Release Notes
RSA enVision 4.0 Service Pack 3

February 17, 2010
Revision 2

Introduction

This document describes what is new and changed in RSA enVision 4.0 Service Pack 3. It includes installation information, as well as workarounds for known issues. Read this document before installing the service pack. This document contains the following sections:

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

What's New in This Release

This section describes the major changes introduced since the release of RSA enVision 4.0.

New in Service Pack 3

NIC Packager Service Update

RSA updated the NIC Packager Service to address supportability of the packager process. The NIC Packager Service indexes, compresses, and stores the files created by the NIC Collector Service in the event database (IPDB).

As part of these updates, RSA has added a new message indicating the NIC Packager Service may be falling behind. The following table describes this message.

Item	Description
Message	NIC-4-508046, PKG_STATUS_WARNING
Recommendation	If you receive the PKG_STATUS_WARNING message, call RSA Technical Support immediately. **CAUTION: Do not restart the NIC Packager Service.**
To alert on this message	RSA recommends that you install the January 2010 Event Source Update, which contains the new message that will automatically be alerted on in the NIC View.
Best practices for alerting on this message	RSA strongly recommends that you monitor the NIC-4-508046 message using an output action, due to the severe ramifications that could occur if the NIC Packager Service stops or hangs completely. As you cannot modify the **NIC_View** or the NIC correlated rules associated with it, RSA recommends that you either add the NIC-4-508046 message to an existing view that you are monitoring or create a new view to include this message, and add an output action to notify you when this message is received. See the enVision Help for information on adding or modifying a view, and creating an output action.

Device Down Message

Use the **Device Down** message (NIC message 400029) to determine when an event source (device) has not sent a message in a specified amount of time. Using this message greatly improves the efficiency of the enVision system in contrast to using the default, NIC message 508100.

To configure how and when the system generates Device Down messages, set parameters in the following files:

- Initialization file (**pi.ini**)
- Configuration file (**devicedown.conf**)
- Position file (**devicedown.pos**)

Initialization File

The **pi.ini** file contains flags that determine whether or not NIC 508100 and 400029 messages are generated.

Flag	**Default**	**Description**
ENABLE_508100_MESSAGE	True	Enables the generation of NIC message 508100. Set to **FALSE** to disable generation of NIC message 508100.
ENABLE_400029_MESSAGE	False	Enables the generation of NIC message 400029. Set to **FALSE** to disable generation of NIC message 400029.

If neither parameter is included in the **pi.ini** file, enVision generates NIC message 508100 and does not generate NIC message 400029.

The NIC Logger Service continues to generate NIC 508100 messages. That is, setting ENABLE_508100_MESSAGE to false does not affect messages coming from the NIC Logger Service.

NIC message 400029 is not generated for devices that are disabled.

Restart the Collector only if the settings in the pi.ini files have changed. The system reads the devicedown.conf file every 30 minutes. Any changes to the file will be reflected the next time the configuration file is read.

Restart the Collector if you change the settings in the **pi.ini** file. The system reads the **devicedown.conf** file every thirty minutes. Any changes to the **devicedown.conf** file are reflected the next time the configuration file is read.

Configuration File

You can place the **devicedown.conf** file in either of the following locations:

- **..\nic\csd\config\collectors** directory. If placed here, it is used by all Collectors in the site.
- **..\nic\csd\config\collectors\*node_name*** directory. If placed here, it applies only to the *node_name* Collector. For the *node_name* Collector, settings in this file have priority over more global settings in the **devicedown.conf** file in the parent folder.

The configuration file specifies time-outs, polling period, configuration period, and alert period.

Parameter	**Description**	**Syntax**	**Valid Values**
Time-out	Time-outs specify how long the Collector waits for a message to arrive from an event source before determining that it is not working. All time-out values are specified in minutes. You can specify time-outs at the following levels: • System-wide • Device type • Device group • Device The system applies the time-outs to the event sources in the order listed. Thus, a device type time-out overrides a system time-out, a device group time-out overrides a device type time-out, and so on. You can configure time-outs for a maximum of 250 device types. A time-out value of zero disables the generation of the NIC 400029 message. This allows you to selectively disable the Device Down message for a particular device type or device level.	SYSTEM_TIMEOUT time DEVICETYPE_TIMEOUT device_type time DEVICEGROUP_TIMEOUT device_group time DEVICE_TIMEOUT device_type ip_address time	1 - 1000000 Default is 120 0 - 1000000 0 - 1000000 0 - 1000000
Polling Period	The polling period is the interval at which the Collector checks for time-outs. For example, if the polling period is set to 2, every two minutes the Collector checks for event sources that have exceeded their time-out. RSA recommends that you set the value to half the shortest time-out. For example, if the shortest time-out is set to two minutes, set the polling period to one minute.	POLLING_PERIOD time	1 - 1000000 Default is 5
Configuration Period	The configuration period is the interval at which the Collector reads the configuration file. For example, if the configuration period is set to 20, every twenty minutes the Collector reads the configuration file and applies its settings to the time-outs for the event sources from which it is collecting. This operation is expensive in terms of system resources because it requires database access. Avoid setting the value any lower than necessary. RSA enVision reads the configuration file whenever the Collector starts.	CONFIGURATION_PERIOD time	1 - 1000000 Default is 30

