# The troubleshooting guide

## Overview：

If the account is displayed on the client side and the login interface is popped up after the account is logged in, perform the following operations:

1. Export the log and record the time point

2. According to the different error reports in the log, it can be divided into the following two situations. The detailed troubleshooting plan is shown below
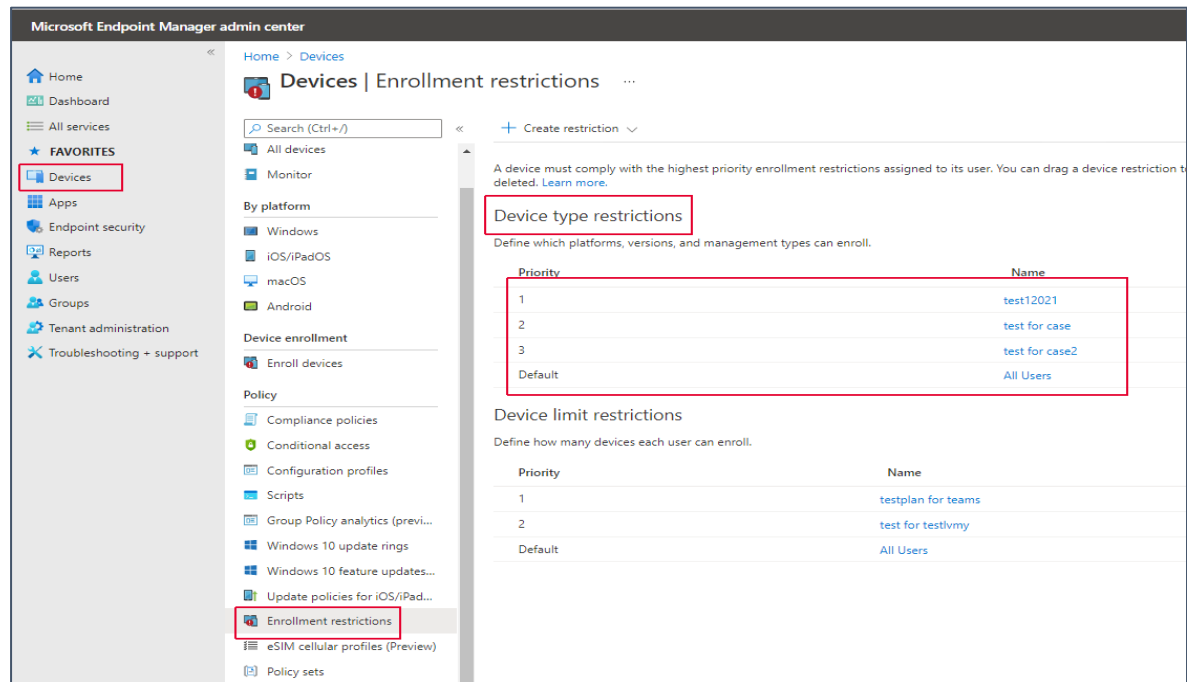
## 一、 Device type restriction

1. Export the log and search for the keyword "failurereason" near the time when the record appears. If the word "FailureReason[100]" appears, it is judged that there is a device type restriction, as shown in the following figure:



Ask the customer to do the following：

1. Visit Microsoft Endpoint Manager admin center：
   https://endpoint.microsoft.com/?ref=AdminCenter#home

2. Choose "Device-->Enrollment restrictions", and you can see the "Device type restriction"

3. Check the restriction status of each strategy, take "test for case" as an example, click on the strategy to enter the details interface, and switch to the "Properties" page
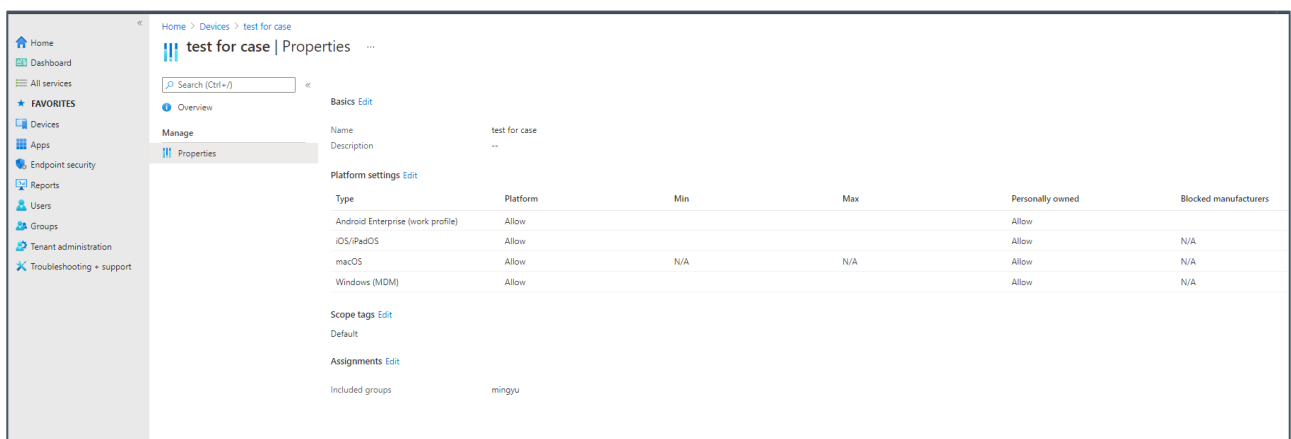


