SAPinsider

This article appeared in the Oct ▪ Nov ▪ Dec 2016 issue of *SAPinsider* (www.SAPinsiderOnline.com) and appears here with permission from the publisher, WIS Publishing.

WIS pubs

Donka Dimitrova
(donka.dimitrova@sap.com) joined SAP in 2007. For several years, she worked as a product expert for the SAP Business Process Management solution before moving into the security area and becoming part of the SAP HANA Cloud Platform Security team, where she focuses on identity management and single sign-on solutions.

End-to-End Identity and Access Management in the Cloud

Managing User Access to Business Applications with SAP HANA Cloud Platform Services for Identity Provisioning and Identity Authentication

Businesses are pushing their technology into the cloud to harness its agility and flexibility, but doing so presents questions around security. How do you protect your data? How do you ensure users have access to the right information — and only that information? And how do you make the experience seamless enough to increase user productivity and use of their business applications?

In the SAP HANA Cloud Platform family, there are security services designed to ease the adoption of cloud applications by providing features for end-to-end identity and access management:

- **SAP HANA Cloud Platform Identity Provisioning** (released in September 2016), which ensures that employees have up-to-date access rights in the cloud for their entire tenure at the company
- **SAP HANA Cloud Platform Identity Authentication** (available since 2014 and formerly known as SAP Cloud Identity), which provides simple and secure authentication for all web and cloud applications that users need to access, regardless of location and device

This article introduces these two security services of SAP HANA Cloud Platform and looks at how they work together to improve access and identity management for businesses with increasingly cloud-heavy technology deployments.

Provisioning Users to the Cloud

The SAP HANA Cloud Platform Identity Provisioning service helps companies easily onboard users onto cloud applications. Using the administrative user interface of the service (see **Figure 1** on page 52), companies can simply take identity data from their on-premise Microsoft Active Directory or from the SAP NetWeaver Application Server (SAP NetWeaver AS) ABAP user store and provision these user identities to cloud applications such as SAP Hybris Cloud for Customer.

Once the identities are available in the cloud application, they need to have proper authorization roles to run the scenarios that are relevant for them. This is exactly the purpose of the

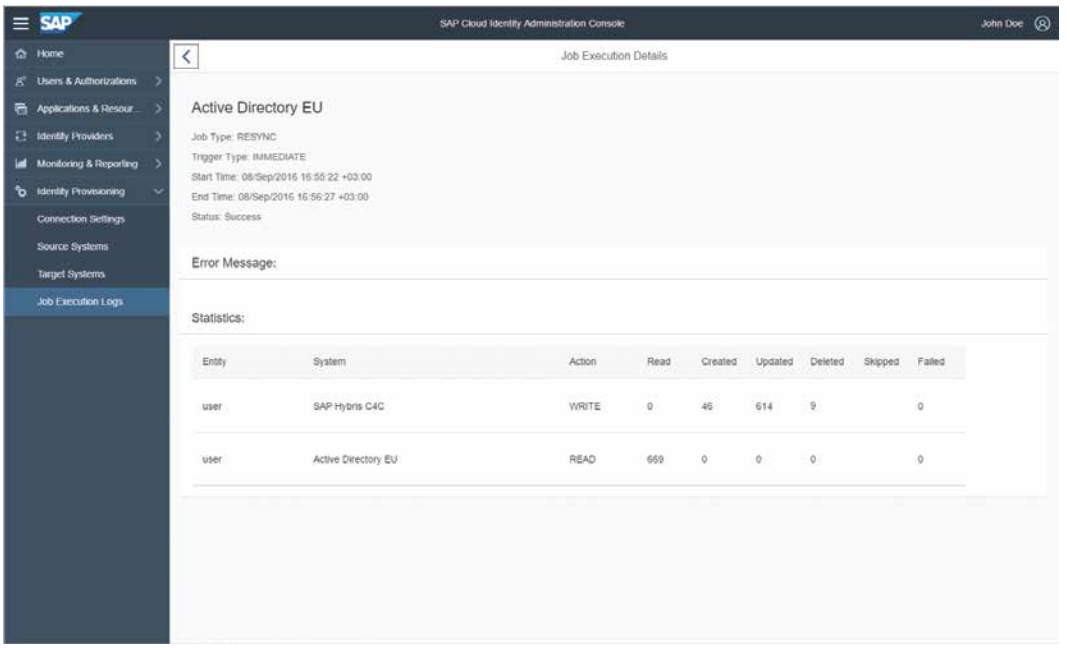

Figure 1 Using the administrative user interface of the SAP HANA Cloud Platform Identity Provisioning service, you can provision identity data from on-premise user stores to cloud applications

policy management feature in SAP HANA Cloud Platform Identity Provisioning. Companies can define authorization policies using a simple mapping of the grouping artifacts maintained in the corporate user store with the authorization artifacts of the respective cloud-based business application — such as a mapping between Microsoft Active Directory groups and SAP Hybris Cloud for Customer roles, for instance. During the provisioning process, these policies are considered, and the authorizations of the individual user are determined and provisioned to the respective cloud applications.

