

IBM zSystems and LinuxONE

Remote Code Load for IBM Z Firmware



Note:

Before you use this information and the product it supports, read the information in [“Safety” on page v](#), [Appendix A, “Notices,” on page 43](#), and *IBM Systems Environmental Notices and User Guide*, Z125-5823.

This edition, SC28-7044-02, applies to IBM zSystems and LinuxONE. This edition replaces SC28-7044-01.

There might be a newer version of this document in a **PDF** file available on **IBM Documentation**. Go to <https://www.ibm.com/docs/en/systems-hardware>, select **IBM zSystems** or **IBM LinuxONE**, then select your configuration, and click **Library Overview** on the navigation bar.

© **Copyright International Business Machines Corporation 2022, 2023.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Safety.....	v
Safety notices.....	v
World trade safety information.....	v
Laser safety information.....	v
Laser compliance.....	v
 About this publication.....	 vii
Revisions.....	vii
Accessibility features.....	vii
Consult assistive technologies.....	vii
Keyboard navigation.....	vii
IBM and accessibility.....	vii
How to provide feedback to IBM.....	vii
Introduction.....	9
Requirements.....	11
Technical requirements.....	11
Scheduling requirements.....	13
Planning.....	15
Authorization token usage rules or restrictions.....	16
Authorization token general rules.....	16
Authorization token replication.....	17
Using the Manage Remote Firmware Updates task.....	19
Generate an authorization token.....	19
Scheduling a Remote Code Load.....	21
Remote Code Load request actions on Resource Link.....	29
Remote Code Load requests table on Resource Link.....	31
View the scheduled remote firmware updates locally on the HMC by using the	
Manage Remote Firmware Updates task.....	33
Canceling a remote firmware update.....	35
Remote code load firmware update in progress.....	37
Dual-HMA HMC Remote Code Loads.....	39
 Appendix A. Notices.....	 43
Trademarks.....	43
Class A Notices.....	44

Safety

Safety notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

World trade safety information

Several countries require the safety information contained in product publications to be provided in their local language(s). If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the translated safety information with references to the US English source. Before using a US English publication to install, operate, or service this product, you must first become familiar with the related safety information in the *Systems Safety Notices*, G229-9054. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

All IBM zSystems and IBM LinuxONE (LinuxONE) models can use I/O cards such as FICON®, Open Systems Adapter (OSA), RoCE Express, Integrated Coupling Adapter (ICA SR, ICA SR1.1), zHyperLink Express, or other I/O features which are fiber optic based and utilize lasers (short wavelength or long wavelength lasers).

Laser compliance

All lasers are certified in the US to conform to the requirements of DHHS 21 CFR Subchapter J for Class 1 or Class 1M laser products. Outside the US, they are certified to be in compliance with IEC 60825 as a Class 1 or Class 1M laser product. Consult the label on each part for laser certification numbers and approval information.

Laser Notice: U.S. FDA CDRH NOTICE if low power lasers are utilized, integrated, or offered with end product systems as applicable. Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.

CAUTION: Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION: This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

About this publication

You can use this publication to guide you through the steps for remotely applying firmware updates.

Revisions

A technical change from the previous edition of this document is indicated by a thick vertical line to the left of the change.

Accessibility features

Accessibility features help users who have physical disabilities such as restricted mobility or limited vision use software products successfully. The accessibility features can help users do the following tasks:

- Run assistive technology such as screen readers and screen magnifier software.
- Operate specific or equivalent features by using the keyboard.
- Customize display attributes such as color, contrast, and font size.

Consult assistive technologies

Assistive technology products, such as screen readers, function with the user interfaces found in this product. Consult the product information for the specific assistive technology product that is used to access our product information.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

IBM and accessibility

See <http://www.ibm.com/able> for more information about the commitment that IBM® has to accessibility.

How to provide feedback to IBM

We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

For additional information use the following link that corresponds to your configuration:

Configuration	Link
IBM z16 Model A02	How to send feedback to IBM
IBM z16 Rack Mount Bundle	How to send feedback to IBM
IBM LinuxONE Rockhopper 4 Model LA2	How to send feedback to IBM
IBM LinuxONE Rockhopper 4 Rack Mount Bundle	How to send feedback to IBM

Introduction

The IBM z16™ and IBM z15™ (z15™) supports the Remote Code Load for IBM Z® Firmware (Remote Code Load) feature. This feature allows you to remotely schedule and install the most recent Remote Code Load firmware updates on your Hardware Management Console (HMC) or Support Element (SE). See [Figure 1](#) on page 9 for the process flow of a typical, successful Remote Code Load firmware update.

Note: There is communication between you and IBM Support, which is monitoring the firmware update.

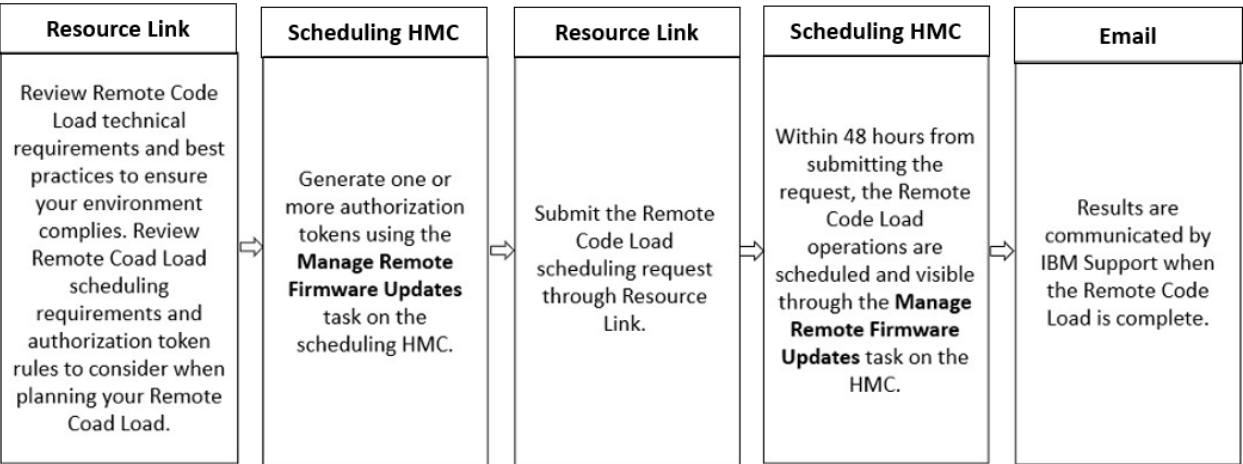


Figure 1. Remote Code Load firmware update process flow

This document takes you through the requirements and planning for setting up a Remote Code Load firmware update. It requires the use of the **Manage Remote Firmware Updates** task to acquire an authorization token, which is then used to schedule the Remote Code Load operation.

