v1.0 | 01 04 2019

IDM Commercial User Stories

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INDEX

INTRODUCTION

Your organization's technology environment must serve numerous and varied user types grappling with decidedly different daily dilemmas and demands. Most people believe that meeting all of these needs and remaining within budget requires serious tradeoffs – often with one or more user groups' needs left unmet. However, Identity Management (IDM) solutions provide any enterprise with the foundation to maximize, track, and secure their operational efforts.

IDM solutions ensure your identity information for each individual contains all the associated permissions, security, and organizational and "tribal" knowledge it should have. By implementing verifiable identities, automated processes, access governance, and self-service and delegation modules, an IDM solution suite constructs an organization's controlling framework.

IDM solutions are dynamic, leveraging technologies that manage, integrate, and synthesize user identities, account lifecycles, user permissions, and activities. These organizationally-driven technical implementations enable enterprises with respect to facilitating rapid access to necessary resources as well as assisting critical security and compliance needs.

IDM solutions manage the who, what, where, when, why, and how as they relate to users operating across any organization's "increasingly heterogeneous technological environments" (Gartner). The implementation of this platform allows verified users to access necessary resources, IT professionals to focus on productive work instead of menial management tasks, and the enterprise as a whole to operate more efficiently. IDM give the ability to shift energy towards ROI-focused, and beneficial operations rather than being restrained by its own systems.

The User Stories presented within this document are intended to provide the reader with an understanding of different individuals' needs throughout their responsibilities and how implementing a results-driven IDM solution benefits all of them.

USER STORIES

MANAGER

"As a manager, I wish I had the insight and controls to optimize operations by ensuring every employee had the access and authority their roles require. I am responsible for organizing business processes to be productive and efficient regardless of the scenario. I cannot be everywhere all the time and, without data, I rely on my gut a lot. There has to be a better method of managing access to keep our workflows efficient and regulation-compliant."

SOLUTIONS:

Individuals in management positions are responsible for making decisions when necessary, delegating whenever possible, addressing impediments to operations, and finding the best way to utilize their personnel. Combining these responsibilities is what makes day-to-day management seem like a non-stop whirlwind of extinguishing fires. Unless a time-freezing octopus runs your organization, management's ability and free hands never quite seem to be enough. When they are only human, how do you manage management's inability to be everywhere all the time?

Prior to automating technologies, the best solution was to set your workflows up with the right people in the right positions with the right authority to execute the right processes the right way. Gaining access to a given technological resource required endless forms and tracking down IT. Because IT is removed from some business processes, they may not know if granting that access is a compliance risk. If it sounds like such a system's success is entirely dependent on consistent, informed execution without any complications or variables messing things up, you are correct. If you live in the real world, you are already laughing at the implication that life – and especially any organization – could ever be so easy. Instead, the best method for achieving uniform results is automation.

Identity Management solutions automate or facilitate business processes to ensure consistent execution. Regardless of the specific process – such as onboarding a new hire, requesting file share access, or simply notifying relevant parties via email – administrative controls assist management in building out how workflows are specifically executed.

However, designing processes without business intelligence still relies on guessing. Whenever anyone organizes a group or designs a process, there are always major differences between what should work "on paper" and what does work in practice. Without data to help guide management's decision-making and refinement, any adjustments are based on past choices or assumptions – and with markets and technology ever changing, you simply cannot rely on what worked before to automatically achieve the same results. Like painting in the dark, it is possible to accidentally recreate a masterpiece – but it is infinitely more likely you are wholly dissatisfied and confused with the results once the lights are back on.

Identity and Access Management solutions provide managers with a variety of reporting capabilities because the solutions log all of the activity that occurs when processes are executed. This business intelligence includes everything from the simple "How many times did this user log in last month?" to "Who approved Tim's access to the payroll application, what date and time did that approval go through, and did they set a revocation date or leave a note in the record?". Backed by your IAM solution's extensive data collection, reports can be pulled at a moment's notice to provide detailed information and help you make new business decisions or review the old ones come your next audit.

NEW HIRE

“As a newly hired employee, I just want to make sure I have access to the resources I need for my job. I am excited to hit the ground running and want to make an immediate impact. At my last job, it took weeks or months to receive access to some of the resources that I was supposed to start with. I am worried that if this experience is similar, that my new boss will start to question my value. I just want to be an effective contributor as fast as possible.”

