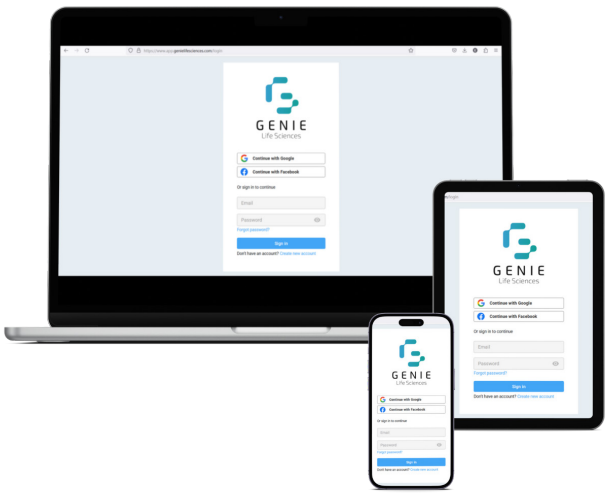
GENIE
Life Sciences

Security Features in Genie LabOS

Overview



Genie Life Sciences provides Genie LabOS, a cloud automation platform for defining, orchestrating and executing multi-instrument assays. Our platform interfaces with instruments built by Genie as well as other automatable laboratory equipment. This white paper details security functionality, architecture and policies of Genie LabOS and is intended for technology professionals seeking a high-level overview of the platform security posture.

Strong Identity

Any action performed on or to the Genie platform must be accompanied by a cryptographically verifiable identity or the requested action is rejected. There are four types of principals who may perform actions on or to the platform:

1. Platform Users who, for example, may perform actions through the Genie UI. Genie customers fall into the category of platform users.

2. Instruments which, for example, may send operation results and preventative maintenance data to the Genie platform.
3. Genie Platform Services which, for example, may interact with other platform services to fulfill user or instrument requests and may run scheduled maintenance workloads.
4. Genie Infrastructure Administrators who, for example, may perform troubleshooting and maintenance tasks such as system upgrades.

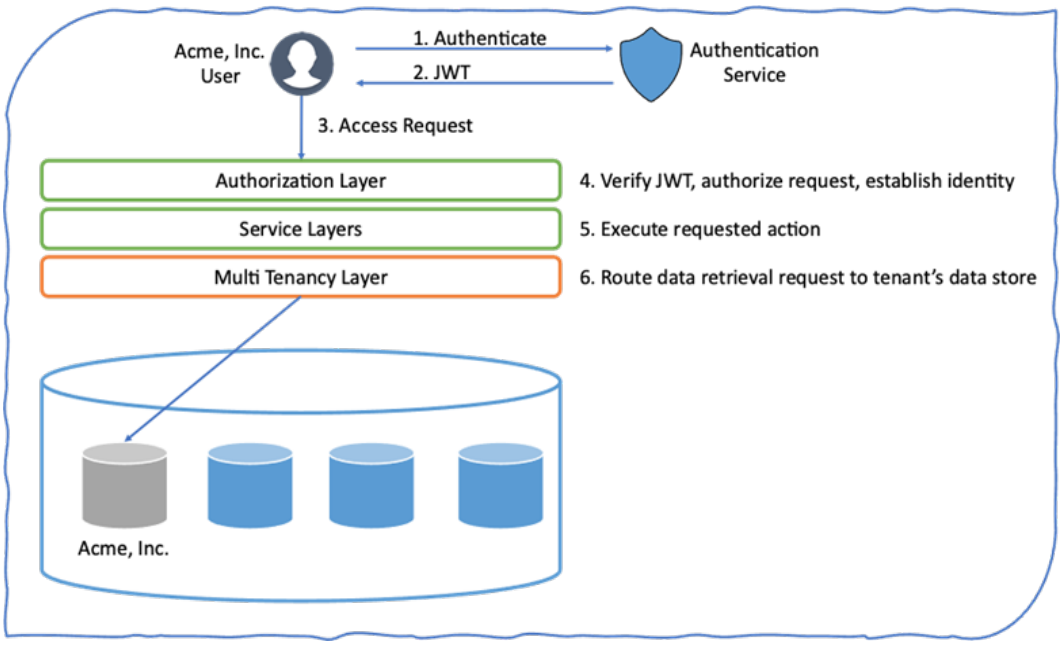
Customers are authorized to access and manage their data on the Genie platform. Their identity is established by authenticating to a centralized single sign-on service using a unique identifier (email address) and password. Once authenticated, they are granted short lived cryptographically signed tokens (JWT) that establishes their identity, roles and tenancy information. The token is signed using the RS256 algorithm (2048-bit RSA signature with SHA-256). All subsequent requests to the platform, such as REST API calls, must be accompanied by this token. The token is validated, and the customer is authorized against the requested action.

When an instrument is initially registered with the Genie platform, it is bound to a tenant and provisioned with a unique 2048-bit RSA key and an X509 certificate. The private key and certificate pair are used in TLS (Transport Layer Security) protocol's client authentication mode (see RFC 8446) to establish a strong identity for the instrument. When an instrument is deprovisioned from a tenant, its certificate is revoked.

Genie Platform Services are provisioned with long lived cryptographically signed tokens (JWTs). When a service-to-service request is made, the initiating service includes its token which is validated and authorized before the request is fulfilled. Token validation and authorization mechanisms are the same as the ones used for platform users.

