
# OAuth 2.0 Device Posture Signals

IETF 101 London, March 2018

William Denniss

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Use-Case: BYOD


Bring your own device (BYOD) is an increasingly common phenomenon in enterprise.

But users are hesitant to install invasive mobile device management (MDM) profiles that may let their company erase their device

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Common Enterprise Requirements


Enterprises generally want to know at least three things:

a) The user has a lock screen.
b) The operating system is up to date.
c) The phone is not rooted/jailbroken.

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Alternative to MDM


Rather than a “heavyweight” Mobile Device Management (MDM) solution, device posture signals can be used to communicate the device’s compliance state.

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Device Posture Signals


Device posture signals are simply bits of information send along with the authorization and token requests.

Authorization Servers (and the IDPs that sit behind them) can use them to make informed access decisions, and guide users to more secure installations.

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# The Spec


This spec creates an IANA registry for common signals, which are sent in a JSON dictionary, e.g.:

```
{
    "screen_lock": true,
    "root_privileges": false,
    "full_disk_encryption": true,
    "device_os": "iOS",
    "device_os_version": "11.1",
    "device_vendor": "Apple",
    "device_model": "iPhone X",
    "app_id": "ios:bundle-id:com.example.myapp",
}
```

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Token Request (Code Exchange)


```
device_posture={JSON}
```

Device Posture Signals are re-sent during the code exchange so that the token endpoint can validate that the signals were not modified in the user-agent (browser) during the authorization request.

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Token Request (Token Refresh)


```
device_posture={JSON}
```

Device Posture Signals are during token refresh so that the token endpoint can validate continued compliance.

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# App Adoption Viability


Not all apps will need to implement this for it to be effective.

Combined with a session identifier (assuming you’re using RFC 8252, and the session is shared), signals from one app can be applied to multiple.

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Protection Offered


This system can prevent authorization tokens being issued to honest users who don’t meet the security requirements (e.g. lockscreen) of the enterprise.

It is not designed to prevent authorization tokens being issued to dishonest users, who may be able to modify their own clients.

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# Device Posture + Token Binding


It may be possible to create a robust, unforgeable system combining token binding, with operating system attestations, wrapped up in a device posture signal.

John Bradley has the details ;-)

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01

# OAuth 2.0 Device Posture Signals


Discuss

https://tools.ietf.org/html/draft-wdenniss-oauth-device-posture-01