

*Delta Pages (P/N 03GH512)
for
8561 Service Guide
GC28-6998-01*





8561 Service Guide

P/N 03GH512

Delta

Base Publication Number:	GC28-6998-01	Date: 02 March 2021
	GC28-6998-01a	31, March 2021
	GC28-6998-01b	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 -01a

Replace 8561 Service Guide (GC28-6998-01) pages 63-64 with delta pages 63-64
Replace 8561 Service Guide (GC28-6998-01) pages 177-184 with delta pages 177-184
Replace 8561 Service Guide (GC28-6998-01) pages 353-354 with delta pages 353-354

Level -01b

Replace 8561 Service Guide (GC28-6998-01) pages 129-130 with delta pages 129-130
Replace 8561 Service Guide (GC28-6998-01) pages 177-178 with delta pages 177-178

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

This Delta contains information about machine type 8561.

Note: Please save this page along with the publication to provide a record of the changes.

P/N 03GH512 Copyright IBM Corp. 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.

Internal Battery Feature (IBF)

The Internal Battery Feature (IBF) is an optional feature that is only available with BPA powered systems. This feature provides internal battery backup to the system in the event of an outage.

CAUTION: Only trained service personnel may replace this battery. The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not: Throw or immerse into water, heat to more than 100°C (212°F), repair or disassemble. (C002)



Attention:

- The IBF contains Lithium ion batteries that are greater than 300 Wh.
- The IBFs are fully regulated Dangerous Goods and premium costs are associated with owning.
- The need for the IBF is redundant if your location provides uninterruptible power.
- For 8561 systems that ship with the IBFs and IBF field-replaceable units (FRUs), arrival times might be delayed due to availability of freight carriers rated for Dangerous Goods.
- If the system is moved at all, the IBFs **must** be removed prior to transport.
- The IBF rated output is 350VDC. If the IBFs are transported by air, the lithium-ion batteries **must** first be discharged to 30% SOC (30% State of Charge) or less using the IBF Discharge Tool.
For information about using the IBF Discharge Tool, see [“Discharging IBFs” on page 64](#).
- Only an individual that is certified in Dangerous Goods transportation is authorized to package and ship IBFs. It is the responsibility of the client to arrange this using a logistics provider.
- The client is responsible for proper handling of the IBFs; in accordance with all local, legal, and environmental requirements for uninstalled IBFs as a result of a repair action, relocation, or machine return.
- IBM Global Financing (IGF) or any leaser may not receive IBF returns.
- Where IBM has Extended Producer Product Take Back Responsibilities, refer to <https://www.ibm.com/ibm/recycle/ww/>.

A BPA powered 8561 may have 2, 4, 6, 8, 10, or 12 batteries. Similar to Bulk Power Regulators (BPRs), the IBFs are always plugged in pairs. The number of IBFs, when installed, must always equal the number of BPRs.

Additional service considerations:

- The service procedures and requirements for the IBFs in the 8561 are different than those in previous systems.
- Service representatives **must** use the procedure in Repair and Verify for IBF removal. After you complete the procedure, Repair and Verify will refer you to [“Discharging IBFs” on page 64](#), in this document.

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

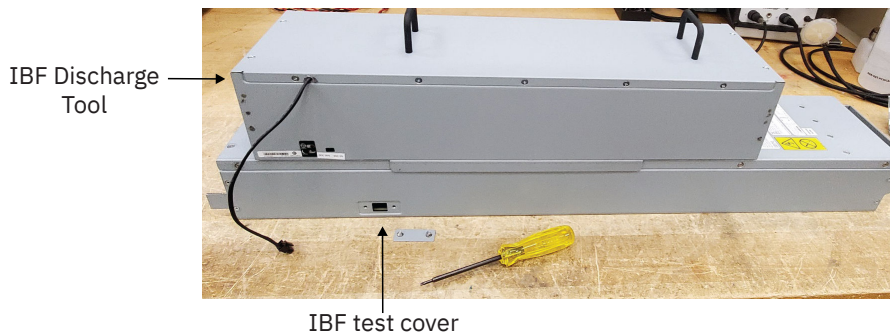
Discharging IBFs

Complete the following steps to discharge the Lithium ion batteries that make up the Internal Battery Feature (IBF).

- ___ 1. Locate the IBF Discharge Tool (**P/N 02RA062**) from the initial system ship group or subsequent Engineering Change Announcement (ECA) shipment.
- ___ 2. Place the discharge tool (**P/N 02RA062**) on top of the IBF, as shown in the following graphic.

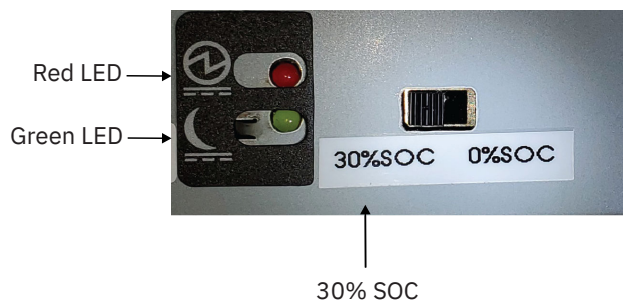


- ___ 3. Remove the cover from the test connector on the IBF.

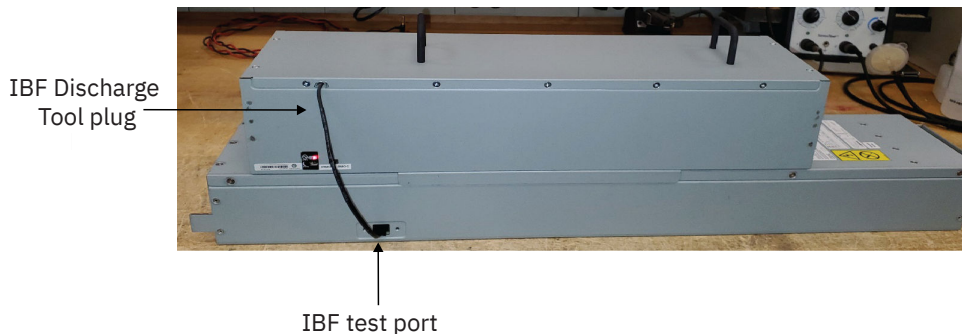


- ___ 4. On the discharge tool, set the discharge threshold switch to **30%SOC** (30% State of Charge).

