

IBM Z 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 39](#), and *IBM Systems Environmental Notices and User Guide*, Z125–5823.

This edition, SC28-7068-00, applies to the IBM z17 Model ME1 and IBM LinuxONE Emperor 5 Model ML1.

There might be a newer version of this document in a **PDF** file available on **IBM Documentation**.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 Z** or **IBM LinuxONE**, then select your configuration, and click **Library Overview** on the navigation bar.

© **Copyright International Business Machines Corporation 2025.**

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.....	vi
Laser safety information.....	vi
Laser compliance.....	vii
About this publication.....	ix
Revisions.....	ix
Accessibility features.....	ix
Consult assistive technologies.....	ix
Keyboard navigation.....	ix
IBM and accessibility.....	ix
How to provide feedback to IBM.....	ix
Chapter 1. Introduction	1
Chapter 2. Requirements.....	3
Technical requirements.....	3
Scheduling requirements.....	5
General scheduling requirements.....	5
Remote Code Load on the Hardware Management Appliance.....	6
Driver 41 HMA scheduling requirements.....	7
Driver 51 HMA Scheduling Requirements.....	7
Chapter 3. Planning.....	9
Restrictions.....	9
Authorization token usage.....	9
Sourcing an authorization token.....	9
Authorization token attributes.....	10
Authorization token replication.....	10
Chapter 4. Using the Manage Remote Firmware Updates task.....	11
Generate an authorization token.....	11
Chapter 5. Scheduling a Remote Code Load.....	13
Chapter 6. Remote Code Load request actions on Resource Link.....	21
Chapter 7. Remote Code Load requests table on Resource Link.....	23
Chapter 8. Update Staged Requests on Driver 61 Schedule HMCs.....	25
Chapter 9. View the scheduled remote firmware updates locally on the HMC by using the Manage Remote Firmware Updates task.....	27
Chapter 10. Canceling a remote firmware update.....	29
Chapter 11. Remote code load firmware update in progress.....	31

Chapter 12. Driver 61 Remote Code Load alert notifications.....	37
Appendix A. Notices.....	39
Trademarks.....	39
Class A Notices.....	40

Safety

Safety notices

Safety notices may be printed throughout this document. **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.

DANGER notices:

DANGER: To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables. (D001)

DANGER: If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, **STOP**. Ensure the improper voltage or impedance conditions are corrected before proceeding. (D003)

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

DANGER: Heavy equipment — personal injury or equipment damage might result if mishandled. (D006)



DANGER: When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard: If IBM supplied the power cord(s), connect power to this unit only with the IBM provided power cord. Do not use the IBM provided power cord for any other product. Do not open or service any power supply assembly. Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.



- The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords. For AC power, disconnect all power cords from their AC power source. For racks with a DC power distribution panel (PDP), disconnect the customer's DC power source to the PDP.
- When connecting power to the product ensure all power cables are properly connected. For racks with AC power, connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate. For racks with a DC power distribution panel (PDP), connect the customer's DC power source to the PDP. Ensure that the proper polarity is used when attaching the DC power and DC power return wiring.
- Connect any equipment that will be attached to this product to properly wired outlets.
- When possible, use one hand only to connect or disconnect signal cables.
- Never turn on any equipment when there is evidence of fire, water, or structural damage.
- Do not attempt to switch on power to the machine until all possible unsafe conditions are corrected.
- When performing a machine inspection: Assume that an electrical safety hazard is present. Perform all continuity, grounding, and power checks specified during the subsystem installation procedures to ensure that the machine meets safety requirements. Do not attempt to switch power to the machine until all possible unsafe conditions are corrected. Before you open the device covers, unless instructed otherwise in the installation and configuration procedures: Disconnect the attached AC power cords,

turn off the applicable circuit breakers located in the rack power distribution panel (PDP), and disconnect any telecommunications systems, networks, and modems.

- Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.

To Disconnect: 1) Turn off everything (unless instructed otherwise). 2) For AC power, remove the power cords from the outlets. 3) For racks with a DC power distribution panel (PDP), turn off the circuit breakers located in the PDP and remove the power from the Customer's DC power source. 4) Remove the signal cables from the connectors. 5) Remove all cables from the devices.

To Connect: 1) Turn off everything (unless instructed otherwise). 2) Attach all cables to the devices. 3) Attach the signal cables to the connectors. 4) For AC power, attach the power cords to the outlets. 5) For racks with a DC power distribution panel (PDP), restore the power from the Customer's DC power source and turn on the circuit breakers located in the PDP. 6) Turn on the devices.



- Sharp edges, corners and joints may be present in and around the system. Use care when handling equipment to avoid cuts, scrapes and pinching. (D005)

CAUTION notices:

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)

CAUTION: The doors and covers to the product are to be closed at all times except for service by trained service personnel. All covers must be replaced and doors locked at the conclusion of the service operation. (C013)

CAUTION: Ensure the building power circuit breakers are turned off BEFORE you connect the power cord or cords to the building power. (C023)

CAUTION: 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. (C003)



CAUTION: This equipment is not suitable for use in locations where children are likely to be present. (C052)

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 Z® and IBM LinuxONE (LinuxONE) models can use I/O cards such as FICON®, Open Systems Adapter (OSA), Network Express, Integrated Coupling Adapter 2.0 SR (ICA SR2.0), 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)



IEC 1068/14

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 z17® Model ME1	How to send feedback to IBM
IBM LinuxONE Emperor 5 Model ML1	How to send feedback to IBM

Chapter 1. Introduction

The Driver 41 (Version 2.15.0) and above Hardware Management Console (HMC), Hardware Management Appliance (HMA), and Support Element (SE) support the Remote Code Load (RCL) for IBM Z Firmware feature. This feature allows an authorized user to remotely schedule and install the most recent firmware updates (Machine Change Levels (MCLs)). This secure firmware update operation calls home with live progress updates that are remotely monitored by IBM support. See [Figure 1 on page 1](#) for the process flow of a typical, successful Remote Code Load firmware update.

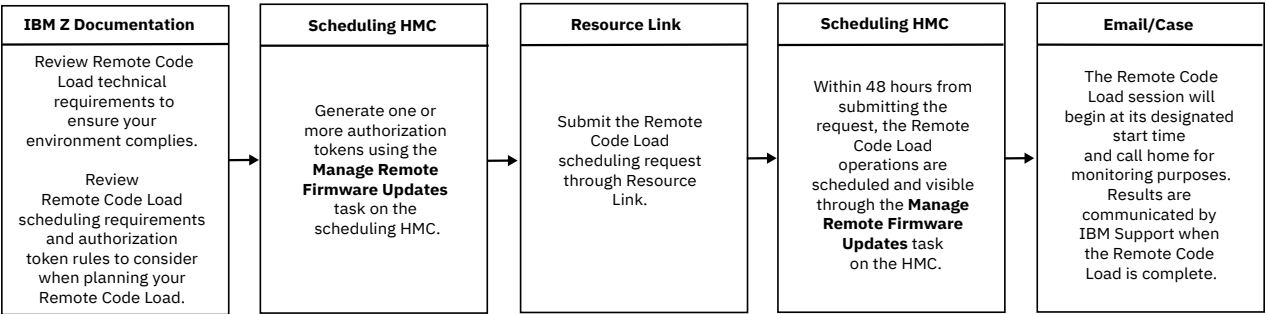


Figure 1. Remote Code Load firmware update process flow

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.