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

Requirements

This section describes the “[Technical requirements](#)” on page 11 and “[Scheduling requirements](#)” on page 13 that need to be considered before you can remotely install the firmware updates.

Technical requirements

See [Table 1 on page 12](#) for the technical requirements when you are installing firmware updates on an HMC or on an SE.

Table 1. Technical requirements

Remote Code Load on an HMC	Remote Code Load on an SE
• Targeted HMC must adhere to the following technical requirements: – HMCs must be updated before the SEs they manage so that they are always at an MCL level equal to or above the highest level SE they manage. – Using the View Console Information task, ensure that bundle level: - H05 (for Driver 51) or above is installed. - H37 (for Driver 41) or above is installed. – Ensure that a minimum of two call home servers are configured and available at the time of the Remote Code Load. This can be done by using the Customize Outbound Connectivity task to configure one of the two options: - Select the Use discovered callhome server consoles option with at least two HMCs listed. - Select the Use discovered callhome server consoles option with at least one HMC listed and select Enable the local console as a callhome server. – 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. – Ensure the target HMC is entitled under warranty or a hardware maintenance agreement. – Review the target HMC hardware messages to ensure it has no outstanding issues, is successfully backing up, and is consistently calling home.	• Targeted SE must adhere to the following technical requirements: – The target SE is being updated to a level equal to or less than the lowest level of the HMC managing it. – Using the System Information task, ensure that bundle level: - S05 (for Driver 51) or above is installed. - S56 (for Driver 41) 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, select Options, then select View All Call Home Servers, verify that a minimum of two or more HMCs are acting as a call-home server for the target SE and are available at the time of the Remote Code Load. – 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. – SE must be defined as an object to the scheduling HMC using the Add Object Definition task on the HMC. – Ensure the target SE is entitled under warranty or a hardware maintenance agreement. – Review the target SE hardware messages to ensure it has no outstanding issues, is successfully backing up, and is consistently calling home.

Table 1. 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 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 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.
• 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: – Must be local to the target SE they are calling home for. – Minimum of two call-home server consoles available to handle call home functions throughout the Remote Code Load operation (cannot be rebooting, installing MCLs, handling large amounts of traffic, etc.). – Using the View Console Information task, ensure that bundle level: - H05 (for Driver 51) or above is installed. - H37 (for Driver 41) 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>, SC28-7026, 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: – Must be local to the target SE they are calling home for. – Minimum of two call-home server consoles available to handle call home functions throughout the Remote Code Load operation (cannot be rebooting, installing MCLs, handling large amounts of traffic, etc.). – Using the View Console Information task, ensure that bundle level: - H05 (for Driver 51) or above is installed. - H37 (for Driver 41) 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>, SC28-7026, for setting up and testing the network configuration.)

Scheduling requirements

Ensure that following scheduling requirements are followed:

- Schedule the Remote Code Load firmware update to take place within a 2-day (48 hours) and 45-day timeframe out from the time the scheduling request was submitted.
- Remote Code Load firmware updates that are registered under the same customer number cannot be scheduled within 4 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 staged or 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 supplied in the local time zone of the system that you are targeting to install the MCLs on.

Note: The time zone field in Resource Link 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.

- Ensure that the Remote Code Load firmware updates that are scheduled do not conflict with other scheduled operations against the machine.
 - The **Manage Remote Firmware Updates** task lists all other Remote Code Load firmware updates that are scheduled through the HMC.
 - You can also check for more scheduled operations from the **Customize Scheduled Operations** task to avoid any potential scheduling conflicts.
- Specific process requirements for the Driver 41 Hardware Management Appliance (HMA) include the following:
 - When you apply firmware updates on a Driver 41 HMC, the HMC must be hosting the Alternate SE, otherwise, a check at the beginning of the Remote Code Load firmware update will prevent it from proceeding.
 - You can use the Virtual Support Element Management task on the HMC to verify that the HMC is hosting the Alternate SE. Ensure that **Alternate** is identified in the **Type** field under **SE Information**. If **Primary** is identified, then the HMC is hosting the Primary SE.

Note: You can perform an SE role switch by using the **Alternate Support Element** task, and then select the **Switch the Primary Support Element and the Alternate Support Element** option.

- The firmware update convention of the Driver 41 HMC hosting the Alternate SE at the time of a firmware update holds for every Driver 41 HMA unit. Since one of two peer HMCs will always be hosting the Primary, two firmware update sessions cannot take place on two IBM z15 Hardware Management Consoles without manual intervention to perform an SE switch in between. To update both peer Driver 41 HMCs, you must use the following general process today:
 1. Schedule for the first Remote Code Load firmware update to take place on the Driver 41 HMC that is hosting the virtual Alternate SE.
 2. Schedule for the second Remote Code Load firmware update to take place on the peer Driver 41 HMC at a minimum of 48 hours after the first Remote Code Load firmware update to ensure that there is enough time to manually perform an SE switch.
 3. After the first Remote Code Load firmware update on the Driver 41 HMC that is hosting the virtual Alternate SE completes successfully, you (the customer) must perform a manual SE switch so the peer Driver 41 HMC is now hosting the Alternate SE.
 4. After the second Remote Code Load firmware update completes, both HMCs are now updated.

Note: If the Driver 41 HMC is not hosting the Alternate SE by the time the second Remote Code Load firmware update begins, an initial check for this will prevent the firmware update operation from taking place.

- The previous step in this list (the bullet containing four numbered steps) is not necessary for HMCs that are Driver 51 and above in an HMA environment, as a single RCL operation will update both peer HMCs automatically (see [“Dual-HMA HMC Remote Code Loads”](#) on page 39 for more information).

Planning

This section describes the information that you need to know before you generate the authorization token, the information that you need to prepare ahead of scheduling, and the actions that you can take to submit the scheduling request.

