RSA Authentication Manager 5.2 and 6.1 Security Best Practices Guide

Version5

Contact Information

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: **www.rsa.com**.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation ("EMC") in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**.

License Agreement

The guide and any part thereof is proprietary and confidential to EMC and is provided only for internal use by licensee. Licensee may make copies only in accordance with such use and with the inclusion of the copyright notice below. The guide and any copies thereof may not be provided or otherwise made available to any other person.

No title to or ownership of the guide or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of the guide may be subject to civil and/or criminal liability.

The guide is subject to update without notice and should not be construed as a commitment by EMC.

Note on Encryption Technologies

The referenced product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting the referenced product.

Distribution

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Disclaimer

EMC does not make any commitment with respect to the software outside of the applicable license agreement.

EMC believes the information in this publication is accurate as of its publication date. EMC disclaims any obligation to update after the date hereof. The information is subject to update without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED TO SUGGEST BEST PRACTICES, IS PROVIDED "AS IS," AND SHALL NOT BE CONSIDERED PRODUCT DOCUMENTATION OR SPECIFICATIONS UNDER THE TERMS OF ANY LICENSE OR SIMILAR AGREEMENT. EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

All references to "EMC" shall mean EMC and its direct and indirect wholly-owned subsidiaries, including RSA Security LLC.

November 2011

Revision History

Revision Number	Date	Section	Revision
1	March 17, 2011		Version 1
2	March 21, 2011	Critical Sections	New section with links to important areas of the document.
		Immediately After Setup	• New information on disabling local host mode administration. • New section for recommendations on password policies.
		Protecting Tokens	Recommendations on PINless tokens.
		System Hardening and Deployment Considerations	New recommendations on Authentication Manager self-service policies and access.
		Using a Firewall	New recommendation on using software and hardware firewalls.
		Preventing Social Engineering Attacks	New reminder that users should be familiar with the Help Desk phone number.
		PIN Management	• Revised recommendations for configuring PIN policies. • Note on issue when changing short PINs to 8-digit PINs and new PIN mode. • New recommendation on using 4-character PINs. • New description of the potential impact of changing PIN policies. • New recommendation on lockout policy. • New recommendation on using system-generated PINs with RADIUS PAP.
		Customer Support Information	New list of Customer Support phone numbers.

3	April 8, 2011	• Protecting Tokens • Monitoring Authentication Manager • PIN Management • Emergency Access and Static Passwords	New links to Knowledgebase articles that provide procedures related to the recommendations.
		PINless Tokens	New section of recommendations for using PINless tokens.
		Distributing Software Tokens	Added information about using default settings when issuing software tokens.
		Protecting Authentication Manager Environment	Added a note about securing test environments.
		Preventing Social Engineering Attacks	New recommendations about Help Desk administrators interacting with users.
		Confirming A User's Identity	New section for Help Desk administrators describing methods of confirming a user's identity.
		PIN Management	• Reprioritized the list of recommendations. • New recommendations about changing PIN policy and the effect on Help Desk calls.
4	July 28, 2011	Masking Token Serial Numbers Displayed in Log messages	New recommendation and description of the new functionality that allows administrators to restrict the inclusion of token serial numbers in logs.
5	November 2011	Preventing Social Engineering Attacks	Additional information about resynchronizing tokens.
		PIN Management	New note to restart the server after making changes to PIN policies.

Critical Sections

Protecting the Authentication Manager Environment: Page 10

Protecting Sensitive Data: Page 14

Preventing Social Engineering Attacks: Page 16

PIN Management: Page 17

Introduction

This guide is intended to help identify configuration options and best practices designed to help ensure correct operation of RSA® Authentication Manager 5.2 and 6.1, and offer maintenance recommendations. However, it is up to you to ensure the products are properly monitored and maintained when implemented on your network, and to develop appropriate corporate policies regarding administrator access and auditing.

RSA periodically assesses and improves all product documentation. Please check RSA SecurCare® Online (SCOL) for the latest documentation. When deploying software tokens, use this guide in conjunction with your software token documentation and the *RSA SecurID Software Token Best Practices Guide*.

In addition to the recommendations in this best practices document, RSA strongly recommends that you follow industry best practices for hardening the network infrastructure, such as keeping up with the latest operating system patches, segmenting your network and monitoring your network for intrusions.

Important: All references to Authentication Manager also apply to RSA SecurID Appliance 2.0.

