RES

BEST PRACTICES FOR SECURE AND EFFICIENT ONBOARDING AND OFFBOARDING

Imagine hiring someone and not having a place for them to sit their first day. Or their first week. They wouldn't be very productive. They would probably also not feel that great about their new employer. Today's workforce is far less dependent on the chair or desk of a physical workspace as they are on the applications, content and services that constitute their digital workspace. So, when companies are slow to provide employees with the digital workspaces they need, business performance suffers—as does employee morale.

Slow provisioning of digital workspaces isn't just a problem at onboarding time. It also saps productivity and morale throughout every employee's tenure as their roles and responsibilities constantly change—and as they constantly experience delays in gaining access to the corresponding digital resources they require.

The more automated a company's workspace processes are, the less of a burden they will be on IT.

Fig. 1: Each employee now works in a digital workspace which provides the IT services and content they need to be productive, in accordance with increasingly mobile, multi-device workstyles.

Worse yet is what happens at the end of an employee's tenure. Few security risks are as serious as a disgruntled employee whose passwords are still active. But companies that can't quickly and reliably de-provision their employees' digital workspaces expose themselves to that risk with every termination.

Automated workspace provisioning and de-provisioning pay off in other ways, too. The more automated a company's workspace processes are, the less of a burden they will be on IT. That frees IT to focus on more strategic endeavors— a significant advantage as technology keeps becoming a greater factor in business success.

Every company can thus benefit significantly by better automating the provisioning, re-provisioning and de-provisioning of its digital workspaces. In fact, such automation is a must-have for any company seeking to:

- Attract and retain top talent
- Optimally motivate and equip that talent
- Optimize its organizational agility
- Diligently mitigate digital risk
- Get more value from IT

This white paper outlines best practices for implementing a streamlined and secure onboarding and offboarding strategy. Utilize this as a guide to fully understanding the most common onboarding challenges and obstacles, seeking out an effective solution and realize the benefits the business will see when a proper solution is in place.

UNDERSTAND THE CHALLENGE: SECURE WORKSPACES FOR DIGITAL WORKERS

Work is increasingly digital. Think about what happens when the network crashes. Within seconds, cubicle aisles are filled with aimlessly wandering employees and text messages start flying "Hey, did the network just crash?" Productivity simply halts.

As important as it is for employees to be able to access the resources they need, however, it is also important for companies to not allow employees to access resources inappropriately.

This is true for everyone from front-line customer service reps and delivery truck drivers to top-level managers and executives. We all digitally access a variety of resources that include:

- Applications (Word, Salesforce, SAP, etc.)
- Content such as shared documents in collaboration applications
- Services including IT help desk and corporate travel booking

As important as it is for employees to be able to access the resources they need, however, it is also important for companies to not allow employees to access resources inappropriately. Permissions can be restricted for several reasons, including role (non-clinical staff should not be allowed to see clinical data) and location/context (SSNs should not be viewable from a remote WiFi location such as Starbucks or an airport lounge).

The set of resources an employee (or a virtual employee, such as a temp or contractor) can access digitally at any given time and place can be understood as that employee's "digital workspace*." The lifecycle of a workspace can be broadly divided into three phases:

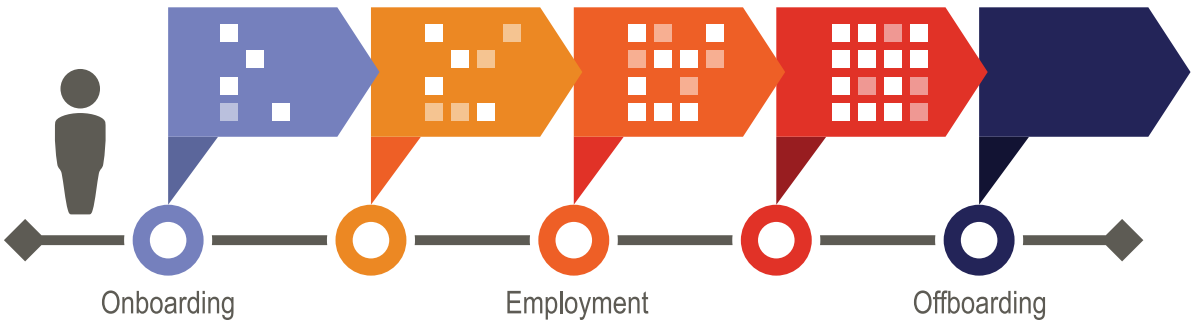


Fig. 2: Onboarding and offboarding now takes place with often dizzying frequency among the current generation of workers, where workplace transitions — including changing roles in the company — pose special challenges for IT.

