

# Readme RSA® Key Recovery Manager 6.9 build558 for RSA Certificate Manager



February 25, 2015

---

## Introduction

This document includes installation information, fixed issues, as well as workarounds for known issues in RSA® Key Recovery Manager 6.9 build558. Read this document before installing the software. This document contains the following sections:

- [New Features](#)
- [Enhanced Functionality](#)
- [Existing Features](#)
- [Package Contents](#)
- [Distribution Media Verification](#)
- [Installation](#)
- [Fixed Issues](#)
- [Support and Service](#)

For the complete RSA Key Recovery Manager 6.9 documentation set, go to RSA SecurCare® Online at <https://knowledge.rsasecurity.com> or contact RSA Customer Support.

---

Note: You must install RSA Certificate Manager 6.9 build558 before you install RSA Key Recovery Manager 6.9 build558 for RSA Certificate Manager. For Certificate Manager installation instructions, see the *RSA Certificate Manager 6.9 build558 Readme*. To install RSA Key Recovery Manager 6.9 build558 for RSA Registration Manager, see the *RSA Key Recovery Manager 6.9 build558 for RSA Registration Manager Readme*.

---

## New Features

### Support for New Platforms

RSA Key Recovery Manager 6.9 build 558 for RSA Certificate Manager can be installed on Red Hat Enterprise Linux (RHEL) 6.5 64-bit operating system, Microsoft Windows Server 2012 Enterprise Edition, and Windows Server 2012 R2 Enterprise Edition.

You must install the following libraries while installing the RHEL 6.5 operating system:

- libstdc++.so.
- Compatible libraries

These libraries can be installed from the following packages available in the Red Hat Linux 6.5 installation CD:

- libstdc++-4.4.7-4.el6.i686.rpm

## Enhanced Functionality

### Support for Internet Explorer 11

RSA Key Recovery Manager 6.9 build 558 for RSA Certificate Manager is designed to support Internet Explorer 11 on Windows Server 2008 R2 Enterprise Edition, Windows 7, Windows 8.1 and Windows Server 2012 R2 Enterprise Edition.

### Support for Firefox 31

RSA Key Recovery Manager 6.9 build558 for RSA Certificate Manager is engineered to support Firefox 31

### Luna SA v5.4.3-1 qualification with RSA Key Recovery Manager

RSA Key Recovery Manager 6.9 build558 for RSA Certificate Manager is qualified with Luna SA v5.4.3-1 with Client v5.4.2.

---

## Existing Features

This section describes the features introduced or enhanced in the previous releases.

### Support for nCipher security world with AES (SP800-131) algorithm

RSA Key Recovery Manager 6.9 build 557 for Certificate Manager is engineered to support nCipher security world with AES (SP800-131) algorithm. RSA Key Recovery Manager 6.9 build 557 for Certificate Manager is updated with nCipher libraries v11.62

### Support for Internet Explorer 10

RSA Key Recovery Manager 6.9 build 555 is engineered to support Internet Explorer 10 for Administration and Enrollment on Windows 2008 and Windows 8 platform.

### Support for New Platforms

RSA Key Recovery Manager 6.9 build555 for RSA Certificate Manager can be installed on Red Hat Enterprise Linux (RHEL) 6.3 64-bit operating system.

You must install the following libraries while installing the operating system:

- libstdc++.so.
- Compatible libraries

These libraries can be installed from the following packages available in the Red Hat Linux 6.3 installation CD:

- libstdc++-4.4.6-4.el6.i686.rpm

### Support for VMWare ESXi v5.1

RSA Key Recovery Manager 6.9 build555 for RSA Certification Manager is enhanced to support VMware ESXi Server 5.1 for the following platforms:

- Windows Server 2003 with Service Pack 2
- Windows Server 2008 with Service Pack 2
- Windows Server 2008 R2 64-bit with Service Pack 1
- Red Hat Enterprise Linux 5.5/6.3
- SUSE Linux Enterprise Server 11 Service Pack 1

