

IBM z17 HMC (Hardware Management Console) Enhancements

February 26, 2026

*Jason Stapels, Brian Valentine
HMC/SE Development*

SHARE in Orlando

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 \(z17, z16, z15\)](#)

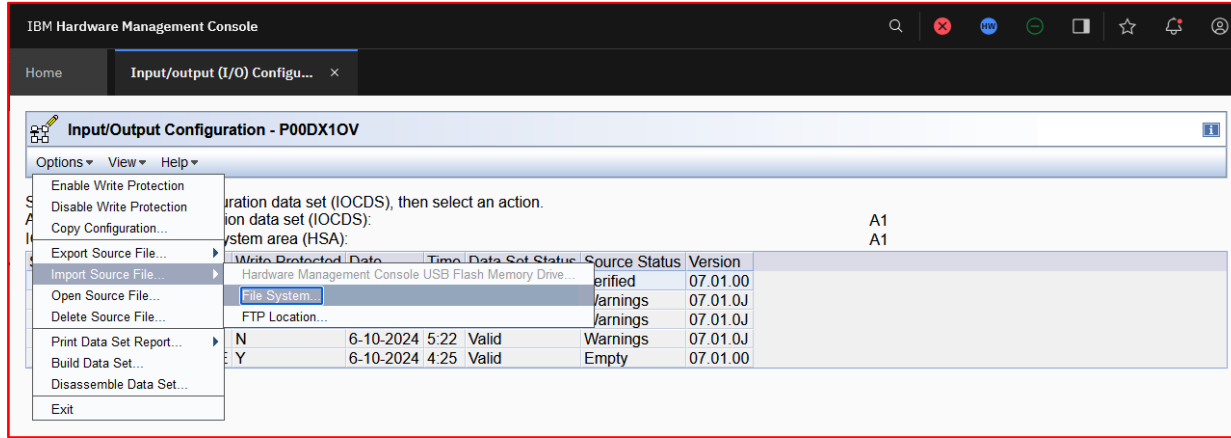
➤ MES available for adding HMA to z17 CPC

- [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](#)

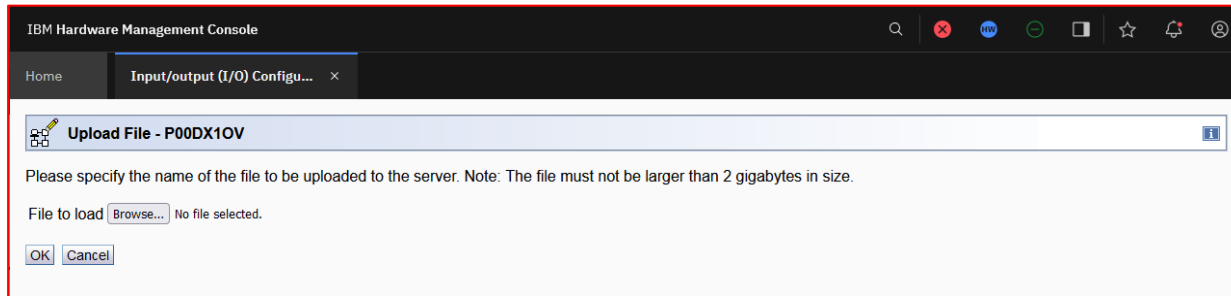
Import/Export Remote File System



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

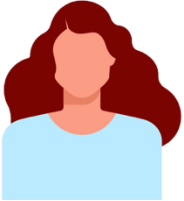
- Run by requester restricted to time window in the future
- Run by requester
 - No time window restriction
- Run immediately
 - Automatically without requester further involvement
- Run on a specific date and time

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)

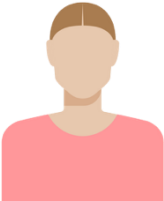
Primary user personas



Adele
Junior system administrator



Easton
Experienced system administrator



Sage
Security administrator

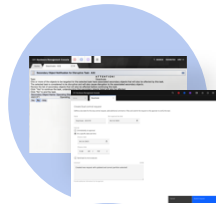


Hardware management



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

IBM Hardware Management Console

Home x User management x **New role** x

New Role

Dual control

An optional security feature that you can enable for specified task and object mappings which will require a second level of verification from an approver before being run.

Enable for tasks and objects

Select the task and object mappings to enable for dual control.

[Add task and object mapping +](#)

Task	Objects by type	Specific objects	Objects by group
No task and object mappings.			

Approver permissions

- _____
- _____
- _____
- _____
- _____

Back Next Finish Cancel Help

Dual control set-up for the deactivate task



Sage selects the Deactivate task to be enabled for dual control

The screenshot shows the IBM Hardware Management Console interface. The main window is titled 'New Role' and has a 'Dual control' section. A modal dialog box titled 'Create a task and object mapping' is open, showing a list of tasks. The 'Deactivate' task is selected. The dialog has tabs for 'Task', 'Objects by type', 'Specific objects', 'Objects by group', and 'Step Optional label'. The 'Task' tab is active, and the list shows the following tasks:

Task	Description
<input type="radio"/> Load	Content
<input checked="" type="radio"/> Deactivate	Content
<input type="radio"/> Activate	Content
<input type="radio"/> Manage systems time	Content
<input type="radio"/> User management	Content

At the bottom of the dialog, there are 'Cancel' and 'Next' buttons. A hand cursor is pointing at the 'Next' button. The background shows the 'New Role' configuration page with a 'Dual control' section and a list of objects by group.

Dual control set-up for the deactivate task



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

IBM Hardware Management Console

Home x User management x **New role** x

New Role

Dual control

Objects by group
Dual control

Create a task and object mapping

Task Objects by type **Specific objects** Objects by group Summary

Select the objects for which dual control will be required when the Deactivate task is launched (optional).

<input type="checkbox"/>	Name	Type	Description	System
<input type="checkbox"/>	A32	Defined CPC	Central processing complex (CPC)	A32
<input checked="" type="checkbox"/>	A32:CF1	LPAR Image	LPAR Image	A32
<input checked="" type="checkbox"/>	A32:CF2	LPAR Image	LPAR Image	A32
<input type="checkbox"/>	A214:FEB28B	LPAR Image	LPAR Image	A212
<input type="checkbox"/>	A214:KATESSE	LPAR Image	LPAR Image	A212

100 1 - 100 of 100 items 1 of 10 pages

Cancel Back Next

Back Next Finish Cancel Help

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.

IBM Hardware Management Console

Home x User management x **New role** x

New Role

Dual control

An optional security feature that you can enable for specified task and object mappings which will require a second level of verification from an approver before being run.

Enable for tasks and objects

Select the task and object mappings to enable for dual control.

[Add task and object mapping](#) +

Task	Objects by type	Specific objects	Objects by group
Deactivate		A32:CF1, A32:CF2	

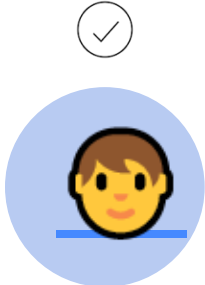
Approver permissions

Select which roles should have dual control approver permissions for the above task and object mappings.

- Anyone with this role other than the requester
- Operator tasks
- Jr system programmer tasks
- System programmer tasks
- Sr system programmer tasks

[Back](#) [Next](#) [Finish](#) [Cancel](#) [Help](#)

Dual Control Task use touch points



Adele

*Selections made in
task and approval
request submitted*

*Easton
Approval/Rejection*

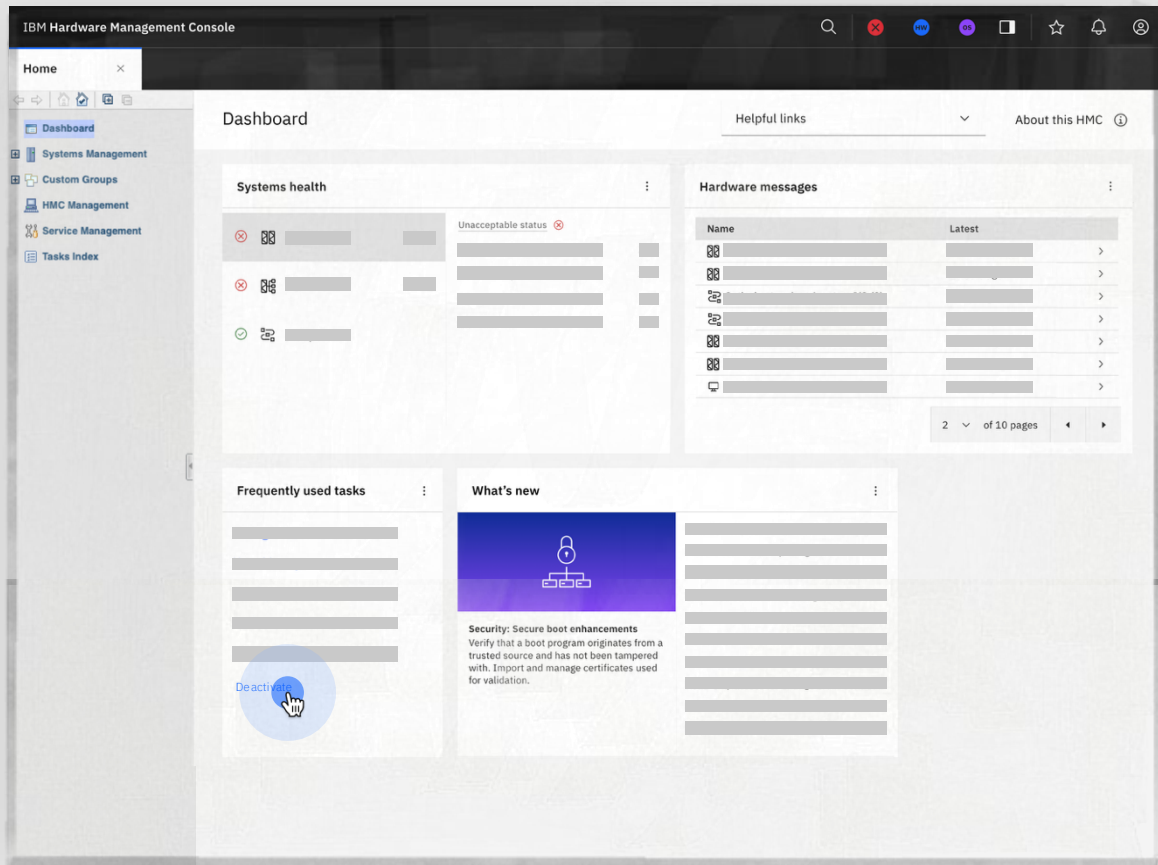
Task is run

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*

The screenshot shows the IBM Hardware Management Console interface. At the top, there's a navigation bar with 'Home' and 'Deactivate - A32:CF1'. Below that, a yellow warning icon is followed by the title 'Disruptive Task Confirmation : Deactivate - A32:CF1'. A blue information bar states 'Dual control enabled This task requires dual control in order to run the action.' with a link to 'Learn more about dual control'. A red attention bar reads 'Attention: The Deactivate task is disruptive.' Below this, a paragraph explains that executing the task may affect objects listed below. A table lists affected objects with columns for System Name, Type, OS Name, Status, Confirmation Text, and Confirmation Status. The table contains one row: A32:CF1, Image, Not operating, and an empty confirmation text box. The text asks 'Do you want to execute the Deactivate task?' and 'Type the password below for user "ada1" then click "Yes".' with a password input field. At the bottom, there are three buttons: 'Cancel', 'Help', and 'Create dual control request'. A hand cursor is pointing at the 'Create dual control request' button, which is highlighted with a blue circle.

System Name	Type	OS Name	Status	Confirmation Text	Confirmation Status
A32:CF1	Image		Not operating		

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

IBM Hardware Management Console

Home User Management x Deactivate - A32:CF1 x

Create dual control request

This task requires approval before you can run it. Create a dual control request that includes an approval due date and instruction that indicates how you want to proceed after receiving an approval. You can also provide a description of the request, and comments for the approvers.

GUIDANCE

After you send the request, reviewers are notified and either approve or deny the request. You can track the status of your request through the Dual Control Management task.

If your request is approved, the task is run according to the instruction that you select.

