

RSA® Authentication Manager

Navigating Your Success

This guide provides an easy-to-follow, step-by-step methodology for navigating your way to a successfully implemented RSA® Authentication Manager solution. It is based on RSA Security's years of experience with authentication technology. By leveraging our lessons learned, you can smooth the implementation process.

TABLE OF CONTENTS

I. INTRODUCTION	PAGE 1
The Business Case for Strong Authentication	PAGE 1
RSA Authentication Manager Overview	PAGE 1
Steps to a Successful Authentication Manager Implementation	PAGE 1
Gaining Valuable Assistance from RSA Professional Services	PAGE 2
II. STEP 1: PLAN	PAGE 2
Capture Objectives and Requirements	PAGE 2
Lay the Foundation	PAGE 3
Develop the High-level Project Plan	PAGE 3
III. STEP 2: ARCHITECT	PAGE 4
Define the Solution Architecture	PAGE 4
Develop the Implementation Roadmap	PAGE 4
IV. STEP 3: IMPLEMENT	PAGE 5
Pilot	PAGE 5
Testing	PAGE 5
Training	PAGE 5
Deployment	PAGE 6
V. CONCLUSION	PAGE 6
About RSA Security	PAGE 6

I. INTRODUCTION

The Business Case for Strong Authentication

RSA® Authentication Manager software is the management component of the RSA SecurID® solution. They are used together to authenticate users based on two factors: something they know and something they possess. As the premier enterprise-class security solution, Authentication Manager scales to the needs of any size network and is capable of authenticating millions of users. It can protect remote dial-in sessions, VPN access (both IPSec and SSL) and e-business web applications across the enterprise. In addition, it can provide desktop authentication to the Microsoft® Windows® operating system, giving users within the enterprise the protection of two-factor authentication. RSA Authentication Manager is interoperable with more network, dial-up access, VPN and business applications than any other authentication system available today.

As the need for positive user identification and protection of valuable corporate information has increased, so has the need for an authentication solution that is a strategic, mission-critical component of an organization's network security infrastructure. RSA Authentication Manager provides this mission-critical component by scaling to support millions of users and protect multiple applications and resources across numerous physical sites.

RSA Authentication Manager Overview

- Powers strong authentication for millions of RSA SecurID end users worldwide,
- Supports millions of users and hundreds of simultaneous authentications,
- Offers high performance and scalability with database replication and multiple server configurations,
- Provides centralized, easy and cost-effective administration,
- Delivers robust logging and reporting capability and
- Interoperates with more than 290 products and applications out of the box.

RSA Authentication Manager is used to verify authentication requests and administer authentication policies for enterprise networks. Through its extensive suite of Agent software, RSA Authentication Manager is able to provide protection to users accessing computing platforms, and critical applications, from either outside or inside the corporate firewall. Agents function much like security guards, standing between the user and a protected resource or device to enforce two-factor authentication via the Authentication Manager.

RSA Authentication Manager features, such as database replication and load balancing; high-availability platform support; automated LDAP import and synchronization; and web-based configuration and user administration make RSA Authentication Manager the ideal solution for any size network that requires a robust authentication server.

In addition to Authentication Manager, RSA Security provides token management software as part of the RSA SecurID solution. The RSA Deployment Manager software is a workflow product for hardware token distribution and software seed distribution. Deployment Manager automates most business processes involved in the deployment of authenticators. It can also be used to provide end user "self service", where users can request, deploy and activate tokens from a web browser. This reduces the burden on IT for deployment of authenticators and provides significant savings in deployment time and cost.

Steps to a Successful Authentication Manager Implementation

Since authentication is a mission-critical technology, its implementation must be planned carefully. Close attention to the following steps will help ensure your project's success.

Step 1– Plan. Several planning activities must take place prior to the actual project start. First and foremost, management must buy into the project. This means that not only must senior management approve and fund the project, but the end user and application-owning communities must also agree to employ strong authentication using the RSA SecurID solution. After obtaining management approval, administrators may need to refine business objectives (e.g., budget and schedule), and clearly document the project's success factors. Other planning activities include defining the initial technical requirements and creating a high-level project plan.

Step 2 – Architect. During this step, project staff works with the Authentication Manager solution team to turn initial business and technical requirements into solution architecture. This step may include a prototype implementation to drive out potential technical issues. Early training for selected staff will ensure that these critical staff members gain a detailed understanding of the RSA SecurID technology. The result of this step should be documented in a solution architecture and a detailed project plan.

Step 3 – Implement. This step encompasses the suite of roll-out preparation and deployment activities, including:

Pilot and test. A pilot lets administrators try out the solution with a selected user community in an environment that simulates the production environment on a limited basis. Any operational issues should surface here. As administrators work through these issues, the implementation can be iteratively tested and refined until ready for full deployment.

Train. RSA Authentication Manager training will be needed the help desk staff who support users and the system administrators who operate the Authentication Manager servers.

Communicate. Because the RSA SecurID solution will impact end users directly, communication to the end user community is critical for ensuring a successful deployment.

