Delta Pages (P/N 03GH503)
for
8562 Service Guide
GC28-7010-00



IBM®

8562 Service Guide

P/N 03GH503

Delta

Base Publication Number:	GC28-7010-00	Date: 15 May 2020
	GC28-7010-00a	15 Sept 2020
	GC28-7010-00b	31 Dec 2020
	GC28-7010-00c	31 March 2020
	GC28-7010-00d	20 May 2021

This Delta provides replacement pages and additional information for the base publication described above. The replacement pages and additional information remain in effect for subsequent editions unless specifically altered.

Pages to be inserted and replaced are:

Level -00a

Replace z15 8562 Service Guide (GC28-7010-00) pages 11-38 with delta pages 11-38
Replace z15 8562 Service Guide (GC28-7010-00) pages 57-58 with delta pages 57-58b
Replace z15 8562 Service Guide (GC28-7010-00) pages 103-104 with delta pages 103-104
Replace z15 8562 Service Guide (GC28-7010-00) pages 169-170 with delta pages 169-170
Replace z15 8562 Service Guide (GC28-7010-00) pages 253-258 with delta pages 253-258
Replace z15 8562 Service Guide (GC28-7010-00) pages 365-366 with delta pages 365-366

Level -00b

Replace z15 8562 Service Guide (GC28-7010-00) pages 17-18 with delta pages 17-18
Replace z15 8562 Service Guide (GC28-7010-00) pages 41-50 with delta pages 41-50
Replace z15 8562 Service Guide (GC28-7010-00) pages 167-178 with delta pages 167-178f
Replace z15 8562 Service Guide (GC28-7010-00) pages 225-226 with delta pages 225-226
Replace z15 8562 Service Guide (GC28-7010-00) pages 253-262 with delta pages 253-262
Replace z15 8562 Service Guide (GC28-7010-00) pages 337-340 with delta pages 337-340b
Replace z15 8562 Service Guide (GC28-7010-00) pages 369-370 with delta pages 369-370

Level -00c

Replace z15 8562 Service Guide (GC28-7010-00) pages 57-58 with delta pages 57-58b
Replace z15 8562 Service Guide (GC28-7010-00) pages 59-62 with delta pages 59-62h
Replace z15 8562 Service Guide (GC28-7010-00) pages 169-170 with delta pages 167-170
Replace z15 8562 Service Guide (GC28-7010-00) pages 339-340 with delta pages 339-340
Replace z15 8562 Service Guide (GC28-7010-00) pages 365-366 with delta pages 365-366
Replace z15 8562 Service Guide (GC28-7010-00) pages 369-370 with delta pages 369-370

Level -00d

Replace z15 8562 Service Guide (GC28-7010-00) pages 121-122 with delta pages 121-122n

A change to the text is indicated by a vertical line to the left of the change.

This Delta contains information about machine type 8562.

Note: Please save these pages along with the publication to provide a record of the changes.

P/N 03GH503 Copyright IBM Corp. 2020, 2021 All rights reserved.
Note to US Government Users - Documentation related to restricted rights - Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Chapter 3. Power information

Use this section to assist in diagnosing power problems.

If you were directed to diagnose system power problems, go to “System power problems” on page 64. The following additional information is provided:

Action or Information	Go to
Resolving Support Element power problems	“Console failures” on page 48
General power information	“Power system information” on page 60
Power system problems	“PDU system power problems” on page 65
Removing system power	“System shutdown” on page 190

© Copyright IBM Corp. 2020, 2021

Power system information

The 8562 is powered by Power Distribution Unit (PDU) power.

Power system information

The highlights of the PDU power system are:

- The main power supplies are Power Distribution Units (PDU). For locations within the system, see "Power Distribution Unit (PDU)" on page 414.
- The 8562 supports 2 or 4 PDUs for Model T02 and Model LT2, and 4 PDUs for Model GT2.
- Model T02 and Model LT2 require 2 or 4 line cords, depending on the number of PDUs. Model GT2 requires 4 line cords.

  For information about the line cords that are supported by the PDU power system, refer to the *8562 Installation Manual for Physical Planning*, GC28-7011.
- The power system is a dual source, redundant power supply, referred to as 2N power. This means that the customer can continue to run when one side of the power system fails.
- Voltage ranges:

  Single-phase

  – 30/32A, 200-240V AC (Wye)

  3-phase

  – 30A, 200-240 V AC (Delta)
  – 30/32A, 380-415V AC (Wye)

  Notes:

  – 480 V AC and HVDC are not supported.
  – Single-phase voltage can be used only when the frame contains one CPC drawer (does not apply to Model GT2).
- The CPCs are powered up and down from the Support Element (SE).
- There are two industry-standard Ethernet switches that the SEs use to control individual outlet power.

Attention: Reseating of FRUs is only supported when directed by Product Engineering or a Retain Tip (TDR) applicable to the fault that is being worked.

CAUTION: Servicing of this product or unit is to be performed by trained service personnel only. (C032)

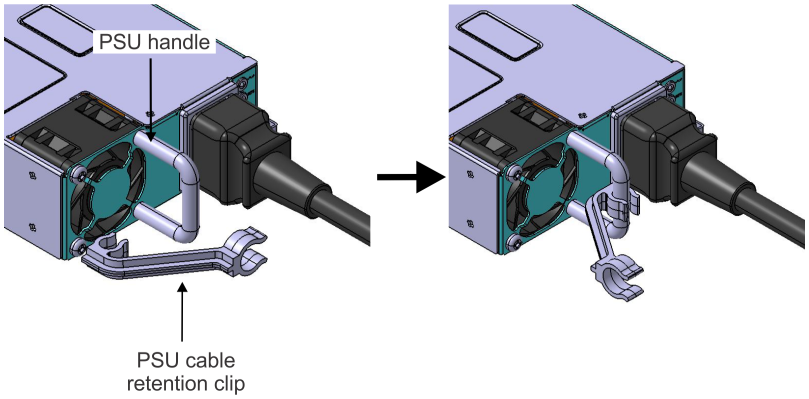
Power Supply Unit (PSU) cable retention clips

The 8562 requires that cable retention clips be installed on all Power Supply Units (PSUs) within the system.

Note: If hook-and-loop fasteners are present on the PSUs, you must remove them before you can install the cable retention clips.

CPC drawer PSUs (2000 W)

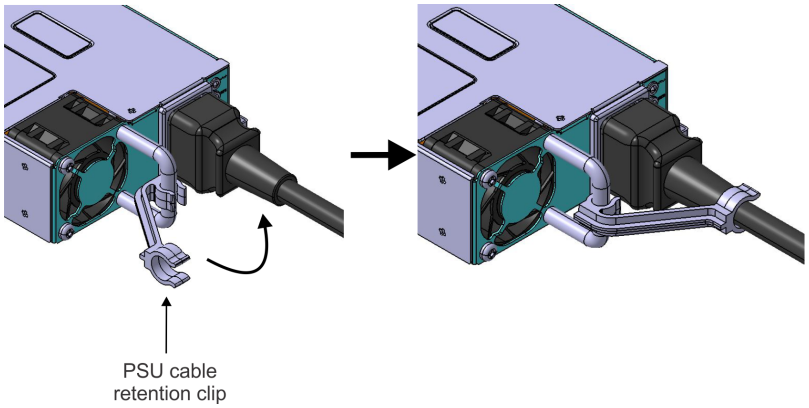
__ 1. Attach the larger PSU cable retention clip (**P/N 03FM860**) to the PSU handle, as shown below:



__ 2. Ensure that the PSU is pushed back into its slot.

__ 3. Ensure that the power cord is plugged into the PSU.

__ 4. Rotate the retention clip and attach the other end of the clip to the power cord, as shown below:

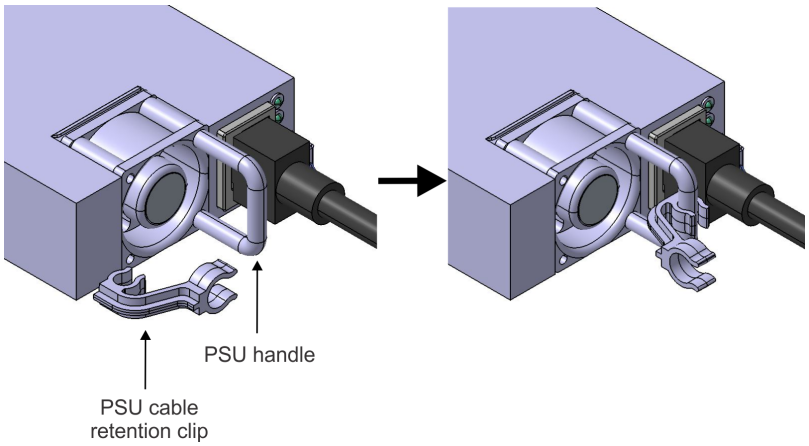


Note: If the power cord is not fully plugged into the PSU, the retention clip will not properly attach to the power cord.

__ 5. Repeat this procedure for all of the appropriate PSUs.

Support Element (900 W) and PCIe+ I/O drawer PSUs (1400 W)

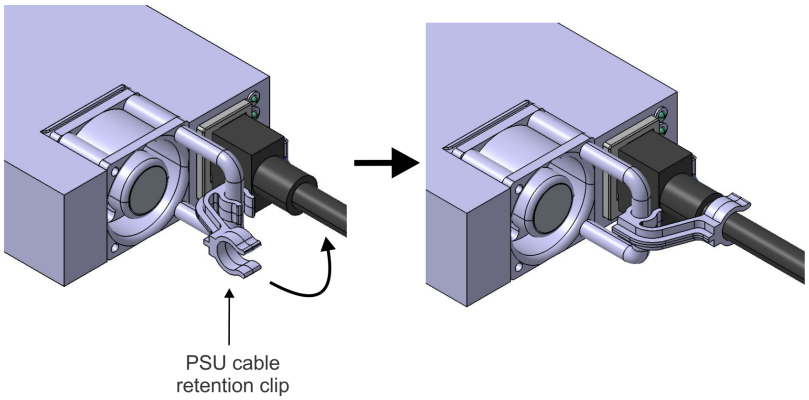
__ 1. Attach the small PSU cable retention clip (**P/N 03FM859**) to the PSU handle, as shown below:



__ 2. Ensure that the PSU is pushed back into its slot.

__ 3. Ensure that the power cord is plugged into the PSU.

__ 4. Rotate the retention clip and attach the other end of the clip to the power cord, as shown below:



Note: If the power cord is not fully plugged into the PSU, the retention clip will not properly attach to the power cord.

__ 5. Repeat this procedure for all of the appropriate PSUs.

Color coding of UPIC cables

The power cables are color-coded to make it easier to determine where the cables go. They have the following color coding on the connectors:

PDU power

- To determine "N" or "Z" side, as addressed by the horizontal label located at the top of the frame:
  - All N-side (left side PDUs at the rear of the frame) power connectors have a striped band label.
  - All Z-side (right side PDUs at the rear of the frame) power connectors have a solid band label.



Attention: Power cables associated with hardware installed in the 16U Reserved Space (FC 0151) or 8U Reserved Space (FC 0150) are not color-coded as described above. This hardware is powered by the PDUs, but the power cables are not serviced by an IBM Z authorized service provider except as follows: power cables associated with storage networking switches in the 8U Reserved Space are installed and serviced by an IBM Z authorized service provider, and they are labeled with plug locations, but they do not use the colored-band label format described above. For more information about the 16U and 8U Reserved Space features, refer to *8562 Installation Manual for Physical Planning*, GC28-7011.

System power problems

This is the starting point for system power problems when all system power (N mode) is missing or lost.

Attention: Reseating of FRUs is only supported when directed by Product Engineering or a Retain Tip (TDR) applicable to the fault that is being worked.

CAUTION: Servicing of this product or unit is to be performed by trained service personnel only. (C032)

You are here because:

- The system is not operational.
- The Support Element might or might not be operating.
- You were directed here by Chapter 1, “Start,” on page 1 or an online procedure.

The problem can be one of the following:

- Customer power is missing
- The room temperature exceeds 40° Celsius
- **Power Distribution Unit (PDU) power**

  The system is PDU powered. Continue to “PDU system power problems” on page 65.

PDU system power problems

Attention: Reseating of FRUs is only supported when directed by Product Engineering or a Retain Tip (TDR) applicable to the fault that is being worked.

CAUTION: Servicing of this product or unit is to be performed by trained service personnel only. (C032)

__ 1. Check to ensure that the following are true:

- All line cords are properly connected.
- The room temperature is below the maximum of 40° Celsius (104° Fahrenheit).

Are all of the previously listed conditions true?

NO
Go to the next step.

YES
Go to Step “3” on page 65.

__ 2. Correct any problems found. When complete, go to the next step .

__ 3. Go to Chapter 1, “Start,” on page 1, and follow the online service procedures to resolve the other power problems.

If there are no other problems, close the call. For information, see “Closing a call” on page 192.

End of procedure

__ 4. Prepare a meter to measure system voltage.

- **Three-phase AC voltage:** The acceptable three-phase voltage range for 50 Hz or 60 Hz measured phase to phase is 200-240 V AC or 380-415 V AC.

DANGER: An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

Are all voltages acceptable?

NO
Go to the next step.

YES
End of procedure.

__ 5. Have the customer repair the line voltage problem. Recommend that a qualified electrician make the repairs.

End of procedure

__ 6. Call your next level of support for assistance resolving the system power problem.

End of procedure

Replacing a LinuxONE III 8U Reserved Space (FC 0150) SAN switch power jumper cord

CAUTION: Servicing of this product or unit is to be performed by trained service personnel only. (C032)

Before starting this procedure, order the following parts, tools, and materials:

- (1) **P/N 39M5392** - Power Jumper Cord, C13-C20, 9-ft
- (1) **P/N 03JJ394** - Label Sheet for Power Jumper Cords
- (1) **P/N 41U8365** - Clear Tape Strips Sheet
- (1) **P/N 15R8270** - Push-Pull Tool
- (1) **P/N 00RR794** - Hook-and-Loop Cable Tie Wraps “Puck”
- (1) **P/N 00LR054** - Vinyl Tape

Notes:

- This procedure describes removal/replacement of a storage networking switch power jumper cord only. Service of the switch itself is not covered here because that responsibility belongs to the customer.
- This procedure does not include Problem Determination.
- The storage networking switch power jumper cord is replaceable concurrently with IBM Z operation. **However**, all storage and storage networking switch hardware must be removed from the 8U Reserved Space for this procedure in order to gain access to the jumper routing path.

1. Properly shut down and remove all storage and storage networking switch hardware, **except for the storage networking switch power jumper cords**, from the 8U Reserved Space (EIA 23 – EIA 30). This is necessary to allow access to the switch power jumper routing path.

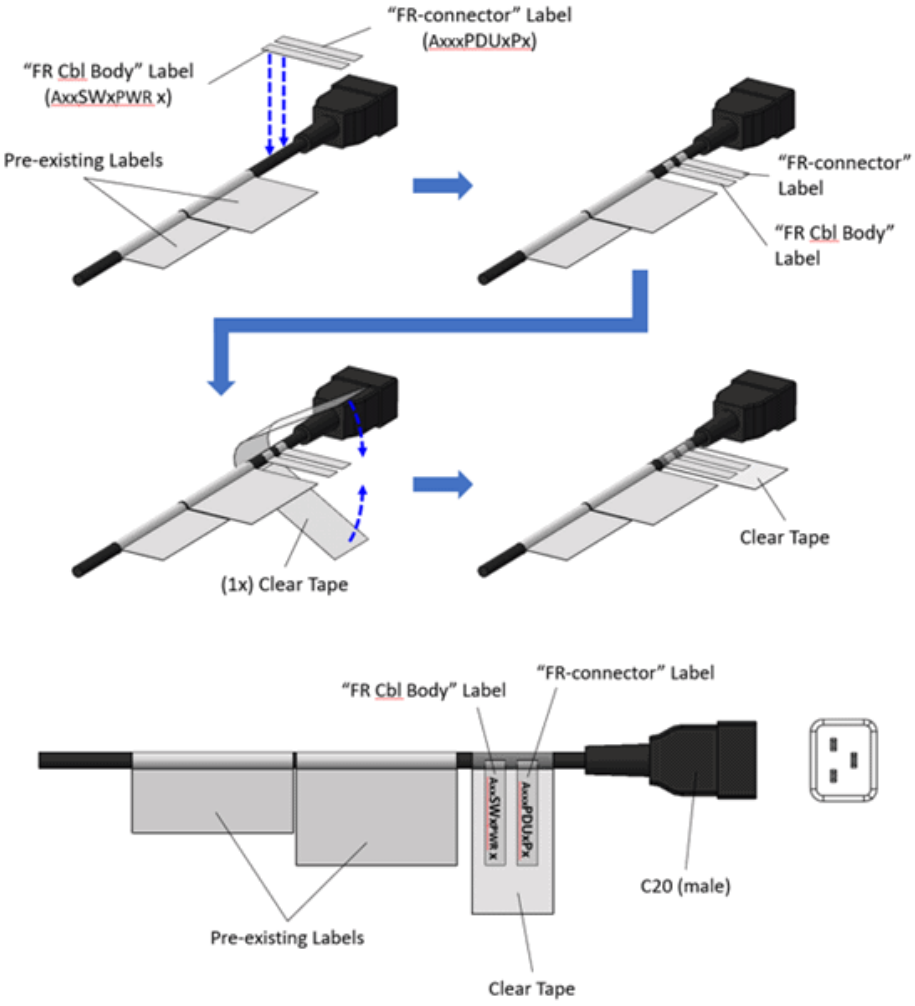
   Note: IBM Z hardware and FS9200 Storage hardware are serviced by IBM. FS7200 Storage and storage networking switch hardware are serviced by the customer. Coordinate shutdown and removal of hardware with all necessary parties.

2. Unplug the failed power jumper from the PDU at the rear of the system.
3. Pull the failed power jumper completely out of the frame side channel from the rear of the system. The other power jumper in that route should remain in place.
4. Match the location ID labels on the failed jumper to a set of labels on the Label Sheet **(P/N 03JJ394)**, as shown below.