Request name: Deactivate - A32_CF1

Approval due date: 09/25/2024

Description (optional): 57/1024
Deactivation of the CF1 partition per direction from **BDV**.

Instructions for running the approved task

- Run immediately ⓘ
- Run at a specific date and time ⓘ
- Run the task manually ⓘ

Comment (optional): 81/1024
Please approve this deactivate request as discussed in planning meeting with **BDV**.

Help Cancel Submit request

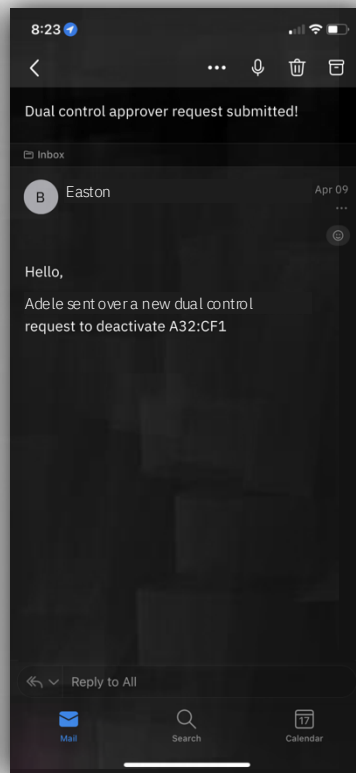
Approver notified of dual control request



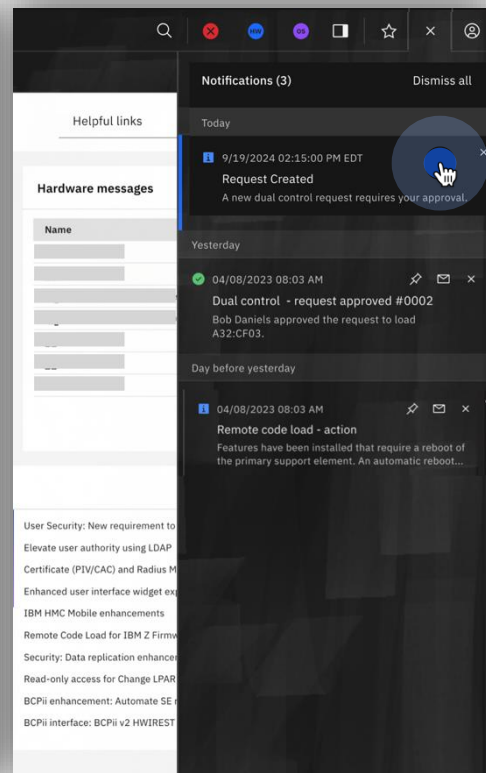
Easton, a dual control approver, is notified of the request via mobile, email, APIs, BCPii, and the notification panel in the HMC



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.

A screenshot of the IBM Hardware Management Console interface. The browser title is "IBM Hardware Management Console". The page shows a request for deactivation of a CF1 partition. A yellow warning banner at the top states: "Disruptive Approval of this request might result in the disruption of partition operations." The request details include: Name: #0152 Deactivate - A32_CF1, Description: Deactivation of the CF1 partition per direction from BDV. The "Request information" section shows: Task: Deactivate, Target(s): CF1, Approval due: 9/25/24, Approver(s): Not assigned, Requester: adal, Request sent: 9/19/24, 2:16:40 PM EDT, Run: Scheduled, Immediately on approval. The "History" section shows: adal created the request. 9/19/24, 2:16:40 PM EDT. The "Comments" section shows: adal commented. 9/19/24, 2:16:28 PM EDT. Please approve this deactivate request as discussed in planning meeting with BDV. At the bottom right, there are three buttons: "Help", "Reject", and "Approve". A mouse cursor is hovering over the "Reject" button.

Approver rejects the request



Easton writes a comment to explain why it was rejected

A screenshot of the IBM Hardware Management Console interface. The main window displays a request for 'Deactivate' with target 'CF1' and an approval due date of '9/25/24'. A 'Reject request' dialog box is open in the foreground, containing a text area with the comment: 'The partition you selected is incorrect! It should be CF2 on A32.' The 'Reject' button in the dialog is highlighted with a blue circle and a hand cursor. The background interface includes a navigation bar, a warning message about disruptive operations, and a 'Request information' section with fields for task, target, approval due, and requester.

Notified of rejection,
launches the dual control
management task



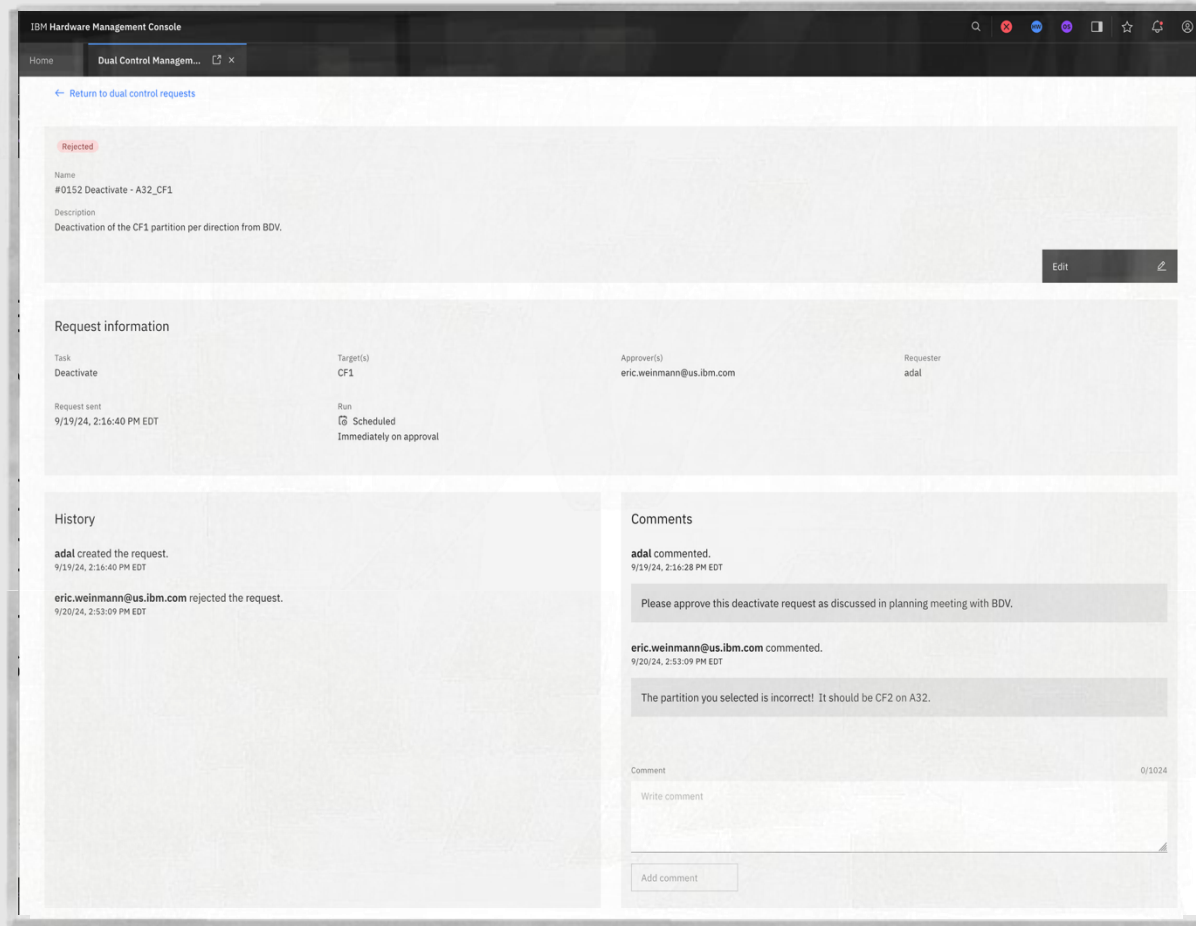
Adele is notified that her request has been rejected so she launches the dual control management task and clicks into request card to view details

The screenshot shows a web application interface titled "Dual Control Management". At the top, there is a search bar labeled "Search requests". Below it, the interface is divided into three columns: "Open" (1 request), "Approved" (1 request), and "Closed" (80 requests). Each column contains a request card. The "Open" column shows a card for "#0151 Activate - A32_CF2" with details for requester 'adal', request sent on 9/19/24, and approval due on 9/25/24. The "Approved" column shows a card for "#0112 Load - B32_Z05" with details for requester 'dcuser1', request sent on 9/5/24, and a status of "Approved". The "Closed" column shows a card for "#0152 Deactivate - A32_CF1" with details for requester 'adal', request sent on 9/19/24, and a status of "Rejected". A blue circle with a hand cursor icon is overlaid on the "Rejected" card, indicating it is being clicked. In the top right corner, a notification pop-up is displayed with the title "Request Rejected" and the message: "Dual control request, 'Deactivate - A32:CF1', has been rejected by easton." The pop-up also shows the date and time: "9/19/2024 02:16:40 PM EDT".

Realizing mistake

Oh no!

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



The screenshot displays the IBM Hardware Management Console interface. At the top, the browser tab is titled "Dual Control Managem...". A navigation link "Return to dual control requests" is visible. The main content area shows a "Rejected" request with the following details:

- Name:** #0152 Deactivate - A32_CF1
- Description:** Deactivation of the CF1 partition per direction from BDV.

An "Edit" button is located in the top right corner of the request details section.

The "Request information" section contains a table with the following data:

Task	Target(s)	Approver(s)	Requester
Deactivate	CF1	eric.weinmann@us.ibm.com	adal

Below the table, the "Request sent" date is 9/19/24, 2:16:40 PM EDT, and the "Run" status is "Scheduled Immediately on approval".

The "History" section shows two entries:

- adal created the request. 9/19/24, 2:16:40 PM EDT
- eric.weinmann@us.ibm.com rejected the request. 9/20/24, 2:53:09 PM EDT

The "Comments" section shows two comments:

- adal commented. 9/19/24, 2:16:28 PM EDT: Please approve this deactivate request as discussed in planning meeting with BDV.
- eric.weinmann@us.ibm.com commented. 9/20/24, 2:53:09 PM EDT: The partition you selected is incorrect! It should be CF2 on A32.

At the bottom right, there is a "Comment" field with a "Write comment" placeholder and an "Add comment" button. The character count "0/1024" is displayed next to the field.

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



IBM Hardware Management Console

Home Activate - A32:CF2

Create dual control request

This task requires approval before you can run it. Create a dual control request that includes an approval due date and instruction that indicates how you want to proceed after receiving an approval. You can also provide a description of the request, and comments for the approvers.

Request name Approval due date

Activate - A32_CF2 09/25/2024

Description (optional) 57/1024

Deactivation of the CF2 partition per direction from BDV.

Instructions for running the approved task

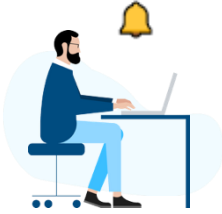
- Run immediately ⓘ
- Run at a specific date and time ⓘ
- Run the task manually ⓘ

Comment (optional) 84/1024

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

Help Cancel **Submit request**

Approver is notified of the new request



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

IBM Hardware Management Console

Home Dual Control Managem... x

← Return to dual control requests

! Disruptive Approval of this request might result in the disruption of partition operations.

Name
#0151 Activate - A32_CF2

Description
Deactivation of the CF2 partition per direction from BDV.

Request information

Task Activate	Target(s) CF2	Approval due 9/25/24	Approver(s) <input type="radio"/> Not assigned
Requester adal	Request sent 9/19/24, 2:12:48 PM EDT	Run <input checked="" type="checkbox"/> Scheduled Immediately on approval	Assign myself +

History

adal created the request.
9/19/24, 2:12:48 PM EDT

Comments

adal commented.
9/19/24, 2:12:47 PM EDT

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

adal commented.
9/23/24, 12:14:00 PM EDT

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

Comment

Write comment

Help Reject **Approve**

Notifications (3) Dismiss all

Today

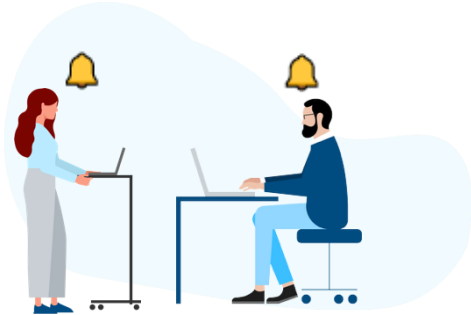
9/19/2024 02:15:00 PM EDT

Request Created

A new dual control request requires your approval.

