IBM Z HMC (Hardware Management Console) 2.15.0 Security Enhancements

February 25, 2021

Z Exchange

Brian Valentine
HMC/SE Development
File Updated: 02-25-21

IBM Z

Z Exchange

Topics

- HMC 2.15.0 System Support
- HMC/SE/TKE HDD Encryption
- Audit Mgmt offload support to Remote Syslog (includes Splunk)
  -- Enhancements
  -- HMC Data Replication Terminology Change
- HMC Support of new SE Tasks/Channel Objects (User Security for HMC and SE)
- New HMC View Only support
- Integration of IBM MFA for z/OS/Support for RSA SecurID
- Integrated 3270 Console Security Benefits reminder/Performance Enhancements
- HMC Mobile Security Enhancements
- January 2020 CA Password Law
- Fibre Channel Endpoint Security (Authentication and EDiF (Encrypted Data in Flight))
- YouTube Videos for HMC Content

Appendix I

- SNMP support for Offload Audit Logs and System Events
- Crypto Signed UDXes
- Linux Secure IPL
- Data Replication for Last Login

Appendix II

- Fibre Channel Endpoint Security Certificate Management

HMC 2.15.0 System Support

HMC 2.15.0 System support

- **HMC support to n-2 only**
- **zBX support removed**

Machine Family	Machine Type	Firmware Driver	SE Version
z15	8561, 8562	41	2.15.0
z14 M0x/LMx	3906	36	2.14.1
z14 ZR1/LR1	3907	36	2.14.1
z13	2964	27	2.13.1
z13s	2965	27	2.13.1

HMC/SE/TKE HDD Encryption

HDD Encryption for HMC & SE

- HMC/SE Security continued emphasis
  - Passwords never stored in clear (one way hash)
  - HMC/SE Closed Appliance => no means to get to HDD
  - All Network traffic TLS encrypted
  - HMC/SE Embedded Firewall
  - Firmware Digitally Signed/Validated for delivery
  - Firmware Integrity Monitoring for any attempted tampering post delivery
    - Secure Boot & TPM (Trusted Platform Module)
    - IBM Resource Link Third Party Analysis of Attestation Data

- HMC & SE 2.15.0 HDD Encrypted
  - Utilizes TPM
  - LUKS (Linux Unified Key Setup) technology
  - HDD data also protected prior to 2.15.0
    - Encrypted HDD provides easier IBM & Client security audit statement of protection for
      - Client HMC data (which is very limited) &
      - IBM data/firmware

Audit Mgmt offload support to Remote Syslog

Goals and Approach

- Goals
  - **Consolidation** of key HMC/SE log information to new log entries as a supplement to existing logs (i.e. no current logs are being removed)
  - Customizable **forwarding** of selected consolidated log entries to a customer-controlled centralized gathering point or points
- Approach
  - Leverages syslog capability
    - syslog is a logging component and protocol
    - HMC/SE will utilize a standard rsyslog component within its environment
    - rsyslog supports forwarding to syslog servers for log consolidation and analysis
    - Commonly used syslogging tools (such as rsyslog itself) and products (such as ***Splunk Enterprise***) are capable of acting as syslog servers

Consolidation

- Types of logs being consolidated
  - Audit logs
  - Security logs
  - Console events
  - Hardware messages
  - Web Services API request logs
  - BCPii logs

- Consolidation approach
  - Summary information is captured and formatted at the existing logging points and syslogged
  - For remote consolidation
    - New HMC task
      - Configure rsyslog to forward selected consolidated syslog entries from the HMC or managed SEs to customer-controlled syslog servers

Sample consolidated log entries

```
Apr  3 10:02:24 HMC0318A zHMC.HMC0318A.SecurityLog: The user browser logged into the
underlying console operating system platform.


Apr  3 10:02:29 HMC0318A zHMC.HMC0318A.AuditLog: A device monitor event occurred; Device
Type: usb, Action: discovered at startup, Vendor: QEMU, Model: QEMU USB Tablet, Serial:
42


Apr  3 10:03:13 HMC0318A zHMC.HMC0318A.HwMsgLog: AttentionID: 38b59cc0-5619-11e9-a82d-
fa163e302a96 Creation Date: Wed Apr 03 10:03:13 EDT 2019 Description: ACT04320I Device
Monitor. Device Type: usb, Action: discovered at startup, Vendor: QEMU, Model: QEMU USB
Tablet, Serial: 42


Apr  3 10:03:14 HMC0318A zHMC.HMC0318A.EventLog: The console application was
initialized.
```

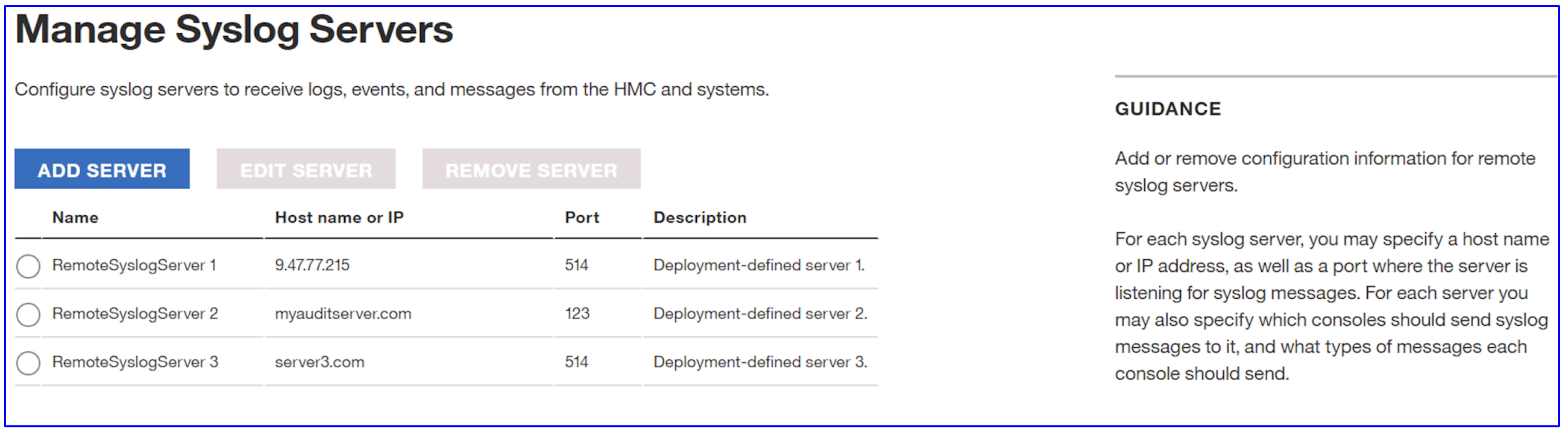
Forwarding

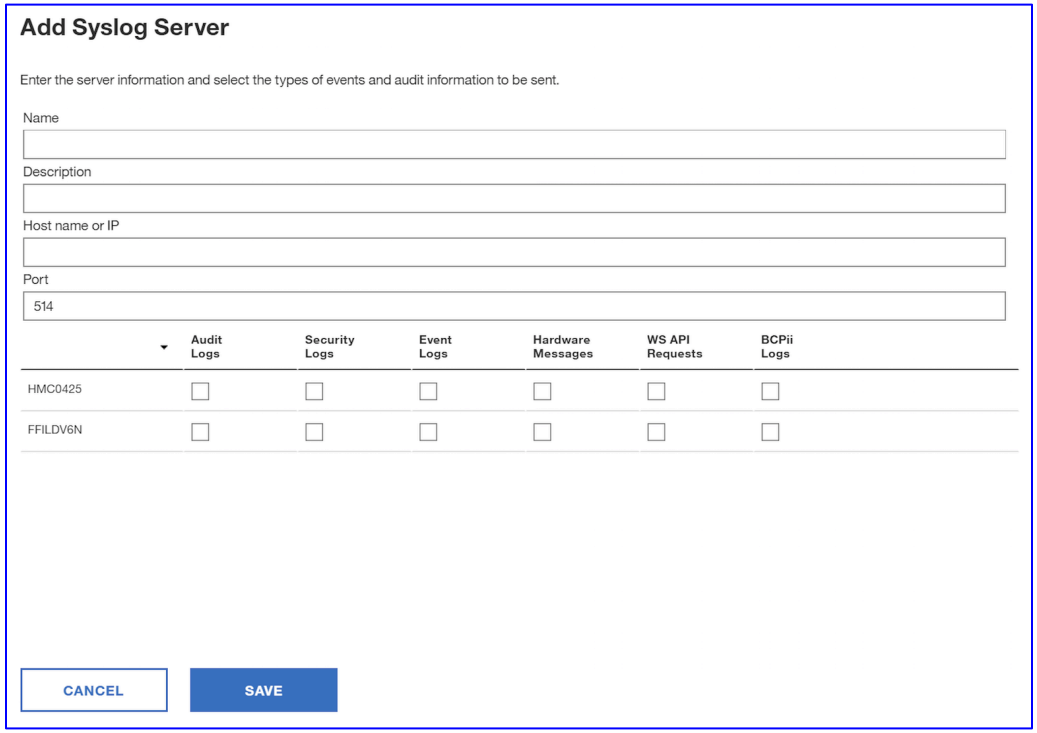
- New HMC *Manage Syslog Servers* task
  - allows specification of a list of remote syslog servers as targets for
    - the HMC itself as well as for any managed CPC (SE) (2.15.0 or newer)
  - **Note:**
    - Currently must configure each additional HMC uniquely
      - Or recommend using HMC Data Replication and configure one HMC/replicate
    - When configuring a 2nd HMC, any previous CPC (SE) configurations will be shown with the previous customization settings
      - which can also be altered further

- For each remote syslog server you must specify:
  - The server
  - The port where the server is listening for syslog messages
  - Which of the 6 supported logs types should be forwarded
    - For each server you may select any mix of the 6 log types,
      - from a single type to all types

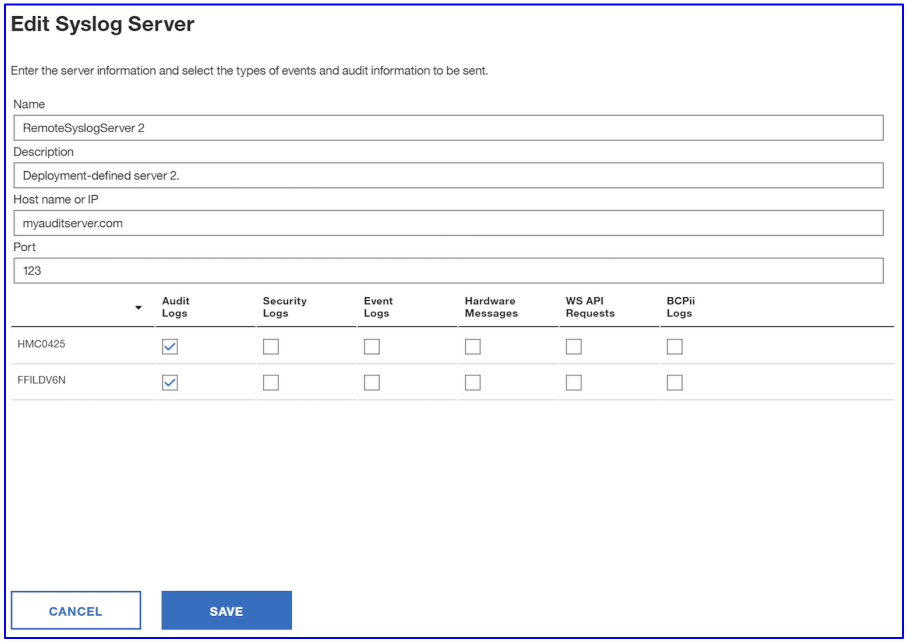
- The task configures rsyslog to do the forwarding.

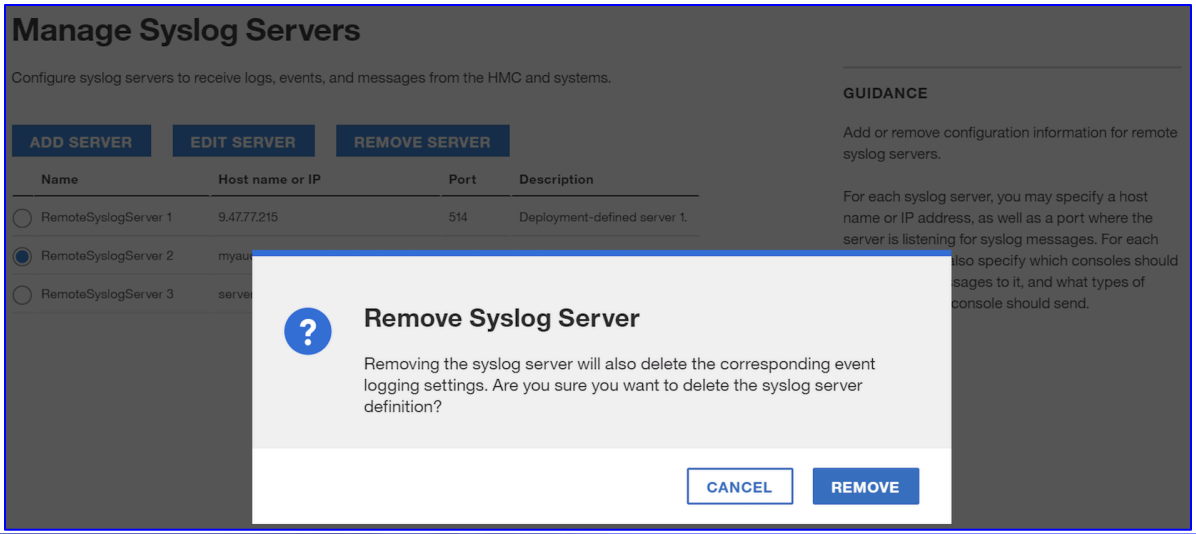
Manage/Add Syslog Servers



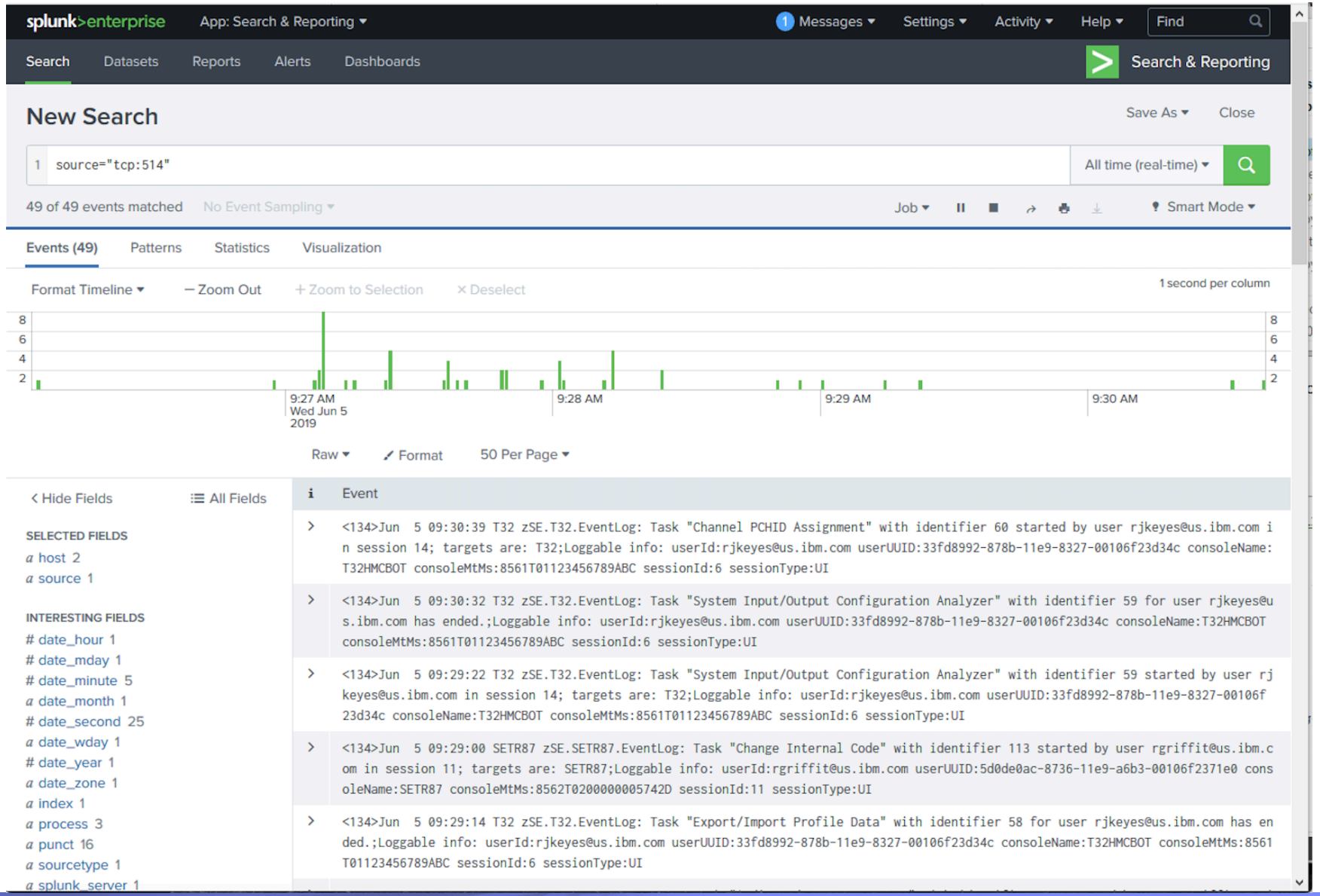


Edit/Remove Syslog Servers





Splunk Example Data

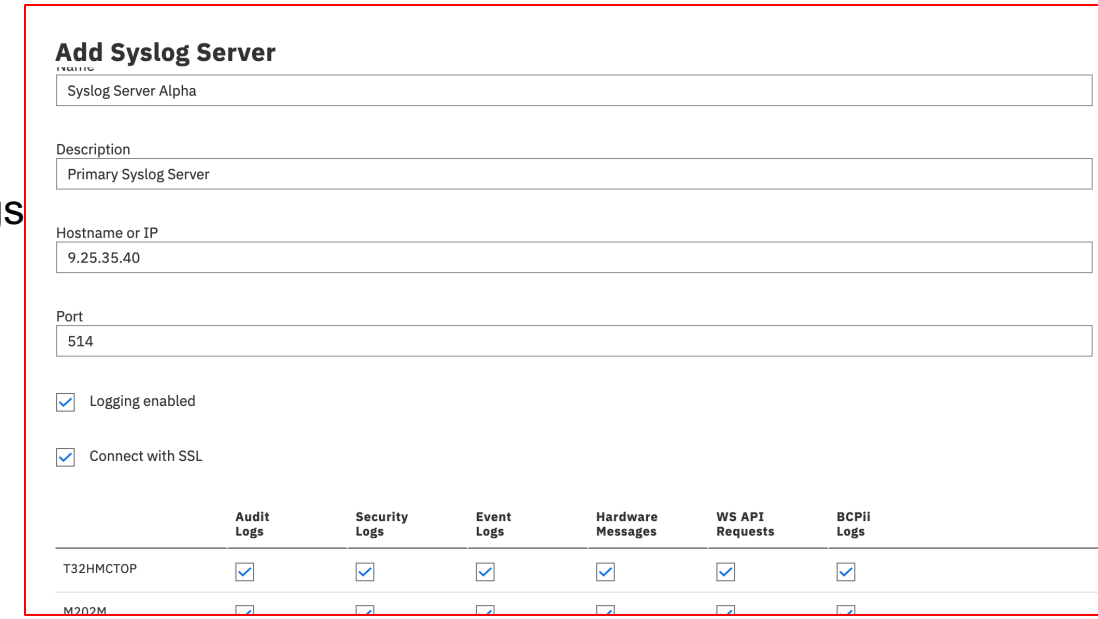


Forwarding connectivity

- **Recommendation:** HMC to SE network is isolated to HMC to SE/CPC network traffic
  - **Net result:** Forwarding from the HMC and SE work differently although they are configured in the same manner
    - *HMC:* For each configured remote syslog server, the HMC must have connectivity directly to the server.
    - *SE:* For each configured remote syslog server, there must be a managing HMC that has connectivity to that server.
      - **If there is such an HMC**, the SE will discover it automatically and proxy the forwarding through it.
        -- This is conceptually similar to SE tasks that support FTP today: the FTP traffic is automatically proxied through a capable discovered managing HMC.
      - **If an SE cannot locate an HMC** with connectivity, or if an **HMC does not have connectivity for its own logs**,
        - a rolling buffer of logs is kept for forwarding when connectivity is restored.
        - This exploits buffering capability built into rsyslog.