Chapter 2. Requirements

This section describes the “[Technical requirements](#)” on page 3 and “[Scheduling requirements](#)” on page 5 that must be followed to use Remote Code Load.

Technical requirements

See [Table 1](#) on page 3 and [Table 2](#) on page 4 for the technical requirements when using Remote Code Load to install firmware updates on an HMC or SE.

Table 1. Technical requirements - Part 1 of 2	
Remote Code Load on an HMC	Remote Code Load on an SE
<ul style="list-style-type: none">Targeted HMC must adhere to the following technical requirements:<ul style="list-style-type: none">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:<ul style="list-style-type: none">H04 (for Driver 61) or above is installed.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 firmware update. This can be verified using the Customize Outbound Connectivity task, in which the table under the Call-Home Server Consoles section must list at least two HMCs.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.Using the Block Automatic Licensed Internal Code Change Installation task, ensure that the Block automatic Licensed Internal Code Change Installation setting is disabledEnsure the target HMC is entitled under warranty or a hardware maintenance agreement.Review the target HMC hardware messages to ensure it is successfully backing up and consistently calling home.	<ul style="list-style-type: none">Targeted SE must adhere to the following technical requirements:<ul style="list-style-type: none">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:<ul style="list-style-type: none">S04 (for Driver 61) or above is installed.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 Block Automatic Licensed Internal Code Change Installation task, ensure that the Block automatic Licensed Internal Code Change Installation setting is disabledUsing 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.

Table 2. Technical requirements - Part 2 of 2

Remote Code Load on an HMC	Remote Code Load on an SE
<ul style="list-style-type: none"> Targeted HMC must adhere to the following technical requirements (continued): <ul style="list-style-type: none"> If the HMC is in an HMA environment, ensure: <ul style="list-style-type: none"> It shares a common subnet with its peer HMC The hosted Primary SE is defined and communicating as an object to both peer HMCs. For Driver 51 HMCs only: Automatic Switch is enabled for the hosted virtualized Primary SE, which can be checked using the Query Switch Capabilities function in the Alternate Support Element task 	<ul style="list-style-type: none"> Targeted SE must adhere to the following technical requirements (continued): <ul style="list-style-type: none"> 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 is successfully backing up and consistently calling home. If the SE is in an HMA environment, ensure: <ul style="list-style-type: none"> It shares a network with both of the peer HMCs hosting it It is defined as an object to both of the peer HMCs hosting it.
<ul style="list-style-type: none"> Using the Authorize Internal Code Changes task, ensure that the Do not allow installation and activation of internal code changes option is not selected. 	<ul style="list-style-type: none"> Using the Service Status task, ensure that the Disable service status option is selected. 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 2. Technical requirements - Part 2 of 2 (continued)

Remote Code Load on an HMC	Remote Code Load on an SE
<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – Must be local to the target HMC 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: <ul style="list-style-type: none"> - 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.) 	<ul style="list-style-type: none"> • All HMCs acting as call-home servers for the SE must adhere to the following technical requirements: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> - 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 the scheduling requirements covered in this chapter are followed.

General scheduling requirements

Ensure that the 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.
- Each system is restricted to one Remote Code Load firmware update with a “Staged” or “Scheduled” status. It must reach completion or be canceled before attempting to schedule another Remote Code Load firmware update.
- The selected start time of a Remote Code Load firmware update occurs within the operational time zone of the system targeted for the firmware update, which will display under the “Time zone” field in the Resource Link form.
 - The time zone field in Resource Link is informational and can be confirmed using the **Customize Console Date / Time** task on an HMC or the **Customize Date / Time** task on an SE.

- Ensure that the Remote Code Load firmware update does not conflict with other scheduled operations on the system targeted for the installation, which can be checked using the **Customize Scheduled Operations** task.
- RCLs targeting systems registered to the same customer number must be spaced out a minimum of 4 hour apart, with the following exceptions:
 - An RCL targeting a Driver 51 (Driver 2.16.0) and above HMC may be scheduled within 4 hours of RCL(s) targeting other Driver 51 (Version 2.16.0) and above HMCs so long as all non-call home capable HMC(s) have a minimum of one "Added" or "Discovered" call home server defined that is not scheduled to perform an RCL within the same 4 hour window.

Note: Account for at least one call home capable HMC to be available during the window to monitor the RCL sessions.

- An RCL targeting a z16 Driver 51 (Version 2.16.0) and above SE can be scheduled within 4 hours of another z16 Driver 51 (Version 2.16.0) and above SE RCL so that a maximum of two (2) RCLs targeting z16 Driver 51 (Version 2.16.0) and above SEs occur within a 4-hour window.

See [Figure 2 on page 6](#) for more information.

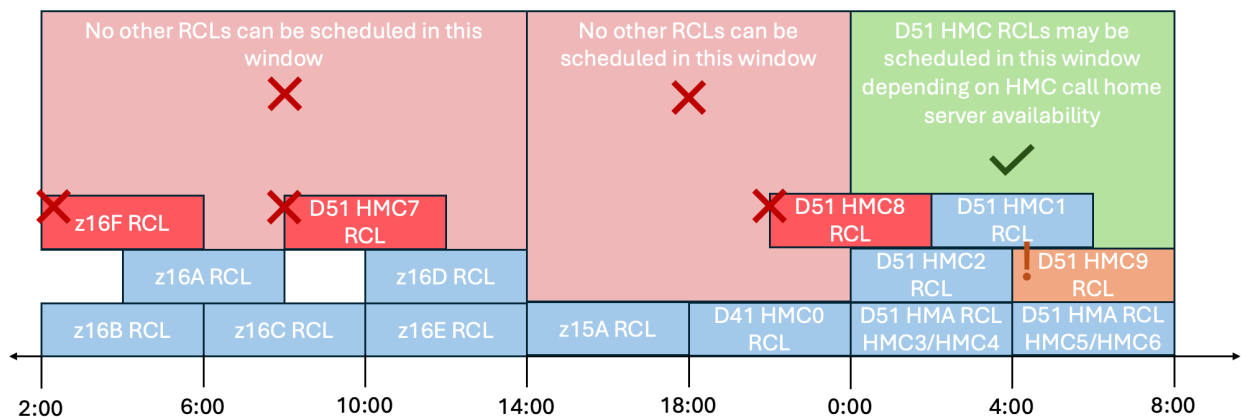


Figure 2. Example of scheduling RCLs

Figure 2 on page 6 is an example timeline of RCL scheduling windows for systems that all share the same customer number. The timestamps shown in this timeline are in UTC, and the shown RCL windows are converted to UTC from the operational timezone of the target system. In [Figure 2 on page 6](#):

- z16F RCL can not be scheduled at 2:00 because its window would overlap with z16A's and z16B's RCL windows. This is blocked because a maximum of two overlapping D51 or above SE RCL windows may be scheduled.
- HMC7 RCL can not be scheduled at 8:00 because its window would overlap with z16D's and z16E's RCL windows. This is blocked because a D51 or above SE RCL window cannot overlap with any HMC RCL windows.
- HMC8 RCL can not be scheduled at 8:00 because its window would overlap with HMC0's RCL window. This is blocked because D41 RCL windows cannot overlap with any other RCL window.
- It is not recommended to schedule HMC9 RCL at 4:00 because it is not call-home capable, it uses only HMC1 and HMC5 as its call home servers, and its window overlaps with HMC1 and HMC5's RCL windows. Although scheduling this RCL will not be logically blocked, neither of HMC9's call home servers would not be available for the first half of HMC9's window.