Note: The setting for 0% SOC is available but not used at this time.



- ___ 5. Plug the discharge cord into the IBF test connector.



- ___ 6. The red LED will turn on when the discharge cord is attached.



Note: If no LED turns on then the IBF is completely discharged (0% SOC).

After a few minutes, the IBF Discharge Tool cooling fans will turn on. The red LED will remain lit while the tool discharges the IBF. This may take up to 1 hour to complete.

- __ 7. The green LED will turn on when the IBF is discharged successfully.



- __ 8. Remove the discharge cord from the IBF.

Note: If you do not disconnect the IBF Discharge Tool from the IBF, the tool will continue to load the IBF with a few watts. If left connected for an extended period of time, the IBF will be discharged to a lower SOC. For this reason, the tool should be disconnected within one hour of the discharge being complete (green LED on).

- __ 9. Reinstall the cover on the IBF test connector.
- __ 10. Repeat Steps “2” on page 64 through “9” on page 65 to discharge each additional IBF where shipment is required.
- __ 11. Store the IBF Discharge Tool in a known location for potential future use. One option is to store it with the Fill & Drain Tool (FDT).

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

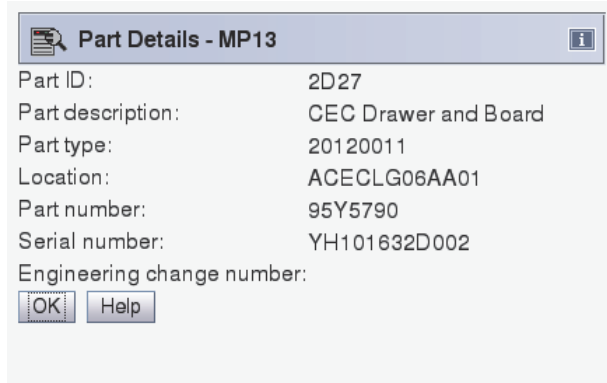
- To determine "N" or "Z" side, as addressed by the horizontal label located at the top of the frame:
 - All N-side (left side PDUs at the rear of the frame) power connectors have a striped band label.
 - All Z-side (right side PDUs at the rear of the frame) power connectors have a solid band label.

BPA power

- To determine "A" or "B" BPE side:
 - All A-side power connectors have a striped band label.
 - All B-side power connectors have a solid band label.

- Click **Details**.

___ 4. • Review the information.



The screenshot shows a dialog box titled "Part Details - MP13". It contains the following information:

Part ID:	2D27
Part description:	CEC Drawer and Board
Part type:	20120011
Location:	ACECLG06AA01
Part number:	95Y5790
Serial number:	YH101632D002
Engineering change number:	

At the bottom of the dialog box are two buttons: "OK" and "Help".

- 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 5 on page 180 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.**

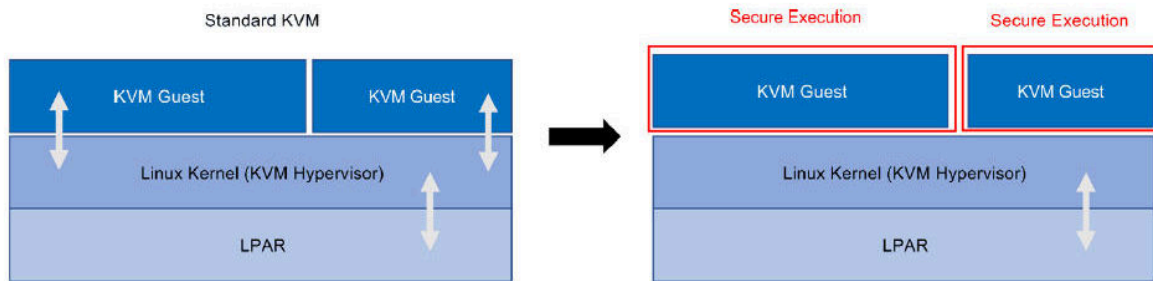


Figure 5. Secure Execution for Linux - KVM implementation

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 follows:

T204 Details - T204

Instance Information

Product Information

Acceptable CP/PCHID Status

STP Information

Energy Management

Security

Group:

CP status: Operating

Channel status: Exceptions

Crypto status: Not operating

Alternate SE status: Operating

Activation profile: DEFAULT

Last profile used: DEFAULT

IOCDs identifier: A0

IOCDs name: T204 Rev

System mode: Logically Partitioned

Service state: false

Number of CPs: 6

Number of ICFs: 0

Number of IFLs: 0

Number of zIIPs: 0

Dual AC power maintenance: Fully Redundant

CP Assist for Crypto functions: Installed

Licensed Internal Code security mode: Monitor

Secure Execution for Linux: Enabled [Manage](#)

Lock out disruptive tasks: ☐ Yes ☒ No

[OK](#) [Apply](#) [Change Options...](#) [Cancel](#) [Help](#)

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

Manage Secure Execution Keys

View and update keys used by IBM Secure Execution for Linux.

Global keys

The global private key used to decrypt Linux images for systems.

Search

Update

Refresh

Type	Key hash
Primary	PG F0 CB AB 46 BC 78 46 CF BE 72 38 CD 89 34 CA 64 7E 1A 98 45 CA 35 67 4C DA CE F6 A7 C6 AC 54
Secondary	SG F0 CB AB 46 BC 78 46 CF BE 72 38 CD 89 34 CA 64 7E 1A 98 45 CA 35 67 4C DA CE F6 A7 C6 AC 54

Host keys

The host-specific private key used to decrypt Linux images for this system.

