Single Sign-on:
with passwords, less is more.

The changing nature of access

For years, employees have needed ways to access files and applications for work. But what it means to get "access" has changed significantly over the last several years. Today, companies use technology in dramatically different ways than they did as recently as five years ago. Not only are there a host of new applications to improve productivity, those applications are now often available "in the cloud." The move to cloud applications has shifted the relationship between users, IT and business technology. Further, employees are increasingly accessing data and applications from remote locations—at home or on the road—and they expect to be able to use their personal devices to do so.

These changes can be problematic, though. With these new technologies, it can be difficult for users to keep the right level of productivity. This is in part because it is more difficult for the users themselves, if applications are a mixture of cloud-based services, native apps and legacy applications that require a secure network connection like VPN. It is also because control has shifted away from IT, making managing complex business IT infrastructures a challenge. In this sort of environment, a simple request—like granting access—can be time consuming and difficult.

To eliminate the complexity for users, many companies have turned to single sign-on (SSO) solutions. SSO gives users a streamlined way to access applications and data and gives IT a unified way to manage access. But this dynamic, complex world is precisely why some companies have waited. For these organizations, SSO has been on the project roadmap but never near the top. Budget realities and lack of staff or skills frequently and repeatedly push SSO to the back of the queue. If you're one of those companies, now may be the time to pull SSO off the back burner.

CHOOSING THE RIGHT SOLUTION

There are many benefits to SSO and many options. But with so many choices, picking the right one can be a real challenge. As you evaluate your choices, however, there are some simple questions you should consider. Does the system you're considering offer:

- *Fast, secure simple authentication?*
- *Breadth of SSO integration?*
- *Self-service password reset?*
- *Ease of application and authentication integration?*
- *Ability to reference other identity information to gain comprehensive sign-on context?*
- *Freedom to use current or future authentication systems or methods?*

Use these questions as your evaluation criteria, and you'll be ready to enjoy the benefits of SSO in your organization quickly and painlessly.

NetIQ.
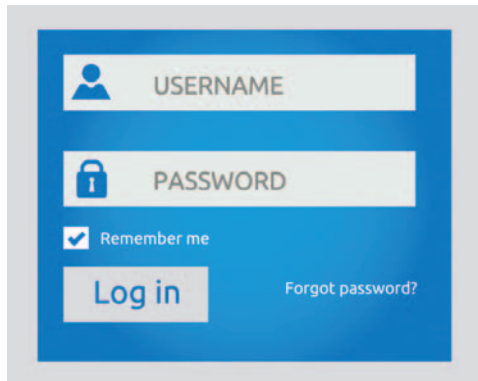
SSO: Why now?

Today there are some compelling reasons to reconsider SSO solutions. First, there are more options and choices for how to implement SSO. You can select from a range of on-premises and as-a-service options, as well as fully managed solutions. Most importantly, with today's complex technology environments, there's both a practical need for SSO and business value to be gained.

The first—and most obvious—benefit of SSO is productivity. Improving efficiency and driving productivity is a key focus for many businesses. SSO can improve productivity and efficiency in two ways. First, it helps users overcome the inherent complexity of accessing multiple platforms. They simply log in, and they've got access to everything. Second, it makes IT administrators more efficient, because they can manage access from a central platform.

SSO helps with more than just productivity, though. With data and applications no longer behind corporate firewalls, there is an increasing amount of risk in corporate IT. Without

SSO, you're putting a critical security responsibility in the hands of users. But the systems and applications they use—each of which requires a login—don't always make it easy. Systems often have different password protocols, or different password reset frequencies. With many passwords, users struggle to remember them all—so they create their own password management "strategies," many of which increase risk: Users reuse passwords across systems, write them down, or even practice "social" password behavior by sharing their credentials with coworkers.

This poses a significant risk because shared, reused or poorly guarded credentials can put multiple resources in danger, even if only one application is compromised. This vulnerability is compounded in the cloud, since it means that it only takes one vulnerable application to compromise the rest of your internal and as-a-service resources. An SSO solution puts security issues back in the control of the organization by making it easier for users to use a single, more secure, more unique password.

