Rehydrate Onboarding Guide

April 2026

ABSOLUTE

Table of Contents

Introduction

Purpose

This guide serves as a supplemental resource for organizations evaluating or implementing the Rehydrate feature (also known as Playbooks), available with the Absolute Resilience tier or as a standalone licensed capability.

Because customer environments vary widely and Rehydrate testing and troubleshooting may depend on infrastructure and configurations beyond the Absolute product, this guide outlines a structured approach to validation and deployment, along with proven best practices.

Audience

This guide is intended for a broad audience but includes references and technical details most familiar to IT and network administrators with knowledge of their organization's environment. Familiarity with filesystems, network configuration—including enterprise VPNs or 802.1x certificates—and options for hosting OS images will be beneficial.

Using this guide

To ensure that your onboarding is effective and delivers the intended outcomes, it is important that you complete all sections of this guide in the order they are presented.

The structure of this guide has been carefully designed to build knowledge progressively. Each section introduces key concepts, skills, or context that serve as a foundation for the material that follows. Skipping ahead or completing sections out of sequence may result in gaps in understanding, making later content more difficult to grasp and reducing the overall effectiveness of the onboarding experience.

For these reasons, you are strongly encouraged to follow the guide as intended and complete each section before moving on to the next.

Permissions

To complete all section in this guide, your user role needs to be granted the following permissions:

- To download and install the agent on your test devices, the *Manage* permission for **Version Control** and the *Perform* permission for **Agent Installer** are required
- To activate and configure the Playbooks policy, the *Manage* permission for **Policies** is required
- To run playbooks, the *Perform* permission for **Run playbook** is required

All Administrators roles are granted these permissions. For more information, see Getting started with roles in the help documentation.

Overview of Rehydrate capabilities

Rehydrate enables remote recovery and remediation of endpoints affected by IT or security incidents, including BSOD events, to reduce downtime and operational impact. Recovery is performed from a firmware-based environment that operates outside the operating system, allowing devices to be repaired or restored even when the OS is corrupted or compromised. This approach reduces incident response effort by eliminating the need for physical access, removable media, or onsite intervention.

For more details about the capabilities of Rehydrate and its uses and benefits, review the Absolute Rehydrate data sheet.

Environment requirements and prerequisites

Rehydrate is supported on Windows devices, but not all Windows devices that support the Absolute Secure Endpoint Agent can run Rehydrate playbooks. Devices must meet specific hardware, disk space, and driver requirements. For detailed system requirements and recommendations, see System requirements in the help documentation.

Currently, the console does not enforce all device prerequisites for Rehydrate provisioning. As a result, devices within a policy group that are ineligible for Rehydrate will fail to be provisioned when the Playbooks policy is activated. To help avoid this, ensure that you complete the following sections in this guide:

- Collect disk space information
- Check license eligibility
- Check device eligibility

Working with network access certificates

A network access certificate (NAC) may be required to connect to a corporate network. When a device executes a Rehydrate playbook, it uses the network stack provided by the Absolute Recovery Environment (WinPE), which does not include customer-specific NAC certificates by default.

To establish a reliable baseline and minimize complexity, we strongly recommend that initial Rehydrate testing be performed on networks that do not require NAC authentication. This allows you to validate core Rehydrate functionality independently of network security constraints.

For testing or proof of value (POV) scenarios, a customer-specific NAC can be stored on a removable USB device, which the Absolute Recovery Environment (WinPE image) will detect and use during playbook execution. In production deployments, however, the NAC must be embedded directly into the WinPE image. At present, this requires the image to be built by Absolute. To request a NAC enabled WinPE image , please submit a support case to Absolute Technical Support.

Deploying Rehydrate

Goal: The purpose of this section is to confirm that your test devices support Rehydrate and to configure your Secure Endpoint account to run Rehydrate playbooks. Continue to refer to these instructions until you are confident in the Rehydrate provisioning process and troubleshooting approach. You may need to revisit this section if issues arise later in the process.

By the end of this section, you will be able to:

- Verify that Absolute Persistence is activated
- Identify devices that meet—or do not meet—the requirements for Rehydrate
- Troubleshoot ineligible devices
- Provision devices within your test policy group
- Verify and interpret provisioning success or failure

Enroll your test devices

Important: This is a mandatory first step for all devices and must be performed before Rehydrate provisioning can be performed. If your test devices are already enrolled in the Secure Endpoint Console and are actively connecting to the Absolute Monitoring Center, you can skip this section and go to Verify Absolute Persistence activation.

Before you can provision your devices for Rehydrate, you need to enroll your test devices in the Secure Endpoint Console. Enrollment consists of installing the Secure Endpoint Agent for Windows on each test device and waiting for the devices to connect to the Absolute Monitoring Center.

Complete the following steps to install the agent and activate Persistence:

1. Log in to the Secure Endpoint Console using your Absolute credentials.
2. On the navigation pane, click **Settings** > **Agent Management** to download your account-specific agent. For details, see Downloading the Secure Endpoint Agent in the help documentation.
3. Run the *full agent installer* on your test devices to install the agent. Note that to complete the agent installation process, two reboots are required. For details, see Installing the Windows agent in the help documentation.
4. Wait for each test device's agent to connect to the Absolute Monitoring Center. This may take a few hours, so you may want to wait until the following day to resume the onboarding process.

Verify Absolute Persistence activation

Rehydrate is supported on active Windows devices with Absolute Persistence version 2.0 or higher.

You can view the status of Absolute Persistence on your test devices using the Activation report. For more information, see Activation report in the help documentation.

To verify Persistence activation:

1. Log in to the console and click **Reports** on the navigation pane.
2. Use the **Search** field to search for "Activation". Click the report to open it.