Immediately After Setup

Log on to Authentication Manager locally, set up an RSA SecurID-protected Administrator account that you can use to perform the rest of the initial setup using Authentication Manager in remote mode. After configuring the Authentication Manager for remote administration, disable local host mode on the Authentication Manager system. Instead, manage the Authentication Manager from a machine running the Remote Administration application.

To disable local host mode, add one or more administrators in addition to the administrator who installed Authentication Manager and enable them for RSA SecurID tokens. Then delete the account of the administrator who installed Authentication Manager.

During installation, a single Authentication Manager administrator account is created. By default, RSA Authentication Manager is configured to allow remote administration.

Immediately after accessing the Database Administration application for the first time, RSA strongly recommends that you do the following:

- Create a user record for yourself and assign administrator privileges and an RSA SecurID token to it.
- Verify that the System Parameters require RSA SecurID Cards and Fobs for authentication of remote administrator accounts.
- Install the remote database administration software on a secure Windows-based machine.

Protecting Tokens

Importing new tokens and distributing tokens to users are sensitive operations and if not done properly could expose an organization to security risks. Below is a list of recommendations designed to minimize risk during these sensitive operations.

Important: RSA strongly recommends that you do not assign more than one token to a user as this may reduce the likelihood that users will report a lost or stolen token.

For information about determining which users have PINless tokens, see the Knowledgebase article: **a54307 - Identify all Tokencode-Only (PINless) tokens**.

PINless Tokens

If you use PINless RSA SecurID tokens (also known as Tokencode Only), you should immediately ensure that a second authentication factor, such as a Windows password, is required to authenticate to protected systems.

Important: If the system does not have a second factor and one cannot be implemented, RSA strongly recommends switching your RSA SecurID tokens to require a PIN immediately. If you cannot switch all tokens to require a PIN, RSA strongly recommends auditing agents on systems that do not require a second authentication factor for PINless token users.

- Implement help desk procedures that ensure that administrators:
    - allow a user to authenticate with a PINless token only when the user requires access to systems that enforce an additional authentication factor.
    - allow a user to authenticate with a PINless token only when there is a second authentication factor required on every system the user may access.
    - flag groups that contain users with PINless tokens to ensure that these groups are enabled only on agents that protect systems that require a second authentication factor.
    - flag users of PINless tokens to ensure that these users are enabled only on agents that protect systems that require a second authentication factor.
- If you use PINless tokens, RSA strongly recommends that the audit trails of the following administrative activities be carefully monitored:
    - agent creation
    - group creation and assignment
    - group membership changes
    - token assignment
    - PINless token enablement

Protecting Token Files

RSA Manufacturing or certified partners deliver token files for import into your systems. These files enable the use of strong authentication, and they contain sensitive information about tokens. RSA strongly recommends the following best practices:

- Limit access to these files to individuals responsible for the import of tokens into Authentication Manager.
- Store backup copies of Token XML files in a secure location, preferably encrypted in a secure location with no network connectivity.
- Files used for the import operation should be permanently deleted from the file system when the import operation is complete. If you use multiple systems as temporary storage locations, immediately delete the token files from the temporary location as soon as you copy it.
- Secure any media used to deliver token information to you.

Masking Token Serial Numbers Displayed in Log Messages

For Authentication Manager 6.1 installations, RSA strongly recommends that you install RSA Authentication Manager 6.1.2 Hot Fix 239 to enhance protection of your token serial numbers.

The hot fix is designed to allow you to mask part of the token serial number in log data that is sent over the network. This capability helps ensure that any log data sent in the clear over a non-secured network that has Windows Event Logging or Automated Log Maintenance configured follows RSA Authentication Manager Best Practices. You can configure how many token serial number digits to display in the log message.

Masked digits display as the 'x' character. The masked digits are always at the beginning of the serial number, while the exposed digits are always at the end. For example, if you configure token serial number masking to include 4 digits, the number displays as xxxxxxxx7056.

For information about how to configure token serial number masking, see the RSA Authentication Manager 6.1.2 Hot Fix 239 Readme.

Distributing Hardware Tokens

RSA strongly recommends that you take the following steps to protect your hardware tokens:

- Distribute Hardware Tokens in a disabled state. Before enabling a token, Help Desk administrators should perform an action to confirm the user’s identity. For example, ask the user one or more questions to which only he or she knows the answer.
- Do not record the user’s serial number outside the Authentication Manager server.

