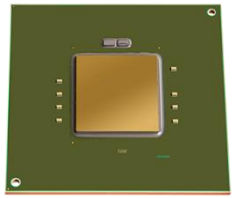


PCIe I/O Drawers

CPC Drawer



PU SCM
Each PU is capable of CPACF function



Crypto Express6S

TKE is required for management of Crypto Express6S in EP11 mode

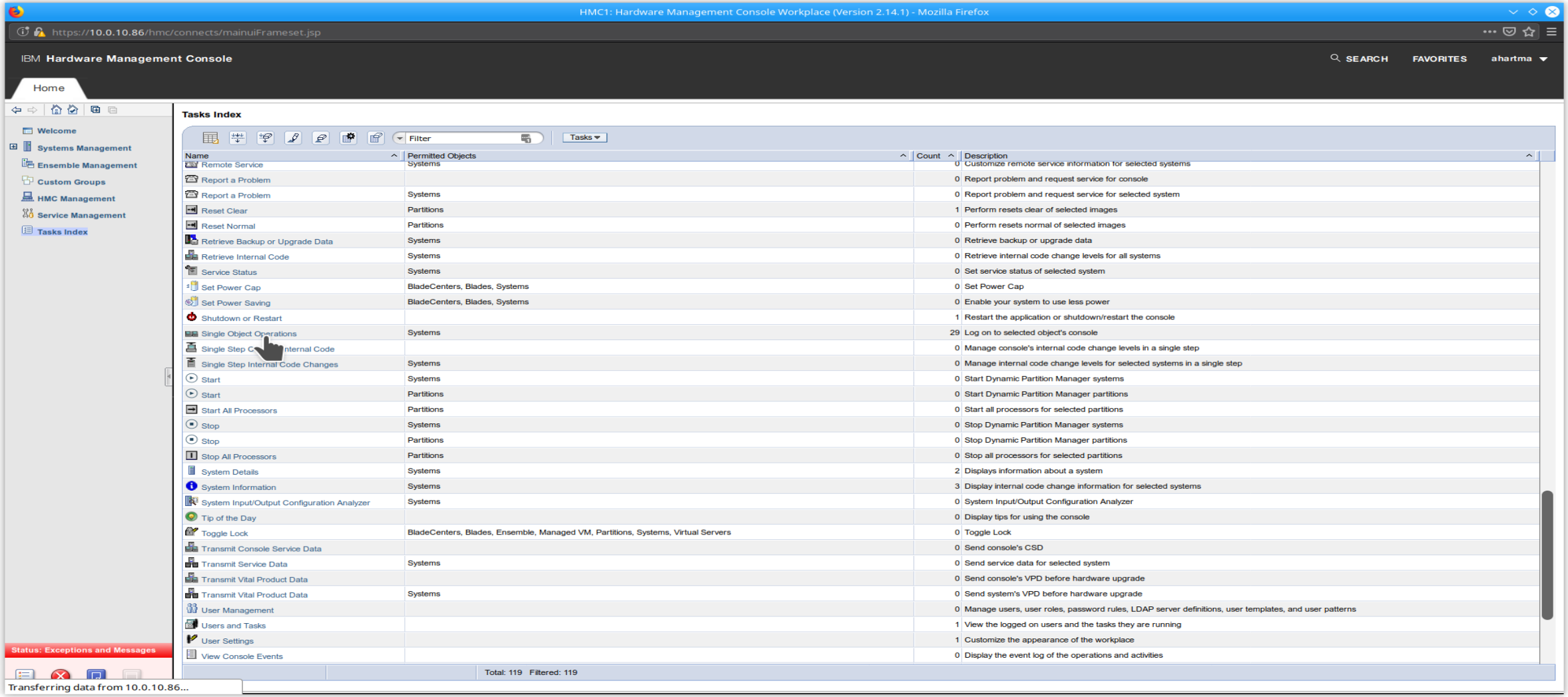
Trusted Key Entry (TKE)

Smart Cards

Smart Card Readers

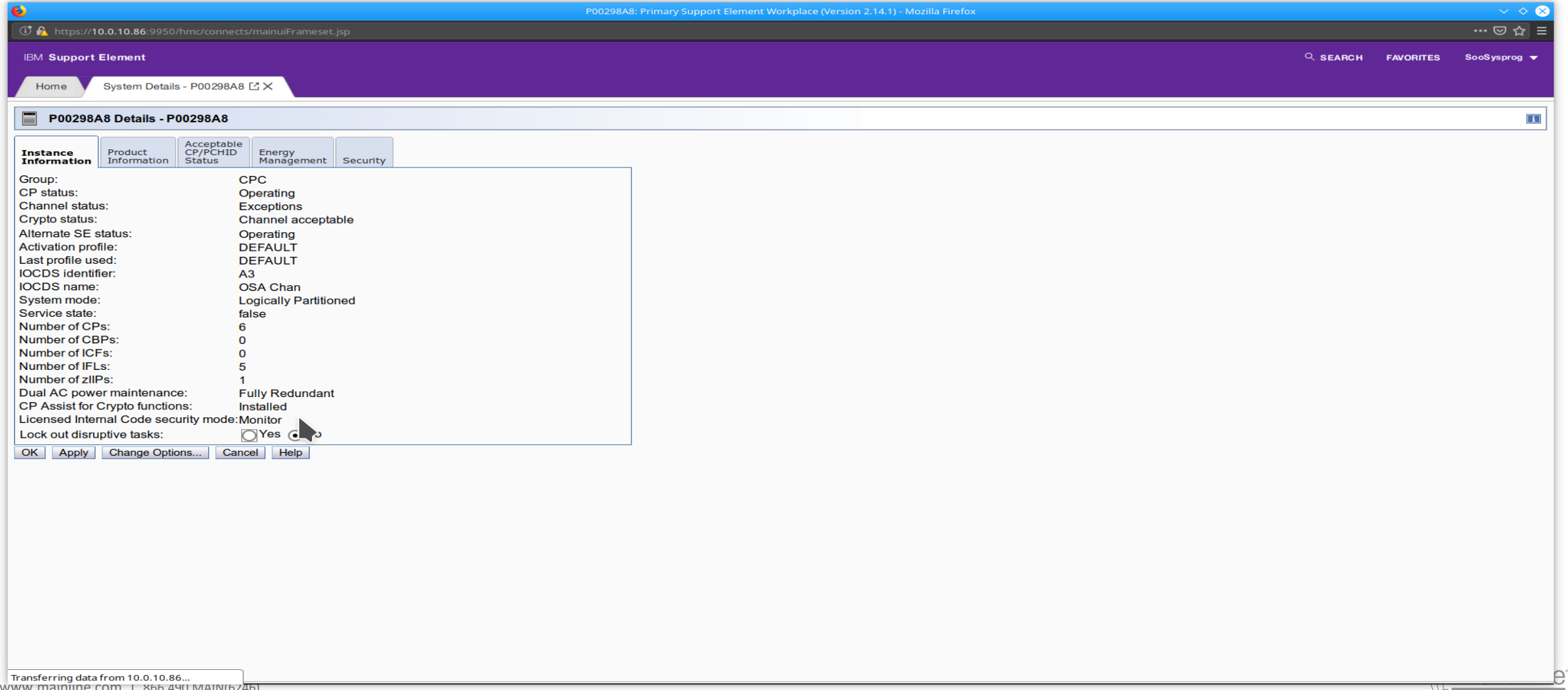
How to Implement Crypto Express Cards with Linux on z

- Sign into the Support Element from the HMC – Single Object Operations
- HMC / Tasks Index / Single Object Operations



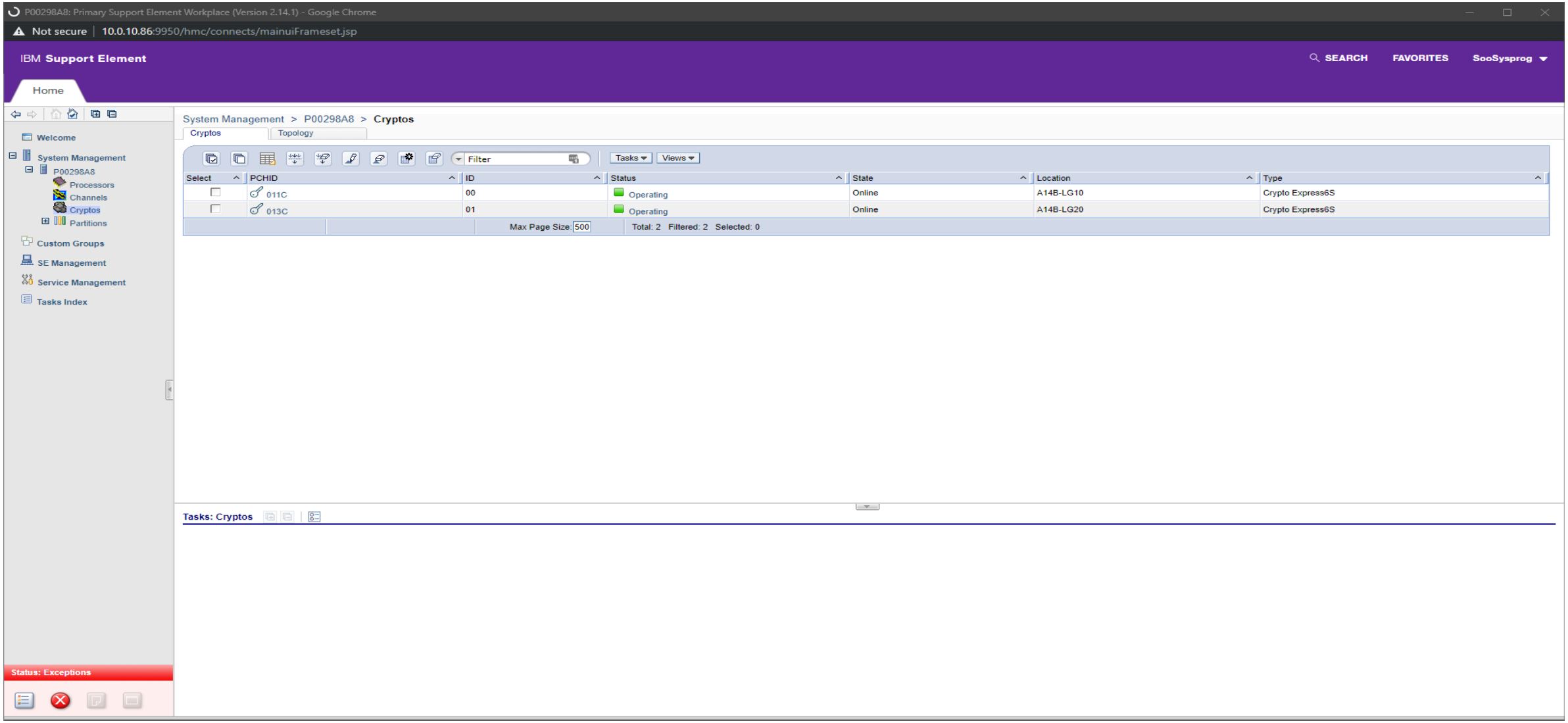
How to Implement Crypto Express Cards with Linux on z

- Check that the CPACF feature is enabled on your processor
- Click on System Management / CPU Serial No. / System Details at the bottom



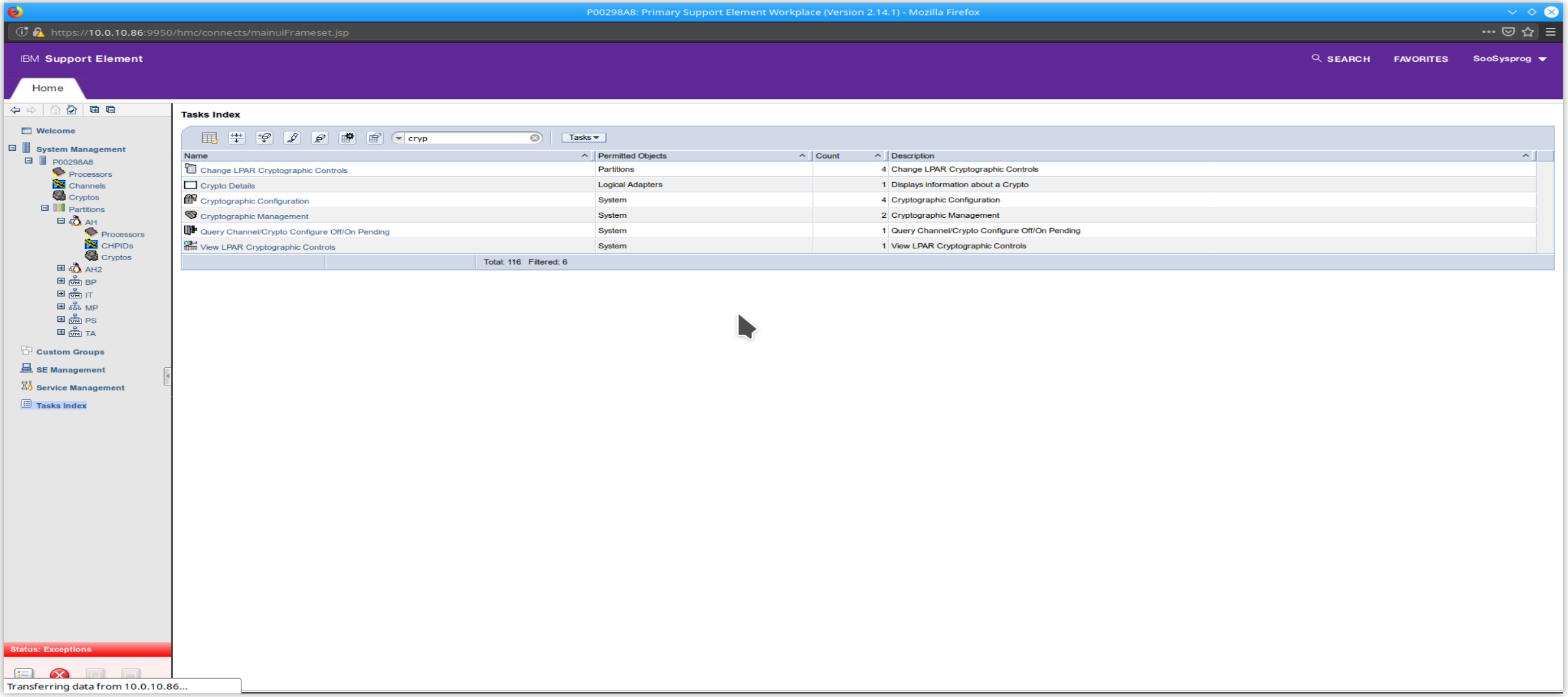
How to Implement Crypto Express Cards with Linux on z

