5 Steps to Create Dynamic Identity Management

elevateHR®
Taking Talent to the Top

Elevate HR, Inc.

Published: January 2018

Microsoft Partner
Microsoft
Gold Enterprise Resource Planning
Microsoft Dynamics 365
Certified

www.elevate-hr.com

Active Directory Integration with Microsoft Dynamics

5 Steps to Create Dynamic Identity Management: Active Directory Integration with Microsoft Dynamics

Identity and Access Management (IAM) ensures that the right people in an organization access only the computer applications, systems, and information they require. IAM is the solution to this mission-critical need for organizations to comply with international data regulations and privacy standards, while providing consistent access for their people to such diverse technology environments as email, office applications such as Word and Excel, enterprise resource systems such as Dynamics, shared drives and databases, even the computers they use.

According to Gartner: "[Identity and Access Management] is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise. Enterprises that develop mature Identity and Access Management capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives."

Rule-defined technology access and application security is an absolute imperative for any 21st century enterprise, large or small. With 95% market share in the enterprise space, Microsoft Active Directory (AD) is the service most companies rely on to authenticate users and assign security clearance to individual employees and computers in a given domain. While Active Directory is a mainstay for enterprise Identity Management, IT departments face the logistical nightmare of threading this AD constant through the heterogenous enterprise resource planning (ERP) terrain. Whatever ERP or HR system you use—Microsoft Dynamics 365, NAV, Workday, Oracle, or SAP—IT and HR must work overtime to manually enter and synchronize employee information in both AD and their ERP.

For example, when you hire an employee/contractor or onboard a vendor/customer contact in your ERP, you must then create a user account in AD, assign AD security groups, import that AD account into your ERP and assign ERP security roles, among other tasks. You also need to keep this data in sync as employee attributes change, or people are promoted within the organization.

This process of manually transporting data between AD and your ERP results in duplicate data entry, human errors, and significant delays—and can rapidly domino from basic organizational inefficiency to catastrophic breach of enterprise security.

This data entry is rarely a one-time event. Without constant maintenance, data starts to 'decay' in aggregate, and the risk of erroneous data greatly increases. $1,000,000 is lost every minute in the U.S. due to poor data quality, and half the tickets logged by help desks are traced to master data errors (Data Warehousing Institute). Dynamic integration between ERP software and AD ensures that downstream data in AD is constantly maintained in real-time, through a direct connection with the data source (ERP).

What makes Identity Management dynamic? *Dynamic Identity Management* describes automation of the bridge between AD and your ERP. Dynamic Identity Management is predicated on the identification of a single source of truth for employee data, which protects data integrity, mitigates risk of human error, tightens enterprise security with pre-defined security matrices, and saves hundreds of hours a year that are normally spent updating security access, properties, and accounts.

This whitepaper will outline the "Five Steps to Create Dynamic Identity Management":

1. Understand the business requirements driving system access in your company
2. Assess your current process for maintaining user identity and access in Active Directory
3. Define data sources, record creation, change and deactivation triggers, and Active Directory update rules
4. Design a Dynamic Identity Management process that fulfills the business requirement documented in 1), mitigates the issues, risks, and costs uncovered in 2), and utilizes the information and outcomes defined in 3).
5. Automate the process.

We'll discuss each of these steps, and conclude with options to consider when automating the mission-critical activities involved in Dynamic Identity Management.

Step 1: Understand Your Business Requirements

A Gartner study observed that network security practices for the contemporary enterprise require business engagement and expertise, not just technical capability. It is critical that IT and business functions—Human Resources, Finance, Operations, Sales—align on the functional need for system access and control, and determine the rules by which access is granted, updated, and removed. Often, existing process complexities and internal communication channels limit the native utility of Active Directory. For instance, many companies don't take full advantage of the fact that Active Directory allows companies to record organizational elements such as departments, contact information, and hierarchies to reflect the organizational chart of your company. This enables workflow and internal company directories, but becomes a challenge for companies to maintain. Maintenance is often manual, requiring duplicate data entry when employees transfer or entities reorganize, and is therefore often wrong and unreliable. All too frequently, companies choose not to maintain such valuable information in Active Directory for this reason. Be sure, as you talk to business leaders about what they require for system access and security, that you explore not only what they *need* today, but also what additional features would *benefit* them going forward, without the constraints of current practice. As you collect this information, be sure to document which organizational roles require what security clearance, and which policies are needed for each security role (whether organized by groups, job, position, department, organizational unit, etc.).