SOLUTIONS:

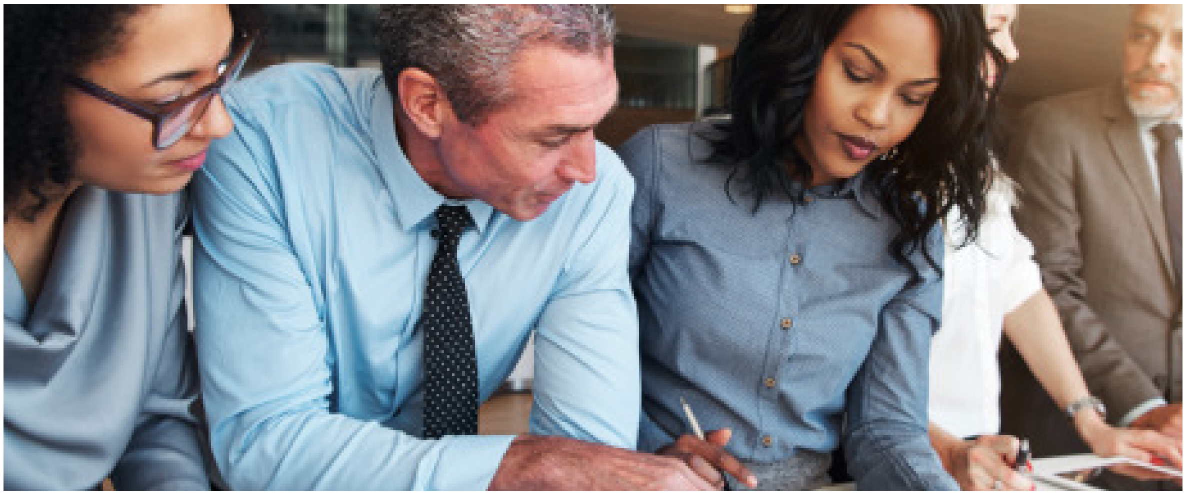
There is a lot on the mind of a new employee: “I want to make a strong impression and impact”, “I hope this organization is the right fit”, “Did I really just miss my exit on the first day?”. From the off, they must adapt to a new environment with new people and processes. This includes everything from remembering the second bathroom’s location for when all the stalls are full to learning the hard way which processes are snail-on-a-salted-speedway-slow or simply stalled-out dead ends. Overcoming those structural productivity barriers is not easy, especially when new hires lack the fallback projects to pick up and remain productive during those delays.

Automated provisioning comprehensively ensures that from the second a new employee is entered into your systems, they will have access to all their resources. Manual provisioning processes often begin with HR's entry of a new user into their system followed by untracked strings of emails intended to kick off the remaining steps. Typically, one IT staff member or a disjointed process susceptible to inconsistencies and oversights carries out the rest. Such a process lacks coherent or accessible audit information (inbox searches do not count). Further, onboarding processes often begin on the new hire's first day and regularly drag out or remain incomplete after hours, weeks, or longer – which is what allows that brand-new employee you are so excited about to collect a check while waiting to work and nervously twiddling their thumbs.

Automating your provisioning maintains uniform execution per job role every single time. The new employee's role determines their accounts, file system access, and applications. The structure that governs what user roles are provisioned with is called Access Governance and accomplishes what legacy "Copy User Template" workarounds could only hope to ever achieve with their spreadsheets. Access Governance actively controls and updates a user's resources based upon their identity information within the system for the entire lifecycle of their user account – first day to last.

If the user's role changes, an IDM solution automatically reprovisions accounts accordingly; that means no more having to comb back through endless spreadsheets to see who might have been granted noncompliant access nearly 7 years ago. IDM solutions utilize automations to ensure your employees have what they need to be successful. In doing so, they also significantly decrease a new user's "time to effectiveness" and help facilitate their become a contributing member for your team.

TEAM/PROJECT LEAD



"As a Team/Project Lead, I need the infrastructure to keep my group 'on-deadline' with the flexibility to adapt to any obstacle. When one of my team members lacks access to an app, file share, or other resource, it stalls the entire rest of the project that is depending on their contribution. These delays ripple and compound throughout project stages. I cannot lose whole days to chasing down IT and the appropriate approvals for one person's access just to get the whole team moving again."

