

ORACLE DATABASE USER MANAGEMENT

New Simplified Single Sign-on and Directory Synchronization



Simon Pane
Principal Consultant
Oracle ACE

BACKGROUND

One of the feature requests Oracle Database customers have been asking for for the longest time is simplified user management and sign-on, especially customers who also run Microsoft SQL Server databases where integrated logins have been standard virtually since that product's inception. They see how simple it is with SQL Server and want the same with Oracle.

With Oracle Database 18c and above, Oracle included a new feature branded as "Centrally Managed Users" or "CMU" allowing direct synchronization and connectivity with Microsoft Active Directory (AD). The implication of this is profound yet the news has largely flown under the radar with modest promotion and little fanfare. But this is exactly what customers have been wanting all these years and Oracle Database customers around the world should rejoice.

One of the best parts is that this new feature of Oracle Database 18c/19c Enterprise Edition (EE) does not require any new or separate licensing or option packs.

WHAT DOES THIS MEAN TO END USERS—THE USER EXPERIENCE

Business users are often unaware of which back-end database tier technologies are used. All they know is that different applications log on in different ways:

Some log in automatically:

Users log into their Windows desktops and then automatically are authenticated for some applications. A very simple example might be a network shared drive. When “Mary” starts her day and logs into her Windows PC, she doesn’t have to enter a new set of credentials to access her “T:\” (team) network drive. For her, it “just works” but behind the scenes the technology has authenticated her based on her Windows credentials. Opening her email client (such as Microsoft Outlook) might be a similar experience.

Some use the same password:

Mary might use a timesheets application that does ask for a username and password (“credentials”) whenever she fires it up. But she knows that it’s the same username and password that she uses to log in to Windows. If she changes her Windows password, then she’ll need to use the updated Windows password the next time she logs into the timesheets application. The login isn’t transparent and automatic but at least it’s her regular Windows password that she has memorized. So while it does mean some extra typing, at least the process is fairly simple and reliable.

Some use application specific usernames and/or passwords:

Mary might also occasionally use a purchasing app. This application is far less convenient as she has a unique password for this application which is not synchronized with her Windows password. It could even use a different associated username. She might try to manually synchronize her password by changing it through the purchasing app whenever she changes her Windows password but this is not reliable. Each system may have different password complexity rules, expiration periods, grace periods, etc. So typically she has to memorize a separate application specific credential or track it in a secure password management tool. At best, this is inconvenient. At worst, she risks entering the wrong password and locking herself out, inadvertently exposing passwords, or managing and storing her credentials insecurely (i.e. using anything from a post-it note to an Excel spreadsheet).

Unfortunately, Oracle Database-based applications traditionally, for the most part, fall under the third category: separate credentials for users to know and manage. There are exceptions to this and technical solutions from both Oracle and third-party vendors, but those solutions are complex and likely expensive (in both software acquisition costs and resources to support it).

But with Oracle Database 18c CMU, moving to the first or second categories (which of those used might be application-specific) is simple and inexpensive. Meaning Mary's user experience is simpler and more convenient and, at the same time, reducing her risk of poor password management due to having to manage numerous different credentials.

WHAT THIS MEANS FOR ORACLE DBAS AND OTHER IT STAFF

The benefits to the Oracle DBAs and other IT staff are equally significant. Without user centralization, users are replicated in databases. User "Mary" has a login in Active Directory for her Windows and Microsoft products and then completely independent users in any number of Oracle databases. Hence, the number of separate and independent "Mary" users accounts across the estate can add up quickly.

Having so many redundant users makes on-boarding, off-boarding, password resets, and other typical user management activities burdensome for service desk users, and risk-prone and password resets need to be securely communicated, etc. For DBAs there's an extensive list of database users where they have to manage password profile assignments, validate usage, etc.

Then there's the audit overhead: hundreds, thousands, or more database users to check on, report on, etc.

The simpler solution is to offload all of this and centralize the list of users in one place—which is exactly what Oracle CMU provides.

AUTHORIZATION AND AUTHENTICATION

The technical implementation provides both authorization and authentication options via Active Directory "Security Groups".