4. From "Properties", Check platform setting contains "Android device administrator", If
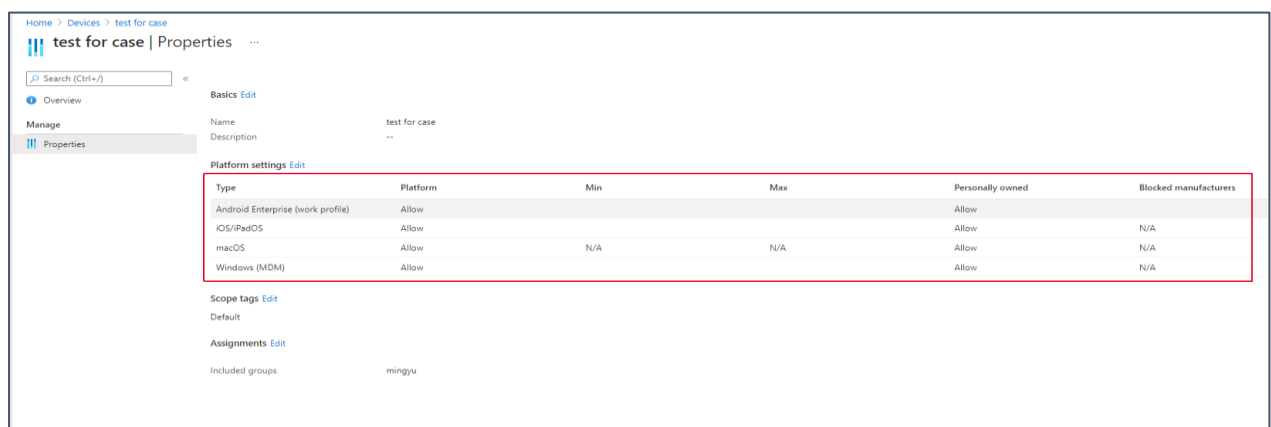
not, you can click "Edit"

5. From "Platform settings", adjust "Android device administrator" "Platform" and "Personally owned" to "Allow", save the setting

6. If the above restrictions are not set, please visit: https://aad.portal.azure.com and log in with an administrator account:

Select Azure Active Directory -> Security
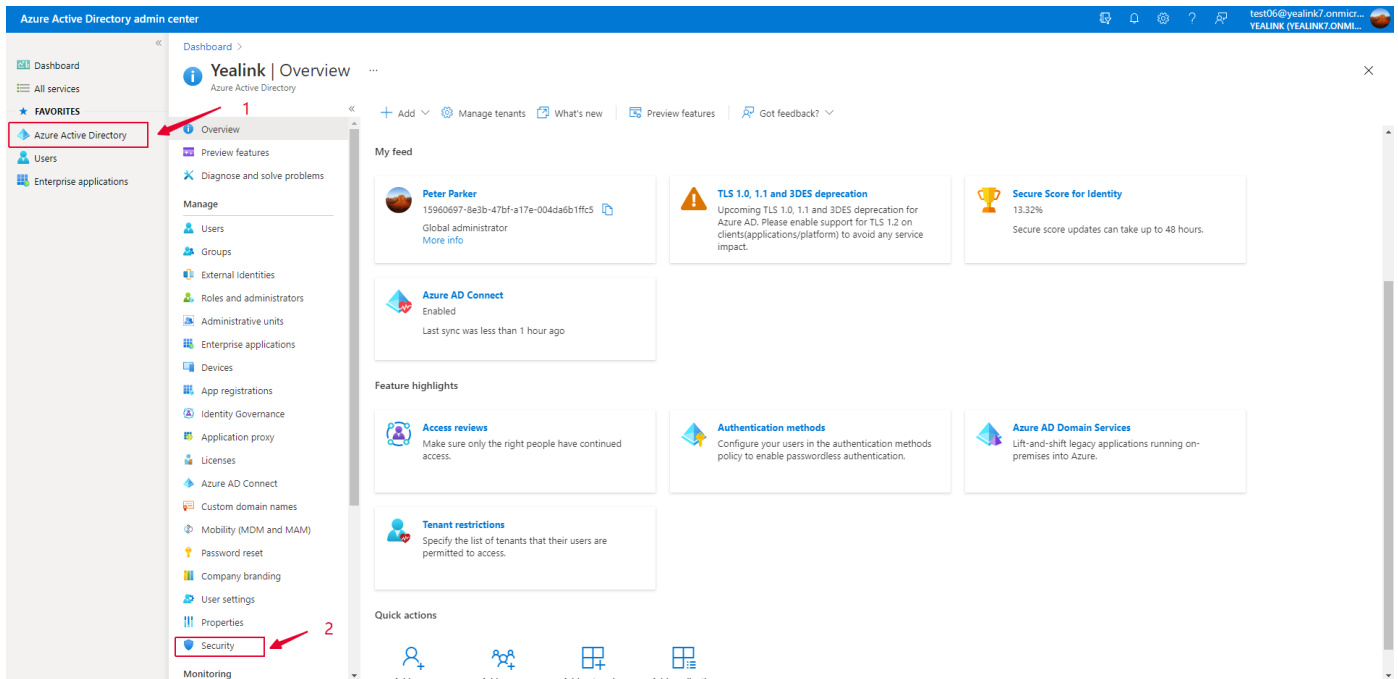


7. Select Conditional Access
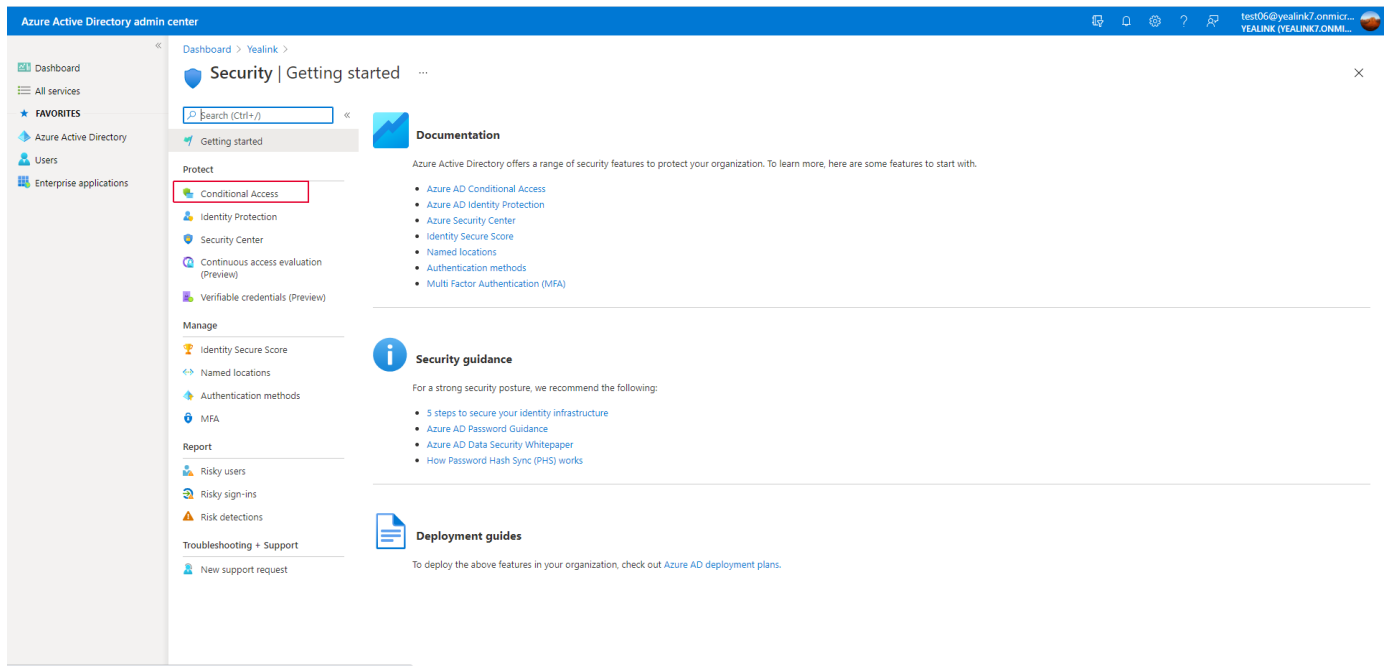
8. Check whether there is currently a policy that restricts the login of the phone