Remote Syslog Server enhancements

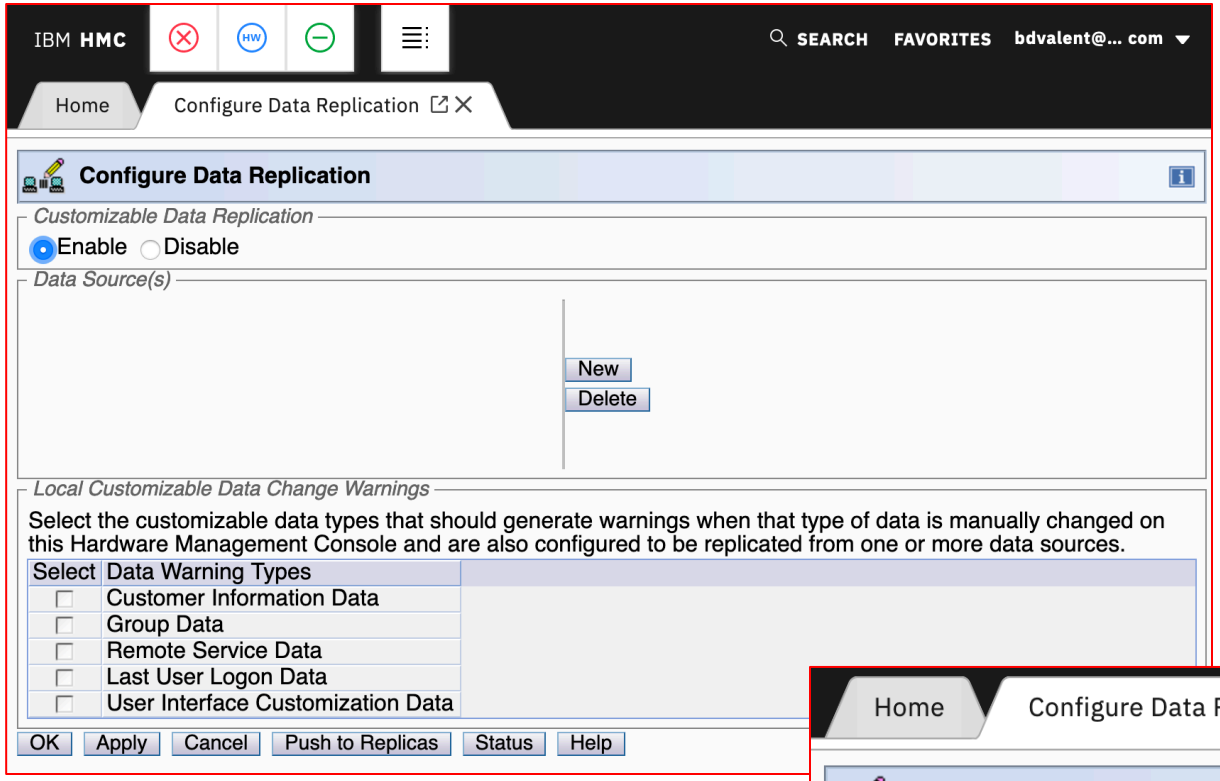
- z15 Initial Support
  - Configure rsyslog to forward selected consolidated syslog entries from the HMC or managed SEs to customer-controlled syslog servers
    - Audit logs
    - Security logs
    - Console events
    - Hardware messages
    - Web Services API request logs
    - BCPii logs

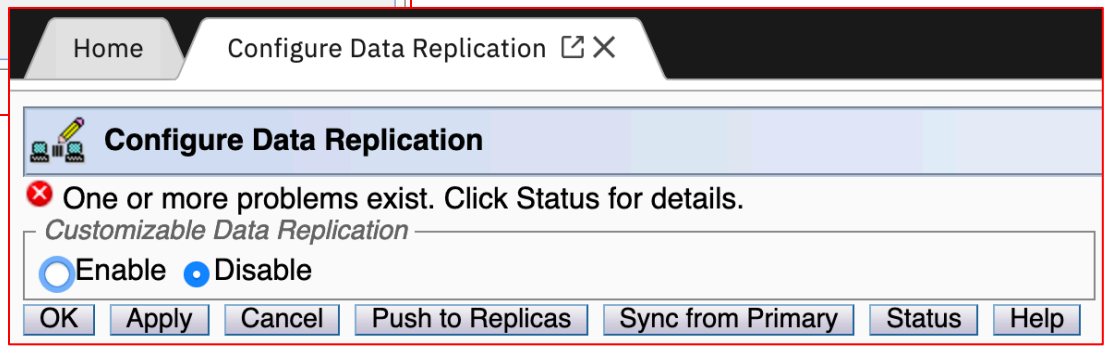


- Enhancements
  - z14 CPC support in addition to z15 CPC
  - HMC Data Replication support
  - Support of SSL connections between HMC and syslog server
  - Support *IBM QRadar DSM for IBM Z Hardware Management Console*

HMC Data Replication Terminology Change

- HMC Data Replication Terminology Change
  - Master/Slave HMCs => Primary/Replica HMCs





HMC Support of new SE Tasks/Channel Objects

HMC Function Addition to address SE Userid Security

- Prior to z15:
  - **Most clients did NOT create Unique SE Userids for task/object access**
    - On SOO (Single Object Operations) =>
      - SE Userid defaults inherited from HMC calculated user authority
      - Didn't always get intended default user role

- Starting with HMC 2.15.0 & z15 CPC,
  - **Consolidated User Management at HMC for HMC & SE**
  - **Single Object Operations (SOO) users and permissions carried over from HMC**
  - **Additional SE tasks on the HMC**

- Once at z15 CPC
  - **Remove any explicitly created SE users using SE User Management and SOO**
    - Should consider removing SE Default users
      - IBM intent will be to remove those default users on SE in a future code release
  - **Defer all User Management to HMC User Management**
  - **Stop using default users (eg, SYSPROG)**
    - Create unique users for all individuals even if you base them on default user roles
      - Important for Security Controls & Audit
  - Use HMC Data Replication for HMC/SE Consolidated User Management

User Management - continued

- **Managed object permissions**
  - Object Type
    - All HMC & SE object types supported (includes CHPID, CRYPTO, FID, & CP now)
  - Object instance
    - Only supported for HMC object types (includes PCHIDs now)

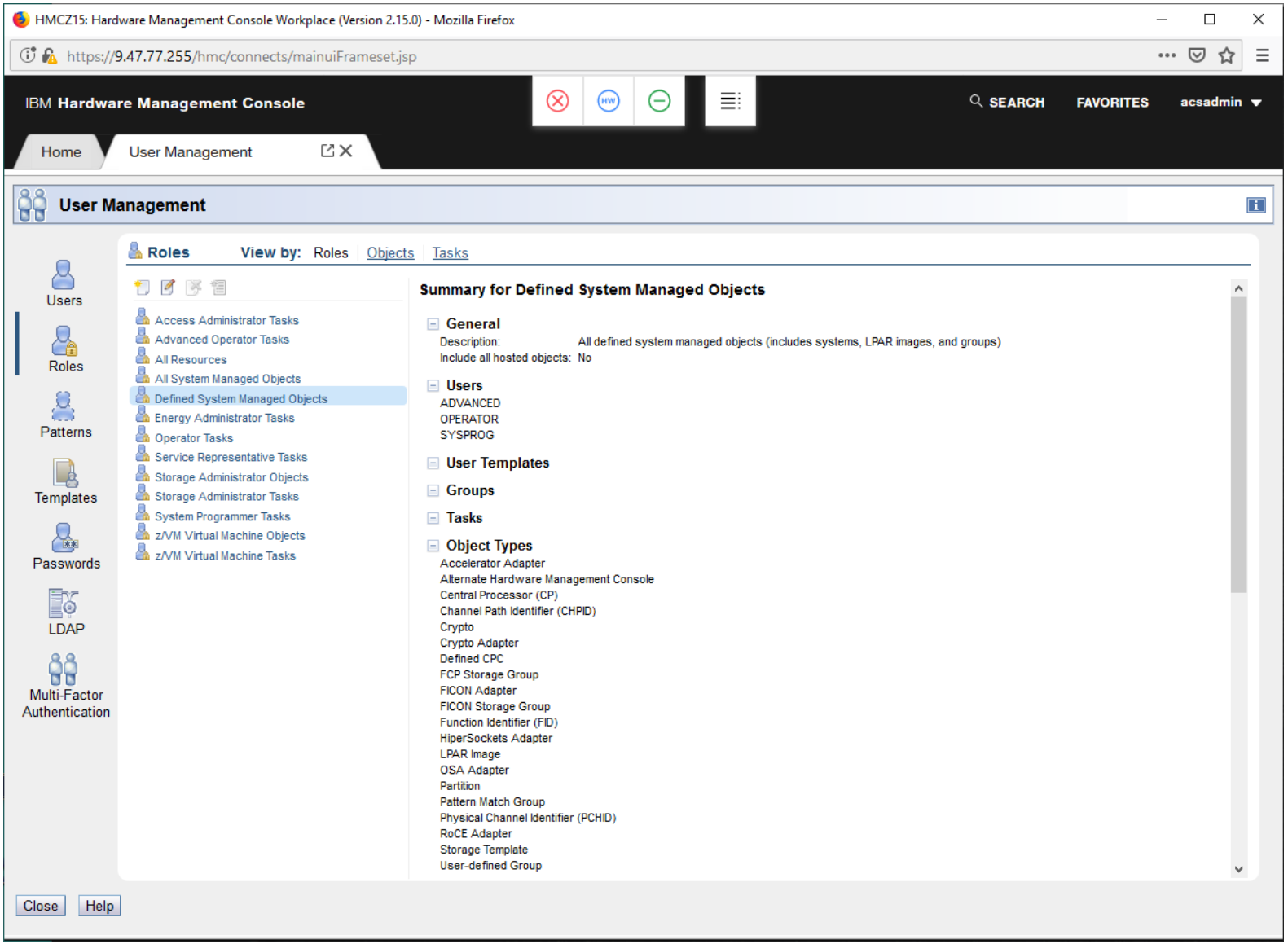
- **System defined roles on HMC updated to contain unique SE tasks**
  - **Note for customized roles:**
    - Must enhance them now include new HMC tasks and any SE tasks
    - SE no longer inherits user roles, but takes what is defined in HMC role for HMC and SE tasks!

- **Net:**
  - HMC can be a single point of control for user/permission management,
    - especially when coupled with data replication on the HMC

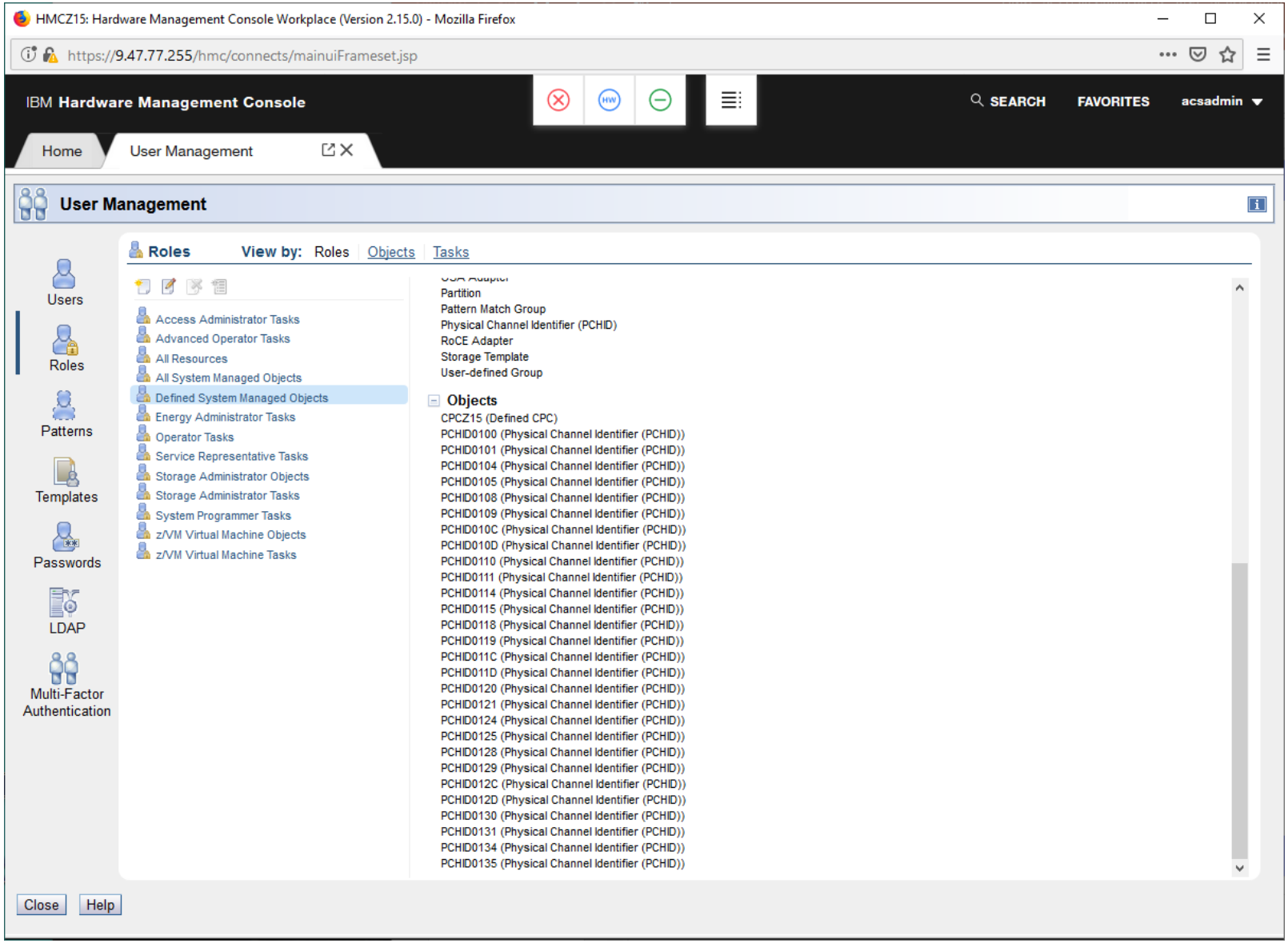
User Management - continued

- **Managed object permissions**
  - Object Type
    - All HMC & SE object types supported (includes CHPID, CRYPTO, FID, & CP now)
  - Object instance
    - Only supported for HMC object types (includes PCHIDs now)
- **System defined roles on HMC updated to contain unique SE tasks**
- **Net:**
  - HMC can be a single point of control for user/permission management,
    - especially when coupled with data replication on the HMC

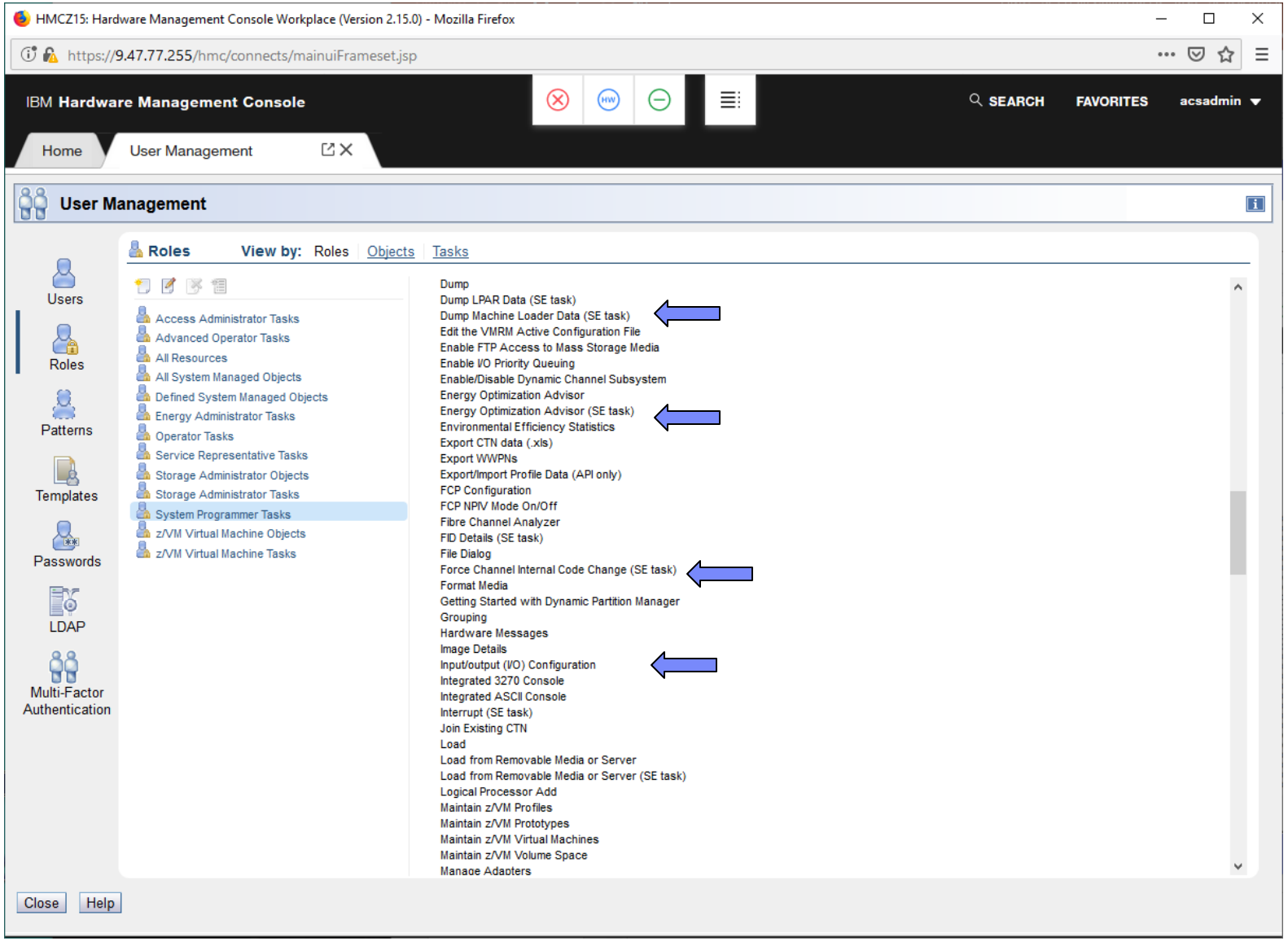
Managed Object Types



PCHID Objects



Support Element Tasks



Single Object Operations (SOO)

- **No more use of SOO interpreted level users on the SE**

- **What user and permissions are used for SOO?**
  - If matching user exists on SE, SE user is used (existing behavior)
  - If matching user pattern/template exists on SE, it is used (existing behavior)
  - Otherwise, utilizes HMC user/permissions

- **Steps to single point of control for user management**
  - Eliminate default users on SE (i.e. OPERATOR, SYSPROG, etc.)
    - The removal will carry forward on future machine upgrades
  - Eliminate any unique users created on SE
  - Move/incorporate SE user patterns/templates into HMC user management
    - still need local access administrator
    - service users should be defined on HMC

