Smart Business Architecture
Borderless Networks for Enterprise Organizations

RSA Security Information and Event Management (SIEM)
Deployment Guide

Revision: H1CY10
Table Of Contents

Cisco Smart Business Architecture Borderless Networks for Enterprise .................. 5

Business Benefits ................................................................. 5

  Enhanced Security and Risk Management
  Simplifying Compliance
  Optimizing IT and Network Operations.

RSA enVision Product Overview .................................................. 6

Deploying RSA enVision ............................................................... 7

  Cisco Adaptive Security Appliance Configuration Instructions
  Cisco Secure IDS/IPS Configuration Instructions
  Cisco IronPort Email Security Appliance Configuration Instructions
  Cisco IronPort Web Security Appliance Configuration Instructions
  Cisco MARS Configuration Instructions
  Configure Cisco MARS for File Reader Service to Collect Raw Message Logs
This document is for the reader who:

• Has read the Cisco Security Information and Event Management and Borderless Networks Enterprise Deployment Guide
• Wants to connect Borderless Networks to an RSA SIEM solution
• Wants to gain a general understanding of the RSA SIEM solution
• Has a level of understanding equivalent to a CCNA certification
• Wants to solve compliance and regulatory reporting problems
• Wants to enhanced network security and operations
• Wants to improve IT operational efficiency
• Wants the assurance of a validated solution
Cisco Smart Business Architecture
Borderless Networks for Enterprise

The Cisco Smart Business Architecture for Enterprise offers partners and customers valuable network design and deployment best practices; helping organizations deliver superior end-user experiences that include switching, routing, security, and wireless technologies combined with the comprehensive management capabilities for the entire system. Customers can use the guidance provided in the architecture and deployment guides to maximize their Cisco network’s value in a simple, fast, affordable, scalable, and flexible manner.

Cisco offers a number of options to provide Security Management capabilities. This guide is focused on our partnership with RSA and their products that meet Cisco’s goal to deliver affordable, easy-to-use security information and an event management (SIEM) solution.

The modular design of the architecture means that technologies can be added when the organization is ready to deploy them. It also provides configurations and topologies tested by Cisco that CCNA®-level engineers can use for design and installation, and to support organizational needs.

Figure 1. RSA enVision
RSA SIEM Deployment Guide

Business Benefits
The RSA enVision platform collects event logs generated by Cisco’s Network and Security Infrastructure, permanently archives copies of the data, processes the Cisco logs in real-time, and generates alerts when it observes suspicious patterns of behavior. Security and IT administrators can interrogate the full volume of stored data through an intuitive dashboard, and advanced analytical software turns the complex, unstructured mass of raw data into structured information, giving administrators actionable insights to help them in three main areas:

Enhancing Security and Risk Mitigation
With real-time security event alerts, monitoring, and drill-down forensic functionality, the platform gives administrators a clear view of important information. Because they can see and understand the threats and risks, they can take more effective actions to mitigate those risks.

Simplifying Compliance
Administrators can automatically collect log data about the Cisco network and security infrastructure, file, application, and user activity that can significantly help simplify the compliance process. Over 1100 included reports are tailored to today’s specific compliance requirements. The solution simplifies compliance with whatever legislation emerges in years to come, because it stores all log data without filtration or normalization and protects it from tampering, providing a verifiably authentic source of archived data.

Optimizing IT and Network Operations
Managed log data is the best source of information about infrastructure performance and user behavior. IT support staff can utilize the RSA enVision platform to track and manage activity logs for servers, networking equipment, and storage platforms, as well as monitor network assets, the availability and status of people, hardware, and business applications. It provides an intelligent forensic tool for troubleshooting infrastructure problems and protecting infrastructure resources, and it assists IT managers in help desk operations and provides granular visibility into specific behaviors by end users.

