RSA® Registration Manager 6.9 build 563 Readme

This document lists what's new and changed in RSA Registration Manager 6.9 build 563 (Registration Manager). It includes installation information, as well as information about the fixed issues and the known issues. Read this document before installing the software.

For the complete Registration Manager documentation set, go to the Registration Manager page on RSA Link or contact RSA Customer Support.

Contents:

New Features

There are no new features in this release of Registration Manager.

Enhanced Functionality

This release of Registration Manager is designed to contain the following enhanced functionality:

- Upgraded embedded components to the latest secure version: RSA BSAFE Micro Edition Suite 4.1.6.

- Upgraded platform and compiler support:

  - Added Red Hat Enterprise Linux 7.3.

    You must install the following libraries when installing Red Hat Enterprise Linux 7.3:

    - `nss-softokn-freebl-3.16.2.3-14.4.e17.i686.rpm`

    - `libgcc-4.8.5-11.e17.i686.rpm`

    - `glibc-2.17-157.e17.i686.rpm`

    - `libstdc++-4.8.5-11.e17.i686.rpm`

    - Compatible libraries

- Upgraded browser support: Internet Explorer 11 enrolment on systems running a Windows 10 operating system.

- Upgraded cryptographic hardware device support:

  - nCipher client v12.3

  - Luna SA 6

- Upgraded virtualization software support: VMware Esxi 6.0.

- Fixes for specific issues. For more information, see .

Package Contents

The Registration Manager package for this hotfix release is designed to contain the following:

- `RSARM-v6.9build563r-package.zip` (for systems running a Windows operating system)

- `RSARM-v6.9build563r-solaris-package.tar` (for systems running a Solaris operating system)

- `RSARM-v6.9build563r-linux-package.tar` (for systems running a Red Hat Enterprise Linux operating system)

- `RSARM-v6.9build563r-SuSE-linux-package.tar` (for systems running a SUSE Linux operating system)

- Product documentation consisting of this *Readme* document in Portable Document Format (PDF).

Note: In the event of a discrepancy, this *Readme* document takes precedence over the *Administrator's Guide*, the *Vettor's Guide*, the *Installation Guide*, and the Help information.

Installation

You must perform all the tasks in the "Preparing to Install" section in the "Installing RSA Registration Manager" chapter of the *Installation Guide*, before installing the hot fix files for this release.

Install the Full Build

To install the full build of Registration Manager, use the appropriate file from this package. On systems running a:

- Windows operating system, use `RSARM-v6.9build563r-WIN32.zip`.

  Note: During Registration Manager installation, install the Microsoft Visual C++ 2013 Redistributable Package by agreeing to the Microsoft Software License Terms.

- Solaris operating system, use `RSARM-v6.9build563r-sparc-sun-solaris.tar`.
- Red Hat Linux operating system, use `RSARM-v6.9build563r-linux.tar`.
- SUSE Linux operating system, use `RSARM-v6.9build563r-SuSE_linux.tar`.

For full instructions on how to install Registration Manager, see the *Installation Guide*.

Install the Hotfix Files

This section describes how to install the hot fix files. Instructions to install the hotfix files on the following platforms are provided:

- Windows Operating System
- Solaris or Linux Operating Systems.

Note: The hot fix files can be installed on any previous Registration Manager 6.9 installation.

Windows Operating System

This hotfix does not require a new installation of the product, but rather a drop-in replacement of 174 files into the appropriate Registration Manager directory and updating the Help.

To apply Registration Manager 6.9 build 563:

1. Stop all Registration Manager services.

2. Extract the files from `SSLC_CryptoCME_Libs-WIN32.zip` provided with this drop-in package.

3. Replace the following files located at `\WINDOWS\system32` (for Windows 32-bit operating system) or `\Windows\SysWOW64` (for Windows 64-bit operating system) with the ones in the unzipped folder:

   – `ccme_base.dll`

   – `ccme_ecc.dll`

   – `ccme_eccaccel.dll`

   – `cryptocme2.dll`

   – `cryptocme2.sig`

4. Create a backup of the Registration Manager installation directory.

5. Copy `RSARM-v6.9build563r-dropin-WIN32.zip` to the installation directory.

6. Extract the files from the .zip file, ensuring the new files replace the old files.

   Note: If you modified any xuda templates in your Registration Manager installation, you must make those modifications again.