1. **Onboarding:** This phase occurs when an employee is first hired and given his or her first digital workspace. It includes initial creation of the employee's identity as a consumer of digital resources.

2. **Employment:** During this phase, the employee's role and responsibilities change over time—which typically requires corresponding changes in their resource requirements and authorizations.

3. **Offboarding:** At this point, all access rights should be immediately terminated and the ex-employee's identity as a potential consumer of digital resources should be immediately disabled.

A company's objectives regarding the provisioning of employee's digital workspaces are generally similar across this entire lifecycle. Those goals are for provisioning to be:

Fast	So employees can be productive sooner, rather than later
Accurate	Because security requires that employees only be given access to appropriate resources
Efficient	Because operational budgets and staff are limited
Agile	Because business needs and digital resources are both in constant flux
Scalable	To accommodate future growth in the number of employees and digital resources
Accountable	Because compliance requires auditability of who could access what at any given time
Self service	To optimally empower employees and meet their workplace expectations

From a technical perspective, a digital workspace is very different from a "virtual desktop." A virtual desktop is the interface an employee is given on a particular device to access certain resources in their digital workspace. However, an employee may have access to resources in their digital workspace beyond what is presented in their virtual desktop. For example, their digital workspace may include an IT help desk that they can access outside their virtual desktop so they can get technical assistance even if their virtual desktop isn't functioning. Similarly, icons that remain on their virtual desktop may be functionally disabled (and thus not part of their digital workspace) if they are using a public WiFi connection.

The question facing organizations now is, how well can they meet these goals today — and how might they go about meeting them in a faster, easier and lower-cost way?

IDENTIFY THE OBSTACLE: INADEQUATE PROCESS AUTOMATION

The first and most obvious reason that employee workspace provisioning is slower than it ought to be is a lack of automation. If it were sufficiently automated, someone somewhere could click the right button and— ding!—a new employee would have the digital workspace he or she needed immediately. Or by the same token—ding!—a terminated employee's digital access rights would be immediately and completely removed.

However, given the fact that so many other business processes have been effectively automated, it is worth considering exactly why companies have not yet applied the same principles to digital onboarding, lifecycle re-provisioning and offboarding.

The "low-hanging fruit" for automation at most companies have been business processes that center in a single department—such as sales, marketing or finance.

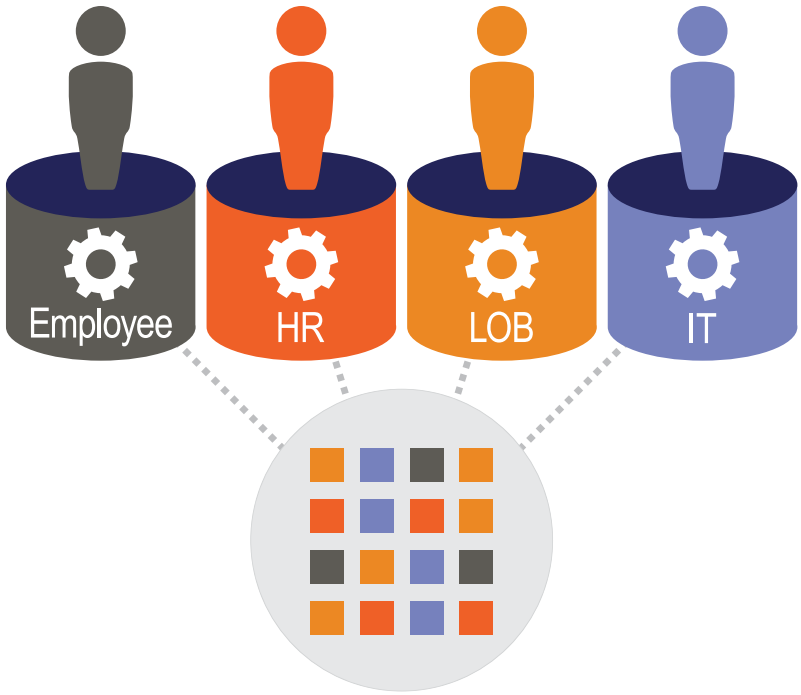


Fig. 3: Multiple stakeholders make effective automation of workspace provisioning a special challenge for IT.