016024

Deactivate is run and both Adele and Easton are notified



The screenshot displays the IBM Hardware Management Console (HMC) interface. The main dashboard includes the following sections:

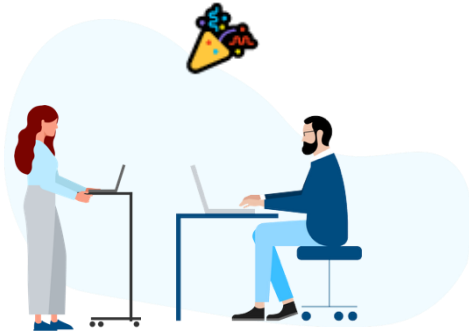
- Systems health:** A table showing the status of various system components.

Component	Status	Count
Systems	Unacceptable status	630
Partitions	No power	300
Partitions	Service required	300
Partitions	Communications not active	20
Adapters	Service	10
- Hardware messages:** A list of messages with columns for Name and details.

Name	Details
S202B (12)	
SETR70 (2)	
Optical network and syst	
Fibre channel network (1	
R31 (1)	
S15 (4)	
HMCL (1)	
- Frequently used tasks:** A list of tasks including Change Password, User Management, Configure Data Replication, Activate, Archive Security Logs, and Load.
- What's new:** A section with a lock icon and text about Security: Secure boot enhancements, stating: "Verify that a boot program originates from a trusted source and has not been tampered with. Import and manage certificates used for validation."

On the right side, a **Notifications (4)** panel is open, showing a "Request Run Successful" notification for "Deactivate - A32-CF2" completed successfully, and a "Request Running" notification for "Deactivate - A32-CF2" started running. A mouse cursor is pointing at the notification.

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.

Enable for tasks and objects

Select the task and object mappings to enable for dual control.

			Add task and object mapping +
Task	Objects by type	Specific objects	Objects by group
Load		A32:LPAR1, A32:LPAR2	

Approver permissions

Select which roles should have dual control approver permissions for the above task and object mappings.

- Anyone with this role other than the requester
- Operator tasks
- Jr system programmer tasks
- System programmer tasks
- Sr system programmer tasks

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

IBM Hardware Management Console

Home Load - A32:CF2

Create dual control request

The task you have launched requires dual control and will need approval prior to execution. Please define an approval due date and when/how the request should execute if it is approved. You may also add a description or comment to provide additional information to the reviewers.

Request name: Load - A32:CF2

Approval due date: 09/23/2024

Description (optional): 0/1024

Instructions for running the approved task

- Run immediately
- Run at a specific date and time
- Run the task manually

Restrict running task within time window

Start date: mm/dd/yyyy

Start time: hh:mm AM EDT

End date: mm/dd/yyyy

End time: hh:mm AM EDT

GUIDANCE

After you send the request, reviewers are notified and either approve or deny the request. You can track the status of your request through the dual control management task.

If your request is approved, the task is run according to the instruction that you select.

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.

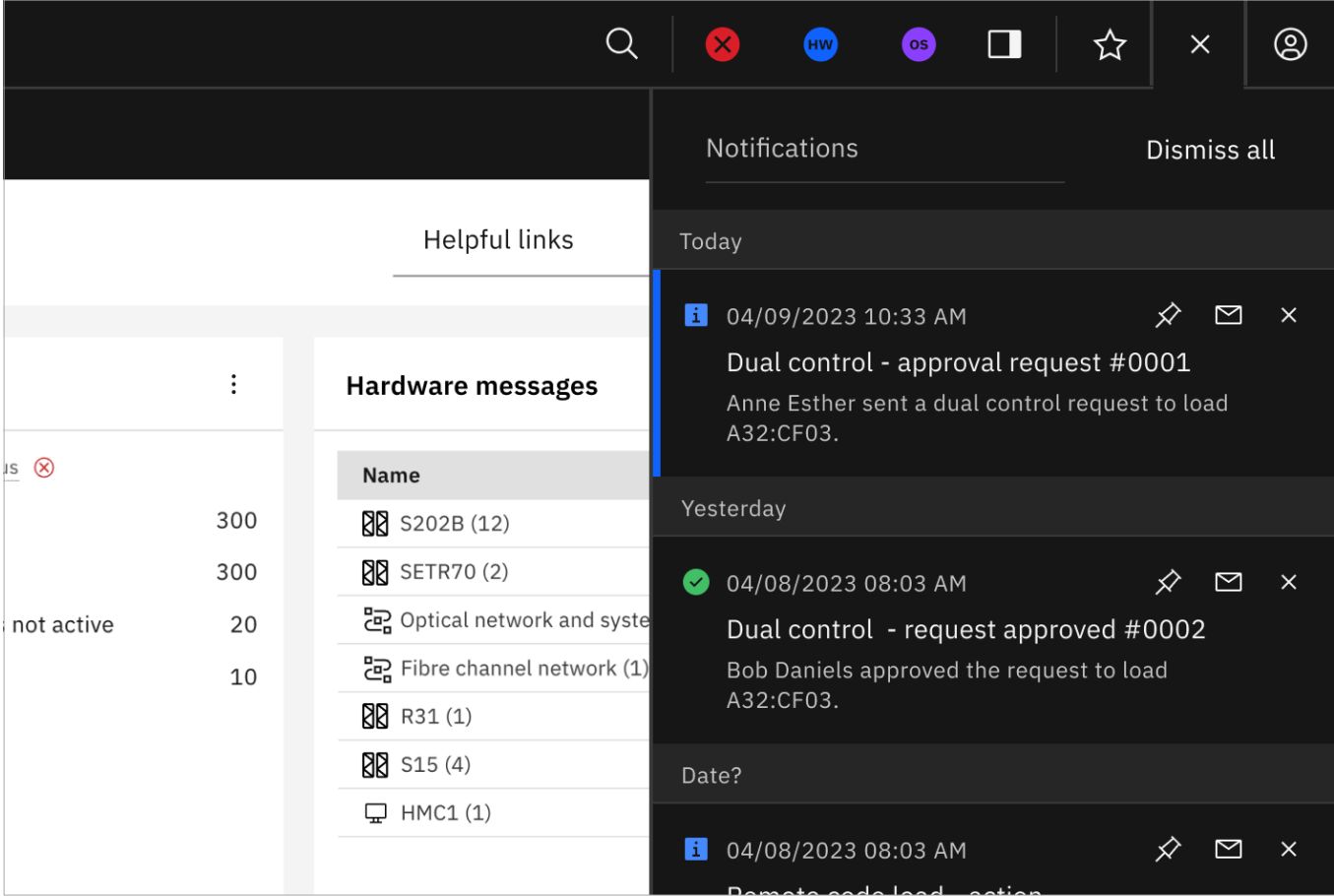


Image: Notifications panel on the HMC

Dual Control Summary

04

Request management and tracking

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

The screenshot displays the IBM Hardware Management Console interface for Dual Control management. The top navigation bar includes 'Home' and 'Dual Control Managem...'. The main header is 'Dual control management' with a search bar and a filter icon. The board is organized into three columns: 'Open' (1 request), 'Approved' (1 request), and 'Closed' (73 requests). Each column contains cards for individual requests, providing details such as the request ID, title, requester, approver, request sent time, and status.

Column	Request ID	Title	Requester	Approver	Request Sent	Status
Open	#0158	Activate - A32_CF22	eric.weinmann@us.ibm.com	dcadmin	9/23/24, 12:23:58 PM EDT	Not assigned
Approved	#0112	Load - B32_Z05	dcuser1	dcadmin	9/5/24, 5:21:14 PM EDT	Approved
Closed	#0160	Deactivate - A32 CF2	adal	eric.weinmann@us.ibm.com	9/23/24, 2:12:08 PM EDT	Failed
Closed	#0159	Activate - A32_CF222	adal	eric.weinmann@us.ibm.com	9/23/24, 12:24:55 PM EDT	Failed
Closed	#0152	Deactivate - A32_CF1	adal	eric.weinmann@us.ibm.com	9/19/24, 2:16:40 PM EDT	Rejected
Closed	#0157	Load - LCST3T40_T13CHP51	dcuser1	dcadmin	9/19/24, 4:25:41 PM EDT	Past

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

The screenshot displays the IBM Hardware Management Console interface for a Dual Control request. At the top, a navigation bar includes a search icon, a close button, and a refresh button. Below the navigation bar, a breadcrumb trail shows 'Home' and 'Dual Control Management...'. A yellow warning banner at the top states: 'Disruptive Approval of this request might result in the disruption of partition operations.' Below this, the request details are shown in a light gray box with the following information:

- Approved:** (indicated by a blue checkmark)
- Name:** #0112 Load - B32_ZOS
- Description:** --

The 'Request information' section is presented as a table:

Task	Target(s)	Approver(s)	Requester
Load	ZOS	dcadmin	dcuser1

Below the table, the 'Request sent' date is 9/5/24, 5:21:14 PM EDT, and the 'Run' options are 'Manual' and 'After approval'.

The 'Inputs' section lists various parameters:

- CPC:** B32
- Image:** ZOS
- Force:** true
- Options:** Normal
- Load Address:** 04801
- Load Parameters:** 481351
- Device Type:** ECKD
- IPL Type:** CCW
- Load:** OS
- Time-out Value:** 60

The 'History' section shows a log of events:

- dcuser1** created the request. 9/5/24, 5:21:14 PM EDT
- dcadmin** approved the request. 9/5/24, 5:21:27 PM EDT

The 'Comments' section is currently empty, displaying 'No comments' and a prompt to 'Add comments to share information.' At the bottom, there is a text input field labeled 'Write comment' and a character count of 0/1024.

Image: Dual control request review page

Dual Control

Dual Control Task List

Supported tasks

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

Customer prioritized task list

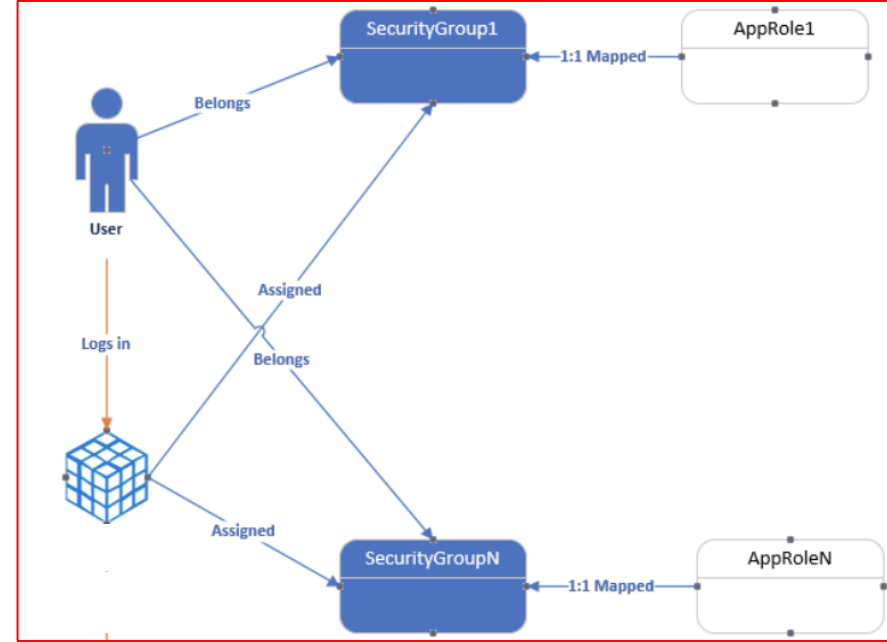
Activate (System & Partition) Activate a system	Deactivate (System & Partition) Deactivate a system	Reset (Clear/Normal) Perform resets clear of selected images, and Perform resets normal of selected images	Load Remembers last used values for all of its fields (woohool), also Load from Removable Media or Server
Change LPAR Controls Customize logical partition processor resources for selected CPCs	Change LPAR Cryptographic Controls	Change LPAR Group Controls Customize a group assignment for logical partitions of selected CPCs	Configure Channel Path On/Off Toggle channel paths between online and standby states
Change LPAR Security Change LPAR Security	Customize / Delete Activation Profiles Customize or delete activation profiles for selected objects	Customize / Delete Activation Profiles - Cryptographic section	Perform Model Conversion (Capacity on Demand) Perform Model Conversion
Power off or restart NEED FULL TASK LIST (restart console, SE, system, etc)	Manage System Time Setup, modify, and view a topographical visualization of an STP-only Coordinated Timing Network. This task is formerly known as "System (Sysplex) Time."		

