

RSA® Certificate Manager API 6.9 build 563 Readme

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

For the complete Certificate Manager API documentation set, go to the Certificate Manager API page on [RSA Link](#) or contact [RSA Customer Support](#).

Contents:

New Features	2
Enhanced Functionality	2
Package Contents	3
Installation	4
Install the Full Build	4
Install the Hot Fix Files	5
Fixed Issues	9
Known Issues	9
RSA Customer Support	10

New Features

There are no new features in this release of Certificate Manager API.

Enhanced Functionality

This release of Certificate Manager API 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

As well as the above, the following libraries are required for building the Certificate Manager API programs on Red Hat Enterprise Linux 7.3:

- `cpp-4.8.5-11.e17.x86_64.rpm`
- `glibc-headers-2.17-157.e17.x86_64.rpm`
- `glibc-devel-2.17-157.e17.x86_64.rpm`
- `libmpc-1.0.1-3.e17.x86_64.rpm`
- `mpfr-3.1.1-4.e17.x86_64.rpm`
- `gcc-4.8.5-11.e17.x86_64.rpm`
- `gcc-c++-4.8.5-11.e17.x86_64.rpm`
- `libstdc++-devel-4.8.5-11.e17.x86_64.rpm`
- `libstdc++-static.i686.rpm`
- `libstdc++-static.x86_64.rpm`
- On systems running Solaris 10, upgraded compiler from gcc 2.9.5 to gcc 3.4.6 and qualified on Solaris 10 update 11.

Note: Support for gcc 2.9.5 is removed.

- On systems running a Windows operating system, added support for Visual Studio 2013.

Note: Support for Visual Studio 6 and Visual Studio 2005 is removed.

- Upgraded cryptographic hardware device support:
 - nCipher client v12.3
 - Luna SA 6
- Fixes for specific issues. For more information, see [“Fixed Issues” on page 9](#).

Package Contents

The Certificate Manager API package for this release is designed to contain the following:

- `RSACMAPI-v6.9build563r-package.zip` (for systems running a Windows operating system)
- `RSACMAPI-v6.9build563r-solaris-package.tar` (for systems running a Solaris operating system)
- `RSACMAPI-v6.9build563r-linux-package.tar` (for systems running a Red Hat Enterprise Linux operating system)
- `RSACMAPI-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 *Reference Manual*.

Installation

Install the Full Build

To install the full build of Certificate Manager API for C, use the appropriate file from this package and follow the steps outlined in the *Reference Manual*. On systems running a:

- Windows operating system, for:
 - Visual Studio 2013, use
`RSACMAPI-v6.9build563r-WIN32_VS2013.zip`.
 - Visual Studio 2008, use
`RSACMAPI-v6.9build563r-WIN32_VS2008.zip`.
- Solaris operating system, use
`RSACMAPI-v6.9build563r-sparc-sun-solaris.tar`.
- Red Hat Linux operating system, use
`RSACMAPI-v6.9build563r-linux.tar`.
- SUSE Linux operating system, use
`RSACMAPI-v6.9build563r-SuSE_linux.tar`.

To install the full build of Certificate Manager API for Java, use the appropriate file from this package and follow the steps outlined in the *Java API Developer's Guide*. On systems running a:

- Windows operating system, use
`RSACMAPI-java-v6.9build563r-WIN32.zip`.
- Solaris operating system, use
`RSACMAPI-java-v6.9build563r-sparc-sun-solaris.tar`.
- Red Hat Linux operating system, use
`RSACMAPI-java-v6.9build563r-linux.tar`.
- SUSE Linux operating system, use
`RSACMAPI-java-v6.9build563r-SuSE_linux.tar`.

Install the Hot Fix Files

This section describes how to install the hotfix files for this release. Instructions for the following platforms are provided:

- [Windows Operating System](#)
- [Solaris or Linux Operating System](#).

Windows Operating System

To apply Certificate Manager API 6.9 build 563:

1. Back up `API_INSTALL\lib\xuda.lib` (`API_INSTALL` is the directory path where Certificate Manager API is installed).
2. If you are upgrading from Certificate Manager API 6.9 build 558 or earlier, upgrade to Certificate Manager API 6.9 build 560 before proceeding with these instructions.
3. If you are upgrading from Certificate Manager API 6.9 build 560 or later:
 - a. Copy the hotfix .zip file to the `API_INSTALL` directory. On systems with:
 - Visual Studio 2008, use `RSACMAPI-v6.9build563r-dropin-WIN32_VS2008.zip`.
 - Visual Studio 2013, use `RSACMAPI-v6.9build563r-dropin-WIN32_VS2013.zip`.
 - b. Extract the file from the .zip file, ensuring the new file replaces the old one.
4. Extract the files from `SSLC_CryptoCME_Libs-WIN32.zip` provided with the full build package.
5. 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`
6. Perform an API samples rebuild.

