



## **SecureVue Cryptographic Modules FIPS 140-2 Level 2 Non-Proprietary Security Policy**

**Version 2.4**

**Vendor: eIQnetworks, Inc**

This document is provided for informational purposes about the structure of the Cryptographic Module as it pertains to FIPS 140-2 validation.

**Contact:**

eIQnetworks, Inc.  
31 Nagog Park  
Acton, MA 01720  
United States of America

Tel: +1 978 266 9933  
Fax: +1 978 266 0004

Website: <http://www.eIQnetworks.com>

## Table of Contents

|                                                                            |           |
|----------------------------------------------------------------------------|-----------|
| <b>1. CRYPTOGRAPHIC MODULE SPECIFICATION.....</b>                          | <b>2</b>  |
| SOFTWARE ENVIRONMENT .....                                                 | 3         |
| CRYPTOGRAPHIC BOUNDARY.....                                                | 6         |
| <i>Physical Boundary</i> .....                                             | 6         |
| <i>Hardware Block Diagram</i> .....                                        | 6         |
| <i>Logical Boundary</i> .....                                              | 6         |
| <i>Software Block Diagram</i> .....                                        | 7         |
| APPROVED MODE OF OPERATION .....                                           | 8         |
| <b>2. CRYPTOGRAPHIC MODULE PORTS AND INTERFACES.....</b>                   | <b>9</b>  |
| <b>3. ROLES, SERVICES, AND AUTHENTICATION.....</b>                         | <b>11</b> |
| ROLES .....                                                                | 11        |
| SERVICES .....                                                             | 12        |
| AUTHENTICATION .....                                                       | 13        |
| <i>Strength of Authentication Mechanism</i> .....                          | 13        |
| <b>4. PHYSICAL SECURITY .....</b>                                          | <b>15</b> |
| <b>5. OPERATIONAL ENVIRONMENT.....</b>                                     | <b>16</b> |
| <b>6. CRYPTOGRAPHIC KEY MANAGEMENT.....</b>                                | <b>17</b> |
| <b>7. SELF-TESTS .....</b>                                                 | <b>21</b> |
| POWER-UP SELF-TESTS .....                                                  | 22        |
| <i>Software Integrity Test</i> .....                                       | 22        |
| <i>Critical Functions Test</i> .....                                       | 23        |
| CONDITIONAL SELF-TESTS .....                                               | 23        |
| <i>Software/Firmware Load Test</i> .....                                   | 23        |
| <i>Manual Key Entry Test</i> .....                                         | 23        |
| <i>Continuous Random Number Generator Test</i> .....                       | 23        |
| <i>Bypass Test</i> .....                                                   | 23        |
| <b>8. MITIGATION OF OTHER ATTACKS.....</b>                                 | <b>24</b> |
| <b>9. APPENDIX-A SHA256 DIGESTS OF SECUREVUE MODULES .....</b>             | <b>25</b> |
| <b>10. APPENDIX-B ADMINISTERING SERVICES &amp; FOLDER PERMISSIONS.....</b> | <b>26</b> |
| <b>11. APPENDIX-C EXECUTABLES.....</b>                                     | <b>33</b> |

# 1. CRYPTOGRAPHIC MODULE SPECIFICATION

SecureVue from eIQnetworks is a leading IT security, risk and audit management platform that combines next-generation security information management (SIM) with governance, risk and compliance (GRC) to improve operational efficiency and reduce management complexity. Using an integrated model, SecureVue goes beyond traditional log-based SIM solutions to collect, correlate, archive, analyze and report on all critical security and compliance data. Through end-to-end correlation, SecureVue transforms volumes of log, vulnerability, configuration, asset, performance and flow data into actionable intelligence. Built-in network behavioral anomaly detection (NBA) automatically profiles flow data to identify anomalies. Additionally, a comprehensive compliance library - containing more than 5,000 control objectives - maps directly to specific regulations, best practices and control frameworks.

This Security Policy covers four SecureVue cryptographic modules:

1. SecureVue Central Cryptographic Module
2. SecureVue Regional Cryptographic Module
3. SecureVue Data Collector Cryptographic Module
4. SecureVue Agent Cryptographic Module

Cryptography is used to secure communications between each cryptographic module.

For FIPS 140-2 purposes, each Cryptographic Module is classified as a multi-chip standalone module. The module meets the Overall Level 2 requirements. Each SecureVue cryptographic module meets the following security levels.

Table 1 – Security Level

| FIPS Section                              | Level |
|-------------------------------------------|-------|
| Cryptographic Module Specification        | 2     |
| Cryptographic Module Ports and Interfaces | 2     |
| Roles, Services, and Authentication       | 2     |
| Finite State Model                        | 2     |
| Physical Security                         | N/A   |
| Operational Environment                   | 2     |
| Cryptographic Key Management              | 2     |
| EMI/EMC                                   | 2     |
| Self-Tests                                | 2     |
| Design Assurance                          | 2     |
| Mitigation of Other Attacks               | N/A   |

Each SecureVue cryptographic module uses FIPS approved cryptographic algorithms. The following table identifies the algorithms used:

**Table 2 - Approved Cryptographic Algorithms**

| <b>Algorithm</b>                                       | <b>FIPS Validation Certificate #</b>                                                                                         | <b>Use</b>                                                                         | <b>Module</b> |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|---------------|
| AES(ECB mode)<br>(Advanced Encryption Standard)        | Windows Server 2003 SP2,<br>Windows Server 2003 R2 SP2<br>and Windows XP Pro x64 SP2 -<br>#1277<br>Windows XP Pro SP2 - #695 | encrypt/decrypt<br>operations                                                      | All           |
| RSA <sup>1</sup> (Rivest Shamir<br>Adleman) - 2048 bit | Allowed in FIPS mode                                                                                                         | key-wrapping and<br>key-establishment<br>methodologies                             | All           |
| ANSI X9.31                                             | Windows Server 2003 SP2,<br>Windows Server 2003 R2 SP2<br>and Windows XP Pro x64 SP2 -<br>#712<br>Windows XP Pro SP2 - #407  | random number<br>generation                                                        | All           |
| SHS                                                    | Windows Server 2003 SP2,<br>Windows Server 2003 R2 SP2<br>and Windows XP Pro x64 SP2 -<br>#1175<br>Windows XP Pro SP2 - #723 | digest computation                                                                 | All           |
| HMAC                                                   | Windows Server 2003 SP2,<br>Windows Server 2003 R2 SP2<br>and Windows XP Pro x64 SP2 -<br>#742<br>Windows XP Pro SP2 - #373  | 1) module integrity<br>check<br><br>2) digest<br>comparison during<br>key-exchange | All           |

The modules also support the use of the following non-Approved algorithms: MD5 and non-Approved RNG. This algorithm is Allowed in FIPS mode as it is used as part of an approved key transport scheme (SSL v3.1).