Note: Some restrictions between a Remote Code Load firmware update and a Single Step Code Load firmware update, include the following:

- There are no options to opt out of the "Accept" step during the Single Step Code Load firmware update. The firmware updates that are installed on the system at the time of the Remote Code Load firmware update will be accepted and can no longer be removed.
- You cannot opt out of the "Retrieve" step of the Single Step Code Load firmware update.
- You can only "Target by Bundle" and you cannot "Install and Activate All" for a Remote Code Load firmware update.
- IBM z16 Driver 51 peer Hardware Management Appliance (HMA) HMCs must always be updated together by using a dual-HMA HMC Remote Code Load (see [“Dual-HMA HMC Remote Code Loads” on page 39](#)).

Before you can schedule a Remote Code Load, ensure you have access to the machine information reports. Use these reports to verify that all your machines are visible on Resource Link.

- To access your machine information from Resource Link, select **Tools** (from the left navigation pane) and then select **Machine information** (under **Servers**). The machine list is displayed.
 - If you are not registered to receive the machine information, select **Register for machine information**. The Machine information registration page is displayed. Provide your information for each of the fields, then click **Submit**. If you need assistance, select **Help for Machine information registration**.
- When you have access to the list of machines, you can select a machine and request an **EC/MCL report**. This displays the status of the latest bundles and MCLs for that machine.

For each Remote Code Load firmware update that you want to schedule, obtain the following information to be used or supplied for the Remote Code Load scheduling request form:

- 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 scheduling HMC (HMC containing the authorization token in the **Manage Remote Firmware Updates** task.)

Note: The backup location that is used for an SE is the Primary/Alternate HDD (even if backup to FTP is configured).

- For a Remote Code Load firmware update for either an HMC or SE:
 - 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 you are targeting to install the MCLs on.

Note: This is scheduled in the time zone of the system that you are targeting to install the MCLs on regardless of the time zone that is inputted into Resource Link.

- A valid authorization token.
 - This authorization token is generated on or replicated to the HMC that you are targeting to perform the Remote Code Load firmware updates on or generated on or replicated to a local HMC managing the SE that you want to perform the Remote Code Load firmware updates on.
 - This authorization token expires after seven days from generation regarding scheduling a session. To avoid a failed scheduling attempt by using an expired token, the Remote Code Load request must be submitted on Resource Link a minimum of 48 hours before the token is set to expire.

Note: For steps on how to generate the authorization token, see [“Using the Manage Remote Firmware Updates task”](#) on page 19. For determining which HMCs to generate the authorization token on, see [“Authorization token usage rules or restrictions”](#) on page 16.
- Service window information that the SSR needs for every Remote Code Load firmware update that is scheduled.

Note: Additional time needs to be added to the service window, greater than the amount of time you would have used for a traditional Single Step Code Load firmware update.
- Provide your contact name, email address, telephone number, and how you would prefer to be contacted so the IBM Support team monitoring the firmware updates can contact you with the results of the Remote Code Load firmware update. See the following example of information that is required for the email.

Authorization token usage rules or restrictions

This section discusses some authorization token usage rules or restrictions that need to be considered.

Authorization token general rules

This section describes some of the general authorization token rules.

- While the authorization token is still valid, it can be used to schedule a Remote Code Load firmware update between 2 days (48 hours) and 45 days in the future. Once the Remote Code Load firmware update is scheduled by using the authorization token, it does not matter if the authorization token expires after this date.
 - To schedule a Remote Code Load firmware update on an HMC, the authorization token must be generated on that same HMC or replicated to that HMC (IBM z16 Driver 51 only). One HMC cannot be used as a scheduling HMC for a Remote Code Load firmware update for another HMC. However, if there is a dual-HMA HMC Remote Code Load, then the target HMC's authorization token is used to schedule a Remote Code Load on itself and its peer.
 - Similar to how an MCL session targeting an SE must be started through an HMC, a Remote Code Load targeting an SE must be scheduled through a scheduling HMC using a token that is generated on or replicated to (IBM z16 Driver 51 only) that HMC. This scheduling HMC must be local to the SE it is targeting.
 - One authorization token that is generated on or replicated to (for IBM z16 Driver 51 only) an HMC can be used to schedule multiple Remote Code Load firmware updates through that scheduling HMC. 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 more than once if the initial scheduling was not successful and the authorization token is not expiring within 48 hours of the next Remote Code Load request submission.
- If multiple tokens are generated on or replicated to (for IBM z16 Driver 51 only) the same HMC, all tokens are valid for scheduling a Remote Code Load firmware update until they expire 7 days from creation. However, only the most recently generated token is displayed on the **Manage Remote Firmware Updates** task on the HMC.

Authorization token replication

Generated authorization tokens can be replicated from the IBM z16 HMC they are generated on to other peer or replica IBM z16 HMCs:

Note: Authorization tokens **cannot** be replicated across z15 HMCs.

- If not configured already, configure the HMC you would like to generate the authorization token from for data replication as a **Primary** or **Peer** role to other HMCs on the local network by using the **Configure Data Replication** task.
- If not configured already, configure the HMC to replicate the **Firmware Update Data** data type.
- Navigate to the **Manage Remote Firmware Updates** task on the same **Primary** or **Peer** HMC and generate an authorization token (see [“Generate an authorization token”](#) on page 19).
- Log on the **Peer** or **Replica** HMCs and navigate to the **Manage Remote Firmware Updates** task to ensure that the displayed authorization token matches the one you previously generated on the **Primary** or **Replica** HMCs.

Using the Manage Remote Firmware Updates task

This section describes the steps that are required before you schedule a Remote Code Load (RCL) request to remotely install firmware updates.

Use the **Manage Remote Firmware Updates** task on the HMC to receive an authorization token. This authorization token is used to schedule a Remote Code Load for firmware updates on an HMC and on any systems the HMC manages by using IBM Resource Link®.

Note: You need to generate only one authorization token on an HMC to be able to schedule Remote Code Load firmware updates on that HMC and any systems that HMC is managing.

Generate an authorization token

1. Log on to the HMC you would like to target for the Remote Code Load or an HMC local to the SE you would like to target for the Remote Code Load with a user ID that is assigned a SYSPROG user role.

Note: A user ID that is assigned a SERVICE user role can only view the Scheduled remote firmware updates table.

2. Open the **Manage Remote Firmware Updates** task. The Manage remote firmware updates window is displayed.
3. Select **Generate token**.

Manage remote firmware updates

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

 **Generate a token to authorize remote firmware updates.** [Generate token](#)

Scheduled remote firmware updates

All times displayed are local time

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

4. Before the token is generated, you must select the statement **I agree to allow IBM service to schedule remote firmware updates** and then click **Generate token** from the Authorize remote firmware updates window. If you decide you don't want to generate a token, then click **Cancel**.

