

Readme

RSA® Registration Manager 6.9 build555



February 28, 2014

Introduction

This document lists what's new and changed in RSA® Registration Manager 6.9 build555. It includes installation information, as well as workarounds for known issues. Read this document before installing the software. This document contains the following sections:

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

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

New Features

This section describes the new features engineered to be included in this release.

Support for Internet Explorer 10

RSA Registration Manager 6.9 build 555 supports Internet Explorer 10 for Administration and Enrollment on Windows 2008 and Windows 8.

Support for new Platforms

RSA Registration Manager 6.9 build 555 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 Registration Manager is supported on 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

Registration Manager supports the following features on VMware ESXi Server 5.1

- Cloning
- Snapshots

RSA Registration Manager 6.9 build 555 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. Registration Manager is not tested with PCI-based or SCSI-based HSMs.

Upgrade Libraries

The following embedded components of RSA Registration Manager have been upgraded to the most recent secure versions:

- Apache HTTP Server 2.2.22 with additional security fixes from Apache 2.2.23
- RSA B-Safe SSL-C 2.8.8.1

Ability to Search for a Certificate Using the Serial Number

You can now search for a certificate by the serial number using the RSA Registration Manager Administration Server interface.

To search for a certificate by the serial number:

1. On the Registration Manager Administration Server interface, click **Certificate Operations**.
2. Select the **Jurisdiction** and the **Status** of the certificate you are searching for.
3. From the search filters, select the qualifier, **Serial Number**.

The screenshot shows the RSA Registration Manager Administration Server interface. The top navigation bar includes the RSA logo and four icons: Certificate Operations, Administrator Operations, System Configuration, and Auditor Operations. The main content area is titled "Certificate Search" and features a search form. The form includes a "Jurisdiction" dropdown menu set to "targetrm's Initial Jurisdiction" and a "Status" dropdown menu set to "Active". Below these are three search filter rows, each with a "Qualifier" dropdown menu and a "Value" text box. The first row has "Serial Number" selected in the Qualifier dropdown and "FEB4C0123A32293F030ED5A" in the Value text box. The second and third rows have "No Qualifier" selected. Below the filters are radio buttons for "And" (selected) and "Or", and two buttons: "List All Active" and "Search". A sidebar on the left contains a "Certificate Operations" menu with sub-items: Requests (active, approved, deferred, refused), Certificates (active, suspended, revoked), and Reporting.

4. Provide the serial number of the certificate in the corresponding text box, and click **Search**.
A link to the certificate that has the specified serial number is displayed.
5. Click the link to the certificate.
The certificate opens in a new window.

Package Contents

The RSA Registration Manager 6.9 build555 package contains:

Software

For Windows:

- Media verification file associated with the hotfix:
media.sig
- Files (zipped) associated with the hotfix:
 - LogServer\bin\xslogmgr.exe
 - LogServer\bin\xslogsrv.exe
 - LogServer\bin\xslogsrvStrings.dll
 - Upgrader\bin\setupSSL.exe
 - Upgrader\bin\setupSSLStrings.dll
 - Upgrader\bin\upgrader.exe
 - Upgrader\bin\xu_ldbmcats.exe
 - Utils\ppencryption.exe
 - Utils\vcrcdist_x86.exe
 - WebServer\admin-server\ra\about.xuda
 - WebServer\admin-server\ra\admin\schemaUpdate.xuda
 - WebServer\admin-server\ra\admin\updateprofiles6.9.xuda
 - WebServer\admin-server\ra\admin-navbar.html
 - WebServer\admin-server\ra\admin-ops\rekey\racertretrieval.xuda
 - WebServer\admin-server\ra\admin-ops\rekey\rarekey-main.xuda
 - WebServer\admin-server\ra\admin-ops\rmjuri-rmops.xuda
 - WebServer\admin-server\ra\cert-ops\cert-report-results.xuda
 - WebServer\admin-server\ra\cert-ops\cert-search.html
 - WebServer\admin-server\ra\cert-ops\req-search.html
 - WebServer\admin-server\ra\cert-ops\shared\cc-fwd-cert-view.html
 - WebServer\admin-server\ra\cert-ops\shared\cert-edit.html
 - WebServer\admin-server\ra\cert-ops\shared\cert-publish.xuda
 - WebServer\admin-server\ra\cert-ops\shared\cert-renewal-policy.html
 - WebServer\admin-server\ra\cert-ops\shared\cert-role-edit.html
 - WebServer\admin-server\ra\cert-ops\shared\cert-send-msie.xuda
 - WebServer\admin-server\ra\cert-ops\shared\cert-vet-edit.html
 - WebServer\admin-server\ra\cert-ops\shared\cert-view.html
 - WebServer\admin-server\ra\cert-ops\shared\get-endEntity-cert.xuda
 - WebServer\admin-server\ra\cert-ops\shared\req-authorize.xuda
 - WebServer\admin-server\ra\cert-ops\shared\req-edit.html
 - WebServer\admin-server\ra\cert-ops\shared\req-get-extensions.xuda

WebServer\admin-server\ra\cert-ops\shared\status-change-details.xuda
WebServer\admin-server\ra\cert-ops\shared\view-cert.xuda
WebServer\admin-server\ra\config\domain-config-sync.xuda
WebServer\admin-server\ra\config\log-control.xuda
WebServer\admin-server\ra\config\profile-editor.xuda
WebServer\admin-server\ra\help\rrm-help.zip
WebServer\admin-server\ra\popup-frameset.html
WebServer\bin\apache.exe
WebServer\bin\libapr-1.dll
WebServer\bin\libapriconv-1.dll
Webserver\bin\libaprutil-1.dll
Webserver\bin\libhttpd.dll
WebServer\bin\strongStrings.dll
WebServer\enroll-server\auto-add-msie-request.xuda
WebServer\enroll-server\cert-search-script.xuda
WebServer\enroll-server\exttests.js
WebServer\enroll-server\get-cert.xuda
WebServer\enroll-server\get-cert-msie.xuda
WebServer\enroll-server\get-endEntity-cert.xuda
WebServer\enroll-server\icontrol.vbs
WebServer\enroll-server\request-dc.xuda
WebServer\enroll-server\request-msie.xuda
WebServer\enroll-server\request-msie-admin.xuda
WebServer\enroll-server\send-ca-cert.xuda
WebServer\enroll-server\view-cert.xuda
WebServer\extensions\policyQualifierInfo.xuda
WebServer\extensions\qualifiedCertificateStatements.xuda
WebServer\images\corner.gif
WebServer\images\enrollbg.gif
WebServer\modules\mod_actions.so
WebServer\modules\mod_alias.so
WebServer\modules\mod_asis.so
WebServer\modules\mod_auth_basic.so
WebServer\modules\mod_authn_alias.so
WebServer\modules\mod_authn_anon.so
WebServer\modules\mod_authn_file.so
WebServer\modules\mod_authz_groupfile.so
WebServer\modules\mod_authz_host.so
WebServer\modules\mod_authz_user.so