See “Preventing Social Engineering Attacks” on page 16.

Distributing Software Tokens

RSA strongly recommends that you take the following steps to protect your software tokens:

- When generating the token files for distribution, protect the files with a password, which encrypts the file. Use passwords that conform to industry best practices.
- Use the Authentication Manager Database Administration application to bind software tokens to device IDs when issuing software tokens. This limits the installation of tokens to only those machines that match the binding information. See your Authentication Manager documentation.
- By default, the software token seed is securely randomized when the token is issued so that the previous seed is no longer valid. To ensure the default setting is always used, make sure "Retain Token Info" is disabled before issuing a software token.

Handling Lost Tokens

When a user reports a lost token, RSA strongly recommends that you take the following steps:

- Help Desk administrators should perform an action to confirm the user’s identity. For example, ask the user one or more questions to which only he or she knows the answer to verify their identity.
- Ask the user when they lost the token.
- Disable the token.
- Make note of the date and audit your logs for authentication attempts with the lost token until the token is recovered. Follow your organization’s security policy to address any suspicious authentication attempts.

Protecting the Authentication Manager Environment

It is very important to protect all physical, local and remote access to the Authentication Manager environment, including the Authentication Manager server, the database server, and Agent hosts. It is also very important to restrict all access methods to the bare minimum required to maintain Authentication Manager.

Note: RSA strongly recommends that your Authentication Manager test environments not be exact copies of your full production environment. If they are, you should take the same precautions to protect the test environment as you do your production environment.

Physical Security Controls

Physical security controls enable the added protection of resources against unauthorized physical access and physical tampering. Authentication Manager is designed to be a critical infrastructure component so it is very important that physical access be restricted to authorized personnel only. After installation, authorized users only need limited access to Authentication Manager and its operating system instance.

While following your organization's security policy, RSA strongly recommends the following physical security controls:

- Allow only authorized users to physically access Authentication Manager. After installation, authorized users only need limited access to Authentication Manager systems and components.
  - Access to systems hosting Authentication Manager or its components should be physically secured, for example, in cabinets with tamper-evident physical locks, audited on-site access.
  - Secure the server room such that it's only accessible by authorized personnel and audit that access.
  - Use room locks that allow traceability and auditing.
  - Minimize the number of people who have physical access to devices hosting Authentication Manager server, agents, and instances of the Administration Toolkit (ATK).
- Employ strong access control and intrusion detection mechanisms where the product cabling, switches, servers, and storage hardware reside.
- Place tamper evident stickers on each server chassis and other hardware.

Remote Access to Server Environments

- Remote access to server system components should be limited, at a minimum using the following approaches:
  - Disable remote access methods for the operating system, for example telnet or ftp, that communicate over unsecured channels.
  - Disable any other remote access method for the operating system, for example SSH, unless absolutely required for maintenance. Disable immediately when maintenance is complete.
- Remote access to any host or system connected to or managed by Authentication Manager, for example, hosts with Agents installed, should be limited as indicated above.
- Properly scope administrators to limit the sites and groups they can manage based on your corporate policies for their role and position.
- Minimize the use of realm administrators.
- Change the administrator authentication methods to require RSA SecurID Cards and Fobs for authentication of remote administrator accounts.

System Hardening and Deployment Considerations

To help ensure the highest level of security and reduce the risk of intrusion or malicious system or data access, RSA strongly recommends that you follow industry best practices for hardening the network infrastructure, including without limitation:

- Run anti-virus and anti-malware tools with the most current definition files.
- Do not directly connect Authentication Manager servers to the Internet or place them in a De-Militarized Zone (DMZ).
- Do not co-host Authentication Manager on the same operating system instance with other software.
- Examine your self-service policies and consider hardening self-service access and functionality.
  - Limit access to Deployment Manager only to users inside your corporate network.
  - RSA strongly recommends that you do not allow users to clear their PIN with Deployment Manager. Users that must clear their PIN should contact the Help Desk.
- On UNIX systems, run Authentication Manager under its own service account and restrict access to its files to that service account. This cannot be changed after installation.

Using a Firewall

It is important to restrict network traffic between Authentication Manager services and external systems.

