Readme
RSA Validation Manager 3.2

July 22, 2013

Introduction

This document lists what's new and changed in RSA Validation Manager 3.2. It includes fixed issues and workarounds for known issues. Read this document before installing the software. This document contains the following sections:

- What's New
- Fixed Issues
- Known Issues
- Getting Support and Service

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

What's New

This section describes the major changes introduced in this release. For detailed information on each change, refer to the appropriate Validation Manager document.

Support for RSA SHA-2 Signature Algorithms

In addition to RSA SHA-1, RSA Validation Manager 3.2 supports RSA SHA-256, RSA SHA-384, and RSA SHA-512 signature algorithms for the following operations:

- Verifying an OCSP Request
- Signing an OCSP Response
- Creating an OCSP Signer with the Desired Cryptographic Provider, Signature Algorithm, and Key Size
- Viewing the Signature Algorithm Details of an OCSP Signer
- Adding a CA
- Importing a CRL
- Generating System Certificates During Installation
- Generating System Certificates and Keys Using the SystemCA Utility

Verifying an OCSP Request

You can configure Validation Manager to verify an OCSP request signed by any or all of the following signature algorithms:

- RSA SHA-1
- RSA SHA-256
- RSA SHA-384
- RSA SHA-512

If you configure Validation Manager by system default, the configuration applies to all the known CAs of Validation Manager. If you configure Validation Manager by CA based, the configuration applies only to the selected CA.

If the signature algorithm in the OCSP request does not match with the signature algorithms configured in Validation Manager, the OCSP request is not processed. A signature verification failed message is logged in the audit log file for that OCSP request and also in the **vm _trace log** file if the log level is LOW.

If the signature algorithm is accepted, the success log is logged in the **vm_trace log** file if the log level is HIGH.

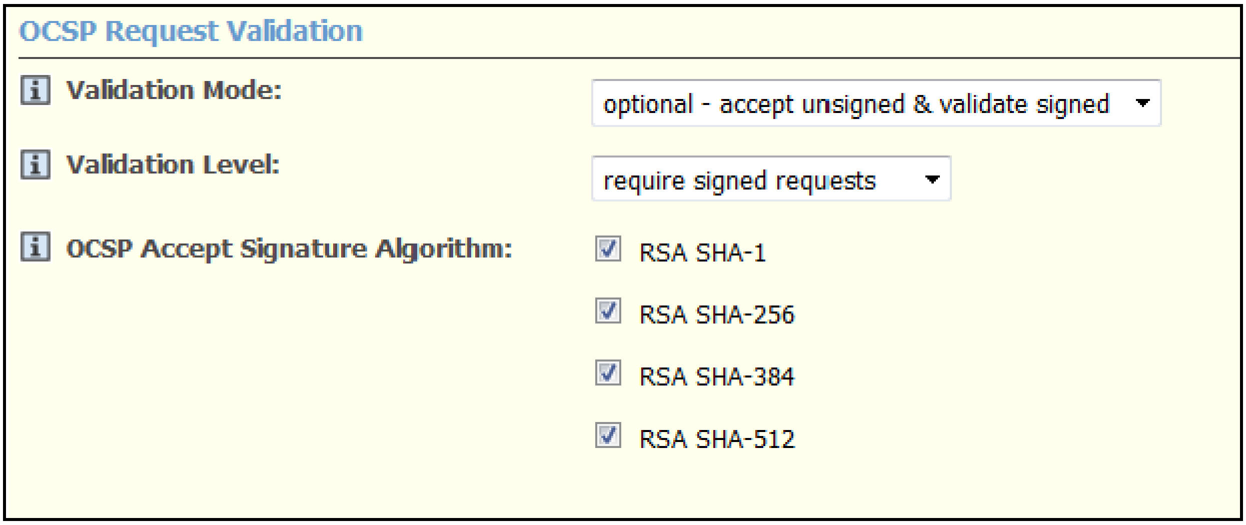
To configure Validation Manager by system default:

1. Access the Validation Manager GUI.
2. Click **Configure System** > **OCSP Configuration**.
3. Under the **OCSP Request Validation** section, select the acceptable signature algorithms for an OCSP request under **OCSP Accept Signature Algorithm**.