RSA enVision Product Overview
RSA enVision™ is a feature-rich compliance and security application. It allows you to capture and analyze log information automatically from your network, security, application, operating, and storage environments. The enVision LogSmart™ Internet Protocol Database (IPDB) provides the architecture to collect and protect all the data automatically, from any network device, without filtering or agents. It gives you an accurate picture of how your network is being used, and by whom. It independently monitors your network to verify security policies, to generate alerts for possible compliance breaches, and to analyze and report on network performance.

enVision is tightly coupled with its underlying appliance operating system and hardware, and together they comprise a highly scalable platform that provides guaranteed levels of performance.

RSA enVision™ Platform Architecture

[Diagram of RSA enVision™ Platform Architecture]

Universal Device Support

Agentless Collection

Compressed Original Logs

Index & Meta Data

LogSmart™ IPDB

Intelligent Event & Payload Inspection

Advanced Correlation & Alerting

Reporting Engine

Automatic Baselines

Forensics

Incident Management & Analysis

Notification & Reporting

Action

Devices

Collect

Manage

Analyze

All Data

Compressed Original Logs

Index & Meta Data

LogSmart™ IPDB

Intelligent Event & Payload Inspection

Advanced Correlation & Alerting

Reporting Engine

Automatic Baselines

Forensics

Incident Management & Analysis

Notification & Reporting

Action
RSA enVision is made up of three components:

- **Application**: supports interactive users and runs the suite of analysis tools.
- **Collector**: captures incoming events.
- **Database**: manages access and retrieval of captured events.

The enVision ES series appliances are designed to operate in a standalone, nondistributed mode. They have all three enVision components—Application, Collector, and Database—installed on one appliance. The single appliance is a site. Some single-appliance sites have an external storage system.

A range of appliances are available; all are based on the same hardware with licensing to suit specific requirements. To choose the most appropriate, look at the number of network devices to be monitored and the number of events per second to process.

<table>
<thead>
<tr>
<th></th>
<th>ES 560</th>
<th>ES1060</th>
<th>ES1260</th>
<th>ES2560</th>
<th>ES3060</th>
<th>ES5060</th>
<th>ES7560</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Users</td>
<td>6</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>(Admin)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Events Per</td>
<td>500</td>
<td>1000</td>
<td>1200</td>
<td>2500</td>
<td>3000</td>
<td>5000</td>
<td>7500</td>
</tr>
<tr>
<td>Second</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


### Deploying RSA enVision

**Step 1: Setting Up RSA enVision**

The configuration process takes approximately 30 minutes to complete. You cannot change any of the site configuration options after the wizard is finished. The configuration tasks for a single-appliance site are as follows:

<table>
<thead>
<tr>
<th>Task</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Plan the installation according to the enVision Configuration Wizard Planning Worksheet—Single Appliance Site.</td>
</tr>
<tr>
<td>2</td>
<td>Set up the RSA enVision appliance hardware.</td>
</tr>
<tr>
<td>3</td>
<td>Connect to the appliance using a KVM switch. (You can also connect remotely using DRAC instead of using a local KVM. See Appendix B “Dell Remote Access Controller Utility.”) The Configuration Wizard starts automatically.</td>
</tr>
</tbody>
</table>
| 4    | Complete the enVision Configuration Wizard.  
**NOTE**: enVision uses the default IP address 192.168.1.55. IP address conflicts can occur if the LAN cable is connected to an existing network when you run the configuration wizard. For this reason, you should verify the LAN cable is not connected to an existing network or confirm the IP address is not being used before you run the configuration wizard. 
If you click **Cancel** at any time while using the wizard, you must restart the wizard to configure your site. To restart the wizard, double-click the lsconfigurationwizard.exe file in the c:\windows\installations directory.  
When the wizard displays the Review Page window, verify that everything is correct on the Review Page. Click **Finish**. (If the Review page is not correct, click **Cancel** and check your hardware setup.)  
In the last step, the wizard displays the enVision Configuration Wizard Log window. The log displays the steps the system is performing to configure the site. The system restarts several times while completing the setup. The appliances restart automatically when the site configuration process is complete. |
| 5    | Immediately after you configure RSA enVision 4.0, RSA strongly recommends that you download and install two Content Updates: Event Source Update Package and VAM & Signature Content Update Package.  
Go to RSA SecurCareOnline [https://knowledge.rsasecurity.com](https://knowledge.rsasecurity.com). Click on **Products**. Under RSA enVision click **Content Updates**. Complete the instructions available on that page to download and install the updates. |
| 6    | Apply the license keys that were sent via email to the contact provided when you ordered the enVision appliance. |
Step 2: Adding Cisco devices in RSA enVision to receive logs