## Software Environment

Each SecureVue cryptographic module runs on any general purpose computer running Microsoft Windows 2003/XP Operating System in the Controlled Access Protection Profile v1.d compliant CC evaluated mode with the assurance level of EAL 4, augmented with ALC\_FLR.3 and AVA\_VLA.4. The protection of all the certificate and the keys relies on the file system access control settings of the Operating System. The SecureVue Central and Data Collector modules are also

<sup>1</sup> RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength).

capable of zeroizing persistent keys, if really needed in the eventuality of a compromised Operating System.

Following are the Recommended System Requirements:

- For Central and Regional module Deployments:-
  - *Processor:* Intel Dual Xeon Quad Core 2.00 GHz or higher
  - *Memory:* 8 GB or higher
  - *Storage:* 500 GB or higher on 15K RPM SCSI drives
  - *Operating System:* Windows Server 2003 in the Controlled Access Protection Profile v1.d compliant CC evaluated mode with the assurance level of EAL 4, augmented with ALC\_FLR.3 and AVA\_VLA.4
  - *Java:* Java (JRE) 1.6 or higher
  - *Web-service:* IIS
- For Data Collector module Deployment:-
  - *Processor:* Intel Pentium 4 Processor 2.4 GHz or higher
  - *Memory:* 1 GB minimum
  - *Storage:* 50 GB or higher
  - *Operating System:* Windows XP in the Controlled Access Protection Profile v1.d compliant CC evaluated mode with the assurance level of EAL 4, augmented with ALC\_FLR.3 and AVA\_VLA.4
- For Agent module Deployment:-
  - *Processor:* Intel Pentium 4 Processor 2.4 GHz or higher
  - *Memory:* 1 GB minimum
  - *Storage:* 10 GB or higher
  - *Operating System:* Windows XP in the Controlled Access Protection Profile v1.d compliant CC evaluated mode with the assurance level of EAL 4, augmented with ALC\_FLR.3 and AVA\_VLA.4

The following table identifies the platform each SecureVue cryptographic module was tested on.

**Table 3 - Test Platform Information**

| Test Platform         | Processor       | CC Evaluated Operating System | Module         |
|-----------------------|-----------------|-------------------------------|----------------|
| Dell PowerEdge 1800   | Intel Xeon      | Windows Server 2003 SP2       | Central        |
| Dell PowerEdge 1420   | Intel Xeon      | Windows Server 2003 R2 SP2    | Regional       |
| HP XW9300 Workstation | AMD 64 Opteron  | Windows XP Pro x64 SP2        | Data Collector |
| Dell Optiplex Gx620   | Intel Pentium D | Windows XP Pro SP2            | Agent          |

Each module must be installed on a separate platform running a CAPP-compliant Operating System configured in the CC evaluated mode.

## Cryptographic Boundary

### Physical Boundary

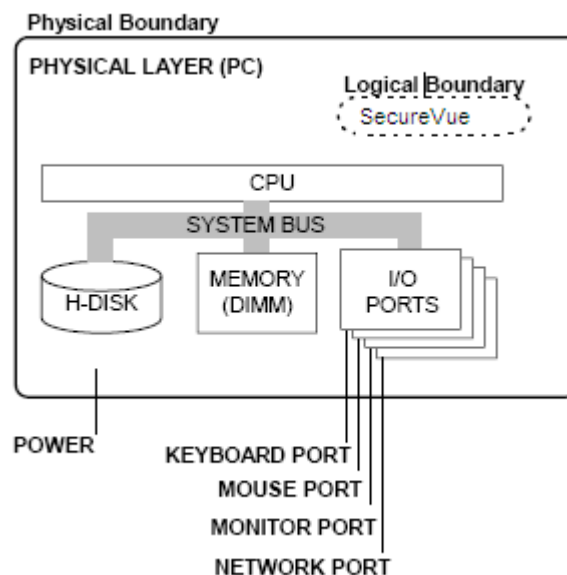
The *physical boundary* for each module is defined as the enclosure of the computer system on which the module runs. The general purpose, Intel compatible computer consists of the following physical components:

- CPU (microprocessor, Intel x86 compatible)
- Memory (RAM) including working memory (input/output buffers, plaintext/cipher text buffers and control buffers) and program memory
- Hard disk (or disks)
- Display controller
- Keyboard interface
- Mouse interface
- Network interface (Ethernet)
- Serial port
- Parallel port
- Power supply

### Hardware Block Diagram

The following block diagram shows the keyboard and mouse ports as physical ports for data or control input, and the monitor port as the physical port for data and status output.

Figure 1 - Cryptographic Boundary

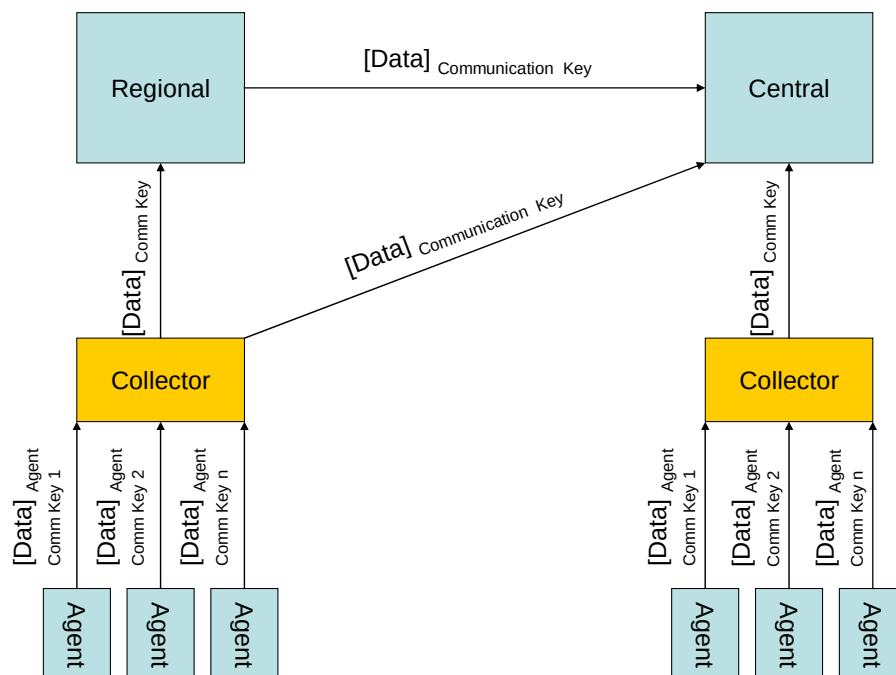


### Logical Boundary

Each SecureVue cryptographic module is composed of multiple binary executables. The complete list of executables for each SecureVue cryptographic module is provided in Appendix C of this security policy. The list of executables defines the logical boundary for each Cryptographic module.

