Readme
RSA Registration Manager 6.9

March 30, 2012

Introduction

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

This *Readme* may be updated. The most current version can be found on RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Readme Revision History

Revision 1	March 30, 2012	Removed RSA Registration Manager 6.8 hot fix functionality; revised list of product documentation; added known issues.

What's New in This Release

This section describes the major changes introduced in this release.

Apache Server upgrade. The Apache HTTP Server on which RSA Registration Manager is based is upgraded to version 2.0.64.

Support for Internet Explorer 9. RSA Registration Manager supports Internet Explorer 9 for administration and enrollment. For more information, see the *Installation Guide*.

Package Contents

Your RSA Registration Manager product folder contains:

CDs and Diskettes

- RSA Registration Manager CD

Licenses

- License Agreement

Important: Remove the license certificate and keep it in a safe place.

Product Documentation

The following documentation is on the RSA Registration Manager 6.9 CD, in the **\Documentation** directory.

Title	Filename
Readme	**RSARegistrationManager69Readme.pdf**
Installation Guide	**RSARegistrationManagerInstallationGuide.pdf**
Administrator's Guide	**RSARegistrationManagerAdministratorsGuide.pdf**
Vettor's Guide	**RSARegistrationManagerVettorsGuide.pdf**

Limitations

This section describes limitations that exist in RSA Registration Manager 6.8. If workarounds exist, they are described.

Title	Description	Workaround (if available)
Browser Support Issues		
Certificate requests cannot be submitted using Microsoft Internet Explorer 6 Service Pack 1 without the Xenroll patch Q323172. Bz 31659	Requesting a certificate from the Enrollment Server through Internet Explorer 6 SP1 results in an error and no request is made.	This is an issue with Internet Explorer 6 SP1. Go to the Microsoft web site at **http://www.microsoft.com/technet/security/bulletin/MS02-048.mspx** and follow the directions to download the appropriate patch, Q323172. Make the certificate request again.
Microsoft Internet Explorer 6.0 prompts you with a message because SSL certificate status is unavailable. Bz 32520	Internet Explorer 6 is set by default to check the status of all SSL certificates. As a result the following message is displayed: `Revocation information for the security certificate for this site is not available. Do you want to proceed?`	Do one of the following: • Make the appropriate complete certificate revocation list (CRL) available for download. • Disable SSL certificate status checking in Internet Explorer 6: 1. Click **Tools** > **Internet Options**. 2. Click the **Advanced** tab. 3. Under **Security**, clear **Check for server certificate revocation**. 4. Click **OK**.

Known Issues

This section explains 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)
Installation and Upgrade Issues		
User/Group ownership change incorrectly reports success on Solaris platform. Bz 31684	During the web-based portion of a installation on a Solaris platform, the rsakeon_setup CGI script modifies permissions to the files in **/*installed-dir*/WebServer** based on the User/Group that was entered on the General Configuration Information page. If you enter an incorrect or invalid User/Group, the operation is reported as successful, even though it was not. However, the syslog reports the following message: httpsd 'unknown group xxxx, bad user name xxxx The ownership of the files and directory does not change.	
Installation fails if the passphrase protecting the Registration Manager SSL keys contains "+". Bz 59855	If you provide a passphrase for the SSL keys that includes the character "+", when you click **Next** after entering the general configuration information, you see the following message: The CA server you specified either does not exist or is not reachable from this machine. You can deselect the check box below the input fields if you would like to skip this check. You cannot proceed with the installation. (The checkbox at the bottom of the page allows you to skip the check for the mail server.)	
Hardware Key Issues		
Changing the passphrase for software SSL keys reports improper error when some keys are in software and some keys are in hardware. Bz 30853	Scenario: • The SSL keys are a mixture of software keys and hardware keys. • The wrong card set for the hardware keys is present on the device. • You use the Change Passphrase operation to change the passphrase on the software keys. The passphrase is changed on only some of the software keys and you may see the following error message: change-server-key-passphrase.xuda: Line 91: [XrcUNKNOWN] unknown member of enumerated set encountered.	If you have software SSL keys and hardware SSL keys, be sure that the correct card set for the hardware keys is present on the device before changing the passphrase on software keys. Although the hardware keys are not affected, it is nevertheless necessary to have the correct card set for the SSL keys present in the device for the operation.