WebServer\modules\mod_autoindex.so
WebServer\modules\mod_cgi.so
WebServer\modules\mod_cmp.so
WebServer\modules\mod_dir.so
WebServer\modules\mod_env.so
WebServer\modules\mod_gencert.so
WebServer\modules\mod_imagemap.so
WebServer\modules\mod_include.so
WebServer\modules\mod_isapi.so
WebServer\modules\mod_log_config.so
WebServer\modules\mod_mime.so
WebServer\modules\mod_negotiation.so
WebServer\modules\mod_reqtimeout.so
WebServer\modules\mod_rewrite.so
WebServer\modules\mod_setenvif.so
WebServer\modules\mod_ssl.so
WebServer\modules\mod_userdir.so
WebServer\modules\mod_xdaacl.so
WebServer\modules\xuda_wrapper.dll
WebServer\OneStep\cgi-bin\onestep.exe
WebServer\OneStep\samples\htmldocs\corner.gif
WebServer\OneStep\samples\htmldocs\enroll_lotus.html
WebServer\OneStep\samples\htmldocs\enroll_msie_ace.html
WebServer\OneStep\samples\htmldocs\enroll_msie_flat.html
WebServer\OneStep\samples\htmldocs\enroll_msie_ldap.html
WebServer\OneStep\samples\htmldocs\enroll_ns_flat.html
WebServer\OneStep\samples\htmldocs\enrollbg.gif
WebServer\OneStep\samples\htmldocs\error.html
WebServer\OneStep\samples\htmldocs\icontrol.vbs
WebServer\OneStep\samples\htmldocs\index_lotus.html
WebServer\OneStep\samples\htmldocs\install_lotus.html
WebServer\OneStep\samples\htmldocs\install_msie.html
WebServer\OneStep\samples\htmldocs\install_ns.html
WebServer\OneStep\samples\htmldocs\success_msie.html
WebServer\OneStep\setup\setupSSL.conf
WebServer\OneStep\setup\setupSSL.exe
WebServer\OneStep\setup\setupSSLStrings.dll
WebServer\scripts\BackupConfig.js
WebServer\scripts\CA.js

WebServer\scripts\EndEntity.js
WebServer\scripts\exttests.js
WebServer\scripts\icontrol.vbs
WebServer\scripts\library.js
WebServer\scripts\RenewalAttributes.js
WebServer\scripts\SubjectRenewalAttributes.js
WebServer\scripts\support.js
WebServer\scripts\ttl.js
WebServer\scripts\upgrade.js
WebServer\scripts\Validation.js
WebServer\scripts\ValidityPeriod.js
WebServer\x-templates\x-construct-domain-form.xuda
WebServer\x-templates\x-email-admin-vettor.xuda
WebServer\x-templates\x-sca-type-input.xuda
WebServer\x-templates\x-userInfo-input.xuda
WebServer\x-templates\x-xenroll-include.xuda
Xudad\bin\xudad.exe
Xudad\bin\xudadStrings.dll

For Solaris, RedHat Linux and SUSE Linux:

- Media verification file associated with the hotfix:

media.sig

- Files (tarred) associated with the hotfix:

LogServer/bin/xslogmgr
LogServer/bin/xslogsrv
LogServer/bin/xslogsrvStrings.so
Upgrader/bin/setupSSL
Upgrader/bin/setupSSLStrings.so
Upgrader/bin/upgrader
Upgrader/bin/xu_ldbmcats
Utils/ppencryption
WebServer/admin-server/ra/about.xuda
WebServer/admin-server/ra/admin/schemaUpdate.xuda
WebServer/admin-server/ra/admin/updateprofiles6.9.xuda
WebServer/admin-server/ra/admin-navbar.html
WebServer/admin-server/ra/admin-ops/rekey/racertretrieval.xuda
WebServer/admin-server/ra/admin-ops/rekey/rarekey-main.xuda
WebServer/admin-server/ra/admin-ops/rmjuri-rmops.xuda
WebServer/admin-server/ra/cert-ops/cert-report-results.xuda

WebServer/admin-server/ra/cert-ops/cert-search.html
WebServer/admin-server/ra/cert-ops/req-search.html
WebServer/admin-server/ra/cert-ops/shared/cc-fwd-cert-view.html
WebServer/admin-server/ra/cert-ops/shared/cert-edit.html
WebServer/admin-server/ra/cert-ops/shared/cert-publish.xuda
WebServer/admin-server/ra/cert-ops/shared/cert-renewal-policy.html
WebServer/admin-server/ra/cert-ops/shared/cert-role-edit.html
WebServer/admin-server/ra/cert-ops/shared/cert-send-msie.xuda
WebServer/admin-server/ra/cert-ops/shared/cert-vet-edit.html
WebServer/admin-server/ra/cert-ops/shared/cert-view.html
WebServer/admin-server/ra/cert-ops/shared/get-endEntity-cert.xuda
WebServer/admin-server/ra/cert-ops/shared/req-authorize.xuda
WebServer/admin-server/ra/cert-ops/shared/req-edit.html
WebServer/admin-server/ra/cert-ops/shared/req-get-extensions.xuda
WebServer/admin-server/ra/cert-ops/shared/status-change-details.xuda
WebServer/admin-server/ra/cert-ops/shared/view-cert.xuda
WebServer/admin-server/ra/config/domain-config-sync.xuda
WebServer/admin-server/ra/config/log-control.xuda
WebServer/admin-server/ra/config/profile-editor.xuda
WebServer/admin-server/ra/help/rrm-help.tar
WebServer/admin-server/ra/popup-frameset.html
WebServer/bin/apr.exp
WebServer/bin/aprutil.exp
WebServer/bin/httpd
WebServer/bin/libapr-1.a
WebServer/bin/libapr-1.la
WebServer/bin/libapr-1.so.0
WebServer/bin/libapr-1.so.0.4.5
WebServer/bin/libaprutil-1.a
WebServer/bin/libaprutil-1.la
WebServer/bin/libaprutil-1.so
WebServer/bin/libaprutil-1.so.0
WebServer/bin/libaprutil-1.so.0.4.1
WebServer/bin/libexpat.a
WebServer/bin/libexpat.la
WebServer/bin/libexpat.so.0
WebServer/bin/libexpat.so.0.5.0
WebServer/bin/libwrapper.so
WebServer/bin/strongStrings.so