SAP customers that use SAP SuccessFactors Employee Central to manage their employees will be able to configure the SAP SuccessFactors system as a source system in SAP HANA Cloud Platform Identity Provisioning and to reuse the up-to-date employee data for synchronization of the user identities across the SAP cloud applications.

> Using these SAP HANA Cloud Platform services enables companies to leverage their existing infrastructure while adopting cloud applications.

The frequency with which identity and access provisioning occurs for cloud applications is configurable, and can be adjusted to comply with corporate processes and practices. Organizations can use the comprehensive scheduler that comes with the service to define the timing of the provisioning process, ensuring up-to-date identity and access management in the cloud for all users.

Support for additional provisioning integrations — such as SAP Ariba, Concur, and others — is planned for future releases of SAP HANA Cloud Platform Identity Provisioning.

Once the identity provisioning is complete and the user is assigned with proper access in all cloud applications, the integrated SAP HANA Cloud Platform Identity Authentication service is then available for handling secure authentication and single sign-on to those applications.

Authentication and Single Sign-On in the Cloud

The SAP HANA Cloud Platform Identity Authentication service is a single sign-on (SSO) service

that enables users to sign in once to access multiple cloud applications securely. It offers a standard SAML identity provider (IDP) that runs in the cloud and can integrate with SAP web and cloud applications. It can also handle secure authentication and SSO for any non-SAP application or platform that supports SAML as a standard service provider.

The cloud IDP available with SAP HANA Cloud Platform Identity Authentication offers a set of authentication mechanisms to help companies manage SSO scenarios and other challenging authentication scenarios, such as strong authentication from outside the corporate network, mobile SSO, and others. Using the administrative user interface of the service (see **Figure 2**), companies can easily implement simple and secure cloud application access for their users from anywhere and on any device. Users who have already been provisioned for the necessary cloud applications can benefit from SSO right away when they work in the company intranet due to the Kerberos/SPNEGO support offered by the SSO service.

When users want to access a cloud application from outside the corporate network, perhaps to work from home or while on a business trip, they can simply authenticate themselves with the same username and password they use when logging on to their office PC (see **Figure 3** on the next page). The SSO service makes this possible by integrating with on-premise systems via a secure tunnel established by the SAP HANA cloud connector included with SAP HANA Cloud Platform. When users log on, the cloud IDP checks the user credentials against the Microsoft domain. If the credentials are correct, the cloud IDP issues the required SAML assertions and the users are granted SSO to the cloud application.

The SSO service also offers strong authentication for protecting sensitive applications and scenarios based on risk. For example, if the security policies of a company require stronger authentication for external access, administrators can easily configure a corresponding rule on the application level. Based on this rule, users would be prompted for two-factor authentication when they access the cloud application from outside the corporate network.

SAP Authenticator, a lightweight SSO mobile app, is also available for any web-based application configured to trust the cloud IDP of SAP HANA Cloud Platform Identity Authentication. With SAP Authenticator, users can access apps on their mobile device without having to log in with their credentials each time.

