Quest One Identity Manager 5

Product Research Note

Author: Martin Kuppinger

1 Executive summary

In 2010, Quest Software acquired the German software vendor Völcker Informatik AG, based in Berlin. Völcker had established itself in recent years as a provider of technically innovative solutions and a vendor to be reckoned with in the field of Identity and Access Management (IAM). In the process, the company has become highly visible in the German-speaking market and has succeeded in creating a substantial customer base including many large and well-known corporations, particularly in the German-speaking market. However, Völcker has no longer been a niche player, but instead enjoyed a solid reputation as an established vendor in the IAM market space. The product which has been renamed Quest One Identity Manager – formerly known name as ActiveEntry – is a core piece of Quest's IAM offerings now, called Quest One. In contrast to Völcker, Quest has the marketing and sales reach to address customers worldwide. Thus Quest One Identity Manager counts to the leading products in the IAM market not only technology-wise but also from its market relevance.

The product's strengths lie, among other things, in a very sophisticated identity data model for the realization of automated processes and workflows, and in an outstanding approach for auditing and testing for contradictions among provisioning rules. Thus, Attestation, Re-certification, and SoD (segregation of duties) are very well supported. Another strength of Quest One Identity Manager lies in its integrated, self-consistent object model, which serves as the central repository for identity and access data across all enterprise where comprehensively and correctly identifies dependencies between different sets of data. This model is the foundation for the product's flexibility in supporting specific customer requirements.

Quest One Identity Manager's access request process for business users through an IT-Shop (shopping cart) self-service interfaces form a solid basis and can be adapted further without the need to write code. This is generally true for Quest One Identity Manager as a whole, which requires very little programming effort compared to other provisioning products. In addition, Quest has massively invested in the access request portal and added many wizards to simplify configuration and administration tasks.

Over the past years, Völcker had considerably expanded the number of its technology and implementation partners. In addition, it has increased its visibility outside of German-speaking areas, although the majority of customers continued to hail from Central Europe. Being now a part of Quest, there are many more partners on a worldwide basis. A multitude of unique technical features makes it definitely advisable to consider Quest One Identity Manager during the selection processes for an Enterprise Provisioning and Access Governance solution.

2 Highlights of the analysis

- ↗ Powerful provisioning functions
- ↗ Comprehensive adaptability without coding
- → Enhanced, good basis of standard connectors, including Quest QuickConnect integration
- ↗ Existing connectors with technically sophisticated, functionally comprehensive architecture
- ↗ Far-reaching SAP integration with GRC functionality for SAP environments.
- ↗ Worldwide market reach, increased visibility outside of German speaking areas
- ↗ Powerful workflow engine for provisioning and role lifecycle management
- ↗ Consistent orientation on standards
- ↗ Very powerful auditing functions with powerful analysis functions
- → Interesting dashboard functionality, but integration with other portals is still limited
- ↗ SoD (segregation of duties) support with specific functions for SAP environments.
- ↗ Integrated functions for attestation and recertification
- → Comprehensive password management functions only via Quest Password Manager
- ↗ Outstanding self-service and access request interface
- ↗ Clear development, test, and production segregation via a transport system.
- ↗ Integration with other automation functions, particularly through the in-house, integrated IT shop
- ↗ Integrated role-mining functionality
- ↗ Significantly improved partner infrastructure
- ↗ Rich Role Management
- ↗ Integration with Microsoft ILM/FIM
- ↗ Comprehensive experience in project implementation
- ↗ Consistent, thought-out object model
- → Customization in general simple, but some more complex requests might become difficult due to the consistent object model

3 Product category

Quest One Identity Manager is classified as an *enterprise provisioning* product with significant access governance functionality. These products support the structured, traceable administration of identities and access privileges in heterogeneous IT infrastructures via automated processes based on roles and rule types using connectors to the target systems.

Things like user self-service access request, delegated administration, and password management, which are now considered standard for most provisioning solutions, are also offered as part of the self-service function. Besides, configurable workflows for application processes and approvals are supported, as are auditing functions for change logging and analysis.

The product offers all basic functions to be found in most provisioning solutions from other vendors in the market, and no major feature is lacking.

In addition, Quest One Identity Manager offers a number of implementation details which are not to be found in other products in this market segment.