Failure to adhere to password protocol often comes back to user productivity. If users feel like they're wasting time, they'll look for their own ways to make things easier or more convenient. They don't maliciously seek to circumvent policy—they just want to be able to access and use their stuff. This is particularly true for high-value employees (or high-cost employees) such as doctors or financial experts. These audiences don't have time to

waste logging in every time they access a new application. And if a business can make them even a little bit more productive, it can pay huge dividends.

Further, users often make other "convenience" or productivity-driven decisions—which can include some very risky behaviors, especially with sensitive information in highly regulated environments. To "save time," they might leave workstations turned on rather than turning them off when they leave. Or they might simply neglect to log out when leaving a workstation. SSO makes accessing systems securely easier and increase the productivity of all workers, which can pay additional dividends for high-value employees.

Finally, SSO can help you take advantage of new advanced authentication technologies. Passwords are basically an outdated mode of security. That's why companies are increasingly relying on multi-factor or advanced authentication. These systems incorporate physical or biometric credentialing (access cards, fingerprint scans, etc.) into the login process, making it more secure. The cost of implementing advanced authentication has gone down dramatically in recent years. But for advanced authentication to work, it needs to be fast, easy to use and comprehensive. If you're only using advanced authentication for a few systems, you aren't really enjoying the true benefit and neither are your users. And if done in an incomplete fashion, advanced authentication can cause more problems by increasing the complexity of workflow for your users.

NetIQ has a range of options that can help you address your SSO needs. Our Identity-Powered Solutions use identity information intelligently to make your business more responsive and secure. They leverage your existing resources and infrastructure so you don't have to start from scratch. And they deliver sustained business value while driving lower TCO. Specific products that can help you address your SSO needs include:

- **NetIQ Access Manager**
  Deliver simple, secure, scalable web access to internal and external resources, with standards-based federation and support for advanced authentication.

- **NetIQ SecureLogin**
  Streamline user authentication for enterprise applications by providing a single login experience to users through multiple login methods.

- **NetIQ Self-Service Password Reset**
  Enable users to reset their passwords themselves so they don't have to call IT.

- **NetIQ CloudAccess**
  Provide simple access to your private or regulated information hosted in the cloud.

About NetIQ

We are a global enterprise software company that meets the demands of today's IT environments with a wide range of proven solutions for identity and access management, security and data center management.

Today's hybrid IT infrastructures are creating new challenges for business and IT leaders. IT services are now being delivered across an increasingly fragmented combination of physical, virtual and cloud environments. These services are being accessed from an expanding number of locations, on a growing variety of devices. And the technology environment is changing faster than ever. In the face of this combination of forces, organizations like yours often struggle to balance consumerized user expectations with the need to reduce organizational risk. All while still embracing the business value that can be achieved by leveraging innovations like cloud computing and mobile technologies.

So how do you keep access to IT services simple, while preventing unauthorized or risky user activity—all in the context of where and how users are connecting?

That's where NetIQ comes in. Our broad portfolio of solutions helps you manage the complexity of hybrid environments to ensure that the right people have the right level of access to the IT services they need, whenever they need them. With NetIQ, you can incorporate new technologies and services more securely, faster and with less effort. And our solutions help you understand what is going on in your environment—in real time—so you can mitigate risk while still taking advantage of opportunities.

Quite simply, this means that you can secure, manage and measure what matters most to your organization. Even more important, this new level of clarity will create new opportunities—and competitive advantage—by enabling you to understand, maintain and make sense of the shifting relationships between individuals, devices, behaviors and technology services. That's how you can drive the successful business outcomes that will deliver ongoing value to your organization.

Learn what next steps you can take by visiting **www.netiq.com/sso**

Worldwide Headquarters

515 Post Oak Blvd., Suite 1200
Houston, Texas 77027 USA
Worldwide: +1 713.548.1700
U.S. / Canada Toll Free: 888.323.6768
info@netiq.com
www.netiq.com
http://community.netiq.com

For a complete list of our offices
in North America, Europe, the Middle East, Africa, Asia-Pacific and Latin America, please visit **www.netiq.com/contacts.**

Follow us:

NetIQ®