Aquera

SCIM Gateway for SailPoint

The Challenge

Organizations have many applications and are adding more all of the time. Being able to monitor, administer and govern user access in these applications is critical to running a compliant and secure enterprise. Manual exporting of user lists and their entitlements for each in-scope application into file extracts creates an operational and compliance audit challenge. Application owners must participate on a regular basis to generate and often edit the files, IT operations need to be scaled to support error handling and the file management process, and compliance audits must review the file creation and modification process for each application because there was human involvement. If people are involved in these processes, the accuracy and credibility of the audit can be questionable. Further, the generation and review of manual file extracts is very time consuming, often leading to infrequent imports and subsequent gaps in visibility. For these reasons the automated collection and transformation of the data contained in the above-mentioned file extracts is the preferred approach and is only possible via connectors being controlled by SailPoint identity governance solutions. Connectors remove the need for costly operational staff or application owner involvement with files, improve the efficacy of the data to shorten costly compliance audits, and enable the SailPoint platform to continuously import governance data for real-time analysis which improves the security and compliance posture of the organization. SailPoint has an extensive connector portfolio for this purpose, but how can other target applications be connected to the SailPoint platform?

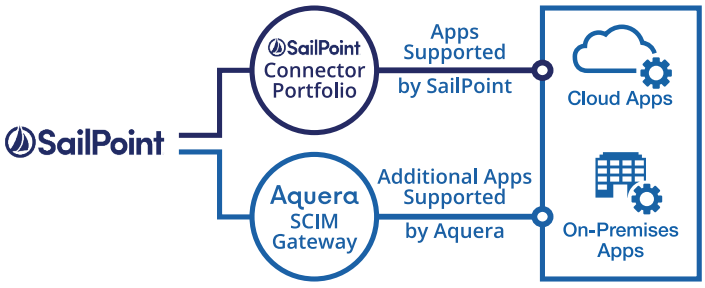
A related challenge is the automation of the account provisioning lifecycle. This starts with importing users and their data into SailPoint IdentityIQ from various HR sources such as applications, directories and databases. Once the users are imported into the SailPoint platform many organizations start the account provisioning lifecycle by first automating the immediate deactivation or deletion of the accounts of departing employees from applications, and then later add automated account provisioning. For the applications with high user churn it is important to automate user deactivation for security and compliance reasons, to automate provisioning for employee experience and to eliminate costly and error prone manual provisioning. Both the user import and provisioning lifecycle, similar to governance, require real-time connectors to exist between SailPoint and the target applications. And as with governance how will connectivity be achieved for targets not already available in the SailPoint connector portfolio?

The Complication

When an organization's IT group or third-party system integrator attempts to build custom connectors for the SailPoint platform to connect to the range of necessary user import sources and governance and provisioning target applications, directories, and databases, they are undertaking a complex and costly task. Skilled developers are required to write code specific to the user data source or governance and provisioning target, often taking three to four weeks per target to complete, and the resulting code remains the organization's responsibility to maintain and support for years to come. Further, the custom created code must be hosted somewhere, which creates additional complexity and cost.

The Solution

The **SCIM Gateway for SailPoint** from Aquera is a cloud-based service providing instant out-of-the-box, fully bi-directional connectivity between SailPoint IdentityIQ and all user import sources and governance and provisioning target applications, directories, and databases that an organization operates, which are not covered by the SailPoint connector portfolio. The SCIM Gateway powers SailPoint IdentityIQ to monitor and govern risk in real time across the entire application infrastructure by continuously importing, monitoring and governing user account information including entitlements and activity from all the targets through the SailPoint IdentityIQ SCIM (System for Cross-domain Identity Manage-



SCIM Gateway for Sailpoint

ment) protocol interface. The Aquera platform also supports SailPoint's JDBC interface to collect user activity from the various applications where user activity information is available. The benefits of having a fully automated and real-time data extraction and transformation infrastructure orchestrated by SailPoint IdentityIQ are now fully realizable with the combination of the SailPoint connector portfolio and the SCIM Gateway for SailPoint from Aquera.