# 二、Device number limit

1. Export the log and search for the keyword "failurereason". If the word "FailureReason[102]" appears, it is judged that there is a limit on the number of devices, as shown in the figure below:



2. Azure registration restriction configuration (registration restriction for account)

   Visit https://aad.portal.azure.com/ through a browser, browse to "Azure Active Diretory-->Devices-->Device settings", in the "Maximum number of devices per user" parameter, you can customize each The maximum number of devices that a user can register, here is unlimited, as shown in the figure:
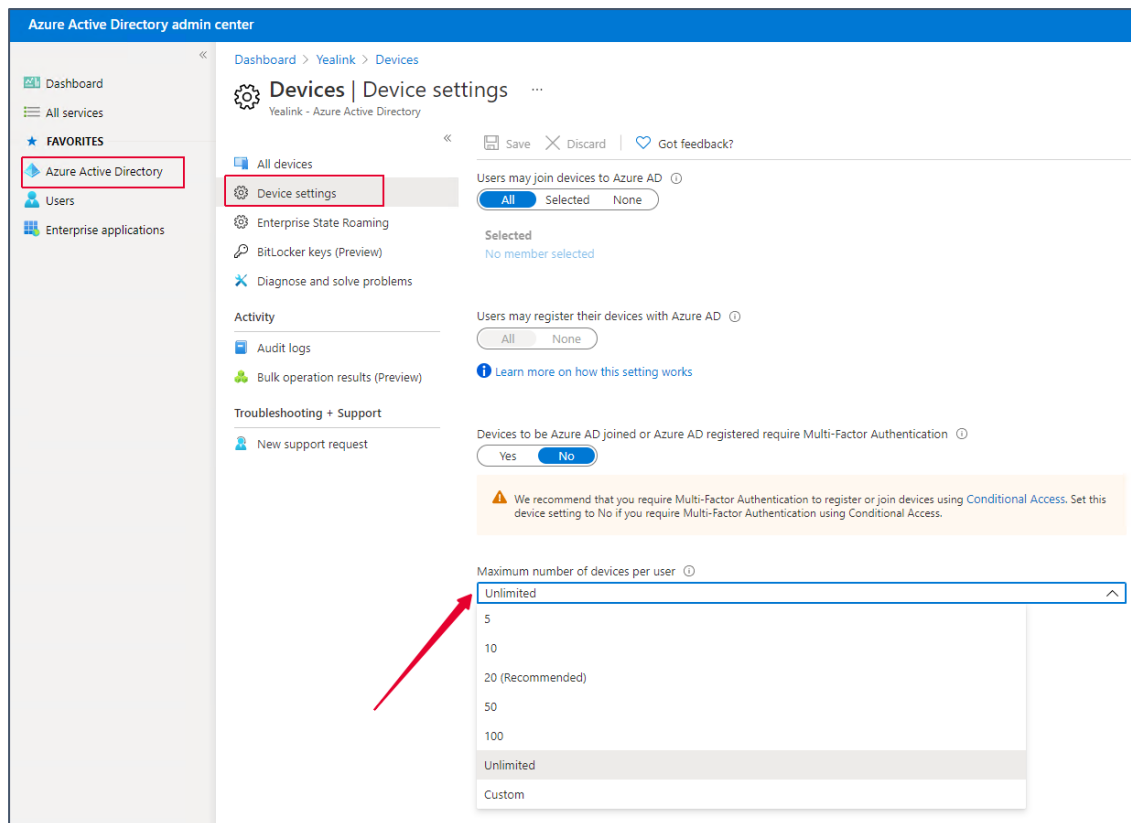
3. Intune registration restriction configuration (for device registration management)

3.1 Visit https://endpoint.microsoft.com/ through the browser, browse to "Devices-
->Enrollment restrictions", click the "Create restriction" button, and select "Device limit
restriction", as shown in the figure:

# Microsoft Endpoint Manager admin center

Home > Devices

## Devices | Enrollment restrictions ···

### Overview
### All devices
### Monitor

**By platform**
- Windows
- iOS/iPadOS
- macOS
- Android

**Device enrollment**
- Enroll devices

**Policy**
- Compliance policies
- Conditional access
- Configuration profiles
- Scripts
- Group Policy analytics (preview)
- Windows 10 update rings
- Windows 10 feature updates (Pre...
- Update policies for iOS/iPadOS
- **Enrollment restrictions**
- eSIM cellular profiles (Preview)
- Policy sets

**Other**
- Device clean-up rules
- Device categories

**Help and support**
- Help and support

+ Create restriction ⌄

Device type restriction

Device limit restriction

... with the highest priority enrollment restrictions assigned to its user. You can drag a device restriction to change its priority. Default restrictions are lowest pri...

