IBM z17 HMC (Hardware Management Console) Enhancements

February 26, 2026

Jason Stapels, Brian Valentine
HMC/SE Development

SHARE in Orlando

File Updated: 01-23-26

Topics

- HMA (Hardware Management Appliance) only for HMC 2.17.0
  - HMA Order/MES Options
  - Import/Export from/to Remote Browsing File System
- Security Enhancements
  - Dual Control
  - Single Sign On (SSO)
  - Network Time Security
  - TLS Cipher Suite Configuration
  - Complete HMC User configuration replication to SEs
  - Quantum-Resistant Password Hashing
  - Replicate HMC Certificates to SE
  - HMC OSA ICC CA Signed Shared Certificates
- BCPii Enhancements/SOD
  - BCPii HMC Targeting with Enhanced Security and Asynchronous Notification support
  - Statement of Direction (SOD) on BCPii v1 & SNMP Deprecation
- Remote Code Load
- IBM HMC Mobile 5.0

HMA Only:
Hardware Management Appliance
For HMC 2.17.0

HMC 2.17.0 System support

- **HMC support to n-2 only**
  - z14 no longer supported
  - same as SYSPLEX support

Machine Family	Machine Type	Firmware Driver	SE Version
IBM z17	9175	61	2.17.0
IBM z16	3931, 3932	51	2.16.0
IBM z15	8561, 8562	41	2.15.0

- **Note:**
  - HMC 2.17.0 can be loaded on
    - z17 HMA (Hardware Management Appliance)
    - IBM z16 HMA
    - IBM z15 HMA
  - Standalone HMC hardware: no longer supported

HMA HMC only z17 Offering

➢ Only HMC hardware supported for z17 is HMA (Feature Code 355)

- No Standalone (SA) HMC hardware will be supported
  - No MES support of SA HMC hardware
    - » Can use Export/Import of SA HMC data and HMC Data Replication to HMA HMCs

➢ Import/Export from Remote Browsing File system

- With HMA HMC, all clients only remote browse into HMC
  - Client requirement to have import/export from remote browsing systems for all HMC tasks using import/export
    - » Adding import/export to remote browsing workstation (in addition to USB & 3 FTP options) (see Slide 7)

➢ z17 HMC 2.17.0 code level can be loaded on z16 & z15 HMAs

- New process to no longer set Service Status for z17 HMC code load of z16 & z15 HMAs
  - *Automatic SE powercycle* option will be disabled in *Customize Console Settings* by SSR instead of setting Service Status
  - HMC visibility & manageability of Images remains during the extended time to upgrade the z16/z15 HMAs

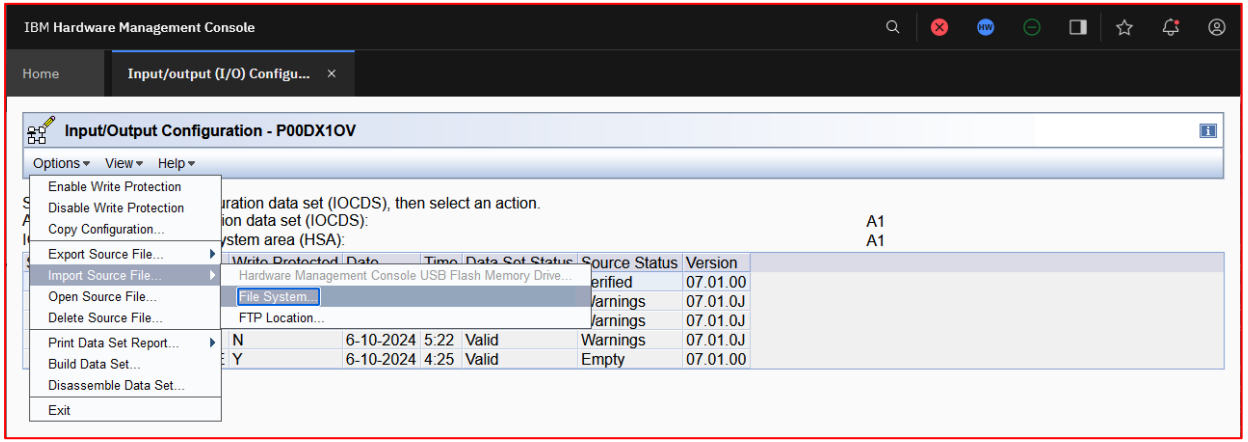
HMA (Hardware Management Appliance) Ordering

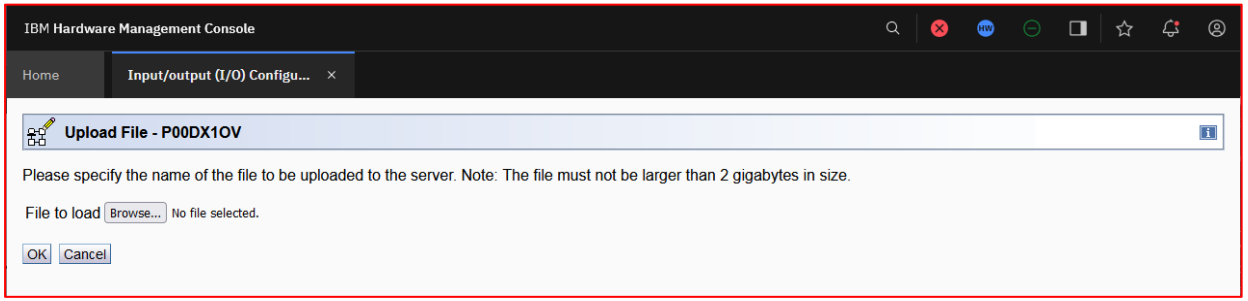
- **Only HMC hardware supported for z17 is HMA**
  - Can be optionally ordered with Feature Code 355
  - Strong IBM Recommendation: Should not have HMA feature on more than 2 CPCs per data center location (z17, z16, z15)

- **MES available for adding HMA to z17 CPC**
  - Add Feature Code 0355 to existing field system

- **With z17, new MES option to remove HMA feature from z17 CPC**
  - eConfig offering to initiate HMA feature process without any special interaction with IBM
  - Remove Feature Code 0355 from existing field system

Import/Export Remote File System





Provide option to import/export files directly from/to client workstation remotely connecting to the HMC

Addresses

- USB access to HMA HMC inside CPC
- Complexity of SFTP/FTPS
- Secure connection

Security Enhancements: Dual Control

Dual Control Value Proposition

Dual control adds an extra layer of security for critical tasks on the HMC.

Dual control enabled tasks require another level of verification from an approver before they can be run.

Requirements/Value

- Industry or Company Security Standard

- User action error protection
  - Unintended activation of a wrong active LPAR

- Fraud Protection (most likely insider)
  - Misuse of Crypto
  - Security Attack (take down one or more LPARs)

- Financial Protection or Workload Performance Degradation
  - Capacity on Demand (eg. On/Off Capacity on Demand)
  - User mistake or Fraud protection

Dual Control Design Highlights

Dual Control definitions in User Management roles

- Optionally assigned to users

Dual Control available to z17, z16, z15 using HMC 2.17.0

Dual Control Target per User Role

– Object and
– Task

Dual Control Approver per User Role

– Any User Role for task/object authorization control
– Can also create special User Role with list of specific users for DC approval

Dual Control Management Execution Requests for Approval

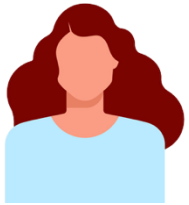
– Run by requester restricted to time window in the future
– Run by requester
  - No time window restriction
– Run immediately
  - Automatically without requester further involvement
– Run on a specific date and time

Dual Control CPCs supported (Requires z17 HMC 2.17.0)

– z17 CPC (no restrictions)
– z16 & z15 CPCs
  - Should remove Single Object Operations in any role applied to a User under Dual Control
  - *Perform Model Conversion (Capacity on Demand)* & *Change LPAR Cryptographic Controls* tasks not available for HMC 2.17.0 z16 & z15 targets

Dual Control external interfaces (UIs, WS APIs, BCPii v2, IBM HMC Mobile)

Primary user personas



Adele
Junior system administrator

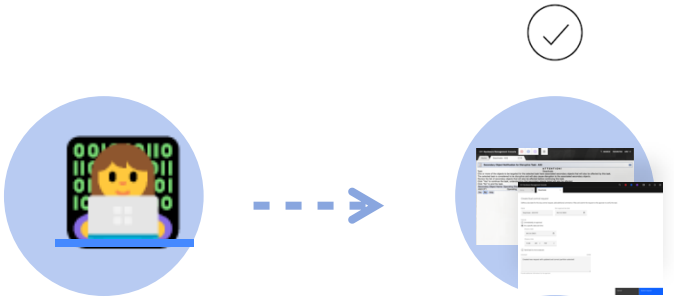
Easton
Experienced system administrator

Hardware management

Sage
Security administrator

Security

Dual Control
Security Admin Touch Points



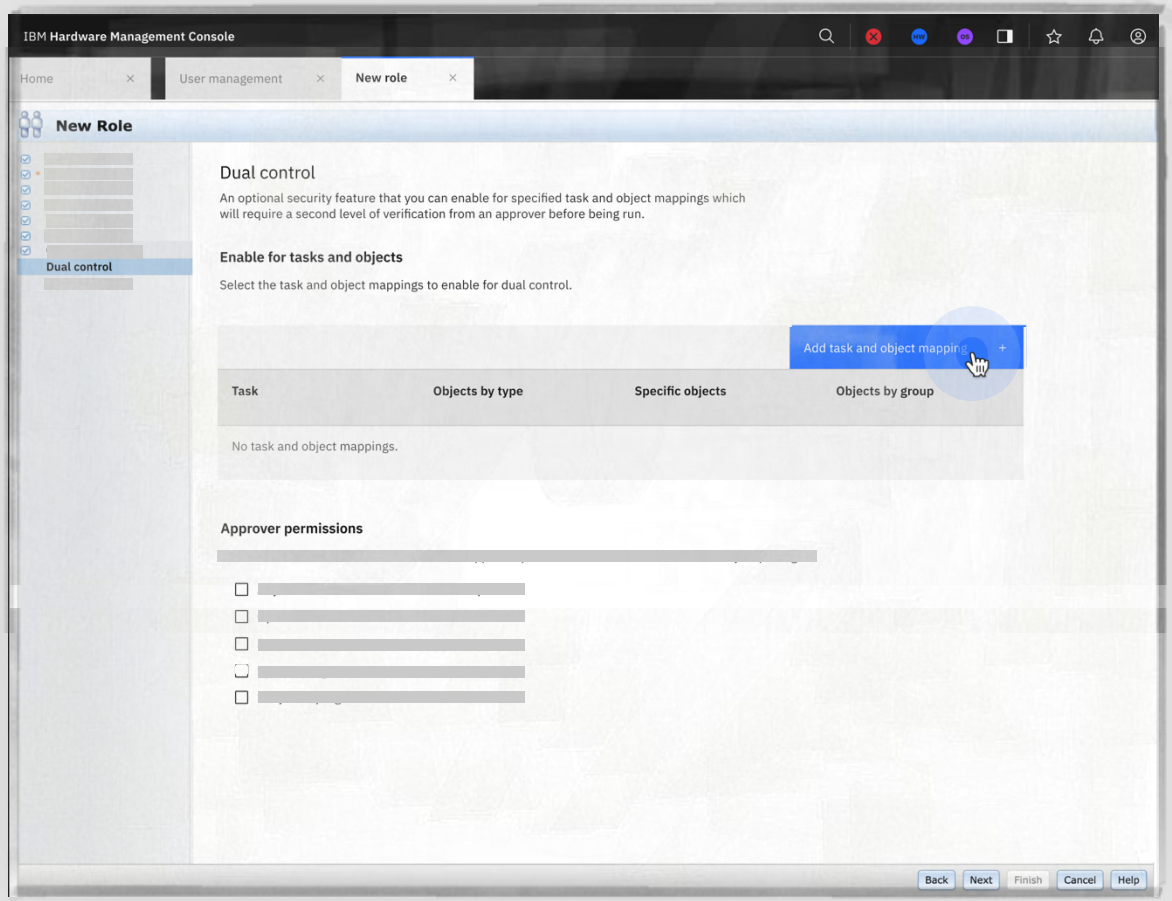
Security Admin Sage

Enables Dual Control for tasks when targeting specific objects (e.g. system, partition, IO adapter)

Selects roles of users that can approve.

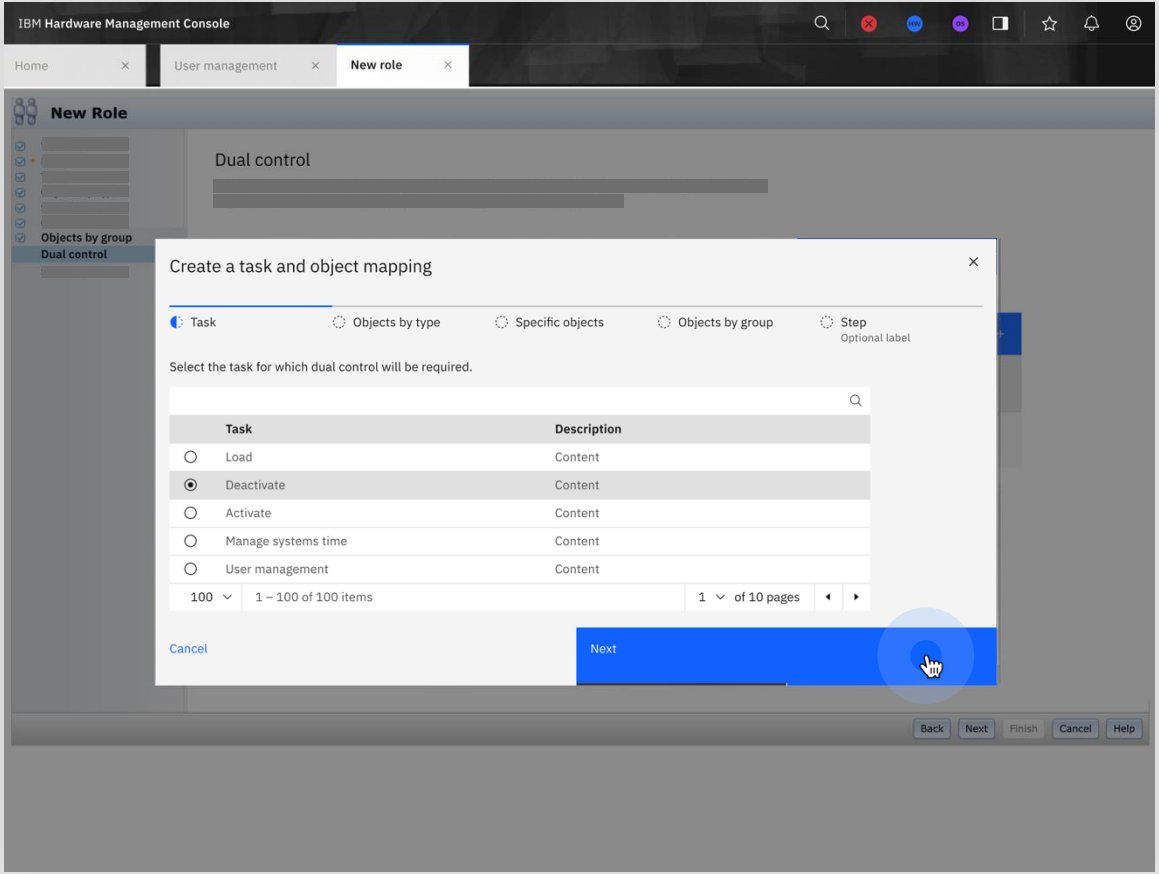
Dual control setup for the deactivate task

Adele’s security administrator, **Sage**, selects the tasks and objects enabled for Dual Control using the role permissions in user management



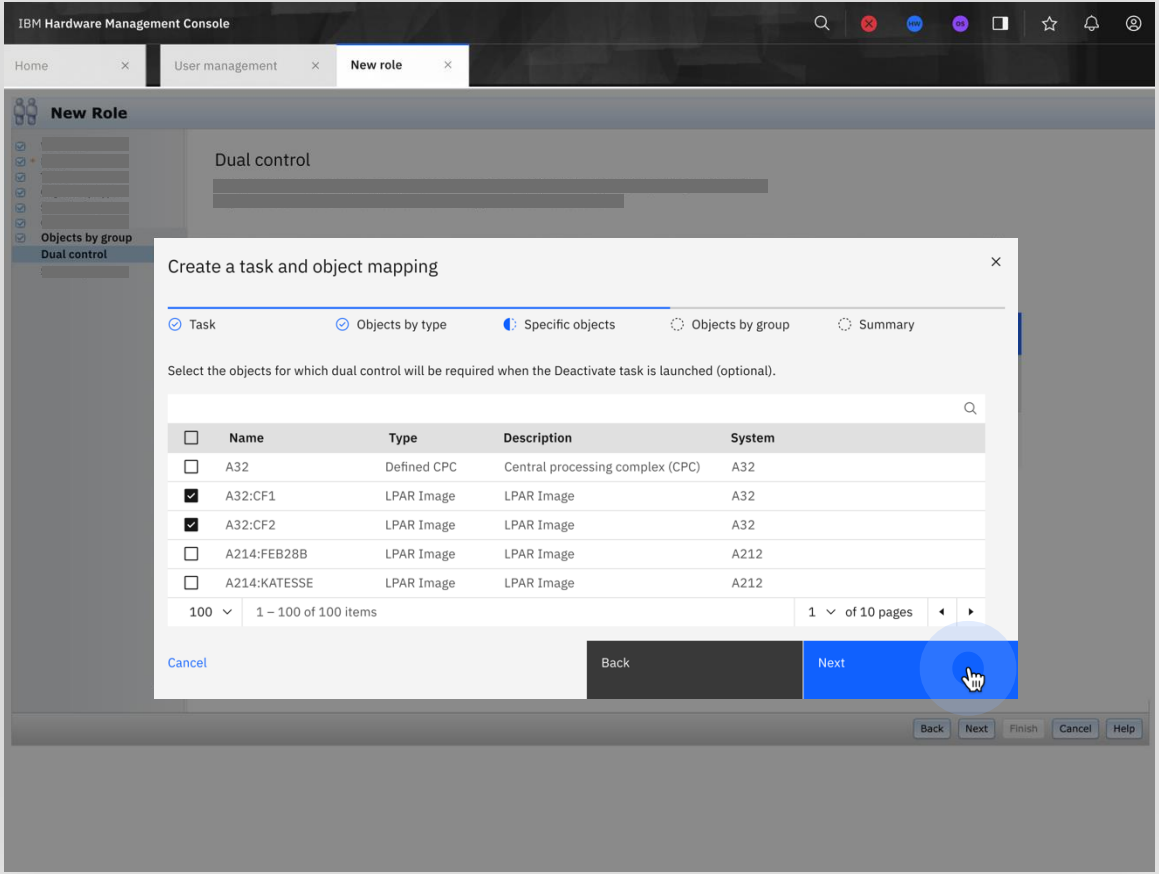
Dual control set-up for the deactivate task

Sage selects the Deactivate task to be enabled for dual control



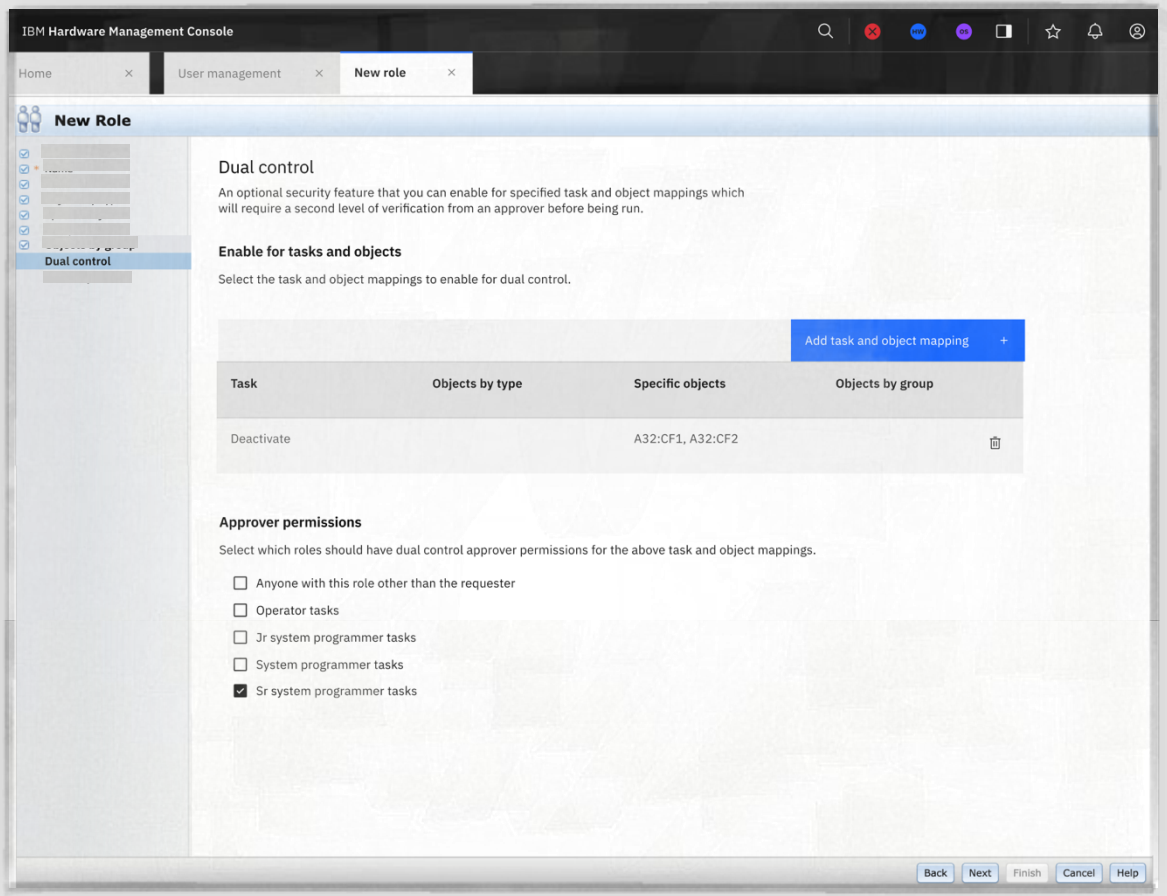
Dual control set-up for the deactivate task

Sage selects the objects that should be enabled for dual control with the deactivate task



Defining approver permissions

Once all the tasks and object mappings are defined, Sage selects the roles of the users that should have approver permissions for the designated task and object mappings.