   The following algorithms are available:

   - RSA SHA-1
   - RSA SHA-256
   - RSA SHA-384
   - RSA SHA-512

   By default, all the algorithms are selected.



OCSP Request Validation

Validation Mode: optional - accept unsigned & validate signed

Validation Level: require signed requests

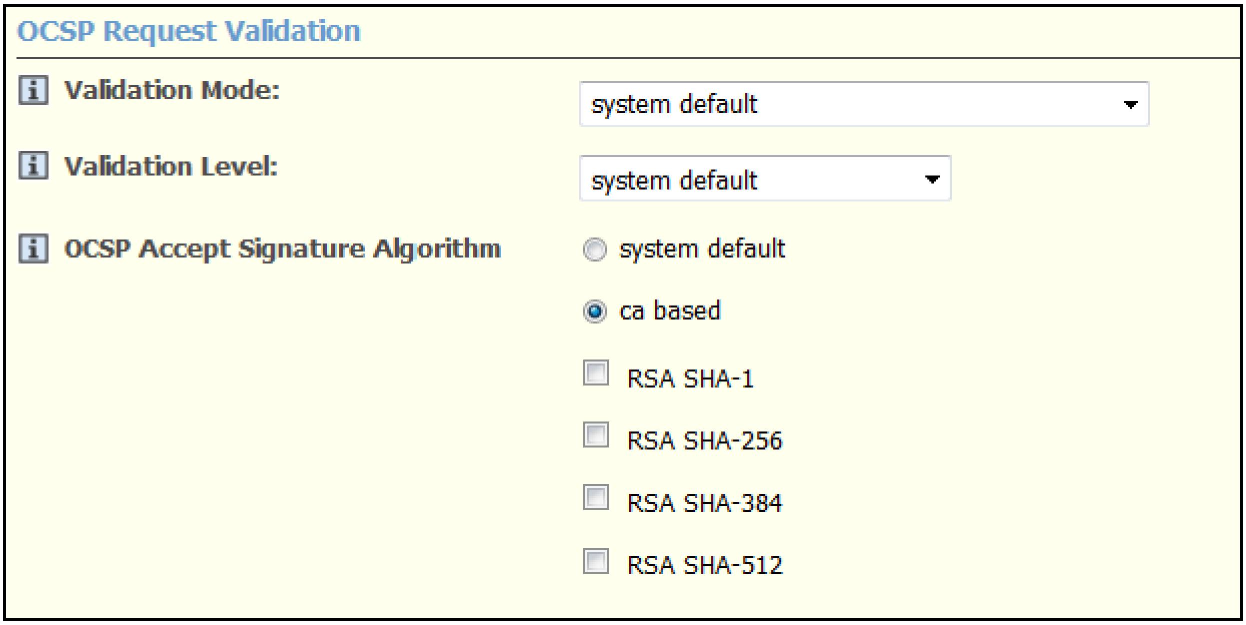
OCSP Accept Signature Algorithm:
☑ RSA SHA-1
☑ RSA SHA-256
☑ RSA SHA-384
☑ RSA SHA-512

4. Click **Save**.

To configure Validation Manager by CA based:

1. Access the Validation Manager GUI.
2. Click **CAs** > **Manage Existing**.
3. Select the CA from the list of known CAs that appears, and click **Edit Advanced**.
4. Under the **OCSP Request Validation** section, select **ca based** under **OCSP Accept Signature Algorithm**.

A list of acceptable algorithms appears.



OCSP Request Validation

Validation Mode: system default

Validation Level: system default

OCSP Accept Signature Algorithm

○ system default

● ca based

□ RSA SHA-1

□ RSA SHA-256

□ RSA SHA-384

□ RSA SHA-512

Note: If you select **system default**, the settings made on the OCSP Configuration page are applied to the CA.