Title	Description	Workaround (if available)
Rekeying and Re-signing Issues		
Verification of existing Registration Manager log files fails after Log Signing keys have been converted from nCipher native to nCipher PKCS #11. CERTMGR-4014	If Registration Manager uses nCipher native SSL and Log Signing keys, you must convert the keys to software-based keys before upgrading to RSA Registration Manager 6.9. After the upgrade is complete, you can convert the software-based keys to PKCS #11 keys. You cannot verify log files from your old installation with the new Log Signing certificate.	Before converting the nCipher native Log Signing keys to software, back up **LogServer/sign/certs/signing.cert**, and rename the file **LogServer/sign/certs/signing-native.cert**. After converting the nCipher native keys to software keys, upgrading Registration Manager, and converting the software keys to nCipher PKCS #11 keys, the following files are available: • **LogServer/sign/certs/signing.cert** - created during conversion from software to nCipher PKCS #11 keys • **LogServer/sign/certs/signing.cert.bak** - created during nCipher native to software conversion • **LogServer/sign/certs/signing-native.cert** - renamed nCipher native signing certificate **To verify the old log files after converting the keys from nCipher native to nCipher PKCS #11 keys** 1. Create a copy of **LogServer/conf/xslogconf.xml** file, and rename the file **LogServer/conf/xslogconf-native.xml**. 2. In the **LogServer/conf/xslogconf-native.xml** file, search for the ServerSigningCertificate parameter, and replace “signing.cert” with "signing-native.cert". 3. Verify the old log files using the **signing-native.cert** file as follows: a. Open a command prompt and change directories to the Registration Manager installation directory. b. To verify a log file, type: `INSTALL_DIR\LogServer\bin>xslogmgr.exe verify -f ..\conf\xslogconf-native.xml ..\logs\xslog_YYYYMMDD.xml` where *YYYYMMDD* is the date of the log file. If there are multiple log files for a date, the date will have incrementing numbers appended, for example 20111219_1.

Title	Description	Workaround (if available)
ACL Issues		
The postal address certificate attribute cannot be used in ACL rules if multi-lined. Bz 31866	The certificate attribute “Postal Address” containing more than one line cannot be used to create an ACL rule with the “is” operator. It is not possible to type an end of line character in the ACL rule editor.	
Certificate Issues		
Unable to revoke certificate from Enrollment Server using Microsoft Internet Explorer 5.00.3315.1000. Bz 30925	If you attempt to revoke your end-entity certificate (requested through the Enrollment Server and downloaded into your browser), you see the following message: The page cannot be displayed. The page you are looking for is currently unavailable. The Web site might be experiencing technical difficulties, or you may need to adjust your browser settings.	This is an issue only with a specific sub-version of Internet Explorer. Other builds of Internet Explorer 5, as well as Internet Explorer 5.5 and later, do not have this issue.
Displayed status of an expired certificate remains “Active”. Bz 32787, 72141	When the validity period of an end-entity certificate or cross-certificate has passed, the displayed status of the certificate remains “Active”. Expired certificates are displayed in the Active Certificates list on the Certificate Operations workbench and the CA Operations workbench.	
Cannot edit the Vettor Jurisdiction list. Bz 37966	Editing the Vettor Jurisdiction list of a Vettor certificate (either to add or to remove Jurisdictions) fails with the following message: LDAP_Query: [XrcXUDAUNABLE] unable to contact directory server. LDAP_Replace failed! objectClass (xuda_certificate), dn (md5=*md5 of Vettor certificate*)	Issue a new Vettor certificate, selecting the Jurisdictions at the time of certificate issuance.
Cannot search on Extended Validation attributes and custom attributes. Bz 102230	Jurisdiction of Incorporation attributes (used for Extended Validation certificates) and custom attributes are not available as qualifiers for search filters.	
Certificate Report Issues		
Clicking **Download** does not download report in certain cases. Bz 33138	If you use Microsoft Internet Explorer 6 on a Windows Server 2003 machine with Service Pack 1 installed, and you click the **Download** link of a generated certificate report, no pop-up dialog box opens. The report opens in the browser window.	Right-click the **Download** link and select **Save As** to save the report to a file.