Step 2: Assess Your Current Process (And the Associated Cost)

You may have procedure manuals or process flow documents that describe how your company currently maintains Active Directory. This next step is to gather that information, update it to accurately reflect current practice, and quantify the amount of time spent on the activities. It may surprise you to find out how many individuals are involved in each Active Directory entry or change, and how much time is actually consumed. Inspect the workflow chain of command or flow of communications to make sure you have accounted for the complete work effort involved, and be sure to factor in case management for reported problems and re-work to correct them. A poll of our customers and other Microsoft AD users indicates an average 30 to 45 minutes total time per Active Directory transaction (factoring in original request for access, system administrator reading the request, making the Active Directory change,

validating the change, communicating the change, and finally the requester validating and communicating the update to the user).

In one example, a company with 500 Active Directory user records concluded that they spent $30,000 total per year maintaining Active Directory. Another company of 2,000 employees, with a lot of churn within their organization but more efficiency than the first company, spent over $100,000 per year simply maintaining their Active Directory. It is important to note that, in both cases, the actual benefit of using Active Directory was diminished by each company utilizing only a limited amount of AD capability due to the time and effort needed to maintain it.

Finally, add a risk factor to your calculation—what happens if the termination of an employee or dismissal of a contractor is *not* immediately reflected in Active Directory? Or if assignment to the wrong Active Directory OU group exposes information to an employee who should not have access to it? Risk equals cost, and we've seen customers quantify that potential risk in the hundreds of thousands of dollars *per potential incident.*

Some companies opt to limit the amount of time they spend on this Step #2, assessing their current process. The amount of time you spend on this "As-Is" process is up to you, and depends on what kind of information you need to collect before you move on to the next step of creating the "To-Be" Dynamic Identity Management process for your company. We recommend, however, that some "As-Is" assessment be done for the following reasons:

1. Any implementation of a new business process means change for your organization. Involving current participants in the assessment begins the change management steps that your project will require. Understanding the current process is important to explain to participants *why* things need to change.
2. An understanding of the potential costs and risks of the current process helps you build a business case for internal discussion and decision-making around your Dynamic Identity Management project.

Step 3: Define the Business Rules

The objective of any Dynamic Identity Management program is to ensure there is a single source of truth for your company when it comes to data needed for all Active Directory user accounts. For the purposes of this white paper, that single source of truth is your ERP, Microsoft Dynamics 365 or Dynamics 2012. In this step, map the information you collect in Dynamics to properties in Active Directory. Where in Dynamics are you tracking vendor, customer, and worker data? How does this translate to a user account in AD? Now map the business requirements documented in Step 1 (above) to different events or transactions that are captured in Dynamics. For example, when you hire a new employee, what *event* in Dynamics will trigger the creation of an Active Directory account? What attributes of that person (e.g. employee type, department, position or role, etc.) determine which security groups they will need associated with their Active Directory record? What attributes for a contractor, customer, or vendor will determine those AD policies? Inversely, what role and security access should that individual have in Dynamics? What Active Directory information—such as email address—is created first in Active Directory and then later manually recorded back in Dynamics? What is the timing associated with these policies? Should the AD account be created before an employee or contractor starts, so that computers can be provisioned and imaged? Does one kind of termination require immediate disablement of an AD account, while a resignation or retirement may require a different timeframe, or a change in the kind of