Dual Control
Task use touch points

Adele

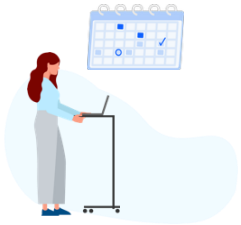
Selections made in task and approval request submitted

Easton

Approval/Rejection

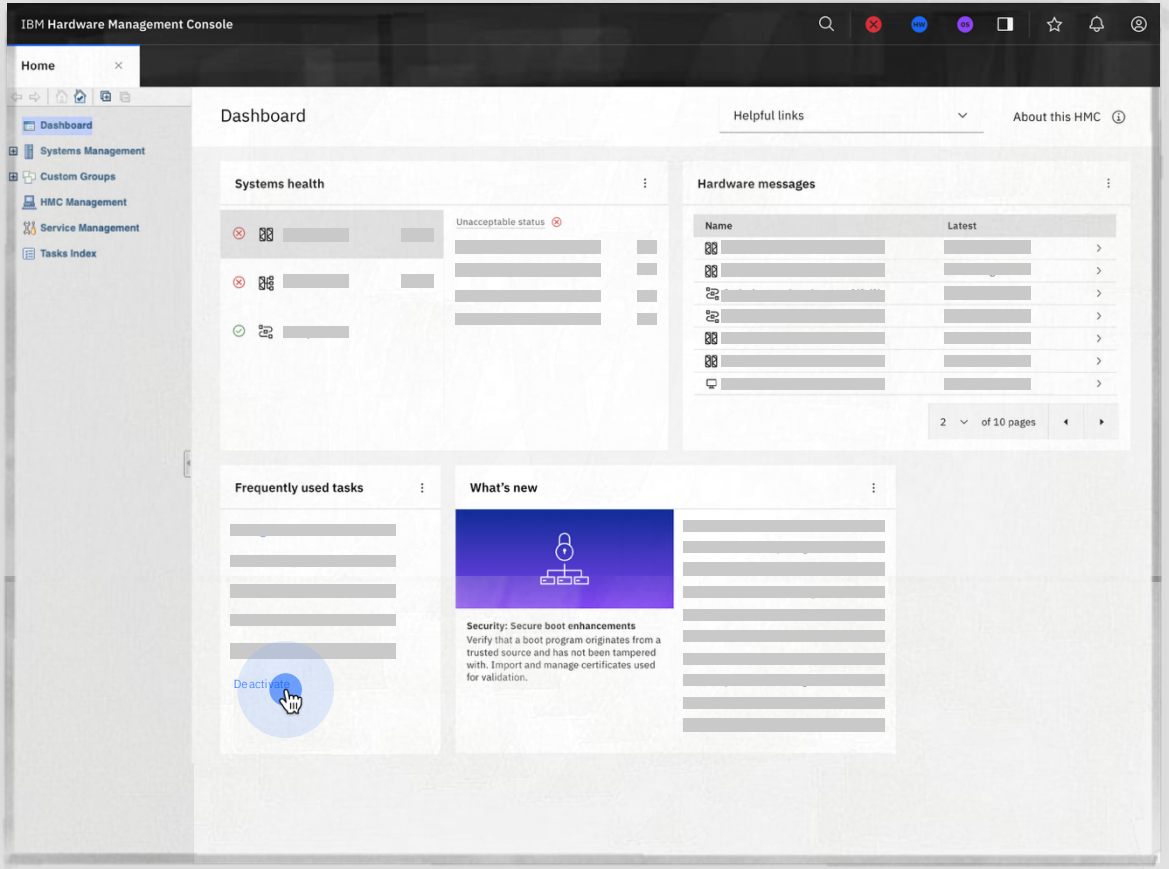
Task is run

The next day



Adele logs onto the HMC to complete her daily tasks, the first of which is to deactivate partition CF2

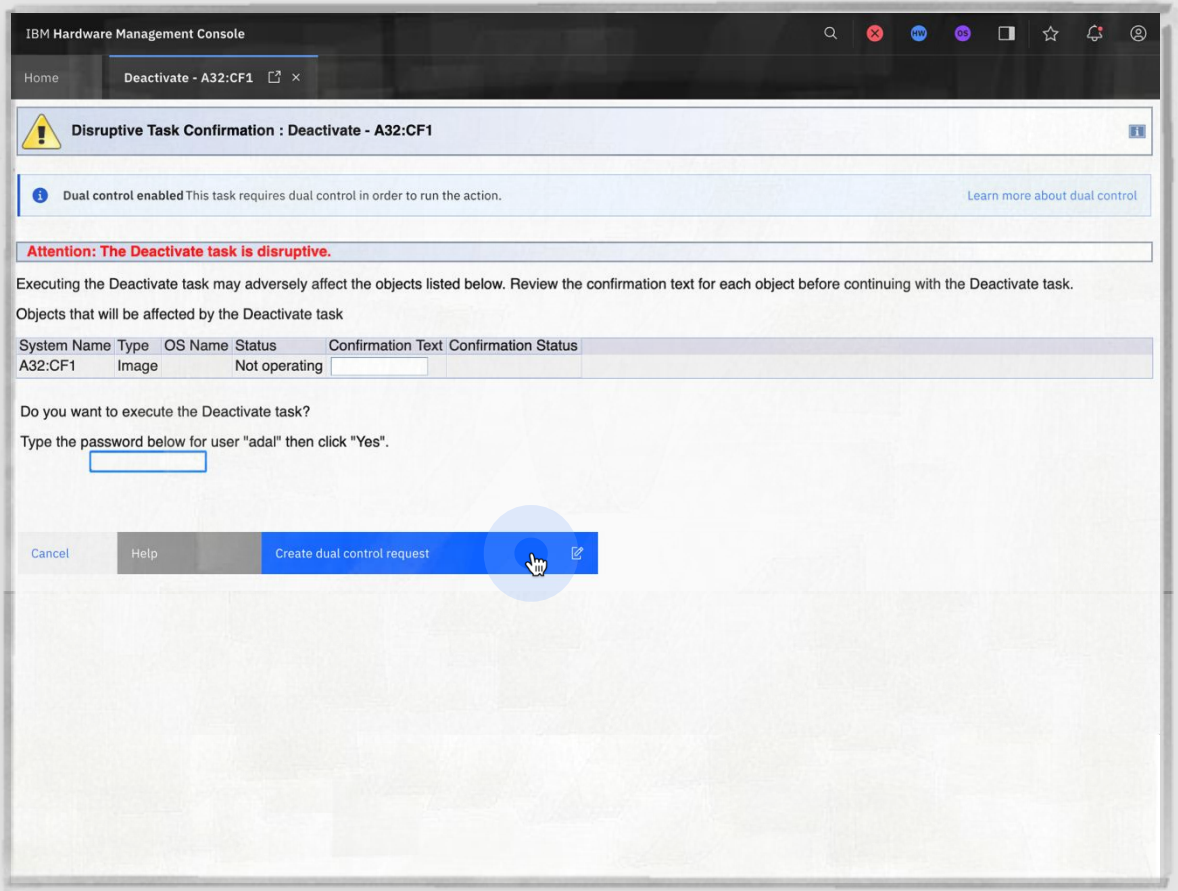
She launches deactivate and accidentally selects partition CF1



In task

Adele sees that this is a *dual control enabled task and object mapping*

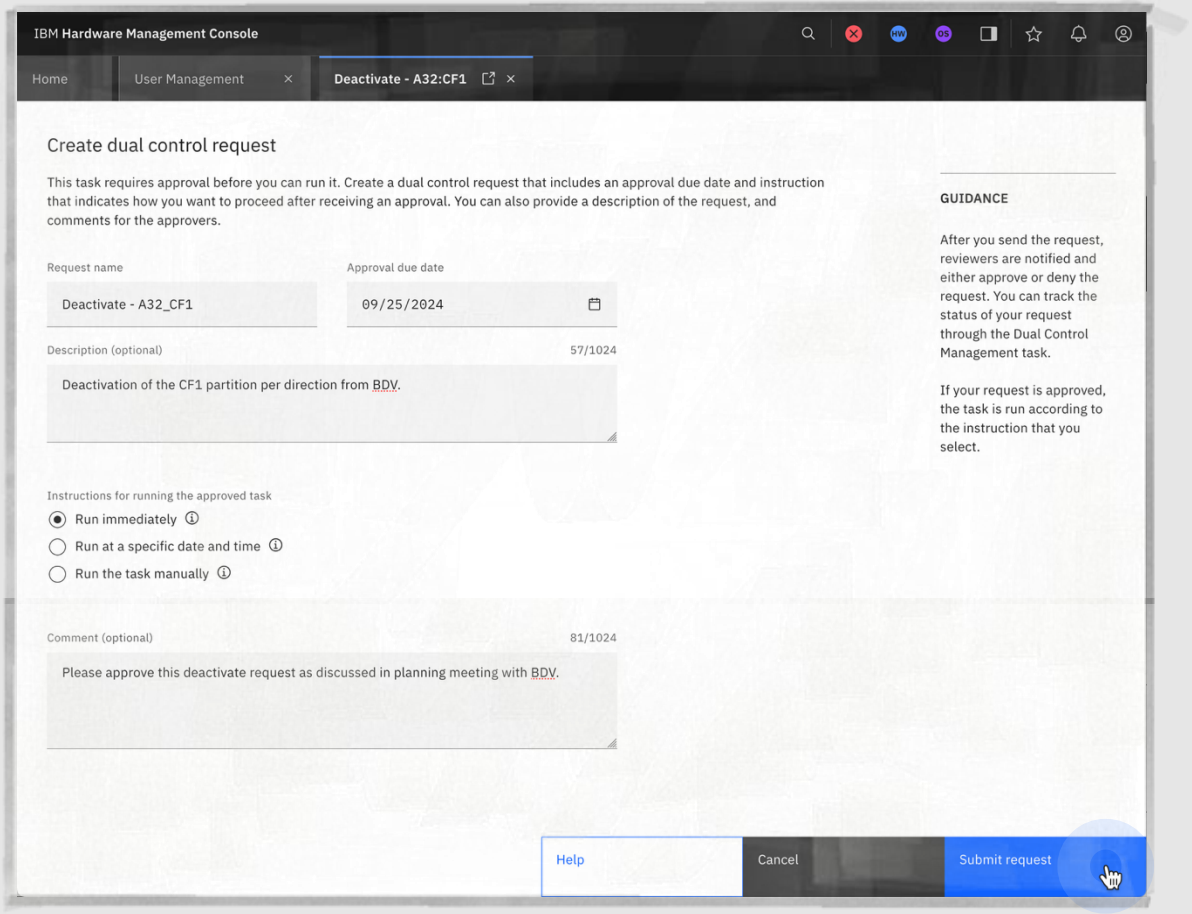
Once she has made her selections and is done within task, she *creates a dual control request*



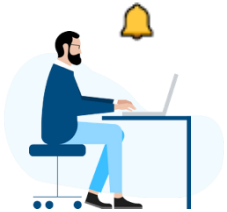
Submitting a dual control request

Adele selects an *approval due date*, and that the Deactivate should run immediately after it's approved.

She submits the request



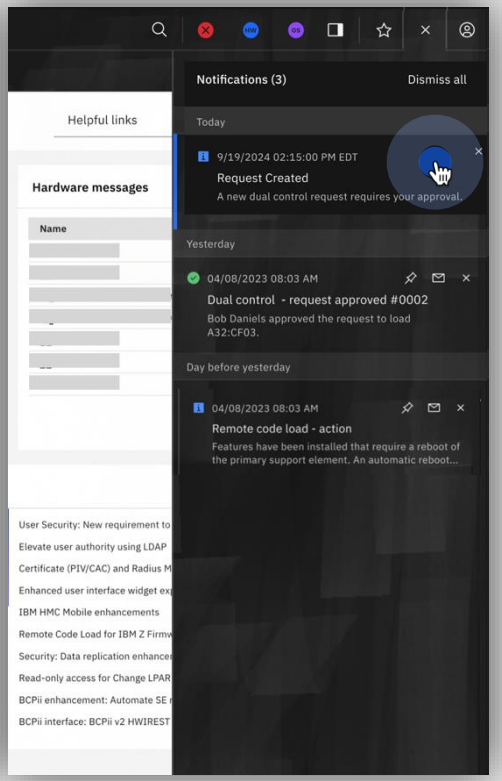
Approver notified of dual control request



Easton, a dual control approver, is notified of the request via mobile, email, APIs, BCPii, and the notification panel in the HMC

HMC Mobile

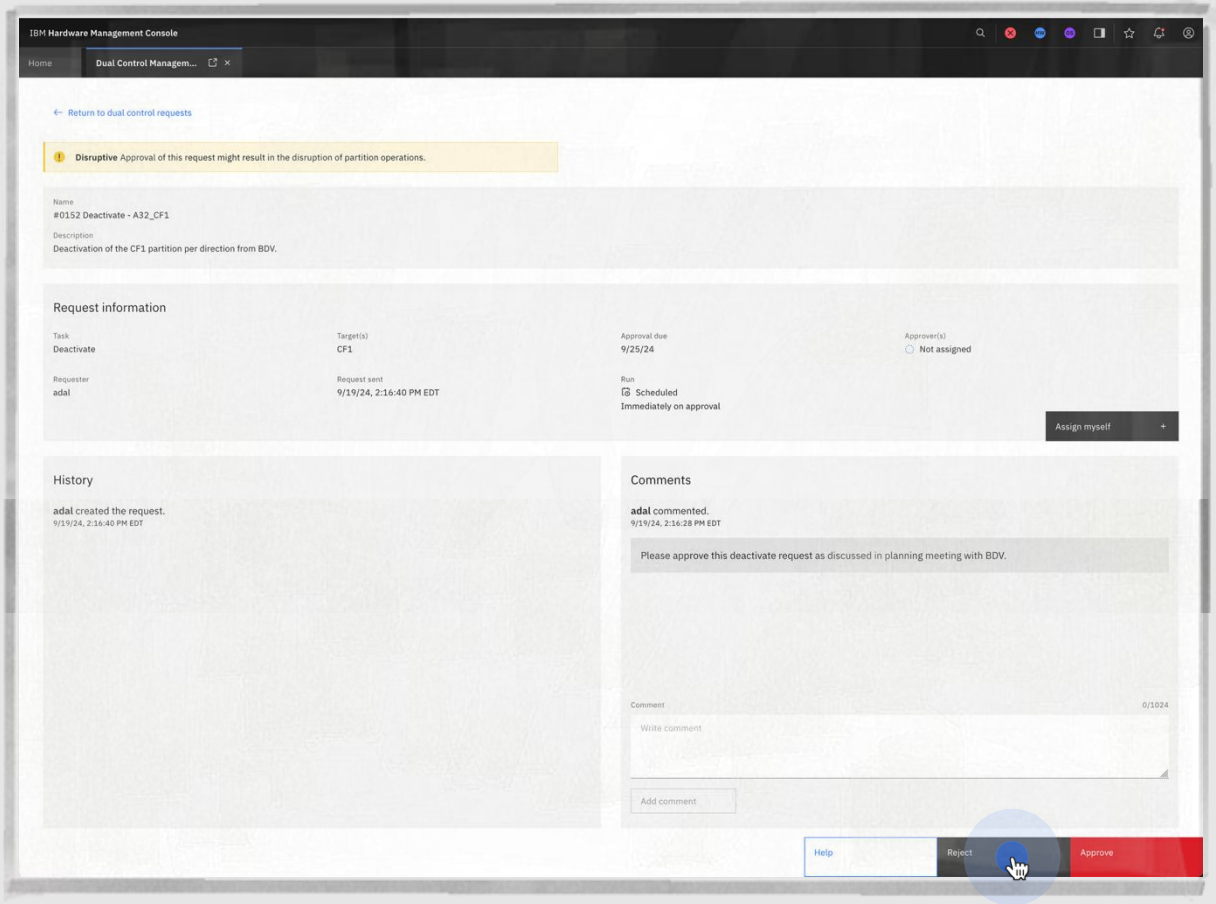
Email



Notification/Alert panel

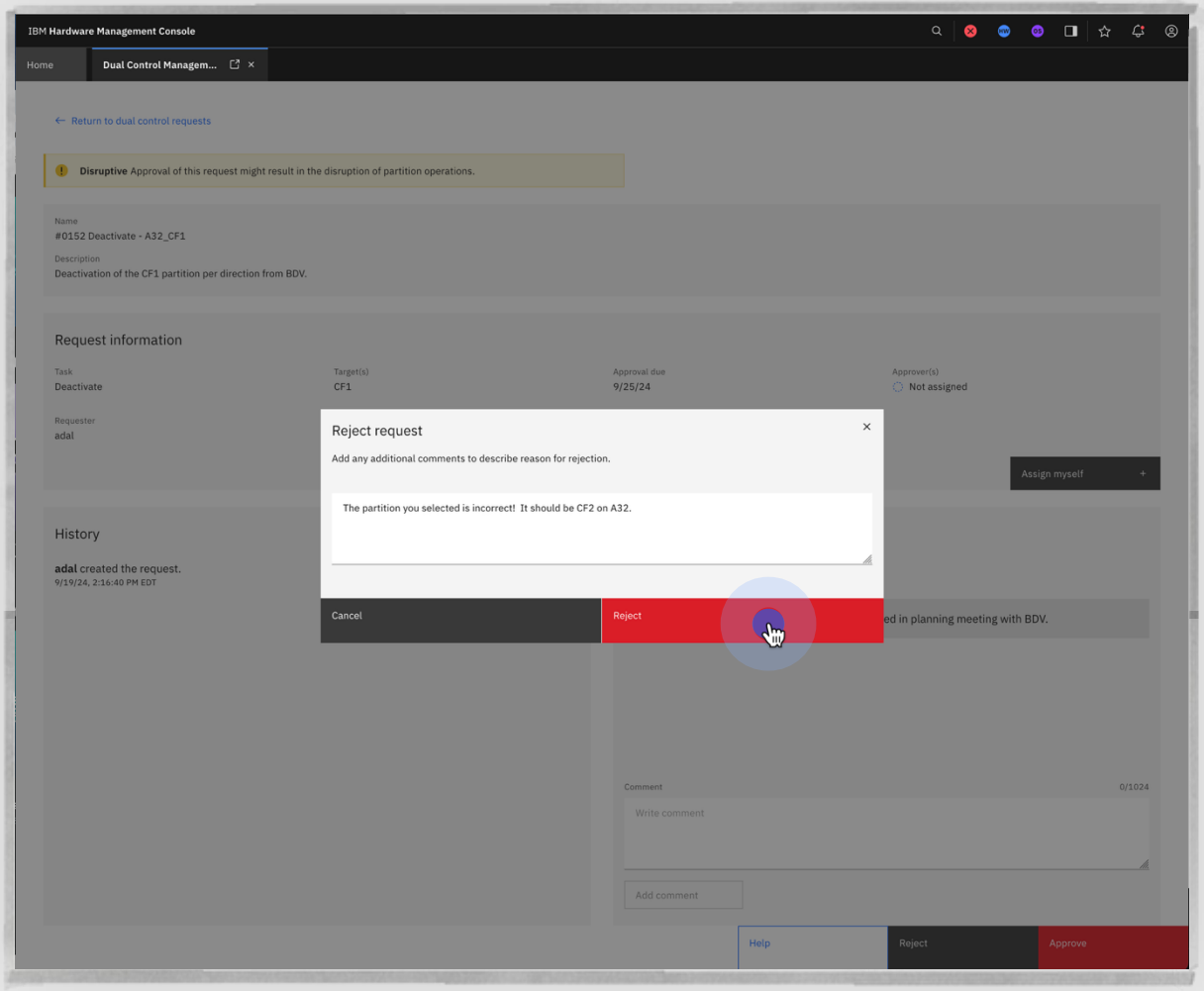
Approver reviews the request

Easton reviews the request and sees that Adele selected the wrong partition to deactivate. He clicks reject.



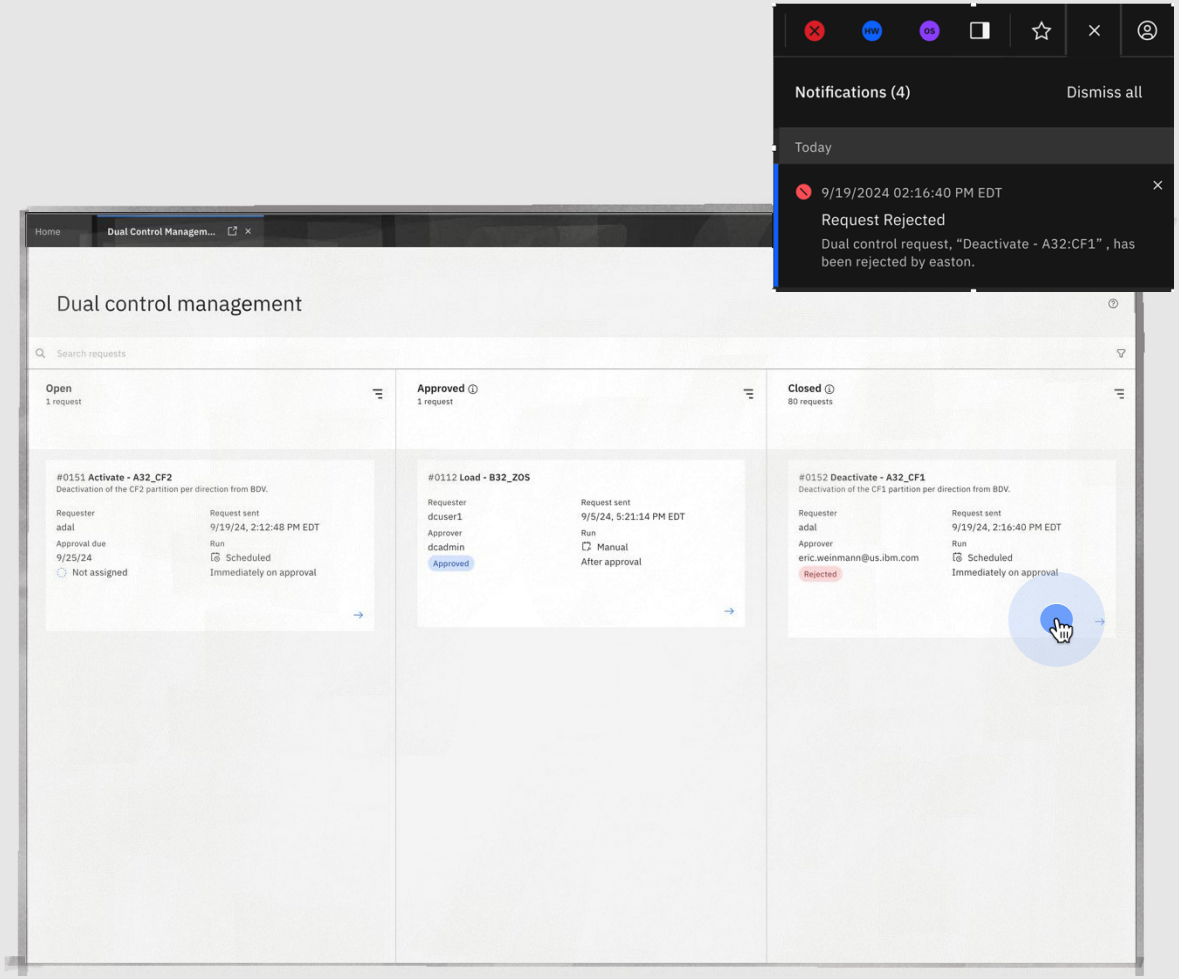
Approver rejects the request

Easton writes a comment to explain why it was rejected



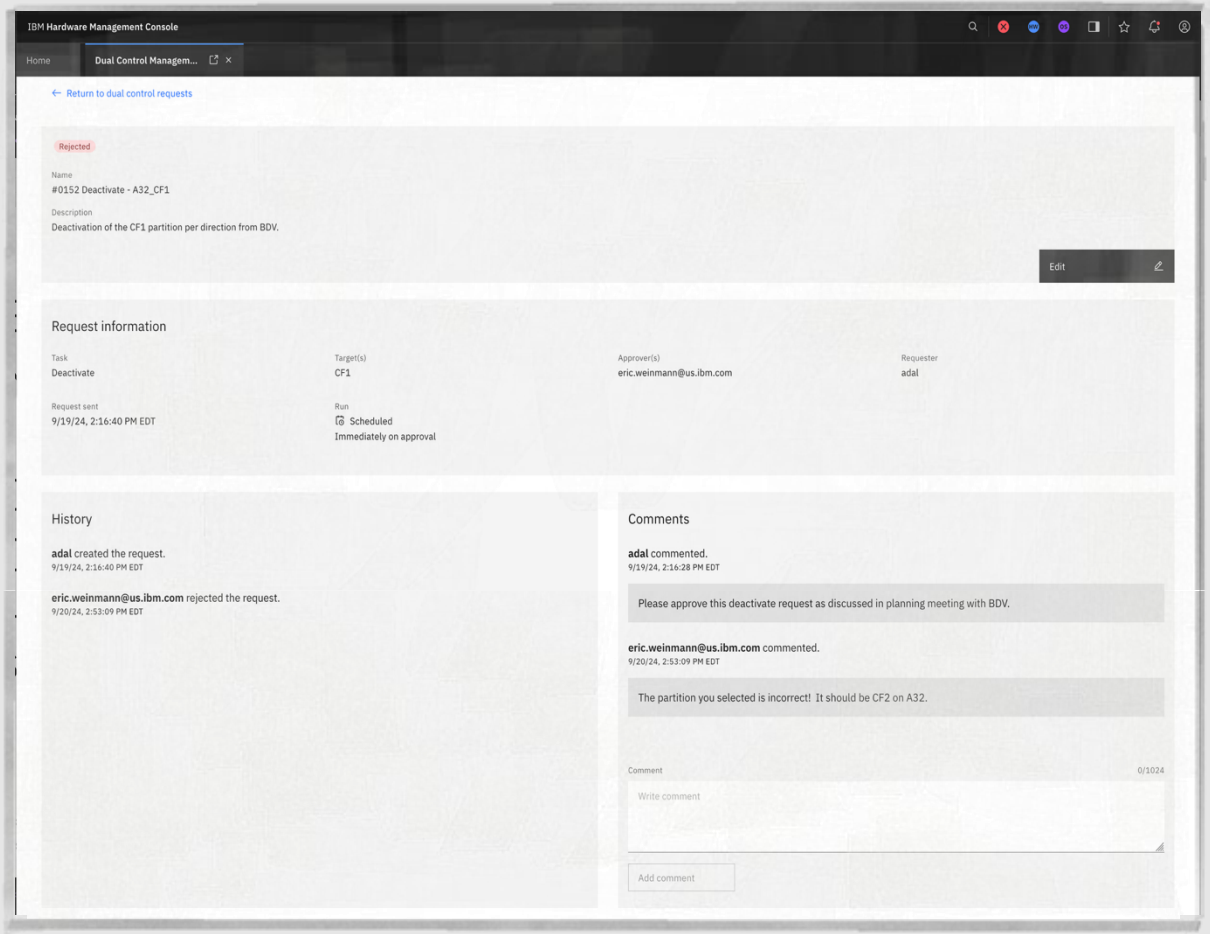
Notified of rejection, launches the dual control management task

Adele is notified that her request has been rejected so she launches the dual control management task and clicks into request card to view details



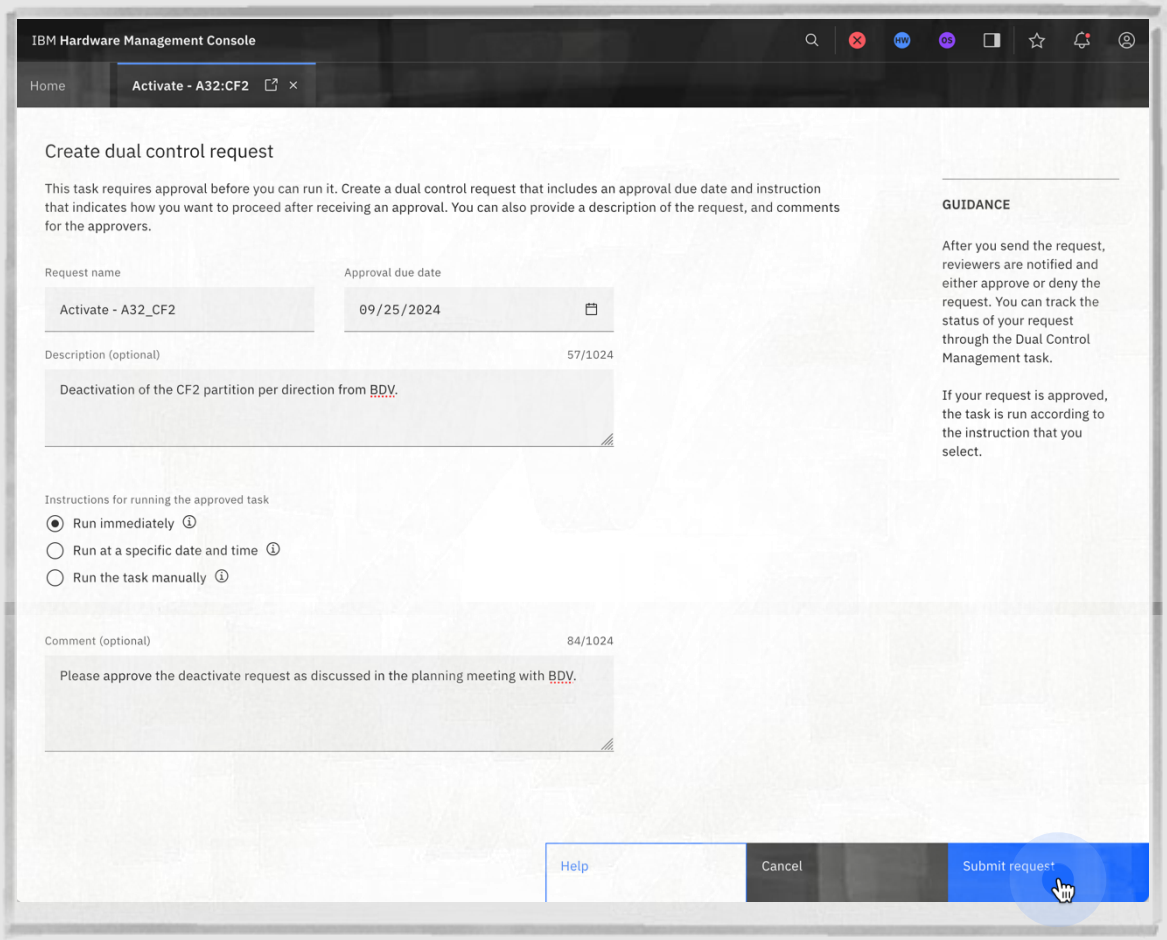
Realizing mistake

Adele reads Easton's comment about selecting the wrong partition. She proceeds to submit a new request