5. Select the acceptable signature algorithms for an OCSP request.
6. Click **Save**.

Signing an OCSP Response

You can configure Validation Manager to sign an OCSP response with any one of the following algorithms:

- RSA SHA-1
- RSA SHA-256
- RSA SHA-384
- RSA SHA-512

If you configure Validation Manager by system default, the configuration applies to all the known CAs of Validation Manager. If you configure Validation Manager by CA based, the configuration applies only to the selected CA.

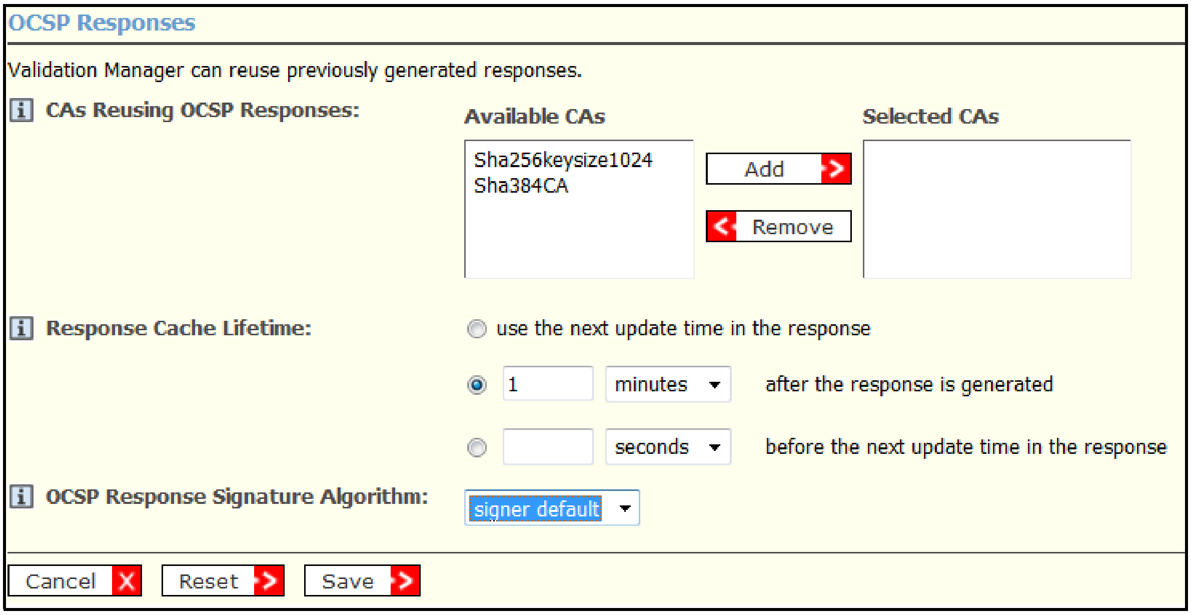
To configure Validation Manager by system default:

1. Access the Validation Manager GUI.
2. Click **Configure System** > **OCSP Configuration**.
3. Under **OCSP Responses**, select the required algorithm under **OCSP Response Signature Algorithm**.

   The following algorithms are available:

   - RSA SHA-1
   - RSA SHA-256
   - RSA SHA-384

- RSA SHA-512



OCSP Responses

Validation Manager can reuse previously generated responses.

CAs Reusing OCSP Responses:

Available CAs	Selected CAs
Sha256keysize1024 Sha384CA	

Response Cache Lifetime:

○ use the next update time in the response

● 1 minutes after the response is generated

○ seconds before the next update time in the response

OCSP Response Signature Algorithm: signer default

If you select **Signer Default** (default option), the algorithm used in the OCSP signer certificate is used to sign the OCSP response.