## Device type restrictions

Define which platforms, versions, and management types can enroll.

| Priority | Name |
| --- | --- |
| 1 | test12021 |
| Default | All Users |

## Device limit restrictions

Define how many devices each user can enroll.

| Priority | Name | Device limit |
| --- | --- | --- |
| 1 | testplan for teams | 1 |
| 2 | test for testlvmy | 10 |
| Default | All Users | 15 |

3.2 On the "Basic" page, provide a name and optional description for the restriction, and select "Next", as shown in the figure:



3.3 In the "Device limit" page, select the maximum number of devices that the user can register as 15, as shown in the figure:

**Create restriction** ···

Device limit restriction

✓ Basics  ② Device limit  ③ Scope tags  ④ Assignments  ⑤ Review + create

Specify the maximum number of devices a user can enroll.

Device limit

| 15 | ∧ |

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

3.4 In the "Scope tags" page, fill in according to the tenant's own situation, and choose not to fill in here, as shown in the figure:

**Create restriction** ···

Device limit restriction

✓ Basics  ✓ Device limit  ③ Scope tags  ④ Assignments  ⑤ Review + create

Scope tags

Default ···

+ Select scope tags

3.5 In the "Assignment" page, click the "add groups" button, as shown in the figure:
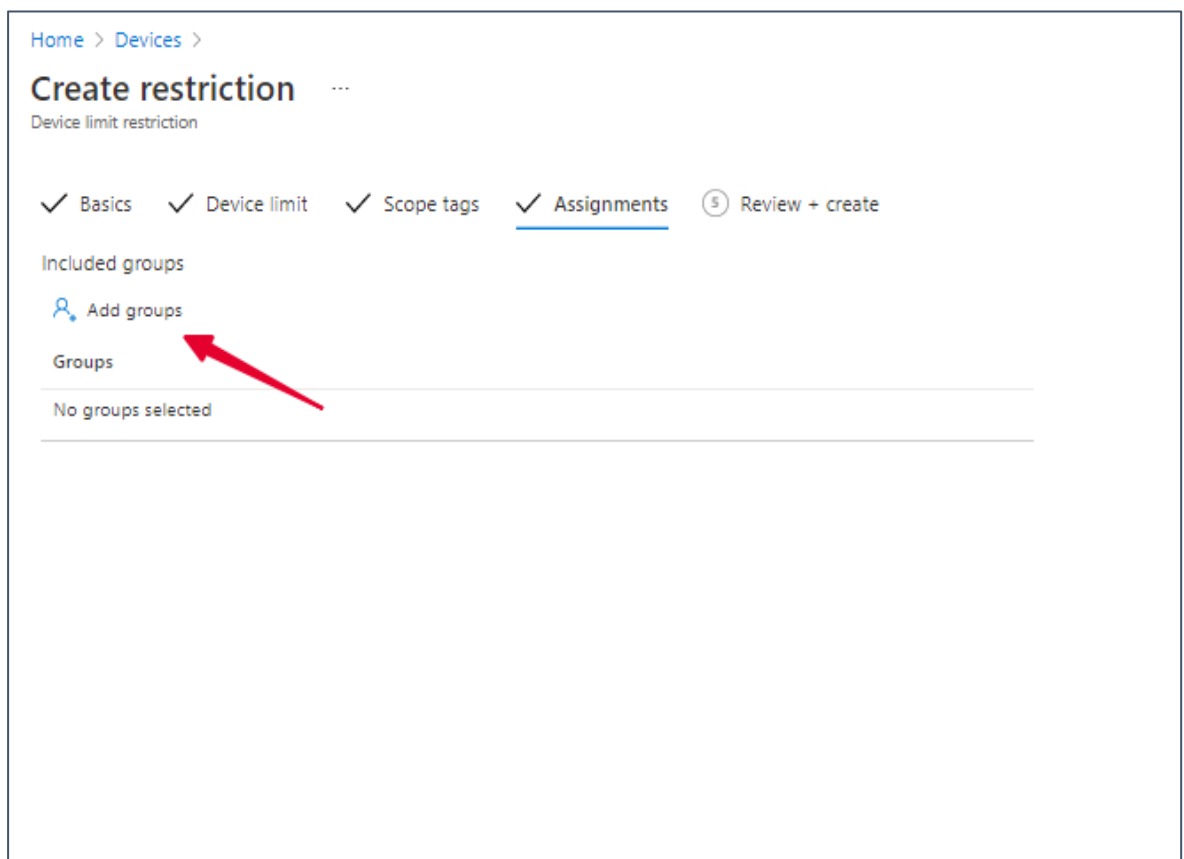


3.6 In the search box that pops up on the right, select the group that needs to apply the registration restriction policy, and click Add, as shown in the figure:

Select groups to include
Azure AD Groups

🔍 mingyu

m  mingyu
   mingyu1@yealink7.onmicrosoft.com
   Selected

Selected items

m  mingyu
   mingyu1@yealink7.onmicrosoft.com                    Remove
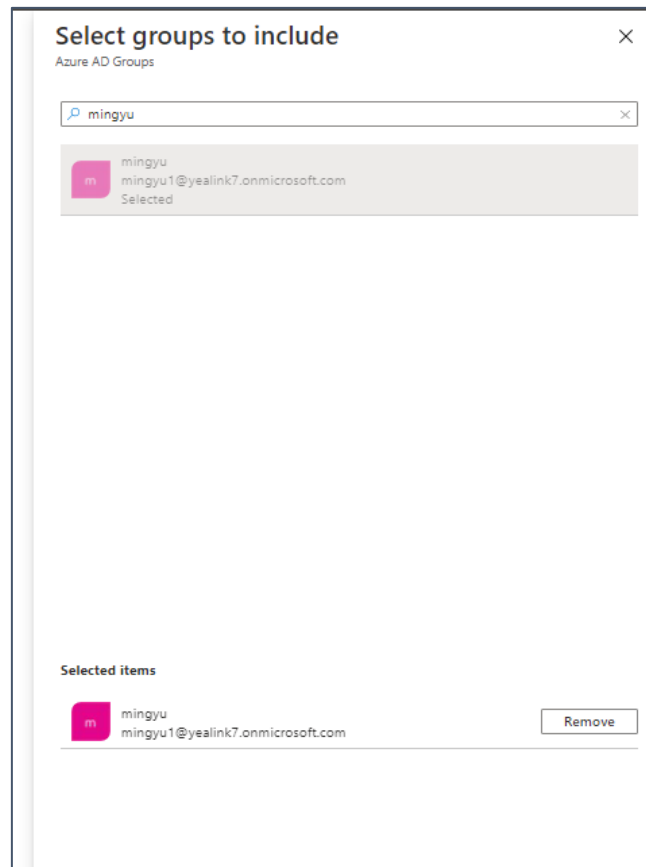
3.7 Preview the policy configuration in "Review+create", click Create after confirming that it is correct, as shown in the figure:



Home > Devices >

# Create restriction ···
Device limit restriction

✓ Basics   ✓ Device limit   ✓ Scope tags   ✓ Assignments   ⑤ Review + create

Summary

**Basics**

Name                          Test
Description                   This is a test

**Device limit**

Device limit                  15

**Scope tags**
 Default

**Assignments**

Included groups               mingyu
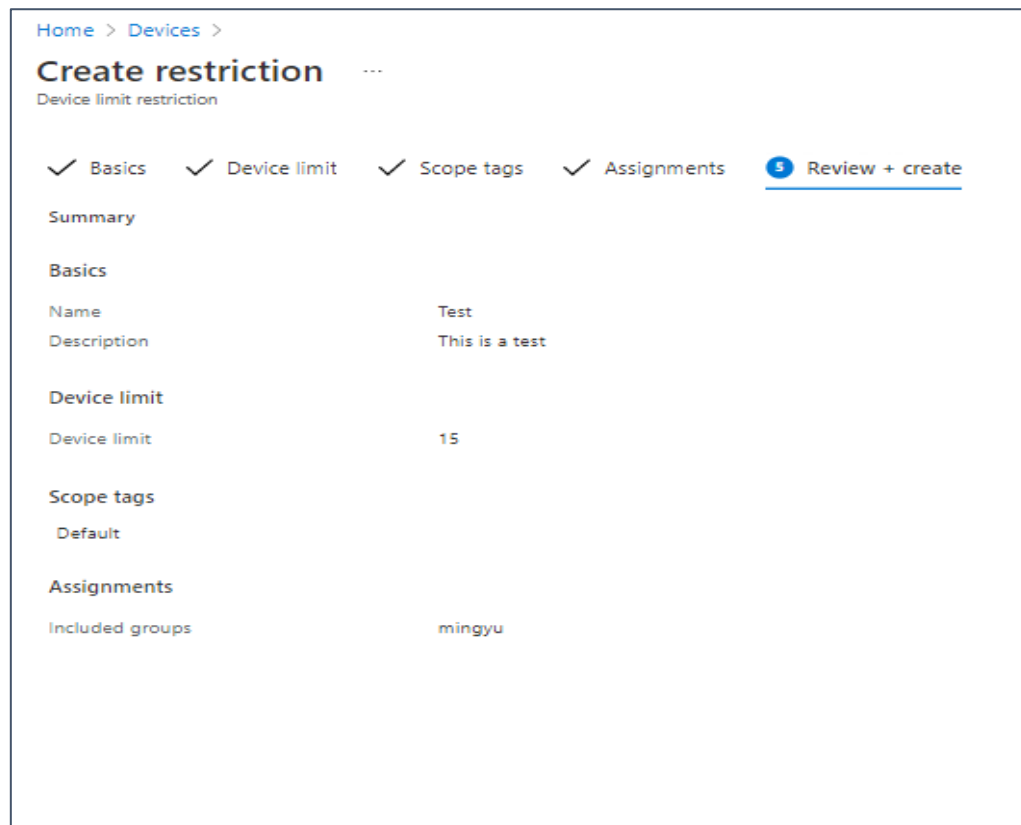
4. Lift the registration limit (delete the old registered device)

4.1 View user registration: Visit https://endpoint.microsoft.com/ through a browser, browse to "Home-->Resource alerts", click the "Device enrollment" button, as shown in the figure:
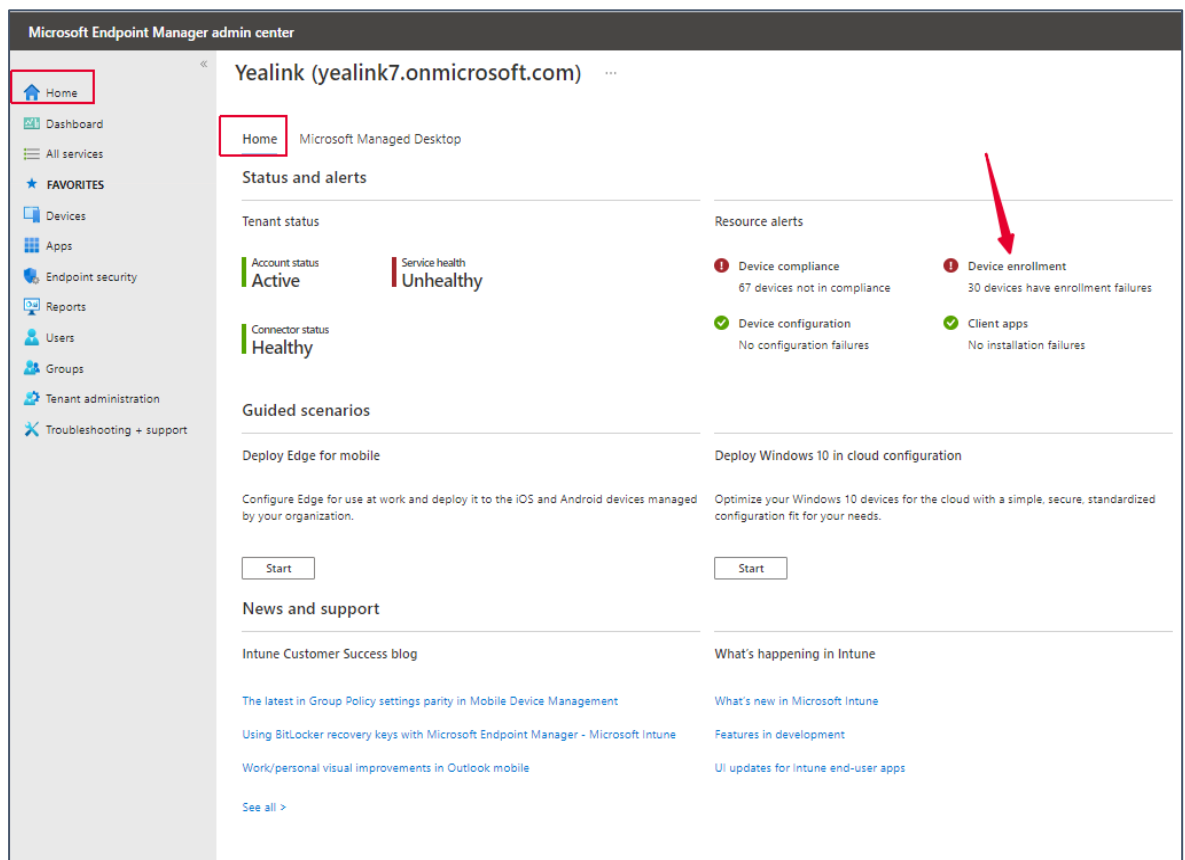