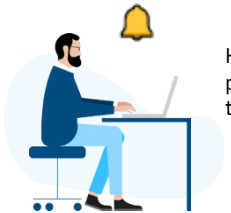


Submitting new request

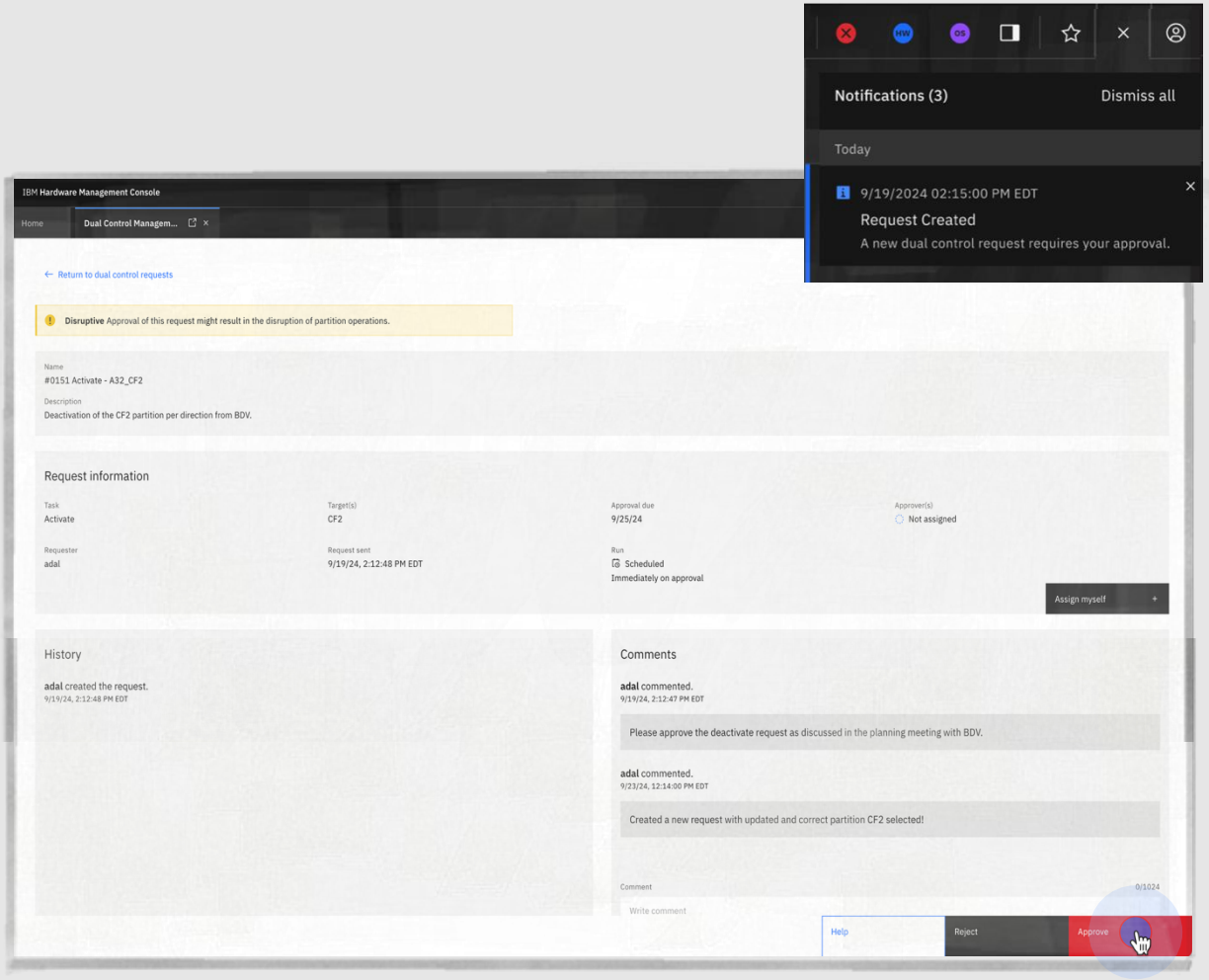
Adele makes her selections once again and ensures she has selected the correct partition to deactivate. She then submits the new request



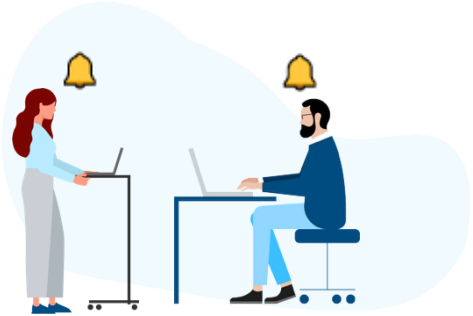
Approver is notified of the new request

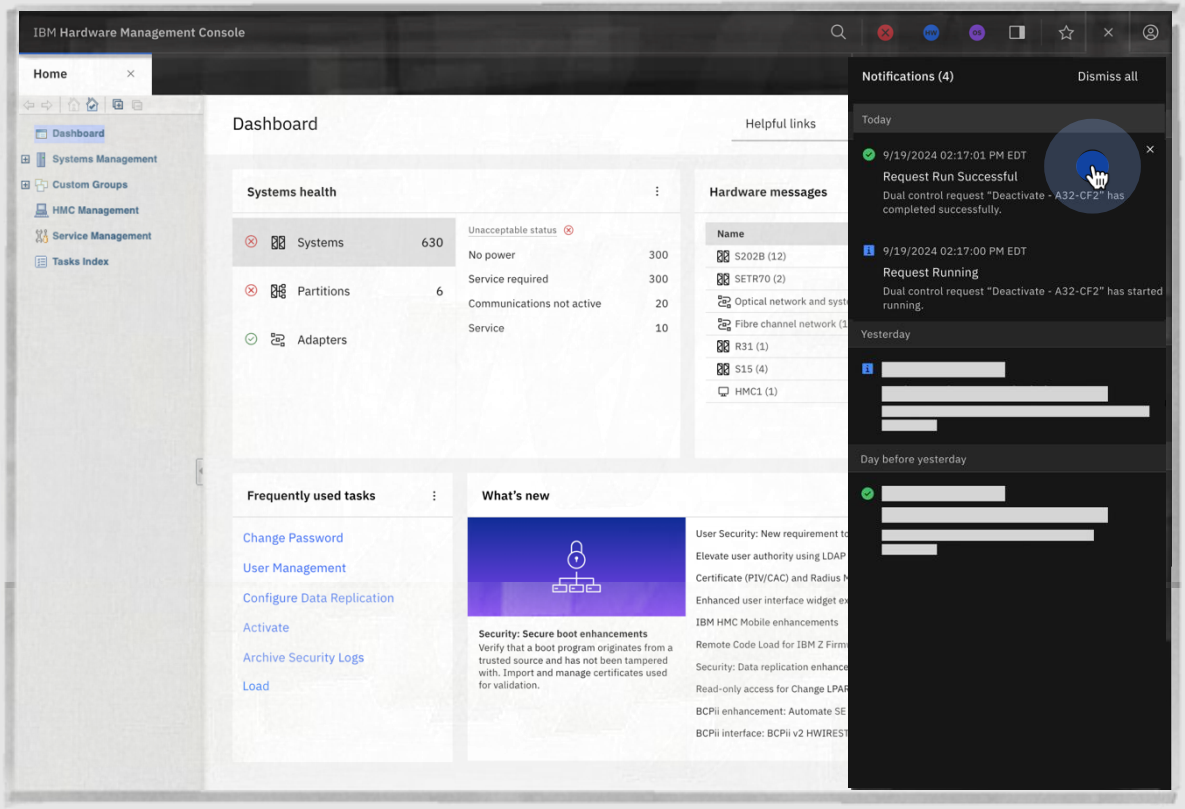


He ensures it is for the correct partition. He sees it is and approves the request



Deactivate is run and both Adele and Easton are notified





Adele and Easton are review the results

← Return to dual control requests

Successful

Name
#0160 Deactivate - A32 CF2

Description
Deactivation of the CF2 partition per direction from BDV.

Edit

Request information

Task
Deactivate

Target(s)
CF2

Approver(s)
eric.weinmann@us.ibm.com

Requester
adal

Request sent
9/23/24, 2:12:08 PM EDT

Run
Successful
9/12/24, 5:01:09 PM EDT

History

adal created the request.
9/23/24, 2:12:08 PM EDT

eric.weinmann@us.ibm.com approved the request.
9/23/24, 2:14:44 PM EDT

Deactivate has started.
9/23/24, 2:14:44 PM EDT

Deactivate has completed.
A32:CF2 is in a deactivated state.
9/23/24, 2:14:45 PM EDT

Comments

adal commented.
9/23/24, 2:12:08 PM EDT

Please approve the deactivate request as discussed in the planning meeting with BDV.

adal commented.
9/23/24, 2:13:37 PM EDT

Created a new request with the updated and correct partition CF2 selected!

Comment 0/1024

Dual Control Summary

01

Role-based task and object enablement

Security Administrators can enforce controls on which tasks & objects & users require Dual Control, and which users are granted permission to approve a Dual Control request.

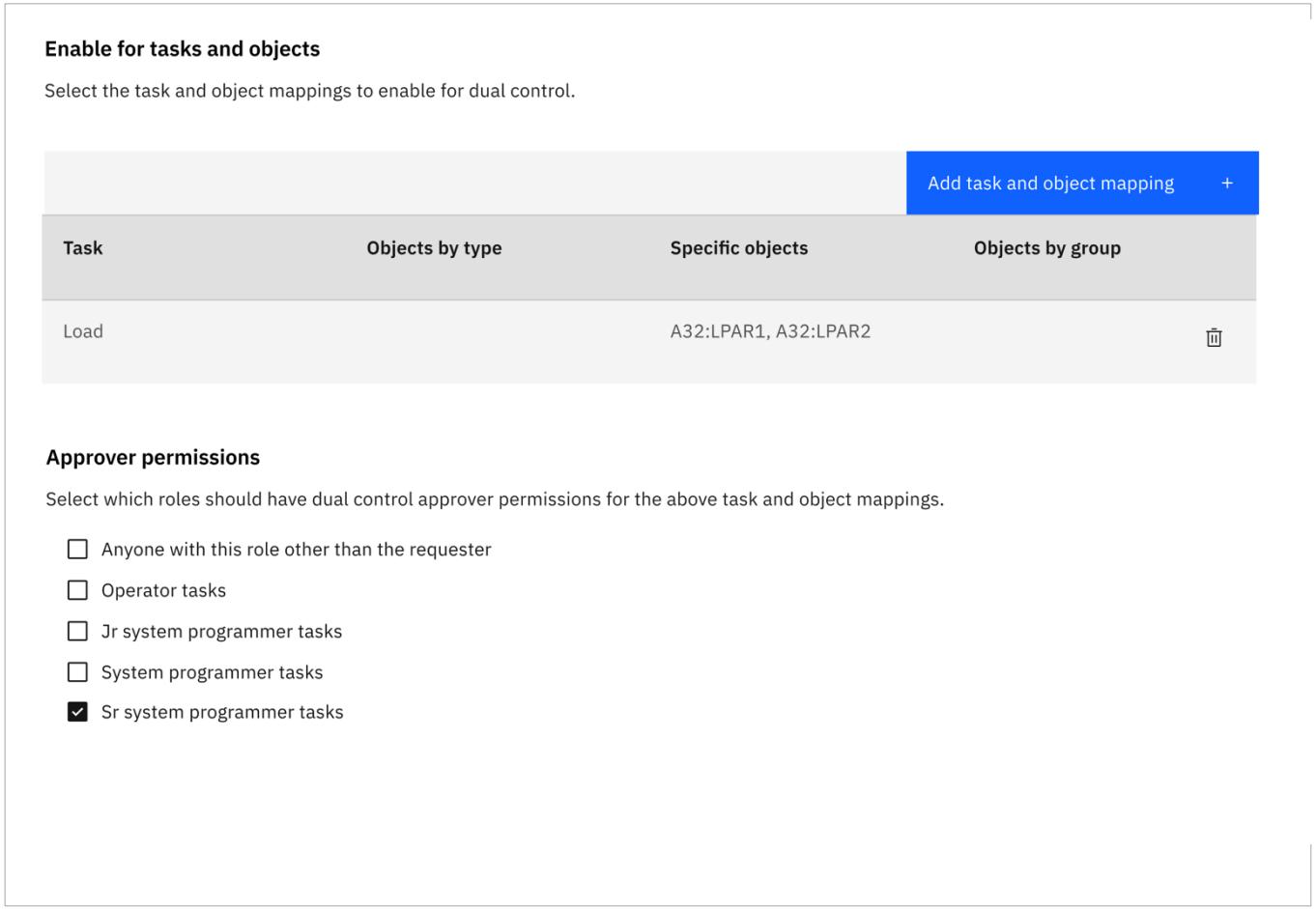


Image: Task and object mappings selection, approver permissions

Dual Control Summary

02

Flexible request options

Users can submit Dual Control requests for supported tasks with different run options:

- Run immediately
- Run at specific date and time
- Run manually by requester
- Run manually by requestor restricted to a time window

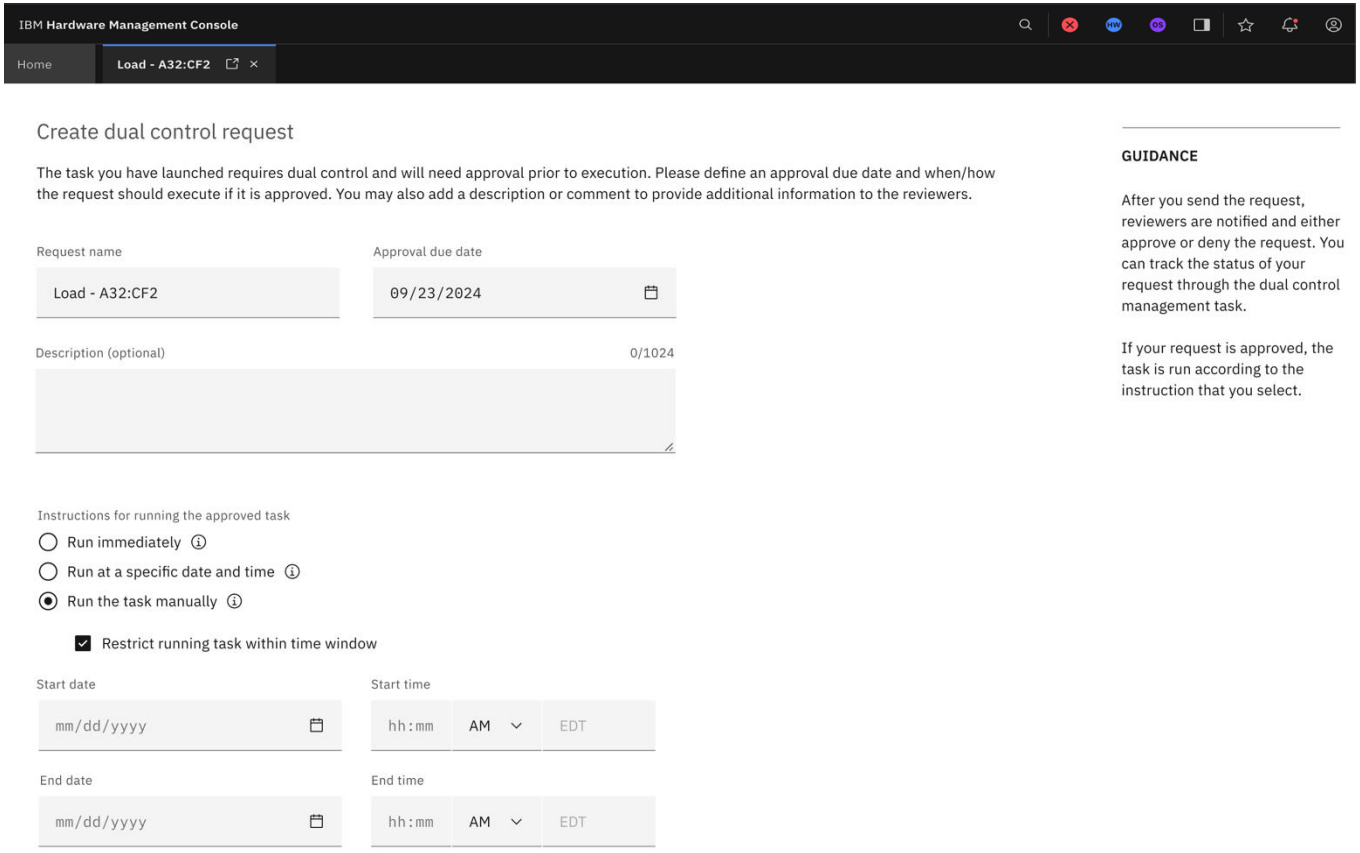


Image: Task to be run by requestor restricted to a time window

Dual Control Summary

03

Real-time notifications

Users are notified about the status of a dual control requests on the HMC, and through external methods (emails, HMC mobile notifications, APIs) to get as close to real-time visibility as possible.

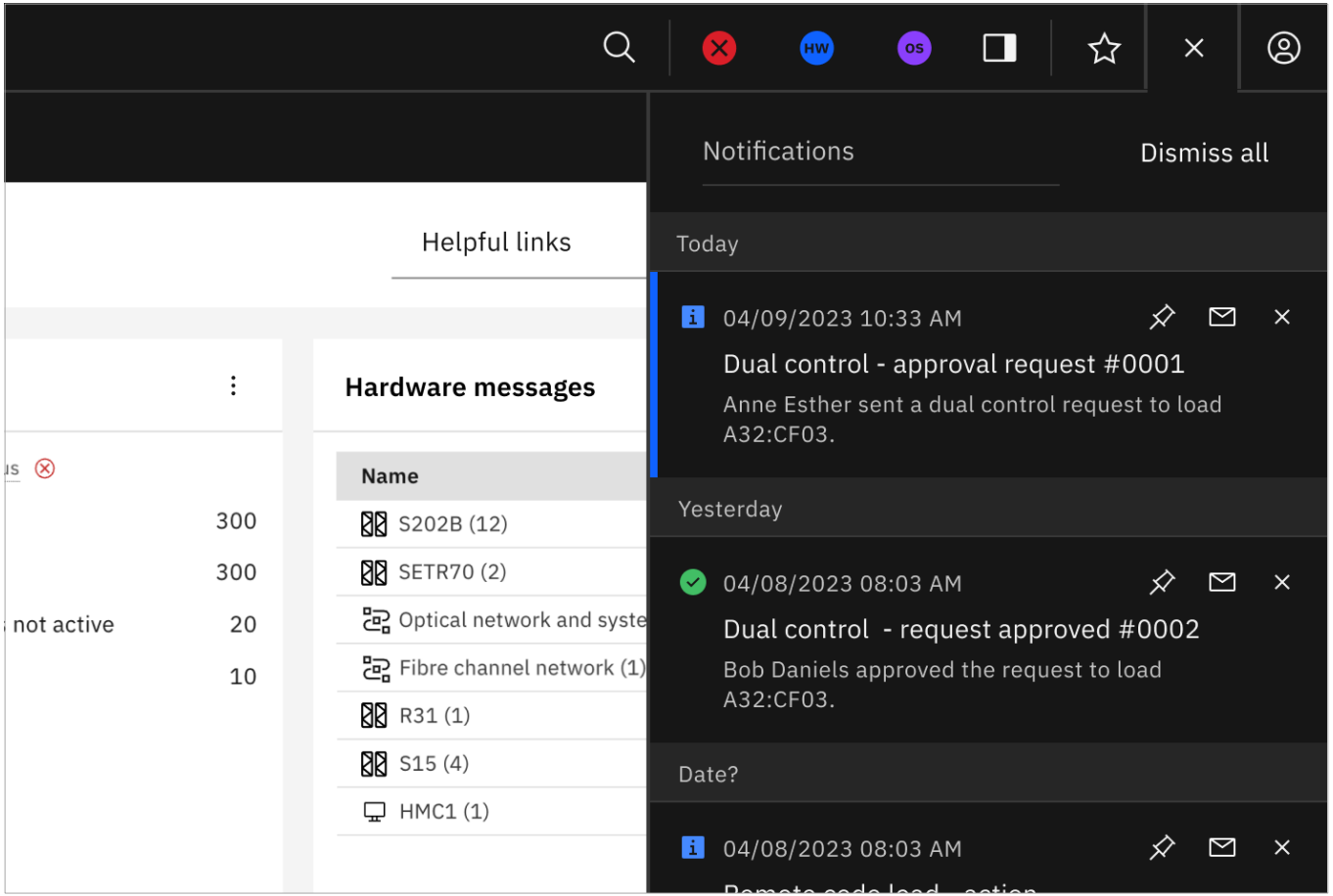


Image: Notifications panel on the HMC

Dual Control Summary

04

Request management and tracking

Requestors and approvers track the status of Dual Control requests in the Dual control management task.

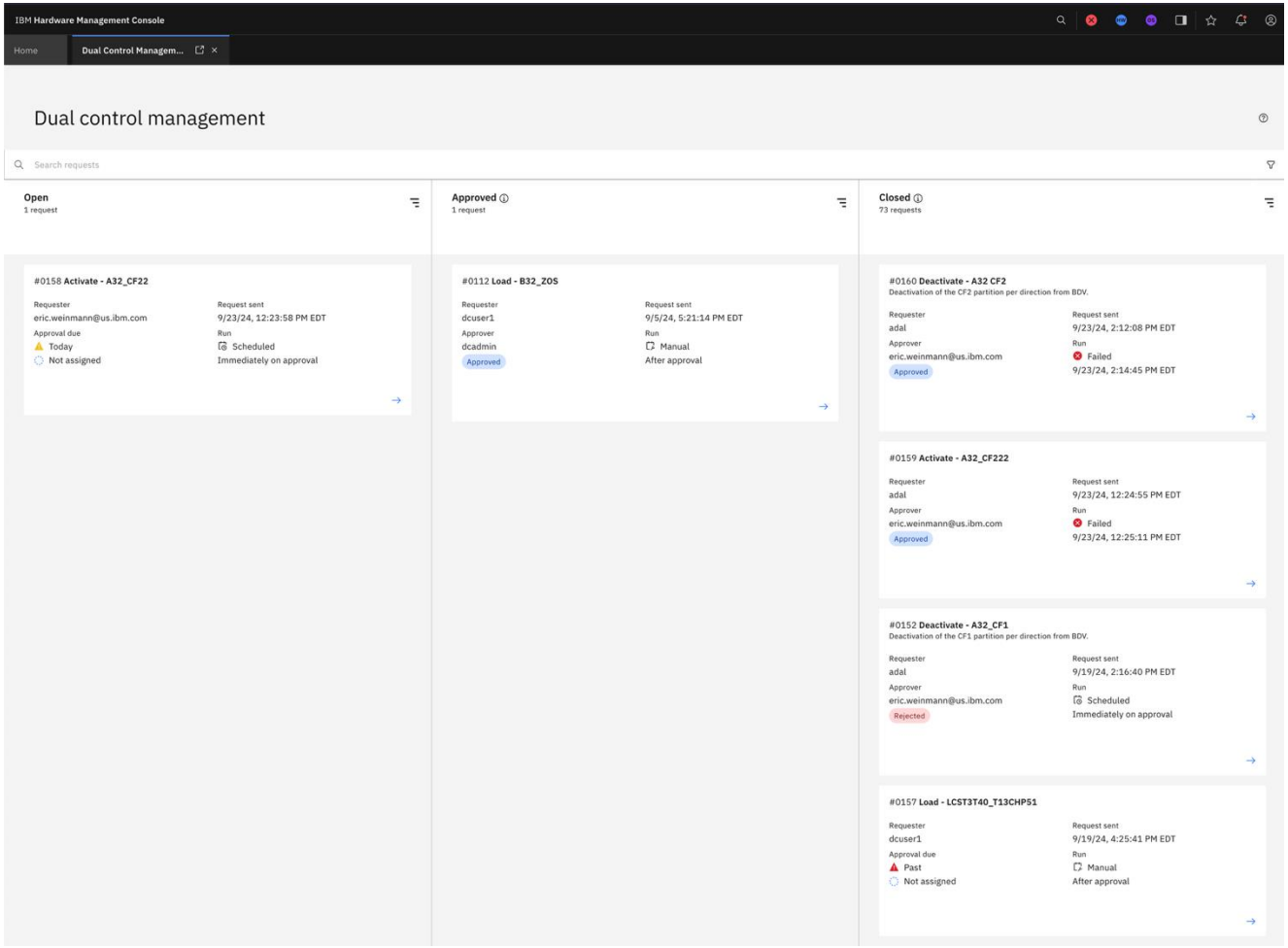


Image: Dual control management task kanban board

Dual Control Summary

05

Approver autonomy

Approvers can assign themselves to requests. They are provided with supporting information to make an accurate judgement to approve or reject a Dual Control request. Key information is:

- Requestor and approver information
- Task inputs
- History of events
- Comments
- Approval due date
- Run options
- Run time window

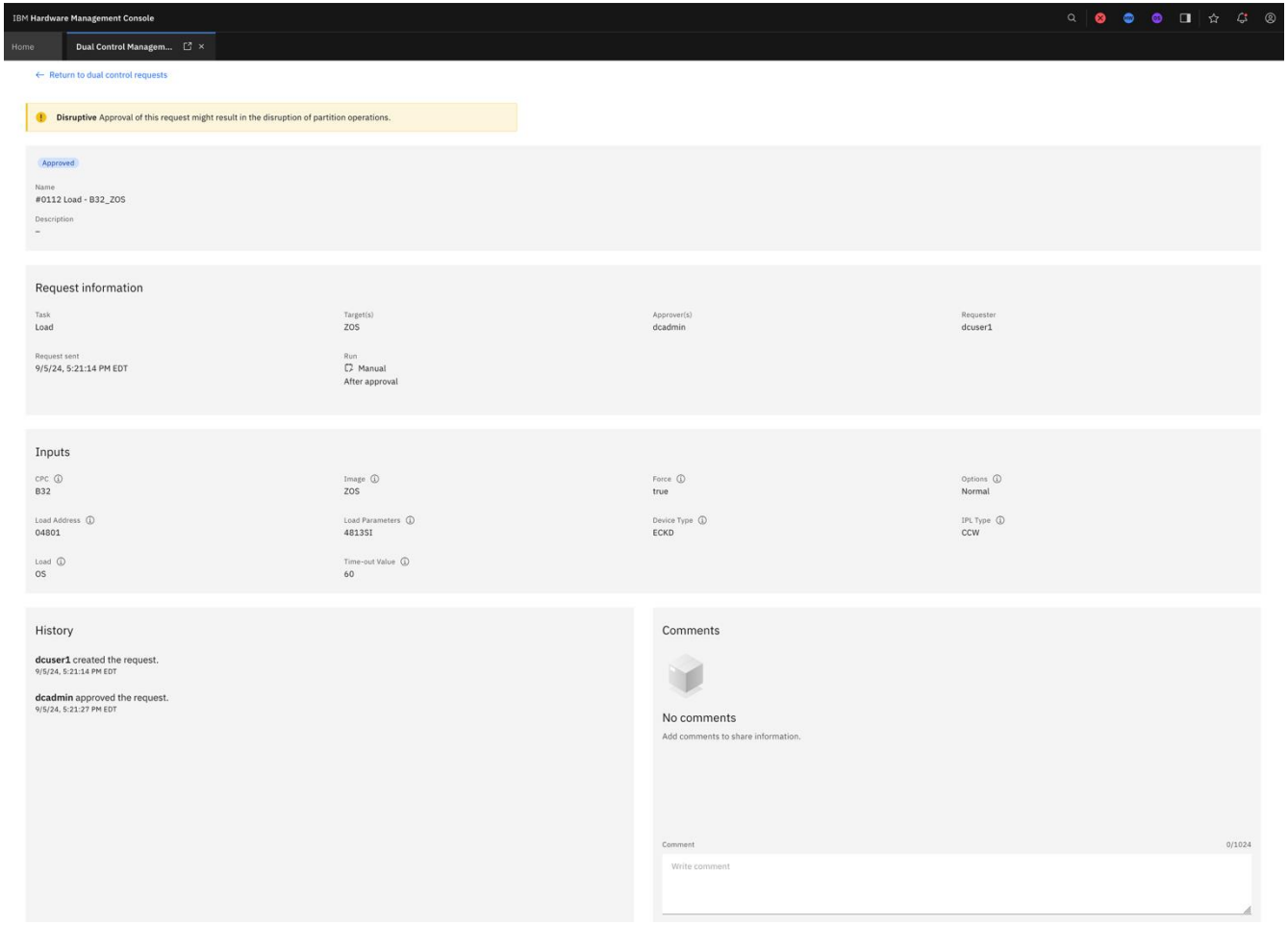
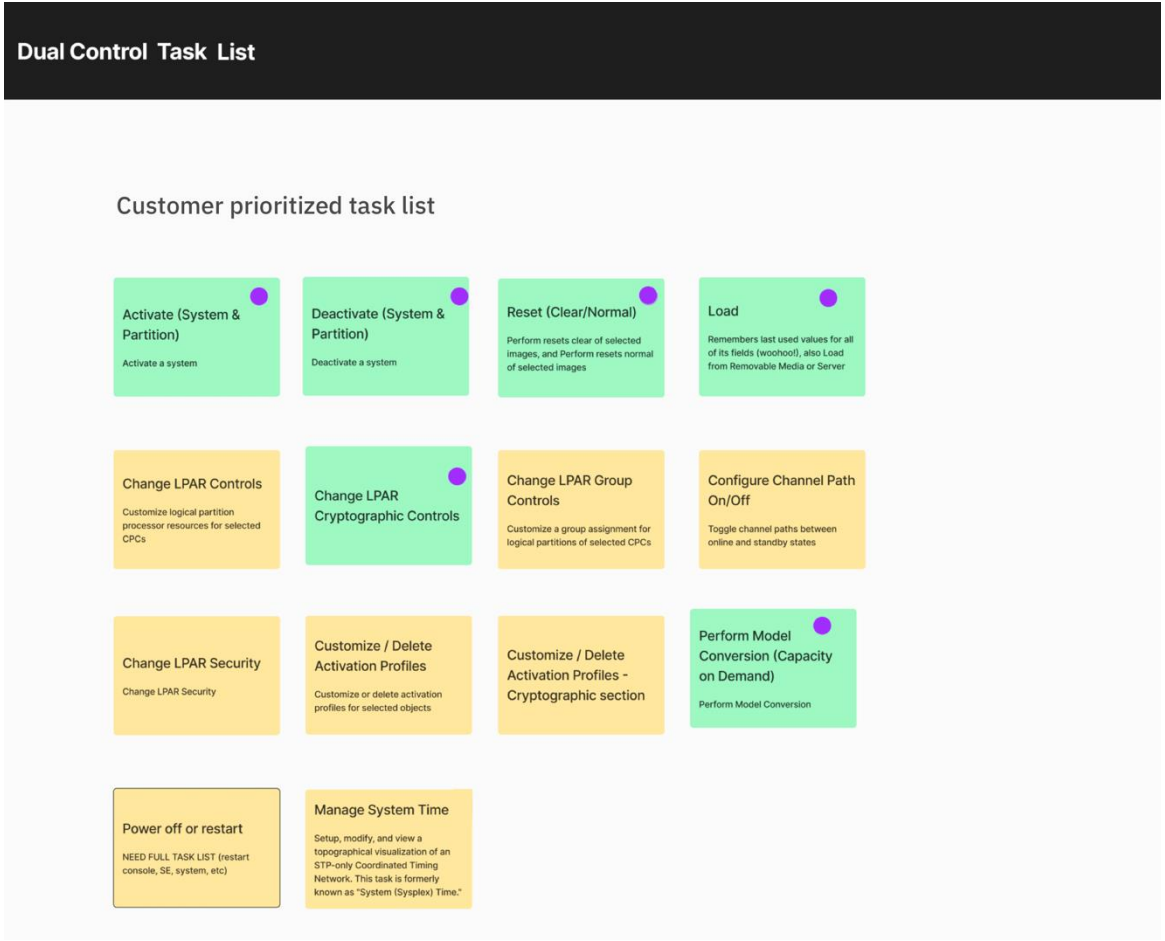


Image: Dual control request review page

Dual Control

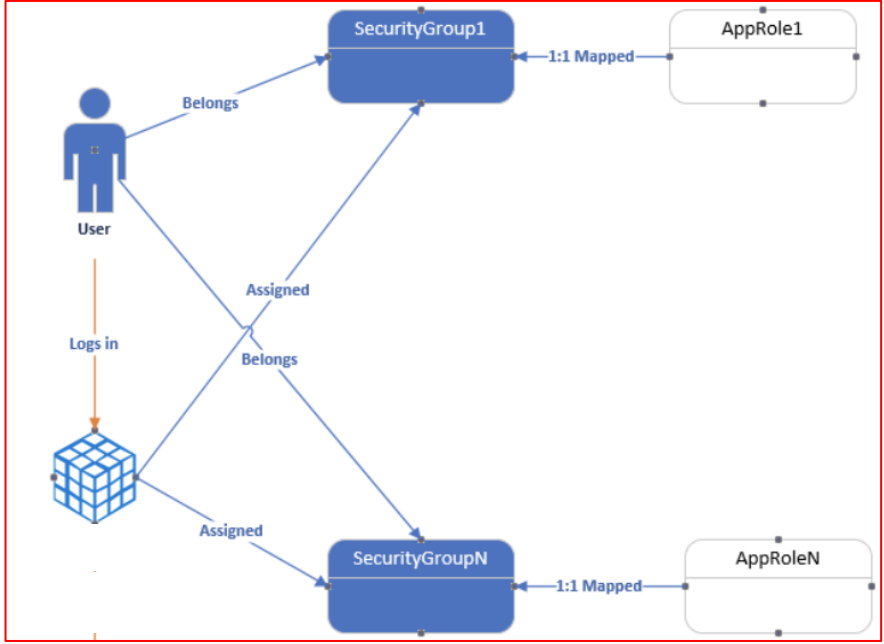
Supported tasks

- Activate
- Deactivate
- Stop (DPM)
- Reset
- Load
- Change LPAR Cryptographic controls
- Perform Model Conversion



Single Sign On

Single Sign On (SSO)



➢ Requirement for Federated IDs

- Protocol
  - OIDC (OpenID Connect)

➢ Design Approach

- Utilize SSO server Logon UI for userid, password, MFA code leveraging SSO server for validation
- Map authorization to User Templates with updated mapping controls of LDAP Groups to OIDC Groups

What is Single Sign On?

- New authentication method for the HMC/SE
- HMC/SE never knows the user's credentials
- Allows for users to use existing credentials from other services on the HMC/SE
- OpenID Connect (OIDC) is the technology used
- **Note:**
  - This provides a means for clients to utilize various MFA types which are only provided by IBM Z MFA OS component
    - SSO server provides the MFA support
    - Note that the only native HMC MFA is TOTP (Time based One Time Password)

Network Time Security

Network Time Security (NTS) And Other Enhancements

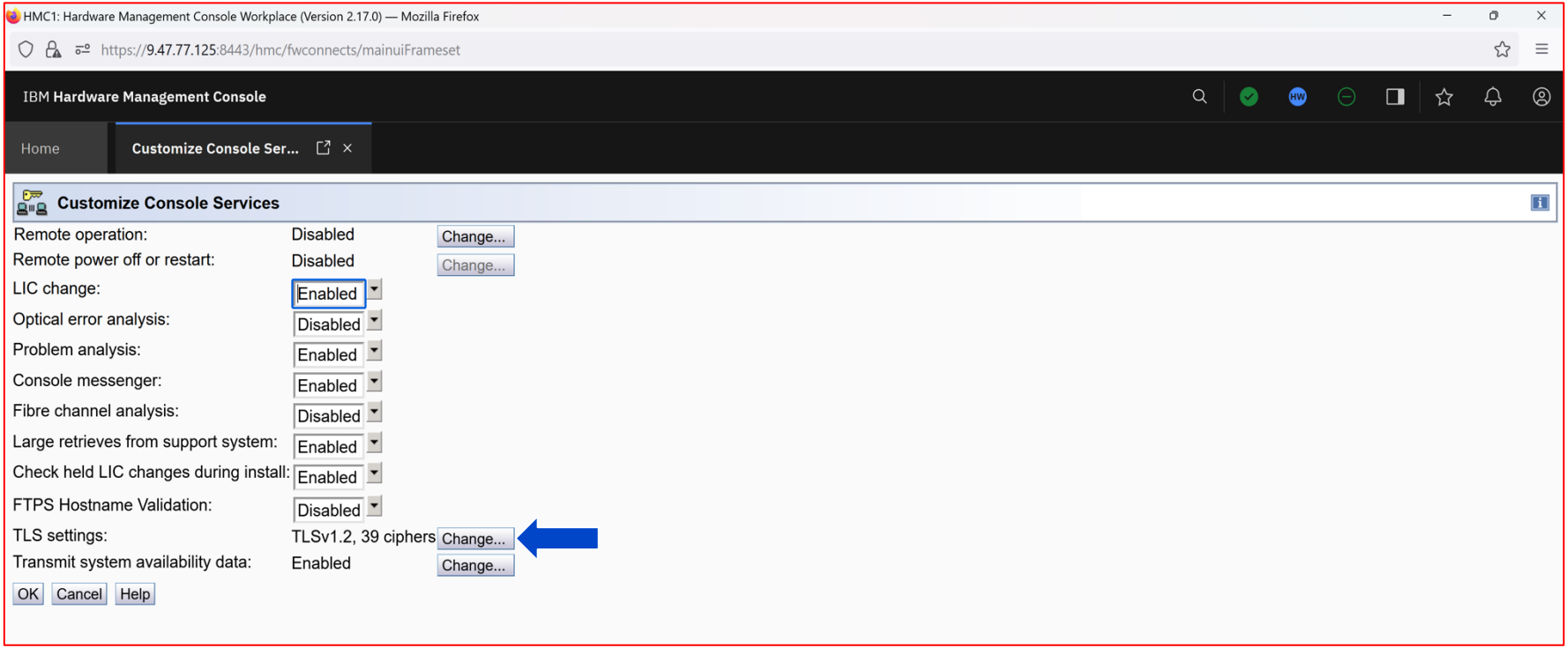
- HMC Manage System Time task Enhancements
  - Configure External Time Source (ETS) action
    - Support for 3 Network Time Protocol (NTP) servers
    - Support for 2 Precision Time Protocol (PTP) servers
    - Support for Mixed Mode (use of both NTP and PTP servers in parallel)
  - Manage CTN Certificates STP action
    - Allow use of certificates for secure NTS NTP communications between the CPC and configured ETS(es)
  - HMC Customize Console Date\Time task
    - NTP NTS support for HMC ↔ External Time Source connections
  - PTP Communication support
    - Multicast & Unicast (new)

TLS Cipher Suite Configuration

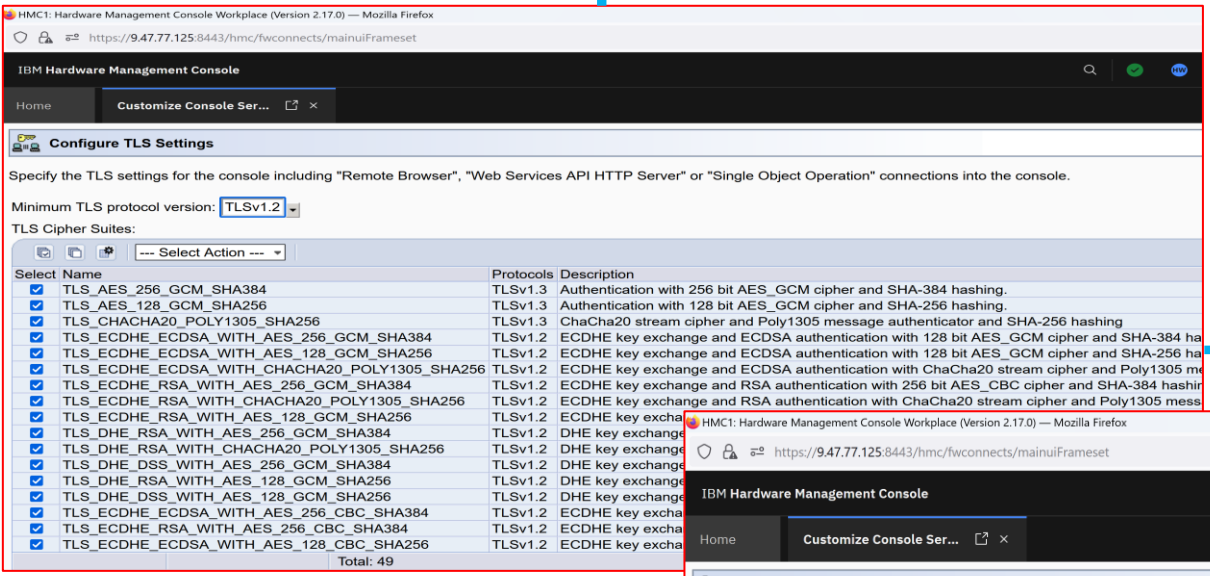
Cipher Suites Filtering per TLS

➢ Single Customize Console Services sub-task, Configure TLS Settings => mapped to Cipher Suites

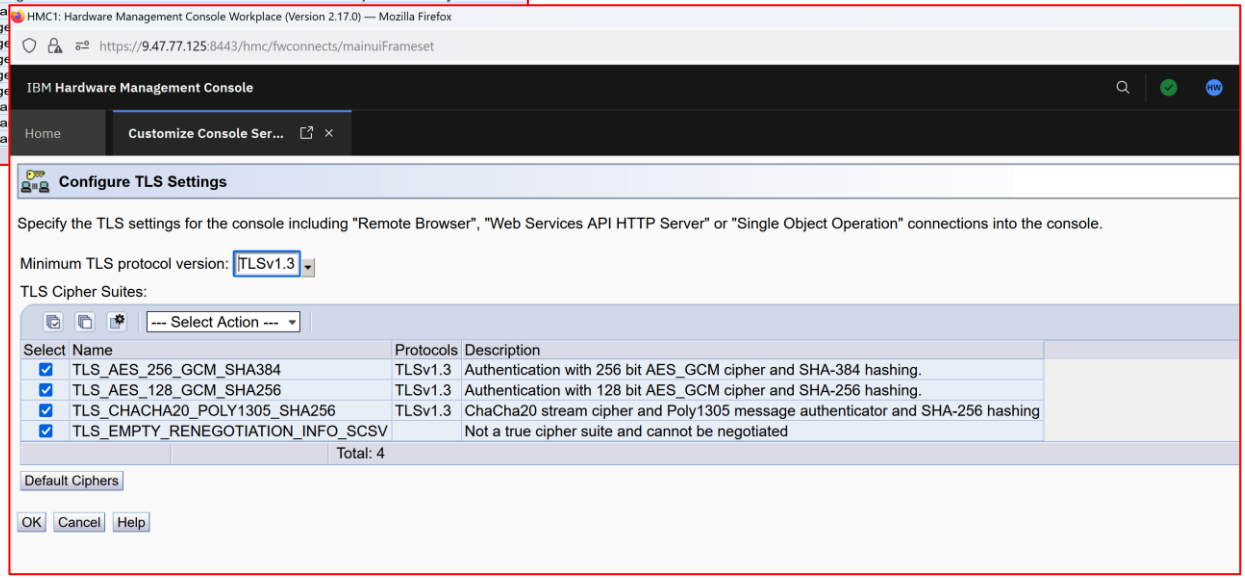
- Individual cipher suite shown for management based on Minimum TLS level



TLS 1.2 Filtered Ciphers



TLS 1.3 Filtered Ciphers



Complete HMC User configuration replication to SEs

HMC User Data Replicated to SE

➢ Strategy

- Provide ability to manage all user data in a single place, i.e., the HMC

➢ Existing support

- Standard HMC user definitions are replicated to managed SEs
- Clients can utilize these HMC user definitions to logon locally to the SE

➢ What's changing?

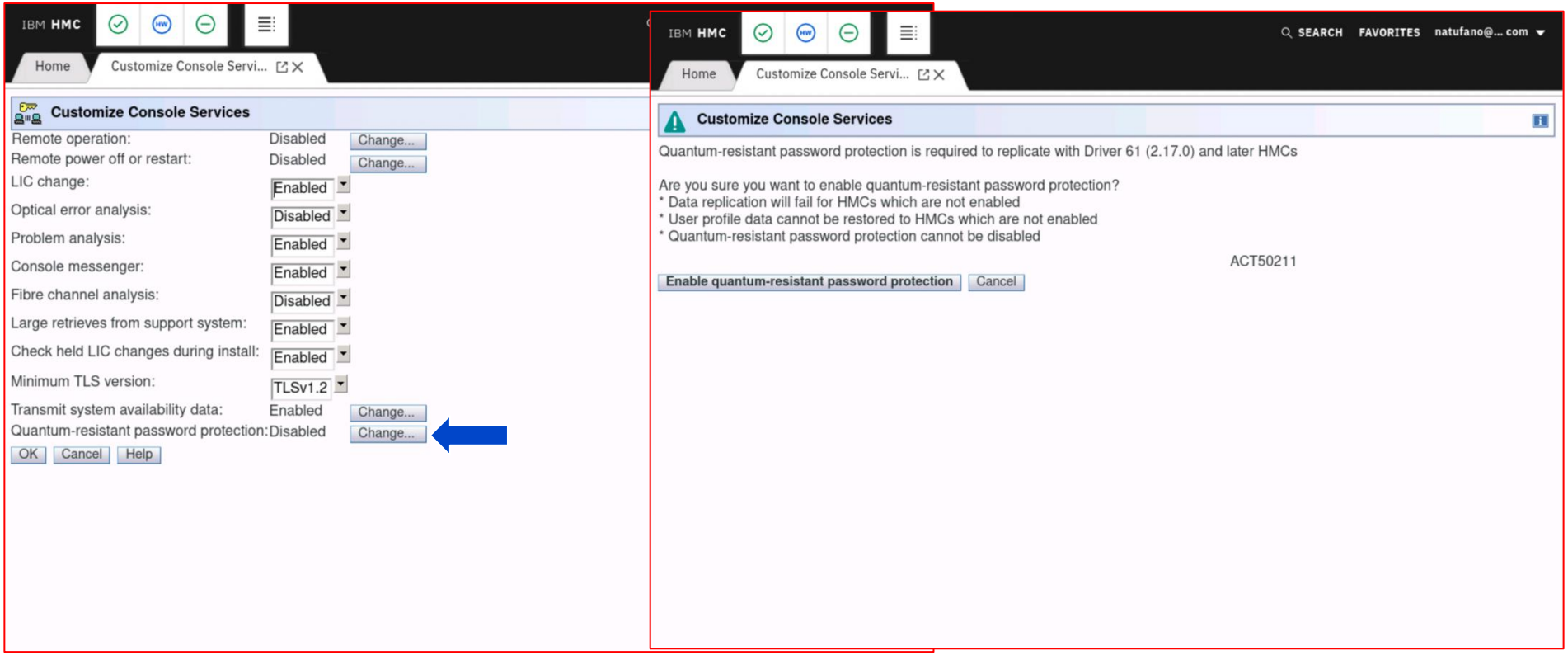
- HMC defined user patterns and templates including LDAP Server definitions are now replicated to managed SEs
- Clients can utilize these HMC definitions to logon locally to the SE with pattern-based users
- Recommend doing all HMC User Data definitions (not just users) only on HMC, no User Mgmt on SE

Quantum-Resistant Password Hashing

Local Users Quantum-Resistant Password Hashing

- With z17, quantum-resistant hashing algorithm applied to storage of local users passwords
  - Prior to z17, local user password hashing used, but with z17, now it's quantum-resistant
  - **Note:** HMC/SE are also closed appliances with no access and additionally have an encrypted SSD
- User recommendation: define HMC Users on one HMC & allow replication to other HMCs and to SEs
- Implications of z17 HMC Local users replicated to other HMC/SE levels
  - **z17 HMCs/SEs:** none
  - **z16/z15 HMCs/SEs**
    - HMCs => HMC Data Replication of User Profile Data will be blocked until MCL/Opt In for new quantum-resistant
      - » MCL Bundle: z16 – H31, z15 – H62
      - » Must also Opt in ==> see next chart
    - SEs
      - » For SE local console logon (not Single Object Operations), HMC user/password is normally authenticated to connected HMC
      - » If no connection to HMC, SE local console logon would fail until Quantum Resistant MCL (z16 - S44, z15 – S98)/Opt In for new quantum-resistant
- **Note:** HMC LDAP or SSO authenticated users are not affected by this change

Quantum-Resistant Password Hashing – Opt In

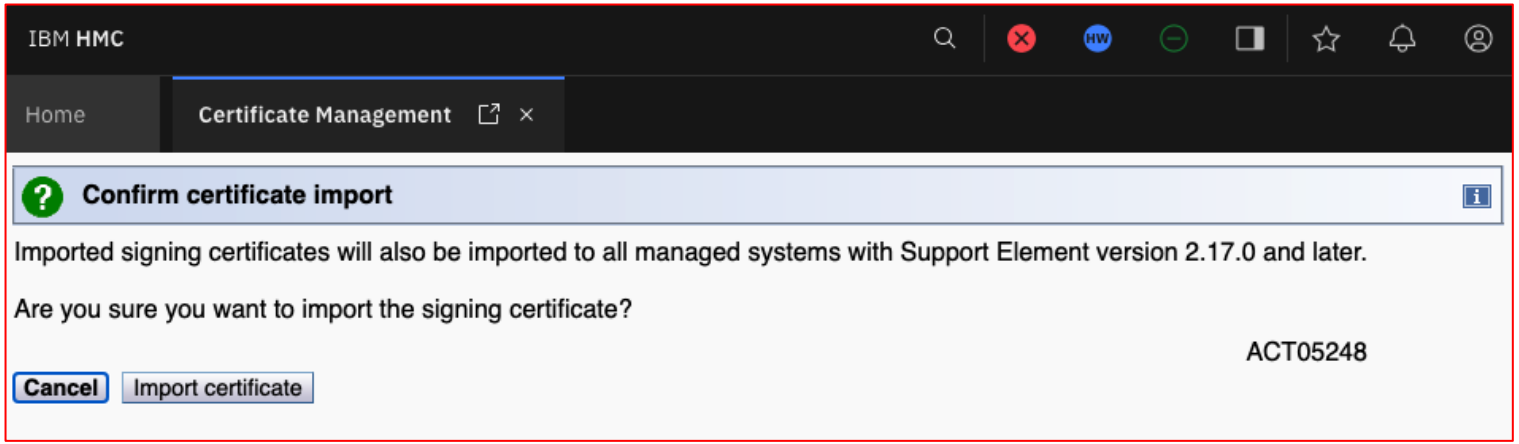


Replicate HMC Certificates to SE

Replicate HMC Certificates to SE

- Certificates imported to the HMC *Certificate Management* task will also be imported to managed IBM z17 SEs.
  - Certificates deleted from the Certificate Management task will also be deleted from managed IBM z17 SEs.
    - If multiple HMCs are managing the same SE, certificate is only deleted if no other HMC has that certificate imported.
    - If the HMC and SE stop communicating, certificates associated with that HMC are removed from the SE until communications are reestablished.
- Tasks/Options that can take advantage of this enhancement include:
  - LDAP
  - MFA
  - Remote Syslog Server
  - FTPS

