

Web Access Management

Navigating Your Success

This guide provides an easy-to-follow, step-by-step methodology for navigating your way to a successfully implemented web access management solution—from planning through designing, building and integration to final implementation and training. By following the helpful navigational points and recommendations in this guide, you will stay on the path to a successful implementation.

TABLE OF CONTENTS

I. INTRODUCTION	PAGE 1
Dawn of a New Risk Era	PAGE 1
Web Access Management	PAGE 1
Gaining Valuable Assistance from RSA Professional Services	PAGE 1
II. STEP 1 – PLAN	PAGE 2
Capture Objectives and Requirements	PAGE 2
Lay the Foundation	PAGE 2
Develop the High-level Project Plan	PAGE 3
III. STEP 2 – ARCHITECT	PAGE 3
Define the Solution Architecture	PAGE 3
Develop the Implementation Roadmap	PAGE 4
IV. STEP 3 – IMPLEMENT	PAGE 4
Pilot	PAGE 4
Testing	PAGE 4
Training	PAGE 5
Deployment	PAGE 5
V. CONCLUSION	PAGE 6
About RSA Security	PAGE 6

I. INTRODUCTION

Dawn of a New Risk Era

The web browser is the center of today's universe. With a few clicks, employees can now gain entry to a vast array of corporate, partner and Internet resources. Never before has access been so ubiquitous. Never before has everything - your corporate financial data, your corporate intellectual property, your employees' and customers' sensitive information - been so accessible.

Scared yet? You should be, because today's e-business is no longer about network-enabling applications and resources. It's about managing business risk. It's about complying with an expanding set of government regulations while boosting productivity and the bottom line. And, most importantly of all, it's about controlling what your employees and others can access via those browsers. To put it another way—it's all about web access management.

Web Access Management

Web access management enforces corporate security policy compliance, protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs. How? Centralized policy management is the key. Web access management centralizes the establishment and enforcement of policies that control what users can access. More specifically, web access management translates business policies into user access rights and then enforces those rights.

Here's how it works. A web access management administrator defines the rights needed to access particular corporate resources, say the HR system's employee performance review page. The administrator makes the rights granular to match corporate policy, so each department's reviews require specific access rights. For example, Department XYZ manager group membership is required to access Department XYZ reviews. Another administrator assigns users to groups (separation of duty). When user Joe Manager attempts to access the Department XYZ review page, the web access management system intercepts the request, verifies that Joe Manager is in the Department XYZ manager group, and only then permits Joe to access the department XYZ reviews.

Web access management policies can be static, for example, based on job responsibility, or dynamic, for example, based on the user's current location. Web access management can support hybrid policies, or even policies based on external information, where the decision data resides in a separate data repository.

What else can web access management do? One of the biggest efficiency boosters is single sign on (SSO). With a web access management solution that supports SSO, users can gain transparent access across protected sites, even when they travel from the corporate site to business partners' sites. Web access management does this by authenticating the user and then creating a secured, encrypted token as proof of the authentication. The secured token travels along with the user through browser cookies, or in the case of cross-domain transversals, SAML assertions. When the destination site receives, decrypts and validates the token or assertion, it uses the token's data instead of making the user re-authenticate.

Robust web access management products, like RSA® Access Manager, implement both access control and SSO. When coupled with identity management products, like RSA® Federated Identity Manager, the result is a single, unified framework for access control and SSO that can extend across multiple companies. But truly achieving the benefits of an enterprise-wide framework for web access management is a project that encompasses broad-reaching planning, design, integration, implementation and training activities. That's where RSA Professional Services can help.

Gaining Valuable Assistance from RSA Professional Services

Throughout your web access management implementation—whether you use in-house resources or outsource the entire project—RSA Professional Services stands behind you. Professional Services provides services for every step in the web access management implementation process, drawing on broad experience in aligning technology investments with business requirements.

