Expert Advice - 20 Practical Tips on Authentication and Access Management from Practiced Professionals

INTRODUCTION

You know your organization's need for stronger IT security can't wait any longer. Regulatory compliance and the risk of a data breach are forcing you to implement more stringent security policies and procedures. However, user password problems continue to consume time, resources and money. With the cost of a security breach far outweighing the cost of a solution, the benefits of single sign-on (SSO) and strong authentication are too significant to pass up. But with tight budgets, resource constraints, and the prospect of a disruptive enterprise-wide deployment, the idea of such an undertaking can be daunting.

At times like these, you need expert advice - not from a vendor, but from actual peers who have successfully deployed SSO and strong authentication at their own companies - from those who have measured the results against the investment, and can share their experiences. So we approached some of our customers and asked them what advice they'd give to other IT executives who are contemplating the implementation of SSO and strong authentication. What follows are 20 tips for ensuring success based on their experiences.

BEFORE YOU DO ANYTHING ...

Proper planning can prevent many problems before they occur. If you're still in the evaluation process, you may want to follow these words of advice from people who have evaluated just about every solution out there.

1. Consider how the solution fits into your long-term authentication and access management strategy.

It is important for the acquisition and implementation to be part of a planned authentication strategy. Even if user convenience, or reduced help desk calls are your immediate goals, the objective should go beyond providing convenient authentication for the sake of technology, to actually being part of an overall security plan.

Paul De Vroede, Manager, Telecommunication & Office Automation
Bridgestone Europe - Brussels, Belgium

2. Perform due diligence to find the best form of strong authentication for each of your user groups.

Remember that different user groups have different requirements for access. Make sure that the solutions that you are considering are flexible enough to accommodate the access needs of all groups – today and down the road.

Dr. Stephen Patterson, Chief Medical Information Officer
H. Lee Moffitt Cancer Center - Tampa, Florida

3. Highlight the positive – beyond security -- to senior management.

Get them on board early on. An appreciation of the overall benefits will not only help with the purchase process, but it will pay off down the road, when it is time to deploy to users. They will look forward to the new solution.

Damian Atkinson, CIO
ING Wholesale Banking – London, England

4. Understand how the solution works with technologies from other vendors.

Multiple vendors can and will work together if you push them. If integration is an important element of your project, bring it up early and don't move ahead without knowing that the vendor is committed to making it happen.

Joe Greene, CISSP, Information Security Director
OhioHealth - Columbus, Ohio

5. Learn exactly what is required to profile all types of applications.

At the City of Miami Beach we have a real mix of applications, including some specialty niche applications that are ubiquitous in local government environments. If your system includes various types of applications, before implementing SSO, make sure that the vendor demonstrates that their solution will not leave you high and dry when it comes to that odd application.

Nelson Martinez, System Support Manager
City of Miami Beach - Florida

6. Ask which strong authentication methods the products support directly.

Even if you have already decided on a method for today, user requirements and technologies are apt to change and you want to be sure that you have choices down the road. Also ask if strong authentication methods can be mixed and matched for different user groups.

Mike Mitchell, Network and Applications Analyst
William Osler Health Centre - Brampton, Ontario

7. Have a clear understanding of the amount of services entailed with deployment and maintenance.

Know what is required in terms of consulting services, and budget for that cost as well as for the product itself.

Rifat Ikram, Vice President of Electronic Delivery and Support Services
Justice Federal Credit Union - Chantilly, Virginia

8. Know the cost of failure. If you have to remove the solution – for whatever reason, what is that going to require?

The nice thing about OneSign is that it is architected in a way that is non-intrusive to the applications. That means that it never touches the application code or requires an agent on the server. This was reassuring for me as I could tell myself that if the solution didn't work out, I could just unplug the appliance. With other solutions I would have had to undo a lot scripting, and the reworking could end up taking longer and costing more than the install.

Christopher Paidhrin, HIPAA and Security Officer
ACS/Southwest Washington Medical Center - Vancouver, Washington

ONCE YOU'VE MADE YOUR DECISION ...

In today's economic climate it is critical that you are efficient and effective with your time, resources and budget. Making the right decisions - from installation and deployment to user training and measuring your ROI – in your SSO and strong authentication strategy will be the key to your project's success. Make sure you consider the following tips as you progress from vendor selection to solution implementation.

9. Engage your end-users early on.

Before you roll out, do a product demonstration for them – perhaps even before you have purchased. Odds are the users will be blown away with the simplicity of the authentication process and will clamber to sign up. In our case, it was the SSO and Strong Authentication solution that actually got the physicians excited about implementing the entire healthcare IT solution.

Bill McQuaid, AVP and CIO
Parkview Adventist Medical Center - Brunswick, Maine

10. Take a phased approach to your deployment.

Start with a pilot, and roll out in phases from there. We began a testing phase with 40 users. Then we collected feedback and deployed to the 400 users who access our five core applications. Since then we have enabled many other applications, mostly web-based, for various user groups.

Michael Lewis, System Administrator
West Liberty Foods - West Liberty, Iowa

11. Enable your most frequently accessed applications first.

Then move to the favorites of particular users. We started with our largest applications, the ones that were being accessed by the most users. We didn't allow ourselves to be distracted by special requests for obscure applications accessed by one or a few users. We continue to enable applications on an as-needed basis. This gives us the greatest return.