New Confirmation Dialogue



HMC OSA ICC CA Signed Shared Certificates

OSA-ICC CA Signed Shared Certificates

➢ Requirements

- Prior to z17, customers must go to each individual OSA-ICC PCHID and import a CA-signed certificate one at a time
- For z17, importing a CA-signed certificate in shared scope for OSA-ICC will now be supported

➢ Base design approach

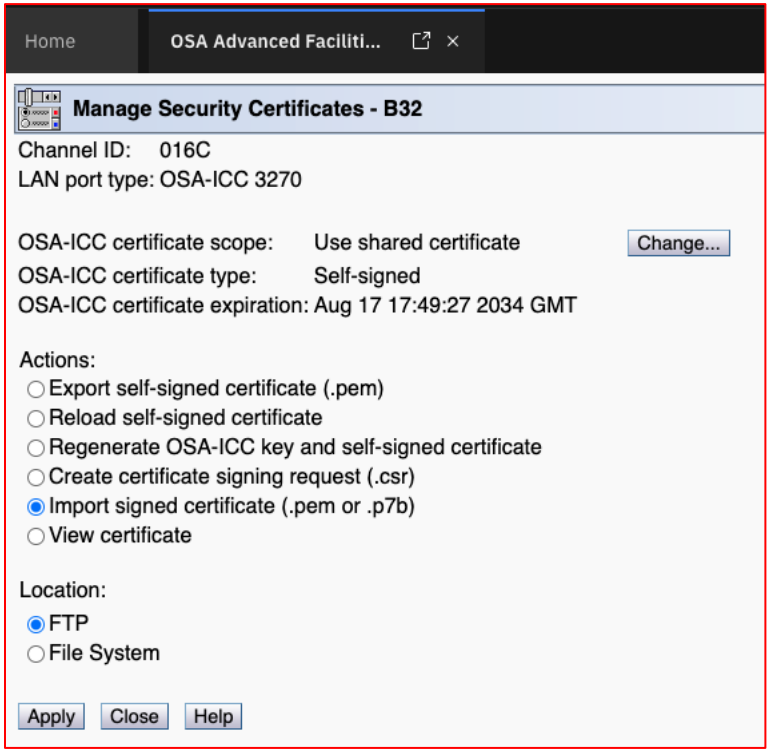
- Once a user imports a CA-signed certificate in shared scope, the panel will replace a certificate that's shared across OSA PCHIDs with the imported CA-signed certificate

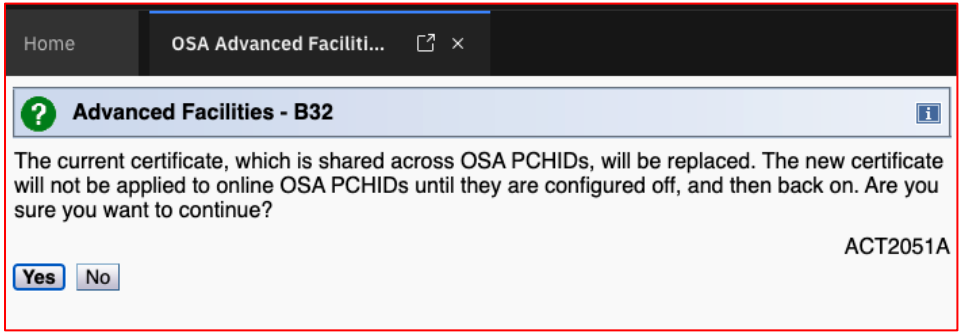
➢ User Interface (UI) Changes

- OSA Advanced Facilities Manage Security Certificates
  - Import signed certificate

Note: The new certificate will not be applied on the online OSA PCHIDs until they are configured off, and then back on.

OSA-ICC CA Signed Shared Certificates





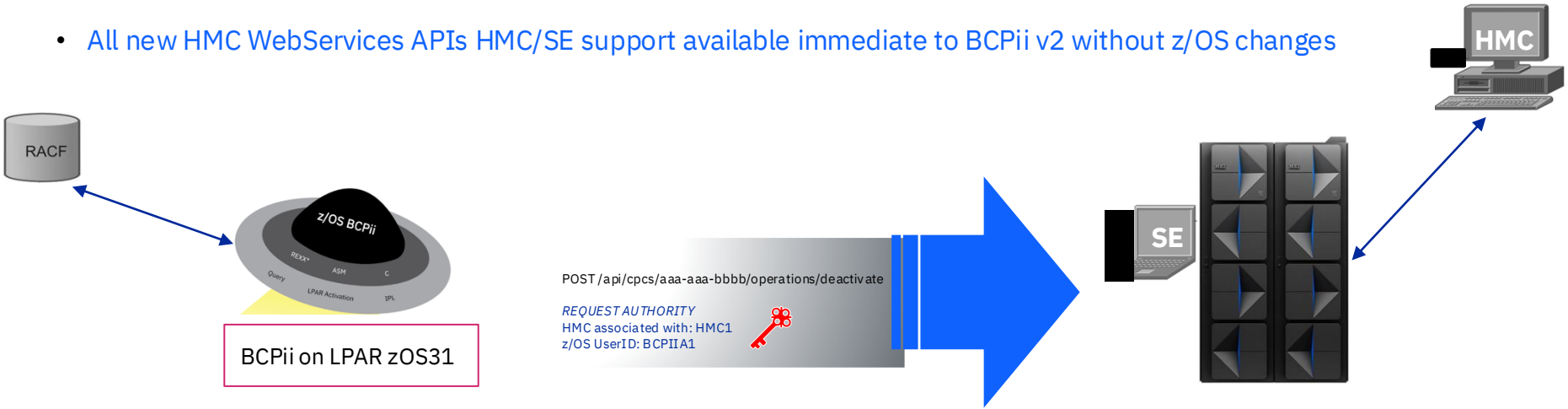
BCPii Enhancements/SOD

BCPii v2 Enhanced Security, HMC Target, Async support

- BCPii HWIREST/v2 will pass the z/OS USER ID to SE/HMC via signed JSON Web Token (JWT)
  - *z/OS user mapped/limited to HMC user task/object permissions*
- Enhanced Security plus
  - *HMC Target support*
  - *BCPii HWIREST/v2 Asynchronous Notification support*
- BCPii HWIREST/v2 Infrastructure fully complete with z17 GA1 with associated z/OS release
  - All new HMC WebServices APIs HMC/SE support available immediate to BCPii v2 without z/OS changes

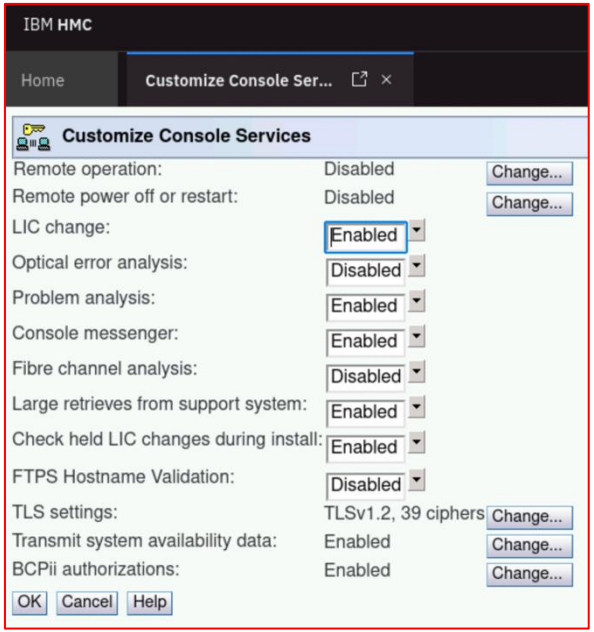
map zos UserID **BCPIIA1** to
HMC UserID **BCPiiAutomation1**

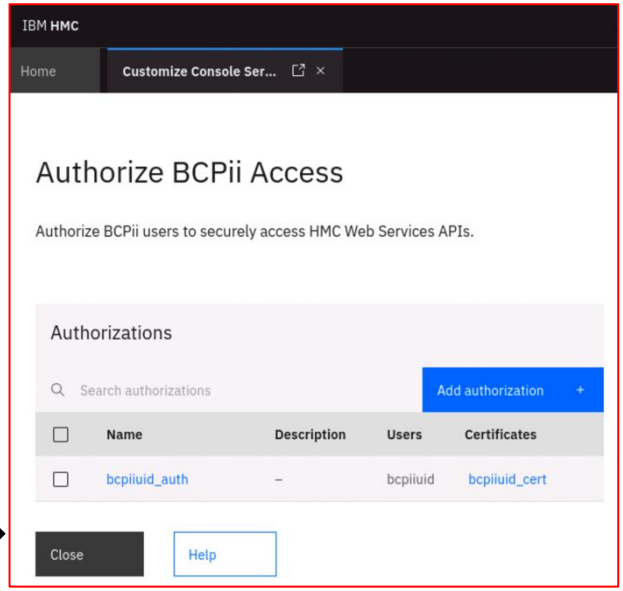
BCPiiAutomation1
Tasks: Activate, IPL
Resources: zOS24, zOS25

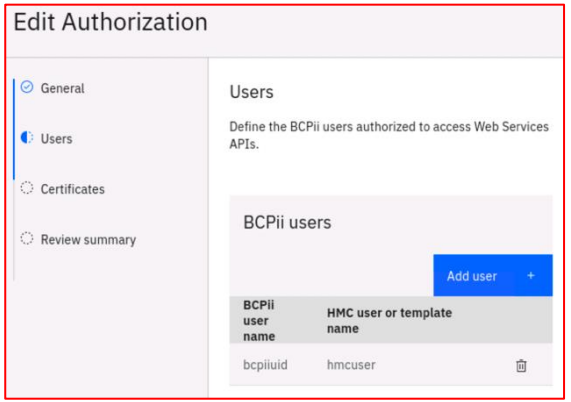


Configuring an HMC for BCPii Targeting

- The HMC needs to be configured to validate a JWT and map the z/OS BCPii ID to an HMC user
  - Import bcpii-authorization certificate used to validate JWT signature to HMC
  - Associate the certificate(s) with a BCPii to HMC user mapping
- The *Authorize BCPii Access* sub-task can be launched from *Customize Console Services*







SOD for BCPii v1/SNMP Deprecation

- z17 addresses BCPii v2 limitation on Asynchronous Notifications
- There will be no further feature enhancements in BCPii v1
  - Nor for the HMC/SE SNMP automation interface
- All future feature enhancements will only be for HMC/SE WS APIs & BCPii v2

- Above Translation: BCPii v1 & SNMP are being deprecated
  - BCPii v1 & SNMP are available or allowed; would recommend developing migration plan once a client has a z17 CPC
  - From Google:
    - A functionality that is deprecated is likely to be removed in the future, hence it is not advisable to use it.
    - Deprecated functional items are usually replaced or updated with newer versions.
  - IBM has no roadmap target to remove BCPii v1 (yet)
    - IBM also has no timeline to remove HMC/SE SNMP support (yet)

Remote Code Load

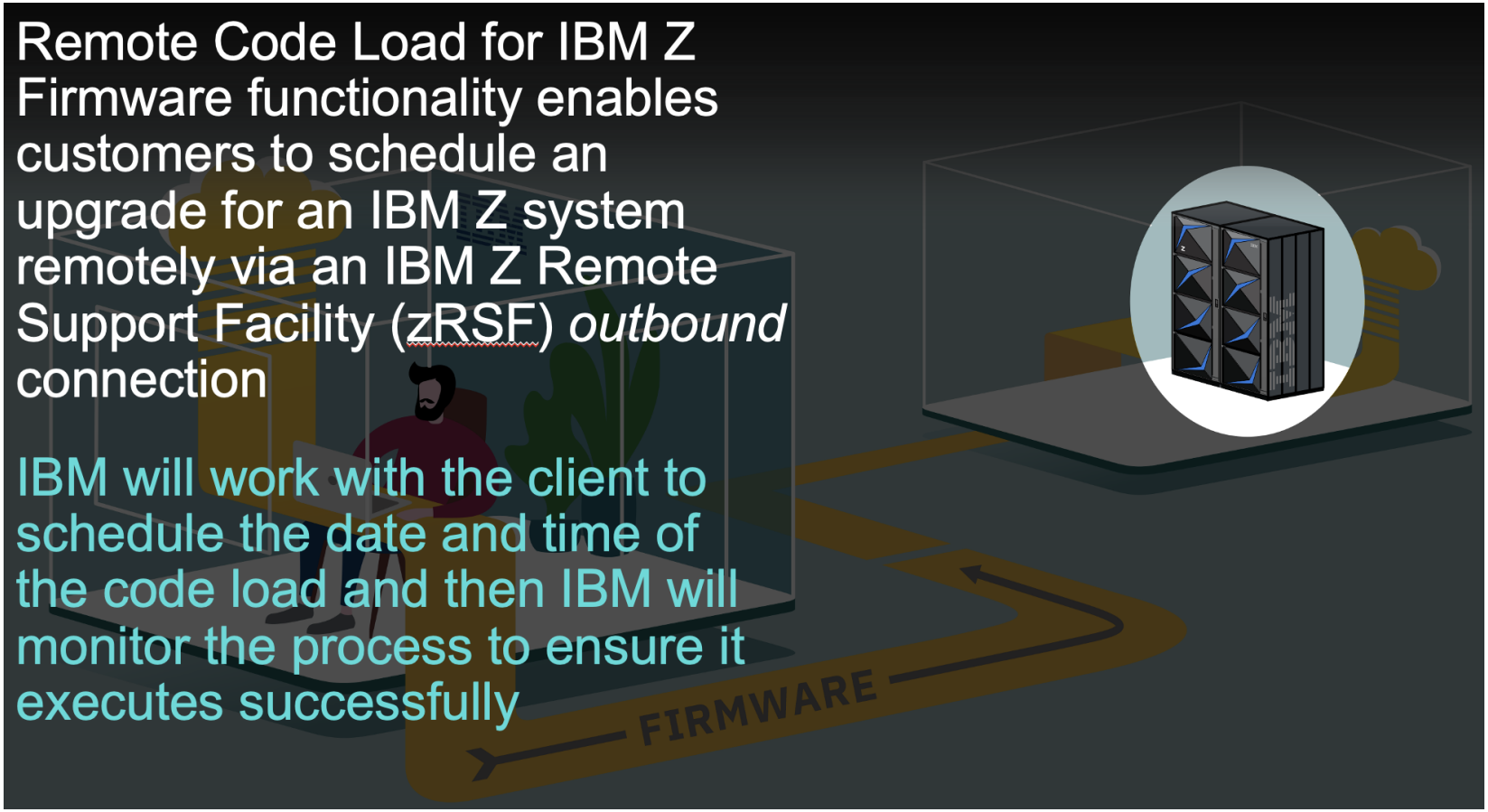
Firmware Update Process for MCLs: Remote Code Load (RCL)

- Prior to z15 2Q2021 Release
  - Firmware update on IBM Z systems could be performed by
    - IBM SSR coming onsite
- z15 2Q2021 Release introduced IBM Z Remote Code Load
  - Remote Code Load is an option which a client can request ==> Remains IBM responsibility
  - Client can also choose IBM SSR onsite method for Firmware Update
- For IBM z17, IBM recommendation is to use Remote Code Load for firmware update of MCL Bundles
  - Remote Code Load Value:
    - Flexible scheduling of MCL Bundle update via IBM Resource Link
    - No need for clients to be onsite for IBM update of MCL Bundles => clients can also perform subsequent testing remotely
  - z16 & z17 significant amount of RCL Enhancements (see Appendix for additional info on Remote Code Load & z16 RCL Enhancements)
    - Request client feedback on Remote Code Load end to end process
  - Both Remote Code Load & IBM SSR onsite options will be available for z17 Firmware Update of MCL Bundles
    - z16 Statement of direction for RCL standard service offering for z17 being delayed until future
    - Highly recommend that clients start using Remote Code Load from the beginning of their z17 installations

Remote Code Load Enhancements

Remote Code Load for IBM Z Firmware functionality enables customers to schedule an upgrade for an IBM Z system remotely via an IBM Z Remote Support Facility (zRSF) *outbound* connection

IBM will work with the client to schedule the date and time of the code load and then IBM will monitor the process to ensure it executes successfully

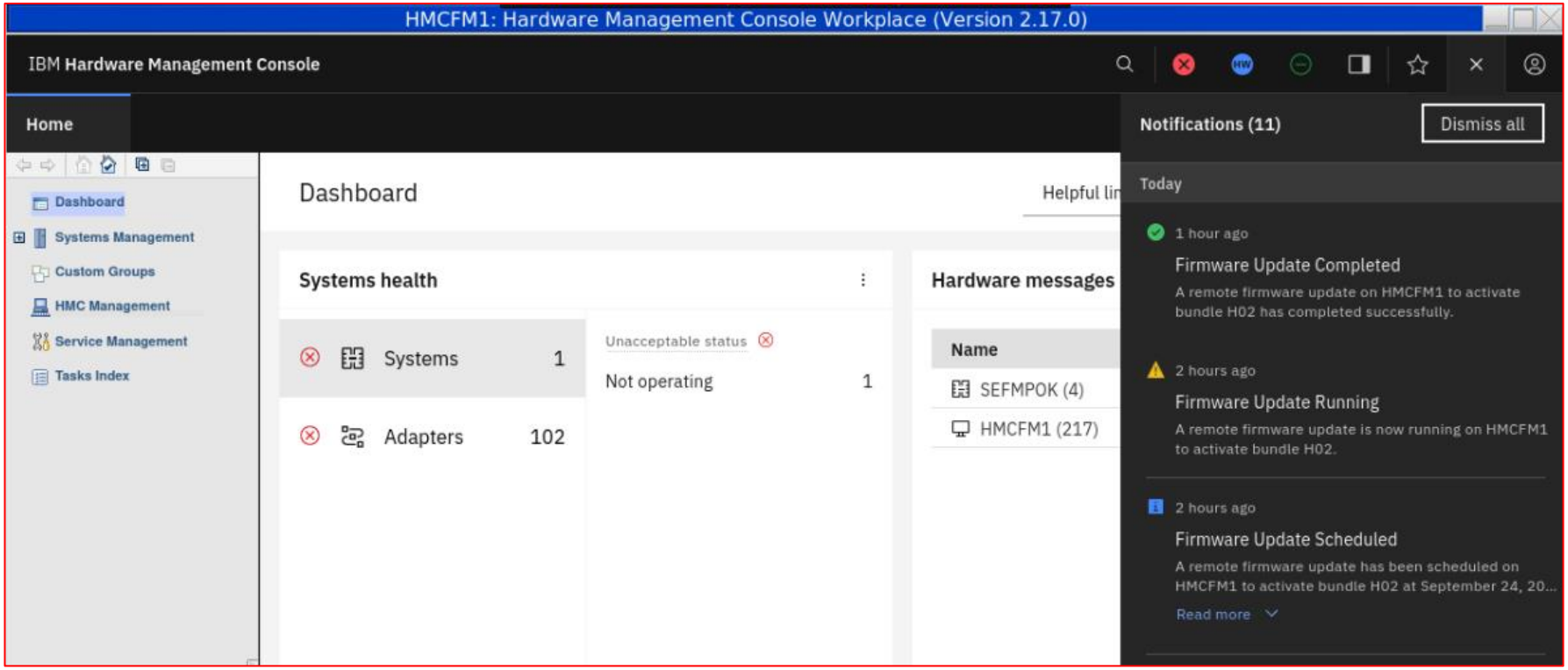


z17 Remote Code Load Enhancements

➢ Notable z17 RCL Enhancements

- HMC RCL Alerts => HMC UI, Email, WebServices API, or IBM HMC Mobile notifications (in addition to IBM Monitoring Emails)
  - RCL Scheduled
  - RCL Running
  - RCL Completed
- Additional RCL Health checks (eg., condition of Alternate SE switchover capability needed for HMA update)
- RCL Health checks available on IBM Resource Link prior to or at scheduling time
  - Will block RCL scheduling rather than RCL scheduling failing after further verification on the HMC
  - Can be aware to address any blocking RCL conditions prior to the need to schedule RCL
- Autopopulate RCL Backup location
- Several other RCL infrastructure enhancements were made which should provide
  - Overall better client scheduling/notification experience
  - Higher quality execution of RCL

z17 HMC RCL Alerts



IBM HMC Mobile 5.0

IBM Z HMC Mobile Field Data

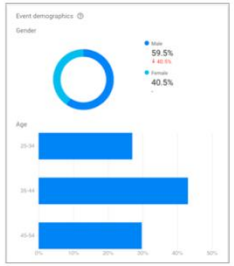
Allows systems administrators to monitor and manage their hardware from anywhere.

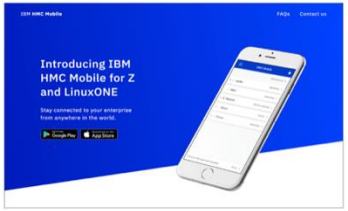
16600 IOS APP INSTALLS

2820 ANDROID APP INSTALLS

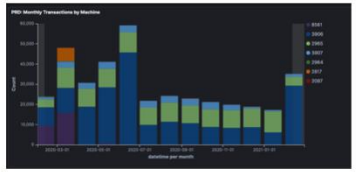
824000 PRODUCT PAGE VIEWS

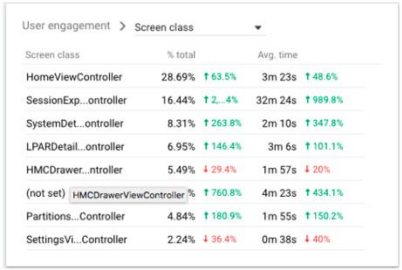
30,308 PUSH NOTIFICATIONS PER MONTH

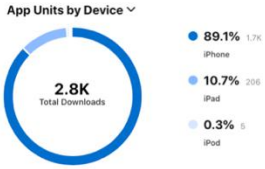




ibm.biz/hmc-mobil







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?

