Release Notes
SecureVue® v3.6.6.0.28
Released on Date 11/15/2013

EiQ Networks, Inc. •31 Nagog Park •Acton, MA 01720 •t. +1 978.266.9933 •f. +1 978.266.0004 •www.eiqnetworks.com

Table of Contents

1.0 What's New in SecureVue v3.6.6

The following features have been added in SecureVue v3.6.6 over v3.6.5:

Functional Area	Description
Product Configurability	Feature driven configurations are provided with SecureVue. Premium Configurations: Comprehensive solutions offered by EiQ. User has to purchase these configurations for enabling functionality. 1. Enterprise 2. LogSIEM 3. ThreatVue 4. ComplianceVue Free Configurations: Point Solutions offered by EiQ. User can evaluate functionality free of cost for 25 nodes. 1. FIMVue 2. USBVue 3. DiscoveryVue 4. LogVue 5. EventVue 6. VulnerabilityVue 7. FlowVue 8. PerformanceVue Configurations can be managed (Add, Delete, Enable, Disable) from Administration > Configurations and Licenses > Configurations. See Premium and Free Configurations for a summary on each configuration.
Simplified Installation	1. Express and Custom Modes are provided in the Central installer. No user inputs are required in the Express mode. 2. Central installation has the provision to automatically install the local Data Collector (or DC). Also, each Data Collector has to be associated with a Network Name – a Name to which the DC belongs to (the default local data collector will have a network name of 'Local Network').
Nodes	'Node Discovery' option is provided to the user for discovering and managing nodes.
Alerts Notification	Alert supporting evidence where Subject is per notification and a notification can be set for multiple alert policies. In order to have a clear identification, subject line is prefixed with Alert name.
Analysis of Threat Control Evaluation	Ability to alert/report/forensics on ThreatVue Control Status. Support for alerts, reports, forensics on the ThreatVue controls and

Results	their evaluated results.
Alerts Table of Contents	Table of Content for Alerts is provided on pre-defined set of fields which will be used for further filtering in Alert Archives. This is available at 2 levels 1. *Global Level* (TOC at Alerts Portal): Provides the count of events which are contributed to trigger all the alerts. 2. *Alert Level* (TOC on Alert Archives): Provides the count of events which are contributed to trigger a specific alert.
Administration > Preferences > User Sessions	Option is provided in SecureVue using which user can limit Concurrent sessions for a SecureVue user account (login at same time w/ same user name)
Administration > Preferences > General	'Configured Node limit per Data Collector' option is provided in General Preferences using which user can limit number of nodes configured to a Data Collector.
Administration > Nodes > Configure > Manage White/Black list	Introduced concept of "whitelist" or "blacklist" in SV3.6.6 for allowed or disallowed entities which can be used in ThreatVue Control evaluation.
Password Strength Meter	Password Strength Meter has been provided to evaluate the strength of password as the characters are entered in the password field.
ThreatVue UI	1. Controls implemented in SecureVue are mapped to SANSTOP20 controls. User can view the mapped control numbers in the external reference column on the GUI. 2. A status panel is provided to the user to track the control evaluation process when user re-evaluates a control.
Administration > Global Categorization	Monitoring Policies in Administration tab is renamed to 'Global Categorization' 1. Policy Group on left pane is removed. 2. Selecting of Policy group in creation of Event Categorization is removed as Group display is not allowed. 3. Policy Type is introduced in the display of 'Global Categorization'
New/Updated Device Support	New Device Support is listed below: 1. Sophos Enterprise Console v5.2 (AV) (Only with SQL Server) 2. Imperva SecureSphere 9.5 3. DB Protect 6.2 (Only with SQL Server) 4. BlueCoat Proxy SG 5.5.x Updated Device Support is listed below: 1. Tipping Point SMS 3.2 2. McAfee Web Gateway 7.2 3. McAfee Email Gateway 7.5 4. MSSQL 2008/2012 5. Universal Parser – Multiline (Through TCP Streaming and File Collector on DC)