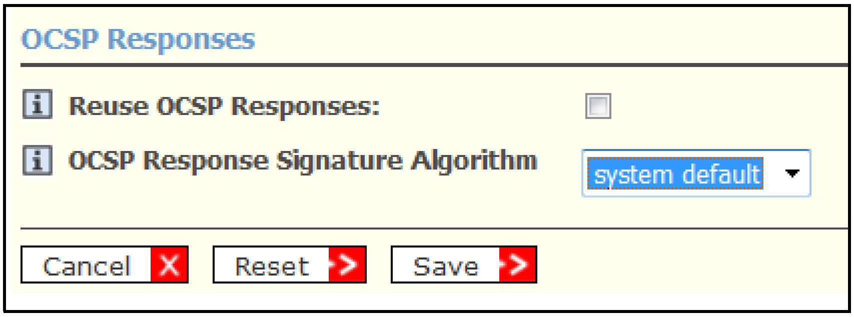
4. Click **Save**.

To configure Validation Manager by CA based:

1. Access the Validation Manager GUI.
2. Click **CAs** > **Manage Existing.**
3. Select the CA from the list of known CAs that appears, and click **Edit Advanced**.
4. Under the **OCSP Responses** section, select the required algorithm under **OCSP Response Signature Algorithm**.

   The following algorithms are available:

   - RSA SHA-1
   - RSA SHA-256
   - RSA SHA-384
   - RSA SHA-512



OCSP Responses

Reuse OCSP Responses: □

OCSP Response Signature Algorithm: system default

If you select **signer default**, the algorithm used in the OCSP signer certificate is used to sign the OCSP response.

If you select **system default**, the algorithm configured by system default is used to sign the OCSP response. This is the default value.

5. Click **Save**.

Creating an OCSP Signer with the Desired Cryptographic Provider, Signature Algorithm, and Key Size

You can create an OCSP signer with the following cryptographic providers, signature algorithms, and key sizes:

Cryptographic providers:

- Software
- nCipher
- PKCS #11

Signature algorithms:

- RSA SHA-1
- RSA SHA-256
- RSA SHA-384
- RSA SHA-512

Key sizes:

- 1024
- 2048
- 4096

To create an OCSP signer:

1. Access the Validation Manager GUI.
2. Click **OCSP Signers** > **Add New**.
3. Under **OCSP Signer Basics**:
   a. Type a name for the OCSP signer in the **OCSP Signer Nickname** field.
   b. If you want to make this the default signer, select **Make this the Default OCSP Signer**.
   c. Select a **Cryptographic Provider**. The default option is **Software**.
   d. Select a **Signature Algorithm**. The default option is **RSA SHA-1**.
   e. Select a **Key Size** for the algorithm. The default option is **1024**.
4. Under **Passphrase Configuration**, type a new passphrase to protect the OCSP signer private key, and confirm the same.
5. Click **Save**.

Viewing the Signature Algorithm Details of an OCSP Signer

You can view the details of the signature algorithm configured for an OCSP Signer.

To view the signature algorithm details of an OCSP signer:

1. Access the Validation Manager GUI.
2. Select **OCSP Signers** > **Manage Existing**.
3. Select the OCSP signer from the list that appears, and click **Edit**.

   You can view the details of the signature algorithm configured for the OCSP signer on this page.

Adding a CA

You can configure Validation Manager with a new CA whose certificate is signed by any of the following signature algorithms:

- RSA SHA-1

- RSA SHA-256
- RSA SHA-384
- RSA SHA-512

For instructions on how to add a CA, refer to the section “Importing a CA Certificate” in the chapter “Getting Started with RSA Validation Manager” in the *Administrator’s Guide*.

Importing a CRL

You can import a CRL into Validation Manager or verify a CRL that has been signed by the following signature algorithms:

- RSA SHA-1
- RSA SHA-256
- RSA SHA-384
- RSA SHA-512

For instructions on how to import a CRL into Validation Manager, refer to the section “Importing Revocation Lists” in the chapter “Managing CAs” in the *Administrator’s Guide*.

Generating System Certificates During Installation

You can configure Validation Manager to use any one of the following signature algorithms and key sizes while generating System certificates during installation.