Remote Code Load on the Hardware Management Appliance

The following restrictions apply to Remote Code Load firmware updates on Hardware Management Appliances based on driver level:

Driver 41 HMA scheduling requirements

- Specific process requirements for the Driver 41 Hardware Management Appliance (HMA) include the following:

Note: The following section does not apply to HMCs that are Driver 51 (Version 2.16.0) and above in an HMA environment, as a single RCL operation will update both peer HMCs automatically. See [“Driver 51 HMA Scheduling Requirements” on page 7](#) for more information.

- When you apply firmware updates on a Driver 41 HMC, the HMC must be hosting the Alternate SE at the start time of the Remote Code Load firmware update. Otherwise, a check at the beginning of the Remote Code Load firmware update will block 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 Driver 41 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 with sufficient time after the first Remote Code Load firmware update 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 must perform a manual SE switch so the peer Driver 41 HMC is now hosting the Alternate SE. This is not done automatically at the Driver 41 HMC level, and it must be done manually by the client team.
 4. After the second Remote Code Load firmware update completes, both Driver 41 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.

Driver 51 HMA Scheduling Requirements

This section describes how Remote Code Load functions for Driver 51 HMCs that are Hardware Management Appliances (HMAs). These systems use dual-HMA HMC Remote Code Loads, in which a single Remote Code Load request submitted on Resource Link installs firmware updates on both peer HMCs through the following process:

1. Firmware updates are first installed on the HMC that is hosting the virtualized Alternate SE at the time the Remote Code Load starts, which will be monitored remotely by IBM Support.
2. When the firmware updates complete successfully, the hosted virtualized SEs automatically switch roles, so that the peer HMC is hosting the virtualized Alternate SE.
3. Firmware updates are installed on the peer HMC that is now hosting the virtualized Alternate SE, which will be remotely monitored by IBM Support.

Notes:

- Dual-HMA HMC Remote Code Loads do not apply to stand-alone rack-mount or tower Driver 51 HMCs that have been upgraded from Driver 41 (IBM z15) or Driver 36 (IBM z14) HMCs.

- Dual-HMA HMC Remote Code Loads do not apply firmware to the hosted virtual SEs. This still requires scheduling a separate Remote Code Load operation targeting the SE.
- Both Driver 51 (Version 2.16.0) and above peer HMCs in a Hardware Management Appliance (HMA) environment must always be updated together by using a Dual-HMA HMC RCL.

For a Dual-HMA HMC Remote Code, the initially selected target HMC will also act as the schedule HMC (that the authorization token resides on). The Dual-HMA HMC RCL begins with respect to the operational timezone of this scheduling HMC as well, regardless of which HMC updates first.

Chapter 3. Planning

This section describes the restrictions applicable to Remote Code Load as well as the general rules that apply to the authorization-token functionality.

Restrictions

The following general restrictions apply to all Remote Code Load firmware updates:

- 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.
- There are no options to opt out of the "Accept" step during the RCL firmware update. The firmware updates that are installed on the system at the start time of the RCL firmware update will be accepted and can no longer be removed.
- You cannot opt out of the "Retrieve" step of the RCL firmware update.
- You can only "Target by Bundle" and you cannot "Install and Activate All" for a Remote Code Load firmware update.
- Remote Code Load utilizes the same installation mechanisms as a Single Step MCL Installation operation, as used for onsite firmware maintenance. Therefore, you should plan to be unable to perform any other operations against your target HMC or SE or CPC/LPARs at this time, including Power On Reset, Activate, IPL, Load, and so on. It is recommended you plan a service window for your Remote Code Load in which no other scheduled activity is planned to take place. The length of this window varies based on the size and amount of MCLs being installed, which the service window should account for with extra buffer time.

Authorization token usage

An authorization token must be generated on an HMC and provided in the Remote Code Load scheduling form on Resource Link. This section discusses authorization token usage rules or restrictions that need to be considered.

Sourcing an authorization token

This section describes how an authorization token is sourced and its relation to the schedule HMC specified on Resource Link.

- The authorization token provided in the Remote Code Load scheduling form on Resource Link must be either be sourced through:
 - Generation using the **Manage Remote Firmware Updates** task on the selected schedule HMC specified in the same form
 - Replication to the schedule HMC specified in the same form (for IBM Driver 51 (Version 2.16.0) and above HMCs only).
- The following restrictions apply when selecting the schedule HMC:
 - If the RCL target is an HMC, that same HMC must also act as its own schedule HMC. This HMC must be where the authorization token provided in the RCL scheduling form was generated on or replicated to (for Driver 51 and above only).
 - If the RCL target is an SE, the schedule HMC may be any HMC the SE is defined to that adheres to the HMC call-home server technical requirements (see [“Technical requirements” on page 3](#)). The selected HMC must be where the authorization token provided in the RCL scheduling form was generated on or replicated to (for Driver 51 and above only).

Authorization token attributes

This section describes the attributes of an authorization token.

- An authorization token is valid for scheduling an RCL session for 7 days after it is generated.
Note: It takes an average of 6 to 12 hours (maximum 48 hours) to automatically process the RCL request, at which point the token must still be valid.
- If multiple tokens are generated on or replicated to the same HMC, all tokens are valid for scheduling a RCL firmware update until they expire (7 days from creation). However, only the most recently generated or replicated token is displayed on the **Manage Remote Firmware Updates** task on the HMC.
- The authorization token is not single-use. The same authorization token can be used to schedule multiple RCL firmware updates targeting different systems.

Authorization token replication

Authorization tokens can be replicated from the Driver 51 or above HMC they are generated on to other Peer or Replica Driver 51 or above HMC(s) via the following steps:

Note: Authorization tokens **cannot** be replicated across IBM Driver 41 (Version 2.15.0) HMCs

- Use the **Configure Data Replication** task to configure the roles between each of your HMCs, in which authorization tokens generated on Primary or Peer HMCs will be replicated to their corresponding Replica or Peer HMCs.
Note: The option to generate authorization tokens on a Replica HMC is disabled. Configuring an HMC as a Replica will overwrite any prior authorization tokens on the Replica HMC with the authorization tokens from its Primary HMC.
- When configuring the Peer or Replica HMCs through the **Configure Data Replication** task, select the "Firmware Update Data" data type to enable the replication of authorization tokens
- When an authorization token is generated using the **Manage Remote Firmware Updates** task on a Primary or Peer HMC, it will also display on the **Manage Remote Firmware Updates** task of its Replica or Peer HMC(s) configured with the "Firmware Update Data" data type. (see ["Generate an authorization token" on page 11](#)).