RSA Key Recovery Manager for RSA Certification Manager is engineered to support the following features on VMware ESXi Server 5.1:

- Cloning
- Snapshots

RSA Key Recovery Manager 6.9 build555 for RSA Certification Manager has been tested with network-based hardware security modules (HSMs), such as SafeNet LunaSA and nCipher nethSM, with guest operating systems running on VMware ESXi Server 5.1. RSA Key Recovery Manager for RSA Certification Manager is not tested with PCI-based or SCSI-based HSMs

---

## Package Contents

The RSA Key Recovery Manager 6.9 build558 package contains:

### Software

For Windows:

- Media verification file associated with the hotfix:  
media.sig
- Files (zipped) associated with the hotfix:
  - WebServer\admin-server\ca\admin-navbar.html
  - WebServer\admin-server\ca\ca-ops\ca-juri-config.xuda
  - WebServer\admin-server\ca\ca-ops\config-domain-logmsg.xuda
  - WebServer\admin-server\ca\ca-ops\config-domain-modify.xuda
  - WebServer\admin-server\ca\ca-ops\config-domain-print.xuda
  - WebServer\admin-server\ca\ca-ops\config-domain-query.xuda
  - WebServer\admin-server\ca\cert-ops\shared\cc-cert-view.html
  - WebServer\admin-server\ca\cert-ops\shared\cert-view.html
  - WebServer\admin-server\ca\help\rcm-krm-help.zip
  - WebServer\enroll-server\get-cert.xuda
  - WebServer\enroll-server\get-encryption-cert-onestep.xuda
  - WebServer\enroll-server\request-msie-kro.xuda
  - WebServer\scripts\library.js
  - WebServer\x-templates\x-construct-domain-form.xuda
  - Xudad\bin\mfProvider.dll
  - Xudad\bin\pkcs11Provider.dll

For Solaris, RedHat Linux, and SUSE Linux:

- Media verification file associated with the hotfix:  
media.sig
- Files (tarred) associated with the hotfix:
  - WebServer/admin-server/ca/admin-navbar.html
  - WebServer/admin-server/ca/ca-ops/ca-juri-config.xuda
  - WebServer/admin-server/ca/ca-ops/config-domain-logmsg.xuda

WebServer/admin-server/ca/ca-ops/config-domain-modify.xuda  
WebServer/admin-server/ca/ca-ops/config-domain-print.xuda  
WebServer/admin-server/ca/ca-ops/config-domain-query.xuda  
WebServer/admin-server/ca/cert-ops/shared/cc-cert-view.html  
WebServer/admin-server/ca/cert-ops/shared/cert-view.html  
WebServer/admin-server/ca/help/rcm-krm-help.tar  
WebServer/enroll-server/get-cert.xuda  
WebServer/enroll-server/get-encryption-cert-onestep.xuda  
WebServer/enroll-server/request-msie-kro.xuda  
WebServer/scripts/library.js  
WebServer/x-templates/x-construct-domain-form.xuda  
Xudad/bin/nfProvider.so  
Xudad/bin/pkcs11Provider.so

## Documentation

The product documentation is a printable PDF of this *Readme*.

---

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

---

## Distribution Media Verification

### On Windows

To verify the download package:

1. From the FTP server, download the release package.
2. Unzip the hotfix files into an empty working directory (for example, C:\temp\verifyPath\).
3. Locate the mediaverify.exe executable in the *INSTALL\_DIR*\Utils folder of the Certificate Manager installation.
4. From the command prompt in the working directory, type:  
`<path from Certificate Manager installation>\Utils\mediaverify.exe .`
5. Check the success message at the end of the output and verify that the media verification utility did not report any errors.

If there are any errors, contact RSA Customer Support. For a list of error messages, see the *Administrator's Guide*.

If the verification is successful, you see output similar to the example shown in Appendix C of the *Installation Guide*.