WebServer/enroll-server/auto-add-msie-request.xuda
WebServer/enroll-server/cert-search-script.xuda
WebServer/enroll-server/exttests.js
WebServer/enroll-server/get-cert.xuda
WebServer/enroll-server/get-cert-msie.xuda
WebServer/enroll-server/get-endEntity-cert.xuda
WebServer/enroll-server/icontrol.vbs
WebServer/enroll-server/request-dc.xuda
WebServer/enroll-server/request-msie.xuda
WebServer/enroll-server/request-msie-admin.xuda
WebServer/enroll-server/send-ca-cert.xuda
WebServer/enroll-server/view-cert.xuda
WebServer/extensions/policyQualifierInfo.xuda
WebServer/extensions/qualifiedCertificateStatements.xuda
WebServer/images/corner.gif
WebServer/images/enrollbg.gif
WebServer/modules/libwrapper.so
WebServer/modules/mod_cmp.so
WebServer/modules/mod_gencert.so
WebServer/modules/mod_xudaacl.so
WebServer/OneStep/cgi-bin/onestep
WebServer/OneStep/samples/htmldocs/corner.gif
WebServer/OneStep/samples/htmldocs/enroll_lotus.html
WebServer/OneStep/samples/htmldocs/enroll_msie_ace.html
WebServer/OneStep/samples/htmldocs/enroll_msie_flat.html
WebServer/OneStep/samples/htmldocs/enroll_msie_ldap.html
WebServer/OneStep/samples/htmldocs/enroll_ns_flat.html
WebServer/OneStep/samples/htmldocs/enrollbg.gif
WebServer/OneStep/samples/htmldocs/error.html
WebServer/OneStep/samples/htmldocs/icontrol.vbs
WebServer/OneStep/samples/htmldocs/index_lotus.html
WebServer/OneStep/samples/htmldocs/install_lotus.html
WebServer/OneStep/samples/htmldocs/install_msie.html
WebServer/OneStep/samples/htmldocs/install_ns.html
WebServer/OneStep/samples/htmldocs/success_msie.html
WebServer/OneStep/setup/setupSSL
WebServer/OneStep/setup/setupSSL.conf
WebServer/OneStep/setup/setupSSLStrings.so
WebServer/scripts/BackupConfig.js

WebServer/scripts/CA.js
WebServer/scripts/EndEntity.js
WebServer/scripts/exttests.js
WebServer/scripts/icontrol.vbs
WebServer/scripts/library.js
WebServer/scripts/RenewalAttributes.js
WebServer/scripts/SubjectRenewalAttributes.js
WebServer/scripts/support.js
WebServer/scripts/ttl.js
WebServer/scripts/upgrade.js
WebServer/scripts/Validation.js
WebServer/scripts/ValidityPeriod.js
WebServer/x-templates/x-construct-domain-form.xuda
WebServer/x-templates/x-email-admin-vettor.xuda
WebServer/x-templates/x-sca-type-input.xuda
WebServer/x-templates/x-userInfo-input.xuda
WebServer/x-templates/x-xenroll-include.xuda
Xudad/bin/xudad
Xudad/bin/xudadStrings.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*, the *Vettor's Guide*, the *Installation 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_DIRUtils** folder of the Registration Manager installation.
4. From the command prompt in the working directory, type:
<path from Registration 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 Registration Manager installation.
4. From the command prompt in the working directory, type:

<path from Registration 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

You must perform all the tasks mentioned in the section “Preparing to Install” in the chapter “Installing RSA Registration Manager” of the *Installation Guide*, before performing one of the following:

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

Installing the Full Build

If you want to install the full build of RSA Registration Manager 6.9 build555, use the following files that come with this package:

- On Windows, use **RSARM-v6.9build555r-WIN32.zip**.
- On Solaris, use **RSARM-v6.9build555r-sparc-sun-solaris.tar**.
- On RedHat Linux, use **RSARM-v6.9build555r-linux.tar**.
- On SUSE Linux, use **RSARM-v6.9build555r-SuSE_linux.tar**.

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

Installing the Hotfix Files

On Windows

This hotfix does not require a new installation of the product, but rather a drop-in replacement of 127 files into the appropriate Registration Manager directory and the unzipping of a .zip file to update the Help.