## Software Block Diagram

Figure 2 - Software Block Diagram



The interaction of the four modules is outlined above.

The Agent module resides on the host to be monitored, sending its monitored data to the Collector. The Collector then forwards the data to Central, which stores it in its database and displays it to the user.

Regional is an optional module which can be utilized to lessen the load on Central, or to provide another instance on which the User can view the data collected. In this case, Regional would be an intermediary between Central and Collector: collecting the relevant data, storing it in a local database, displaying it to the user, and ultimately forwarding it to Central.



All traffic between each of the four SecureVue cryptographic modules is encrypted with AES Communication Keys.

## Approved Mode of Operation

The System Administrator installing SecureVue Central and Regional modules should use local Windows user accounts for SecureVue user accounts. If LDAP or ActiveDirectory users are to be imported, then even those user accounts should be on a Windows System configured to be compliant with CAPP.

**NOTE:** SecureVue module operates in FIPS mode ‘**only**’ when configured as follows:

- Windows/ActiveDirectory user accounts are used as SecureVue Users (i.e. - SecureVue user authentication is not used)
- Only a System Administrator may have Full Control over the folder in the respective SecureVue module installation paths. No other user should be granted any kind of access to the SecureVue module installation folders. Please refer to [Appendix-B](#) for details on how to set the folder permissions.

## 2. CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

The *physical interfaces* are standard I/O ports of a computer on which the application is installed. Please refer [Software Block Diagram](#)

Table 4 - Physical Interfaces

| FIPS Interface | Physical Port          |
|----------------|------------------------|
| Data Input     | Ethernet Ports         |
| Data Output    | Ethernet Ports         |
| Control Input  | Keyboard               |
|                | Ethernet Port          |
| Status Output  | Monitor, Ethernet Port |

The *logical interfaces* of the Module are separated based on the services provided by the executables defined with the cryptographic boundary for each SecureVue cryptographic module. The following table identifies the FIPS logical interfaces supported by each executable. Please refer to the Roles, Services, and Authentication section for details on the specific services provided by each executable.

Figure 3 - Logical Interfaces

| FIPS Interface | Regional/Central Module Executables                                                                                   | Data Collector Module Executables                                                                                                           | Agent Module Executables          |
|----------------|-----------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| Data Input     | FileSync.exe,<br>ForensicSearchEngine.exe,<br>MainEngine.exe,<br>MonitoringEngine.exe,<br>Topology.exe                | Configmon.exe,<br>HostCollector.exe,<br>Leaserver.exe,<br>MonitoringEngine.exe,<br>Snmppmon.exe,<br>Snmpttrapagent.exe,<br>syslogserver.exe | HostCollector.exe,<br>SVAgent.exe |
| Data Output    | FileSync.exe,<br>ForensicSearchEngine.exe,<br>MainEngine.exe,<br>ParserEngine.exe,<br>Topology.exe,<br>VizConsole.exe | HostCollector.exe,<br>Snmpttrapagent.exe,<br>WatchDog.exe                                                                                   | HostCollector.exe,<br>SVAgent.exe |
| Control Input  | MainEngine.exe,<br>VizConsole.exe                                                                                     | Configmon.exe,<br>DCConf.exe<br>HostCollector.exe,                                                                                          | HostCollector.exe,<br>SVAgent.exe |

| <b>FIPS Interface</b> | <b>Regional/Central Module Executables</b>         | <b>Data Collector Module Executables</b>             | <b>Agent Module Executables</b>   |
|-----------------------|----------------------------------------------------|------------------------------------------------------|-----------------------------------|
| Status Output         | MainEngine.exe,<br>Topology.exe,<br>VizConsole.exe | DCCnf.exe,<br>HostCollector.exe,<br>syslogserver.exe | HostCollector.exe,<br>SVAgent.exe |

### 3. ROLES, SERVICES, AND AUTHENTICATION

Each SecureVue module specifies the roles, access controls, services, and security-relevant data items so that operators can perform specific services in specific roles.

Each SecureVue module uses role based access for performing cryptographic functions.

#### Roles

- *Crypto Officer Role: **System Administrator*** - This role is assumed by users logging onto the operating system as System Administrator. The FIPS 140-2 Crypto-Officer is responsible for installation of the Central, Regional(s), Collectors and Agents. The Crypto-Officer of Central and Collector is also responsible for the generation of the encryption keys either by manual trigger or a scheduled change. Once the Encryption keys are changed, they are automatically transferred to the remote components. See table 4.1 for details on services.
- *User Role:* This role is assumed by users (not System Administrator) logging onto the operating system. SecureVue users have access to the SecureVue GUI to view event data.

## Services

**Table 4.1: Cryptographic Services and Roles**

| <i>Service</i>                                                               | <i>Role</i>             | <i>Logical Interface</i> | <i>CSP</i>                                                 | <i>Access</i> | <i>Module</i>                        |
|------------------------------------------------------------------------------|-------------------------|--------------------------|------------------------------------------------------------|---------------|--------------------------------------|
| Module Installation                                                          | Crypto Officer          | Control Input            | Central RSA Private Key and Data Collector RSA Private Key | Read/Write    | All                                  |
| Database Key Generation                                                      | Crypto Officer          | Data Input               | AES Database Key                                           | Write/Execute | Central                              |
| File/Password Key Generation                                                 | Crypto Officer          | Data Input               | AES File/Password Key                                      | Write/Execute | Central                              |
| AES Communications Key Generation                                            | Crypto Officer          | Data Input and Output    | AES Communications Key                                     | Write/Execute | Central                              |
| AES Agent Communications Key Generation                                      | Crypto Officer          | Data Input and Output    | AES Agent Communications Key                               | Write/Execute | Data Collector                       |
| AES Communication Keys Entry                                                 | Crypto Officer          | Data Input               | AES Communications Key                                     | Write         | Data Collector and Regional          |
| AES Agent Communication Keys Entry                                           | Crypto Officer          | Data Input               | AES Agent Communications Key                               | Write         | Agents                               |
| Event and data collection output                                             | User                    | Data output              | AES Communication Key and AES Agent Communication Key      | Execute       | All                                  |
| Event and data collection input                                              | User                    | Data input               | AES Communication Key and AES Agent Communication Key      | Execute       | Central, Regional and Data Collector |
| Self test                                                                    | Crypto Officer and User | Control Input            | None                                                       | Execute       | All                                  |
| Show Status (statistics, logging, configuration info and self-test results ) | Crypto Officer and User | Status Output            | None                                                       | Read          | All                                  |
| Zeroize                                                                      | Crypto Officer          | Control Input            | All symmetric and private keys                             | Write         | All                                  |

## How to run FIPS self-tests

See section 7.