What this means is that purpose-specific security groups can be added to Active Directory and users added. In fact, for access to network shares and other resources, those groupings likely already exist. But for the sake of example, an Active Directory security group called "Finance Team" could be created and Mary and her colleagues added. Then in the Oracle Database only the Active Directory "Finance Team" is added. Of course Mary could be added as a dedicated user as well, but for simplicity and cleanliness, there's no need—the AD security group can map to a "shared" database user. So maybe the DBAs create an Oracle Database user called FINANCE_USERS which maps to (or "authorizes against") the Active Directory "Finance Team" security group. The DBA can grant database privileges directly to that user or via a database role. The database role may also map to the same or a different Active Directory security group, hence providing "authorization" options via Active Directory group membership, as well. And that's it—from the Oracle DBA perspective, they are done.

Mary is part of the “Finance Team” in Active Directory and hence can connect to the FINANCE_USERS database user using her own AD (aka “Windows”) username and password. The Oracle DBAs can still see, and the audit trails still reflect, the fact that Mary connected to the database as FINANCE_USER, but authorization against AD specifically with the username “Mary”. Those details are not lost—they are still exposed to the Oracle database and can be used for auditing or other mechanisms such as database logon triggers.

The Oracle DBAs don’t have a list of users to manage, report on, ensure password profiles are correctly assigned, etc. They just have FINANCE_USERS. The rest is managed by Active Directory, including password complexity rules, expiration policies, lock-outs, etc. All of that is offloaded to the centralized Active Directory.

Onboarding “John” and offboarding “Mary” becomes simple: user accounts are created or conversely locked in Active Directory (undoubtedly an existing workflow) and added/removed from the “Financial Team” security group. Absolutely nothing needs to be done against the Oracle Database. Hence the benefit of this new feature! And exactly what customers have been wanting all these years!

TERMINOLOGY AND UNDERSTANDING THE OPTIONS

Before getting more detailed on this topic, it is important to understand the proper terminology and the associated definitions:

“Single Sign-on” (SSO):

SSO really means that the application does not prompt for credentials to log on. The authentication happens transparently.

“Directory Synchronization”:

Often confused with SSO, Directory Synchronization means that applications still require a credential to be provided, but that username and password are centralized or synchronized with in a single location.

Oracle CMU provides both SSO and Directory Synchronization with Microsoft Active Directory. This is a huge step forward, especially considering it’s relatively simple to implement, and requires no additional software or additional licenses!

The one restriction is that Oracle CMU works only with Microsoft Active Directory and not other directory services. However, most organizations do use Active Directory (in layman’s terms a “Windows login”) so this likely isn’t a limitation for most.

IMPLEMENTATION AND CONSIDERATION OF OPTIONS

When implementing, the first decision is essentially , “What do you want to achieve”? Single sign-on, directory synchronization, or both? For almost all, the answer is probably “both”. Which really isn’t a problem—just a few additional deployment steps but nothing complex or overwhelming.

The reason both are likely required is because it might depend on which is the most applicable due to both application/technology requirements and internal policies and requirements. There are pros and cons to both.

Single Sign-on

- **PRO:** Much simpler user experience—more convenient for users.
- **PRO:** Less password typing means less exposure to malicious tools or software (i.e. keyloggers).
- **PRO:** Applications are not handling and transmitting passwords.
- **CON:** An exposed/compromised desktop means access to applications.

Directory Synchronization

- **PRO:** Fewer passwords for users to manage/memorize means safer password management and handling.
- **PRO:** Applications essentially “re-authenticate,” meaning an exposed desktop doesn’t mean access to applications.
- **CON:** Still typing in credentials when launching applications.
- **CON:** Applications are still accepting passwords and transmitting those (hopefully securely) to the back-end database.

Organizations may have internal security policies or controls that require applications to re-authenticate. Or there may be technical requirements: applications may not accept null (blank) usernames or passwords and might validate that values of a minimum length are provided before they even try to authenticate against the back-end database.

Fortunately, implementing both options concurrently is not a problem at all with Oracle CMU. Regardless of which option is used, both are likely a huge security improvement over the option of doing neither and relying on traditional database managed users.