- **Note:**
  - If log on locally at SE KMM, HMC users are available for logon

Additional SE tasks/objects now on HMC

- **Starting with z15 targeted CPCs,**
  - Additional SE tasks are now available on the HMC user interface
  - PCHID objects available on the HMC
- **Long term intent**
  - Migrate all SE tasks to HMC
  - Potentially eliminate most SE task launch directly from SE local logon
    - Other than Guided Repair actions for Service
- **Most I/O & Crypto Problem Determination & Configuration should be possible via additional tasks and PCHIDs/Cryptos on HMC**
  - Will work with clients to understand scenarios where that isn't the case
- **Note:**
  - These new additional tasks/PCHID objects are not available for CPCs prior to z15

SE tasks now on HMC – CPC targets

Tasks	Target Object
Service Required State Query	CPC
Channel Problem Determination	CPC
Perform Model Conversion	CPC
Advanced Facilities[1]	CPC or PCHID
Input/output (I/O) Configuration	CPC or LPAR
Cryptographic Configuration[1]	CPC
Cryptographic Management[1]	CPC
Channel Interface Tests	CPC
Channel PCHID Assignment	CPC
Redundant I/O Interconnect Status and Control	CPC
Storage Information	CPC
View LPAR Cryptographic Controls	CPC
FCP Configuration	CPC
Query Channel/Crypto Configure Off/On Pending	CPC
View Internal Code Changes Summary	CPC
Manage PCI System Services	CPC
Display Adapter ID	CPC
Enable/Disable Dynamic Channel Subsystem	CPC
Update PCI Adapter Internal Code	CPC
Query Coupling Facility Reactivations	CPC

1. *Includes “view only” version of task*

SE tasks now on HMC – LPAR targets

Tasks	Target Object
Input/output (I/O) Configuration	CPC or LPAR
Change LPAR Cryptographic Controls	LPAR

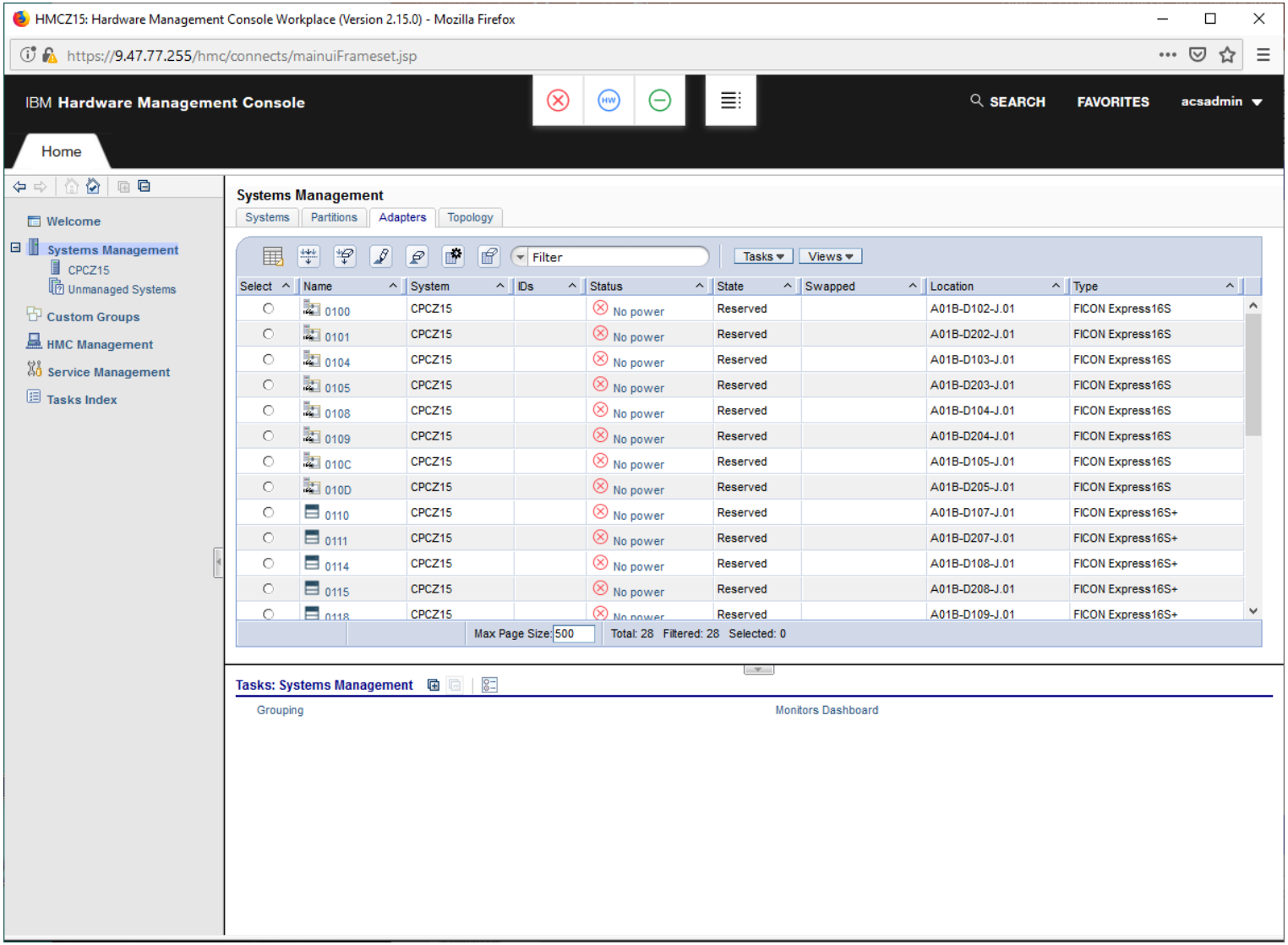
1. *Includes “view only” version of task*

SE tasks now on HMC – PCHID targets

Tasks	Target Object
Configure On/Off[1]	PCHID
PCHID Details	PCHID
Advanced Facilities[1]	CPC or PCHID
Show LED	PCHID
Service On/Off	PCHID
Reset Error Thresholds	PCHID
FCP NPIV Mode On/Off	PCHID
Network Traffic Analyzer Authorization	PCHID
Release I/O Path	PCHID

1. *Includes "view only" version of task*

PCHID Objects on the HMC



New HMC View Only support

View Only Users

- ***View Only tasks for HMC***
  - *The HMC and SE User support added the ability to create users who have View Only access to select tasks.*
  - *The View Only tasks are simply the full function tasks with minor modifications to their GUI controls which prevent any actions from being taken. The following subset support a View Only version of the task. The **User Management** task, Roles navigation, indicates these tasks as such with the "(view only)" indication following the task name.*
    - ***HMC Tasks:***
      - *Hardware Messages (view only)*
      - *Operating System Messages (view only)*
      - *View Activation Profiles*
      - *Manage System Time (view only)*
      - *Manage Coupling Facility Port*
        - *Enablement (view only)*
      - *OSA Advanced Facilities (view only)*
      - *Advanced Facilities (view only)*
      - *Configure Channel Path On/Off (view only)*
      - *Configure On/Off (view only)*
      - *Cryptographic Configuration (view only)*
      - *Cryptographic Management (view only)*
  - ***To support View Only users:***
    - *When adding tasks into a new Role, the option of adding the View Only version of that task is provided.*
    - *The Access Administrator can then specify these Roles to create View Only users if desired.*

Integration of IBM MFA for z/OS & Support for RSA SecurID

Background – z14 MFA Support

- Additional authentication factor: TOTP (Time-based One-Time Password)
  - Provided by user's smartphone/desktop app (e.g., Google Authenticator)
- Standalone solution
  - TOTP validated by the console (HMC/SE/TKE 2.14.0)
- Optional, configurable on a per-user/template basis
- No change to logon password requirements
- GUI and APIs

z15 Requirements

- Customer requests
  - “**zHMC Multi-Factor Authentication - RSA Token**”
    - Requesting an additional authentication factor:
      - RSA SecurID token
- Must work with LDAP logon password validation
- Must work with User Patterns and User Templates

Solution

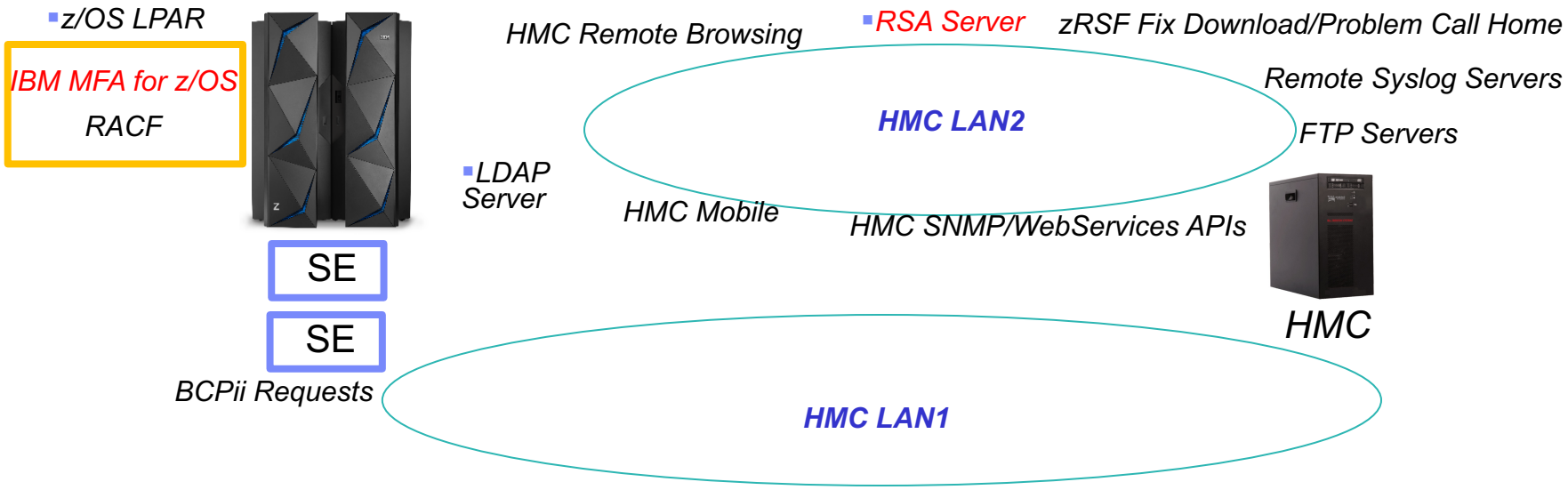
- Integrate HMC authentication and IBM MFA for z/OS support
  - **Allow RSA SecurID**, in addition to HMC logon password
  - **Leverage MFA support in z/OS** and **RACF***
    - Centralized MFA support via IBM MFA server (“IBM MFA”)
      - Same as for TSO and other MFA-enabled z/OS applications
    - HMC supports RSA SecurID only
  - **HMC validates logon password (no change)**
    - Could involve LDAP server (no change)
  - **IBM MFA validates RSA SecurID passcode**
    - Requires RSA authentication server
  - **HMC only** - not supported on SE or TKE
    - * RACF or compatible external security manager (e.g. TopSecret, ACF2)

Solution (Cont.)

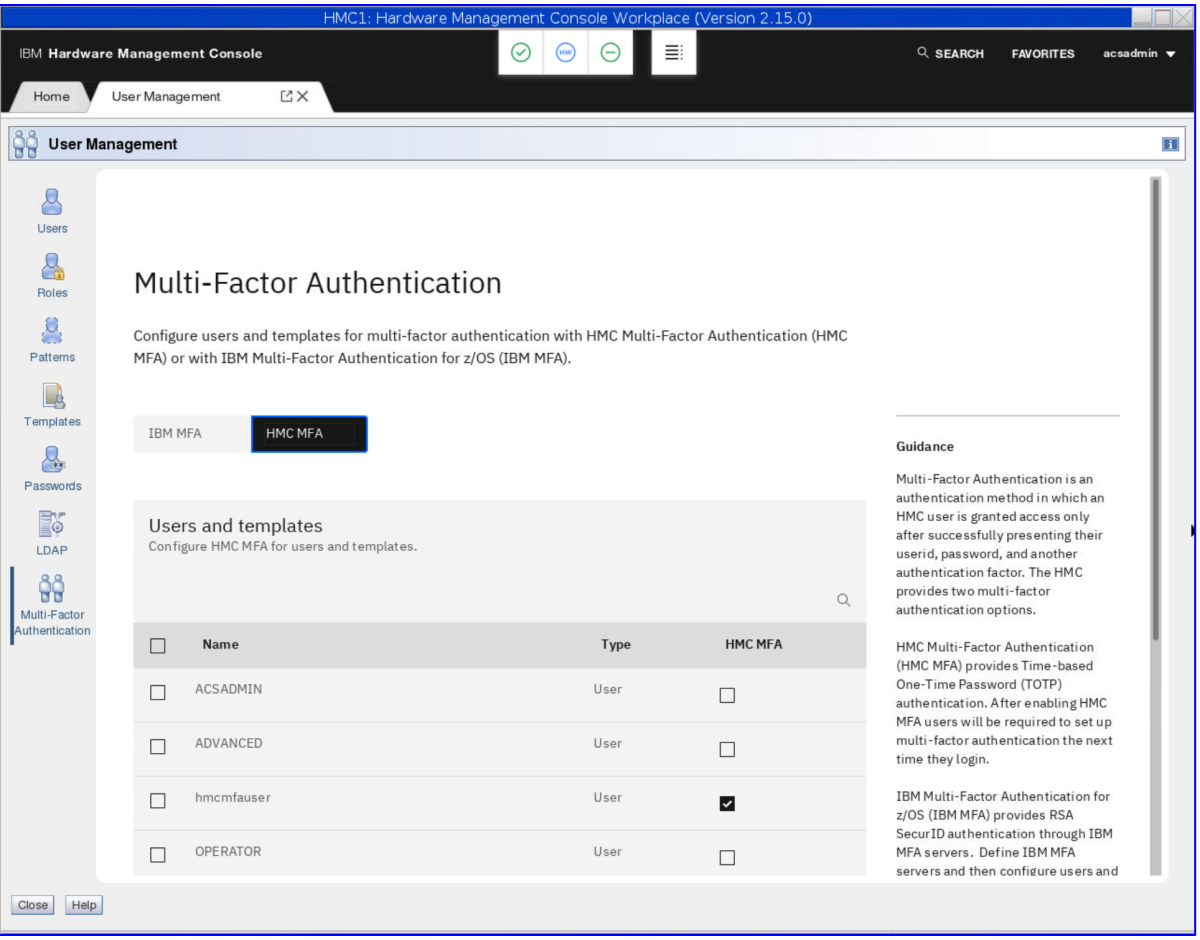
- Customer must provide:
  - “IBM Multi-Factor Authentication for z/OS” V2
  - RACF or equivalent
  - RSA authentication server and RSA SecurID tokens (hard or soft)
  - Network connectivity HMC -> IBM MFA on z/OS -> RSA server
- No change to “*Compound Inband Authentication*” approach
  - HMC logon password =
    - Password/PIN concatenated with MFA tokencode
  - Verified by LDAP server
- User Interface & Web Services API enhancements for new support

zHMC with IBM MFA on z/OS

- HMC 2.15.0 will provide RSA SecurID authentication
  - Via centralized support from IBM MFA for z/OS
  - MFA policy defined in RACF and assigned to RACF user IDs
  - RSA SecurID passcode verified by RSA authentication server

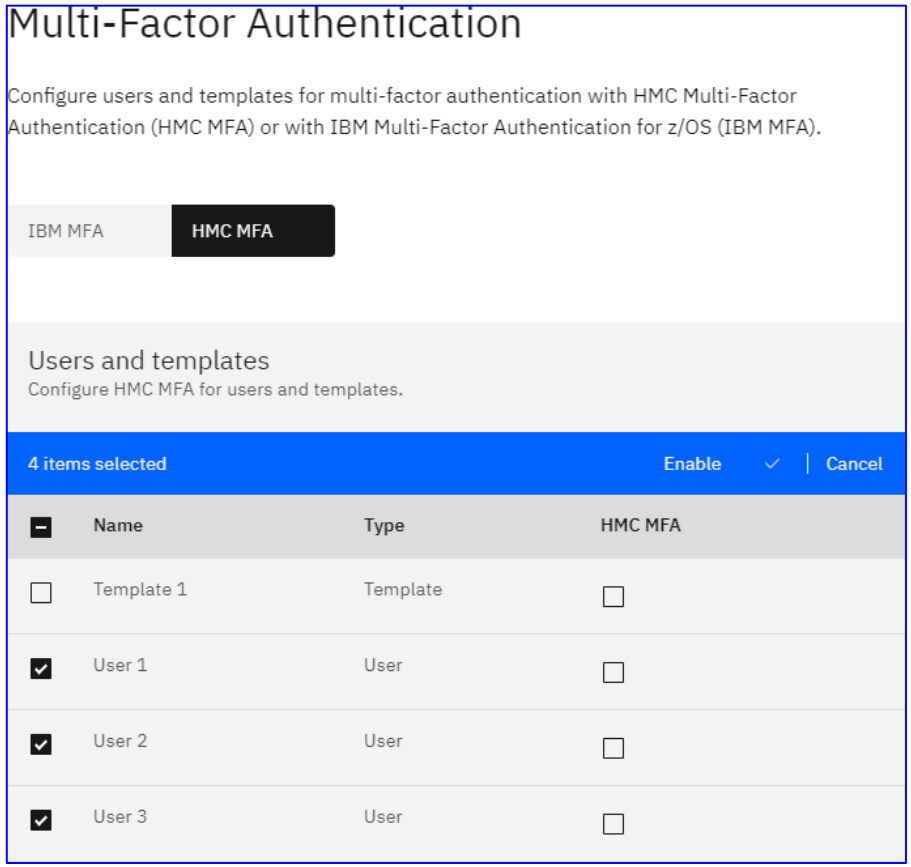


User Management – MFA Tab

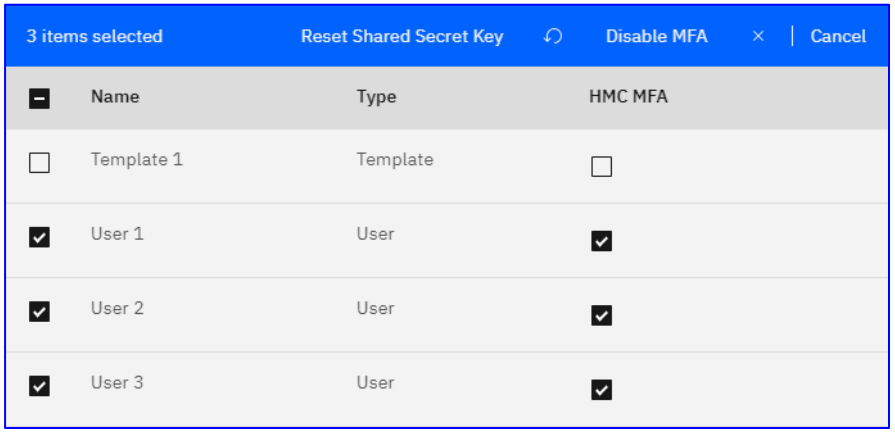


- User Management Multi-Factor Authentication tab updated to support both
  - HMC MFA (Local TOTP MFA)
  - IBM MFA