## How to run Key Zeroization

Key Zeroization can be performed from command prompt on Central. Change Directory to SecureVue module installation path and type *MainEngine.exe -key-zeroization*. Invocation of this Central command will zeroize the two persistent Central symmetric keys; AES Database Key and the AES File/Password Key.

To zeroize the RSA private key on Central and Data Collector, the operator must uninstall the module software and format the hard drive in which the module was originally installed. This will ensure proper zeroization of the RSA private key (as well as any other module key).

All ephemeral keys are automatically zeroized by the module when they are no longer needed. Zeroization of these ephemeral keys occurs when the module closes an SSL session or when the module is powered off.

## Authentication

The module supports the following 3 authentication modes:

- SecureVue Authentication<sup>2</sup>
- Windows Authentication
- LDAP/ActiveDirectory authentication

For the module to run in FIPS mode, only Windows authentication or ActiveDirectory authentication may be used. Both authentication methods are provided by the Common Criteria evaluated operating system.

## Strength of Authentication Mechanism

Operating system enforces strong shield to address the brute-force password attacks. This is done through:

- Password Strength
- Account Lockout for consecutive failed login attempts.

**Password Strength:** Passwords must be alphanumeric with at least one special character and must be at least 12 characters for a Crypto Officer and 8 characters for other Users

As we have 26 lower case + 26 upper case +10 digits + special characters which are approximately almost equivalent to 75 characters.

---

<sup>2</sup> SecureVue authentication is not to be used in FIPS mode.

Minimum password combinations that are possible are:

- For Crypto Officer:  $75! / (75 - 12)! = 75 \times 74 \times 73 \times 72 \times 71 \times 70 \times 69 \times 68 \times 67 \times 66 \times 65 \times 64 = 12513384826762659840000$
- For Users:  $75! / (75-8)! = 75 \times 74 \times 73 \times 72 \times 71 \times 70 \times 69 \times 68 = 680240886192000$ .

Both the above numbers are significantly large and hence brute force mechanism would take significantly long time to succeed.

As the length of password can stretch to 31 characters, it will practically rule out the option of cracking it.

**Account Lockout:** Windows System will manage the account lockout policy and lock out a user performing a brute force attack if windows native authentication is used or domain authentication is used with the system in Common Criteria mode.

Both the above rules make it very difficult for a brute-force password attack to break through the defenses of authentication mechanism.

## **4. Physical Security**

SecureVue module is a software based cryptographic module and not subject to the Physical Security Requirements of FIPS 140-2.



## 5. OPERATIONAL ENVIRONMENT

SecureVue v3.1.2.3 is a software application suite (see section 2) that can be installed on systems running on Windows 2003/XP when configured in their Common Criteria (CC) evaluated configuration which is compliant with the Controlled Access Protection Profile (CAPP) version 1.d. The evaluated configuration of these operating systems is at Evaluation Assurance Level (EAL) 4 and augmented with the following additional assurances: Systematic Flaw Remediation (ALC\_FLR.3) and Highly Resistant (AVA\_VLA.4).

The operating system, hereafter referred to as OS, is responsible for multitasking operations so that other processes cannot intervene when the application is active at a particular instance in time. This ensures that multiple processes do not clash or overwrite into the data/object-space used or is being referred to by a different process. This assumes greater significance because not only should the data be secure all the time, the integrity of the data should also be guaranteed. Cryptographic module relies on the OS for ensuring the data integrity when the same piece of data is accessed by multiple processes concurrently. The OS also provides authentication, access control using Discretionary Access Control List (DACL), and auditing mechanism. The links to the validation report and security target for the CAPP-compliant OS are provided below:

Validation Report

[http://www.niap-ccevs.org/st/st\\_vid10184-vr.pdf](http://www.niap-ccevs.org/st/st_vid10184-vr.pdf)

Security Target

[http://www.niap-ccevs.org/st/st\\_vid10184-st.pdf](http://www.niap-ccevs.org/st/st_vid10184-st.pdf)

## 6. CRYPTOGRAPHIC KEY MANAGEMENT

The SecureVue cryptographic modules utilize the following cryptographic keys.

Table 5 - Central Cryptographic Keys

| Key                     | Size      | Strength | Storage           | Description                                                                                                                                                                                                                          |
|-------------------------|-----------|----------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AES Communication Key   | 192 bits  | 192 bits | Ephemeral, memory | <ul style="list-style-type: none"><li>Used to encrypt/decrypt all communication between Central and Regional/Data Collector</li><li>Generated each time during startup of Central</li></ul>                                          |
| AES Database Key        | 192 bits  | 192 bits | Disk, Plaintext   | <ul style="list-style-type: none"><li>Used to encrypt/decrypt of database information</li><li>Generated once during installation of the module</li></ul>                                                                             |
| AES File/Password Key   | 192 bits  | 192 bits | Disk, Plaintext   | <ul style="list-style-type: none"><li>Used to encrypt/decrypt passwords and user credentials</li><li>Generated once during installation of the module</li></ul>                                                                      |
| SSL Session Key         | 256 bits  | 256 bits | Ephemeral, memory | <ul style="list-style-type: none"><li>Used to encrypt/decrypt SSL session information</li><li>SSL session is used by Central to securely distribute the AES Communication Key, AES Database Key, and AES File/Password Key</li></ul> |
| SSL Authentication Key  | 160 bits  | 160 bits | Ephemeral, memory | <ul style="list-style-type: none"><li>Used to authenticate data passed within SSL session</li></ul>                                                                                                                                  |
| Central RSA Public Key  | 2048 bits | 112 bits | Disk, Plaintext   | <ul style="list-style-type: none"><li>Used to verify identity of Central during SSL session establishment</li></ul>                                                                                                                  |
| Central RSA Private Key | 2048 bits | 112 bits | Disk, Plaintext   | <ul style="list-style-type: none"><li>Used to authenticate itself to all components during SSL session establishment</li><li>Entered during initial Installation</li></ul>                                                           |
| Seed                    | 192 bits  | 192 bits | Ephemeral, memory | <ul style="list-style-type: none"><li>Used as input (Seed) into the Approved RNG</li></ul>                                                                                                                                           |
| Seed Key                | 192 bits  | 192 bits | Ephemeral, memory | <ul style="list-style-type: none"><li>Used as input (Seed key) into the Approved RNG</li></ul>                                                                                                                                       |