RSA enVision collects, analyzes, and stores logs from event sources throughout an organization’s IT environment. The logs and the descriptive metadata that enVision adds are stored in the LogSmart Internet Protocol Database (IPDB).

Event sources are the IP assets on the network, such as servers, switches, routers, storage arrays, operating systems, and firewalls.

The enVision administrator configures event sources to send their logs to the Collector or configures the Collector to poll event sources and retrieve their logs. As a result, the Collector receives all system logs in their original form, without filtering, normalization, or compression.

Cisco Adaptive Security Appliance Configuration Instructions

Cisco ASA generates ASA syslog events. It also generates IDS events by Cisco ASA Security Services Module.

To configure Cisco ASA to generate syslog events:
1. Connect to the ASA box via telnet or SSH.
2. Enter the enable mode by typing the following command:
   enable
3. Enter the configure mode by typing the following command:
   config terminal
4. Type the following lines:
   no logging timestamp
   logging trap debugging
   logging host inside 10.4.200.115
   (where 10.4.200.115 is enVision’s IP address)
5. Press Ctrl + Z to exit config mode.
6. Type the following command to save the configuration changes:
   copy running-config startup-config

To configure enVision to enable SDEE for ASA IPS AIP-SSM Events:
1. Log in to enVision.
2. Depending on your enVision version, do one of the following:
   - If you are using an enVision version prior to 4.0, Click Overview > System Configuration > Services > Device Services > Manage Secure IDS (XML) Service
   - If you are using enVision version 4.0 or newer, Click Overview > System Configuration > Services > Device Services > Manage SDEE Service
   enVision displays the Manage Secure IDS (XML) Service or Manage Secure SDEE Service window.
3. Perform one of the following actions:
   - Click Add to add an IDS server.
   - Click the IP Address of the server to modify an IDS server.

The system displays the Add/Modify Secure IDS (XML) Server window.
4. Complete the window as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Host-ip value of the Cisco ASA SSM.</td>
</tr>
<tr>
<td>Username</td>
<td>User account on the Cisco ASA SSM with administrative privileges.</td>
</tr>
<tr>
<td>Password</td>
<td>Password to the user account with administrative privileges.</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Password to the user account with administrative privileges.</td>
</tr>
</tbody>
</table>

5. Click **Apply**.
   The system saves the information and displays the Manage Secure IDS (XML) Service window.

6. Click **Start Service** (or **Restart Service**).

7. Click **Apply**.

**Cisco Secure IDS/IPS Configuration Instructions**

**NOTE:** Cisco IDS/IPS version 7.0 is supported in the latest enVision 4.0 only.

**To set up Cisco Secure IDS/IPS to work with enVision:**

1. **(SKIP this step if you are using enVision version 4.0 or newer.)** Starting in version 6.1, RDEP is disabled by default (it was replaced with SDEE starting in IDS/IPS 5.0/IPS 5.1). You must enable the RDEP event server on the sensor to allow enVision event collection. Complete the following task on the Cisco Secure IDS/IPS event source.
   a. Access the Cisco IDS/IPS console and log on using administrative credentials.
   b. Type the following commands:
      ```
      configure terminal
      service web-server
      configurable-service rdep-event-server
      enabled true
      ```
   c. Exit the configuration mode, confirming to save changes when prompted.

2. You must apply access-list to the sensor to allow enVision access to the sensor. Complete the following task on the Cisco Secure IDS/IPS event source.
   a. Access the Cisco IDS/IPS console and log on using administrative credentials.
   b. Type the following commands:
      ```
      configure terminal
      service host
      network-settings
      ```
   c. Configure the access-list to allow enVision host or the network that hosts enVision to access the sensor. Here are some examples:
      ```
      access-list 10.4.200.0/24 (to allow a network)
      access-list 10.4.200.66 (to allow a host)
      ```
   d. Exit the configuration mode, confirming to save changes when prompted.

