

Single Sign-On (SSO) for Your Employees



10Duke



www.10duke.com

Introduction

So, you keep hearing about SSO and how it can improve the efficiency and security of your business, but you'd like to know what this means in practice? Read on, this whitepaper has been written specifically for you.

In it, you will learn:

1. How SSO can make your employees more efficient.
2. How SSO can help to improve the security of your IT systems.
3. How SSO can give you better control over your employee's usage of cloud-based applications and help secure your company's data held in them.
4. How SSO can be easy to setup and deploy – so easy that you can be up and running in less than 30 minutes.

1. Efficient work

When one of your team sits down at their desk, they will initially have to login to their corporate workstation. Once they've logged in, if they try to access cloud-based applications like Office365 to use email or compose a document, they will have to login separately to access each application, if you haven't yet implemented SSO. If they are also using other cloud-based productivity apps like Slack or Zendesk, they will have to login again to each of these services. It becomes a pain as they have to remember multiple usernames and passwords for each application they want to use. This time spent logging into apps would also be better spent actually getting work done.

By contrast, if you implement SSO, all an employee will need is the single username and password to access their corporate domain – from there they will automatically be able to access all of the cloud apps that you choose to bring under your SSO umbrella without having to remember or enter another username or password.

2. Improve security

If your employees are having to keep track of multiple usernames and passwords, they are likely doing so in one of two ways:

a. Same username, same password

A lot of people simply use the same username and the same password across multiple applications. Unfortunately, these are usually the same ones they use to login to your corporate network! While this makes it easy for them to remember, it creates a huge security risk for your organisation. If one of the cloud app providers is compromised, any hacker who gains access to the username and password of your employee can easily turn and try to attack your network using those same credentials.

b. Post-it Notes

The other approach is for your employees to use different usernames and passwords for each cloud service, but they will likely keep

track of all of these different credentials using Post-it notes stuck to their monitor or desk. This too creates a big security problem for your company as their notes are easily seen and copied.

Regardless of approach a or b, using cloud applications without implementing SSO creates some significant security vulnerabilities for your company.

3. A Single Point of Control

If you're using Microsoft Active Directory (AD) you currently provision and deprovision new or departing employees in AD. However, as your team increasingly relies on cloud-based productivity apps you've likely lost this central point of control. If an employee leaves your business and you remove her domain access in AD, how do you know that she still doesn't have access to all of your company files sitting in Dropbox?

Similarly, if you have a new person joining your company, you will have to provision them in AD but you'll then have to do the same thing for each individual cloud application your team uses. In some cases, this might be more than 50 different applications! It might not be rocket science, but even for a small team where reliance on cloud apps is likely to be quite high, the time you'll have to spend on manual provisioning will be significant.

With SSO life becomes much easier. Once you've provisioned a new starter in AD, they will automatically have access to different cloud apps, based on the permissions you define in AD. Each cloud app will look to AD to authenticate and authorise the user, so AD remains your single point of control.

Similarly, if an employee leaves your business, once you remove her from AD, she will automatically lose her access rights to those same clouds apps and the company data held in them.

4. SSO Easy...

There is a general perception that implementing SSO for your employees is hard to do, requires lots of expertise and takes a long time to

implement. That is not the case. Clearly more complex requirements (including device certificates, multi-factor authentication or supporting remote working) can extend implementation times, but with the 10Duke Identity Bridge Service (IdB) you can configure and deploy an SSO solution for your employees in under 30 minutes.

There are four steps involved:

1. Request access to your IdB tenant by emailing support@10duke.com.
2. On your Identity Bridge management console, configure Identity Bridge to talk to the Identity Provider (such as Microsoft Active Directory) that your company is using.
3. On your Identity Bridge management console, configure Identity Bridge to talk to the 'Consumer' applications you want SSO to; these are the cloud-based apps like Office365, Salesforce, Trello, etc. that your team is using.
4. In your cloud-based consumer apps, configure each of them to delegate authentication to the Identity Bridge service. Not sure what's involved here? No problem - you'll find simple to follow guides in your IdB support pages or you can ask us for help.

... using cloud applications without implementing SSO creates some significant security vulnerabilities for your company.

The Identity Bridge service provides you with templates to make the correct configuration so this process should take about 30 minutes to connect Identity Bridge to talk to 3 or 4 cloud applications.

Summary

If your employees are using multiple cloud productivity apps such as Office365, Slack, Salesforce, Zendesk or Trello to get their work done, implementing Single Sign-On is the best way for you to make their lives easier, secure your IT systems and keep a single point of control over which cloud applications your team is using.

Implementing SSO doesn't have to be a headache and can be done quickly and easily and with the 10Duke Identity Bridge service you can be up and running with a cost-effective solution in less than 30 minutes.

Next Steps

To learn more about the 10Duke Identity Bridge service or to set up a free trial please visit the product page or contact us for a trial:

www.10duke.com/products/idbridge
www.10duke.com/contactUs.html