   All newly enrolled devices show at the top of the report. If your test devices are not shown, wait a few more hours for enrollment to complete.
3. Search for each of your test devices and confirm that the following report columns are set to the specified values:
   - **Agent status**: Active
   - **Firmware Persistence** > **Status**: Active
   - **Firmware Persistence** > **Version**: 2.0 or higher

   For example:

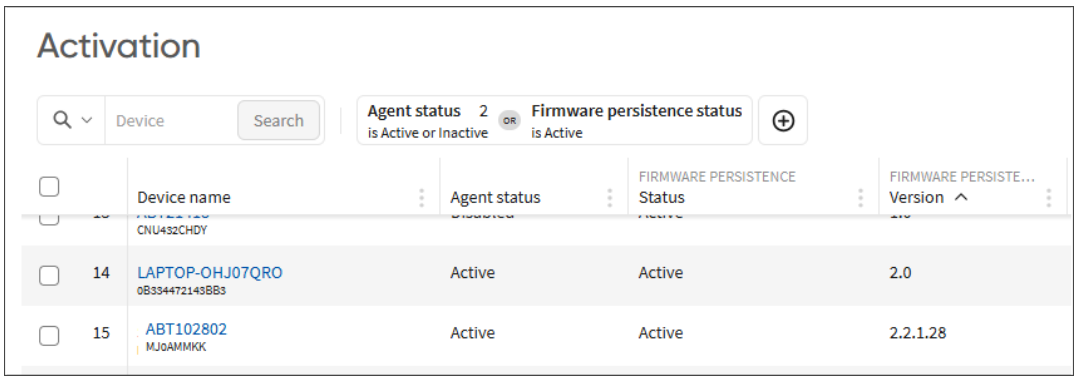

Figure 1: Activation report showing two devices with activated Absolute Persistence

If any of your test devices do not meet these requirements, they are not eligible for Rehydrate.

Review baseline requirements for Rehydrate

Review the section System requirements in the help documentation.

Review the Rehydrate provisioning process

Review the section About the Playbooks policy in the help documentation.

Prepare your test environment and enable Rehydrate

You're now ready to set up your test environment in the Secure Endpoint Console and enable Rehydrate on your test devices.

This process includes the following key steps:

1. Create a test policy group
2. Collect disk space information
3. Check license eligibility
4. Check device eligibility
5. Troubleshoot ineligible HP devices
6. Activate the Playbooks policy
7. Verify Rehydrate provisioning

Best practices

We strongly recommend that you roll out Rehydrate to your devices in a controlled fashion. Specifically, you should begin by creating a policy group for testing purposes, move a small number of test devices into it, and then activate the policy group's Playbooks policy. After you are comfortable running playbooks on your test devices, you can roll it out to more devices in other policy groups.

To simplify Rehydrate onboarding:

- Choose test devices that are the same make and model to simplify any troubleshooting that may be required. Transitioning from a few homogeneous devices to a heterogeneous pool of many devices/models/configurations will complicate any troubleshooting. When you're comfortable with the provisioning process, you can gradually expand to more models and manufacturers.
- Start small. Do not activate the Playbooks policy in the Global Policy Group. Instead, try out the feature on a small number of devices in a test policy group.

The steps included in this section follow these best practices.

Step 1: Create a test policy group

To create a policy group of test devices:

1. On the navigation pane, click **Policies** > **Policy Groups.**
2. Click **Create policy group.** A new policy group named *Untitled custom policy group -<date>* opens.
3. Click the policy group name field and update it to *Rehydrate test devices*.
4. Move your test devices to the *Rehydrate test devices* policy group. If you enrolled new devices, they are in the Global Policy Group. For details, see Moving devices between policy groups in the help documentation.

Note: Do not activate the Playbooks policy yet.

Step 2: Collect disk space information

To help you determine if each test device has enough disk space available to complete Rehydrate provisioning, you need to assign the **Shrinkable disk space** data point to the *Rehydrate test devices* policy group and activate it. For more information about custom data points, see Getting started with Custom Data policies in the help documentation..

To activate the data point:

1. With the *Rehydrate test devices* policy group open, click **Configure** next to **Custom Data**. The Custom Data overview opens.
2. Using the **Search** field, search for **Shrinkable disk space** and click its ⊕ icon to assign it to the policy group.

   Note: Shrinkable disk space is the amount of free, movable space in a disk volume that can be safely reduced (shrunk) without data loss. It is more accurate than "free disk space" because it excludes immovable files.

3. Click **Activate**.

   The new data point request is sent to each test device on its next connection to the Absolute Monitoring Center, which is typically within the next 15 minutes.

4. After waiting at least 30 minutes, go to each device **Details** > **Custom Data Points** page and confirm that the **Value** column for the new data point is populated. For more information, see Viewing a device's Custom Data Points in the help documentation.

If a device's reported shrinkable disk space is less than 25 GB, there is not enough disk space to provision the device and run playbooks. Do one of the following:

- Replace the test device with a device that satisfies this requirement
- Run the *Absolute partition creation preparation and restoration utility* Reach script using the `Fix` option to attempt to resolve the issue.

  This script disables the following features and then runs disk defragmentation to consolidate the disk volume's free space:

  - Hibernation
  - Fast Boot
  - Automatic Page File
  - System Protection/Restore Points
  - Volume Shadow Copies
  - Windows Search service

  For more details about this script, go to **Settings** > **Script library** and view the script content.

  For more information about running Reach scripts, see Running scripts on devices in the help documentation. To check the status of your Run Script request, go to the device's Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.

  Important: After completing Step 7: Verify Rehydrate provisioning, re-run this Reach script using the `Restore` option to re-enable the disabled features.

Step 3: Check license eligibility

To ensure that the test devices are assigned a license that supports Rehydrate:

1. On the navigation pane, click **Policies** > **Policy Groups** and then click the *Rehydrate test devices* policy group to open it.
2. For the Playbooks policy, check if this warning (or a similar one) shows under **License Status**:

   

3. If it shows, click **Show devices** to view the devices that require a license upgrade. For details about assigning the required license, see Changing the license assigned to devices in the help documentation.

Step 4: Check device eligibility

To check if any devices fail to meet the system requirements for Rehydrate:

1. With the *Rehydrate test devices* policy group open in Policies > Policy Groups, check if the following icon shows next to the Playbook policy's activation slider:

   

   The number indicates the count of ineligible devices.

2. If it shows, click the icon to review the ineligibility reasons shown for each device in the **Playbook** > **Status details** column. For more information about each reason, see Checking device eligibility in the help documentation.
3. If any devices are ineligible, determine if there are steps you can take to resolve ineligibility by reviewing Troubleshooting ineligible devices in the help documentation. Also see the next step below.

   If you can't resolve the ineligibility issues, you'll need to replace the ineligible test device.

Step 5: Troubleshoot devices with a missing Microsoft 3rd-party UEFI CA certificate

If a device shows the following value in the **Playbooks > Status details** column, it is ineligible due to a Secure Boot configuration issue:

3rd-party CA must be active when Secure Boot is enabled

Do one of the following:

- To resolve this issue on HP devices, run the *Enable Microsoft 3rd-party UEFI CA on HP devices* Reach script. This script enables the **Enable MS EUFI CA key** option in the device's BIOS settings. For details about this script, go to **Settings** > **Script library** and view the script content.