IBM HMC Mobile Release 5.0 — IBM z17 HMC 2.17.0

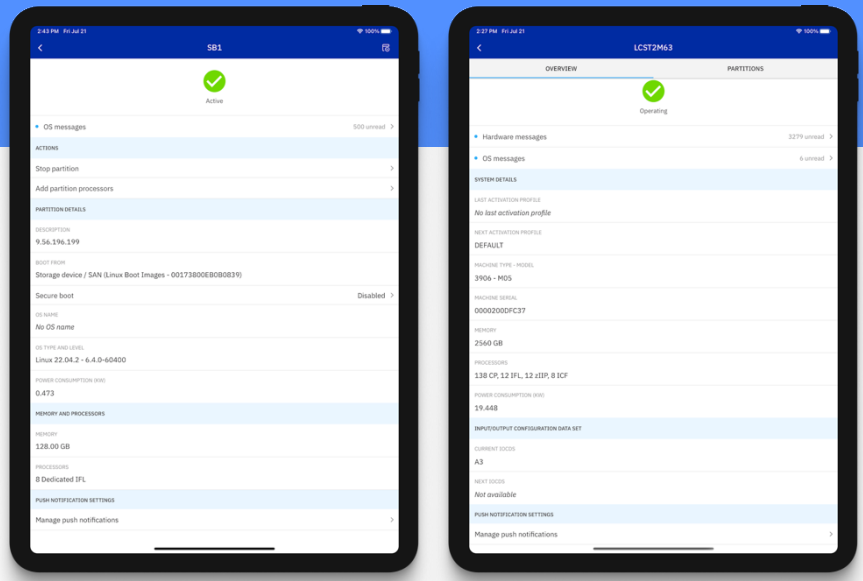
Dual Control request management & enablement for actions
- Activate, Deactivate
- Load, Reset

Alerts and push notifications for Dual Control events

Sustainability metrics (Real-time)

Survey intercept

Sustainability Metrics



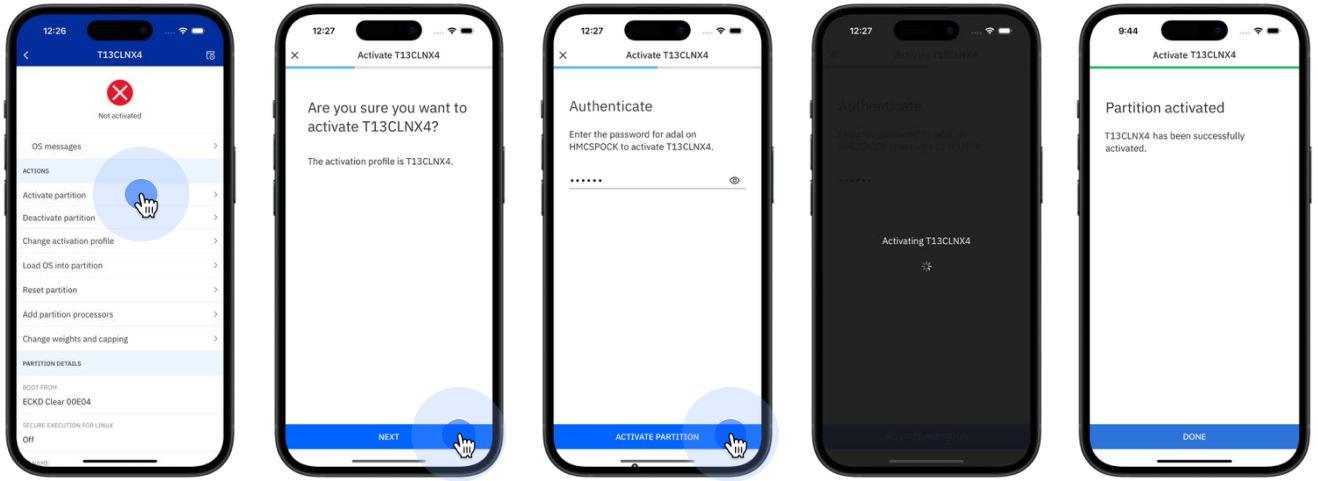
System and Partition
Power Consumption (KW)

- Real-time metrics (HMC Mobile 5.0)
- IBM HMC Mobile 4.2
  - ✤Average over time window
  - ✤Smallest window 30 minutes

Dual Control

Activate

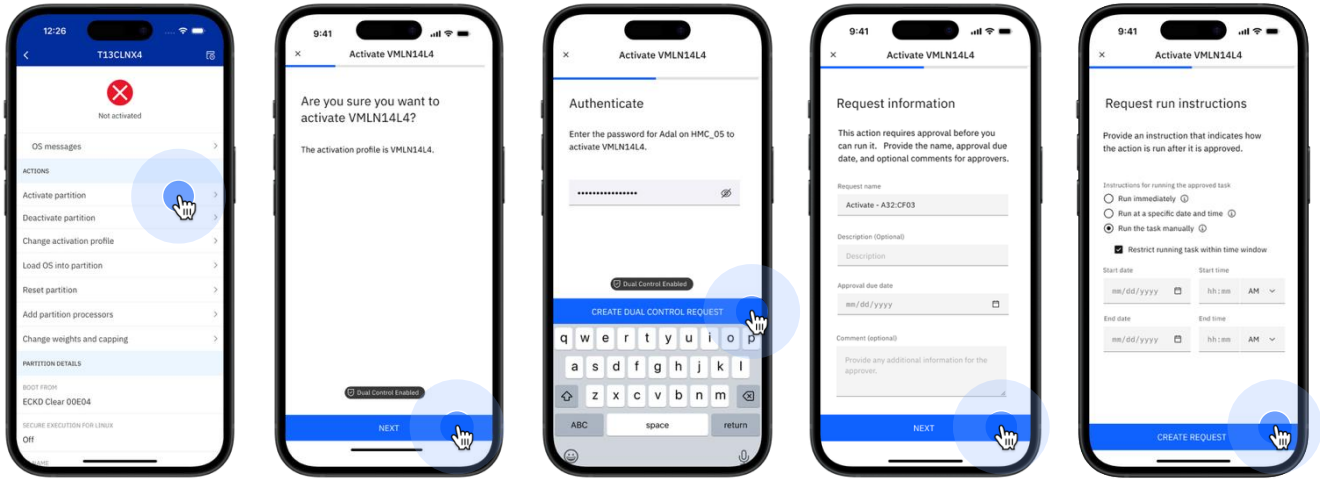
Dual Control
Not Enabled



Dual Control
Create Request

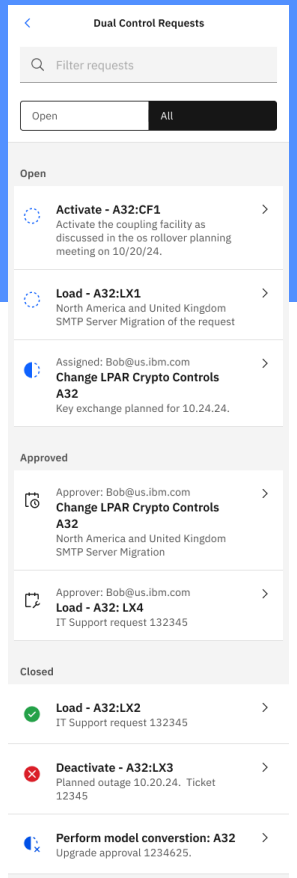
Activate

Dual Control Enabled



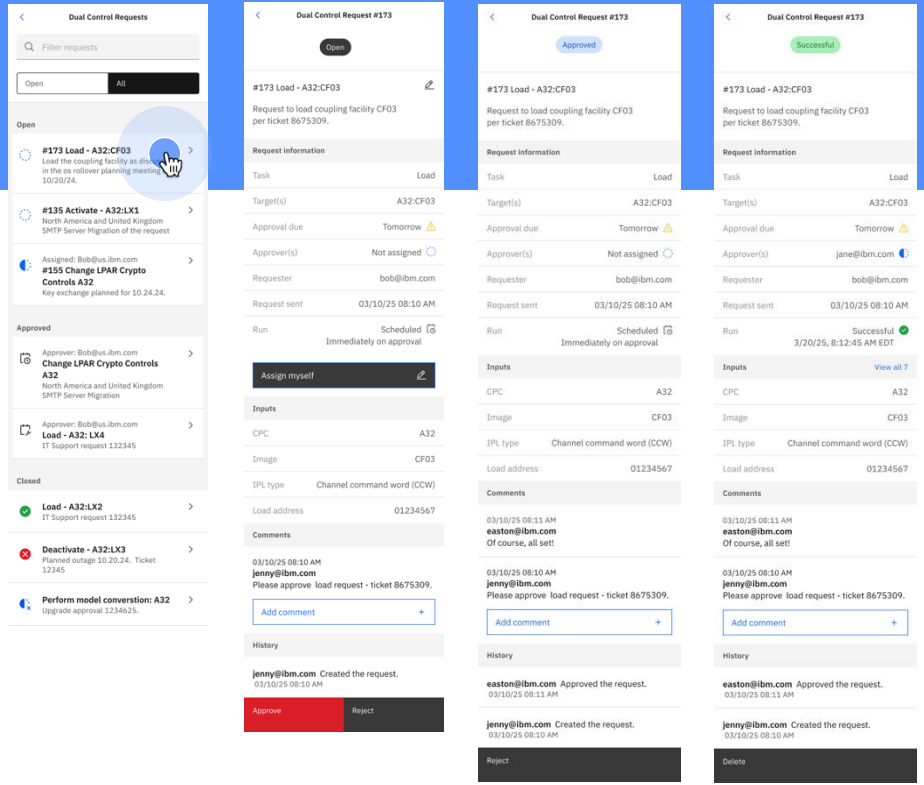
Dual Control Request Management

View and Manage Dual Control Requests



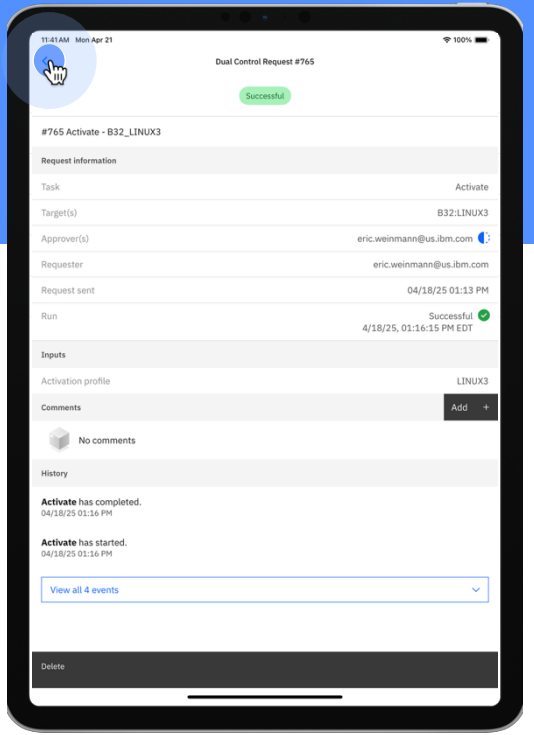
Dual Control Request Details

View, Approve, Reject, Run, Comment



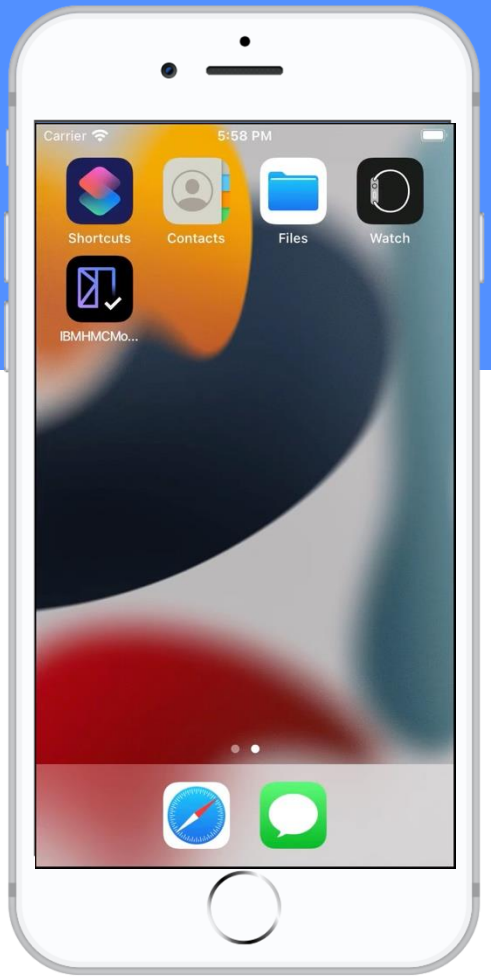
Dual Control Notifications

Created, assigned, approved, rejected, canceled, running, run success



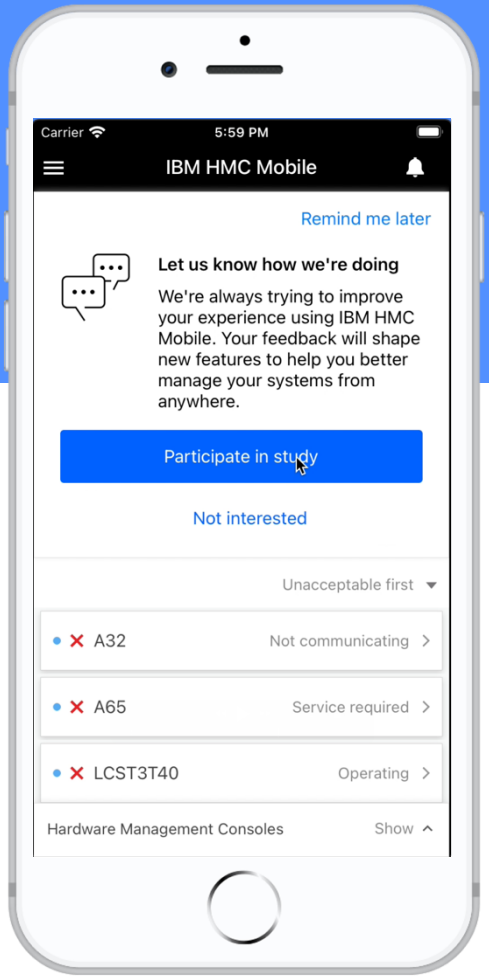
Survey

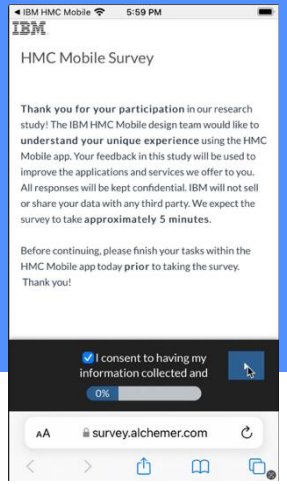
Survey intercept for users

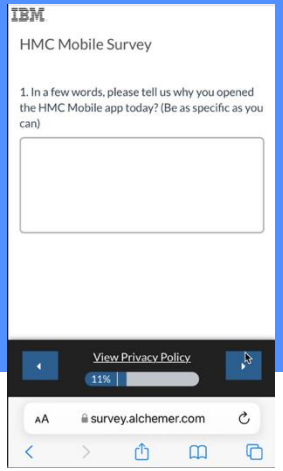


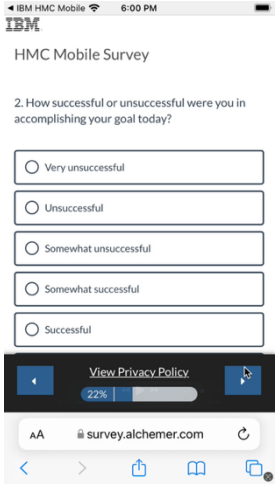
Survey

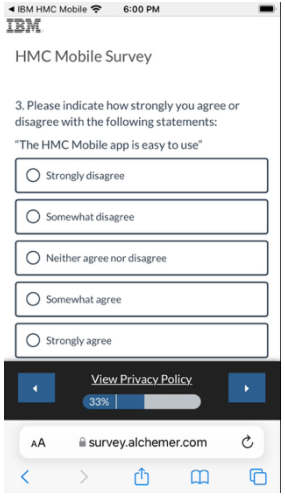
Survey intercept for users





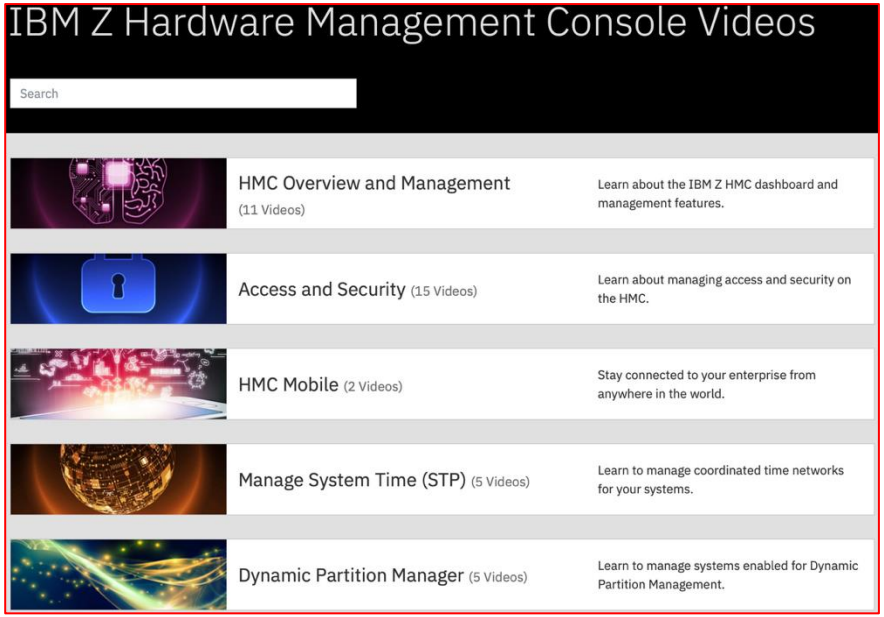






HMC Videos for HMC Content

- Formal Release Documentation on HMC
  - Online Help and IBM Resource Link
- Additional information on HMC via HMC videos
  - Monitor for videos being added to the IBM HMC playlist url: *https://ibm.biz/IBM-Z-HMC*
  - For additional topic areas of interest, notify Brian Valentine (bdvalent@us.ibm.com)



Thank you for your time and consideration....

Jason Stapels
HMC/SE Team

Contact for questions or additional feedback:
Jason Stapels, jstapels@us.ibm.com
Brian Valentine, bdvalent@us.ibm.com

Experience more with IBM

Visit us at the IBM Booth #113

After a full day of technical sessions, take a break with us!

Connect with our experts, snap a photo with the z17 Plexi or the latest Telum II, and get an up-close look at our Spyre Accelerator.

Come back each day for fresh topics and demos at our expert stations.

Think 2026

Join 5000+ senior business and technology leaders who are seizing the AI revolution to unlock unprecedented growth and productivity at **Think 2026**.

Find out more information using the QR code below.

IBM Digital Asset Haven

IBM Digital Asset Haven is the operational backbone for financial institutions and regulated enterprises entering the digital asset economy.

Find out more information using the QR code below.

Trademarks

Please see

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

for copyright and trademark information.

Appendix

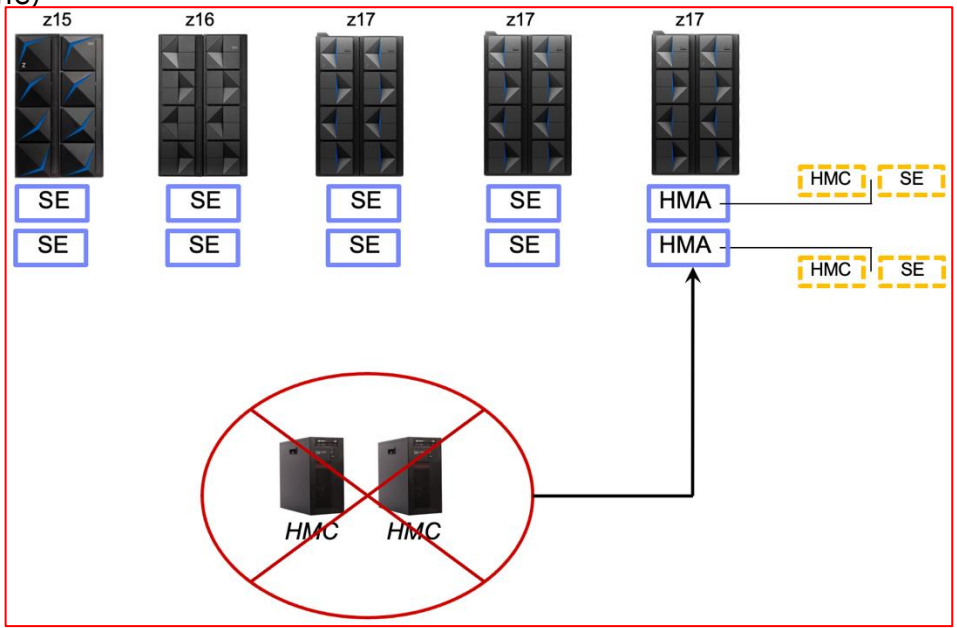
HMC/HMA Additional Info

Method to Order IBM z17 HMC code prior to IBM z17 CPC

- **Reasons to order IBM z17 HMC code version prior to having IBM z17 system**
  - Method to load IBM z17 HMC code on z16/z15 HMA hardware prior to IBM z17 system arrival for installation
  - Obtain access to IBM z17 HMC functionality provided that client systems can be managed by IBM z17 HMC
    - IBM z17 HMC Managed CPCs: z17, z16, z15 (n-2)
    - Generally, 60 to 70 % of IBM z17 HMC new functions are available regardless of CPC level (don't require IBM z17 CPC)
- **No longer a requirement to set Service Status for HMC HMA upgrade (keep visibility to Images) (see previous chart)**
- **Method to order IBM z17 HMC code version (2.17.0) prior to IBM z17 CPC (only if on IBM Z Service):**
  - (Technical Service Program) TSP 428 for IBM z17 HMC code version
    - Client open a CSP (Cognitive Support Platform) case as "Preventative Maintenance (TSP 415)" to initiate Service Rep
    - Supported for HMA (Hardware Management Appliance) HMC on z16/z15 ==> SE (Support Element) remains at z16/z15 code level

New Build HMC ==> HMA (Hardware Management Appliance)

- **IBM z17 only supported HMC hardware is HMA**
- **HMA feature (2 HMCs/CPC) should be limited to at most 2 CPCs (z15 or z16) per data center location**
  - When HMA is ordered, both HMCs must be configured with fixes maintained
- z15 introduced HMA (Hardware Management Appliance)
  - HMC & SE packaged in HMA (redundantly inside Z CPC frame)
  - Eliminates need for managing separate box outside of CPC
  - No real change in general user experience
  - Can be used to manage n-2 legacy systems

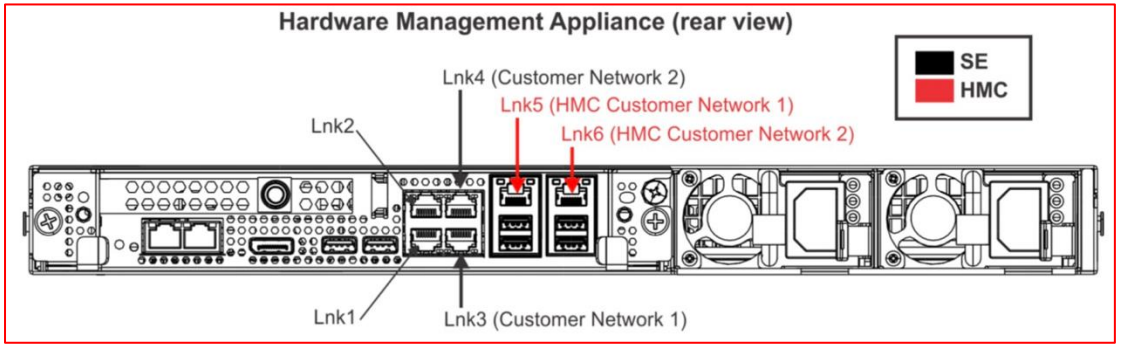


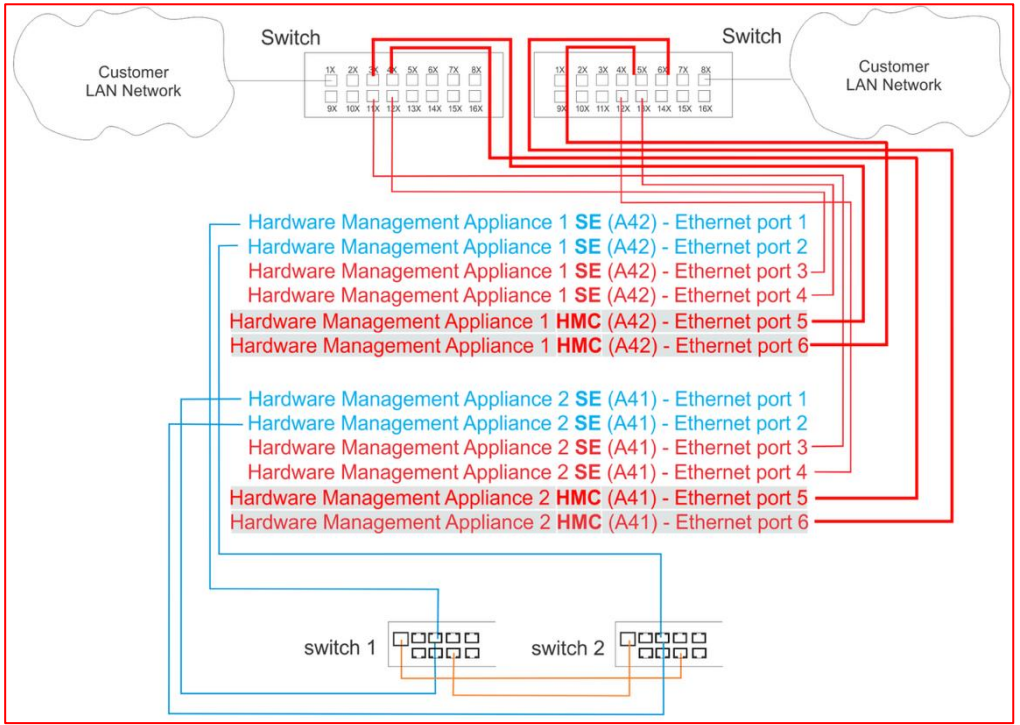
HMA Networking

- Same number of physical networking on HMA HMC/SE as Standalone HMCs & SEs

- HMC/SE Customer Ports
  - HMC: Lnk 5 & 6
  - SE: Lnk 3 & 4
  - Plug one of each into two separate Switches

- Private Internal Service Network from SE to CPC
  - SE: Lnk 1 & 2
  - Plugs into Service Network Switches by SSR





HMA HMC: Console Room Approach & No Access to CPC HMA

➢ Console Room Approach

- Some clients used the HMC as physical device for Console Room access
  - Can create a workstation which is designated for remote browsing access to HMA HMC in the CPC
- Some clients didn't allow remote browsing to HMC
  - On console room workstation used for remote browsing to HMA HMC
    - » Can limit users to only be able to remote browse from the IP address of one or more console room workstations (see next slide)

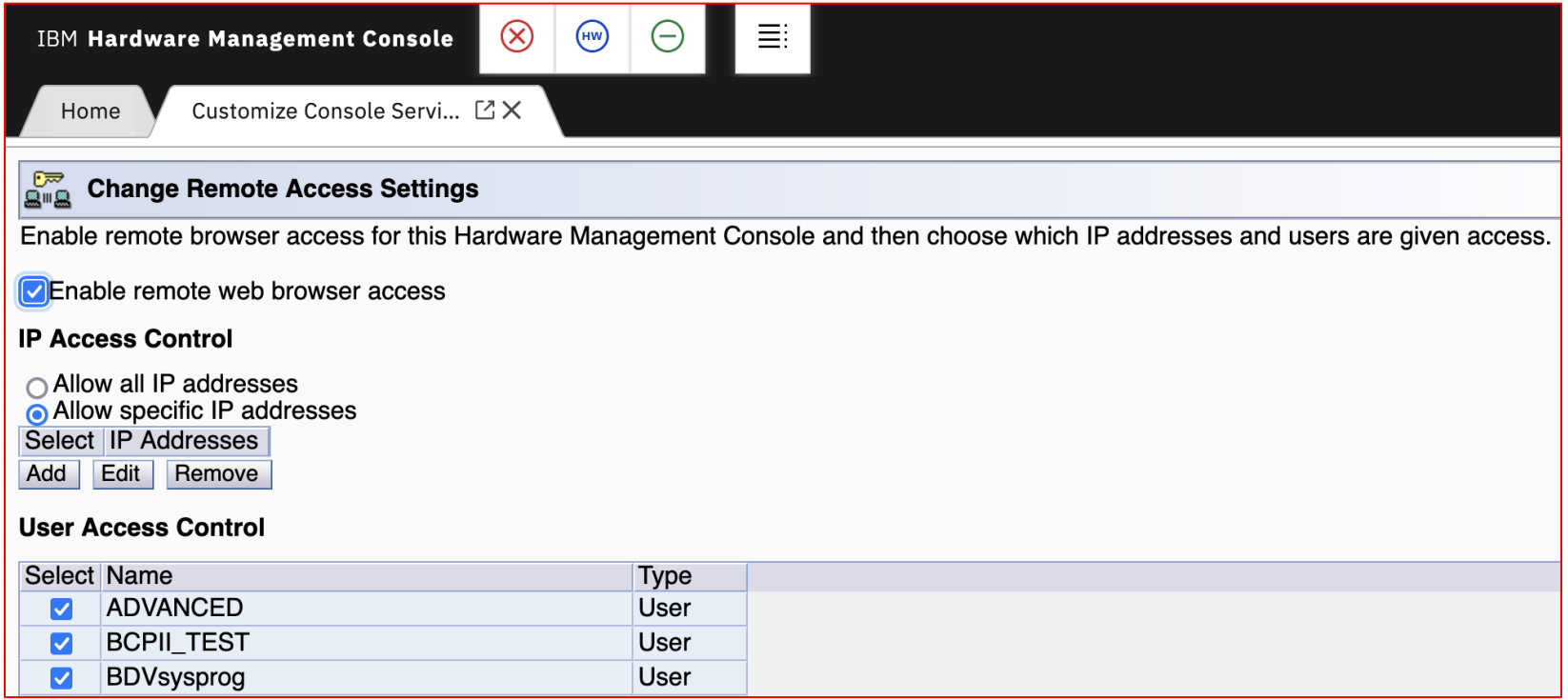
➢ No Access to CPC HMA

- Clients have need for import/export of data for certain HMC tasks => Can't access the HMA HMC inside the CPC on the system floor
  - Some clients used to use USB plugged into Standalone HMC for import/export
    - » Clients should now use SFTP, FTPS, or FTP (only if isolated LAN)
    - » Some newer HMC tasks have support for import/export from remote browsing workstation file system
    - » For z17, adding import/export to remote browsing workstation for all tasks (in addition to USB & 3 FTP options) (see slide 7)