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

The screenshot shows the 'Customize Console Services' dialog box in the IBM Hardware Management Console. The dialog is titled 'Customize Console Services' and contains several configuration options. The 'TLS settings' option is highlighted with a blue arrow, showing 'TLSv1.2, 39 ciphers' and a 'Change...' button. Other options include 'Remote operation', 'Remote power off or restart', 'LIC change', 'Optical error analysis', 'Problem analysis', 'Console messenger', 'Fibre channel analysis', 'Large retrieves from support system', 'Check held LIC changes during install', and 'FTPS Hostname Validation'. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

Remote operation:	Disabled	Change...
Remote power off or restart:	Disabled	Change...
LIC change:	Enabled	
Optical error analysis:	Disabled	
Problem analysis:	Enabled	
Console messenger:	Enabled	
Fibre channel analysis:	Disabled	
Large retrieves from support system:	Enabled	
Check held LIC changes during install:	Enabled	
FTPS Hostname Validation:	Disabled	
TLS settings:	TLSv1.2, 39 ciphers	Change...
Transmit system availability data:	Enabled	Change...

TLS 1.2 Filtered Ciphers

HMCI: Hardware Management Console Workplace (Version 2.17.0) — Mozilla Firefox
https://9.47.77.125:8443/hmc/fwconnects/mainuiFrameset

IBM Hardware Management Console

Home Customize Console Ser... x

Configure TLS Settings

Specify the TLS settings for the console including "Remote Browser", "Web Services API HTTP Server" or "Single Object Operation" connections into the console.

Minimum TLS protocol version: **TLSv1.2**

TLS Cipher Suites:

Select	Name	Protocols	Description
<input checked="" type="checkbox"/>	TLS_AES_256_GCM_SHA384	TLSv1.3	Authentication with 256 bit AES_GCM cipher and SHA-384 hashing.
<input checked="" type="checkbox"/>	TLS_AES_128_GCM_SHA256	TLSv1.3	Authentication with 128 bit AES_GCM cipher and SHA-256 hashing.
<input checked="" type="checkbox"/>	TLS_CHACHA20_POLY1305_SHA256	TLSv1.3	ChaCha20 stream cipher and Poly1305 message authenticator and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2	ECDHE key exchange and ECDSA authentication with 128 bit AES_GCM cipher and SHA-384 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2	ECDHE key exchange and ECDSA authentication with 128 bit AES_GCM cipher and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	TLSv1.2	ECDHE key exchange and ECDSA authentication with ChaCha20 stream cipher and Poly1305 message authenticator and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	ECDHE key exchange and RSA authentication with 256 bit AES_GCM cipher and SHA-384 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLSv1.2	ECDHE key exchange and RSA authentication with ChaCha20 stream cipher and Poly1305 message authenticator and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	ECDHE key exchange and RSA authentication with 128 bit AES_GCM cipher and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	DHE key exchange and RSA authentication with 256 bit AES_GCM cipher and SHA-384 hashing
<input checked="" type="checkbox"/>	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLSv1.2	DHE key exchange and RSA authentication with ChaCha20 stream cipher and Poly1305 message authenticator and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	TLSv1.2	DHE key exchange and DSS authentication with 256 bit AES_GCM cipher and SHA-384 hashing
<input checked="" type="checkbox"/>	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLSv1.2	DHE key exchange and DSS authentication with 128 bit AES_GCM cipher and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	TLSv1.2	DHE key exchange and DSS authentication with 128 bit AES_GCM cipher and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2	ECDHE key exchange and ECDSA authentication with 256 bit AES_CBC cipher and SHA-384 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	ECDHE key exchange and RSA authentication with 256 bit AES_CBC cipher and SHA-384 hashing
<input checked="" type="checkbox"/>	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2	ECDHE key exchange and ECDSA authentication with 128 bit AES_CBC cipher and SHA-256 hashing

Total: 49

TLS 1.3 Filtered Ciphers

HMCI: Hardware Management Console Workplace (Version 2.17.0) — Mozilla Firefox
https://9.47.77.125:8443/hmc/fwconnects/mainuiFrameset

IBM Hardware Management Console

Home Customize Console Ser... x

Configure TLS Settings

Specify the TLS settings for the console including "Remote Browser", "Web Services API HTTP Server" or "Single Object Operation" connections into the console.

Minimum TLS protocol version: **TLSv1.3**

TLS Cipher Suites:

Select	Name	Protocols	Description
<input checked="" type="checkbox"/>	TLS_AES_256_GCM_SHA384	TLSv1.3	Authentication with 256 bit AES_GCM cipher and SHA-384 hashing.
<input checked="" type="checkbox"/>	TLS_AES_128_GCM_SHA256	TLSv1.3	Authentication with 128 bit AES_GCM cipher and SHA-256 hashing.
<input checked="" type="checkbox"/>	TLS_CHACHA20_POLY1305_SHA256	TLSv1.3	ChaCha20 stream cipher and Poly1305 message authenticator and SHA-256 hashing
<input checked="" type="checkbox"/>	TLS_EMPTY_RENEGOTIATION_INFO_SCSV		Not a true cipher suite and cannot be negotiated

Total: 4

Default Ciphers

OK Cancel Help

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

IBM HMC

Home Customize Console Servi... X

Customize Console Services

Remote operation:	Disabled	Change...
Remote power off or restart:	Disabled	Change...
LIC change:	Enabled	
Optical error analysis:	Disabled	
Problem analysis:	Enabled	
Console messenger:	Enabled	
Fibre channel analysis:	Disabled	
Large retrieves from support system:	Enabled	
Check held LIC changes during install:	Enabled	
Minimum TLS version:	TLSv1.2	
Transmit system availability data:	Enabled	Change...
Quantum-resistant password protection:	Disabled	Change...

OK Cancel Help

IBM HMC

Home Customize Console Servi... X

Customize Console Services

Quantum-resistant password protection is required to replicate with Driver 61 (2.17.0) and later HMCs

Are you sure you want to enable quantum-resistant password protection?

- * Data replication will fail for HMCs which are not enabled
- * User profile data cannot be restored to HMCs which are not enabled
- * Quantum-resistant password protection cannot be disabled

ACT50211

Enable quantum-resistant password protection Cancel

Replicate HMC Certificates to SE

Replicate HMC Certificates to SE

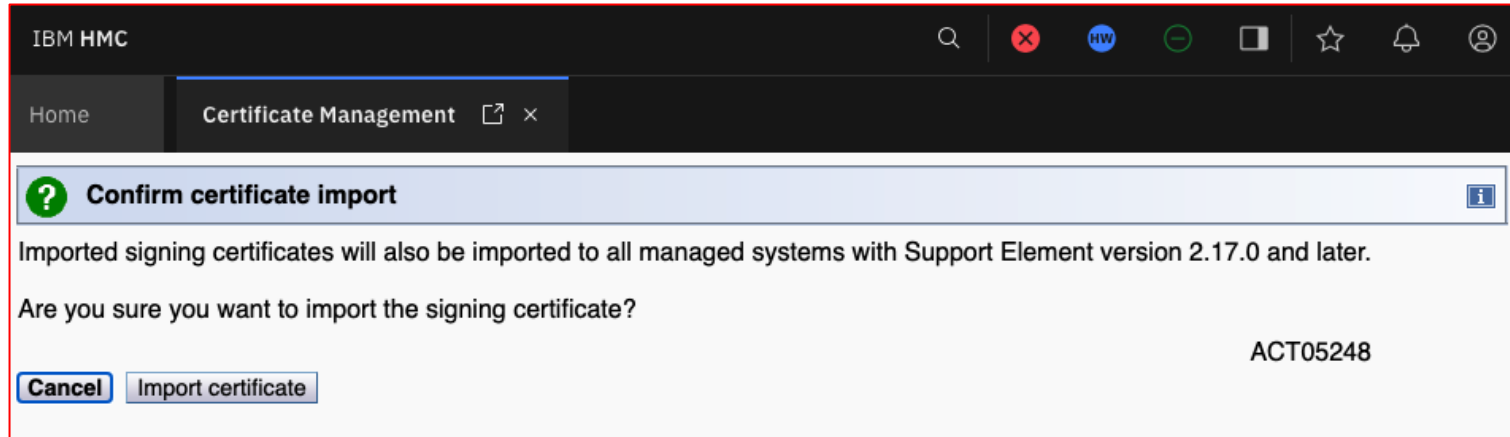
➤ Certificates imported to the *HMC Certificate Management* task will also be imported to *managed IBM z17 SEs*.

- 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

Home OSA Advanced Faciliti... [icon] x

Manage Security Certificates - B32

Channel ID: 016C
LAN port type: OSA-ICC 3270

OSA-ICC certificate scope: Use shared certificate [Change...](#)
OSA-ICC certificate type: Self-signed
OSA-ICC certificate expiration: Aug 17 17:49:27 2034 GMT

Actions:

- Export self-signed certificate (.pem)
- Reload self-signed certificate
- Regenerate OSA-ICC key and self-signed certificate
- Create certificate signing request (.csr)
- Import signed certificate (.pem or .p7b)
- View certificate

Location:

- FTP
- File System

[Apply](#) [Close](#) [Help](#)

Home OSA Advanced Faciliti... [icon] x

Advanced Facilities - B32 [info icon]

The current certificate, which is shared across OSA PCHIDs, will be replaced. The new certificate will not be applied to online OSA PCHIDs until they are configured off, and then back on. Are you sure you want to continue?

[Yes](#) [No](#)

ACT2051A

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 **BCPiAutomation1**

BCPiAutomation1
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 bcp-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*

IBM HMC

Home Customize Console Ser... x

Customize Console Services

Remote operation: Disabled [Change...](#)

Remote power off or restart: Disabled [Change...](#)

LIC change: **Enabled**

Optical error analysis: Disabled

Problem analysis: Enabled

Console messenger: Enabled

Fibre channel analysis: Disabled

Large retrieves from support system: Enabled

Check held LIC changes during install: Enabled

FTPS Hostname Validation: Disabled

TLS settings: TLSv1.2, 39 ciphers [Change...](#)

Transmit system availability data: Enabled [Change...](#)

BCPii authorizations: Enabled [Change...](#)

[OK](#) [Cancel](#) [Help](#)

IBM HMC

Home Customize Console Ser... x

Authorize BCPii Access

Authorize BCPii users to securely access HMC Web Services APIs.

Authorizations

Search authorizations [Add authorization +](#)

<input type="checkbox"/>	Name	Description	Users	Certificates
<input type="checkbox"/>	bcp-iiuid_auth	-	bcp-iiuid	bcp-iiuid_cert

[Close](#) [Help](#)

Edit Authorization

General

Users

Certificates

Review summary

Users

Define the BCPii users authorized to access Web Services APIs.

BCPii users

[Add user +](#)

BCPii user name	HMC user or template name
bcp-iiuid	hmcuser

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

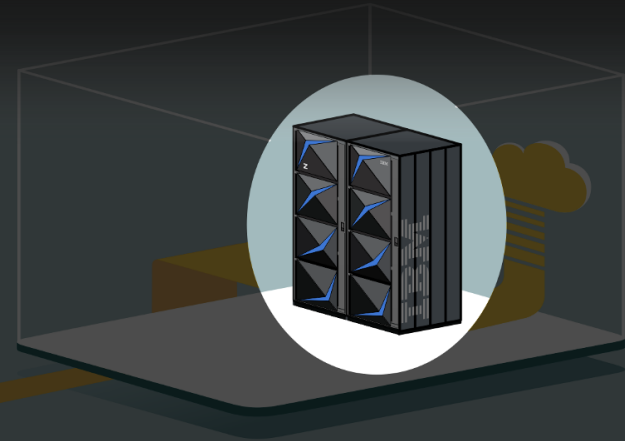
➤ For IBM z17, IBM recommendation is to use Remote Code Load for firmware update of MCL Bundles

- 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

The screenshot displays the IBM Hardware Management Console (HMC) interface. The title bar reads "HMCFCM1: Hardware Management Console Workplace (Version 2.17.0)". The main header is "IBM Hardware Management Console".