**Table 6 – Regional Cryptographic Keys**

| <i>Key</i>             | <i>Size</i> | <i>Strength</i> | <i>Storage</i>    | <i>Description</i>                                                                                                                                                                                                                                 |
|------------------------|-------------|-----------------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AES Communication Key  | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt all communication between Regional and Central/Data Collector</li> <li>Received from Central encrypted with SSL Session Key</li> </ul>                                              |
| AES Database Key       | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt of database information</li> <li>Received from Central encrypted with SSL Session Key</li> </ul>                                                                                    |
| AES File/Password Key  | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt passwords and user credentials</li> <li>Received from Central encrypted with SSL Session Key</li> </ul>                                                                             |
| SSL Session Key        | 256 bits    | 256 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt SSL session information</li> <li>SSL session is used by Regional to securely receive the AES Communication Key, AES Database Key, and AES File/Password Key from Central</li> </ul> |
| SSL Authentication Key | 160 bits    | 160 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to authenticate data passed within SSL session</li> </ul>                                                                                                                                              |
| Central RSA Public Key | 2048 bits   | 112 bits        | Disk, Plaintext   | <ul style="list-style-type: none"> <li>Used to verify identity of Central during SSL session establishment</li> <li>Entered during initial Installation</li> </ul>                                                                                 |
| Seed                   | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used as input (Seed) into the Approved RNG</li> </ul>                                                                                                                                                       |
| Seed Key               | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used as input (Seed key) into the Approved RNG</li> </ul>                                                                                                                                                   |

**Table 7 – Data Collector Cryptographic Keys**

| <i>Key</i>                   | <i>Size</i> | <i>Strength</i> | <i>Storage</i>    | <i>Description</i>                                                                                                                                                                                                           |
|------------------------------|-------------|-----------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AES Agent Communication Keys | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt all communication between Data Collector and Agents</li> <li>Generated by Data Collector and output (encrypted) to each Agent it communicates with</li> </ul> |
| AES Communication Key        | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt all communication between Data Collector and Central/Regional</li> <li>Received from Central encrypted with SSL Session Key</li> </ul>                        |
| AES File/Password Key        | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt passwords and user credentials</li> <li>Received from Central encrypted with SSL Session Key</li> </ul>                                                       |

| <i>Key</i>                     | <i>Size</i> | <i>Strength</i> | <i>Storage</i>    | <i>Description</i>                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|-------------|-----------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSL Session Key                | 256 bits    | 256 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt SSL session information</li> <li>SSL session is used by Data Collector to securely receive the AES Communication Key and AES File/Password Key from Central</li> <li>SSL session is also used by Data Collector to securely distribute the AES Agent Communication Keys to each Agent</li> </ul> |
| SSL Authentication Key         | 160 bits    | 160 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to authenticate data passed within SSL session</li> </ul>                                                                                                                                                                                                                                                           |
| Data Collector RSA Public Key  | 2048 bits   | 112 bits        | Disk, Plaintext   | <ul style="list-style-type: none"> <li>Used to verify identity of Data Collector during SSL session establishment with Agents</li> </ul>                                                                                                                                                                                                                        |
| Data Collector RSA Private Key | 2048 bits   | 112 bits        | Disk, Plaintext   | <ul style="list-style-type: none"> <li>Used to authenticate itself to Agents during SSL session establishment</li> <li>Entered during initial installation</li> </ul>                                                                                                                                                                                           |
| Central RSA Public Key         | 2048 bits   | 112 bits        | Disk, Plaintext   | <ul style="list-style-type: none"> <li>Used to verify identity of Central during SSL session establishment</li> <li>Entered during initial Installation</li> </ul>                                                                                                                                                                                              |
| Seed                           | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used as input (Seed) into the Approved RNG</li> </ul>                                                                                                                                                                                                                                                                    |
| Seed Key                       | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used as input (Seed key) into the Approved RNG</li> </ul>                                                                                                                                                                                                                                                                |

**Table 8 - Agent Cryptographic Keys**

| <i>Key</i>                    | <i>Size</i> | <i>Strength</i> | <i>Storage</i>    | <i>Description</i>                                                                                                                                                                                              |
|-------------------------------|-------------|-----------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AES Agent Communication Key   | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt all communication between Agent and Data Collector</li> <li>Received from Data Collector encrypted with SSL Session Key</li> </ul>               |
| SSL Session Key               | 256 bits    | 256 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to encrypt/decrypt SSL session information</li> <li>SSL session is used by Agent to securely receive the AES Agent Communication Key from Data Collector</li> </ul> |
| SSL Authentication Key        | 160 bits    | 160 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used to authenticate data passed within SSL session</li> </ul>                                                                                                           |
| Data Collector RSA Public Key | 2048 bits   | 112 bits        | Disk, Plaintext   | <ul style="list-style-type: none"> <li>Used to verify identity of Data Collector during SSL session establishment</li> <li>Entered during initial Installation</li> </ul>                                       |

| <i>Key</i> | <i>Size</i> | <i>Strength</i> | <i>Storage</i>    | <i>Description</i>                                                                               |
|------------|-------------|-----------------|-------------------|--------------------------------------------------------------------------------------------------|
| Seed       | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used as input (Seed) into the Approved RNG</li> </ul>     |
| Seed Key   | 192 bits    | 192 bits        | Ephemeral, memory | <ul style="list-style-type: none"> <li>Used as input (Seed key) into the Approved RNG</li> </ul> |

## 7. SELF-TESTS

SecureVue modules perform a number of power-up and conditional self-tests to ensure proper operation of the module. Power-up tests include cryptographic algorithm known answer tests (KATs) and integrity tests.

The integrity tests are performed using a HMAC-SHA digest calculated over the object code of each SecureVue module.

Power-up tests are run automatically when the each module is initialized. Additionally, power-up tests may be executed at any time by requesting the module to force re-run of self-tests.

No FIPS mode cryptographic functionality will be available until after successful execution of all power-up tests. Power-up self tests are run by each SecureVue module and since only a Crypto-Officer can launch SecureVue, the authentication of the same is delegated to the native windows Operating System.

