PhenixID

SCIM

PhenixID and System for Cross-domain Identity Management (SCIM)

Summary

With the vast number of applications and services used by organizations, in the cloud or internally, the burden of managing identities and access rights has increased dramatically. From a security and compliance standpoint it is vital that identities have the correct information and status in all connected application and services.

The IETF standard *System for Cross-domain Identity Management, SCIM*, was introduced with the intention to make it fast, inexpensive, and effortless to move users in to, out of, and around the cloud.

Identity administration increases exponential for each connected application/service. Furthermore organisations experience increased complexity as business owners often dictates what services and applications that needs to be added without considering operational turnover for the IT-department.
SCIM framework reduces the need for cumbersome custom development resulting in a cost of implementation decrease. Organisations that operate according to SCIM also benefit from a higher flexibility regarding onboarding and reassurance of avoiding orphan accounts.

PhenixID clients report of a considerable reduction in total cost of ownership (TCO) easily connecting new applications and services and a much more satisfying situational awareness on who has access to what.

Background

With the vast number of applications and services used by organizations, the burden of managing identities and access rights has increased dramatically. A use case such as change of surname may require manual updates in some systems, processing identity update batch files in some systems while some systems fetch the surname change automatically, typically using proprietary or legal APIs. The same update procedure is also applied for use cases with

more frequent updates, such as changing of permissions. This is time consuming, expensive, frustrating, insecure and complicated.

Also, identity data and permissions are spread across different systems. For example: The corporate user directory is the master of my work email address. The HR system is the master of my employee number. My permissions are mastered by the IGA system. How can you find a current, consolidated view of an identity and its permissions?

Solution

SCIM

The IETF standard *System for Cross-domain Identity Management, SCIM*, was introduced with the intention to make it fast, inexpensive, and effortless to move users in to, out of, and around the cloud.

Simply, to solve the issues described above.

SCIM contains a set of operations and schemes, all extensible, with an emphasis on rapid integration and deployment.

PhenixID

PhenixID utilize the SCIM standard to make identity management effortless, inexpensive and secure.

Using PhenixID as the SCIM Provider will allow connecting applications and systems to read, create, update and delete identity data and permissions in a fast, streamlined, effective manner. These changes can also be reflected in one or more internal systems.

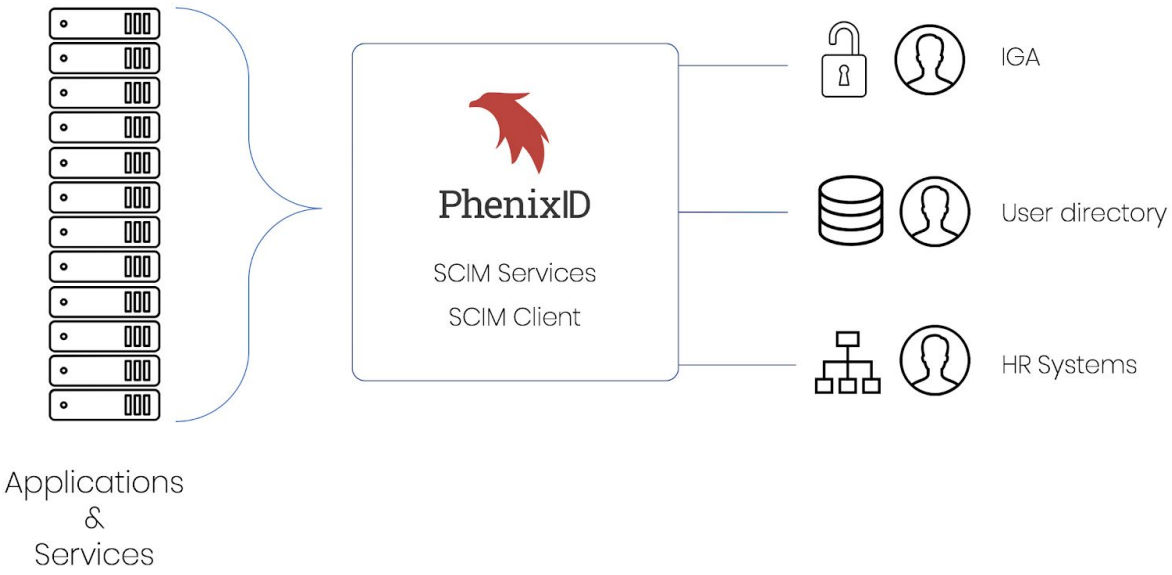

Image 1: Example of internal systems are HR system, Identity Governance and Administration (IGA), User Directory.

Technical resources

http://support.phenixid.se/psd/psd-phenixid-authentication-service/scim-overview/

https://support.phenixid.se/psd/psd-phenixid-identity-service/psd-user-provisioning/psd1102-scim-actions-for-identity-provisioning/

http://document.phenixid.net/m/75522/l/941608-draft-feature-use-phenixid-server-as-scim-bulk-endpoint

Please contact PhenixID to find more information about our SCIM solutions.