3. Set up the NIC SDEE Service (prior to enVision 4.0 known as Secure IDS/IPS XML Service) in enVision. See the enVision online Help for instructions on how to set up this service.

**NOTE:** enVision uses the TCP port 443 (open outbound) to obtain information from this device.
**Cisco IronPort Email Security Appliance Configuration Instructions**

You must complete these tasks to configure Cisco IronPort Email Security Appliance:

I. Configure Cisco IronPort ESA  
II. Configure RSA enVision

**Configure Cisco IronPort Email Security Appliance**

**To configure Cisco IronPort ESA:**

1. Log on to the IronPort web interface.
2. To edit the settings of the Authentication Logs subscription, follow these steps:
   a. From the top menu, click **System Administration > Log Subscriptions**.
   b. In the Log Subscriptions window, click **authentication** to view the Authentication Logs subscription.
   c. In the **Retrieval Method** section of the Edit Log Subscription window, select **SCP on Remote Server**.
   d. Under **SCP on Remote Server**, complete the fields as follows.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Time Interval Between Transferring</td>
<td>Type 180.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Select SSH2.</td>
</tr>
<tr>
<td>SCP Host</td>
<td>Enter the IP address of your enVision system.</td>
</tr>
<tr>
<td>Directory</td>
<td>Type CISCO_IRONPORT_ESA_ironport-IP-address where ironport-ip-address is the IP address of Cisco IronPort ESA.</td>
</tr>
<tr>
<td>Username</td>
<td>Type nic_sshd.</td>
</tr>
</tbody>
</table>

   e. Click **Submit**.  
      An SSH key is generated.

   f. Copy the generated SSH key to a new text file, and save the text file as **id_rsa.pub**.  
      **NOTE:** The entire SSH key must be on a single line and cannot include any spaces. If necessary, remove spaces.

3. To edit the settings of the IronPort Text Mail Logs subscription, follow these steps:
   a. From the top menu, click **System Administration > Log Subscriptions**.
   b. In the Log Subscriptions window, click **mail_logs** to view the IronPort Text Mail Logs subscription.
   c. In the **Retrieval Method** section of the Edit Log Subscription window, select **SCP on Remote Server**.
   d. Under **SCP on Remote Server**, complete the fields as described in Step 2.
   e. Click **Submit**.  
      **NOTE:** The same SSH key as in Step 2 is generated. You can ignore this SSH key.

4. To edit the settings of the CLI Audit Logs subscription, follow these steps:
   a. From the top menu, click **System Administration > Log Subscriptions**.
   b. In the Log Subscriptions window, click **cli_logs** to view the CLI Audit Logs subscription.
   c. In the **Retrieval Method** section of the Edit Log Subscription window, select **SCP on Remote Server**.
   d. Under **SCP on Remote Server**, complete the fields as described in Step 2.
   e. Click **Submit**.  
      **NOTE:** The same SSH key as in Step 2 is generated. You can ignore this SSH key.

5. Click **Commit Changes** to save all log settings.

6. In the Uncommitted Changes window, click **Commit Changes** to apply all log settings.
Configure RSA enVision

To configure enVision to collect Cisco IronPort ESA messages:

1. In enVision, add the Cisco IronPort ESA event source to the NIC File Reader Service, and start the NIC File Reader Service. For instructions, see the enVision Help topic “Set Up the NIC File Reader Service.”

2. Copy the `id_rsa.pub` file that you saved to the `envision\bin` folder on your enVision system.

3. On your enVision system, open a command prompt and change directories to `envision\bin`.

4. To install the public key on enVision, type:
   ```
   add_winsshd_key.bat id_rsa.pub
   ```

Cisco IronPort Web Security Appliance (WSA) Configuration Instructions

To configure IronPort WSA, you must complete these tasks:

I. Configure IronPort WSA
   NOTE: All logs are optional, however, enVision parses only the logs that are configured as follows.

