

# McAfee Cloud Identity Manager

Simplify and secure cloud application access

Add strong authentication, automated account provisioning, and single sign-on for your software-as-a-service (SaaS) applications. McAfee® Cloud Identity Manager helps you gain control of your cloud-based applications by enabling enforcement of your corporate requirements access and strong authentication—all while providing the convenience and simplicity of single sign-on, automated provisioning, and consolidated audit logs.

## Key Advantages

### More control

- Single sign-on for cloud applications enforcing corporate standards for security
- Enforce context-aware authentication requirements
- Automated, accurate account provisioning/deprovisioning
- Auto-synchronization of identity data for change management

### Increased visibility

- Monitor all access activity
- Provisioning change and service level agreement (SLA) alerting

### Simplified compliance

- Enforce standards for security
- Centralize audit logs and access reports
- Orphan account reporting
- Exportable audit report data

## Breaking the Barriers to Cloud Application Adoption

Cloud applications are enabling new business and IT models through hosted and flexible, scalable applications. Yet, mass migration to cloud-delivered applications has been slowed due to concerns about security. Key barriers to entry are focused around loss of control, lack of cloud access visibility, and enforcement of corporate governance and regulatory compliance.

Central to these concerns is that corporate users manage their own accounts for cloud applications, typically using weak passwords that are disconnected from the corporate identity infrastructure. User actions in these disconnected applications go without oversight or authorization, leading to risk of sensitive data loss and compliance violations. Additionally, the lack of standardized logging prevents administrators from monitoring and correlating cloud application user activity with internal audit repositories.

### The federation barrier

So how do the organizations gain control access and security for cloud environments that are outside of their traditional security models? Why not just extend internal access management systems to the cloud application? This is possible with authentication and authorization standards such as security assertion markup language (SAML). However, point solutions designed to broker or “federate” trust between the enterprise and a service provider ran into a major barrier—they could not be scaled fast enough across multiple

providers. The cause? Federation solutions had a narrow scope that still required manual provisioning of accounts, did not include an authorization model, and lacked integration with existing/additional strong authentication technologies, a prerequisite for access to sensitive corporate data. McAfee Cloud Identity Manager removes these barriers by automating account provisioning, enforcing strong authorization models, and integrating with existing enterprise identity management systems.

### Control the Lifecycle of Access to the Cloud

McAfee Cloud Identity Manager 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 connectors

The McAfee Cloud Identity Manager administrative console makes it easy to view, author, and control access policy by cloud providers. Packaged with the solution are several plug-and-play connectors to common identity management and enterprise platforms such as Microsoft SharePoint. Also included are session creation and account provisioning connectors to popular SaaS and service provider platforms. Federated authentication and authorization protocols are based on standards like SAML, eXtensible access control markup language (XACML), and emerging open authorization (OAuth) and OpenID identity standards that can connect Internet-based identity providers (for example, Facebook) with corporate identities and authorization policy.

### Automated provisioning

A rich set of account provisioning and deprovisioning functions are delivered by the embedded provisioning engine. No more manual account creation is needed. Provisioning of accounts is seamlessly pushed from the enterprise to all cloud applications authorized for corporate use. Key attributes can be fetched from multiple authoritative attribute sources (service provisioning markup language [SPML]-capable provisioning systems and directories databases) and kept in perfect synchronization across cloud providers as updates are made.

### Mobile strong authentication

Cloud access is becoming increasingly mobile. This means that the access to your cloud applications must be accessible regardless of time and place. For access from mobile devices (not behind the corporate firewall), stiffer security standards need to be enforced. McAfee Cloud Identity Manager's one-time password server enables enforcement of second-factor authentication from mobile clients by policy. Second-factor authentication is easily enforced with a one-time password (OTP) requirement. The OTP can be delivered to cell phones via SMS (Flash or storable), email, chat programs, or generated using the included Pledge OTP mobile client application—no expensive hardware-based tokens are required.

### Enterprise client validation

For sensitive cloud applications, you may only want to allow access from approved enterprise laptops or PC clients that are confirmed to be free of malware. Federated single sign-on and even strong authentication technologies do not present enough assurance to allow access to mission-critical cloud applications. To solve this weakest link in the secure client to cloud connection, McAfee Cloud Identity Manager leverages Intel Identity Protection Technology (IPT) that is built into second-generation Intel Core i3, i5, or i7 Processors.