To install RSA Registration Manager 6.9 build555:

1. Stop all Registration Manager services.
2. Unzip the **SSLC_CryptoCME_Libs-WIN32.zip** file 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 following files (**INSTALL_DIR** is the directory path where Registration Manager is installed):
 - INSTALL_DIR\LogServer\bin\xslogmgr.exe
 - INSTALL_DIR\LogServer\bin\xslogsrv.exe
 - INSTALL_DIR\LogServer\bin\xslogsrvStrings.dll
 - INSTALL_DIR\Upgrader\bin\setupSSL.exe
 - INSTALL_DIR\Upgrader\bin\setupSSLStrings.dll
 - INSTALL_DIR\Upgrader\bin\upgrader.exe
 - INSTALL_DIR\Upgrader\bin\xu_ldbmcacat.exe
 - INSTALL_DIR\Utils\ppencryption.exe
 - INSTALL_DIR\Utils\vcredist_x86.exe
 - INSTALL_DIR\WebServer\admin-server\ra\about.xuda

- INSTALL_DIR\WebServer\admin-server\ra\admin\schemaUpdate.xuda
- INSTALL_DIR\WebServer\admin-server\ra\admin\updateprofiles6.9.xuda
- INSTALL_DIR\WebServer\admin-server\ra\admin-navbar.html
- INSTALL_DIR\WebServer\admin-server\ra\admin-ops\rekey\racertretrieval.xuda
- INSTALL_DIR\WebServer\admin-server\ra\admin-ops\rekey\rarekey-main.xuda
- INSTALL_DIR\WebServer\admin-server\ra\admin-ops\rmjuri-rmops.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\cert-report-results.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\cert-search.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\req-search.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cc-fwd-cert-view.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cert-edit.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cert-publish.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cert-renewal-policy.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cert-role-edit.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cert-send-msie.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cert-vet-edit.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\cert-view.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\get-endEntity-cert.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\req-authorize.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\req-edit.html
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\req-get-extensions.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\status-change-details.xuda
- INSTALL_DIR\WebServer\admin-server\ra\cert-ops\shared\view-cert.xuda
- INSTALL_DIR\WebServer\admin-server\ra\config\domain-config-sync.xuda
- INSTALL_DIR\WebServer\admin-server\ra\config\log-control.xuda
- INSTALL_DIR\WebServer\admin-server\ra\config\profile-editor.xuda
- INSTALL_DIR\WebServer\admin-server\ra\help\rrm-help.zip
- INSTALL_DIR\WebServer\admin-server\ra\popup-frameset.html
- INSTALL_DIR\WebServer\bin\apache.exe
- INSTALL_DIR\WebServer\bin\libapr-1.dll
- INSTALL_DIR\WebServer\bin\libapriconv-1.dll
- INSTALL_DIR\Webserver\bin\libaprutil-1.dll
- INSTALL_DIR\Webserver\bin\libhttpd.dll
- INSTALL_DIR\WebServer\bin\strongStrings.dll
- INSTALL_DIR\WebServer\enroll-server\auto-add-msie-request.xuda
- INSTALL_DIR\WebServer\enroll-server\cert-search-script.xuda
- INSTALL_DIR\WebServer\enroll-server\exttests.js
- INSTALL_DIR\WebServer\enroll-server\get-cert.xuda
- INSTALL_DIR\WebServer\enroll-server\get-cert-msie.xuda

- INSTALL_DIR\WebServer\enroll-server\get-endEntity-cert.xuda
- INSTALL_DIR\WebServer\enroll-server\icontrol.vbs
- INSTALL_DIR\WebServer\enroll-server\request-dc.xuda
- INSTALL_DIR\WebServer\enroll-server\request-msie.xuda
- INSTALL_DIR\WebServer\enroll-server\request-msie-admin.xuda
- INSTALL_DIR\WebServer\enroll-server\send-ca-cert.xuda
- INSTALL_DIR\WebServer\enroll-server\view-cert.xuda
- INSTALL_DIR\WebServer\extensions\policyQualifierInfo.xuda
- INSTALL_DIR\WebServer\extensions\qualifiedCertificateStatements.xuda
- INSTALL_DIR\WebServer\images\corner.gif
- INSTALL_DIR\WebServer\images\enrollbg.gif
- INSTALL_DIR\WebServer\modules\mod_actions.so
- INSTALL_DIR\WebServer\modules\mod_alias.so
- INSTALL_DIR\WebServer\modules\mod_asis.so
- INSTALL_DIR\WebServer\modules\mod_auth_basic.so
- INSTALL_DIR\WebServer\modules\mod_authn_alias.so
- INSTALL_DIR\WebServer\modules\mod_authn_anon.so
- INSTALL_DIR\WebServer\modules\mod_authn_file.so
- INSTALL_DIR\WebServer\modules\mod_authz_groupfile.so
- INSTALL_DIR\WebServer\modules\mod_authz_host.so
- INSTALL_DIR\WebServer\modules\mod_authz_user.so
- INSTALL_DIR\WebServer\modules\mod_autoindex.so
- INSTALL_DIR\WebServer\modules\mod_cgi.so
- INSTALL_DIR\WebServer\modules\mod_cmp.so
- INSTALL_DIR\WebServer\modules\mod_dir.so
- INSTALL_DIR\WebServer\modules\mod_env.so
- INSTALL_DIR\WebServer\modules\mod_gencert.so
- INSTALL_DIR\WebServer\modules\mod_imagemap.so
- INSTALL_DIR\WebServer\modules\mod_include.so
- INSTALL_DIR\WebServer\modules\mod_isapi.so
- INSTALL_DIR\WebServer\modules\mod_log_config.so
- INSTALL_DIR\WebServer\modules\mod_mime.so
- INSTALL_DIR\WebServer\modules\mod_negotiation.so
- INSTALL_DIR\WebServer\modules\mod_reqtimeout.so
- INSTALL_DIR\WebServer\modules\mod_rewrite.so
- INSTALL_DIR\WebServer\modules\mod_setenvif.so
- INSTALL_DIR\WebServer\modules\mod_ssl.so
- INSTALL_DIR\WebServer\modules\mod_userdir.so
- INSTALL_DIR\WebServer\modules\mod_xudaacl.so

