RSA NETWITNESS® SUITE

Security Configuration Guide

for Version 11.1

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

Security Configuration Guide Overview

This guide provides information about the security configuration settings and security best practices for RSA NetWitness Suite.

This guide applies to NetWitness Suite version 11.0 or later. There will be periodic updates made to the content.

Anyone using this guide should possess experience as a network engineer, equivalent to at least that of a journeyman, and also have a strong understanding of network concepts and TCP/IP communications.

Security Configuration Settings

This topic describes information about various security configuration settings that are designed to help you securely operate RSA NetWitness Suite.

You can adjust the following security configuration settings:

- Access Control Settings
- Log Settings
- Communication Security Settings
- Data Security Settings
- Alert System Settings
- Other Security Considerations

Access Control Settings

Access control settings are designed to enable the protection of resources against unauthorized access or by external components.

- User Authentication
- User Authorization
- Component Authentication

User Authentication

User authentication settings are designed to control the process of verifying an identity claimed by a user for accessing RSA NetWitness Suite.

NetWitness Suite Core Trusted Connection

NetWitness Suite Core 11.1 has the ability to connect and authenticate over SSL without having to provide user account information on the service itself. This feature is only available over the native port and not the REST interface. For more information on trusted connection, see *Host and Services Getting Started Guide*.

User Accounts

The following table identifies the default RSA NetWitness Suite user roles including the Administrator (admin) account and several service accounts. When deploying, you must enter a password for the system administrator account and all the service accounts. For more information on passwords and password strength, see "Settings Tab" Help topic in *System Security and User Management Guide*.

Note: Custom roles can be added as required. For instructions, see "Add a Service User Role" topic in *Host and Services Configuration Guides*.

User Roles	Description
Administrators	Full system access
Operators	Access to configurations but not to meta and session content.
Analysts	Access to meta and session content but not to configurations.
SOC_Managers	Same access as Analysts plus additional permission to handle incidents.
Malware_Analysts	Access to malware events and to meta and session content.
Data_Privacy_Officers	Access to meta and session content as well as configuration options that manage obfuscation and viewing of sensitive data within the system (see Data Privacy Management).
Respond_Adminstrator	Access to all Respond server and Incidents permissions.

Note: By default, the Administrator user is assigned to each NetWitness Suite service.

Configuring New Accounts

Each RSA NetWitness Suite user must have an account to log on to the UI. For instructions on adding new user accounts, see "Manage Users with Roles and Permissions" Help topic in *System Security and User Management Guide*.

Caution: RSA recommends that you ensure that users are approved by the company for logging on to the system before creating an account for them. Even if users are approved, RSA recommends that you only assign the minimum set of access permissions that enable the users to perform their jobs.

Authentication Configuration

User authentication settings are designed to control the process of verifying an identity claimed by a user for accessing NetWitness Suite. For more information, see "Set Up System Security" topic in the *System Security and User Management Guide*.

Below are recommendations for some of the configurations:

- **Default System Administrator Account**: RSA recommends that you instruct RSA NetWitness Suite administrators on your corporate IT policy and security best practices to generate and manage passwords for the default System Administrator account. RSA recommends that you change the default System Administrator password and the admin passwords for the service accounts per your company's password policy. For more information on password strength settings, see "Password Strength" topic in the *System Security and User Management Guide*. You should change the System Administrator password using the Admin user preferences. For instructions on how to change the password, see "Change the Default admin Passwords" in the *System Security and User Management Guide*.
- **External Authentication**: RSA NetWitness Suite supports external authentication. For more information, see "Configure External Authentication" topic in the *System Security and User Management Guide*.

User Passwords

NetWitness Suite Users

Administrators can set the appropriate level of password strength for the user and can force users to change their passwords when password strength policy changes. Administrators can specify global default user password expiration period and the notification period for the password expiry. For more information, see "Configure System-Level Security Settings" topic in the *System Security and User Management Guide*.

