

Limit Self-Service to Primary Devices

Last Modified on 02.09.26

In order to simplify the tracking of administrative privilege usage, you can opt to make self-service privileges available only when a user is logged into their designated primary device(s). This feature will work for both on-premises AD joined devices and Entra joined devices.

To define the user's primary devices

On-prem Active Directory: Populate the 'msDS-PrimaryComputer' attribute in the user's account object in AD
Entra: Intune/Entra ID automatically sets the primary user for devices. You can check, or manually change, the primary user following the steps in [Find the primary user of a Microsoft Intune device | Microsoft Learn](#).

To set up a self-service rule on just a user's primary devices:

1. On the Privileged Access **Self Service Rules** page, click **Add Self Service Rule**.
2. In the side panel that opens, choose the following options:
 - Rule Type: **Allow**
 - Users: **Everyone**
 - Devices: **User's primary devices**

Add Self-Service Rule ×

Type:
☐ Deny ☒ Allow

Users:
☒ Everyone ☐ Domain user or group

Devices:
☐ Target group ☒ User's primary devices

Rule is active ☒

3. Confirm that the **Rule is active**.
4. Click **Save**.