- Support Element / Cryptos



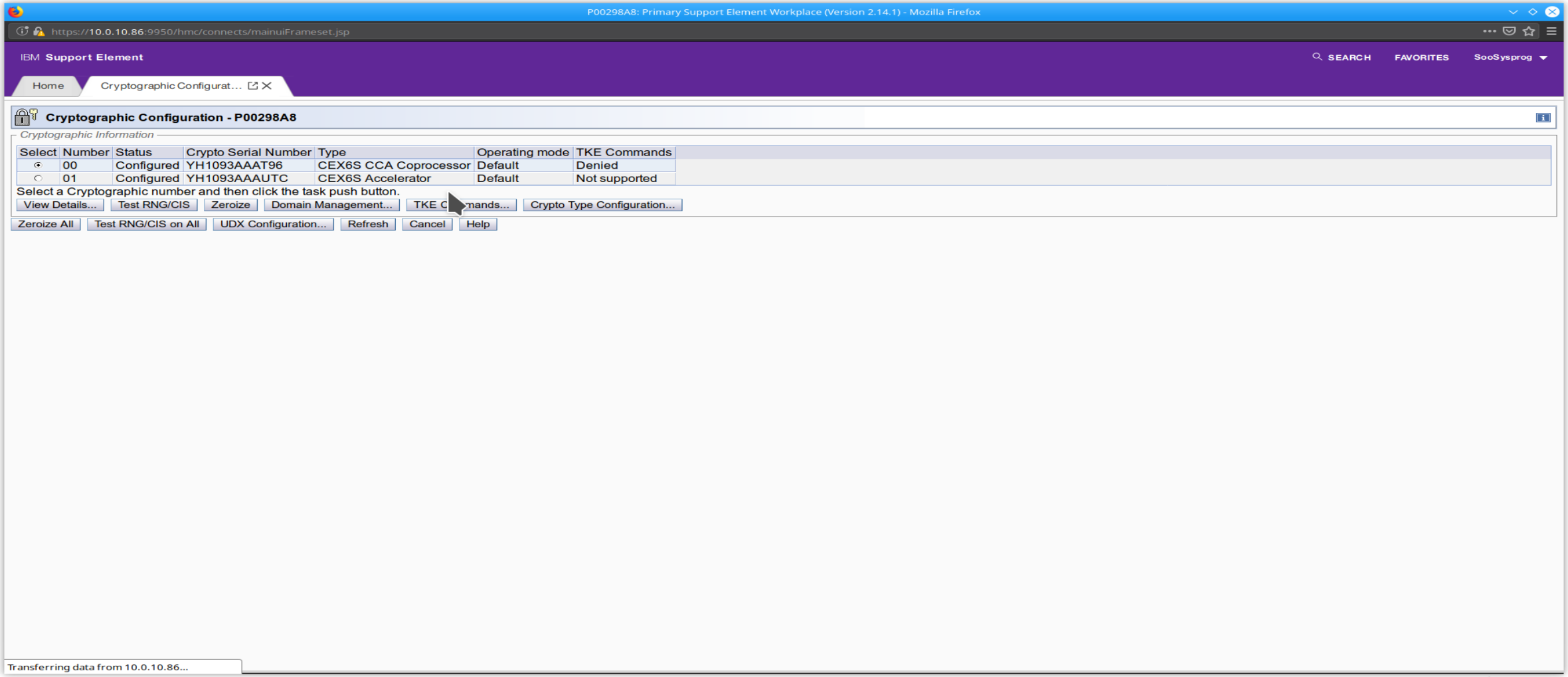
How to Implement Crypto Express Cards with Linux on z

- Support Element / Tasks Index / Filter 'crypt'



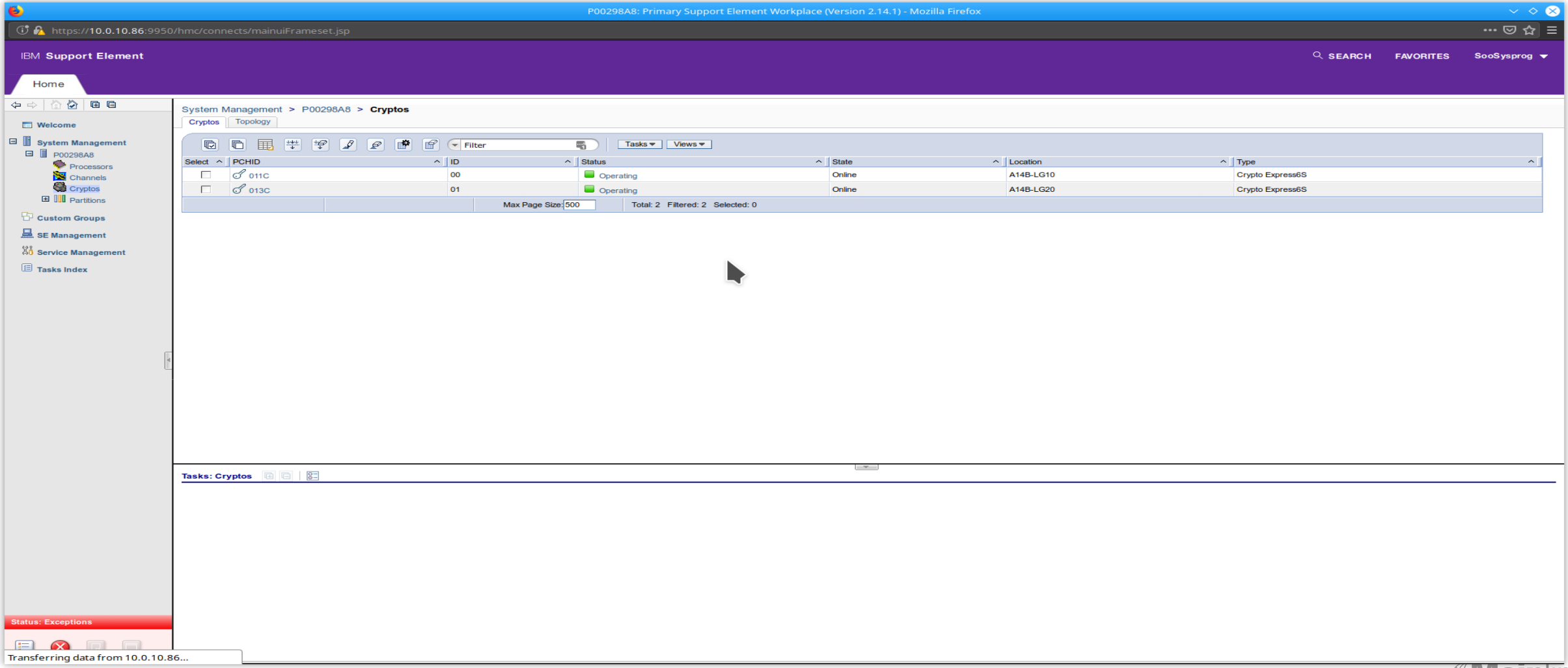
How to Implement Crypto Express Cards with Linux on z

- Click on Crypto Configuration / Review the Crypto Type / Note the Crypto Type Configuration
- Cancel to return to the Tasks Index



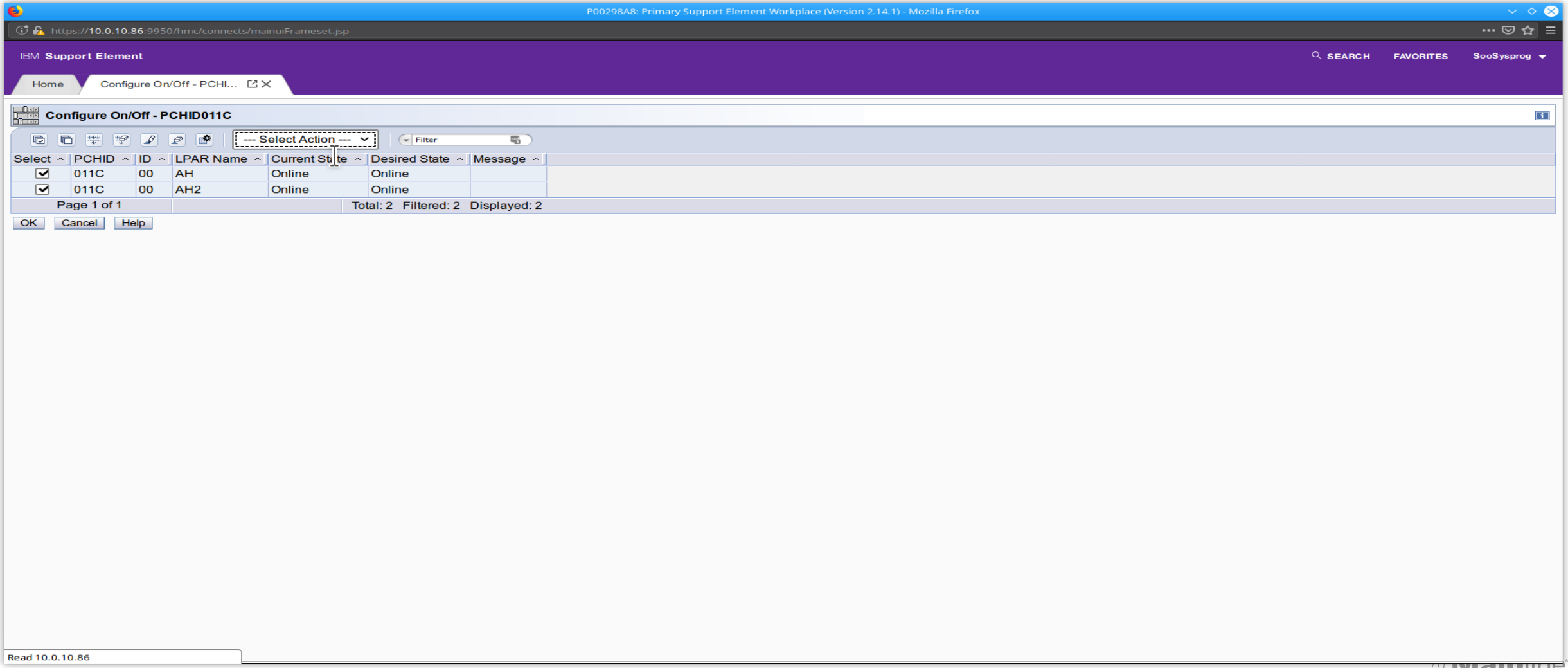
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos
- PCHID's need to be in Standby to change from CCA to Accelerator Mode



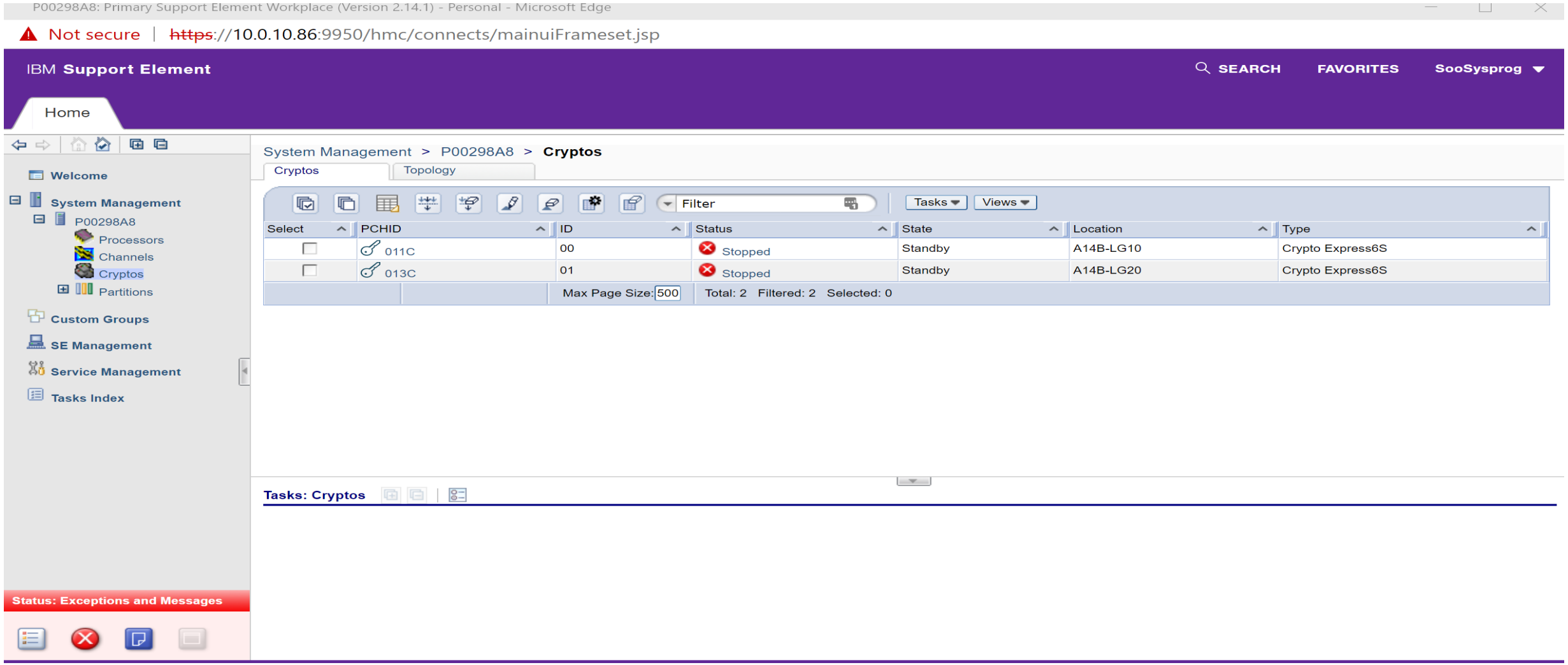
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos / Select the Cards / Configure On/Off
- Select Actions / Select All / Select Toggle All Standby