### On Solaris or Linux

To verify the download package:

1. From the FTP server, download the release package.
2. Untar the hotfix files into an empty working directory (for example, */home directory/verifyPath/*).
3. Locate the mediaverify executable in the *INSTALL\_DIR*\Utils folder of the Certificate Manager installation.

4. From the command prompt in the working directory, type:  
    <path from Certificate Manager installation>/Utils/mediaverify .
5. Check the success message at the end of the output and verify that the media verification utility did not report any errors.

If there are any errors, contact RSA Customer Support. For a list of error messages, see the *Administrator's Guide*.

If the verification is successful, you see output similar to the example shown in Appendix C of the *Installation Guide*.

## Installation

To install RSA Key Recovery Manager 6.9 build558 for RSA Certificate Manager, you must perform one of the following:

- [Installing the Full Build](#)
- [Installing the Hotfix files](#)

### Installing the Full Build

If you want to install a full build of RSA Key Recovery Manager 6.9 build558 for Certificate Manager, use the following files that come with this package, and follow the procedure described in the *RSA Key Recovery Manager Administrator's Guide*:

- On Windows, use RSAKRM-CM-v6.9build558r-WIN32.zip.
- On Solaris, use RSAKRM-CM-v6.9build558r-sparc-sun-solaris.tar.
- On RedHat Linux, use RSAKRM-CM-v6.9build558r-linux.tar.
- On SUSE Linux, use RSAKRM-CM-v6.9build558r-SuSE\_linux.tar.

### Installing the Hotfix files

This section describes how to install the hotfix files.

#### On Windows

This hotfix does not require a new installation of the product, but rather a drop-in replacement of 16 files into the appropriate Certificate Manager directory and the unzipping of a .zip file to update the Help.

To apply RSA Key Recovery Manager 6.9 build558:

1. Stop all Certificate Manager services.
2. Create a backup of the following files (*INSTALL\_DIR* is the directory path where Certificate Manager is installed):
  - `INSTALL_DIR\WebServer\admin-server\ca\admin-navbar.html`
  - `INSTALL_DIR\WebServer\admin-server\ca\ca-ops\ca-juri-config.xuda`
  - `INSTALL_DIR\WebServer\admin-server\ca\ca-ops\config-domain-logmsg.xuda`
  - `INSTALL_DIR\WebServer\admin-server\ca\ca-ops\config-domain-modify.xuda`
  - `INSTALL_DIR\WebServer\admin-server\ca\ca-ops\config-domain-print.xuda`
  - `INSTALL_DIR\WebServer\admin-server\ca\ca-ops\config-domain-query.xuda`
  - `INSTALL_DIR\WebServer\admin-server\ca\cert-ops\shared\cc-cert-view.html`
  - `INSTALL_DIR\WebServer\admin-server\ca\cert-ops\shared\cert-view.html`
  - `INSTALL_DIR\WebServer\admin-server\ca\help\rcm-krm-help.zip`
  - `INSTALL_DIR\WebServer\enroll-server\get-cert.xuda`
  - `INSTALL_DIR\WebServer\enroll-server\get-encryption-cert-onestep.xuda`
  - `INSTALL_DIR\WebServer\enroll-server\request-msie-kro.xuda`
  - `INSTALL_DIR\WebServer\scripts\library.js`
  - `INSTALL_DIR\WebServer\x-templates\x-construct-domain-form.xuda`
  - `INSTALL_DIR\Xudad\bin\InfProvider.dll`
  - `INSTALL_DIR\Xudad\bin\pkcs11Provider.dll`

3. Copy the zipped file to the *INSTALL\_DIR* directory.
4. Unzip and extract the files ensuring that the new files replace the old files.

---

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

---

5. To update the Help, in the *INSTALL\_DIR*\WebServer\admin-server\ca\help directory, unzip and extract the files from rcm-krm-help.zip ensuring that the new files replace the old files.