Parameter	Description	Syntax	Valid Values
Alert Period	The alert period specifies the interval at which the system generates a NIC 400029 message after a time-out is reached. For example, assume an event source times out after thirty minutes. If the alert period is set to three minutes, the system generates a NIC 400029 message every three minutes until the event source begins working. The default value for the alert period is five minutes. If the alert period is set to zero, the alert period defaults to the time-out specified for the event source. For example, if the time-out for an event source is 30, the system generates the NIC 400029 message every thirty minutes while the event source is not working.	ALERT_PERIOD time	0 - 1000000 Default is 5

Syntax

For efficient processing, always specify parameters in the following order:

1. SYSTEM_TIMEOUT
2. POLLING_PERIOD
3. CONFIGURATION_PERIOD
4. ALERT_PERIOD
5. Any device type time-out settings
6. Any device group time-out settings
7. Any specific device time-out settings
8. END

The only required line is END. All the other parameters are optional.

Example

Here is an example of a complete configuration file (line numbers are added to help identify the lines, and are not part of the actual file):

```
01 SYSTEM_TIMEOUT                                   60
02 POLLING_PERIOD                                   1
03 CONFIGURATION_PERIOD                             20
04 ALERT_PERIOD                                     3
05 DEVICETYPE_TIMEOUT ciscopix                      150
06 DEVICETYPE_TIMEOUT ciscorouter                   1500
07 DEVICETYPE_TIMEOUT checkpointfw1                 5
08 DEVICEGROUP_TIMEOUT ExchangeServers              10
09 DEVICE_TIMEOUT checkpointfw1 196.24.90.3         0
10 DEVICE_TIMEOUT checkpointfw1 196.24.90.4         3
11 DEVICE_TIMEOUT checkpointfw1 196.24.90.5         4
12 DEVICE_TIMEOUT checkpointfw1 196.24.90.6         0
13 END
```

Line by line details:

Line 01: sets the default time-out for all devices to sixty minutes
Line 02: sets the polling period to one minute
Line 03: sets the configuration period to twenty minutes
Line 04: sets the alert period to three minutes
Line 05: sets the time-out for the **ciscopix** device type to one hundred and fifty minutes
Line 06: sets the time-out for the **ciscorouter** device type to fifteen hundred minutes
Line 07: sets the time-out for the **checkpointfw1** device type to five minutes
Line 08: sets the time-out for devices in the **ExchangeServers** device group to ten minutes
Line 09: disables the NIC 400029 message for the specific checkpointfw1 device with the IP address of 196.24.90.3
Line 10: sets the time-out for the specific checkpointfw1 device with the IP address of 196.24.90.4 to three minutes
Line 11: sets the time-out for the specific checkpointfw1 device with the IP address of 196.24.90.5 to four minutes
Line 12: disables the 400029 message for the specific checkpointfw1 device with the IP address of 196.24.90.6
Line 13: ends the configuration file and is a required statement

Position File

The devicedown.pos file exists in the **..\nic\csd\config\collectors\*node_name*** directory. For each event source (device), it keeps track of the time when enVision last received a message from that event source. The system updates this file every five minutes, and whenever the Collector shuts down.

When the NIC Collector Service starts, it reads this file to update its internal cache with the time values for each event source. If the file does not exist, the system creates the file, using the current time as the “last message received” time for each event source.

New in Service Pack 2

FIPS 140-2 Cryptography Support

With the introduction of FIPS 140-2 Level 1 validated cryptography in RSA enVision 4.0 Service Pack 2, enVision now supports FIPS mode. FIPS mode is supported only for new enVision installations. For further information, contact RSA Customer Support.

WinSSHD Upgrade

The service pack provides a new version of WinSSHD, which is required to support FIPS compliance. After applying the service pack, some users may see a logon error for the **NIC_sshd** account. If you experience this issue, update the WinSSHD credential cache as follows:

1. Launch WinSSHD by selecting **Start** > **Administrative Tools** > **WinSSHD Control Panel**.
2. On the **Server** tab, click **Manage Password Cache**.
3. Click **Manage Password Cache**.
4. Select **Add Item**.
5. In the dialog box, in the **Domain** field, enter the NIC site name. For the account name, enter **NIC_sshd**, and enter the password for this account.
6. Click **Apply**, and then click **OK**.
7. Repeat steps 4 to 6 for the **NIC_sftp** account.