Search

Update

Refresh

Type	Key hash
Primary	PH F0 CB AB 46 BC 78 46 CF BE 72 38 CD 89 34 CA 64 7E 1A 98 45 CA 35 67 4C DA CE F6 A7 C6 AC 54
Secondary	SH F0 CB AB 46 BC 78 46 CF BE 72 38 CD 89 34 CA 64 7E 1A 98 45 CA 35 67 4C DA CE F6 A7 C6 AC 54

GUIDANCE

Secure Execution for Linux is a z/Architecture security technology that allows Linux workloads to run in a KVM guest with maximum privacy by protecting system memory and data from external attacks and insider threats. The KVM guest (virtual machine) environment is fully isolated and protected from the hypervisor with encryption keys that only the IBM Z hardware and firmware have access to.

Host key

The host key is a private key specific to the system. An encrypted Linux image can be created using the corresponding host public key. Since the host private encryption key is stored on the IBM Z hardware and firmware, the encrypted image can only be executed in a virtual machine on the system (host) it has been prepared for, and the image can't be decrypted or tampered with outside of the designated system.

Global key

The global key is a private key which is not specific to a particular system. The global key is used with the IBM Hyper Protect Virtual Servers product to protect Linux workloads deployed to multiple systems.

Updates to these keys are managed by IBM Support Services Representatives (SSR). If keys are updated by an IBM SSR, the new key will be displayed as the primary key and the previous key will be displayed as the secondary key. This feature allows Linux images to be decrypted by either the primary or secondary key while migrating to Linux images encrypted with the new, primary, key.

Do not update keys unless you are explicitly instructed by the client to continue. There is no roll-back or key management capability.

Care should be taken when removing secondary keys as any Linux image encrypted with this key will no longer be usable and workloads will no longer be operational. Once removed, the secondary key can not be added back to the system.

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 7 on page 184](#) for flowchart representation)
- CPC drawer replacement (see [Figure 8 on page 184](#) for flowchart representation)
- CP SCM replacement (see [Figure 9 on page 185](#) 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.

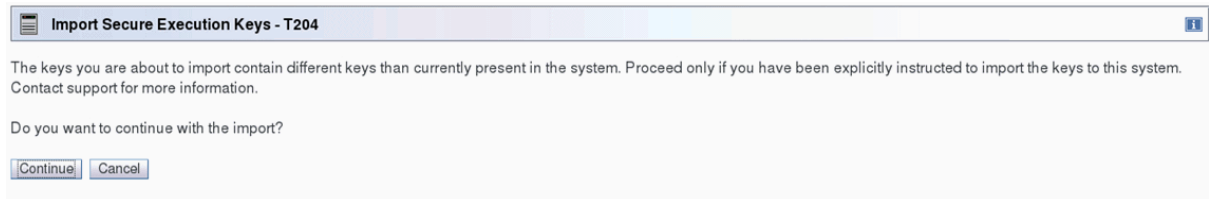
IMPORTANT:

- See [Figure 11 on page 186](#) for a flowchart representation of the *Import Secure Execution Keys* 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 182](#) 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 182](#) 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 10 on page 185 for a flowchart representation of the new key bundle service scenario.