What is more, the solution can also hold its own in the related market for identity and access governance products segment, thanks to its comprehensive functions in the area of auditing, role management, attestation, re-certification and segregation of duties. In particular, it offers impressive integration with powerful provisioning as well as access governance functions. The decision of whether to introduce such solutions separately or to opt for an integrated solution depends first and foremost on the infrastructure and architecture of the available IT and cannot be answered across the board. The current version is limited when it comes to using access governance as integration layer across one or more legacy provisioning tools together with the provisioning features of Quest One Identity Manager itself. Quest plans to expand its access governance functionality which then will enhance the flexibility to serve different customer requirements.

4 Product description

Quest One Identity Manager was designed from the start as a service-oriented solution for the automation of IT requirements. The management of users and authorizations plays an important role here. Through its conception, however, Quest One Identity Manager exceeds the basic functions in this area. For instance, it offers an integrated “IT Shop” (shopping cart) for requesting access authorization to IT resources and other self-service tasks. It also offers good integration with other IT service management products and client life- cycle management solutions. A particular strength of the product is that it still can serve as the central request management interface for all types of user requests, well beyond access requests. This is provided through the flexible user interfaces and the integration capabilities of the product.

In its current release, the product comes with mature functions in the area of authorization control and analysis authorizations as well as role management. Essential functions from access governance solutions have also been integrated. Basic functions are controlled from a unit Quest calls its "identity dashboard" which is an interface that gives a bird’s-eye view of the status of identities and user privileges, as well as "identity intelligence", namely analysis functions which highlight rates of change, thus giving useful insights for Service Management in IT organisations. The “Identity Dashboard” also provides comprehensive SoD (segregation of duties) functionality as well as attestation and recertification.

The product's workflow functions are likewise extremely powerful. Workflows can be configured and adapted via a graphical editor. Both request and approval workflows are supported. For instance, standardized responsibility rules, with which persons participating in workflows are dynamically selected, are automatically stored via the consistent object model. That makes for flexibility, because individuals aren’t “hardwired” into the system, but instead can be given adaptable roles based on rules. Ad hoc workflows are a special function that can be simply defined and activated for querying an approver.

The Self Service interfaces are one of the biggest strengths of the current product release. The new version boasts its own Web designer which generates the executable Web environment. It relies on defaults to achieve a high degree of reusability. In typical use cases, a shop paradigm is employed which allows users to can easily request new functions or create other users, among other things. Based on this functionality, simple adjustments can be carried out via a configurator quickly and easily. More complex changes are also possible if need should arise. Advanced functions include an integrated debugger and a declarative language, ensuring simple usability are among these functions. It is important that the efficiency of integrators in customer projects is also increased significantly with this approach since in-house templates can be adapted and reused. According to Kuppinger Cole's assessment, the implementation of Quest One Identity Manager in the area of Web frontends is arguably the best technological solution in the market today. In the current release, the functionality of the Self-Service frontend has been further enhanced, including features like configuration wizards, web-based role management, attestation and re-certification and improved customization capabilities.

The auditing functions in the new release, which were mentioned before, represent a substantial expansion in functionality. The object-oriented approach followed here leads to very good comprehensibility. At the same time, Quest One Identity Manager has a comprehensive rule approach for realization of compliance requirements which allows very good comprehensibility and analysis of possible compliance problems. The simulation mode, as well as the analysis of SAP systems with their profiles and transactions as well as ACLs in the file systems further introduced in the 4.x releases increase the already considerable power of earlier versions.

Quest One Identity Manager can be run on Windows as well as on Linux systems. Völcker originally designed the platform and development environment with a high degree of flexibility for identical functionality. Seen technically, it relies on Microsoft .NET so that Safe Code is used 100% in this environment. Quest One Identity Manager differentiates itself from other products on the market through its self-contained object model and consistent architecture. The core functionality are, on the one hand, objects for users, groups, roles, and other infrastructure elements, and on the other, defined sequence descriptions used to automate sequences. A large number of these descriptions (over one thousand), also called "job chains", are included and only need to be selected during configuration. But most sequences are based on preconfigured components like job chains or on new ones that can be created without too much time and effort. The object model is the foundation for a very efficient and flexible customization in most cases. However, there might appear situations where it also can appear as an inhibitor to very complex customizations, which then require Quest to adopt the object model as part of its regular product releases. Nevertheless, the product has frequently demonstrated that its overall flexibility is far above average.

Data about configuration and objects are stored in a central database. Support is provided for Microsoft SQL Server as well as current Oracle databases, as well as cluster infrastructures. In our view this provides sufficient flexibility. Since many processing steps are carried out via stored procedures on database servers these systems must be able to scale up depending on infrastructure. However, the product's reference implementations show that this scalability could also provided for very large environments, even while there are still very few of these implementations.