SOLUTIONS:

You would hope that your onboarding process for new hires is so complete that they will never need another resource from you again; you would also be asking for inefficiencies to plague your organization. You need to have request and approval processes in place should something still slip through the initial provisioning. If your new hire somehow did not receive access to a resource necessary for their daily duties or special projects (e.g. Adobe Suite), a sophisticated IDM solution will provide your users with a self-service interface. This allows them to request anything – including applications, file shares, or even to play their favorite song over the office speakers after closing that big deal.

Workflow processes are easy to design given the right interface, whether management is technically inclined or not and without ever involving IT. For example, building the process below is actually quite easy:

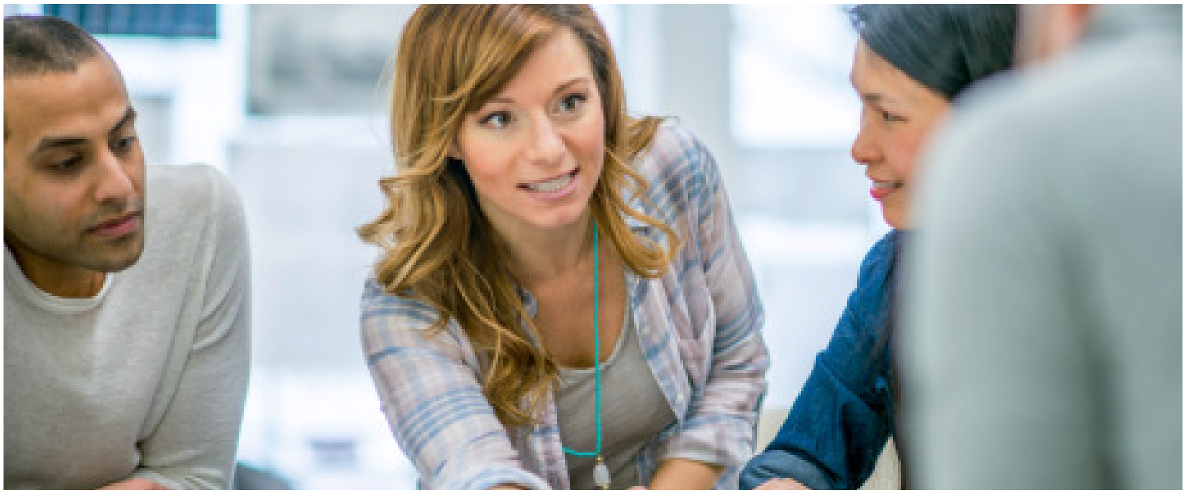
- An employee needs to request access to an application via a self-service portal;
- The request is routed to the appropriate, specified roles (e.g. manager, department head, etc.);
- The request is approved or denied with a simple click, which kicks off the back-end processes to fulfill it;
- The employee now has access to the file share and any relevant parties have received a notification email to keep them in the loop – without ever having to get the IT department involved.

When it comes to Self-Service actions and Service Automation workflows, your imagination really is the limit. All a workflow requires is an action, service, or thing to be requested; the owner of such (the "approver" to which all requests are routed); and the resulting process(es) carried out upon approval or denial (e.g. provision access, send email notification, etc.). Building automated workflows helps remove the potential for any unexpected variables to bring your organization's efforts to a screeching halt. Further, because the requests are all routed to the "owners" and handled within the automation software, there is never a need to hunt down approval signatures, fill out paper forms in-triplicate, or track down available IT staff to convince them why you need access.

A well-configured self-service automation interface will even remove IT as a potential approval bottleneck for those resources. Traditionally, technology access requests always went to IT as the only department with the technical knowledge capable of fulfilling them. However, IT also gets pulled all over to handle myriads of technology issues, mishaps, and endless password resets. Once you have managed to find someone, they may require approval from someone else – or worse, grant open, potentially noncompliant access without review.

Instead, service automations for these processes route the requests directly to the "resource owner" or the user's manager. These positions are the best for making and reviewing access decisions based on the real, day-to-day business activity and processes. When a request is sent or acted upon, all configured parties for that workflow receive notification or are prompted to respond. Self-service automation's back end kicks off the processes to wrap up the rest and the user should have access in no time.