  For more information about running Reach scripts, see Running scripts on devices in the help documentation. To check the status of your Run Script request, go to the device's Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.
- To resolve this issue on all other Windows devices, refer to manufacturer documentation about enabling the Microsoft 3rd-party UEFI CA certificate in Secure Boot settings.

  Note: An *Enable Microsoft 3rd-party UEFI CA* Reach script that supports all device manufacturers will be available in a future release.

Step 6: Activate the Playbooks policy

Activating the Playbooks policy in your test policy group enables Rehydrate on the group's devices.

To activate the Playbooks policy:

1. With the *Rehydrate test devices* policy group open in Policies > Policy Groups, click the Playbooks policy's activation slider:

   

   The Playbook configuration dialog opens.
2. Leave the **Automated playbook actions** option unselected.
3. Under **System restart**, clear the checkbox next to **Restrict restarts to a time window**. This ensures that the reboots required to provision each test device will occur automatically without any unnecessary delay.

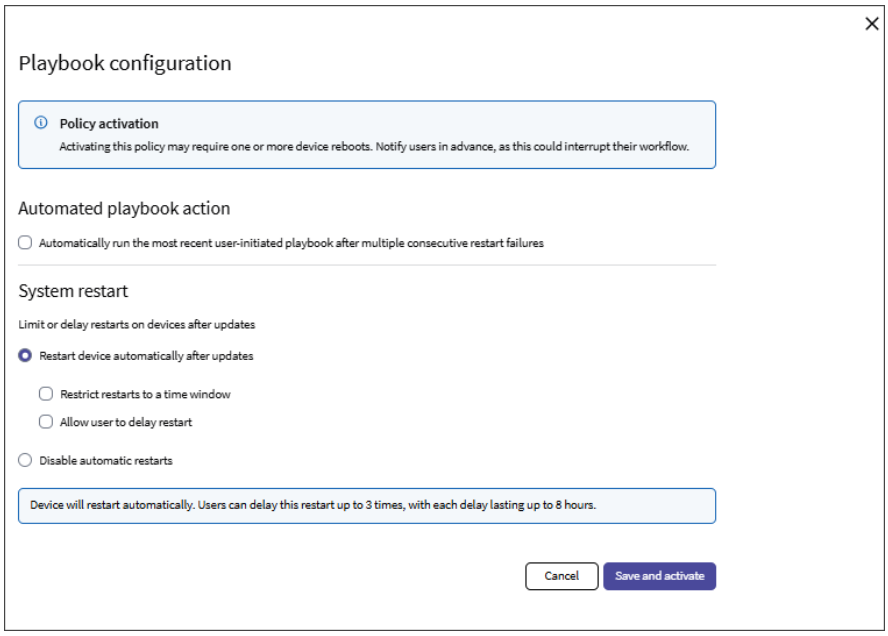

Figure 2: Playbook configuration dialog

Note: This configuration facilitates testing of the Rehydrate feature. When deploying Rehydrate to your production devices, apply a system restart policy that aligns with your IT policies, but be aware that it may take longer to fully provision the devices.

4. Click **Save and activate**. The policy is activated.

On each device's next connection to the Absolute Monitoring Center, which is typically within the next 15 minutes, the Secure Endpoint Agent downloads approximately 2 GB of data, consisting mainly of the Absolute Recovery Environment (WinPE image), and device drivers that work across the various makes and models that Rehydrate supports.

To fully provision each device, ***two reboots are required***.

Important: Deployment of Rehydrate is staggered to minimize the impact on your network, so it may take up to 24 hours to complete provisioning of all devices in your test policy group.

Step 7: Verify Rehydrate provisioning

The most reliable way to confirm that a device is fully provisioned is to check the **Playbooks** field on each device's Summary page in Device Details.

To open a device's Summary page:

1. On the navigation pane, click **Devices** and search for your test device.
2. Click the device name to open its Device Details pages.
3. Click the **Details** tab. The Summary page opens.

   Provisioning is complete when the **Playbooks** field shows **Enabled** along with an obscured playbook passcode.

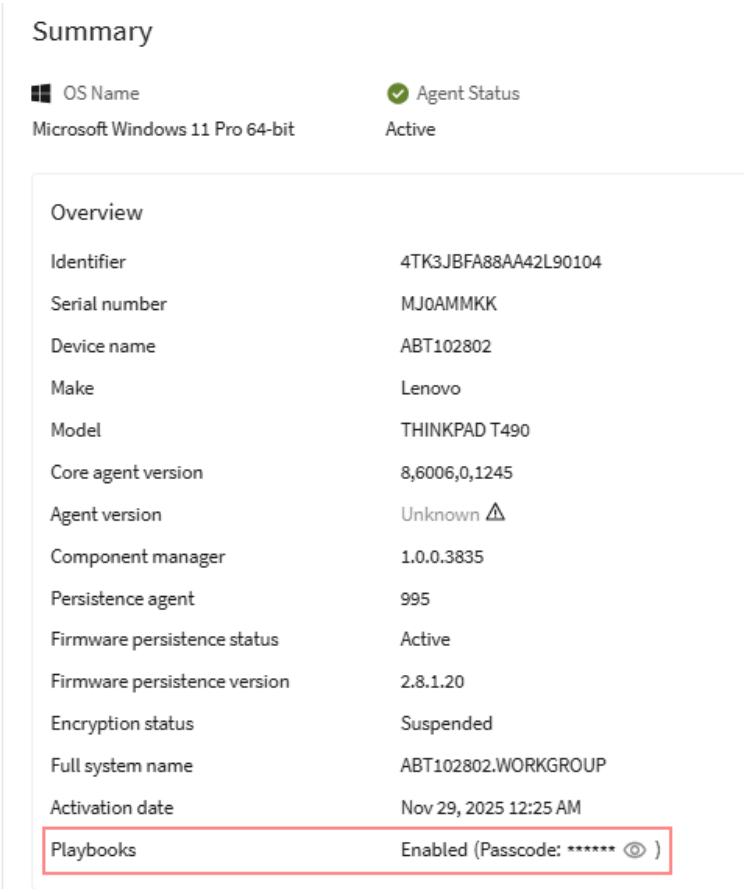

Figure 3: Summary page showing that the device is fully provisioned

If the Playbooks field shows **Not enabled**, provisioning is not yet complete. You may need to wait a few more hours for the device's provisioning status to be updated.

If a test device fails to be provisioned after waiting 24 hours, and the device is online, submit a support case to Absolute Technical Support.