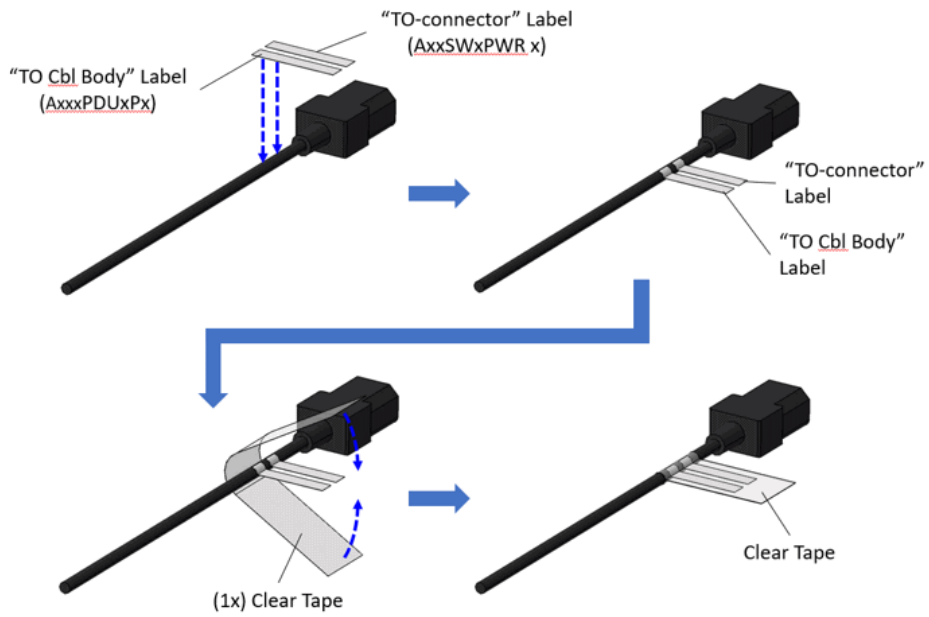


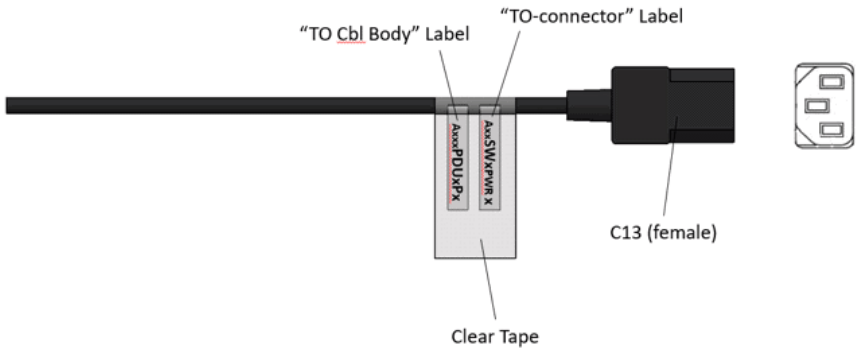
5. Apply the matched set of (4) labels from the Label Sheet **(P/N 03JJ394)** and (2) tape strips from the Clear Tape Sheet **(P/N 41U8365)** to the new Power Jumper **(P/N 39M5392)**, as shown below.

C20 Plug (male) – PDU end of Power Jumper:



C13 Plug (female) – SAN Switch end of Power Jumper:

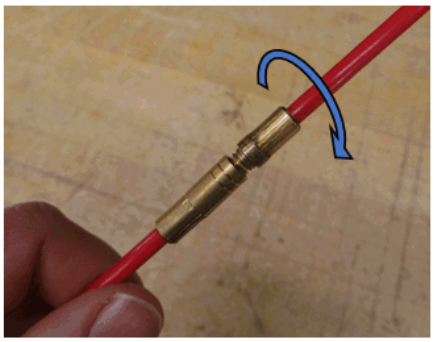




6. Assemble (3) rigid sections of the Push-Pull Tool **(P/N 15R8270)**. Hand-tighten the sections together. Do not use the flexible section or the *keyring* tip.

   Note:





7. Remove (2) pre-cut lengths from the Hook-and-Loop Cable Tie Wraps "Puck" **(P/N 00RR794)**, and affix those pieces together into a single longer length that is at least (7) inches.

8. Depending on the features that are available at the rear of the system frame, do one of the following:
   a. Loosely loop the cable tie from Step “7” on page 68 on the frame’s rear corner post at location N18 or Z18 (or level with the tops of PDU’s 1 and 2), depending on which side of the rack needs the jumper replacement. The loop should be about (1) inch in diameter.

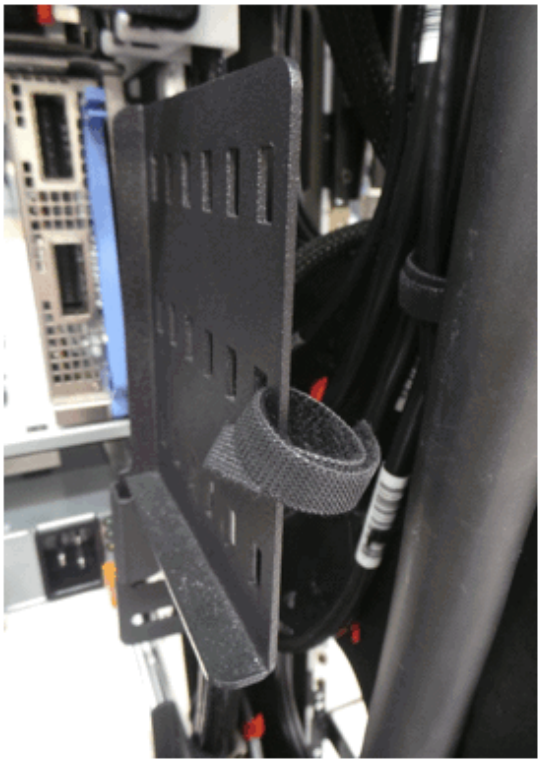


   b. Wrap the cable tie from Step “7” on page 68 around a system line cord at location N18 or Z18 (or level with the tops of PDU’s 1 and 2), depending on which side of the rack needs the jumper replacement, leaving the end of the tie hanging loose.

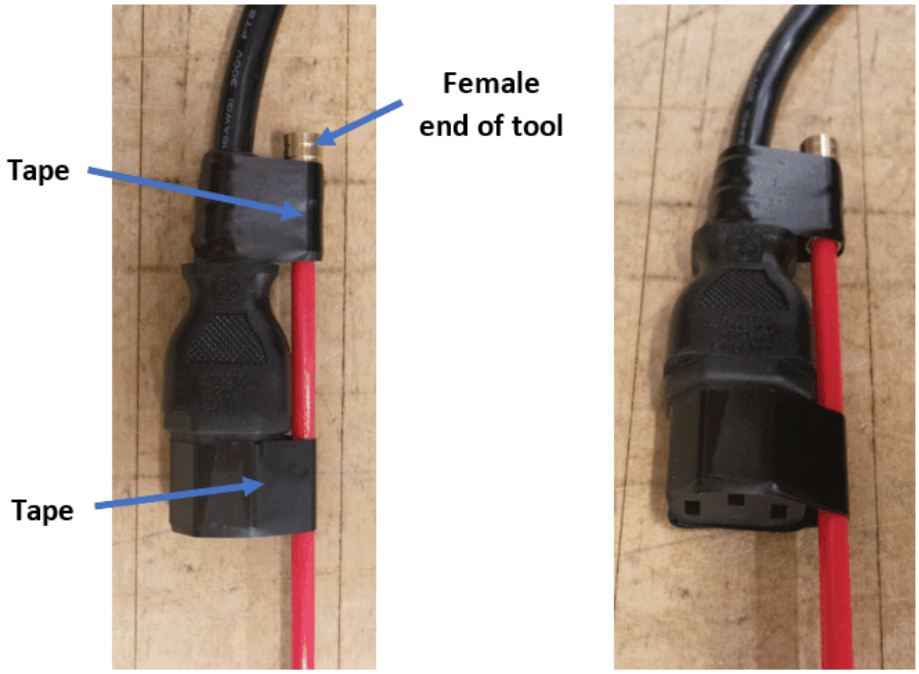


   c. Loosely loop the cable tie from Step “7” on page 68 through a slot on the CPC drawer cable management bracket at location N18 or Z18 (or level with the tops of PDU’s 1 and 2), depending

on which side of the rack needs the jumper replacement. The loop should be about (1) inch in diameter.

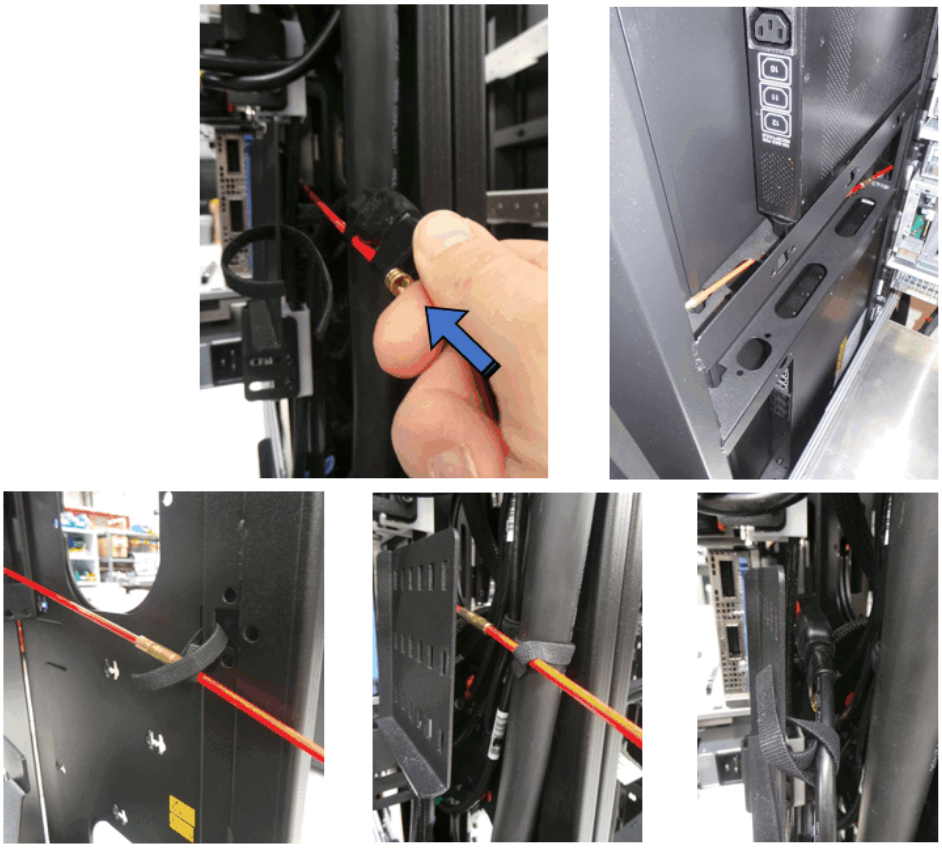


9. Tightly strap the C13 (female) plug end of the new Power Jumper to the female end of the assembled Push-Pull Tool with Vinyl Tape (**P/N 00LR054**, approximately (5) inches long each) **in the (2) locations and in the orientation shown below**. Tape the long side of the plug in line with the Push-Pull Tool, as shown, to help direct it through the holes in the system frame.



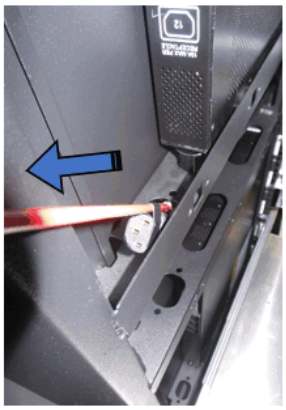
10. From the rear of the system frame, feed the male end of the Push-Pull Tool through the frame's side channel opening directly above the lower PDU, angling the tool upward to exit the top side of the channel through the small cutout behind the PDU. Stop feeding when the tool passes through the

small cutout and hits the hard stop at the back of the PDU cavity. Use the hook-and-loop cable tie positioned in Step “8” on page 69 to temporarily wrap around the cord and keep it from falling during the next step.



11. At the front of the system frame, grasp the protruding end of the Push-Pull Tool with your fingers and pull it toward the front of the frame. The rigid Push-Pull Tool will bend enough to clear the frame members. With an original power jumper already installed, some extra manipulation of the new Power Jumper’s plug end through the frame channel cutout might be necessary. If the Power Jumper plug catches during this action, pause pulling and walk to the rear of the frame to push the Tool/ Jumper past the obstacle. Then return to the front of the frame and resume pulling until the Jumper plug head passes through the channel cutout. Leave about (2) feet of slack hanging out of the channel cutout at the **front** of the frame.









12. Remove all tape from the Power Jumper plug head and the Push-Pull Tool.
13. Re-install all storage and storage networking switch hardware that was removed from the 8U Reserved Space in Step “1” on page 66, except for fillers at the front of the system frame.

    Note: IBM Z hardware and FS9200 Storage hardware are serviced by IBM. FS7200 Storage and storage networking switch hardware are serviced by the customer. Coordinate installation of hardware with all necessary parties.
14. At the front of the system frame, plug the new Power Jumper to the storage networking switch.
15. Re-install all remaining EIA fillers at the front of the system frame.
16. At the rear of the system frame, plug the new Power Jumper to the appropriate PDU receptacle. Either stow any cable slack inside the frame’s side channel or retain it with hook-and-loop cable ties to the side of the frame. **The storage networking switch is now ready to power on.**

End of procedure

Diagnosing power problems with 8U Reserved Space power jumper cords and PDUs

Attention: Reseating of FRUs is only supported when directed by Product Engineering or a Retain Tip (TDR) applicable to the fault that is being worked.

CAUTION: Servicing of this product or unit is to be performed by trained service personnel only. (C032)

Use the instructions in this section when a storage networking (SAN) switch that supports storage hardware in the 8U Reserved Space has indicated a loss of input power to one power supply. In this situation, the customer has verified that the switch is not the issue.

__ 1. Verify that the cable to the power supply is plugged in securely and is in the correct location (including system input).

Is the cable plugged in correctly?

NO

Correct the issues found.

Is the SAN switch power supply getting power now?

NO

Go to Step “2” on page 73.

YES

End of Procedure

YES

Go to Step “2” on page 73.

__ 2. Check the PDU circuit breaker for indication that is has been tripped.

Is the PDU circuit breaker tripped?

NO

Go to Step “3” on page 73.

YES

Reset the PDU circuit breaker.

Is the SAN switch power supply getting power now?

NO

Go to Step “3” on page 73.

YES

Go to Step “5” on page 74.

__ 3. Replace the power jumper cable that is connected to the failing power supply. Use the procedure in “Replacing a LinuxONE III 8U Reserved Space (FC 0150) SAN switch power jumper cord” on page 66.

Is the SAN switch power supply getting power now?

NO

Go to Step “4” on page 73.

YES

End of Procedure

__ 4. Replace the PDU using the Repair and Verify "Open FRU" procedure.

Is the SAN switch power supply getting power now?

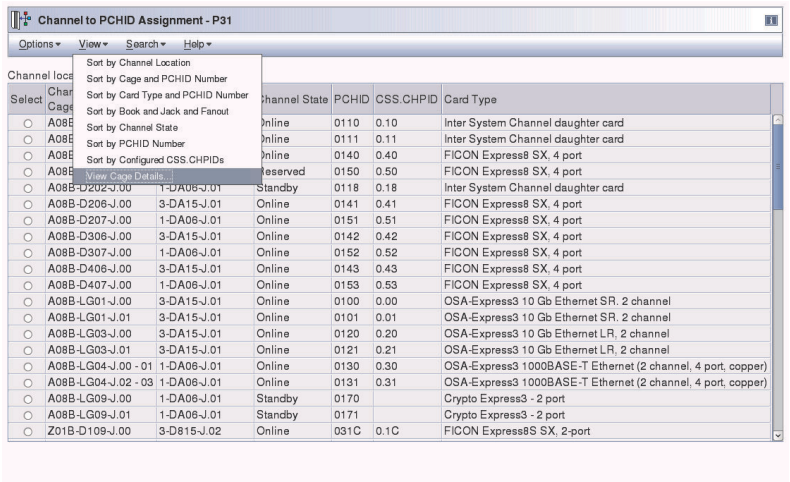
NO

Go to Step “5” on page 74.

YES
End of Procedure

__ 5. Call next level of support.

End of Procedure



- Click **View** and then the desired sort method.

OR

- Click Search and then enter the desired search parameter.
- When you have located the needed information, click Options and then Exit.

The physical interface might be presented in the form of a byte mask number. For example:

Byte mask Converts to
80EB CSS 0 CHPID EB
40EB CSS 1 CHPID EB

If another procedure directed you here, return to that procedure.

End of procedure

Displaying I/O card information

Use this procedure to display information about the I/O cards (channels and OSA) in any of the systems PCIe+ I/O drawers.

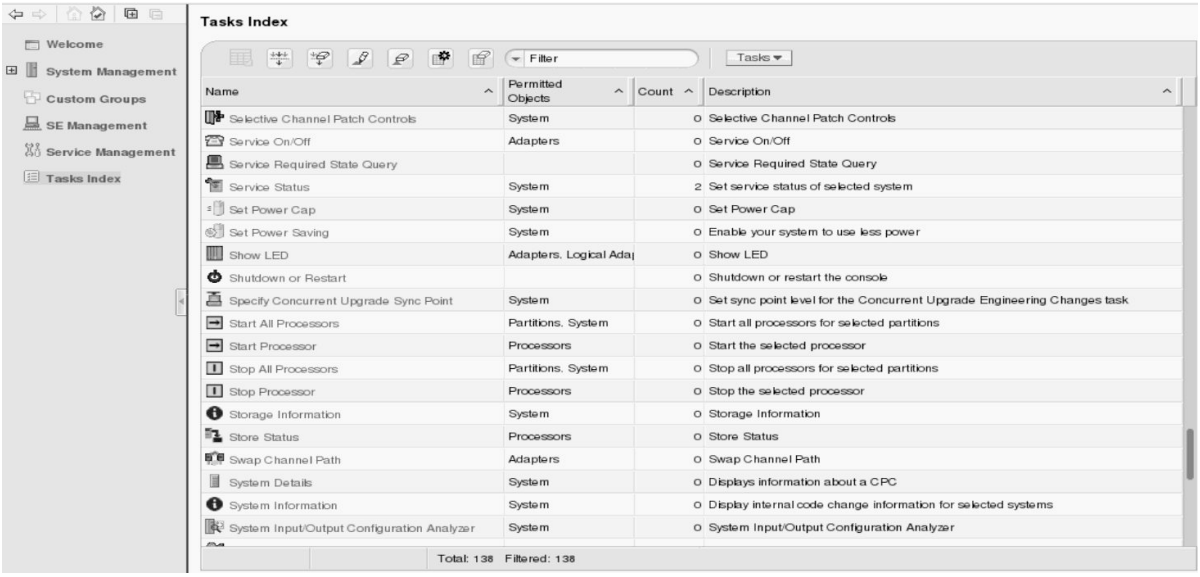
Note: The system power must be on. The Support Element must be powered on and the Licensed Machine Code must be loaded.