- INSTALL_DIR\WebServer\modules\xuda_wrapper.dll
- INSTALL_DIR\WebServer\OneStep\cgi-bin\onestep.exe
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\corner.gif
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\enroll_lotus.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\enroll_msie_ace.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\enroll_msie_flat.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\enroll_msie_ldap.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\enroll_ns_flat.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\enrollbg.gif
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\error.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\icontrol.vbs
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\index_lotus.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\install_lotus.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\install_msie.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\install_ns.html
- INSTALL_DIR\WebServer\OneStep\samples\htmldocs\success_msie.html
- INSTALL_DIR\WebServer\OneStep\setup\setupSSL.conf
- INSTALL_DIR\WebServer\OneStep\setup\setupSSL.exe
- INSTALL_DIR\WebServer\OneStep\setup\setupSSLStrings.dll
- INSTALL_DIR\WebServer\scripts\BackupConfig.js
- INSTALL_DIR\WebServer\scripts\CA.js
- INSTALL_DIR\WebServer\scripts\EndEntity.js
- INSTALL_DIR\WebServer\scripts\exttests.js
- INSTALL_DIR\WebServer\scripts\icontrol.vbs
- INSTALL_DIR\WebServer\scripts\library.js
- INSTALL_DIR\WebServer\scripts\RenewalAttributes.js
- INSTALL_DIR\WebServer\scripts\SubjectRenewalAttributes.js
- INSTALL_DIR\WebServer\scripts\support.js
- INSTALL_DIR\WebServer\scripts\ttl.js
- INSTALL_DIR\WebServer\scripts\upgrade.js
- INSTALL_DIR\WebServer\scripts\Validation.js
- INSTALL_DIR\WebServer\scripts\ValidityPeriod.js
- INSTALL_DIR\WebServer\x-templates\x-construct-domain-form.xuda
- INSTALL_DIR\WebServer\x-templates\x-email-admin-vettor.xuda
- INSTALL_DIR\WebServer\x-templates\x-sca-type-input.xuda
- INSTALL_DIR\WebServer\x-templates\x-userInfo-input.xuda
- INSTALL_DIR\WebServer\x-templates\x-xenroll-include.xuda
- INSTALL_DIR\Xudad\bin\xudad.exe
- INSTALL_DIR\Xudad\bin\xudadStrings.dll

5. Copy the zipped file to the **INSTALL_DIR** directory.
6. Unzip and extract the files ensuring that 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, in the **INSTALL_DIR\WebServer\admin-server\ra\help** directory, unzip and extract the files from **rrm-help.zip** ensuring that the new files replace the old files.

However, if you are upgrading from RSA Registration Manager 6.9 build551, this is not required.