- Plan – Professional Services staff will help ensure that your web access management strategy is aligned with business and IT objectives.
- Architect – Professional Services works with IT, network, user communities and application owners to understand your environment. With this understanding, RSA Security can then turn your business and technical requirements into an architecture that captures the best solution for your needs.
- Pilot, test and implement – RSA Security's hands-on knowledge transfer will help you avoid potential pitfalls and implement the web access management solution as quickly and as cost-effectively as possible.
- Train – Professional Services training ensures that your staff has the knowledge it needs to operate a successful web access management solution. Web access management technology classes are offered in our classrooms or can be given onsite at your locations.

- Project management – Professional Services project managers can smooth your web access management implementation process when you leverage their lessons learned.

RSA Security tailors its services to suit your project scale and unique requirements, with your project's success as the goal. Additional guidance and recommendations to help you navigate the steps to a successful web access management implementation follow.

II. STEP 1 – PLAN

Web access management uses two main elements: RSA Access Manager agents, the front-end components that integrate with your web servers, portals or application servers to intercept access requests; and RSA Access Manager servers, the back-end components that process access requests and manage policies. If coupled with RSA® Federated Identity Manager, additional front-end and back-end elements integrate with the web access management solution. Given the mission-critical nature of web access management, you must plan the deployment carefully with your IT staff, your web applications staff and your user data repository administrators. This core team will need a good understanding of web access management, how it works and how it integrates with your existing infrastructure.

Three main activities occur during this planning step: capturing your objectives and requirements; laying the foundation for the rest of the project and developing an initial, high-level project plan.

Capture Objectives and Requirements

The first planning activity is to capture your web access management business objectives and technical requirements. This plan will form the basis for discussions about web access management throughout your organization. The format of the planning document is up to you, but you will need an executive-level version and a more detailed, working-level version. Suggested topics for this document follow.

Web access management business objectives

- Problems to be solved
- Budgets and time frames

Web access management technical requirements

- Security requirements
 - Corporate security policies for authentication, including types of authentication to be supported, cases where multiple authentication is required
 - Corporate access control policies
 - Separation of duty policies for administrators
 - Delegated administration requirements
- Application requirements
 - The number and types of applications that your web access management solution will integrate with
 - Each application's authentication requirements
 - The user community for each application
- Environment requirements
 - Web access management server platforms
 - User data repositories
 - End-user geographic locations (for server placement and load distribution)
 - Web server, portal and application server versions and platforms

Lay the Foundation

The next planning activity is to lay the foundation for the project start. Some of the actions needed for a solid project foundation are these:

- Obtain management and organizational buy in. This is where your objectives document/briefing is useful.
- Identify, select and prepare the project team members. At a minimum, your team should include:

Management sponsor. This person will receive reports of overall project status and will likely have budgetary authority over the effort.

Project manager. This is the person with day-to-day responsibility for the project.

Core team. This team will perform most of the project work. The staff members should include a security architect, a web access management solution architect and one or more web server/portal/application server specialists.

Extended team. This team supplements the core team with specialists in corporate networks, user data repositories, help-desk/end-user support and application specialists for the applications to be integrated into the web access management solution.

Stakeholder/review team. This team will review progress and issues during the project life cycle. It generally includes senior representatives from executive management, security management, IT, applications and vendors (such as RSA Security).

- Develop communications, change and risk management plans. Web access management should make web application usage simpler for users, but will introduce additional steps for application development and rollout. To ease web access management acceptance, you may want to develop a communications plan for notifying your organization of upcoming changes as well as developing change and risk management plans.
- Review network and system infrastructure capacity. The IT and corporate network specialists will help determine if your current infrastructure has enough capacity for the new web access management solution.
- Train core team members in web access management. You may want your principal team members to receive web access management training. This will help them to better understand web access management technology and how it will fit in your organization.
- Review existing or create new security policies. Web access management will provide access control and SSO capabilities that your security staff may not have considered feasible for your organization before. They may wish to update corporate security policies to encompass these new capabilities.
- Refine requirements and validate. Given the increased understanding of your organization's needs, you may wish to revise your objectives and requirements at this point. Your team members should validate these changes.