__ 1. Access the compact KMM (keyboard, monitor, mouse) from the storage box and assemble for use. For assembly instructions, see “Preparing the compact KMM” on page 11.

__ 2. Login to the Support Element in service mode.

I/O card information can also be displayed from the Hardware Management Console workspace window by clicking **Tasks Index** and **Single Object Operations**.

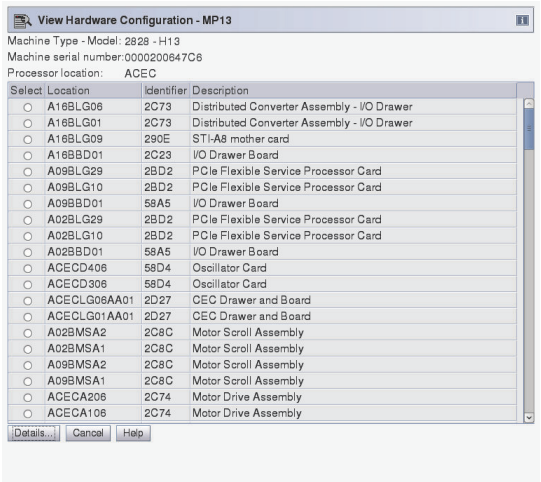
On the Support Element workspace window:



- Click **Tasks Index** on the left navigation pane.
- From the Tasks Index, click **View Hardware Configuration**.

Go to Step “3” on page 182

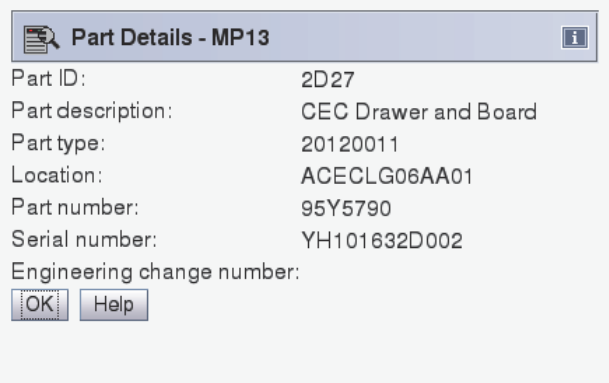
__ 3. On the View Hardware Configuration window:



- Select a location in the table.

- Click **Details**.

__ 4. • Review the information.



- Click **OK**
- Click **Cancel** to exit task.

End of procedure

Secure Execution for Linux (FC 0115)

Secure Execution for Linux® on Z is a new capability introduced with the z15 T02, available for all models of the z15 generation. Engineered to help protect against insider and outsider threats in multi-tenanted cloud environments, it ensures that users, and even system administrators, are unable to access sensitive data in Linux-based virtual environments. Secure Execution for Linux protects the confidentiality and integrity of data at enterprise scale by isolating data at the virtual machine level, and ensuring that only the people within the organization that have a need-to-know have access to data in the clear.

Figure 4 on page 184 provides a visual representation of the Secure Execution for Linux feature being implemented on a standard Kernel-based Virtual Machine (KVM). With Secure Execution for Linux:

- KVM guests are fully isolated and protected from the KVM Hypervisor.
- The Hypervisor administrator can still manage and deploy workloads, but is unable to view any guest data.
- Multiple tenants and/or applications that are running on a shared LPAR have fully-isolated environments.
- Protected intellectual property and proprietary secrets.
- ***z15 holds specific keys in trusted (persistent) memory.***
- ***Secure Execution for Linux is enabled through Feature on Demand (FOD) and is dependent on CP Assist for Cryptographic Functions (CPACF) code being present in the system.***

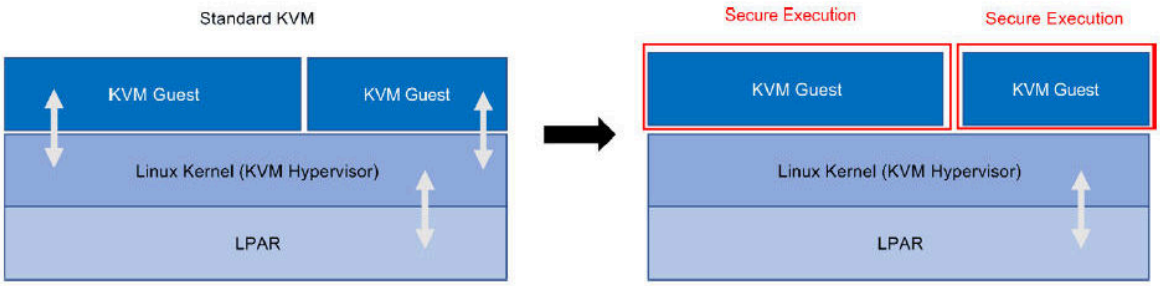


Figure 4. Secure Execution for Linux - KVM implementation

For more information, refer to https://www.ibm.com/support/knowledgecenter/linuxonibm/com.ibm.linux.z.lxse/lxse_c_intro.html.

Secure Execution-related keys

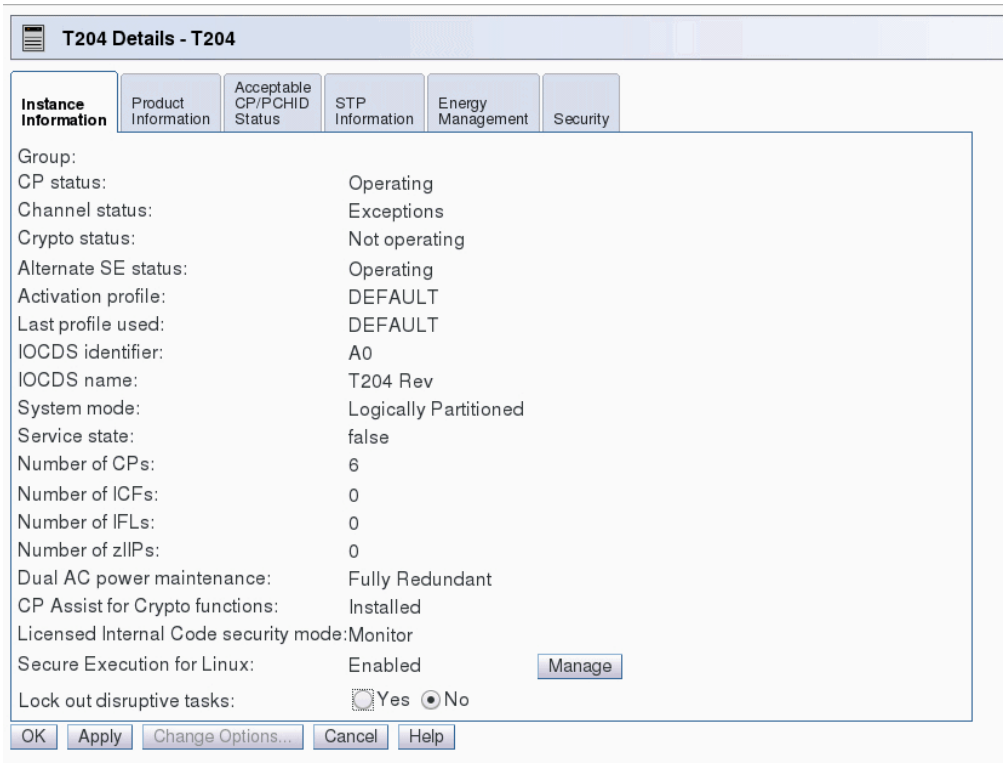
Secure Execution is built with encryption, and with encryption, comes key usage. Review the following information to familiarize yourself with the specific keys that are used for Secure Execution.

- There are two keysets (the same common process, but different scope):
  - **Host-specific**: Host Key
  - **HyperProtect-specific**: Global Key
- Transfers between IBM and systems in the field are done using a *key bundle file*.
- A *key bundle file* contains encrypted Host or Global keys, and decryption is dependent on the Central Processor (CP) in a given system.

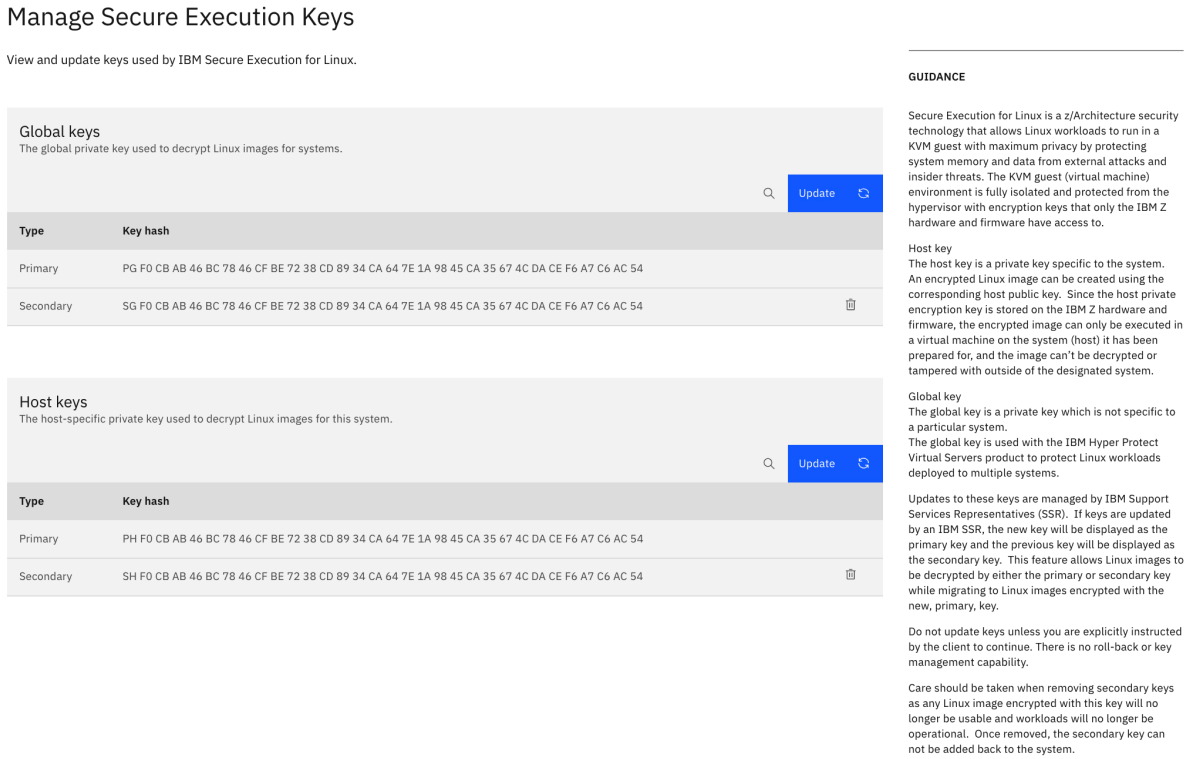
  Note: The bundle file contains the list of CPs that are supposed to be present on the system. At least **one** functional CP is needed to decrypt.
- A *key bundle file* is host-specific (identified by Host serial number).

Manufacturing (MFG) is responsible for generating these *key bundle files* on demand and uploading them to the Remote Support Facility (RSF).

On the Support Element, the **System Details** page displays the current status of Secure Execution for Linux, as shown in the following panel:



From the System Details page, click **Manage** to open the Manage Secure Execution Keys panel, as shown in the following panel:



Required service procedure for Secure Execution

If Secure Execution for Linux is included on the initial system order, the required Secure Execution keys are imported at the time of system or order fulfillment and no SSR action should be needed.

Note: If the feature is ordered after the system is shipped, the key load will occur as part of the FOD install in the system.

If this feature is ordered later, however, a manual key load must be completed by the SSR at the time of any service action. This manual task is also required for systems that do **not** have the Remote Support Facility (RSF) installed.

The following provides a high level overview of the service procedure that might be required for Secure Execution:

1. Complete the necessary service action. Some examples include:
   - CPC drawer add (see Figure 6 on page 187 for flowchart representation)
   - CPC drawer replacement (see Figure 7 on page 188 for flowchart representation)
   - CP SCM replacement (see Figure 8 on page 188 for flowchart representation)
2. Push the latest Vital Product Data (VPD) to Manufacturing (MFG).

   Note: Pushing the VPD to MFG triggers MFG to generate a new key bundle file for that specific system.
3. If the system has RSF installed, MFG uploads the latest key bundle file. You must then retrieve the latest key bundle from RSF.
4. If the system does **not** have RSF installed, you must contact the Support Center to retrieve the latest key bundle file.
5. Once retrieved, you must navigate to the Manage Secure Execution Keys panel on the Support Element (click **Manage** on the System Details page) and click **Update** to import the latest key bundle file to the system.

   IMPORTANT:

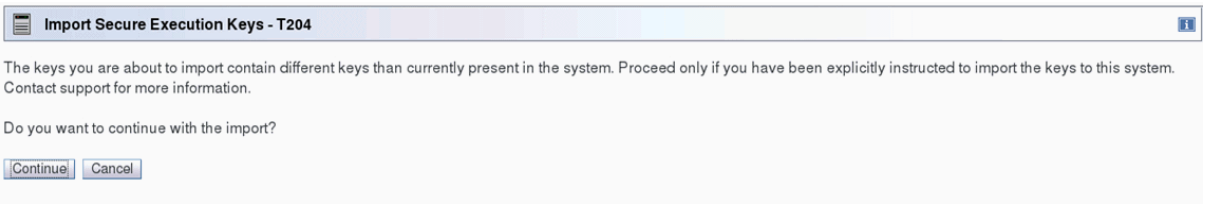
   - See Figure 10 on page 189 for a flowchart representation of the *Import Secure Execution Key* procedure.
   - If you do not complete the key import within 72 hours, the system goes into a service required state. If the import task returns an error or warning, return to Step “2” on page 186 and repeat this procedure.
   - If a CPC drawer replacement service action is completed and the import task fails, returning a *No keys are present* error message, the system goes into a service required state. In this case, return to Step “2” on page 186 and repeat this procedure.
   - If you import a Global and Host Key, whose Public Key differs from the keys that are present on the system, you will be required to perform a *key roll* when doing a key bundle import. **This is a special procedure and should only be performed if instructed to do so!**

     A key roll can be caused by the following two scenarios:

     – If the signed keys in the key bundle file have expired based on the policy after a given period of time.

     – If any private key, in the Secure Execution context, is potentially leaked.

     If prompted to perform a key roll, the following panel will be displayed and you must STOP the key import unless you are explicitly instructed by the client to continue. There is no roll back or key management capability.



When a new key is introduced, a grace period starts, during which the revoked key remains present on the system. The grace period duration is defined by the partition owner, the workload provider, and/or the machine owner.

Note: This is a procedural grace period that is neither enforced nor set in the system.

See Figure 9 on page 189 for a flowchart representation of the new key bundle service scenario.

