Software

Reduce Risk by Cleaning Up and Maintaining Your User Accounts

Dell One Identity Manager automates and streamlines identity governance

Abstract

A healthy organization today is anything but static. Growing enterprises are always hiring new talent, enabling employees to pursue new opportunities within the organization, and seeing some employees leave the organization. They often make use of contractors and other temporary resources who come and go. Moreover, the organization's employee base can change radically due to mergers and acquisitions.

Such changes can keep organizations vibrant and successful, but they also often introduce risk. Over time, the changes pile up and the enterprise may discover it can no longer be sure that users have access to only the resources they need to do their jobs or even that accounts are deleted promptly when a user leaves the organization. The organization recognizes that it is at risk of security breaches and compliance violations. But cleaning up the existing identity store — and keeping it cleaned up — can seem like insurmountable tasks.

Fortunately, they are not. This technical brief explains the three steps required to clean up and properly maintain your user accounts in accordance with industry best practices. Then it explains how Dell One Identity Manager can streamline the process, enabling your organization to easily and effectively implement identity governance that reduces security and compliance risks.

Introduction

User accounts are constantly in flux at nearly every organization. Ideally, a digital identity is created when an employee joins the organization; modified appropriately when the individual assumes new responsibilities, relocates or changes his or her name; and deleted when the employee leaves the organization. In that ideal world, all users have exactly the rights they need to do their jobs — no more, no less.

Adopting an identity management system can help you clean up your user accounts and keep them in order, thereby reducing security and compliance risks.

In practice, managing the user identity lifecycle is far more complex and comes with far less transparency. Do any of these situations sound familiar?

- A user changes roles within the organization. She is given the new permissions she needs to do her new job, but she retains permissions from her old role that she no longer needs.
- An employee is required to fulfill several roles simultaneously, perhaps due to restructuring, and the authorizations are issued quickly, without proper review.
- An employee is asked to cover for another person who is on leave, but the additional access rights that were meant to be temporary are never rescinded.
- A user leaves the company and his account is not deleted promptly, or even at all.
- An individual is authorized to act as both a purchaser and an authorizer at the same time because the role conflict was not visible.

This complexity and lack of transparency in user identity management add up to one thing: security risk. Organizations, of course, are keen to mitigate this risk — but the challenge of cleaning up their existing identity stores can seem overwhelming.

Adopting an identity management system can help you clean up your user accounts and keep them in order, thereby reducing security and compliance risks. This paper explains the three steps involved in implementing an identity management system and explains how Dell One Identity Manager can streamline the process of cleaning up and properly maintaining your user accounts.

Implementing an identity management system

Successfully implementing an identity management involves three steps:

- Cleaning up your data
- Choosing a solution with the right features
- Ensuring your organization is ready to use the solution

Data cleanup

Best practices

Before you can effectively use an identity management system, you need to clean up your data so that:

- Each employee has a unique ID that is valid organization-wide.
- Each account on each IT system is assigned a unique ID.
- The assignment of employees to organizational structures and functional units is unique and consistent.

When to automate

While manual cleanup is possible for some organizations, automation is advisable if any of the following conditions exist:

- **The organization has more than 1,000 IT users** — With so many users, manual assignment methods become unwieldy, and accuracy and consistency will suffer.
- **There is no reliable master structure for the administration of unique IDs** — In principle, an HR system could suffice, since HR has to identify each employee to ensure that each person gets exactly one paycheck. In practice, however, using an HR system to assign unique IDs is problematic. HR systems are often distributed over several unconnected systems; new employees are often not entered into the system until weeks after they have joined the organization (in time to issue their first paycheck); and external personnel may not be included in the HR system at all.
- **Organizational structures have grown over time** — Organizational growth often results in a complex system landscape, which may be largely undocumented. For example, uncompleted migration projects may have left behind old, unmaintained systems, and mergers and takeovers may have added new IT systems with different structures. Large organizations may have several HR systems and dozens of enterprise resource planning (ERP) systems, and directory services may not be centrally organized.
- **Data models are too different** — Sometimes data models are so different that data cannot be automatically consolidated on one system, even when the standard software release versions are the same.