The database is designed as a CMDB (Configuration Management Database) thereby following ITIL guidelines. This means that things like change processes supported. Most importantly, the configuration data in the database are protected by the same security model as for the user data. The configurable workflows allowing configuration changes to be approved before they are executed are also remarkable.

Analyses can also be partly executed through the administration clients. That is the case for instance during advance analysis of the compliance effects of rule changes. However, the processing of most actions also occurs here on the back end, sometimes in delayed time. Through extensive use of Microsoft .NET frameworks and other concepts, even the processing of very large administration data sets and lists can be carried out very efficiently.

The concept relies on an efficient segregation of processing between the database server and the administrative clients. It is thus flexible and scalable. In addition, the server infrastructures are comparatively lean. This avoids the often very high cost of installation and configuration of application server platforms, at least within Windows environments.

The integrated concept's advantage is also its consistent object model that is to be assessed in this consequence as a unique feature of Quest One Identity Manager among leading provisioning products and which forms the basis for many functions like history processing.

The product's object-oriented approach mentioned above, along with the sophisticated approach for a rule-based definition of authorizations and compliance requirements are doubtless among its most interesting functions. The strength of this approach lies in the exact traceability of all changes and the persons executing them, which answers the vital question of why someone was permitted to carry out changes. Meanwhile, rollbacks to any time in the history can be carried out via a functionality designated as “time trace”. In this connection, all dependencies among objects are correctly taken into consideration.

5 Provisioning

Provisioning is the product's core functionality, relying on the automation mechanisms already mentioned. For object class property changes it can be configured which processing steps will be activated. Control can take place via rules and is very flexibly adaptable via the graphical administration interface. It must also be considered that the configuration of core areas of the graphical interface can be made in this way.

Processing is basically event driven. In this connection, the fact that threshold values that can be set during group operations on several objects—like deleting multiple users—is particularly pleasing. Thus, the risk of administrative error, like deleting all of the users in an entire organizational unit, can be minimized. Since the change history of objects is always available, faulty operations can be comparatively easily traced and corrected.

Time-controlled execution of operations is basically also possible by configuring the appropriate automated processing steps. This means, for instance, that changes such as deleting user accounts at a given date can be triggered. The reconciliation process, through which changes in connected systems are detected, is likewise supported by processing rules and automated processing steps, which identify changes to objects and process them in a defined way.

The workflow designer already mentioned is among the best solutions on the market, because the connections between workflows and objects are very clear and also simultaneously more complex decisions and operations can be very simply configured in the workflows.

Support for role models, which are becoming more and more important, is embedded into the Quest One Identity Manager object model. Once one is familiar with it, it becomes easy to display virtually any kind of complex connection between roles with the help of this object orientation. At the same time, functions for change simulation and possible rule violations ensure that faulty information is not passed on to other systems even within very complex environments.

As with other provisioning solutions, the system of roles used by Quest One Identity Manager is part of the product itself. Unlike most other comparable solutions, however, role-mining functions are also integrated into the product. Thus, for instance, roles can be optimized on the basis of cluster analyses or direct assignments through more efficient, role-based approaches. Business-oriented role management can also be implemented through the assignment of authorizations to organizational and project nodes.

Departmental approval processes may require some adaptation of the standard user interfaces. This, however, can be accomplished easily with the help of the Quest One Identity Manager concept.

Delegation of administration can be controlled well via the flexible Web interfaces and the roles and rules for the objects. In comparison with other products, the fact that the Web interfaces can be adapted without special programming skills is a notable feature. However, the standard interfaces that come with the current release are already very impressive. The drag-and-drop mechanisms employed and the graphical structures, which highlight the connections between of objects and allow for quick navigation, are unique in this form on the market.

With Quest One Identity Manager, Quest demonstrates its technological leadership in the international provisioning market. While the approaches followed differ considerably from those of other vendors, they offer a high degree of consistency within the product and form the basis for the product's special performance and many of its unique features.

6 Password management

Password management in the sense of the ability to distribute keyword changes and to reset keywords is an important part of any enterprise provisioning product. In this area, Quest One Identity Manager offers basic functionality via the self-service access request interface or rich password management capabilities via the integration with Quest Password Manager. Keyword reset is available for all supported target systems. Integration with standard Windows authentication mechanisms is possible on a project basis.

Changes on Windows systems and in Active Directory can also be detected and automatically distributed to the target systems. These are, of course, standard functions in all enterprise provisioning products.