User Management – MFA Tab – HMC MFA

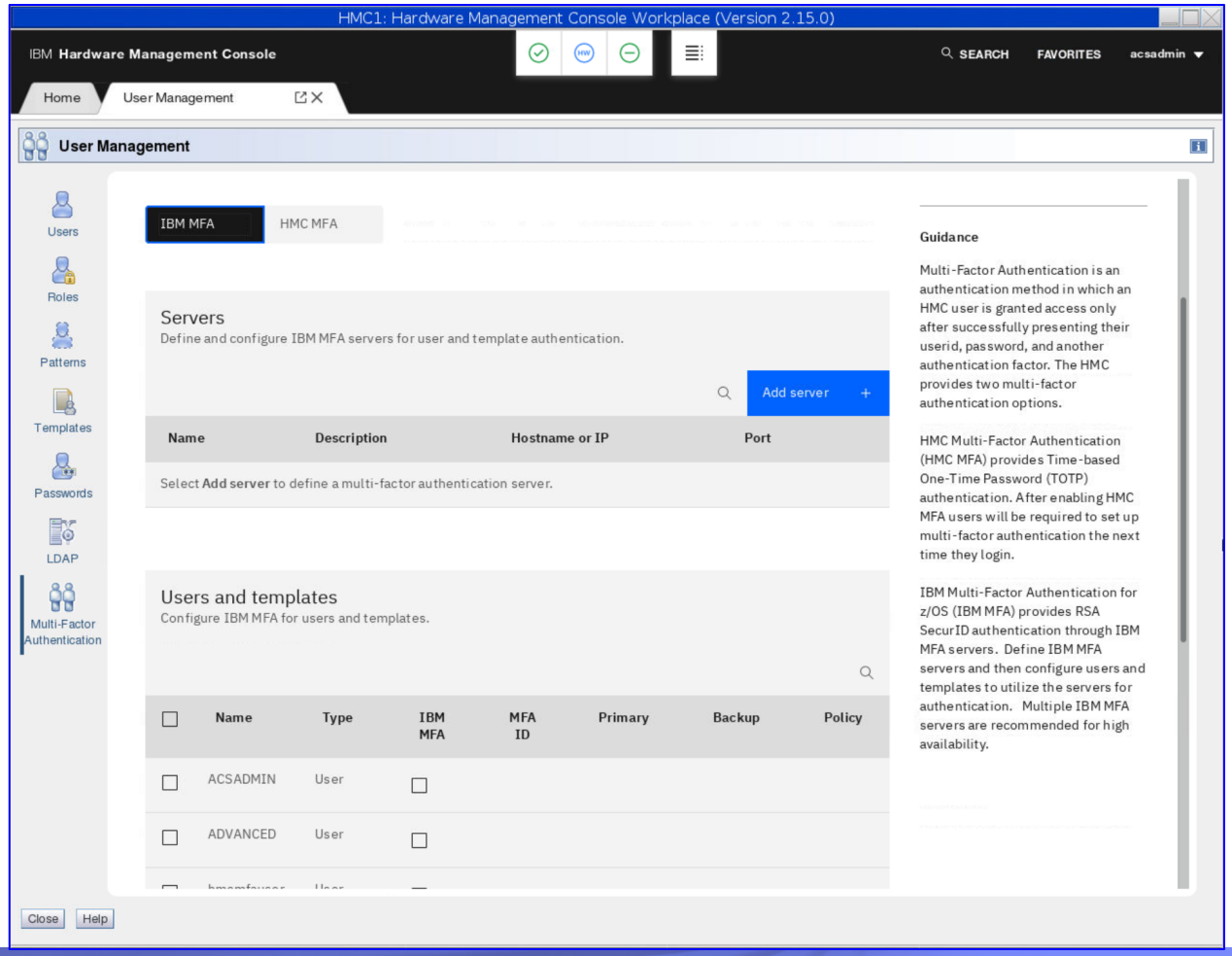


- HMC MFA section allows administrator to configure HMC MFA (local TOTP) for multiple users and templates
  - If HMC MFA is not enabled for the selected users and templates,
    - Enable action is available
  - If HMC MFA is enabled for the selected users and templates,
    - Disable and Reset Shared Secret Key actions are available

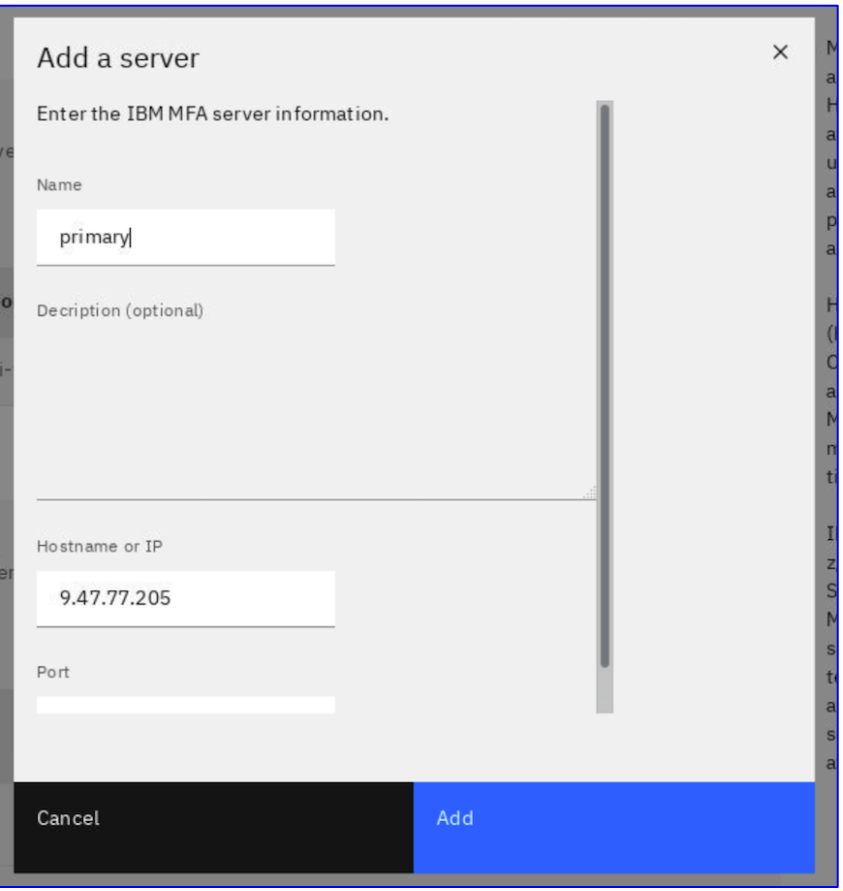


User Management – MFA Tab – IBM MFA

- IBM MFA section allows administrator to manage IBM MFA servers, users, and templates



User Management – MFA Tab – IBM MFA - Servers

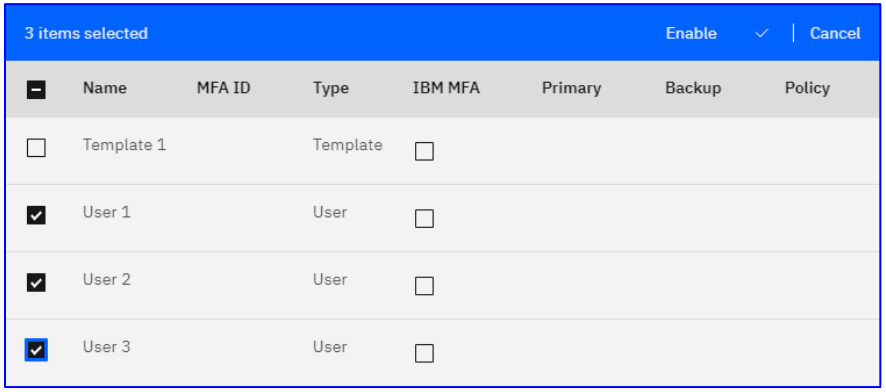


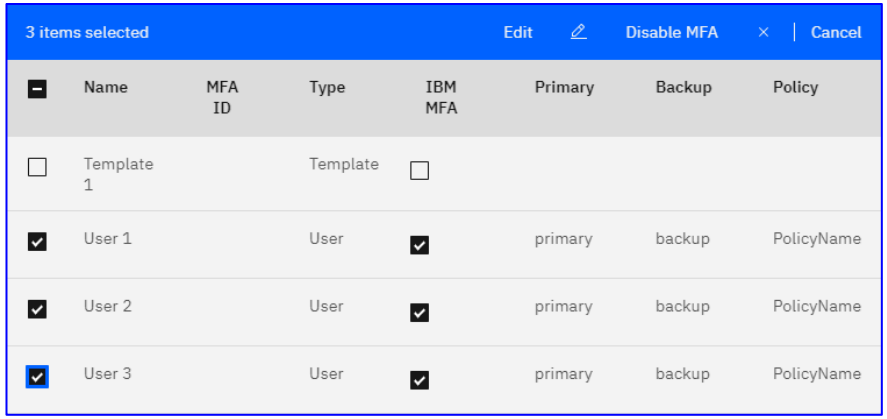
- IBM MFA section includes a table to manage IBM MFA servers
  - Add new servers
  - Edit and test existing servers
  - Remove existing servers

Edit/Test | Remove | 1 item selected | Cancel

	Name	Description	Host name or IP	Port
◉	Server 1	Main primary	main@ibm.com	443
○	Server 2	Main secondary	main2@ibm.com	443
○	Server 3	Tertiary backup	tertiary@ibm.com	443

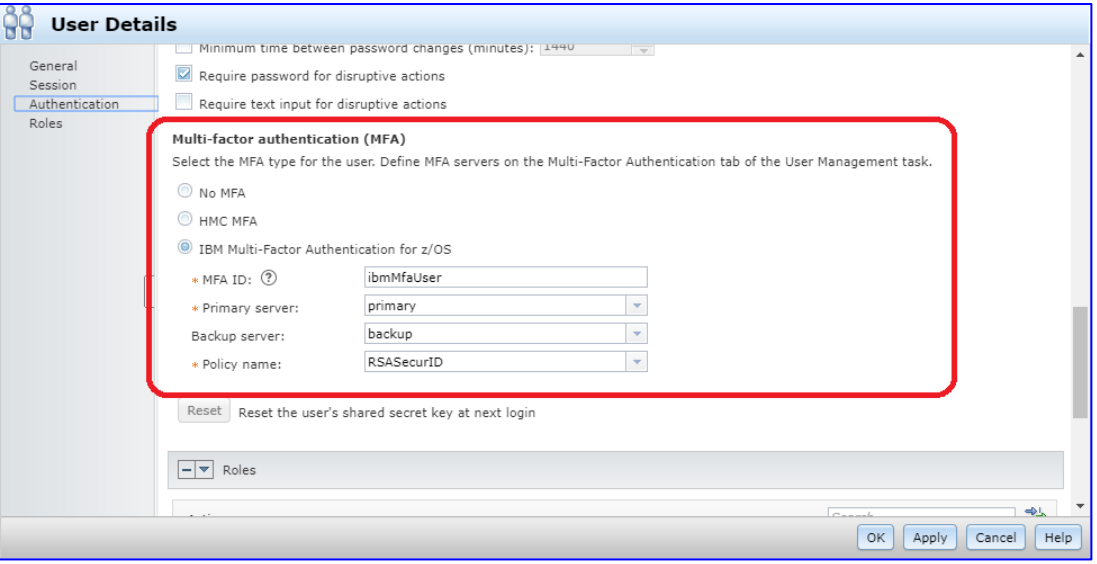
User Management – MFA Tab – IBM MFA – Users/Templates





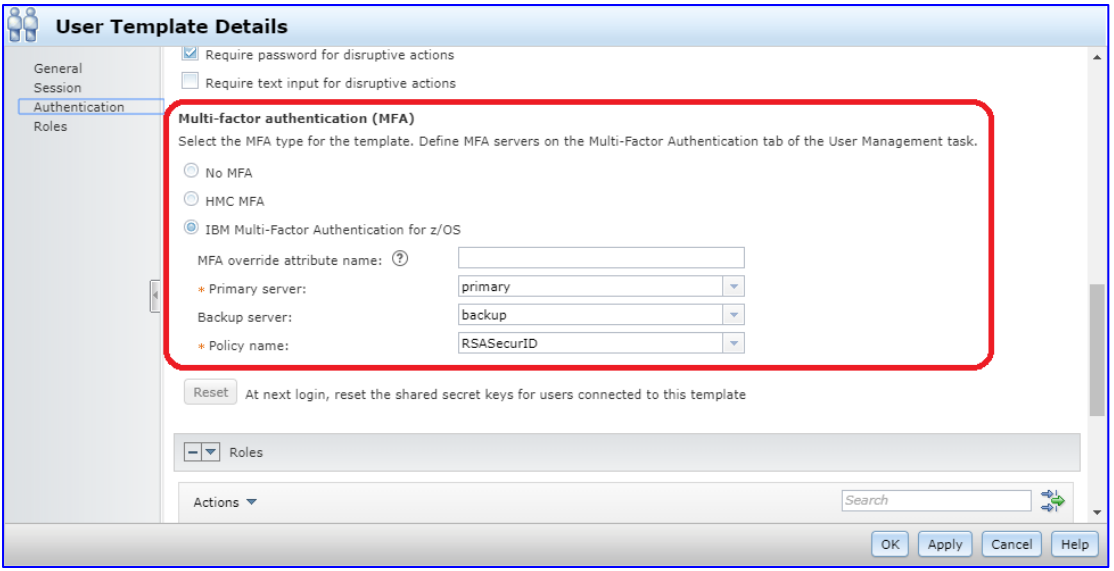
- IBM MFA section allows administrator to configure IBM MFA for multiple users and templates
  - If IBM MFA is not enabled for the selected users and templates,
    - Enable action is available
  - If IBM MFA is enabled for the selected users and templates,
    - Disable and Edit actions are available

User Management – User Definition



- 3 MFA choices
- IBM MFA
  - MFA ID
    - **Default:** HMC user ID
    - RACF ID
  - IBM MFA servers
  - RACF policy
    - RSA SecurID factor only

User Management – User Template Definition



- 3 MFA choices
- IBM MFA
  - MFA ID
    - **Default:** HMC user ID
    - MFA ID override
      - LDAP attribute name
  - IBM MFA servers
  - RACF policy
    - RSA SecurID factor only

Integrated 3270 Console Security & Performance

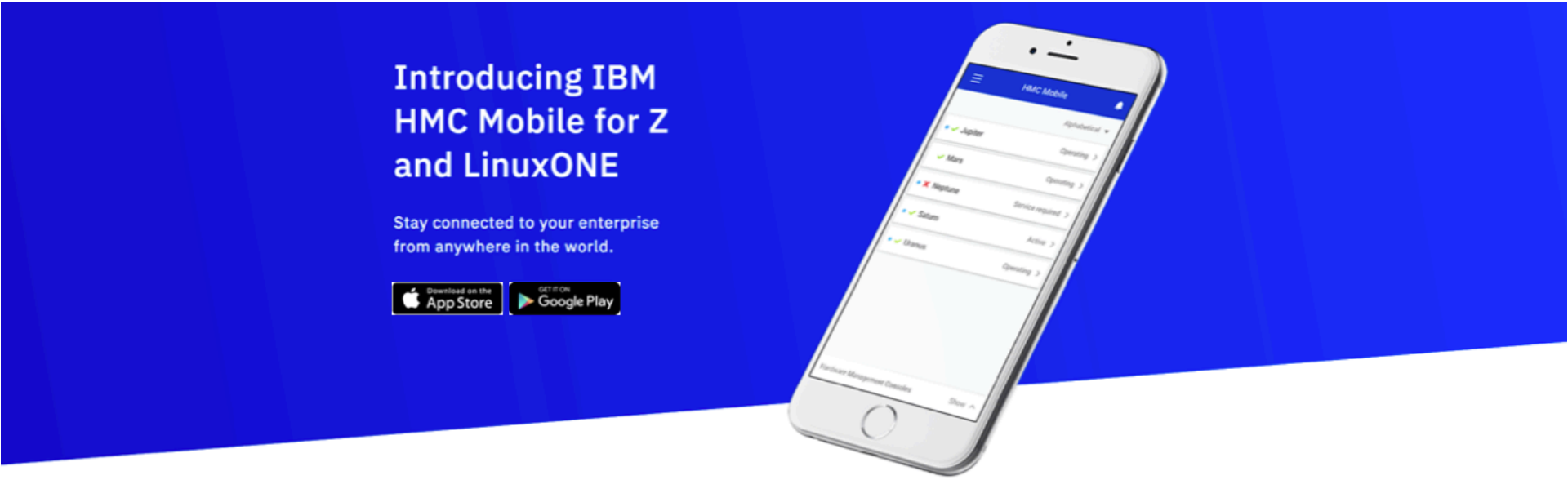
Integrated 3270 Console Security & Performance

- RACF Security for z/VM & z/LINUX
  - HMC User Logon for both
    - Operating System Messages & Integrated 3270 Console
- z/OS Console Security via HMC tasks
  - **Operating System Messages** (no HMC user logon) => recommendation if used
    - Read Only Users for Monitoring => very limited users for NIP console (R/W)
      - R/W users get *System Console* user authority
  - **Integrated 3270 Console** => RACF security based on user logon

- HMC 2.15.0 Performance Improvements for Integrated 3270 Console
  - HMC 2.13.1 removed Java Applet dependency
    - Performance sluggishness sometimes seen
  - HMC internal framework reworked => Noticeable Performance Improvement
  - Only HMC 2.15.0 required => z15/SE 2.15.0 not required
    - Can order HMC 2.15.0 ECA if don't currently have z15 CPC

IBM HMC Mobile

HMC Mobile Introduction → ibm.biz/hmc-mobile



Keep watch over all your systems and partitions and receive alerts when messages or status changes arise.

Monitor your systems

Access all your systems, even if they are spread across multiple HMCs.

Comprehensive security

Take advantage of a wide range of fully customizable security features.

Getting started is easy!

Try a demo HMC before connecting to your network.