Dashboard Overview:

- Systems health:** A table showing the status of systems and adapters.
- Hardware messages:** A list of messages, including "SEFMPOK (4)" and "HMCFCM1 (217)".

Component	Count	Status
Systems	1	Unacceptable status
Adapters	102	Not operating

Notifications (11):

- 1 hour ago:** Firmware Update Completed. A remote firmware update on HMCFCM1 to activate bundle H02 has completed successfully.
- 2 hours ago:** Firmware Update Running. A remote firmware update is now running on HMCFCM1 to activate bundle H02.
- 2 hours ago:** Firmware Update Scheduled. A remote firmware update has been scheduled on HMCFCM1 to activate bundle H02 at September 24, 20...

IBM HMC Mobile 5.0

IBM Z HMC Mobile Field Data

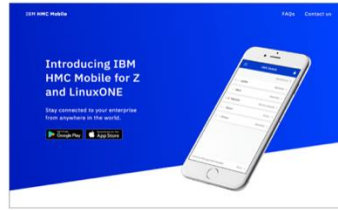
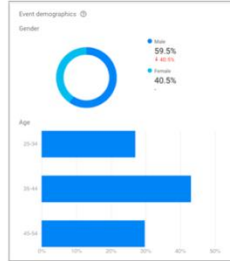
Allows systems administrators to monitor and manage their hardware from anywhere.

16600 IOS APP INSTALLS

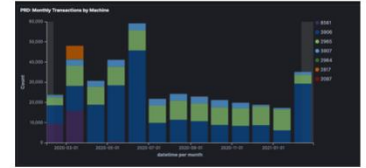
2820 ANDROID APP INSTALLS

824000 PRODUCT PAGE VIEWS

30,308 PUSH NOTIFICATIONS PER MONTH

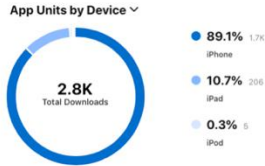


ibm.biz/hmc-mobile



User engagement > Screen class

Screen class	% total	Avg. time
HomeController	28.69% ↑ 63.5%	3m 23s ↑ 48.6%
SessionExp...ontroller	16.44% ↑ 2...4%	32m 24s ↑ 989.8%
SystemDet...ontroller	8.31% ↑ 263.8%	2m 10s ↑ 347.8%
LPARDetail...ontroller	6.95% ↑ 146.4%	3m 6s ↑ 101.1%
HMCDrawer...ntroller	5.49% ↓ 29.4%	1m 57s ↓ 20%
(not set) HMCDrawerViewController%	↑ 760.8%	4m 23s ↑ 434.1%
Partitions...Controller	4.84% ↑ 180.9%	1m 55s ↑ 150.2%
SettingsVi...Controller	2.24% ↓ 36.4%	0m 38s ↓ 40%



“

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)



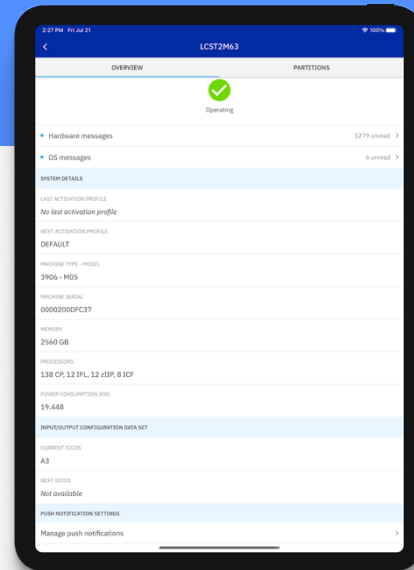
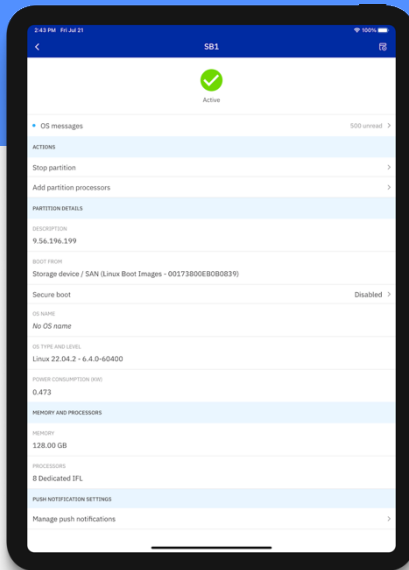
Survey intercept



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

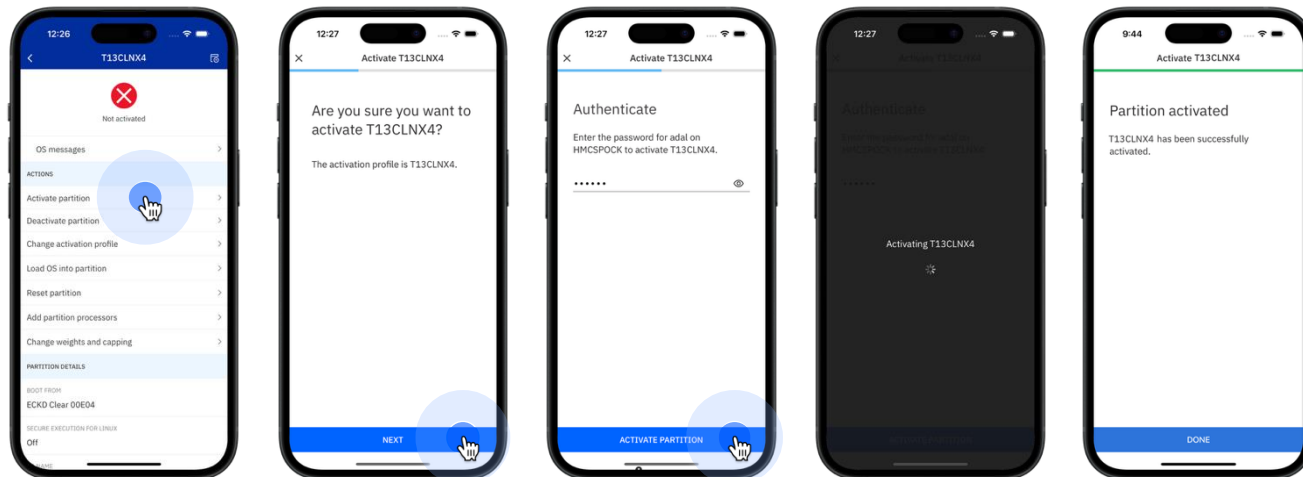




Dual Control

Activate

Dual Control
Not Enabled

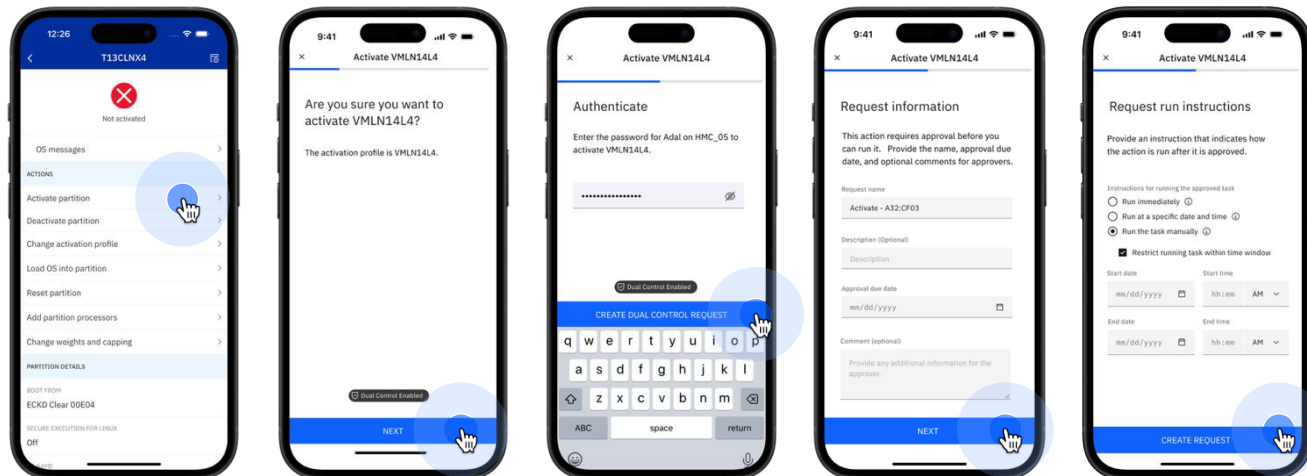




Dual Control Create Request

Activate

Dual Control
Enabled





Dual Control Request Management

View and Manage Dual Control Requests

The screenshot displays the 'Dual Control Requests' mobile application interface. At the top, there is a search bar labeled 'Filter requests' and a filter dropdown menu currently set to 'Open'. Below the filter, the requests are categorized into three sections: 'Open', 'Approved', and 'Closed'. Each request entry includes a status icon, a title, a brief description, and an assigned approver. The 'Open' section contains three requests: 'Activate - A32:CF1', 'Load - A32:LX1', and 'Change LPAR Crypto Controls A32'. The 'Approved' section contains two requests: 'Change LPAR Crypto Controls A32' and 'Load - A32: LX4'. The 'Closed' section contains three requests: 'Load - A32:LX2', 'Deactivate - A32:LX3', and 'Perform model conversion: A32'.

Status	Request ID	Description	Assigned To / Approver
Open	Activate - A32:CF1	Activate the coupling facility as discussed in the os rollover planning meeting on 10/20/24.	Assigned: Bob@us.ibm.com
Open	Load - A32:LX1	North America and United Kingdom SMTP Server Migration of the request	Assigned: Bob@us.ibm.com
Open	Change LPAR Crypto Controls A32	Key exchange planned for 10.24.24.	Assigned: Bob@us.ibm.com
Approved	Change LPAR Crypto Controls A32	North America and United Kingdom SMTP Server Migration	Approver: Bob@us.ibm.com
Approved	Load - A32: LX4	IT Support request 132345	Approver: Bob@us.ibm.com
Closed	Load - A32:LX2	IT Support request 132345	Approved
Closed	Deactivate - A32:LX3	Planned outage 10.20.24. Ticket 12345	Approved
Closed	Perform model conversion: A32	Upgrade approval 1234625.	Approved



Dual Control Request Details

View, Approve, Reject, Run, Comment

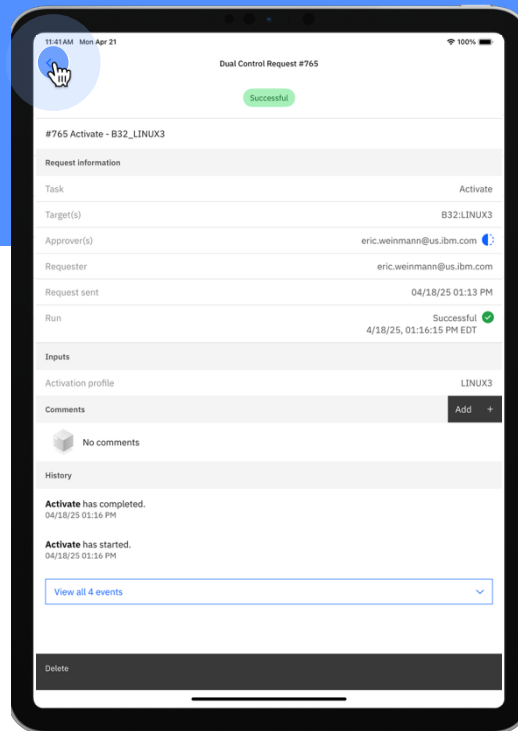
The screenshots show the following details for request #173:

- Open Status:** Request to load coupling facility CF03 per ticket 8675309. Includes fields for Task, Target(s), Approval due, Approver(s), Requester, Request sent, and Run options (Scheduled, Immediately on approval).
- Approved Status:** Shows the request has been approved by jane@ibm.com. Includes an 'Assign myself' button and 'Inputs' section with CPC, Image, IPL type, and Load address.
- Successful Status:** Shows the request was successfully completed on 3/20/25 at 8:32:45 AM EDT. Includes a 'View all 7' link for inputs and a 'Delete' button.



