



Fact Sheet

Dell One Identity Cloud Access Manager Unifies and Controls Access to Both Cloud-Based and On-premise Applications

What is Dell One Identity Cloud Access Manager?

The newest addition to the Dell One Identity solution set helps users safely and effectively access browser-based applications both on-premises and in the cloud via single sign-on. By giving IT greater control and users more accessibility, businesses can save money, enhance security and increase employee productivity through unified access to browser-based applications, wherever they reside, from whatever device the user chooses. Dell One Identity Cloud Access Manager:

- Addresses the need to control and secure access to cloud apps, and internally-owned and developed browser-based apps from multiple end points – including office desktops, laptops, and mobile devices
- Provides an increased layer of security with access management for both on-premises browser-based applications and software as a services (SaaS) applications like Salesforce, Google Apps and Office 365
- Delivers browser-based access through unified and secure single sign-on, with just-in-time cloud provisioning, federation, authorization, and audit capabilities

Key Features Bring Unique Value to Both IT and the Business:

- **Single Sign-on:** Removes the burden of remembering and managing multiple, disparate login credentials for browser-based access to internal resources, as well as access to cloud-based applications. Instead, Cloud Access Manager presents the end user with flexible, advanced password management and a unified login experience, enhancing security and giving IT relief from managing multiple passwords
- **Access Control:** Eliminates the need to control access and implement security on a point-by-point basis for diverse applications, including cloud-based applications. Facilitates on-premises access to resources via the Web, remote and federated access to internal resources, and access to cloud applications regardless of the user's location (on-premises or remote)
- **Access Provisioning:** Makes administering access easier by fulfilling access requests through a wide range of provisioning options. Delivers rule-based auto provisioning to a large number of directories, applications and platforms, granting precisely what a user is allowed to access, at the level of access approved by policy without IT intervention. In addition, Cloud Access Manager provides just-in-time provisioning for Office365, Salesforce, and Google Apps to reduce licensing costs and accelerate user access to these valuable resources

- **Audit:** Provides audit trails and reporting of the access policy and activities, to make proving the compliance of access activities easier

Why It Matters

Rapidly growing mobility needs and the diversity of applications that users must access – including cloud-based applications and internally developed, owned, and hosted apps – has created a complex environment that requires a new level of IT security. Users now are located everywhere, requiring access to the applications they need to stay productive on a growing list of devices, and IT feels the strain from providing this access when it's needed, as well as addressing the increasing demand that access be appropriate, cost-effective, secure and compliant. For IT to become a business enabler rather than an inhibitor, they must be able to provide access, regardless of employee location or application type, in a unified, yet secure manner.

Dell One Identity Cloud Access Manager addresses this critical need by giving users their required access without diminishing (or duplicating) the security already in place, and giving the business greater control over access to applications including cloud-based applications like Salesforce.com, Google Apps and Office 365. Instead of having to remember and manage multiple, disparate logon credentials for browser-based access to internal resources, as well as access to cloud-based applications, Dell One Identity Cloud Access Manager now enables users to have a unified logon experience that addresses the real world needs of security, efficiency and cost containment faced by businesses today.

Dell One Identity Cloud Access Manager is part of Dell's [Connected Security](#) portfolio of comprehensive solutions that address all priority security needs – including governance, BYOD and mobility, cloud and compliance – and help mitigate risks from the device to the data center to the cloud. Dell's solutions give organizations the capabilities to build a seamless, Connected Security strategy, allowing them to choose the right entry point for the business and grow as needed. Software is the connection point, providing a predictive, context-aware intelligence that eliminates threats from both inside and outside the environment.

What is Dell One Identity?

Cloud Access Manager is the first IAM product to carry the Dell One Identity name. Over time, the balance of the Quest One Identity Solutions products, from ActiveRoles Server to Password Manager, will be rebranded to the Dell One Identity brand. This transition, which will cause minimal customer interruption, will take place during future releases of each product. Customers and partners will be alerted during this transition.

Quotes

John Milburn, executive director, identity and access management

“In response to the industry's demand, Dell Software is leveraging revolutionary technology to deliver a better way to ensure secure, yet convenient, access. Dell One Identity Cloud Access Manager delivers unified and secure single sign-on for both cloud and on-premises browser-based applications, regardless of the user's

location or device. This unique solution removes the complexity of managing multiple, disparate login credentials for browser-based access to internal resources, as well as access to cloud-based applications. Cloud Access Manager enables the organization to choose the best SSO option for each of its on-premises, remote access and SaaS needs, presenting the end user with a unified login experience and IT with relief from management of multiple passwords.”

Mike Johnson, president and CEO, Cerdant

“We view Dell’s focus on security and its drive to deliver a comprehensive portfolio around its Connected Security strategy as an exciting development for channel partners like us. We are seeing great revenue potential in helping customers leverage Dell’s industry-leading end-to-end security solutions to tackle their most critical security issues, and we look forward to continuing to build our arsenal of security solutions using Dell’s best-of-breed software products.”

Pricing & Availability

Call for pricing on Dell One Identity Cloud Access Manager. The solution is available through the channel.

Connected Security

Dell Connected Security gives organizations the power to solve their biggest security and compliance challenges today, while helping them better prepare for tomorrow. From the device to the data center to the cloud, Dell helps mitigate risks to enable the business. To learn more about Dell’s Connected Security vision, visit [Direct2Dell](#) and read the blogs by Patrick Sweeney, executive director, product management, and Tom Kendra, vice president and general manager, Dell Software.

About Dell One Identity Manager Suite

Providing employees with the right access to business-critical information should be under the control of the business, not IT. IT staff can’t afford to spend time and budget preparing for audits while unknown administrators being able to access sensitive corporate information and intellectual property expose the organization to significant risks. To address these critical needs, Dell has built a family of IAM solutions that reduce risk, reduce the cost of audit, and empower the business to govern the access that is needed to operate an agile and effective business. These identity and access management solutions uniquely benefit both IT users and business users.

#