7. To update the Help information, in the `<INSTALL_DIR>\WebServer\admin-server\ra\help` directory, extract the files from `rrm-help.zip`, ensuring the new files replace the old files.

   Note: If you are upgrading from Registration Manager 6.9 build 551 or later, this step is not required.

8. If you are upgrading from:

   – RSA Registration Manager 6.9 build 559 or older, go to step 9

   – RSA Registration Manager 6.9 build 560, complete step 9.f, then go to step 12

   – RSA Registration Manager 6.9 build 561 or newer, go to step 12.

9. Create a backup of `INSTALL_DIR\WebServer\Conf\httpd.conf` and edit the file as follows:

   a. Add the following line for virtual hosts of Administration, Enrollment and Renewal Server above the `SSLCipherSuite` directive to disable SSLv2 and SSLv3:

      `SSLProtocol all -SSLv2 -SSLv3`

   b. For each virtual host of Administration, Enrollment, and Renewal servers, update the `SSLCipherSuite` directive as follows:

      ```
      SSLCipherSuite EDH-DSS-AES256-SHA:EDH-RSA-AES256-SHA:
         AES256-SHA:EDH-DSS-AES128-SHA:EDH-RSA-AES128-SHA:
         AES128-SHA:EDH-DSS-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:
         DES-CBC3-SHA
      ```

   c. Comment the following line:

```
SSLSessionCache none
```

    d.   Uncomment the following line:

```
SSLSessionCache dbm:logs/ssl_scache
```

    e.   Uncomment the following line:

```
SSLSessionCacheTimeout 300
```

    f.   Under `RSA RM SCEP server configuration`, add the following lines after `SSL_PKI_PORT`:

```
#verify the signature of certificate responses, '1' for
    verify '0' for disable
VerifySignature 1
```

10. Create a backup of `<INSTALL_DIR>\Xudad\conf\xudad.conf` and edit the file to add:the following line above the `cipherlist` directive to disable SSLv2 and SSLv3:

```
SSLProtocol "all -SSLv2 -SSLv3"
```

11. Create a backup of `<INSTALL_DIR>\LogServer\conf\xslogconf.xml` and edit the file to add the following line after the `ServerSSLKey` configuration parameter to disable SSLv2 and SSLv3:

```
<CONFIG_PARAM>
<!--
This parameter specifies the SSLProtocol that are allowed for
the SSL connection. This protocol is used to set up secure
communications with clients connecting to the logging server.
Default: None, this file must exist.
-->
<PARAM_NAME> SSLProtocol </PARAM_NAME>
<PARAM_VALUE> all -SSLv2 -SSLv3 </PARAM_VALUE>
</CONFIG_PARAM>
```

12. Install the Microsoft Visual C++ 2013 Redistributable Package on the target machines.

    The Redistributable Package executable file, `vcredist_x86.exe`, is in the `<INSTALL_DIR>\Utils` folder.

13. Start all Registration Manager services.

14. If you are upgrading from Registration Manager 6.9 build 560 or later, steps 15 to 17 are not required.

15. Update the profile, go to
    https://hostname:admin-port/ra/admin/updateprofiles6.9.xuda.

    The certificate extension profiles are updated.

16. Update the schema, go to
    https://hostname:admin-port/ra/admin/schemaUpdate.xuda.

    The schema is updated.

17. Restart all Registration Manager services.

Solaris or Linux Operating Systems

This hotfix does not require a new installation of the product, but rather a drop-in replacement of 154 files into the appropriate Registration Manager directory and updating the Help.

To apply Registration Manager 6.9 build 563:

1. Stop all Registration Manager services.

2. Extract the files from the appropriate .tar file provided with this drop-in package. On systems running a:

   – Red Hat Linux operating system, `SSLC_CryptoCME_Libs-RH_Linux.tar`

   – SUSE Linux operating system, `SSLC_CryptoCME_Libs-SuSE_Linux.tar`

   – Solaris operating system, `SSLC_CryptoCME_Libs-sparc-sun-solaris.tar`.