Eric Kloss, Manager of Technology Consulting
AAA National - Heathrow, Florida

12. Make your users part of the process.

Seek their advice and learn their needs. We set up a physician steering committee to help guide our identity management strategy. It not only helped us to find the right product for our users' needs, but it helped us when the time came to roll out to the users. They were invested and ready to adopt the new system.

Dr. Michael Westcott, Chief Medical Information Officer
Alegent Health - Omaha, Nebraska

13. Maximize the consulting hours you have for implementation.

Do the install yourself. In our case, we purchased OneSign from Imprivata and we made sure that the appliance was delivered before the Imprivata engineer came on-site for the three-day services package. That way we had everything installed and ready to go and we were able to make efficient use of our time while we had the engineer on-site. After Day 1, the OneSign system was operational in a test environment and several applications were already SSO-enabled. By the third day, over 30 applications - including our core banking software - were SSO-enabled. We had time left to work with the engineer on our roll out and user training strategy.

Steve Siress, Network Systems Administrator
Enterprise Bank & Trust - St. Louis, Missouri

14. Don't expect Security alone to justify budget and enthusiasm from management.

Use features like easy access to all your applications, roaming user sessions, fast user switching to get your boss excited about SSO and Strong Authentication. That is where the Return on Investment comes from. After all, how many people select an insurance policy based on the actual content versus the offered rebate?

Michel Bouquet, IT Manager
Spaarne Ziekenhuis - Hoofddorp, Netherlands

15. Understand that no two departments / user groups are the same.

Work with your "super users" well ahead of time. Help them to test, test and test. SSO is simple, but it is a change, and it ultimately affects everyone and everything. Identify unique users and PCs early on and have a plan for them.

Todor Yordanov, Systems Administrator
The Credit Valley Hospital - Mississauga, Ontario

16. Write a user deployment plan and share it with your users.

Communication with users is critical to success. People are averse to change – even when it is for the better. Don't spring a new technology on them. Send email messages, hang posters communicating the benefits of SSO and SA. Let them know what's in it for them. Let them know that their workflow won't change.

Chuck Christian, Chief Information Officer
Good Samaritan Hospital - Vincennes, Indiana

17. Create a dedicated, detail-oriented team for deployment.

Dedicate a project manager and, depending on the size of your project, perhaps a deployment team. A train-the-trainer approach works well for large, multi-site deployments. We had two primary people in charge of the deployment, with other resources available to support them as necessary. We rolled it out enterprise-wide at all five locations in short order. Today, the entire company uses the product.

Nick Voutsakis, Chief Technology Officer
The Glenmede Trust Company - Philadelphia, Pennsylvania

18. Develop a tightly managed internal security policy before you deploy authentication and access management solutions.

Though we are not bound by HIPAA, we feel that it is good practice to comply and follow guidelines where ever it makes sense. Our internal policies dictate that certain user access is limited to certain systems. Having our security policy defined and understanding the requirements helped us to come up with a deployment strategy to match that policy.

Michael Wilson, Infrastructure Director
The Henry M. Jackson Foundation for the Advancement of Military Medicine, Inc. - Rockville, Maryland

19. Measure your progress and return on investment.

It is just one more thing to do when you are thinking about your deployment, but putting measures in place before you begin makes evaluating the satisfaction and ROI much easier. Compared with volume before implementing SSO, our help desk calls have come down by 25%. We can translate that into hard savings for Verity Credit Union, which makes it easier to justify spending. And through user surveys we have learned that the system has saved our users significant time, allowing them to focus on serving our members.

Jon Wu, System Engineer
Verity Credit Union - Seattle, Washington

20. Do not over promise to your internal customers.

Once they have the convenience of SSO and strong authentication for access to critical applications, department heads will want every user enabled for every application. Stick to your rollout plan and don't promise what you can't deliver.

Josh Rosales, Administrator, Security / Web / Backup / Network
Lake Forest Hospital - Lake Forest, IL

ADDITIONAL RESOURCES

As you continue down the evaluation path, consider the following resources:

1. Gartner's 2008 Enterprise Single Sign-On Magic Quadrant, by Gregg Kreizman, September 2008 - According to Gartner, the enterprise single sign-on (ESSO) market moved toward maturity in 2008. For a free copy of the report, visit Imprivata.com.

2. Additional Imprivata Whitepapers available on Imprivata.com.
   - A More Secure Front Door: SSO and Strong Authentication.
   - Directory vs. Database: In Search of the Optimal Identity and Access Management Authentication.
   - Imprivata OneSign Release 4.1: A Platform Overview.

3. For more helpful tips and words of advice from other OneSign customers, please visit the Imprivata Interactive Demo Site.

4. To schedule a demo to see OneSign in action, contact us at sales@imprivata.com.

While every organization and environment is different, these tips should prove valuable to meeting your authentication and access management goals.

Imprivata has worked with hundreds of customers ensuring their authentication and access management projects are successful. For more information about Imprivata and OneSign, please contact us at 1-781-674-2700 or sales@imprivata.com.

Offices In:
Belgium • Germany
Italy • Singapore
UK • USA

1 877 ONESIGN
1 781 674 2700
www.imprivata.com

WP-EA-Ver1-0109