For further information, contact RSA Customer Support.

New Parameters in pi.ini

To help address performance issues with the NIC Alerter Service, RSA added the following parameters to the **pi.ini** file.

Variable Name	**Description**	**Range**	**Default**	**Comments**
AL_MTNODE_PRESERVE_COUNT	Determines the number of unused nodes to leave after cleanup.	0 to 4096	1024	When the alerter is consuming a lot of memory, lower the value from 1024 as necessary.

Variable Name	**Description**	**Range**	**Default**	**Comments**
AL_MTNODE_CLEANUP_INTERVAL	Determines the interval (in seconds) after which the alerter checks for any unused nodes to clean up.	1 to 86400	300	For frequent cleanup of memory, lower the default value.
AL_ANODE_STATISTICS	Determines whether a NIC message 608803 should be posted showing information regarding cleanup.	TRUE or FALSE	FALSE	Set to TRUE to see NIC message 608803, which contains information about the cleanup. This information is useful for fine tuning the following parameters: AL_ANODE_PRESERVE_COUNT AL_ANODE_CLEANUP_INTERVAL
AL_ANODE_PRESERVE_COUNT	Determines the number of unused nodes to leave after cleanup.	0 to 4096	1024	When the alerter is consuming a lot of memory, lower the value from 1024 as necessary.
AL_ANODE_CLEANUP_INTERVAL	Determines the interval (in seconds) after which the alerter checks for any unused nodes to clean up.	1 to 86400	300	For frequent cleanup of memory, lower the default value.

For example, consider the following settings:

- AL_ANODE_STATISTICS=TRUE
- AL_ANODE_CLEANUP_INTERVAL=120
- AL_ANODE_PRESERVE_COUNT=16

These settings keep 16 inactive memory instances, while de-allocating all the remaining inactive instances in a two-minute interval. Also, the system generates NIC message 608803, displaying information about the number of instances currently in use per view.

Product Documentation

The following documentation is available on RSA SecurCare Online, at **Products** > **RSA enVision** > **enVision** > **RSA enVision Platform 4.0 Documentation**.

- *RSA enVision 4.0 Configuration Guide*
- *RSA enVision 4.0 Hardware Guide*
- *RSA enVision 4.0 Migration Guide*
- *RSA enVision 4.0 Factory Re-Imaging and Typing Guide*
- *RSA enVision Overview Guide*

  Note: The Overview Guide is new for RSA enVision 4.0 SP 3, and provides an introduction to RSA enVision features and capabilities. The guide is intended for enVision administrators, enVision users, and other readers who require a high-level understanding of enVision.

- RSA enVision 4.0 Help

Service Pack Installation

This section describes how to install the service pack.

Prerequisite

Ensure that RSA enVision 4.0, 4.0 SP 1, or 4.0 SP 2 is running on the appliances on which you are installing the service pack.

Installation

Download the service pack executable file, and run the installer, as described in the following procedure. For multiple appliance sites, complete the following procedure on each appliance within the site.

Note: RSA requires that, if you install content updates, you do so after you install the service pack.

Installation Order

Depending on the type of enVision site, install the service pack in the following order:

- In multiple appliance sites:
  - Install on the D-SRV first
  - Install on the other appliances in any order
- In a multiple appliance site with Enhanced Availability:
  - Install on the DA1 Server (D-SRV) first
  - Install on the A-SRV
  - Install on an inactive CA
  - Manually failover to the just upgraded CA
  - Install on the CA made inactive by the failover
  - If applicable, failover and install on any remaining CAs
- In a multiple site deployment, with or without Enhanced Availability:
  - Install on the master site first
  - Install on the slave site or sites

To install the service pack:

1. Log on to RSA enVision as the master user account.
2. From RSA SecurCare Online, download **enVision Version 4.0 SP 3**. Save the file in the **E:\nic\installables** folder of the appliance. In a multiple appliance site, copy the file to the **E:\nic\installables** folder of each appliance.

   Note: Close the enVision folder to avoid a “Folder in use” error.

3. Close all applications running on the appliance, including any third-party applications, and all windows.
4. Double-click the enVision software update file, **RSA_enVision4.0SP3b0311.exe**, to launch it.
5. Read the License Agreement, and click **Yes**.

   The installation utility installs the files, backs up the database and configuration information, updates the software files and configuration files, and prompts you to restart the appliance.

6. Click **Finish**.

   The appliance restarts.

7. Repeat this procedure for each appliance in the site.

When you have completed the installation on all appliances in the site, you have successfully installed the service pack.

Note: If you had applied a recent hot fix for RSA enVision 4.0.0 that is not included in this service pack, you must reapply the hot fix after you install the service pack. For more information, see the following section, “Fixed Issues.”

