One of today’s big security marketing pushes is enterprise single sign-on (ESSO). Many companies struggle with the stresses associated with forgotten passwords, lost productivity characterized by end-user frustration and high service-desk costs associated with resetting the numerous passwords of users. The ESSO solution primarily touts lower operational costs for enterprises and stronger enterprise security, but how does ESSO reduce the risk, especially when it comes to public cloud-based services? This article outlines how CA Technologies implemented ESSO to drive value.

CA Technologies has several cloud environments for which security is required, and ESSO was implemented to federate identities in the cloud. In this example, CA-SiteMinder was utilized, but there are numerous products in this space. In a summary-level example, when a user joins the organization, CA Technologies no longer has to worry about managing the namespace at the cloud-based application after implementing ESSO; instead, the internal identity store (such as Active Directory) is leveraged to authenticate the individuals. Nothing granular is done with SiteMinder to manage the access roles inside the cloud-based application. Instead, the enterprise is quickly able to provision/deprovision users to that application, at least from an authentication perspective, by leveraging its own identity store to provide timely security access.

ESSO TECHNOLOGY
In an ESSO implementation, the ESSO takes an authentication token processed on CA Technologies’ internal system and sends it to the cloud. The cloud-based application will take the token and authenticate it through a “handshake,” using Security Assertion Markup Language (SAML) as the protocol. A few years ago, security protocols were not standardized, but SAML has become more of an industry standard recently. Therefore, most of the ESSO products on the market are based on the SAML protocol.

ESSO helps drive consistent levels of access and security across all applications. However, all of the following tools are needed to make secure access across environments work properly: identity management, provisioning and role management. ESSO is not about one technology; it is about how technologies work together.

H O W I T W O R K S
Using ESSO federation with a cloud-based, publicly hosted Software as a Service (SaaS), the user gains access to the cloud-based application with a single click. If the user is not already logged onto the corporate network, the user is redirected to a login screen; however, if the user is on the corporate network, then the corporate credentials are sent to the ESSO federation site using SAML for automated login. The user information is constructed in an eXtensible Markup Language (XML) format, is secured and is sent to the service provider. The service provider checks the document to validate that the user exists and has permission to access the requested application (figure 1). No password is exchanged in the process since the user is already validated by the ESSO prior to getting access to the cloud-based application.

ESSO is not to be confused with identity management. ESSO is about authenticating, not about provisioning/deprovisioning. Only if the person is listed as active in the identity store will that person be authenticated. If a person is terminated, the transaction will not process. The enterprise is not provisioning/deprovisioning access to the application; ESSO will simply not allow access if the individual is not active in the corporate identity store. The business sees value in this because the security is strong and there is less management on the part of the business. By leveraging ESSO, it does not matter where
the application resides. It can be on-premise or off-premise, SaaS, Platform as a Service, or Infrastructure as a Service. The technology is the same regardless of the platform, and the end user has the same experience whether in the corporate office or coming in from the web/outside. The user goes to the application wherever it may reside. The authentication takes place using the user's domain credentials, which are passed to ESSO. ESSO validates the credentials and, in turn, passes a secure token to the application, which then grants access to the user. It is a seamless, simple method of gaining access to the application. In this example, the security model is location-agnostic; the application does not have to be on-premise or off-premise or cloud-based, legacy or hybrid.

**IDENTIFICATION FEDERATION IN THE CLOUD**

Cloud is part of the delivery of services to IT customers. Federation is the concept of having an application running internally within the enterprise and somewhere else in the cloud, but an enterprise may want them working together as if they are one application when presented to the end user. For example, suppose a portion of an enterprise resource planning (ERP) system is with a service provider (the majority being internally hosted). In this example, after entering the ERP system and clicking on “SRM” (for “Supplier Resource Management”), the user leaves the enterprise’s system and goes to the service provider’s. With federation, the user would not be redirected to the SaaS, but the screens would appear seamlessly from an identity perspective. ESSO needs federation to work between an external cloud and internal systems. Federation is a way to have the systems collaborate without having to integrate. The goal is to manage security and access to all core systems whether they are cloud, ERP, legacy applications or a combination.

**REDUCING THE NEED FOR ADDITIONAL SIGN-ONS**

ESSO provides convenience for end users so that they do not need to authenticate multiple times. It also provides security in the workplace by reducing the need for multiple sign-ons. Many ESSO users utilize multiple applications. When users have multiple applications to access, they tend to write down their passwords, stick them under their keyboards or post them on their monitors. ESSO helps eliminate those activities
by reducing the number of passwords that people need to remember, thus reducing the risk of compromising passwords. Without passwords, the risk of e-mail scams requesting usernames and passwords is substantially reduced.

An identity manager is the provisioning piece of the puzzle. Depending on the trigger, the identity manager (in this example, CA-Identity Manager was used) will provision the account to the application where ESSO picks up and authenticates access. There are several ways an identity manager can be triggered. Two examples include a human resources (HR) feed from an ERP system or from a role management tool (CA Technologies uses CA-RCM). The role management tool handles end-user requests for new roles. It seeks business-access-reviewer approval and, once approved, triggers the identity manager.

THE RISK
The biggest risk for ESSO is that the enterprise is putting all its eggs in one basket. If the solution is not architected with proper resiliency, an outage of the ESSO will have a profound effect: Access to all applications will be denied. Careful consideration needs to be given to the design of the solution. Significant redundancy, load balancing and monitoring must be in place to mitigate risk. This is a tough lesson to learn—better to learn it from this article than from real-life experience.

By introducing ESSO, an enterprise reduces the security risk around human error—provisioning improper access. With ESSO, one provision/deprovision can handle all applications for an individual as opposed to separately provisioning access to the multitude of applications to which a user typically needs access. When not properly planned, certain bulk upload functions such as deprovisions of groups can cause significant exposure if controls are not in place to ensure that the bulk change is completely accurate.

THE OUTCOMES AND VALUE OF APPLYING ESSO
From an end-user perspective, the biggest win from implementing ESSO is that the users do not have to manage more passwords. Although thrilled, they do not necessarily see the security value, but the enterprise does. Worrying about thousands of salespeople writing down passwords to key financial applications is no longer necessary. The big value is in IT: With a large workforce, even a small amount of turnover can represent a lot of manual effort to provision and deprovision access across multiple systems and environments. Now, through this integrated security solution, the enterprise is able to provision and deprovision access in a timelier manner, with greater accuracy and less effort. For example, when the HR department receives notice that someone is being terminated, the master employee/contractor file is updated by HR. The identity manager gets the feed periodically throughout the day, and when it sees a difference in the file, it updates the identity store. ESSO then uses the identity store for authentication, and if the person is no longer in the identity store, the user does not get authenticated. Because of the proliferation of cloud-based applications, business units are finding it easier to add cloud applications. With the low cost of cloud services, old procurement controls do not necessarily catch departments that procure these services. Once procured, departments wonder how they can manage access to the application for their people. ESSO makes it easier for IT to be responsive to the needs of these departments, despite the fact that, in these situations, IT was not included in the plan-and-analyze phase of the cloud project.