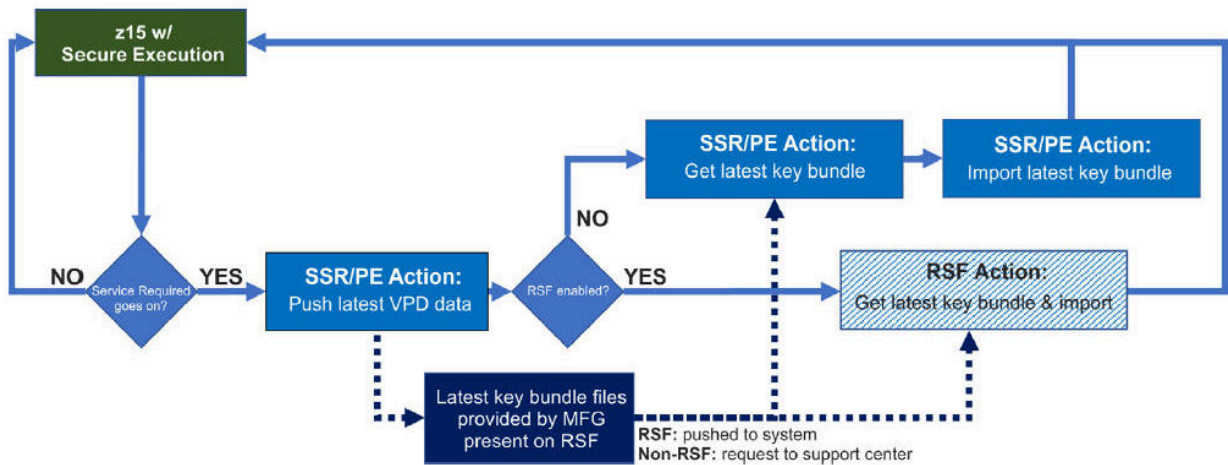


Figure 6. Service Required status flow

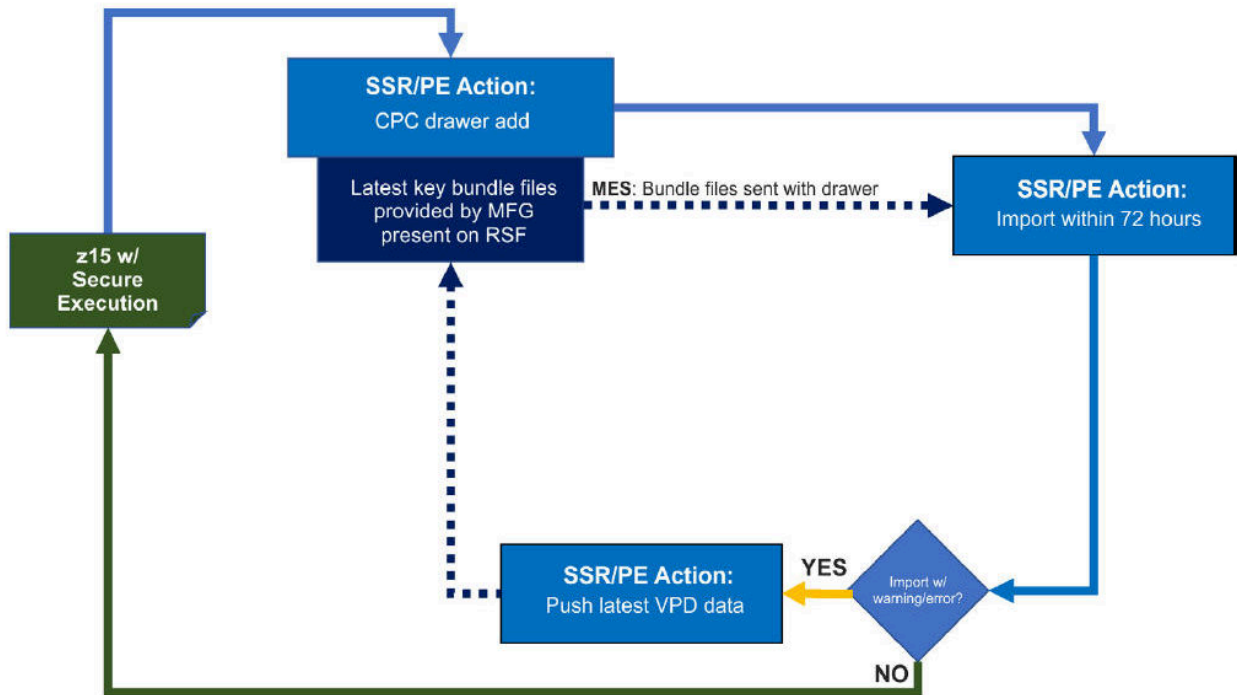


Figure 7. Service scenario flowchart - CPC drawer add

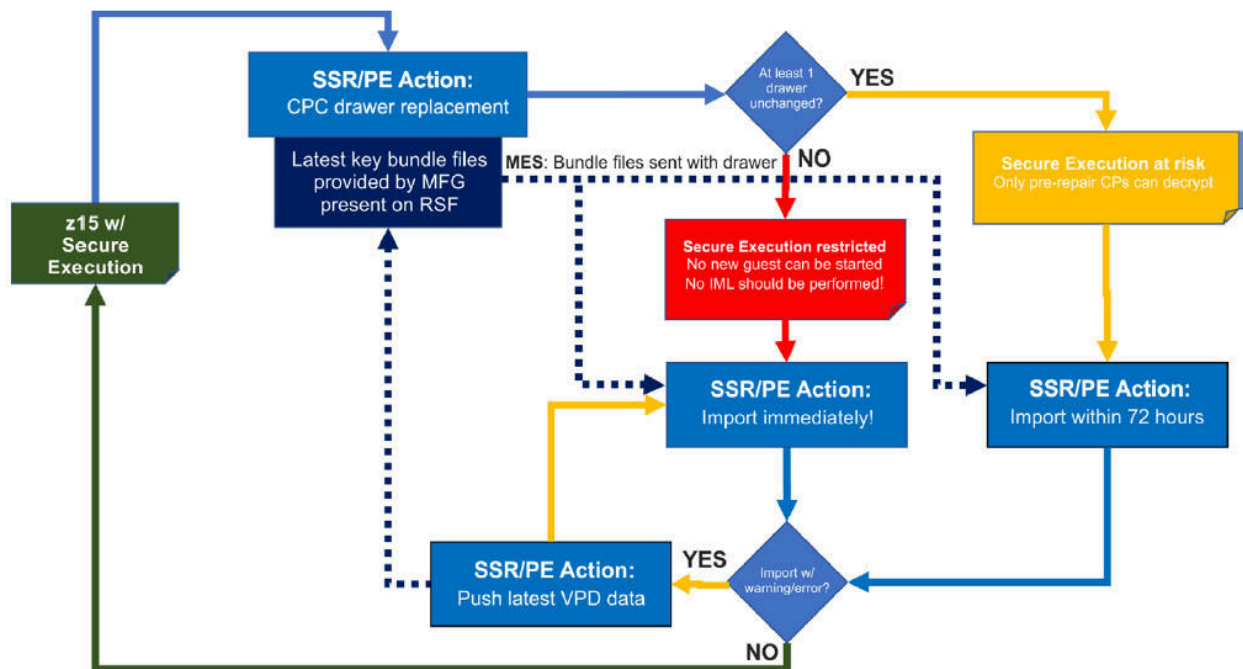


Figure 8. Service scenario flowchart - CPC drawer replacement

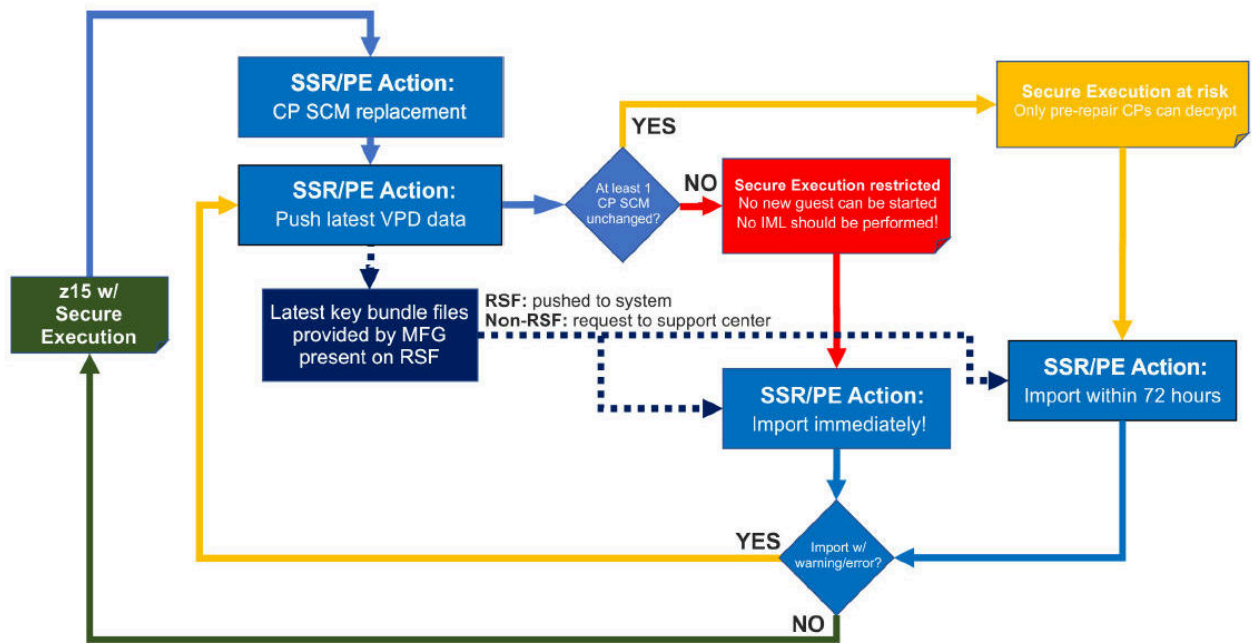


Figure 9. Service scenario flowchart - CP SCM replacement

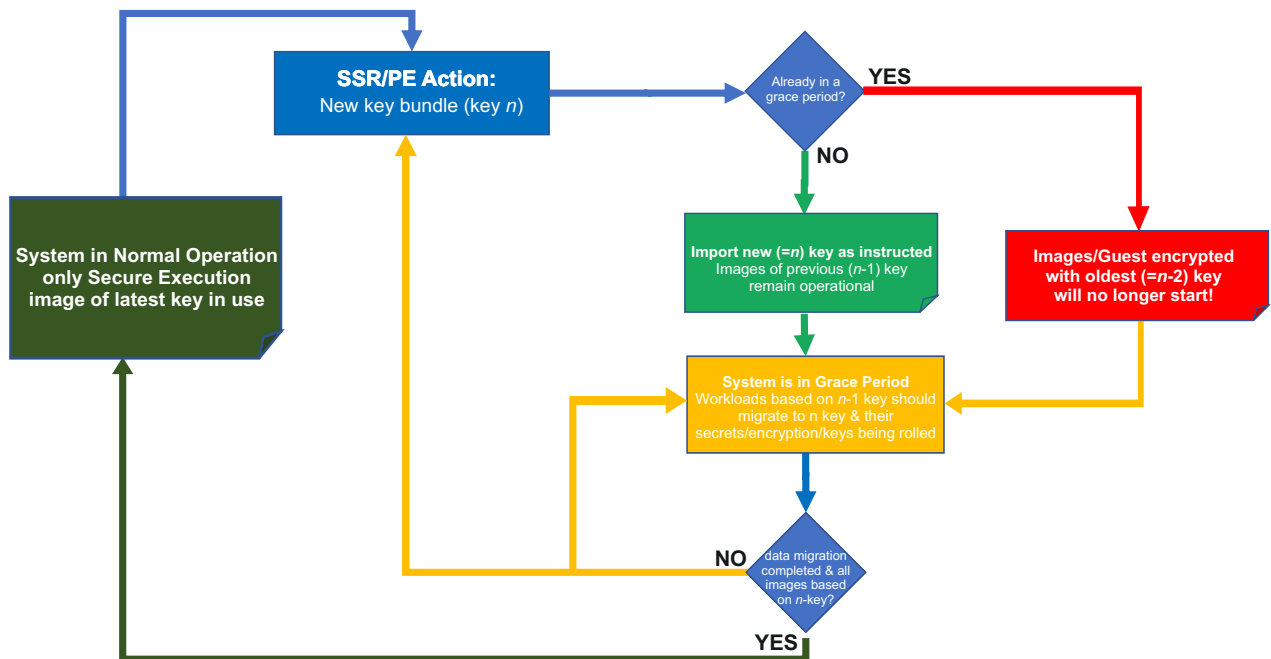


Figure 10. Service scenario flowchart - New key bundle

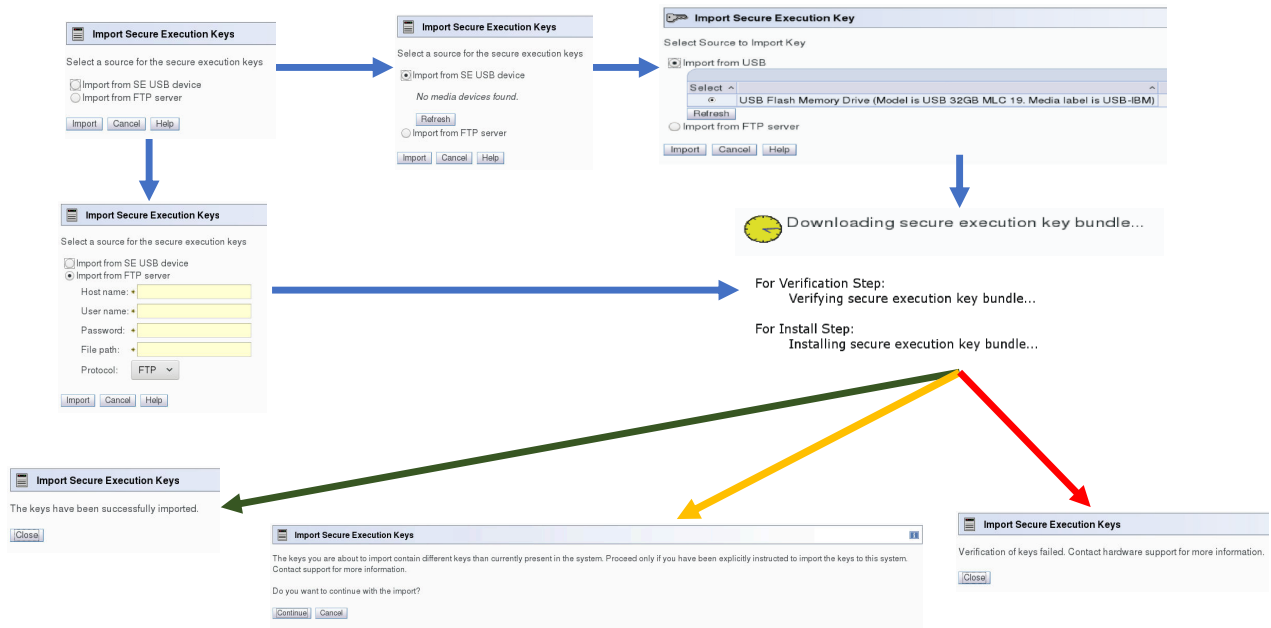


Figure 11. Import Secure Execution Keys task flow

IBM Adapter for NVMe

Note: This feature is only available with IBM LinuxONE.

Repair information for the IBM Adapter for NVMe feature is provided by online procedures on the Support Element. This section provides information for running tests and checking adapter status.

Find the information that you want in the following table and go to the page indicated.

Action or Information	Go to
View Function ID Configuration	“Function ID Configuration” on page 370
Manage PCI System Services	“Manage PCI System Services” on page 372
Update PCI Adapter Internal Code	“Update PCI Adapter Internal Code” on page 375
Placing a channel in single channel service	“Placing a channel in standby or reserved status” on page 166
Running IBM Adapter for NVMe tests	“IBM Adapter for NVMe tests” on page 359

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.

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**).
 - Customer can carry forward IBM Adapter for NVMe (**FC 0435**).

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/downloads/cas/PDGXWWO3>) 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 tmclass="IGNORE" Express Card Electro-Mechanical Spec. Rev 3.0