To confirm the installation in a single appliance site:

1. On the appliance, log on to enVision.
2. Click **Overview** > **System Performance**, and verify that RSA enVision 4.0 SP 3 Build:0311 is installed.

To confirm the installation in a multiple appliance site:

1. On each A-SRV, follow these steps to confirm the installation:
   a. Log on to enVision.
   b. Click **Overview** > **System Performance**, and verify that enVision 4.0 SP 3 Build 0311 is installed.
2. On the D-SRV and each LC, follow these steps to verify the installation:
   a. Log on to the appliance.
   b. Open the **ver.dat** file, located in the **E:\nic\*version**system_name*\etc** folder, and ensure that VERSION=4000.0311 and SERVICEPACKNUMBER=3.

Fixed Issues

This section lists the issues that have been fixed since the release of RSA enVision version 4.0.

Fixed in Service Pack 3

The following table lists issues fixed in Service Pack 3.

Jira ID #	Bugzilla	Description
env-26239	108569	RSA corrected an issue where certain special characters in report criteria caused a loss of data in the report.
env-28222	116785	RSA optimized the way filters are applied to correlated rules.
env-29495	122393	RSA corrected an issue where the System Performance window did not update the SDEE Total Events Per Second (EPS) values.
env-29844	123988	RSA corrected an issue where any enVision user, with or without permission to access reports, could browse reports created by the Scheduler.
env-29869, env-30549, env-30466, env-30809, env-30945, env-31274	124052, 126391, 126612, 127504, 128967, 128010	RSA made enhancements to the Windows Agentless Collector: • RSA addressed an issue where the Windows Agentless Collector sometimes stopped collecting messages. • The Windows Agentless Collector sometimes lost events in some high-message-volume scenarios. RSA modified the Windows Agentless Collector to minimize the event loss in case the Windows log files are being written to at a very high rate. • RSA updated the parsing algorithm so that all strings in events are correctly stored to the IPDB.
env-29978	124403	RSA corrected an issue with the **taskcreate** output action, where certain characters in group names caused menu items to display incorrectly.

Jira ID #	**Bugzilla**	**Description**
env-30078, env-31273, env-32091	124823	Report generation was taking excessive time, compared to RSA enVision 3.7. RSA optimized parser performance.
env-30145, env-31151	125130, 128624	RSA corrected an issue with the SDEE Service, where it did not correctly delete temporary data files.
env-30285, env-29707, env-30850	125634, 123502	RSA corrected an issue where the Checkpoint FW-1 event source was not sending audit logs to enVision.
env-30347, env-31127	127574, 128549	RSA updated the NIC Packager Service to check the size of the message ID constructed by certain functions.
env-30355	125971	RSA corrected an issue where Japanese characters in a scheduled report would not display correctly.
env-30565, env-31669	126671	RSA enVision now logs a NIC message for any event source (device) that is not functioning. For details, see Device Down Message on page 2.
env-30590	126828	RSA corrected an issue where imported watchlists were not formatted correctly.
env-30648, env-31155	127059, 128638	The names of dashboard reports are limited to 64 characters. RSA enVision did not enforce this limitation. If users created reports that exceeded this limit, the reports disappeared from the list but remained in the Manage Dashboard screen (with the name truncated to 64 characters). RSA enVision now enforces the 64-character limit for report names.
env-30735	127289	RSA corrected an issue in the NIC Server where events were not displayed correctly if they contained characters from the Japanese SHIFT-JIS character set (or any other non-UTF-8 characters).
env-30753, env-30815	127402, 127520	RSA corrected several issues with the Maintenance Command Line Interface (CLI) utility, **lsmaint.exe**.
env-30810, env-32379	127505	In a multiple-site configuration, a remote query (data does not reside on the site running the query) would cause a memory spike on the remote NIC Server (server with the data). This issue has been corrected.
env-31047, env-31157	128258, 128640	RSA added the ability to sort the list of event sources in the **Analysis** tab.
env-31153	128634	If a user tried to cancel an ad-hoc report while it was running, enVision closed the Progress Bar window, but continued to process the report or query in the background. This suggests that the NIC Server Service continued to retrieve event data. This issue has been corrected.
env-31154, env-28880	128635, 119110	RSA addressed issues where, under certain conditions, enVision did not properly release database connections.
env-31156	128639	RSA addressed an issue where the enVision UI sometimes stopped responding when users ran reports.
env-31234, env-29671	128884, 123315	The instructions in the Help topic, **Add Second LC to a Multiple Appliance (Also Referred to as an LS) Cluster**, are incorrect and must not be used. A new document, **Add a New Appliance to an Existing Site**, is available on RSA SecurCare Online with the RSA enVision 4.0 documentation. Customers must download this document for the correct set of instructions. This document is valid for 60 series appliances running RSA enVision 3.7 or 4.0.

