RSA SecurID Authentication Manager

Secure Configuration Guide

**Version 2, Release 2**

21 September 2017

**Developed by DISA for the DoD**

**Trademark Information**

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

**Page**

[1. secure configuration guide overview 1](#_Toc493760121)

[1.1 Scope 1](#_Toc493760122)

[2. Authentication manager deployment considerations 2](#_Toc493760123)

[2.1 Vendor Recommendations 2](#_Toc493760124)

[2.1.1 Physical Security Recommendations 2](#_Toc493760125)

[2.1.2 Data and Network Security Recommendations 2](#_Toc493760126)

[3. Secure operation configuration recommendations 3](#_Toc493760127)

[3.1 Operating System Access and Hardening 3](#_Toc493760128)

[3.2 Operations Console Security Configurations 3](#_Toc493760129)

[3.2.1 Maintenance Menu 4](#_Toc493760130)

[3.2.2 Administration Menu 5](#_Toc493760131)

[3.3 Security Console Security Configurations 6](#_Toc493760132)

[3.3.1 Authentication Menu 7](#_Toc493760133)

[3.3.2 Setup Menu 10](#_Toc493760134)

[3.3.3 Network Monitoring (SNMP v3) Menu 13](#_Toc493760135)

[4. Summary 14](#_Toc493760136)

LIST OF TABLES

**Page**

[Table 3.2‑1: Maintenance Menu 4](#_Toc493760137)

[Table 3.2‑2: Administration Menu 5](#_Toc493760138)

[Table 3.3‑1: Authentication Menu 7](#_Toc493760139)

[Table 3.3‑2: Setup Menu 10](#_Toc493760140)

[Table 3.3‑3: Network Monitoring (SNMP v3) Menu 13](#_Toc493760141)

# secure configuration guide overview

## Scope

This document presents recommended security configurations for both the physical and virtual deployment and operation of the RSA SecurID Authentication Manager based on common information system security practices for secure operation in a DoD environment and is limited to the following areas:

* Vendor-recommended deployment considerations
* Configuration options available using the RSA SecurID Authentication Manager’s Operations Console
* Configuration options available using the RSA SecurID Authentication Manager’s Security Console
* Implementation of the RSA-provided hardening scripts

# Authentication manager deployment considerations

## Vendor Recommendations

### Physical Security Recommendations

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

* Allow only authorized users to physically access Authentication Manager systems and components.
  + After installation, authorized users need only limited access to Authentication Manager systems and components.
* Employ strong access control and intrusion detection mechanisms where the product cabling, switches, servers, and storage hardware reside.

### Data and Network Security Recommendations

To help ensure the highest level of security and reduce the risk of intrusion or malicious system or data access, RSA strongly recommends following industry best practices for hardening the network infrastructure, including:

* 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 demilitarized zone (DMZ).
* Do not co-host Authentication Manager on the same operating system instance with other software.
* Use firewalls designed to remove unnecessary network access to Authentication Manager and follow network security best practices.
* Only allow inbound and outbound traffic on the documented ports to reach Authentication Manager.
* Segment the Authentication Manager network with a hardware firewall.
* Run Network Intrusion Detection Systems and Host Intrusion Detection Systems in the environment.
* Run Simple Network Management Protocol (SNMP) systems. SNMP can monitor the state of Authentication Manager and perhaps indicate possible attacks.
* Audit and analyze system and application logs periodically, using Security Information and Event Management to help with this task.
* Retain log data in compliance with organization security policies and local laws.

# Secure operation configuration recommendations

## Operating System Access and Hardening

Access to the RSA SecurID Authentication Manager’s operating system is intended for use during maintenance and troubleshooting of the device. Console and Secure Shell (SSH) access to the operating system should be limited to authorized administrators and SSH access should be disabled during normal device operation. During initial configuration of the device, the “rsaadmin” account is created to allow access to the operating system. Access to the account should be limited to authorized administrators and treated as a group account. It is recommended that any time this account is used, that use is documented to include the name of the administrator, the purpose of access, and the date and time the account was accessed.

As part of the hardening of this device, it is recommended that the RSA-provided hardening scripts are applied to the operating system, which will require access to the operating system and the “rsaadmin” account. To apply the hardening script, use the following procedure:

1. Contact your RSA support representative to obtain the hardening control file.
2. Enable SSH access to the operating system.
3. Log on to the operating system using the “rsaadmin” account.
4. Copy the hardening control file to a directory on the RSA Authentication Manager appliance where it can be accessed by the hardening script.
5. Change to the directory where the hardening script is installed:

# cd /opt/ADG/hardening

1. Execute the hardening script:

# sudo utils/harden.pl -f <hardening\_control\_file>

1. Log off of the operating system.
2. Disable SSH access to the operating system.

## Operations Console Security Configurations

This section presents the recommended security configurations that should be configured using the Operations Console. The tables have been separated based on the top-level menu in the Operations Console.

