DATASHEET

Identity Manager

Take the risk out of enterprise identity and access management

Benefits

- Achieve identity governance by providing employees with the correct access and nothing more
- Mitigate risk by securing the enterprise
- Unify access to accounts, external accounts, privileged accounts, data and applications
- Put access decisions where it belongs — in the hands of the business
- Build on existing investments and infrastructure and grow from there

System requirements

For a complete list of system requirements, visit https://support.quest.com/identity-manager/7.0

Traditional identity and access management (IAM) frameworks are expensive to build and time-consuming to implement and maintain. They are burdens on most IT departments as IT typically handles all user identity lifecycle management. To meet the varied IAM needs of different business units, IT often works with a siloed set of narrowly focused tools and security policies and relies on manual processes for enforcement. This leaves the environment vulnerable and increases risk, and makes it difficult to meet SLAs.

Organizations need to mitigate risk, secure data, meet uptime requirements, satisfy compliance obligations and increase productivity by giving users access to the data and applications they need to do their jobs—and nothing more.

Be the security risk mitigator an organization needs. Control user and privileged access. Govern identities. Secure data. Get more done with less. Now, identity and access management (IAM) can finally be driven by business needs, not IT capabilities. With Identity Manager you can unify security policies, meet compliance needs and achieve governance .And

ONE IDENTITY

By leveraging an automated architecture, Identity Manager simplifies **critical** identity and access management tasks to **a fraction** of the complexity, time or expense of "traditional" framework solutions.

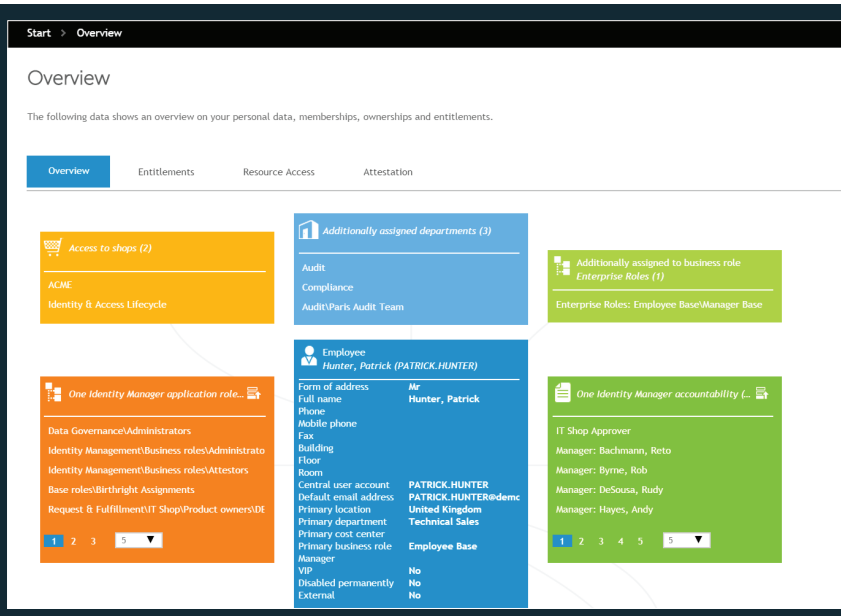

Figure 1. Entitlement visibility. View all the entitlements, personal data, group memberships and ownerships of user in one clear view.

you can do this while improving business agility today and in the future with a modular and scalable IAM solution.

Features

Governance 360
Provide auditors with detailed, real-time governance reports that includes information about what resources are in your environment, who has access to them and when, and why that access was granted and terminated. Experience a stress-free audit with our customizable reporting engine that gives you and the auditors what you need.

Connect for Cloud
Extends investment in identity governance beyond on-premises applications to cloud applications with an add-on cloud-based, managed-service offering that builds upon One Identity Manager (7.x or later).

Provisioning done right
Eliminate manual mistakes by automating provisioning to any system, platform or application.

Access done right
Enhance security by providing employees, contractors, partners, customers, students, alumni, constituents and patients with only the access they absolutely need - nothing more and nothing less.

Self-service access portal
Saves time and reduces IT effort via a customizable online intuitive "shopping cart". This enables users to request access to network resources, physical assets, groups and distribution lists, and control access rights and permissions for their entire identity lifecycle while leveraging predefined approval processes and workflows.

Scale up and out
There's no need to start over. Build on the investments and infrastructure you already have and grow from there. Move from your current platform by integrating a modular and integrated solution into your "traditional" IAM frameworks as you progress to a single, consistent IAM strategy.

Comply now
External regulations? No problem. Internal policies? No problem. Get the complete visibility you need while meeting the demands of all the other groups.

Attestation dashboard
Enables you to schedule on-demand or routine attestation and display the status of group or distribution list in a clear, concise dashboard view; and enables you to produce detailed reports for discovery, as well as to substantiate compliance.

Privileged governance
Achieve a unified governance approach for all employees, regardless of their role and level of access. By integrating Privileged Password Manager with Identity Manager, users can request, provision and attest to privileged and general user access within the same console.

About One Identity

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

Learn more at OneIdentity.com

Datasheet-IdentityMgr-DataGovEd-US-CW-24725

ONE IDENTITY