Choosing the right tool

When manual assignment of unique IDs is not feasible, the organization should look for tools to help. Be sure to choose a tool that offers all of the following features:

- **Automated data cleanup with supplemental manual processes** — A good identity management solution will support data cleanup through fully developed, built-in business logic. The tool should be able to assign unique identities automatically in most cases and provide an efficient suggestion generator to help handle exceptions that require manual attention.
- **Mapping** — The identity management tool should also be capable of mapping the organizational complexity, including provisioning, on to the target systems. For example, the tool should not only enable you to add a user to the directory service; it should also enable you to administer user groups and subgroups.
- **Bi-directional synchronization** — The identity management tool should offer bi-directional synchronization between the source and the target systems, so changes to either system are reflected in the other system.
- **Secure storage of user data** — It is not enough to store data sets by reference (store by reference); to ensure a secure data history, the solution must keep all relevant user information in a central repository (store by value).

Getting the organization ready

You also need to make sure your organization is ready to use the identity management solution. Be sure to heed the following best practices:

Secure management support.
A clear commitment from management to clear out the authorization structures is vital. Otherwise, the project teams may be overwhelmed by the special interests of regional and functional organizational units. When obstacles threaten to block the project, a sponsor at the director level needs to be available to intervene.

Define the project structure.
The project should integrate the largest possible number of users with the least possible effort into the most frequently used target system. For example, a fast 90 percent solution for three important target systems is better than a 100 percent solution for a single target system.

Your project should also include ongoing data cleanup using a mandatory authorization process and a defined expiry date for all accounts — especially for any authorizations that are not automatically assigned.

Ensure data quality.
The master data for each account should include:

- Unique identification of internal and external employees
- Unique assignment of all accounts and authorizations to unique IDs
- Contact information (address, telephone, email and more as needed)
- Organizational assignments (department, functions, cost centers and others as needed)

Require regular attestation.
Department managers must confirm on a regular schedule (perhaps quarterly) the authorizations of every employee who reports to them.

Use generic (role-based) authorization rules.
Create authorization rules that are generic instead of ones that name specific employees, departments and so on. For example, do not create a rule that states that "Chris Smith of the Manchester office authorizes all the purchase orders for cost center 0815." Instead, create a rule such as "The cost center manager authorizes the purchase orders for the cost center" or "The controller authorizes all read access to accounting codes 27xxx and 19xxx."

A good identity management solution will support data cleanup through fully developed, built-in business logic.

Figure 1. The data loading, cleanup and maintenance process

Dell One Identity Manager streamlines the process of cleaning up and managing user identities across your entire enterprise, improving security and compliance.

Streamlining account cleanup and ongoing management with Dell One Identity Manager

Dell One Identity Manager streamlines the process of cleaning up and managing user identities across your entire enterprise, improving security and compliance. Figure 1 illustrates how Identity Manager loads, cleans up and maintains user data. Each step is explained in further detail below.

Step 1: Initial data load

The first step in implementing an identity management solution is the initial loading of the main identities, preferably from a trusted source. Normally this source is the HR system where, ideally, each employee is uniquely identified and employees who are no longer with the organization are clearly marked. Identity Manager automates the initial data loading and facilitates manual loading of user accounts not present in the data source.

Automated data import

Using a configurable import function, Identity Manager reads all the user data from the target system and sorts it according to built-in rules and any additional rules you choose to define. Data is sorted into two categories:

- **Clean data** — Accounts that can be safely assigned (marked in green)
- **Dirty data** — Accounts that cannot be uniquely assigned (marked in red)

Figure 2 illustrates Identity Manager's data sorting process.