Deploy. Full-scale operations begin in this step, as the operational Authentication Manager system goes into wide production. RSA Security recommends that organizations phase in RSA SecurID capabilities to allow settling-in time for users, application administrators, help desk staff and system administrators.

Gaining Valuable Assistance from RSA Professional Services

Throughout the solution implementation—whether using in-house resources or out-sourcing the entire project—RSA Professional Services stands behind you. RSA Professional Services provides services for every critical step in the implementation, drawing on the Company’s broad experience in aligning technology investments with business requirements.

Plan. RSA Professional Services staff will help ensure that the strong authentication strategy is aligned with business and IT objectives.

Architect. We work with an organization’s IT, network, user communities, and application owners to understand the environment. With this understanding, RSA Security can then turn business and technical requirements into a solution architecture that captures the best solution for that organization.

Pilot, test and implement. RSA Security’s hands-on knowledge transfer will help administrators avoid potential pitfalls and implement the authentication solution as quickly and as cost effectively as possible.

Train. RSA Security’s training organization ensures that your staff has the knowledge it needs to have a successful RSA SecurID solution. RSA Authentication Manager installation and administration classes are offered in our classrooms or can be given on-site.

Project management. RSA Security’s project managers can smooth the Authentication Manager implementation process when you leverage their lessons learned.

RSA Security tailors its services to suit your unique requirements and the scale of the project. The Authentication Manager project’s success is our goal. Following are additional guidance and recommendations to help navigate each of the implementation steps.

II. STEP 1 – PLAN

Authentication Manager requires the integration of IT, network, desktop, application, and security technologies. Given the mission-critical nature of the Authentication Manager solution, planning activities will require a team of experts spanning these areas. Generally, this means a cross-organizational team. This core team must have a good understanding of RSA SecurID and how it works.

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

Capture Objectives and Requirements

The first planning activity is to capture objectives and technical requirements in a document. This document will form the basis for discussions about Authentication Manager throughout your organization. The document format is up to you, but there will need to be an executive-level version and a more detailed, working-level version. Suggested topics for this document follow.

Strong authentication business objectives

- Problems to be solved,
- Provisioning and token deployment needs and
- Budgets and time frame.

Authentication Manager technical requirements

- Security requirements:
 - Corporate security policies for authentication.
 - Authentication methods to be supported:
 - Local, Domain, Remote, Wireless LAN and Terminal services.
- Application requirements:
 - The number and types of applications that your Authentication Manager solution will encompass,
 - Each application's authentication requirements and
 - The number and types users to challenge.
- Environment requirements:
 - Desktop and server platforms,
 - User data repositories and
 - End user geographic locations.
- User registration:
 - Manual,
 - Directory synchronization and
 - Self registration via RSA Deployment Manager.

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:

- Obtain management and organizational buy-in. This is where your objectives/requirements document 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 should include a security architect, an Authentication Manager solution architect, a user administration specialist and a desktop environment specialist.

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 Authentication Manager 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 and change management plans. Authentication Manager may affect most or all of your end users. To ease the introduction of the new system, you should develop a communications plan for notifying your end user organization of the upcoming changes.
- Review network and system infrastructure capacity. The IT and corporate network specialists will help determine if the current infrastructure has enough capacity for the Authentication Manager solution.
- Train core team members in Authentication Manager. You may want principal team members to receive Authentication Manager training. This will help them to better understand the technology and how it will fit in your organization.
- Review existing or create new security policies. Authentication Manager will provide authentication capabilities that your security staff may not have considered feasible before. They may wish to understand possible effects to existing security policies to accommodate the 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. Team members should validate these changes.

Develop the high-level project plan

Now that the requirements are firm, you can create an 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 roll-out phase. This plan will form the basis for the next project phases. As with any major IT project, the plan will evolve over the course of the Authentication Manager implementation.

III. STEP 2 – ARCHITECT

The main objective of this step is to turn the requirements into a technical solution architecture and to define a detailed implementation work plan. In many cases, you will need to work with the RSA Authentication Manager vendor to create an architecture that takes full advantage of the 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 for the Authentication Manager:
 - Availability and disaster recovery,
 - Trust relationships and
 - Numbers and types of agents.
- The Authentication Manager system architecture, including both logical and physical views.
- The end user data repository for the Authentication Manager solution:
 - Integration requirements and
 - Maintaining synchronization.
- The token provisioning methods to be used.
- The numbers and types of applications to be integrated, including the type of authentication for each application.
- Any custom integration work needed.
- 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 Authentication Manager technology in your specific environment. In particular, your lab should include at least one of each end user desktop and/or business application environment to ensure that potential issues are found early in the planning process.

Develop the Implementation Roadmap

With the architectural design in hand and some laboratory testing completed, you can now turn the high-level project plan into a detailed implementation roadmap. Some of the work items to include in the roadmap are as follows:

- Creating or revising security policies for strong authentication:
 - Defining authentication methods for specific applications and
 - Defining emergency access procedures for users who lose their authenticators.
- Defining installation work items:
 - Installing Authentication Manager servers,
 - Integrating Authentication Manager servers with user data repositories,
 - Installation of the RSA Deployment Manager software and its integration with the user data repository,
 - Creating test plans for development, QA and production environments,
 - Defining roll-back procedures and
 - Planning user roll-out and authenticator deployment phases.
- Operations and support activities:
 - Defining fail-over and recovery plans and
 - Identifying help desk staff to support the RSA SecurID solution.
- Training:
 - Developing training materials, such as online training, for end users,
 - Planning training sessions for 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 roll-out. The main activities in this step are conducting one or more Authentication Manager pilots, testing and refining the solution, training operations staff and end users, and, finally, production deployment.