- **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 GAⁿ⁺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 GAⁿ⁺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 GAⁿ⁺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 GAⁿ⁺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 GAⁿ⁺¹ code level transitions have completed. Once this GAⁿ⁺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 GAⁿ⁺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 GAⁿ⁺¹ level on the Primary system, you need to bring the Alternate system to the GAⁿ⁺¹ level. To accomplish this upgrade, proceed with the following:

1. Use the **Backup Critical Data** task on the GAⁿ⁺¹ system.
2. Using the CUEC AROMs, perform a hard disk restore on the GAⁿ 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 5 on page 132 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.

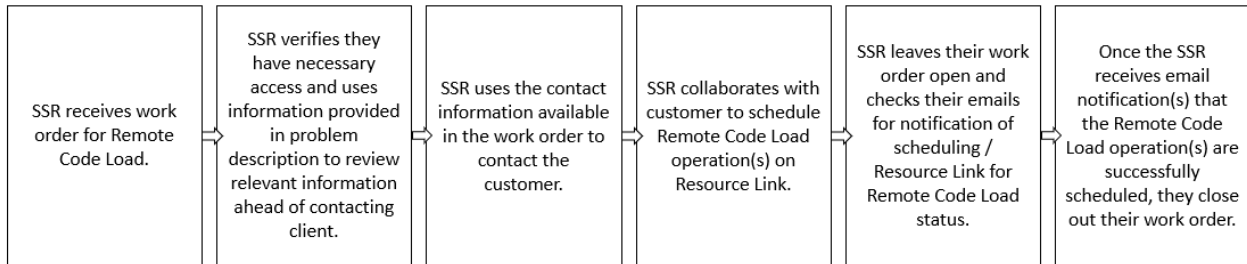


Figure 5. Remote Code Load firmware update process flow

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 137. 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.

The screenshot shows the IBM CSP Work Order interface. The top navigation bar includes the IBM logo, a search bar with 'TS003627928', and various icons. The main header displays 'z15 Remote Code Load Request' and 'Work Order WO00263007'. The left sidebar contains 'Related List Quick Links' such as Diagnostics, Related Cases, Work Orders, Case History, Attached Assets, and Case Known Issues. The main content area shows the work order details, including Status (Draft), Client Reference