A Crypto-Officer can also request the module to perform self-tests using the “FIPS Self-Test” button provided in the Setup -> Options window of the SecureVue Central GUI.

On-demand self-test can also be run as follows:

By executing a command on command-line - an operator user should have to be logged onto the box so as to be able to run the above command. Authentication would be performed by the native windows operating system.

- From the CLI, go to the install path of Central/Regional and type *MainEngine.exe -fips-self-test*
- From the CLI, go to the install path of Collector and type *syslogserver.exe -fips-self-test*
- From the CLI, go to the install path of SVAgent and type *SVAgent.exe -fips-self-test*

The failure of any power-up self-test or conditional (on-demand) self-test causes the Module to enter the Error State, and all cryptographic operations are disabled until the Module is reinitialized. When self-tests are being performed, no external data is taken as input and no data is sent as output. And when the module is in error-state, the process is immediately terminated. So, there is no data-output path.

Note the most likely cause of a self-test failure is memory or hardware errors. In practice a self-test failure means the module must exit and be restarted.

The following sections discuss the application’s self-tests in more detail.

## Power-Up Self-Tests

SecureVue modules boot-up process performs a suite of self tests to ensure the integrity and correct operation of the cryptographic algorithms. Power-up tests include cryptographic algorithm tests and integrity test. These tests are initiated automatically every time when each SecureVue module boots up (after power-off, reset, re-boot etc.). Availability of required Keys is verified as part of Power-Up Self-Tests. If these keys are not found or if any of the self-test fail, application does not initialize and enter in to an error state, preventing users from accessing the services and performing any cryptographic operations.

The following cryptographic algorithm self-tests are performed at power-up:

- AES Known Answer Test
- HMAC Known Answer Test
- RNG Known Answer Test
- RSA Encrypt/Decrypt Known Answer Test
- RSA Pairwise Consistency test
- SHS Known Answer Test

All Power-Up self-tests must be passed before a user can utilize the cryptographic services. Also self-tests can be run on-demand by re-booting the cryptographic module.

## Software Integrity Test

Only a Crypto Officer who has physical access to the system can install SecureVue module. To protect the Package integrity, 'sha256' digest files will be made available to the customers when they contact eIQ Support, or as identified in this Security Policy. To verify the integrity of the package, user can generate a sha256 digest for the downloaded package and compare the generated digest with the digest fetched from eIQ Support, or as identified in this Security Policy.

In addition, each module performs a software integrity test as part of power-up integrity test. Each Cryptographic module performs its own integrity checks by computing the HMAC-SHA digests of all the software executables within its logical boundary. The computed digests are compared against the known digest. If any of the digest comparison fails, then SecureVue module shuts itself down.

Only when the integrity check of each SecureVue module passes, does each SecureVue module proceed to perform the Power-Up Self-Tests. Only when the Power-Up self-Tests succeed, does each SecureVue module proceed to the operational state.

**NOTE:** [Appendix-A](#) lists the sha256 digests of the SecureVue modules distribution.

## **Critical Functions Test**

Encryption Key Sanity test is performed for the Critical Functions test. This test simply encrypts a string and then decrypts and compares it to the original string to ensure they match.

## **Conditional Self-Tests**

### **Software/Firmware Load Test**

Software load test is not applicable as it is not supported by module.

### **Manual Key Entry Test**

Neither Cryptographic keys nor the cryptographic key components can be manually entered into the SecureVue module.

As such, manual key entry test is not applicable.

### **Continuous Random Number Generator Test**

The module performs a Continuous Random Number Generator Test on both the Approved and non-Approved RNG's. This test is performed when the AES Communications Key and AES Agent Communication Keys are generated by Central and Data Collector, respectively. This test is also performed when the AES Database key and/or AES File/Password Key is generated at Central.

### **Bypass Test**

Bypass test is not applicable as it is not supported by module.



## **8. MITIGATION OF OTHER ATTACKS**

The Mitigation of Other Attacks area of FIPS 140-2 is not applicable as the module does not claim to mitigate attacks outside the scope of FIPS 140-2.

## 9. Appendix-A SHA256 Digests of SecureVue Modules

SHA256 digests of SecureVue module distribution files are listed below:

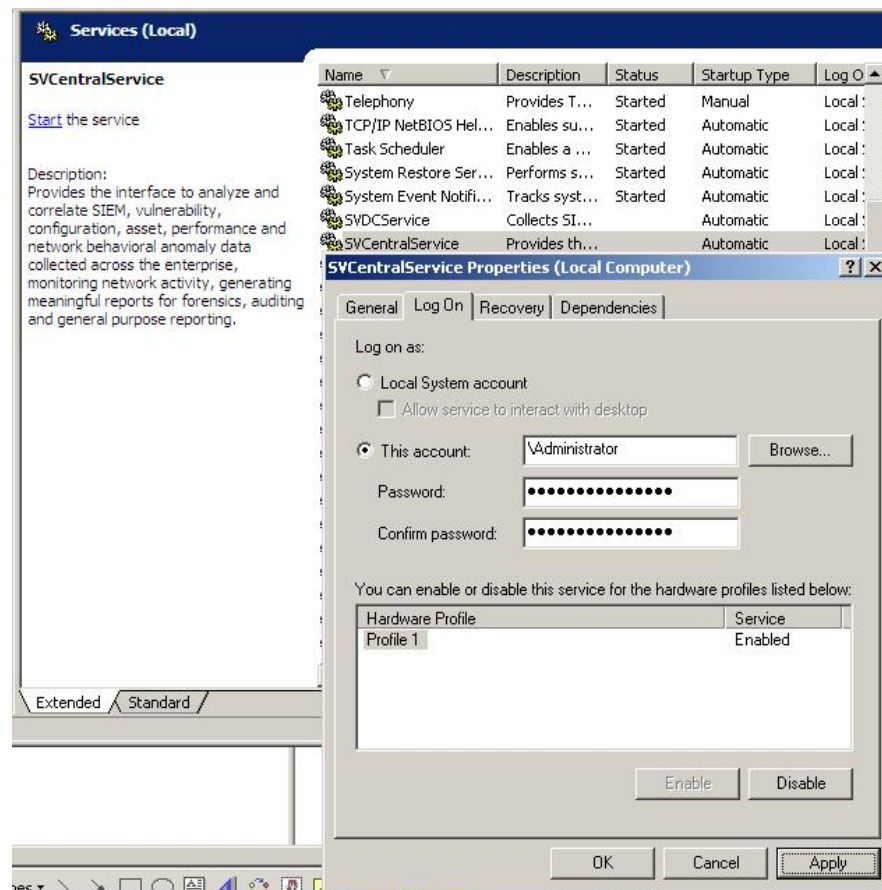
- SecureVueCentralSetup\_Win32\_3.1.2.3.exe  
**6e24d960c1a9d2b44da3593809f64a4a6758e55704d9debfbfd828d30482f0e51**
- SecureVueRegionalSetup\_Win32\_3.1.2.3.exe  
**c91d580f3940a5890b175712f6d55a4e4b4a7ea2dbc6ae3b8ef0475df523ba25**
- SecureVueDCSetup\_Win32\_3.1.2.3.exe  
**bbe7bba00c847821586df41d6a4af81c6c0c8841161d9e98d067e3d60228ad73**
- SecureVueAgentSetup\_Win32\_3.1.2.3.exe  
**140cf4265c70ec25560bb312ca0bbf6b1c57a6ab3088133174f00178af78ab95**