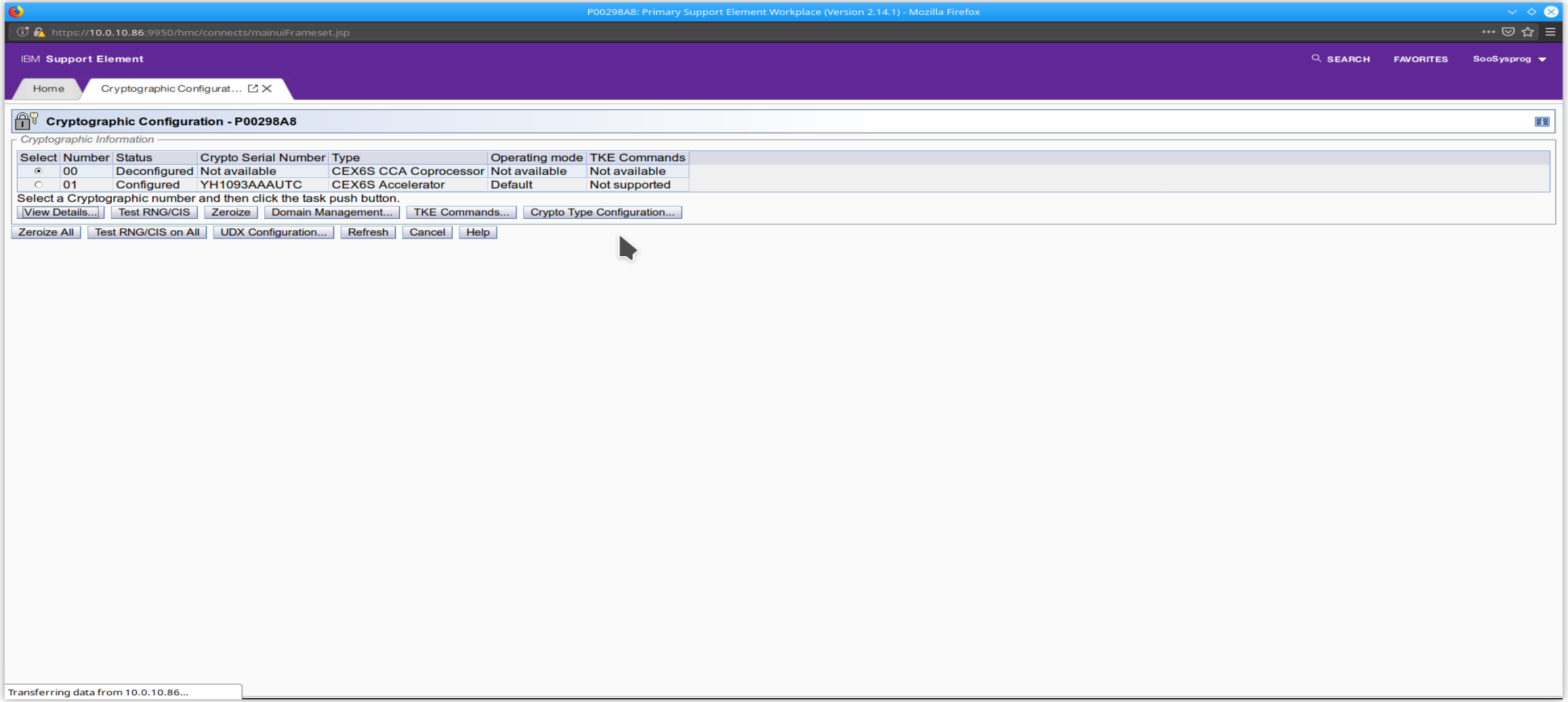
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos / Configure On/Off
- PCHID shows Stopped – Remember this is disruptive to anyone using this card/cards



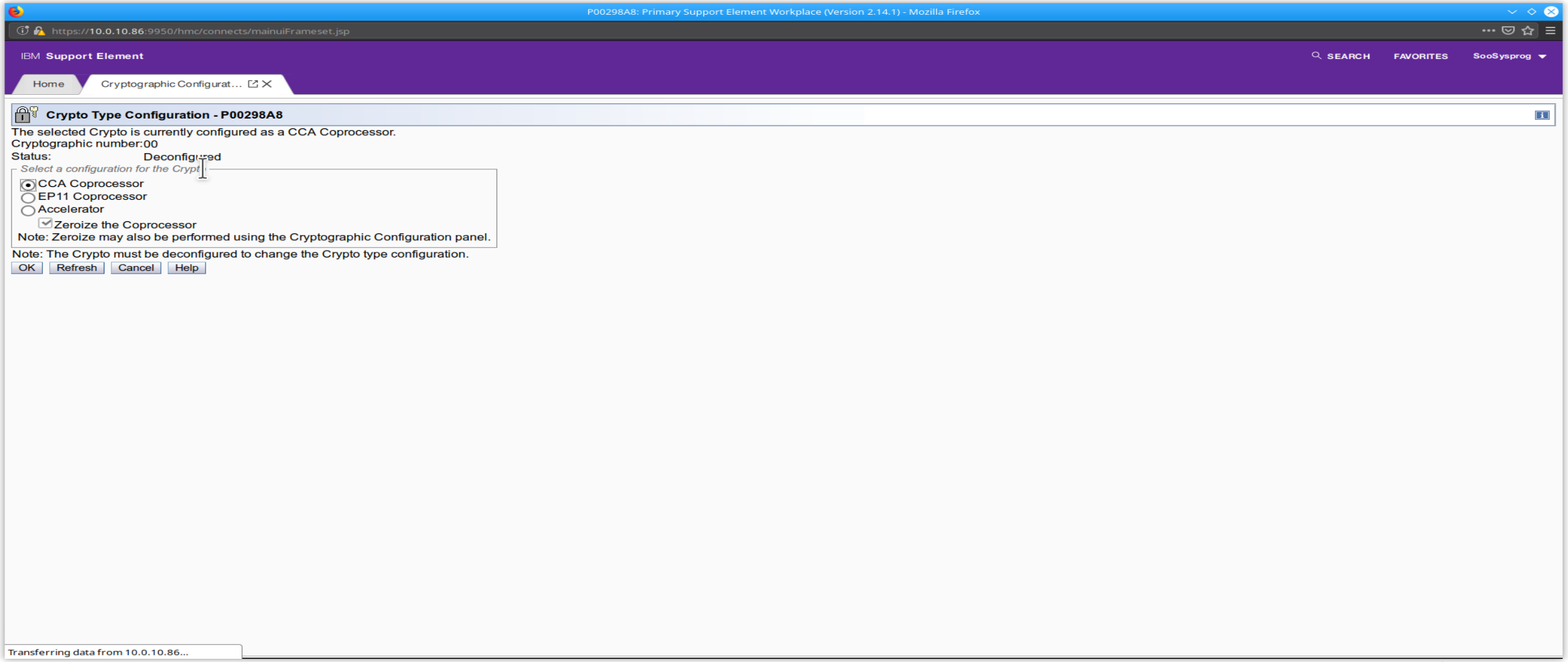
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Crypto Configuration
- Card Number shows Deconfigured – Remember this is disruptive to anyone using this card



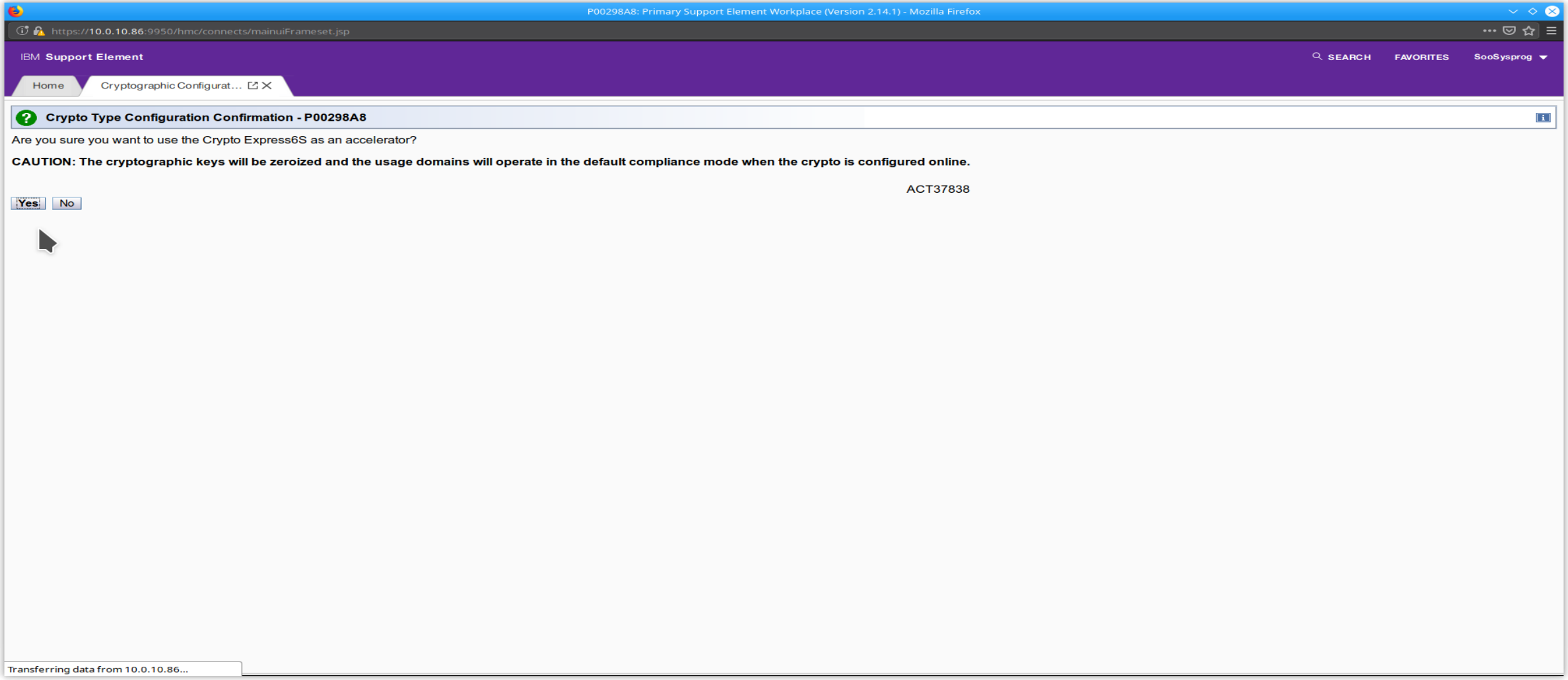
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Crypto Configuration
- Select Accelerator / Uncheck or check the Zeroize the Coprocessor



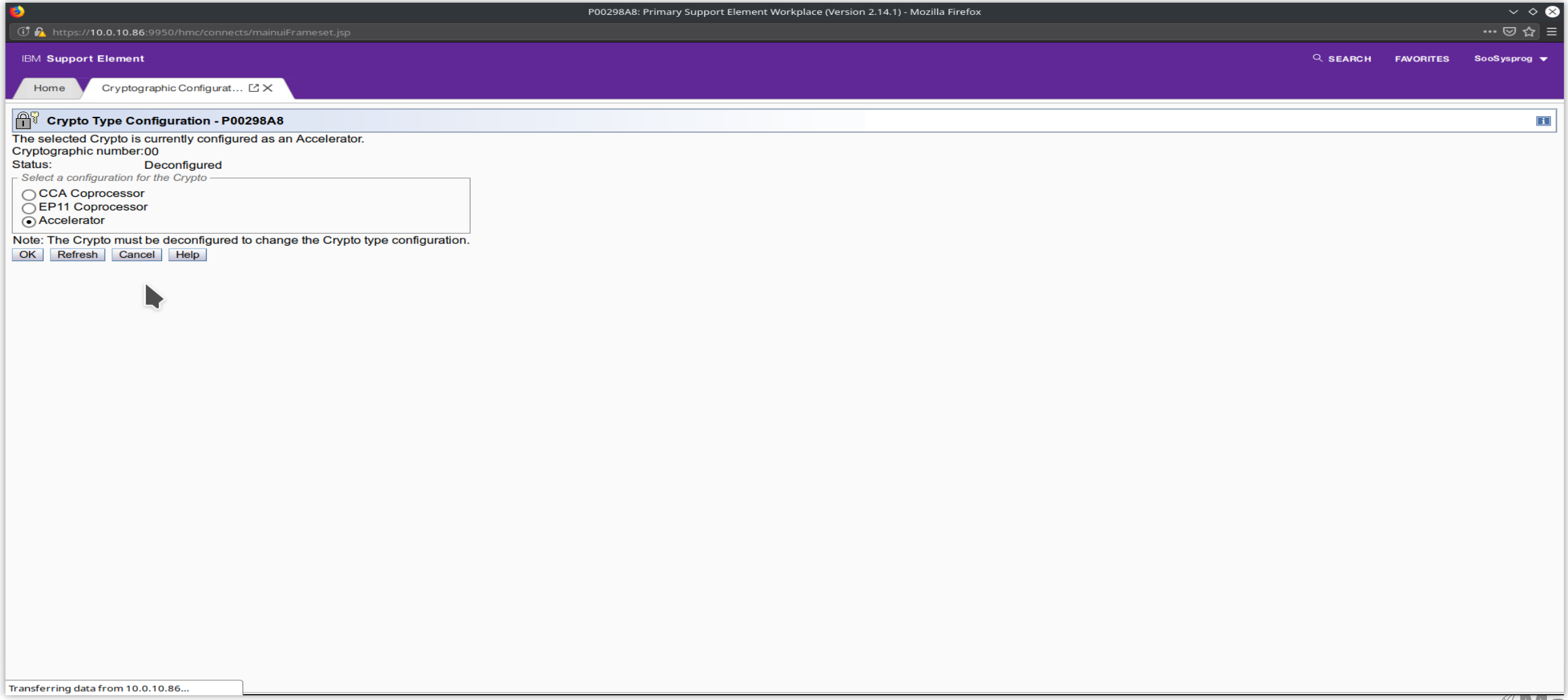
How to Implement Crypto Express Cards with Linux on z

- Select Accelerator / Then select Yes on the screen below /
- This will wipe out any keys you have stored on this card – make sure you select the correct card
- If you unchecked the zeroized box then the keys will NOT be removed



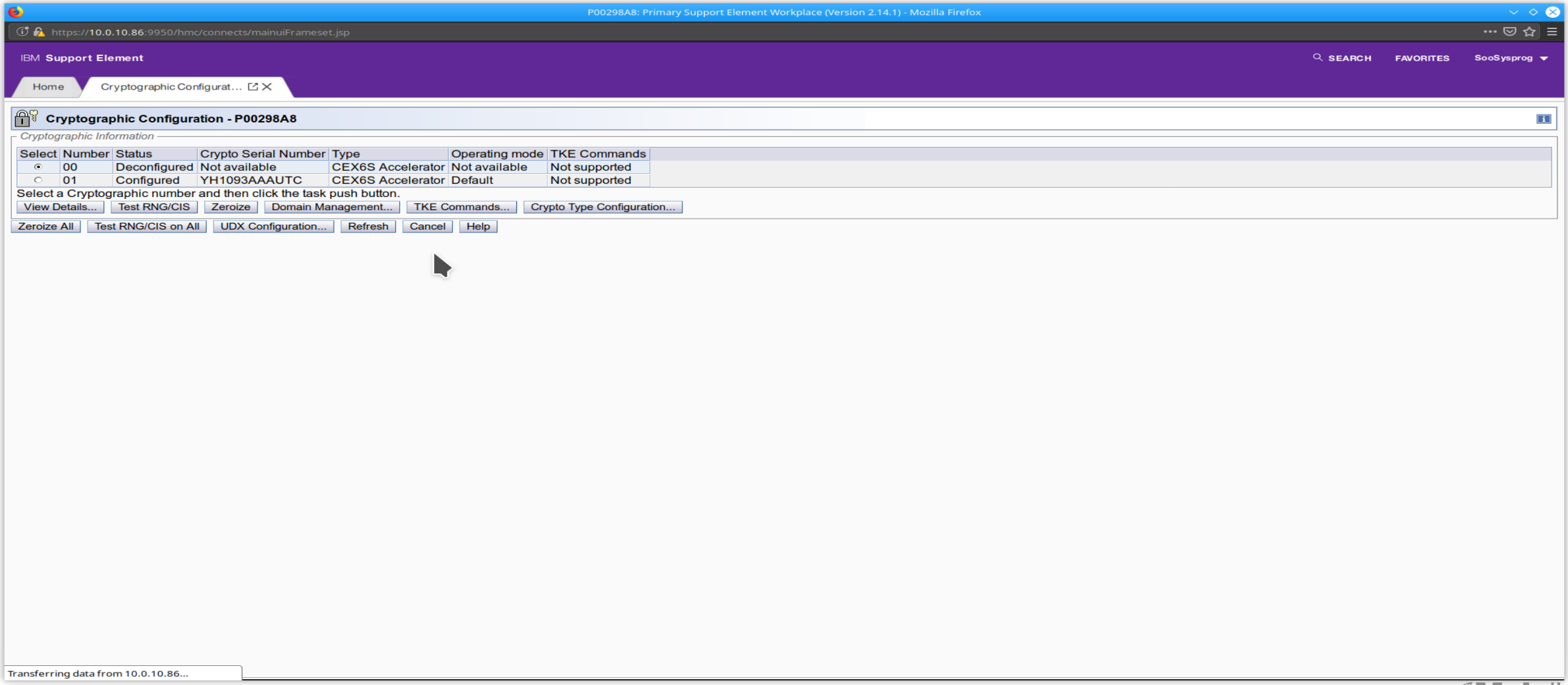
How to Implement Crypto Express Cards with Linux on z