Jira ID #	Bugzilla	Description
env-31258, env-32283, env-32285, env-31309	128933, 129055	RSA increased efficiency for DNS lookups.
env-31311	129060	An internal and unsupported utility, lsdata, has been updated to change the way it communicates with enVision nodes.
env-31344	129157	The NIC Web Server Service sometimes ran out of memory and stopped working. RSA corrected this issue by enabling the LAA flag (Large Address Aware).
env-31868, env-32450	N/A	RSA addressed an issue where the NIC Forwarder Service stopped sending logs from the Remote Collectors (RC) to the Data Servers (D-SRV).

Fixed in Service Pack 2

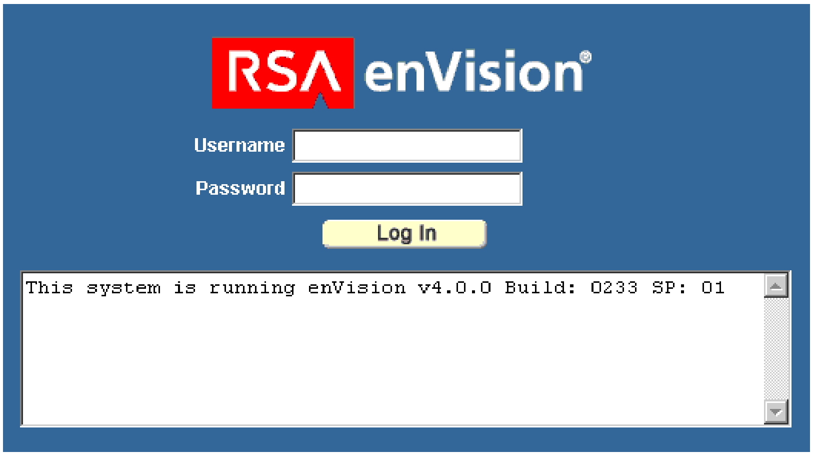
The following table lists issues fixed in Service Pack 2.

Tracking Number	Description
118199	RSA addressed an issue where ODBC event collection from an Oracle event source caused a memory leak.
123186, 121996, 124632, 123784	RSA addressed an issue where event collection from a Checkpoint event source was running behind. The time difference in Event Viewer (in real time) and the message time stamp was as much as 10 hours.
124747	RSA added support for Tenable Nessus version 4.0.1.
124871	RSA addressed a performance issue with the Alert history not updating in a timely manner.
125440, 125435, 125436, 125437, 125442, 126073	RSA addressed several issues to improve the performance of the NIC Alerter Service. As part of this fix, RSA added several variables to the **pi.ini** file. For details, see New Parameters in pi.ini on page 5.
125906	RSA addressed a connection count limit issue that caused NIC Server Service exceptions.
125965	RSA added support for Oracle version 10.2.0.4.

Fixed in Service Pack 1

The following table lists issues fixed in Service Pack 1.

Identifier	**Description**
Issue 117820	RSA enVision now enforces complex passwords for all user accounts. If you do not set the parameters for complex passwords, no minimum requirements are enforced. Passwords may be any length and format. Your administrator can configure the following parameters: • minimum number of characters: **password.minLength** • minimum number of lower case letters: **password.minLengthLowerCase** • minimum number of upper case letters: **password.minLengthUpperCase** • minimum number of non-alpha characters: **password.minLengthNonAlphaCharacters** • minimum number of non-alphanumeric characters: **password.minLengthNonAlphanumericCharacters** Use the **login.ini** file to add or edit these parameters. The file is in the **E:\nic\*version*\system_Name\etc** folder, where *version* is your enVision version number, and *system_Name* is the name of your enVision server. **Note:** Adding any of these lines to the **login.ini** file turns on password complexity, and all values are set to the default automatically. The default values are as follows: • password.minLength=8 • password.minLengthUpperCase=1 • password.minLengthLowerCase=1 • password.minLengthNonAlphaCharacters=0 • password.minLengthNonAlphanumericCharacters=0 For example, the following password setting accepts the value **@BCdef&8**: • password.minLength=8 • password.minLengthUpperCase=2 • password.minLengthLowerCase=3 • password.minLengthNonAlphaCharacters=1 • password.minLengthNonAlphanumericCharacters=2