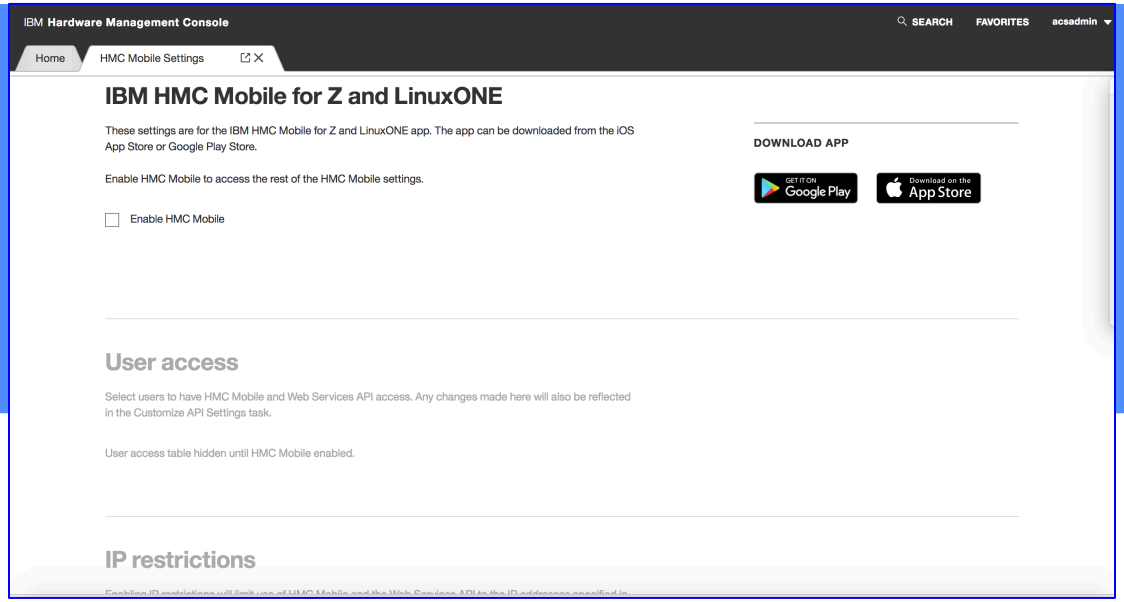
IBM HMC Mobile Security

- Connectivity
  - Device WiFi or VPN access to the Hardware Management Console
  - Network Transport is HTTP over TCP/IP Sockets, TLS 1.2 for connection security
  - App notifications, if enabled, are proxied through IBM RSF Proxy to the Apple/Google Push Notification Services

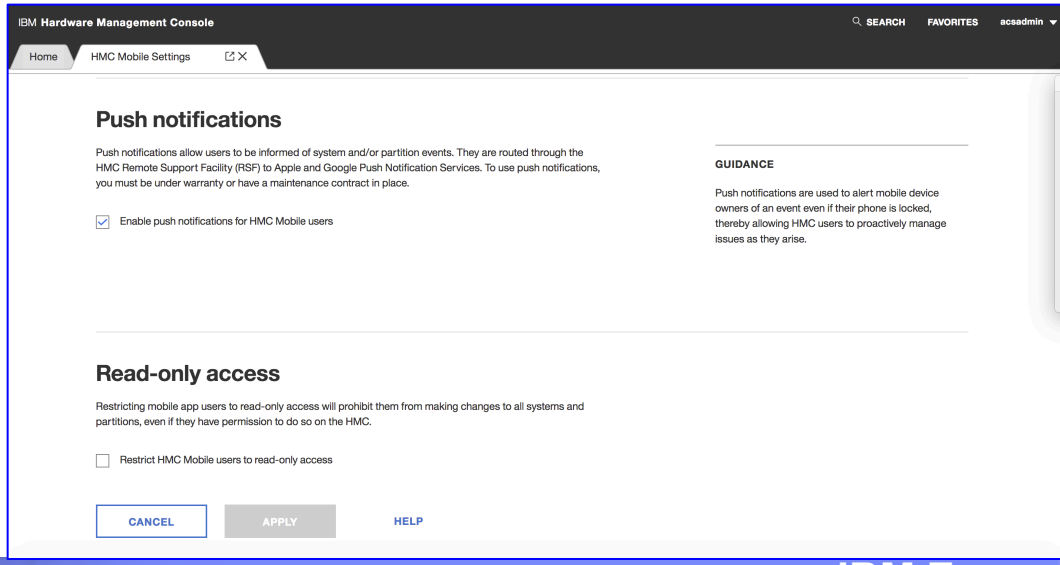
- Controls
  - Disable app access (default)
  - Restrict app access to specific users and IP addresses
  - Multi-Factor Authentication
  - Restrict object access and actions with HMC user and role based authorization controls
  - Disable storage of user authentication password in the device native encrypted keychain
  - Disable all app actions (view-only)
  - Disable app notifications (server side)
  - Require app password

IBM HMC Mobile – z14 Action Permissions – All or None

Enable mobile access



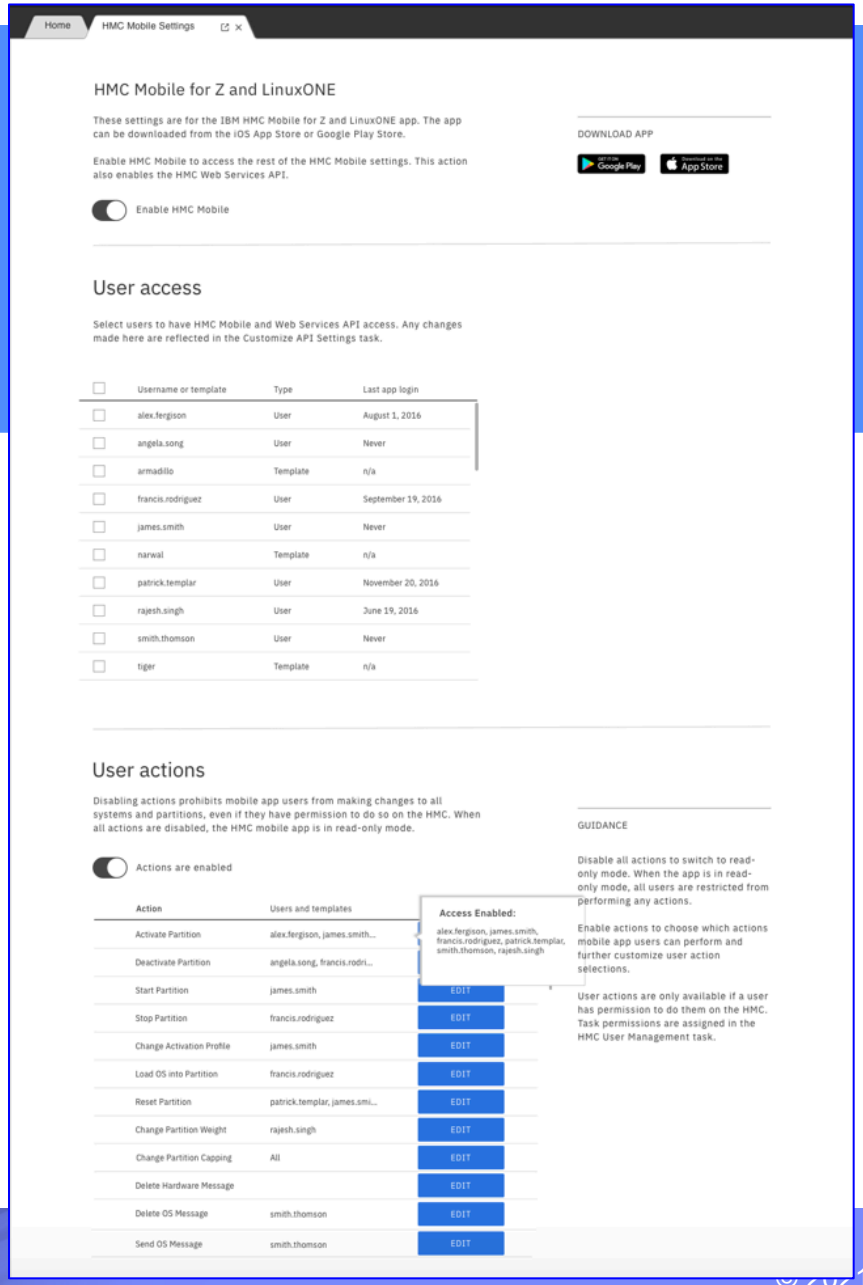
Enable access and tailor settings in the HMC Mobile Settings task.



IBM HMC Mobile – z15 Granular Action Permissions

Granular action permissions

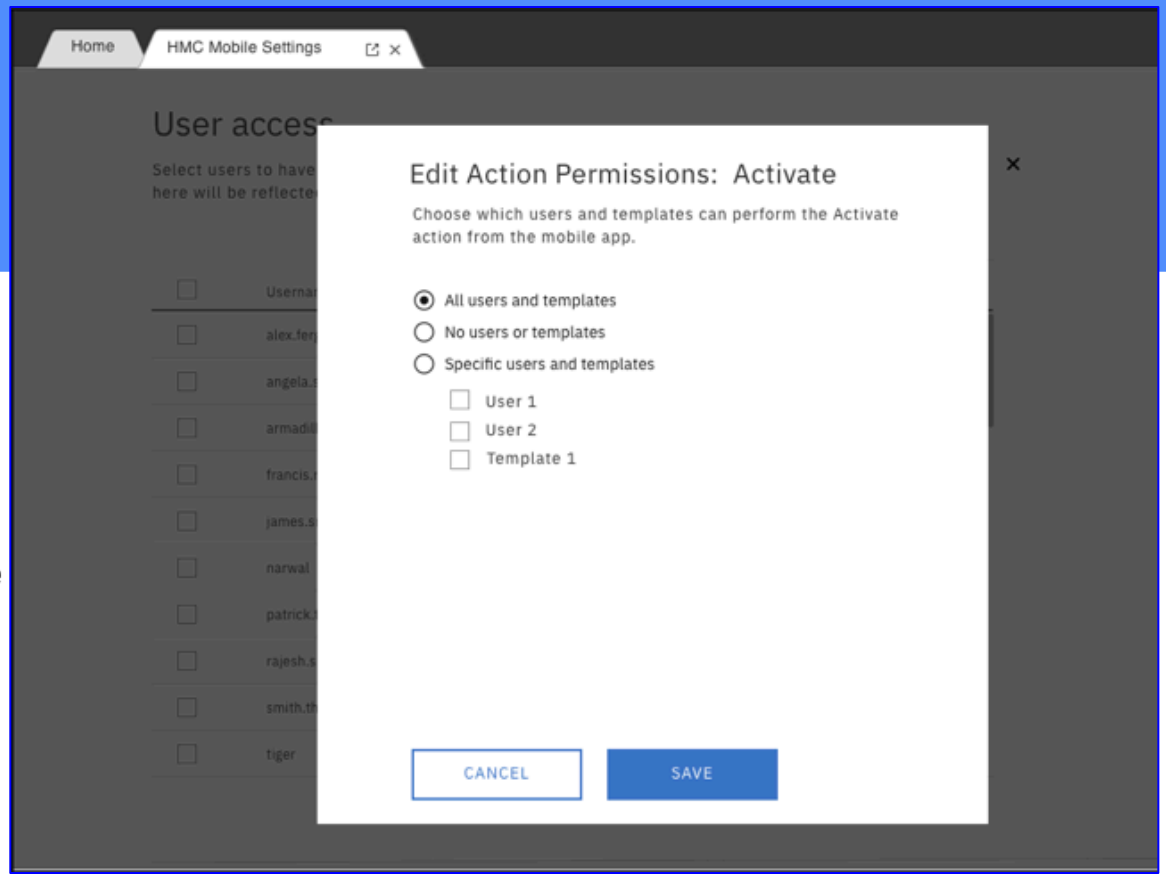
Select which actions users can perform. Disable actions to make the app read-only.



IBM HMC Mobile – z15 Granular Action Permissions

Granular action permissions

Select which actions users can perform. Disable actions to make the app read-only.



IBM HMC Mobile Field Data

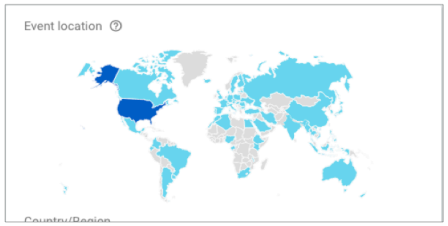
Allows systems administrators to monitor and manage their hardware from anywhere.

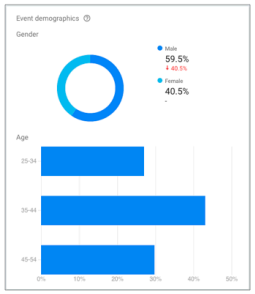
1934 IOS APP INSTALLS

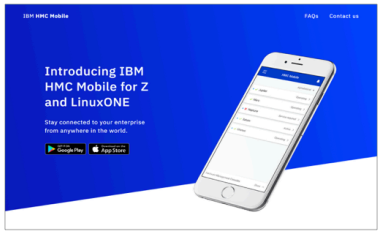
1150 ANDROID APP INSTALLS

14280 PRODUCT PAGE VIEWS

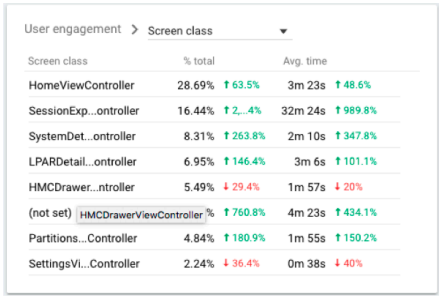
30,308 NOTIFICATIONS PER MONTH

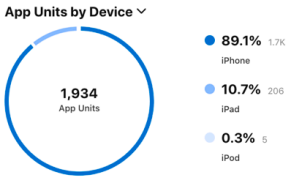






ibm.biz/hmc-mobile





I can't wait to get this on my personal device. It's more convenient and faster to get an answer. the learning curve is great, there isn't one!

When will this be replacing the HMC?

January 2020 CA Password Law

January 2020 CA Password Law – Background

- New California "password law" that bans the use of default passwords in connected devices
  - Internet of Things password law
  - Requires any default shipped passwords to be
    - Changed on installation
    - Or unique per device shipped
  - Full description of law
    - *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327*

- IBM Z Platform Management consoles (HMC, SE)
  - Have default users shipped with default passwords
    - ACSADMIN
    - ADVANCED
    - OPERATOR
    - SERVICE
    - STORAGEADMIN
    - SYSPROG

HMC Security Best Practices

- Pre-defined users exist for out-of-the-box configuration
  - After installation, the default users should be **disabled**, **deleted**, or **have their passwords changed**
    - Consider removing the default users other than ACSADMIN
      - ACSADMIN can also be removed if equivalent user is created from ACSADMIN role
  - Create your own roles (objects/resources and tasks) and users
    - The role assignments of the default users cannot be modified
    - System defined roles cannot be modified
- IBM's recommendation to clients is to have unique users for all consoles, including Service users
  - Only a few clients currently direct unique Service users
- You decide how much to open the console and to whom

California & Probably Future IBM Z System Installs

- Current Law is limited to California for new system installs
  - For now, IBM Z will limit Default User password behavior to CA
  - However, other states are considering similar laws.
  - Very likely that Future IBM Z will require all to change passwords for default users

- Client Considerations => All Default user passwords will require change on 1st logon
  - Need to start planning for a process for this upcoming change!
    - Recommend unique userids per user => audit requirements/best practices
  - Client userids responsible for their passwords
    - ACSADMIN equivalent users can reset passwords if forgotten
  - Need to establish a plan for Service users
    - IBM SSRs (System Serviceability Reps) may be different for various visits
      - Generally, no longer have dedicated SSRs per client
    - IBM SSRs may show up at any time (including middle of night)
      - Planned (firmware update)
      - Unplanned (Repair actions)
  - Should be ready to provide userid and password to SSR upon arrival to IBM Z system
    - Client should maintain list of unique SERVICE IDs and passwords
    - Need an established process to avoid service delay

Fibre Channel Endpoint Security (Authentication & EDiF (Encrypted Data in Flight))

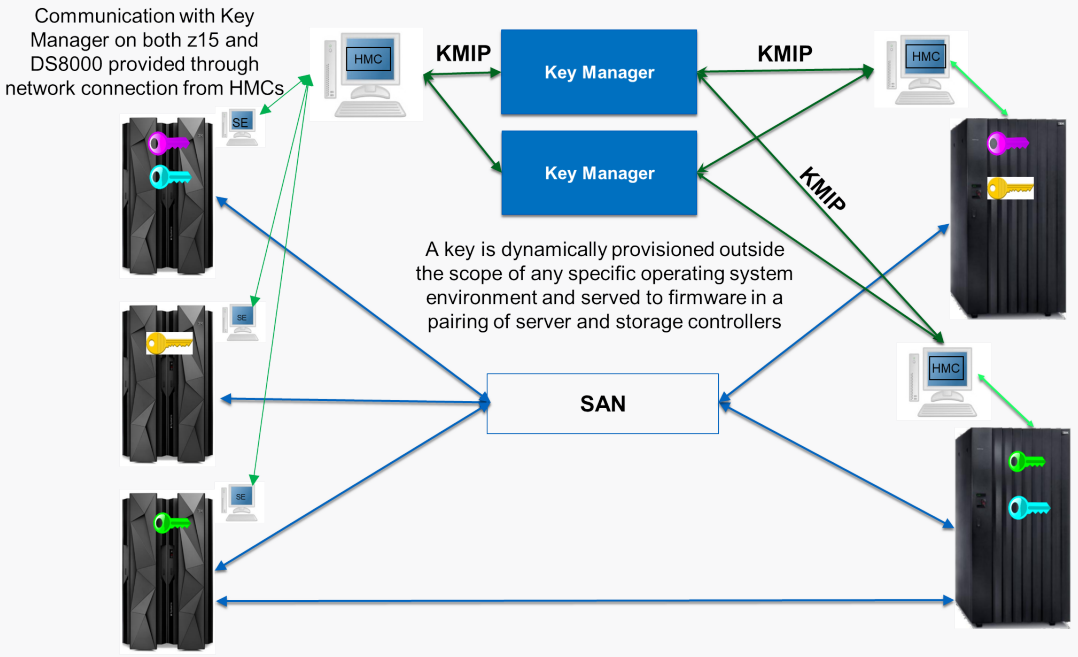
Overview

- An end-to-end solution, requires support from both endpoints
  - IBM Z server channel
  - Storage controller port
- Fibre Channel Endpoint Security includes
  - Endpoint authentication
  - Data encryption
- The solution ensures all data flowing on fibre channel links within the datacenter is protected from unauthorized access.
- No changes required in the operating systems, file systems or applications.

The Big Picture

High Level View

- Provide capability to authenticate/encrypt between IBM Z systems and IBM DS8000 storage controllers
- Secure connections created between systems and external key managers via HMC



KMIP *- Key Management Interoperability Protocol*

Hardware Requirements

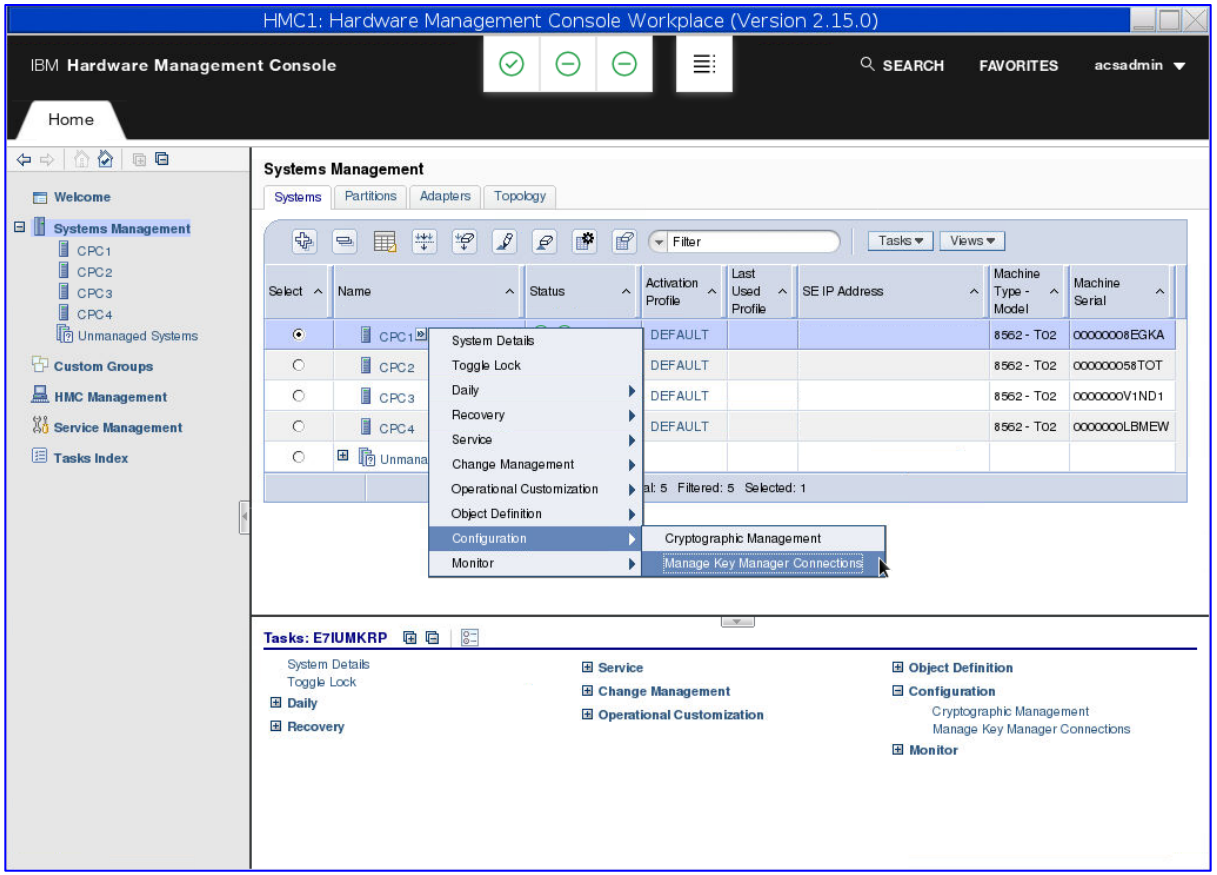
- Encryption-capable and authentication-capable FICON and FCP channels
  - On **FICON Express 16SA** adapter
- Authentication-capable FICON and FCP channels
  - On **FICON Express16S+** adapter
- Neither authentication nor encryption
  - **FICON Express 8S**
  - **FICON Express 16S**

Software and Firmware Requirements

- **z15 server**
  - HMC and SE – 2.15.0
  - FoD – Feature on Demand record installed on SE
  - CPACF – Central Processor Assist for Cryptographic Functions
  - CPC must not be in DPM (Dynamic Partition Manager) mode
- **External key manager** – IBM Security Key Lifecycle Manager 3.0.1.
- **Storage controller** – DS8900F & associated HMC.