3. Replace the following files located at **/usr/lib** with the ones in the untarred folder:

   – `libccme_base.so`

   – `libccme_ecc.so`

   – `libccme_eccaccel.so`

   – `libcryptocme2.so`

   – `libcryptocme2.sig`

   Note: Make sure that you logon as the root user and give proper permissions to the users to access the library files.

4. Create a backup of the Registration Manager installation directory.

5. Copy the appropriate .tar file to the installation directory. On systems running a:

   – Solaris operating system, use `RSARM-v6.9build563r-dropin-sparc-sun-solaris.tar`.

   – Red Hat Linux operating system, use `RSARM-v6.9build563r-dropin-linux.tar`.

   – SUSE Linux operating system, use `RSARM-v6.9build563r-dropin-SuSE_linux.tar`.

6. Extract the files from the .tar file, ensuring the new files replace the old files.

7. To update the Help information, in the `INSTALL_DIR/WebServer/admin-server/ra/help` directory, extract the files from `rrm-help.tar` ensuring the new files replace the old files.

   Note: If you are upgrading from Registration Manager 6.9 build 551 or later, this step is not required.

8. Ensure the permissions and ownership of the extracted files match the permissions and ownership of other files in the same directories.

   For example, the files in the `/WebServer` directory must be readable by the user and/or group under which the server runs. If you encounter permission problems, change the ownership of the files in the `INSTALL_DIR/WebServer` directory to the user and group under which the Registration Manager Web Server was installed.

   From the `INSTALL_DIR` directory, type:

   ```
   chown -R <install_user>:<install_group> WebServer
   ```

   Note: If you modified any xuda templates in your Registration Manager installation, you must make those modifications again.

9. If you are upgrading from:

   – RSA Registration Manager 6.9 build 559 or older, go to step 10

   – RSA Registration Manager 6.9 build 560, complete step 10.f, then go to step 13

   – RSA Registration Manager 6.9 build 561 or newer, go to step 13.

10. Create a backup of `INSTALL_DIR/WebServer/conf/httpd.conf` and edit the file as follows:

    a. Add the following line for virtual hosts of Administration, Enrollment and Renewal Server above the `SSLCipherSuite` directive to disable SSLv2 and SSLv3:

    ```
    SSLProtocol all -SSLv2 -SSLv3
    ```

    b. For each virtual host of Administration, Enrollment, and Renewal servers, update the `SSLCipherSuite` directive as follows:

    ```
    SSLCipherSuite EDH-DSS-AES256-SHA:EDH-RSA-AES256-SHA:
    AES256-SHA:EDH-DSS-AES128-SHA:EDH-RSA-AES128-SHA:
    AES128-SHA:EDH-DSS-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:
    DES-CBC3-SHA
    ```

    Note: If you are using Mozilla Firefox browser, then update `SSLCipherSuite` to `AES256-SHA`.

    c. Comment the following line:

    ```
    SSLSessionCache none
    ```

    d. Uncomment the following line:

    ```
    SSLSessionCache shm:logs/ssl_scache(512000)
    ```

    e. Uncomment the following line:

    ```
    SSLSessionCacheTimeout 300
    ```

    f.   Under `RSA RM SCEP server configuration`, add the following lines after `SSL_PKI_PORT`:

```
#verify the signature of certificate responses, '1' for
    verify '0' for disable
VerifySignature 1
```

11. Create a backup of `INSTALL_DIR/Xudad/conf/xudad.conf` and edit the file to add the following line above the `cipherlist` directive to disable SSLv2 and SSLv3:

```
SSLProtocol "all -SSLv2 -SSLv3"
```