4. If you ran the *Absolute partition creation preparation and restoration utility* Reach script in Step 2: Collect disk space information, re-run the script now on all fully provisioned devices. This restores the features that were disabled when you first ran the script.

About testing Rehydrate on BitLocker encrypted devices

If your test devices are encrypted by BitLocker Drive Encryption, you will need to enter each device's BitLocker recovery key when you run a playbook. The recovery key unlocks the drive so the playbook can access the file system or Windows registry.

You can enter BitLocker recovery keys manually, or you can use a variable based on the **BitLocker recovery key** custom data point. Using a variable allows you to run a playbook on multiple devices from a single Run Playbook request.

To collect the BitLocker recovery key data point from your test devices, you need to assign the data point to the *Rehydrate test devices* policy group and activate it. For more information about custom data points, see Getting started with Custom Data policies in the help documentation.

Before proceeding to the next section, do ***both*** of the following:

To be able to…	Do this…
Enter recovery keys manually	Record the recovery key for each test device and have it accessible for the exercises that follow. To find a device's recovery key, see Microsoft documentation or contact your IT department. **Note**: You will not be able to complete Exercise #4: Run a playbook on multiple devices using this method. You must use a variable for this exercise.
Use a variable	To collect the data point: 1. Ensure that all test devices are online. 2. With the *Rehydrate test devices* policy group open in Policies > Policy Groups, click **Configure** next to **Custom Data**. The Custom Data overview opens. 3. Using the **Search** field, search for **BitLocker recovery key** and click its ⊕ icon to assign it to the policy group. 4. Click **Activate**. The new data point request is sent to each test device on its next connection to the Absolute Monitoring Center, which is typically within the next 15 minutes. To verify that the data point has been collected, go to each device **Details** > **Custom Data Points** page and confirm that the **Value** column is populated for the new data point. For more information, see Viewing a device's Custom Data Points in the help documentation. **Note**: Currently, BitLocker recovery keys are not redacted in the **Value** column. In a future release, the Full-Disk Encryption Status policy will be able to collect BitLocker recovery keys and store them in the Absolute database for use in playbook variables. The key values will not show in the console. At that time, you can deactivate the BitLocker recovery key data point.

Note: If a test device's drive in encrypted by another full-disk encryption product, it is not eligible for Rehydrate.

Running simple, non-recovery playbooks

Goal: The purpose of this section is to validate that the Rehydrate agent components are installed and functioning correctly and to build confidence running simple playbooks. At this stage of your onboarding, the goal is to eliminate as much variation as possible to simplify any troubleshooting that may be required.

By the end of this section, you will be able to:

- Execute simple, non-recovery playbooks on devices
- Validate that the test device can retrieve files from a network location
- Use the console's Action History to check the status of your Run Playbook requests

To simplify troubleshooting, the suggested learning path starts with the scenario with the fewest environmental and device dependencies. Complete the tests in the order they are presented.

Available playbooks

The Rehydrate feature currently includes six playbooks:

- File Operations (add or delete)
- Restore from image

- Run script
- Run script from file
- Set/remove registry keys
- Multi operations

These playbooks can be system- or user-initiated. A system-initiated playbook is deployed to the device on its next connection to the Absolute Monitoring Center, and the playbook runs automatically. A user-initiated playbook is not deployed to the device until a device user initiates it. In this section, you'll run some system-initiated playbooks, which streamlines the playbook validation process. Later in this guide, you'll run a user-initiated playbook.

Before proceeding to the next section, review About user-initiated playbooks in the help documentation.

Exercise #1: Delete a file from a test device

In this exercise, you'll remotely delete a file from a test device using the *File Operations (add or delete)* playbook.

For detailed instructions while performing these steps, see the *File Operations (add or delete)* section in Running a playbook in the help documentation.

To delete a file:

1. On a test device, create a file in a known location. For example, use Notepad to create a document named `test.txt` and save it to `c:\test.txt`. All file types are supported.
2. Ensure that the test device is online.
3. In the console, go to **Policies** > **Policy Groups** and click the *Rehydrate test devices* policy group to open it.
4. Near the top of the page, click the **<count> devices** link to view the devices included in the policy group.

Figure 3: Devices link in a policy group

5. Select the test device and click ⋮ > **Run playbook**. The Run playbook dialog opens.
6. Click the **Select playbook** field and select **File Operations (add or delete)**.
7. If the device is BitLocker encrypted, manually enter its recovery key in the **BitLocker Recovery key** field.
8. Under Parameters, click **Add action** > **Delete file.**
9. Enter the file's full path in the **Path and file name to delete** field. For example, enter `C:\test.txt`.

   Note: Paths are case sensitive.

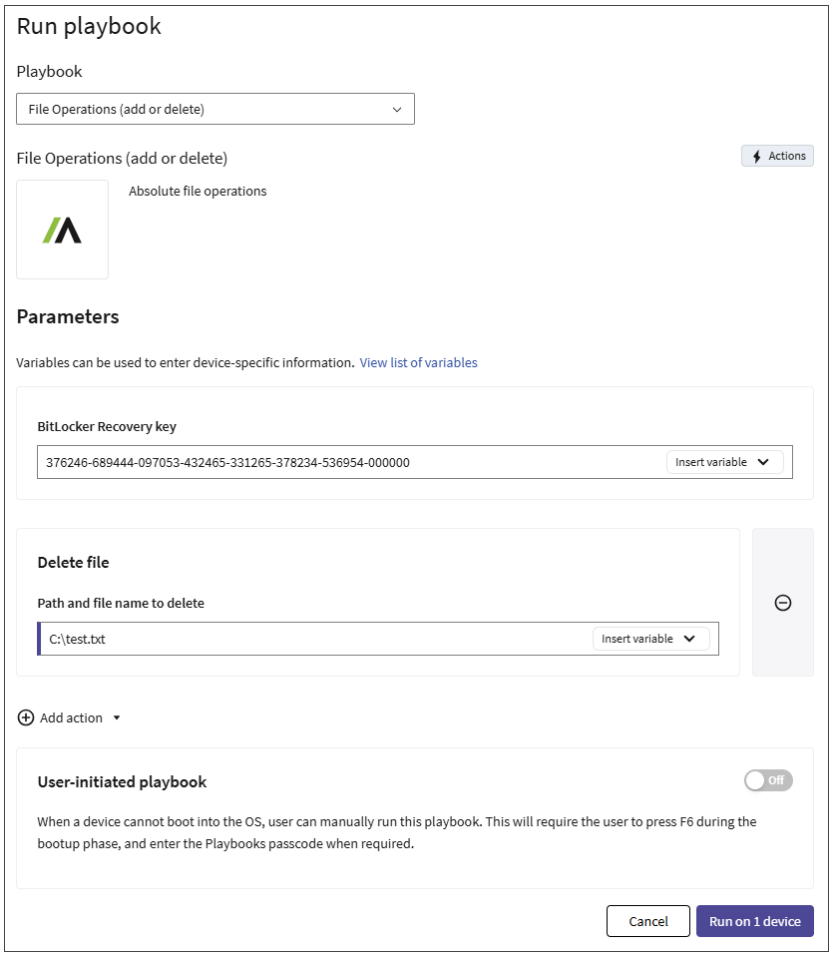

Figure 4: Example of File operations (add or delete) playbook configurations for the Delete file action