4.2 Select "Select user" and select the user to be viewed in the pop-up search box, as shown in the figure:
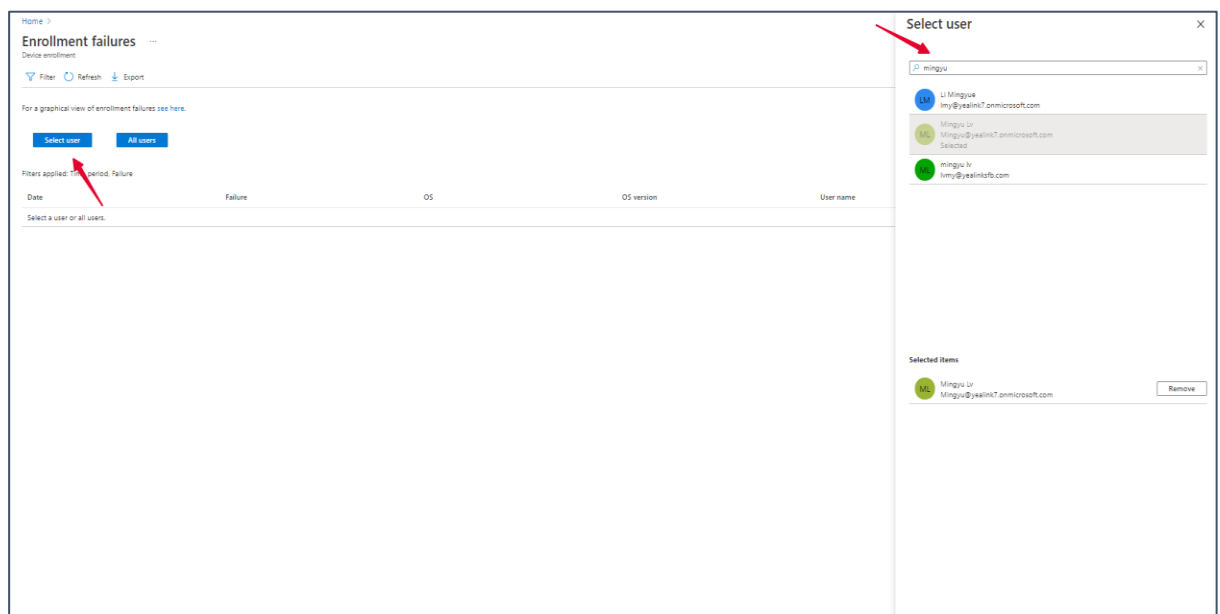
4.3 It can be seen from the query result that the user has reached the upper limit of registration, and the registered device needs to be cleaned up before logging in to the new device, as shown in the figure:
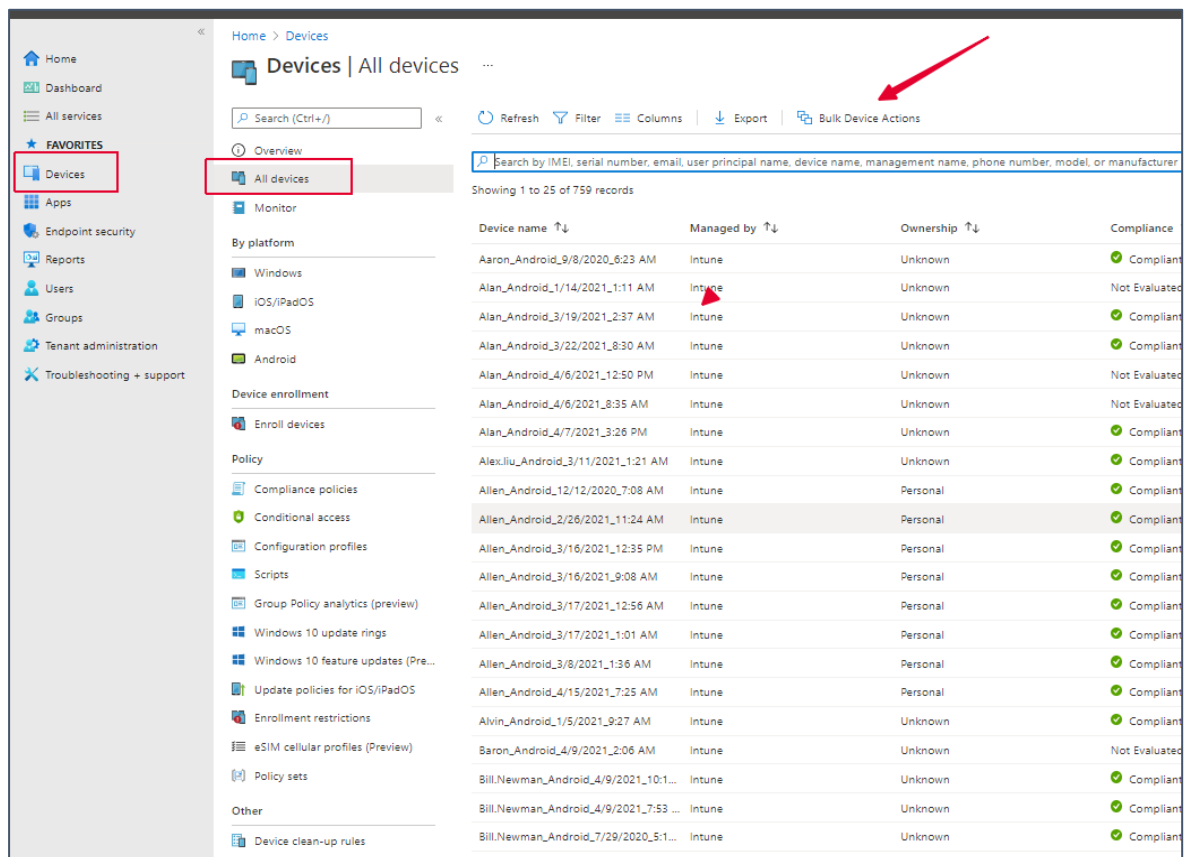