Number, Legacy Reference Number, Service Type (H/A), Record Type (Draft WO), and External Status. A 'Select The Step You Want To Go To Directly.' section lists steps like Basic Information, Work Order Record Type, Appointment Preferences, Onsite Resource Information, and Critical Information Summary. The right sidebar shows 'Asset Information' (Serial Number, Machine Type, Model) and 'Time Zones' (Asset and Agent time zones). The bottom status bar includes 'Instant Feedback', 'Mini CP', 'Omni-Channel (Offline)', 'Status - Offline', 'Out of Office', 'Request Case Access', 'Add to Account Team', 'Request CM Access', 'History', and 'Create Case'.

Figure 6. 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.

The screenshot shows a feed for a Remote Code Load problem description. At the top, there's a header with a green circle containing the number 4, followed by 'z15 Remote...' and a search bar. Below this, the text 'TS003627928 (PC) | Call Home SME Test | James K' is visible. Four red status boxes are displayed: 'no owner assigned', 'no Next Action Datetime set', 'no solution provided', and 'ARM incomplete'. A 'Post...' button is located below these boxes. The main content area lists details: Country: US, Postal Code: 12603, Account: Call Home SME Test, Product:, Manufacturer:, Liability Organization:, and Liability Category:. A yellow box contains the text 'JK 5/10/2021 1:12 PM | Internal | James Kabo (Customer) on WO WO00263007 at CC | CC: Default'. Below this, the 'Subject: z15 Remote Code Load Request' is shown. The 'Problem Description:' section includes 'HMCName Remote code load request', 'Date', 'Time', and 'Bundle level'.