These are the factors that, in particular, have typically delayed the effective automation of workspace provisioning at most organizations.

Factor 1: multiple stakeholders

The "low-hanging fruit" for automation at most companies have been business processes that center in a single department—such as sales, marketing or finance. Employee workspaces present a somewhat more complex challenge, because there are four sets of stakeholders involved.

Clearly, all these stakeholders have an interest in the automation of workspace provisioning. The differences in these interests, however, must be properly resolved and orchestrated in order to make automated workspace provisioning a reality.

Human Resources owns the employee lifecycle from start to finish. It has primary responsibility for overall workplace quality and compliance issues, of which digital workspace is just one piece. Improved workspace provisioning will help HR fulfill its talent retention goals—but, given its limited resources, HR cannot afford to get involved in the day-to-day technical issues associated with authorizing employee access to a company's various applications, content and services.

Line-of-Business managers supervise employees' work. They have primary responsibility for assigning roles and responsibilities. Improved workspace provisioning will help LOB managers fulfill their productivity objectives, but they need that provisioning to be flexible enough to meet their constantly changing needs— rather than having it impose counter-productive restrictions on their ability to give their people the resources they need.

Employees actually use digital resources to get their work done every day. They experience frustration when they can't get access to those resources on a timely basis. Improved workspace provisioning can eliminate this frustration and empower them to achieve what they desire to achieve—but it must provide a reasonably "consumer-like" self-service experience or they will simply work around it, which can lead to compliance and security issues.

Improved workspace provisioning can free IT from very time-consuming tasks and shed its "bad guy" image as the cause of aggravating delays.

IT owns the digital environment. It has primary responsibility for operating that environment, which includes the digital resources themselves (or, in the case of cloud, the relationships with resource providers), the network that connects employees to those resources, and the access control mechanisms that secure those resources. Improved workspace provisioning can free IT from a large number of individually small but collectively very time-consuming tasks, while also helping it shed its "bad guy" image as the cause of aggravating delays— but it must retain appropriate control over allocation of the digital resources in order to maintain security and protect service levels.

Factor 2: lack of a champion

Because workspace provisioning involves multiple stakeholders, it has not always been clear who should lead automation efforts. On one hand, IT and HR obviously have an important role to play. But neither IT nor HR is typically able to fund a workspace initiative on their own. Individual LOB leaders may also see workspace provisioning as an enterprise-level issue that should be driven from the C-suite, rather than their individual business units.

The result of this it's-a-great-idea-and-somebody-ought-to-do-it scenario, workspace automation initiatives can languish despite their tremendous potential business value.

Workspace automation may also have failed to attract necessary champions/ sponsors in the past because it was not viewed as a sufficiently strategic issue. Circumstances have changed dramatically, though, as digital enablement of employees has become a central factor in business success and as the attraction—and as a company's ability to attract and retain an entire generation of Millennial talent has become increasingly dependent on the quality of that digital enablement.

Factor 3: inadequate technology

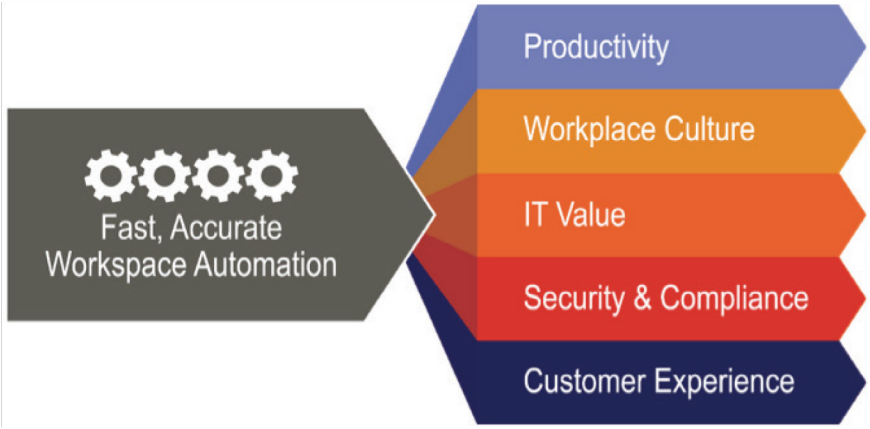
Even if stakeholders could come to consensus and find the appropriate champion, workspace automation may have historically been difficult to achieve due to the inadequacies of available technology solutions. Virtual desktops provide a technical mechanism for dynamically delivering access to digital resources, but they lack business-driven policy controls. Identity management tools provide policy-based access controls, but do not balance their ability to deny unauthorized access with a corresponding ability to proactively let employees know about available services that they can access. Nor do identity management tools selectively deny access based on awareness of the employee's or contractor's current context—such as being outside a geo-fenced area or using an unsecure public WiFi connection.

