



# **Return to Factory Image information**

## **Element Software**

NetApp  
April 17, 2024

This PDF was generated from [https://docs.netapp.com/us-en/element-software/hardware/concept\\_rtfti\\_configure.html](https://docs.netapp.com/us-en/element-software/hardware/concept_rtfti_configure.html) on April 17, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Return to Factory Image information ..... 1
  - Configure the Return to Factory Image ..... 1
  - RTFI deployment and installation options ..... 1
  - The RTFI process..... 2
  - RTFI options menu..... 4

# Return to Factory Image information

## Configure the Return to Factory Image

NetApp SolidFire storage systems use the Return To Factory Image (RTFI) process to write a software image to a new node or restore a node to its original factory state. The RTFI process securely erases all existing data and configurations (if any) and installs an unconfigured NetApp Element software image. The RTFI process is available for all SolidFire nodes.

SolidFire systems use one RTFI process for all Element software installations. This includes internal manual installations performed by developers, automatic installations by automated framework tests, field installations by service engineers and customers, and installations performed by various integrators and partners. The same RTFI process is used on all SolidFire nodes, regardless of the chassis or node type in use, to automatically fix any issues.

The intended audience for this guide is integrators who install, configure, use, or troubleshoot storage-related issues.

- **Linux:** You have some background with Linux systems.
- **Networking:** You have a familiarity with server networking and networked storage, including IP addresses, netmasks, and gateways.



The RTFI process is data destructive and securely erases all data and configuration details from the node and installs a new operating system. Verify that the node used for the RTFI process is not active as part of a cluster.

Deploy and install the RTFI International Organization for Standardization (ISO) image and perform the RTFI process:

- [RTFI deployment and installation options](#)
- [Perform the RTFI process](#)
- [RTFI options menu](#)

## Find more information

- [SolidFire and Element Software Documentation](#)
- [Documentation for earlier versions of NetApp SolidFire and Element products](#)

## RTFI deployment and installation options

The Return To Factory Image (RTFI) process uses a bootable, installable media with a completely self-contained, minimalistic Linux OS to deploy Element software on a node. You can download the RTFI ISO image specific to your Element software version from the [NetApp support site](#).

After you download the RTFI ISO image, you can deploy it according to one of the following commonly used methods:

- **Physical USB key:** You can write a bootable Element software ISO to a USB key. For instructions, see the Knowledge Base article [How to create an RTFI key to re-image a SolidFire storage node](#). Insert the USB key with the ISO into the node and boot from the USB key.
- **Virtual media using the baseboard management controller (BMC) management port:** You can use the BMC to dynamically attach to the ISO located on your client system. The ISO is made available to the host OS as a virtual drive (CD or DVD). For more information, see the Knowledge Base article [How to RTFI a node via BMC](#).
- **Network boot using a Preboot Execution Environment (PXE), Trivial File Transfer Protocol (TFTP), or FTP:** Instead of manually unpacking an ISO image, you can use `autoofs` to automatically extract an image when the RTFI process requests it. This deployment mechanism requires more initial setup but allows for correct automation and scalability of installation.

## Find more information

- [SolidFire and Element Software Documentation](#)
- [Documentation for earlier versions of NetApp SolidFire and Element products](#)

## The RTFI process

You can begin the Return to Factory Image (RTFI) process by interacting with the node through text console prompts that appear before the system boots.



The RTFI process is data destructive and securely erases all data and configuration details from the node and installs a new operating system. Verify that the node used for the RTFI process is not active as part of a cluster.



The RTFI process performs the following high-level operations:

1. Starts the installation after user confirmation and validates the image.

2. Unlocks all drives on a node.
3. Validates and flashes firmware.
4. Checks hardware.
5. Tests hardware.
6. Secure erases all selected drives.
7. Partitions the root drive and creates file systems.
8. Mounts and unpacks the image.
9. Configures the host name, networking (Dynamic Host Configuration Protocol), default cluster configuration, and GRUB bootloader.
10. Stops all services, collects logs, and reboots.

To configure your node after the RTFI process successfully completes, see the [documentation for your Element software version](#). After a node successfully completes the RTFI process, it transitions to the *available* (unconfigured) state by default.

## Perform the RTFI process

Use the following procedure to restore the Element software on your SolidFire node.

For information on creating a USB key or using the BMC to perform the RTFI process, see [RTFI deployment and installation options](#).

### Before you begin

Verify that you meet the following requirements:

- You have access to a console for the SolidFire node.
- The node on which you are performing the RTFI process is powered up and connected to a network.
- The node on which you are performing the RTFI process is not part of an active cluster.
- You have access to bootable installation media that contains the image of the relevant Element software version for your configuration.