×

Authorize remote firmware updates

By checking the box below and clicking "Generate token," you agree to allow IBM service to schedule remote firmware updates on one or more systems.

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

Once the token is generated, share it with IBM service to allow scheduling of remote firmware updates.

☒ I agree to allow IBM service to schedule remote firmware updates

Cancel

Generate token

- An authorization token is generated and is displayed in the task window, along with the expiration time remaining for the authorization token.

Note: The authorization token expires after seven days. All authorization tokens that are generated are valid and can be used up until they expire after seven days. The expiration date of the authorization token is displayed on the Manage Remote Firmware Updates window. Only the most recent authorization token that is generated is displayed in the task window.

i

Your remote firmware update authorization code is 493022.

Token expires in 06:14:49:20.

Copy token

Generate new token

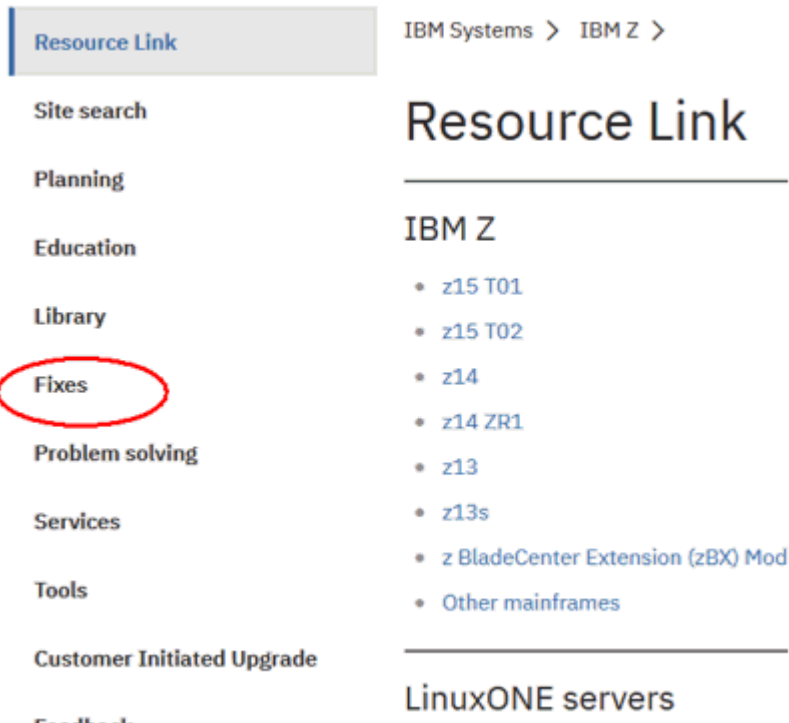
- Make note of the authorization token or use the **Copy token** selection. Also, make note which HMC this token corresponds to. This authorization token is needed when you are scheduling the remote code load from IBM Resource Link (see [“Scheduling a Remote Code Load”](#) on page 21).

Note: Once a Remote Code Load has been successfully scheduled, this task can also be used to cancel it from any HMC managing the SE object. This can be done at any point after the Remote Code Load has been successfully scheduled up to a minute before the Remote Code Load operation taking place. The steps to perform this are available in the [“View the scheduled remote firmware updates locally on the HMC by using the Manage Remote Firmware Updates task”](#) on page 33 .

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 requests** link.

Resource Link

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

Fixes

Your machine information

- z15 T01 (2)

Hardware

Known defects/problems

- Exception letters

Alerts

- Machine alerts
- Hiper alerts
- Red alerts

Report problems

- Hardware problem reporting

Downloads

- AROM images
- SUL images
- SUL control file

Licensed internal code

- Remote Code Load requests**
- System update levels (SUL)
 - Machine alerts

Software

Get fixes

- Download
- Check status of ordered fixes

Report problems

- Software problem reporting

Preventive actions

- Preventive Service Planning buckets (PSP)
- Subscribe to APARs
- Search for APARs

Maintenance

- z/OS and OS/390 enhanced holddata

Other resources

→ Shopz

4. The Remote Code Load requests page is displayed. This page contains a table of all Remote Code Load requests submitted for all IBM Z assets that are defined to the customer number(s) for your Resource Link account. Refer to the [“Remote Code Load requests table on Resource Link”](#) on page 31 for information on how to interface with this table.

Note: This table should be used to ensure that the Remote Code Load request you would like to submit is a minimum of 4 hours apart from other Remote Code Load requests that are scheduled or staged under your customer number(s) for your account. If possible, try to balance the amount of Remote Code Loads across time. You can also use this page to filter requests in the **Search** entry field.

5. To schedule a new firmware update, select the **Remote Code Load** link under **Schedule**.

Resource Link

Site search

Planning

Education

Library

Fixes

Problem solving

Services

IBM Systems > IBM Z > Resource Link > Fixes >

Remote Code Load requests

Search:

Help

- Help about Remote Code Load
- Remote Code Load for IBM Z Firmware (SC28-7044)
- Request assistance

When	Target	Bundle	Status	Submitted	Customer	W
2021-12-25 15:00 UTC	HMC M3AHMC3 2461 DK8MJA3 VA3	H02	Unknown	2021-12-08 19:53 UTC	B123456 Mike Co	Mi all
2021-12-15 15:41 UTC	HMC VAHMC34 2461 DKHMC34 VA3	H02	Complete	2021-12-15 15:38 UTC	B123456 IBM	De De
2021-12-15	HMC VAHMC34	H02	Complete	2021-12-15	B123456	De → Remote Code Load

The **Help** area includes links to:

- Summary information about Remote Code Load, select **Help about Remote Code Load**.
- Detailed information about Remote Code Load, select **Remote Code Load for IBM Z Firmware (SC28-7044)**.

- Assistance for scheduling a Remote Code Load from IBM Support, select **Request assistance**. This option will bring you to a page where you will need to complete fields for your contact information, system serial number, and an explanation of the assistance you require.

RCL request assistance

If you have questions or would like assistance scheduling a Remote Code Load session fill out the form below and our support team will reach out to you to assist.

The fields indicated with an asterisk (*) are required to complete this transaction; other fields are optional. If you do not want to provide us with the required information, close the window or tab that is displaying this page.

Customer name:*

Contact name:*

Contact information:
Email or Phone*

System serial number:*

Comment:

By submitting this form I agree that IBM may process my data in the manner indicated above and as described in IBM's [Privacy statement](#).