10. Click **Run on 1 device**.

A Run Playbook request is created. After the device receives the Run Playbook request, it reboots and runs the playbook. You can confirm that the file was successfully deleted by checking:

- The device's action status on its Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.
- The device's Windows event log.
- That the file is no longer stored in its original location.

If desired, resubmit the same playbook on the same device without performing step 1, so that the request fails. Go to the device's Actions page to see the action status for a failed playbook. To view the failure reason, click > **Edit columns** and add the Action > Status details column to the page.

Troubleshooting

If a playbook failed unexpectedly, the most common cause is an incorrect file path or file name. Check the spelling, spacing, and direction of the slashes, and try again.

Congratulations! You have finished testing the delete file option in the *File Operations (add or delete)* playbook.

Exercise #2: Add a file to a test device

In this exercise, you'll remotely add a file to a test device using the *File Operations (add or delete)* playbook.

For detailed instructions while performing the following steps, see the *File operations (add or delete)* section in Running a playbook in the help documentation.

To add a file:

1. Ensure that the test device is online.
2. Select the test device and click ⋮ > **Run playbook**. The Run playbook dialog opens.
3. Click the **Select playbook** field and select **File Operations (add or delete)**.
4. If the device is BitLocker encrypted, manually enter its recovery key in the **BitLocker Recovery key** field.
5. To specify the file to download, click **Add action** > **Add file** and enter a URL in the **Host file URL** field.

   For example, enter the following URL to download the Absolute Rehydrate datasheet:
   `https://go.absolute.com/rs/258-HSL-350/images/ds-absolute-rehydrate-se.pdf`

   Note: If the file had been stored on a file-sharing service, only direct download links are supported.
6. To specify the location to store the file, enter the full file path on the device in the **File path** field. You can use the original file name or a file name of your choosing. For example, enter `C:\\absolute-rehydrate.pdf`.

   Note: Paths are case sensitive.

Figure 5: Example of File operations (add or delete) playbook configurations for the add file action

7. Click **Run on 1 device**.

After the device receives the Run Playbook request, it reboots and runs the playbook. You can confirm that the file was successfully added by checking:

- The device's action status on its Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.
- The target file path on the device.

Troubleshooting

If the playbook failed, the most common cause is an invalid target file path—either the path does not exist, or it contains a typo. Verify the path and try again.

Note: File access may be blocked by corporate network controls, such as configurations that require network access certificates (NAC).

Congratulations! You have finished testing the add file option in the *File Operations (add or delete)* playbook.

Exercise #3: Update a registry setting on a test device

In this exercise, you'll remotely add (and then delete) a registry key value using the *Set/remove registry keys* playbook. The new registry key value allows Notepad to start up on reboot.

For more information about this playbook, see Set/remove registry keys in the help documentation.

Important: Changing registry keys can result in an unstable Windows configuration. Existing keys should not be changed or deleted unless done by a trained IT professional.

For detailed instructions while performing these steps, see the *Set/remove registry keys* section in Running a playbook in the help documentation.

To update a registry setting:

1. Ensure that the test device is online.
2. Select the test device and click ⋮ > **Run playbook**. The Run playbook dialog opens.
3. Click the **Select playbook** field and select **Set/remove registry keys**.
4. If the device is BitLocker encrypted, manually enter its recovery key in the **BitLocker Recovery key** field.
4. Click **Add action** > **Set registry key.**
5. Complete the fields as follows:
   - **Registry path**: Enter `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

     Note: `HKEY_LOCAL_MACHINE` is the only supported hive.
   - **Registry name**: Enter `notepad`
   - **Registry type**: Select **Reg_SZ**
   - **Registry value**: Enter `C:\Windows\System32\notepad.exe`

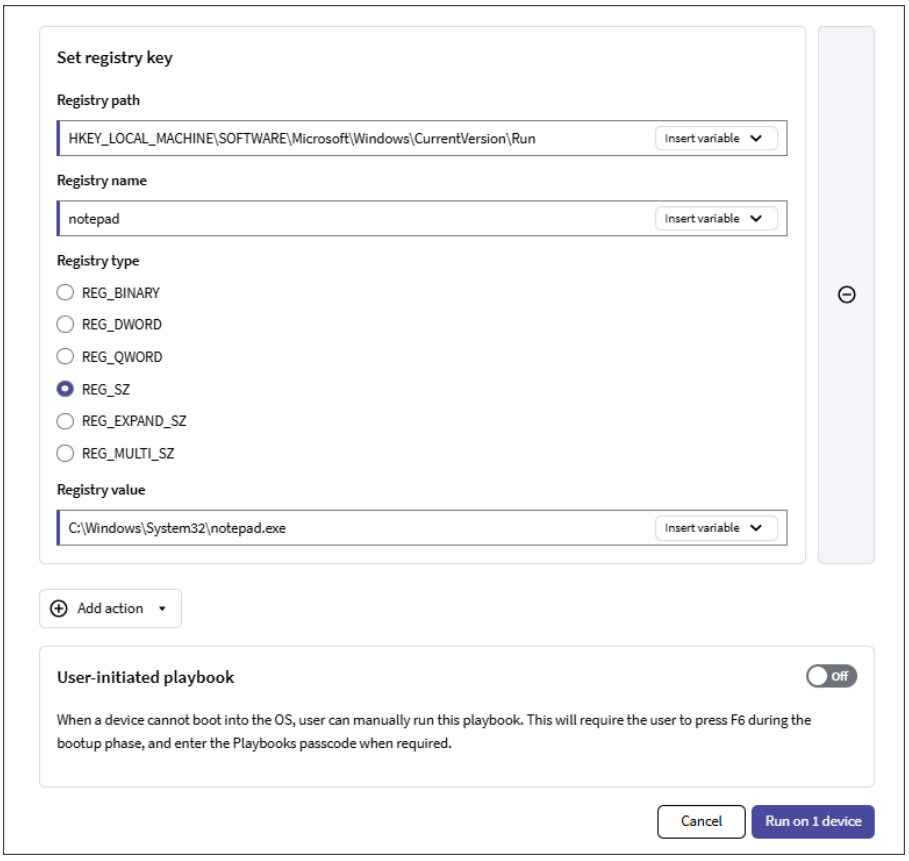

Figure 6: Example of Set/remove registry keys playbook configurations for the Set registry key action