Fortunately, the tremendous need companies have to improve the way they deliver digital resources to their employees—a need that is now acutely perceived by IT, LOB managers, HR and employees alike—has resulted in the emergence of a new class of solutions specifically designed to meet this need.

RECOGNIZE THE SOLUTION: POLICY-DRIVEN DIGITAL WORKSPACE AUTOMATION

Companies can automate the provisioning, re-provisioning and de-provisioning of employees' digital workspaces in a variety of ways using a variety of technologies. But, at its core, any effective workspace automation solution must provide several core capabilities:

An effective workspace can activate or deactivate resource access when certain criteria are met.



1. Employees lose valubale time waiting for IT services they need due to manual processes and overworked IT teams.

2. Reduce the complexity. Provide employees a personalized digital workspace with self-service and automation to increase productivity, lower costs with reduce risk.

Programmable automation fabric. Workspace automation requires an underlying operational capability to perform the various technical actions required to activate or de-activate access to the applications, content or services appropriate for any particular employee in a repeatable manner, without requiring error-prone manual intervention. These actions can include account creation, password set and reset, creation of an appropriate virtual desktop on a VDI server, and/or creation of a VPN session. Ideally, a solution should also make it as easy as possible for IT staff to define these provisioning-related actions for each resource.

Adaptive rules/policy engine. In addition to being able to activate or deactivate resource access, an effective workspace automation solution must also be capable of performing those actions when and only when certain criteria are met. In some cases, those criteria will be defined by business rules—such as an employee getting promoted or a department contracting with an approved software-as-a-service (SaaS) provider. In other cases, those criteria will be defined by security and compliance policies—such as restrictions on remote access or recent excessive/anomalous utilization.

Stakeholder-appropriate interfaces. As noted above, there are multiple stakeholders in the digital workspace. An effective automation solution must therefore provide these stakeholders with functional interfaces appropriate to their particular needs. An authorized LOB manager that wants team members to use a particular application, for example, should be able to activate that resource for that team. Individual employees should likewise be able to self-serve from a menu of available resources.

Open integration. A workspace automation solution must integrate tightly with many other systems in the enterprise environment. These include:

- Hardware and software infrastructure management controls such as PC lifecycle management, mobile device management, etc.
- Identity and access management systems
- Virtual desktop infrastructure (VDI)
- HR systems
- Third-party cloud resources (SaaS, PaaS, IaaS, etc.)
- Security, mobility and other management/monitoring systems

Every organization's IT and HR environments are different—and the enterprise technology landscape is in such a constant state of flux. Therefore, a workspace automation solution's integration facilities should be sufficiently open and extensible to accommodate any third-party system that can help facilitate the delivery of the right digital workspace to the right employee at the right time.

Auditability and reporting. Compliance, security and good governance require that both employee access and the actions of those managing employee access be fully auditable. An inherent advantage of unified, automated provisioning processes over disparate manuals ones, in fact, is this auditability. A truly enterprise-class workspace automation solution should therefore provide full after-the-fact auditability, in addition to current-state reporting.

Workspace automation solutions can be differentiated in many ways—including ease of implementation, granularity of policy controls, predictive vs. purely reactive provisioning, etc. But these five core attributes are essential for companies seeking to respond to the increased important of digitally enabled work with better digital enablement of its workers.

REALIZE THE BENEFITS: BETTER PEOPLE DOING BETTER WORK—WITH SECURITY IN PLACE

When employees consistently have the digital resources they need, when they need them—and when providing them with those resources requires far less work on IT's part—lots of good things happen. These include:

By making it easier for employees to get rapid access to the tools they need, it makes them less likely to resort to potentially non-secure workarounds.