7 User interfaces

Administration and configuration are achieved through a set of very well designed graphical interfaces. As mentioned before, Windows as well as Web interfaces are available for most functions. Quest has added new features for the self-service access request interfaces including role management in the new releases. The interfaces are easily adaptable and have high, up-to-standard functionality. Here, Quest has made significant improvements compared with earlier versions of the product. Certain functions can now even be accessed via an iPhone or iPad app.

Design and production phases are well-separated. Changes can first be simulated to identify possible side effects before going ahead with actual implementation.

That can take a while if complex object relationships are to be handled, but the resulting comprehensive information delivered is well worth the effort. All configuration changes are meticulously logged. Change activation can be flexibly configured. In addition, a transport system for structured transfer between development, test, and production environments is supported.

8 Connectors

A look at the list of connectors delivered with Quest One Identity Manager may create the faulty impression that relatively few are being offered. However, the manufacturer correctly points out that it is not really necessary to include every LDAP single directory in the list. Whether this approach, while candid, is in fact advisable from a marketing perspective, is debatable.

Taking a closer look at the current list of connector shows that almost all of the important systems are supported. Among these, naturally, are connectors for Microsoft Active Directory, and via LDAP to a great number of other directory services such as Lotus Notes and SAP. Even RACF is supported via LDAP. Given that hooking up to Lotus Notes is always fraught with complexity, the connector from Quest offers some very deep integration which provides complete support for Notes ID management on this platform, up to release 8.5.

Based on the existing Quest QuickConnect technology, Quest One Identity Manager has further enhanced the number of available connectors. The product integrates with Quest QuickConnect and can use the connectors available there.

Adapters for SAP are another daunting challenge for provisioning products. Quest One Identity Manager offers deep integration with various SAP components, basically providing support for all release versions from 4.6 onwards, as well as all components dealing with identity data. Quest also offers a toolbox of in-house BAPIs in case deeper integration is required. Integration is achieved via the various interfaces offered by SAP, for instance SPML or LDAP, as well as via enterprise portal. The depth of integration is considerable, and the adapter is certified. Quest has added additional features like support for SAP analysis authorizations or collective profiles in the recent releases.

Standards are always a good idea, and Völcker Informatik AG was one of the first solution vendors to lend wholehearted support to SPML (Service Provisioning Markup Language). As a result, target systems can be connected without need for special connectors. The system can also act as a client within SPML environments receiving and processing change information from other systems.

The connectors are configured via XML, which is also used to customize the target system description. It is important to note that the connectors are adaptable in many cases through a declarative development environment. In this case, LDAP, XML, CSV, Web services, and SPML are all supported. This means that multiple system environments can be specifically integrated way without having to resort to complex coding. Of course, partial connector programming may be required in certain cases, but that goes for the solutions of other vendors, too.

The connectors provided by Quest offer significantly deeper integration than most other products, which can be an important decision factor. Within Quest One Identity Manager, information is standardized through the so-called "unified namespace", which allows for implementation of a number of specific functions. For instance, authorization information in Windows file systems as well as in the DFS (distributed file system) are processed this way, allowing detailed analysis of rights and privileges.

In sum, Quest's connector offering is much more comprehensive than might appear at first glance, since it covers most systems in use today. Other systems can be connected thanks to the flexible adaptation functions mentioned above. And even connectors for rather systems like SAP and Lotus Notes which are usually difficult to manage can be implemented at a high level.

Besides, the number of available standard connectors from Quest is growing continually. The company also offers integration additional target systems through strategic partnerships, for instance for mainframes. And since Microsoft FIM/ILM is also an option, all connectors supported by this platform are also available. Some of the newer additions around Microsoft technology include Exchange 2010 integration and SharePoint integration.

9 Auditing and access governance

As mentioned before, Quest One Identity Manager offers comprehensive support for those functionalities generally grouped today under the heading "access governance". The functions formally known as *identity auditor* in the 3.x versions were already among the best integrated auditing functions in any enterprise provisioning product. These functions have been significantly expanded for the new release.

They are based on the object model on the one hand, the rule base and processing functions for rules on the other. Rules are stored in the database; and changes to them are logged automatically. Rule violations, for instance potential problems with the SoD (Segregation of Duties), are detected via simulation functions.

The defined owners of data or persons designated by them can monitor change approvals and conduct regular automated reviews of privileges through the workflows for attestation and recertification. That can be necessary for compliance reasons in order to deactivate unneeded privileges and is achieved through a defined process. This is currently one of the most popular functions in most provisioning and access governance solutions. Quest One Identity Manager's integrated rule base makes setting up such workflows and rules testing very simple and reliable.