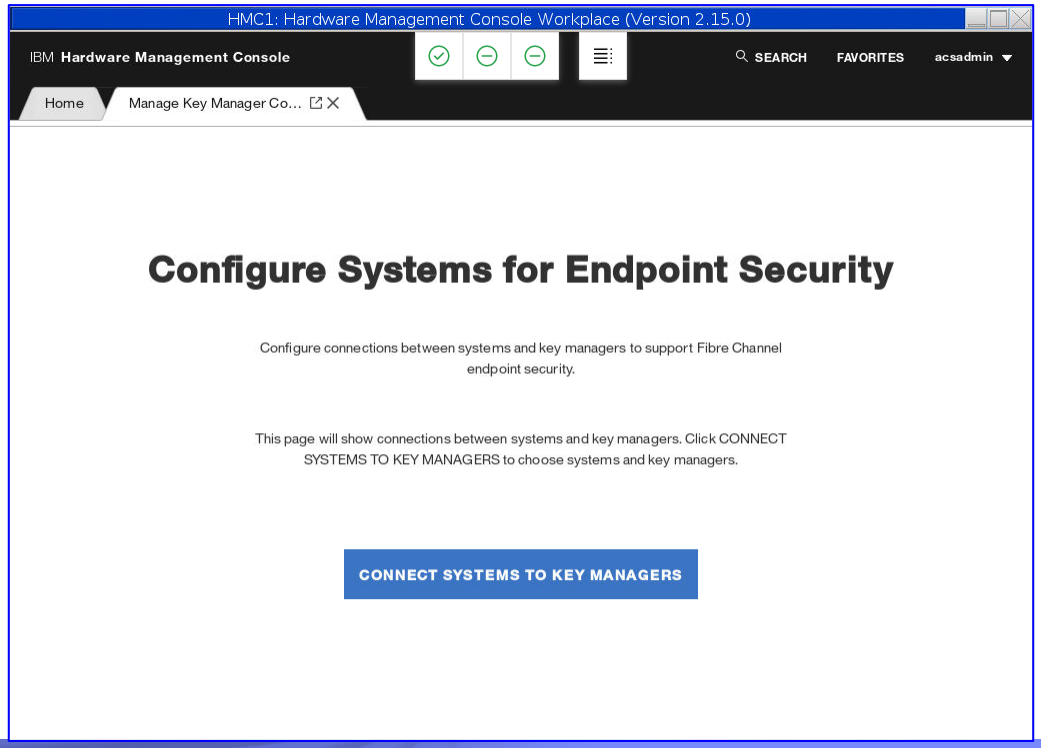
Configuration on the zHMC

- New *Manage Key Manager Connections* task configures Endpoint Security

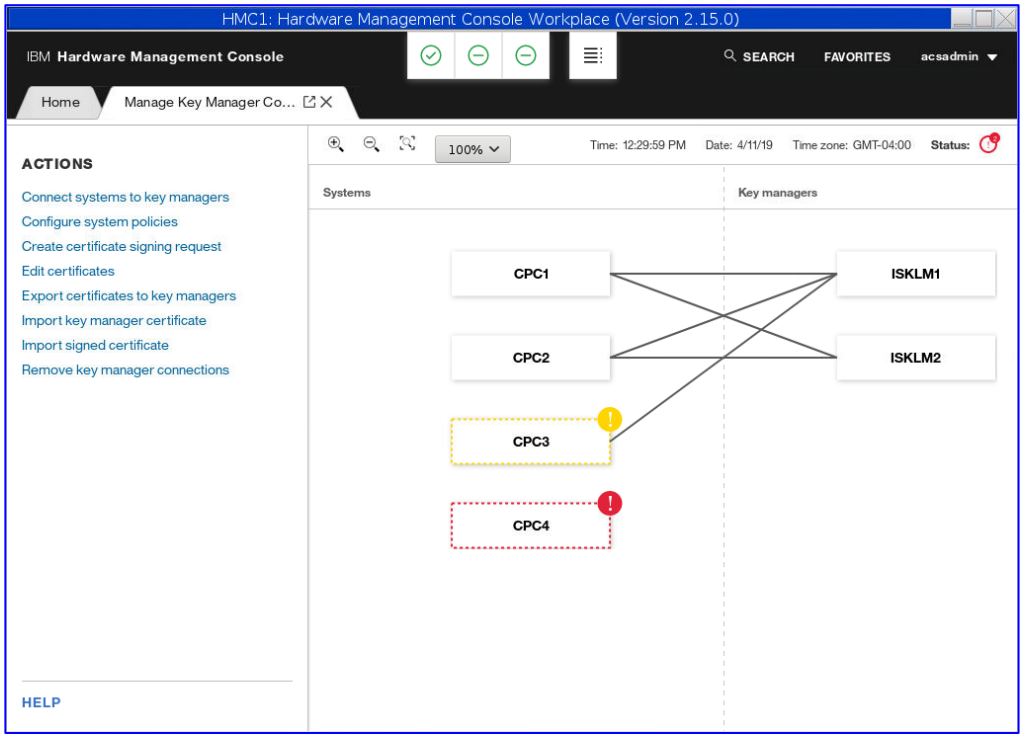


Configuration on the zHMC

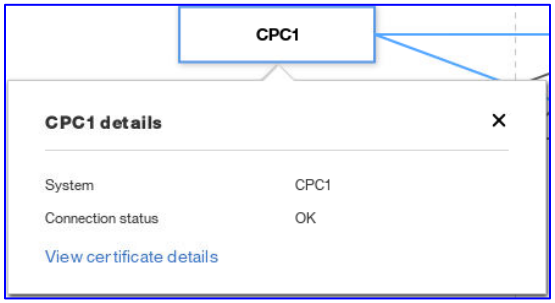
- When no key manager are defined, the task describes how to Configure Systems for Endpoint Security.
  - See appendix on certificate mgmt. between HMC and Key Server to add Key Server
- Connect Systems to Key Managers button launches the connect action.
- Initially, user can only launch the Connect System to Key Managers action.

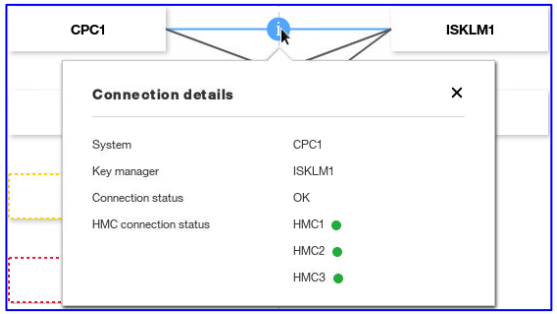


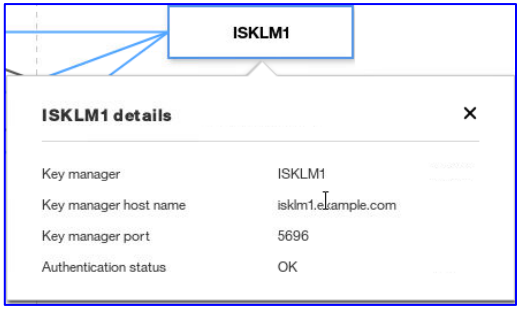
Configuration on the zHMC



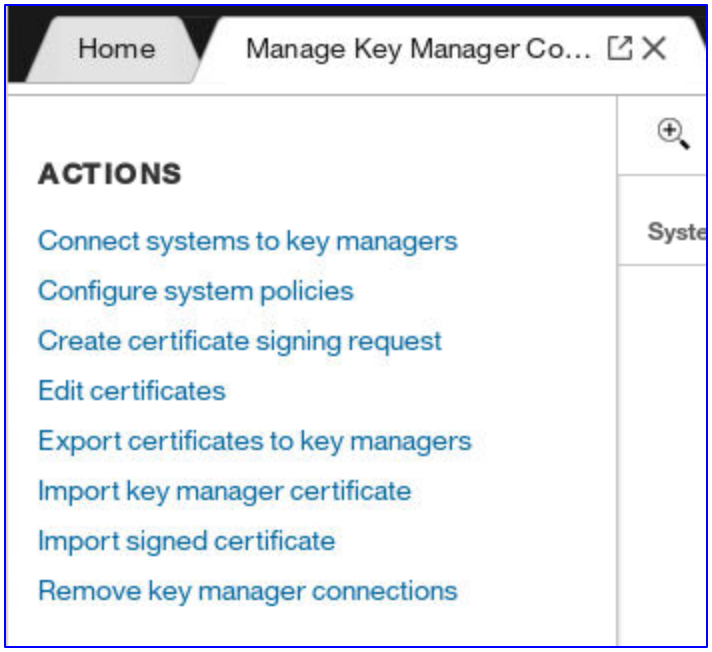
- After connecting systems to key managers, a topology shows systems and their key managers.
  - Topology only shows systems that support Endpoint Security
  - At least two key managers are recommended for each system.
    - Systems with only one key manager are in warning state.
    - Systems with no key managers are in error state.
- Click on a system, key manager, or link between them for more information.







Configuration on the zHMC



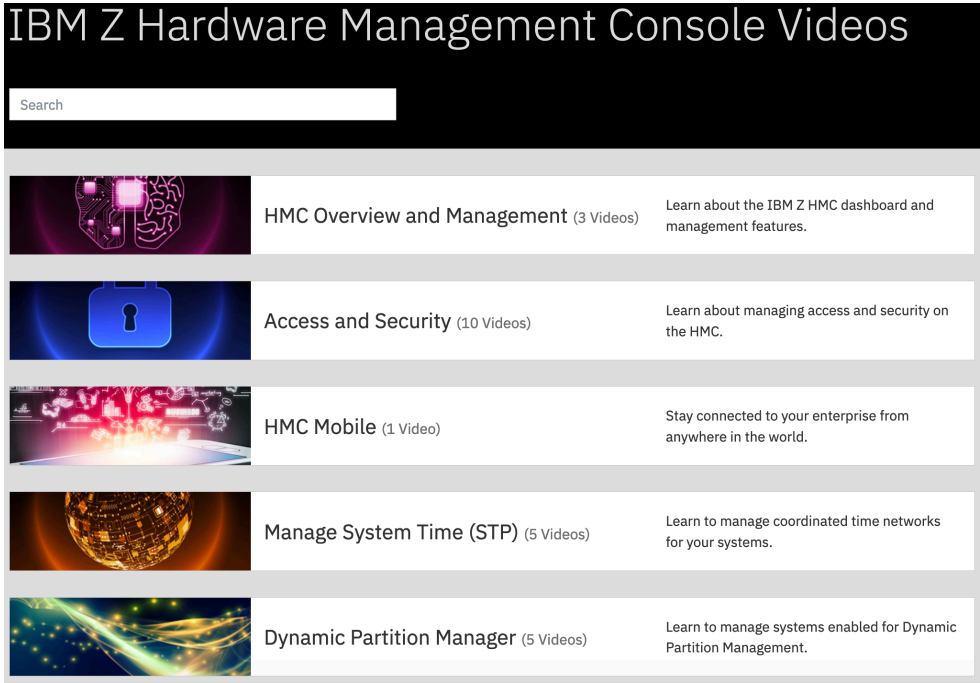
- Left side has list of actions a system administrator can perform to manage connections between systems and key managers.
  - Connect systems to key managers
    - Define key managers
    - Trust key manager certificates
    - Export a system's Endpoint Security certificate to key managers
  - Remove key manager connections
  - Manage a system's Endpoint Security certificate
    - Export for CA signing
    - Import a CA signed certificate

HMC YouTube Videos

YouTube Videos for HMC Content

- Current Documentation on HMC
  - Online Help information
    - Also, can be found on
      - IBM Resource Link

- New additional information on HMC via YouTube videos
  - Monitor for videos being added to the IBM HMC playlist url
    - **https://ibm.biz/IBM-Z-HMC**
    - Initial topic areas to be covered
      - Manage System Time
      - User Management
      - HMC Mobile
      - Tree Style User Interface
      - Dynamic Partition Manager
    - Additional areas of interest, notify
      - **bdvalent@us.ibm.com**
      - Brian Valentine



Thank you for your time and consideration….

Brian Valentine

HMC/SE Team

Twitter: @bdvalent125

Contact for questions or additional feedback:

Brian Valentine, (607) 429-4382, bdvalent@us.ibm.com

Trademarks

Please see

http://www.ibm.com/legal/copytrade.shtml

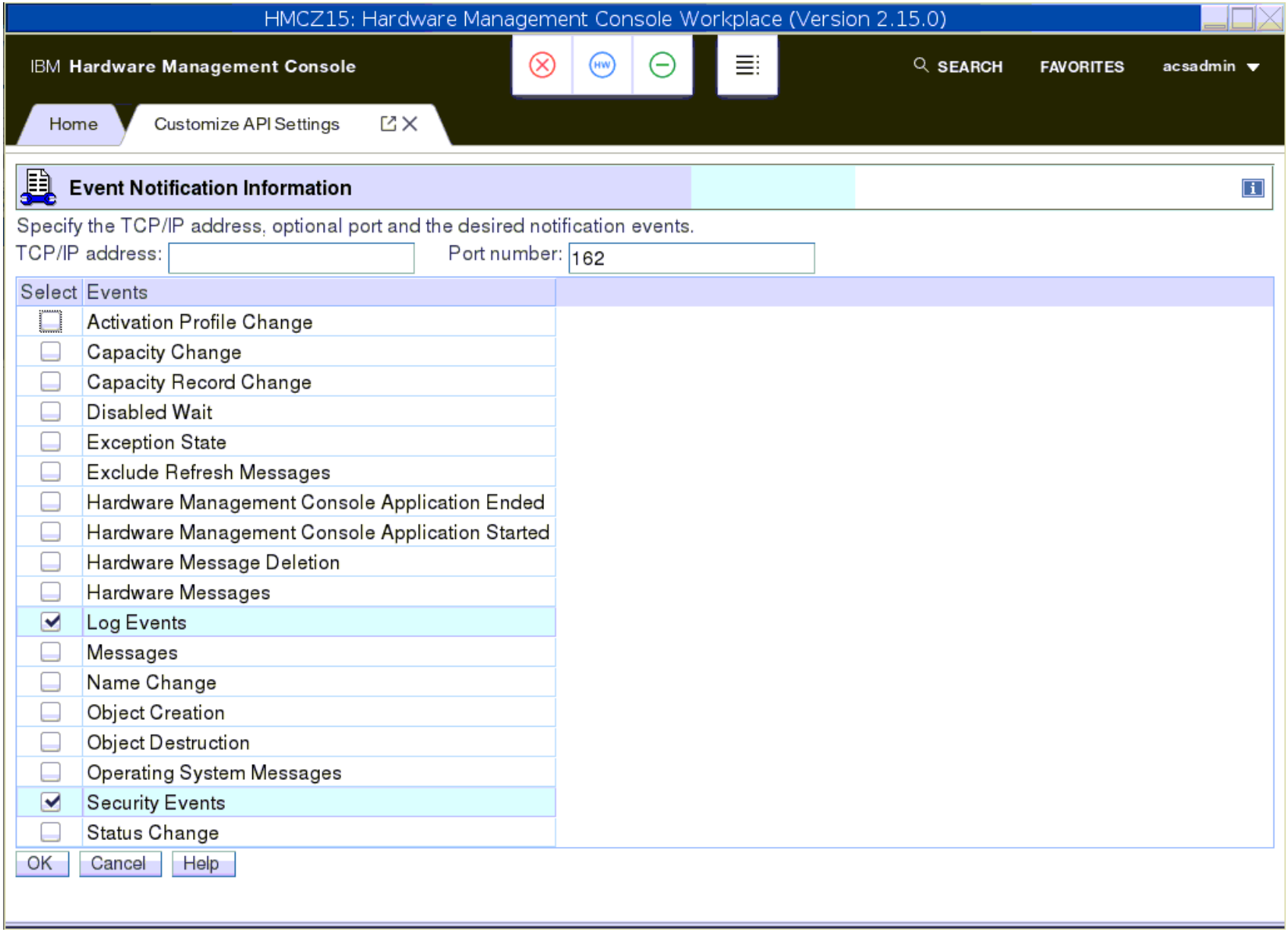
for copyright and trademark information.