Alerts	A new field 'Application Name' as criteria in Alerts for dynamic lists has been added.
Dynamic Filters	A filter has been added, for Forensics, Alerts, Reports and Monitors, where a user can define a set of dynamic search criteria within a file.
Enhancements to Collection Policies	1. A new feature 'Collect Now' has been introduced to trigger an instant data collection for devices and hosts. 2. 'Enable Flow Collection' in Device collection policies 3. Support for adding a custom event facility option is now provided in Collection Policies for Hosts.
Unified Node License	Only one license type is supported which is capable to manage/un-manage any node type. Default/Application/BULK licenses are replaced with 'Node' license.
DB Agents node handling	Only DB Server need to be managed. Data from all the end points under DB agent will be fetched and processed.
Workflow	A new naming mechanism for Remedy tickets has been added.
Usability Enhancements to Sorting Options and Alert Notifications	Ability to sort on column headers for Reports and Monitors.
User Right-click options and Workflow tickets	Right click options and Workflow tickets are provided based on Role Based Access Control permissions given to the user.
Alerts View	A new column has been introduced in the user interface to show each notification type configured per alert with their respective icons. New icons include on-screen notifications for: Email, SNMP Trap, SecureVue Ticket, Remedy Ticket, and Running External Executable.
	The user interface has been enhanced to display multiple eMail addresses for a SMTP alert notification.
Enhancements to Reports	In Reports pane, 'Show this Report in ForensicVue' is provided for all applicable Reports.
	A link to ForensicVue is provided in the help card for some reports where all the information is not displayed due to topping of data.
Renamed Features	- 'Custom Source' criteria in Alerts/Monitors/Forensics modules is renamed to 'Extended Sources'.
Unsupported Features	- Removal of SV HA support - Data Processor GUI functionality is removed.

Premium and Free Configurations - Summary

Configuration	Description
Enterprise Configuration	This Premium configuration provides all capabilities of SecureVue application 'except' ThreatVue and ComplianceVue.
LogSIEM Configuration	This Premium configuration provides Log Management and Intelligent Security Search.

ComplianceVue™	This Premium configuration is an add-on Premium configuration of the SecureVue solution. 1. Provides comprehensive configuration auditing across servers, desktops, network and security devices and applications to help organizations implement prescriptive configuration standards such as CIS benchmarks, DISA STIGs and customized minimum security requirements (MSRs). 2. This helps improve overall security and proactively identify misconfigured systems, policy violations as well as unauthorized changes across the enterprise. SecureVue provides the capability to monitor and control a broad spectrum of controls.
ThreatVue™	This Premium configuration is provided for innovative automation to monitor the status of an organization's information security posture through the ongoing evaluation of security controls that are based on SANS top 20. Controls available in SecureVue v3.6.6 include: 1. **Control 1 Unauthorized nodes detected** – For detecting unauthorized nodes in a network by comparing nodes discovered by various techniques (Nmap scan, DHCP servers, Qualys and Nessus Vulnerability scan result files) against Managed Nodes 2. **Control 2 Unauthorized Software Detected** – For detecting Unauthorized software on Managed Nodes 3. **Control 3 Vulnerabilities Discovered in IT Infrastructure** – For Identifying the Vulnerabilities and attacks performed on the Managed Nodes 4. **Control 4 Malware Defenses Deployed** – For Anti-Malware detection on Managed Nodes 5. **Control 5 Rogue Access Points Detected** – For Continual assessment for wireless activity by Nessus and Nmap scans. 6. **Control 6 Unauthorized Ports and Protocols** – For Classification of unauthorized port and protocols, firewall service status on managed nodes. 7. **Control 7 Log Monitoring** – For Audit log management
FIMVue™	This Free Configuration is provided for evaluating File Integrity Monitoring 1. Ensures that integrity is truly intact from top to bottom, with visibility into raw file contents, attributes, permissions, registry settings and security parameters. 2. Monitors specified files and directories for change events such as File Added, Deleted, Modified or Renamed in order to detect unusual or suspicious activity. 3. Historical reporting of file changes using dashboards that allow users to quickly and easily identify long term patterns.