The following table shows the default security parameters settings for passwords.

Caution: RSA recommends that you change these settings in accordance with your corporate policy. Users must ensure the idle period and session time-out is specified.

Parameter	Default Setting
Global Default User Password Expiration Period	0
Notify User <n> Days Prior to Password Expiry	5

NetWitness Suite Core Service Users

Administrators can change the password of a service user and replicate the new password to all the NetWitness Suite Core services with the defined user account. For more information, see "Change a Service User Password" topic in the *Host and Services Configuration Guides*.

You can also change your password from the Preferences panel in the Profile view. For more information, see "Profile View Preferences Panel" topic in the *NetWitness Suite Getting Started Guide*.

Security Parameter Settings

The following table shows the default security parameters settings.

Caution: RSA recommends that you change these settings in accordance with your corporate policy.

Parameter	Default Setting
Lockout Period	20 minutes
Idle Period	10 minutes
Session Timeout	480 minutes

Parameter	Default Setting
Max Login Failures	5

For more information on security parameter settings, see "Configure System-Level Security Settings " topic in the *System Security and User Management Guide*.

User Authorization

User authorization settings are designed to control rights or permissions that are granted to a user for accessing a resource managed by RSA NetWitness Suite.

Access Roles

RSA NetWitness Suite allows you to create access roles that you can assign to users. Each access role is mapped to a list of user authorization settings.

For more information, see the following NetWitness Suite 11.1 topics:

- "Role Permissions" in the *Alerting Using ESA Guide*.
- "Manage Users with Roles and Permissions" in the *System Security and User Management Guide*.

Note: Additionally, RSA NetWitness Suite recommends that you review users' task permissions on a routine basis to ensure that each user is granted the correct task permissions.

RSA NetWitness Suite allows access roles to be assigned to users through external group membership or directly to user accounts. RSA recommends that you assign permissions through group membership and not assign permissions directly to user accounts. For more information, see "Map User Roles to External Groups" Help topic in the *System Security and User Management Guide*.

The user roles assigned also control permissions that are granted to accounts that need access to a specific component of NetWitness Suite.

Component Authentication

This topic describes Component authentication settings control the process of verifying an identity claimed by an external or internal system or component.

Host Configuration and Service Authentication

When you install or upgrade to RSA NetWitness® Suite 11.0 or later, trusted connections are established by default with two settings:

1. SSL is enabled.
2. NetWitness Server is connected to core services using the encrypted SSL port.

RSA NetWitness Suite allows secure authentication services for the following hosts as SSL is enabled by default:

- Decoder
- Log Decoder
- Concentrator
- Broker
- Log Collector
- Archiver
- ESA
- Malware Analysis
- Endpoint

Note: By default all the services on the hosts have SSL enabled.

For more information, see Help topic in the *Host and Service Configuration Guides*.

Changing Credentials for Default Configuration Service Accounts

For instructions on resetting the password for the admin of the host service accounts, see "Users Tab" topic in the *Host and Services Configuration Guides*.

Note: The default user name that the host service accounts admin cannot be modified.

Configuring Live Account Authentication

RSA NetWitness Suite supports secure authentication for the Live account connection to Content Management System (CMS) as the SSL is enabled by default. The default communications port on the CMS is 443. For instructions on configuring this setting, see "Configure Live Settings" topic in the *System Configuration Guide*.

Configuring Lockbox Authentication

Lockbox provides an encrypted file that Warehouse Connector or Log Collector uses to store and protect sensitive data. You need to create the lockbox by providing a lockbox password while configuring the Warehouse Connector or Log Collector for the first time. For more information on lockbox setup, see the following topics:

- "Log Collector - Step 3: Set Up a Lockbox" in the *Log Collection Guides*.
- "Warehouse Connector - Step 2: Create Lockbox" in the *Host and Services Configuration Guides*.