Submit

Once you submit your Remote Code Load help request, IBM Support contacts you with the next steps.

6. The Remote Code Load page is displayed to select the system to upgrade.

Resource Link

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

IBM Systems > IBM Z > Resource Link > Fixes >

Remote Code Load

Select system to upgrade.

Target:*

Continue

Help

[Help about Remote Code Load](#)

[Remote Code Load for IBM Z Firmware \(SC28-7044\)](#)

[Request assistance](#)

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

Note: If you select a Driver 51 HMC that is an HMA, which will be on 2461-VA3 (FC 0100) or 2461-SE4 (FC 0129) hardware, then the peer HMC to the one selected will also be targeted. See [“Dual-HMA HMC Remote Code Loads” on page 39](#) for more information.

Resource Link

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

IBM Systems > IBM Z > Resource Link > Fixes >

Remote Code Load

Select system to upgrade.

Target:*

Continue

Select one

Select one

HMC HMC1D50 2461 2461SE2 SE2

HMC MJAHMC1 2461 DK8MJA1 TW3

HMC MJAHMC2 2461 DK8MJA2 VA3

HMC MJAHMC3 2461 DK8MJA3 VA3

Help

[Help about Remote Code Load](#)
[Remote Code Load for IBM Z Firmware \(SC28-7044\)](#)
[Request assistance](#)

8. The Remote Code Load page is displayed with certain fields pre-filled.

Resource Link

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

IBM Systems > IBM Z > Resource Link > Fixes >

Remote Code Load

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

Customer number:

B123456

Target:

HMC MJAHMC1 2461 DK8MJA1 TW3

Schedule HMC:*

HMC MJAHMC1 2461 DK8MJA1 TW3

?

Current bundle:

H25

Target bundle:*

Select one

Date:*

Time (24 hour):*

HH:MM

Target time zone:*

(UTC-06:00) Central Time (US & Canada) (CST/CDT)

?

Authorization token:*

?

Backup location:*

Select one

Customer contact

Name:*

Jane Doe

Email:*

janedoe@gmail.com

?

Phone number:*

+1 555 555 5555

Company:*

Comment:

Submit

Help

[Help about Remote Code Load](#)
[Remote Code Load for IBM Z Firmware \(SC28-7044\)](#)
[Request assistance](#)

You need to provide additional information where an asterisk is displayed.

Customer number

Specifies the account number that is associated with the target machine serial number where the Remote Code Load firmware update will be applied.

Target

Specifies the HMC or SE identifier where the Remote Code Load firmware update will be applied, which is based on your selection from the previous page.

Schedule HMC*

From the drop-down list, select the HMC that was containing the authorization token that you would like to schedule through. This HMC must be local to the targets data center.

Notes:

- If the target system is an HMC, the **Schedule HMC** field will be pre-filled with the target HMC information, and no other HMCs will be listed in the drop-down. This is because a target HMC must act as its own scheduling HMC.
- If you are scheduling a dual-HMA HMC Remote Code Load in which a Driver 51 HMC, that is an HMA, was selected as the target in step “7” on page 23, then that HMC will also be the scheduling HMC used to generate the authorization token (not its peer that is also being targeted). See “Dual-HMA HMC Remote Code Loads” on page 39 for more information.

Current bundle

Specifies the currently installed bundle based on weekly data reports from your target system.

Target bundle*

From the drop-down list, select the target bundle identifier you would like your target system to have installed at the end of the Remote Code Load.

Date *

Use the calendar icon to schedule the date you would like the firmware update to take place. You need to ensure that there are 4 hours between multiple Support Element requests on the same scheduled HMC. Once the date is selected, it is displayed in this format: YYYY-MM-DD.

Note: The Remote Code Load request must be scheduled between 2 days (48 hours) and 45 days before execution.

Time (24 hour)*

Provide the time (HH:MM) in the input area.

Notes:

- Verify that the date and time that is provided is within the time zone that the target system is operating in. The time zone that the target system is operating in might be different than your local time zone or the local time zone of the target system. Ensure that you account for these possible differences by converting the time for this field to be in the time zone that the target system is operating in.
- If you are scheduling a dual-HMA HMC Remote Code Load in which a Driver 51 HMC, that is an HMA, was selected as the target in step “7” on page 23, then the Remote Code Load will be scheduled within the time zone of that HMC (not in the time zone of its peer that is also being targeted). See “Dual-HMA HMC Remote Code Loads” on page 39 for more information.

Target time zone*

Specify the time zone of the system that you are targeting to install the MCLs on.

Notes:

- The **Target time zone** field likely does not need to be manually changed, as it should be accurate based on weekly data reports from your target system. You can verify this is correct by checking the **Customize Console Date/Time** task on the HMC or the **Customize Date/Time** task on the SE.
- If you are scheduling a dual-HMA HMC Remote Code Load in which a Driver 51 HMC, that is an HMA, was selected as the target in step “7” on page 23, then the Remote Code Load will be scheduled within the time zone of that HMC (not in the time zone of its peer that is also being targeted). (See “Dual-HMA HMC Remote Code Loads” on page 39 for more information.)

Authorization token*

Provide the authorization token number in the input area. (Use the **Copy token** function from the **Manage Remote Firmware Updates** task or type the number in the input area.)

Backup location*

From the drop-down list, select the HMC backup location of **USB** or **FTP**.

Note: This field is only present if the target system is an HMC. If you are scheduling a dual-HMA HMC Remote Code Load in which a Driver 51 HMC, that is an HMA, was selected as the target in step “7” on page 23, both peer HMCs must back up to USB or back up to FTP; you cannot have one HMC back up to USB and its peer back up to FTP.

Customer contact*

Specifies the customer name, email, telephone number, and company name to be contacted with the results of the Remote Code Load. IBM Support contacts you with the results of the Remote Code Load by using the email or telephone number provided.

Note: Additionally, you can provide more than one email address, each one separated by a comma.

Comment

Provide service window information. Include any additional actions or contact information that might be needed. Here's a standard format of information that can be obtained and provided in the **Comments** section:

Service window length:

Contact preferences:

Additional comments

9. When all fields are complete, as shown in the following screen, click **Submit**. Ensure that there are no errors with the submission.

