RSA® Registration Manager 6.9 build 560 Readme

This document lists what's new and changed in RSA® Registration Manager 6.9 build 560 (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 RSA SecurCare® Online at **https://knowledge.rsasecurity.com** or contact RSA Customer Support.

Contents:

New Features

This release of Registration Manager is designed to include the following new features:

- Transport Layer Security (TLS) 1.2 support during secure communication on Registration Manager servers, including Web Servers (Administration, Enrollment, and Renewal), Secure Directory Server, and Secure Logging Server.

Enhanced Functionality

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

- Qualification with nCipher client v11.70.
- Registration Manager now uses Apache HTTP Server 2.2.24, with additional security fixes from Apache 2.2.29.

Package Contents

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

- `RSARM-v6.9build560r-package.zip` (for systems running a Windows operating system)
- `RSARM-v6.9build560r-solaris-package.tar` (for systems running a Solaris operating system)
- `RSARM-v6.9build560r-linux-package.tar` (for systems running a Red Hat Enterprise Linux operating system)
- `RSARM-v6.9build560r-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 performing one of the following:

- Installing the Full Build
- Installing the Hotfix Files.

Installing 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-v6.9build560r-WIN32.zip`.
- Solaris operating system, use `RSARM-v6.9build560r-sparc-sun-solaris.tar`.
- Red Hat Linux operating system, use `RSARM-v6.9build560r-linux.tar`.
- SUSE Linux operating system, use `RSARM-v6.9build560r-SuSE_linux.tar`.

For instructions on installing Registration Manager, see the *Installation Guide*.

Installing the Hotfix Files

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 162 files into the appropriate Registration Manager directory and updating the Help.

To apply Registration Manager 6.9 build 560:

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 `RSACM-v6.9build560r-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 above, this step is not required.

8. If you are upgrading from Registration Manager 6.9 build 555 or later, go to step 11.
9. Create a backup of `INSTALL_DIR\Web Server\Conf\httpd.conf` and edit the file as follows:
   a. Under the section, “Apache Modules compiled into the standard Windows build”, replace the existing “LoadModule files” with the following content:

```
LoadFile modules/xuda_wrapper.dll
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule asis_module modules/mod_asis.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule authn_alias_module modules/mod_authn_alias.so
LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_user_module modules/mod_authz_user.so
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule cgi_module modules/mod_cgi.so
LoadModule dir_module modules/mod_dir.so
LoadModule env_module modules/mod_env.so
LoadModule imagemap_module modules/mod_imagemap.so
LoadModule include_module modules/mod_include.so
LoadModule isapi_module modules/mod_isapi.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule mime_module modules/mod_mime.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule reqtimeout_module modules/mod_reqtimeout.so
```

```
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule ssl_module modules/mod_ssl.so
LoadModule gencert_module modules/mod_gencert.so
LoadModule xudaacl_module modules/mod_xudaacl.so
LoadModule cmp_module modules/mod_cmp.so
```

b. Under `Section 2: 'Main' server configuration`, add the following lines:

```
<IfModule mod_reqtimeout.c>
RequestReadTimeout header=60,MinRate=500 body=60,MinRate=500
</IfModule>
```

c. Save the file.

10. Install the Microsoft Visual C++ 2005 SP1 Redistributable Package on the target machines.

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

11. 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. Save the file.

12. Create a backup of `INSTALL_DIR\Xudad\conf\xudad.conf` and edit the file as follows:

    a. Add the following line above the `cipherlist` directive to disable SSLv2 and SSLv3:

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

    b. Save the file.