- This shows the card has been changed to an Accelerator
- Select Cancel to return to the Crypto Configuration Screen / Select Cancel or close the tab



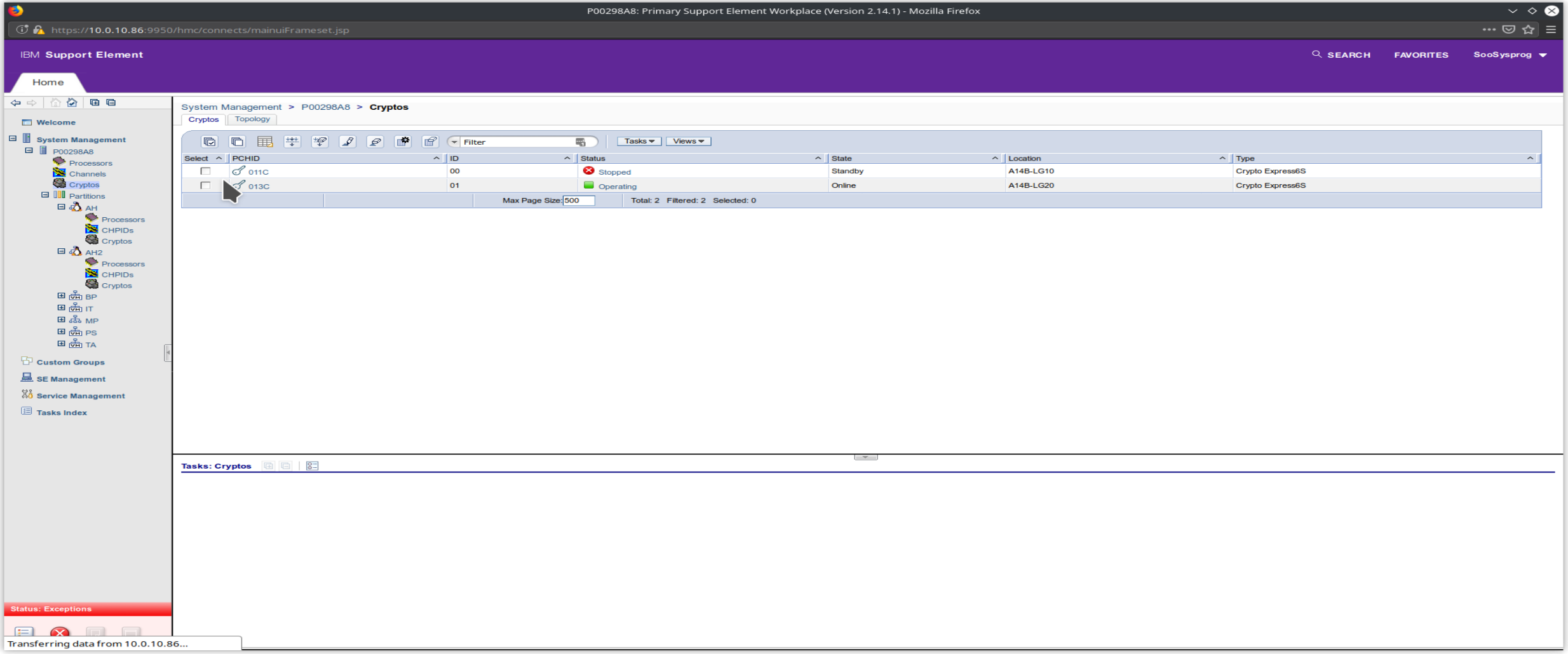
How to Implement Crypto Express Cards with Linux on z

- This shows the card has been changed to an Accelerator
- Select Cancel to return to the Tasks Index or Close the Crypto Config tab



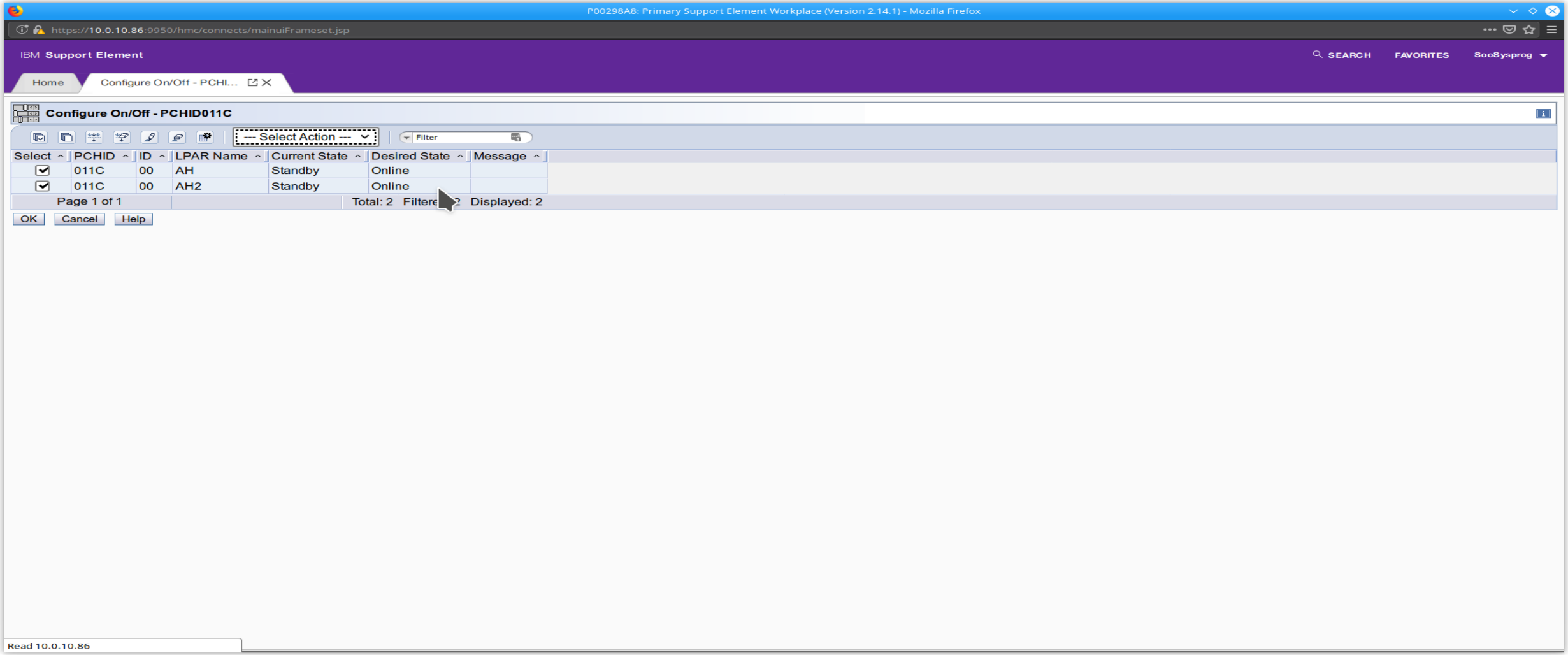
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos
- PCHID will show as stopped/standby - Select the PCHID / Tasks / Channel Operations / Configure On/Off



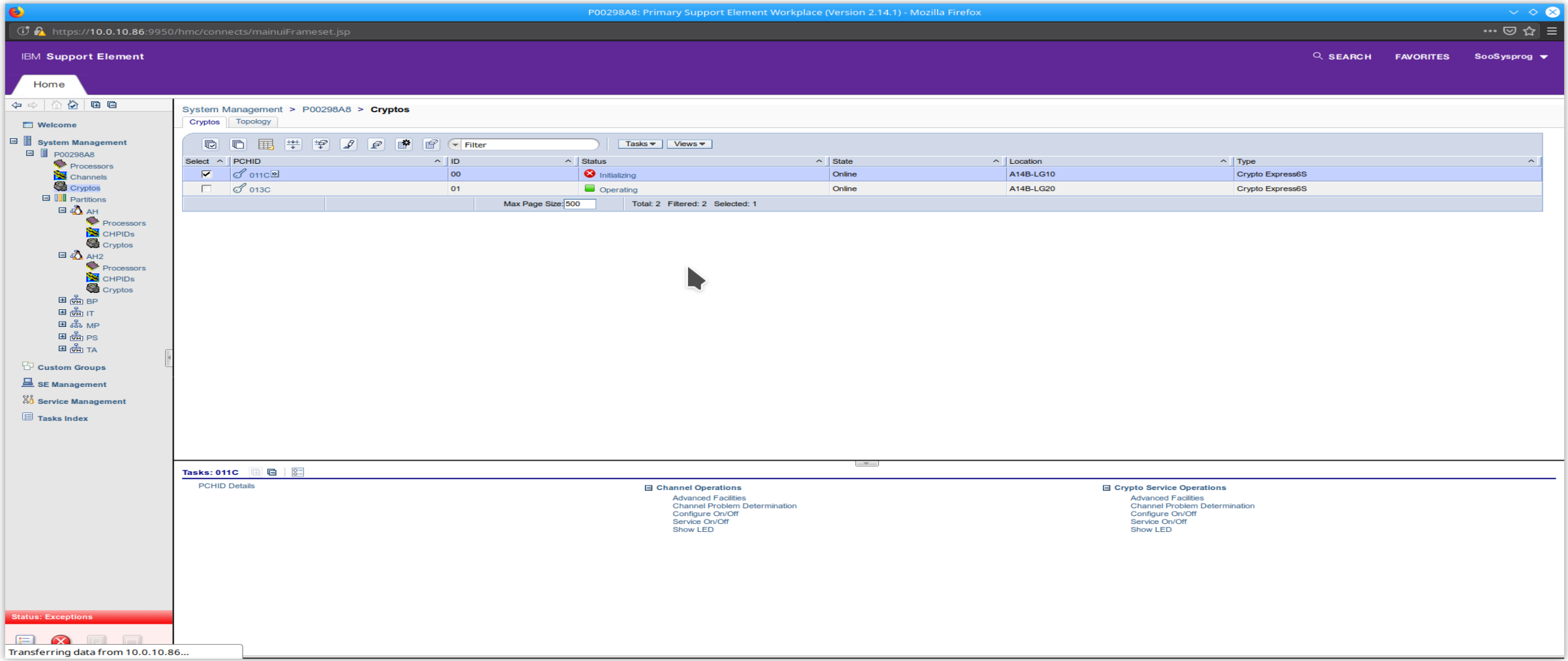
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos / Configure On/Off
- Select Action – Toggle All Online / Press Ok



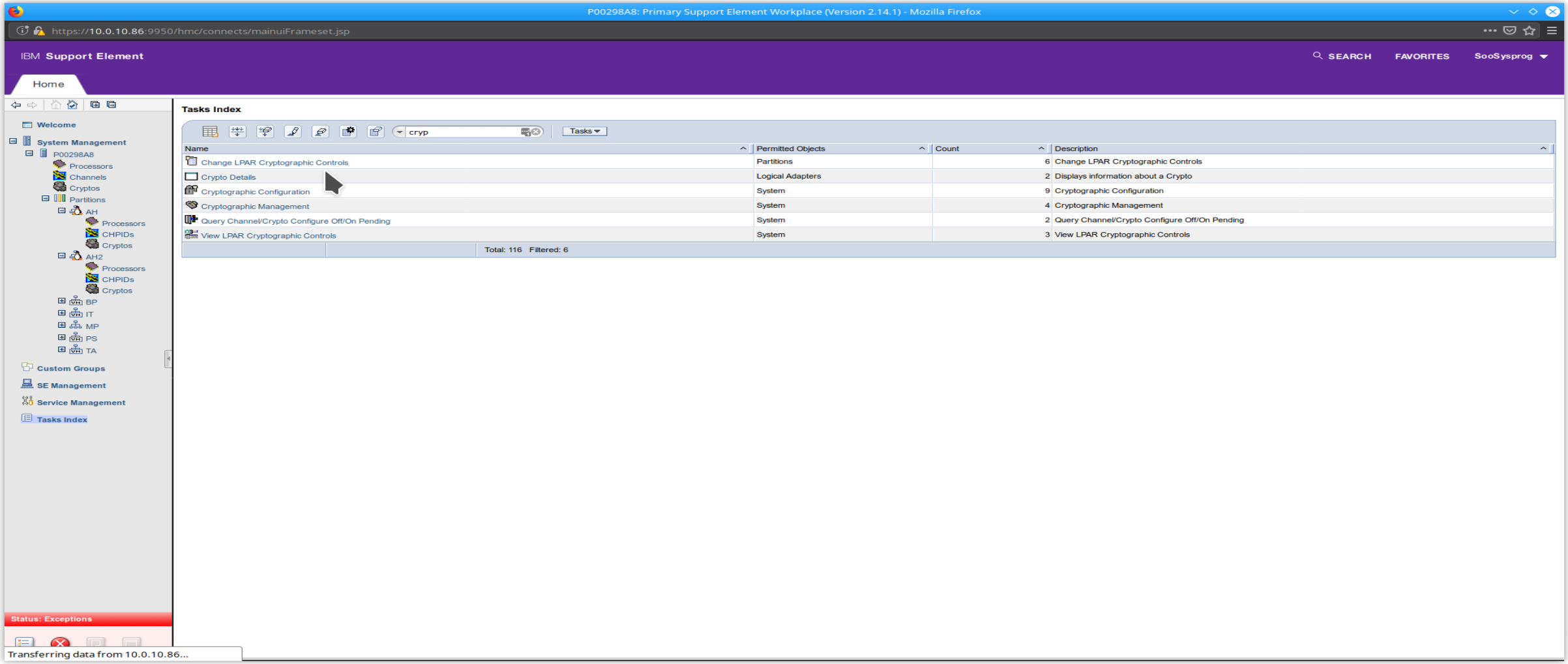
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Cryptos
- This screen will show initializing then online when the card is ready to use



