RSA Authentication Manager 7.1
Security Best Practices Guide

Version 5

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.
		Introduction	New reminder that recommendations also apply to RSA SecurID Appliance 3.0.
		Immediately After Setting Up Your Software	• Revised description of Super Admin. • Correction to the name of the Manage Operations Console Administrators command line utility.
		Password Policies	New list of the special characters that cannot be used in passwords.
		Protecting Tokens	New reminder to use a second factor with 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.
		Agents	New reference to additional documentation.
		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 and recommendations on how to help ensure a smooth transition when rolling out a new PIN policy. • New recommendations on PINs for software tokens. • 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	The Master Password	New recommendations about protecting the master password.
		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	Potential Privilege Escalation Issue	Added guidance on restricting the scope of some administrators to safeguard Super Admin accounts.
		Preventing Social Engineering Attacks	Additional information about resynchronizing tokens.

Critical Sections

Introduction

This guide is intended to help identify configuration options and best practices designed to help ensure correct operation of RSA® Authentication Manager 7.1, 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 monitor your network for intrusions.

Important: All references to Authentication Manager also apply to RSA SecurID Appliance 3.0.

Immediately After Setting Up Your Software

When you install RSA Authentication Manager, you are prompted to create a Super Admin ID and password, which creates the following three accounts, all with the same initial password.

Type	Purpose	Management
Super Admin	An administrator with permissions to perform all administrative tasks in the Security Console. A Super Admin user is also required for some administrative tasks that are performed outside the Security Console. You can create additional Super Admin accounts if you require them.	A Super Admin is an administrative role assigned that gives permission to perform all administrative tasks in the security console. Any user with the Super Admin role can manage all users including other administrators and other users with the Super Admin role.
Operations Console administrator	An administrator with permissions to perform all administrative tasks in the Operations Console. **Note:** Some tasks in the Operations Console also require you to provide the logon credentials for a Super Admin user. Only Super Admins stored in the internal database are accepted by the Operations Console.	Any Super Admin can manage this account using the Manage Operations Console Administrators command line utility. RSA strongly recommends that you limit Operations Console access to Authentication Manager administrators only.
Master Password	Used to perform some administrative tasks and to access sensitive data about your RSA deployment.	On an Authentication Manager or local RADIUS server machine, any Operations Console administrator, and any administrator with knowledge of the master password. On a remote RADIUS server machine, Operations Console administrators created before the creation of the RADIUS package and any administrator with knowledge of the master password on the remote RADIUS server.

The Master Password

The master password is created during installation and initially is the same as the Super Admin account password and the Operations Console account password. It is imperative that you secure the master password, as it protects all of the system passwords required to run Authentication Manager.

Because the master password is such a key piece of information, RSA strongly recommends the following:

- Entrust knowledge of the master password only to a limited number of personnel who require it to access the key materials and run command line utilities.
- Ensure that the master passwords on each RSA Authentication Manager instance and RSA RADIUS server stay in synch by formulating a policy that ensures that when you change the master password on any instance, you change it on all the other instances and RSA RADIUS servers.

  For more information, see the section "Changing the Master Password" in the chapter "System Maintenance and Disaster Recovery" in the *Administrator's Guide*.

- Create additional Operations Console administrator accounts to ensure that there is always an administrator who has the ability to reset the master password in the event that it is lost or forgotten. Store a set of Operations Console administrator credentials encrypted in a secure location with no network connectivity.

  Important: If the master password is lost or forgotten, you cannot reset it without an Operations Console administrator account.

As part of failover and disaster recovery planning, the master password can be exported as part of a backup of all of the system passwords, and exported to an encrypted, password-protected file. RSA strongly recommends storing the exported file in a safe and secure manner.

Password Policies

To enforce strong passwords, which will help secure sessions, RSA strongly recommends that you configure all password policies to meet the following minimum requirements:

- Minimum Password Length: 15 Characters
- Alpha Characters Required: 2 Characters
- Numeric Characters Required: 1 Character
- Special Characters Required: 1 Character

  Users cannot use the following characters: space / ; : ,

- Uppercase Characters Required: 1 Character
- Lowercase Characters Required: 1 Characters
- Password Change Interval: 90 Days

- Previous Passwords Disallowed: 20 Passwords
- Maximum Failed Login Attempts: 3 Attempts

Managing Accounts and Secrets

Create an Operations Console administrator account for each Operations Console user. Do not share account information, especially passwords, among multiple administrators.

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: **a54325 – Identify all Tokencode-Only (PINless) tokens**.

For information about determining which users have fixed passcodes, see the Knowledgebase article: **a54308 - Create custom SQL report to list all RSA SecurID users with a fixed passcode**.

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.