Develop the High-level Project Plan

Now that your requirements are firm, you can create your initial project plan. The project plan should outline the main solution phases. At a minimum, these should include a laboratory test phase, a QA phase and a production rollout phase. This plan will form the basis for next project phases. As with any major IT project, the plan will evolve over the course of the web access management implementation.

III. STEP 2 – ARCHITECT

The main objective of this step is to turn your requirements into a technical solution architecture and to define a detailed implementation work plan. In many cases, you will need to work with the web access management vendor to create an architecture that takes full advantage of the web access management product's capabilities. The vendor can also steer you away from potential pitfalls.

Define the Solution Architecture

The output from this step is an architecture document that captures these items:

- Detailed technical requirements, including the web access management client and server platform environment(s),
- The web access management system architecture, including both logical and physical views,
- The end-user data repository to be integrated with the web access management solution,
- The authentication methods to be used,
- The numbers and types of applications to be integrated, including the type of authentication and access policies for each application,
- Any custom integration work needed and
- An overview of operations, administration and help-desk processes needed to support the solution.

During this phase, prototyping or laboratory testing will help you evaluate the web access management technology in your specific environment. In particular, your lab should include at least one of each web server/application server/portal environment to ensure you find potential issues early in the planning process.

Develop the Implementation Roadmap

With the architectural design in hand and some laboratory testing under your belt, you can now turn your high-level project plan into a detailed implementation roadmap. Some of the work items to include in this roadmap follow.

- Creating or revising security policies for web access management –
 - Defining access policies for specific applications, user communities, or data categories and
 - Revising authentication policies to include SSO capabilities.
- Defining installation and testing work items –
 - Installing web access management servers,
 - Integrating web access management servers with user data repositories,
 - Creating test plans for development, QA and production environments,
 - Defining rollback procedures and
 - Planning user rollout phases.
- Operations and support activities –
 - Defining fail-over and recovery plans and
 - Identifying help-desk staff to support web access management
- Training –
 - Developing training materials for end-users, such as online training,
 - Planning training sessions for web access management operations staff and
 - Planning training sessions for help desk staff.
- Developing communications plans to notify the end-user community of upcoming changes.

IV. STEP 3 – IMPLEMENT

This step encompasses the broad set of activities needed to prepare for and to execute the web access management rollout. The main activities in this step are conducting one or more web access management pilots, testing and refining the solution, training operations staff and end users, and, finally, production deployment.

Pilot

A pilot lets you test your solution architecture in an operational environment, but on a controlled basis. Most organizations start with a small pilot of representative applications. The pilot activities will likely include:

- Selecting the applications,
- Installing the servers,
- Configuring the servers with the policies to be tested – for example, you will likely want to test basic access controls, applications that require multiple authentications and access policies based on dynamic or external data,
- Training the operations staff on how to install, configure and troubleshoot the web access management agent software,
- Training the help desk on potential SSO issues, particularly if identity federation is used,
- Collecting feedback – as the pilot progresses, both the end users and the web access management operations staff can provide valuable feedback on the web access management solution and
- Reviewing, revising and updating the solution based on the feedback gathered.

Options for next steps are to extend the pilot for a longer period, to increase the size of the pilot or to move into the full deployment phase.

Testing

Testing should take place throughout the pilot phase and with one or more test bed systems. Many organizations establish separate test beds for development, QA and pre-production testing. Ideally, the pre-production system should be an exact clone of your production environment so you can test changes before operational release. The test program allows evaluation of the solution in areas such as:

- Compatibility with your information system infrastructure and current end-user environments (browser types and versions, in particular),
- Validity of the production architecture,
- Additional needs for customized application integration,
- Changes to user administration processes,
- Updates for server operations processes,
- Performance under different loading scenarios and
- Accuracy of fail-over, recovery and disaster-recovery plans.