II. Set up the NIC File Reader Service

III. Configure enVision to collect IronPort WSA messages

Configure IronPort WSA

To configure Cisco IronPort WSA:

1. Log on to the IronPort web interface.

2. Select System Administration > Log Subscriptions.

3. To configure Access Logs, complete these tasks:
   a. Select Access Logs and use the following settings.
      - Log Style = Apache
      - Custom Fields = %k %p %u %XF
      - Retrieval Method = SCP on Remote Server
      - Max Time Interval = 180
      - Protocol = SSH2
      - SCP Host = IP Address of enVision device
      - Directory = `CISCO_IRONPORT_WSA_ironport-IP-address`, where `ironport-IP-address` is the actual IP address of the device, for example, `CISCO_IRONPORT_WSA_1.2.3.4`
      - Username = nic_sshd
   b. Click Submit.
   c. Copy the generated SSH Key to a new text file. Save the text file as `id_rsa.pub`.

   NOTE: The entire key must be on a single line. Also, remove any spaces from the key.
4. To configure W3C Logs, complete these tasks:
   a. Select **W3C Logs** and use the following settings:
      NOTE: The Selected Log Fields must be in this exact order.
      - **Selected Log Fields** = timestamp, x-elapsed-time, c-ip, s-ip, s-port, x-resultcode-httpstatus, sc-bytes, cs-method, cs-url, cs-username, x-hierarchy-origin, cs-mime-type, x-acltag, x-result-code, cs(User Agent), x-webcat-code-full
      - **Retrieval Method** = SCP on Remote Server
      - **Max Time Interval** = 180
      - **Protocol** = SSH2
      - **SCP Host** = IP Address of enVision device
      - **Directory** = CISCO_IRONPORT_WSA_ironport-IP-address, where ironport-IP-address is the actual IP address of the device, for example, CISCO_IRONPORT_WSA_1.2.3.4
      - **Username** = nic_sshd
   b. Click **Submit**. The generated SSH Key will be identical to the one initially generated.
      NOTE: IronPort creates the same SSH Key for all log subscriptions. The key only needs to be saved the first time.

5. To configure CLI Audit Logs, complete these tasks:
   a. Select **CLI Audit Logs** and use the following settings:
      - **Retrieval Method** = SCP on Remote Server
      - **Max Time Interval** = 180
      - **Protocol** = SSH2
      - **SCP Host** = enVision_IP_address
      - **Directory** = CISCO_IRONPORT_WSA_ironport-IP-address
      - **Username** = nic_sshd
   b. Click **Submit**.

6. To configure IDS Data Loss Logs, complete these tasks:
   a. Select **IDS Data Loss Logs** and use the following settings:
      - **Retrieval Method** = SCP on Remote Server
      - **Max Time Interval** = 180
      - **Protocol** = SSH2
      - **SCP Host** = enVision_IP_address
      - **Directory** = CISCO_IRONPORT_WSA_ironport-IP-address
      - **Username** = nic_sshd
   b. Click **Submit**.

7. Click **Commit Changes**.
8. Click **Commit Changes**.

**Set up the NIC File Reader Service**
Set up the NIC File Reader Service for the device. See Set Up File Reader Service topic in the RSA enVision Online Help for complete instructions.

To configure enVision to receive IronPort WSA log files:
1. Log on to RSA enVision.
2. Click **Overview > System Configuration > Services > Device Services > Manage File Reader Service**.
3. Click Add.
4. To complete the Add/Modify File Reader Device window, select IronPort from the File reader type drop-down list.
5. In the Site/Node: field, note the site/node from which you are collecting.
6. Click Apply.
7. To have RSA enVision recognize the configuration change:
   - On a single-appliance site, enVision starts the NIC File Reader Service recognizing the configuration change immediately so no action is necessary.
   - On a multiple-appliance site, complete the following:
     a. Wait 3 minutes.
     b. Go to the Overview > System Configuration > Services > Manage Services window.
     c. Select Start/Stop Service to stop the NIC Reader Service on the site/node you noted in Step 5.
     d. Click Apply.
     e. Click Refresh until the Status column shows the site/node is stopped.
     f. Select Start/Stop Service to start the NIC File Reader Service on the site/node you noted in Step 5.
     g. Click Apply.
     h. Click Refresh until the Status column shows the site/node is running.