However, if you are upgrading from RSA Key Recovery Manager 6.9 build551 or above for RSA Certificate Manager, this is not required.

6. Start all Certificate Manager services.

## On Solaris or Linux

This hotfix does not require a new installation of the product, but rather a drop-in replacement of 16 files into the appropriate Certificate Manager directory and the untarring of a .tar file to update the Help.

To apply RSA Key Recovery Manager 6.9 build558:

1. Stop all Certificate Manager services.
2. Create a backup of the following files (*INSTALL\_DIR* is the directory path where Certificate Manager is installed):
  - *INSTALL\_DIR*/WebServer/admin-server/ca/admin-navbar.html
  - *INSTALL\_DIR*/WebServer/admin-server/ca/ca-ops/ca-juri-config.xuda
  - *INSTALL\_DIR*/WebServer/admin-server/ca/ca-ops/config-domain-logmsg.xuda
  - *INSTALL\_DIR*/WebServer/admin-server/ca/ca-ops/config-domain-modify.xuda
  - *INSTALL\_DIR*/WebServer/admin-server/ca/ca-ops/config-domain-print.xuda
  - *INSTALL\_DIR*/WebServer/admin-server/ca/ca-ops/config-domain-query.xuda
  - *INSTALL\_DIR*/WebServer/admin-server/ca/cert-ops/shared/cc-cert-view.html
  - *INSTALL\_DIR*/WebServer/admin-server/ca/cert-ops/shared/cert-view.html
  - *INSTALL\_DIR*/WebServer/admin-server/ca/help/rcm-krm-help.tar
  - *INSTALL\_DIR*/WebServer/enroll-server/get-cert.xuda
  - *INSTALL\_DIR*/WebServer/enroll-server/get-encryption-cert-onestep.xuda
  - *INSTALL\_DIR*/WebServer/enroll-server/request-msie-kro.xuda
  - *INSTALL\_DIR*/WebServer/scripts/library.js
  - *INSTALL\_DIR*/WebServer/x-templates/x-construct-domain-form.xuda
  - *INSTALL\_DIR*/Xudad/bin/nfProvider.so
  - *INSTALL\_DIR*/Xudad/bin/pkcs11Provider.so
3. Copy the tar file to the *INSTALL\_DIR* directory.
4. Untar and extract the files ensuring that the new files replace the old files.
5. To update the Help, in the *INSTALL\_DIR*/WebServer/admin-server/ca/help directory, untar and extract the files from rcm-krm-help.tar ensuring that the new files replace the old files.

However, if you are upgrading from RSA Key Recovery Manager 6.9 build551 or above for RSA Certificate Manager, this is not required.

6. Ensure that the permissions and ownership of the untarred 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 Certificate 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 Key Recovery Manager installation, you must make those modifications again.

---

7. Start all Certificate Manager services.

---

## Fixed Issues

This section lists the issues that have been fixed in the previous releases:

| Tracking Number   | Description   | Resolution   |
|-------------------|---|--|
| Fixed in build551 |   |  |
| CERTMGR-3935      | When a certificate was downloaded from the Enrollment Server, the filename began with a quotation mark ("). | This issue is resolved in RSA Key Recovery Manager 6.9 build551. |

---

---

## Support and Service

|   |   |
|---|---|
| RSA SecurCare® Online                   | <a href="https://knowledge.rsasecurity.com">https://knowledge.rsasecurity.com</a>   |
| Customer Support Information            | <a href="http://www.emc.com/support/rsa/index.htm">www.emc.com/support/rsa/index.htm</a>  |
| RSA Secured Partner Solutions Directory | <a href="https://community.emc.com/community/connect/rsaxchange/rsa-ready?view=overview">https://community.emc.com/community/connect/rsaxchange/rsa-ready?view=overview</a> |

---

Copyright © 2015 EMC Corporation. All Rights Reserved. Published in the USA.

## Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to <http://www.emc.com/legal/emc-corporation-trademarks.htm#rsa>.