- RSA strongly recommends that customers utilize firewalls designed to remove unnecessary network access to Authentication Manager, and follow network security best practices.
- For information about port usage, see the *Authentication Manager Installation Guide*, and only allow inbound and outbound traffic on the documented ports to reach Authentication Manager.
- RSA also recommends that customers use a software firewall on the Authentication Manager server and segment Authentication Manager network with a hardware firewall.

Ongoing Monitoring & Auditing

As with any critical infrastructure component, you should constantly monitor your system and perform periodic and random audits (configuration, permissions, and so on).

Configuration Settings and Roles

At a minimum, you should review that the following settings match company policy and functional needs:

- Configuration Settings
- Administrators and their task lists and scope
- Agent Host enabled lists

Monitoring Authentication Manager

RSA strongly recommends the following:

- Run network intrusion detection systems and host intrusion detection systems in your environment.
- Be sure to monitor which ports are open. For information about port usage, see the *Authentication Manager Installation Guide*.
- Audit and analyze system and application logs periodically. You can use Security Information and Event Management to help you with this task.

  For information about the SNMP Plug-in for RSA SecurID Appliance 2.0, see the following Knowledgebase article: **a54310 - How to obtain SecurID log messages from Appliance 2.0**.

  For information about using RSA enVision for alerts, and for the collection and analysis of data, see the following Knowledgebase article: **https://knowledge.rsasecurity.com/docs/rsa_env/device_config/RSAAuthManager.pdf**.
- Retain log data in compliance with your security policies and local laws.

For information about methods of monitoring the Authentication Manager, see the following Knowledgebase articles:

- **a54309 – How to send SecurID logs to syslog for monitoring**
- **a54300 - Use Custom Query to capture security-related audit log messages**

Secure Maintenance

Always apply the latest security patches for RSA Authentication Manager, which are available from RSA on RSA SecureCare Online (SCOL).

Security Patch Management

All security patches for RSA products originate at RSA and are available for download as an update as long as you have a current maintenance agreement in place with RSA. Updates are available on RSA SecurCare Online at **https://knowledge.rsasecurity.com**. RSA strongly recommends that you immediately register your product and sign up for RSA SecurCare Online Notes & Security Advisories, which RSA distributes via e-mail to bring attention to important security information for the affected RSA products. RSA strongly recommends that all customers determine the applicability of this information to their individual situations and take appropriate action.

If you want to receive or change which RSA product family Notes & Security Advisories you currently receive, log on to RSA SecurCare Online at **https://knowledge.rsasecurity.com/scolcms/mysupport.aspx**.

When you apply an update, first apply it on the primary system, and then apply it on the replica systems.

RSA strongly recommends that customers follow best practices for patch management and regularly review available patches for all software on systems hosting Authentication Manager, including anti-virus and anti-malware software, and operating system software.

Note: Apply patches to embedded third-party products only as part of RSA-delivered patches. For example, all patches to the embedded Progress database must come from RSA. Any required but not embedded third party components for software form factor should be patched according to the vendor specific recommendations.

For more information, see your RSA SecurID Appliance or Authentication Manager documentation.

Protecting Sensitive Data

Sensitive Files

Consider keeping an encrypted copy of the following data offline in a secure physical location, such as a locked safe, in accordance with your disaster recovery and business continuity policies:

- Authentication Manager license files (sdti.cer, server.cer, server.key, and license.rec)
- Backup data
- Authentication Manager passwords
- Archived log files and report data

To help protect online data, such as current log files and configuration files, restrict access to the files and configure file permissions so that only trusted administrators are allowed to access them.

Backups

Most sensitive data stored in a backup, such as user PINs, is encrypted. However, other sensitive data such as token serial number and token assignments are not. For this reason you must take the following steps to protect your backup data:

- When creating Appliance backups, generate the backup to the local file system. When moving it to a remote system, use a secure tool to perform the data transfer.
- Encrypt your backups, especially when containing software tokens. Protect the encryption key in a secure location, such as a safe.

LDAP Synchronization

LDAP systems hold sensitive data that Authentication Manager frequently accesses. Take the following steps designed to increase the security of this flow of information:

- Use SSL to communicate with all directory servers.
- Regularly change the password for the accounts that connect to your LDAP. The password is specified as the password for the Binding DN in your LDAP synchronization job.

Agents

Agent hosts are often more exposed to external threats than Authentication Manager. RSA strongly recommends that you take the following steps to help protect your agent hosts.

