RSA® SecurID
Authentication Manager AM-250 Appliance
Integrated Lights Out Manager (RMM4)
Integration and Configuration Guide
Contact Information
Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: [www.rsa.com](http://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](http://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.
Preface

About This Guide

This guide provides installation and configuration procedures for the RSA® Authentication Manager AM-250 Appliance Integrated Light Out Manager (RMM4). This document is being provided for information only and is not a supported feature or function of the Authentication Manager appliance. By using this document, you accept all responsibility for the configuration changes made.

Product Name Changes

Product changes include renaming the following components.

<table>
<thead>
<tr>
<th>Old Name</th>
<th>New Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DRAC</td>
<td>RMM4</td>
</tr>
</tbody>
</table>

Name changes are reflected in the documentation to the extent possible. Some name artifacts exist in the product source code and these have not all been changed.

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date</th>
<th>Revision Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Jim Mandelbaum</td>
<td>10/29/2015</td>
<td>Creation of the RMM4 instruction guide</td>
</tr>
<tr>
<td>1.1</td>
<td>Jim Mandelbaum</td>
<td>11/5/2015</td>
<td>Document redone on new template with additional topics and table of contents</td>
</tr>
</tbody>
</table>
# Table of Contents

**PREFACE**  
3  
About This Guide  
3  
Product Name Changes  
3  
Version History  
3  
Assign IP Address to the iLOM  
5  
BIOS Configuration:  
5  
Connecting to the Integrated BMC Web Console  
6  
Completion of the iLOM (RMM) Network settings  
7  
Additional Configuration Tasks  
8  
  Security Settings:  
  8  
  VLAN:  
  9  
  SSL:  
  9  
  Remote Session:  
  9  
  Alerts:  
  10  
  Alert Email:  
  10  
Remote Control  
11  
  Using JViewer  
12  
Customer Support Information  
13
Assign IP Address to the iLOM

In order to utilize the iLOM, you will need to configure the IP address of the module. You can do this either through the BIOS of the system or via the command line. For the ease of configuration we will utilize the BIOS method.

BIOS Configuration:

To facilitate configuration of the IP Address configuration via the BIOS you will need a monitor and keyboard available.

Steps:

- Connect Monitor and Keyboard to the Unit
- During POST, hit the <F2> key to enter BIOS Setup
- Enter ‘rsabios’ when prompted for the password
- Navigate to the Server Management tab
- Navigate to the BMC LAN Configuration and hit Enter
- Scroll down to the RMM4 LAN Configuration
- Enter the IP Address for the Management Module
- Enter the Subnet Mask for the Management Module
- Enter the Default Gateway for the Management Module
- Scroll down and select user ID – set to root
- Scroll down to User Password and enter a password to protect the interface (you will enter the password twice)
- Verify that the User Status is now set to Enabled
- Press <F10> to save and reboot the server
Connecting to the Integrated BMC Web Console

After the unit has rebooted you can access the Web Console by opening your browser and navigating to the IP Address you specified in the prior step (Example: http://192.168.0.220)

You will see the Web Console:

- Enter Root for the Username
- Enter the password you created in the prior step
- Click on Login

You will now be presented with the main screen that will show the system information. You can click through the information pages as well as the Server Health pages to see the configuration and status of the system modules.
Completion of the iLOM (RMM) Network settings

You will need to complete the configuration of the iLOM by clicking on the Configuration tab

- Click on the LAN Channel and select <Intel ® RMM>
- Enter the Primary DNS Server and Secondary DNS Server
- Click Save

You will be told that the information has been saved by this popup

- Click OK
- Click OK at the logout prompt
- Log back into the management module
- Click on the Configuration Tab
Additional Configuration Tasks

On the side of the configuration tab you will see some additional options that you may want to configure.

**Users:** This will allow you to define additional users that can access the remote module.

To add or modify a user you will want to click on a row (1-15) and select either <Add User> or <Modify User>

When creating a user they can be an Administrator, Operator or a User. Each level of authorization reduces capabilities with the management console.

<table>
<thead>
<tr>
<th>User ID</th>
<th>User Name</th>
<th>User Status</th>
<th>Network Privilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>anonymous</td>
<td>Enabled</td>
<td>Administrator</td>
</tr>
<tr>
<td>2</td>
<td>root</td>
<td>Enabled</td>
<td>Administrator</td>
</tr>
<tr>
<td>3</td>
<td>jim</td>
<td>Enabled</td>
<td>Operator</td>
</tr>
<tr>
<td>4</td>
<td>jmar</td>
<td>Enabled</td>
<td>User</td>
</tr>
</tbody>
</table>

**Security Settings:**

This will allow you to define the failed login attempts, lockout time, if you want to force https, and session timeouts.

**It is recommended that you enable the “Force HTTPS” option.** When you enable this feature and click Save, the screens will all blank out until you logout and log back into the system using https://
VLAN:

If you utilize VLANs for your management segment, this is where you can define that value.

Be sure to select the correct LAN Channel when you enter the VLAN ID.

SSL:

This allows you to upload a Cert if you so desire to the Management Module.

Remote Session:

The values in the Remote Session configure how the handling of the connection to the server is established and controlled.

You can set encryption for the KVM session, if you want to allow remote USB Key access and how to emulate that remote USB.

This tab also allows you to create a port forward setting for the KVM, CD-ROM and USB/Floppy session.
Alerts:

The Alerts page is geared towards the hardware management and not the software.

You can have alerts sent via email or SNMP on most hardware issues. There are check boxes to determine the alerts you want to receive.

Alert Email:

This is where you configure the SMTP Server for the email alerts that you selected in the Alerts Tab
Remote Control

By clicking on the top tab labeled Remote Control, you can invoke the java remote Control Console. You will need to accept the java messages regarding running the processes.

You may get a security warning about the Java applet, select continue

You will then get asked if you want to run the application, click Run
Using JViewer

At this point you will have a JViewer window open that will provide full KVM controls. There is a menu bar across the top to configure settings and send key sequences. The default settings should function as needed for the Authentication Manager server.

If you plan on restarting the server at any point you can have the JViewer up and running prior to the restart and you will have full visibility and control of the entire boot process.

Any commands to reboot, shutdown or visualize the status of the server is still available back in the web browser management session.

**IMPORTANT:** If you use the “Power OFF Server” option, it does not provide a second challenge and it does not pause for graceful software shutdown.
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