Dual Control Notifications

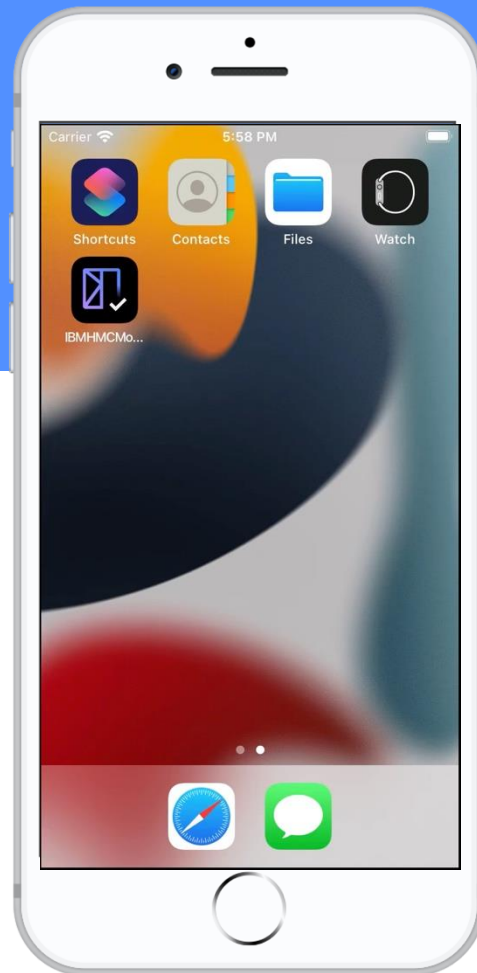
Created, assigned, approved, rejected, canceled, running, run success





Survey

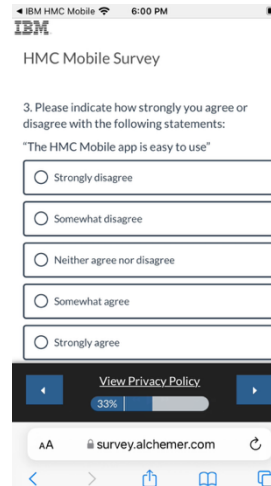
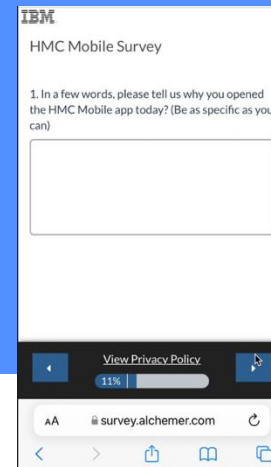
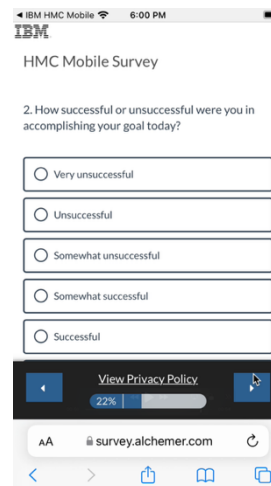
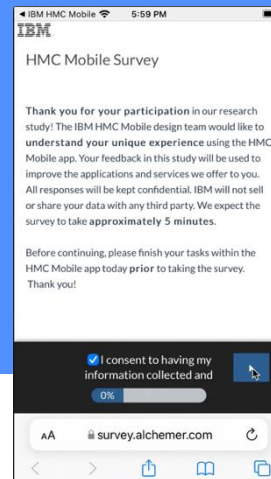
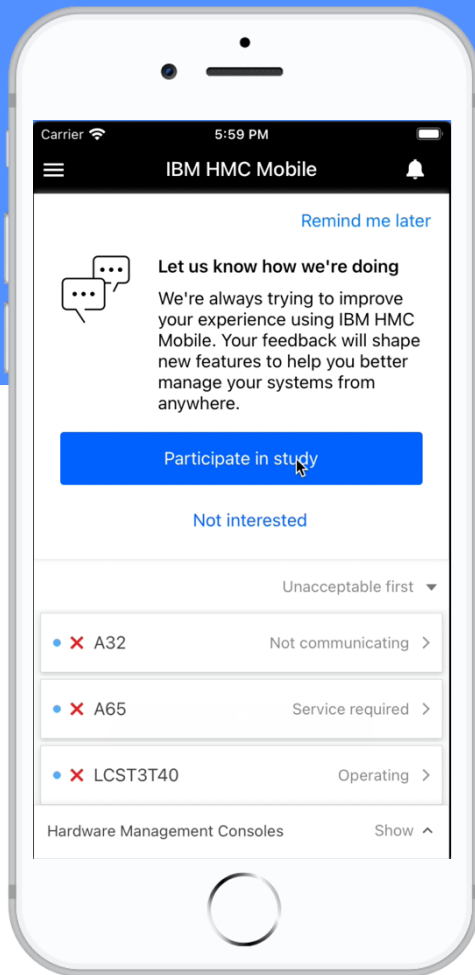
Survey intercept for users





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](https://ibm.biz/IBM-Z-HMC)
- For additional topic areas of interest, notify Brian Valentine (bdvalent@us.ibm.com)

IBM Z Hardware Management Console Videos

Search

	HMC Overview and Management (11 Videos)	Learn about the IBM Z HMC dashboard and management features.
	Access and Security (15 Videos)	Learn about managing access and security on the HMC.
	HMC Mobile (2 Videos)	Stay connected to your enterprise from anywhere in the world.
	Manage System Time (STP) (5 Videos)	Learn to manage coordinated time networks for your systems.
	Dynamic Partition Manager (5 Videos)	Learn to manage systems enabled for Dynamic Partition Management.

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)

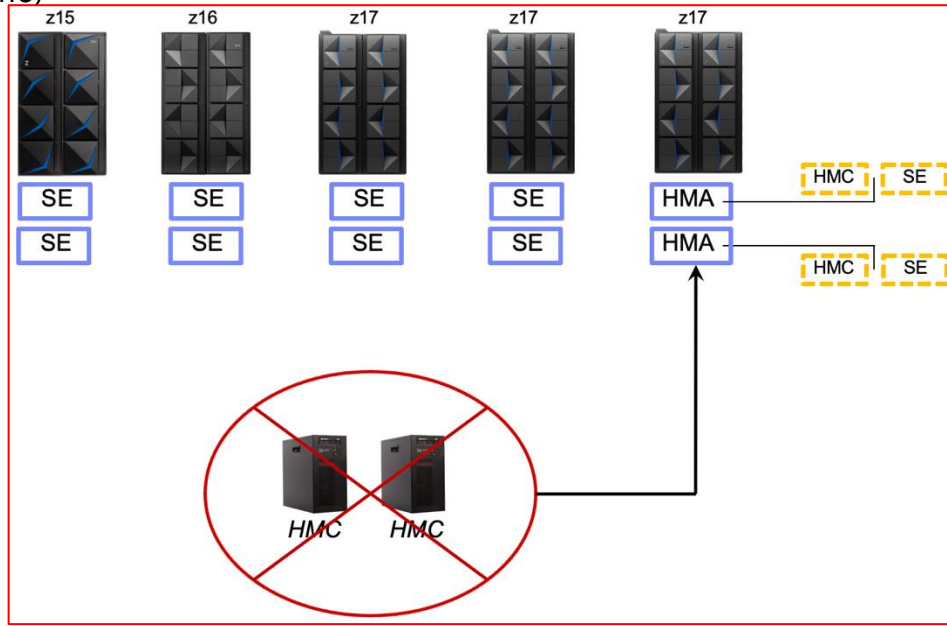
➤ No longer a requirement to set Service Status for HMC HMA upgrade (keep visibility to Images) (see previous chart)

➤ 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

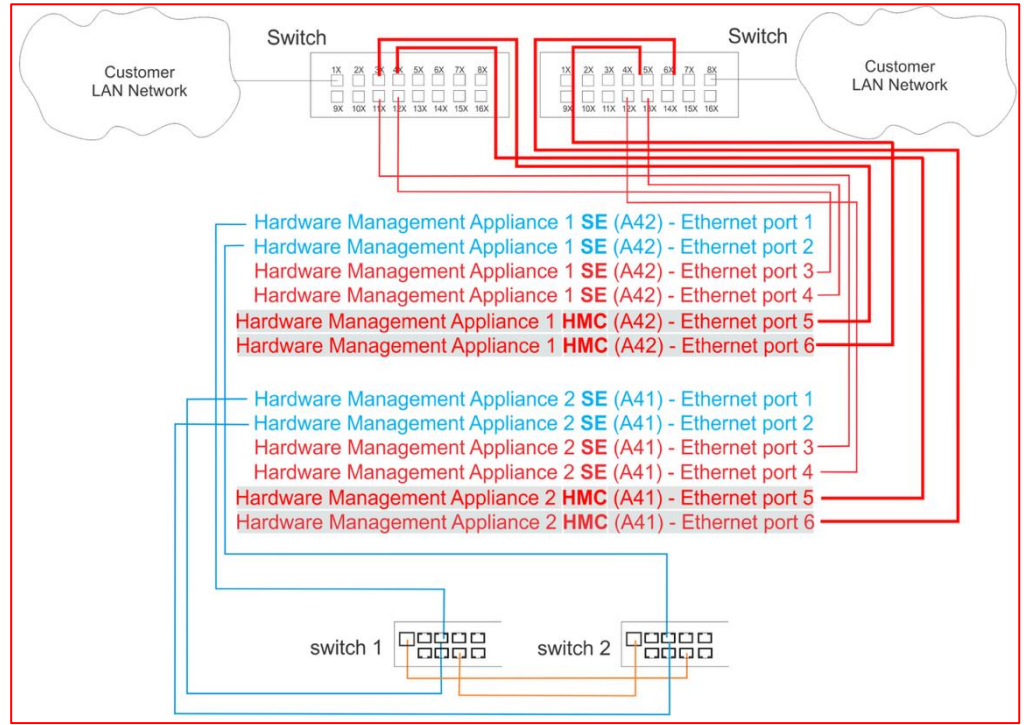
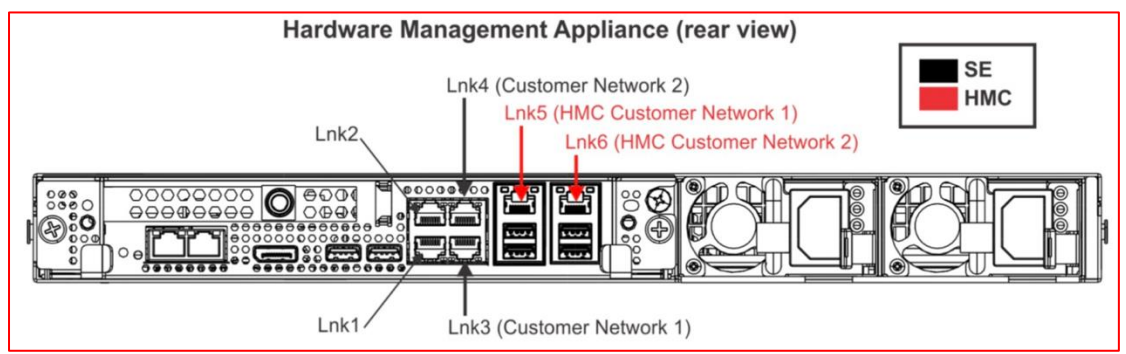
➤ Same number of physical networking on HMA HMC/SE as Standalone HMCs & SEs

➤ 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

IBM Hardware Management Console

Home Customize Console Servi... [X]

Change Remote Access Settings

Enable remote browser access for this Hardware Management Console and then choose which IP addresses and users are given access.