USBVue™	This Free Configuration is provided for evaluating USB Monitoring 1. Monitor all USB file transfers that occur on Windows and Red Hat Linux systems. 2. Can be used to identify file transfers that could potentially expose sensitive information protected by HIPAA, GLBA and other data privacy regulations.
LogVue™	This Free Configuration is provided for evaluating Log Management and Searching 1. Collect Syslog and Windows event logs from network devices, workstations and servers. 2. Utilizes ForensicsVue™, an integrated component of the SecureVue platform, to perform high-speed searches of event log data. 3. Quickly respond to security incidents and policy violations by searching across a wide spectrum of network devices and systems.
DiscoveryVue™	This Free Configuration is provided for evaluating Asset Policy Management capabilities 1. SecureVue collects detailed asset information without the use of agents, including complete and intricate details of hardware, OS, application state and asset value. 2. All asset critical data collected by SecureVue is stored in the platform's secure, fully authenticated database, and is made available for monitoring, reporting and analysis.
FlowVue™	This Free Configuration is provided for evaluating Network Traffic Analyzing capabilities 1. This configuration helps analyze the traffic in your network. 2. Collects netflow data from managed routers, switches, firewalls and other devices that generate flow packets to provide detailed, normalized information regarding ports, protocols, bandwidth and connection state between devices both inside and outside the network. 3. Monitors traffic flow and bandwidth utilization by user, application, interface and protocol to provide real-time insight into network resource consumption.
VulnerabilityVue™	This Free Configuration is provided for evaluating Vulnerability Management capabilities 1. This configuration helps evaluate the vulnerability management capabilities of SecureVue. 2. Integrates with trusted vulnerability scanners out-of-box, and correlates this information. 3. Provides the ability to establish policies and proactively identify and fix vulnerabilities.
PerformanceVue™	This Free Configuration is provided for evaluating Network Performance Monitoring

	1. This configuration helps evaluate the network performance management capabilities of SecureVue. 2. Performance variables/factors of an asset in the network can also indicate possible malicious activity. If a windows host does lot of network activity during weekends it might indicate a hostile application running and using the network to transfer mission critical data to some malicious user's machine. 3. Provides the ability to establish policies and identify the node and host performance metrics through alerts, monitors and reports.
EventVue™	This Free Configuration is provided for evaluating Network Event Monitoring 1. This configuration helps evaluate the event monitoring capabilities of SecureVue. 2. Collect data from hundreds of network, security and computing devices, applications and databases, and easily import custom application and database logs for monitoring purposes.

What's New from NGS v3.0 to SV 3.6.6

Functional Area	Description
ThreatVue Sub-Controls	Newly added Sub-Controls in SecureVue v3.6.6 include: 1. **Control 1: Unauthorized nodes Detected** – For detecting unauthorized nodes in a network by comparing nodes discovered by Rapid7 Vulnerability scan result file against Managed Nodes 2. **Control 5: Rogue Access Points Detected by Nessus Scanner** – For Continual assessment for wireless activity 3. **Control 6: Unauthorized Ports and Protocols** – For Classification of unauthorized port and protocols based on nodes detected by Nessus and Unauthorized Ports & Protocols based on hosts detected by Flow and Firewall service status on managed nodes.
ThreatVue Control Evaluation Results	Ability to alert/report/forensics on ThreatVue Control Status. Support for alerts, reports, forensics on the ThreatVue controls and their evaluated results.
Product Configurability	Refer Product Configurability section for more details.
Alerts Table of Contents	Table of Content for Alerts is provided on pre-defined set of fields which will be used for further filtering in Alert Archives. This is available at 2 levels 1. Global Level (TOC at Alerts Portal): Provides the count of events which are contributed to trigger all the alerts. 2. Alert Level (TOC on Alert Archives): Provides the count of events