With a computer using Intel IPT, a cloud service provider or enterprise can validate that users are logging on from a known and trusted PC.

In addition to a username and password, the PC will generate a unique code at time of login to verify that users are requesting access from the PC where they registered their accounts. The technology works within the embedded Intel Chipset Management Engine isolated from the operating system.

### Bringing It All Together: Trusted Client to Cloud

#### Ubiquitous user access

So what does McAfee Cloud Identity Manager mean for the end user? It means a simplified and secure mechanism to access their cloud-based productivity tools. It means simplified single sign-on 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 Identity Manager provides the missing element of control. Control is achieved from a single administrative console where complex role-based access, time, network, and location-based authorization policies are authored and enforced per cloud application. Compliance is delivered with account deprovisioning reports and aggregated audit logging correlated with log management platforms. Visibility is gained by monitoring user activity and developer application programming interface (API) access across cloud applications and provider platforms.

#### Enterprise-class security and trust

Corporations can expand beyond internal applications and private clouds. McAfee Cloud Identity Manager simplifies integration of single sign-on and enterprise security for the cloud application access. McAfee Cloud Identity Manager enforces Pledge OTP strong authentication for applications that require additional security without costly hardware tokens. It includes all the tools your organization needs to extend your enterprise security to the cloud simply and effectively.

Category	Description
Salesforce.com Connector	<ul style="list-style-type: none"> <li>Federated single sign-on</li> <li>Salesforce.com data access using OAuth</li> <li>Multiple connectors supported by a single product instance</li> <li>Salesforce Connect for Microsoft Outlook</li> <li>Third-party vendor and custom applications deployed on Force.com platform</li> <li>Automated account (de)provisioning, user identity attribute synchronization, support for split users and split profiles</li> </ul>
Google Applications Connector	<ul style="list-style-type: none"> <li>Federated single sign-on</li> <li>Google data access using OAuth</li> <li>Multiple connectors supported by a single product instance</li> <li>Third-party vendor and custom applications deployed on Google AppEngine</li> <li>Automated account (de)provisioning, user identity attribute synchronization, support for split users and split profiles</li> </ul>
Custom Connector	<ul style="list-style-type: none"> <li>Federated sign-on into any third-party vendor or custom application that supports SAML, OpenId, or OAuth standard</li> </ul>
Application Integrations	<ul style="list-style-type: none"> <li>Microsoft Sharepoint 2007/2010, .NET 2.0 and above</li> </ul>
Manageability	<ul style="list-style-type: none"> <li>Centralized administrative console</li> <li>Command line and scripting support</li> <li>Test to production migration</li> </ul>
Certificate Management	<ul style="list-style-type: none"> <li>CRL- and OCSP-based certificate revocation check</li> </ul>
User and Data Stores	<ul style="list-style-type: none"> <li>Any LDAP v3-compliant directory</li> <li>Central authentication service (CAS) 3.3/3.4.2</li> <li>Data store (Optional) for monitoring and auditing.</li> <li>Any JDBC supported database</li> </ul>
Standards	<ul style="list-style-type: none"> <li>SAML 2, Open Id, OAuth, XACML, LDAP v3, JMX</li> </ul>
Supported Hardware	<ul style="list-style-type: none"> <li>On-premises or in the cloud</li> <li>Look aside or reverse proxy mode</li> <li>Software, virtual appliance, Amazon EC2, or DMZ-ready hardware appliance (cloud identity and access management [IAM] in a box)</li> <li>Horizontal migration for test to production support</li> </ul>
System Requirements	<ul style="list-style-type: none"> <li>Browser: Internet Explorer 6, 8, Firefox 3.6</li> <li>Server operating system: 32- or 64-bit</li> <li>Red Hat Enterprise Linux Server and Advanced Platform 5.0</li> <li>Microsoft Windows 2003, 2008</li> <li>Hardware requirements: Any Intel multicore server with 2 GB RAM</li> </ul>

For information or to start an evaluation of McAfee Cloud Identity Manager, contact your McAfee representative, or visit [www.mcafee.com/cloudsecurity](http://www.mcafee.com/cloudsecurity).