The screenshot shows the 'Remote Code Load' form in the IBM Systems console. The left sidebar contains a navigation menu with 'Fixes' selected. The main form area is titled 'Remote Code Load' and includes a breadcrumb trail: 'IBM Systems > IBM Z > Resource Link > Fixes >'. Below the title, a message states: 'Select the Hardware Management Console (HMC) where this remote code load will be scheduled.' The form fields are as follows:

- Customer number:** B123456
- Target:** HMC MJAHC3 2461 DK8MJA3 VA3 (HMA). A note below states: 'Note: HMC MJAHC2 will also be updated.'
- Schedule HMC:*** HMC MJAHC3 2461 DK8MJA3 VA3 (with a help icon)
- Current bundle:** H00
- Target bundle:*** H03 2021/08/16 (dropdown)
- Date:*** 2022-01-12 (calendar icon)
- Time (24 hour):*** 13:00
- Target time zone:*** (UTC-05:00) Eastern Time (US & Canada) (EST/EDT) (dropdown with help icon)
- Authorization token:*** 12345678 (help icon)
- Backup location:*** FTP (dropdown)
- Customer contact:**
 - Name:*** Jane Doe
 - Email:*** janedoe@email.com (help icon)
 - Phone number:*** +1 555 555 5555
 - Company:*** IBM
- Comment:** A text area containing the following text:
Service window length: xx hours
Contact preferences: email
Additional comments: N/A

At the bottom of the form is a black 'Submit' button.

Help

- Help about Remote Code Load
- Remote Code Load for IBM Z Firmware (SC28-7044)
- Request assistance

10. After the request is submitted, a summary of the request and the **Status history** of the submission is displayed.

Resource Link

Site search

Planning

Education

Library

Fixes

Problem solving

Services

Tools

Customer Initiated Upgrade

Feedback

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

Remote Code Load

Status:

Staged

Customer number:

B123456

Target:

HMC MJAHC3 2461 DK8MJA3 VA3 (HMA)

Note: HMC MJAHC2 will also be updated.

Schedule HMC:

HMC MJAHC3 2461 DK8MJA3 VA3

Associated CPC:

3931 02MJA02

Bundle:

H00 to H03

Date:

2022-01-20 13:00 EST (Eastern Standard Time)

UTC date:

2022-01-20 18:00 UTC

Authorization token:

12345678

Backup location:

FTP

Customer contact

Name:

Jane Doe

Email:

janedoe@email.com

Phone number:

+1 555 555 5555

Company:

IBM

Comment:

Service window length: xx hours
Contact preferences: email
Additional comments: N/A

Help

Help about Remote Code Load

Remote Code Load for IBM Z Firmware (SC28-7044)

Request assistance

Actions

Clone

Edit customer data

Cancel

Status history:

12 Jan 2022 19:22:21 GMT - Request staged by janedoe@email.com

11. At any point from now on, you can revisit this page containing the summary of your request, which allows you to monitor the status of your request. The status of the upgrade changes from **Staged** to **Scheduled** within 48 hours.

Note: If an error occurs while scheduling the Remote Code Load, the status changes to **Failed** and error text is displayed on the status page. IBM Support is notified by email when the status changes and notifies you with the next steps.

12. An email notification is sent to you when the request is scheduled, canceled, failed, or completed. The status is processed hourly and can also be monitored from Resource Link.

You can expect to receive the following emails:

- After the Remote Code Load request is scheduled successfully, an email from the Remote Code Load team that confirms the details of the remote code load and the assigned Remote Code Load case number.
- Approximately 30 - 60 minutes before the scheduled Remote Code Load, an email that reminds you that the Remote Code Load begins soon.
- Shortly after a successful start to the Remote Code Load, an email that confirms that the upgrade started.
- At the end of the Remote Code Load, an email that indicates that the upgrade completed.
- If a problem exists during the upgrade, an email that notifies you of the issue and the next actions to take.

Remote Code Load request actions on Resource Link

Use the appropriate **Actions** on the Resource Link summary page.

Clone

To create another Remote Code Load request similar to the request that was submitted, select **Clone**. This opens up a Remote Code Load submission that is pre-populated with selections you made in this Remote Code Load request. Note that some fields might be incorrect and require specific information for the new Remote Code Load, such as the authorization token and the date or time.

Edit customer data

To make updates to the customer contact information or comment field that you provided, select **Edit customer data**.

Reschedule

To make updates to the target bundle, date, time, and time zone to an RCL if the status is **Scheduled**. If these fields are updated to an already Scheduled RCL, check the **Manage Remote Firmware Updates** task on the scheduling HMC 48 hours after the **Reschedule** action was submitted to ensure that the changes took place.

Note: As these changes need to be delivered to the HMC, do not use the **Reschedule** action to make these changes within 48 hours of the RCL taking place. Instead, cancel the RCL locally on the scheduling HMC using the **Manage Remote Firmware Updates** task, see [“Canceling a remote firmware update” on page 35](#) for more information.

Cancel

To cancel the remote firmware upgrade, if the status is **Staged**, select **Cancel**. The request is canceled immediately.

If the **Status** of the remote firmware update is **Scheduled**, the option to cancel from Resource Link by selecting **Cancel** will stage a cancel request to be processed within 48 hours. Check the **Manage Remote Firmware Updates** task locally on the scheduling HMC within 48 hours of submitting the cancel request to ensure it was canceled. The Resource Link status will also indicate that the Remote Code Load is canceled if the request is processed successfully.

Note: As the cancellation needs to be delivered to the HMC, do not use the **Reschedule** action to make these changes within 48 hours of the RCL taking place. Instead, cancel the RCL locally on the scheduling HMC by using the **Manage Remote Firmware Updates** task, see [“Canceling a remote firmware update” on page 35](#) for more information.

Remote Code Load requests table on Resource Link

Each entry within the table corresponds to a Remote Code Load request that was submitted. This allows you to review the field selections made when submitting the Remote Code Load request. This also allows you to check the status of the Remote Code Load request:

- Staged requests have been submitted but have not been processed for scheduling yet.

Note: These requests should be processed for scheduling within 48 hours of being submitted. Once they are processed, their status will change to either **Scheduled** (if successful) or **Failed** (if an issue was encountered while scheduling). If the status of the request remains staged for over 48 hours, IBM Support will contact you with next steps.

- Scheduled requests have been successfully processed and are now visible from the **Manage Remote Firmware Updates** task on the scheduling HMC. Requests with this status indicate that the Remote Code Load is set to take place at the specified date and time on that target system (unless manually canceled).
- Failed requests either encountered an issue at the scheduling step in the process or the Remote Code Load execution step in the process. In either case, IBM Support will contact you with next steps.
- Canceled requests were staged requests that were canceled by the user on Resource Link or scheduled requests that were canceled by the user locally on the HMC using the **Manage Remote Firmware Updates** task.