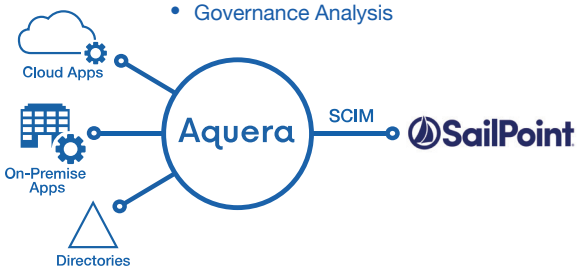
For the account provisioning lifecycle, the SCIM Gateway enables the SailPoint platform to create, update, deactivate and delete user accounts in any application, database or directory. The scope of this even includes governing and provisioning cloud apps without user management APIs via screen scraping and custom homegrown applications via SQL/JDBC (Java Database Connectivity) calls or screen scraping. The comprehensive list of methods for integrating with the targets include REST APIs, SOAP or web service APIs, admin console automation, SQL/JDBC, FTP, LDAP, SDKs and middleware messaging queues.

The SCIM Gateway for SailPoint can be configured to support various use cases and these configurations are illustrated in the diagrams. The **Governance Data Bridge** configuration is used for importing governance and user activity data from any source into SailPoint IdentityIQ. The **Provisioning Gateway** configuration is used for updating, deactivating, deleting and provisioning accounts for any target from SailPoint IdentityIQ. Finally, the **User Import Bridge** configuration is used for importing users into SailPoint IdentityIQ from any source.

Aquera connects the source and target sources to SailPoint IdentityIQ using the SCIM protocol. This allows SailPoint IdentityIQ to carry out both read and write operations against the target sources including user information sources. The SCIM protocol is an IETF standard for automating the exchange of user identity information between identity domains or IT systems. For all employees, partners and customers, SailPoint IdentityIQ will have the ability to create, read (import), update, and delete any number of users, groups, and entitlement attributes available from the target sources for monitoring, administration, governance, user importation, automated account deactivation and deletion, and when ready, automated account provisioning.

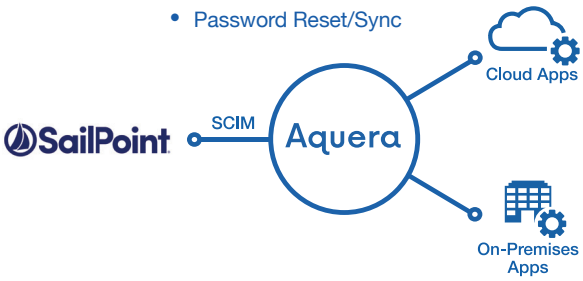
Governance Data Bridge

- Account Aggregation
- Governance Analysis



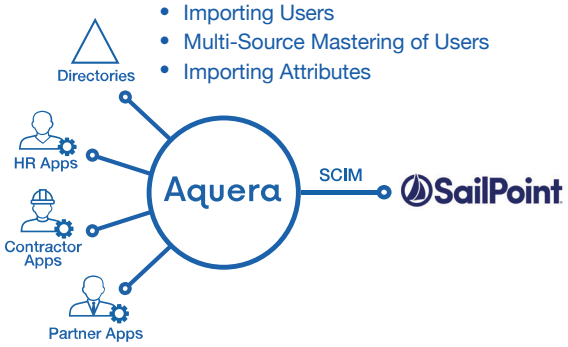
Provisioning Gateway

- Account Provisioning
- Account Deactivation
- Password Reset/Sync



User Import Bridge

- Importing Users
- Multi-Source Mastering of Users
- Importing Attributes



About Aquera

Aquera extends the user provisioning and governance coverage of identity management platforms with the Aquera Identity Fabric Platform. The platform offers SCIM gateway services and out-of-the-box connectivity from any identity management platform to any cloud or on-premises application, database, directory or device. The gateway services support user account provisioning and deprovisioning, importation of HR data, and the aggregation of governance data. The connectivity is plug-n-play requiring zero coding and instantly deploys in 5 minutes or less. The business results are more applications under management of your identity platform in less time, cost savings in development time and maintenance, an agile IT architecture, a secure infrastructure, and accelerated projects yielding top line benefits. Aquera makes it our business to make the CIO's vision a reality for automated provisioning, deprovisioning and governance of user accounts across the entire IT infrastructure.