4.4 Delete the registered device: In the Endpoint Management Center, browse the "Devices-->All Devices" page and select "Bulk Device Actions", as shown in the figure:

4.5 In the "Basic" page, select the system to which the device belongs and the actions to be performed on the device to be deleted, as shown in the figure:



4.6 On the "Devices" page, click the "+Select devices to include" button, search for the device to be deleted in the pop-up box, and add it, as shown in the figure:

4.7 Preview the deleted task information in "Review+create", click Create after confirming that it is correct, as shown in the figure:
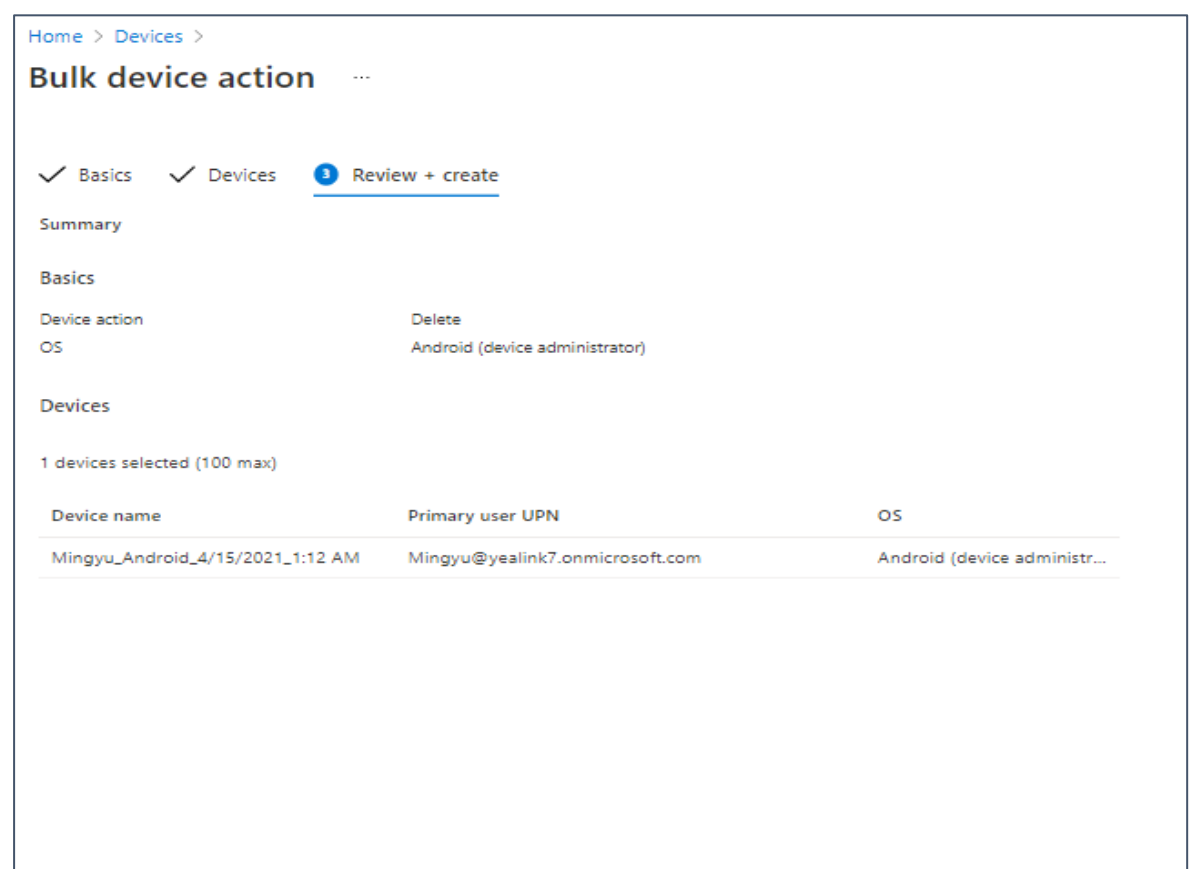