6. Click **Run on 1 device**.

   After the device receives the Run Playbook request, it reboots and runs the playbook. You can confirm that the registry entry was successfully updated by checking:

   - The device's action status on its Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.
   - The test device's Windows registry to confirm that the `notepad` registry value was added to the `HKEY_LOCAL_MACHINE` hive.
7. In the console, delete the `notepad` registry key value you just added:

a. Select the same test device and create a new Run Playbook request containing the *Set/remove registry keys* playbook.

b. Click **Add action** > **Remove registry key.**

c. Enter the **Registry path** and **Registry name**.

d. Click **Run on 1 device**.

After the device receives the Run Playbook request, it reboots and runs the playbook. You can confirm that the registry entry was successfully updated by checking:

- The device's action status on its Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.
- The test device's Windows registry to confirm that the `notepad` registry is deleted.

Troubleshooting

If a playbook fails, the most common cause is incorrect registry details. Verify that the registry path, name, and type are correct and then try again.

Congratulations! You have finished testing the *Set/remove registry keys* playbook.

Running playbooks on multiple devices

Goal: The purpose of this section is to introduce you to some of the more advanced capabilities of Rehydrate.

By the end of this section, you will be able to:

- Submit a single Run playbook request to run a playbook on multiple devices
- Use variables in a Run playbook request

Exercise #4: Run a playbook on multiple devices

Up to this point in the guide, you've run playbooks in the context of a single device.

Rehydrate supports the use of variables in playbook parameters, which allows you to submit a single Run playbook request on multiple devices. Variables can include device-specific information, such as hardware data points, custom fields, or custom data points. For more information about when and how to variables, see About using variables in playbook parameters in the help documentation.

In this exercise, you'll run a *File Operations (add or delete)* playbook on two devices using variables in two fields.

Note: If any devices are BitLocker encrypted, ensure that you have activated the BitLocker recovery key data point in the *Rehydrate test devices* policy group before starting this exercise .

To run a playbook that includes variables:

1. Ensure that the device is online.
2. In the console, select two test devices. For details about selecting multiple devices, see *To run a playbook on multiple devices* in Running a playbook in the help documentation.
3. Click ⋮ > **Run playbook**. The Run playbook dialog opens.
4. Click the **Select playbook** field and select **File operations (add or delete)**.
5. Click **Add action** > **Add file** and enter a file's URL in the **Host file URL** field.

   For example, enter the following URL to download the Absolute Rehydrate datasheet:
   `https://go.absolute.com/rs/258-HSL-350/images/ds-absolute-rehydrate-se.pdf`
6. Click **View list of variables** to view the supported variables. Click outside the dialog to close it.

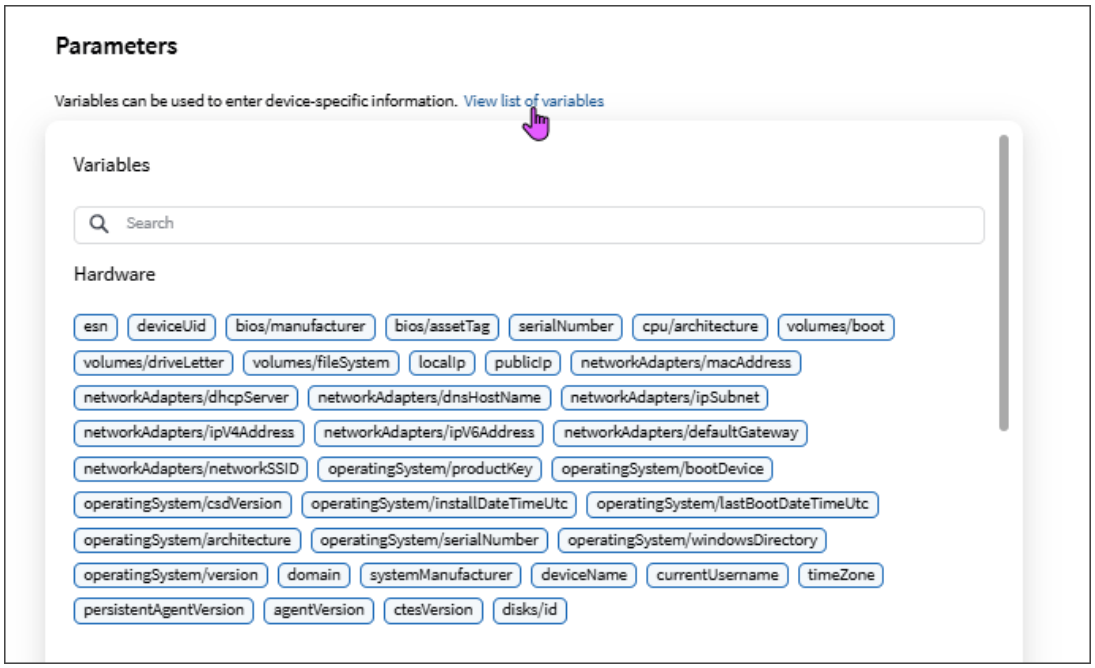

Figure 7: Selection list of parameter variables in a playbook configuration

7. If any of the test devices are BitLocker encrypted:
    a. Next to the **BitLocker Recovery key** field, click **Insert variable.**
    b. Search for and select **BitLocker recovery key**. The variable is inserted in the field.
8. In the **File path** field, enter a path that contains the `currentUsername` variable.

    For detailed instructions about inserting a variable in a path, see About using variables in playbook parameters in the help documentation.
9. Click **Run on 2 devices**.

After the device receives the Run Playbook request, it reboots and runs the playbook using the applicable parameter values for each device. You can confirm that the file was successfully added to each device by checking:

- Each device's action status on its Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.
- The target file path on the device.

Troubleshooting

If the playbook failed, the most common cause is an invalid target file path—either the path does not exist, or it contains a typo. Verify the path and try again.

Congratulations! You have finished testing the use of variables in a playbook configuration.