Identifier	Description
Issue 117821	RSA enVision displays configurable banner text on the logon screen. To add banner text, edit the **login.ini** file, and set the **banner.text** parameter to the required text. The length of the string is limited to 2048 characters and is displayed as plain text. Example: banner.text=This system is running enVision v4.0.0 Build: 0233 SP: 01 **Note:** After you enable the banner by editing and saving the **login.ini** file, restart the NIC Web Server Service for the change to take effect. The following figure shows an example banner.  This system is running enVision v4.0.0 Build: 0233 SP: 01
Issue 118913	When users restarted a view that referred to a correlated rule containing a device group, the system may have generated a web server error. RSA has corrected the issue.
Issue 120035	The logger logs startup and shutdown events. It uses the following message IDs to log these events: • <5> %NIC-5-450000: Logger, Logger, -, -, -, -, Detail: pid: Started on Host data/info • <5> %NIC-5-450001: Logger, Logger, -, -, -, -, Detail: pid: Stopped on Host data/info
Issue 120113	RSA enVision now retains changes applied during a bulk modify to the Manage Messages screen.
Issue 120922	You can locate the Service Pack information (in addition to the version information) of the installed enVision software in the following locations: • In the **pi_webserver.log** file, after you restart the NIC Web Server Service. • On the Log In window. Press CTRL+A to display the information. • On the System Performance window
Issue 121091	When you run a query or ad hoc report, the progress bar is now available.
Issue 121271	RSA corrected the issue where the NIC SDEE Collection Service occasionally stopped functioning.
Issue 121647	RSA addressed an issue where restarting the NIC Service Manager Service on a Remote Collector (RC) or a Local Collector (LC) caused the system to stop functioning.
Issue 122456	RSA updated the NIC Asset Processor Service to address issues with the **nCircle** event source (device).
Issue 123420	RSA corrected the issue where the NIC Alerter Service stopped functioning.
Issue 124372	Users can now modify the site or node selection when adding or modifying an ODBC service configuration.

Identifier	Description
MCR-#12 Issue 124272	RSA addressed a potential security issue with saved user query data.
MCR-#21 Issue 124274	The RSA enVision Log On window limits the size of user names to a maximum of 32 characters.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it has been noted.

Discovered in Service Pack 3

The following issues were found during development of Service Pack 3.

Request to update migration documentation

Tracking Number: env-31895
Problem: If you use EMC Centera for offline backup of RSA enVision, when you upgrade enVision from 3.x to 4.0, the **offLineData.ini** file is not updated to point to the correct folder. For example, if you are running RSA enVision 3.5.1, **offLineData.ini** points to **E:\nic\3510**.
Workaround: Manually configure **offLineData.ini** to point to **E:\nic\4000**.

Filter in a correlation rule cannot be given a date later than 01-01-2006

Tracking Number: env-30883
Problem: When adding a filter for a correlated alert, the enVision UI does not allow you to select a date beyond January 1, 2006.
Workaround: None.

Discovered in Service Pack 2

The following issues were found during development of Service Pack 2.

WinSSHD credential cache should be refreshed after upgrade

Tracking Number: 128792 (env-31197 in Jira)
Problem: Service Pack 2 Changes NIC_System Password.
Workaround: Refresh the WinSSHD credential cache by using the WinSSHD Control Panel. For details, see WinSSHD Upgrade on page 5.

Discovered in Service Pack 1

The following issue were found during development of Service Pack 1.

Request to update migration documentation

Tracking Number: 123469
Problem: Instructions are not clear
Workaround: In the chapters “Migrate a Multiple Appliance Site” and “Migrate a Multiple Appliance Site with EA” in the *RSA enVision 4.0 Migration Guide*, the instructions in “Task III. If You Are Using Task Triage at 3.5.1, 3.5.2, or 3.7.0, Correct Alerter Data Before Upgrading to 4.0" does not state that you run the **Updated_Rule-name_Correction.vbs** script only on the A-SRV where the NIC App Server Service is installed

Documentation Errata

This section describes changes to documentation that remain unresolved in this release. This section contains an updated version of the **Ports Used by enVision** topic from the Help.

Note the following changes:

- Added ports used by Windows Time Service
- Added port for TCP syslog event collection
- Corrected destination process for FTP event collection
- Corrected direction for QualysGuard asset collection
- Made multiple corrections to Remote Appliance Management section

Ports Used by enVision

RSA enVision services use certain TCP and UDP ports to communicate with:

- Each other
- The enVision user interfaces
- Event sources (devices) or vulnerability assessment tools
- Other network services

RSA enVision also depends on Windows services that use TCP or UDP ports.

The tables below identify ports used by enVision. In the tables:

- The **Item** column describes the communication that uses TCP or UDP ports. The description may include the protocol, the hosts or processes with which enVision appliances communicate, and the applicable enVision configurations, features, or versions.
- The **Port** column specifies one or more TCP or UDP ports, and the **Direction** column specifies whether the usage is Inbound to and/or Outbound from the enVision appliance. For each **Item**, all of the specified ports are used in all of the specified directions.
- For an enVision deployment with multiple appliances, the **Appliance Type** column identifies the node types that pertain to each **Item**. For a deployment with a single appliance, every **Item** is applicable unless otherwise noted.

Make sure that your network is configured to allow the communications that apply to your deployment.