8. Create a backup of the **httpd.conf** file located at **INSTALL_DIR\Web Server\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 xdaacl_module modules/mod_xdaacl.so
LoadModule cmp_module modules/mod_cmp.so
```

RSA Registration Manager 6.9 build555 Readme

- 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. Search for the line "SSLSessionCache", and uncomment the following line:
SSLSessionCache none
- d. Comment the following line:
SSLSessionCache dbm:logs/ssl_scache
9. Save the **httpd.conf** file.
10. Install the Microsoft Visual C++ 2005 SP1 Redistributable Package on the target machines. The Redistributable Package vcredist_x86.exe is available at <INSTALL_DIR>\Utils folder.
11. Start all Registration Manager services.
12. If you are upgrading from RSA Registration Manager 6.9 build551 or earlier versions to RSA Registration Manager 6.9 build555, to update the profile, go to <https://hostname:admin-port/ra/admin/updateprofiles6.9.xuda>.
The certificate extension profiles are updated.
13. If you are upgrading from RSA Registration Manager 6.9 build551 or earlier versions to RSA Registration Manager 6.9 build555, to update the schema, go to <https://hostname:admin-port/ra/admin/schemaUpdate.xuda>.
The schema is updated.
14. Restart all Registration Manager services.

On Solaris or Linux

This hotfix does not require a new installation of the product, but rather a drop-in replacement of 113 files into the appropriate Certificate Manager directory and the untarring of a .tar file to update the Help.

To install RSA Registration Manager 6.9 build555:

1. Stop all Registration Manager services.
2. Extract the following tar file provided with this drop-in package.
 - For Redhat Linux, SSLC_CryptoCME_Libs-RH_Linux.tar.
 - For SUSE Linux, SSLC_CryptoCME_Libs-SuSE_Linux.tar.
 - For Solaris, SSLC_CryptoCME_Libs-sparc-sun-solaris.tar.
3. Replace the following files located at /usr/lib folder with the ones in the untarred folder:
 - libccme_base.so
 - libccme_ecc.so
 - libccme_eccaccel.so
 - libcryptocme2.so
 - cryptocme2.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 following files (**INSTALL_DIR** is the directory path where Registration Manager is installed):
 - INSTALL_DIR/LogServer/bin/xslogmgr

- INSTALL_DIR/LogServer/bin/xslogsrv
- INSTALL_DIR/LogServer/bin/xslogsrvStrings.so
- INSTALL_DIR/Upgrader/bin/setupSSL
- INSTALL_DIR/Upgrader/bin/setupSSLStrings.so
- INSTALL_DIR/Upgrader/bin/upgrader
- INSTALL_DIR/Upgrader/bin/xu_ldbmcats
- INSTALL_DIR/Utils/ppencryption
- INSTALL_DIR/WebServer/admin-server/ra/about.xuda
- INSTALL_DIR/WebServer/admin-server/ra/admin/schemaUpdate.xuda
- INSTALL_DIR/WebServer/admin-server/ra/admin/updateprofiles6.9.xuda
- INSTALL_DIR/WebServer/admin-server/ra/admin-navbar.html
- INSTALL_DIR/WebServer/admin-server/ra/admin-ops/rekey/racertretrieval.xuda
- INSTALL_DIR/WebServer/admin-server/ra/admin-ops/rekey/rarekey-main.xuda
- INSTALL_DIR/WebServer/admin-server/ra/admin-ops/rmjuri-rmops.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/cert-report-results.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/cert-search.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/req-search.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cc-fwd-cert-view.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cert-edit.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cert-publish.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cert-renewal-policy.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cert-role-edit.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cert-send-msie.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cert-vet-edit.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/cert-view.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/get-endEntity-cert.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/req-authorize.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/req-edit.html
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/req-get-extensions.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/status-change-details.xuda
- INSTALL_DIR/WebServer/admin-server/ra/cert-ops/shared/view-cert.xuda
- INSTALL_DIR/WebServer/admin-server/ra/config/domain-config-sync.xuda
- INSTALL_DIR/WebServer/admin-server/ra/config/log-control.xuda
- INSTALL_DIR/WebServer/admin-server/ra/config/profile-editor.xuda
- INSTALL_DIR/WebServer/admin-server/ra/help/rrm-help.tar
- INSTALL_DIR/WebServer/admin-server/ra/popup-frameset.html
- INSTALL_DIR/WebServer/bin/apr.exp
- INSTALL_DIR/WebServer/bin/aprutil.exp
- INSTALL_DIR/WebServer/bin/httpd

- `INSTALL_DIR/WebServer/bin/libapr-1.a`
- `INSTALL_DIR/WebServer/bin/libapr-1.la`
- `INSTALL_DIR/WebServer/bin/libapr-1.so.0`
- `INSTALL_DIR/WebServer/bin/libapr-1.so.0.4.5`
- `INSTALL_DIR/WebServer/bin/libaprutil-1.a`
- `INSTALL_DIR/WebServer/bin/libaprutil-1.la`
- `INSTALL_DIR/WebServer/bin/libaprutil-1.so`
- `INSTALL_DIR/WebServer/bin/libaprutil-1.so.0`
- `INSTALL_DIR/WebServer/bin/libaprutil-1.so.0.4.1`
- `INSTALL_DIR/WebServer/bin/libexpat.a`
- `INSTALL_DIR/WebServer/bin/libexpat.la`
- `INSTALL_DIR/WebServer/bin/libexpat.so.0`
- `INSTALL_DIR/WebServer/bin/libexpat.so.0.5.0`
- `INSTALL_DIR/WebServer/bin/libwrapper.so`
- `INSTALL_DIR/WebServer/bin/strongStrings.so`
- `INSTALL_DIR/WebServer/enroll-server/auto-add-msie-request.xuda`
- `INSTALL_DIR/WebServer/enroll-server/cert-search-script.xuda`
- `INSTALL_DIR/WebServer/enroll-server/exttests.js`
- `INSTALL_DIR/WebServer/enroll-server/get-cert.xuda`
- `INSTALL_DIR/WebServer/enroll-server/get-cert-msie.xuda`
- `INSTALL_DIR/WebServer/enroll-server/get-endEntity-cert.xuda`
- `INSTALL_DIR/WebServer/enroll-server/icontrol.vbs`
- `INSTALL_DIR/WebServer/enroll-server/request-dc.xuda`
- `INSTALL_DIR/WebServer/enroll-server/request-msie.xuda`
- `INSTALL_DIR/WebServer/enroll-server/request-msie-admin.xuda`
- `INSTALL_DIR/WebServer/enroll-server/send-ca-cert.xuda`
- `INSTALL_DIR/WebServer/enroll-server/view-cert.xuda`
- `INSTALL_DIR/WebServer/extensions/policyQualifierInfo.xuda`
- `INSTALL_DIR/WebServer/extensions/qualifiedCertificateStatements.xuda`
- `INSTALL_DIR/WebServer/images/corner.gif`
- `INSTALL_DIR/WebServer/images/enrollbg.gif`
- `INSTALL_DIR/WebServer/modules/libwrapper.so`
- `INSTALL_DIR/WebServer/modules/mod_cmp.so`
- `INSTALL_DIR/WebServer/modules/mod_gencert.so`
- `INSTALL_DIR/WebServer/modules/mod_xudaacl.so`
- `INSTALL_DIR/WebServer/OneStep/cgi-bin/onestep`
- `INSTALL_DIR/WebServer/OneStep/samples/htmldocs/corner.gif`
- `INSTALL_DIR/WebServer/OneStep/samples/htmldocs/enroll_lotus.html`
- `INSTALL_DIR/WebServer/OneStep/samples/htmldocs/enroll_msie_ace.html`

- INSTALL_DIR/WebServer/OneStep/samples/htmldocs/enroll_msie_flat.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/enroll_msie_ldap.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/enroll_ns_flat.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/enrollbg.gif
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/error.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/iconcontrol.vbs
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/index_lotus.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/install_lotus.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/install_msie.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/install_ns.html
 - INSTALL_DIR/WebServer/OneStep/samples/htmldocs/success_msie.html
 - INSTALL_DIR/WebServer/OneStep/setup/setupSSL
 - INSTALL_DIR/WebServer/OneStep/setup/setupSSL.conf