Note: If the user cancels locally on the HMC using the **Manage Remote Firmware Updates** task, the request status on Resource Link will not change to Canceled immediately. It will take time for the status on Resource Link to update.

View the scheduled remote firmware updates locally on the HMC by using the Manage Remote Firmware Updates task

Once the Remote Code Load operation is set to **Scheduled** (see “Scheduling a Remote Code Load” on page 21), you can view the scheduled Remote Code Load firmware update from the **Manage Remote Firmware Updates** task.

1. Log on to the scheduling HMC specified for that Remote Code Load with a user ID that is assigned a SYSPROG or SERVICE user role.

Note: A user ID that is assigned a SERVICE user role can only view the Scheduled remote firmware updates table.

2. Open the **Manage Remote Firmware Updates** task. The Manage remote firmware updates window is displayed.
3. You can view the Remote Code Load firmware update entry in the Scheduled remote firmware updates table. The entry includes the target bundle that is applied to the system, the date and time the upgrade begins, the name of the system the firmware update is being applied to and the status of the Remote Code Load firmware update.

Note: The date of the upgrade is displayed in this format: MM/DD/YYYY.

Scheduled remote firmware updates					
	Target bundle	Date	Time ⓘ	Target name	Status
▼	H12	01/14/2021	03:01 AM	SYSOLD22	Scheduled 

The **Scheduled** status is displayed until the update begins, and changes to **In Progress** (see “Remote code load firmware update in progress” on page 37).

If you do not see an entry after 48 hours after the remote code load request has been submitted, a scheduling failure most likely occurred. IBM Support will contact you and let you know the next steps to take.

Canceling a remote firmware update

If you decide that you do not want to proceed with the Remote Code Load firmware update, then you can use the **Manage Remote Firmware Updates** task to cancel the Remote Code Load firmware update anytime after it is scheduled up to the minute before it begins.

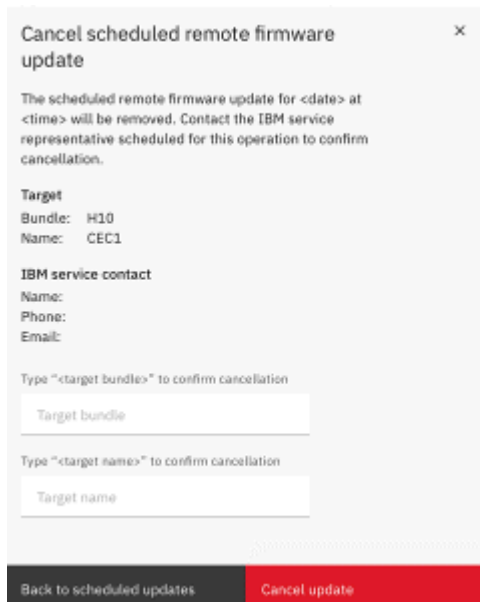
1. Log on to the scheduling HMC specified for that Remote Code Load with a user ID that has a SYSPROG user role.

Note: A user ID that is assigned a SERVICE user role can only view the Scheduled remote firmware updates table.

2. Go to the **Manage Remote Firmware Updates** task.

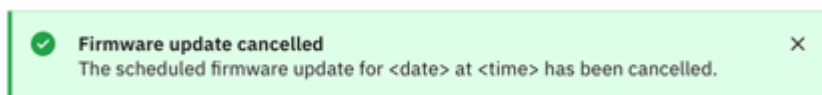
3. To remove the remote firmware update entry that you want to cancel, click the **Trash can**  icon that is displayed next to the status of the entry. The Cancel scheduled remote firmware update window is displayed.

Note: If the Trash can icon is disabled, the Remote Code Load firmware update has started, and the firmware update cannot be removed.



The screenshot shows a modal window titled "Cancel scheduled remote firmware update" with a close button (X) in the top right corner. The window contains the following text: "The scheduled remote firmware update for <date> at <time> will be removed. Contact the IBM service representative scheduled for this operation to confirm cancellation." Below this is a "Target" section with "Bundle: H10" and "Name: CEC1". An "IBM service contact" section follows with fields for "Name:", "Phone:", and "Email:". There are two input fields: "Type '<target bundle>' to confirm cancellation" with a placeholder "Target bundle", and "Type '<target name>' to confirm cancellation" with a placeholder "Target name". At the bottom are two buttons: "Back to scheduled updates" and "Cancel update".

4. To confirm the cancellation of the Remote Code Load firmware update, provide the target bundle and target name in the input areas of the Cancel scheduled remote firmware update window that you want to remove, then click **Cancel update**. The **Firmware update canceled** message is displayed in the task window.



Remote code load firmware update in progress

While the Remote Code Load firmware update is in progress, it cannot be canceled.

1. When the Remote Code Load firmware update begins at the specified date and time, the **In Progress** status is displayed.

Note: When the operation starts, it cannot be stopped.

Scheduled remote firmware updates					
Target bundle	Date	Time ⓘ	Target name	Status	
▼ H12	01/14/2021	03:01 AM	SYSDLD22	● In Progress	🗑
IBM service contact					
Name:					
Phone:					
Email:					

As the firmware update is progressing, IBM Support is remotely monitoring the progress of the firmware updates that the target system is transmitting and will communicate the results of the operation to you, by the email or telephone contact information supplied in the initial Remote Code Load request on Resource Link.

2. The Remote Code Load entry on this task is no longer displayed when the firmware update has completed. When the Remote Code Load firmware update completes, IBM Support relays the successful completion status by the email or telephone contact information supplied in the initial Remote Code Load request on Resource Link.

Note: If the Remote Code Load firmware update does not complete successfully, IBM Support will contact you with the details of the failure indication and with the follow-up actions. These actions might result with an SSR arriving to your site, if necessary.

Dual-HMA HMC Remote Code Loads

This section describes how the Remote Code Load functions differently for Driver 51 HMCs that are Hardware Management Appliances (HMAs), indicating that they are on 2461-VA3 (FC 0100) hardware or 2461-SE4 (FC 0129) hardware. These systems use dual-HMA HMC Remote Code Loads, in which a single Remote Code Load request submitted on Resource Link remotely installs firmware updates on both peer HMCs by using the following process:

1. Firmware updates are installed on the HMC that is hosting the virtualized Alternate SE at the time the Remote Code Load runs, which will be monitored remotely by IBM Support.
2. When the firmware updates complete successfully, an SE switch takes place so that the other, HMC (which is now down level) is hosting the virtualized Alternate SE.
3. Firmware updates are installed on the other HMC that is now hosting the virtualized Alternate SE, which will be remotely monitored by IBM Support.