Figure 7. Remote Code Load problem description

Technical requirements and best practices

See Table 3 on page 134 for the technical requirements and Table 4 on page 135 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 <i>Integrating the Hardware Management Console's Broadband Remote Support Facility</i>, 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 <i>Integrating the Hardware Management Console's Broadband Remote Support Facility</i>, 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 HXX+. - 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 SXX+. - 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 134.
- 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: HXX for HMC, SXX 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 137.
- 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**.

Resource Link

IBM Systems > IBM Z >

Resource Link

IBM Z

- [z15 T01](#)
- [z15 T02](#)
- [z14](#)
- [z14 ZR1](#)
- [z13](#)
- [z13s](#)
- [z BladeCenter Extension \(zBX\) Mod](#)
- [Other mainframes](#)

LinuxONE servers

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

Library	HARDWARE	SOFTWARE
Fixes	Known defects/problems • Large Systems Support • Exception letters	Get fixes • Download • Check status of ordered fixes
Problem solving		
Services	Alerts • Machine alerts • Hiper alerts • Product support alerts • Red alerts	Report problems • Software problem reporting
Tools		
Customer Initiated Upgrade		
Feedback		
	Report problems • Hardware problem reporting	Preventive actions • Preventive Service Planning buckets (PSP) • Subscribe to APARs • Search for APARs
	Downloads • AROM images • SUL images • SUL control file • LIACC fast upgrade • zSeries diskette images • S/390 diskette images • HMC Support for Director/Timer Consoles	Maintenance • z/OS and OS/390 enhanced holddata
	Licensed internal code • PE MCL information • Remote code load schedule	

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.

Resource Link IBM Systems > IBM Z > Resource Link > Fixes >

Remote Code Load Schedule

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Search:

Help

Help about Remote Code Load

When	Target	Bundle	Customer	Status	Who
2021-02-13 16:00:00	SE 8561 00END01 LT1	S15	B111117	Staged	Michael Allen allenmj@us.ibm.com

Schedule

→ Remote Code Load

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.

Resource Link IBM Systems > IBM Z > Resource Link > Fixes >

Remote Code Load

Enter customer number.

Customer number:*

Continue

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

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.

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

Resource Link IBM Systems > IBM Z > Resource Link >

Tools

Site search

Planning

Education

Library

Problem solving

Services

Tools

Product tools

Customer Initiated Upgrade

Feedback

Your machine information

- z15 T01 (2)
- z15 T02 (1)

Servers

- CHPID Mapping Tool
- WWPN Tool
- 1090 support (zPDT)
- **Machine information**
- Customized installation manual search
- MES search
- Capacity Planning Tools (Advanced Technology Group)
- Power and weight estimation

Software

- z/OS and OS/390
- z/VM and VM/ESA
- VSE/ESA
- IBM Z Systems Software Pricing tools

Linux on IBM Z

- Open source software

Developer

- developerWorks
- alphaWorks

Technology

- XML Tools
- Java Tools
- Web Services Tools

- 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 141.

Resource Link IBM Systems > IBM Z > Resource Link > Machine information >

Machine information search

View all accessible machines or use this form to search for machines by enterprise, customer, or machine serial number.

Enterprise number:

Customer number:

Machine serial number:

Submit

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Product tools

Customer Initiated Upgrade

Feedback

Help

- Help about machine information
- Frequently Asked Questions

- 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 141.

Resource Link IBM Systems > IBM Z > Resource Link > Tools >

Machine information

→ [View all machines](#)

You have access to machine information for at least one customer number.
Register again for your other customer numbers, if any.

Register

→ [Register for machine information](#)

You will be notified by email when your registration is processed and your request to access machine information is approved. Afterwards, you can return to this page to browse the machine information for your servers.

Learn more

- [About machine information](#)
- [Frequently Asked Questions](#)
- Examples:
 - [Machine list](#)
 - [Machine profile page](#)
 - [System status report](#)
 - [EC/MCL report](#)
 - [PCHID report](#)
 - [MES report](#)

- 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 139.

Resource Link IBM Systems > IBM Z > Resource Link > Machine information >

All accessible machines

1-3 of 3 machines

Enterprise #	Customer #	System Name	Type	Serial
EN000ENT0001	B1111117	T32	8561	26EA8
EN000ENT0001	B123456	T253	8562	5A198
EN000ENT0001	B123456	T32	8561	26EA8

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.

Resource Link

IBM Systems > IBM Z > Resource Link > Fixes >

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

Remote Code Load

Select the Hardware Management Console (HMC) where this remote code load will be scheduled.

Customer number: 4600302

Target: HMC HMC2CEB8T 2461 DK92013 VA3 (HMA)

Schedule HMC:* HMC HMC2CEB8T 2461 DK92013 VA3

Current bundle: H19

Target bundle:* H24 2021/12/31

Date:* 2021-05-04

Time (24 hour):* 13:00:00

Time zone:* (GMT-5:00) EST

Authorization token:* 12345678

Backup Location:* FTP

IBM requestor

Name:* Jane Doe

Email:* JaneDoe@ibm.com

Phone number:* 0123456789

Customer contact

Name:* John Doe

Email:* JohnDoe@email.com

Phone number:* 9876543210

Comment:

Service Window: # Hours
Client Contact Preference: Email
Additional Comments: N/A

Submit

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

Resource Link

IBM Systems > IBM Z > Resource Link > Fixes > Remote Code Load >

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

Remote Code Load

Status:	Staged
Customer number:	B111117
Target:	SE 8561 00END01 LT1
Schedule HMC:	HMC ENDHMCCLONGNAME 2461 DK01END TW3
Bundle:	S00 to S15
Date:	2021-02-13 16:00:00
Authorization token:	abcd1234
IBM requestor	
Name:	Michael Allen
Email:	allenmj@us.ibm.com
Phone number:	+1 6074293319
Customer contact	
Name:	Client
Email:	client@company.com
Phone number:	6075554321

Status history:

- 10 Feb 2021 18:31:12 GMT - Staged on zRSF

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.

