



**[breadcrumb]**

Home > Products & Services > Selling Products

**[Page title]**

Cloud Identity Manager

**[short description]**

McAfee Cloud Identity Manager enables control of the entire lifecycle of cloud access security, and provides single sign-on, automated provisioning, strong authentication, authorization, and consolidated audit.

**[search title]**

McAfee Cloud Identity Manager | McAfee Partner Portal

**[keywords]**

Cloud Identity Manager  
cloud  
cloud application  
cloud computing  
cloud security  
cloud user  
enterprise security  
cloud applications  
password  
password protection  
password reset  
password security  
SaaS  
SaaS apps  
SaaS authorization  
data leakage  
compliance risk

**Is this content suitable for both reseller and distributor partners?**

Yes

**Is this content suitable for a global audience? If content is global, it will be translated into the following languages: Brazilian Portuguese, Spanish (both MX and ES), French, Italian, Dutch, German, Russian, Korean, Simplified Chinese, Traditional Chinese.**

Yes

**[H1]**

McAfee Cloud Identity Manager

**[body copy]**

**>Overview**

Adoption of cloud computing has been hampered by the overwhelming complexity of cloud security and shortage of comprehensive solutions that can effectively extend enterprise security

to the cloud. As a result, users have created redundant accounts for cloud applications with weak passwords that are disconnected from the corporate identity infrastructure, and user actions in SaaS apps have no oversight or authorization, leading to leakage of sensitive data and enhanced compliance risks. In addition, lack of standardized logs block administrators from monitoring or correlating cloud user activity with internal audit repositories.

How can control be regained in an environment where security models vary by cloud application and provider? McAfee Cloud Identity Manager enables you to control the entire lifecycle of cloud access security, and provides single sign-on (SSO), automated provisioning, strong authentication, authorization, and consolidated audit.

McAfee Cloud Identity Manager relieves the pain that end users have managing multiple passwords for cloud applications. It also provides enterprises with the ability to enforce corporate standards for cloud application access and improves productivity for IT and end users by relieving password reset requests.

### **What's Included**

McAfee Cloud Identity Manager provides everything the customer needs to implement SSO and strong authentication for SaaS applications:

- SSO module
- One-time password (OTP) server module
- SaaS connectors to common SaaS providers
- Internal connectors to Active Directory/internal directory

### **>Customer Problems Solved**

**Remove Multiple Logins/Add Strong Passwords for SaaS Access**

Adds SSO for SaaS applications using enterprise credentials; removes requirement to log into each SaaS application; enforces corporate standards for password strength; provides two-factor authentication via OTP by policy (e.g., the OTP requirement can be added for users outside the corporate firewall)

**Add Visibility into SaaS Usage**

Centralized management console provides log information on all SaaS user activities; easy access to aggregated log details

### **Simplify SaaS Account Provisioning and Management**

Automated provisioning using the organizations' existing directory (e.g., Active Directory); user attributes determine account types; if user attributes change (e.g., a user moves from Marketing to Sales), the account type is automatically synchronized; accounts are automatically de-provisioned when users leave the company

### **Integrate with Existing AD and IAM Systems**

Out-of-the-box integration with both internal directories and the most popular SaaS applications, such as Salesforce.com and Google Apps; out-of-the-box connectivity simplifies and accelerates deployment

### **Remove Audit Silos**

Provides centralized audit information for all SaaS application access — no more pulling and correlating logs from each SaaS provider

### **Add Scalability and Federated Trust**

CLIENT: McAfee  
PROJECT: Int'l. Partner Portal > Products & Services  
COPYWRITER: Mark Marinovich



The content in this document is presented as drafted in its original form.

Supports multiple protocols and any number of cloud providers; enables organizations to easily establish federated trust to with any standards-enabled SaaS provider

## >Qualifying Questions

Focus On

- Two-factor authentication for access to SaaS
- Federated provisioning and SSO

## Questions to ask

- What SaaS applications are you using Salesforce.com? Google Apps? Custom built? (If the customer is not using SaaS, it is not a good prospect)
- How do users sign into these apps? Are policies always enforced?
- How much time do you spend provisioning user accounts?
- What are the benefits of centralized reporting of all of your users' SaaS access?