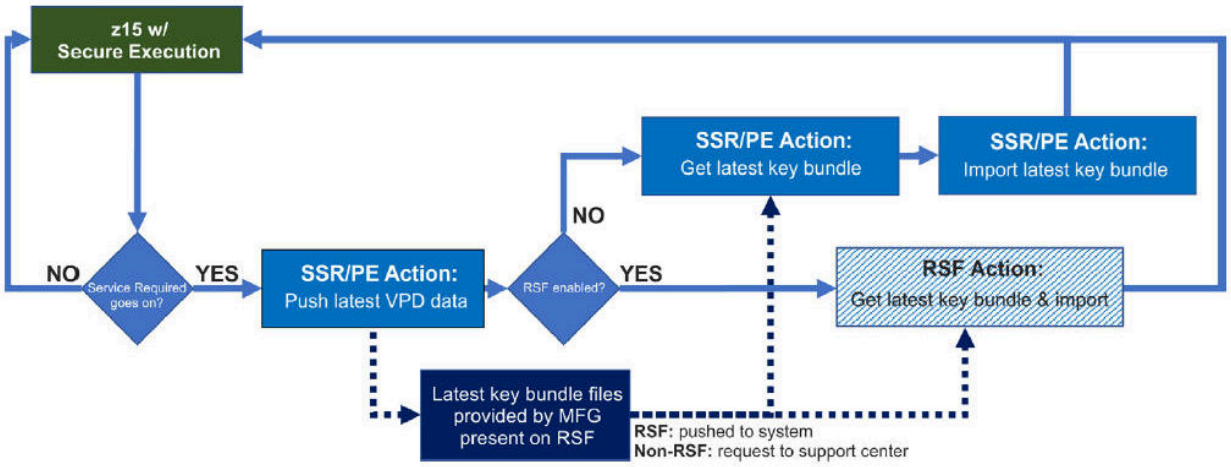


Figure 5. Service Required status flow

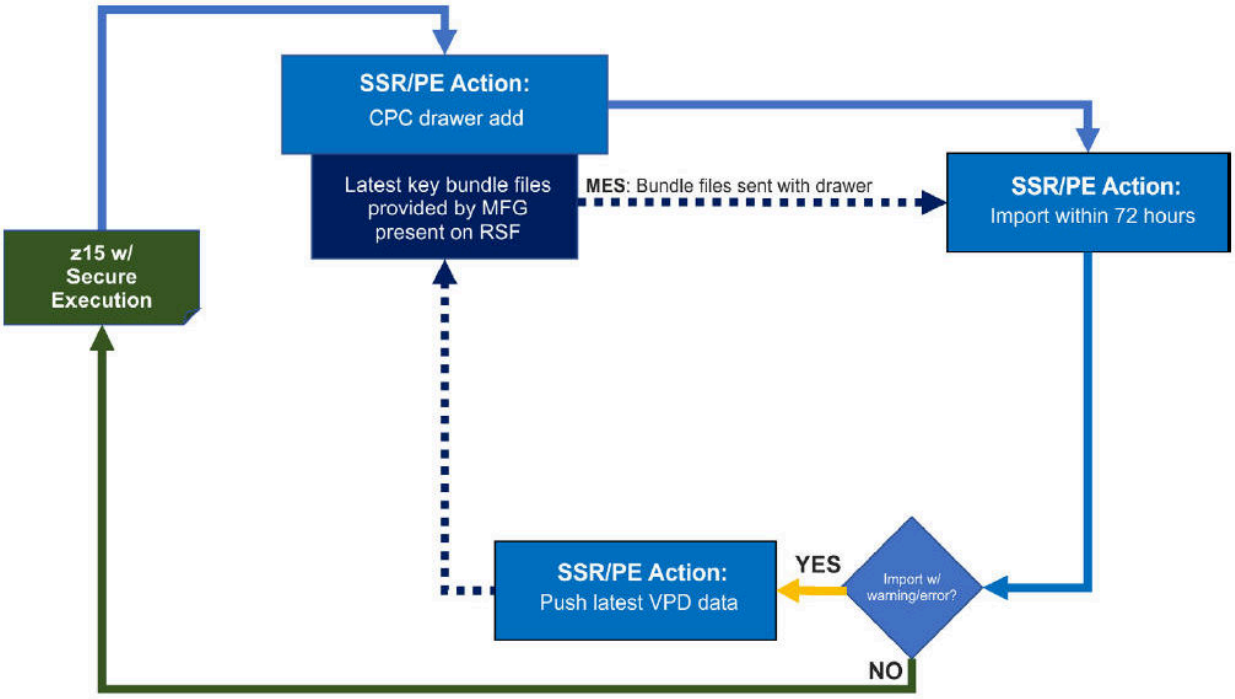


Figure 6. Service scenario flowchart - CPC drawer add

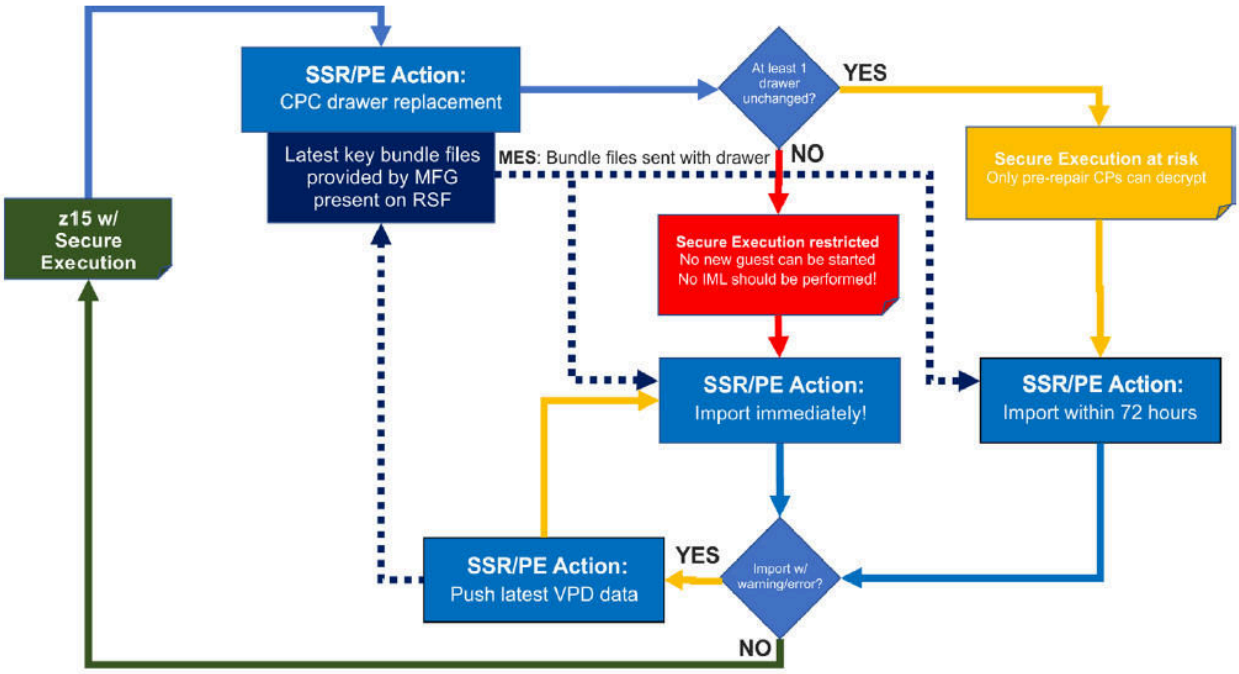


Figure 7. Service scenario flowchart - CPC drawer replacement

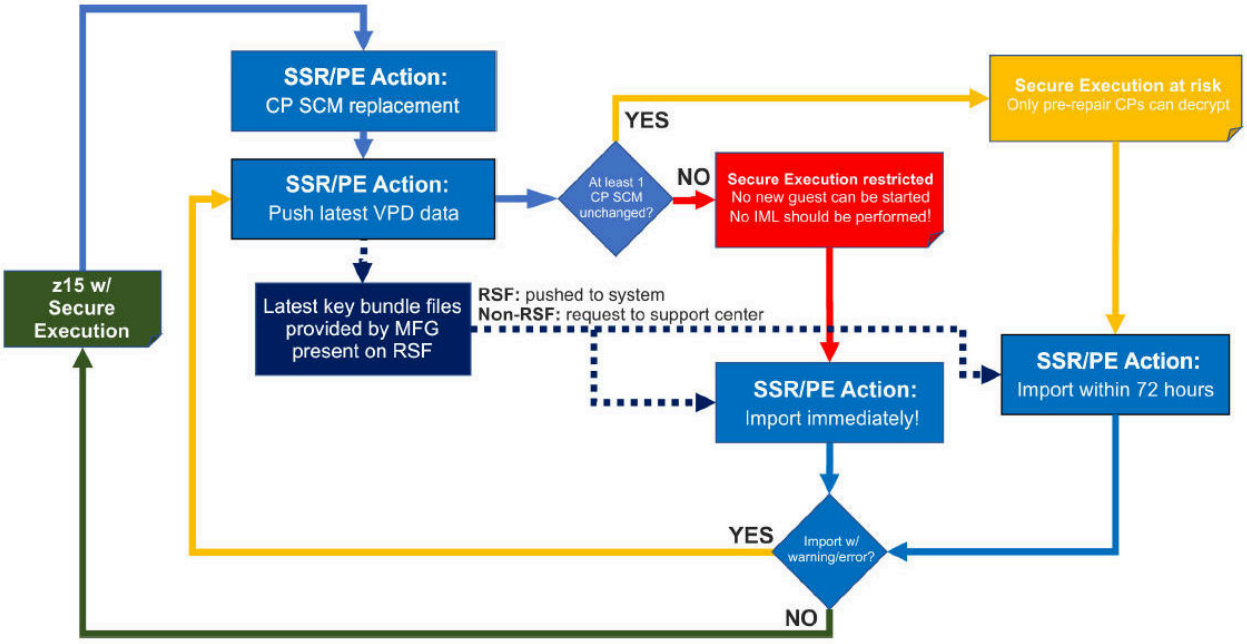


Figure 8. Service scenario flowchart - CP SCM replacement

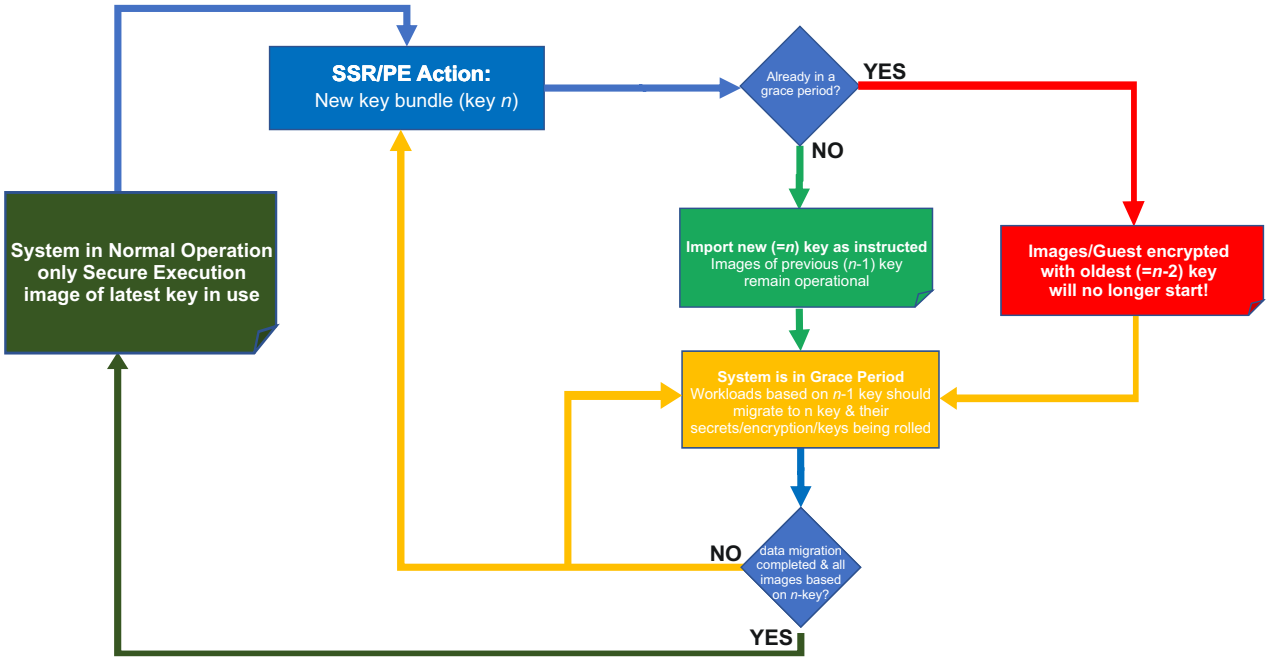


Figure 9. Service scenario flowchart - New key bundle

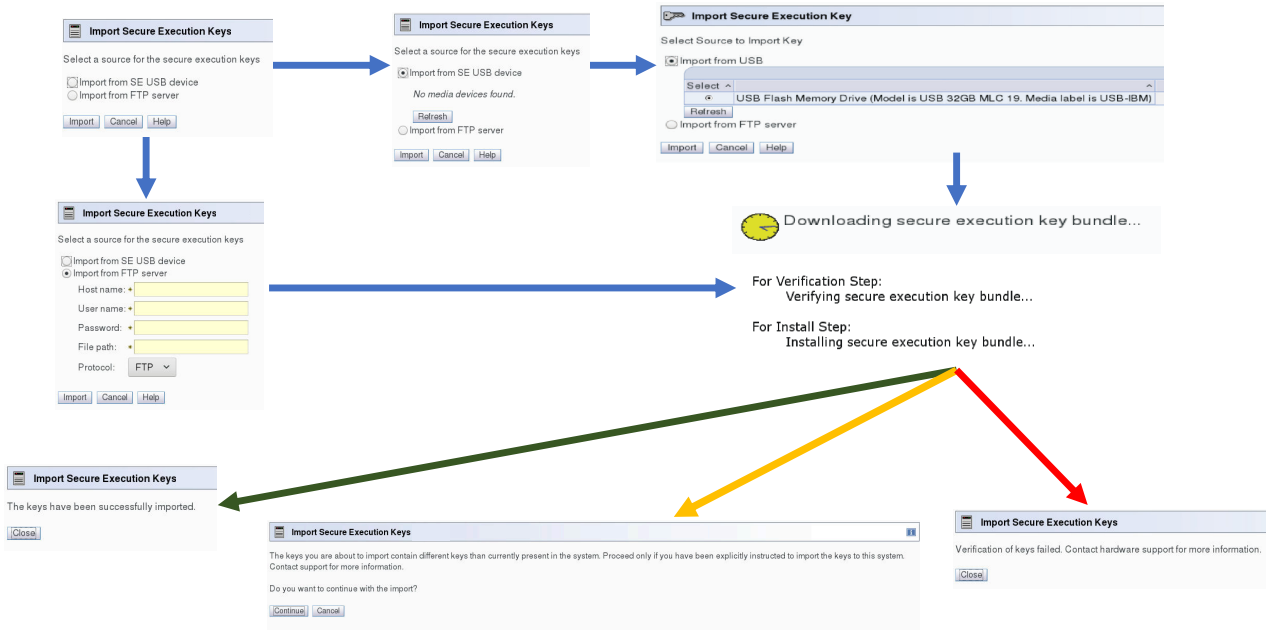


Figure 10. Import Secure Execution Keys task flow

System shutdown

Use this procedure to avoid loss of data on the Hardware Management Console or Support Element hard drives when customer power must be removed from a Hardware Management Console or a system.

Prepare the Hardware Management Consoles and Support Elements for power off as follows:

__ 1. Did an online procedure direct you to shut down a Support Element and power off the system?

YES
Go to the next step.

NO
Go to Step "4" on page 190.

__ 2. Are you supposed to shut down the system?

YES
Go to the next step.

NO
Go to Step "7" on page 191.

__ 3. This step prepares the system and Support Elements for power off.

Have the customer verify that operations are complete on the system to be powered off.

Have the customer deactivate the system from the Hardware Management Console workspace window as follows:

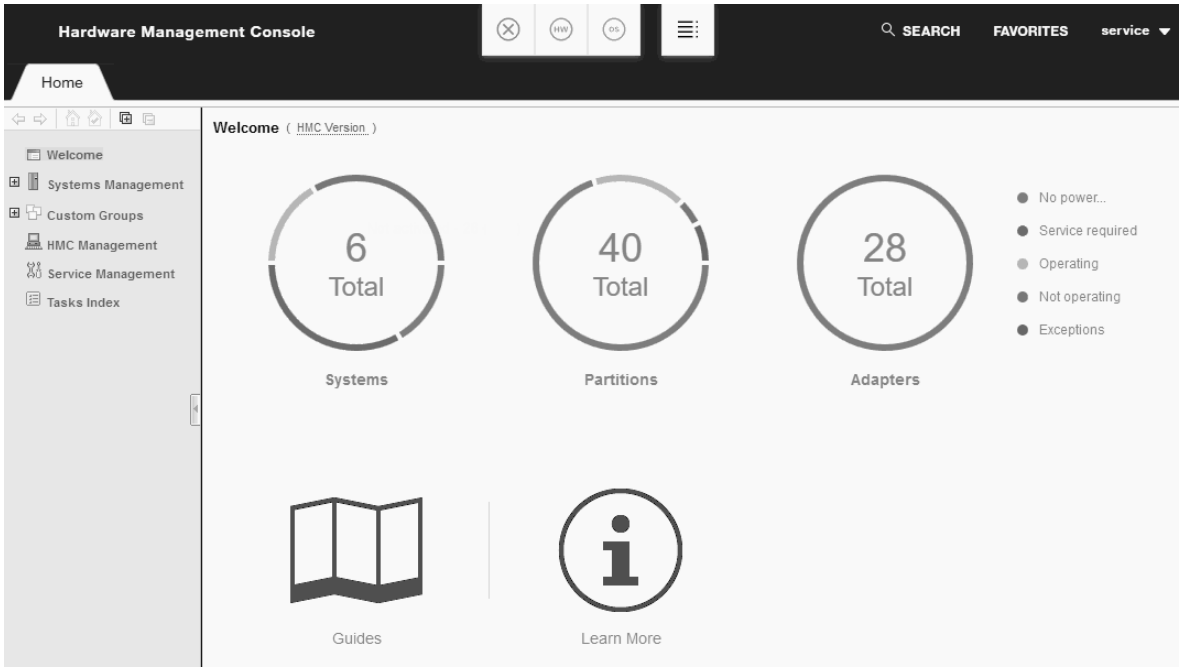
- Click **Tasks Index** on the left navigation pane.
- From the Tasks Index, click **Deactivate**.

Repeat until all CPCs to be powered off are deactivated; then, go to Step "7" on page 191.

__ 4. **Logging Off**

On each Hardware Management Console that is to be powered off:

- Click **Tasks Index** on the left navigation pane.



- From the Tasks Index, click **Power Off or Restart**.

IBM Adapter for NVMe

The IBM Adapter for NVMe (Non-Volatile Memory Express) feature uses NVMe to provide IBM LinuxONE fast access to data stored on Solid State Drives (SSDs). NVM Express is an open collection of standards and information to fully expose the benefits of non-volatile memory in all types of computing environments from mobile to data center. NVMe is designed from the ground up to deliver high bandwidth and low latency storage access for current and future NVMe technologies.

Note: The IBM Adapter for NVMe is available with Model LT2 model only.

IBM Adapter for NVMe details:

- Only available with IBM LinuxONE
- A zero port, single PCHID adapter card
- Order the adapter in increments of 1 feature, with maximum of 16 features
  - Customer can order the IBM Adapter for NVMe1.1 (**FC 0448**).

IBM provides the adapter card into which a vendor NVMe SSD can be plugged. The NVMe SSD is customer supplied and installed into the IBM adapter card by the IBM service representative.

Important:

Once installed, any future servicing of the customer supplied NVMe SSD requires a service contract to be in place. The servicing or replacement of the NVMe SSD by an IBM service representative is **not** covered under Warranty or Maintenance Agreement.

Attention: The selection and purchase of the SSDs in this feature is the responsibility of the client. The *IBM LinuxONE NVMe white paper (70019570-USEN-00)* (https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=70019570USEN&) lists the performance of SSDs that IBM has tested for LinuxONE. IBM can only comment on the functionality of the SSDs that have been tested. The client assumes all risk in, and IBM is not responsible for, the use of SSDs as the functionality or performance may vary.

Attention: SSRs must never take possession of the customer-supplied NVMe SSD devices because they might contain client data. When the server is discontinued, the NVMe SSD devices must be removed and given to the client.

Notes:

- Hot plug or removal is **not** supported. Use IBM support system when installing or removing SSDs.
- The NVMe SSD must meet the following optional specification items:
  - Support 64 bit PCIe addressing
  - Support Host Controlled Thermal Management
  - Support Thermal Throttling
  - Support single port PCIe x4 only
- Linux on Z:
  - Ubuntu 18.04 LTS with service
  - IBM is working with its Linux distribution partners to include support in future distributions releases
- Specifications:
  - NVM Express 1.2b
  - PCI Express Base Specification Rev 3.1
  - Enterprise SSD Form Factor Version 1.0a (Single Port Only)

  - PCI Express Card Electro-Mechanical Spec. Rev 3.0
- Form Factor:
  - U.2 2.5'' (15 mm) Form factor U.2-compatiable connector (formerly SFF-8639)
  - 25W max power consumption

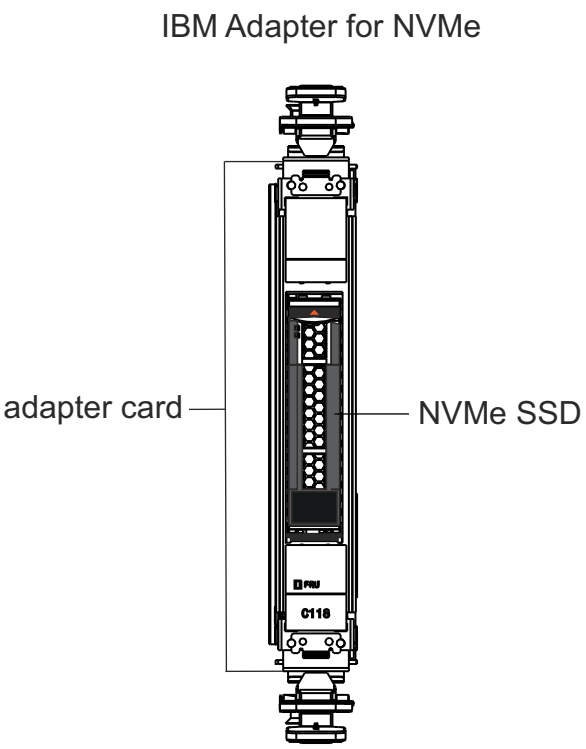


Figure 34. IBM Adapter for NVMe feature

The IBM Adapter for NVMe feature resides in the PCIe+.

