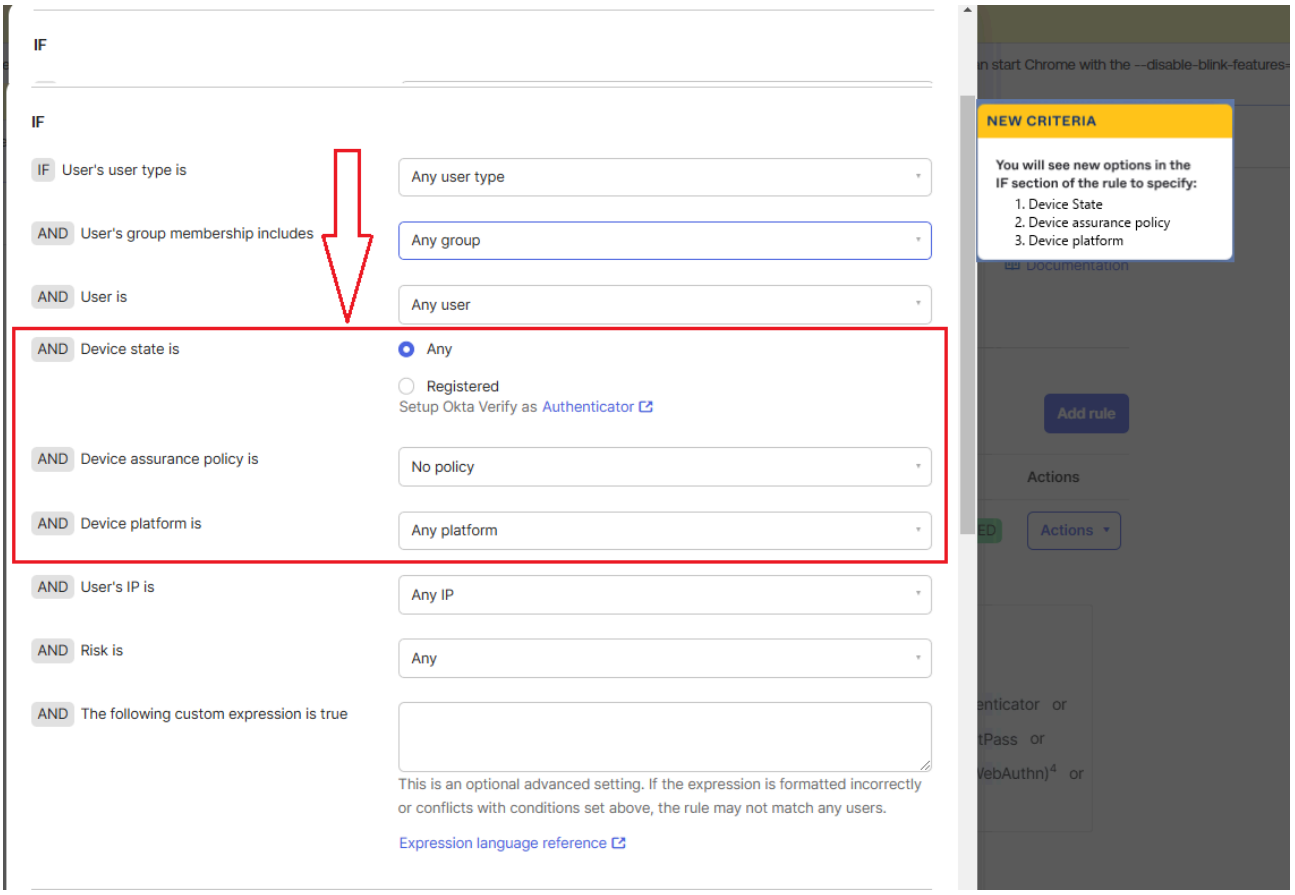
Conditional Access Based on Device Security Posture

Archived: 2026-04-06 00:48:44 UTC

Okta Identity Engine (OIE) can make application access decisions based on the device context in an incoming request. Device states, device assurance policies, and platforms can be used as conditions in the authentication policy for each app.



Okta Verify is required to be installed on that device to make it registered or registered and managed so admins can see details such as device name, platform, manufacturer, model, and Unique Device Identifier (UDID) in Universal Directory. Admins can **Suspend**, **Un-suspend**, or **Deactivate** a device. See Device lifecycle.

The device platform is determined by the User-Agent used in the authentication request.

Use signals from EMM & EDR solutions

If Device Trust has been purchased, it can be integrated with major Enterprise Mobility Management (EMM) and Endpoint Detection and Response (EDR) solutions to capture even more device signals and use custom expressions to make access decisions in the authentication policy.

Related References

- Devices inventory
- Device Trust on Identity Engine
- Endpoint security integrations
- EDR signals for custom expressions
