

Generate an Activation Code

Last Modified on 08.20.25

If you are acting in a Service Desk (or similar) role, you can generate an activation code using Privileged Access to temporarily elevate permissions for specified end users on target devices. The activation code can be used to run actions with a specific local user account. An activation code can be used even where the device is not connected to the Internet or if the device cannot reach the Agent Gateway. Once the activation code is generated, its details are included on the Privileged Access Activation Codes report.

You can generate an activation code directly from your Configuration Manager console or from the Recast Management Server interface.

Generate an Activation Code in Configuration Manager

To generate an activation code in Configuration Manager:

- 1. In your Configuration Manager console, right-click on one or more devices.
- 2. Select **Privileged Access** > **Create Activation Code**.
- 3. In the Create Activation Code window that opens, choose activation code settings and click Generate.

The activation code will appear and can be copied to selected devices.

Generate an Activation Code in Recast Management Server

To generate an activation code in RMS:

1. On the Privileged Access **Agents** page, click the Lock icon to the left of the agent.

Agents			
		🤍 Search 🔯	Export 🖒 Refresh
Drag a column header and drop it here to group by that column			
Actions	Name	Domain	
P 16	cmcbhekcl01	contoso.com	÷
К 4 1 > н			1 - 1 of 1 items

2. In the **Generate Activation Code** panel that opens, choose activation code settings and click **Generate**.

The activation code will appear and can be copied to selected devices.

Activation Code Options

• Activation Code Expires: Select the amount of time the user has to apply the activation code. This time period begins as soon as the activation code is generated. The default is 1 hour.

- Activation Code Valid for: Select the amount of time that the activation code will elevate permissions on the target device. By default, permissions will remain elevated for 1 hour. You can also choose to activate the code for Single usage.
- **Temporary Account Name**: Select the temporary account that the user is able to access using the activation code.
- Category (in RMS only): If the Require reason category in temporary elevation setting has been enabled by the Privileged Access administrator in the Client Settings, you are required to select a pre-defined reason category to describe why permissions are being elevated.
- **Reason**: Enter a reason permissions are being elevated.

Copyright © 2025 Recast Software Inc. All rights reserved.