- 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 RSA SecurID 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

RSA strongly recommends that you install RSA Authentication Manager 7.1SP4 patch 5 to enhance protection of your token serial numbers.

The patch 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.

Distributing Hardware Tokens

Take the following steps to protect your hardware tokens:

- 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.
- 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 19.

Distributing Software Tokens

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

- Use CT-KIP over SSL.
- When generating the token files for distribution, protect the files with a password, which encrypts the file. Use passwords that conform to best practices. For more information, see "Password Policies" on page 7.
- Use the RSA Security Console 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 "Regenerate Token" is enabled before issuing a software token.

On Demand Tokens

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. Ensure that on-demand tokencodes expire within a short period of time. Configure as short a period of time as your organization needs. RSA strongly recommends that this be no more than 15 minutes.

Users should be trained to use on-demand tokencodes immediately when they receive them.

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.
- 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 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 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 SDK.

- 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 using at least 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.
- The RSA SecurID Appliance provides SSH as a remote management capability. Refer to the *RSA SecurID Appliance Owner's Guide* for details on how to enable and disable SSH.
- 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.

Potential Privilege Escalation Issue

The default security domain and administrative role settings for Authentication Manager allow any administrator, who has permission to edit the same credential that is required to authenticate to the Security Console, and whose administrative scope includes a higher level administrator's security domain to edit a higher level administrator's account.

For example, suppose that an administrator, who is not a Super Admin, has administrative scope that includes the Super Admin's security domain. Suppose that the administrator who is not a Super Admin has permission to edit passwords, and that the Security Console for the security domain requires only a password for authentication. The administrator who is not a Super Admin can change the Super Admin's password and subsequently authenticate to the Security Console as that Super Admin.

The previous example also applies when the Super Admin is in a lower-level security domain than the administrator who is not a Super Admin. It also applies to security questions, LDAP password, RSA Password, SecurID, assigning tokens, clearing pins, and so on.

The proposed remedy is to move the Super Admin into the top level security domain, and move all other administrators into a lower-level security domain. This prevents lower-level administrators, for example Help Desk Administrators, from editing the Super Admin password and then using the Super Admin account to access the Security Console.

Customers should modify their deployments to use one or more of the following remedies:

- Configure Authentication Manager according to the following model:
  - Place all Super Admins in the top level security domain.

  - Place all other administrators, who have permission to edit users or authentication credentials, in lower-level domains.

  - Place all other users in another security domain.

  - Assign the appropriate role and scope to administrators. An administrator's scope should exclude the administrator's own security domain. The administrator's scope should include only the security domain over which the administrator has authority. For example, suppose that a Help Desk administrator exists in a security domain. Ensure that the Help Desk administrator only has scope for the security domain of end users, and not for the security domain of the Super Admin.

- Do not allow a lower level administrator to edit an authentication credential of a higher level administrator.

- Do not create a new way for a lower level administrator to edit a higher level administrator's credentials.

  For example, suppose that the Authentication Manager is configured to use LDAP password authentication, the LDAP server is protected by RSA SecurID, and Windows password integration is enabled. Suppose that the lower level administrator has permission to assign tokens and is in the same security domain as the higher-level LDAP Admin. The lower-level administrator could assign a new token to the LDAP Admin, log into LDAP as the LDAP Admin, change the LDAP credential of the higher level admin, and log on to the Security Console as the higher level administrator.

  In this scenario, simply disabling Windows password integration on the SecurID agent protecting the LDAP server would maintain the strength of the security. Similar considerations must be made for all credentials that can be used to authenticate to Authentication Manager.

- Configure Authentication Manager to require a combination of authentication credentials. If Authentication Manager is configured to require multiple credentials, at least one of which the lower level administrator does not have permission to edit, the lower level administrator cannot masquerade as the higher level administrator.

- If you do not use the RSA Self-Service console in your deployment, do the following:

  - Remove the Reset Password permission from the Help Desk administrator who is helping end users.

  - Assign the Assign Token and Reset Password permissions to an administrator other than the Help Desk administrator.

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.
- In deployments that use the Self Service Console or CT-KIP, use a proxy with SSL/TLS support. You should enable SSL/TLS between the proxy and the Self Service Console or CT-KIP. You should have the proxy support only the pages that are required.
- Examine your self-service policies and consider hardening self-service access and functionality.
  - Limit access to the self-service console only to users inside your network.
  - RSA strongly recommends that you do not allow users to clear their PIN with the Self-Service Console. Users that must clear their PIN should contact the Help Desk.
- On UNIX systems, run the Authentication Manager under its own service account and restrict access to its files to that service account. This service account 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 and Configuration 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).

Policies and Roles

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

- Configuration Settings
- Policies
- Administrative roles and associated permissions
- Which administrators are assigned to which roles
- Agent Host enabled lists

Note: Verify that unauthorized users are not enabled through membership in a nested group.