Limit remote browse from the IP addresses of workstations

➢ Customize Console Services => Change Remote Access Settings

- Select Allow specific IP addresses for IP Access Control
  - Add one or more IP addresses for each workstation which you allow HMC Remote Browsing from



Single Sign On Details

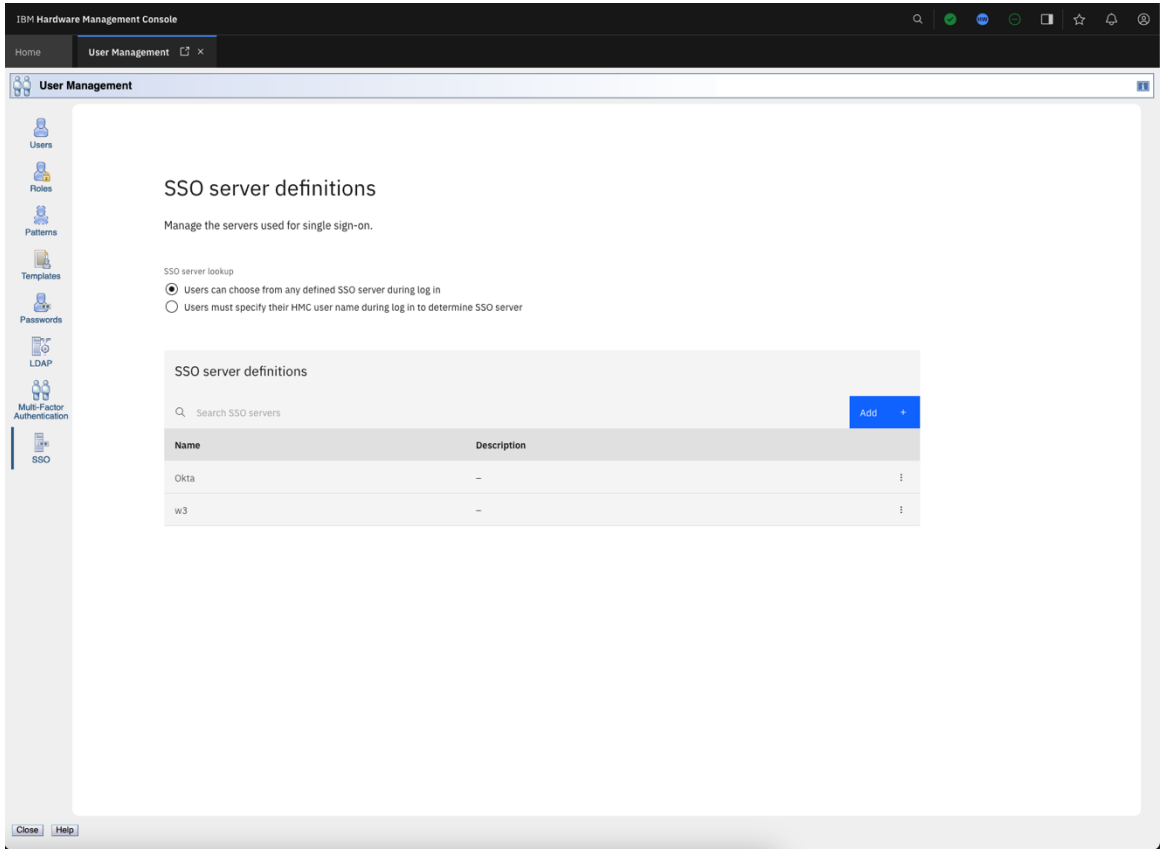
User Management Changes

➢ SSO tab

- SSO server lookup
  - User can choose from any defined SSO server during log in
  - Users must specify their HMC user name during log in to determine SSO server
- SSO server definitions
  - Supports OIDC (OpenID Connect) servers
  - Name
  - Description
  - OIDC URLs
  - Client ID
  - Client secret
  - Log out SSO session when HMC session re-authentication fails
  - Authentication page servers

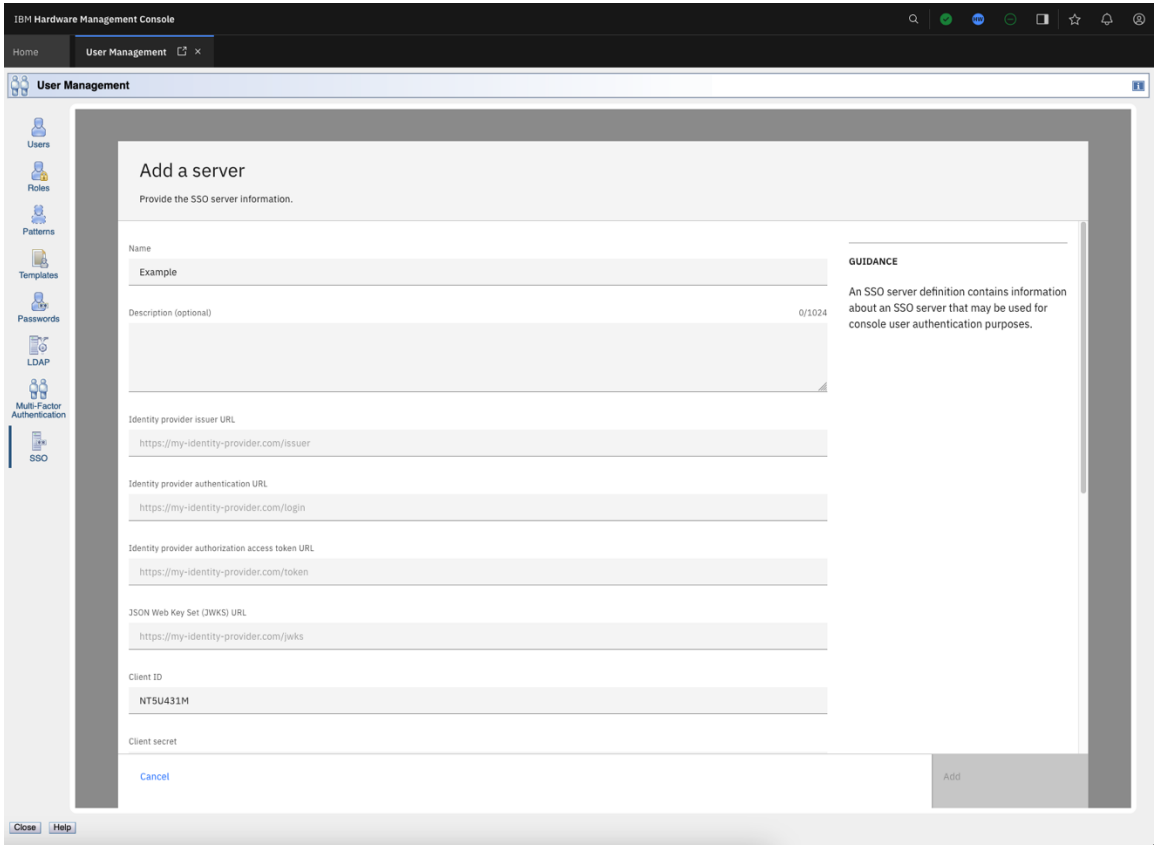
User Management Changes

- SSO tab
  - SSO pushbuttons
  - SSO checkbox



User Management Changes

- SSO tab



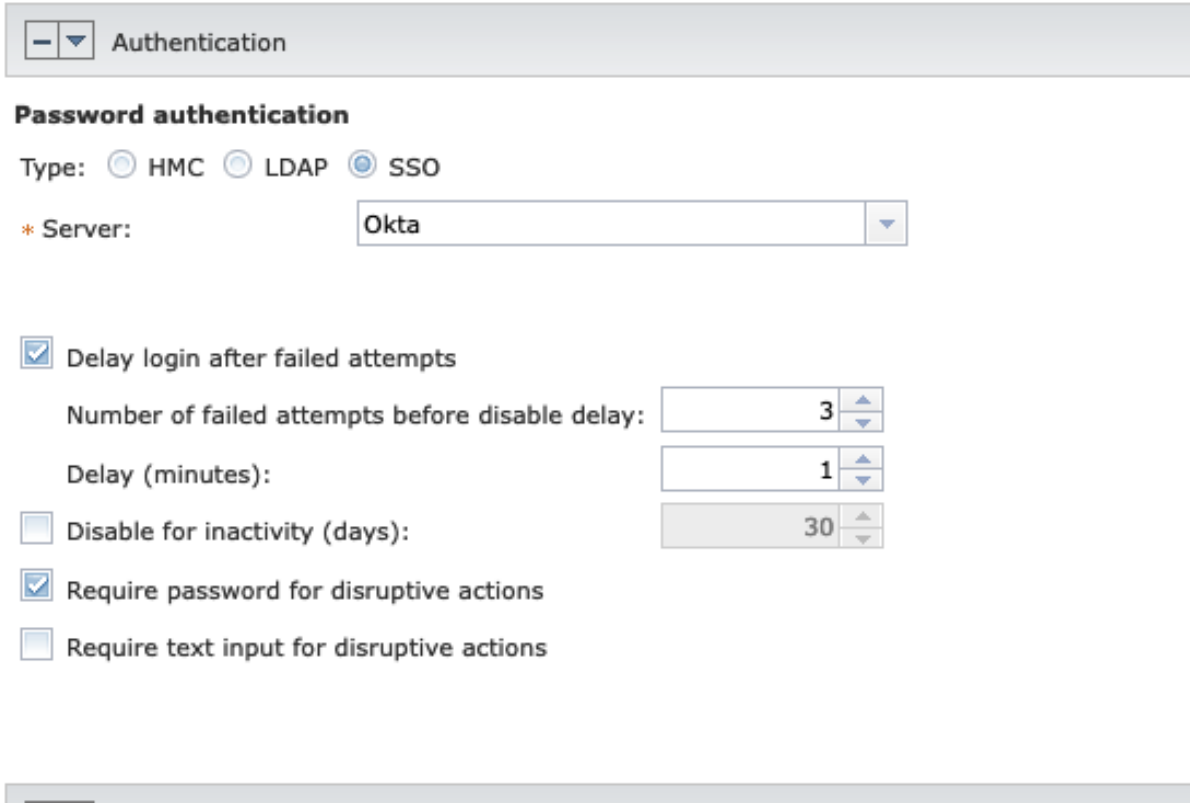
User Management Changes

➢ Users tab

- New authentication type – SSO
- SSO authentication type adds a dropdown for the SSO server definition to be used for authentication.
- SSO authentication type removes Multi-factor authentication (MFA) section as that is handled by the SSO server.

User Management Changes

- User details



User Management Changes

- Templates tab
  - New authentication type option
  - SSO authentication type removes Multi-factor authentication (MFA) section.
  - SSO authentication type removes Enterprise Directory Server (LDAP) selection.

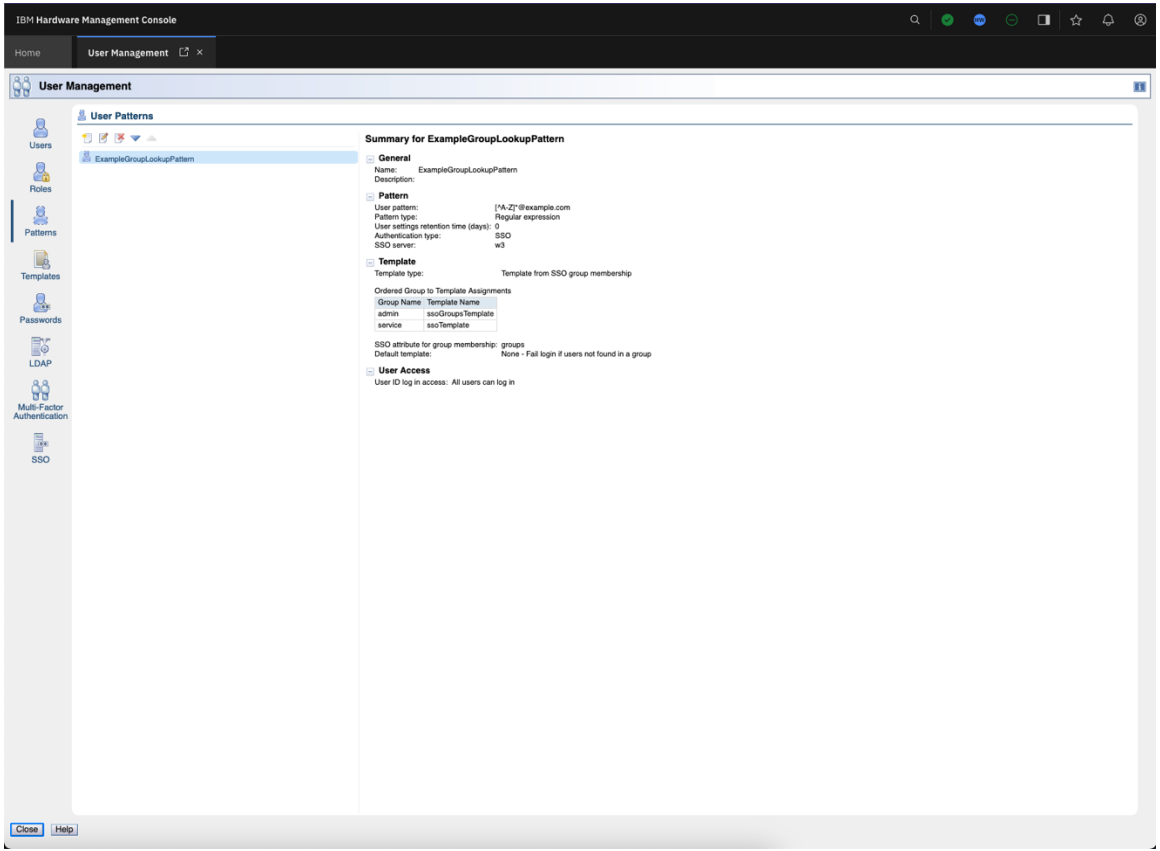
User Management Changes

➢ Patterns tab

- New authentication type option
- SSO authentication type adds a dropdown for the SSO server definition to be used for authentication.
- Template type options
  - Specific template
  - Template from SSO attribute
    - » Template SSO lookup attribute is the attribute that contains the template to use to log in.
  - Template from SSO group membership
    - » SSO attribute for group membership is the attribute that contains the groups the user is a member of to determine the template to use to log in.

User Management Changes

- Patterns tab

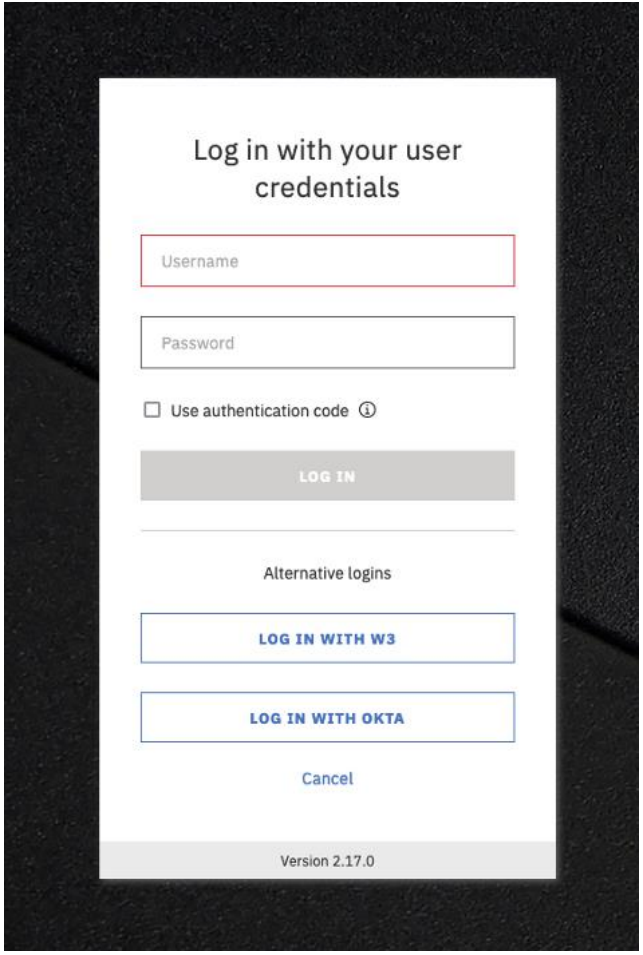


Logon Changes

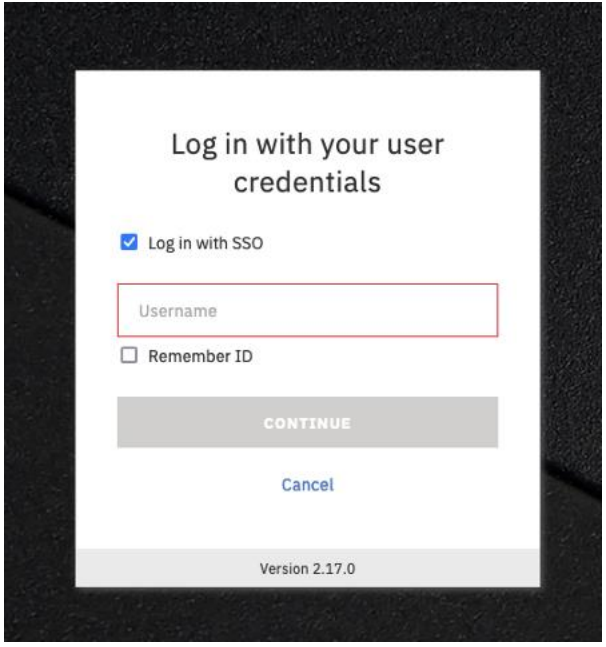
- New buttons to initiate SSO logon flow
  - Log in with <SSO server definition name> button
  - Log in with SSO checkbox
    - User must enter their HMC username to determine which SSO server definition to use
- Redirect to SSO server for authentication
- Redirect back to HMC/SE after successful authentication

Logon Changes

SSO Pushbuttons Logon



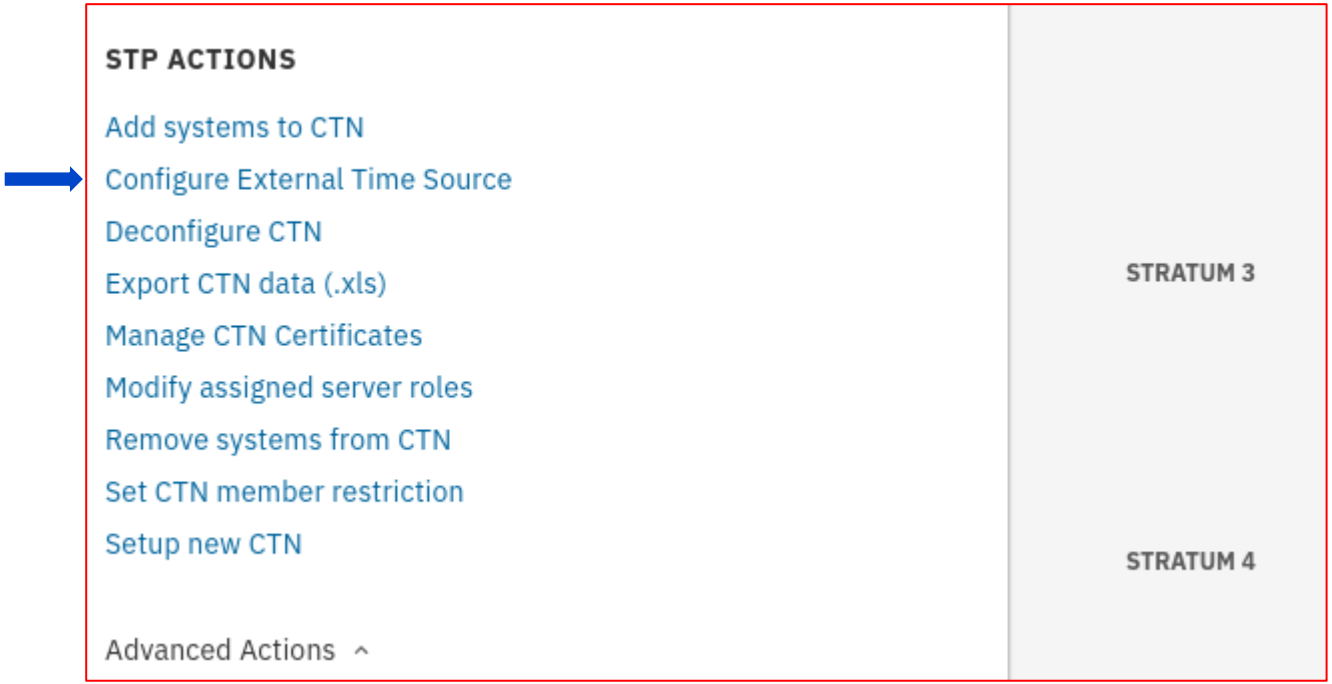
SSO Checkbox Logon



Network Time Security Details

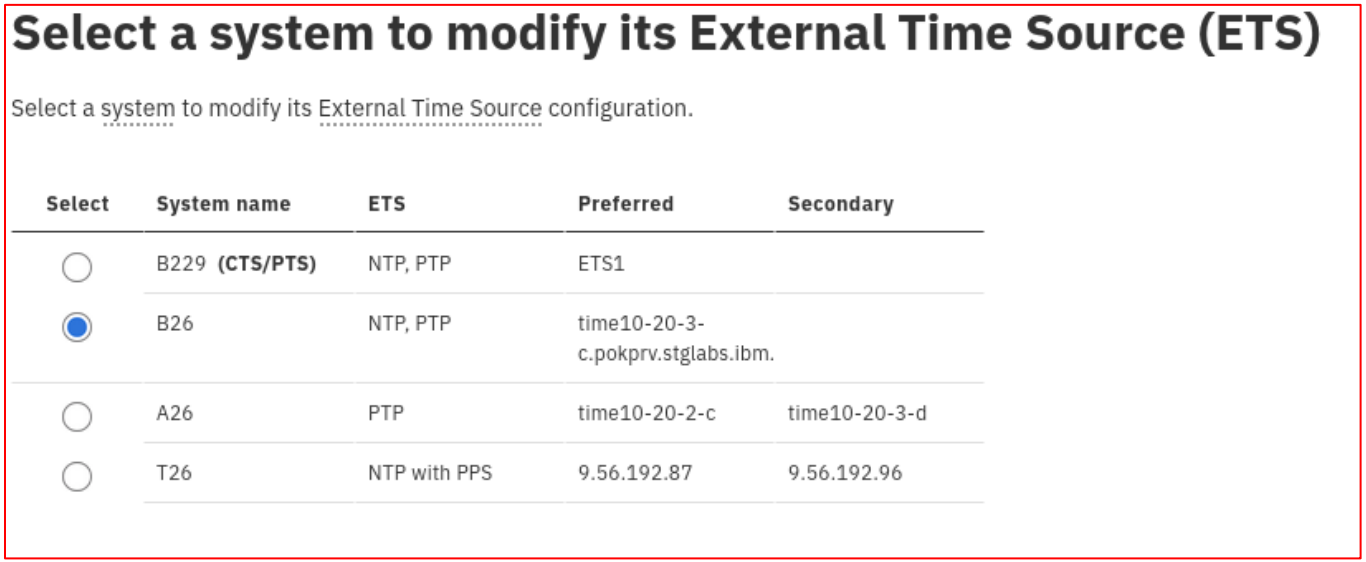
Configure Eternal Time Source

- Updates to Configure ETS STP ACTION used to manage ETS connections to the CPC



Configure ETS - Select a System

- Choose a system to modify the ETS configuration
- All systems listed here are managed by this HMC and are members of the currently selected Coordinated Time Network (CTN)



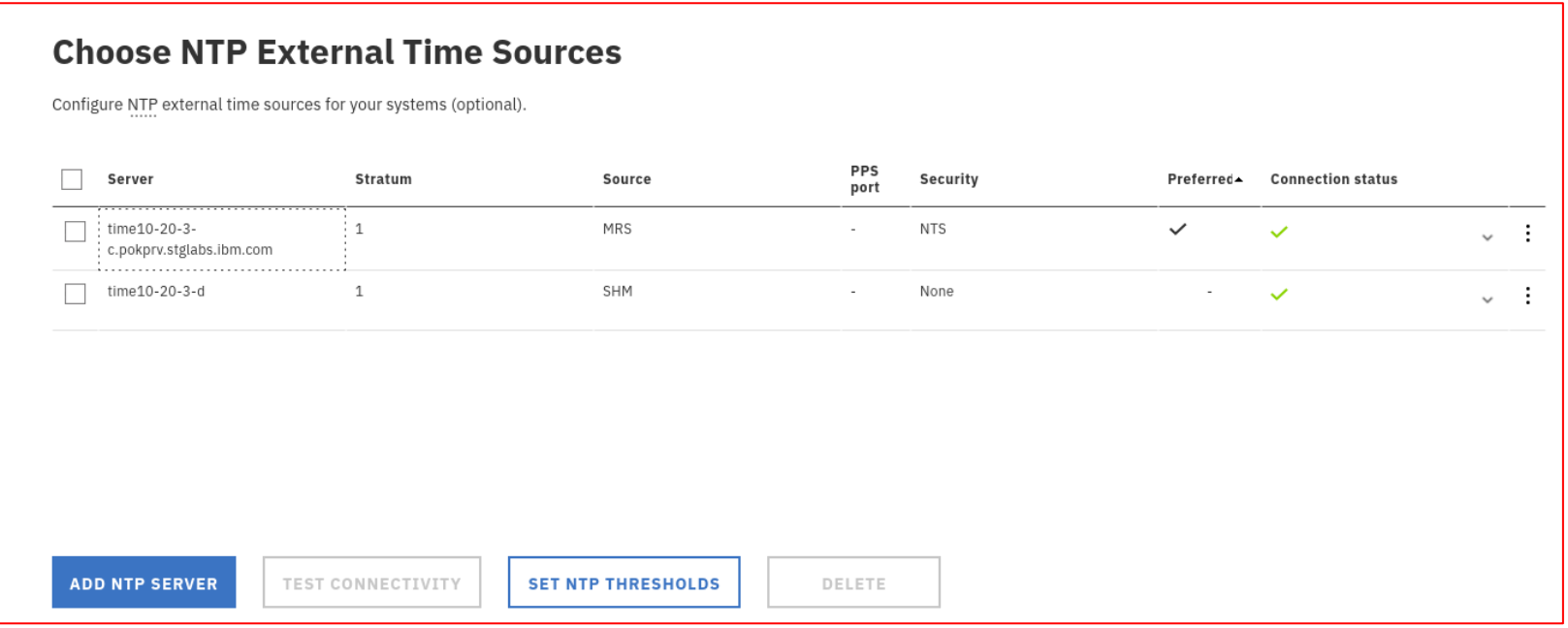
Select a system to modify its External Time Source (ETS)

Select a system to modify its External Time Source configuration.