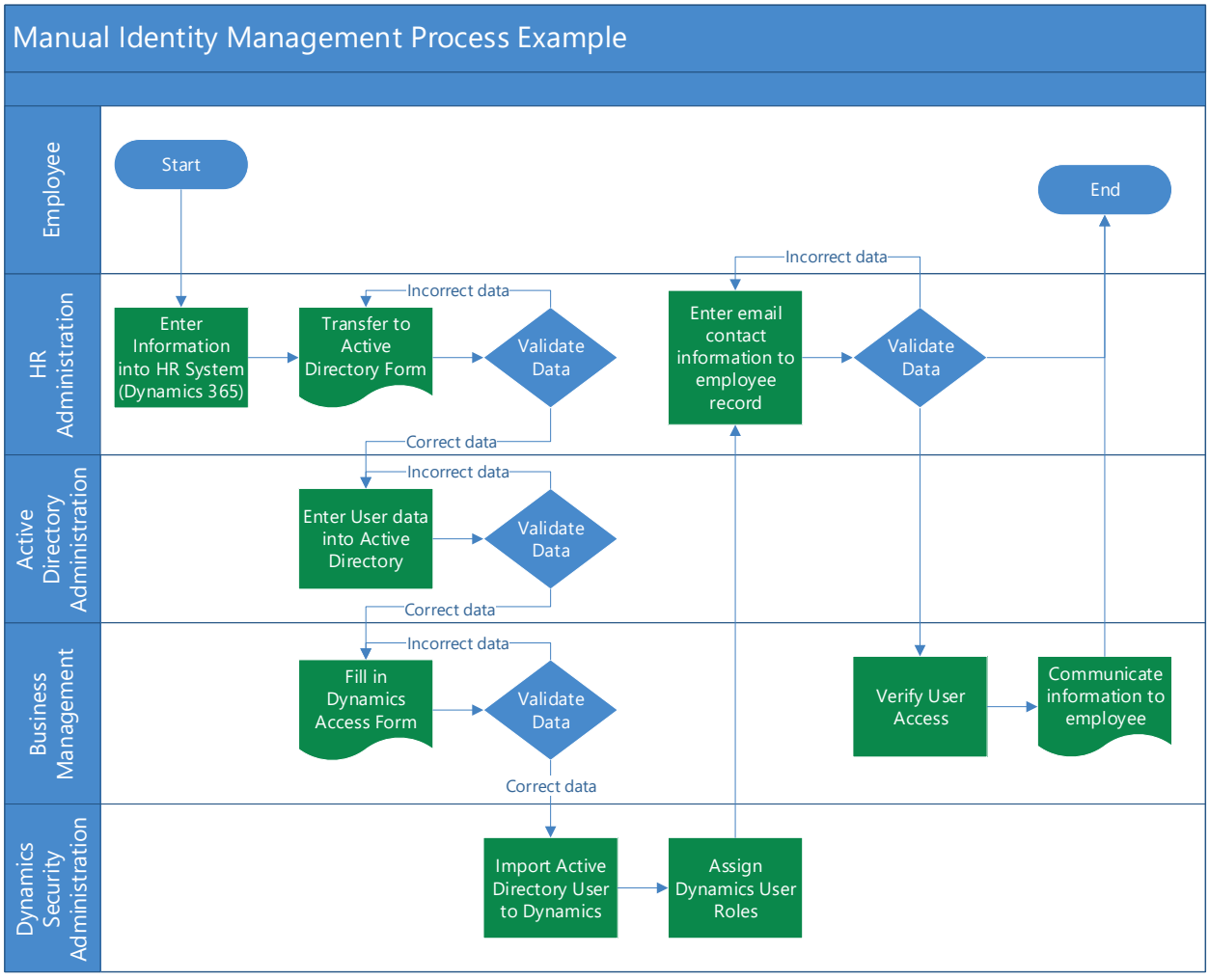
access? This information will help you create the process for Dynamic Identity Management in Step 4 and 5, below.

Step 4: Design the Dynamic Identity Management Process

If you plan to automate your Dynamic Identity Management, then the *process resources* you employ will be different, but the general activities you need to follow are analogous to a manual process. In this step, we will describe a typical manual process, and in step 5 we will explore automated processes.

