Realtime publishers

The Essentials Series: Architecting the Right Solution for Strong Authentication

Deployment and Management of Strong Authentication Solutions

sponsored by

imprivata®

by Jeffery Hicks

Copyright Statement

Deployment and Management of Strong Authentication Solutions

Congratulations. You've recognized the need and value in a strong authentication solution. Of course, it has no value if it remains in the box. In this article, I'll discuss ways to take advantage of your new solution and pitfalls to avoid. I also believe that you should use this information as part of your planning and selection process. A solution that you can't easily deploy and manage is not a solution worth having.

Control Deployment Risks

I'm sure you are aware of the adage about reading the manual, and this most definitely applies here. This is not the time to "wing it" and think you know what steps to take. Although, hopefully, implementation and deployment steps are simple, you should not ignore the documentation. You can't afford to miss any critical step.

Once you know what steps to take, it is very important, in my opinion, to start small. Don't introduce an enterprise-wide solution to the entire enterprise on Monday morning. You can control deployment risks by starting small. Identify a core group of users and administrators that represent a cross-section of your employees. These individuals should have some technical savvy and be willing to deal with an occasional problem.

When I have been involved in pilot programs in the past, very often, a core group of IT administrators is first targeted. I think of this as the pilot's alpha stage. This provides an opportunity for you to work out enrollment procedures, troubleshooting experience, exposure to the management tools, and a first-hand understanding of what an end user might face.

The next part is the pilot's beta phase. This is the time to introduce end users to the process. You must understand and document their experiences. This provides Help desk knowledge as well as information that can be used to refine or revise policies and procedures. Some organizations may begin this phase with a very small set of users and, should all go well, extend the pilot to a slightly larger group.

When including end users in your pilot, don't forget to involve their management layer so that managers understand what is happening and can accept the potential for a temporary loss of productivity. Obviously, don't include users in mission-critical roles. Your pilot users should receive training in the product and tools they will be using. They should also have a mechanism to provide feedback and report problems.

The final way to control overall deployment risk is to break things. By that, I mean find ways to intentionally introduce problems or errors into the system. If using smart cards, what happens if the card reader is broken or missing? If using one-time use tokens, what happens if clocks are out of sync? What is the effect if a network switch goes belly up? Perform your own version of white-hat hacking. Attempt to circumvent the solutions and tools you are considering deploying. If a single sign-on platform is part of your overall solution, what happens if it is offline? Many administrators neglect to test for failure, which is just as important as testing for success. This sort of failure testing can have a bonus of revealing other deficiencies that need to be addressed.

Administrator Training

Any sort of IT management tool is only as good as the administrators who use it. You cannot neglect administrator training into all aspects of your authentication solution. If you are deploying smart cards, do your administrators know how to enroll a user? Do they know how to troubleshoot authentication and access problems? Do they know how to revoke authorization? When it comes to reporting, do your administrators know how to create the reports you need? If patches or updates are required for your solution, does your staff know how to deploy them with minimal interruption to your network and users?

This type of training does not necessarily have to be formal, classroom-led instruction; although, if your vendor offers it, I suggest you at least seriously consider it for a few key administrators. Very often, these types of security upgrades require a shift in corporate culture and paradigm. You need to make sure your IT staff is onboard from the very beginning, and proper training goes a long way toward that cooperation. Well-trained staff also mitigates deployment risks, as the staff should have the knowledge to handle problems and a thorough understanding of all aspects of your strong authentication solution.

End User Training

Training your IT staff is only one half of the equation for success. If your end user population is not properly trained on all the new technologies and tools that are part of your strong authentication solution, your odds of success are greatly diminished. It is well known that people fear what they don't understand, so you must educate them.

Not only do your end users need to understand the mechanics, they should be educated as to why all this change is occurring. Again, it is human nature to resist change, and the more you can get users to understand the benefits, the better off you will be.

I would venture that this level of understanding is even greater for all levels of management within the organization. If management doesn't recognize the value and benefits, their staff won't either. Any sort of IT-related project benefits when driven from the top down.

End user training can be delivered in a variety of ways from formal classroom training, perhaps vendor-provided, to informal hands-on training sessions led by your IT staff in your own test lab. If you have the expertise in house, there are plenty of tools for creating short video tutorials and training material that can be delivered via an intranet. In fact, ask your vendors if they have any end-user–oriented training material, especially material that can be centrally delivered.

If your authentication solutions will extend to external partners, vendors, and/or users, they too will need proper training not only on mechanics but also on Help desk procedures. Ideally, you should incorporate some of these users in the pilot deployments I mentioned earlier.