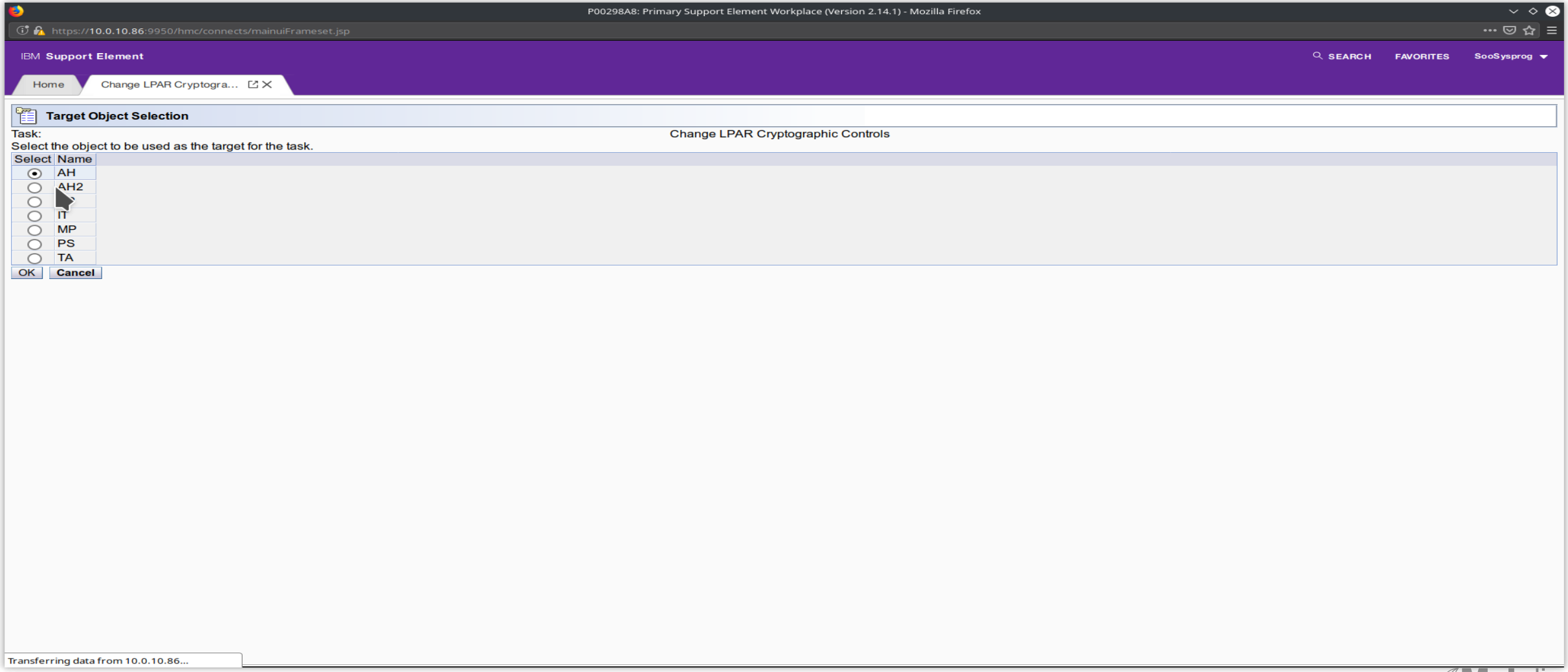
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Filter for Crypt / Select Change LPAR Crypto Controls
- This will allow you to assign crypto domains/indexes to your partitions



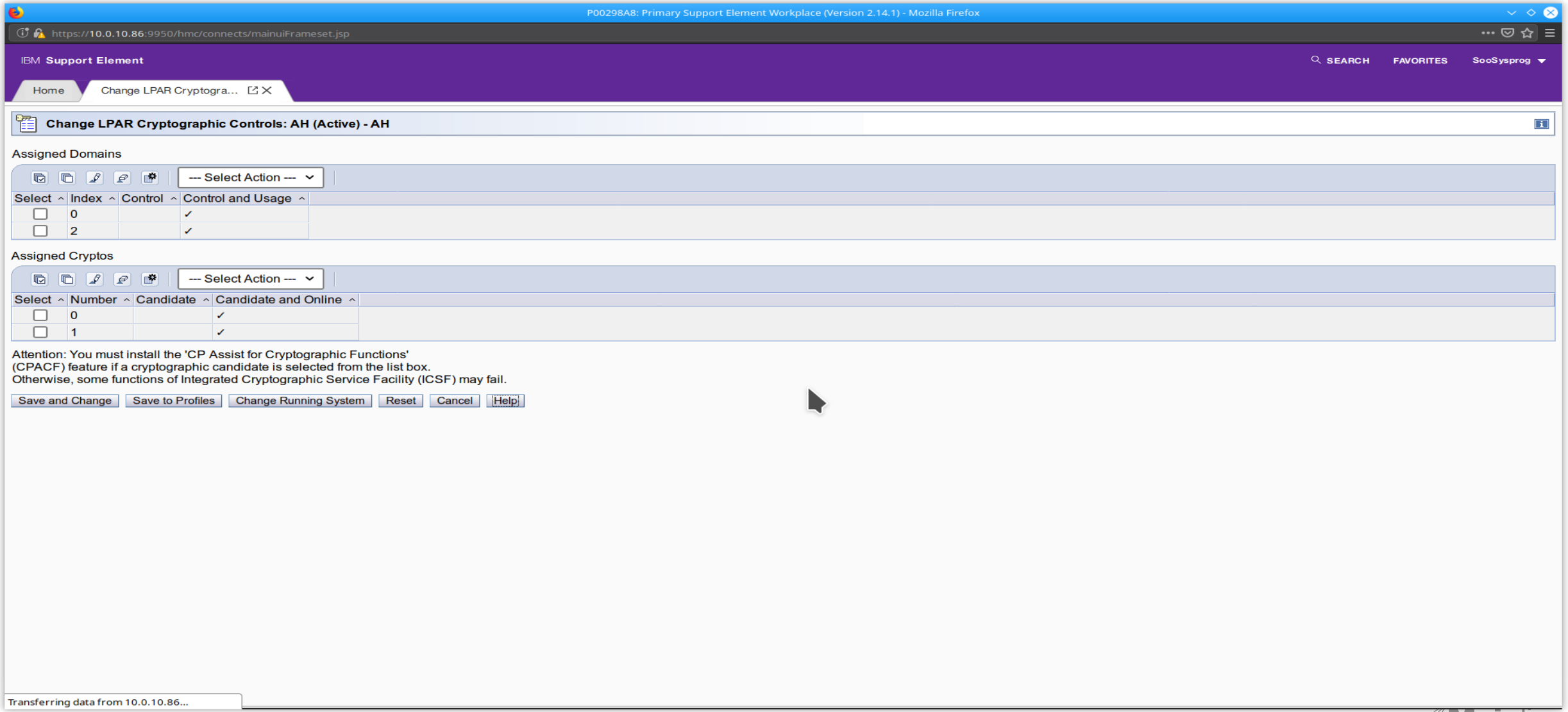
How to Implement Crypto Express Cards with Linux on z

- Select the partition you wish to configure
- This will need to be done for each partition you wish to configure



How to Implement Crypto Express Cards with Linux on z

- Explained on the next Slide

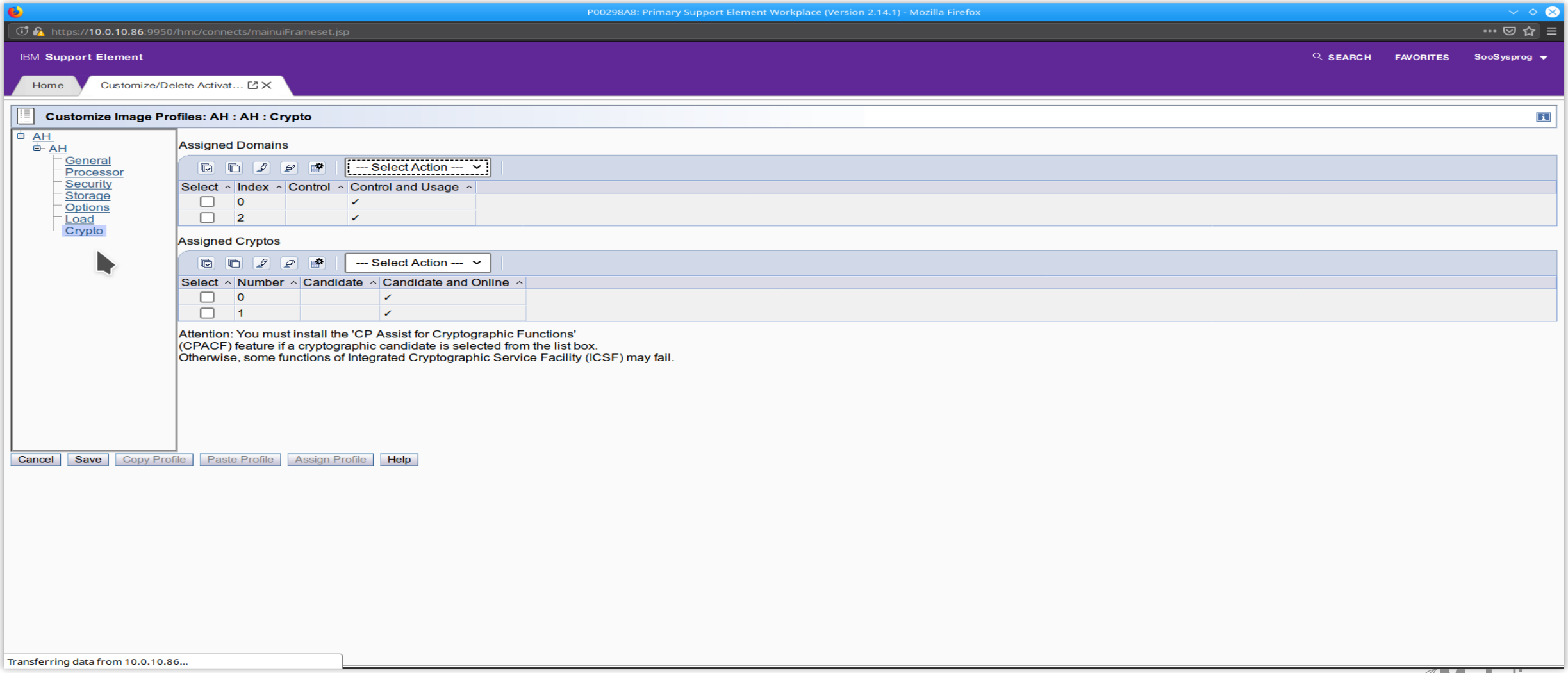


How to Implement Crypto Express Cards with Linux on z

- This screen allows you to choose your index (must be unique for active partitions)
- This screen allows you to choose which crypto cards are used
- The Save and Change button , dynamically changes the configuration and saves these setting in your LPAR image profile under the crypto tab
- This screen shows I selected Control and Usage – allowing me to use these indexes and Candidate and Online giving me access to these two crypto cards
- You can select one or more Indexes for each LPAR and Crypto Card, you may want to select more than one index per LPAR if you are planning to dedicate resources to specific users for example

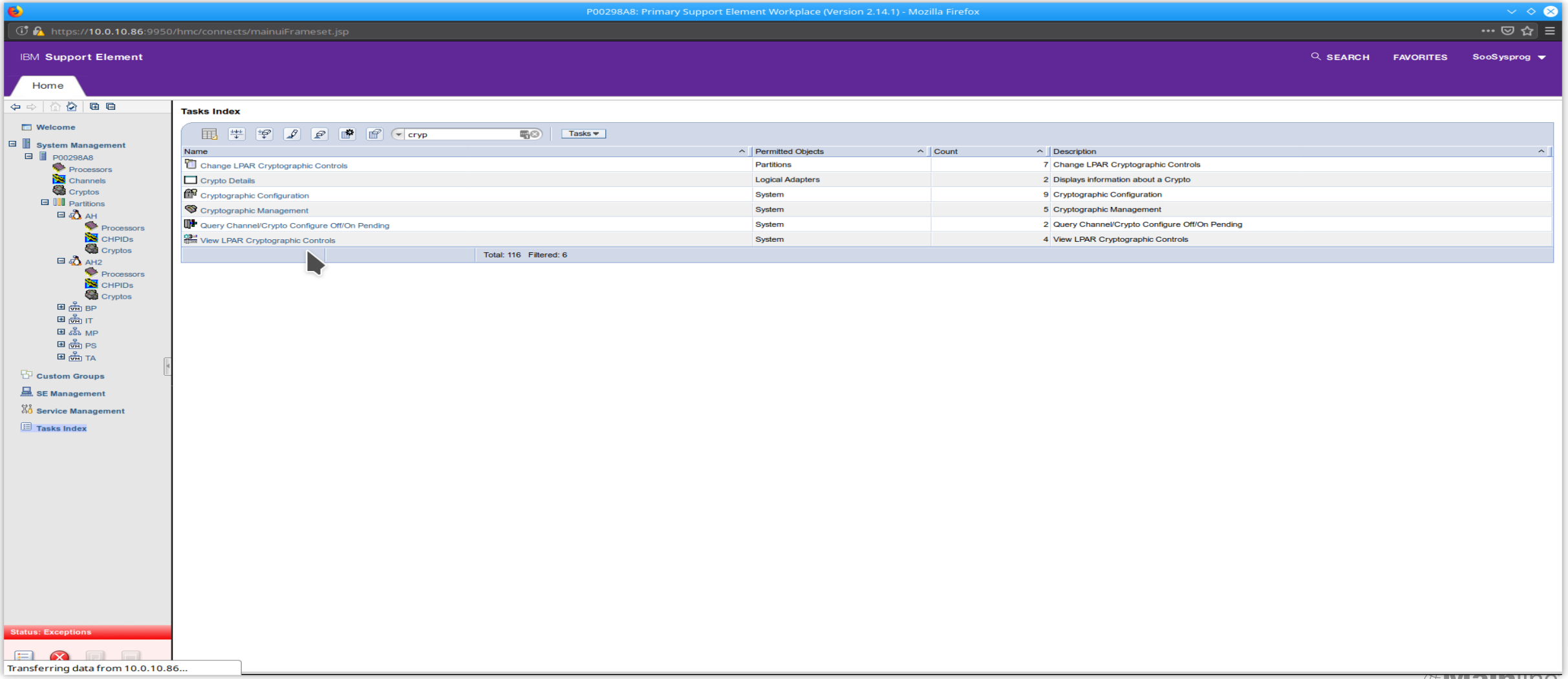
How to Implement Crypto Express Cards with Linux on z

- System Management / Partitions / Customize Delete Activation Profiles
- This shows the Activation Profile for the AH partition after the previous step was complete