In a manual process, it is crucial that every Active Directory entry pass through a verification or audit step. (Note that an automated process is self-auditing because audit has already occurred in Dynamics, the single source of truth, and any Active Directory record entry issues are trapped in error handling.)

You will need to follow a standard process design exercise, for example:



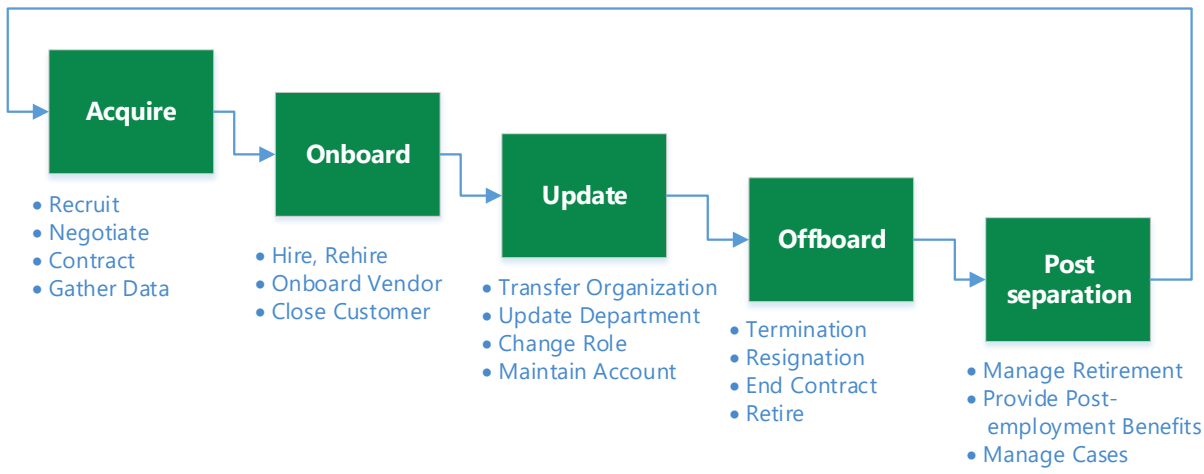
1. As you develop your process flow, describe each activity, or "node," in the process at a high level, for example:
    a. Collect required information from a Dynamics Hire or Onboarding event

b. Convert the Dynamics New Hire or Onboarding information through Map to Active Directory Form
c. Validate Accuracy of Active Directory Form
d. Enter Data from Active Directory Form to Active Directory Record
e. Validate Accuracy of Active Directory Record
f. Fill in Dynamics Access form
g. Validate Accuracy of Active Directory Form and the Dynamics Access form
h. Import User Record from Active Directory into Dynamics
i. Assign Dynamics User Roles
j. Verify User Access
k. Enter email address and other Active Directory information into Dynamics
l. Validate Accuracy of Dynamics User Access and user email address
m. Communicate Status of System Access to User

(Note: each of these activities need to be "decomposed" into sub-activities to fully document the process; for the purposes our discussion, we will remain at this high-level view.)

2. Describe the inputs and outputs for each of these activities; for instance, the "collect required information" activity may have a "report" as an input, and a "completed form" as an output.
3. For each of these activities you will need to assign a person, or a *process resource*, such as an HR Administrator to "collect required information" and a System Administrator to "enter data to Active Directory Record." (Note: in an automated Dynamic Identity Management process, the *process resource* will become the system itself [Microsoft Dynamics].)
4. Finally, you will need to add any constraints an activity may have, such as SOX regulations in "termination for cause" events, or your network security policies for business unit transfers.

The high-level process outlined above may occur in five different versions (below), based on the type of Dynamics event that triggers it, and variations of the process may be needed to fulfill the needs of each version:



Recognizing the steps in your manual process is critically important in order to understand the extent and complexity of your business process, and to help you document variations for the next step: automation.