Significantly improved security. Automated workspace provisioning enhances security in several important ways. It enables complete revocation of digital privileges immediately upon termination. And by making it easier for employees to get rapid access to the tools they need, it makes them less likely to resort to potentially non-secure workarounds. It also enables IT to granularly implement policies that prevent multiple high-risk behaviors—without blocking access that is essential for productivity.

Enhanced compliance. Automated workspace provisioning brings a new level of auditability to both employee access histories and the past actions of those with employee access management privileges. It also concretely demonstrates best-practices due diligence to regulators.

More productive workforce. This part of the equation is obvious and powerful. If people have the tools they need to do their jobs right away, they can be productive right away. If they don't, then they can't. A fairly straightforward calculation of gained productivity alone will often cost-justify investment on automated workspace provisioning.

Engaged workplace culture. Every business leader knows that culture trumps strategy. A highly engaged, high-morale workforce therefore has strategic value when it comes to recruiting, retaining and motivating talent— especially as that talent increasingly consists of digital-centric Millennials.

Better allocation of IT staff time. IT currently spends a lot of time activating and de-activating resource access for employees whose needs are constantly changing. A lot of time is also spent on password resets and other services that could be handled via automated self-service. Re-allocation of this time is a major benefit for companies that would like to achieve more strategic technology objectives.

Greater business value from IT investments. Companies get more value from their IT investments when they can put those investments in the hands of more employees sooner. Also, most IT organizations currently spend a lot of time activating and de-activating resource access for employees whose needs are constantly changing. They also spend time on password resets and other services that could be handled via automated self-service. Companies can benefit significantly by re-allocating that staff time to the accomplishment of more strategic technology objectives.

More effective leveraging of the non-employee workforce. Most companies are making more use of contractors, freelancers and other nonemployee talent. In fact, there are industries marked by massive-scale seasonal transitions, such as shipping, transportation and tax preparation industries. They can, however, have difficulty leveraging digital resources to rapidly and fully include these non-employees in virtual teams with employees. Automated workspace provisioning can address this common difficulty by empowering LOB managers to quickly give non-employees access to team resources such as SharePoint document repositories, while ensuring that appropriate IT security safeguards are in place.

Superior customer experience. In today's high-choice marketplace, every company must consistently deliver superior customer experiences—or risk losing those customers to competitors. Automated workspace management directly and positively impacts customer experience by better equipping employees to respond to customers' needs and desires in real time at any touch-point.

The simple reality is that the increasingly digital nature of work, the escalating importance of optimizing the engagement of Millennial talent, the relentless demands of the business, and the need to free IT from routine operational tasks all make it essential to more intelligently automate provisioning of employees' digital workspaces. Companies that want to win in today's customer-centric real-time markets should therefore strongly consider investing in technology and processes necessary to make it that automation happen.

RES ONE solutions bring unmatched security, automation and control to the provisioning, re-provisioning and deprovisioning of employees' digital workspaces.

TAKE A PEOPLE-CENTRIC APPROACH TO ONBOARDING AND OFFBOARDING WITH RES

The expectations of the digital workforce and the number security threats are higher than ever before. Organizations should augment their traditional onboarding process with a more people-centric, streamlined approach. Taking this approach means immediate and effortless provisioning of access to the resources workers need and for which they are authorized. A comprehensive onboarding and offboarding plan improves security and worker productivity, not act as a roadblock.

RES ONE solutions bring unmatched security, automation and control to the provisioning, re-provisioning and de-provisioning of employees' digital workspaces. With robust delegation and self-service capabilities, RES enables employees and LOB managers to easily administer resource access — while still providing the centralized policy-based governance necessary to ensure security and compliance.

RES can secure workspaces, keep workers productive and give back more control to IT organizations. With a quick time to value, get up and running in days, not months or years. To learn more or speak with a RES support agent, visit www.RES.com/Security.

ABOUT RES

RES creates, automates and secures digital workspaces to improve the experience and productivity of the workforce while lowering IT costs. RES takes a people-centric approach to making technology access secure, even in complex multi-device/multi-location scenarios, across physical, virtual and cloud environments. RES boasts numerous patented technologies, fast time to value, and superior customer support for more than 2,500 companies around the world. For more information, visit www.res.com, contact your preferred RES partner, or follow updates on Twitter @ressoftware.

© Copyright 2017 RES Software. All Rights Reserved.
All other trademarks are the properties of their respective companies.
RES ONE is a trademark of Real Enterprise Solutions Nederland B.V.

v 1.0 01/06/17