Title	Description	Workaround (if available)
Jurisdiction Issues		
Registration Manager Vettors and Administrators receive e-mail notification when certificate request submitted to Certificate Manager. Bz 30860	If a Jurisdiction has **All Administrators** and **All Vettors** selected to receive e-mail notification of a certificate request, all Registration Manager Administrators and Vettors receive the e-mail message even if Registration Manager does not issue certificates for that Jurisdiction.	A Certificate Manager Administrator can explicitly select the Administrators and Vettors to receive e-mail notification rather than selecting **All Administrators** or **All Vettors**: 1. On the Jurisdiction Configuration page, from the **Sections** drop-down list, select **E-mail Notification**. 2. Under **Notification to vettors**, from the **All Chosen Recipients** list, remove **All Administrators** and **All Vettors**. 3. In the **Add Additional Recipients** text box, enter the e-mail addresses of the Administrators and Vettors who are to receive e-mail notification. 4. Click **Add Additional Recipients**. 5. Click **Save and Exit**.
Removing an active request for access to a Jurisdiction makes the Jurisdiction permanently unavailable. Bz 104413	If a Certificate Manager Administrator removes an active request for access to a Jurisdiction, the Jurisdiction remains in the disabled list at Registration Manager without a checkbox. You cannot make another request for access to this Jurisdiction.	
Enrollment Server Issues		
Certain pages on the Enrollment Server require JavaScript to be enabled. Bz 30765	The following pages on the Enrollment Server require the browser to be JavaScript-enabled: • Install the CA Certificate into a browser • Install Revocation List Signer Certificate into a browser • Save the CA Certificate to a file • Save Revocation List Signer Certificate to a file • Examine a CA Certificate (Designated Revocation List Signer).	JavaScript-enable the browser you use to access these capabilities at the Enrollment Server. It is possible to enroll for a certificate with a non-JavaScript enabled browser.
Back button on end-entity certificate search page navigates to the Enrollment Server welcome page. Bz 100497	With Firefox on a Linux or Solaris platform, if you click **End-Entity Certificate Options** on the Jurisdiction Options page and then click **Back** on the end-entity certificate search page, the Enrollment Server welcome page is displayed.	
Tool Issues		
Mediasign tool does not send passphrase to back end when Certificate Manager is started in “prompt” mode. Bz 31738	If Certificate Manager is started with CA passphrase set to **prompt every time**, the mediasign tool does not detect this and does not send the passphrase to the backend.	Start Certificate Manager with passphrases for CAs, and do not use “prompt every time” mode.

Title	Description	Workaround (if available)
SCEP Issues		
Approving a SCEP request fails when the issuing Jurisdiction is not the initial target Jurisdiction. Bz 37965	Approving a SCEP request fails when the issuing Jurisdiction is not the initial target Jurisdiction of the Registration Manager installation.	Submit SCEP requests to the initial target Jurisdiction of the Registration Manager installation.
HSM Issues		
Registration Manager installation fails against nCipher software v11.11 on Windows Server 2003 or Windows Server 2008. CERTMGR-3672, CERTMGR-3713	When you attempt to install Registration Manager with nCipher v11.20 on Windows Server 2003 or Windows Server 2008, the installation fails.	Before installing Registration Manager with nCipher, install nCipher. **To install nCipher v11.11 or later:** 1. Install the nCipher software **nfast** directory in C:\. 2. Change the following directories: On Windows Server 2003, change **C:\Documents and Settings\AllUsers\Application Data\nCipher** to **C:\nfast**. On Windows Server 2008, change **C:\ProgramData\nCipher** to **C:\nfast**. 3. Rename the following folders: • **Key Management Data** as **kmdata** • **Feature Certificates** as **femcerts** • **Log Files** as **log** 4. Click **Control Panel > System > Advanced > Environmental variables**, and create the following environmental variables that point to the renamed directories: • NFAST_CERTDIR = **C:\nfast\femcerts** • NFAST_KMDATA = **C:\nfast\kmdata** • NFAST_LOGDIR = **C:\nfast\log** **Note:** The installation automatically creates the NFAST_HOME variable, which points to **C:\nfast**.

Title	Description	Workaround (if available)
		To upgrade to nCipher v11.20 when Registration Manager is already installed with nCipher v10.50 or earlier: 1. Back up the **kmdata**, **log**, and **femcerts** folders of the existing nCipher installation. 2. Uninstall the existing nCipher software. 3. Install the nCipher v11.20 software. **Note:** The installation folders are created in the **C:\Program Files\nCipher\nfast** folder, and the Key Management data is created in the **C:\Documents and Settings\All Users\Application Data\nCipher\Key Management Data** folder. 4. Copy the **kmdata** and **log** folders that you backed up in step 1 to **C:\nfast\kmdata** and **C:\nfast\log**, respectively. 5. Reload the nCipher security world. 6. Change the following environment variables as specified below: • NFAST_KMDATA = **C:\nfast\kmdata** • NFAST_HOME = **C:\Program Files\nCipher\nfast** • NFAST_CERTDIR = **C:\Documents and Settings\All Users\Application Data\nCipher\Feature Certificates** • NFAST_LOGDIR = **C:\nfast\log*logfilename*** 7. Restart the nfast server and the existing Registration Manager services.

Installation of nCipher 11.30 (32-bit) on SUSE Linux Enterprise Server 11, Service Pack 1 fails.
CERTMGR-3845
	While installing nCipher from the **/opt/nfast/sbin/** directory, if you select option 1, the following error message is displayed: "User nfast does not exist or is in wrong group (users, not nfast)".	This problem occurs because the nfast user is assigned to the default group users instead of the nfast group.
		Before running the nCipher install script, you must manually create the nfast and ncsnmpd groups to resolve this error.
		To create nfast groups and users, type:
		`groupadd nfast`
		`useradd -r nfast -g nfast`
		To create ncsnmpd groups and users, type:
		`groupadd ncsnmpd`
		`useradd -r ncsnmpd -g ncsnmpd`

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**

Trademarks