ALTERNATIVES

This fundamental requirement isn’t new. It’s the Oracle 18c-specific solution that is new. But prior to Oracle CMU there were some alternative options:

ORACLE UNIFIED DIRECTORY (OUD) AND ORACLE ENTERPRISE SECURITY (EUS)

OUD combined with EUS provides essentially the same functionality but is a far more complex and expensive solution. OUD essentially means having an extra tier of software that sits in between the Oracle database and Active Directory. This software tier is relatively complex to implement. It probably needs to be implemented in a redundant and highly available architecture, and is generally much more difficult to understand and manage. Oracle’s licensing of this software has changed over time, but software licenses aside, it’s still expensive in terms of having another tier to monitor, patch, etc., servers to run it, etc.

It is important to note that OUD and EUS still exists and still provides functionality not included with Oracle CMU. But for the purposes of Active Directory integration for database authentication and authorization, it has essentially become redundant. And hence, it's sensible to replace this complex software stack with the much simpler and more practical solution when only Active Directory authorization and authentication are required.

THIRD PARTY PASSWORD SYNCHRONIZATION AND MANAGEMENT TOOLS

Numerous password synchronization tools from third-party vendors are available. The way they generally work is that users change their passwords using the tool and it then works behind the scenes to change the password in multiple locations including Active Directory and Oracle Databases.

But again, this is an additional piece of software to acquire, maintain, and support, and almost certainly at a financial cost. Plus, these tools are prone to risk and error. For example, how securely do they capture, manage, and transmit updated passwords? What happens if they can't reach a particular system or database at password change time? What if the provided password passes complexity rules on some systems but fails against others? What if the username part of the credential varies between databases?

A separate set of password management tools exist just for the storage and auto-completion of usernames and passwords. But again, these are likely separately licensed third-party tools. And their ability to auto-populate username and/or password fields may depend on the application. They may work fine on web-based front ends but not so well on applications developed in Oracle Forms.

Overall, these tools have limitations and costs, whereas Oracle CMU has no additional financial costs and requires no additional software tiers.

CONCLUSION

The new Oracle 18c Centrally Managed Users feature provides exactly what most businesses have been asking for and waiting for since probably the very beginning of their Oracle database usage.

It's finally here with very few downsides. The most notable is that it's only a feature of Oracle Database 18c and 19c. It's not back-ported to earlier releases. Customers should be upgrading to Oracle 19c regardless—this functionality should just help motivate those initiatives.

With the continual news reports of corporate hacks and sensitive data being extracted and exposed by bad actors, all organizations should be striving to increase their security posture. To make environments more secure, we need to work towards

having fewer passwords, manually typing fewer passwords, and having to securely handle fewer passwords. Remember, it may not be users who manage passwords insecurely. Business applications or even security tools can sometimes be the culprit.

Fortunately CMU is an all-around win, because it means:

- Fewer user passwords overall.
- Reduced password management and handling.
- Reduced software tiers for directory synchronization tools or third-party password synchronization tools.

Best of all, no additional licenses or software components are required. Which leaves only a few final questions:

1. Why aren't all Oracle Database customers implementing this feature immediately?
2. Why did Oracle wait so long for this gift? It should have been part of Oracle7!

THE AUTHOR



Simon Pane


*Principal Consultant
Oracle ACE*

Simon is an accomplished Principal Consultant, who has developed a multitude of complex solutions for Pythian clients. He leverages his understanding of the industry and technologies such as Oracle, SQL Server, Linux, Oracle Cloud, AWS and more, to propose timely solutions that best suit the needs of clients. As a technology enthusiast, Simon is a highly sought-after speaker at many user groups and international conferences.

 info@pythian.com

 twitter.com/Pythian

 linkedin.com/company/pythian

 +1-866-798-4426

ABOUT PYTHIAN

Founded in 1997, Pythian is a global IT services company that helps organizations transform how they compete and win by helping them turn data into valuable insights, predictions and products. From cloud automation to machine learning, Pythian designs, implements and supports customized solutions to the toughest data challenges.

OFFICES

Ottawa, Canada

London, England

New York City, USA

Hyderabad, India