Pilot

A pilot allows testing your solution architecture in an operational environment, but on a controlled basis. Most organizations start with a small pilot of selected end users and a limited set of representative applications. The pilot activities will likely include:

- Select the end users and applications for the pilot.
- Install the pilot servers.
- Configure the pilot servers with the policies to be tested. For example, testing PIN rules, emergency access methods and authentication to selected applications are possibilities.
- Create the Authentication Manager Agent installation packages.
- Train the pilot users on how to authenticate using the Authentication Manager software.
- Deploy the agent installation packages, including the end user desktop agent (if RSA SecurID for Microsoft® Windows® is being implemented).
- Implement the token deployment process for use with the pilot users.
- Collect feedback. As the pilot progresses, both the end users and the Authentication Manager operations staff can provide valuable feedback on the solution.
- Review and revise the solution. Based on the feedback gathered, update the Authentication Manager solution architecture.

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 your 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 changes may be tested 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,
- Validity of the production architecture,
- Additional needs for customized agent 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, the results should be fed back into the architecture document so that it accurately reflects your design. Additionally, you may need to revisit your implementation roadmap to accommodate any new or revised tasks.

Training

Training will likely occur during several project steps. Core team members, for example, need to be up-to-speed in Authentication Manager technology early in the project. Most other staff, however, may receive training shortly before the solution begins deployment. This includes the IT support staff who will maintain the Authentication Manager servers, the help-desk staff who 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 Authentication Manager concepts and benefits; an overview of the solution components and a summary of typical resource requirements.
- Support staff training. This training covers administration, maintenance and support.
- End user training. This training covers the use of Authentication Manager Agents for strong authentication from the end user perspective and gives users how-to instruction for using their RSA SecurID token with the Authentication Manager solution.

Deployment

The Authentication Manager solution goes live in this step. If the organization is small, you may choose to transition all end users in one phase. Most organizations, however, begin with a pilot roll-out to a small, select community in a common geography or a single application (as described above). After gaining experience during the pilot, they then introduce Authentication Manager to the rest of the company in phases.

The main activities for this step:

- Phasing in the Authentication Manager system. The Authentication Manager solution is rolled out to the rest of the organization.
- Rolling up support. As the Authentication Manager solution goes live for more of the organization, 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,
 - Techniques for consolidating and monitoring security logs across geographies and
 - Emergency access for different user communities.
- Life cycle maintenance. After the Authentication Manager solution “settles in”, support needs change from initial troubleshooting to maintenance. Some of the issues you will need to consider in this phase:
 - Controlling Authentication Manager server revisions across geographies,
 - Controlling the versions of and the deployment of Authentication Manager agents to additional devices or web applications and
 - Managing the life cycle of the deployed authenticators.

V. CONCLUSION

RSA Authentication Manager software helps enterprises implement a strong authentication policy. The RSA SecurID time-synchronous token solution can greatly reduce attacks (phishing and man-in-the-middle) which capitalize on weak user name-and-password authentication techniques. Furthermore, the RSA Authentication Manager solution offers industry-leading capabilities today and on-going enhancements from RSA Security’s world-class engineering organization to meet future 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 pave the 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 more than 18,000 customers around the globe and interoperate with more than 1,000 technology and integration partners. For more information, please visit www.rsasecurity.com

RSA PROFESSIONAL SERVICES—YOUR PARTNER FOR SUCCESS

RSA Security offers a full complement of services for enterprise provisioning and user management and our other security technologies. RSA 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. As outlined below, our services can provide the leadership and assistance required to make your project a success.

Planning services

- Enterprise provisioning and user management business goals assessment
- Pilot and production roll-out plans, including implementation work breakdown structures

Architecture development services

- Operational and end user support design
- Logical and physical enterprise provisioning and user management system design
- Design of provisioning and user management application integration customizations

Implementation services

- Provisioning and user management deployment in test bed, pilot and production systems

- Provisioning and user management component installation, configuration and integration
- Application integration into the Provisioning and User Management solution
- Testing support during key implementation phases
- Training
 - Operations
 - Administrators
 - Software developers

- Deployment assistance for test beds, pilots and production roll-outs

Project Management

- Monitoring, measuring and reporting project progress
- Change control and risk management
- Vendor and cross-organizational resource coordination

For additional information on any of our service offerings, please contact your RSA Security sales representative or RSA 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.



RSA Security Inc.
www.rsasecurity.com

RSA Security Ireland Limited
www.rsasecurity.ie

©2005 RSA Security Inc. All Rights Reserved

RSA, RSA Security, the RSA logo, SecurID and *Confidence Inspired* are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other products and services mentioned are trademarks of their respective companies.

SIDNAV GD 0905