4.8 In the notification bar, you can see that the delete task has been successfully issued, as shown in the figure:
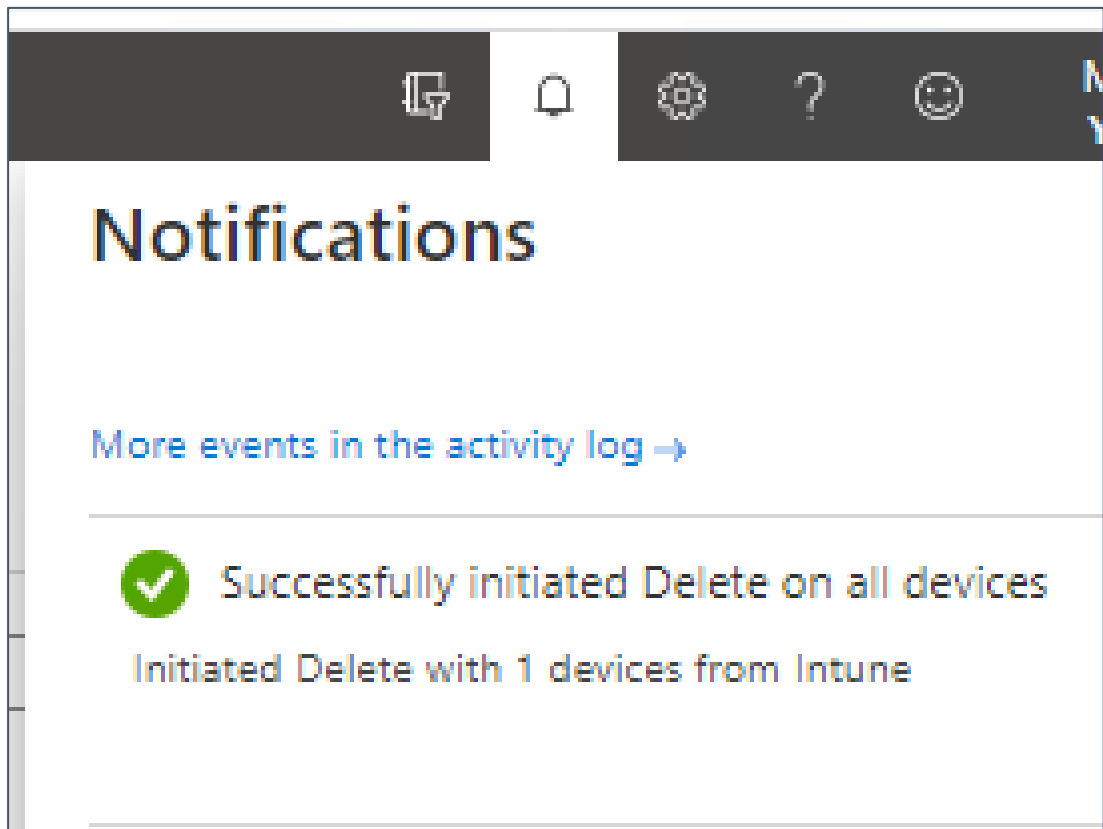
Reference

Other questions FAQ
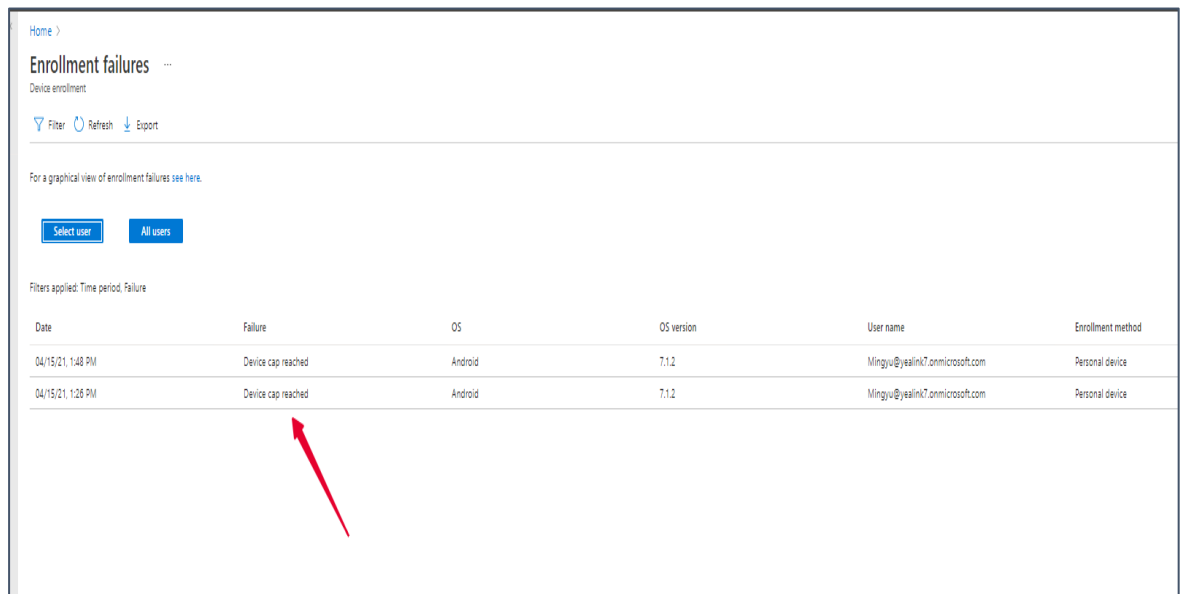
# 1. Reasons for account login upper limit

When you log out of your account, the regulations on Intune will not disappear after you log out. The regulations on Intune will only be deleted after automatic cleaning or manual cleaning. The shortest time limit for automatic cleaning is 30 days. It has not been manually deleted before. The maximum limit of the regulations is 15, so it is easy to reach the limit.

## 2. I found that there are more than 15 regulations on Intune. Why is there such a situation?

应用的筛选器:OS

🔍 yj08

🔍 yj09

Showing 1 to 18 of 18 records

Showing 1 to 19 of 19 records
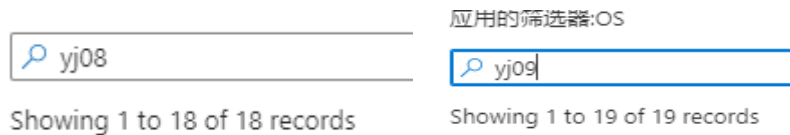
answer:
The reason for more than 15 items is because the old equipment records have been deleted but the table entries have not been cleared, resulting in more than 15 regulations.

## 3. After logging in to a restricted account and then logging in to a normal account, you will get stuck in verify a things

Answer: It may be that the cache of the previously registered account has not been cleared in the device, and the background has shown that the login is successful, but in fact the device has been stuck on the verify a things interface. Local verification is normal on the 7.22 version, and detailed verification will be performed on Teams update #4 in the follow-up
Temporary solution:
1. Restore the device to factory settings, the cache can be cleared
2. If you still cannot log in after restoring the factory settings, export the log to the development analysis, and try to log in again after waiting a few hours

## 4. Why do you need to configure Azure registration restrictions and Intune registration restrictions, two

Answer: There are two kinds of restrictions. Azure restricts the total number of simultaneous account logins, Intune restricts the total number of simultaneous login devices for accounts, and the limit configured by Intune is applied to the company portal. In other words, if the device does not have company portal software (such as PC) installed, it will not be intercepted by Intune login