

Migration to RSA® Authentication Manager 7.1

How RSA Professional Services Can Help

Authentication and identity assurance has become a necessary element of all enterprise security initiatives. And as organizations continue to increase the number of applications on the network and provide more users with access, the need to protect access to that information is critical.

Two-factor authentication has become the gold standard for securing access. First, it is inexpensive to operate and allows organizations to evaluate and select from a diverse set of form factors depending on their budget and the needs of users. Second, it is a portable solution that provides users with “anytime anywhere access.” Finally, and most important, it offers strong security on a much higher level than password authentication alone in order to prevent unauthorized access.

RSA has been providing strong authentication solutions to organizations around the world for over 20 years. Today, RSA SecurID® two-factor authentication provides tens of millions of users with secure access to virtual private networks (VPNs), wireless access points, remote access firewalls, web applications and network operating systems.

Realizing the Benefits of Authentication Manager 7.1

In the same way customers have come to rely on RSA SecurID and RSA® Authentication Manager to protect access and assure user identities, they have come to rely on RSA Professional Services to help realize the benefits of the RSA SecurID solution while reducing the risks often associated with new technology initiatives. Here is how RSA Professional Services can help organizations make a successful migration and realize the benefits of the Authentication Manager 7.1 platform:

1. In the process of a software/infrastructure upgrade, a new hardware environment (hardware upgrade) is often desired or required. This usually consists of a new host name and IP address which will have a definite impact on the device agents within the environment. RSA Professional Services has the skill and knowledge for creating a proper agent migration plan to minimize downtime and end user interruption.
2. Authentication Manager 7.1 has introduced server nodes (server clusters) that can supplement Authentication Manager Primary and Replica instances; up to three additional server nodes per instance. This may result in a change in a customer’s Authentication Manager infrastructure that is more desirable resulting in fewer Replica instances which were initially implemented to increase performance and availability. Another infrastructure change may consist of merging multiple Authentication Manager realms into one as this is managed much better under Authentication Manager 7.1. RSA Professional Services can assist in defining the best Authentication Manager architecture for their organization.
3. Authentication Manager 7.1 has a new and improved Java™-based administrative API (toolkit) designed to interface with the new Authentication Manager architecture components. Customers that have utilized the Authentication Manager administrative API from previous versions of Authentication Manager 7.1 within their environment (scripts/ applications) will require rewriting applications or scripts with the new set of APIs. This applies to all custom administrative applications built using:





- Version 6.1 and prior administrative API
- Custom Java Admin API (PsoAceAdmin)
- ACE BULK ADMIN (ABA)

RSA Professional Services has extensive experience in creating custom solutions (including custom reports) and can help design a structure that meets the needs of your organization.

4. Prior to Authentication Manager version 7, obtaining user data from a directory services was accomplished through scheduled LDAP synchronizations jobs (non-real-time). Authentication Manager 7.1 supports native LDAP connections (real-time directory information), which tightly couples the SecurID solution to the organization's infrastructure. This feature greatly enhances capabilities such as delegated administration and access controls based on organizational structure. RSA Professional Services can assist in a migration to leverage your directory service structure to better meet your business needs.

5. Authentication Manager 7.1 has a revised Administrative Model consisting of the following roles:

- | | |
|---------------------------------|--|
| - Super admin | - Privileged help desk administrator 7.1 migration |
| - Realm administrator | - Agent administrator |
| - Security domain administrator | - RADIUS administrator |
| - User administrator | - Trusted administrator |
| - Token administrator | - Request approver |
| | - Token distributor |

A migration can affect the administrative capabilities of some administrators from the previous environment. RSA Professional Services will work with customers to leverage and configure these roles (scope, capabilities and privileges) to ensure the most desirable business work flow.

6. Authentication Manager 7.1 now offers a new token provisioning and self-service application called Credential Manager. As a result of the close integration with Authentication Manager, there is no migration path from RSA Deployment Manager / Web Express 1.x (previous token provision and self-service application for version 6.1 and prior) to Credential Manager. RSA Professional Services can assist customers that are presently utilizing Deployment Manager or a customized version of Deployment Manager to develop a migration plan and provide implementation support to ensure a smooth transition.

7. Legacy Agent Hosts are agents implemented for SecurID technology prior to RSA Authentication Manager version 5 (A.K.A. RSA ACE/Server®) utilizing a different protocol. Authentication Manager 7.1 no longer supports legacy Host Agents and an alternative agent solution is required. RSA Professional Services can define the needs of your organization – whether it be as simple as a device upgrade or a new access control mechanism – in order to minimize end user impact.

Solid Security Requires More than Just Technology

Great technology isn't always enough. Sometimes, having world-class expertise to guide solution strategy, design, implementation and management is essential to ensuring your organization receives the most value from its investment in RSA SecurID technology. Here is how RSA Professional Services helps organizations to achieve that success:

- **Proven experience.** RSA offers proven experience in deploying RSA authentication solutions for organizations across the globe. By utilizing RSA Professional Services, customers ensure their authentication infrastructure is architected using RSA and industry best practices in support of business requirements.
- **Minimize risk.** RSA Professional Services can help minimize risk, the duration of the implementation phase and any downtime associated with upgrading their RSA SecurID environment to the newest available release.
- **Proactive.** As a result of the significant change in Authentication Manager 7.1 architecture, a planned migration is a very good opportunity to consider a "health check" of the complete SecurID infrastructure as well as a customer's strong authentication requirements, strategy and policies.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

©2009 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, ACE/Server, SecurID and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.