Select	System name	ETS	Preferred	Secondary
○	B229 **(CTS/PTS)**	NTP, PTP	ETS1	
◉	B26	NTP, PTP	time10-20-3-c.pokprv.stglabs.ibm.	
○	A26	PTP	time10-20-2-c	time10-20-3-d
○	T26	NTP with PPS	9.56.192.87	9.56.192.96

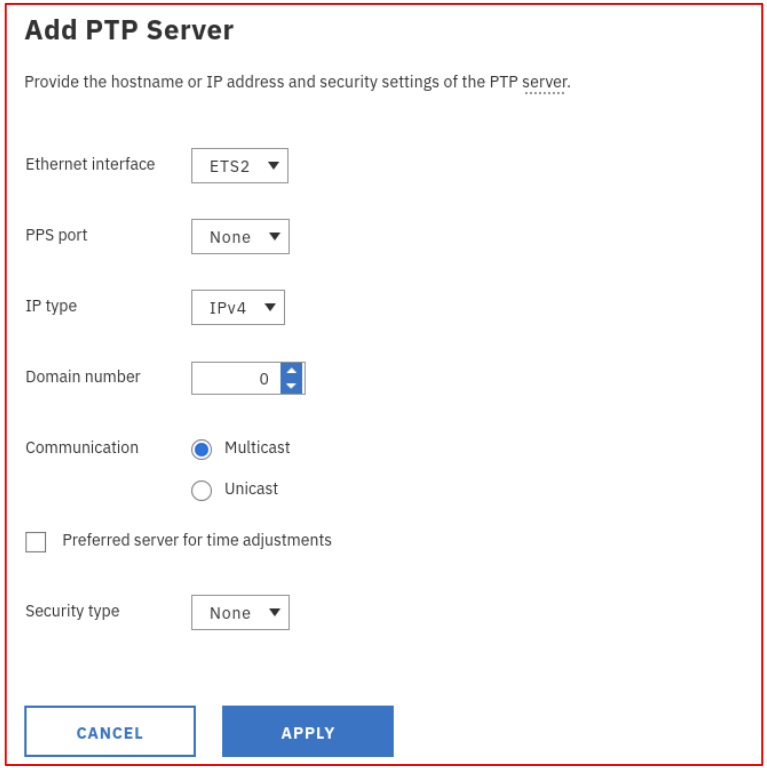
Configure ETS – Choose NTP ETS

- View the currently configured NTP time sources
- Add new or Delete old NTP time sources
- Up to 3 NTP time sources now supported



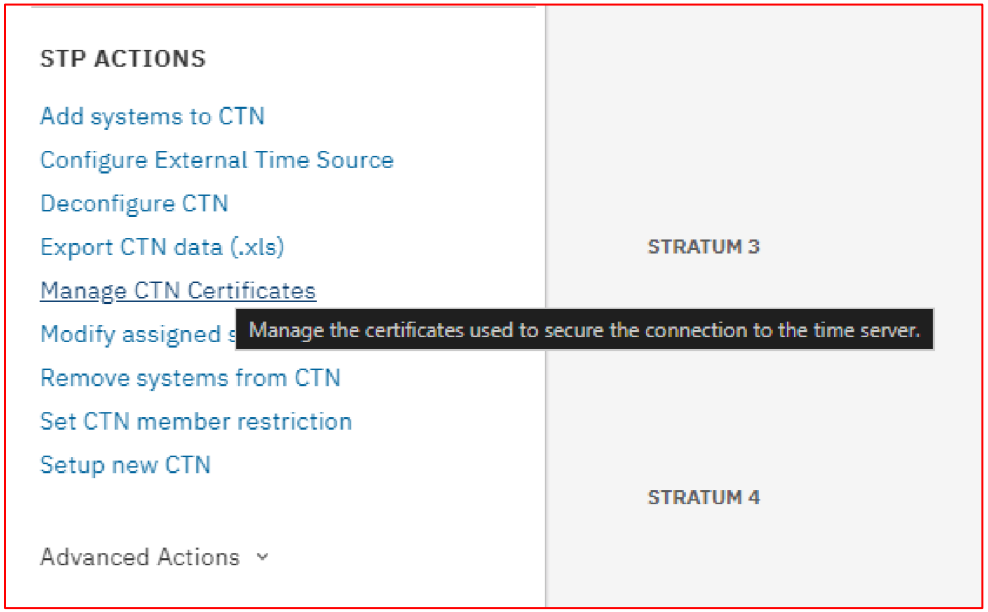
Add PTP Server

- Select the appropriate interface (ETS1 or ETS2)
- If PPS supported select the appropriate port (0 or 1)
- Select IPv4 or IPv6
- Enter the Domain number
- Choose Multicast or Unicast (new support)
- If Unicast enter the appropriate unicast server IPs
- Indicate whether this ETS is preferred
- Enter the selected Security type (currently None supported)



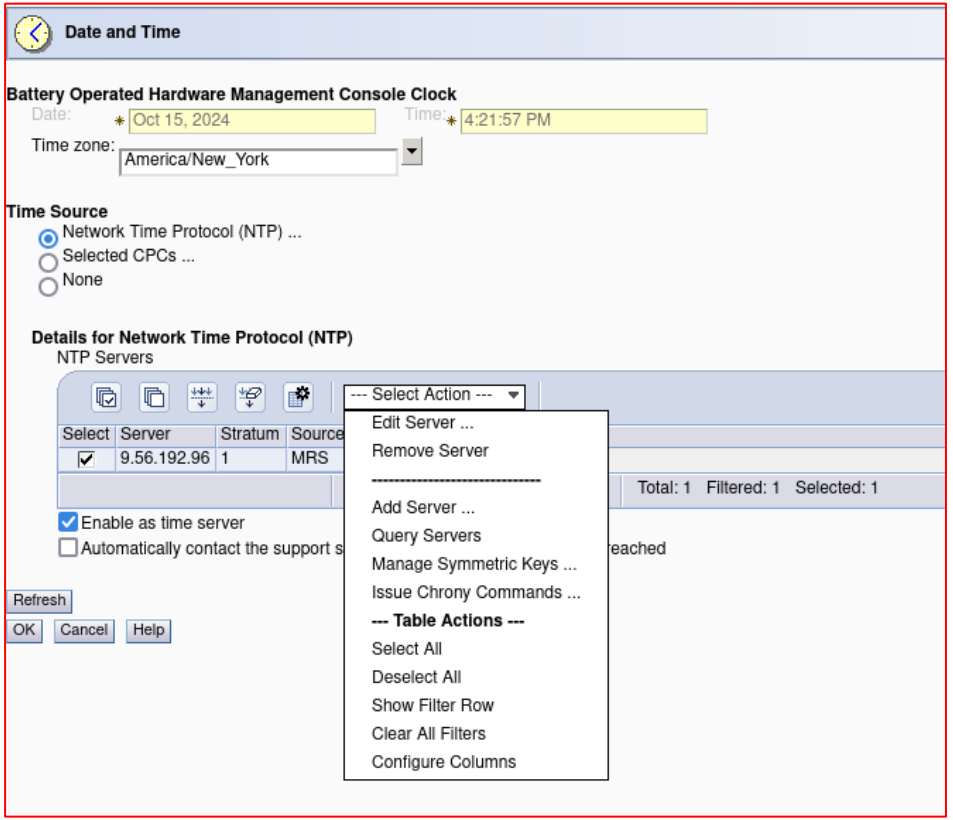
Manage CTN Certificates for NTP Server connections

- New STP ACTION to manage the certificates used to secure the connection between the CPC and the time server
- Supports importing certificates to and removing certificates from all CTN members



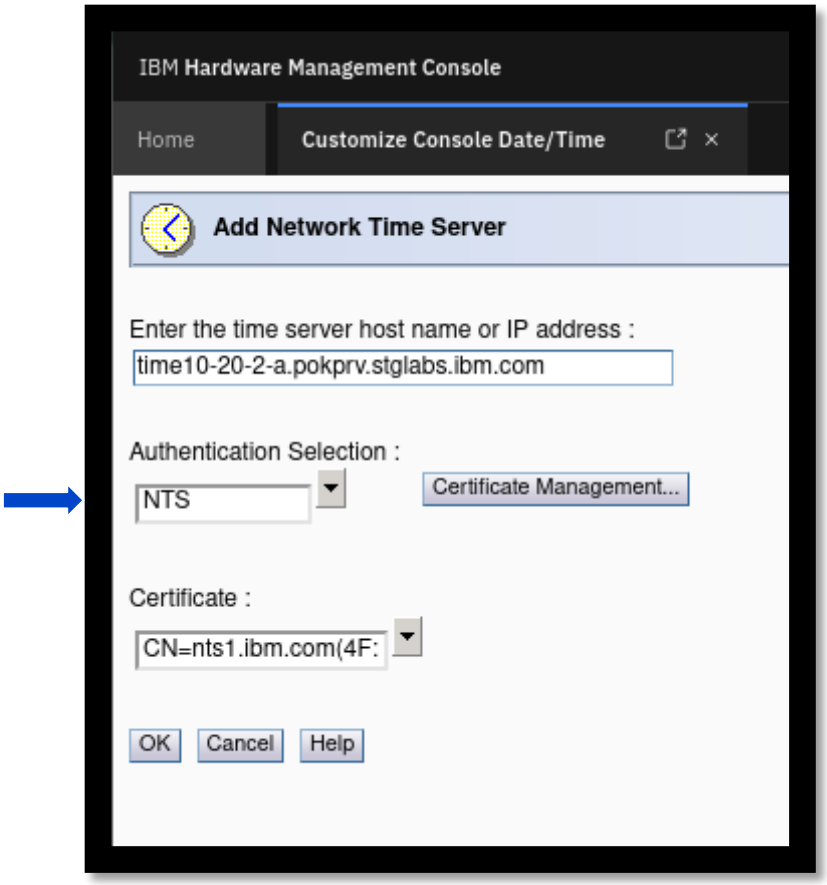
Customize Console Date\Time for HMC

- When adding or editing an NTP server a new option to select NTS security type



Customize Console Date\Time – Add Server

- New option to select NTS security type
- Once selected a drop down of available NTS certificates will be selectable
- Certificates are imported via the Certificate Management task



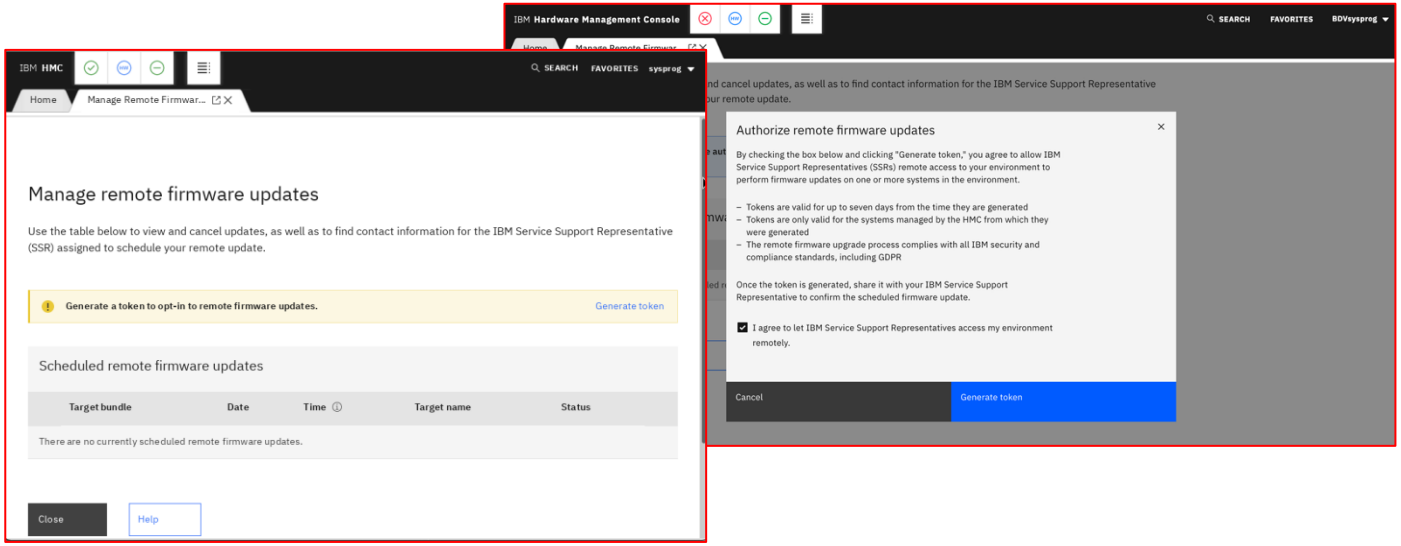
Remote Code Load

Remote Code Load Option for IBM Z Firmware

- Remote Update Controls for Setup and Monitoring **without connection into HMC**
- Utilizes existing zRSF Call Out Connection Infrastructure
  - Means to configure Single Step MCL Scheduled Ops via IBM Resource Link & zRSF response
  - IBM Team Monitors Sales Force Call Home for Intermediate & Completion Status
    - Will be equivalent to same information as if SSR sitting next to HMC
    - When complete, IBM will notify client.
      - Client could start remote testing at that point.
- Requires Opt In Security Configuration by Client & Scheduling on IBM Resource Link
  - Client creates authorization token on HMC & schedules Firmware Update on IBM Resource Link using seeded information for most selections
  - Client has ability to
    - Confirm what FW Updates are scheduled both on IBM Resource Link and HMC
    - Can easily cancel any scheduled FW Update
- 96 % Success Rate => If exception issue encountered, IBM SSR dispatched immediately
  - FFDC (First Failure Data Capture) already complete
  - SSR dispatch time could be up to 2 hours
    - However, should arrive with Next Level of Support actions in hand => goal of concurrent recovery
    - System normally continues to run even if exceptions encountered
- Client Benefit (& IBM) for Migration to Remote Code Update Orchestration
  - Provides ability for both Client/SSR to not be onsite for update process
  - Potential for Client to do acceptance test remotely as well

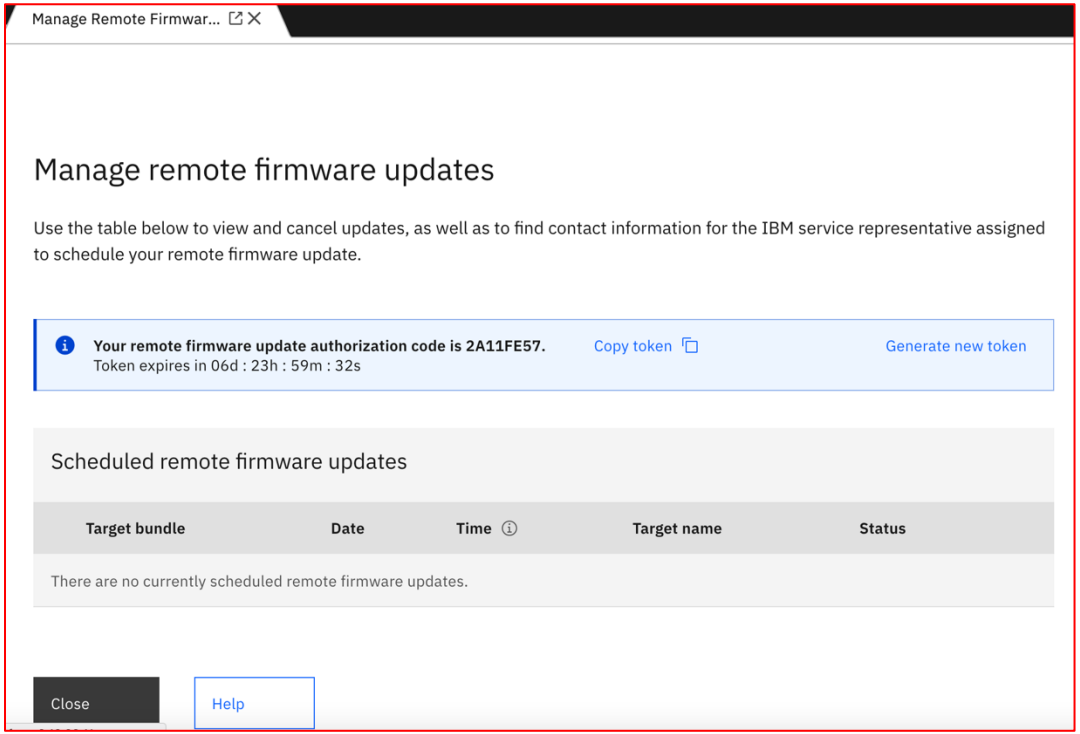
Remote Code Load for IBM Z Firmware – Opt In

- Client makes decisions on execution direction
  - MCL Bundle, HMC or CPC Target (if CPC, must specify HMC for orchestration), date/time
  - When client inputs on IBM Resource Link,
    - will look at mostly seeded data for his/her systems for allowable options
- Client Opts in on HMC to create Authorization Token for scheduling Remote Code Load
  - Select Generate Token on *Manage Remote Firmware Updates* task



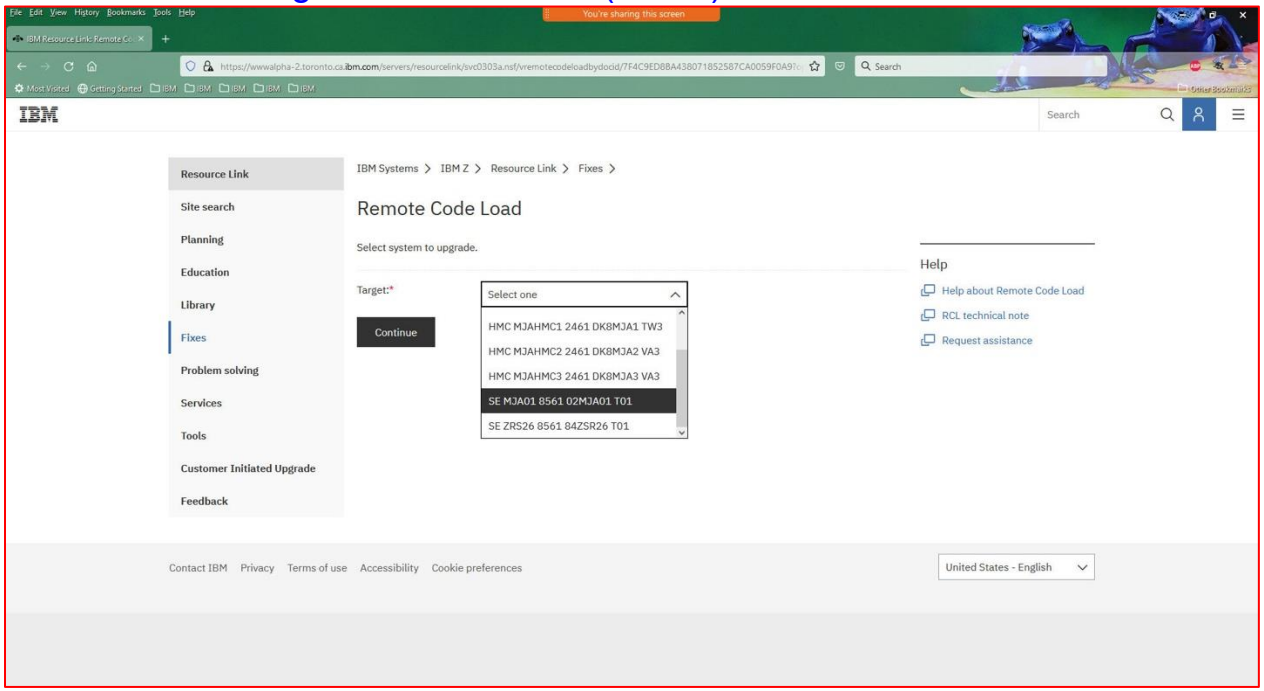
Remote Code Load for IBM Z Firmware – Opt In

- Client Opts in on HMC – create Authorization Token to schedule Remote Code Load
  - Client can use copy button if on same workstation for HMC Browsing/Resource Link Input
    - Expiration: days:hours:minutes:seconds (initial expiration 7 days)



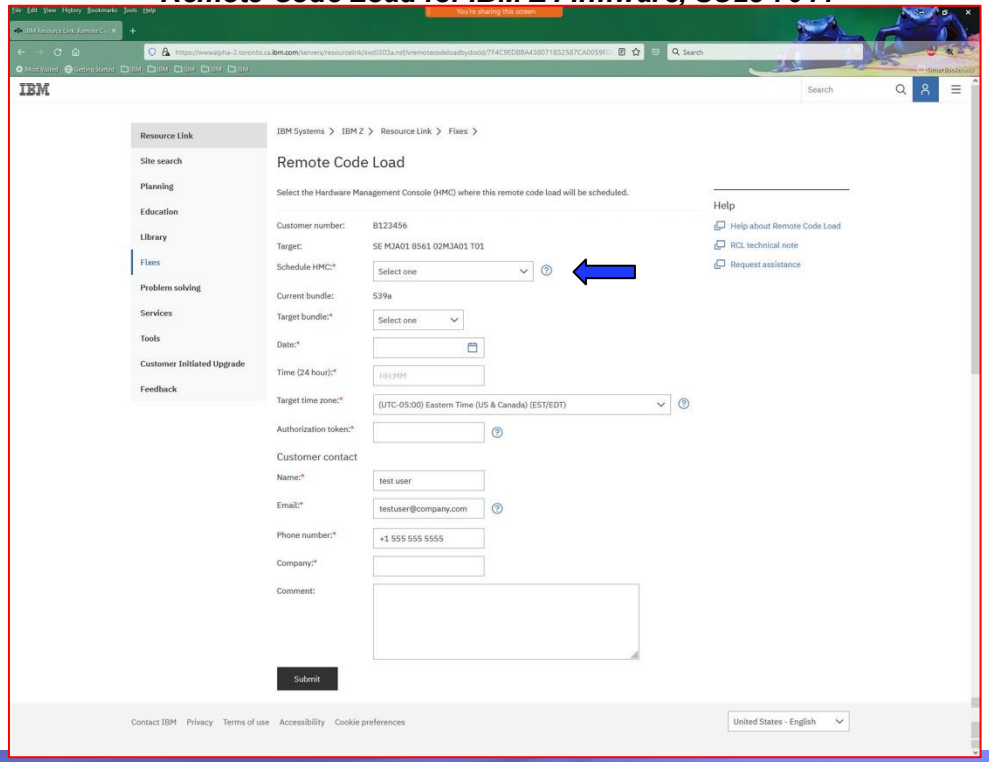
Remote Code Load for IBM Z Firmware – Client Schedules

- Client Schedules Remote Code Load on IBM Resource Link
  - Must be Scheduled 48 hours prior to execution
    - Recommendation will be 7 days prior to allow client & SSR opportunity for confirmation
- Client selects Target from list of SEs (CPCs) or HMCs



Remote Code Load for IBM Z Firmware – Client Schedules

- Client Schedules rest of input field mostly from seeded data options
  - Following publication provides detailed instructions to aid any questions
    - ***Remote Code Load for IBM Z Firmware, SC28-7044***



- *For firmware update of a CPC/SE target, the scheduling/orchestration HMC should be one which is local in the same DataCenter as that targeted CPC/SE.*

z16 Remote Code Load Enhancements

➢ Notable z16 RCL Enhancements

- HMA HMC pairs scheduled as one RCL update managed by Firmware
- Capability to reschedule a Remote Code Load from IBM Resource Link without requiring client to do a HMC RCL Cancel
- Parallel RCL Execution of Multiple HMCs
  - provided there is at least one HMC for zRSF Call Home which is not part of the parallel RCL execution
- Parallel RCL Execution of 2 CPCs
- HMC Data Replication of the Remote Code Load authorization token allowing it to be used on any HMC in the enterprise
- HMC Mobile Enhancements ==> Authorization Token Opt In, View/Cancel Scheduled Updates
- HMC UI RCL In Progress details and RCL Execution History