MOBILE/FIELD EMPLOYEES



"As a mobile/field employee, I wish logins and password resets were so much easier. Having to authenticate every time I switch between all my apps and mobile browsers is incredibly frustrating. Every time I get logged out, I want to throw my phone. Being in the field makes it harder to connect with the helpdesk if I forget a password. When I do get ahold of them, it makes me very uneasy when they go ahead and reset a password for my accounts without verifying who I am."

SOLUTIONS:

Do you remember how terrible it was the last time you had to log in to anything on your phone? The fields are too small, your thumbs are too big, you still need to use browsers for some applications, you messed up the password again, and timed logouts force you to start all over. Mobile employees are part of any organization's "front-line"; sending them into the field without the necessary resources to be effective is a great way to demonstrate how much you support them. With a mobile SSO dashboard, a single login (with 99 to go) goes from being 1/100th of your problem to your productivity gateway.

An Identity-as-a-Service (IDaaS) solution featuring mobile SSO capability brings all of your mobile resources into a single dashboard – accessible anytime in any location from any device (e.g. phone, tablet, laptop). Regardless of what app, file share, or other resource you need out in the field, mobile SSO guarantees it is at your fingertips. Furthermore, using an SSO dashboard better protects against the security risks of BYOD (Bring Your Own Device) policies favored by some businesses. Any time your employees have a chance to combine their personal sensitive data and your organization's sensitive data on the same device, you are asking for problems.

If a mobile employee gets locked out of their accounts and cannot reach the helpdesk, what happens? Most likely, all productivity has plummeted to zero until someone can reset their credentials. Whatever role or task your mobile employee needed to accomplish is now so much more difficult, if still possible, that the entire rest of their day and schedule are thrown off. A self-service password reset solution allows employees to fix their own lockouts or preemptively change their password prior to scheduled expiries. Personalized challenge and response questions help protect the functionality behind solid security, so that only the user should be able to access the reset portal.

How long did it take your last password reset request to be fulfilled? If the answer is more than 30 seconds, you are incrementally wasting a very valuable aggregate of time. Password resets are a double-pronged productivity problem: the locked-out user cannot work and the average helpdesk is buried in so many reset requests that it prevents them from accomplishing other, more impactful work (e.g. supporting implemented resources, network management, etc.). A self-service reset solution can reduce your helpdesk's password workload by roughly 80%.

If that mobile employee was able to reach the helpdesk for a reset, how do they know that the caller is the user they claim to be? Does your helpdesk simply reset anyone's password because someone asked? When your password reset solution supports capability for users to identify themselves with questions regarding non-sensitive information, you ditch that verification problem. Any helpdesk employee can ask the caller for a given value related to information specific to them (e.g. "What is the third letter of the street you grew up on?"). Because these values are already included as challenge/response questions in some resources, the helpdesk employee can receive an encrypted string hiding most of its characters. Without being able to see the full value, the helpdesk employee can verify against the information without compromising the credential's secret and security.

TERMINATIONS/DEPARTURES

"As the helpdesk employee responsible for executing termination or departure workflows, I wish our process was centrally managed to ensure speedy, accurate, and complete deprovisioning. If I forget any part of the manual process, I expose the organization to massive risks and oversights. Former employees have sometimes retained access to our apps, data (including customer information), and physical locations – which we did not always discover until weeks, months or even years after the fact."

SOLUTIONS:

Deprovisioning is just as crucial as provisioning. The cold side to provisioning's pillow, these equal processes are the user account lifecycle's extreme ends. Deprovisioning is arguably more important: without provisioning, your employees are slower to be effective at their start; without deprovisioning, former employees can wreak utter havoc. Because the day-to-day effort of manual access management is so cumbersome to maintain, reviewing and deprovisioning a user's account becomes the most tedious challenge you can imagine. You might as well set out into a forest to find 5 specific trees. Digging through all of that data is so time consuming that many simply put it off until too late.

Security risks begin whenever an employee is hired. This risk is exacerbated most when an employee departs an organization without a deprovisioning process. Without an IDM solution, securely tracking all of a given user's accounts, credentials, and access (physical or digital) – let alone removing them in a timely manner – becomes impossible because of decentralization. If their directory account is missed or forgotten, the user may still be able to log into your network remotely so long as the ex-employee remembers the credentials. These "orphan accounts" add to system clutter, contribute to license costs, affect overall performance speeds, or become camouflage for intruders. The same applies for all of their 3rd party resources utilizing external accounts. Cloud storage, customer data, upcoming projects, marketing materials and more suddenly become susceptible to malicious theft and tampering.