Running OS recovery playbooks

Goal: The purpose of this section is to start to use the system recovery capabilities of Rehydrate to reinstall the operating system on a test device.

By the end of this section, you will be able to:

- Understand which image files are supported and how to host them
- Run the *Restore from image* playbook to reinstall the OS using an ISO or WIM image file

Important: Unlike the non-destructive playbooks you ran in the previous section, an OS restore permanently overwrites the existing operating system on the device. Before proceeding, ensure that you are comfortable running playbooks, that the device can successfully access the required network locations, and that no irreplaceable data resides on the test device.

Hosting a recovery image

Rehydrate supports two recovery image formats: **ISO** (Windows Disk image) and **WIM** (Captured Windows Image). An ISO uses a generalized installer process, while a WIM is a snapshot of a specific device. As a result, a WIM image typically includes device specific configurations and drivers, which can simplify recovery on identical hardware but may not work reliably on devices from a different manufacturer or model. For information about creating an ISO image, see Microsoft documentation. For information about creating a WIM image, see Microsoft documentation.

Before running the *Restore from image* playbook, you will need to store your image file in an accessible location that is *not* password protected. If the file is stored on a file-sharing service, only direct download links are supported.

The *Restore from image* playbook includes a configuration that points to a manifest file. This file contains pointers to the image file and an answer file, if required.

Note: An answer file (`unattend.xml` or `autounattend.xml`) is a key configuration file used to automate the Windows installation process, eliminating the need for manual input. For more information about answer files, see Microsoft documentation.

Review recovery image requirements

Review the section Restore from image in the help documentation.

Exercise #5: Reinstall the OS on a test device

In this exercise, you'll use the *Restore from image* playbook to reinstall the OS on a test device.

For detailed instructions while performing these steps, see the *Restore from image* section in Running a playbook in the help documentation.

To restore a device's OS:

1. Prepare your ISO or WIM image:
   - **ISO**: create your ISO image, answer file, and manifest file. For details, see Windows Disk Image (ISO) in the help documentation.
   - **WIM**: create your WIM image and manifest file. For details, see Captured Windows Image (WIM) in the help documentation.
2. Ensure that the test device is online.
3. In the console, select the test device and click ⋮ > **Run playbook**. The Run playbook dialog opens.
4. Click the **Select playbook** field and select **Restore from image**.
5. If the device is BitLocker encrypted, manually enter its recovery key in the **BitLocker Recovery key** field, or use the variable.
6. In the **Manifest file URL** field, specify the location of the manifest file. If the file is stored on a file-sharing service, only direct download links are supported.
7. If credentials are required to access the manifest file on the server, enter the applicable **Username** and **Credentials**.

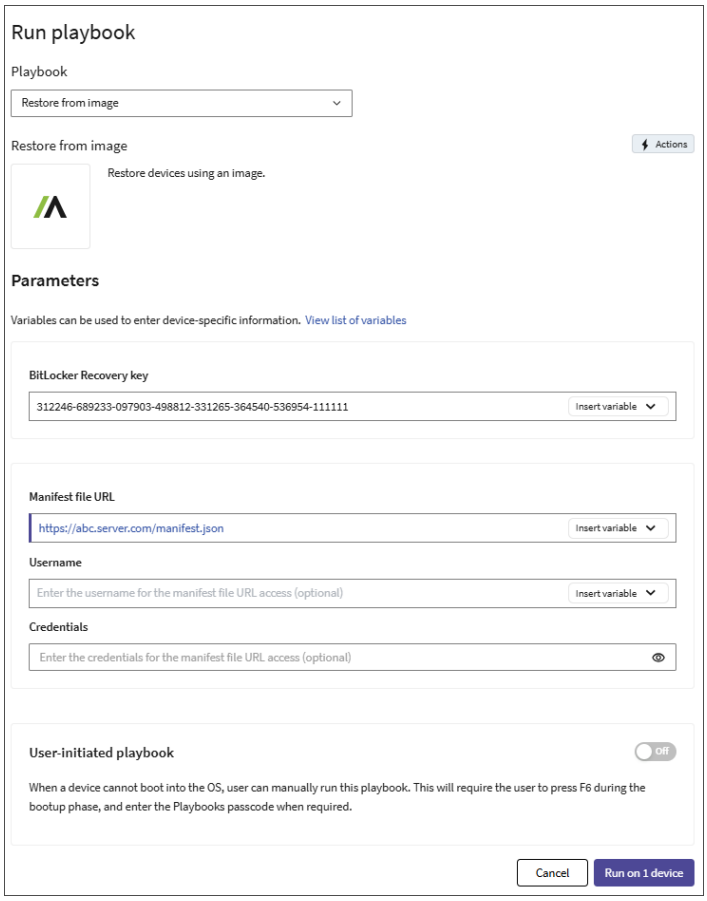

Figure 8: Example of Restore from image playbook configurations

8. Click **Run on 1 device**.

After the device receives the Run Playbook request, it reboots and runs the playbook. You can confirm that the operating system was restored successfully by checking:

- The device's action status on its Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.
- The device successfully boots into Windows.

Troubleshooting

If the playbook fails, confirm that the manifest file and playbook configurations are configured correctly.

Congratulations! You have finished testing the *Restore from image* playbook.

Advanced concepts

Goal: The purpose of this section is to introduce advanced topics that build on the knowledge gained in earlier sections.

By the end of this section, you will be able to:

- Create and run playbooks that execute batch or PowerShell scripts
- Create playbooks that run multiple actions from various playbook types
- Understand and run user-initiated playbooks

Running scripts

The Rehydrate feature includes two playbooks for running scripts:

- **Run script**

  Remotely runs a script on a device by pasting the script content into a field. For more information, see Run script in the help documentation.

- **Run script from file**

  Remotely runs a script stored in an accessible location. For more information, see Run script from file in the help documentation.

You can run batch scripts and PowerShell scripts using either of these playbooks.

Note: Windows scripting is beyond the scope of this onboarding guide, so we suggest validating that you understand how to run a playbook by running a simple “Hello World!” script.

Batch script	PowerShell script

`@echo off`
`echo Hello World!`
`pause`
	`#PS`
	`Write-Host 'Hello, World!'`

Exercise #6: Run a batch script on a test device

In this exercise, you’ll use the Run script playbook to run a batch script on a test device.

For detailed instructions while performing these steps, see the *Run script* section in Running a playbook in the help documentation.