Enable remote web browser access

IP Access Control

Allow all IP addresses
 Allow specific IP addresses

Select IP Addresses

Add Edit Remove

User Access Control

Select	Name	Type
<input checked="" type="checkbox"/>	ADVANCED	User
<input checked="" type="checkbox"/>	BCPII_TEST	User
<input checked="" type="checkbox"/>	BDVsysprog	User

Single Sign On Details

User Management Changes

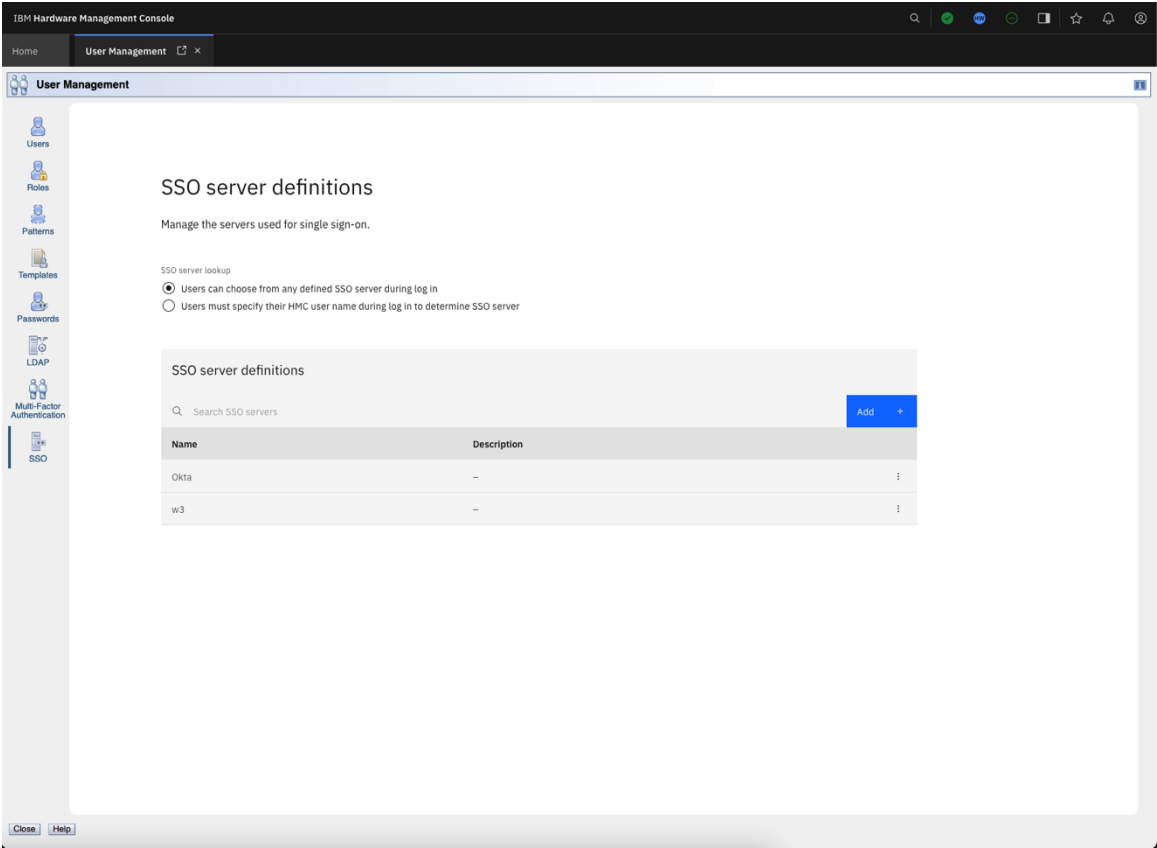
➤ SSO tab

- 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

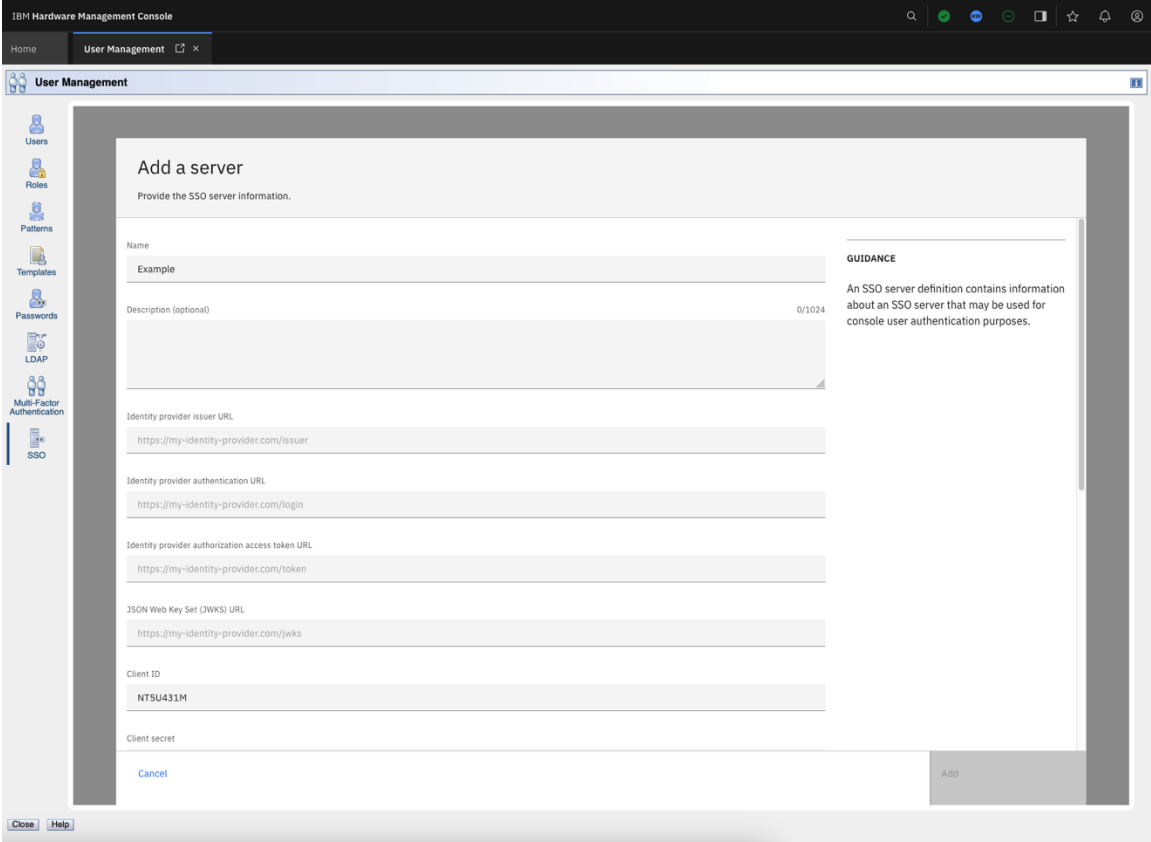
➤ SSO tab

- 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

Authentication

Password authentication

Type: HMC LDAP SSO

* Server:

Delay login after failed attempts

Number of failed attempts before disable delay:

Delay (minutes):

Disable for inactivity (days):

Require password for disruptive actions

Require text input for disruptive actions

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.

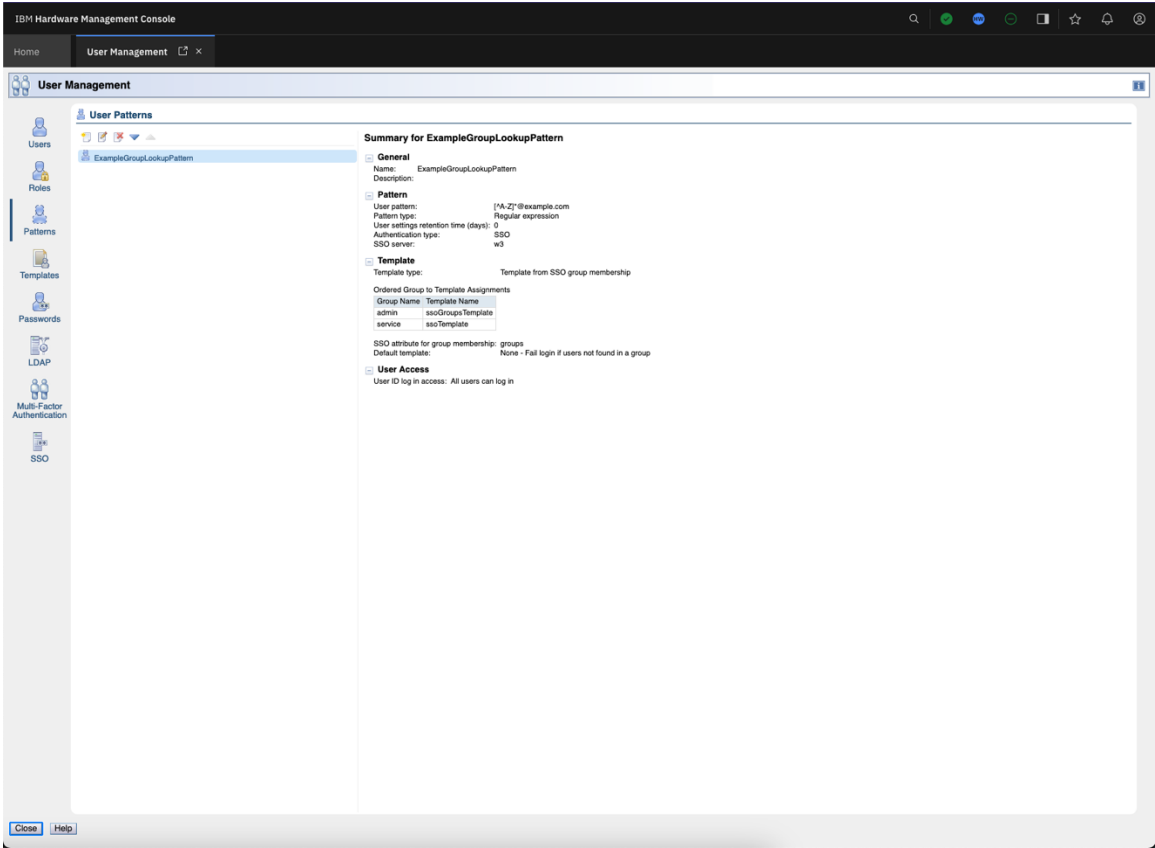
User Management Changes

➤ 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

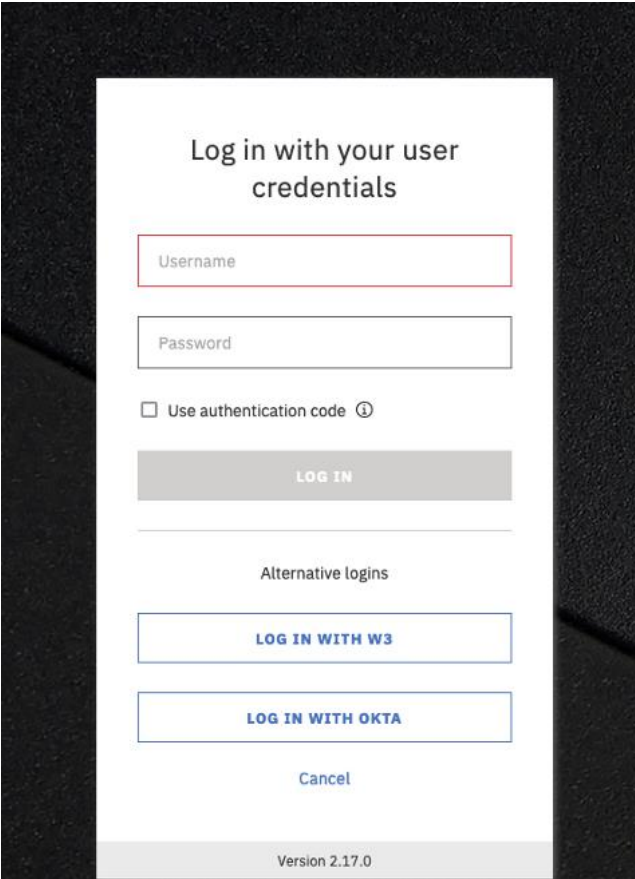


Logon Changes

- 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



Log in with your user credentials

Username

Password

Use authentication code ⓘ

LOG IN

Alternative logins

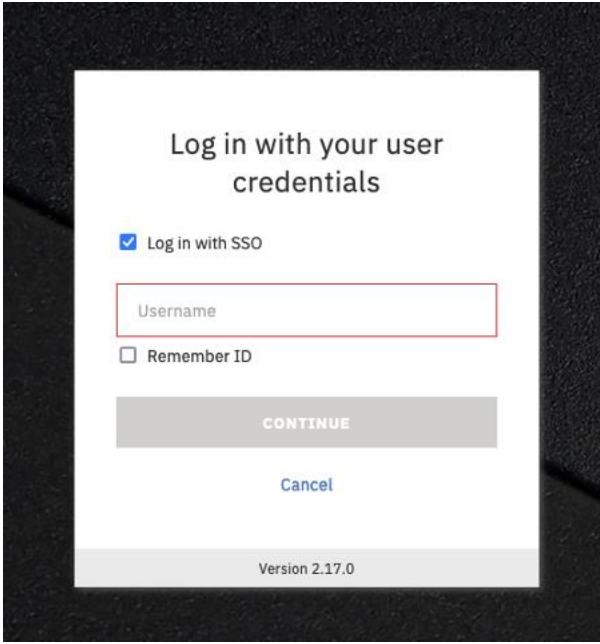
LOG IN WITH W3

LOG IN WITH OKTA

Cancel

Version 2.17.0

SSO Checkbox Logon



Log in with your user credentials

Log in with SSO

Username

Remember ID

CONTINUE

Cancel

Version 2.17.0

Network Time Security Details

Configure Eternal Time Source

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

STP ACTIONS

- Add systems to CTN
- ➔ Configure External Time Source
- Deconfigure CTN
- Export CTN data (.xls)
- Manage CTN Certificates
- Modify assigned server roles
- Remove systems from CTN
- Set CTN member restriction
- Setup new CTN