Ports Used by enVision for User Interfaces

Item	Port	Direction	Appliance Type
JNDI, RMI, and EJB client proxy connections from the NIC Web Server service to the NIC App Server service for VAM browsing in the enVision web UI	TCP 1098 TCP 1099 TCP 3873 TCP 4444	Outbound from any A-SRV Inbound to the A-SRV that runs the NIC App Server service	A-SRV
Connection from Event Explorer to the NIC App Server service for Task Triage and VAM browsing	TCP 1098 TCP 1099 TCP 3873 TCP 4444	Inbound to the A-SRV that runs the NIC App Server service	A-SRV
Connection from the Event Viewer in the enVision Web UI to the NIC Server service	TCP 2010	Inbound	D-SRV
Connection from Event Explorer to the NIC Server service	TCP 2010	Inbound	D-SRV
HTTP Connection from the enVision Web UI to NIC Web Server service	TCP 8080	Inbound	A-SRV

Item	Port	Direction	Appliance Type
HTTP Connection from Event Explorer to the NIC Web Server service	TCP 8080	Inbound	A-SRV
HTTPS Connection from the enVision Web UI to the NIC Web Server service	TCP 8443	Inbound	A-SRV
HTTPS Connection from Event Explorer to the NIC Web Server service	TCP 8443	Inbound	A-SRV

Ports Used for Remote Appliance Management

Item	Port	Direction	Appliance Type
Connection to Internet Information services (part of the appliance OS) to download the Terminal Server ActiveX web client	TCP 80	Inbound	All
HTTP Connection to DRAC	TCP 80*****	Inbound	All Node Types, 60 Series Only
HTTPS Connection to DRAC	TCP 443*	Inbound	All Node Types, 60 Series Only
Connection to Terminal Server (part of the appliance OS) from the ActiveX web client or the full Remote Desktop Connection Client	TCP 3389	Inbound	All
DRAC Desktop Console Redirection (remote desktop capability)	TCP 5900* TCP 5901*	Inbound	All Node Types, 60 Series Only

* Configurable port. See the DRAC 5 User Guide for information on how to change ports and information about other ports that may be used by DRAC.

Ports Used by enVision for Communications Between Services

See also the communication on TCP ports 1098, 1099, 3873, and 4444 from the NIC Web Server service to the NIC App Server service for VAM browsing described under Ports Used by enVision for User Interfaces.

Item	Port	Direction	Appliance Type
FTP File transfer connection from the NIC Forwarder service to forward collected data from the RC to the D-SRV (applies only to deployments with an RC at version lower than 3.5.0 forwarding to a D-SRV at version 3.5.0 or higher)	TCP 20 TCP 21	Outbound from the RC Inbound to the D-SRV	RC, D-SRV
SFTP File transfer connection from the NIC WinSSHD service to forward collected data from the RC to the D-SRV (applies only to deployments with an RC at version 3.5.0 or higher)	TCP 22	Outbound from the RC Inbound to the D-SRV	RC, D-SRV
Windows Time Service connections for time synchronization (deployments with multiple appliances only; connections are from A-SRV or LC to D-SRV within an LS site)	UDP 123	Outbound	A-SRV, LC

Item	Port	Direction	Appliance Type
Connection from the NIC Logger service for collection of internal events from NIC services and from the NIC SFTP agent for Windows (in deployments with multiple appliances, communications from NIC services are to the D-SRV from all appliances within the site; in deployments with an RC, communications from NIC services on the RC are local; NIC SFTP agents communicate to their associated D-SRV or RC)	UDP 600	Outbound from any appliance and from all services and devices with SFTP agents Inbound to D-SRV or RC	All, D-SRV, RC
Connection to the NIC Server service for IPDB (connections across sites are between any two D-SRVs or between any D-SRV and any RC)	TCP 2010	Inbound and Outbound	D-SRV, RC
Connections from the NIC Server service to the NIC Packager service (deployments with multiple appliances only; connections are from the D-SRV to any LC within the site)	TCP 2015	Inbound to the LC Outbound from the D-SRV	LC, D-SRV
Connection from the NIC DB Replication Client service to the NIC DB Replication Server service (deployments with multiple appliances only; within a site, connections are to the D-SRV from any other appliance; in a deployment of multiple sites, connections between sites are from a D-SRV to its master D-SRV)	TCP 2439	Inbound to the D-SRV Outbound from any appliance	D-SRV
Connection to the NIC DB Server service for the configuration database (For enVision versions: 3.5.0 and higher, connections are local only. Lower than 3.5.0, communications include local connections on any appliance, connections within a site to the D-SRV from any other appliance, and connections across sites to a master D-SRV from its slave D-SRV or RC.)	TCP 2638	3.5.0 and higher: Inbound to any appliance Lower than 3.5.0: Inbound to and Outbound from any appliance	All
Connection to the NIC DB Report Server service for the report database (communication is local only)	TCP 3989	Inbound	A-SRV