Chapter 4. Using the Manage Remote Firmware Updates task

This section describes the steps that are required on the schedule HMC before you submit a scheduling request to remotely install firmware updates.

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

Generate an authorization token


1. Log on to the schedule HMC with a user ID that is assigned a SYSPROG user role:
 - If you are scheduling an RCL targeting an HMC, log on to that HMC.
 - Otherwise, if you are scheduling an RCL targeting an SE, log on to any HMC the SE is defined to that adheres to the HMC call-home server technical requirements.

Note: A user ID that is assigned a SERVICE user role has view-only access to this task and cannot generate an authorization token.

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

Manage remote firmware updates

View and cancel firmware updates.


 Generate a token to authorize remote firmware updates.

Generate token

Updates in-progress

Bundle	Date	Time ⓘ	Target	Scheduling HMC	Status ⓘ
No updates in-progress.					

Scheduled updates



Bundle	Date	Time ⓘ	Target	Scheduling HMC	Status ⓘ
No scheduled updates.					

Completed updates

4. Before the token is generated, you must select the statement **I agree to let IBM access my environment remotely**, 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 remote access to your environment to perform firmware updates on one or more systems in the environment.

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

☒ I agree to let IBM access my environment remotely.

Cancel

Generate token

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

Note: Only the most recent authorization token that is generated is displayed in the task window.

?

Your remote firmware update authorization code is 44032220. Token expires in 06d : 23h : 59m : 54s

Generate new token

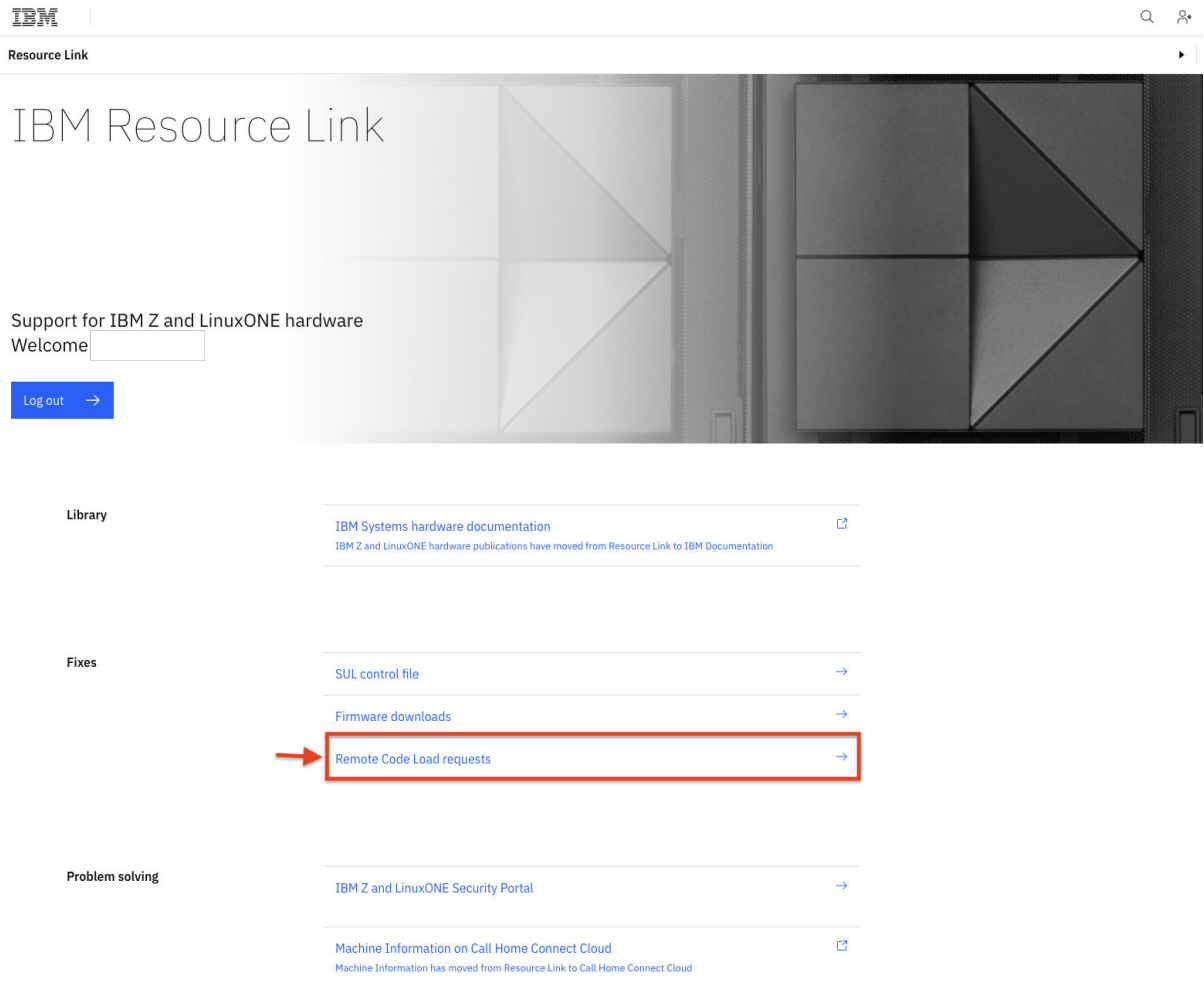
6. Make note of the authorization token and the HMC it corresponds to.

Note: If the HMC is a Primary or Peer for data replication of the "Firmware Update Data" data type, any of its Replica or Peer HMCs can use the same token as well.

Chapter 5. 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/support/resourcelink/> and log on with your user ID and password.
2. From the main page, select **Remote Code Load requests**.



3. 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) registered to your Resource Link IBMId. Refer to the [Chapter 7, “Remote Code Load requests table on Resource Link,”](#) on page 23 for information on how to interface with this table.
4. To submit a Remote Code Load firmware update scheduling request, select the **Schedule a Remote Code Load** link at the top of the table.