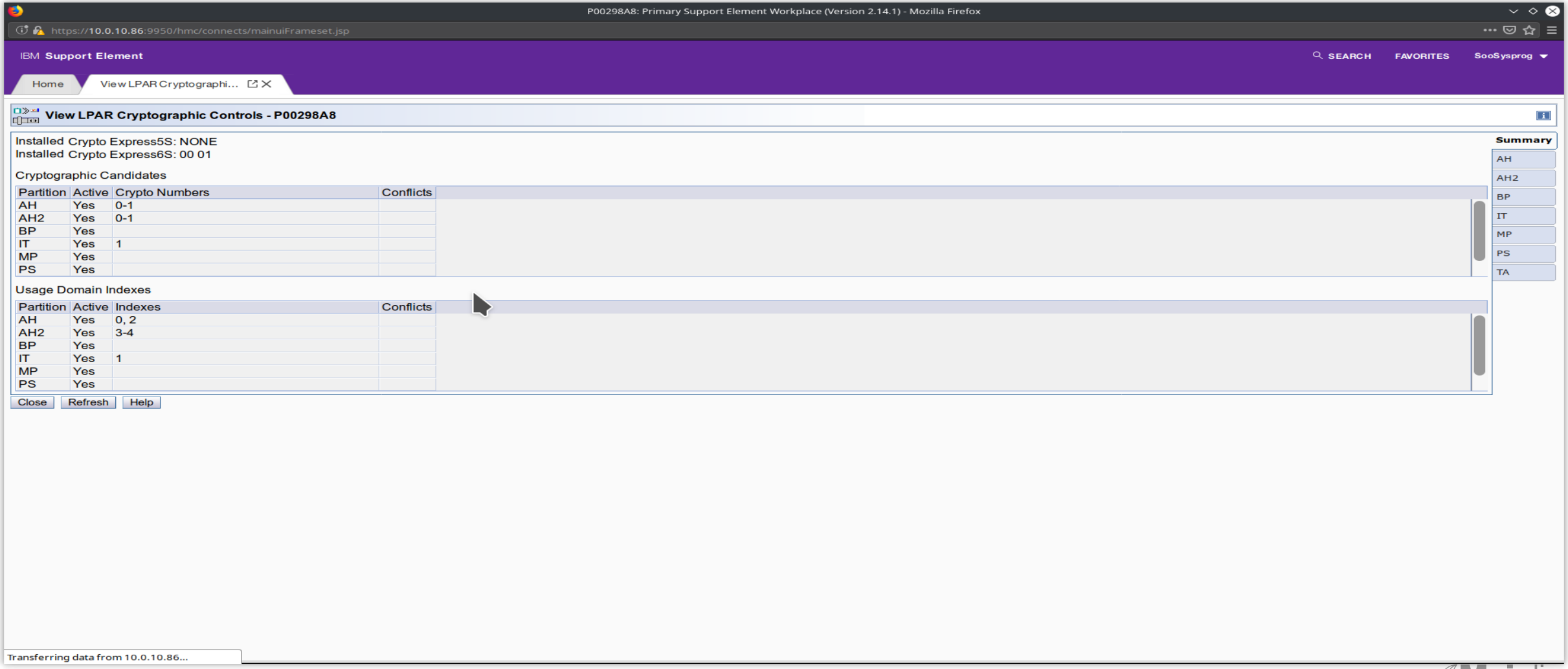
How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Filter for Crypt / Select View LPAR Crypto Configuration
- This will allow you to see all the crypto cards and indexes for all partitions



How to Implement Crypto Express Cards with Linux on z

- Systems Management / Tasks Index / Filter for Crypt / Select View LPAR Crypto Configuration
- This will show you if you have any conflicts



How to Implement Crypto Express Cards with Linux on z

- Z/VM 7.1 does not require an IPL to recognize a new crypto card – RSU 2001 – APAR – VM66266
- Z/VM 6.4 requires and IPL to see changes to crypto hardware
- I’m using CRYPTO APVIRT for the accelerator cards which is fine for clear key acceleration
- Use CRYPTO APDEDICATED if you need specific resources for specific guests for performance etc.
- When using APVIRT z/VM will dynamically choose which crypto resources to use
- When using APVIRT Linux configurations will always show only one crypto card , even though 2 or more may be in use to satisfy the requests
- The CRYPTO APVIRT can be placed in the user's directory or in a common profile if all the Linux guests will use the crypto cards

How to Implement Crypto Express Cards with Linux on z

- Z/VM setup crypto express definitions in the system config file
- System Config File

```
/*********************************************************************/
/* CRYPTOGRAPHIC CO-PROCESSORS AND ACCELERATORS                      */
/*********************************************************************/

 AHZVMM01:  BEGIN
          CRYPTO APVIRT AP 0 DOMAIN 0 2
          CRYPTO APVIRT AP 1 DOMAIN 0 2
        /* ENCRYPT PAGING ON ALG AES256 */
          ENCRYPT PAGING REQUIRED ALG AES256
 AHZVMM01:  END

 AHZVMM02:  BEGIN
          CRYPTO APVIRT AP 0 DOMAIN 3 4
          CRYPTO APVIRT AP 1 DOMAIN 3 4
   /*       ENCRYPT PAGING ON ALG AES256 */
          ENCRYPT PAGING REQUIRED ALG AES256
 AHZVMM02:  END
```

AP – equates to crypto card number | Domain equates to Index number from the hardware configuration earlier

How to Implement Crypto Express Cards with Linux on z

- Z/VM setup crypto express definitions in the Linux directory statements

- AHUBCRPT DIRECT

```
USER AHUBCRPT XXXXXXXX 4G 12G G
   INCLUDE LNXDFLT
   CPU 0
   CPU 1
   CPU 2
   CPU 3
   CRYPTO    APVIRT
*
*  IP ADDRESS - 10.0.10.196
*
* 0100 - DASDA1 SWAP DEFINED IN SWAPGEN EXEC
* 0101 - DASDB1 SWAP DEFINED IN SWAPGEN EXEC
*
   MDISK 0200 3390 1 END AHB701 MR READPASS WRITPASS MULTPASS
```

AHUBBASE does not contain the crypto entry since it doesn’t use the crypto express cards

How to Implement Crypto Express Cards with Linux on z

- Z/VM Query Crypto Express cards available for use

```
Q CRYPTO
Crypto Adjunct Processor Instructions are installed  - OR - Crypto Adjunct Processor Instructions are not installed

Ready; T=0.01/0.01 15:44:33

q crypto domain users
AP 000 CEX6A  Domain 000 operational  online  shared
AP 000 CEX6A  Domain 002 operational  online  shared
AP 001 CEX6A  Domain 000 operational  online  shared
AP 001 CEX6A  Domain 002 operational  online  shared

Shared-Crypto Users:
AHUBCRPT
Ready; T=0.01/0.01 10:16:12

q crypto domain users
AP 000 CEX6A  Domain 000 operational  online  shared
AP 000 CEX6A  Domain 002 operational  online  shared
AP 001 CEX6A  Domain 000 operational  online  shared
AP 001 CEX6A  Domain 002 operational  online  shared

There are no shared-crypto users.
Ready; T=0.01/0.01 10:17:57
```

How to Implement Crypto Express Cards with Linux on z

- AHUBCRPT – Ubuntu 20.04

andy@ahubcrpt:~$ sudo apt upgrade

andy@ahubcrpt:~$ sudo apt upgrade

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
.
Adding #2: IPL section 'old'
Preparing boot device: dasda (0200).
Done.
```

sudo apt install openssh-client openssh-server openssl openssl-ibmca libica3 libica-utils

Openssh-client , openssh-server and openssl are usually already installed by default

zcrypt is part of the device drivers for IBM z and installed by default

Make a copy of openssl.cnf in /etc/ssl

Modify the openssl.cnf file in /etc/ssl to use the ibmca engine

Add the following two lines to the openssl.cnf file right after the HOME line near the top of the file

```
# Line inserted to use ibmca
openssl_conf = openssl_def
```

Append /usr/share/doc/openssl-ibmca/examples/openssl.cnf.sample to the end of the openssl.cnf file

Comment out the line open_conf =

Completely shut down the Linux guest and bring it back up to enable the changes

How to Implement Crypto Express Cards with Linux on z

- AHRHCRPT – RHEL 8.2

[root@ahrhcrpt card01]# dnf upgrade

```
Updating Subscription Management repositories.
Red Hat Enterprise Linux 8 for IBM z Systems - AppStream (RPMs)      769  B/s | 4.5 kB     00:05
Red Hat Enterprise Linux 8 for IBM z Systems - BaseOS (RPMs)         744  B/s | 4.0 kB     00:05
Dependencies resolved.
Nothing to do.
Complete!
```

dnf install libica openssl-ibmca openssl openssh

openssh and openssl are usually already installed by default

zcrypt is part of the device drivers for IBM z and installed by default

Make a copy of openssl.cnf in /etc/pki/tls

Modify the openssl.cnf file in /etc/pki/tls to use the ibmca engine

Add the following two lines to the openssl.cnf file right after the HOME line near the top of the file

```
# Line inserted to use ibmca
openssl_conf = openssl_def
```

Append /usr/share/doc/openssl-ibmca/openssl.cnf.sample.s390x to the end of the openssl.cnf file

Comment out any other openssl_conf = statements and there directives

Completely shutdown the Linux guest and bring it back up to enable the changes

How to Implement Crypto Express Cards with Linux on z

- AHSLCRPT – SLES 15 SP 1

ahslcrpt:~ # zypper update

Refreshing service 'Basesystem_Module_15_SP1_s390x'.
Refreshing service 'SUSE_Linux_Enterprise_Server_15_SP1_s390x'.
.
Core libraries or services have been updated.
Reboot is required to ensure that your system benefits from these updates.

zypper install openssh openssl openssl-ibmca libica3 libica-tools
openssh and openssl are usually already installed by default
zcrypt is part of the device drivers for IBM z and installed by default

Make a copy of openssl.cnf in /etc/ssl
Modify the openssl.cnf file in /etc/ssl to use the ibmca engine
Add the following two lines to the openssl.cnf file right after the #RANDFILE line near the top of the file
# Line inserted to use ibmca
openssl_conf = openssl_def
Append /usr/share/doc/packages/openssl-ibmca/openssl.cnf.sample to the end of the openssl.cnf file
Completely shut down the Linux guest and bring it back up to enable the changes

How to Measure Crypto Express Usage

- Vmcp q v crypto – shows virtual cryptographic card available to this Linux guest

```
root@ahubcrpt:~# vmcp q v crypt
AP 001 CEX6A Domain 001 shared online
```

This only shows 1 but VM will use all available crypto cards to satisfy the requests

- ls /sys/devices/ap/cardxx - shows various files associated with the virtual crypto card

```
root@ahubcrpt:~# ls /sys/devices/ap/card01/
01.0001     depth   hwtype  modalias  pendingq_count  request_count  subsystem  uevent
ap_functions  driver  load    online    raw_hwtype      requestq_count  type
```

- cat /sys/devices/ap/card01/request_count

```
root@ahubcrpt:~# cat /sys/devices/ap/card01/request_count
21179
```

How to Measure Crypto Express Usage

Icainfo – Display cryptographic functions supported by libica

```
andy@ahubcrpt:~$ icainfo
            Cryptographic algorithm support
-------------------------------------------------------
              |        hardware       |
 function     |  dynamic  |   static  |  software
--------------+-----------+-----------+-----------
       SHA-1 |     no    |    yes    |    yes
     SHA-224 |     no    |    yes    |    yes
     SHA-256 |     no    |    yes    |    yes
     SHA-384 |     no    |    yes    |    yes
.
      RSA ME |    yes    |     no    |     no
     RSA CRT |    yes    |     no    |     no
.
      -------------------------------------------------------
      No built-in FIPS support.
```

– Lszcrypt –V – Displays available cryptographic cards and requests

```
andy@ahubcrpt:~$ lszcrypt -V
CARD.DOMAIN TYPE  MODE        STATUS  REQUESTS  PENDING HWTYPE QDEPTH FUNCTIONS  DRIVER
-----------------------------------------------------------------------------------------
01          CEX6A Accelerator online     21179        0     12     08 -MC-A-NF-  cex4card
01.0001     CEX6A Accelerator online     21179        0     12     08 -MC-A-NF-  cex4queue
```

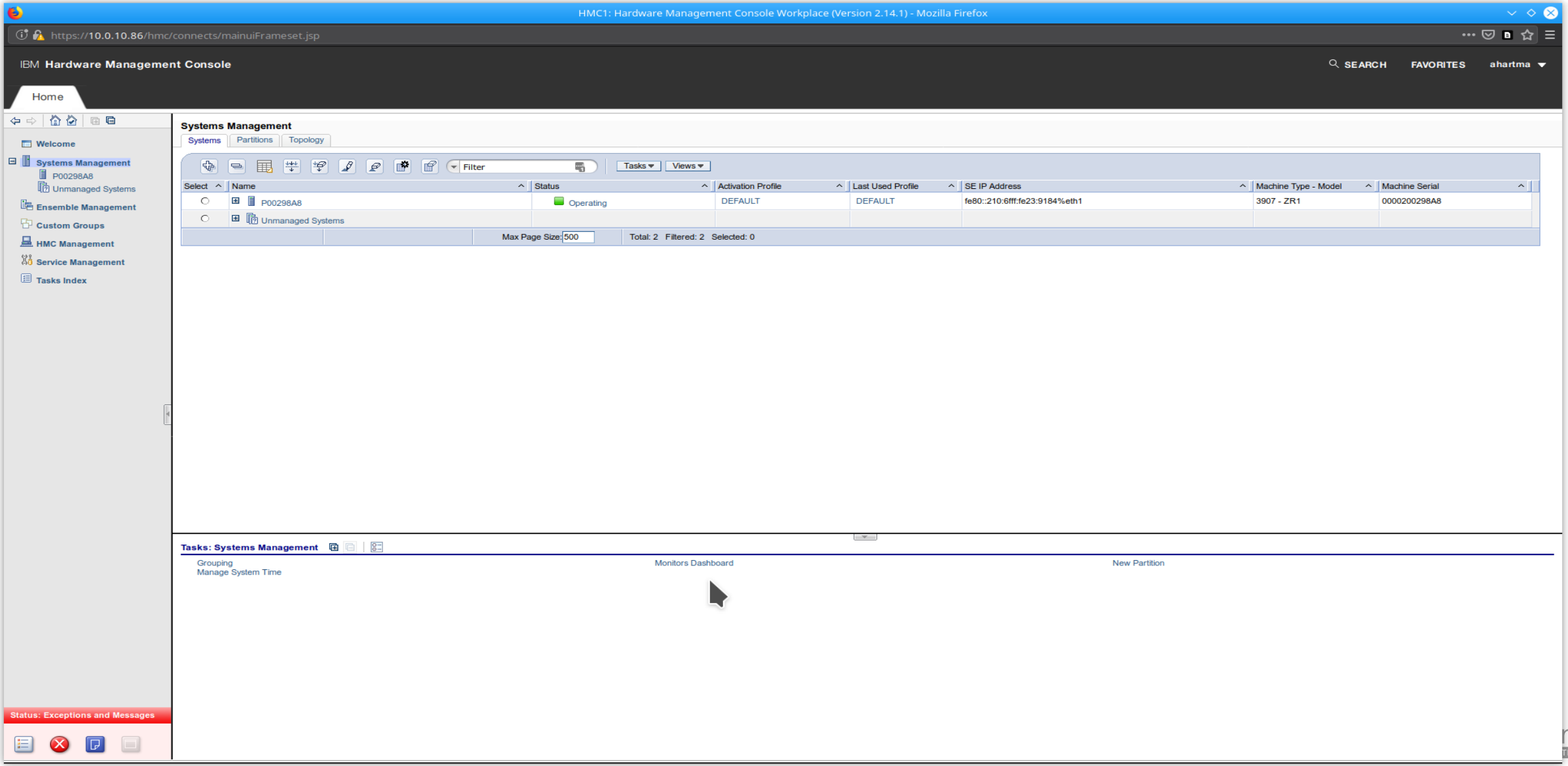
How to Measure Crypto Express Usage

- Icastats – Shows statistics for hardware and software cryptography used by the libica functions