12. Create a backup of `INSTALL_DIR/LogServer/conf/xslogconf.xml` and edit the file to add the following line after `ServerSSLKey` configuration parameter to disable SSLv2 and SSLv3:

```
<CONFIG_PARAM>
<!--
This parameter specifies the SSLProtocol that are allowed for
SSL connection
This protocol is used to set up secure communications with
clients connecting to the logging server.
Default: None, this file must exist.
-->
<PARAM_NAME> SSLProtocol </PARAM_NAME>
<PARAM_VALUE> all -SSLv2 -SSLv3 </PARAM_VALUE>
</CONFIG_PARAM>
```

13. Start all Registration Manager services.

14. If you are upgrading from Registration Manager 6.9 build 560 or later, steps 15 to 17 are not required.

15. Update the profile, go to
    https://hostname:admin-port/ra/admin/updateprofiles6.9.xuda.

    The certificate extension profiles are updated.

16. Update the schema, go to
    https://hostname:admin-port/ra/admin/schemaUpdate.xuda.

    The schema is updated.

17. Restart all Registration Manager services.

Fixed Issues

This section lists the issues fixed in this release of RSA Registration Manager. For the list of issues fixed in previous releases, see the appropriate Readme documents.

Table 1   Fixed Issues

ID	Description
CERTMGR-4680	Potential SSL Diffie-Hellman key reuse (CVE-2016-0701), SSL/TLS alert message (CVE-2016-8610), and denial of service (CVE-2016-6306) vulnerabilities in RSA BSAFE Micro Edition Suite.
REGMGR-366	Registration Manager rekey or reissue operation does not produce V3 SCEP signing and SCEP encryption certificates.

Known Issues

The following table describes the issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Table 2   Known Issues

ID	Description
CERTMGR-4034	On systems running a Linux operating system, Registration Manager will not function properly if the system time is changed to beyond the year 2038.
	According to the rfc2459 "Internet X.509 Public Key Infrastructure" section 4.1.2.5, CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime.
	In Registration Manager, the certificate validity TIME is stored in the following UTCTime format: YYMMDDHHMMSSZ. Certificate Manager only supports certificates with validity up to year 2050.
CERTMGR-4173	On systems running a Solaris or Linux operating system, installing Registration Manager using Firefox, the browser fails to trust the default SSL cipher used by Registration Manager and you cannot complete the installation.
	Workaround
	While installing Registration Manager, modify the default values of the SSL Cipher Suite and the SSL Cipher as follows:
	1. Open the following files:
	– `iws/dist/iws.conf`
	– `WebServer/dist/scep.conf`
	– `WebServer/dist/admin.conf`
	– `WebServer/dist/enroll.conf`
	2. Comment the following line:

	`SSLCipherSuite EDH-DSS-AES256-SHA:EDH-RSA-AES256-SHA:`
	`AES256-SHA:EDH-DSS-AES128-SHA:EDH-RSA-AES128-SHA:AES128-SHA:`
	`EDH-DSS-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:DES-CBC3-SHA:`
	`EDH-DSS-RC4-SHA:RC4-SHA:RC4-MD5`

	3. Add the following line:
	`SSLCipherSuite AES256-SHA`
CERTMGR-4186	Installing Registration Manager on a system running the Windows 2008 operating system (32-bit and 64-bit), the Media Verify utility crashes, although the Media Sign utility works.
	Workaround
	Install Registration Manager on a system running the Windows 2003 operating system, and run the Media Sign and Media Verify utilities.
CERTMGR-4295	When a non-persistent card is inserted, then the Administration Server is not accessible if SSL keys are protected with nCipher HSM.
	Workaround
	Set `CKNFAST_NONREMOVABLE=1` in the `cknfastrc` file and restart the nCipher services