 - INSTALL_DIR/WebServer/OneStep/setup/setupSSLStrings.so
 - INSTALL_DIR/WebServer/scripts/BackupConfig.js
 - INSTALL_DIR/WebServer/scripts/CA.js
 - INSTALL_DIR/WebServer/scripts/EndEntity.js
 - INSTALL_DIR/WebServer/scripts/exttests.js
 - INSTALL_DIR/WebServer/scripts/iconcontrol.vbs
 - INSTALL_DIR/WebServer/scripts/library.js
 - INSTALL_DIR/WebServer/scripts/RenewalAttributes.js
 - INSTALL_DIR/WebServer/scripts/SubjectRenewalAttributes.js
 - INSTALL_DIR/WebServer/scripts/support.js
 - INSTALL_DIR/WebServer/scripts/ttl.js
 - INSTALL_DIR/WebServer/scripts/upgrade.js
 - INSTALL_DIR/WebServer/scripts/Validation.js
 - INSTALL_DIR/WebServer/scripts/ValidityPeriod.js
 - INSTALL_DIR/WebServer/x-templates/x-construct-domain-form.xuda
 - INSTALL_DIR/WebServer/x-templates/x-email-admin-vettor.xuda
 - INSTALL_DIR/WebServer/x-templates/x-sca-type-input.xuda
 - INSTALL_DIR/WebServer/x-templates/x-userInfo-input.xuda
 - INSTALL_DIR/WebServer/x-templates/x-xenroll-include.xuda
 - INSTALL_DIR/Xudad/bin/xudad
 - INSTALL_DIR/Xudad/bin/xudadStrings.so
5. Copy the tar file to the **INSTALL_DIR** directory.
 6. Untar and extract the files ensuring that the new files replace the old files.
 7. To update the Help, in the **INSTALL_DIR/WebServer/admin-server/ra/help** directory, untar and extract the files from **rrm-help.tar** ensuring that the new files replace the old files.

However, if you are upgrading from RSA Registration Manager 6.9 build551, this is not required.

8. Create a backup of the **httpd.conf** file located at **INSTALL_DIR/Web Server/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. Search for the line "SSLSessionCache", and uncomment the following line:
SSLSessionCache none
 - e. Comment the following line:
SSLSessionCache dbm:logs/ssl_scache
9. Save the **httpd.conf** file.
10. 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 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. Start all Registration Manager services.
12. If you are upgrading from RSA Registration Manager 6.9 build551 or earlier versions to RSA Registration Manager 6.9 build555, to update the profile, go to <https://hostname:admin-port/ra/admin/updateprofiles6.9.xuda>.
The certificate extension profiles are updated.
13. If you are upgrading from RSA Registration Manager 6.9 build551 or earlier versions to RSA Registration Manager 6.9 build555, to update the schema, go to <https://hostname:admin-port/ra/admin/schemaUpdate.xuda>.
The schema is updated.
14. Restart all Registration Manager services.

Fixed Issues

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

Tracking Number	Description	Resolution
Fixed in build555		

Tracking Number	Description	Resolution
CERTMGR-3842, CERTMGR-4322	While generating reports, the email address was not displayed if the email address was not part of Subject DN.	This issue is resolved in RSA Registration Manager 6.9 build555. The email address is displayed in reports whether the email address is part of Subject DN or not.
CERTMGR-4034	Support for Features Beyond the Year 2038	<p>RSA Registration Manager supports the following features with validity beyond the year 2038:</p> <ul style="list-style-type: none"> • Creating a CA • Generating Revocation Lists • Issuing End-Entity Certificates <p>Important: RSA Registration Manager will not function properly if the system time is changed to beyond the year 2038. Also, RSA Registration Manager only supports certificates with validity up to year 2050. These issues are described in the Known Issues section.</p>
CERTMGR-4201	If the schema file is customized in the existing RSA Registration Manager installation, the upgrader fails while generating package.tar file. The xu_ldbmcat crashes at the time of merging the existing schema file with the new one.	This issue is resolved in RSA Registration Manager 6.9 build555.
CERTMGR-4203	When you attempt to enroll for a certificate using an SCEP request from the MobileIron MDM application, XrcBADVALUE error is returned. This is because the SCEP server always tries to decrypt the data in the certificate request using the DES-CBC algorithm, instead of using the algorithm in the certificate request.	This issue has been fixed in RSA Registration Manager 6.9 build555. SCEP now decrypts the data using the algorithm in the cert request.
CERTMGR-4219	After upgrading RSA Registration Manager configured with High Availability to the latest versions, the directive "directory" is uncommented.	This issue is resolved in RSA Registration Manager 6.9 build555.
CERTMGR-4228,C ERTMGR-4312	If a delta CRL timer is enabled, the delta CRL is not generated based on the delta CRL timer for some of the CAs.	This issue is resolved in RSA Registration Manager 6.9 build555. When delta CRL generation fails for a particular CA, RSA Registration Manager tries up to three times. If delta CRL generation fails for a CA (even on retrying three times), delta CRL timer will not stop for that CA, rather it will continue to attempt to generate on next delta CRL interval.
CERTMGR-4235 CERTMGR-4157	RSA Secure Directory Server is crashed while creating a CA with AEP HSM.	This issue is resolved while creating a CA with AEP HSM in RSA Registration Manager 6.9 build555.
CERTMGR-4241 CERTMGR-4184	Unable to submit PKCS#10 request if challengePassword value is encoded as UTF8String	This issue is resolved in RSA Registration Manager 6.9 build 555
CERTMGR-4267	RSA Registration Manager fails to show certificate details when Administrator is enabled for multiple vettor jurisdictions and one of the vetting jurisdiction has been deleted	This issue is resolved in RSA Registration Manager 6.9 build555.

Tracking Number	Description	Resolution
CERTMGR-4270	RSA Administration Server had the following vulnerabilities: CVE-2012-2687 For information on these vulnerabilities, go to http://web.nvd.nist.gov/view/vuln/search and search by the CVE ID.	This issue is resolved in RSA Registration Manager 6.9 build555. Important: RSA Administration Server is built on Apache 2.2.22 and the fix for CVE-2012-2687 is incorporated.
CERTMGR-4280	In RSA Registration Manager 6.9 build 553-2038, Secure Directory Server crashes immediately after service starts up if CRL timer is configured	This issue is resolved in RSA Registration Manager 6.9 build555.
CERTMGR-4289	RSA Registration Manager encodes the value of Explicit Text in Certificate Policies extension as BMPString if the value has non-ASCII characters.	This issue is resolved in RSA Registration Manager 6.9 build 555. The encoding type can configured in Certificate Policies extension script for Explicit Text. The supported values are UTF8String, BMPString and PrintableString.
CERTMGR-4316, CERTMGR-4327	When the length of CA certificate's serial number is less than 32 bytes and the SCEP request is made for that CA Jurisdiction, it fails.	This issue is resolved in RSA Registration Manager 6.9 build555.
REGMGR-325	Some of the OneStep files are missing from RSA Registration Manager installation	This issue is resolved in RSA Registration Manager 6.9 build 555
REGMGR-328	When an approved jurisdiction is deleted from RSA Registration Manager, then "Synchronize jurisdiction" operation fails on RSA Registraion Manager	This issue is resolved in RSA Registration Manager 6.9 build 555

Tracking Number	Description	Resolution