The following signature algorithms are available:

- RSA SHA-1
- RSA SHA-256
- RSA SHA-384
- RSA SHA-512

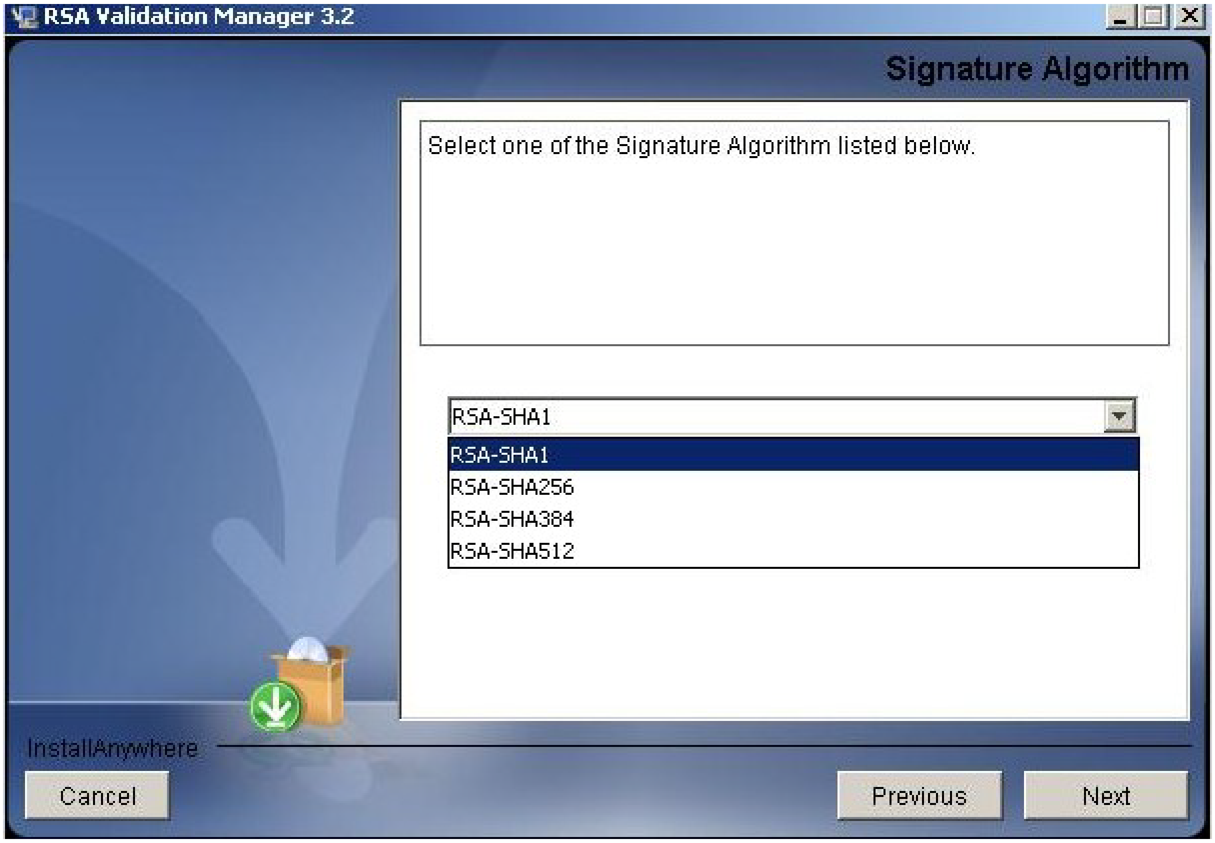
The following key sizes are available:

- 1024
- 2048
- 4096

By default, RSA SHA-1 signature algorithm and 1024 key size are selected.

To configure Validation Manager by GUI Based Installation:

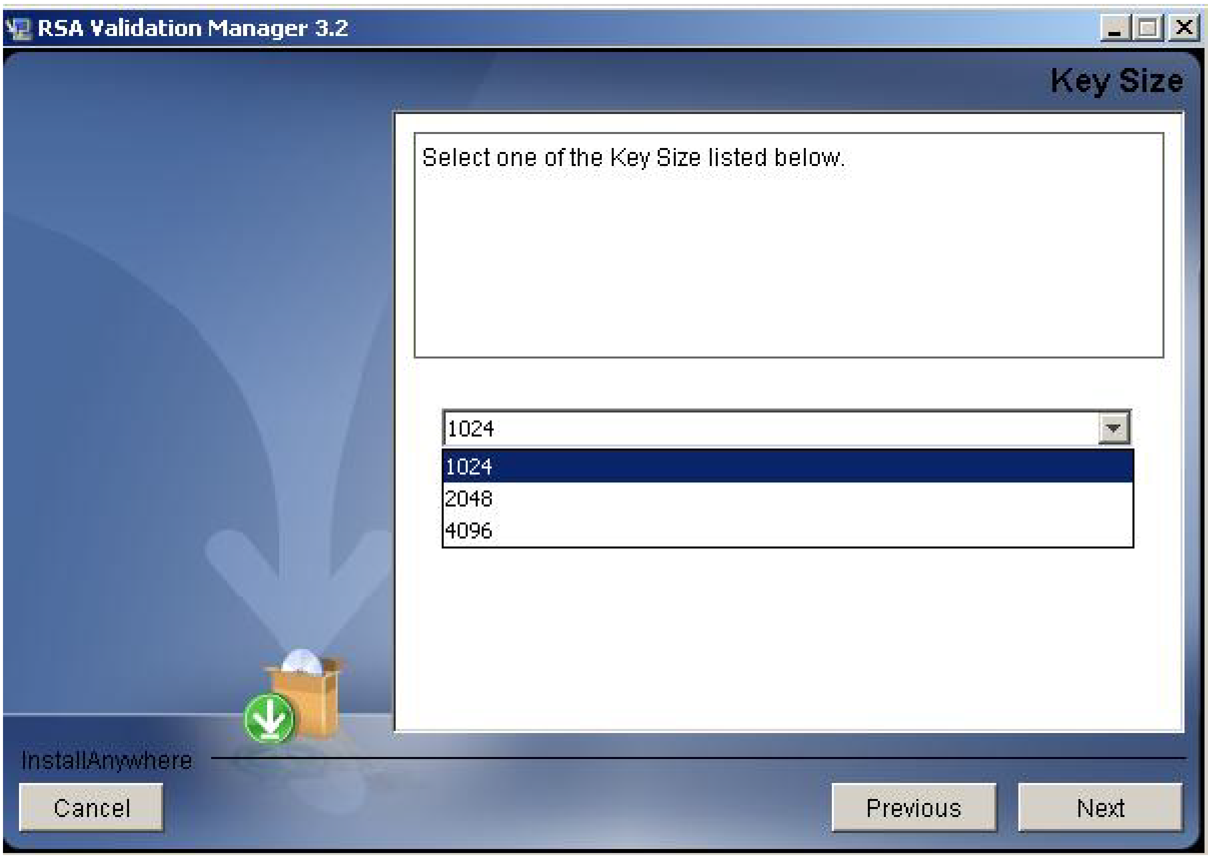
1. After confirming the system passphrase during installation, select one of the Signature Algorithms as shown in the following figure, and click **Next.**



Select one of the Signature Algorithm listed below.

RSA-SHA1

2. Select one of the key sizes from the list as shown in the following figure, and click **Next**.



Select one of the Key Size listed below.

1024

1024
2048
4096

System certificates will be issued with the specified Signature Algorithm and key size.

To configure Validation Manager by Console Based Installation:

1. After confirming the system passphrase during installation, enter the number corresponding to the desired Signature Algorithm, and press ENTER.
2. Enter the number corresponding to the desired key size, and press ENTER.

   System certificates will be issued with the specified Signature Algorithm and key size.

To configure Validation Manager by Silent Installation:

Add the following variable names and values in the java properties file.

- INPUT_SIG_ALGO <signature algorithm>

  Accepted values for <signature algorithm> are RSA-SHA1, RSA-SHA256, RSA-SHA384, and RSA-SHA512
- INPUT_KEYSIZE <key size>

  Accepted values for <key size> are 1024, 2048, and 4096

System/SSL certificate will be issued with the specified Signature Algorithm and key size.