Ports Used by enVision Services for Communication with Other Network Services and Applications

Item	Port	Direction	Appliance Type
Connection from the NIC Alerter service for SMTP e-mail sent by enVision to an SMTP server	TCP 25	Outbound	A-SRV
Connection from the NIC Server service for DNS resolution (local requests use UDP port 53 on the appliance; remote requests use UDP port 53 on the remote DNS server)	UDP 53	Outbound and Inbound	D-SRV, RC
Connection from Windows Time Service to an NTP server for time synchronization	UDP 123	Outbound	D-SRV, RC
Connection from the NIC Alerter service for SNMP traps sent by enVision to a trap receiver	UDP 162	Outbound	A-SRV
Connection from enVision for integration with LDAP servers	TCP 389 TCP 636	Outbound	A-SRV

Item	Port	Direction	Appliance Type
Connection from the NIC Alerter service for SNPP alerts sent by enVision to a paging server	TCP 444	Outbound	A-SRV
Connection from the NIC Alerter service for Syslog messages sent by enVision to a remote syslog server	UDP 514 (this is the default; you can use output action configuration to change this port)	Outbound	A-SRV
Connection from the NIC Alerter service for AIM alerts sent by enVision (authentication uses TCP port 29999 at login.oscar.aol.com; messaging uses TCP port 5190 at toc.oscar.aol.com)	TCP 5190 TCP 29999	Outbound	A-SRV
HTTPS connection from external application such as external ticketing system to NIC App Server to update tasks.	TCP 8086	Outbound from external application Inbound to the A-SRV where the NIC App Server service runs	A-SRV

Ports Used for Event Collection

Item	Port	Direction	Appliance Type
Connection to IIS for FTP sent to enVision (for example, from devices with a UNIX FTP client script)	TCP 20 TCP 21	Inbound	LC, RC
Connection to NIC WinSSHD service for Secure FTP sent to enVision (for example, from devices with the Windows SFTP client or a UNIX SFTP client script)	TCP 22	Inbound	LC, RC
Connection to NIC Trapd service for SNMP traps sent to enVision	UDP 162	Inbound	LC, RC
Connection to NIC Collector service for Syslog sent to enVision	UDP 514	Inbound	LC, RC
Connection to NIC Collector service for Syslog sent to enVision	Configurable TCP port	Inbound	LC, RC
Connection to NIC ODBC service for ODBC event collection (the ports listed are the defaults; ports may be customized on your devices)	TCP 1109 (ActivIdentity) TCP 1433 (ISS SiteProtector, McAfee ePolicy Orchestrator, Microsoft SQL Server) TCP 1521 (Oracle Database)	Outbound	LC, RC

Ports Used for Event Collection, Using Device-Specific Services

Item	Port	Direction	Appliance Type
Connection from NIC Windows service for Windows data collection	TCP 135 TCP 139 TCP 445 dynamic RPC ports	Outbound	LC, RC
Connection from NIC SDEE Collection service for Cisco Secure IDS data collection	TCP 443	Outbound	LC, RC
Connection from NIC FW-1 LEA Client service for Check Point FireWall-1, VPN-l, Provider-1, and SmartDefense data collection	TCP 18184	Outbound	LC, RC
Connection from NIC FW-1 LEA Client service for Check Point FireWall-1, VPN-l, Provider-1, and SmartDefense used to exchange certificates when using authentication type requiring a pull, such as sslca	TCP 18210 TCP 18211	Outbound	LC, RC

Ports Used for Asset Data Collection by NIC Vulnerability Service (Deprecated)

Item	Port	Direction	Appliance Type
Connection to the NIC Vulnerability service for nCircle IP360 data collection. This vulnerability service is deprecated. Please use the Asset Collector Service.	TCP 22	Inbound	D-SRV
Connection from the NIC Vulnerability service for QualysGuard data collection. This vulnerability service is deprecated. Please use the Asset Collector Service.	TCP 443	Outbound	D-SRV

Ports Used for Asset Data Collection by VAM (Vulnerability and Asset Management) Services

Item	Port	Direction	Appliance Type
Connection to the Asset Collector service for Nessus and/or nCircle IP360 data collection	TCP 22	Inbound	LC
Connection from the Asset Collector service for QualysGuard data collection	TCP 443	Outbound	LC
Connection from the Asset Collector service for McAfee Foundscan and/or ISS Site Protector data collection	TCP 1433	Outbound	LC

Ports Used by Windows Services Required by enVision

Item	Port	Direction	Appliance Type
Connection to the Local Security Authentication Server	TCP 88	Inbound	All
Connection to the Local Security Authentication Server	Dynamic RPC ports	Inbound	All
Connection to NT File Replication services	Dynamic RPC ports	Inbound	All

Getting 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

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.