	which are contributed to trigger a specific alert.
Alerts Notification	Alert supporting evidence where Subject is per notification and a notification can be set for multiple alert policies. In order to have a clear identification, subject line is prefixed with Alert name.
Black list	Introduced concept of “blacklist” in SV3.6.6 for disallowed entities which can be used in ThreatVue Control evaluation.
Administration > Global Categorization	Monitoring Policies in Administration tab is renamed to 'Global Categorization' 1. Policy Group on left pane is removed. 2. Selecting of Policy group in creation of Event Categorization is removed as Group display is not allowed. 3. Policy Type is introduced in the display of 'Global Categorization'
Administration > Preferences > User Sessions	Option is provided in SecureVue using which user can limit Concurrent sessions for a SecureVue user account (login at same time w/ same user name)
Administration > Preferences > General	‘Configured Node limit per Data Collector’ option is provided in General Preferences using which user can limit number of nodes configured to a Data Collector.
Renamed Features	The ‘Custom Source’ criteria is renamed to ‘Extended Sources’ in Alerts/Monitors/Forensics modules.

2.0 Installation and Upgrade Notes

EiQ Networks recommends the following for customers looking to upgrade to v3.6.6

- Customers upgrading from any SecureVue v3.6.x version can follow the below upgrade process:
  - SecureVue v3.6.0 and v3.6.5 users can directly upgrade to 3.6.6 using the standard installer
  - SecureVue v3.6.1, v3.6.2, v3.6.3 and v3.6.4 users should contact EiQ Networks customer service for further instructions
  - Customers wishing to upgrade from any version prior to 3.6.x should contact EiQ Networks customer service for further instructions.
- Customers upgrading from SecureVue version v3.6.0, v3.6.1, v3.6.2 and v3.6.3 need to manually update the changes in IndexFields.txt. Contact EiQ Networks customer service for Details.
- NGS 3.0 users are also allowed to migrate to SV 3.6.6. Contact EiQ Networks customer service for Details.
- User can implement distributed indexing procedure to facilitate faster indexing of old forensic logs after upgrading to 3.6.6. Contact EiQ Networks customer service for Details.
- Silent Upgrade Only: 3.6.0/3.6.5 deployments with IIS website or virtual directory for Data Processors have to manually remove the respective website/VD after completion of the Silent upgrade.

3.0 Customer Issues Addressed in SecureVue v3.6.6

The following issues are addressed in SecureVue v3.6.6

Case Number	Bug Number	Summary
7169	28453	To provide an option to choose an alternate storage location for Forensic Reports
10727	38855	Communication issues between Data Processor and Central
10762	38869	Remedy receiving error from SV when multiple XML requests are run in parallel
10842	38910	Remedy receiving wrong ticket data intermittently
	39019	dport is not updating properly for Checkpoint Device
11054	39170	SNMP interface reports show 0's for first collection of the day
11209	39343	Multi Rule alert changing rule expression when editing an aspect of one of the rules
11187	39344	Availability Alert inconsistent in triggering
	39364	Agent stops operating and logging
11373	39693	parsing sip from event 675
11405	39716	Issues in Parsing events from Cisco ASA 8.x device
11407	39718	Mismatch in the parsing of Cisco ASA 7.x logs
	39884	Alert archive is not sorted according to date
12230	40235	'act' field is being updated as numeric in monitor.
	40340	ELF fields from the Oracle DB Connector. Customer would like DB_NAME added to the list of fields returned from Oracle DB
10875	40349	Forensic Temp folder continually increasing and not catching up
12119	40363	Forensic search fails when delta size is greater than 200 MB
11932	40364	Linux/Unix events are not written properly to raw log
12121	40365	Fortigate blade on appearing for 1 out of the 4 cards
12191	40418	Incorrect search expression is being forwarded to Forensics from "Top security events by source" Report
	40431	Custom Logo size limitation for reports an issue
	40704	Fortinet 5.0 parsing issue
	40786	deployment guide mentions installing the agent on windows 2000
12348	40787	Linux DCs consider all the *nix rules instead of only the rules associated with any compliance policies
12317	40788	WMI security event collection fails when there are more than 2 billion events/records
12350	40789	Hide IP address of the SecureVue central in the browser
12275	40790	New pattern window fails when the day has '11' in it

