RSA Authentication Agents Security Best Practices Guide

Version 3

The Security Division of EMC

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.

April 2011

Revision History

Revision Number	Date	Section	Revision
1	March 17, 2011		Version 1
2	March 21, 2011	Introduction	New reference to product documentation.
		RSA Authentication Agents	New recommendation on using firewalls.
		Physical Security Controls	New recommendations on controlling physical access to resources.
		Customer Support Information,	New list of Customer Support phone numbers
3	April 8, 2011	Special Considerations for Web Agents	Clarified the meaning of logoff URL.

Introduction

This guide is intended to help identify configuration options and best practices, and offer monitoring and auditing recommendations for RSA® Authentication Agents, however, it is up to you to ensure they are properly monitored and maintained when put on your network. Use this guide in conjunction with Authentication Agent product documentation.

For guidance on configuring Authentication Manager, see your Authentication Manager documentation.

RSA Authentication Agents

The security provided by an RSA Authentication Agent depends in part on the security of the system on which it is deployed. If the underlying operating system is insecure, the Agent cannot prevent vulnerabilities from being exploited.

To help harden the security of the underlying system, RSA strongly recommends that you do the following:

- Update the operating system and hosted applications protected by agents with the latest security patches.
- Limit remote access to privileged accounts on devices that host agents or protect them with an agent.
- Limit physical access to the devices that host agents.
- Do not configure agents as open to all users. It is more secure to restrict access to specific users and groups.
- For RSA Authentication Agents for Microsoft Windows, verify that the local authentication client (LAC) challenge group has proper access control lists (ACL) such that only authorized administrators can alter the group membership data.
- Run anti-virus and anti-malware software.
- Use appropriate firewall rules to block unnecessary inbound and outbound traffic.
- Run host-based intrusion detection systems.
- 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.

Agent Node Secret Management

The node secret is a symmetric encryption key that RSA® Authentication Manager and RSA Authentication Agents use to encrypt and decrypt packets of data as they travel across the network. Authentication Manager is engineered to create a unique node secret for each Authentication Agent that is installed. After the node secret has been created, it can be delivered to the Authentication Agent using either Automatic Delivery or Manual Delivery.

Important: If you are concerned that your node secret is compromised, generate a new node secret.

Best Practices for Automatic Delivery

If you use Automatic Delivery, which is the default setting, Authentication Manager automatically creates and sends the node secret to the Agent Host in response to the first successful authentication on the Agent Host. The node secret is encrypted with a key derived from the user's passcode and other information.

However, the encrypted node secret may be intercepted if you do not carefully control the circumstances in which the first authentication on each Agent Host occurs.

Adhere to the following guidelines when deploying new agents:

- Do not configure an Agent Host as **Open to All Locally Known Users** until the node secret delivery has taken place. Before the node secret is delivered, only the administrator should be allowed to authenticate on that Agent Host.
- If your system uses **telnet** or **rlogin** or any other unencrypted protocol for remote users, ensure that the first authentication on a new Agent Host is never done remotely. If the first user to be authenticated is connected to the Agent Host remotely, through an application such as **telnet** or **rlogin**, the user's passcode is sent in the clear, where an attacker can easily intercept it and use it to derive the key used to encrypt the node secret.
- Ensure that the first authentication is done with the longest possible *alphanumeric* passcode—15 characters or more. This can greatly increase the time needed to decrypt an intercepted node secret and significantly reduce your vulnerability to attack.
- As the administrator, you can maximize your protection against attack by performing the first authentication yourself. Make sure that the token you use is not in New PIN Mode, has a sufficiently long PIN, and that you authenticate locally.

Best Practices for Manual Delivery

If you choose to send the node secret manually, you must configure Authentication Manager to create the node secret. You then deliver the node secret to the Agent Host and use the Node Secret Load utility to load the node secret onto the Agent Host. The node secret is password protected. When you run the Node Secret Load utility on the Agent Host, the utility decrypts the node secret file, renames the file after the authentication service name (usually **securid**), and then stores the renamed file on the Agent Host.

For security purposes, RSA urges you to follow these guidelines:

- Use the longest possible, *alphanumeric* password—15 characters or more.
- If possible, deliver the node secret on secure media to the RSA Authentication Agent administrator, and verbally deliver the password. Do not write down the password.
- Ensure that the media containing the password-protected node secret is destroyed after the node secret has been loaded onto the Agent Host.
- If you must deliver the node secret through e-mail, deliver the password separately through encrypted e-mail.
- Ensure that both e-mails are permanently deleted after the node secret has been loaded onto the Agent Host.
- Make sure all personnel involved in the node secret delivery are authorized personnel.
- If you think the node secret may be compromised, you must replace it.

Physical Security Controls

Physical security controls help enable the protection of resources against unauthorized physical access and physical tampering. While following your organization's security policy, strongly consider the following physical security controls:

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

Special Considerations for Web Agents

Web Agents are designed to run on third party web servers. The security provided by a Web Agent depends in part on the security of the protected system on which it is deployed. If the underlying OS or web server is insecure, the Web Agent cannot prevent vulnerabilities from being exploited. You are responsible for securing the host servers protected by the Web Agent.

In addition to Agent best practices, RSA strongly recommends the following for Web Agent deployments:

- Use the logoff URL to automatically invalidate users' web access authentication cookies instead of waiting for cookie timeout.

  Note: The logoff url is used to terminate Web Agent sessions. If the browser does not access the Web Agent logoff URL, then the Web Agent session continues until the configured timeout.

- Set restrictive cookie timeouts to prevent session cookies from having long lives, especially if the session is inactive.
- Using domain cookies, allow single sign-on to multiple RSA protected web servers. Make sure appropriate file permissions are set to prevent inappropriate access.
- Machines hosting web servers protected by Web Agents should only be accessed by administrators.
- Enable web site protection for the entire web server or directories and then unprotect pages that do not need to be secure. This will reduce the chances of having sensitive data unprotected.
- For IIS web servers, enable the setting to disable IIS Server if the Agent fails to load.
- Enable the option to prevent caching of protected pages to prevent unauthorized users from accessing protected data on unattended client machines.
- Disable services that are not required by the web server.
- By default, the Web Agent sets the ownership and permission to all the files and directories it uses. Do not change these permissions or ownership properties. Doing so could create a vulnerability in the system.
- The Web Agent includes an auto-redirect script that enables you to require users to authenticate before accessing a URL that is not formally protected by RSA SecurID. The URL does not have to be hosted on the same server or be within the same domain as the server on which the Web Agent is installed. RSA strongly recommends that your script contain a list of URLs that users are allowed to access using the redirect URL.
- On WAP browsers, the cookie expiration times are 15 minutes for idle cookies and 60 minutes for all cookies. For increased security, RSA strongly recommends using lower values for both cookie expiration times. For information, see your *RSA Authentication Agent Installation and Configuration Guide*.

Monitoring Authentication Agents

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

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.
- Audit and analyze system and application logs periodically. You can use security information and event management to help you with this task.
- Retain log data in compliance with your security policies and local laws.

Secure Maintenance

Always apply the latest security patches for RSA Authentication Agents, 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/help.aspx?_v=view5**.

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

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