Data Sheet

McAfee
An Intel Company

McAfee Cloud Single Sign On, SaaS Edition

Identity management in the cloud, for the cloud

Single sign-on (SSO), automated account provisioning/deprovisioning, and strong authentication for your cloud-based Software-as-a-Service (SaaS) applications. McAfee® Cloud Single Sign On helps you regain control of your cloud-based applications by extending your enterprise security policies to cloud-based access—all while providing the convenience, flexibility, and cost savings of a SaaS-based solution.

Key Benefits

Security controls

- Standards-based SSO eliminates weak passwords.
- Built-in, context-aware, multifactor authentication.
- Automated synchronization with enterprise identity profiles.

Cost savings

- Automation reduces administrative time, effort, and expense.
- SSO reduces password-related help-desk calls.
- Cloud connectors and built-in multifactor authentication at no additional cost.

Greater control and visibility

- Monitor all access activity.
- Create alerts for unusual activity.
- Publish compliance and utilization reports.

Simplified compliance

- Enforce enterprise security standards.
- Centralize audit logs and reports.
- Orphan account reporting.

Cloud-based architecture

- Deploy in the cloud for maximum flexibility and cost savings.

Meeting the Challenges of Cloud Application Adoption

Cloud applications enable new business and IT models through hosted, flexible, scalable, and cost-effective applications. But moving to the cloud creates its own unique challenges and risks.

Key concerns focus around loss of control, lack of cloud access visibility, enforcement of corporate security policy, and regulatory compliance.

Corporate users tend to use weak passwords that increase the risk of data exposure. System administrators spend too much time creating cloud accounts for new users and sometimes forget to terminate accounts for ex-users. User activity without oversight or authorization leads to risk of sensitive data loss and compliance violations. Systems with sensitive or regulated data may be vulnerable without additional layers of protection, such as multifactor authentication. Additionally, the lack of standardized logging prevents administrators from monitoring and correlating cloud application user activity with internal audit repositories.

Federation limitations

So how do organizations control access and security for cloud services that are outside of their traditional security models? It is possible to deliver single sign-on with authentication standards such as Security Assertion Markup Language (SAML). However, legacy point solutions designed to broker or “federate” trust between the enterprise and a service provider have run into major barriers—they cannot be scaled fast enough across multiple providers. The cause? Federated SSO solutions still require manual provisioning of accounts, do not include an authorization model, and lack integration with existing/additional strong authentication technologies—a prerequisite for access to sensitive corporate data.

Control the Cloud Access Lifecycle

McAfee Cloud Single Sign On, SaaS Edition removes these barriers by automating account provisioning and deprovisioning, enforcing strong authentication models, and integrating with existing enterprise identity management systems.

McAfee Cloud Single Sign On can be deployed to secure enterprise user access to SaaS providers and to protect access for custom enterprise applications deployed in the cloud.

Out-of-the-box SSO connectors

SSO connectors to hundreds of popular SaaS and service-provider platforms are included at no extra cost. Federated authentication and authorization protocols leverage standards like SAML. Support for HTTP POST-based authentication extends the system to be able to interface with SaaS applications that don’t support SAML SSO.

Automated provisioning

The McAfee Cloud Single Sign On administrative console makes it easy to view, configure, monitor and control access policy. Plug-and-play identity connectors to popular enterprise-identity repositories, such as Microsoft Active Directory, enable automatic, synchronized provisioning and deprovisioning, reducing the need for manual account creation. Provisioning/deprovisioning operations are seamlessly pushed from the enterprise to supported cloud applications. Business rules, based on user attributes, can be configured to synchronize accounts across cloud providers, as updates are made.

For more information, visit www.mcafee.com/SSO.

Flexible, secure authentication choices

McAfee Cloud Single Sign On provides adaptable end-user authentication options. Users can be authenticated directly when they log on to the SSO console. Customers can also deploy an Identity Bridge, an agent which opens a connection to your on-premises Active Directory. This enables users to be automatically authenticated using their Windows credentials, without having to log on to an enterprise network via a VPN, or open an enterprise firewall port.

Since moving sensitive applications and data to the cloud often creates the need for strong authentication, McAfee Cloud Single Sign On includes McAfee One Time Password. McAfee One Time Password provides two-factor authentication for any SaaS application by sending a one-time password (OTP) to any mobile smart phone or PC client. This delivers enterprise-class security for cloud apps without the expense and management headaches of hardware tokens.

Bringing It All Together: Trusted Client to Cloud

Ubiquitous user access

What does McAfee Cloud Single Sign On mean for the end user? It means convenient SSO with secure access to their cloud applications from wherever they are. No more password sticky notes on the keyboards and no more account password reset requests to IT.

Administrative control, compliance, visibility

For administrators, McAfee Cloud Single Sign On provides the missing element of control. Complex role-based network-based authorization policies are authored and enforced per cloud application from a single administrative console. Compliance is verified with account deprovisioning reports and aggregated audit logging correlated with log management platforms. Visibility is gained by monitoring user activity and generating alerts for unusual activities across cloud applications and provider platforms.

Flexible Deployment Options

McAfee Cloud Single Sign On is available as an annual subscription which includes both the SaaS Edition and On-Premise Edition. These editions can be deployed separately, or together in a hybrid configuration. The SaaS Edition is also available separately as a monthly subscription.

The SaaS Edition includes SSO, OTP using the Pledge client, along with provisioning/ deprovisioning and end-user authentication using your existing Active Directory.

System Requirements

	Management Console	Application Portal
Desktop browser	Firefox 9, Internet Explorer 8	Chrome 16, Firefox 9, Internet Explorer 7, Safari 5.1.2
Mobile browser	Not supported	Android 2.0, iOS devices & Safari browser

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com