Generating System Certificates and Keys Using the SystemCA Utility

You can use SystemCA utility to generate system certificates with any one of the following signature algorithms:

- RSA SHA-1
- RSA SHA-256
- RSA SHA-384

- RSA SHA-512

Refer to the “Generating System Certificates and Keys” section in the “Configuring RSA Validation Manager” chapter in the *Administrator’s Guide* for more details.

Support for new platforms

Validation Manager can be installed on Red Hat Enterprise Linux (RHEL) 6.3 operating system.

Important: RSA Validation Manager 3.2 does not support Solaris 10 and SUSE Linux 11 update 1. If you have installed Validation Manager on Solaris or SUSE Linux, you must first create an upgrade package using RSA Validation Manager 3.1 Build 162 installation package, and then upgrade to one of of the supported platforms listed in the “Supported Platforms” section in the “System Requirements” chapter in the Installation Guide.

Support for new browsers

Validation Manager supports browser-based administration with the following browsers:

- Microsoft Internet Explorer 8.0 and 9.0 on Microsoft Windows Server 2008 R2 server
- Mozilla Firefox 10.0 on RHEL 6.3

Qualification of Validation Manager with Luna SA v5.1.1

RSA Validation Manager 3.2 is qualified with Luna SA v5.1.1.

Support for Features Beyond the Year 2038

Validation Manager supports the following features with validity beyond the year 2038:

- Adding a CA
- Importing a CRL
- Adding an OCSP signer certificate
- Regenerating system certificates (system CA and SSL certificates)
- Validating a certificate using OCSP

Important: Validation Manager will not function properly if the system time is changed to beyond the year 2038. Also, Validation Manager only supports certificates with validity up to year 2050. These issues are described in the Known Issues section.

Upgrade on Libraries

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

- Apache HTTP Server 2.2.22 plus additional security fixes from Apache 2.2.23
- Apache Tomcat 7.0.37
- Oracle Berkeley DB (BDB) 5.3.21
- RSA BSAFE SSL-C 2.8.7
- OpenLDAP 2.4.33
- mod_jk 1.2.37

Fixed Issues

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

Tracking Number	Description	Resolution
VALSRV-1553	Validation Manager cannot process a URL-encoded OCSP request when submitted using the HTTP GET method. The returned error code is 404.	This issue has been fixed in RSA Validation Manager 3.2.
VALSRV-1600 VALSRV-1611 VALSRV-1620 VALSRV-1634	RSA Validation Manager is susceptible to the following Apache vulnerabilities: CVE-2003-1567 CVE-2004-2320 CVE-2010-0386 CVE-2011-3192 CVE-2012-0053 Qualys ID: 86847, no CVE assigned For information on these vulnerabilities, go to **http://web.nvd.nist.gov/view/vuln/search** and search by the CVE ID.	This issue has been fixed in RSA Validation Manager 3.2 by upgrading to Apache 2.2.22 plus security vulnerability fixes from Apache 2.2.23.
VALSRV-1234	After starting up the Validation Server, Apache service reports an error message to the Event Viewer (Windows) or syslog (Linux) stating that there are no installed ConfigArgs for the Validation Server service.	This issue has been fixed in RSA Validation Manager 3.2

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.

Issue	Description	Workaround (if available)
Validation Manager will not function properly if the system time is changed to beyond the year 2038 VALSRV-1662	Validation Manager will not function properly if the system time is changed to the year beyond 2038. This issue is applicable only when Validation Manager is installed on Linux.	
Validation Manager only supports certificates with validity up to year 2050. VALSRV-1662	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 Validation Manager, the certificate validity TIME is stored in the following UTCTime format: YYMMDDHHMMSSZ. Validation Manager only supports certificates with validity up to year 2050.	