Monitoring Authentication Manager

RSA strongly recommends the following:

- Run Network Intrusion Detection Systems and Host Intrusion Detection Systems in your environment.
- Run Simple Network Management Protocol (SNMP) systems. SNMP can monitor the state of Authentication Manager and perhaps indicate possible attacks.

  For information on using SNMP, see the following Knowledgebase article: **a54319 – Sending SNMP traps**.
- Be sure to monitor which ports are open. For information about port usage, see the *Authentication Manager Installation and Configuration 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 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:

- **a54320 – How to export logs**
- **a54313 - Monitoring Authentication Activity**

Secure Maintenance

Always apply the latest security patches for RSA Authentication Manager, which are available from RSA on RSA SecurCare 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 Oracle or WebLogic components of Authentication Manager 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
- Backup data
- Authentication Manager passwords
- Archived log files and report data

To help protect online data, such as current log files and configuration files, RSA strongly recommends that you 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 Secure Copy (SCP). Re-enable SSH when you run your backups, and disable it immediately thereafter.
- Encrypt your backups, especially when containing software tokens. Protect the encryption key in a secure location, such as a safe.

External Identity Sources

Your external identity sources hold sensitive data that Authentication Manager frequently accesses. RSA strongly recommends that you take the following steps designed to increase the security of this flow of information:

- Use SSL/TLS to communicate with all external identity sources, i.e., LDAP or Active Directory.
- Change the password for the service accounts that connect to Active Directory and LDAP regularly.

Agents

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

For more information, see the *RSA Authentication Agent Security Best Practices Guide*.

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 he or she calls 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 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 to which only he or she knows the answer. 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 (for example: 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 lockout 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: **a54315 - How to change the failed authentication thresholds**.

- 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.

  To roll out a new Authentication Manager PIN policy, set the maximum PIN lifetime to a period that is short enough so that all users will be forced into New PIN mode but long enough where users will not be forced to change their PIN multiple times. If your user population is segmented by security domains, it is recommended that you stagger the PIN policy change by security domain to avoid overwhelming your Help Desk.

  Be sure to notify the affected users in advance that they should authenticate and change their PIN as soon as possible. To verify all users have changed their PINs, run a report detailing user authentication activity for that period of time.

  After the Authentication Manager PIN policy rollout is complete and you have verified that all users have changed their PINs in accordance with the new policy, the Authentication Manager PIN policy lifetime should be restored to adhere to your corporate security policy. If you have changed your Authentication Manager PIN policy settings and users are not being prompted for a new PIN, please 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.

  For information about changing to a stronger PIN policy, see the following Knowledgebase article: **a54312 - Changing token policies to require 6-character or 8-character PINs**

- 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 policies that restrict the re-use of PINs.
- Configure the use of the dictionary to prevent the use of simple PINs.
- For software tokens:
  - when software tokens are issued as PINPad-style tokens (the Displayed Value is set to Passcode in the Software Token Settings), the software token PIN should be equal in length to the tokencode, and all numeric..
  - when software tokens are issued as fob-style tokens (the Displayed Value is set to Tokencode in the Software Token Settings), the software token PIN should be alphanumeric and eight digits in length.
- 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: **a54316 - How to configure a regular PIN change for users**.

  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 gradually phasing in a requirement for users to change their PINs, see the following Knowledgebase article: **a54314 - Changing token policies on a subset of users**.

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 e-mail. 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

RSA strongly recommends that you do the following:

- Use the random PIN generator to generate emergency access passwords. Do not re-use the same emergency access passwords across multiple users. Do not use predictable static passwords, for example, do not use the date.
- Perform an action to confirm the user's identity before assigning the user an emergency access tokencode. For example, ask the user a question to which only he or she knows the answer.
- Discontinue the use of static passwords.
- Emergency access tokencodes are not a permanent solution to lost tokens. Ensure that emergency access tokencodes expire within a short period of time. RSA strongly recommends that emergency access tokencodes expire within a day.
- Use On Demand tokencodes for emergency access when possible.
- Verify that the user's phone number has not changed.

Software Development Kit

When using the Software Development Kit, RSA strongly recommends that you:

- Obfuscate the command client password whenever possible.
- Never accept passwords on the command line.
- Protect any secrets you manage.

Best Practices for Custom Reports

- For custom reports that directly access the Authentication Manager internal database, make sure that any passwords are obfuscated and rotated on a regular basis.
- Disable the report's service account after the report is run.
- Make sure the report service account only has read-only access to the database.
- Secure output from custom reports in a secure location with no network connectivity. If you need to transfer it over the network, do so in an encrypted state.
- Restrict access to the custom reports and their outputs.

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