Appendix I

SNMP support for Offload Audit Logs and System Events

New SNMP Trap – Log Event

- Prior to z15,
  - **Security Events** entry for SNMP Trap support
    - Security Log
- With HMC 2.15.0,
  - New **Log Events** entry for SNMP Trap support
    - Audit Log
    - Console Event Log
    - Security Log
- Trap contents
  - Time stamp
  - Log message text
  - Log type (i.e. audit, console, security)
  - Log ID(documented in HMC/SE User Guides)
  - Console name
- Generated on both HMC and SE



Crypto Signed UDXs

Crypto Signed UDX file

- Z15 adds an additional security check to affirm to the client that the binary UDX file can be trusted, similar to what is done today for MCLs
  - Validation of the signature occurs when the file is imported, either from removable media or an FTP server.
    - Activation the UDX file can only occur after the file is validated.
- The signing of the file is done internally by IBM
- Only signed UDX files are supported in z15
  - Supported crypto adapters are:
    - Crypto Express5S
    - Crypto Express6S
    - Crypto Express7S
- UDX files are signed specifically for z15

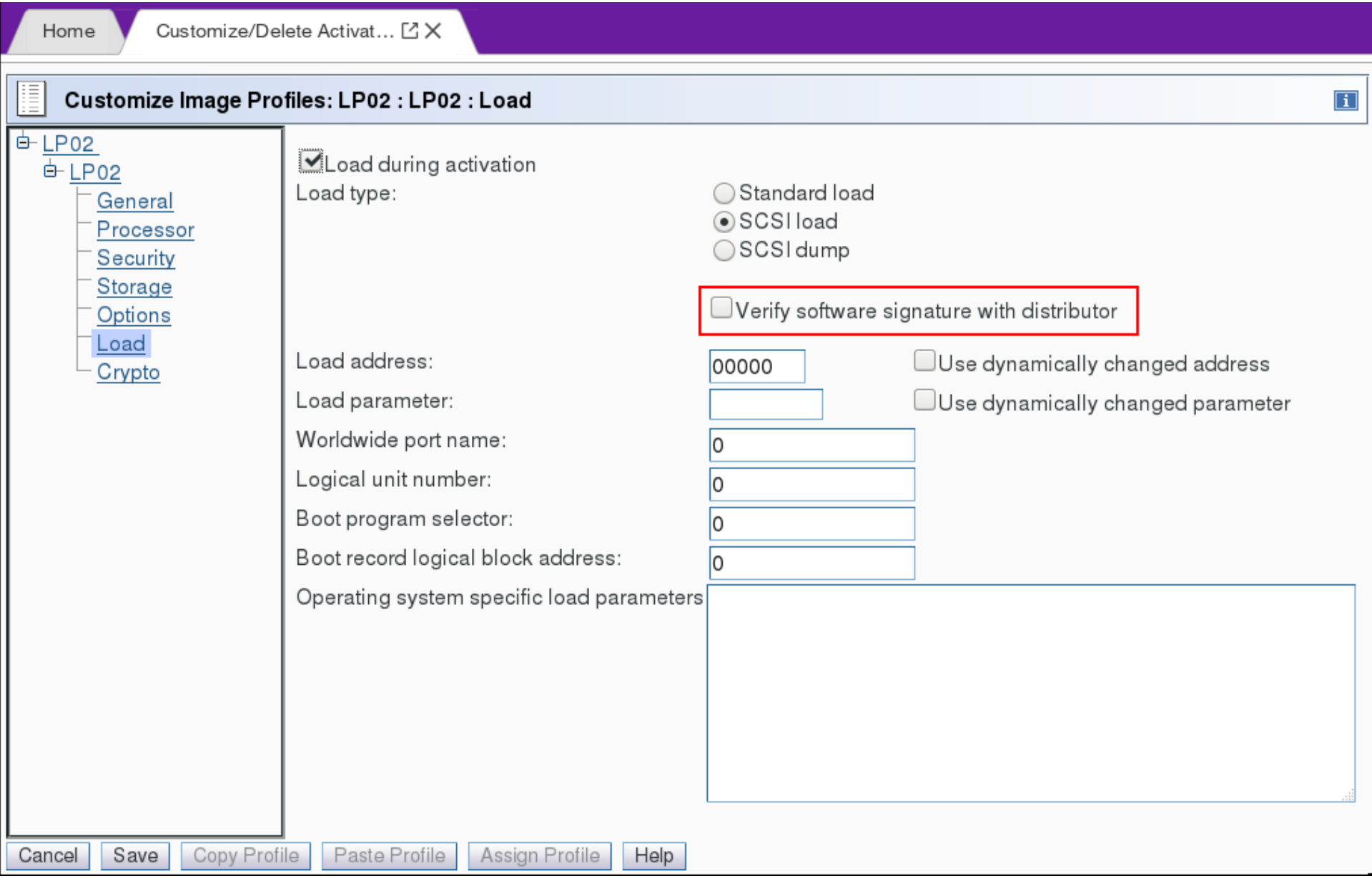
Linux Secure IPL

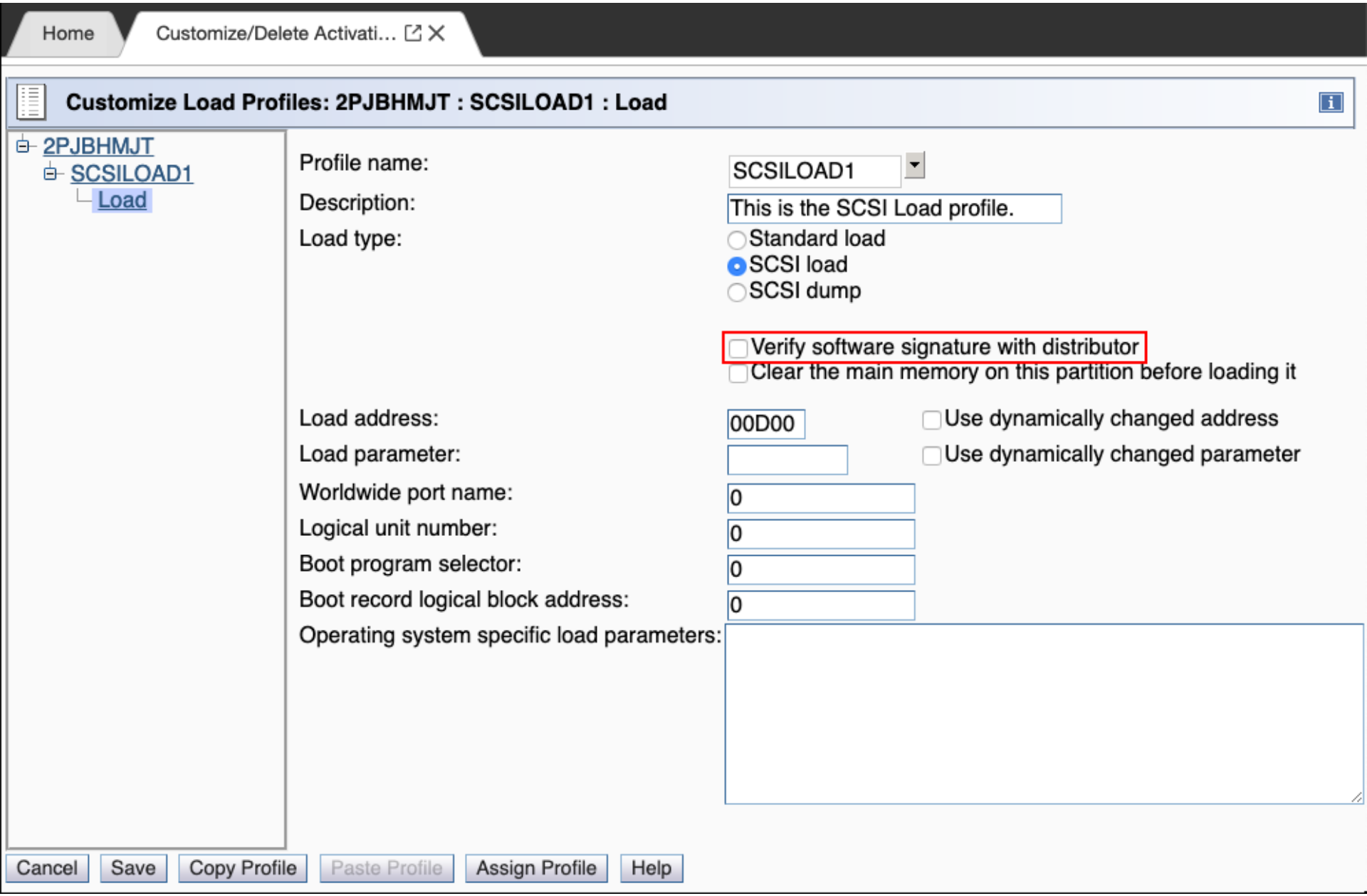
Linux Secure IPL (Load)

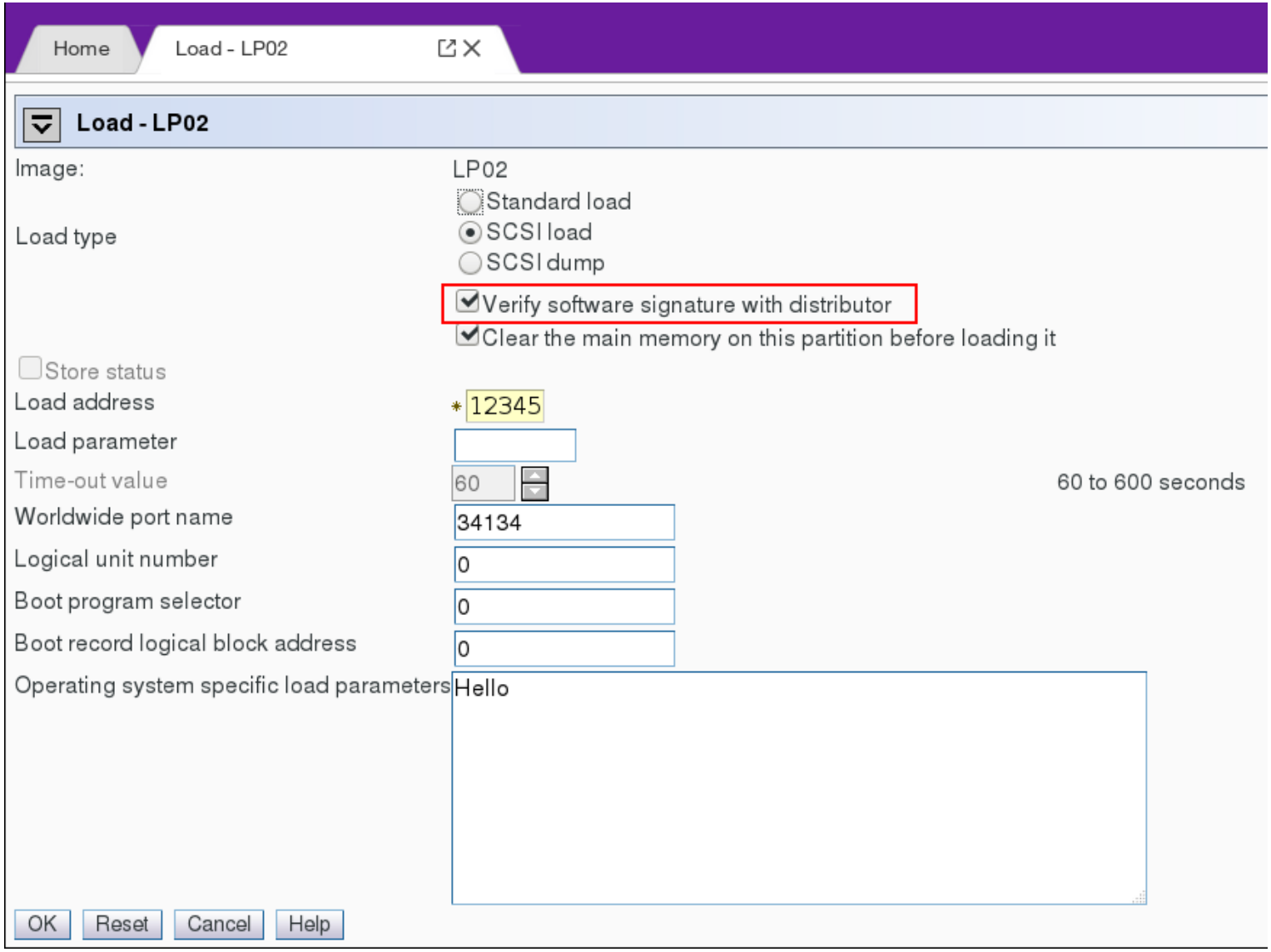
- IBM Z server continues enhancing security
  - Software running on IBM Z continues security enhancements
- IBM Z server's firmware provides Firmware Integrity Monitoring against tampering
  - Software running on IBM Z will begin to validate against tampering
  - Linux Secure IPL (Load) to provide that support
- When enabled, Firmware will validate the signature(s) of the software being loaded in to ensure that the signature(s) matches that used by the distributor.
- HMC/SE support required
- Other Notes:
  - Secure Load is currently only available for some types of IPLs:
    - SCSI and Network Boot (DPM-mode only).
  - Currently only zLinux distributions are being digitally signed.
  - Only available for LPARs running on CPCs at or above the 2.15.0 level

HMC/SE Linux Secure IPL (Load) Changes

- New *Verify software signature with distributor* check box for
  - Activation Profiles and Load
- If checked, the signature of the operating system being loaded into memory will be compared with the signature from its distributor.
  - If validated, Load will proceed.
  - If signature mismatch, Load will Fail
- New check box is only visible when SCSI load or SCSI dump is selected.
  - It is not visible when Standard load is selected.
- Security Log will include new *verify software signature with distributor* setting for Load & Profile actions







Data Replication for Last Login

New Datarep Type: “Last User Logon Data”

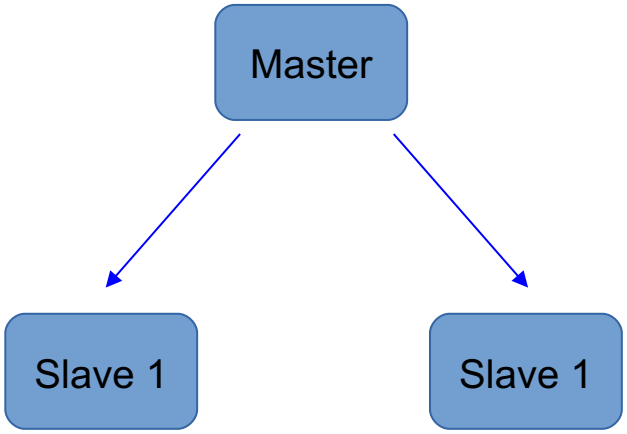
- The date/time that a user last logged in to the console
- Significance?
  - The ‘last login’ is used to determine when we should disable a user due to inactivity
  - Currently kept updated on each machine and not replicated
- **Problem**: What if ?
  - Customer has master/slave configuration… but **only** logged on the slave?
  - Master would eventually disable the user
  - Need enterprise wide way of managing ‘last login’

“Last User Logon Data”

- Give customers flexibility to handle user disablement:
  - Local Only (the way it works today)
    - User login’s only updates the local machine
    - Users disabled if not logged in frequently enough on each node
  - Cooperating collection (enterprise management)
    - Keep last logon date current with peers using data replication
    - No disablement login frequently enough to **any** of the peers

“Last User Logon Data”

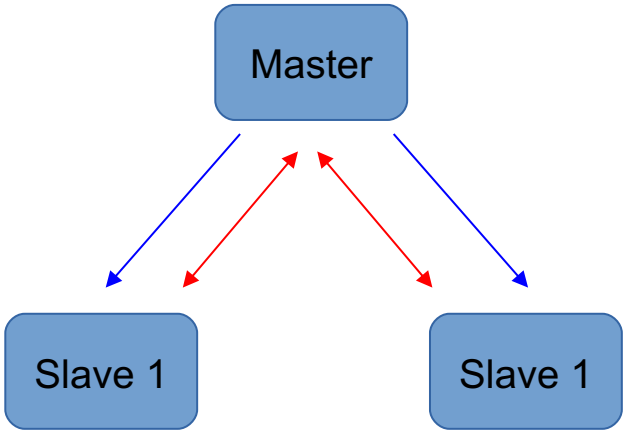
- **Step 1**: Configure ‘typical’ master slave data
  - Per normal operation, selection of data always made on each **slave**



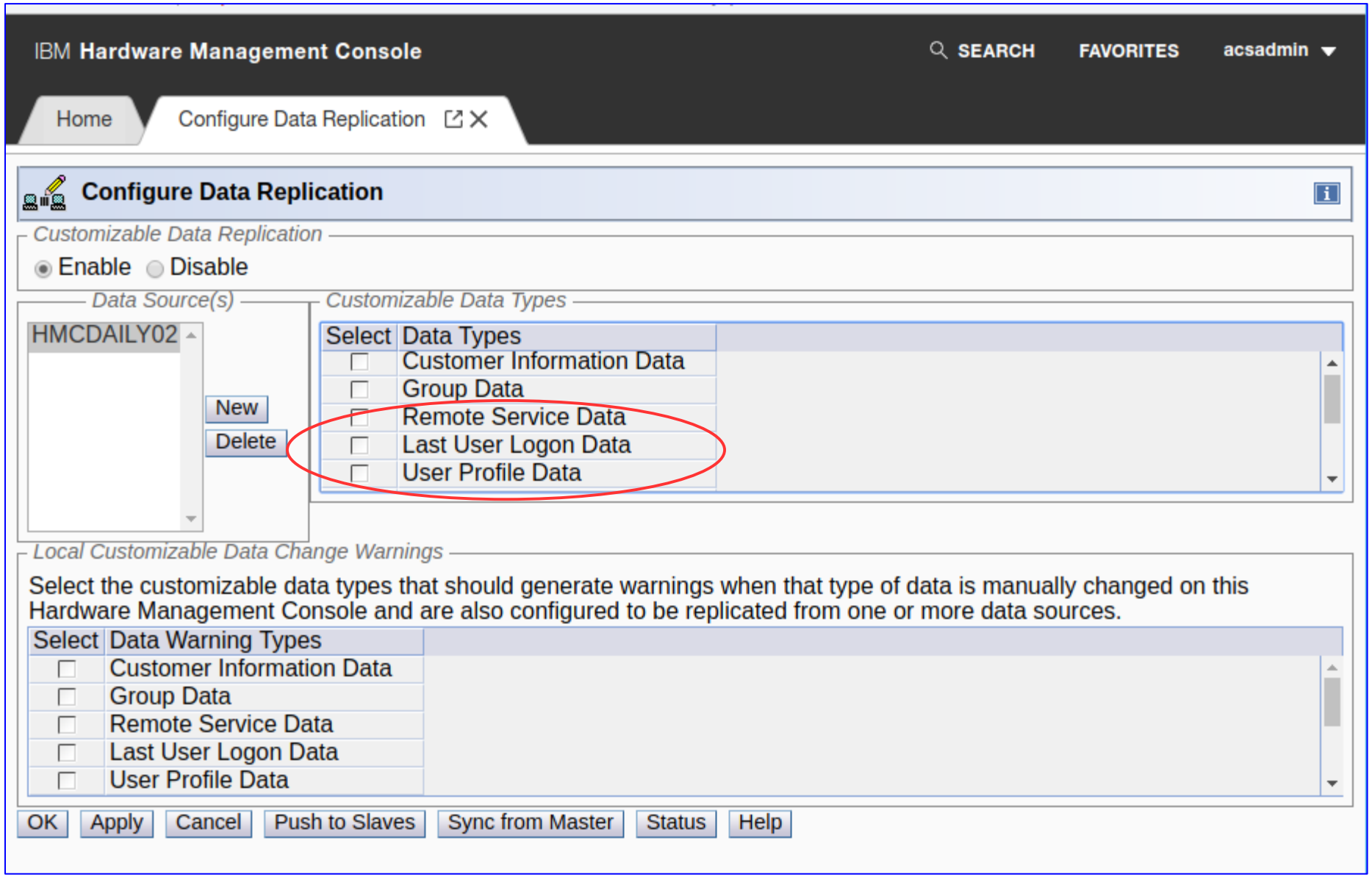
For example:
“Customer Information”
Any changes to Customer Info on master, replicates to slaves.