Configure enVision to collect IronPort messages
1. In enVision, set up the NIC File Reader service for the device.
2. Add the device to the NIC File Reader service.
3. Start the NIC File Reader service. See the enVision Help for instructions.
4. Copy the id_rsa.pub file (from Step 5 above) to the envision\bin folder on your enVision system.
5. Open a command prompt on your enVision system.
6. Change to the envision\bin folder and run the following command:
   add_winsshd_key.bat id_rsa.pub

Cisco MARS Configuration Instructions

Important: For Cisco MARS, you can set up one of two collection methods, the originally supported Syslog collection and the newly added File Reader Service to collect raw message logs. The collection methods function differently. The Syslog collection method collects Cisco MARS log messages. The File Reader Service collects the logs of the event sources which Cisco MARS is reporting on.

To configure Cisco MARS, you must complete these tasks:
I. Configure Cisco MARS to send logs to RSA enVision for syslog collection
II. Set up the NIC File Reader Service
III. Create a Windows user account
IV. Create an SFTP user account
V. Configure Cisco MARS for File Reader Service to collect raw message logs

Set Up the NIC File Reader Service
Set up the NIC File Reader Service for the event source. For complete instructions, see the RSA enVision Help topic “Set Up File Reader Service.”

To configure RSA enVision to receive Cisco MARS log files:
1. Log on to enVision.
2. Click Overview > System Configuration > Services > Device Services > Manage File Reader Service.
3. Click **Add**.
4. Make a note of the value in the **Site/Node** field. This is the site/node from which you are collecting.
5. Enter the IP address of your Cisco MARS appliance.
6. To complete the Add/Modify File Reader Device window, from the **File reader type** drop-down list, select **CiscoMars_Syslog**.
   
   **NOTE:** The “Cisco Mars_Syslog” file reader type option is available only if you have installed the March 2010 Event Source Update.
7. Click **Apply**.
   On a single appliance site, enVision restarts the NIC File Reader Service, recognizing the configuration change immediately so no action is necessary.
8. On a multiple appliance site, to restart the NIC File Reader Service, follow these steps:
   a. Wait three minutes.
   b. Click **Overview > System Configuration > Services > Manage Services**.
   c. Select **Start/Stop Service** to stop the NIC File Reader Service on the site/node that you noted in Step 4.
   d. Click **Apply**.
   e. Click **Refresh** until the Status column shows that the site/node is stopped.
   f. Select **Start/Stop Service** to start the NIC File Reader Service on the site/node that you noted in Step 4.
   g. Click **Apply**.
   h. Click **Refresh** until the Status column shows that the site/node is running.

### Create a Windows User Account

#### To create a Windows user account:
1. Click **Start > Administrative Tools > Active Directory Users and Computers**.
2. Right click **Users**, and select **New > User**.
3. In the New Object – User window, complete the fields using **ciscomars** as the user log on name.
4. Click **Next**.
5. Enter your password for the account and click **Next**.

**NOTE:** Make a note of this password as you will need this password again at a later step.

### Create an SFTP User Account

#### To create an SFTP user account:
1. Click **Start > Administrative Tools > WinSSHD Control Panel**.
2. On the **Server** tab, click **Edit Settings**.
3. Click **Configuration > Access Control > Windows Accounts**.
4. Select the **nic_sshd** account and click **Copy**.
5. Change the Windows account name to the user account that you created in Active Directory Users and Computers, and complete the fields as follows:
   a. Ensure that **Password authentication** is set to **Allowed**.
   b. Ensure that **Public key authentication** is set to **Disabled**.
   c. Ensure that **Permit SCP** is set to **No**.
   d. Ensure that **Permit SFTP** is set to **Yes**.
6. Click **OK**.
7. Click **OK** to commit the changes, and close the WinSSHD Settings window.