Table 2   Known Issues

ID	Description
CERTMGR-4409	While vetting the certificate requests using Internet Explorer 10 on a system running Windows 2008 R2, extensions can not be selected from Mandatory Extensions and Available Extensions list. **Workaround** Upgrade to Internet Explorer 11.
CERTMGR-4433	On systems running the Red Hat Enterprise Linux 6.4 or above operating system, Registration Manager logs incorrect information in syslog. **Workaround** Update `rsylog.conf` as follows: 1. Login in as root user where Registration Manager is installed. 2. Stop the rsyslog service using the following command: `service rsyslog stop` 3. Edit /etc/rsyslog.conf and add the following line at the end of the file: `$EscapeControlCharactersOnReceive off` 4. Start the rsyslog service using the following command: `service rsyslog start` 5. Restart all Registration Manager services.
CERTMGR-4485	Installation of Registration Manager with hardware SSL keys and System Authority keys using nCipher client version 11.70 fails with the following message: `Warning! Can't find <directory>httpd.pid to confirm httpsd is running!` The default location of the domain sockets used for communication with the hardserver was changed from `/dev/nfast` to `/opt/nfast/sockets`. Applications trying to find the sockets in their old location assume the server is not running and then fail. **Workaround** Create a file, `/etc/nfast.conf`, with `NFAST_CREATEDEVNFAST=1` in it and then restart the hardserver. This causes the hardserver to create a symlink to the current socket directories in their old location.

Table 2   Known Issues

ID	Description
CERTMGR-4682	Installing Registration Manager using Internet Explorer 11 installed on Windows 10, the browser fails to trust the default SSL cipher used by Registration Manager and you cannot complete the installation.

Workaround for systems running a Windows operating system:

1. Install Registration Manager.
2. After the installation URL displays, stop the Install Web Service for Registration Manager process.
3. Edit the following files:
   - `iws/conf/httpd.conf`
   - `WebServer/dist/admin.conf`
   - `WebServer/dist/enroll.conf`
   - `WebServer/dist/scep.conf`
4. Comment the following line:

```
SSLCipherSuite
EDH-DSS-AES256-SHA:EDH-RSA-AES256-SHA:AES256-SHA:EDH-DSS-AES1
28-SHA:EDH-RSA-AES128-SHA:AES128-SHA:EDH-DSS-DES-CBC3-SHA:EDH
-RSA-DES-CBC3-SHA:DES-CBC3-SHA
```

5. Add the following line:

```
SSLCipherSuite AES256-SHA
```

6. Restart the Install Web Service for Registration Manager process
7. Proceed with the Web-based installation using the URL.

Workaround for systems running a Solaris or Linux operating system:

1. While installing Registration Manager, edit the following files:
   - `iws/dist/iws.conf`
   - `WebServer/dist/scep.conf`
   - `WebServer/dist/admin.conf`
   - `WebServer/dist/enroll.conf`
2. Comment the following line:

```
SSLCipherSuite
EDH-DSS-AES256-SHA:EDH-RSA-AES256-SHA:AES256-SHA:EDH-DSS-AES1
28-SHA:EDH-RSA-AES128-SHA:AES128-SHA:EDH-DSS-DES-CBC3-SHA:EDH
-RSA-DES-CBC3-SHA:DES-CBC3-SHA
```

3. Add the following line:

```
SSLCipherSuite AES256-SHA
```

ID	Description
REGMGR-322	Registration Manager 6.8 does not work with RSA Certificate Manager 6.9 build 553 or above.

Workaround

Registration Manager must be upgraded to the same version as Certification Manager.

ID	Description
REGMGR-327	Unable to install renewed certificate on Microsoft Internet Explorer 9 or above on Windows 7 64-bit. The error code is 80004005.

Workaround

Add the Enrollment Server to the list of Trusted Sites.

RSA Customer Support

Access these locations for help with your RSA product:

- RSA Link

  RSA Link offers a knowledge base that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

- RSA Customer Support

  The RSA Customer Support site on RSA Link contains information on RSA support programs plus an extensive Content Library of product-related documents such as datasheets, guides and whitepapers.

- RSA Ready

  The RSA Ready Community is a platform for customers, partners, and RSA enthusiasts to learn about products certified to interoperate with RSA products including access to integration guides.

Before You Call Customer Support

Make sure you have direct access to the computer running your RSA product software.

Please have the following information available:

❑ Your RSA Customer Serial Number.

❑ The software version number of your RSA product.

❑ The make and model of the machine on which the problem occurs.

❑ The name and version of the operating system under which the problem occurs.