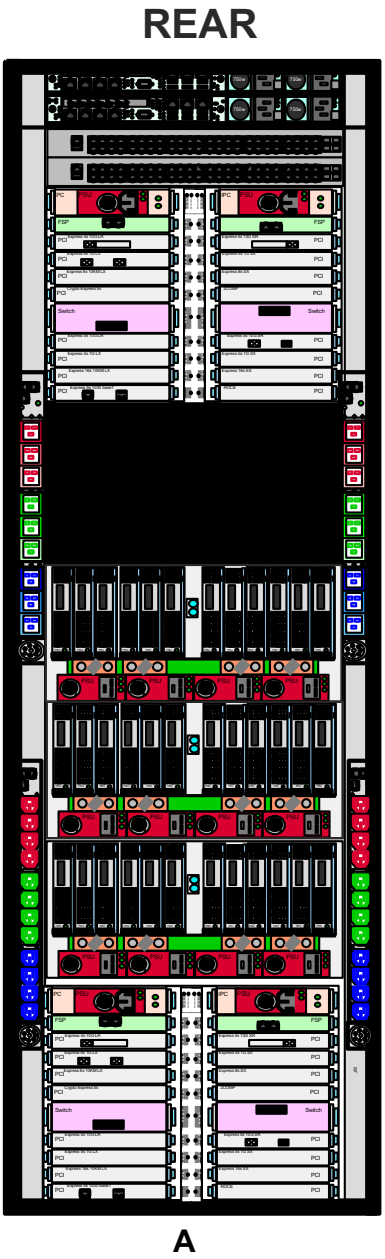


Figure 36. Typical Model GT2 frame configuration for PDU powered systems with three CPCs and two PCIe+ drawers (rear view)

16U and 8U Reserved Space features

The 8562 server provides the following reserved space features.

16U Reserved Space (FC 0151)

16U reserved feature reserves EIA location A23 through A38. This feature is available with IBM z15 Model T02 and IBM LinuxONE III Model LT2.

The reserved space is available for the following storage integration solution only. Use of this space for any other purpose is not permitted.

- One IBM DS8910F Storage Model 993
  - Machine types supported: 5331, 5332, 5333, 5334

  Note: DS8910F Model 993 integration with a z15 T02 system requires FC 0611 to be ordered. DS8910F Model 993 integration with a LinuxONE III LT2 system requires FC 0621 to be ordered.

You must verify that the compliance certifications in your geography are complete before ordering and integrating the storage. Use the link provided in the **IMPORTANT** notes below to review the system's Exception Letter.

8U Reserved Space (FC 0150)

8U reserved feature reserves EIA location A23 through A30. This feature is only available with IBM LinuxONE III Model LT2.

The reserved space is available for the following storage integration solutions only. Use of this space for any other purpose is not permitted.

- 0, 1 or 2 IBM FlashSystem 9200 (Models 9846-AG8 or 9848-AG8) storage devices, with 0, 1 or 2 IBM Storage Networking SAN32C-6 switches (8977-T32)
- 0, 1 or 2 IBM FlashSystem 7200 (Model 2076-824) storage devices, with 0, 1 or 2 IBM Storage Networking SAN32C-6 switches (8977-T32)
- 1 IBM FlashSystem 9200 (Models 9846-AG8 or 9848-AG8) storage device and 1 IBM FlashSystem 7200 (Model 2076-824) storage device, with 0, 1 or 2 IBM Storage Networking SAN32C-6 switches (8977-T32)

Note: Cisco DS-C9132T-MEK9 or DS-C9132T-K9 (MDS 9132T) switches are also supported.

IMPORTANT:

- Storage devices installed in the 8U and 16U Reserved Spaces will follow the terms and conditions of the Storage M/T and are not considered part of the z15/LinuxONE system.
- You MUST review the z15 T02and LinuxONE III LT2 Exception Letter on Resource Link (https://www.ibm.com/servers/resourcelink/lib03020.nsf/pages/exceptionLetters?OpenDocument) to understand when this offering completed its compliance certification in your geography. Failure to do so may result in a non-compliant machine configuration.

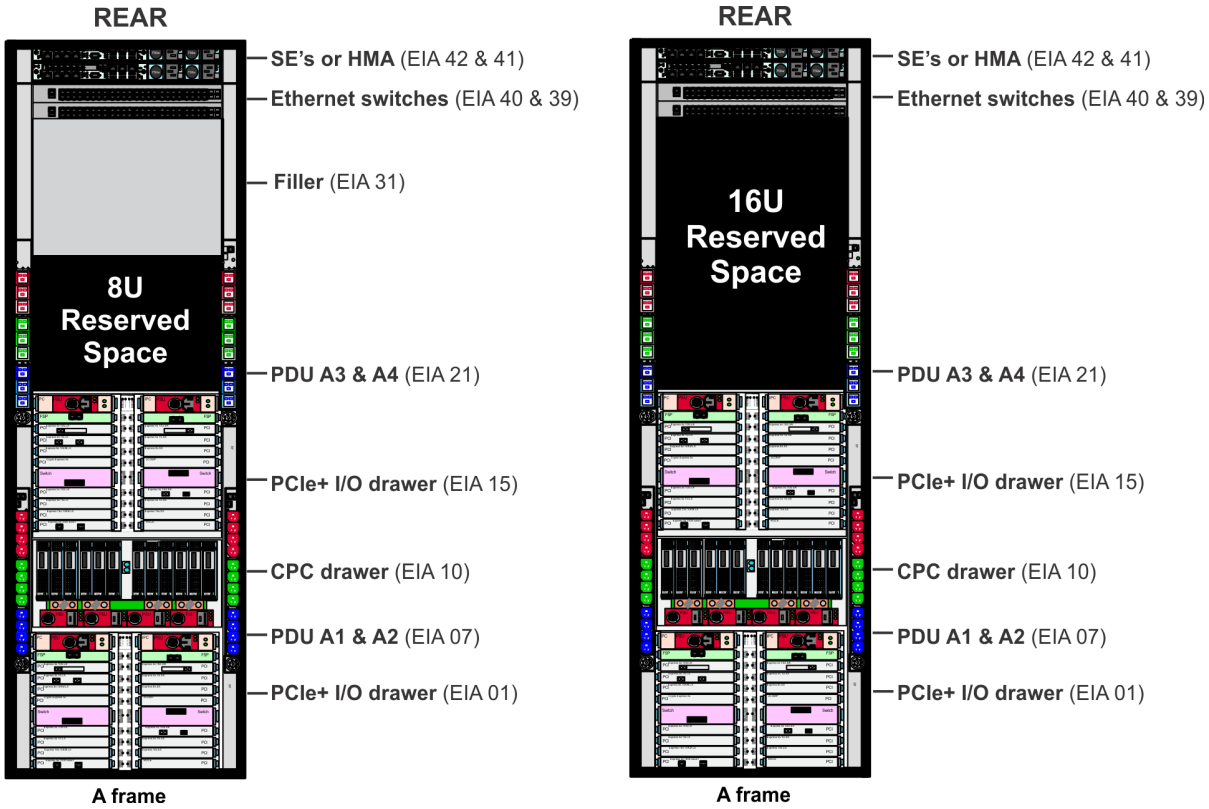


Figure 37. Installed IBM components for 8U and 16U Reserved Space features (Model T02 or Model LT2)

Notes:

- The Reserved Space features are not supported on a system with two or more CPC drawers installed.

- With the 16U Reserved Space feature installed, the 8562 can support a maximum of 2 PCIe+ I/O drawers. With the 8U Reserved Space feature installed, the 8562 can support a maximum of 2 PCIe+ I/O drawers.
  - Five ballasts (P/N 01KL444) may be installed in the bottom of the frame to prevent the machine from tipping.
- The IBM Z or LinuxONE system order does not include the actual storage or switch hardware components with the following exception: Storage networking switch power jumper cords are pre-installed as part of the LinuxONE 8U Reserved Space feature because these cords must be installed prior to any other hardware in that reserved space.
  - **IMPORTANT:** The IBM SSR will first complete the installation of the z15 Model T02 or LinuxONE Model LT2 and turn it over to the client operation. Next, the Business Partner or customer can install storage if the 16U Reserved Space (FC 0151) or 8U Reserved Space (FC 0150) feature has been ordered.

16U and 8U Reserved Space power requirements

The 8562, when configured with the 16U or 8U Reserved Space feature, must be configured with single phase power. The Reserved Space features are not supported on a system with three phase power.

Notes:

- Some IBM Z maintenance service procedures, for example replacing a PDU, may interrupt power to the IBM Storage equipment that is installed in the Reserved Space. SSRs must inform the client of this and coordinate these Z service activities with the client before interrupting power to the IBM Storage equipment that is installed in the Reserved Space.
- Performing a *Restart console and power cycle the system operation* (also referred to as SEPO) on the Z server will **not** cycle power to the IBM Storage equipment installed in the Reserved Space.

16U Reserved Space (FC 0151)

Supports one IBM DS8910F Storage Model 993.

Power cords plugged into the following locations cannot be unplugged or moved. Failure to follow this warning may adversely impact the operation of the 8562, including a possible system outage.

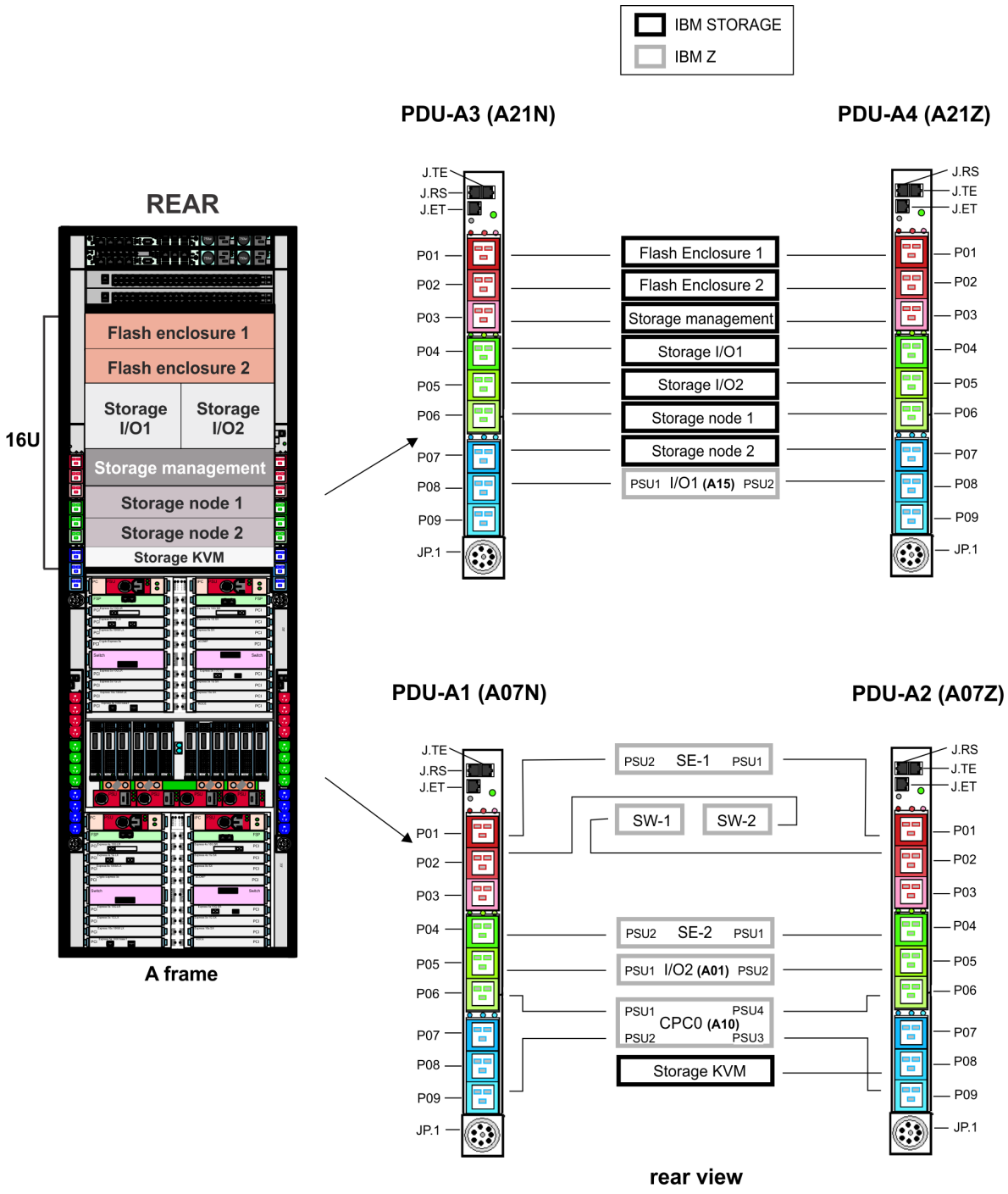


Figure 38. PDU plugging locations for 16U Reserved feature

8U Reserved Space (FC 0150)

Supports one or two IBM FlashSystem 9200 (or 7200) storage devices, with one or two IBM Storage Networking SAN32C-6 switches (8977-T32).

Power cords plugged into the following locations cannot be unplugged or moved. Failure to follow this warning may adversely impact the operation of the 8562, including a possible system outage.

Note: Power jumper cords for storage networking switches are to be serviced by an IBM Z authorized service provider even though the switches themselves are customer-serviced. Replacement of these power jumpers requires removal of all hardware in the 8U Reserved Space in order to gain access to the routing path for the cords.

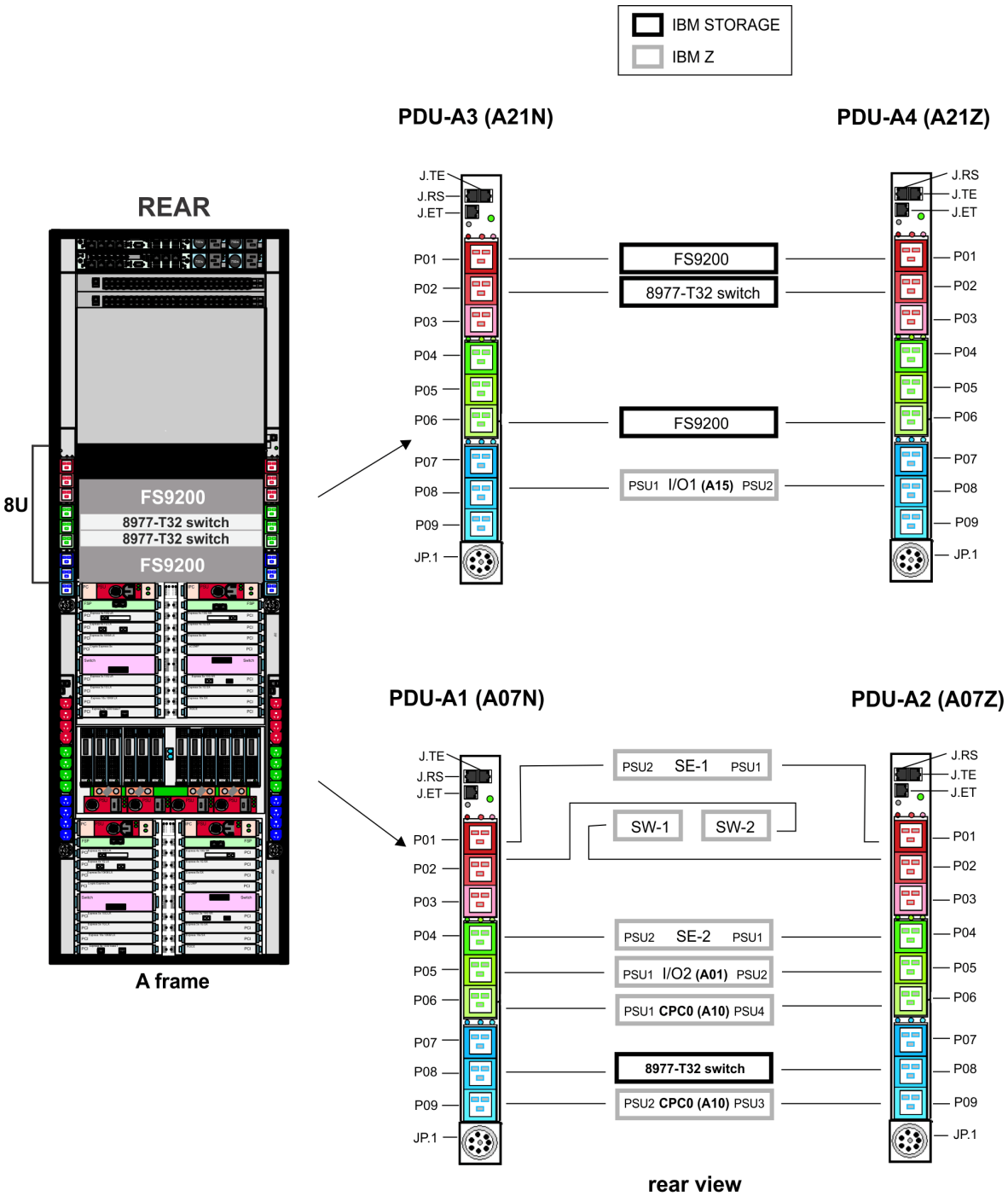


Figure 39. PDU plugging locations for 8U Reserved feature

Note: PDU power jumper cords for 8977-T32 switches (or alternate Cisco switches) are pre-installed as part of the LinuxONE system because these cords must be installed prior to any other hardware in the 8U Reserved Space. Due to complex routing, these power jumpers are to be serviced by an IBM Z authorized service provider even though the switches themselves are customer-serviced.

Locations in the frames

The location of components in the system is identified by using part or all of the following 12-character code, where "a" represents an alphabetic character and "n" represents a numeric character:

Table 40. Location Fields

Field 1	**Field 2**	**Field 3**
anna	aann	aann

Field 1 contains a one character frame identifier, a two digit vertical position identifier, and a one character horizontal position identifier. The vertical and horizontal location is referred to as "Unit".

Field 2 contains a two character code to identify the component type followed by two numeric characters to identify the value.

Field 3 is used when further information about Field 2 is required. It also uses a two character code to identify the component type followed by two numeric characters to identify the value. The codes for Field 2 and Field 3 are defined in "Field 2 and 3 Location Code" later in this section.