### Configure Cisco MARS for File Reader Service to Collect Raw Message Logs

**NOTE:** To configure Cisco MARS for File Reader Service to collect raw message logs, you must obtain RSA enVision 4.0 Service Pack 3, bug fix (EBF) ENV-32744.

#### To collect raw message logs on Cisco MARS:
1. Log on to your Cisco MARS appliance.
2. Under the Device Configuration and Discovery Information section, click **Admin > System Maintenance > Data Archiving**, and complete the fields as follows.
   a. In the **Archiving Protocol** field, select **SFTP**.
   b. In the **Remote Host IP** field, enter the IP address of your enVision appliance.
   c. In the **Remote Path** field, type `/CiscoMars_Syslog_IP address of Cisco MARS`
   d. In the **Remote Storage Capacity in Days** field, leave the default as 10 days.
   e. In the **Username** field, enter the user name that you created for the SFTP account on enVision.
   f. In the **Password** field, enter the password that you created for the SFTP account on enVision.
RSA SIEM Deployment Guide

3. Click **Apply**.
4. Click **Activate**.
   
   **NOTE:** The Activate button remains red until it is clicked.
5. Click **Close** to close the Activating Changes window.

**Step 3: Reporting on RSA Envision**

RSA enVision provides 100+ standard reports that gather common network security and traffic analysis statistics into tables and graphs. Administrators can copy and modify these reports or create custom reports to meet specific reporting needs. Administrators and users with the appropriate permissions can create, manage, and run both scheduled and unscheduled reports. Optionally, a report can run once on a specified day or run repeatedly at specified times. RSA enVision can email generated reports to departments and people who need them such as IT, human resources, the CIO office, compliance officers, and managers. RSA enVision provides reports for security, host, network, storage, and other devices. RSA enVision also provides a number of report packages to satisfy compliance needs such as Sarbanes-Oxley Act (SOX) and Health Insurance Portability and Accountability Act (HIPAA).

An enVision report consists of a single graph or a single table. For some purposes, a user may need more data than can be included in a single graph or table. RSA enVision can group multiple reports together so they run at the same time. The following figure shows examples of a graphical report and a tabular report.

Queries are similar to reports except that queries are unplanned only. They generally execute faster, as they are intended to deal with smaller amounts of data than reports. A query returns only tabular data. Analysts might use queries in forensic analysis, for example to drill quickly into an alert or other condition discovered in RSA enVision Event Explorer or to audit some past event. Queries help users and administrators retrieve and examine any data collected by enVision. Query results can be based on IP addresses, dates and times, event message types, and other criteria. Users can generate a query in response to an alert condition appearing in Event Explorer.

Queries use SQL syntax to construct statements for accessing database tables for conditions and events including:

- General traffic flows and events that were allowed
- Accesses that were denied or prevented from happening based on policy
- Status and health parameters
- URL information indicating where users have visited

Users can compose simple or complex queries:

- A simple query is a single logical statement (a single row in the Edit query table).
- A complex query consists of multiple statements (multiple rows in the Edit query table) logically joined using AND or OR. Multiple statements can narrow a query or extract a more accurate set of results for given criteria.
Step 4: Maintaining RSA enVision

RSA enVision Event Source Update provides you with updates to event source content outside the normal enVision product release cycle. Each monthly update package contains multiple patches that contain the latest event sources (new event sources and changes to existing event sources) supported by enVision. Every new or updated event source in the package has its own patch.

The Event Source Update package also includes a recent VAM & Signature Content Update. If you install the VAM updates regularly, the versions of some VAM sources included with the Event Source Update may be older than ones already on your system. If so, the Event Source Update will not overwrite your newer files.

Packages are not linked to a particular enVision version so you can run an update patch if you have enVision version 3.5.1 or higher. The current package is cumulative, containing patches for all new or changed event source XML since 3.5.1.