Issue	**Description**	**Workaround (if available)**
Unable to access Validation Manager GUI in Internet Explorer 8 VALSRV-1663	If the system CA and SSL certificates use the RSA SHA-2 signature algorithms, Validation Manager GUI is not accessible in Internet Explorer 8 on Windows 2003 server.	Apply the Microsoft patch available at **http://support.microsoft.com/kb/938397**
Validation Manager installation fails against nCipher software 11.11 or later on Windows 2003 or Windows 2008.	When you attempt to install Validation Manager with nCipher 11.11 or later on Windows 2003 or Windows 2008, the installation fails.	**Before installing Validation Manager with nCipher, follow the steps given below:** 1. Install the nCipher software from the **nfast** directory in **C:\**. 2. Change the directories: • from **C:\Documents and Settings\All Users\Application Data\nCipher** to **C:\nfast**, in Windows 2003. • from **C:\ProgramData\nCipher** to **C:\nfast** in Windows 2008. 3. Rename: • **Key Management Data** to **kmdata** • **Feature Certificates** to **femcerts** • **Log Files** to **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** which points to the location **C:\nfast**.
User Authentication Issues		
Unable to logon to Validation Manager configured for certificate authentication only, if users are stored in an LDAP directory. Bz 28016	If you use an LDAP directory to store users and you configure user authentication by certificates only, users cannot logon to Validation Manager due to a deficiency in the application server used to manage users (Tomcat 4.1.27).	Use another user authentication method or store users in the Validation Manager database instead of LDAP.
nCipher Issues		
Loss of communication between Validation Manager and nCipher network HSM. Bz 28728	After an extended period of time, the communication between Validation Manager and nCipher NetHSM may be lost.	Restart Validation Manager and reenter all the nCipher passphrases.
Validation Manager Operations Issues		

Issue	Description	Workaround (if available)
If OCSP requests for certificates issued by a CA are signed by a certificate issued by the same CA, certificate status is returned incorrectly. Bz 28157	If you set CA purposes only to **verify OCSP clients**, the OCSP response returned by Validation Manager is an `unauthorized` OCSP error. A successful OCSP response containing an `unknown` certificate status is the expected behavior. If you set CA purposes only to **provide certificate status**, the OCSP response returned by Validation Manager is a successful OCSP response containing the actual certificate status. The expected behavior is an `unauthorized` OCSP error.	
Configuration with status source always checking CA-issued remote server certificate causes Validation Manager to go into an infinite loop. Bz 28447	The following configuration is not supported: • You add an OCSP-based or revocation list-based status source with a TLS-based retrieval method using the known CA TLS authentication mechanism, and select to always check the remote server certificate. • You import a CA, setting it to use the newly created revocation list based status source. • The imported CA also issues the remote server certificate.	
Audit Log Issues		
Validation Manager does not log OCSP failures to connect to audit log when forwarding. Bz 28452	If an OCSP status source is configured with an invalid URL or if the remote responder is down or unreachable, Validation Manager responds with `unknown` and logs errors in the trace log file, but does not log anything in the audit log about the forwarding failure. There is an audit log entry indicating the success of the OCSP response.	
Revocation list import is not logged on secondary cluster nodes. Bz 28667	By default, Validation Manager is configured to log the import of revocation lists on success and failure. However, the success operation is not logged at secondary cluster nodes because no revocation list imports occur at the secondary node. The revocation list imports occur at the primary node and those imports are logged.	
Clustering Issues		
Configuring Validation Manager for both synchronization and clustering.	You can configure a cluster in Validation Manager as a synchronization server only.	

Issue	Description	Workaround (if available)
Database errors may occur if a revocation list is downloaded during recovery of the primary node. Bz 28860	If a revocation list is retrieved during recovery of the primary node, the database may become out of sync. As a result, some nodes may become outdated and need to be shut down and restored from a hot backup.	To prevent the database from becoming out of sync, RSA strongly recommends that you suspend OCSP services while the primary node is recovering (that is, before the server processes are started). Once replication initialization is complete, you can resume OCSP services.
Uninstallation Issues		
Uninstallation on Windows removes all files. Bz 27782	If you uninstall Validation Manager from your Windows platform, the text displayed during the uninstallation process states that files and folders created after installation are not removed, although, in some cases, all the files and folders are removed from the machine.	

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.emc.com/support/rsa/index.htm**
RSA Secured Partner Solutions Directory	**https://gallery.emc.com/community/marketplace/rsa?view=overview**

Trademarks