## 10. Appendix-B Administering Services & Folder Permissions

### Services

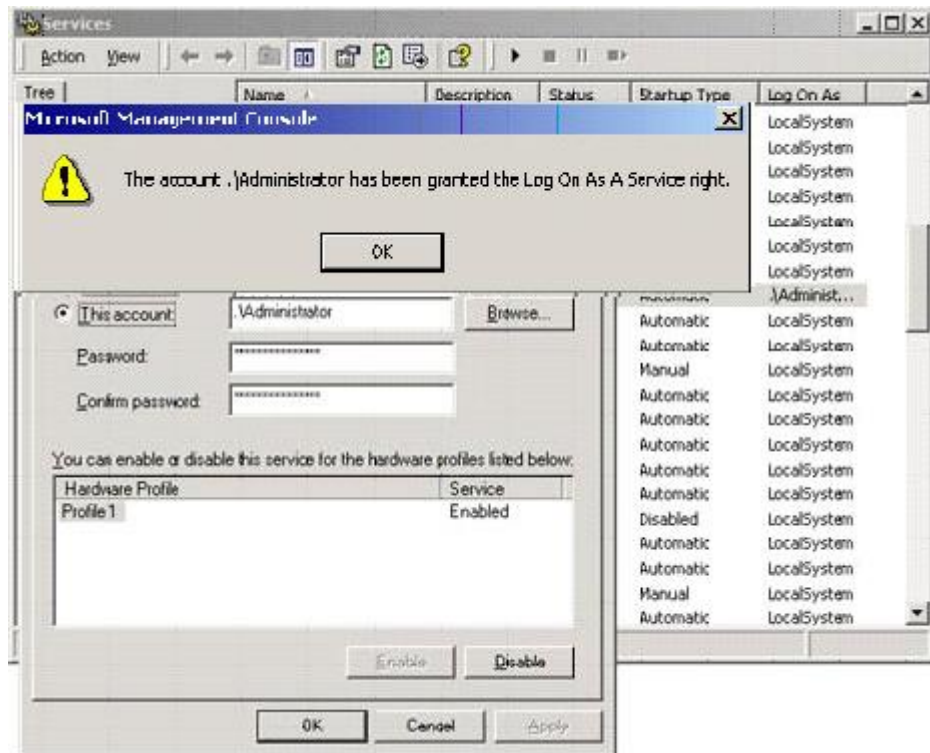
Go to Services in the Administrative Tools of the Control Panel and right click on SVCentralService and select Properties -> Log On tab.

- You will be prompted with the Log On properties window as shown below.
- Delete and retype the 'This account' username and Password of an account with administrative privileges within your messaging environment.
- Then click Apply.



### Granting Privilege

A dialog box will pop-up telling you the account (Username you used with Administrative privileges) has been granted Log On as a Service right. Click OK. (See screen shot attached below).



### Verifying Granted Privileges

You are now returned to a window like below. Click OK and then start the appropriate service. Also check to ensure that the service is set to automatically startup.

### Granting Permissions

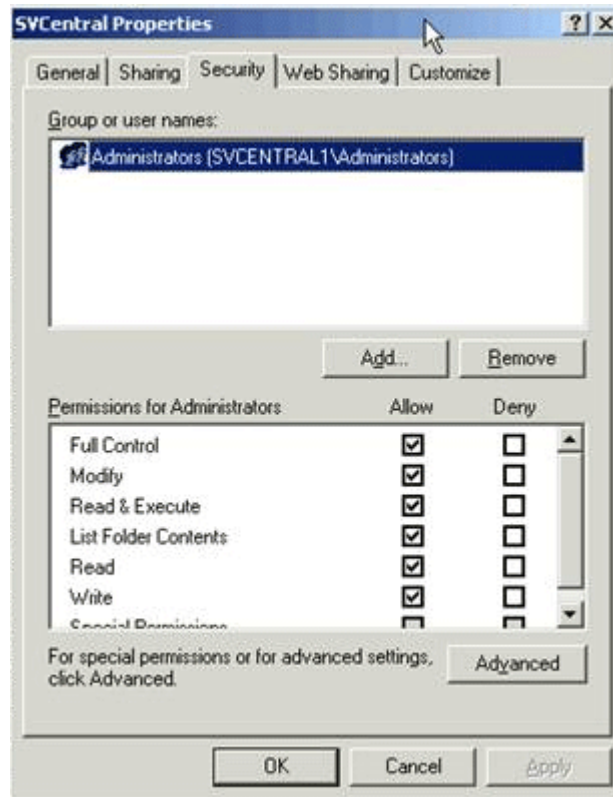
The above mentioned administrative account 'Administrator' must have all permissions for its modules (Central, Regional, Data Collector and SVAgent) on the Security permissions post-installation to ensure SecureVue works in Secure Mode of Operation.

SecureVue Modules -- OS folder permissions and audit settings needed for FIPS Approved Mode of Operation:

#### Central:

The default SecureVue Central module install path folder must be accessible by a Crypto Officer i.e. Windows Server 2003 System User with Administrator role. This user should be given 'all' the permissions. In other words, select all the checkboxes under the 'Allow' category within the 'Security' tab of the SecureVue installation folder properties window. Please also deselect/remove all the checkboxes under the 'Deny' category in the same window.

