Cloud Access Manager

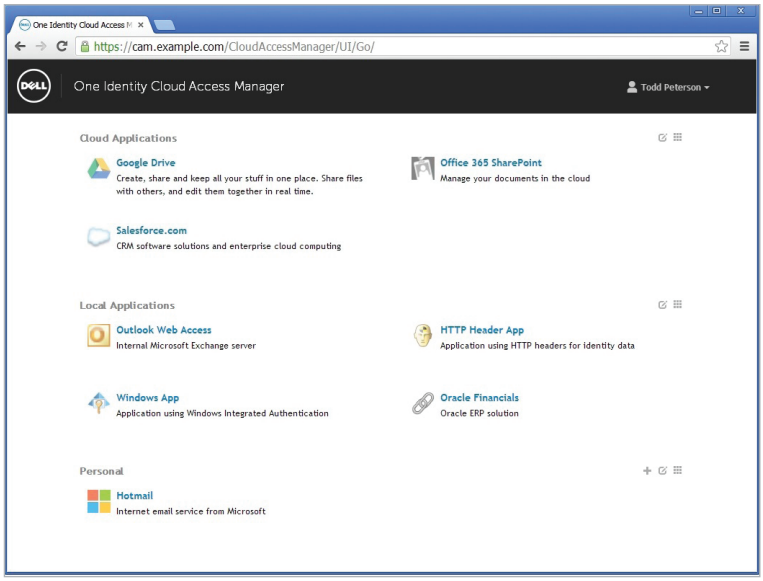
Unifying and securing access for your most pressing challenges

Years ago, when all of an organization's users and applications were on-site, access control was simple. Today, employees, partners and customers access applications from locations around the globe, using an ever-growing variety of devices. Relevant applications include not only those developed and/or hosted internally, but also cloud-based applications such as Salesforce.com®, Google® Apps™ service and Microsoft® Office 365®. Meanwhile, security requirements are growing as fast, if not faster, than user expectations for seamless access.

It's up to IT to efficiently grant users the access they need, when they need it — and to ensure that all access is appropriate, secure and compliant with security policies. What's needed is a way to bring all access — regardless of user type, location or application type — under the same security and management umbrella.

With Cloud Access Manager, part of the One Identity product family, you can meet your users' needs for browser-based access to internal resources, custom-built mobile applications and cloud-based web applications while simultaneously enhancing security and IT efficiency. Cloud Access Manager delivers single sign-on (SSO), context-aware (or adaptive) security, just-in-time cloud provisioning, federation, authorization and auditing, for a wide array of application types and access scenarios.

Features



Cloud Access Manager provides a unified login experience for any internally-developed, browser-based apps, web applications, OpenID Connect mobile apps and SaaS applications.

Meet your users' needs for single sign-on access to internal and cloud-based web applications — while simultaneously enhancing security and IT efficiency.

Benefits:

- Gives users the browser-based access they need to internal and cloud-based web applications, while enabling IT to maintain a high level of control
- Delivers SSO to diverse applications to improve user satisfaction and productivity
- Enables consistent, rule-based adaptive and context-aware security across a wide range of applications and access scenarios, including on-premises, remote, own-hosted and software as a service (SaaS)
- Provides an extra level of login assurance through multifactor authentication available both on-premises and SaaS
- Saves money by controlling license usage with just-in-time provisioning to Salesforce, Google Apps and Office 365
- Easily plugs into existing infrastructure
- Easy to administer through intuitive, wizard-based web interface
- Supports social identity login through the OAuth 2.0 standard and mobile application authentication through OpenID Connect

Centralized authentication, SSO and attribute retrieval

Move away from dedicated, application-centric directories, and the administrative burden they represent, by connecting multiple user directories and applications into a centralized authentication hub. Now a single login event (and password) can create a session spanning multiple web applications, hosted locally or by SaaS vendors, as well as your own custom-built mobile applications through the OpenID Connect protocol. Applications can be integrated through a variety of technologies including credential injection, HTTP headers, Security Assertion Markup Language (SAML) security tokens and OAuth-compliant social login via Google, Microsoft Live ID, Facebook and Twitter. Using a robust, rules-based engine, Cloud Access Manager can deliver additional data about users to protected applications, for fine-grained access control.

Context-aware security

Take into account who, what, when and where for security enforcement, the Security Analytics Engine (SAE), which is included with Cloud Access Manager, gathers information from a number of sources to provide context upon which access decisions can be made and enforced. Contextual information available through SAE includes:

- Browser used — Includes historical analysis of browser use that falls outside of normal user behavior
- Geo-location pattern — Detects if an access activity originates from an abnormal location
- Specific geo-location — Prevents access initiated from specific geographies known to foster malicious activity
- Group membership
- Failed authentication attempt/history
- Time — Detects access activities that occur outside of normal user patterns
- Blacklist — Lists forbidden networks or network addresses
- Whitelist — Lists approved networks or network addresses

Multifactor Authentication

Cloud Access Manager supports multifactor authentication as both a primary source of login and for step-up authentication as dictated by risk scores generated by the Security Analytics Engine. Options for multifactor authentication include both Defender on-premises and Defender as a Service, SaaS-based deployment.

Policy-based access controls

Eliminate inconsistent, ad-hoc security and ensure that users can access only the resources they are authorized to use, based on IT-defined user roles. Roles and role membership can be assigned dynamically based on policies evaluated in real time, using existing identity data. Rules-based access control can be applied down to sub-regions of a web application for enabling granular authorization.

Identity federation

Enable access scenarios that span security boundaries (such as cloud-based applications, multi-forest collaboration, heterogeneous platforms and partner extranets) without the need for redundant user passwords. Cloud Access Manager claims can also be associated to SharePoint resources. With federation support in both identity provider and service provider roles, it easily facilitates user access to web applications, regardless of where the users and/or the apps are located.

Cloud-access provisioning

For federated SSO to cloud applications such as Salesforce.com, Google Apps or Office 365 to work, user accounts have to be provisioned at the cloud application. Cloud Access Manager centralizes access provisioning and SSO functions into a single tool, for greater IT efficiency. Just-in-time provisioning saves money by activating licenses only when access is actually used.

Workspace aggregation and remote access

With the ability to customize your Cloud Access Manager portal, you can simplify how users find all the applications they need to get work done with Cloud Access Manager's Application Portal. Users find an easy-to-read, role-based collection of links to the applications to which they are entitled. Through the Cloud Access Manager proxy, users can access any application via a web browser.

Access auditing

Cloud Access Manager enables security professionals to leverage its role as a centralized authentication and access control solution for auditing and reporting on access events for compliance, repudiation and forensics purposes.

Login types supported by Cloud Access Manager include HTTP header, WS federation/trust, SAML, form fill, federated as an identity provider and federated as a service provider, as well as OpenID Connect and OAuth scenarios.

System requirements

For complete system requirements, please visit quest.com/products/cloud-access-manager.

About One Identity

The One Identity family of identity and access management (IAM) solutions, truly offers IAM for the real world including business-centric, modular and integrated, and future ready solutions for identity governance, access management and privileged management. www.oneidentity.com

One Identity
4 Polaris Way Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

Datasheet-CloudAccessManager-US-VG-27053