With an IDM solution, all of a user's provisioned accounts, access rights, privileges and more are stored in a central repository. This makes executing deprovisioning workflows a snap – and, most importantly, just as fast as one. With the click of a button, your IT team, HR staff, or assigned department (technical or not) can kick off the process to revoke directory and 3rd party accounts, file shares, and even physical building access assigned to security codes or cards. Stop sweating security stress when you employees say sayonara.

HUMAN RESOURCES

“Working in HR, I wish our organization had the infrastructure to collect and preserve all the unwritten ‘tribal knowledge’ our department acquires. Like ancient legends, this information is only passed down occasionally by senior staff and without any ‘backup files’ if lost. We have to mentally track all our process’ nuances and ‘raisons d’etre’ constantly to ensure that onboarding, policy updates, personnel requests and more are handled properly. Further, I simply refuse to put my work on hold even one more time because someone needs to know their official position title instead of the custom one they wanted to make up.”

SOLUTIONS:

Decentralized information is a nightmare. It forces the creation of otherwise inefficient business, provisioning, and access policies as workarounds for the unavoidable lack of communication between resources and personnel. Left unaddressed, these symptoms exacerbate over months or years of workarounds that avoid addressing the cause and only create long-term confusion for your employees regarding “how” and “why” processes are executed. There is a good chance everyone hears “That’s just the way it is…” in such an environment. These formal or ad hoc attempts are not a remedy, but superficial bandages for broken structural bones – and, most likely, HR is the department left trying to remember why all your wounds are dressed the way they are.

Access governance provides any organization with the central information repository of their dreams. A role model built with access governance determines access and privileges according to the identity information stored within the solution. The logic and rules built into this structure will pre-determine much of the permissions, access, and capability granted to users. IDM solutions help guarantee that every user will have the correct title and permissions along with a self-service interface to request more. Simple account editing functionality lets users update basic things like a new home address in their network account without HR having to process any forms. Stop saying "That's just the way it is"; start fixing it with access governance.

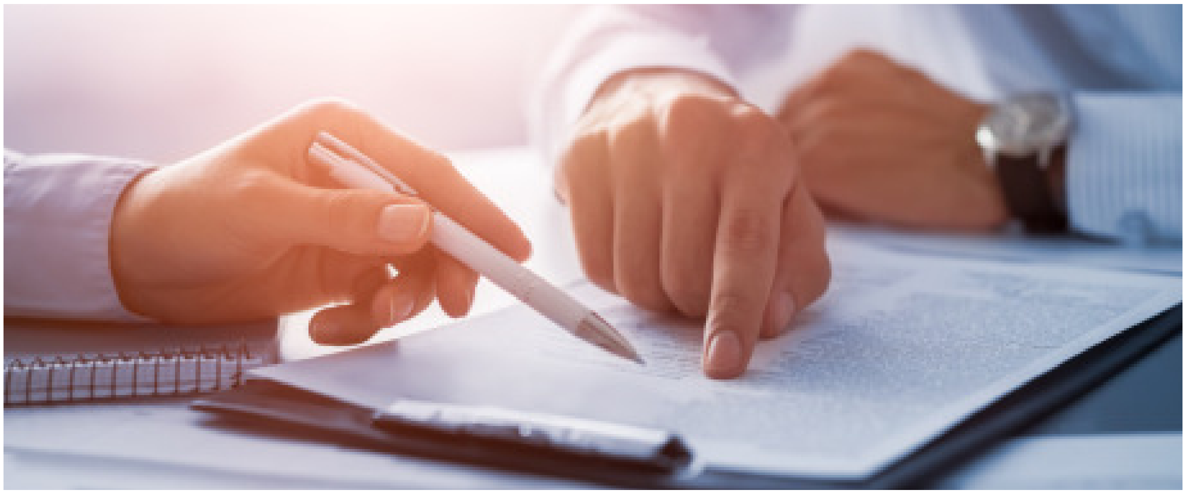
In most scenarios, HR kicks off the provisioning processes when they enter a new hire's data into their system. It is important to highlight that an access governance model is only as strong as the data that drives it. Inconsistent data entry will disrupt your automations when your solution attempts to synchronize or utilize that identity information. One person may receive multiple identities and accounts or be lost in your systems due to an easily avoided clerical error. Similarly, for identity data to reflect the associated individuals throughout your environment accurately, specific fields must only contain relevant values.