Remote Code Load requests

[Schedule a remote code load →](#)

Filter table						
When	Target	Bundle	Status	Customer	Contact	Submitted
2024-02-24 05:00 UTC	HMC HMC1 2461 SE4 3931 0012345	H21	Complete	IBM12345 IBM	John Doe johndoe@ibm.com	2024-02-20 17:33 UTC
2024-02-24 07:00 UTC	HMC HMC2 2461 SE4 3931 0012345	H21	Scheduled	IBM12345 IBM	Jane Doe janedoe@ibm.com	2024-02-20 21:01 UTC
Items per page: 10 ▾		1–10 of 2 items			1 ▾ of 1 pages	◀ ▶

5. The Remote Code Load requests page is displayed.

IBM

Resource Link

Remote Code Load requests

Remote Code Load request

Create new request

Target

Select one ▾ →

Select a target console then click the arrow button

Schedule HMC

Select one ▾

Current bundle

Target bundle

Select one ▾

Date

yyyy-mm-dd 📅

Time

HH:MM

Time zone

Select one ▾

UTC date

yyyy-mm-dd HH-MM UTC

Authorization token

Feedback

6. From the drop-down list of target consoles, select the HMC or SE you want to install the MCLs on, then select the blue arrow button beside the dropdown to proceed.

Notes:

- If you select a Driver 51 or above HMC that is in an HMA environment, this will be a Dual-HMA HMC Remote Code Load operation. This will be indicated by a blue pop up underneath the target dropdown, which will state "[Peer HMC information] will also be updated".

Target

HMC1 2461 DK12345 SE4 ▾ →

i

HMC HMC1 2461 DK12345 SE4 additional information

– HMC HMC2 2461 DK54321 SE4 will also be updated

See [“Driver 51 HMA Scheduling Requirements”](#) on page 7 for more information.

- If the dropdown contains inaccurate or missing systems, please send a request for the system(s) to be added or adjusted via an email to **reslink@us.ibm.com** with your sales representative or account team on copy. This email should contain the customer number, machine type, and serial number(s) pertaining to the system(s) of interest.

7. Once the target is selected, the remaining fields of the scheduling form can now be completed.

[Remote Code Load requests](#)

Remote Code Load request

Create new request

Target
P0012345 9175 0212345 ME1

Schedule HMC
Select one

Current bundle
S06

Target bundle
Select one

Date
yyyy-mm-dd

Time
HH:MM

Time zone
America/New York

Preset to target SE ZDD05P 9175 02C04F8 ME1 date/time customization time zone (not editable)

UTC date
yyyy-mm-dd HH:MM UTC

Authorization token

Customer contact
Name
Jane Doe

Email address
janedoe@ibm.com

Phone number

Company

Comment (optional)
(optional)

Submit

Notes:

- Upon selecting your target, some fields may pre-populate with information pertaining to that system.
- Target systems with exceptions reported by the last weekly system availability data transmission will display in the dropdown as “Ineligible for Remote Code Load”. Selecting an ineligible target system will display additional exception details in red. Scheduling an RCL against this system will be blocked until the exception is reported as resolved by the most recent system availability data transmission.

Target

HMC1 2461 DK12345 SE4



HMC HMC1 2461 DK12345 SE4 does not support remote code load

- Change management is not fully enabled on this HMA HMC.
 - Use the Transmit system availability data option under Customize Console Services to send back health check data and try the operation again or contact your service representative for assistance.
- Change management is not fully enabled on the peer HMA HMC.
 - Use the Transmit system availability data option under Customize Console Services to send back health check data and try the operation again or contact your service representative for assistance.

Target

Specifies the HMC or SE identifier where the Remote Code Load firmware update will be applied.

Schedule HMC

From the drop-down list, select the HMC that the authorization token was generated on or replicated to (for IBM Driver 51 and above only).

Note: 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 schedule HMC, meaning the authorization token provided in the form must reside on it. For a Dual-HMA HMC Remote Code Load, the listed peer HMC does not act as the schedule HMC.

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. 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. The request must also adhere to the 4 hour spacing scheduling requirement described in [“General scheduling requirements” on page 5](#).

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 the target system physically resides in.
- If you are scheduling a dual-HMA HMC Remote Code Load, then the Remote Code Load schedules with respect to the time zone of the target HMC selected in step “6” on [page 14](#) (not in the time zone of its peer that is also being targeted). See [“Driver 51 HMA Scheduling Requirements” on page 7](#) for more information.

Target time zone

The operational time zone of your target system. This field is automatically populated with the correct selection using 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.

Authorization token

Input the authorization token generated on or replicated to the specified schedule HMC.

Backup location

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

Notes:

- If you are scheduling a dual-HMA HMC Remote Code Load, both peer HMCs must back up to the same type of location; you can not have one HMC back up to USB and its peer back up to FTP.
- The backup selection is not available on the Remote Code Load scheduling request form when targeting an SE because the SE will backup to its hard drive disk.

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 using the email address(es) provided.

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

Comment

Provide service window information. Include additional considerations or notes using this field.

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

[Remote Code Load requests](#)

Remote Code Load request

Create new request

Target

P0012345 9175 0212345 ME1



Schedule HMC

HMC1 2461 DK12345 SE4



Current bundle

S06

Target bundle

S07



Date

2025-06-07



Time

09:00

Time zone

America/New York



Preset to target SE ZDD05P 9175 02C04F8 ME1 date/time customization time zone (not editable)

UTC date

2025-06-07 13:00 UTC

Authorization token

12345678

Customer contact

Name

Jane Doe

Email address

janedoe@ibm.com

Phone number

1-800-426-7378

Company

IBM

Comment (optional)

A service window is scheduled from 09:00 EDT to 14:00 EDT.

Submit



9. After the request is submitted, a summary of the request is displayed.

Remote Code Load request

[Clone as new request](#) →

Status

Staged

Customer number

1234567

Target

SE P0012345 9175 0212345 ME1

Schedule HMC

HMC HMC1 2461 DK12345 SE4

Bundle

S06 to S07

Target bundle

S07

Date

2025-06-07

Time

09:00

Time zone

America/New York

UTC date

2025-06-07 13:00 UTC

Authorization token

12345678

Customer contact

Name

Jane Doe

Email address

janedoe@ibm.com

Phone number

1-800-426-7378

Company

IBM

Comment (optional)

A service window is scheduled from 09:00 EDT to 14:00 EDT

Status history



10. 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 Remote Code Load request status changes from **Staged** to **Scheduled** within 48 hours. See [Chapter 7, “Remote Code Load requests table on Resource Link,” on page 23](#) for more information.

Notes:

- If an error occurs while scheduling the Remote Code Load, the status changes to **Failed**, error text is displayed on the status page, and IBM Support will contact you via email.
 - Optionally, additional steps can be taken to update the request status sooner on Driver 61 schedule HMCs (see [Chapter 8, “Update Staged Requests on Driver 61 Schedule HMCs,” on page 25](#) for more information).
11. An email notification is sent to you when the request status changes throughout the lifespan of the Remote Code Load. The status can also be viewed from Resource Link.

You can expect to receive the following emails:

- Shortly after the Remote Code Load request is submitted on Resource Link, an acknowledgement email will be sent.
- 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.

Chapter 6. Remote Code Load request actions on Resource Link

The following Remote Code Load management actions can be performed from the Resource Link summary page.

Clone as new request

To create another Remote Code Load request similar to the request that was submitted, select **Clone as new request** the top of the page. 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.

