Remote password and session locking

A *remote password and session locking* policy can be configured for Windows and macOS devices. This policy enables you to configure rules for security features that help protect endpoint device user accounts from unauthorized access.

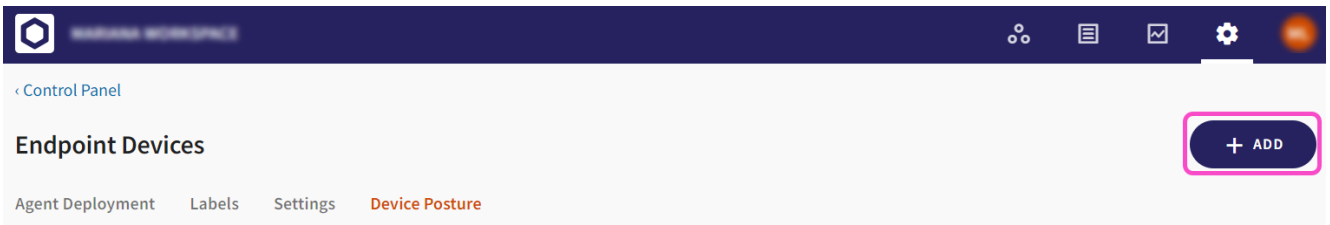
In this policy, you can configure:

- **Password**: Set rules and requirements for user passwords within the device operating system. These rules aim to enhance security by ensuring that passwords meet minimum strictness standards:
  - strength/complexity
  - a limited lifespan
  - not reusable within a defined number of resets
- **Screen lock-out**: Automatically lock the user's device after a specified number of failed password attempts during login (or screen unlock). This can help prevent unauthorized access from a brute force attack on a user's account. Admin users can configure the policy to allow a maximum number of attempts and the duration of the lock-out period.

Configuring password and session locking policies

To configure a new password and session locking policy:

1. From the **Device Posture** tab, select **+ ADD**.



2. Select the device operating system to which the new policy will be added (**Add to macOS** or **Add to Windows**).

   The **Add new device policy** dialog is displayed.

3. Select **Remote Password & Session Locking** from the **Select policy type** dropdown.