Cloud-Based Authentication

KEY BENEFITS

- Centrally managed
- Easy to integrate
- Highly scalable solution
- Secure via SMS, Mobile APP, browser based image or telephony
- Align authentication protocols with risk policies
- Authentication happens on local network
- Employee identities are not revealed or stored in cloud
- Multiple cloud vendors supported from single solution
- Proven solution, with deployments in excess of 100,000 cloud users

The rise of Cloud computing has brought significant benefits to SMB's and Enterprises but with it comes risks. With employees able to access files, CRM systems and office applications anywhere, through any device with an internet connection, the need to consider security around cloud applications is evermore paramount.

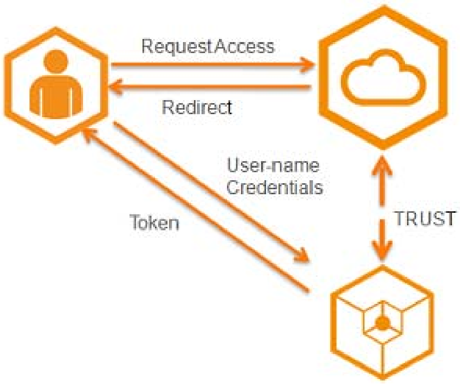
At Swivel we know how important this is. Swivel has developed a range of cloud options ensuring peace of mind when it comes to secure access to cloud services.

How does it work?

In the case of Cloud-based authentication, Swivel supports SAML and ADFS authentication protocols enabling organisations to seamlessly add a two-factor or strong authentication layer to the cloud application user access procedure.

This approach enables users to access their corporate network resources as well as their Cloud applications using the same, highly secure authentication protocol.

The Swivel solution for cloud adopts the "federation model" whereby when a user requests access to a cloud application they are re-directed, via your organisation's Swivel server, to the Swivel Authentication Portal (SAP).



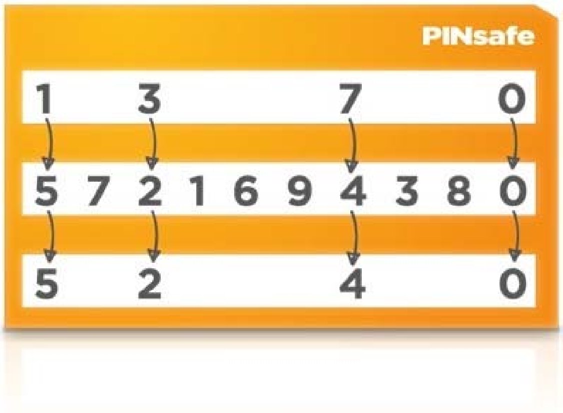
The SAP can be customised to perform whatever form of Swivel authentication is appropriate for access to the cloud services you use. The Swivel core, and the SAP, allows cloud access to be configured to authenticate via two-factor authentication via mobile app, SMS and interactive voice response channels or via strong authentication using our image-based interface options.

Once the user has authenticated using the SAP they are issued with an assertion token (a bit like a cookie) that the cloud service can then use as confirmation that the user is who they claim to be and then allow them access.

SWIVEL
the power of knowing

PINsafe

A key and unique feature, of our authentication platform is our patented one-time code extraction protocol PINsafe. PINsafe combines the use of registered PINs with random 10-digit security strings; you then combine these in your head to work out your unique one-time access codes, putting you at the heart of the strong authentication process.



> "Microsoft Office 365 is live with customers for 2FA integration and only officially supports two vendors, RSA and Swivel Secure"

Steve Patrick

Technical Data

Office 365: The Office 365 domain must be configured to use Active Directory Federation Services (ADFS). The Solution requires the Swivel Filter to be installed on the local ADFS infrastructure to ensure Swivel authentication is completed before the ADFS token is issued.

The filter includes a customisable login page that can be modified to provide the required authentication experience.

Swivel IDP: An additional piece of software, (that can be deployed on the Swivel Appliance) which interprets SAML requests, makes authentication requests to the Swivel server and issues SAML responses accordingly.

The IDP is required for SAML based integrations such as Salesforce.com and Google. It is compatible with SAML 2.0

The Swivel SAP is a customisable login page and is part of the IDP solution. It can be modified to provide the required authentication experience.

More in-depth and detailed integration information on all the cloud applications Swivel can work with can be found on the Swivel Knowledge Base kb.swivelsecure.com