```
root@ahubcrpt:~# icastats
  function      |         hardware      |         software
---------------+-----------------------+-----------------------
               |    ENC   CRYPT   DEC  |    ENC   CRYPT   DEC
---------------+-----------------------+-----------------------
         SHA-1 |       126520          |            0
       SHA-224 |            0          |            0
       SHA-256 |       540257          |            0
       SHA-384 |            0          |            0
       SHA-512 |          151          |            0
.
      RSA-ME   |        12104          |            0
      RSA-CRT  |         9075          |            0
.
      AES XTS  |            0          0 |            0          0
      AES GCM  |        33142      18090 |            0          0
```

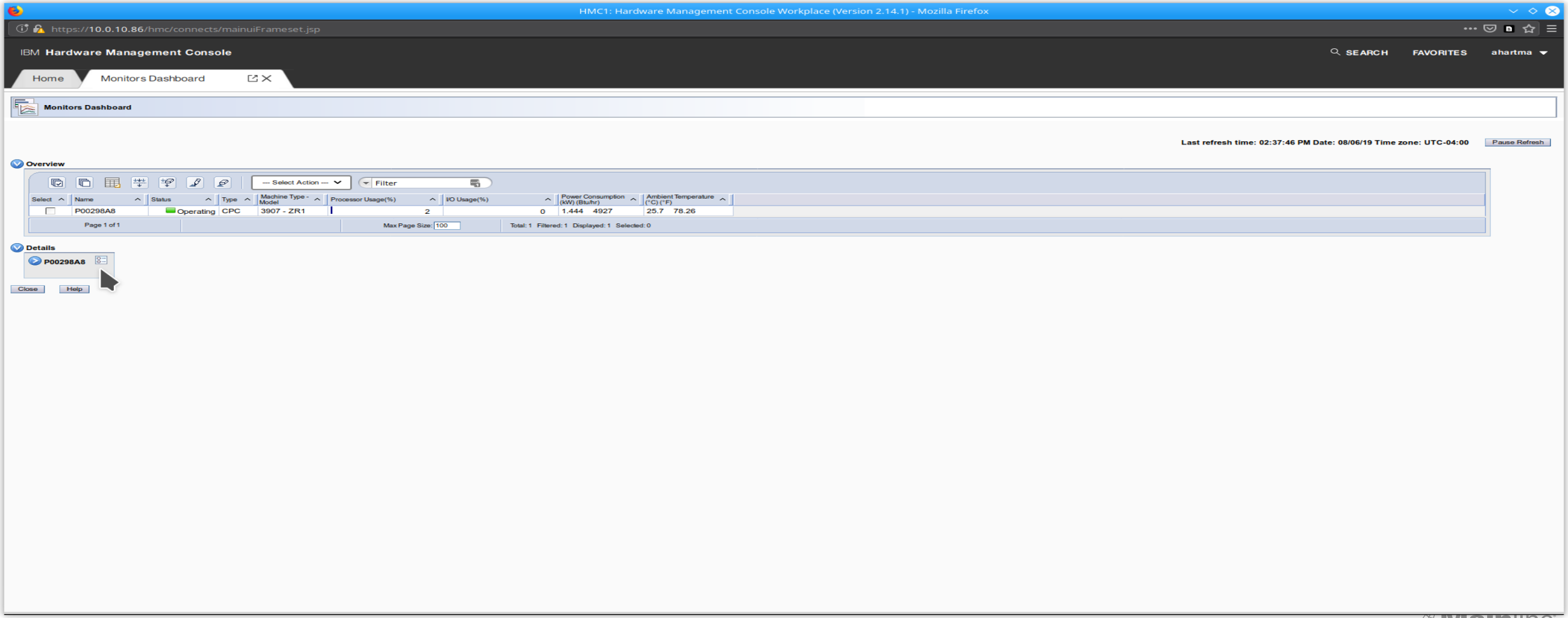
How to Measure Crypto Express Usage

- Systems Management / Monitors Dashboard



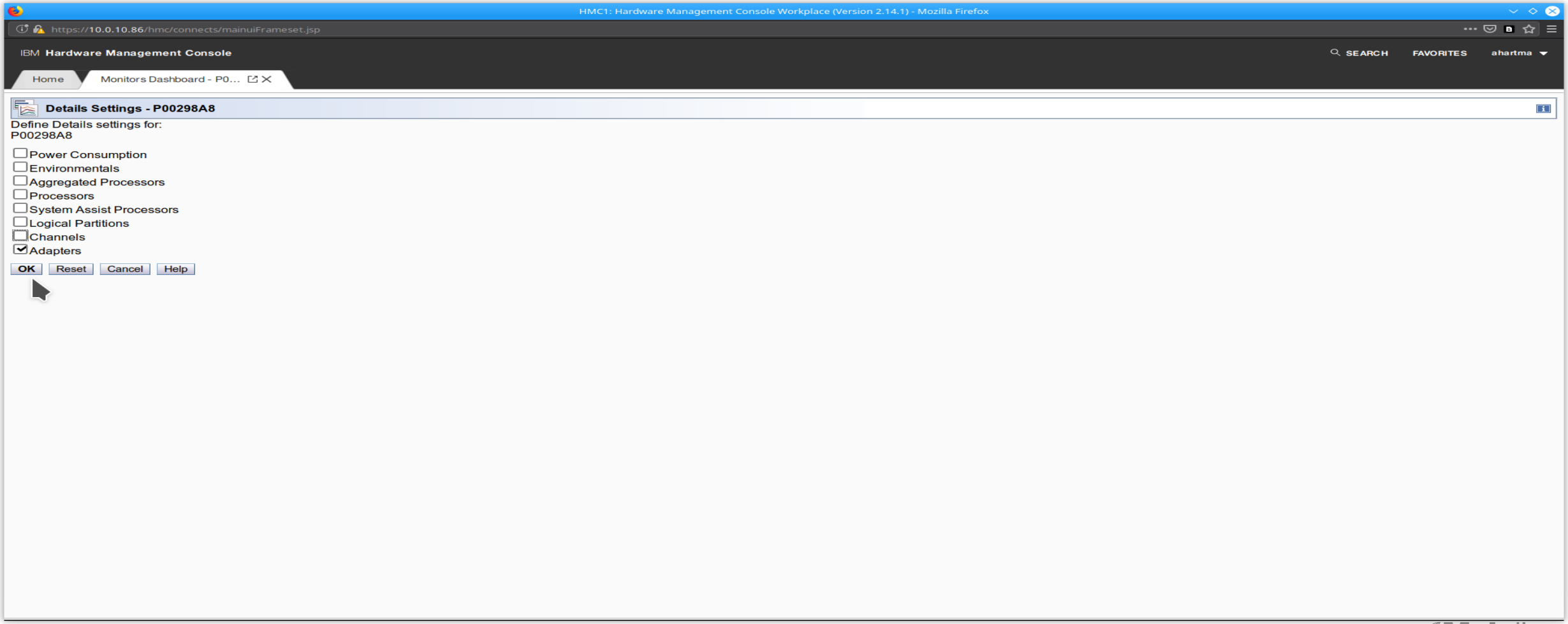
How to Measure Crypto Express Usage

- Click on Details



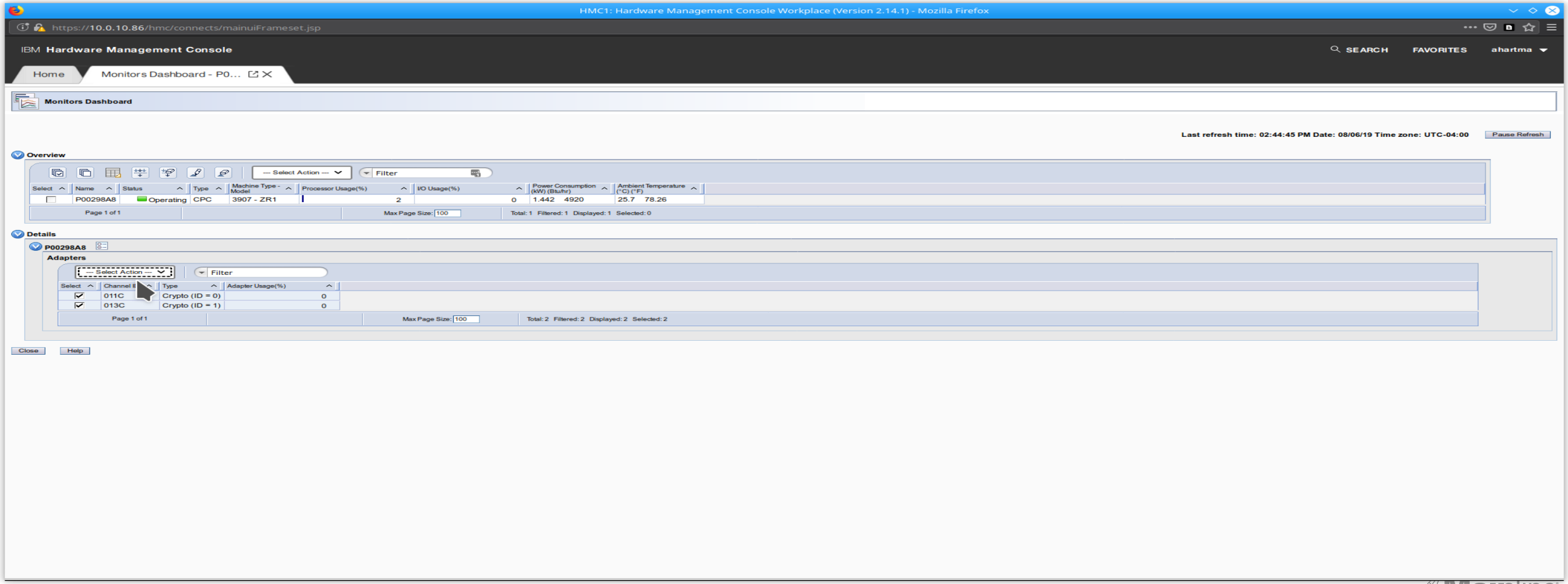
How to Measure Crypto Express Usage

- Select Adapters and Click OK



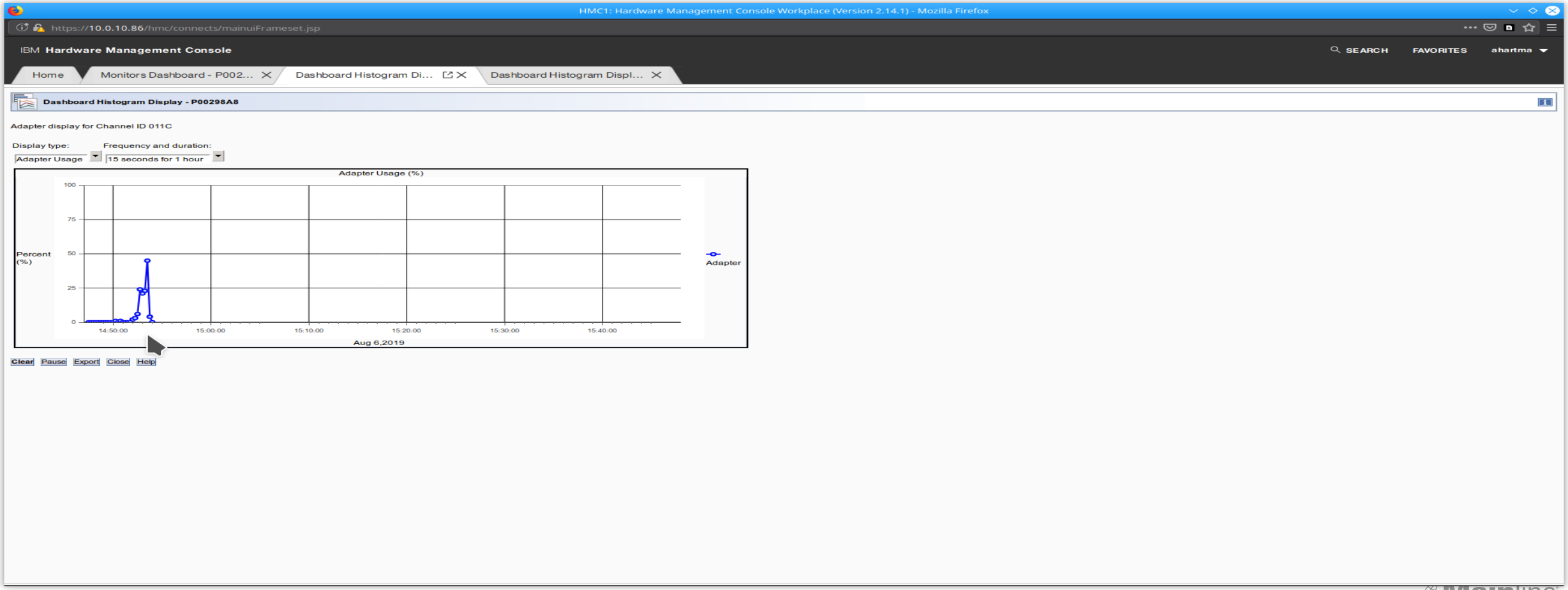
How to Measure Crypto Express Usage

- Select both adapters / Select Start History from Select Action Drop Down
- It will start two new tabs one for each adapter



How to Measure Crypto Express Usage

- Both tabs will look the same – each is used evenly



Show Processing Offloaded By Using The Crypto Cards

DEMO

Show Processing Offloaded By Using The Crypto Cards

ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.194/- No CPACF/ No Crypto Express

ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.196/ - CPACF / Crypto Express

-n 3000 = number of requests to perform during the benchmark

-c 50 = number of requests to perform at the same time

-Z = Encryption suite used for the benchmark

DHE = key exchange via Diffie Hellman

RSA = authentication algorithm

AES128 = bulk encryption algorithm

SHA = hashing algorithm

- Different Cipher Suites will have different affects on CPU utilization – this one showed around a 60-70% utilization without crypto cards / Less than 1% CPU utilization with crypto cards
- Different distributions and releases can affect how the cpu and crypto cards are utilized
- Choose your Cipher Suites based on your specific needs

Show Processing Offloaded By Using The Crypto Cards

