RSA | carahsoft.

A Quick Introduction to Authentication Manager for Moonshot Customers

RSA has a wealth of identity solutions and it can sometimes be difficult to determine exactly what your organization needs. For those looking for the classic deployment of Authentication Manager RSA provides a detailed comprehensive planning guide. The most recent is “RSA Authentication Manager 8.7 Planning Guide” and is available for your review.

In this introduction we quickly review the basics of an Authentication Manager deployment to help you better understand the details addressed in the quick guide above. In brackets, [], will be references to specific pages in this document.

The main function of Authentication Manager enables user authentication to various resources using RSA’s hardware (or software) time-based one-time password tokens. The current version of RSA’s hardware token is the SID700. There is also a software version of this token available for mobile devices, but you will probably not use this. The SID700 displays a set of digits, a tokencode, that change every 30 or 60 seconds. These digits are a function of a secret called a “seed” and “time”. A user is typically provided a PIN (Personal Identification Number) as well, making our solution two-factor. [See page 8, RSA SecurID Tokens]

When a user authenticates to a protected resource they provide their PIN and tokencode to an RSA Agent that sits in front of that resource. The Agent communicates with the Authentication Manager where it uses its copy of the user’s seed to validate the authentication request. If the validation is successful the user is granted access.

When planning an Authentication Manager deployment one of the first things you should do is determine what resources you are protecting. RSA provides agents to enable authentication to a large number of resources. For some of these you will have to install and configure the agents (e.g. a Windows or Linux desktop). In other situations, one of RSA’s partners will have already integrated our agent (e.g. a Cisco VPN). [See page 13, Authentication Agent]

Next you need to identify where your user data, or identity store is located. RSA Authentication Manager has an internal identity store that you can use directly, but usually customers connect Authentication Manager to Active Directory or some other LDAP.

Finally, you need to determine how to deploy Authentication Manager from a form factor, disaster recovery and availability perspective. Authentication Manager is available as a hardware appliance and a virtual appliance. The virtual appliances are available for VMware and Microsoft hypervisors as well as for AWS and Azure clouds. We have been talking about Authentication Manager as if it were a single server, but you can deploy up to 14 Authentication Managers to handle the projected workload and to provide failover. RSA refers to deployment of one or more Authentication Managers as a Realm. In a Realm there must be one Primary server with the remaining servers being referred to as Replicas. All user provisioning, agent configuration and other administrative roles are done on the Primary Authentication Manager which then propagates that information to the Replicas. Since Replicas are identical to the Primary in all aspects except the role they are assigned, it is possible to promote a Replica at any time to replace a Primary if it goes down. This provides the failover mentioned above. [See page 14, Appliance Support]

To pull this together, take a look at the diagram in “RSA network diagram –simplev2.pdf”. This diagram represents a common deployment of Authentication Manager to support a local and remote data center. Note that the two data centers have network access. So, the Primary Authentication Manager is located in the local data center with one replica, while two replicas in the remote data center support all authentication requests there. Each of these Authentication Managers, both primary and replicas, is linked to an LDAP identity repository via secure SSL. In both data centers the Authentication Manager deployment provides MFA to Windows and Linux Servers as well as the Cisco ISE network management solution. To manage this deployment there are three RSA Authentication Manager admin roles. The SuperAdmin is a highly sensitive account, closely guarded and protect, that allows an administrator to implement the most sensitive administrative actions as well as all actions available to other classes of administrators. The Help Desk Administrator address user concerns such as lost tokens and forgotten PINs. The Operations Admin maintains the health of the Authentication Manager infrastructure and in this diagram also has the role of provisioning new users.

There is lot more about Authentication Manager that we could discuss here, but this should give you the information you need to start planning your deployment. Again, refer to the Planning Guide for more detailed information.
RSA looks forward to working with you.