NOTE: To use the correlation rules in the package, you must be running version 3.7.0 or higher. Additionally, some versions of supported event sources require enVision versions newer than 3.5.1.

You can rollback the installation of the package to its pre-update state if necessary. Please contact RSA Customer Support for guidance before you attempt this procedure.

Step 5: Common Troubleshooting Tips

You can monitor the system health of enVision using the system health features to:

- Report on usage patterns in enVision: The NIC view, NIC_View, allows you to monitor the system health—alerting you of possible issues within the enVision software environment. Track configuration changes in enVision using Audit Reports.

The following standard system reports for the system auditing function are included:

Configuration Changes by Action: Lists all the configuration changes with the specified
Configuration Changes by Date/Time: Lists all configuration changes made to the enVision system.
Configuration Changes by Object Type: Lists all configuration changes made against the specified object
Configuration Changes by User: Lists all configuration changes made by the specified user.

User Session Activity by Date/Time: Lists all the successful and failed log in/log out attempts to enVision.
User Session Activity by User: Lists all the successful and failed log in/log out attempts to enVision the specified user.

Step 6: Procedure to handle an incident on RSA enVision

An incident is an event or set of events that warrants further investigation, such as a disk failure, an unexpected spike in network traffic, or the signature of a known threat. Because of the wealth of data that the RSA enVision platform automatically collects, it can be configured to recognize incidents and issue real-time alerts. The alert is the beginning of the enVision incident-management process.

RSA enVision provides for closed-loop incident management, from configuring alerts, through creating and assigning response tasks, to monitoring incident response and resolution.

Real-Time Alerts

RSA enVision generates real-time alerts in response to sets of circumstances that the administrator has specified. RSA enVision analyzes all incoming events, and issues an alert immediately when the specified conditions are met. The alert is reported in the enVision GUI and can be directed to other destinations, such as email, instant message, or a text file stored on the local system. An alert can also be configured to automatically generate an incident-response task.

Incident-Response Tasks

RSA enVision can group events into tasks for the purpose of investigation, and assign the tasks to analysts (or to an intermediate dispatcher) for response. Analysts display and work with the tasks in RSA enVision Event Explorer. Managers and administrators can monitor the analysts’ progress in the enVision GUI.
RSA SIEM Deployment Guide

Monitoring Alerts by Creating Tasks
In enVision, the administrator can specify the creation of a task based on a correlated alert. When the alert fires, enVision creates the task and sends it to Event Explorer for resolution or to an external application, such as a third-party ticketing system.

Managing Tasks in RSA enVision Event Explorer
When enVision forwards tasks to Event Explorer, Event Explorer displays a list of tasks and the details of individual tasks.

Depending on the Event Explorer user’s permissions (as set by the enVision administrator), the user assigned to a task can acknowledge the task, view and edit task data, assign the task to another analyst, and close or delete the task. The user can also escalate the task an external application, such as a ticketing system. The external application can update tasks and send the updates back to Event Explorer.

Multiple users can access the same task from different Event Explorer clients. Event Explorer displays a warning message if different users attempt to make conflicting changes to the task.

Administrators can monitor the status of tasks in the enVision GUI. RSA enVision version v4.0 SP 2 Build 0288 validated across Smart Business Architecture with Cisco products ASA 8.2(1), IPS AIP-SSM 7.0.(2)E3, ESA 7.1, WSA 6.3, and CS-MARS (6.0.5).

NOTE: If you used the 30-day trial version of the enVision for setting up your network, be sure to convert them to full a license before the end of the 30-day evaluation period. All settings will be maintained in the conversion from the 30-day trial to the full license.

How to Contact Us
End Users
- Please contact RSA, the security division of EMC via https://www.rsa.com/go/contactsales.asp for any questions
- Submit an inquiry about enVision and the Cisco Smart Business Architecture Borderless Networks for Enterprise

Resellers
- Please contact RSA, the security division of EMC via https://www.rsa.com/go/contactsales.asp for any questions
- For more information on how to become a RSA reseller, please visit the Partner Section of our website
Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.