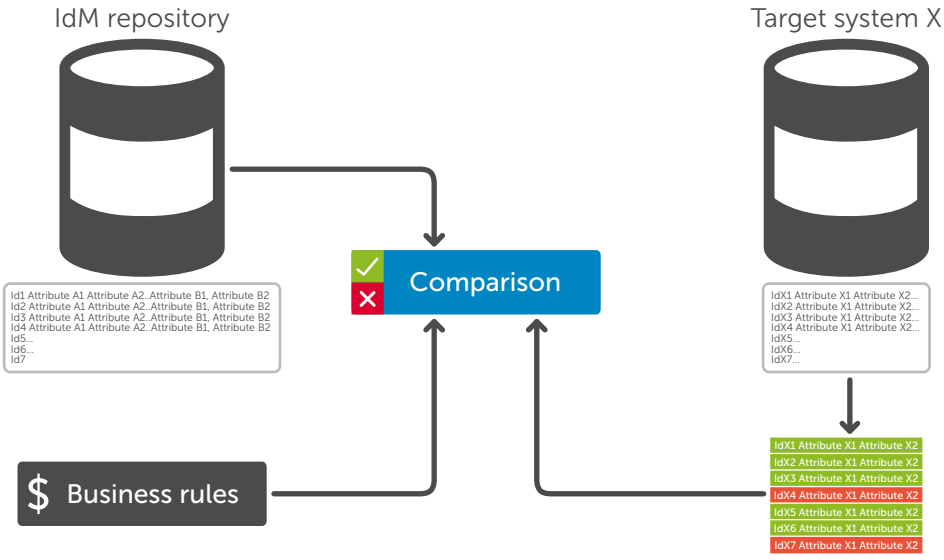

Figure 2. Separating clean data from dirty data according to business rules

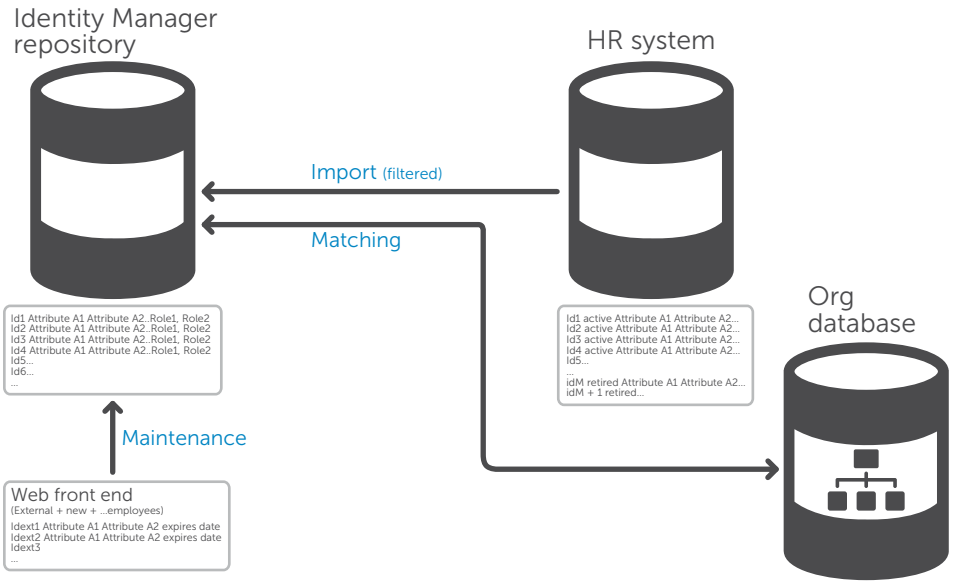

Figure 3. Identity Manager provides a web front end for adding and editing user data, which supplements its automated import and matching processes.

Identity Manager provides a web interface for setting up data for accounts not registered in the HR system.

Manual supplementation of data

Identity Manager provides a web interface for setting up data for accounts not registered in the HR system, such as:

- External employees, who are often not registered in the HR system
- Shared users and service accounts, such as support or security accounts
- New employees who have not yet been inserted into the source HR system

You can also edit imported or manually entered user data via the web portal, as shown in Figure 3.

