User editor

The user editor is available from *Dashboard* → *Users* by clicking a user row. It lets you edit user details, configure per-user Wi-Fi EAP credentials, and view the user's associated devices.

User details

The top section contains the user's main fields. Some fields are required and the editor shows validation errors when they are missing or invalid.

- **Id**: read-only identifier.
- **First name**: required.
- **Last name**: required.
- **Username**: required.
- **Email**: required and must be a valid email address.
- **Telephone number**: optional.
- **Google account**: optional and must be a valid email address when provided.

Google Authentication Default Policy

In Google Workspace environments with Google Authentication enabled, the editor can show **Google Authentication Default Policy**. This is the policy applied to devices enrolled using Google Authentication by this user.

- **Change policy**: opens the policy selection dialog.
- **Open policy**: opens the selected policy in the policy editor (when a policy is set).
- After selecting a new default policy, you must save the user to apply the change. The editor shows a notification reminding you to save.

Wi?Fi EAP credentials

The **WiFi EAP credentials** section is used to configure per-user credentials that are automatically installed on the user's devices when their assigned policy contains a Wi-Fi EAP configuration that requires them. The Wi-Fi EAP configuration is part of the Android policy network configuration.

Client certificate

You can optionally assign a client certificate to a user. When a certificate is assigned, it is shown in the **Client certificate** field and a menu provides actions. When no certificate is assigned, the field shows **No certificate assigned** and you can assign one.

- **Assign certificate**: opens the certificate selection dialog.
- **Open certificate**: opens the certificate editor.
- **Change certificate**: selects a different client certificate.
- **Disassociate certificate**: removes the certificate from the user. The system also removes the certificate from all devices associated with this user.

For certificate import and management, see **Certificate management**.

Identity, anonymous identity, and password

- **Identity**: identity of the user. For tunneling outer protocols (PEAP, EAP-TTLS) this is used inside the tunnel.
- **Anonymous identity**: used for tunneling outer protocols as the identity presented outside the tunnel. When not specified, it defaults to an empty string.
- **Password**: the user password for EAP methods that require it. If not specified, the device can prompt the user. A show/hide action toggles password visibility.

Associated devices

The **Associated devices** section shows the list of devices currently linked to the user. If the user has one or more associated devices, the user cannot be deleted.

Save and delete

- **Save user**: enabled only when the form is valid, there are pending changes, and the license is active. A progress indicator is shown while saving.
- **Delete user**: disabled when the user is associated with devices or when the license is expired/terminated. When deletion is allowed, a confirmation dialog is shown. If the user is assigned to enrollment tokens, the dialog warns that devices enrolled with those tokens will no longer be assigned to a user.

Unsaved changes warning

If you have unsaved changes and try to leave the page, the dashboard asks whether you want to discard the changes.

Revision #35
Created 2026-01-16 17:47:31 UTC by Admin
Updated 2026-04-22 15:46:19 UTC by Admin