Note: API samples must be recompiled to ensure that the new `xuda.lib` and `mesabstraction.dll` files are used.

For more information, see the *Reference Manual*.

7. Copy `mesabstraction.dll` to the location where your application is running.

RSA Certificate Manager API 6.9 build 563 Readme

To apply Certificate Manager API 6.9 build 563 for Java:

1. Back up `API_INSTALL\lib\rormapinative.dll` (`API_INSTALL` is the directory path where Certificate Manager API is installed).
2. If you are upgrading from Certificate Manager API 6.9 build 558 or earlier, upgrade to Certificate Manager API 6.9 build 560 before proceeding with these instructions.
3. Copy the hotfix .zip file, `RSACMAPI-java-v6.9build563r-dropin-WIN32.zip`, and extract the file from the .zip file, ensuring the new file replaces the old one.
4. Install the Microsoft Visual C++ 2013 Redistributable Package on the target machines.

The Redistributable Package executable file, `vc_redist_x86.exe`, is in the `VS2013_Redistributable` folder.

5. Extract the files from `SSLC_CryptoCME_Libs-WIN32.zip` provided with this full build package.
6. 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`

7. Perform an API samples rebuild.

Note: API samples must be recompiled to ensure that the new `rormapinative.dll` and `mesabstraction.dll` files are used.

For more information, see the *Reference Manual*.

8. Copy `mesabstraction.dll` to the location where your application is running.

Solaris or Linux Operating System

To apply Certificate Manager API 6.9 build 563:

1. Back up `API_INSTALL/lib/libxuda.a` (`API_INSTALL` is the directory path where Certificate Manager API is installed).
2. If you are upgrading from Certificate Manager API 6.9 build 558 or earlier, upgrade to Certificate Manager API 6.9 build 560 before proceeding with these instructions.
3. Copy the hotfix .tar file to the `API_INSTALL` directory. On systems running a:
 - Solaris operating system,
`RSACMAPI-v6.9build563r-dropin-sparc-sun-solaris.tar`.
 - Red Hat Linux operating system,
`RSACMAPI-v6.9build563r-dropin-linux.tar`.
 - SUSE Linux operating system,
`RSACMAPI-v6.9build563r-dropin-SuSE_linux.tar`.
4. Extract the file from the .tar file, ensuring the new file replaces the old one.
5. Extract the following .tar file provided with this package. On systems running a:
 - Solaris operating system,
`SSL_CryptoCME_Libs-sparc-sun-solaris.tar`.
 - Red Hat Linux operating system,
`SSL_CryptoCME_Libs-RH_Linux.tar`.
 - SUSE Linux operating system,
`SSL_CryptoCME_Libs-SuSE_Linux.tar`.
6. 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.

7. Perform an API samples rebuild.

Note: API samples must be recompiled to ensure that the new `libxuda.a` and `libmesabstraction.so` files are used.

For more information, see the *Reference Manual*.

8. Copy `libmesabstraction.so` to the location where your application is running.

RSA Certificate Manager API 6.9 build 563 Readme

To apply Certificate Manager API 6.9 build 563 for Java:

1. Back up `API_INSTALL/lib/librcmapinative.so` (`API_INSTALL` is the directory path where Certificate Manager API is installed)
2. If you are upgrading from Certificate Manager API 6.9 build 558 or earlier, upgrade to Certificate Manager API 6.9 build 560 before proceeding with these instructions.
3. Copy the hotfix .tar file to the `API_INSTALL` directory. On systems running a:
 - Solaris operating system,
`RSACMAPI-java-v6.9build563r-dropin-sparc-sun-solaris.tar`.
 - Red Hat Linux operating system,
`RSACMAPI-java-v6.9build563r-dropin-linux.tar`.
 - SUSE Linux operating system,
`RSACMAPI-java-v6.9build563r-dropin-SuSE_linux.tar`.
4. Extract the file from the .tar file, ensuring the new file replaces the old one.
5. Extract the following .tar file provided with this package. On systems running a:
 - Solaris operating system, use
`SSL_CryptoCME_Libs-sparc-sun-solaris.tar`
 - Redhat Linux operating system, use
`SSL_CryptoCME_Libs-RH_Linux.tar`
 - SUSE Linux operating system, use
`SSL_CryptoCME_Libs-SuSE_Linux.tar`.
6. 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.

7. Perform an API samples rebuild.

Note: API samples must be recompiled to ensure that the new `librcmapinative.so` and `libmesabstraction.so` files are used.

For more information, see the *Reference Manual*.

8. Copy `libmesabstraction.so` to the location where your application is running.

Fixed Issues

This section lists the issues fixed in this release of Certificate Manager API. 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.

Known Issues

There are no known issues in this release of Certificate Manager API.

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.