Note: All fields will copy over with the following exceptions:

- Timezone
- Current bundle
- Target bundle
- Date* (if the source date / time is not a minimum of 48 hours in the future).

Edit customer contact

To make updates to the customer contact information or comment field that you provided, select **Edit customer contact**. This can be done at any point on a **Staged** or **Scheduled** Remote Code Load request.

Reschedule request

To make updates to the target bundle, date, and time of an RCL targeting a Driver 51 (Version 2.16.0) and above system. This can be done while the RCL status is **Scheduled** up to 48 hours before the RCL's start time. As this is a remote option, it is recommended to check the **Manage Remote Firmware Updates** task on the scheduling HMC after 48 hours of submitting the **Reschedule** request to ensure all updates were successfully processed.

Notes:

- RCLs that will take place within 48 hours or Driver 41 (Version 2.15.0) RCLs can instead be canceled through the **Manage Remote Firmware Updates** task on the scheduling HMC and another scheduling request may be submitted for a later time. See [Chapter 10, "Canceling a remote firmware update,"](#) on page 29 for more information.
- A Remote Code Load request may be rescheduled within 4 hours of a request with a Driver 61 (Version 2.17.0) schedule HMC. However, after staging the new **Reschedule** request from Resource Link, a "Request update" operation must be manually performed from that HMC immediately afterward (see [Chapter 8, "Update Staged Requests on Driver 61 Schedule HMCs,"](#) on page 25 for more information).

Cancel request

To cancel the RCL targeting a Driver 51 (Version 2.16.0) and above system. This can be done while the RCL status is **Staged** or **Scheduled** up to 48 hours in advance of its start time. As this is a remote option, it is recommended to check the **Manage Remote Firmware Updates** task on the schedule HMC after 48 hours of submitting the cancel request to ensure it was canceled.

Note: If you would like to cancel an RCL within 48 hours of its start time, it can instead be canceled through the **Manage Remote Firmware Updates** task on the schedule HMC. See [Chapter 10, "Canceling a remote firmware update,"](#) on page 29 for more information.

Chapter 7. Remote Code Load requests table on Resource Link

Each entry within the Remote Code Load requests table on Resource Link corresponds to a Remote Code Load request that was submitted. This allows you to review and/or alter the details of previous Remote Code Load scheduling requests and check their statuses, which indicate the following:

- Staged - The RCL form has been submitted but has 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 blocked by a scheduling check or 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 - The RCL form has been processed for scheduling by the schedule HMC and is set to take place at the specified date and time on that target system (unless manually canceled).
- Failed - The RCL 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 - The RCL was canceled while it was Staged or Scheduled. This was done either by a user on ResourceLink or by an HMC user through 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.

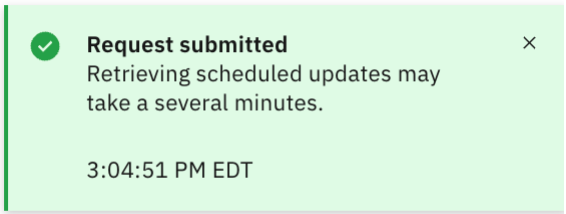
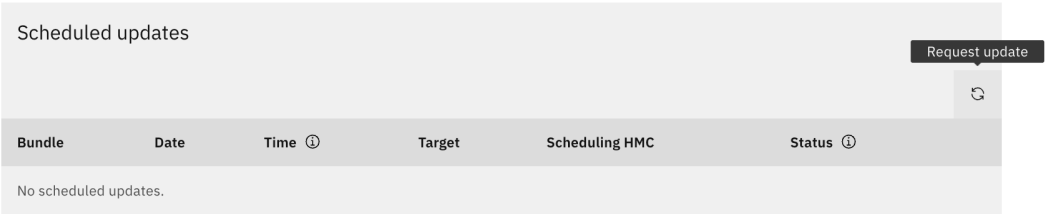
- Complete - The Remote Code Load completed successfully

Chapter 8. Update Staged Requests on Driver 61 Schedule HMCs

The "Request Update" option is available on Driver 61 (Version 2.17.0) HMCs to immediately process newly Staged or Rescheduled Remote Code Load request(s). This option must be used when a user submits a Reschedule request within 48 hours of a Remote Code Load's original start time.

Note: The option to perform the Request Update action is not available on Driver 51 (Version 2.16.0) and below HMCs. Instead, the wait period of up to 48 hours must be adhered to for the Staged Remote Code Load requests to be automatically processed.

1. Log on to the schedule HMC specified for that Remote Code Load with a user ID that is assigned a SYSPROG or SERVICE user role.
2. Open the **Manage Remote Firmware Updates** task. The **Manage Remote Firmware Updates** window is displayed.
3. Select the "Request update" refresh icon within the "Scheduled updates" table. A green pop up confirming the request was submitted will briefly display.



4. The HMC will query any new Staged or Rescheduled Remote Code Load requests that list it as the schedule HMC. If all health checks are passed and the request(s) successfully schedule, they will display in the Scheduled updates table within a few minutes (see [Chapter 9, "View the scheduled remote firmware updates locally on the HMC by using the Manage Remote Firmware Updates task,"](#) on [page 27](#) for more information).

Note: If a scheduling blockage is encountered or no RCL requests listing this HMC as a schedule HMC are found, nothing will display on the HMC. The reason for the scheduling blockage will instead display on Resource Link afterwards.


Scheduled updates						
Bundle	Date	Time ⓘ	Target	Scheduling HMC	Status ⓘ	
S07	6/7/25	09:00 AM	P0012345	HMC1	Scheduled	🗑️

Chapter 9. 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 [Chapter 5, “Scheduling a Remote Code Load,”](#) on page 13), you can view the scheduled Remote Code Load firmware update from the **Manage Remote Firmware Updates** task.

1. Log on to the schedule HMC specified for that Remote Code Load with a user ID that is assigned a SYSPROG or SERVICE user role.
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 updates** table. The entry includes the target bundle that will be applied to the system, the date and time the upgrade begins, the name of the target system, the name of the scheduling HMC (RCLs targeting Driver 51 and above systems only), 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 updates						
Bundle	Date	Time ⓘ	Target	Scheduling HMC	Status ⓘ	
S07	6/7/25	09:00 AM	P0012345	HMC1	Scheduled	

The **Scheduled** status is displayed until the Remote Code Load firmware update begins and changes status during the RCL firmware update (see [Chapter 11, “Remote code load firmware update in progress,”](#) on page 31).


If you do not see an entry after 48 hours after the remote code load request has been submitted, a scheduling check blockage or scheduling issue most likely occurred. IBM Support will contact you with the next steps to take.

Chapter 10. Canceling a remote firmware update

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

1. Log on to the schedule HMC specified for that 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. To cancel a Remote Code Load firmware update, 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: This option will be revoked after the Remote Code Load begins, as it can not be cancelled once it is in progress.

Cancel scheduled remote firmware update

×

The scheduled remote firmware update for 6/7/25 at 09:00 AM will be removed.