12297	40793	Flow anomaly/violation alerts show previous date instead of the event received/actual date
12378	40820	Alert temp files taking up large amounts of disk space
12420	40883	Agent seems to be collecting every event in event log at every collection
12432	40884	Syslogserver.exe restarts while parsing NetScreen events for username
12052	40937	Forensics Search Engine crash when the dynamic list filter contains 2640+ entries

4.0 Known Issues and Workarounds with SecureVue v3.6.6

Bug Number	Issue Summary	Workaround
41524	Silent Upgrade fails on all Data Processors	Silent upgrade from SV3.6.0/SV3.6.5 to SV3.6.6 can be done only after applying the following workaround: - Create a folder with the name 'UpgradeSW' in the target DP/DC system's AppPath (like C:\SVDP\UpgradeSW). - Copy the <CentralAppPath>\ssleay32.dll file to the above created UpgradeSW folder of DP/DC AppPath. - Run the Upgrade.exe with appropriate arguments from the Central server to complete the silent upgrade.
41866	Default collection policies are not applicable for the below configurations and are in disabled mode. • EventVue • FlowVue • DiscoveryVue • VulnerabilityVue • LogVue • ComplianceVue	User needs to create a New Collection Policy for assigning to nodes.
41846	Online help generated from Adobe Robohelp 8 has compatibility issues with IE 10.	Use Compatibility mode when browsing online help.
41915	Rule settings are not saving while edited from rule result window.	Navigate to ComplianceVue > Manage Policies and Select a rule, right click and

		use ‘Edit Rule’ option to edit the rule.
41918	When any rule is edited from rule result window it is showing duplicate rules in drilldown window.	Navigate to ComplianceVue > Manage Policies and Select a rule, right click and use ‘Edit Rule’ option to edit the rule.
	Browser Issues with IE where certain items are NOT displayed properly.	Add the SecureVue application URL to Trusted Sites list.
	When Nmap Scan is performed by a Data Collector that is not under HIPS trusted list, the nodes in Nmap scan range will become temporarily unreachable as per HIPS policy settings.	Add the Data Collector IP to Trusted IPs list on HIPS policy, after which Nmap scanning is able to detect all the nodes in the network without any hindrances.
	DHCP Collection: Data Collector fails to get IPv6 node assignments using IPv6 server IP.	Use Ipv4 server IP with Ipv6 scope for DHCP Collection.
	Unable to browse application in Internet Explorer if underscore ‘_’ exists in the system name.	Browse SecureVue application with IP address.
	Node is getting moved to Default Group on performing Change Node Type activity.	Move the node from Default Group to the required group.
	Since Data Processor GUI support is removed after upgrade to 3.6.6, After upgrade to SV 3.6.6, user can’t manage File collectors (on File Source: Server & FTP) at Data Processor tier.	Stop File Collector collections at DP. User has to manage these File collectors from Central server by adding them again.
	User can’t manage already created schedulers in Scheduled Reports & ForensicVue at Central	Stop all schedulers at DP. User has to create new schedulers in Scheduled Reports & ForensicVue at Central server.
	After upgrade from 3.6.5 to 3.6.6, data will not update at ‘Event Statistics’ report under Reports -> ‘Data Processor Performance Reports’ as File collectors can’t be managed from DP GUI	The ‘Event Statistics’ reports under Reports > ‘Data Processor Performance Reports’ is retained on the Central so that user can see historical data from the respective Data Processor. Note that latest data from DP will not get updated at Central server.
	User cannot see the amount of data uploaded to Central from a particular DP via Bandwidth by Hour of Day query under Health Reports.	Bandwidth by Hour of Day query Is available at Central and user has the facility to apply filter on ‘Source’ column to view respective DP report.
	After upgrade from NGS 3.0 to SecureVue 3.6.6, Compliance reports will not be shown for non-admin users who are assigned with those reports.	Administrator need to reassign the compliance reports as per policy for respective users