Step 5: Automation

Dynamic Identity Management follows discrete and clearly defined rules, and is therefore a perfect candidate for automation. It is, however, a very complex process that is further complicated by the industry, size, business diversity, and geographic reach of your company. The indicative data that drives the rules behind Dynamic Identity Management are all contained in your ERP, Microsoft Dynamics, so any manual administration of Active Directory is, by definition, duplicate data entry, and often results in the degradation of your Active Directory records. If a manual process is chosen, such as the one outlined above, it is critical that precise audit steps are followed to ensure that data in both systems is correct.

If an automation path is chosen, the cost analysis described in the assessment phase (Step 2 above) can help you build a business case to present to management. There are two options for an automated solution:

1. Custom development of a rules-based, bi-directional interface between Microsoft Dynamics and Active Directory
2. Implementation of an off-the-shelf application or service; a configurable, bi-directional Active Directory Integration tool like Elevate HR's **elevateAD®**

Custom Development: Custom development can be written in a combination of X++, C#, or other software programming languages. Microsoft Flow can facilitate some of the workflow elements of the process, and has some limited capability of interacting with Active Directory. As is true in most custom development projects, the resulting software can be inflexible and expensive to create and maintain—in fact, the more complex your Active Directory interface needs become, the more expensive it is to develop sufficiently configurable interface solutions. In addition, any underlying changes from Microsoft Dynamics version upgrades open the possibility for significant rewrites to your customer Active Directory integration.

Configurable "Off-the-Shelf" Active Directory Integration: Packaged software products that offer features for Active Directory Integration are often designed for other needs, and are not purpose-built for the policy- and metadata-driven requirements of Dynamic Identity Management. If any ISV products you currently have installed do not offer rich enough Active Directory Integration features, then you can look in the market for one that does. Elevate HR offers one such product, a purpose-built, highly configurable (no custom code required!) Active Directory Integration product called **elevateAD®**. As in any business case, a "buy vs. build" analysis of elevateAD may offer a greater cost/benefit ratio than a custom interface.

The value of Dynamic Identity Management extends well beyond the hours and costs saved in manual administration of your Active Directory. Time spent requesting updates, resolving support cases for system access issues, productivity losses attributable to down-time while access issues are resolved, and mitigation of risk inherent in managing system security, all contribute to the $1,000,000 per minute loss of productivity in US business cited by Data Warehouse Institute. A solid Dynamic Identity Management process can put you on the right path to more productive business, and automation of this process will greatly reduce the cost and vastly improve the outcome of your Active Directory administration.

About elevateAD®

Elevate HR's on-premise and cloud (Azure) AD integration tool (elevateAD®) automates the exchange of information between your ERP (Dynamics AX 2012 or Dynamics 365, Enterprise Edition) and Active Directory, so all updates between AD and your ERP become an automatic extension and outcome of natural business process.

Users configure policy- and date-driven parameters so anytime you enter a contact, onboard a vendor, or hire an employee, elevateAD triggers the creation and activation of each corresponding AD user account, and automatically assigns security groups in AD and security roles in Dynamics by policy/position. Seamless bidirectional synchronization between your Dynamics ERP and AD provides your company's employees, customers, or vendors the access they need, when they need it, without delay or manual intervention. Terminate an employee or end a contract, and elevateAD automatically disables AD user accounts and cancels access to all systems. elevateAD respects AD account security options, including Kerberos DES encryption types, smart card interactive logins, and sensitive accounts. Auto-account management is available through elevateAD for all Global Address Book records (Customers, Vendors, Workers, Contractors, Applicants, etc.)

Dynamic Identity Management with elevateAD cements your ERP as the single source of truth for all employee information, empowers IT to deliver new applications faster, streamlines security by removing the need to maintain multiple accounts and passwords per user, improves data integrity in AD and all downstream applications, saves time and money, and relieves the burden on IT resources.

About Elevate HR

Elevate HR is the original developer of the HCM component in Microsoft Dynamics. We've attained Microsoft's two highest standards of partner achievement: we are a Microsoft Gold Certified Partner, and all our solutions are CfMD (Certified for Microsoft Dynamics). You can view more information about elevateAD® and our other Microsoft Dynamics ERP product modules through the Solutions and Resources sections of our website (www.elevate-hr.com).