Genie Infrastructure Administrators do not make direct requests to the Genie platform but rather manage the infrastructure on which the Genie platform runs. Infrastructure Administrators are Genie employees authorized to perform maintenance and troubleshooting actions on the platform itself. Their identity is established by Genie's corporate single sign-on service, which forces all infrastructure administrators to use two-factor authentication. They may then SSO (using SAML or OAuth 2) to Genie's cloud providers and assume the assigned infrastructure roles. No other Genie employees are given access to the platform's production infrastructure.

Multitenancy



At the core of Genie's cloud platform is a multi-tenancy architecture that enforces strict segregation of private tenant data. Forcing data of individual tenants to be stored in separate logical data stores makes it technically infeasible to query for data of more than one tenant, thereby establishing a strong layer of defense against

malicious or accidental actions that could otherwise cause one tenant's data to be leaked to another tenant. Strict safety of tenant data is a paramount architecture principle of the Genie platform.

Data-at-Rest

Genie implements multiple safeguards to protect persisted data. The safeguards include the following:

- All data stored on the Genie platform is encrypted at rest with AES 256.
- Decommissioning process of physical storage devices is done in accordance with DoD 5220.22-M.
- Genie maintains a backup retention policy of at least twelve months for all customer data. Deprovisioned customers' live data is deleted and backups naturally age out over the twelve-month retention period.
- Genie Life Sciences does not store any customer PII data on its cloud platform.
- All customer data is stored within the United States. In the future EU customers will have an option to have all of their data reside inside of the EU.

Data-in-Flight

All ingress and service-to-service communication is encrypted and restricted to TLS 1.2 or later.

On-Premises Security

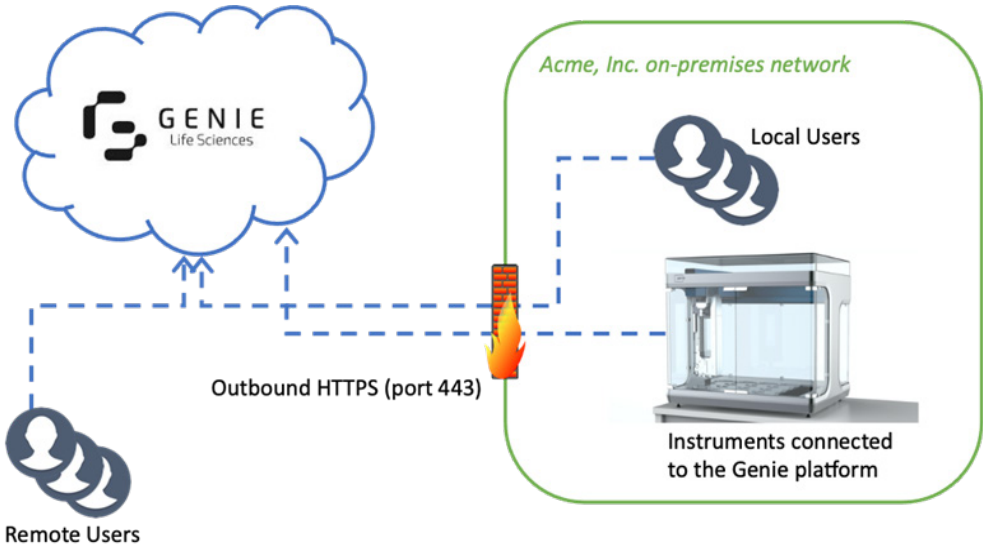
Genie Life Sciences manufactures laboratory instruments and can integrate with automation ready instruments of other vendors. The security posture of both of these deployment scenarios is very similar. In both cases secure communication with the Genie platform is brokered through a module called the Genie Connector.

The Connector establishes outbound HTTPS (port 443) connections with the Genie cloud platform. No inbound connectivity is required and only secure outbound connectivity over port 443 needs to be permitted. In most environments absolutely no changes need to be applied to the local network infrastructure. As discussed in the identity section, each connector is provisioned with a unique private key and certificate which it uses to authenticate to the platform. A connector can only send data to the logical data store of the tenant that owns the connector and only the tenant that owns the connector can send requests to it and therefore to the instrument(s) the connector controls.

Engineering Policies and Procedures

Genie Life Sciences incorporates many of the industry best practices in its software engineering policies and procedures, including

- Change control for all product and infrastructure changes with an audit trail from the originating request to implementation and rollout.
- Fully automated testing of all code and infrastructure changes
- Static code analysis of the product source code
- Security analysis of third-party modules and libraries
- Peer code reviews of all product and infrastructure changes



Operational Policies

Production infrastructure management is performed by Genie employees who are granted special Infrastructure Administration access.

- All Infrastructure Administrators are full time Genie Life Sciences employees and are based in the United States
- Infrastructure Administration access and actions are governed by Genie Life Science's operational policies.
- All infrastructure administrators have a background and past training in cyber security.
- All production access is audit logged.

Cloud Infrastructure Provider

Genie Life Sciences used AWS as its primary cloud provider. AWS maintains many security and operability certifications for its infrastructure, including SOC 2, PCI DSS and FedRAMP. Detailed reports can be downloaded from https://console.aws.amazon.com/artifact/reports.