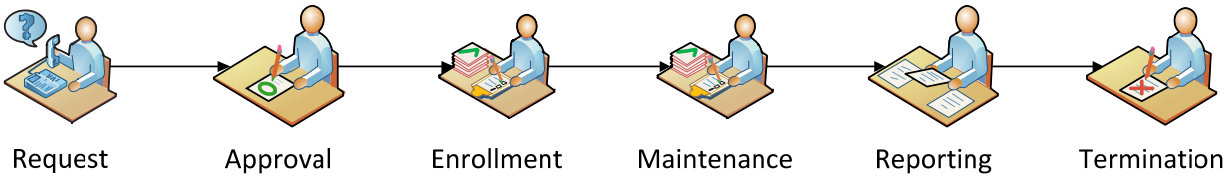
Documentation and Process

I'll admit, I'm like many of you and not a big fan of writing documentation. Unfortunately, a well-documented process is essential for maximizing your investment and achieving maximum efficiency. With a little planning, your documentation efforts can be manageable.

During your development and testing phase, you should have written procedures for setting up your solution, enrolling users, troubleshooting, revoking users, maintenance, and reporting. You need this information so that you know what to test and how to test. There's no reason this information can't rollover into your final documentation. As you are working through the pilot phase, continually update the documentation. If you can use a collaborative tool such as a wiki or even Microsoft SharePoint services, so much the better.

Ideally, your security vendors have their own product documentation that you can integrate into your own. You don't want to have to search half-dozen locations looking for information. This also applies to end-user documentation. You must offer a central location for any information or services a user might require.

In my opinion, well-defined processes and workflow are critical to a successful strong authentication implementation. By this point, you should have identified all the systems you are integrating and how they are used. I recommend defining a life cycle for each element. From a high level, you might have something like this:



Let's assume part of your strong authentication solution uses proximity detectors for physical access. Using the example workflow, you need to define how these events are accomplished:

- A new hire needs access. Who makes the request and how?
- What steps do you take to verify and approve the request? Is there an audit trail?
- Once approved, how is the user enrolled in the system? How is the card delivered to the end user?
- Is there a standard training routine for the new user?
- What is the process for a non-functioning card?
- What is the process for a non-functioning card reader?
- What is the process when the user forgets the card at home?
- What is the process for a lost card?
- What is the process when a user's job status changes and the user requires different access rights?
- What steps do you take to generate access reports? Who can request them? How is the information delivered? How long is it retained?
- What is the process when the user's employment terminates?

This level of detail, if not more, is required for every element of your strong authentication solution. Of course, you need vendor solutions that facilitate all these steps. These are also all the steps you need to define and test anyway before full-scale deployment, at which point your documentation is essentially complete. Although I'm sure you know process documentation is a continual process, which is why a centralized collaborative approach makes the most sense.

Define Reporting Requirements

The final task in your deployment and implementation plan should be to define your reporting requirements. If your organization is covered by regulatory or compliance requirements, you obviously need to meet them. If your strong authentication solution includes report "accelerators" or templates, so much the better. But this is just the beginning.

Because you have implemented an integrated and cohesive strong authentication solution across your environment, there is a wealth of information available. Different parts of your organization will have a vested interest in different parts of your data, so one of the first steps you need to define is the process of requesting information. Who can request reporting data? What data can they access? What form or forms can the data be presented? How long will it be retained? Your strong authentication solution should have a reporting facility that supports delegated permissions. You don't want your systems administrators to be a bottleneck when it comes to reporting. Ideally, you need to be able to assign appropriate reporting permissions to various users and groups as needed so that they can get the reporting they need. Here are some examples:

- The Human Resources department may need physical and file access records to document an employee termination.
- Your server administrators may want to track file access to document obsolete data that can be archived or deleted.
- Your data security team is investigating suspicious file activity and needs to determine who is accessing data, from where, and when.
- Your legal department is responding to a request to verify patient data confidentiality has not been breached.
- Management wants to trim application-licensing costs. They need to see how many people are using an application, when, and for how long.
- A manager with telecommuting employees wants to know when their staff is connecting to the office and for how long.

Once you have an integrated source of authentication and access information, you'll be amazed at how valuable the information is. As part of your search process for strong authentication, hopefully you've identified some critical reporting needs. The more flexible the reporting features, the better.

Conclusion

Putting the pieces together for a strong authentication solution is not something you will achieve in a short period of time. However, the need for strong authentication has never been greater and can actually become a business asset. The more time you take in defining your requirements, working with vendors who understand your needs and can contribute their knowledge, involving end users in your testing, and documenting processes thoroughly, the more successful your deployment and the greater the return on your investment.