Log entries can even be digitally signed at the database level. In terms of flexibility in configuring rules during the conformance analysis process and the ability to analyze functions through the compliance dashboard set a new mark for other vendors of provisioning products that contain built-in auditing functions.

The current versions include many important extensions, first and foremost "identity dashboards" and "identity intelligence" functions already mentioned. The concept of providing selected indicators within the scope of the identity intelligence functionality is unique, at least in this form.

The product not only provides important business-relevant information like rates of change, for example the number of changes of IT services following organisational changes, but also allows quick identification of users within the organisational structure. In addition, methods can be stored for drilling down through data, for instance in order to flag employees who should not have been granted certain privileges. This is augmented by comprehensive analysis functions which can show why a given user was granted these privileges in the first place.

The identity dashboard is currently an integral part the Quest One Identity Manager infrastructure. However, plans are afoot in future to allow its integration into other portals, as well. Plans have also been announced for a simple reader which can display pertinent information from the dashboard, but without the drill-down and reporting functions. This can be especially valuable for non-IT users such as an auditor or top management.

The product also offers a convincingly fresh approach to the question of SoD rules. Here, comprehensive GRC functions are now available for SAP environments, which allow even complex interdependencies all the way down to the level of individual attributes values to be translated directly into rules.

10 Partner infrastructure

Over the past few years, Völcker Informatik AG had systematically expanded its partnership infrastructure which included a series of technology partners, as well as various integration partners, most of them based in German-speaking countries. Right now, Quest One Identity Manager doesn’t only rely on that partner infrastructure anymore but can build on the reach of Quest itself and the Quest partner ecosystem.

Some projects are still supported directly by Quest, partnership deals notwithstanding. However, the amount of resources devoted to project business has been increasingly shrinking as more and more emphasis has been placed on product development, and the amount of project business conducted by partners has therefore been rising steadily. Being a part of Quest, it is now really about product business.

By maintaining a certain amount of involvement in customer projects, however, the company is able to stay abreast of customer requirements, experience that flows immediately into continued product development. Due to the improved partner structure, more capable partners, and the fact that the product is now provided by a large vendor, this is no longer perceived by Kuppinger Cole as a possible impediment to the product development since the structure now in place is flexible enough to scale in the product development area.

10 The view of Kuppinger Cole

Kuppinger Cole rates Quest One Identity Manager as one of the most innovative and technologically appealing products in the field of enterprise provisioning and integrated access governance. Quest One Identity Manager is an impressive offering, and the vendor has access to comprehensive implementation experience besides.

Quest One Identity Manager clearly distinguishes itself from other solutions in the market for enterprise provisioning and access governance, thanks both to the paradigms used and especially to consistent application of object orientation. Comparing Quest One Identity Manager to other products calls for a certain familiarization with these concepts, which are however easily comprehensible through their visibility in the graphical interfaces. In our estimation, it is well worth the time to make exact comparisons, since Quest One Identity Manager's approach brings obvious advantages over conventional concepts for enterprise provisioning in many ways. Simply comparing feature lists isn’t enough, although Quest One Identity Manager in its latest release stands up very well against competitive products. We strongly recommend short listing this product for evaluation when considering an investment in enterprise provisioning.

Of course there are a few weaknesses to take into consideration, too. In terms of functionality, on the other hand, there remains little room for improvement. There are some slight risks around flexibility and scalability which might show up in some use cases, but overall we consider these risks lower than with most of the other products in the markets. Nevertheless, product evaluations always have to be done carefully – for every vendor. The other weakness we've indicated for Völcker Informatik AG has been their lack of an end-to-end offering around IAM. That has changed in the Quest context, with Quest providing one of the most complete portfolios in that market segment. Integration is moving forward quickly, with Quest One Identity Manager integrations to products like Quest Webthority, Quest Password Manager, Quest Defender, and Quest Quick Connect being available today.

In fact, Quest is currently in the process of widening its lead over the competition in terms of innovation and unique features.

In implementation, we see advantages stemming from the widespread use of graphical configuration within the solution. The depth of integration offered by the existing connectors is impressive, to say the least. Potential buyers should also realize that the effort necessary to get a full grasp of the product's concept may not be trivial, a factor that is more than offset in our opinion by the consistency of the solution and the potential benefits compared to most other provisioning solutions. Finally, although Quest relies increasingly on partners, a certain degree of proximity to the vendor especially during complex projects appears to remain and hopefully will do so in the future, which is in itself a good thing.

Summing up, Kuppinger Cole considers Quest One Identity Manager to be among the clear leaders in the market for enterprise provisioning and integrated access governance, and we strongly recommend taking it into consideration for any upcoming projects in this area.