Additional symbolic location designations are used for system components that cannot be described by using the 12-digit scheme or that are outside of the frame. These are defined in "Locations Outside of Grid" later in this section.

Frame: Each frame string has a unique serial number that applies to all frames and CPC in the string. The frame with the first 3 CPC drawers is always frame "A". If the system has a 4th and/or 5th CPC drawer, those are always in frame "B".

Examples of frame locations are given in: “Overview of system configurations” on page 386.

Unit: The unit is a three digit code to specify the vertical and horizontal position of a component within a frame. Unit identifies the position of a component’s lower left corner (when viewed from the front of the frame).

The first two digits specify the height from the bottom of the frame in Electronic Industries Association (EIA) units.

Note: One EIA unit is 44.45mm (1.75 inches).

The next digit specifies horizontal position by an alphabetic character (excluding I and O). Positions "A" through "M " are at the front of the frame, positions "N" through "Z" are at the rear. The horizontal position is used to locate components that are not the full width of the frame (do not start at "A"). Locating strips inside of the frame show the horizontal and vertical positions. Figure 40 on page 393 shows the horizontal positions.

Locations Outside of Grid: Some of the system components are outside of the frame location grid. These components are assigned fixed unit locations. The fixed unit locations are:

Unit A00M
Hardware Management Console

Unit A41C
Support Element (Lower Support Element)

Unit A42C
Support Element (Upper Support Element)

MSAU
LAN_CONNECTOR_DEVICE

FRU lists containing FRUs for the Hardware Management Console and Support Element use character strings following the fixed location identifier.

```
A99S_FIXED_DISK
```

The example indicates the hard disk drive in the Support Element.

Cable Location Labels: System cables have a label on each end to specify where they attach to the system. The labels use R, U, C, and J fields for frame, unit, card, and jack. Figure 41 on page 395 shows an example of a label.

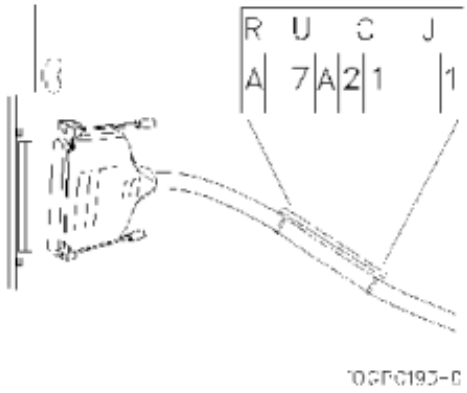


Figure 41. Label on a System Cable

View of system in frames

This section shows the locations of the major components in the system. The method for locating other components within the frame starts at “Locations in the frames” on page 392.

The major components for **PDU powered** systems are:

- System Power Supply - Power Distribution Unit (PDUs)
- CPC drawers
- PCIe+ I/O drawers
- Support Elements or a Hardware Management Appliance

View of 8562 frame (Model T02 and Model LT2)

The following image shows the Model T02 and Model LT2 19-inch frame with a single CPC drawer and four PCIe+ I/O drawers.

Activate EC

The **Activate EC** option is the second step of the CUEC process.

From the **Concurrent Upgrade Engineering Changes (EC)** window:

1. Select **Activate EC**. (This option is available only if your user ID is assigned the service representative task role.)
2. Then click **OK** to proceed.
3. This window allows you to choose which bundles you want to activate on the Engineering Changes (ECs).

   Activate all preloaded bundles
   To activate all the preloaded bundles, select **Activate all preloaded bundles**.

   Activate a specific preloaded bundle
   To activate only a specific preloaded bundle, select **Activate a specific preloaded bundle**, then specify the bundle level in the **Bundle level** field. This option is not available to systems before Version 2.14.0.

   OK
   To proceed with the selection you made, click **OK**.

   Cancel
   To return to the previous window without running with the selections you made, click **Cancel**.

   Help
   To display help for the current window, click **Help**.
4. The following three phases are part of the activation process before the activation of the upgrade is complete:
   a. “Preparation” on page 135
   b. “Transition” on page 135
   c. “Completion” on page 135.

The following three phases are included for the activation of the upgrade.

Preparation

The preparation phase makes sure that the following requirements are verified before the code switch starts:

- The concurrent patch feature is enabled.
- The CUEC GA^{n} switch point requirements are met (if the internal code changes applied to the GA^{n} code on the Primary SE changed since the CUEC preload).
- No pending conditions from previous CUEC or concurrent patch sessions exist.

Transition

The transition phase is the heart of the CUEC activate because it is in this step that the GA^{n+1} code is applied in each firmware subsystem memory. The Support Element (SE) is the first subsystem to have its GA^{n+1} code that is loaded and this is done by running a CUEC Alternate SE switch. This causes the GA^{n+1} code to become the new Primary SE while the GA^{n} code becomes the new Alternate SE. The GA^{n+1} new Primary SE must restart and perform a warm-start resynchronization with the other firmware subsystems. Once the Primary SE completes its warm-start synchronization, it serially triggers each of the subsystems to load its GA^{n+1} firmware.

Completion

The completion phase includes a hardware message that could be displayed directing the operator to invoke two tasks to complete the GA^{n+1} transition from those exception firmware subsystems.

- **Query Channel/Crypto Configure Off/On Pending** - this task allows the operator to see which channels and cryptos must be configured offline and put back online in order to get the GA^{n+1} code loaded.
- **Query Coupling Facility Reactivations** - this task informs the operator whether any coupling facility (CF) partitions must be reactivated in order to move the CFCC code for that partition to GA^{n+1}.

Query function availability from last activate

Once the CUEC activate is complete the final step of the CUEC process is performed.

From the Concurrent Upgrade Engineering Changes (EC) window:

1. Select **Query function availability from last activate**, then click **OK**.
2. The Query Function Availability from Last Activate window is displayed. A list of functions which are not yet available or have not yet been enabled after the CUEC process completed is displayed in the window.

   or

   A message window is displayed, indicating that all functions are enabled and available.

This option addresses the exception cases where one or more new GA^{n+1} functions cannot be made available during the CUEC activation process. Some possible reasons why these functions are not available include:

- Not all subsystems have moved to the GA^{n+1} code level. The operator can use the **Query Channel/Crypto Configure Off/On Pending** and **Query Coupling Facility Reactivations** Support Element tasks to ensure that the GA^{n+1} code level transitions have completed. Once this GA^{n+1} code level validation is completed, the operator can invoke the **Query Function Availability from Last Activate** option to see what functions are still not available.
- One or more exception functions might require some additional action to finalize the enablement/availability for those functions. This could include an action such as configuring off/on for certain types of channel or processors.

See Resource Link (www.ibm.com/servers/resourcelink) for descriptions of the new functions available for the GA^{n+1} release. They can also inform you of any additional actions that are required to fully enable/make available any functions that can be displayed on the **Query Function Availability from Last Activate** window.

Completing the upgrade

Once you have permanently moved to the GA^{n+1} level on the Primary system, you need to bring the Alternate system to the GA^{n+1} level. To accomplish this upgrade, proceed with the following:

1. Use the **Backup Critical Data** task on the GA^{n+1} system.
2. Using the CUEC AROMs, perform a hard disk restore on the GA^{n} system.
3. From the **Restore Critical Data** window, select the backup file that is needed to restore the critical data, then click **OK**.

Scheduling a Remote Code Load firmware update

The IBM z15 supports the new Remote Code Load for IBM Z Firmware (Remote Code Load) feature. This feature allows an IBM Service Support Representative (SSR) to remotely schedule one or multiple Single Step Code Load firmware updates on a Hardware Management Console (HMC) or Support Element (SE) that can be monitored remotely. See Figure 4 on page 137 for an overview of this process. After you (the SSR) are assigned to the one-time Remote Code Load firmware update, you are responsible for scheduling, managing, and coordinating the Remote Code Load firmware update until it is installed and successfully scheduled. After the Remote Code Load is successfully scheduled, it is the Remote Code Load monitoring team's responsibility to monitor the status of the Remote Code Load firmware update.

Note: Screen captures provided throughout this section are for example purposes only.

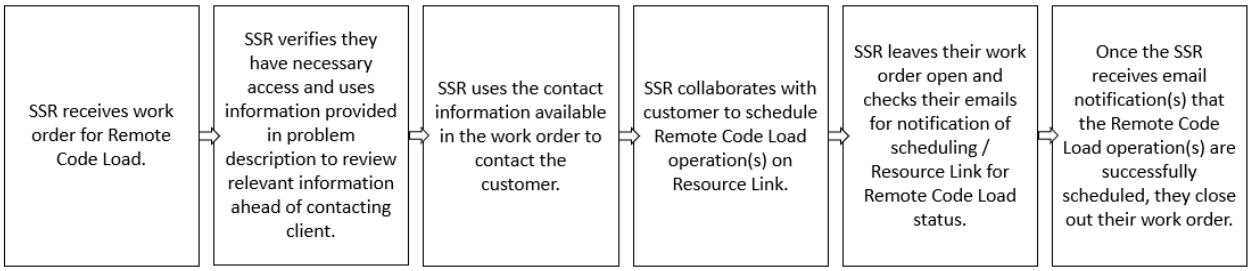


Figure 4. Remote Code Load firmware update process flow

Planning prerequisites

This section describes the planning prerequisites that are required before you schedule the Remote Code Load.

Before contacting the customer

- Ensure that you (the SSR) have the appropriate Resource Link machine information and Remote Code Load permissions before you work with the customer. Refer to the steps in “Scheduling a Remote Code Load” on page 142. If you need additional contact information, send an email to reslink@us.ibm.com and request access to all machine access and Remote Code Load editor access.

  Note: You are initially informed of the Remote Code Load from a Work Order Dispatch from IBM Support. Now, you can contact the customer. See the following figures for an example of the work order procedure.See the following figure for an example of a CSP (Cognitive Support Platform) work order for a Remote Code Load request.

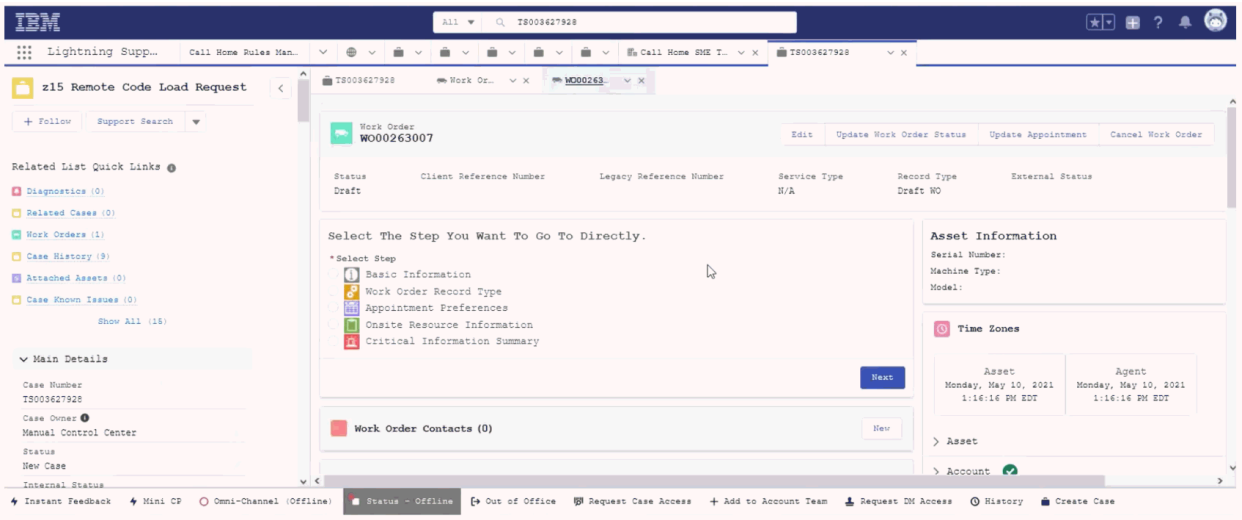


Figure 5. CSP work order for a Remote Code Load request

See the following figure, which displays an example of the Remote Code Load work order feed. As you scroll down the right side of the window the problem description appears and includes additional items such as date and time, bundle level.

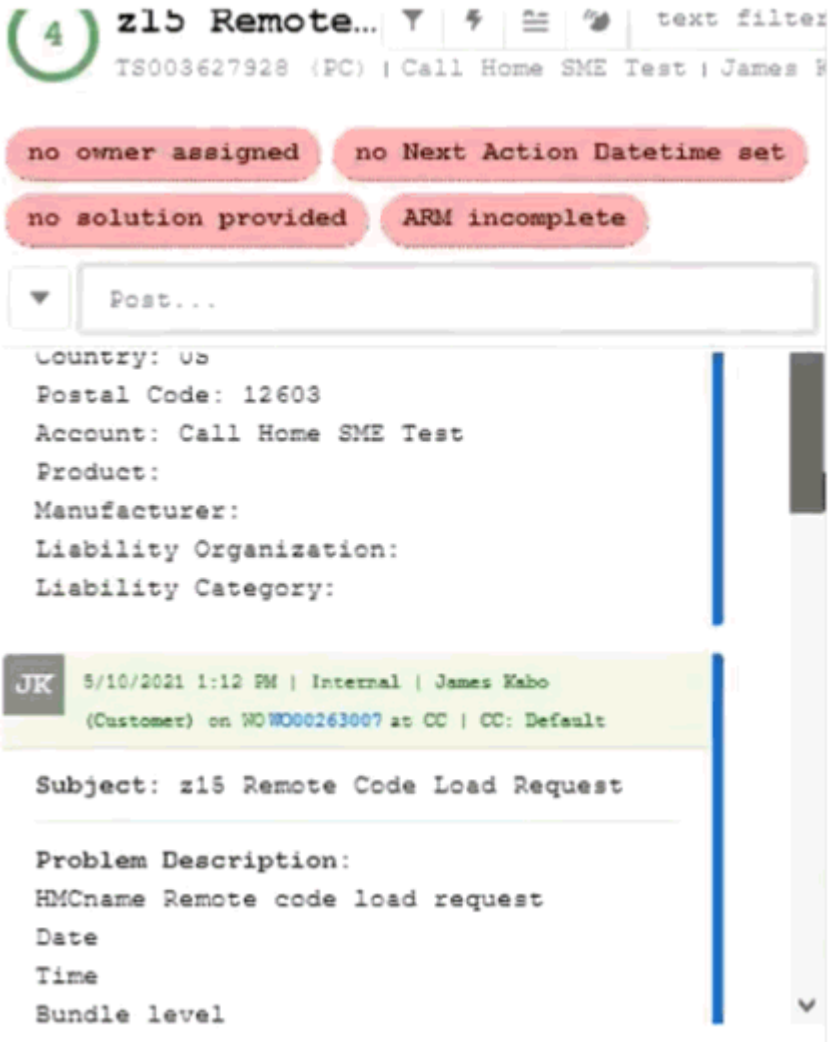


Figure 6. Remote Code Load problem description

Technical requirements and best practices

See Table 3 on page 139 for the technical requirements and Table 4 on page 140 for the best practices when you are installing firmware updates on an HMC or on an SE.

Table 3. Technical requirements

Remote Code Load on an HMC	Remote Code Load on an SE
• Targeted HMC must adhere to the following technical requirements: – Using the **View Console Information** task, ensure that bundle level H25 or above is installed. – Using the **Customize Outbound Connectivity** task, ensure that the **Enable the local console as a call-home server** option or the **Use discovered call-home server consoles** options are selected, or both options are selected. – Using the **Customize Remote Service** task, ensure that the **Enable remote service requests** option is selected. – Using the **Customize Remote Service** task, ensure that the **Authorize automatic service call reporting** option is selected.	• Targeted SE must adhere to the following technical requirements: – Using the **System Information** task, ensure that bundle level S38 or above is installed. – Using the **Remote Service** task, ensure that the **Enable remote service requests** option is selected. – Using the **Remote Service** task, ensure that the **Authorize automatic service call reporting** option is selected. – Using the **Manage Remote Support Requests** task, then selecting **Options**, then **View All Call Home Servers**, verify that one or more HMCs are acting as a call-home server for the SE. – SE must be in a healthy state by viewing **Systems Details** or go to the **Service Required State Query** task. An SE should not be in a **Service Required** state. – SE must not have any uncleared pending conditions before attempting to schedule the Remote Code Load firmware update. Verify by using the **View Internal Code Changes Summary** task.
• All HMCs acting as call-home server consoles for the HMC (including the HMC targeted if acting as a call-home server for itself) must adhere to the following technical requirements: – Using the **View Console Information** task, ensure that bundle level H25 or above is installed. – Using the **Customize Outbound Connectivity** task, ensure that the **Enable the local console as a call-home server** option is selected. – Using the **Customize Remote Service** task, ensure that the **Enable remote service requests** option is selected. – Using the **Customize Remote Service** task, ensure that the **Authorize automatic service call reporting** option is selected. – Appropriate network configuration for call-home (See *Integrating the Hardware Management Console's Broadband Remote Support Facility*, SC28-6986, for setting up and testing the network configuration.)	• All HMCs acting as call-home servers for the SE must adhere to the following technical requirements: – Using the **View Console Information** task, ensure that bundle level H25 or above is installed. – Using the **Customize Outbound Connectivity** task, ensure that the **Enable the local console as a call-home server** option is selected. – Using the **Customize Remote Service** task, ensure that the **Enable remote service requests** option is selected. – Using the **Customize Remote Service** task, ensure that the **Authorize automatic service call reporting** option is selected. – Appropriate network configuration for call-home (See *Integrating the Hardware Management Console's Broadband Remote Support Facility*, SC28-6986, for setting up and testing the network configuration.)

Table 3. Technical requirements (continued)

Remote Code Load on an HMC	Remote Code Load on an SE
• Satisfy the ability to perform internal code changes and call-home during the process by: – Not allowing SERVICE or PEMODE user roles to be logged on during the Remote Code Load firmware update. – Using the **Authorize Internal Code Changes** task, ensure that the **Do not allow installation and activation of internal code changes** option is not selected.	• Satisfy the ability to perform internal code changes and call-home during the process by: – Using the **Service Status** task, ensure that the **Disable service status** option is selected. – Not allowing SERVICE or PEMODE user roles to be logged on during the Remote Code Load firmware update. – Using the **Authorize Internal Code Changes** task, ensure that the **Do not allow installation and activation of internal code changes** option is not selected.

