

Overview

Trusted Login Devices displays devices that have been recognised for user access, together with the device name and the first login date and time. Use this screen when you need to review trusted devices associated with a user, narrow the list by user details, or maintain the identifying information stored on the record.

Sales representatives, account managers, project managers, purchasing officers, warehouse managers, and inventory controllers can use this information when checking which devices have been used to access the application.

Settings

Before saving changes, ensure that the user-identifying details are complete enough to find the correct record:

Field	Use
Enter User Name	Enter the user name used to identify the relevant user.
Enter Email	Enter the user's email address.
Enter Mobile	Enter the user's mobile number.
selectedBranch	Select the relevant branch.
Select...	Choose an available value where the screen provides a selection control.
files[]	Store files attached to the record. Use Attach to add an attachment.

Note: Use consistent user name, email, and mobile details. These fields help you distinguish the correct user record before reviewing or changing its trusted-device information.

Workflow

1. Open the trusted-device record and identify the user whose devices you need to review. Enter the available user details in **Enter User Name** and **Enter Email**. If required, also complete **Enter Mobile** and choose the applicable **selectedBranch** value.
2. Decide whether you need to narrow the displayed information.
 - To search using the entered user details, select **Apply filter**.

- To continue without filtering, review the trusted-device entries currently displayed.

The device list shows each device's name and its first login date and time. Use these details to distinguish devices such as desktop browsers running on different operating systems.

3. Decide whether the user details require correction or supporting evidence.
 - To retain changes to the current record and remain on the screen, select **Save**.
 - To retain changes and leave the record, select **Save and Close**.
 - To add supporting material, select **Attach**, then add the required file to **files[]**.
 - If a confirmation message is displayed after an action, select **Ok** to acknowledge it.
4. Decide whether to keep, discard, or remove the current record.
 - Select **Cancel** if you do not want to continue with the current changes.
 - Select **Delete** only when the displayed record should be removed.

Warning: Review the user details and the displayed device information before selecting **Delete**. The screen provides no separate device-removal action; do not assume that deleting the record affects only one device entry.

Examples

A warehouse manager needs to check trusted devices for a user who reports that they have accessed the system from more than one computer.

1. In **Enter User Name**, enter the user's name. In **Enter Email**, enter the user's business email address.
2. If the user works from a particular location, select the relevant **selectedBranch** value. Select **Apply filter** to focus the displayed information on the entered details.
3. Review the device list. The manager can compare the device names and first-login dates to determine whether the list includes separate desktop browser and operating-system combinations.
4. If the user details need updating, amend the relevant field and select **Save**. If the manager has a supporting document or record of the access review, select **Attach** and add it to **files[]**. When the review is complete, select **Save and Close**.

Tips

Tip: Filter by both **Enter User Name** and **Enter Email** when possible. This reduces the risk of reviewing a similarly named user's devices.

Tip: Use the first-login date and time as a reference point when comparing trusted devices during an access review.

Note: Use **Save** when you need to continue reviewing the record. Use **Save and Close** only after completing the review and any required updates.

Troubleshooting

Symptom	Likely cause	Fix
The required user's devices are not shown.	The entered user name or email does not match the user record, or the filter has not been applied.	Check Enter User Name and Enter Email , then select Apply filter again.
The wrong user's device information is displayed.	The search details are incomplete or identify a different user.	Verify the user name, email, mobile number, and selectedBranch before saving changes.
Changes are not retained after leaving the screen.	The record was not saved.	Select Save to remain on the screen, or select Save and Close to save before leaving.
A supporting file is missing from the record.	The file was not attached.	Select Attach , add the file to files[] , and then select Save or Save and Close .

Related pages

- [users](#)
- [Principal Users](#)
- [Security — Learning Path](#)
- [First Time Login](#)
- [Security — Overview](#)
- [Getting Started with Security](#)