Note: Dual-HMA HMC Remote Code Loads do not apply to stand-alone Driver 51 HMCs that have been upgraded from Driver 41 (IBM z15) or Driver 36 (IBM z14) HMCs and are on the following hardware:

2461-SE3 (FC 0063)
2461-TW3 (FC 0062)
2461-SE2 (FC 0083)
2461-TW2 (FC 0082)

Additionally, dual-HMA HMC Remote Code Loads do not apply to any SEs.

Dual-HMA HMC Remote Code Loads introduces a new concept of an orchestrating HMC. One of the peer HMA HMCs function as the orchestrating HMC, which indicates that this HMC:

- Is the target HMC selected from the initial drop-down when scheduling on Resource Link (see step [“7” on page 23](#)).
- Is the scheduling HMC (see step [“8” on page 24](#)) containing the authorization token used to schedule.
- Functions as the target system from which the time zone will be used to start the Remote Code Load operation within. If the orchestrating HMC is in a different time zone than its peer, the Remote Code Load will start within the time zone of the orchestrating HMC.

The process for scheduling a dual-HMA HMC Remote Code Load follows:

1. As dual-HMA HMC Remote Code Loads target two peer HMCs hosting to install firmware updates, ensure:
 - a. Both of these HMCs adhere to the target technical requirements, see [“Technical requirements” on page 11](#).
 - b. Both of these HMCs are communicating to one another over the local network by using ports **em1** or **em2**.
 - c. The SE virtualized on these HMCs is **not** in Service Required State (use the **Service Required State Query** task) and the SE switch is not blocked (use the **Query Switch Capabilities** action from the **Alternate Support Element** task).
 - d. The SE virtualized on these HMCs is defined to both HMCs as an object by using the **Add Object Definition** task.
2. Generate or replicate over the authorization token on the orchestrating HMC. See [“Generate an authorization token” on page 19](#), for this process.
3. Submit a Remote Code Load request on Resource Link targeting the orchestrating HMC containing the authorization token. See [“Scheduling a Remote Code Load” on page 21](#), for this process. Following are a few differences that you will see:
 - a. After you select the orchestrating HMC as your target system, Resource Link will display both peer HMCs as the targets as seen in the following example.

Target: HMC HMC8F167B 2461 DK92016 VA3 **(HMA)**
Note: HMC HMC2CEB8T will also be updated.

- b. The orchestrating HMC functions as the target system and the scheduling HMC. Therefore, the authorization token must come from the orchestrating HMC. Additionally, the target time zone also comes from the orchestrating HMC.
- c. Both peer HMCs must share backup type. The peer HMCs must either back up to USB or back up to FTP. One HMC **cannot** back up to FTP while the other HMC backs up to FTP.

The following figure shows an example of a dual-HMA HMC Remote Code Load submission.

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

Remote Code Load

Status:	Staged
Customer number:	B123456
Target:	HMC MJAHMC3 2461 DK8MJA3 VA3 (HMA) Note: HMC MJAHMC2 will also be updated.
Schedule HMC:	HMC MJAHMC3 2461 DK8MJA3 VA3
Associated CPC:	3931 02MJA02
Bundle:	H00 to H03
Date:	2022-01-20 13:00 EST (Eastern Standard Time)
UTC date:	2022-01-20 18:00 UTC
Authorization token:	12345678
Backup location:	FTP
Customer contact	
Name:	Jane Doe
Email:	janedoe@email.com
Phone number:	+1 555 555 5555
Company:	IBM
Comment:	Service window length: xx hours Contact preferences: email Additional comments: N/A

Status history:

- 12 Jan 2022 19:22:21 GMT - Request staged by janedoe@email.com

4. You can perform any of the actions that are outlined in [“Remote Code Load request actions on Resource Link”](#) on page 29, against this Remote Code Load request.
5. Once the Remote Code Load is successfully scheduled, it can be viewed and/or canceled by using the **Manage Remote Firmware Updates** task on both of the peer HMCs. For more information on the

process, see [“View the scheduled remote firmware updates locally on the HMC by using the Manage Remote Firmware Updates task”](#) on page 33 and [“Canceling a remote firmware update”](#) on page 35.

6. Once the Remote Code Load begins, it can be viewed as in progress by using the **Manage Remote Firmware Updates** task on both of the peer HMCs. See [“Remote code load firmware update in progress”](#) on page 37 for information.
7. You will receive the same email notifications for a dual-HMA HMC Remote Code Load as you do for a traditional Remote Code Load.

Appendix A. Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprise is entirely coincidental.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)® are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on <http://www.ibm.com/trademark>.

Class A Notices

The following Class A statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

United Kingdom Notice

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2014/30/EU on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55032. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 (0) 800 225 5423 or +49 (0) 180 331 3233
email: halloibm@de.ibm.com

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Japan Voluntary Control Council for Interference (VCCI) Notice

この装置は、クラス A 機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

V C C I - A

The following is a summary of the Japanese VCCI statement above:

This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Japan Electronics and Information Technology Industries Association (JEITA) Notice

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値：IBM Documentationの各製品
の仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

These statements apply to products greater than 20 A, single-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

回路分類：6（単相、P F C回路付）

換算係数：0

These statements apply to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

回路分類：5（3相、P F C回路付）

換算係数：0

People's Republic of China Notice

警告:在居住环境中,运行此设备可能会造成无线电干扰。

Declaration: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may need to perform practical action.

Taiwan Notice

CNS 13438:

警告使用者：

此為甲類資訊技術設備，
於居住環境中使用時，
可能會造成射頻擾動，在此種情況下，
使用者會被要求採取某些適當的對策。

CNS 15936:

警告：為避免電磁干擾，本產品不應安裝或使用於住宅環境。

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용(A급)으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의
지역에서 사용하는 것을 목적으로 합니다.

Germany Compliance Statement

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.

New Orchard Road

Armonk, New York 10504

Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH

Technical Regulations, Abteilung M372

IBM-Allee 1, 71139 Ehningen, Germany

Tel: +49 (0) 800 225 5423 or +49 (0) 180 331 3233

email: halloibm@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse A.

Electromagnetic Interference (EMI) Statement - Russia

ВНИМАНИЕ! Настоящее изделие относится к классу A.

В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры



SC28-7044-02