You might be feeling pretty great about securing your data with just access governance, but just answer one question: how do you deliver credentials to your new users?

If you rely on personal emails or an intermediary to hand them over on Day 1, you have already undermined your security. Onboarding presents one of the riskiest vulnerabilities in organizations. This is because the unclaimed account is phenomenal camouflage for intruders and most new accounts follow some easily guessed default password format. It is not uncommon for the default password to be exactly the same for every new account. Anyone capable of figuring out the value or its format is equally capable of figuring out how to cause all sorts of problems. A fully-fledged IDM solution manages Onboarding through a secure portal designed to prevent such possibilities.

Access governance, onboarding, and HR are 3 things made for each other – like peanut butter and jelly (...and bread).

CISO/INTERNAL AUDIT



"As the CISO, I wish I had the insight and controls to properly prepare for audits. Our last review went poorly, since I lack the holistic view of our environment to determine and clean up different users' access rights. Our infrequent access reviews allow employees to accumulate permissions from previous roles, temporary access rights from old projects, or simple mistakes. Misappropriated permissions have been very costly in the past and it falls on me to ensure everything is compliant come audit time."

SOLUTIONS:

Just the word "audit" is enough to make anyone nervous. Whether internal preparation, under a 3rd party microscope, or the dreaded Feds are knocking down your door, your audited processes, security, and infrastructure must hold up. The decentralized nature of a technology environment without an IDM solution makes this as difficult as conducting deprovisioning reviews for every single employee. Without regular access reviews and audits, users can gain, retain, and abuse noncompliant access throughout the course of their employment without even knowing the extent to which the organization can be penalized if discovered. Utilizing business intelligence reporting (when exports are possible) from all of your systems, apps, and other resources requires painstaking compilation and review efforts. The diverse data categories and focuses are too incompatible to effectively digest without additional interpretive layers involved in the already sluggish process.

As mentioned throughout this document, IDM solutions automatically collect all of the data and activity occurring within the system. IDM solutions securely compile and store these audit logs so you never again have to upend every folder in the file system to piece your information together. When it is time to conduct or answer to an audit, all it takes to collect the reports are a few clicks. Next time you are prepping for a government review, be nice to your auditor; they are about to lose a lot of job security.

CONSULTATION

Tools4ever intends for the information provided in this white paper to be educational and agnostic of any one IDM solution. Tools4ever's IDM solution suite provides all of the capabilities stated herein. A comprehensive technology plan can act as an organizational lever, allowing more accomplishment with less. If that premise is true, then Identity Management is the fulcrum with which that multiplication achieves the greatest benefit.

To learn more about results-based IDM solutions within Education and the varying capabilities, integrations and insight they offer organizations of all types, please contact Tools4ever. With nearly 20 years and more than 10 million managed user accounts of experience helping enterprises of all shapes and sizes transform their information resources into organization-driving solutions, Tools4ever understands that navigating through IDM solutions and implementations is a complex process, to say the least. Given the right knowledge and preparation, understanding IDM projects becomes much less daunting.

CONTACT TOOLS4EVER

If you would like more information on the subject of Commercial IDM solutions or to set up a consultative discussion with Tools4ever regarding steps to improve your organization's processes and maturity, please contact our team at nwsales@tools4ever.com.

For more reading on Tools4ever's IDM solutions and consultative expertise, please visit tools4ever.com/resources/ or tools4ever.com/references/.

Tools4ever's complete range of IDM solutions includes:

1. Identity and Access Manager (IAM)
2. HelloID (Cloud-Based IDaaS & SSO)
3. Self-Service Reset Password Manager (SSRPM)
4. Enterprise Resource Authorization Manager (ERAM)

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER New York

Address 300 Merrick Road, Suite 310
Lynbrook NY 11563
USA

Phone 1-866-482-4414
Website tools4ever.com

Info nainfo@tools4ever.com
Sales nasales@tools4ever.com

TOOLS4EVER Washington

Address 11515 Canyon Road E
Puyallup WA 98373
USA

Phone 1-888-770-4242
Website tools4ever.com

Info nwsales@tools4ever.com
Sales nwsales@tools4ever.com