```
andy@DESKTOP-T02VH7C:~$ ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.194/
This is ApacheBench, Version 2.3 <$Revision: 1843412 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 10.0.10.194 (be patient)
Completed 300 requests
Completed 600 requests
Completed 900 requests
Completed 1200 requests
Completed 1500 requests
Completed 1800 requests
Completed 2100 requests
Completed 2400 requests
Completed 2700 requests
Completed 3000 requests
Finished 3000 requests

Server Software:        Apache/2.4.41
Server Hostname:        10.0.10.194
Server Port:            443
SSL/TLS Protocol:       TLSv1.2,DHE-RSA-AES128-SHA,4096,128
Server Temp Key:        DH 4096 bits

Document Path:          /
Document Length:        10918 bytes
```

Show Processing Offloaded By Using The Crypto Cards

```
Concurrency Level:      50
Time taken for tests:   164.189 seconds
Complete requests:      3000
Failed requests:        0
Total transferred:      33576000 bytes
HTML transferred:       32754000 bytes
Requests per second:    18.27 [#/sec] (mean)
Time per request:       2736.481 [ms] (mean)
Time per request:       54.730 [ms] (mean, across all concurrent requests)
Transfer rate:          199.70 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:      355 2199 594.6   2292    4402
Processing:    57  491 354.7    376    2657
Waiting:       55  287 292.6    147    1844
Total:        430 2690 639.2   2722    6805

Percentage of the requests served within a certain time (ms)
  50%   2722
  66%   2915
  75%   3029
  80%   3124
  90%   3354
  95%   3604
  98%   3915
  99%   4230
 100%   6805 (longest request)
```

What are Crypto Express Cards

```
andy@ahubbase:~$ sar -u 10 1000
Linux 5.4.0-33-generic (ahubbase.s390.mainline.com)     06/10/2020      _s390x_ (4 CPU)

01:00:31 PM     CPU     %user     %nice   %system   %iowait   %steal     %idle
01:00:41 PM     all      0.00      0.00      0.00      0.00      0.00    100.00
01:00:51 PM     all     44.61      0.00      0.15      0.00      0.55     54.69
01:01:01 PM     all     58.29      0.00      0.02      0.00      0.50     41.19
01:01:11 PM     all     68.47      0.00      0.15      0.00      0.62     30.76
01:01:21 PM     all     63.24      0.00      0.07      0.00      0.60     36.09
01:01:31 PM     all     61.07      0.00      0.12      0.00      0.52     38.28
01:01:41 PM     all     60.63      0.00      0.07      0.00      0.52     38.77
01:01:51 PM     all     68.92      0.00      0.17      0.00      0.62     30.28
01:02:01 PM     all     67.29      0.00      0.12      0.00      0.55     32.04
01:02:11 PM     all     63.70      0.00      0.10      0.00      0.55     35.66
01:02:21 PM     all     63.02      0.00      0.10      0.00      0.52     36.36
01:02:31 PM     all     62.19      0.00      0.05      0.00      0.57     37.19
01:02:41 PM     all     60.19      0.00      0.10      0.00      0.57     39.14
01:02:51 PM     all     60.11      0.00      0.12      0.00      0.60     39.17
01:03:01 PM     all     67.73      0.00      0.17      0.00      0.60     31.50
01:03:11 PM     all     67.82      0.00      0.07      0.00      0.60     31.51
01:03:21 PM     all     71.54      0.00      0.10      0.00      0.67     27.69
01:03:31 PM     all     26.34      0.00      0.02      0.00      0.17     73.46
01:03:41 PM     all      0.00      0.00      0.05      0.00      0.00     99.95


Average:        all     54.51      0.00      0.09      0.00      0.49     44.90
```

WITHOUT CPACF OR CRYPTO EXPRESS CARDS

```
ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.194/
```

Show Processing Offloaded By Using The Crypto Cards

```
andy@DESKTOP-T02VH7C:~$ ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.196/
This is ApacheBench, Version 2.3 <$Revision: 1843412 $>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
Licensed to The Apache Software Foundation, http://www.apache.org/

Benchmarking 10.0.10.196 (be patient)
Completed 300 requests
Completed 600 requests
Completed 900 requests
Completed 1200 requests
Completed 1500 requests
Completed 1800 requests
Completed 2100 requests
Completed 2400 requests
Completed 2700 requests
Completed 3000 requests
Finished 3000 requests


Server Software:        Apache/2.4.41
Server Hostname:        10.0.10.196
Server Port:            443
SSL/TLS Protocol:       TLSv1.2,DHE-RSA-AES128-SHA,2048,128
Server Temp Key:        DH 2048 bits

Document Path:          /
Document Length:        10918 bytes
```

Show Processing Offloaded By Using The Crypto Cards

```
Concurrency Level:      50
Time taken for tests:   32.172 seconds
Complete requests:      3000
Failed requests:        0
Total transferred:      33576000 bytes
HTML transferred:       32754000 bytes
Requests per second:    93.25 [#/sec] (mean)
Time per request:       536.200 [ms] (mean)
Time per request:       10.724 [ms] (mean, across all concurrent requests)
Transfer rate:          1019.18 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:      197  323 149.4    298    1751
Processing:    57  201 167.9    128    1339
Waiting:       54  108  72.8     81    1046
Total:        262  524 237.2    435    2319

Percentage of the requests served within a certain time (ms)
  50%    435
  66%    582
  75%    635
  80%    652
  90%    737
  95%    982
  98%   1320
  99%   1528
 100%   2319 (longest request)
```

What are Crypto Express Cards

root@ahubcrpt:~# sar -u 10 1000
Linux 5.4.0-33-generic (ahubcrpt) 06/10/2020 _s390x_ (4 CPU)

01:15:02 PM	CPU	%user	%nice	%system	%iowait	%steal	%idle
01:15:12 PM	all	0.10	0.00	0.10	0.00	0.17	99.63
01:15:22 PM	all	0.60	0.00	0.45	0.00	0.94	98.01
01:15:32 PM	all	0.67	0.00	0.45	0.00	0.92	97.97
01:15:42 PM	all	0.55	0.00	0.42	0.00	0.77	98.26
01:15:52 PM	all	0.00	0.00	0.00	0.00	0.00	100.00
01:16:02 PM	all	0.00	0.00	0.02	0.00	0.00	99.98
01:16:12 PM	all	0.00	0.00	0.00	0.00	0.00	100.00
01:16:22 PM	all	0.00	0.00	0.02	0.00	0.00	99.98

Average: all 0.24 0.00 0.18 0.00 0.35 99.22

WITH CPACF AND CRYPTO EXPRESS CARDS

ab -n 3000 -c 50 -Z DHE-RSA-AES128-SHA https://10.0.10.196

Show Processing Offloaded By Using The Crypto Cards

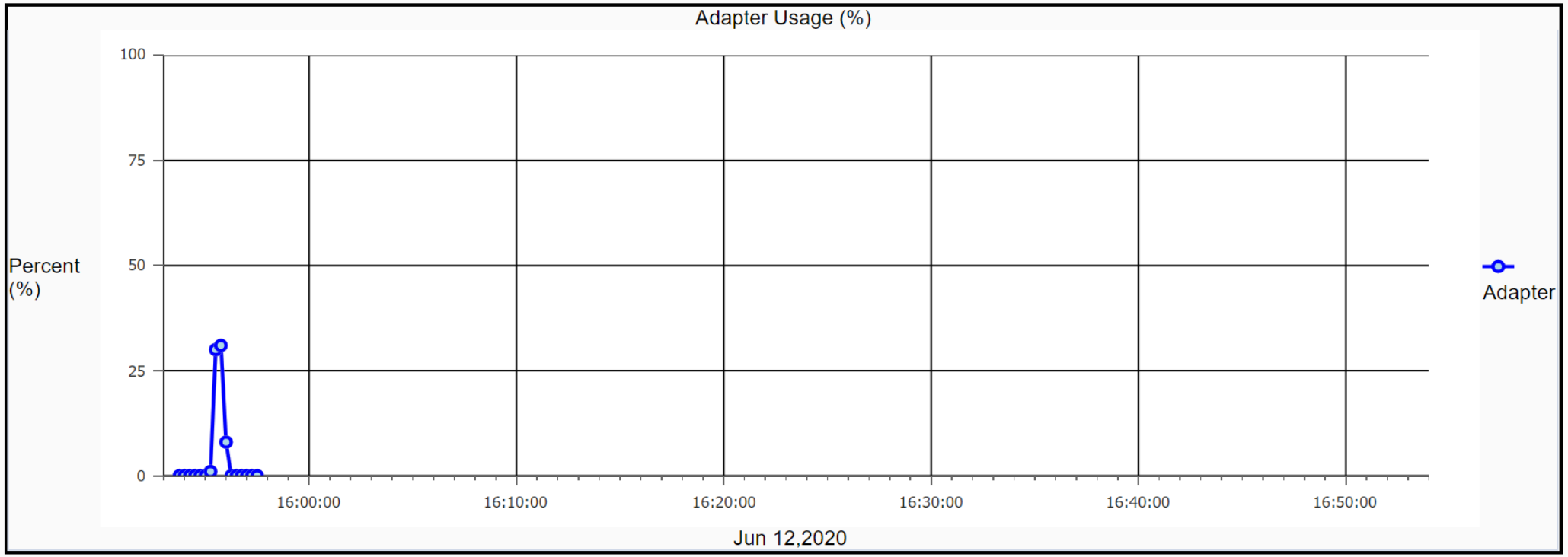
15:53 plus time period

Dashboard Histogram Display - P00298A8

Adapter display for Channel ID 013C

Display type: Adapter Usage

Frequency and duration: 15 seconds for 1 hour



Clear Pause Export Close Help

Show Processing Offloaded By Using The Crypto Cards

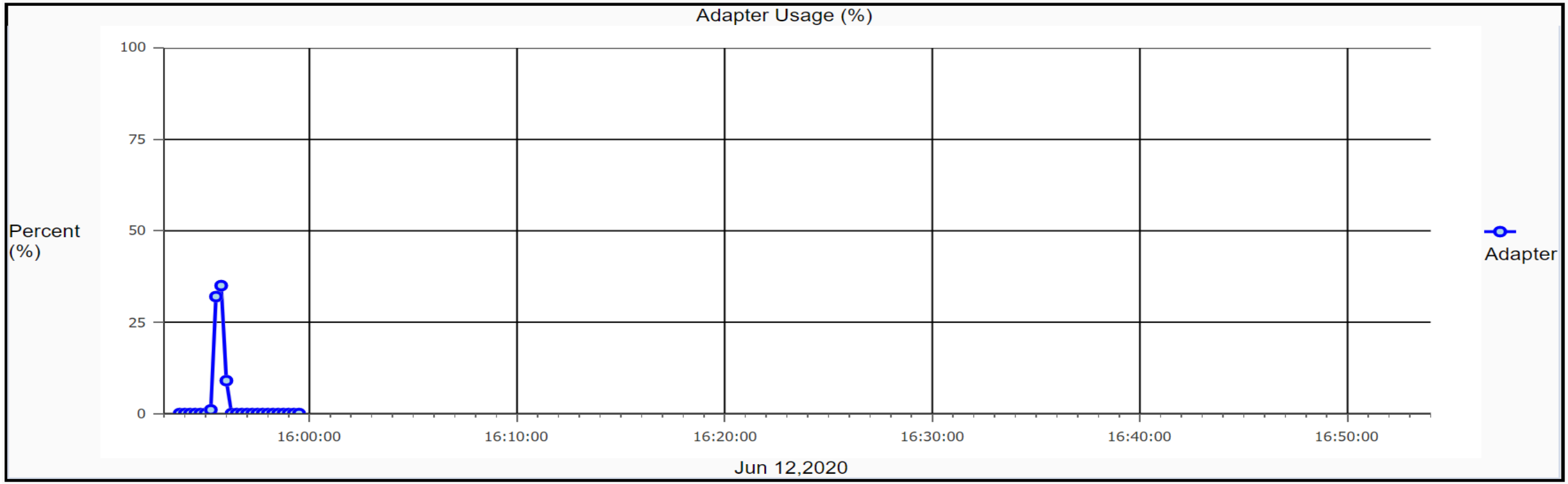
15:53 plus time period

Dashboard Histogram Display - P00298A8

Adapter display for Channel ID 011C

Display type: Adapter Usage

Frequency and duration: 15 seconds for 1 hour



Clear Pause Export Close Help

How to Implement Crypto Express Cards with Linux on z

References

- Z15 Technical Guide
  - http://www.redbooks.ibm.com/abstracts/sg248851.html?Open
- Z15 Configuration Setup
  - http://www.redbooks.ibm.com/abstracts/sg248860.html
- Cryptographic hardware support for IBM Z and IBM LinuxONE
  - https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaaf/sec_hw_supp.html
- Hardware cryptographic support of IBM z Systems for OpenSSH in RHEL 7.2 and SLES 12 SP1 - Older
  - http://www.vm.ibm.com/devpages/spera/MG_OpenSSH.pdf
- Hardware cryptographic support for IBM Z and IBM LinuxONE with Ubuntu Server - Older
  - https://people.canonical.com/~fheimes/MG_HWCrypto_with_Ubuntu_on_z.pdf
- New – z/VM 7.1 CP Planning and Administration Guide – Chapter 5
  - http://www.vm.ibm.com/library/710pdfs/71627104.pdf
- KVM and Virtual Guest Setup for Crypto Express
  - https://www.ibm.com/support/knowledgecenter/en/linuxonibm/com.ibm.Linux.z.lxhq/lxhq_c_welcome.html
- Linux Setup for Crypto Express when install directly into and LPAR
  - https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaab/icwhatsnew.html
- Running Docker Containers on IBM Z with Crypto Express
  - https://www.ibm.com/support/knowledgecenter/en/linuxonibm/com.ibm.Linux.z.ldvd/ldvd_c_welcome.html
- SSL/TLS Cipher Suites – Nice overview of cipher suites
  - https://www.thesslstore.com/blog/cipher-suites-algorithms-security-settings/

Conclusion

- Your company's data is one of your most important assets and needs to be protected
- Data in flight is a critical part of this protection
- By using Crypto Express cards you can significantly reduce the consumption of processor resources while providing the ability to service a great number of SSL/TLS sessions used in web serving for example
- Different cipher suites will have different results – you can choose which ciphers and protocols are used for your websites
- I discussed and demonstrated the Crypto Express Card configured as an Accelerator, but remember that these cards can do much more and can be configured to satisfy many different types of security needs
- If you don't have crypto cards on your system and you want to test out various cipher suites and Linux configurations , Mainline can work with you to set up demonstrations using our system to show what the possible benefits would be for adding crypto express cards to your installation

Questions?

The Technology Partner for Business Results

Mainline INFORMATION SYSTEMS