- Update the operating system and hosted applications protected by agents with the latest security patches.
- Limit physical access to the devices that host agents.
- Limit remote access to privileged accounts on devices that host agents.
- Do not configure agents as open to all users. RSA strongly recommends restricting access to agents to specific users and groups.
- Ensure that the location where your agents are installed is protected by strong access control lists (ACL).
- Run anti-virus and anti-malware software.
- Run host-based intrusion detection systems.

- If logging is enabled, write logs to a secure location.
- Do not modify any agent file permissions and ownerships. Do not allow unauthorized users to access agent files.
- When you integrate an agent into a custom application, make sure you follow industry standard best practices to develop a secure custom application.

Supporting Your Users

It is important to have well defined policies around help desk procedures for your Authentication Manager. Help Desk administrators must understand the importance of PIN strength and the sensitivity of data such as the user's login name and token serial number. Creating an environment where an end user is frequently asked for this kind of sensitive data increases the opportunity for social engineering attacks. Train end users to provide, and Help Desk administrators to request the least amount of information needed in each situation.

Preventing Social Engineering Attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting employees or individuals into divulging sensitive data that can be used to gain access to protected systems. Use the following guidelines to reduce the likelihood of a successful social engineering attack:

- Help Desk administrators should only ask for a user's User ID over the phone when they call the help desk. Help Desk administrators should never ask for token serial numbers, tokencodes, PINs, passwords, and so on.

  Note: When resynchronizing tokens, users should enter tokencodes in the administrative interface under the supervision of the logged in administrator. If the user is unable to enter tokencodes in this way, make sure that the user adheres to the other recommendations in this section and that administrators adhere to the recommendations in the following section “Confirming a User's Identity” when it is necessary to resynchronize a token.

- The Help Desk telephone number should be well-known to all users.
- Help Desk administrators should perform an action to authenticate the user's identity before performing any administrative action on a user's token or PIN. For example, ask the user one or more questions that only he or she knows the answer to verify their identity. For more information, see Confirming a User's Identity.

- If Help Desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call back the Help Desk at a well-known Help Desk telephone number to ensure that the original request is legitimate.
- To confirm that all PIN changes are requested by authorized users, you should have a policy in place to notify users when their PINs have been changed. For example, send an e-mail notification to the user's corporate e-mail address, or leave a voicemail message. Users that suspect a change was made by an unauthorized person should contact the Help Desk.

Confirming a User's Identity

It is critical that your Help Desk Administrators verify the end user's identity before performing any Help Desk operations on their behalf. Recommended actions include:

- Call the end user back on a phone owned by the organization and on a number that is already stored in the system.

  Important: Be wary of using mobile phones for identity confirmation, even if they are owned by the company, as mobile phone numbers are often stored in locations that are vulnerable to tampering or social engineering.

- Send the user an e-mail to a company email address. If possible, use encrypted e-mail.
- Work with the employee's manager to verify the user's identity.
- Verify the identity in person.
- Use multiple open-ended questions from employee records (ex. Name one person in your group; What is your badge number?). Avoid yes/no questions.

PIN Management

RSA strongly recommends the following to help protect RSA SecurID PINs:

- Configure Authentication Manager to lock out a user after three failed authentication attempts. Require manual intervention to unlock users who repeatedly fail authentication.

  For information about configuring the number of failed attempts, see the following Knowledgebase article: **a54318 – How to modify number of Incorrect Passcodes before next tokencode mode or disabling token**.

- Do not use 4-character numeric PINs. If you must use a short PIN (e.g. a 4-character PIN), require alphanumeric characters (a-z, A-Z, 0-9) when the token type supports them.

- Your corporate PIN policy should require the use of 6-character to 8-character PINs. RSA recommends that your PIN policy requires alphanumeric characters (a-z, A-Z, 0-9) when the token type supports them. You must configure Authentication Manager to allow these characters. If you modify your Authentication Manager PIN policy settings, all users who do not meet the new policy settings will be set to New PIN mode. If you have changed your Authentication Manager PIN policy settings and users are not being prompted for a new PIN, contact RSA Customer Support for information on how to force the new PIN mode.

  Note: It is important to strike the right balance between security best practices and user convenience. If system-generated alpha numeric 8-digit PINs are too complex, find the strongest PIN policy that best suits your user community.

- You should notify your users before you update the policy. If you have a large number of users who do not meet the new policy, you may experience an increase in Help Desk calls.