Contact NetApp Support if you have any concerns before performing the RTFI process.

### Steps

1. Connect a monitor and keyboard to the back of the node, or connect to the BMC IP UI, and bring up the **iKVM/HTML5** console from the **Remote Control** tab in the UI.
2. Insert a USB key with an appropriate image in one of the two USB slots in the back of the node.
3. Power on or power reset the node. During the boot-up, select Boot Device by selecting **F11**:



You must select **F11** multiple times in quick succession because the Boot Device screen goes by quickly.

4. In the Boot Device selection menu, highlight the USB option.

The options that appear depend on the USB brand that you are using.



If there are no USB devices listed, go into the BIOS, verify that the USB is listed in the boot order, reboot, and try again.

If that does not resolve the issue, go into the BIOS, browse to the **Save and Exit** tab, select **Restore to Optimized Defaults**, accept and save the settings, and reboot.

5. A list of the images that are on the highlighted USB device appear. Select the desired version and select enter to start the RTFI process.

The RTFI image Element software name and version number appear.

6. At the initial prompt, you are notified that the process will remove all data from the node and that data is not recoverable after the process begins. Enter **Yes** to begin.



All data and configuration details are permanently erased from the node after the process is initiated. If you elect not to proceed, you are directed to the [RTFI options menu](#).



If you want to watch the console during the RTFI process, you can press the **ALT+F8** keys to toggle to the verbose mode console. Press **ALT+F7** to return to the primary GUI.

7. Enter **No** when prompted to perform extensive hardware tests unless you have a reason to suspect hardware failure or are directed to perform the tests by NetApp Support.

A message indicates that the RTFI process has finished and the system powers off.

8. If necessary, remove all bootable installation media after the node powers off.

The node is now ready to be powered on and configured. See the [Element software set up storage documentation](#) to configure the storage node.

If you encountered an error message during the RTFI process, see [RTFI options menu](#).

## Find more information

- [SolidFire and Element Software Documentation](#)
- [Documentation for earlier versions of NetApp SolidFire and Element products](#)

## RTFI options menu

The following options menu appears if the RTFI process is unsuccessful or if you elect not to proceed at the initial RTFI process prompt.



Contact NetApp Support before using any of the following command options.

Option	Description
Reboot	Exits the RTFI process and reboots the node in its current state. No cleanup is performed.
PowerOff	Gracefully powers off the node in its current state. No cleanup is performed.
Exit	Exits the RTFI process and opens a command prompt.
UploadLogs	Collects all logs on the system and uploads a single consolidated log archive to a specified URL.

## Upload logs

Collect all logs on the system and upload them to a specified URL according to the following procedure.

### Steps

1. At the RTFI options menu prompt, enter **UploadLogs**.
2. Enter the remote directory information:
  - a. Type a URL that includes the protocol. For example: `ftp://`, `scp://`, `http://`, or `https://`.
  - b. (Optional) Add an embedded user name and password. For example:  
`scp://user:password@URLaddress.com`.



For a full range of syntax options, see the [cURL](#) user manual.

The log file is uploaded and saved to the specified directory as a `.tbz2` archive.

## Use the support tunnel

If you require technical support for your NetApp HCI system or SolidFire all-flash storage system, NetApp Support can connect remotely with your system. To start a session and gain remote access, NetApp Support can open a reverse Secure Shell (SSH) connection to your environment.

You can open a TCP port for an SSH reverse tunnel connection with NetApp Support. This connection enables NetApp Support to log in to your management node.

**Before you begin**

- For management services 2.18 and later, the capability for remote access is disabled on the management node by default. To enable remote access functionality, see [Manage SSH functionality on the management node](#).
- If your management node is behind a proxy server, the following TCP ports are required in the sshd.config file:

TCP port	Description	Connection direction
443	API calls/HTTPS for reverse port forwarding via open support tunnel to the web UI	Management node to storage nodes
22	SSH login access	Management node to storage nodes or from storage nodes to management node

**Steps**

- Log in to your management node and open a terminal session.
- At a prompt, enter the following:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- To close the remote support tunnel, enter the following:

```
rst --killall
```

- (Optional) Disable [remote access functionality](#) again.



SSH remains enabled on the management node if you do not disable it. SSH enabled configuration persists on the management node through updates and upgrades until it is manually disabled.

**Find more information**

- [SolidFire and Element Software Documentation](#)
- [Documentation for earlier versions of NetApp SolidFire and Element products](#)



## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.