

# Threat model

Status: DRAFT

## OSGi Web Console

The Sling Starter, and other Sling-based applications, embeds the Web Console Provided by Apache Felix ( <https://felix.apache.org/documentation/subprojects/apache-felix-web-console.html> ). The web console offers direct access to many administrative functions, including deploying new code as OSGi bundles and adjusting system-level configurations.

Access to the Web Console must be restricted and only permitted to users trusted with total control over the deployment application.

Resources:

- [https://jackrabbit.apache.org/oak/docs/security/authorization/bestpractices.html#Threat\\_Model](https://jackrabbit.apache.org/oak/docs/security/authorization/bestpractices.html#Threat_Model)
- [https://en.wikipedia.org/wiki/STRIDE\\_\(security\)](https://en.wikipedia.org/wiki/STRIDE_(security))
- <https://shostack.org/resources/whitepapers/threat-modeling-what-why-how>
- [https://owasp.org/www-community/Threat\\_Modeling](https://owasp.org/www-community/Threat_Modeling)
- [https://owasp.org/www-community/Threat\\_Modeling\\_Process](https://owasp.org/www-community/Threat_Modeling_Process)