- You can increase the complexity of user PINs by requiring system-generated PINs. However, you may be reducing security as people may write down complex PINs, or call the Help Desk more frequently to have their PINs cleared.

  Increased phone calls to the Help Desk to clear PINs increases the possibility of a social engineering attack from unauthorized individuals posing as users. For more information, see Confirming a User's Identity.

- Instruct all users to guard their PINs and to never tell anyone their PINs. Administrators should never ask for or know the user's PIN.

- Configure Authentication Manager to require users to change their PINs at regular intervals. These intervals should be no more than 60 days. If you use 4-digit numeric PINs, the intervals should be no more than every 30 days. For software tokens, the PIN should be equal in length to the tokencode, and all numeric.

  For information about requiring periodic PIN changes for users, see the following Knowledgebase article: **a54302 – Configure Authentication Manager to require users to change their PINs at regular intervals**

  Note that more frequent PIN changes may also result in an increase in Help Desk calls.

- RSA strongly recommends that you do not use system-generated PINs in conjunction with the RADIUS PAP protocol.

For information about changing to a stronger PIN policy, see the following Knowledgebase articles:

- **a54294 - How To PIN Management**
- **a54276 - Force all tokens to be in New PIN mode, without clearing PIN**

For information about gradually phasing in a requirement for users to change their PINs, see the following Knowledgebase article: **a54317 – Set tokens specified in a text file into New PIN required mode**.

Important: After making any changes to PIN policies, restart the server to ensure that the changes take effect.

Advice for your Users

RSA strongly recommends that you instruct your users to do the following:

- Never give the token serial number, PIN, tokencode, token, passcode or passwords to anyone.
- To help avoid phishing attacks, do not enter tokencodes into links that you clicked in email. Instead, type in the URL of the reputable site to which you want to authenticate.
- Inform your users of what information requests to expect from Help Desk administrators.
- Always log out of applications when you're done with them.
- Always lock your desktop when you step away.
- Regularly close your browser and clear your cache of data.
- Immediately report lost or stolen tokens

Note: Consider regular training to communicate this guidance to users.

Emergency Access and Static Passwords

Use temporary passwords (either a fixed password or a one-time password set) to grant emergency access to users. RSA strongly recommends that you adhere to the following guidelines:

- Perform an action to confirm the user's identity before assigning the user a fixed password or one-time password set. For example, ask the user a question that only they know the answer to verify their identity
- Do not re-use the same fixed password across multiple users.
- Do not use a predictable password, for example, do not use the date.

- Discontinue the use of static passwords.
- Temporary passwords are not a permanent solution to lost tokens. Ensure that temporary passwords expire within a short period of time. RSA strongly recommends that temporary passwords expire within a day.

For information about determining which users have static passwords, see the Knowledgebase article: **a54330 - Determine all users with static passwords**.

Administration Toolkit

When using the Administration Toolkit (ATK) (C or TCL interface), RSA recommends that you:

- Obfuscate passwords accepted by the software whenever possible (don't show keystrokes).
- Never accept passwords on the command line (STDIN is ok).
- Protect any secrets you manage.
- Do not configure the ATK to allow remote connections.

Deployment Manager and Quick Admin

RSA Authentication Manager 5.2 and 6.1 includes a service called sdcommd or, alternatively the web admin service or the quick admin service, which is needed to run Deployment Manager provisioning and Quick Admin administration.

If you are running Deployment Manager or Quick Admin, do the following:

- Make sure that the sdcommd configuration file contains only those remote systems that need to connect to Authentication Manager using the sdcommd service. On Windows the configuration file is Sdcommdconfig.txt. On Unix the file is sdcommd.txt.
- Periodically audit your sdcommd configuration file to make sure the list of allowed systems is correct.
- Deployment Manager uses an administrator account to perform its tasks.
  - Restrict the scope of this account to the minimal scope appropriate for your environment. For example, if all users created by web express should be in the “self service” AM Group, restrict Web Express to the AM “self service” group.
  - Use the Authentication Manager Database Administration application to assign an empty task list to the account.

Customer Support Information

For information, contact RSA Customer Support:

U.S.: 1-800-782-4362, Option #5 for RSA, Option #1 for SecurCare note

Canada: 1-800-543-4782, Option #5 for RSA, Option #1 for SecurCare note

International: +1-508-497-7901, Option #5 for RSA, Option #1 for SecurCare note