As testing proceeds, results should be fed back into the architecture document so that it accurately reflects your design. Additionally, you may need to revisit the implementation road-map to accommodate any new or revised tasks needed.

Training

Training will likely occur during several project steps. Core team members, for example, will need to be up-to-speed in web access management technology early in the project. Most of your other staff, however, will receive training shortly before the web access management solution begins deployment. This includes the IT support staff who will maintain the web access management servers, the help-desk staff who will assist end-users and the end-users themselves.

In general, you will need three different types of training:

- **Management training.** This provides a high-level introduction to web access management concepts and benefits, an overview of the web access management solution components and a summary of typical resource requirements.
- **Support staff training.** This training covers web access management administration, maintenance and support.
- **End-user training.** This training covers web access management from the end-user perspective and tells users what to expect from the system. If the changes are transparent to the user, then this may not be required.

Deployment

The web access management solution goes live in this step. If your organization is small, you may choose to transition all web applications in one phase. Most organizations, however, begin with a pilot roll-out to a small, select set of applications. After gaining experience with the pilot, they then expand web access management to the rest of the corporate applications in phases. The main activities for this step include:

- Phasing in the web access management system – the web access management solution is rolled out to the remaining applications,

YOUR PARTNER FOR SUCCESS

RSA Security offers a full complement of services for web access management, SSO, federated identity and our other security technologies. RSA Security's Professional Services teams work in partnership with you to help ensure airtight security for your entire enterprise. Our services include security planning and project management, system architecture and design, custom application engineering and implementation. Our services can provide the leadership and assistance required to make your project a success.

For additional information on any of our service offerings, please contact your RSA Security sales representative or RSA Security Professional Services directly. In the Americas:

1-877-RSA-4900; in the UK: +44 (0) 1344 781 318. |
Send e-mail to proservices@rsasecurity.com.

- Ramping up support – as the web access management solution goes live for more of the organization, your support needs may grow. This is particularly true for large organizations covering multiple geographies. Some of the support needs to consider are:

Providing 24x7 support and

Techniques for consolidating and monitoring security logs across geographies.

- Life cycle maintenance – after the web access management solution “settles in”, support needs change from initial trouble-shooting to maintenance. Some of the issues you will need to consider in this phase include:

Enabling additional applications for web access management and

Controlling web access management server revisions across geographies.

CONCLUSION

The RSA Access Manager and RSA Federated Identity Manager products help to eliminate the contradiction between “user-friendly” and “strong security policy.” RSA Security’s web access management products can reduce the authentication burden on users while increasing web access security. RSA Security web access management and federated identity solutions offers industry-leading capabilities today and, furthermore, ongoing enhancements from RSA Security’s world-class engineering organization can help meet tomorrow’s evolving needs.

Mission-critical IT infrastructure components always require thorough planning and strong technical expertise. As a key member of your project implementation team, RSA Professional Services is ready and able to provide the knowledge, business vision and resources to navigate your path to success.

About RSA Security

RSA Security is the expert in protecting online identities and digital assets. The inventor of core security technologies for the Internet, the Company leads the way in strong authentication and encryption, bringing trust to millions of user identities and the transactions that they perform. RSA Security’s portfolio of award-winning identity & access management solutions helps businesses to establish who’s who online—and what they can do.

With a strong reputation built on a 20-year history of ingenuity, leadership and proven technologies, we serve approximately 20,000 customers around the globe and interoperate with more than 1,000 technology and integration partners. For more information, please visit www.rsasecurity.com

RSA, RSA Security and *Confidence Inspired* are registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. All other products or services mentioned are trademarks of their respective owners.
©2006 RSA Security Inc. All rights reserved.

NVSCS GD 0306