To run a script:

1. Ensure that the test device is online.
2. In the console, select the test device and click ⋮ > **Run playbook**. The Run playbook dialog opens.
3. Click the **Select playbook** field and select **Run script**.
4. If the device is BitLocker encrypted, manually enter its recovery key in the **BitLocker Recovery key** field, or use the variable.
5. Using the table above, paste the “Hello World!” batch script content into the **Batch script** field.
6. Click **Run on 1 device**.

After the device receives the Run Playbook request, it reboots and runs the playbook. You can confirm that the script has successfully run on the device by checking the device’s action status on its Actions page in Device Details. For details, see Viewing a device’s actions in the help documentation.

Troubleshooting

If a playbook fails, check the playbook configurations.

Congratulations! You have finished testing the *Run script* playbook.

Exercise #7: Run a PowerShell script on a test device

In this exercise, you’ll use the Run script from file playbook to run a PowerShell script on a test device.

For detailed instructions while performing these steps, see the *Run script from file* section in Running a playbook in the help documentation.

To run a script:

1. Using the table above and Notepad, paste the PowerShell script content into a new file and save it as `a .ps1` file.
2. Save the PowerShell script to an accessible location on your network.
3. Ensure that the test device is online.
4. In the console, select the test device and click ⋮ > **Run playbook**. The Run playbook dialog opens.
5. Click the **Select playbook** field and select **Run script from file**.
6. If the device is BitLocker encrypted, manually enter its recovery key in the **BitLocker Recovery key** field, or use the variable.
7. In the **Host file URL** field, enter the URL (HTTP or HTTPS protocol only) for the location where the PowerShell script is stored.
8. Click **Run on 1 device**.

After the device receives the Run Playbook request, it reboots and runs the playbook. You can confirm that the script has successfully run on the device by checking the device's action status on its Actions page in Device Details. For details, see Viewing a device's actions in the help documentation.

Troubleshooting

If the playbook fails, check the playbook configurations.

Congratulations! You have finished testing the *Run script from file* playbook.

Running a multi-operation playbook on a test device

You can use the *Multi operations* playbook to combine actions from the following playbooks into a single Run Playbook request:

- Run script
- File operations (add or delete)
- Set/remove registry keys

Your playbook can include up to 20 actions, and the actions will run in the order in which you add them.

For more information, see Multi operations in the help documentation.

Exercise #8: Run multiple playbooks on a test device

In this exercise, you'll use the knowledge you've gained completing the previous sections in this guide to run a *Multi operations* playbook.

Create a Run playbook request for one test device using the *Multi operations* playbook. Add three actions of your choosing. For detailed instructions, see the *Multi operations* section in Running a playbook in the help documentation.

Submitting user-initiated playbooks

User-initiated playbooks are not pushed to a device automatically; instead, they are retrieved by the Absolute Recovery Environment installed on each device. This approach is especially useful when the device's operating system has been compromised and cannot boot reliably. In these situations, the device can run a user-initiated playbook in one of two ways:

- A device user restarts the device, presses F6 during the boot process, and then enters the device's playbook passcode

- The playbook runs automatically after the device repeatedly fails to boot into Windows. The number of failed boot attempts is configured in the Playbooks policy. For more information about automated playbook actions, see Configuring Playbook policies in the help documentation.

  Note: Automated playbook actions will be included in a future update to this guide.

Exercise #9: Run a user-initiated playbook

In this exercise, you'll create a Run Playbook request with the **User-initiated playbook** option enabled and then execute the playbook on the test device.

To create a user-initiated Run Playbook request:

1. In the console, select a test device and create a new Run playbook request containing a playbook of your choosing.
2. Complete the required fields for the playbook.
3. Under **User-initiated playbook**, click the toggle to turn it on.

Figure 9: User-initiated playbook option in a playbook configuration

4. Click **Run on 1 device**. The Run Playbook request is sent to the Absolute server to wait for the device's Absolute Recovery Environment to request it.
5. Record the device's playbook passcode. For details, see Getting the device's passcode in the help documentation.
6. To run the playbook:
   a. Restart the device.
   b. When a green asterisk (*) shows in the top left of the screen, press F6 (or Fn+F6, if applicable).
   c. In the passcode field, enter the Playbook passcode. The playbook starts to run.

   For detailed instructions, see Initiating the playbook in the help documentation.

Troubleshooting

If the playbook fails, check the playbook configurations.

Congratulations! You have finished testing user-initiated playbooks.

Replacing a pending Run playbook request

Review the section Updating an outstanding Run playbook request in the help documentation.

Deactivating the Playbooks policy

Congratulations! You've completed your Rehydrate onboarding.

If desired, you can now deactivate the Playbooks policy on your test devices in one of two ways:

- Deactivate the policy in the Rehydrate test devices policy group. For details, see Deactivating the policy in the help documentation.
- Moving the test devices to another policy group. You can then delete the test policy group. For details, see Moving devices between policy groups and Deleting policy groups in the help documentation.

Deactivating the policy removes all Rehydrate agent components and restores the default boot order. A reboot is required to complete the Rehydrate deprovisioning process.
Note: Because the re-provisioning process is fairly involved, devices should not be moved between policy groups with differing Playbooks policy activation states unless this is done intentionally and with an understanding of the impact. Similarly, do not change the activation status of a policy group's Playbooks policy without careful consideration.

Appendix

Logging and Diagnostics Collection

When a device fails to install Rehydrate or execute a playbook, the primary source for diagnosing the issue is the `PERService.log` file. This log is stored locally on the device at:

`C:\ProgramData\CTES\logs\perService.log`

Interpreting this log requires advanced troubleshooting expertise. As an initial step, scan the file for entries labeled **Warning**, which may highlight the underlying cause of the failure. If this review does not clearly identify the issue, submit a support case to Absolute Technical Support.

Getting Help

If you have questions or need assistance while completing this onboarding guide, the following resources are available:

Resource	Helpful links / Details

Help documentation	• Console basics
	• Downloading and installing the agent
	  ○ Downloading the Secure Endpoint Agent
	  ○ Installing the Windows agent
	• Playbooks
	  ○ Getting started with Playbooks policies
	  ○ Configuring Playbooks policies
	  ○ Running playbooks
	• Tracking Run Playbook requests in Action History
	  ○ Viewing a device's actions
	  ○ Monitoring requests
	  ○ Monitoring actions

Technical Support	To submit a Support case: 1. Log in to the Secure Endpoint Console. 2. In the top right of the console, click ⓘ and then click **Support**. 3. Submit a Support case. For details, see Contacting Technical Support in the help documentation. You can also contact Absolute Technical Support by phone. For the list of Support phone numbers by region and language, go to Technical Support**.**