5.0 SecureVue v3.6.6 System Requirements

SecureVue v3.6.6 **Central** minimum system requirements:

- **Processor:** Dual Xeon Quad Core 2.0 GHz or higher
- **Memory:** 32 GB or higher [64 GB Recommended]
- **Storage:** 1 TB or higher on 15K RPM SCSI drives
- **Operating System:** Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit)
- **Java:** Java (JRE) 1.6 r30
- Microsoft Office 2003 or 2007 is required to generate Microsoft Word or Excel reports.

***Note A*:** SecureVue 3.6.6 Central is supported to run on VMWare host with similar configuration.

***Note B*:** User should not revert to a VMWare snapshot. Reverting snapshot will result in corrupting the Central Server data set.

SecureVue v3.6.6 **Data Processor** minimum system requirements:

- **Processor:** Dual Xeon Quad Core 2.0 GHz or higher
- **Memory:** 16 GB or higher [32 GB Recommended]
- **Storage:** 500 GB or higher on 15K RPM SCSI drives
- **Operating System:** Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit)

***Note A*:** SecureVue 3.6.6 Data Processor is supported to run on VMWare host with similar configuration.

***Note B*:** User should not revert to a VMWare snapshot. Reverting snapshot will result in corrupting the Data Processor data set.

SecureVue v3.6.6 **Data Collector** minimum system requirements:

- **Processor:** P4 Processor 2.4 GHz or higher
- **Memory:** 1 GB or higher [4GB Recommended]
- **Storage:** 50 GB or higher on 7200 RPM SATA drives
- **Operating System:** Windows Server 2008 R2 64-bit, Windows Server 2012 64-bit, CentOS 5 64-bit, RHEL 5.X (32-bit and 64-bit), RHEL 6.X 64-bit

***Note A*:** SecureVue 3.6.6 Data Collector is supported to run on VMWare host with similar configuration.

***Note B*:** User should not revert to a VMWare snapshot. Reverting snapshot will result in corrupting the Data Collector data set.

***Note C*:** For IPv6 systems or data collection, EiQ Networks' recommends using Windows Server 2008 R2/2012 as the Operating System for SecureVue Data Collector.

SecureVue v3.6.6 **Windows Agent** minimum system requirements:

- **Processor:** P4 Processor 1.8 GHz or higher
- **Memory:** 1 GB or higher
- **Storage:** 500 MB or higher on 7200 RPM SATA drives
- **Operating System:** Windows Server 2008 R2 64-bit, Windows Server 2012 64-bit, Windows Vista 64-bit, Windows7 64-bit.

SecureVue v3.6.6 **UNIX/Linux Agent** minimum system requirements:

- **Processor:** P4 Processor 1.8 GHz or higher
- **Memory:** 1 GB or higher
- **Storage:** 500 MB or higher on 7200 RPM SATA drives
- **Operating System:** CentOS 5 64-bit, RHEL 5.X 32-bit and 64-bit, RHEL 6.X 64-bit, Solaris 10.X 32-bit, Solaris Sparc10 64 bit, AIX V5.X 64-bit, AIX V6.X 64-bit

***Note*:** USB Monitoring is not supported on RedHat-6.

Special Deployment Notes

64-bit JRE for 64-bit Deployments

In 64-bit OS deployments, you need to install 64-bit JRE and set the JAVA_HOME environment variables.