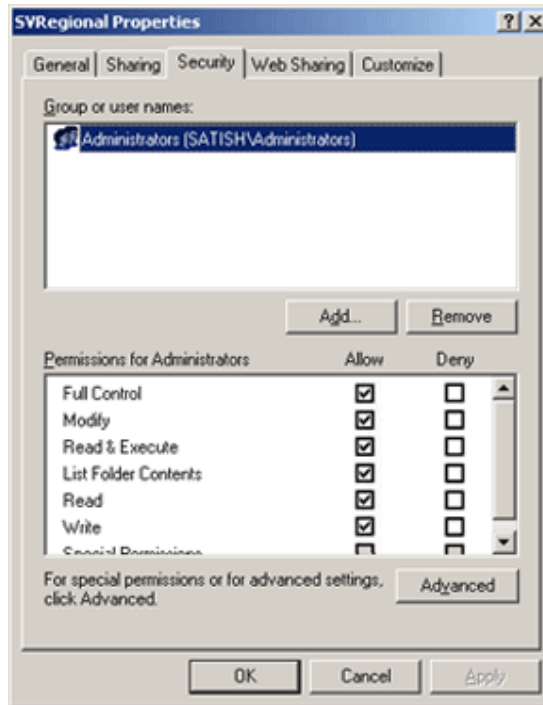
Please see below for a screenshot depicting clearly that all the checkboxes under 'Allow' be granted and not select any of the checkboxes under 'Deny'.



### Regional:

The default SecureVue Regional module install path folder must be accessible by a User with Administrator role. This user should be given 'all' the permissions. In other words, select all the checkboxes under the 'Allow' category within the 'Security' tab of the SecureVue module installation folder properties window. Please also deselect/remove all the checkboxes under the 'Deny' category in the same window.

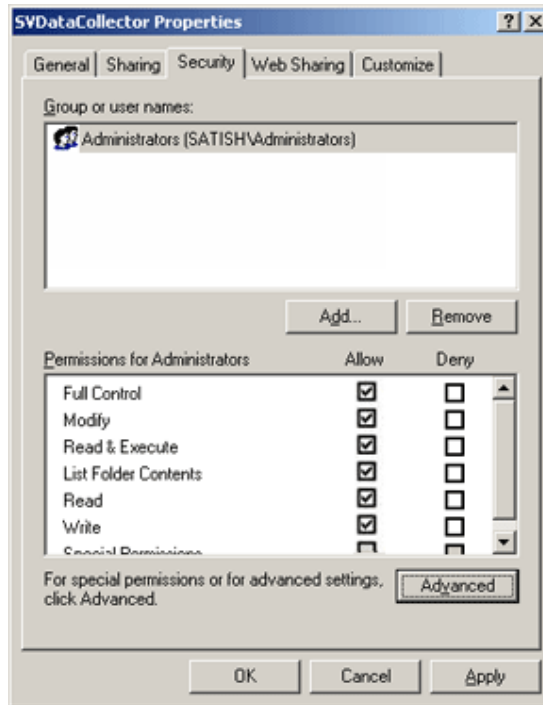
Please see below for a screenshot depicting clearly that all the checkboxes under 'Allow' be granted and not select any of the checkboxes under 'Deny'.



### Collector:

The default SecureVue Collector module install path folder must be accessible by a User with Administrator role. This user should be given 'all' the permissions. In other words, select all the checkboxes under the 'Allow' category within the 'Security' tab of the SecureVue module installation folder properties window. Please also deselect/remove all the checkboxes under the 'Deny' category in the same window.

Please see below for a screenshot depicting clearly that all the checkboxes under 'Allow' be granted and not select any of the checkboxes under 'Deny'.



### SVAgent:

The default SecureVue SVAgent module install path folder must be accessible by a User with Administrator role. This user should be given 'all' the permissions. In other words, select all the checkboxes under the 'Allow' category within the 'Security' tab of the SecureVue module installation folder properties window. Please also deselect/remove all the checkboxes under the 'Deny' category in the same window.

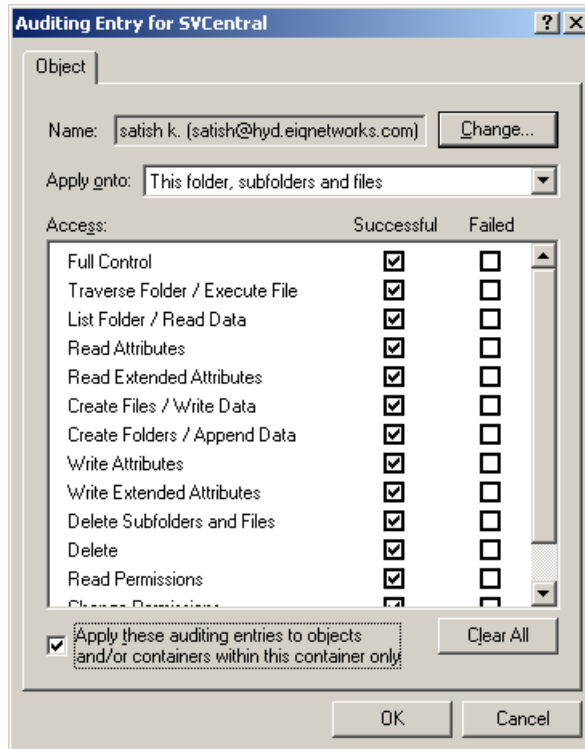
Please see below for a screenshot depicting clearly that all the checkboxes under 'Allow' be granted and not select any of the checkboxes under 'Deny'.



**NOTE:**

- Only the System Administrator is granted full permissions recursively down the installation folder.
- The System Administrator should be granted file/folder audit permissions too.
  - To enable auditing on a folder, open the folder's properties dialog box, select the Security tab, click Advanced, and select the Auditing tab of the Advanced Security Settings window.
  - Click Add and specify the details of the user account (System Administrator) activity that is to be audited for tracking purposes.
  - Select the Auditing entries that are to be applied for objects within the specified folder.
  - Click OK. (Refer screen-shot below)





- All other users should be forbidden **every** kind of access to these folders.

## 11. Appendix-C Executables

The following lists identify the specific executable files that comprise the cryptographic boundary of each SecureVue module.

### Central/Regional

1. MainEngine.exe
2. MonitoringEngine.exe
3. FileSync.exe
4. ParserEngine.exe
5. ForensicsEngine.exe
6. Topology.exe
7. VizConsole.exe

### Data Collector

1. syslogserver.exe
2. HostCollector.exe
3. configmon.exe
4. SnmpMon.exe
5. Leaserver.exe
6. WatchDog.exe
7. MonitoringEngine.exe
8. PatchUpdater.exe
9. SNMPTrapAgent.exe
10. DCConf.exe

### Agent

1. SVAgent.exe
2. HostCollector.exe