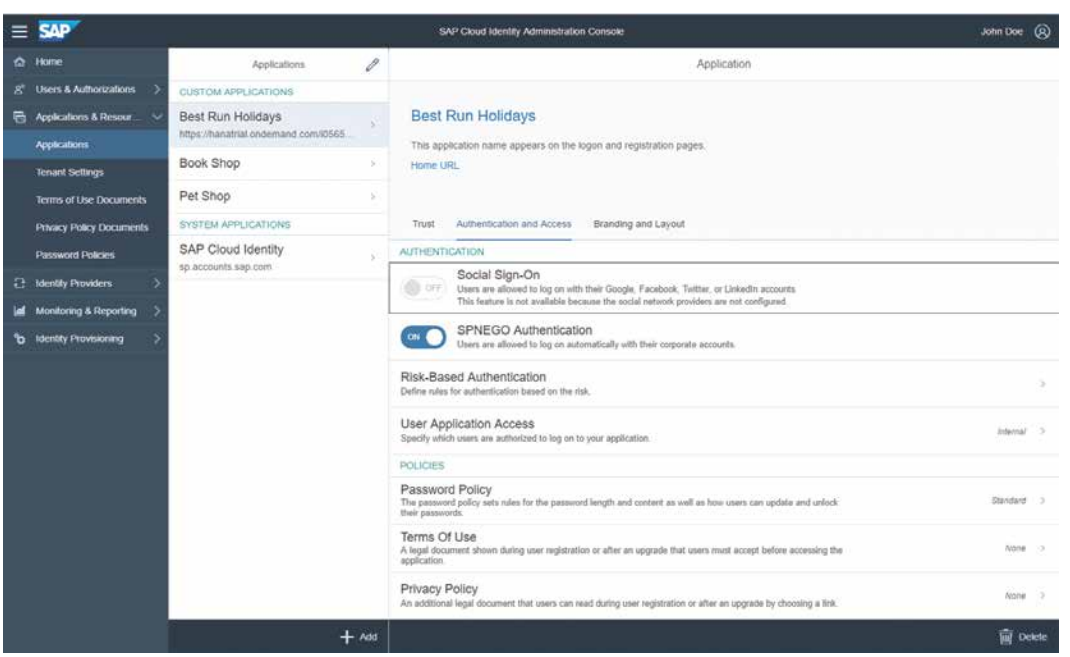

Figure 2 Using the administrative user interface of the SAP HANA Cloud Platform Identity Authentication service, you can configure secure application access for users from any device

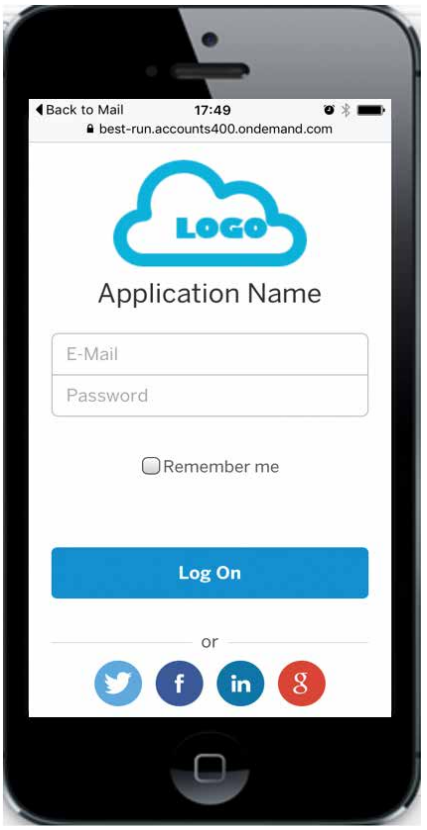

Figure 3 Users can use the same login credentials they use in the office to authenticate from outside the corporate network

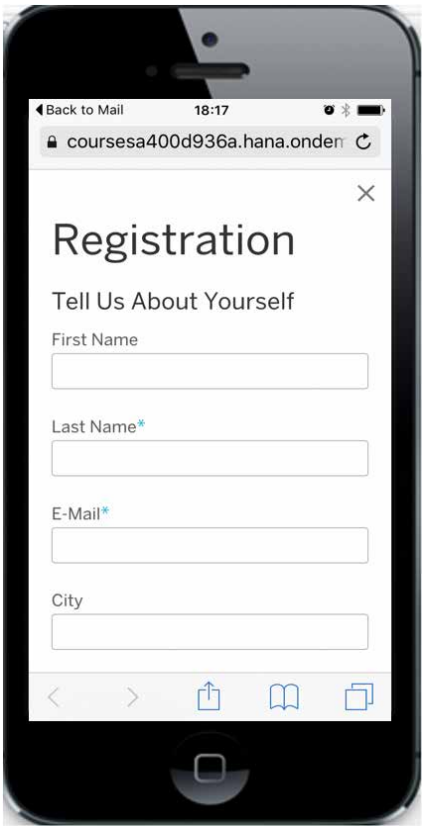

Figure 4 Self-services, such as self-registration, are available out of the box

Additional features of the SSO service include a secure user store in the cloud with self-services available out of the box, such as self-registration and password reset (see **Figure 4**). It also provides social login, branding, privacy policies, terms of use configuration, identity federation, and other features that are crucial for the security of consumer and partner scenarios. Using the SSO service, companies can securely cover all authentication scenarios for both internal and external users out of the box.

Run Secure in the Cloud

The two security services provided by SAP HANA Cloud Platform — SAP HANA Cloud Platform Identity Provisioning and SAP HANA Cloud Platform Identity Authentication — offer an easy way for companies to extend their technology deployments into the cloud. Companies can rely on these two services for the end-to end management of user identities and their access to cloud applications, including secure authentication and single sign-on. Using these services enables companies to leverage their existing corporate infrastructure while also benefiting from the agility, flexibility, and simple and seamless user experience provided by cloud-based applications.

Future plans for identity and access management with SAP HANA Cloud Platform include extending the functionality of these two services and ensuring the tight integration with SAP and non-SAP solutions that is required by cloud computing and heterogeneous IT landscapes. In this way, SAP HANA Cloud Platform Identity Provisioning and SAP HANA Cloud Platform Identity Authentication will continue to provide the reliable, secure, and efficient identity and access management you need to run your critical business applications securely in the cloud.

Learn more at **https://hcp.sap.com/capabilities/security.html**. ■