- 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.
- 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 144 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 144.

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.

Logical partition and coupling facility changes

Use this procedure when IBM product engineering directs you to create and activate a change for logically partitioned mode or coupling facility control code. The fix is created by using the system editor. After creating the fix, use the logical partition utility options to activate it.

To create and activate a change that is provided by product engineering:

__ 1. Select a console

- If you are using the Support Element for this task, prepare the Support Element for service. For information, see “Starting service with the Support Element” on page 18.
- If you are using the Hardware Management Console for this task, make a remote connection to the CPC. For information, see “Starting service with the Hardware Management Console” on page 33.

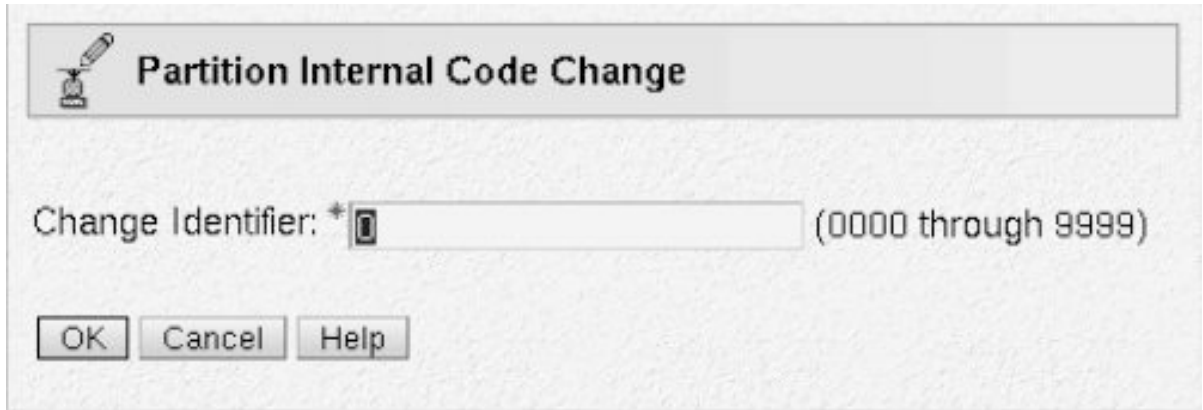
__ 2. Create the fix

Note: If you were directed to activate or deactivate an existing fix, go to Step “5” on page 146.

On the Support Element workspace window:

- Click **Tasks Index** on the left navigation pane.
- From the Tasks Index, click **Edit LPAR Internal Code Change**.

__ 3. On the Partition Internal Code Change window:



- Type in the 4 digits to identify the fix file you are creating.
(Fix files are named IQZQxxxx. TRM where xxxx is any numeric value in the range 0000 - 9999 .)
- Click **OK**.

__ 4. On the Editor window:

- Enter the information about the fix product engineering provided.
- When complete, press **F9** to store the fix on the Support Element hard drive.

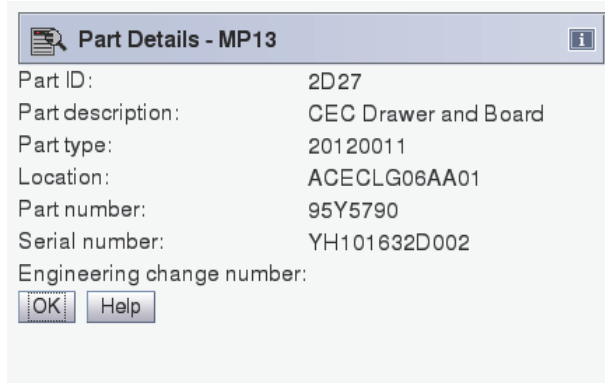
__ 5. On the Support Element workspace window:

- Click **Tasks Index** on the left navigation pane.
- From the Tasks Index, click **LPAR Internal Code Change Utility**.

__ 6. On the LPAR Internal Code Change Utility window:

- Click **Details**.

___ 4. • Review the information.



The screenshot shows a dialog box titled "Part Details - MP13". It contains the following information:

Part ID:	2D27
Part description:	CEC Drawer and Board
Part type:	20120011
Location:	ACECLG06AA01
Part number:	95Y5790
Serial number:	YH101632D002
Engineering change number:	

At the bottom of the dialog box are two buttons: "OK" and "Help".

- 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 8 on page 194 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.**

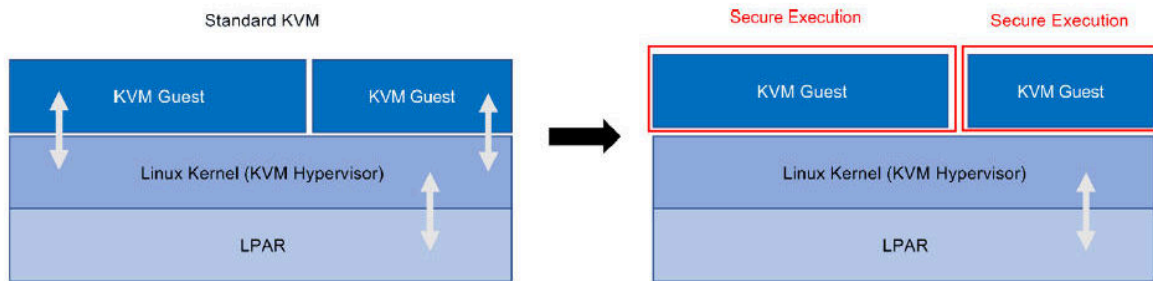


Figure 8. Secure Execution for Linux - KVM implementation

For more information, refer to <https://www.ibm.com/docs/en>.

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).



Part Number: 03GH512

(1P) P/N: 03GH512