### Maintenance Menu

Table 3.2‑1: Maintenance Menu

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub-Menus** | **Configuration Title** | **Setting(s)** | **Comments** |
| Backup and Restore - Schedule Backups - Schedule Backup Status | Scheduled Backups on this deployment is | On |  |
| Backup and Restore - Schedule Backups - Backup Configuration | Backup Password | *{Organizationally defined value}* | This password is used as part of the backup encryption process. |
| Backup and Restore - Schedule Backups - Backup Configuration | Maximum Number of Archived Backups | 4 | This is the vendor default value. |
| Backup and Restore - Schedule Backups - Backup Location | Select Your Backup Location | Windows Shared Folder; NFS Shared Folder | Backups should not be stored on the Authentication Manager. The location should be determined by the organization based on the current infrastructure and access control mechanisms in place for the backup files. |
| Backup and Restore - Schedule Backups - Schedule | Frequency | Weekly | Backups should be performed at least weekly. |

### Administration Menu

Table 3.2‑2: Administration Menu

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub-Menus** | **Configuration Title** | **Setting(s)** | **Comments** |
| Log Rotation Settings - Log Rotation Policy | Log Rotation Options | Daily |  |
| Log Rotation Settings - Log Rotation Policy | Compression Options | Compress rotated log files | The type of compression (bzip2, zip, gzip) can be determined by the organization. |
| Log Rotation Settings - Log Rotation Policy | Shred Options | Do not overwrite log files |  |
| Log Rotation Settings - Log Rotation Policy | Maximum Number of Files Allowed | 99 | This is the vendor default value and can be altered to fit organizational requirements. |
| Operating System Access - SSH Settings | Enable SSH | Disabled | SSH should only be enabled for initial device hardening and maintenance purposes. |
| Operating System Access - Session Lifetime Settings - Timeout | Time out idle sessions | Enabled |  |
| Operating System Access - Session Lifetime Settings - Timeout | Close idle sessions if inactive for | 15 minutes | This value must not exceed 15 minutes. |

## Security Console Security Configurations

This section presents the recommended security configurations to be configured using the Security Console. The tables have been separated based on the top-level menu in the Security Console.

When configuring the settings in Table 3.3-1, the “Manage Existing” or “Add New” option will appear as the final drop-down menu selection. If choosing to “Manage Existing”, ensure the settings are applied to the “Default Policy”. If choosing to “Add New”, ensure the “Set as default {policy-type} policy” is selected.

When configuring the settings in Table 3.3-2, the administrator may be prompted to select an instance to which these settings will apply. Ensure the settings listed in Table 3.3-2 are applied to each instance that is configured on the Authentication Manager.

The Authentication Manager provides the option to configure the device to interface with a pre-existing SNMP v3 Network Monitoring solution. Table 3.3-3 lists the recommended configurations if an organization chooses to implement this optional feature.

### Authentication **Menu**

Table 3.3‑1: Authentication Menu

| **Sub-Menu(s)** | **Configuration Title** | **Setting(s)** | **Comments** |
| --- | --- | --- | --- |
| Policies - Password Policies - Password Policy Basics | Default Policy | Set as the default password policy |  |
| Policies - Password Policies - Lifetime | Periodic Expiration | Require periodic password changes | This configuration should be set as part of the Default Policy. |
| Policies - Password Policies - Lifetime | Maximum Lifetime | 60 days | This configuration should be set as part of the Default Policy. |
| Policies - Password Policies - Lifetime | Minimum Lifetime | 1 day | This configuration should be set as part of the Default Policy. |
| Policies - Password Policies - Lifetime | Restrict Re-Use | 5 passwords | This configuration should be set as part of the Default Policy. |
| Policies - Password Policies - Format | Minimum Length | 15 | This configuration should be set as part of the Default Policy. |
| Policies - Password Policies - Format | Maximum Length | 32 | This configuration should be set as part of the Default Policy. |
| Policies - Password Policies - Format | Character Requirements | Alphabetic: 2  Uppercase: 1  Lowercase: 1  Numeric: 1  Special: 1 | This configuration should be set as part of the Default Policy. |
| Policies - Lockout Policies - Lockout Policy Basics | Default Policy | Set as the default password policy |  |
| Policies - Lockout Policies - Parameters | Lock User Accounts | 3 failures within 15 minutes | This configuration should be set as part of the Default Policy. |
| Policies - Lockout Policies - Parameters | Unlock | Administrators unlock user accounts | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - SecurID Token Policy Basics | Incorrect Passcodes | Require next passcode after 3 incorrect passcodes | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - Token Policy Basics | Default Policy | Set as the default password policy |  |
| Policies - Token Policies - SecurID PIN Lifetime | Periodic Expiration | Disabled | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - SecurID PIN Lifetime | Restrict Reuse | Users can reuse any previous PINs | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - SecurID PIN Format | PIN Creation Method | Require user-generated PIN | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - SecurID PIN Format | Minimum Length | 6 | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - SecurID PIN Format | Maximum Length | 8 | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - SecurID PIN Format | Character Requirements | Allow alphanumeric PINs; require at least 2 numeric characters | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - Fixed Passcode Lifetime | Copy Settings from SecurID PIN Lifetime | Use same settings as SecurID PIN | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - Fixed Passcode Format | Copy Settings from SecurID PIN Format | Use same settings as SecurID PIN | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - Emergency Access Code Format - Character Requirements | Include numeric characters | Enabled | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - Emergency Access Code Format - Character Requirements | Include alphabetic characters | Enabled | This configuration should be set as part of the Default Policy. |
| Policies - Token Policies - Emergency Access Code Format - Character Requirements | Include special characters | Enabled | This configuration should be set as part of the Default Policy. |
| Policies - Offline Authentication Policies - Offline Authentication Policy - Offline Authentication Policy Basics | Offline Authentication | Disabled | This configuration should be set as part of the Default Policy. |
| Policies - Offline Authentication Policies - Offline Authentication Policy Basics | Default Policy | Set as the default password policy |  |
| Policies - Offline Authentication Policies - Offline Authentication Policy - Offline Authentication Security Settings | Minimum Passcode Length | 12 | This configuration should be set as part of the Default Policy. |