Table 4. Best practices

Remote Code Load on an HMC	Remote Code Load on an SE
• HMCs are required to be updated before the SEs to ensure that HMCs are always, at a minimum, the same level or above the highest level SE that they manage. • Recommended that at least one HMC is acting as a call-home server, other than the HMC that the Remote Code Load firmware update is on. • Validate that there are no unresolved issues for the system the customer is targeting to install MCLs that prevent MCL installation. • Ensuring the target system is at a bundle boundary. Not residing at H*XX*+. • Do the MCLs the customer specified that they want to install on their system include Channel, Crypto, or OSA MCLs, which would prevent successful installation if there are uncleared pending conditions? If so, confirm with the customer that they do not have uncleared pending conditions on their system. • Check for known issues against the install on their system that would cause MCLs to not install successfully (due to MCLs on hold, bundle not targetable for install, MCL alerts, known issues encountered when installing MCLs, etc.)	• All HMCs acting as call-home servers must be local to the SE to avoid any communication issues. • All HMCs acting as call-home servers have the **Report loss of communication** option selected for the SE from the **Change Object Definition** task. • SEs updated to a level equal to or less than the lowest level of the HMC managing it. • Recommended one or more call-home HMCs other than the HMC that was scheduled through. • Validate that there are no unresolved issues for the system the customer is targeting to install MCLs that prevent MCL installation. • Ensuring the target system is at a bundle boundary. Not residing at S*XX*+. • Do the MCLs the customer specified that they want to install on their system include Channel, Crypto, or OSA MCLs, which would prevent successful installation if there are uncleared pending conditions? If so, confirm with the customer that they do not have uncleared pending conditions on their system. • Check for known issues against the install on their system that would cause MCLs to not install successfully (due to MCLs on hold, bundle not targetable for install, MCL alerts, known issues encountered when installing MCLs, etc.)

Scheduling requirements

- The SSR must schedule the Remote Code Load firmware update to take place within a 48-hour and 45-day timeframe out from the time they submit the scheduling request.
- Remote Code Load firmware updates that are on different systems cannot be scheduled within four hours of one another (only one system can be updated at a time).

- Multiple upcoming Remote Code Load firmware updates cannot be scheduled targeting the same machine. If a Remote Code Load firmware update is successfully scheduled for a machine, it must reach completion or be canceled before attempting to schedule another Remote Code Load firmware update.
- The time that you want for the Remote Code Load firmware update to take place must be in the local time zone of the system that you are targeting to install the MCLs on.

  Note: The SSR asks you to specify the time zone of the system that you are targeting to install the MCLs on. This information does not dictate the time zone the Remote Code Load firmware update takes place in. If you provide inaccurate time zone information, it still schedules the time that you provided in the local time of the system that you are targeting to install the MCLs on.

While contacting the customer

- Before proceeding with submitting the Remote Code Load schedule request, confirm the following with the customer:
  - Has the customer reviewed the Remote Code Load technical requirements section available in the *Remote Code Load for IBM Z Firmware (Manage Remote Firmware Updates task)* technical note?
  - If so, have they ensured that their environment complies with the technical requirements?

    Note: For initial Remote Code Load requirements set-up: Does Resource link show the customer having any HMCs below H25 in their datacenter? If so, you need to confirm with the customer that these HMCs are not defined as call-home servers to the system, they are targets to install MCLs on, to prevent any Remote Code Load call-home issues.
  - Anything else that needs to be specifically confirmed with the customer based off the "Technical requirements and best practices" on page 139.
- Receive/validate the following information by email or telephone from the customer:
  - System identification information for the machine that requires the firmware update.
    - For a Remote Code Load firmware update for an HMC:
      - CPC serial number associated with the HMC
      - Machine name of the HMC
      - Backup location preference (FTP or USB).
    - For a Remote Code Load firmware update for an SE:
      - Serial number of the SE
      - Serial number and machine name of the HMC used to generate the authorization token.

        Note: The backup location that is used for an SE is the Primary/Alternate HDD (even if backup to FTP is configured).
  - Targeted code bundle (such as: H*XX* for HMC, S*XX* for SE).
  - Date/Time that you want for the Remote Code Load firmware updates, and the time zone of the system that the customer is targeting to install MCLs on.

    Note: This is scheduled in the time zone configured for the system that the customer is targeting to install MCLs on. The Remote Code Load firmware update can be scheduled within 48 hours and 45 days of the scheduling request being submitted, as long as you schedule the Remote Code Load firmware update before the authorization token expires.
  - A valid authorization token.
    - This authorization token is generated on the HMC that you perform the Remote Code Load firmware updates on or it is on a local HMC managing a system that you want to perform the Remote Code Load firmware updates on.
    - This authorization token expires after seven days from generation with regard to scheduling a session. If the session is scheduled within the seven-day window, the session should be bound between 48 hours and 45 days from the day it is scheduled.

- Request the customer contact name, email, telephone number, and preferred contact method.

– **Note:** If a customer needs help understanding which HMCs to generate tokens on, see "Authorization token usage rules or restrictions" on page 142.

– Additionally, the following information can be obtained and provided in the **Comments** section of the Remote Code Load page on Resource Link:

- Service window

  Note: Additional time needs to be added to the service window, above the amount of time you would have used for a traditional Single Step Code Load firmware update. This needs to be communicated for the customer's expectations.

- Customer contact preferences
- Miscellaneous information

– Verify with the customer if they want to open a proactive Change Window to expedite SSR access if manual, onsite, support actions are required.

Authorization token usage rules or restrictions

Some authorization token usage rules or restrictions that need to be considered include the following:

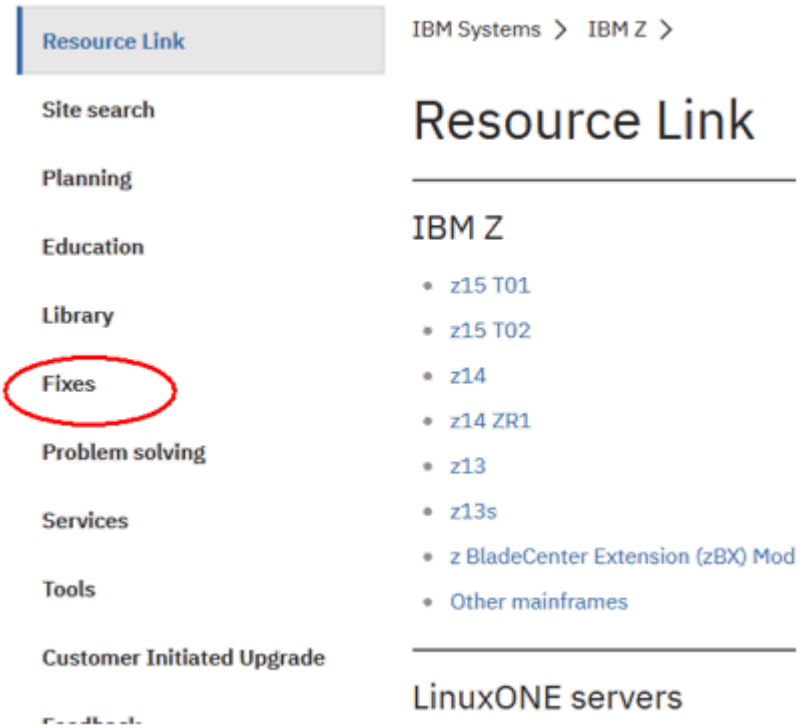
- One authorization token that is generated on an HMC can be used to schedule multiple Remote Code Load firmware updates. This is limited to one staged or scheduled Remote Code Load firmware update per CPC that the HMC manages, in addition to one for that HMC.

  Note: The same authorization token can be used on the same system twice if the initial scheduling failed and the authorization token has not expired.
- If multiple tokens are generated on the same HMC, all tokens are valid for scheduling a Remote Code Load firmware update until they expire. However, only the most recently generated token is displayed on the **Manage Remote Firmware Updates** task on the HMC.
- To schedule a Remote Code Load firmware update on an HMC, the authorization token must be generated on that same HMC. One HMC cannot be used to generate a token and schedule a Remote Code Load firmware update for another HMC.

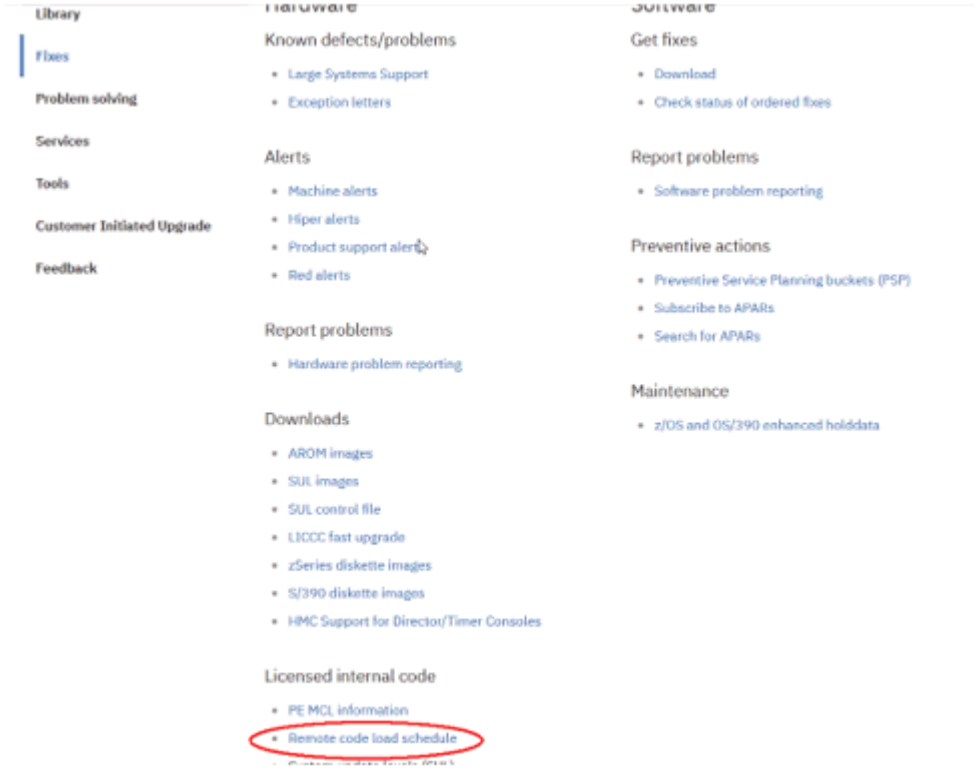
Scheduling a Remote Code Load

This section describes the required steps for scheduling the Remote Code Load firmware updates. Use **Resource Link** to schedule and monitor the Remote Code Load.

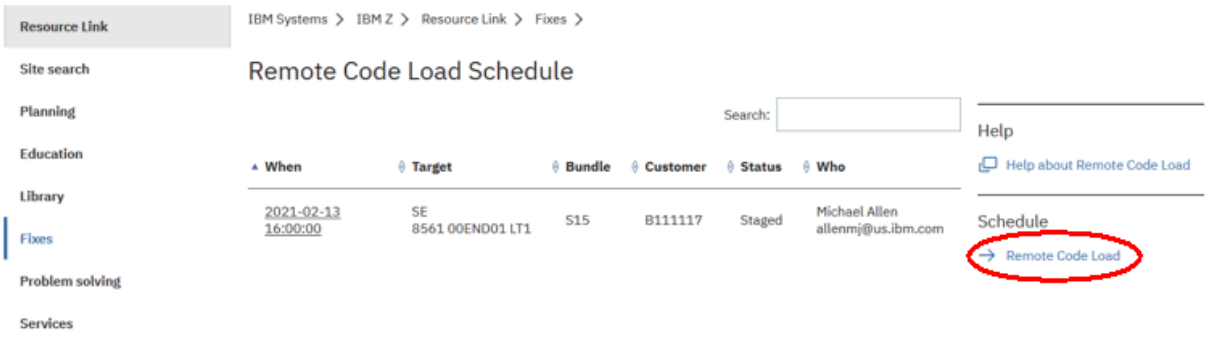
1. Go to Resource Link http://www.ibm.com/servers/resourcelink and log on with your user ID and password.
2. From the left navigation, select **Fixes**.



3. From the Fixes page, scroll down to the **Licensed internal code** section and then select the **Remote code load schedule** link.



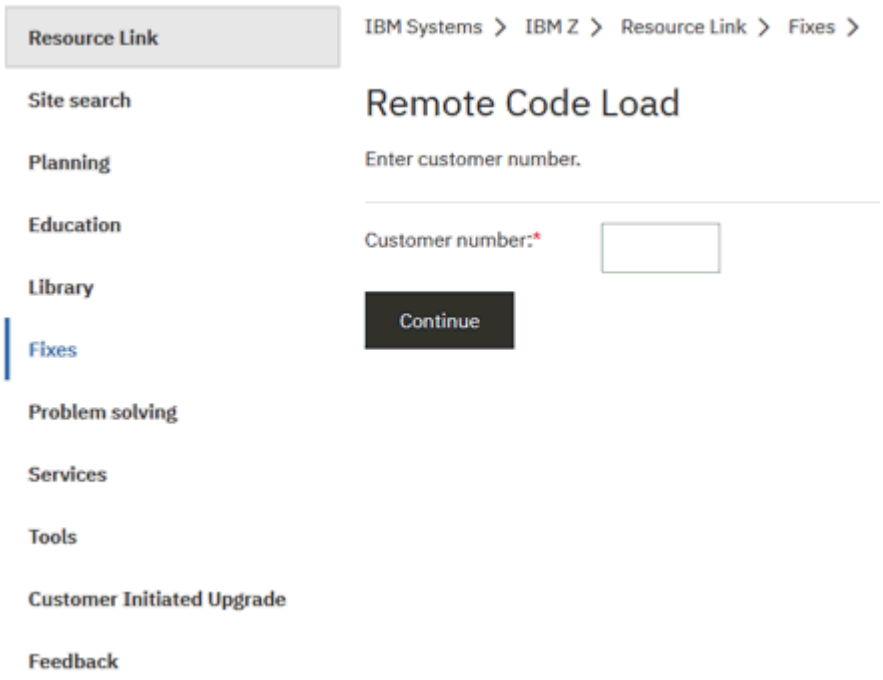
4. The Remote Code Load Schedule page is displayed.
5. To schedule a new firmware upgrade, select the **Remote Code Load** link. You can also use this page to filter requests in the **Search** entry field.



Notes:

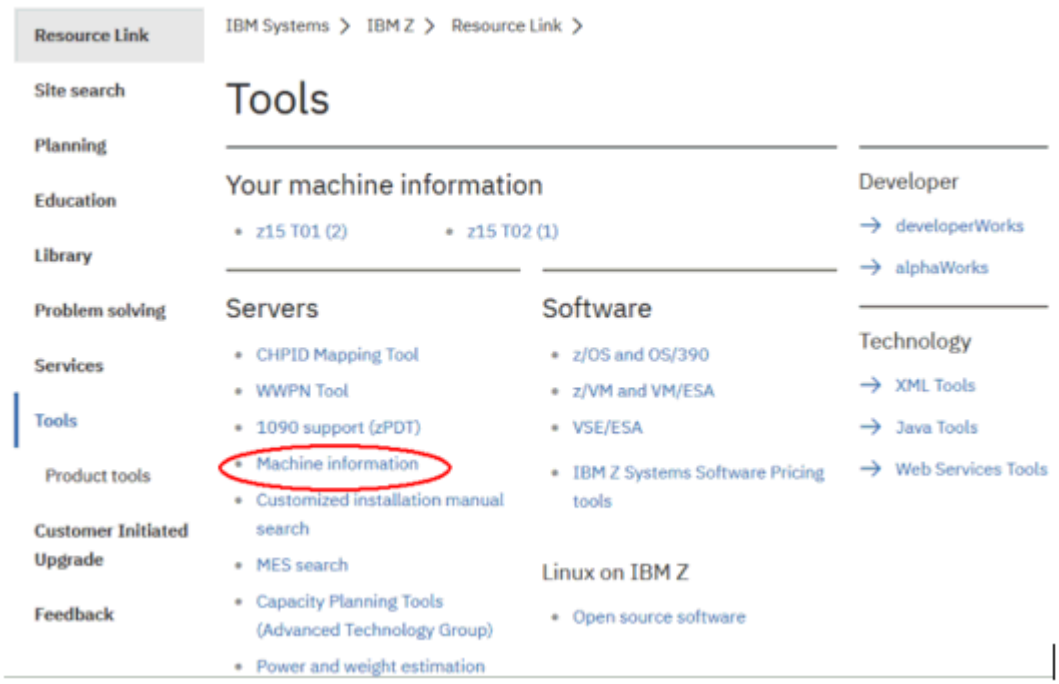
- If there are other Remote Code Load requests scheduled under this customer number, ensure they do not conflict with the Remote Code Load you are currently scheduling. You cannot schedule simultaneous Remote Code Loads on different systems.
- If possible, try to balance the amount of Remote Code Loads across the platform.

6. The Remote Code Load page is displayed. Provide the **Customer number** in the input area, then click **Continue** to proceed.

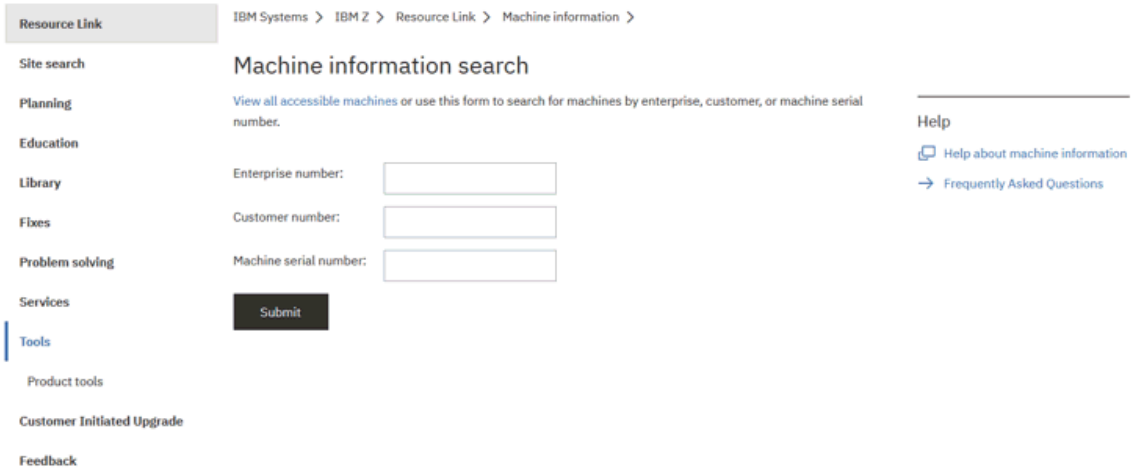


Note: If you need to obtain the customer number, you can obtain it by using the serial number of the targeted machine and the following steps.