Step 2: Transfer of clean data

Next, the clean data is transferred in its entirety to the Identity Manager repository, and existing user data is updated based on any change in the source data. From this point on, changes are initiated from Identity Manager and then transferred to the target system.

As shown in Figure 4, in Identity Manager, user data is kept as either:

- **Fully managed (clean) data** — Identity Manager can perform authorizations, provisioning and, where appropriate,

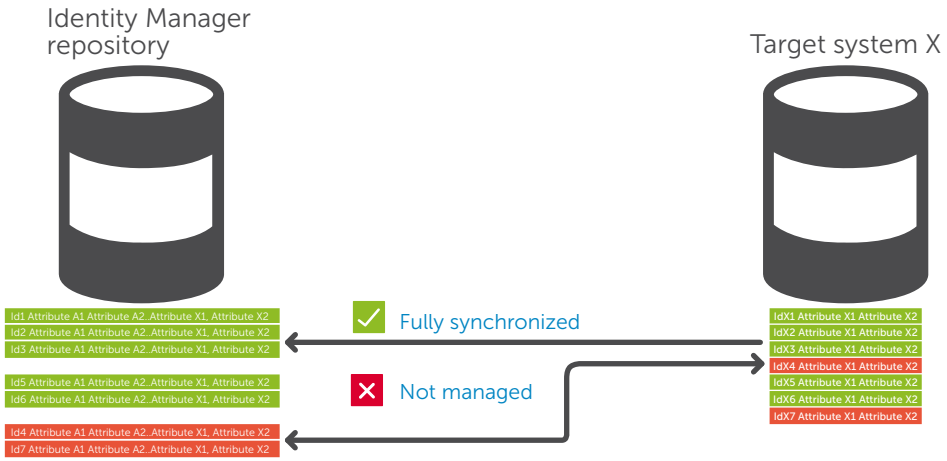

Figure 4. Clean data (shown in green) is fully managed, while dirty data (shown in red) is not.

invoicing. Data administered using Identity Manager is considered clean in the sense that unique assignments are in place and compliance rules are checked for adherence.

- **Unmanaged (dirty) data** — This data is loaded from the target system but not actively administered, so either the accounts are not uniquely assigned to an employee or a user group, or the assignment to organizational or functional structures is not correct or consistent. The data is regularly updated through the reconciliation process but only for transparency and documentation.

To ease manual cleanup of dirty data, Identity Manager can generate a list of alternative assignments for each account identified as dirty, and it offers a convenient web interface for cleaning up the data.

Step 3: Remediation of dirty data

The dirty data is available for cleanup, but is otherwise managed only passively. Copies of the cleaned data are stored in the Identity Manager repository, archived if necessary, and traced by a process that regularly compares it with the target system.

To ease manual cleanup of dirty data, Identity Manager can generate a list of alternative assignments for each account identified as dirty, and it offers a convenient web interface for cleaning up the data.

Step 4: Ongoing data management

To ensure accurate, consistent and documented identity management, further authorizations are made in two ways:

- Employees automatically inherit authorizations based on their assigned roles. Identity Manager can automatically check for possible role conflicts before allowing changes.
- Employees can request specific authorizations using Identity Manager's self-service portal. This web-based portal automates and tracks the authorization workflow.

Special circumstances

For large projects, we recommend using Identity Manager's pulse check feature. This simulates a data load (without actually performing the load) and measures data quality. If the quality is below your threshold, you can perform additional manual cleanup and check again before you proceed with the actual data load.

Conclusion

If your organization is concerned about security and compliance risks from a user account base that has grown out of sync with your real access requirements over time, do not despair. By following the steps in this technical brief, you can regain insight and control over your user accounts and access rights.

As we have seen, a good identity management solution can help. Dell One Identity Manager will enable your organization to clean up your existing user data quickly and maintain it efficiently and transparently. This will not only reduce your security risk, but also provide a trustworthy foundation for future initiatives such as single sign-on (SSO) or federation. To learn more, please visit software.dell.com/products/identity-manager.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.