

**📘 Key Terms to Understand**

**🏢 Authoritative Source**

Trusted data source like an HR application or internal database. Every organization should have at least one.

**🆔 Identity**

A human or non-human user in the organization created from authoritative source data.

**📡 Target Systems**

Applications integrated with SailPoint, including:

**Connected Applications**: Integrated directly via connectors

**Disconnected Applications**: Integrated via CSV files

**🔌 Connectors**

Bridges between SailPoint and target systems

Defines communication protocol and data structure

Over 100+ app-specific connectors in IIQ

**🔄 Aggregation**

**Account Aggregation**: Pulls account data

**Group Aggregation**: Pulls group/entitlement data

**🔗 Correlation**

Links external accounts with internal identities

Critical for preventing **orphan accounts**

**🛂 Entitlements and Roles**

**Entitlements** = Individual access rights

**Roles** = Groupings of entitlements for easier assignment

**✅ Certification**

Access reviews (attestations) conducted periodically

Ensures only valid access exists and helps reduce risk

**🌟 Understanding SailPoint IdentityIQ Architecture: A Step-by-Step Guide**

SailPoint IdentityIQ (IIQ) is a powerful Identity Governance and Administration (IGA) platform that enables organizations to manage user identities, govern access, and ensure compliance. This guide breaks down the architecture into clear, step-by-step components for beginners, using a vibrant and interactive style. 🎨📘

**🧩 Step 1: Authoritative Source Integration**

Begin with integrating an **authoritative source** (e.g., HR system or internal database). This trusted system contains identity data such as name, job title, department, and manager.

✔️ Identity types: Employees, Contractors, Service Accounts  
✔️ Data pulled into IIQ is stored as **digital identities**

**👤 Step 2: Identity Creation in IdentityIQ**

Once identity data is pulled:

SailPoint IdentityIQ creates digital identities 🆔

Each identity is linked to their **manager** 👨‍💼

**🧱 Step 3: Role and Access Assignment**

Roles simplify access assignment and governance:

**Business Roles**: Assigned based on job title, department, and location

**IT Roles**: Contain actual entitlements

🛡️ This promotes consistent and scalable access control.

**🔗 Step 4: Connected Application Integration**

Connected applications use predefined **connectors** for:

🔄 **Data Aggregation** (e.g., accounts, groups)

🚀 **Direct Provisioning** (e.g., add/update/remove accounts)

Examples: Active Directory, SAP, RACF, Oracle, JDBC

**🔓 Step 5: Disconnected Application Integration**

Disconnected apps don’t support direct integration:

Use **Delimited File Connector** (CSV/Excel)

Manual data import and provisioning

📩 Access handled via ticketing tools like ServiceNow or Jira

**🎫 Step 6: Ticketing Tool Integration**

For disconnected apps:

IIQ generates tickets for manual provisioning

Integrated with ServiceNow or Jira

Assigned to the **Application Owner** or **Admin Team**

**🔁 Step 7: Identity Lifecycle Management**

Managed through **Lifecycle Manager**:

🧑‍💼 **Joiner**: New hires

🔄 **Mover**: Departmental changes

📴 **Leaver**: Exit processing

🚀 Automates transitions to reduce manual overhead

**✅ Step 8: Certifications and Access Reviews**

IdentityIQ enables **certification campaigns** to:

Review user access regularly

Validate only needed entitlements remain

Revoke unused or outdated access (remediation)

🔐 Helps maintain **least privilege** access

**⚖️ Step 9: Governance and Compliance**

Ensure policy and regulatory alignment:

📋 **Compliance Manager**: Reporting and audit readiness

📊 **Governance Platform**: Internal policies and standards enforcement

🚫 Enforce SoD (Separation of Duties) to prevent risky access

**📈 Step 10: Reporting and Analytics**

Advanced tools allow:

📤 Exporting reports (PDF, Excel)

📊 Data analysis for trends and policy validation

✅ Audit tracking for compliance

**👥 Step 11: Key Personas in IdentityIQ**

**👨‍💻 End User**: Uses IIQ for access and certifications

**👩‍💼 Manager**: Approves/reviews access

**🧑‍🔧 Entitlement Owner**: Oversees access rights

**👨‍🏫 Application Owner**: Manages integration and provisioning

**🔍 Additional Core Components of SailPoint IIQ Architecture**

**📜 Compliance Manager**

Ensures regulatory and organizational compliance

Uses certifications, policy management, and audit reports

**🔄 Lifecycle Manager**

Minimizes unauthorized access

Automates provisioning based on employment lifecycle

Reduces manual workload for IT help desks

**🛡️ Governance Platform**

Ensures visibility and protection of cloud resources

Used in SailPoint Identity Security Cloud (prebuilt, low customization)

Enforces policies and minimizes risk

**🔐 User Provisioning**

Automates granting and revoking access across systems

Role-based access aligned with policy management

Timely provisioning boosts productivity and security

**🏁 Conclusion**

SailPoint IdentityIQ offers a complete ecosystem for secure identity governance, compliance enforcement, and operational efficiency. Its components and architecture enable organizations to manage access intelligently, automate tasks, and reduce risk—empowering modern enterprise security.