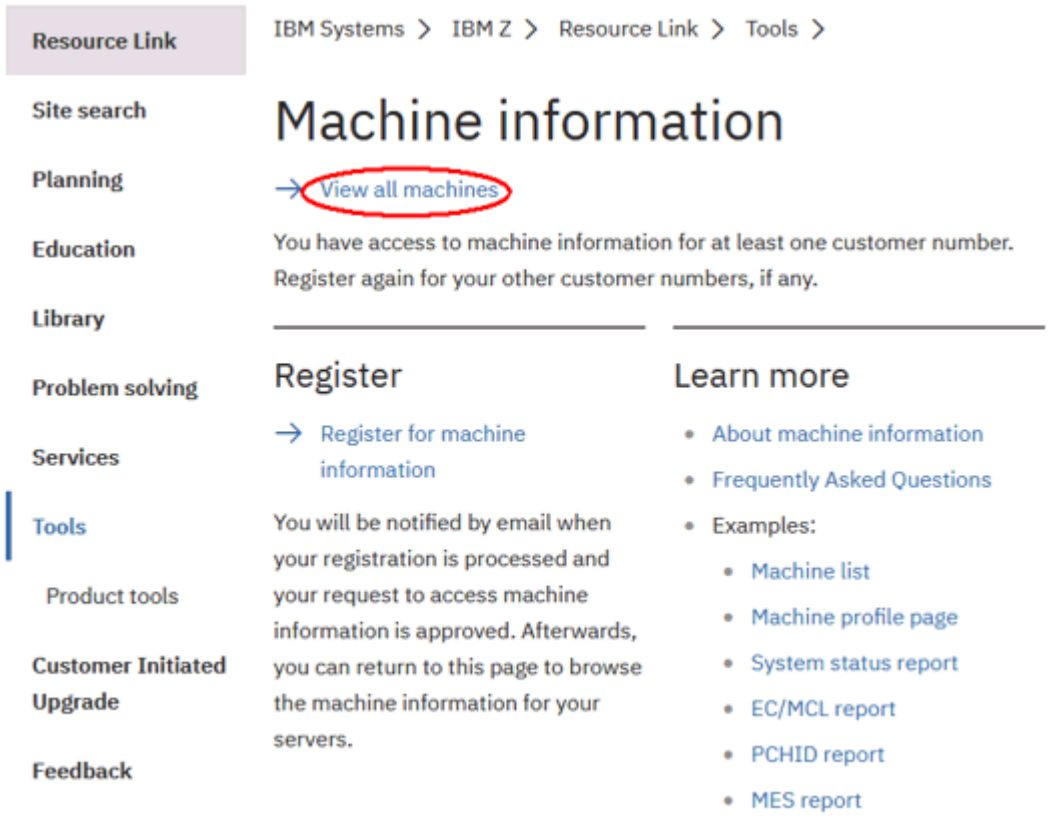
a. Go to **Tools** from the left navigation of Resource Link, then select **Machine information** from the Tools page.



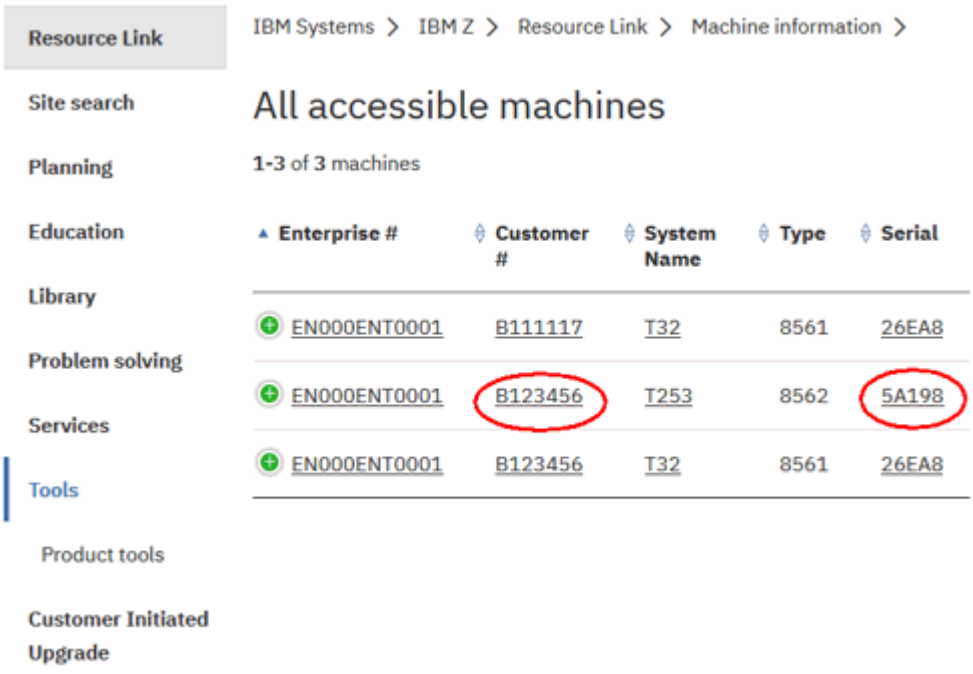
- If you have access to all the machine information, the Machine information search page is displayed. Provide the Machine serial number, click **Submit**, and then proceed to step "6.b" on page 146.



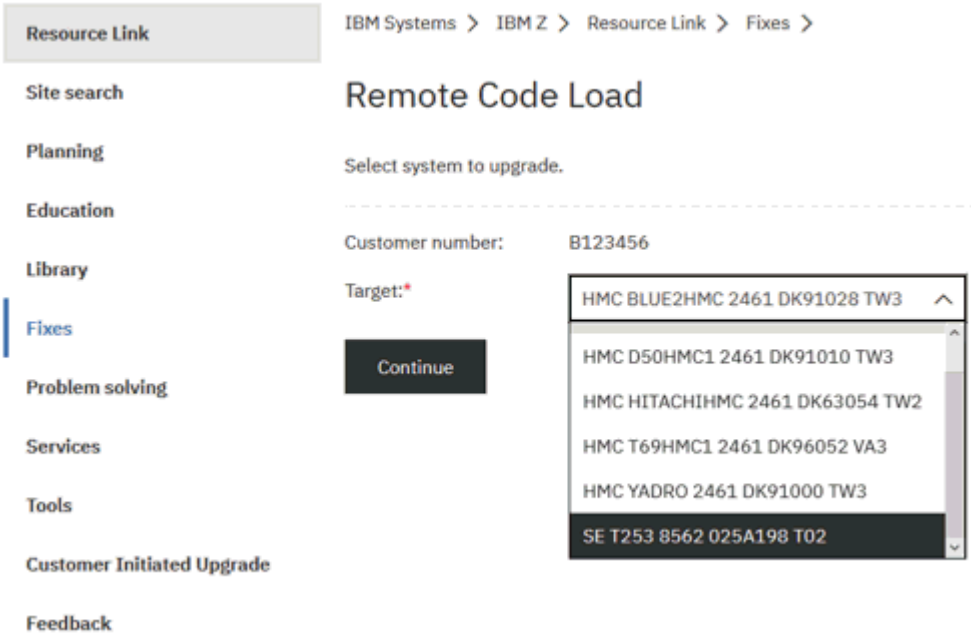
- If you don't have access to all the machine information, the Machine information page is displayed. Select **View all machines** then proceed to step "6.b" on page 146.



b. On the All accessible machines page, match the Serial number with the appropriate customer number and use that customer number for step “6” on page 144.



7. From the drop-down list of target consoles, select a target from the HMC or SE on which the customer wants to install the MCLs, then click **Continue** to proceed.



8. The Remote Code Load page is displayed with the information you are provided.
   - **Customer number**: Number associated with the machine serial number where the Remote Code Load firmware update will be applied.
   - **Target**: HMC or SE identifier where the Remote Code Load firmware update will be applied.

   Note: The Remote Code Load request must be scheduled between 48 hours and 45 days prior to execution.

   - **Schedule HMC**: From the drop-down list, select the HMC that was used to generate the authentication token.
   - **Bundle**: Select the bundle identifier from the drop-down list.
   - **Date**: Use the calendar to schedule the firmware update. Ensure it is before the authorization token expires. Also, ensure it is not during an already previously scheduled Remote Code Load for a separate system.
   - **Time (24 hour)**: Provide the time (HH:MM:SS) in the input area.

     Note: Verify that the date and time that is provided is the local time of the system that the customer is targeting to install the MCLs on.
   - **Time Zone**: Specify the time zone of the system that the customer is targeting to install the MCLs on.

     Note: This can be checked by using the **Customize Console Date/Time** task on the scheduling HMC.
   - **Authorization token**: Provide the authorization token number in the input area.
   - **IBM requester (SSR) name**
     - **Name**: The name of the SSR that will schedule the Remote Code Load firmware update.
     - **Email**: Email address of the SSR that will schedule the Remote Code Load firmware update.
     - **Phone number**: Telephone number of the SSR that will schedule the Remote Code Load firmware update.

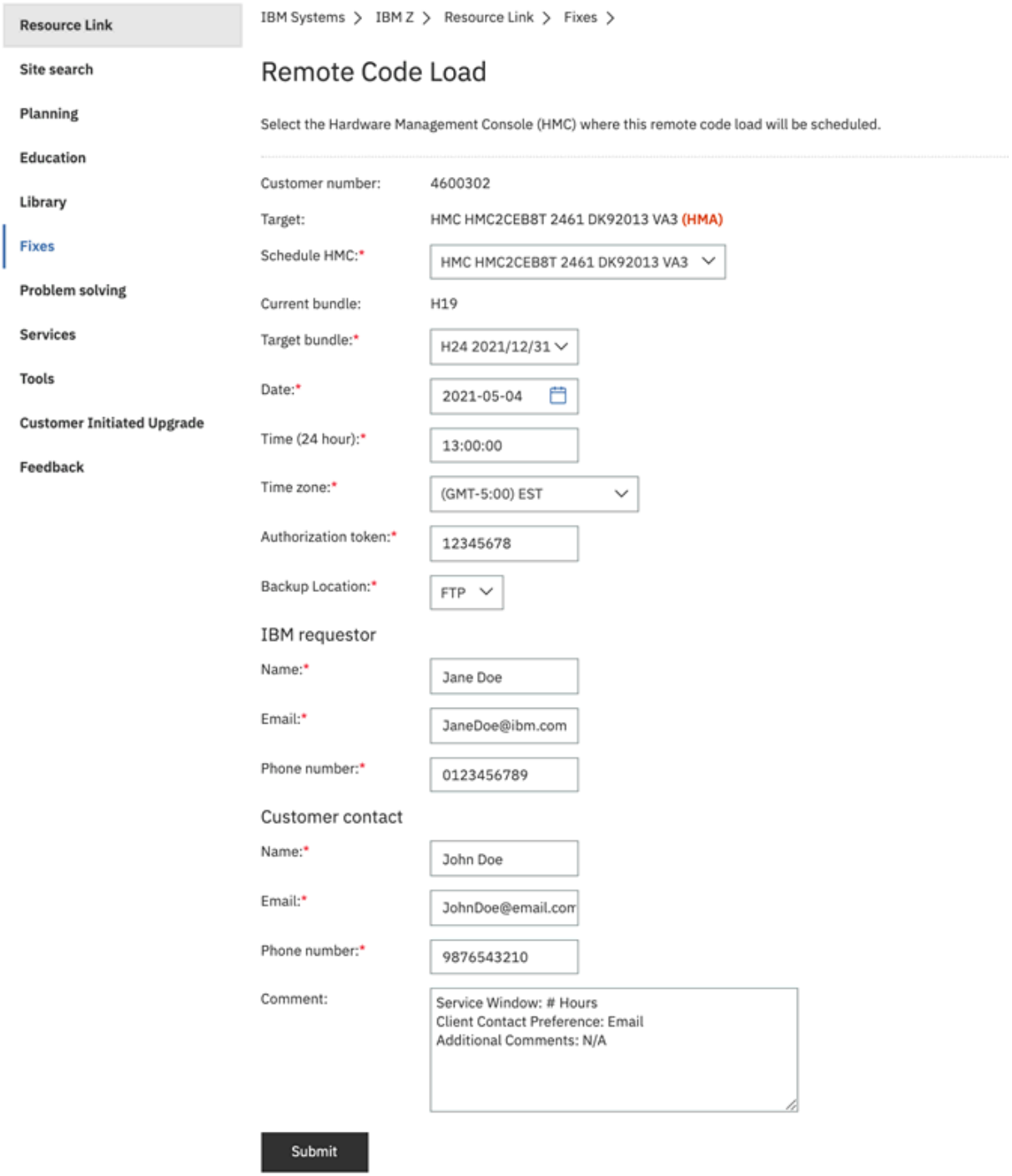
     Provide the remaining required (*) information that was provided to you.
   - **Customer contact**: Provide the customer name, email, and telephone number in the input areas.
   - If the Remote Code Load operation is targeting an HMC, ensure a preferred back-up location is specified (FTP or USB).

- Service window information must be included in the Comment Section. This information provides any additional actions or contact information that may be needed between you and the customer.

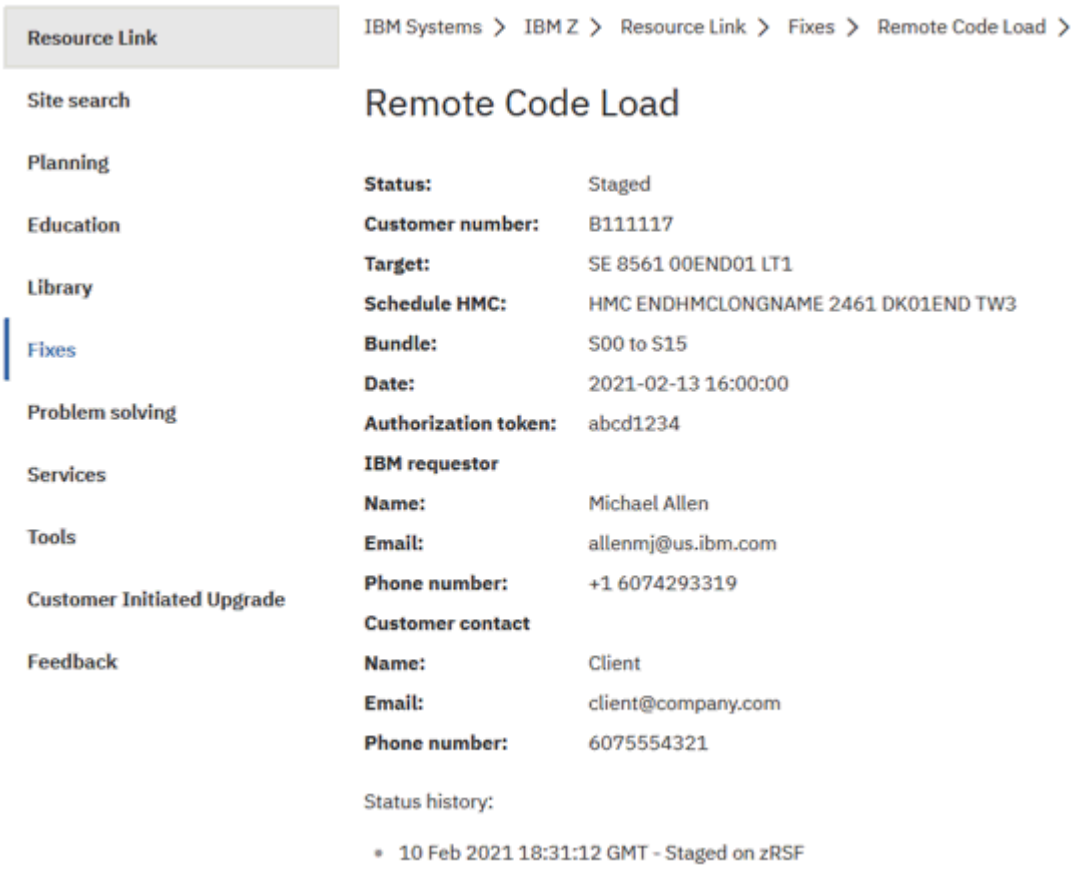
9. Here's a standard format of information that can be obtained and provided in the **Comments** section of the Remote Code Load page on Resource Link:

   Service window length:
   Customer contact preferences:
   Additional comments

10. When all fields are complete, click **Submit**. Ensure that there were no errors with the submission.



11. After the request is submitted the **Status** and the **Status history** of the submission is displayed.



Note: At this point, do not close out your work order. Your work order should remain open until you confirm that the Remote Code Load firmware update is successfully scheduled.

12. In the Remote Code Load table view on Resource Link, the SSR can monitor the status of the upgrade remotely. The status of the upgrade changes from **Staged** to **Scheduled** within 24 hours.
13. An email notification is sent to you when the request is scheduled, canceled, failed, or completed. The status is processed hourly.

    If an error occurs while scheduling the Remote Code Load, the status changes to **Failed** and error text is displayed on the status page. The SSR is notified by email when the status changes. See "Failed status" on page 149 for the next steps in the event of a failure.

    Note: The SSR is notified by email and the status on Resource Link only changes after the scheduling attempt is submitted to the scheduling HMC.

    If the Remote Code Load is scheduled successfully, your work order can be closed out.

    This should be written against ECA *XXX*.

    Otherwise, refer to "Failed status" on page 149.

Failed status

If scheduling fails, the SSR may need to contact the customer to confirm that the token is correct and prerequisites are met. Otherwise, they need to contact the next level of support. The SSR can direct the customer to the **Report a Problem** task to understand why there was a failure. After the problem is resolved, the customer can begin the Remote Code Load firmware update again.

Here are some examples of possible failures:

Reference code
ref 2052: Authorization code for schedule request does not match any current authorization code on this HMC

Reason
The inputted scheduling HMC for that authorization token was incorrect or the authorization token expired.

Reference code
ref 2058: Channel Patch did not complete for target

Reason
The customer needs to clear pending conditions.

Reference code
ref 205A: Operation start date is before current date/time

Reason
This should not happen with the 48 hour warning. If it does, the SSR ignored the warning or the HMC scheduled operation that pulls the file took a while due to call-home issues. If the former, schedule for a time at least 48 hours in the future. If the latter, have the customer validate call-home capability of that HMC.

Reference code
ref 205B: Scheduled operation start or end time overlaps with <sched op description> scheduled operation, or

Scheduled operation <sched op description> start or end time overlaps with scheduled operation time, or

Scheduled operation <sched op description> start or end time is the same as scheduled operation.

Reason
The scheduled operation conflicted with the Remote Code Load scheduled operation. You need to pick another time.

If the problem determination based on the above messages is unsuccessful or if the scheduling failure message was not included above, the SSR should have the customer access the **Report a Problem** task to investigate.



Part Number: 03GH503