### Setup Menu

Table 3.3‑2: Setup Menu

| **Sub-Menu(s)** | **Configuration Title** | **Setting(s)** | **Comments** |
| --- | --- | --- | --- |
| System Settings - Basic Settings - E-mail (SMTP) - Mail Server Settings | Hostname | *{Organizationally defined value}* | An SMTP server must be configured to ensure the delivery of Critical System Event Notifications. This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - E-mail (SMTP) - Mail Server Settings | Port | *{Organizationally defined value}* | An SMTP server must be configured to ensure the delivery of Critical System Event Notifications. This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - E-mail (SMTP) - Mail Server Settings | From Email Address | *{Organizationally defined value}* | An SMTP server must be configured to ensure the delivery of Critical System Event Notifications. This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Levels | Trace Log | Information | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Levels | Administrative Audit Log | Success | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Levels | Runtime Audit Log | Success | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Levels | System Log | Success | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Data Destination | Admin Audit Log Data | Save to internal database and remote SysLog at the following hostname or IP address | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Data Destination | Runtime Audit Log Data | Save to internal database and remote SysLog at the following hostname or IP address | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Data Destination | System Log Data | Save to internal database and remote SysLog at the following hostname or IP address | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Logging - Log Data Masking - Mask Token Serial Number | Number of digits of the token serial number to display | 6 | This configuration must be set for each instance defined on the Authentication Manager. |
| System Settings - Basic Settings - Critical System Event Notification - Enable Critical System Event Notification | Enable Notification | On |  |
| System Settings - Basic Settings - Critical System Event Notification - Enable Critical System Event Notification | Send Notifications for | Backup Events  Identity Source Connection Events  Low Disk Space Events  RADIUS Configuration Events  RADIUS Replication Events  Realm Certificate Removal Events  Replication Events |  |
| System Settings - Basic Settings - Critical System Event Notification - Enable Critical System Event Notification | Send Notifications to | Individual Email Addresses | This list should contain authorized system administrators that are responsible for the system. |
| Console & Session Settings - Session Handling - Console and API Session Restrictions | Maximum System Sessions | 10000 | This is the number of total connections that can be made to the Security Console. This value can be adjusted to fit the needs of the organization. |
| Console & Session Settings - Session Handling - Console and API Session Restrictions | Restrict the number of concurrent sessions per user | Enabled |  |
| Console & Session Settings - Session Handling - Console and API Session Restrictions | Maximum Per User Sessions | 1 | This setting limits the number of concurrent sessions that a single user can maintain with the Security Console. |
| Console & Session Settings - Session Handling - Console and API Session Restrictions | User Over Limit Handling | Deny access to new session |  |

### Network Monitoring (SNMP v3) Menu

Table 3.3‑3: Network Monitoring (SNMP v3) Menu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Main Menu** | **Sub-Menu(s)** | **Configuration Title** | **Setting(s)** | **Comments** |
| Setup | System Settings - Advanced Settings - Network Monitoring (SNMP) - Basics | Network Monitoring SNMP v3 | On |  |
| Setup | System Settings - Advanced Settings - Network Monitoring (SNMP) - Basics | Security Level | Authentication and Privacy |  |
| Setup | System Settings - Advanced Settings - Network Monitoring (SNMP) - Basics | Authentication Protocol | SHA |  |
| Setup | System Settings - Advanced Settings - Network Monitoring (SNMP) - Basics | Privacy Protocol | AES |  |
| Setup | System Settings - Advanced Settings - Network Monitoring (SNMP) - Trap Settings - Send traps for Administrative Audit Log events | When the severity level is | Error, Warning and Success |  |
| Setup | System Settings - Advanced Settings - Network Monitoring (SNMP) - Trap Settings - Send traps for Authentication Log events | When the severity level is | Error, Warning and Success |  |
| Setup | System Settings - Advanced Settings - Network Monitoring (SNMP) - Trap Settings - Send traps for System Log events | When the severity level is | Error, Warning and Success |  |

# Summary

Both RSA- and DISA-recommended configurations are presented for the secure deployment and operation of the RSA SecurID Authentication Manager. All of the settings listed in this document are recommendations based on common information security practices that are currently implemented in the DoD.

It is important to note that all values presented in this document are only recommendations for secure operation in a DoD environment and may be adjusted to fit the security and operational requirements of an organization.