Bring Your Own Device (BYOD)

Deploy an API-centric BYOD Strategy with Axway API Gateway

With the rise of BYOD, today's enterprises must have pragmatic, secure and scalable strategies to deliver applications across multiple mobile platforms such as iOS, Android and Windows.

Consumer mobile devices, namely iOS, Android and Windows smartphones and tablets, have surpassed BlackBerry and Palm as the preferred mobile computing platforms for business use. It is now common for employees to buy and upgrade mobile devices on their own dime for mixed personal and business use, and demand to use them to connect to corporate networks. Enterprises that can't meet this demand risk losing productivity — and talented employees.

Axway API Gateway is an API gateway that enables enterprises to deploy a secure and scalable BYOD strategy that integrates mobile computing with existing business applications and security infrastructures while minimizing the risks introduced by devices that are not chosen or managed by enterprise IT.

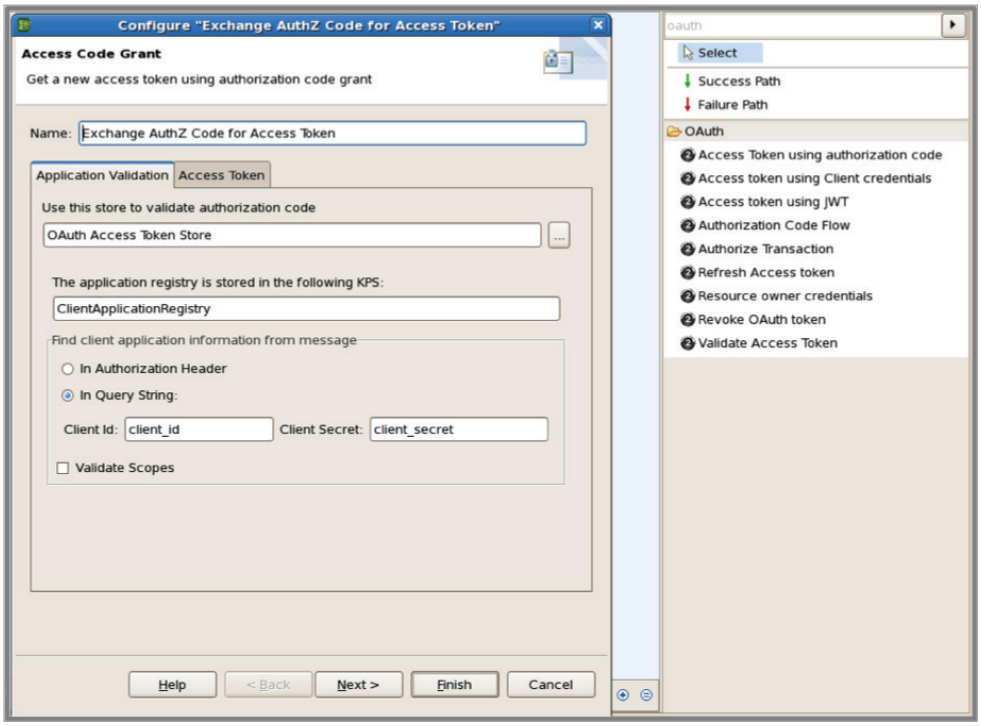
Minimize risk with secure and scalable API delivery

Smartphones and tablets are technically and physically less secure than notebook computers. They are frequently lost and stolen; their hardware and operating systems are lightweight and less hardened; and, because VPN use is not always practical, they gain mobile access to applications and services mostly via untrusted domains. To counteract these risks, most BYOD strategies center on two themes:

- Contained access, where mobile devices are allowed to connect to a guest network only. Some organizations go as far as white-listing devices, which is inconvenient and decreasingly effective over time as more enterprises embrace cloud-based services.
- Remote wiping of devices that have been compromised, which requires that IT gain control over the user's device with special software and access. This approach is intrusive and expensive to scale.

Axway API Gateway is a next-generation technology that enables enterprises to standardize the API development and delivery capabilities required to provide business services via cloud, mobile and partner channels. Encapsulating application gateway, cloud service broker and identity middleware functionality in a unified platform, Axway API Gateway provides an agile API environment that leverages existing back-end applications, services and data to help speed time-to-market for new business services.

Axway API Management Solution Pack is a dedicated API management solution that works with Axway API Gateway to simplify all aspects of publishing, promoting and managing APIs in a secure, scalable environment.



Configure OAuth 2.0 token for mobile clients

Other Axway API Gateway Solutions include:

- API and SOA Security
- API Identity and Access Federation
- Application Services Governance
- Cloud API and Service Brokering
- Cloud Data Security
- Cloud Identity Service
- Cloud Single Sign-On
- Fine-Grained Authorization
- Mobile API
- SharePoint Gateway

Axway API Gateway enables IT to adopt a more secure and scalable strategy leveraging mobile APIs. Without containing access or wiping devices remotely, you can use the Axway API Gateway to configure your API delivery for high availability, load distribution, geographical optimization, elasticity using cloud and virtualized infrastructures, security and disaster recovery. The server is built on an ultra-high-performance engine that executes API transformation, security, traffic management and monitoring tasks at wire speed — no competing product is faster.

Control system and data access at the mobile API level

Mobile applications are lightweight clients that don't do much local processing. Instead, they connect to cloud or on-premise business systems to access data and execute transactions. In this paradigm, it is more secure and scalable to control access at the API level than at the device level.

Axway API Gateway enables enterprises to deploy rigorous API-level authentication and authorization measures that enforce access decisions instantly and better protect against compromised devices and applications.

You can control access using:

- **Out-of-the-box integrations** with all the leading identity management platforms such as CA, IBM, and Oracle.
- **Contextual authorization** that can dynamically adjust access to data and functions based on application type, device location, network, time of day, and access behavior.
- **Multi-factor authentication** to further establish the trust level of the device and the device user.

Limit data storage on devices using mobile APIs

Mobile applications store data locally because connectivity is not always available and APIs are generally not designed to factor in the security risks of mobile devices. Instead of wiping the device of sensitive data after the fact, it is more secure and scalable to limit the amount of data stored on the devices in the first place.

The good news is that, as connectivity becomes faster and more ubiquitous, it is possible to drastically reduce or completely eliminate on-device data storage through proper design of mobile applications and mobile APIs.

Axway API Gateway helps enterprises create and deploy different versions of APIs for different API consumers, including mobile devices and applications. Mobile-specific APIs can be based on existing general-purpose APIs, but with additional data security and management policies to help reduce the need for on-device data storage. By moving more features to the API level, you can also rely more on web applications and less on native applications.