Advanced Actions ^

STRATUM 3

STRATUM 4

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
<input type="radio"/>	B229 (CTS/PTS)	NTP, PTP	ETS1	
<input checked="" type="radio"/>	B26	NTP, PTP	time10-20-3-c.pokprv.stglabs.ibm.	
<input type="radio"/>	A26	PTP	time10-20-2-c	time10-20-3-d
<input type="radio"/>	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

Choose NTP External Time Sources

Configure NTP external time sources for your systems (optional).

<input type="checkbox"/>	Server	Stratum	Source	PPS port	Security	Preferred	Connection status
<input type="checkbox"/>	time10-20-3-c.pokprv.stglabs.ibm.com	1	MRS	-	NTS	✓	✓
<input type="checkbox"/>	time10-20-3-d	1	SHM	-	None	-	✓

ADD NTP SERVER

TEST CONNECTIVITY

SET NTP THRESHOLDS

DELETE

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)

Add PTP Server

Provide the hostname or IP address and security settings of the PTP server.

Ethernet interface

PPS port

IP type

Domain number

Communication Multicast
 Unicast

Preferred server for time adjustments

Security type

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

STP ACTIONS	
Add systems to CTN	
Configure External Time Source	
Deconfigure CTN	
Export CTN data (.xls)	
Manage CTN Certificates	STRATUM 3
Modify assigned s	Manage the certificates used to secure the connection to the time server.
Remove systems from CTN	
Set CTN member restriction	
Setup new CTN	
	STRATUM 4
Advanced Actions ▾	

Customize Console Date\Time for HMC

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

The screenshot shows the 'Date and Time' configuration window in the HMC console. It includes sections for 'Battery Operated Hardware Management Console Clock' (with date and time fields), 'Time Source' (with radio buttons for NTP, Selected CPCs, and None), and 'Details for Network Time Protocol (NTP)'. The NTP Servers table has one entry selected. A context menu is open over the table, showing various actions like 'Edit Server ...', 'Remove Server', and 'Table Actions'.

Date and Time

Battery Operated Hardware Management Console Clock

Date: * Oct 15, 2024 Time: * 4:21:57 PM

Time zone: America/New_York

Time Source

- Network Time Protocol (NTP) ...
- Selected CPCs ...
- None

Details for Network Time Protocol (NTP)

NTP Servers

Select	Server	Stratum	Source
<input checked="" type="checkbox"/>	9.56.192.96	1	MRS

Enable as time server
 Automatically contact the support s...

Refresh OK Cancel Help

--- Select Action ---

- Edit Server ...
- Remove Server
-
- Add Server ...
- Query Servers
- Manage Symmetric Keys ...
- Issue Chronty Commands ...
- Table Actions ---
- Select All
- Deselect All
- Show Filter Row
- Clear All Filters
- Configure Columns

Total: 1 Filtered: 1 Selected: 1

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

The screenshot shows the 'Add Network Time Server' dialog in the IBM Hardware Management Console. The dialog has a title bar with 'IBM Hardware Management Console' and a breadcrumb 'Home > Customize Console Date/Time'. The main content area has a back arrow icon and the title 'Add Network Time Server'. Below this, there is a text input field for 'Enter the time server host name or IP address :' containing 'time10-20-2-a.pokprv.stglabs.ibm.com'. Underneath is the 'Authentication Selection :' section, which includes a dropdown menu currently showing 'NTS' and a 'Certificate Management...' button. Below that is the 'Certificate :' section with a dropdown menu showing 'CN=nts1.ibm.com(4F:'. At the bottom are three buttons: 'OK', 'Cancel', and 'Help'.

IBM Hardware Management Console

Home Customize Console Date/Time

Add Network Time Server

Enter the time server host name or IP address :
time10-20-2-a.pokprv.stglabs.ibm.com

Authentication Selection :
NTS Certificate Management...

Certificate :
CN=nts1.ibm.com(4F:

OK Cancel Help

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

The screenshot displays the IBM Hardware Management Console (HMC) interface. The main window is titled 'Manage remote firmware updates' and contains a yellow notification bar with the text 'Generate a token to opt-in to remote firmware updates.' and a 'Generate token' button. Below this is a table for 'Scheduled remote firmware updates' which is currently empty. A dialog box titled 'Authorize remote firmware updates' is open, containing the following text:

Authorize remote firmware updates

By checking the box below and clicking "Generate token," you agree to allow IBM Service Support Representatives (SSRs) remote access to your environment to perform firmware updates on one or more systems in the environment.

- Tokens are valid for up to seven days from the time they are generated
- Tokens are only valid for the systems managed by the HMC from which they were generated
- The remote firmware upgrade process complies with all IBM security and compliance standards, including GDPR

Once the token is generated, share it with your IBM Service Support Representative to confirm the scheduled firmware update.

I agree to let IBM Service Support Representatives access my environment remotely.

Buttons: Cancel, Generate token

Remote Code Load for IBM Z Firmware – Opt In

- ▶ Client Opt 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)

Manage Remote Firmwar... ✕

Manage remote firmware updates

Use the table below to view and cancel updates, as well as to find contact information for the IBM service representative assigned to schedule your remote firmware update.

i Your remote firmware update authorization code is 2A11FE57. [Copy token](#) [Generate new token](#)
Token expires in 06d : 23h : 59m : 32s

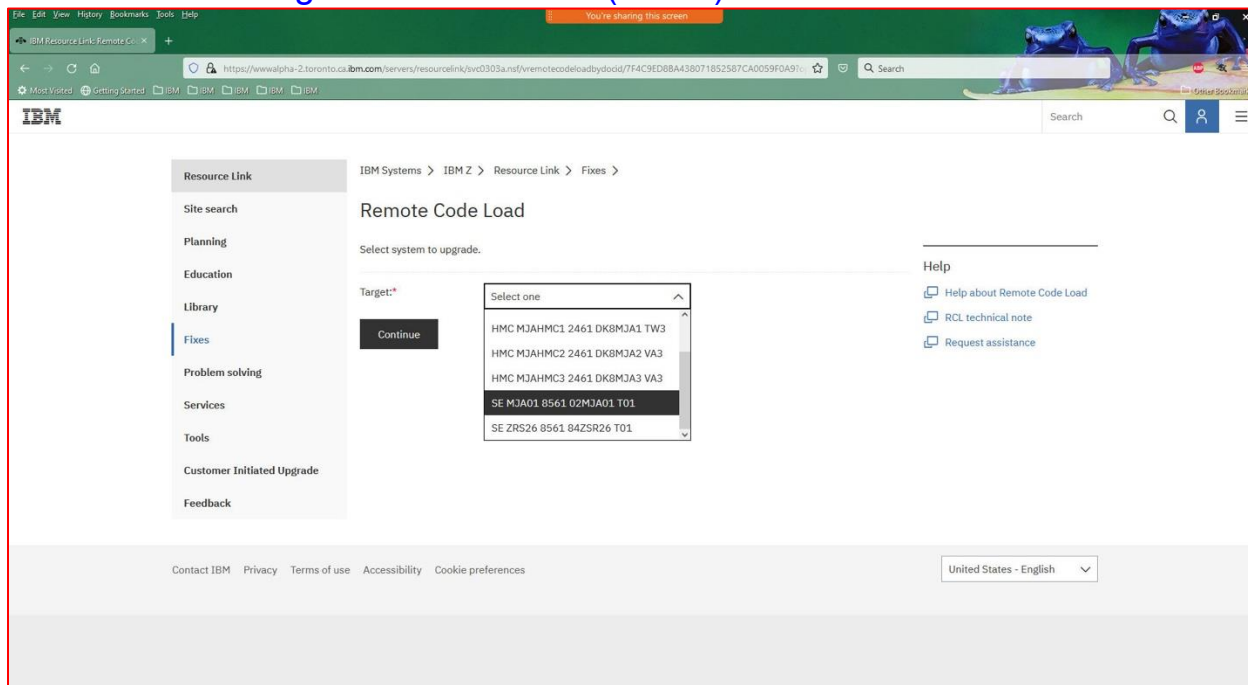
Scheduled remote firmware updates

Target bundle	Date	Time ⓘ	Target name	Status
There are no currently scheduled remote firmware updates.				

[Close](#) [Help](#)

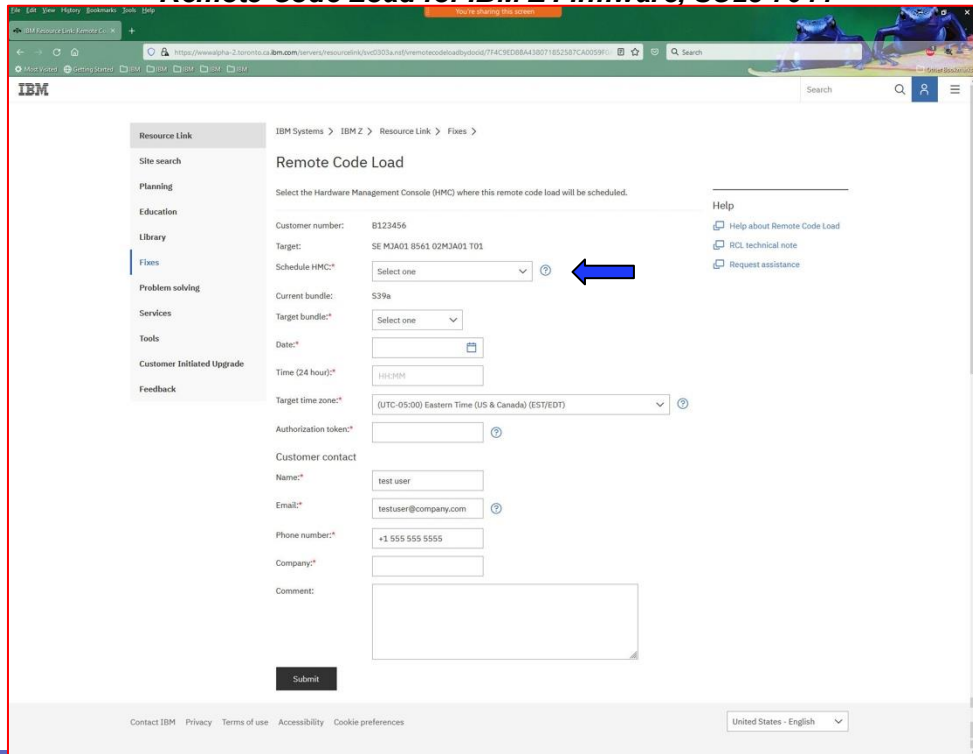
Remote Code Load for IBM Z Firmware – Client Schedules

- ▶ 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

IBM