REGMGR-331	<p>RSA Registration Manager may allow SSL connections with NULL ciphers (eNULL and aNULL). NULL ciphers are considered weak ciphers and are a security risk. Their use is strongly discouraged. This issue may also prevent installation of Registration Manager using the Mozilla Firefox browser.</p>	<p>This issue is resolved in RSA Registration Manager 6.9 build 555.</p> <p>The default SSLCipherSuite is changed to ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</p> <p>Workaround for Hot fix installation or previous versions</p> <p>Modify the default values of the SSL Cipher Suite and the SSL Cipher as follows:</p> <ol style="list-style-type: none"> Open the following files: <ul style="list-style-type: none"> INSTALL_DIR/WebServer/conf/httpd.conf Comment the following line for virtual hosts of Administration, Enrollment, SCEP and Renewal servers: <pre>"SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:SSLv2:+EXP:+eNULL"</pre> For windows platform: Add the following lines for virtual hosts of Administration, Enrollment, SCEP and Renewal servers: <pre>SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</pre> <p>For Unix platforms with Mozilla Firefox browser, Add the following lines for virtual hosts of Administration, Enrollment, SCEP and Renewal servers: SSLCipherSuite AES256-SHA SSLProtocol +TLsv1</p>
ONESTEP-97	<p>RSA OneStep is looking for non-existent files: enrollbg.gif and corner.gif</p>	<p>This issue is resolved in RSA Registration Manager 6.9 build 555</p>
Fixed in build554		
REGMGR-325	<p>When you installed Registration Manager on Windows, the following files were missing in the WebServer\OneStep\samples\html\docs folder:</p> <ul style="list-style-type: none"> corner.gif enroll_lotus.html enrollbg.gif icontrol.vbs index_lotus.html install_lotus.html install_ns.html success_msie.html <p>Because of this, you could not request for a certificate through OneStep using the Registration Manager administrative console.</p>	<p>This issue is resolved in RSA Registration Manager 6.9 build554.</p>

Tracking Number	Description	Resolution
CERTMGR-4175	The Xudad Server initialized tracing twice for each component of Registration Manager, which led to multiple file descriptors for the trace.log file.	This issue is resolved in RSA Registration Manager 6.9 build554. The Xudad Server initializes tracing (that is, opens the trace.log file) only once for each component of Registration Manager.
Fixed in build553		
REGMGR-311	The Administration Server of Registration Manager was vulnerable to a Slowloris attack. In this type of attack, multiple connections were opened to the Server and held for a long time by sending subsequent HTTP headers to the request, without completing any request. This consumed the maximum number of connections allowed for the Administration Server, and thus denied additional connections.	This issue is resolved in RSA Certificate Manager 6.9 build 555. This issue is not applicable if the steps from the know issues is followed to change the SSLCiphersuite.
CERTMGR-3900	When you configured a Jurisdiction to send email notifications to all vettors, Registration Manager sent the email notifications to all the vettors irrespective of the Jurisdiction assigned to each vettor.	In RSA Registration Manager 6.9 build553, if a certificate request is made for a Jurisdiction, and if the Jurisdiction is configured to send email notifications to All Vettors , an email notification is sent only to the vettors assigned to that Jurisdiction.
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 Registration Manager 6.9 build551.
CERTMGR-4017	When a certificate was downloaded from the Enrollment Server in p7b format using Internet Explorer, the full certificate chain was not downloaded.	This issue is resolved in RSA Registration Manager 6.9 build551.
CERTMGR-4030 CERTMGR-4069	Apache 2.0.64 had several vulnerabilities: CVE-2011-3607 CVE-2011-3192 CVE-2012-0053 For information about these vulnerabilities, go to http://web.nvd.nist.gov/view/vuln/search and search by CVE ID.	In RSA Registration Manager 6.9 build551, the Apache Web Server is updated to fix these vulnerabilities.
CERTMGR-4032	WebServer\enroll-server\icontrol.vbs and WebServer\OneStep\htmldocs\icontrol.vbs did not contain the code that allows Administrators to set the default key size on the Enrollment Server to 2048 for users on Windows Vista, Windows 7, or Windows Server 2008.	In RSA Registration Manager 6.9 build551, WebServer\enroll-server\icontrol.vbs and WebServer\OneStep\htmldocs\icontrol.vbs are updated to add the default key size of 2048 for certificate enrollment. For instructions on changing the default key size, see the <i>Administrator's Guide</i> .

Known Issues

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

Title	Description	Workaround (if available)
RSA Registration Manager will not function properly if the system time is changed to beyond the year 2038 CERTMGR-4034	RSA Registration Manager will not function properly if the system time is changed to the year beyond 2038. This issue is applicable only when Certificate Manager is installed on Linux.	
RSA Registration Manager only supports certificates with validity up to year 2050. CERTMGR-4034	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 RSA Registration Manager, the certificate validity TIME is stored in the following UTCTime format: YYMMDDHHMMSSZ. RSA Registration Manager only supports certificates with validity up to year 2050.	
When a non-persistent card is inserted, then the Administration Server is not accessible if SSL keys are protected with nCipher HSM CERTMGR-4295	When a RSA Registration Manager is installed with SSL keys on nCipher HSM and when a non-persistent card is inserted, then the Administration Server is not accessible	Set the following variable 'CKNFAST_NONREMOVABLE=1' in <code>cknfasterc</code> file and restart the nCipher services
Unable to install renewed certificate on Microsoft Internet Explorer 9 or above on Windows 7 64-bit. The error code is 80004005 REGMGR-327	RSA Registration Manager fails to install renewed certificate on Microsoft Internet Explorer 9 or above on Windows 7 64-bit platform	Add Enrollment Server to the list of Trusted Sites
Support of RSA Registration Manager 6.8 with RCM 6.9 build 553 or above REGMGR-322	RSA Registration Manager 6.8 does not work with RSA Certificate Manager 6.9 build 553 or above.	The Registration Manager must be upgraded to the same version as RSA Certification Manager

<p>Installation of Registration Manager using the Mozilla Firefox browser is not possible. CERTMGR-4173</p>	<p>When you install Registration Manager using Firefox, the browser fails to trust the default SSL Cipher used by Registration Manager. Hence, you cannot complete the installation.</p>	<p>While installing RSA Registration Manager 6.9 build554, modify the default values of the SSL Cipher Suite and the SSL Cipher as follows:</p> <ol style="list-style-type: none">1. Open the following files:<ul style="list-style-type: none">• iws/dist/iws.conf• WebServer/dist/scep.conf• WebServer/dist/admin.conf• WebServer/dist/enroll.conf2. Comment the following line: "SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"3. Add the following lines: SSLCipherSuite AES256-SHA SSLProtocol +TLSv1
---	--	---

Support and Service

RSA SecurCare® Online	https://knowledge.rsasecurity.com
Customer Support Information	www.rsa.com/support
RSA Secured Partner Solutions Directory	www.rsasecured.com

Copyright © 2013 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>.