“Last User Logon Data”

- **Step 2**: Create peer relationship for ‘Last User Logon Data’
  - Select ‘Last User Logon Data’ on **both** master and slave machines
  - Makes them peers for this one type of data



“Last User Logon Data”
- Any time user logs on to master, it replicates to the slaves
- Anytime user logs on to slave, it replicates to the master

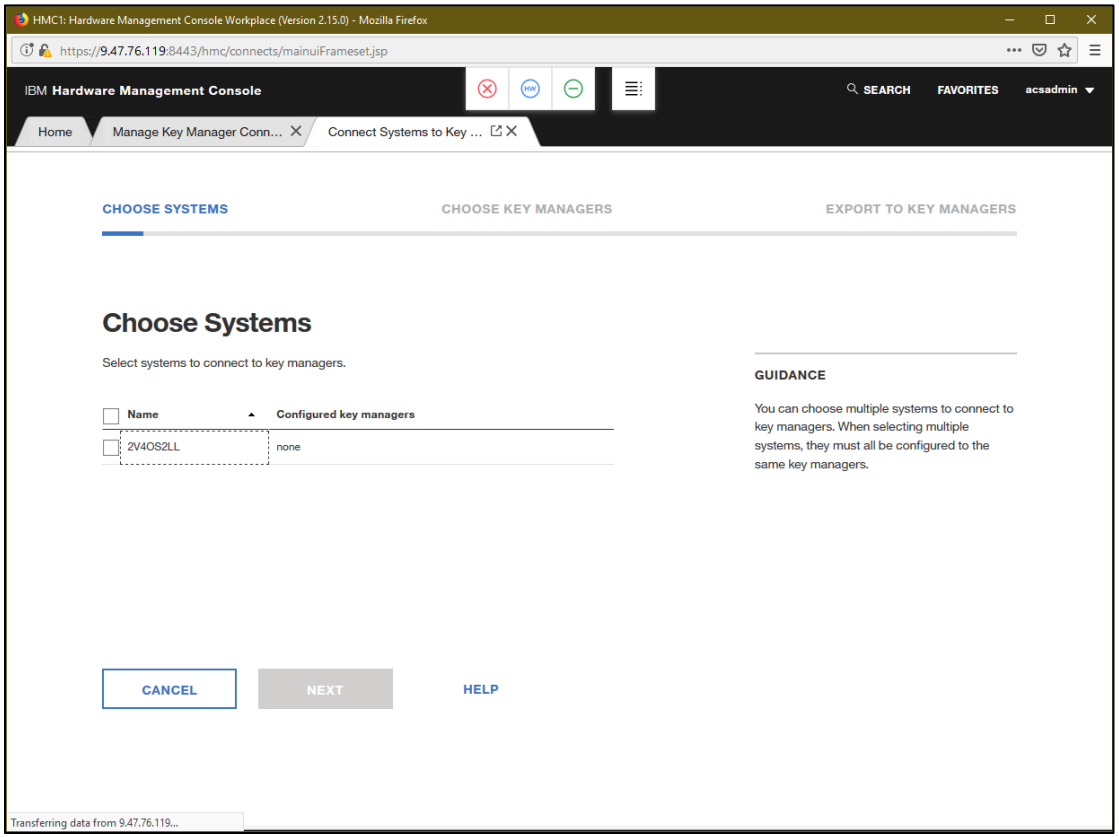


Appendix II

Fibre Channel Endpoint Security Certificate Management

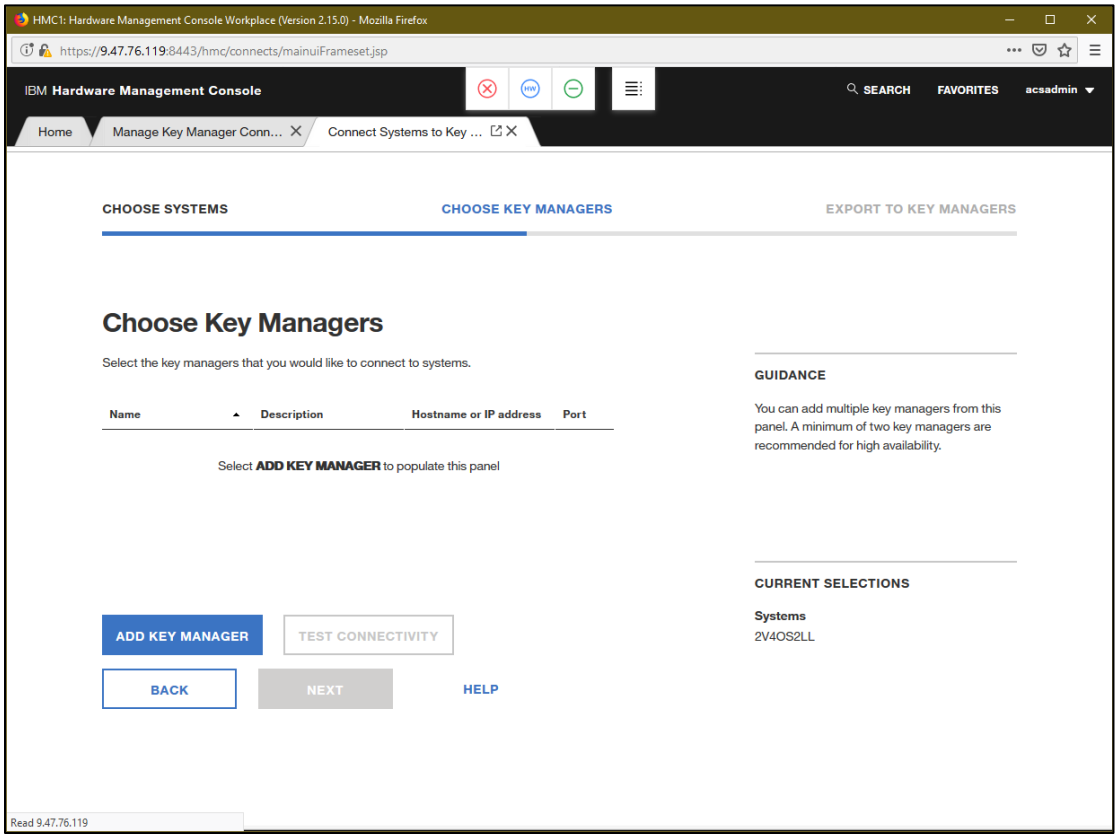
Configuration on the zHMC

- Choose the system(s) to be connected to a key manager(s)



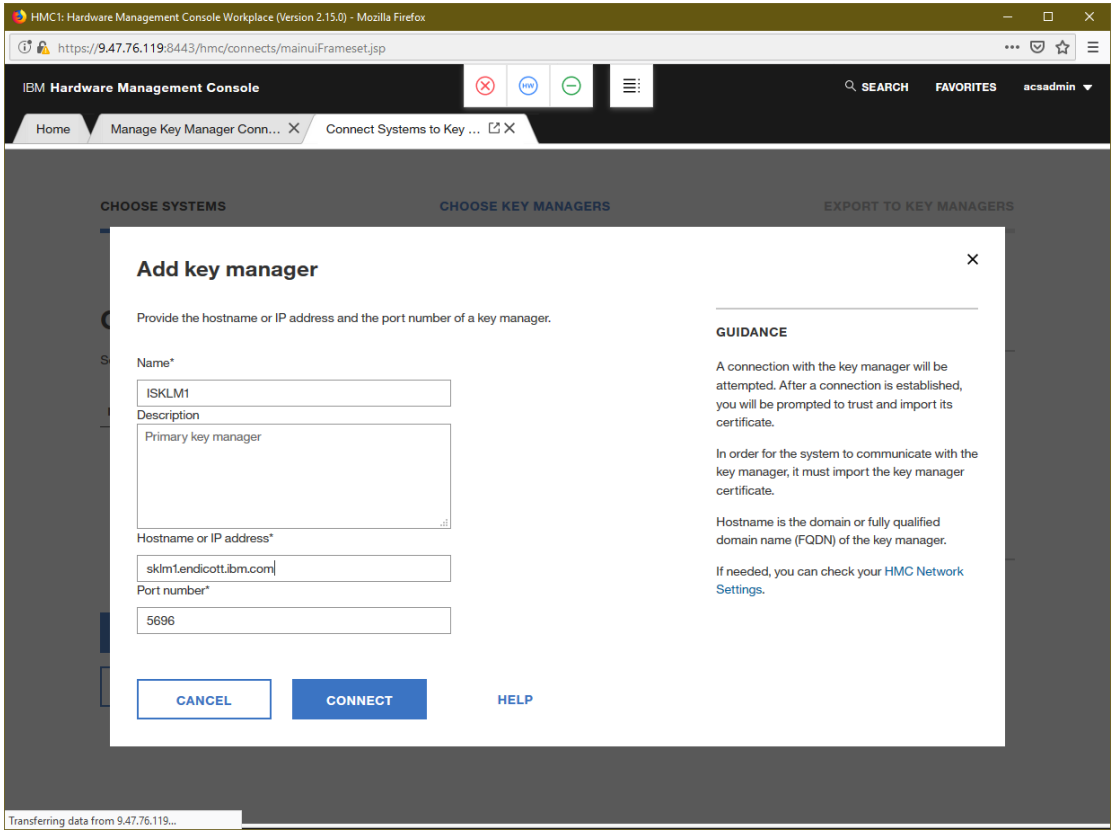
Configuration on the zHMC

- Select the key manager to be connected to the system(s)
- When no key managers are defined, use ADD KEY MANAGER



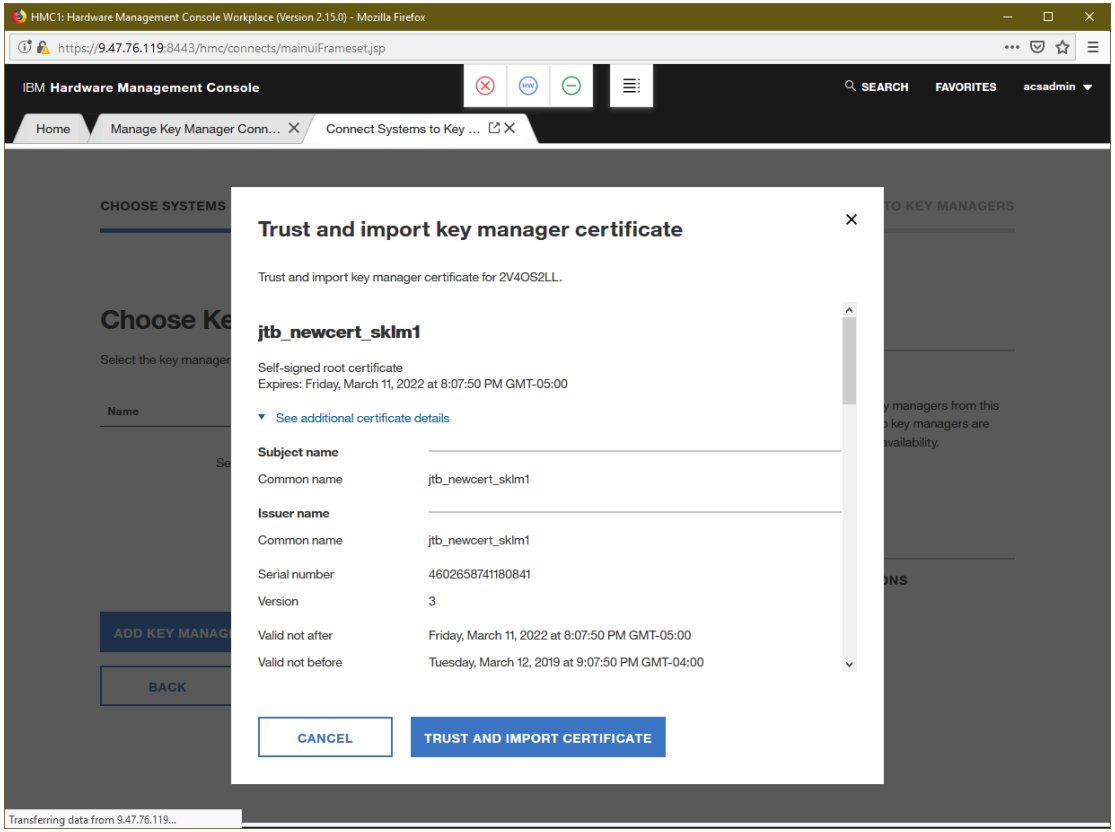
Configuration on the zHMC

- Identify the new key manager by its IP/hostname and port
- Provide a unique name and optional description
- CONNECT will attempt a network connection



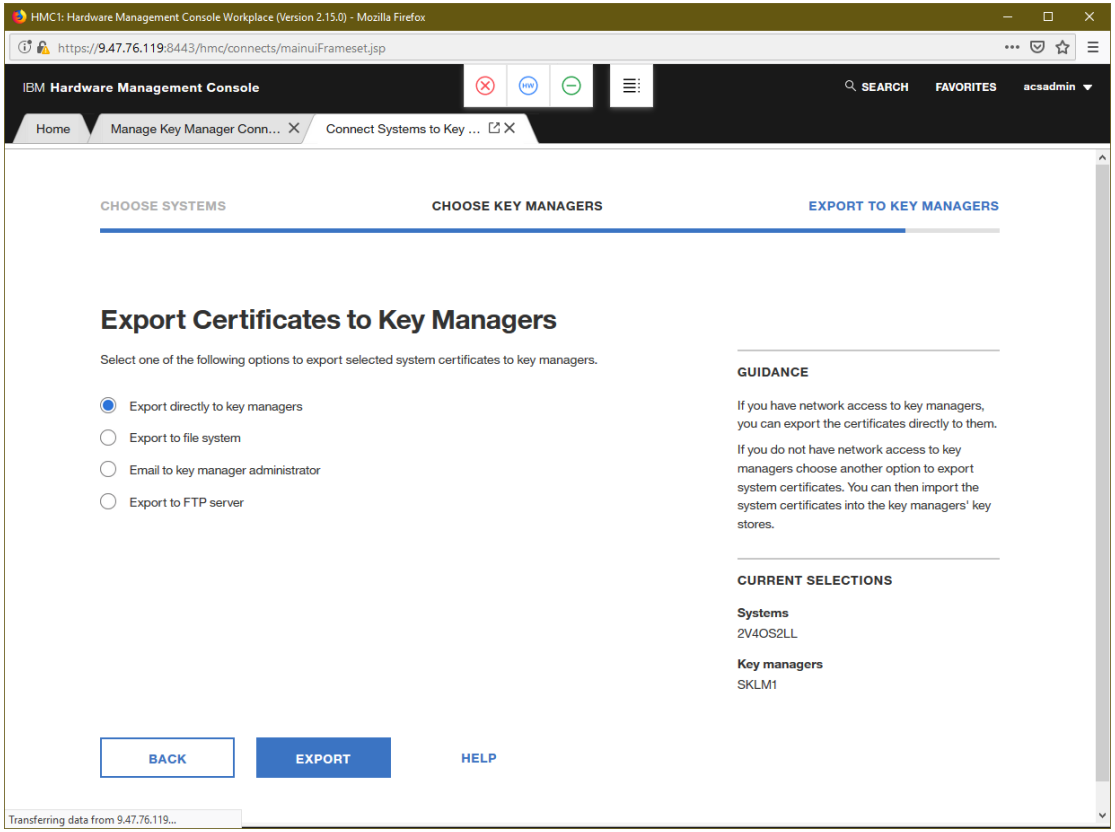
Configuration on the zHMC

- If not already trusted, the key manager's certificate must be trusted and imported into the SE's trust store
- The admin can inspect the certificate from this panel



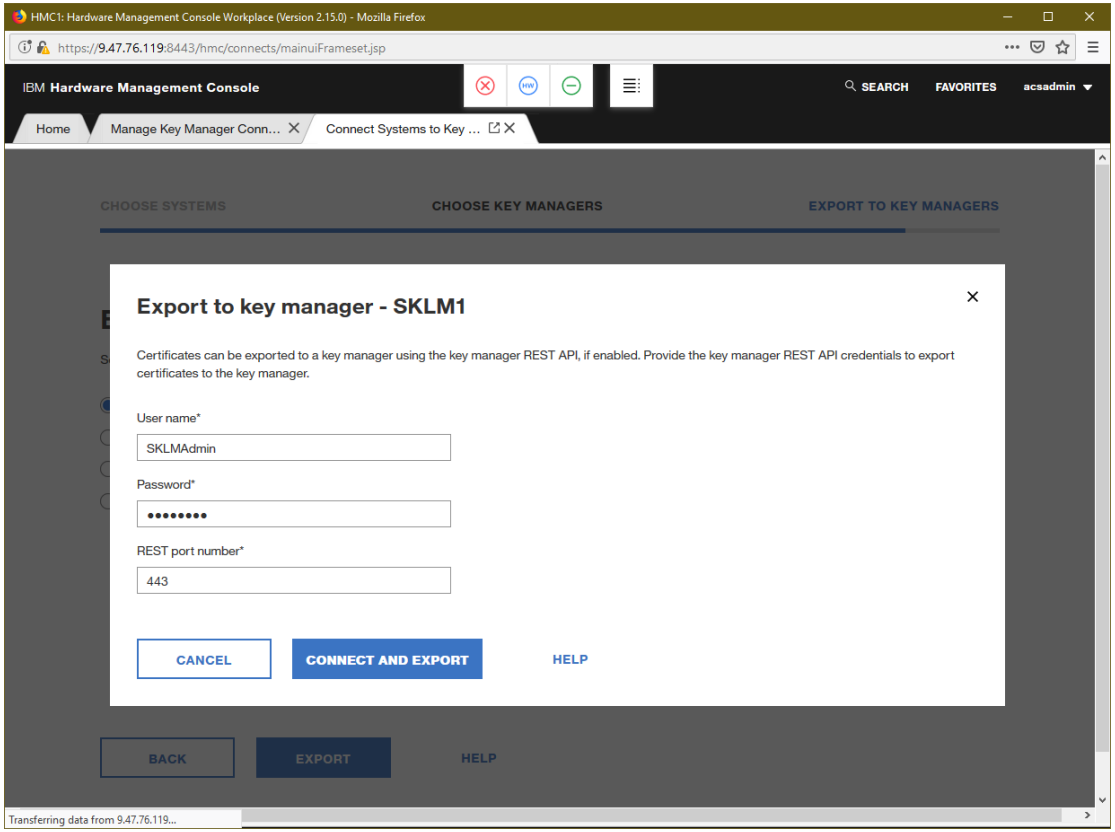
Configuration on the zHMC

- Now the SE's certificate must be exported to the key manager
- Four options; direct export is easiest
  - Requires userid and password of key manager admin ID



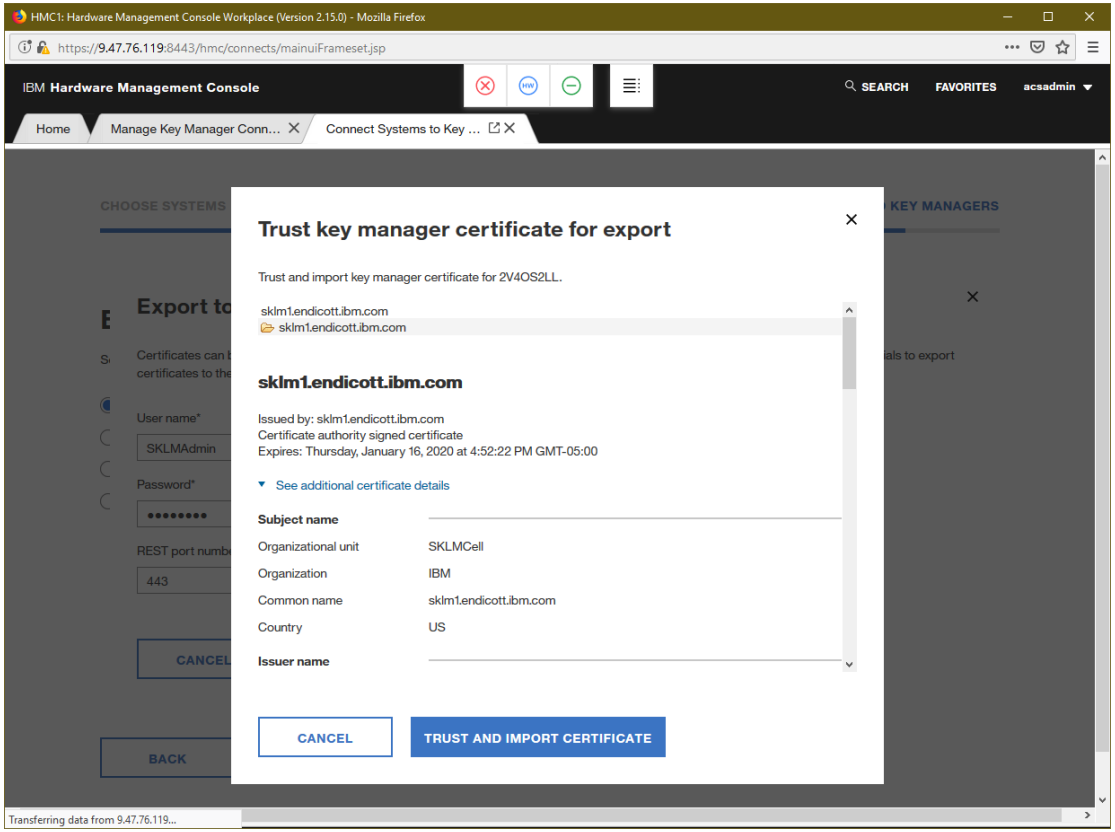
Configuration on the zHMC

- CONNECT AND EXPORT sends the SE's certificate to the key manager via a REST API provided by the key manager



Configuration on the zHMC

- HMC user can inspect the SE certificate via this panel
- TRUST AND IMPORT CERTIFICATE sends it to the key manager



Configuration on the zHMC

- Success!