Bundle	Date	Time	Target
S07	6/7/25	09:00 AM	P0012345

Type CANCEL to confirm cancellation

CANCEL

Back to scheduled updates

Cancel update

4. Follow the prompt to cancel the RCL. Once this is performed, the **Firmware update canceled** message is displayed in the task window

✓

Firmware update cancelled The scheduled firmware update for 6/7/25 at 09:00 AM has been cancelled.

×

Chapter 11. Remote code load firmware update in progress

This section describes what will occur when the Remote Code Load operation begins and is in progress.

- While an IBM support agent will provide email notification that your Remote Code Load operation began, this can also be confirmed using the **Manage Remote Firmware Updates** task during the Remote Code Load.
- One call home case per target system updated will open for monitoring purposes during your Remote Code Load operation. These cases are a normal part of the Remote Code Load operation and will be closed by IBM support.
 - HMC RCL cases will contain the following subject: CALL HOME - REMOTE CODE LOAD PROB TYPE: M CPN: ## REF: E502F743
 - SE RCL cases will contain the following subject: CALL HOME - REMOTE CODE LOAD PROB TYPE: M CPN: ## REF: E002E7B6
- While the Remote Code Load firmware update is in progress, it cannot be canceled.
- If you are tracking the progress of an HMC RCL firmware update through its own **Manage Remote Firmware Updates** task, you may briefly lose visibility to this progress tracking when the HMC reboots.
- A feature that allows for additional details about the Remote Code Load operation progress to display in the **Manage Remote Firmware Updates** task is available on:
 - Driver 61 (Version 2.17.0) HMCs
 - Driver 51 (Version 2.16.0) HMCs that have bundle H16 or above installed and at least on z16 SE at bundle S21 or above defined.

The enablement of this feature can be checked on a Driver 51 (Version 2.16.0) HMC through the **Manage Firmware Features** task, in which the "Support for determinate in progress Remote Code Messages" entry will display as "Enabled".

Note: After installing the enablement bundles on your Driver 51 (Version 2.16.0) HMCs and SEs, you may need to reboot your HMC using the **Power Off or Restart** task for the features described previously in this section to display as "Enabled".

- The progress displayed for your Remote Code Load operation may vary depending on configuration. Please see the section that applies to your situation.
 - An HMC without the feature enabled:
 - Displays the status of an ongoing Remote Code Load operation as "In Progress" for itself and all defined SEs
 - Once the Remote Code Load operation completes, it will no longer display in the **Manage Remote Firmware Updates** task

Scheduled remote firmware updates				
Target bundle	Date	Time ⓘ	Target name	Status
▼ H12	01/14/2021	03:01 AM	SYSDLD22	● In Progress

- An HMC with the feature enabled:
 - Displays Remote Code Load operation in the "Updates in-progress" table with a status of "Updating" for defined Driver 51 SEs that are below bundle S21 and all defined Driver 41 SEs

- Displays Remote Code Load operation in the “Updates in-progress” table with a status of “Updating” alongside a percentage for itself, all defined Driver 61 SEs, and all defined Driver 51 SEs at or above bundle S21.

Updates in-progress						
Bundle	Date	Time ⓘ	Target	Scheduling HMC	Status ⓘ	
▼ H18	9/26/23	02:00 PM	HMC1, HMC2	HMC1	Updating... 10% ▬	🗑

Clicking on “Updating” will display a pop up with additional information pertaining to what step the Remote Code Load operation is currently on as well as a description of the step.

Remote firmware update H18 - HMC1

Backing up critical data...

10% complete

Back up critical data: make a backup of the targeted platform so that if the 1U server needs to be replaced, it can be restored from this data.

▶ [More details](#)

Close

The "More details" drop down on this pop-up will display the steps that have been completed in addition to the remaining steps.

Remote firmware update H18 - HMC1

Backing up critical data...

10% complete

Back up critical data: make a backup of the targeted platform so that if the 1U server needs to be replaced, it can be restored from this data.

▼ [More details](#)

✓

Verify environment

○

Back up critical data

Accept installed changes

Retrieve internal code changes

Apply internal code changes

Transmit system availability data

Close

Note: The percent progress correlates to one of the steps that comprise a Remote Code Load operation, which can cause the percentage to abruptly jump between steps.

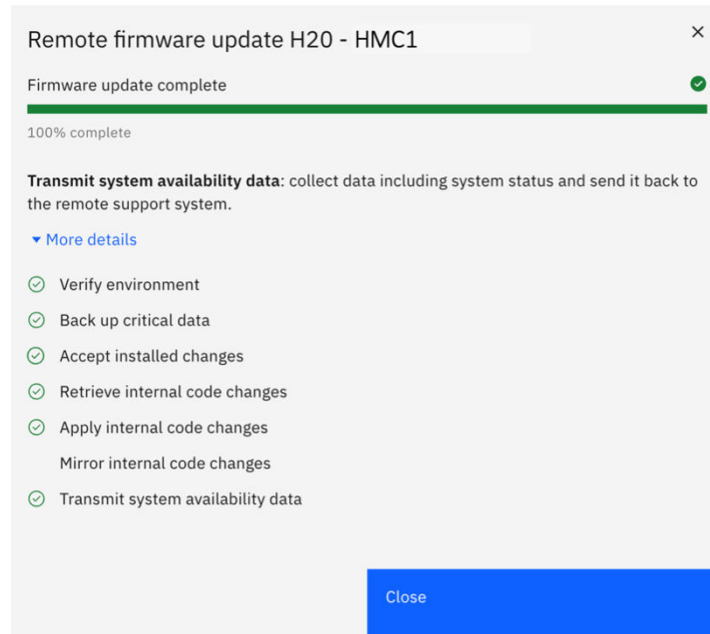
- Once the Remote Code Load operation completes, a record of it will display in the "Completed Updates" table of the **Manage Remote Firmware Updates** task.

Completed updates					
Bundle	Date	Time ⓘ	Target	Scheduling HMC	Status ⓘ
H21	2/22/24	09:00 AM	HMC1, HMC2	HMC1	Completed
S29	2/20/24	05:40 PM	P0012345	HMC3	Pending
H21	2/22/24	09:55 AM	HMC1, HMC2	HMC2	Failed

The Remote Code Load entry for a completed update will display one of the following statuses:

Completed

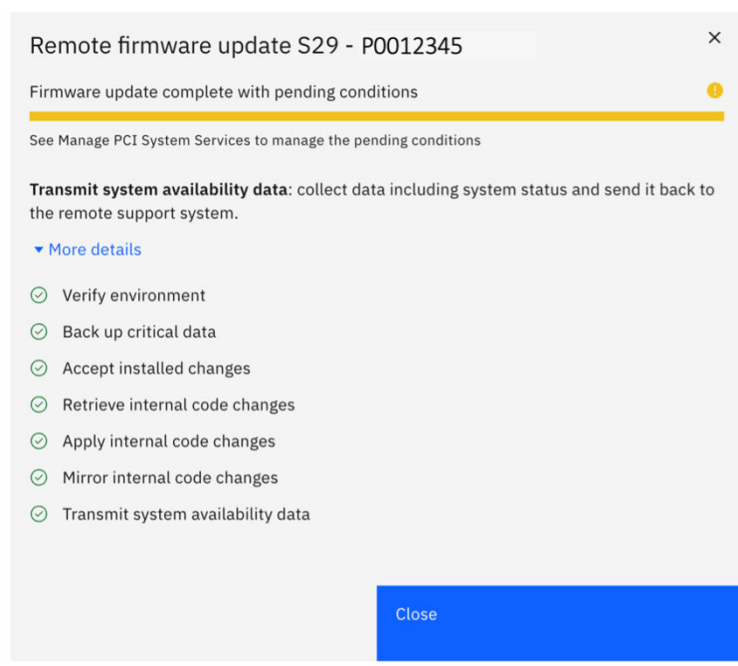
The Remote Code Load operation completed successfully. Clicking “Completed” will display the a pop-up similar to the following that shows all steps completed:



Note: A checkmark will not display next to the mirror step for an HMC Remote Code Load record, as this step is not performed on HMCs.

Pending

The Remote Code Load operation completed successfully and left pending conditions that will need to be manually cleared afterwards by the user. Clicking “Pending” will display the a pop-up similar to the following that shows all steps completed:

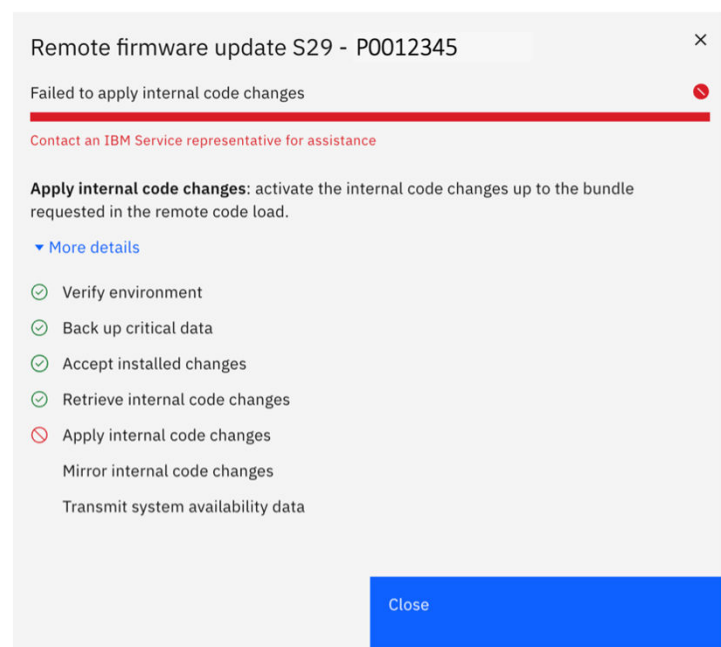


Notes:

- The task used to manage the pending conditions (listed under the yellow progress bar) may vary.
- This status indicates that an RCL operation left a pending condition on your CPC and will remain as "Pending" even after the pending condition is cleared.

Failed

The Remote Code Load operation encountered an issue and therefore did not complete successfully. The IBM Support agent remotely monitoring your Remote Code Load will reach out soon with additional information. Clicking "Failed" will display which step the failure was encountered at:



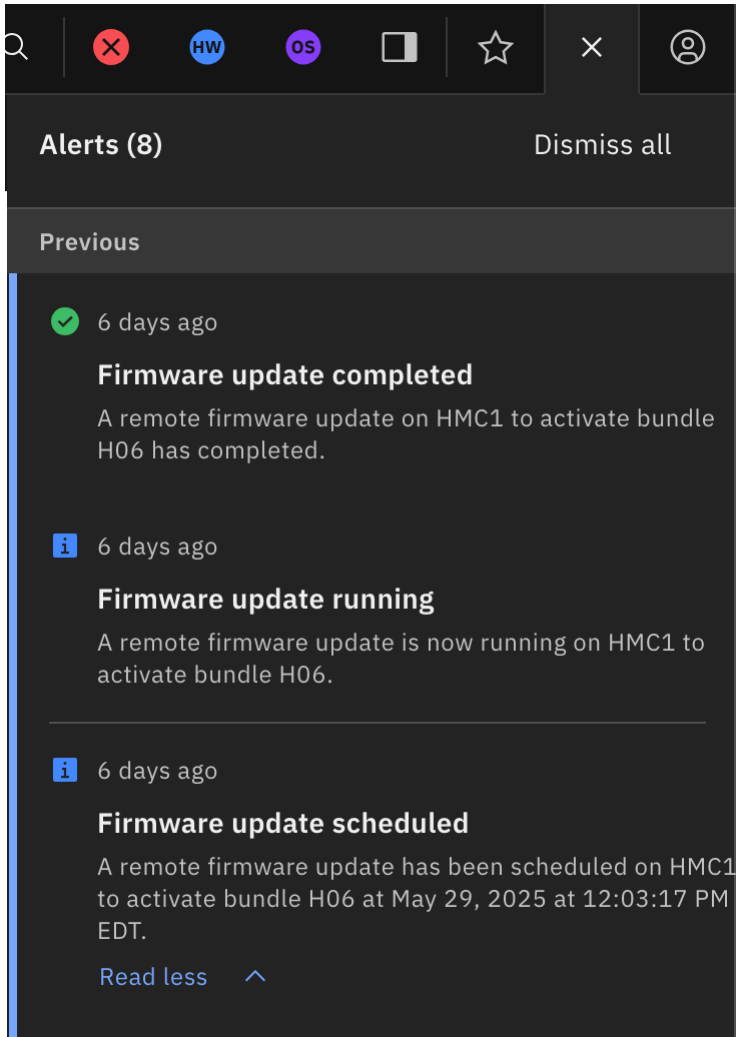
When the Remote Code Load firmware update completes, IBM Support relays the successful completion status by the email contact information supplied in the initial Remote Code Load request on Resource Link.

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

Chapter 12. Driver 61 Remote Code Load alert notifications

Users will receive alert notifications for Remote Code Load events pertaining to the Driver 61 system they are logged into. These alerts include notifications for the following events:

- A Remote Code Load was successfully scheduled targeting the system
- A Remote Code Load firmware update has begun
- A Remote Code Load firmware update finished with its completion status.



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 А.

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

Electromagnetic Interference (EMI) Statement - Kingdom of Saudi Arabia Notice

قد يتسبب هذا المنتج في حدوث تداخل إذا تم استخدامه في المناطق السكنية.

ويجب تجنب هذا الاستخدام ما لم يتخذ المستخدم تدابير خاصة لتقليل الانبعاثات الكهرومغناطيسية لمنع التداخل مع استقبال البث الإذاعي والتلفزيوني.

تحذير: هذا الجهاز متوافق مع الفئة أ من SASO CISPR 32

في البيئة السكنية، قد يتسبب هذا الجهاز في حدوث تداخل لاسلكي.



SC28-7068-00

