Advantage Single Sign-On Overview

Single Sign-On (SSO) is the concept used to describe a centralized access control system managing multiple, related applications requiring authentication. For example, Google provides an SSO mechanism for its suite of products: Analytics, Hangouts, Gmail, YouTube, Photos, etc. In Google's case, only one username/password is required to access all the applications and is managed through its myaccount.google.com hub.

For AdvantageCS clients, it is common to have several applications requiring authentication. These could be eCommerce sites, self-service portals, content sites on multiple platforms and mobile applications such as iPhone apps. Consolidating the access control into a single system provides many benefits—to both the customer and the organization's internal IT staff. The Advantage SSO system provides clients with a flexible, cloud-based SaaS solution to centralize all access control systems, including Advantage's powerful subscription functionality and eCommerce platform, Cider.

Business Need

There are several key reasons for the development of this solution.

- AdvantageCS clients deploy multiple applications requiring customer authentication. In order to offer a consistent customer experience and technological strategy, an SSO solution is required.
- The Advantage system currently maintains user credentials and entitlements. External systems can authenticate against the Advantage system using the Advantage APIs, but that can introduce availability and performance concerns depending on the infrastructure configuration. Additionally, it assumes that Advantage maintains this information for all applications within an organization, which is not always the case. A separate SSO system, integrated with Advantage's native access and control features, provides an out-of-the-box solution to manage the entirety of a client's applications.
- Some AdvantageCS clients have implemented other SSO solutions—either in-house or using a third-party solution. These SSO solutions do not offer native Advantage integration, which must be developed and maintained as the Advantage system evolves. The Advantage SSO solution solves this issue while providing

Application Integration

In SSO, an application is defined as one requesting authentication (user identity) and/or authorization (user entitlement) information. The Advantage SSO solution ships with enhanced support for three specific applications, and is built to support as many as desired. **Some of the key features for each are described below.**

- Advantage – In the SSO context, this application is used to create, market, sell, and provide customer service for subscriptions.
  - Customer authentication records can be configured to use SSO instead of Advantage's local user-credentials database.
  - Customer service representatives can create SSO accounts, reset passwords, change accounts, and link customers to existing SSO accounts, all from the Advantage application.
  - Advantage access information (i.e., entitlements) is fed to SSO anytime access is created or changed. Customer service representatives can see the SSO entitlement information directly from the authentication record within the Advantage application.
  - There is a mechanism to migrate existing Advantage authentication records to SSO.

- Cider – This application is an eCommerce platform where customers can purchase products and perform customer self-service functions.
  - Cider can be configured to use Advantage SSO instead of Advantage's local user-credential database.
  - The registration page creates an SSO user.
  - All login and logout activities are done through SSO.

- WordPress – This application is used to deliver content purchased in Advantage/Cider.
  - WordPress can be configured so that users only get access to certain content if they are logged in and have been granted the appropriate entitlements through Advantage/Cider.
  - All login and logout activities are done through SSO.

AdvantageCS clients can integrate their own applications through the Advantage SSO admin portal. Each connecting application needs to support OpenID Connect, a layer on top of OAuth, which provides security and user-identity features for integrated applications.

User Identity and Access Control

Customer identity and entitlement information is communicated via a claims-based, token-based scheme. Once a user logs in, a token is provided to the requesting application. The requesting application can then use that token to communicate with an entitlement service to retrieve the set of user entitlements (e.g., subscriptions).

The Advantage application maintains an entitlements claim in Advantage SSO. This claim describes the content the customer has purchased through the Advantage application. In addition to the content identifiers, the claim includes the start and stop dates for each entitlement.

Another important concept related to access control is scope. Scopes can be used to limit the amount of information sent to each application. This scheme ensures each application is receiving the appropriate information from SSO.

Key Benefits

The SSO solution offers several key benefits for current and prospective AdvantageCS clients.

- Improved customer experience – Customers no longer have to remember multiple username/password combinations for the various applications for which a publisher requires authentication. Additionally, customers do not have to log in to each individual application separately. This provides a more cohesive experience for the user, as expected when accessing multiple applications under a single brand.
- Simplified technical efforts – In a non-SSO environment, each authenticating system has its own set of functions that must be maintained: registration, password reset, login/logout, etc. In addition, each system has its own technology stack. By combining these functions and technologies into a centralized SSO solution, overall development and maintenance costs are reduced.
- Security – The Advantage SSO solution uses a modern security protocol for interactions with client applications, OpenID Connect. This protocol adds several key security features on top of those provided by OAuth alone. The Advantage SSO solution uses enterprise Microsoft technologies, ensuring the most up-to-date security protocols in the industry.

Deployment

Advantage Single Sign-On is deployed as a cloud-based, SaaS solution. The solution is hosted in Microsoft's Azure platform providing the necessary performance, scale, and security requirements. Each client would minimally have two instances of the solution configured—a test instance and a production instance. Each instance runs the same core SSO application code, but may have other client-driven customizations such as additional SSO applications, claims that are being tested, theme customizations, etc. As AdvantageCS makes changes to the core SSO application, those changes will be pushed to all deployed instances on a regular schedule.