13. Create a backup of `INSTALL_DIR\LogServer\conf\xslogconf.xml` and edit the file as follows:

    a. 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>
```

    b. Save the file.

14. Start all Registration Manager services.

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 147 files into the appropriate Certificate Manager directory and updating the Help.

To apply RSA Registration Manager 6.9 build 560:

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-v6.9build560r-dropin-sparc-sun-solaris.tar`.
   - Red Hat Linux operating system, use `RSARM-v6.9build560r-dropin-linux.tar`.
   - SUSE Linux operating system, use `RSARM-v6.9build560r-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 above, this step is not required.

8. If you are upgrading from RSA Certificate Manager 6.9 build 555 or later, go to step 11.
9. Create a backup of `INSTALL_DIR/Web Server/conf/httpd.conf` and edit the file as follows:
   a. Under the section, “Dynamic Shared Object (DSO) Support”, uncomment the following lines:

      ```
      LoadModule gencert_module modules/mod_gencert.so
      LoadModule xudaacl_module modules/mod_xudaacl.so
      ```

   b. Add the following line after the Load Module, `mod_xudaacl.so`:

      ```
      LoadModule cmp_module modules/mod_cmp.so
      ```

   c. Under `Section 2: 'Main' server configuration`, add the following lines:

      ```
      <IfModule mod_reqtimeout.c>
      RequestReadTimeout header=60,MinRate=500 body=60,MinRate=500
      </IfModule>
      ```

   d. Save the file.

10. 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.

11. Create a backup of `INSTALL_DIR/Web Server/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. Uncomment the following line:

    ```
    SSLSessionCache none
    ```

    d. Comment the following line:

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

    e. Uncomment the following line:

    ```
    SSLSessionCacheTimeout 300
    ```

    f. Save the file.

12. Create a backup of `INSTALL_DIR/Xudad/conf/xudad.conf` and edit the file as follows:

    a. Add the following line above the `cipherlist` directive to disable SSLv2 and SSLv3:

    ```
    SSLProtocol “all -SSLv2 -SSLv3”
    ```

    b. Save the file.

13. Create a backup of `INSTALL_DIR/LogServer/conf/xslogconf.xml` and edit the file as follows:

    a. 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>
```

    b. Save the file.

14. Start all Registration Manager services.

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 Registration Manager. For the list of issues fixed in previous releases, see the appropriate Readme document.

Table 1 Fixed Issues

ID	Description
CERTMGR-4459, CERTMGR-4482	Registration Manager fails to validate the `validUntilPeriodYear` while issuing a certificate.
CERTMGR-4467	For certificate requests, email notifications are being sent to suspended vettors and administrators.
CERTMGR-4497	When daylight saving is observed, on systems running a UNIX operating system Registration Manager fails to send certificate expiry notification.
CERTMGR-4499	Administration Server crashes while creating a CA or vetting a certificate request with Certificate Policies extension if the number of Policy Qualifier Information objects is set to 1 and the UserNotice attribute is configured in the extension profile script.
CERTMGR-4515	Registration Manager is susceptible to the following security vulnerabilities: CVE-2010-4180 and CVE-2015-0204.
CERTMGR-4526	On systems running a Linux operating system, Registration Manager fails to import LDIF files greater than 2GB in size.
CERTMGR-4536	On systems running a Windows Server 2012 operating system, enforced with Group Policy settings, Registration Manager Secure Directory Server crashes when upgrading from 6.8 build 522 to 6.9 build 558.
CERTMGR-4542	Registration Manager Server Directory Server memory usage increases if auto notification for certificate expiry is enabled.
CERTMGR-4551	Registration Manager Administration Server crashes if a PKCS #10 request contains an invalid encoding type for an attribute.
REGMGR-354	Certificate Manager produces an `XrcWRITEFAILURE` error while approving a certificate request.
REGMGR-359	While vetting a certificate request, extensions are not included if the same certificate name is already present in the database.

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 lines:
	`SSLCipherSuite AES256-SHA`
	`SSLProtocol +TLSv1`

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.
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.
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 SecurCare Online

  RSA SecurCare Online 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 contains information on RSA support programs plus an extensive Content Library of product-related documents such as datasheets, guides and whitepapers.

- RSA Ready Community

  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.