Display Logon Banner for Remote SSH Connections

RSA NetWitness Suite allows you to customize the logon banner to display standard government or corporate warning signs for SSH remote connections to the hosts. An example message would be the following:

"This system is private. Use or misuse may be logged and invalid access pursued."

1. Log on to the appliance using root credentials.
2. Type **cd /etc/** to switch to the **/etc/** directory.
3. Edit the **/etc/issue.net** file with the required banner text.
4. Save the changes and exit.
5. Type **cd /etc/ssh** to switch to the **/etc/ssh** directory.
6. Edit the **/etc/ssh/sshd_config** file to remove the comment for the banner and provide the location of the banner text file (For example, **/etc/issue.net**).
   The following file is an example of an **sshd.config** file before being modified:

   ```
   # no default banner path
   #Banner none
   ```

   The following file is an example of an **sshd.config** file after being modified:

   ```
   # no default banner
   #Banner /etc/issue.net
   ```

7. Save the changes and exit.
8. Type **service sshd restart** in order to restart the sshd service.

Log Settings

A log is a chronological record of system activities that enables the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event in a security-relevant transaction.

Global Audit Logging provides NetWitness Suite Auditors with consolidated visibility into user activities within NetWitness Suite in real-time from one centralized location. NetWitness Suite audit logs collect in a centralized system that converts them into the required format and forwards them to an external syslog system. The external syslog system can be a third-party syslog server or a Log Decoder. For more information, see "Global Audit Logging Overview" topic in the *System Configuration Guide*.

Log Description

The following table shows the security-relevant logs provided by RSA NetWitness Suite.

Component	Reference
Appliance and Service Logs	See "Services Explore View and Services Logs View" topics in the *Host and Services Configuration Guides* and "Configure Log File Settings" topic in the *System Configuration Guide*.
Audit Logs	See " Configure Global Audit Logging" topic in *System Configuration Guide*.
Syslogs	See " Configure Syslog and SNMP Settings" topic in the *System Configuration Guide*.

Log Management and Retrieval

For more information on:

- Log settings: See "Configure Log File Settings" topic in the *System Configuration Guide*.

  Note: RSA recommends that you set the maximum log file size in accordance to your corporate policy.

- Log forwarding: See "Set Syslog Forwarding" topic in the *Host and Services Configuration Guides*.
- Setting log overrides:
  You may override the default logging levels if you want to include messages generated by specific modules.

`Syntax: <module>=<level>`

`SDK-Language=none`

Where level is one or more of `"none|debug|info|warning|failure|audit|all"`, all options must be separated by a pipe |

none and all are mutually exclusive with each other and all other options.

Overrides are useful for query auditing (that is, those modules that begin with SDK-) or for debugging by module (that is, Index)

- Data
- Engine
- Index
- Network
- Packet
- Parse
- Decoder
- Rules
- Concentrator
- Appliance
- SDK
- SDK-Query
- SDK-Values
- SDK-Language
- SDK-Info
- SDK-Session
- SDK-Timeline
- SDK-Content
- SDK-Search

Note: RSA recommends that you restrict permissions to the log files folder to the appropriate user.

Communication Security Settings

Communication security settings are designed to enable the establishment of secure communication channels between RSA NetWitness Suite components, as well as between RSA NetWitness Suite components and external systems or components.

Port Usage

To help ensure security, RSA recommends that you configure your firewall rules and access control lists to expose only the ports and protocols necessary for the operation of RSA NetWitness Suite. The services, such as Reporting Engine, Respond Service, Malware, Log Collector, Live account, Broker, Concentrator, Decoder, and Log Decoder, use specific TCP ports to communicate with each other and the following:

- Web user client interfaces
- Live CMS
- LDAP synchronization
- Third-party email server
- NetWitness Suite console

All communication from NetWitness Suite is over the native NetWitness Suite Core ports as against the REST API ports. The additional native NetWitness Suite Core port per appliance allows an administrator to enable secure (SSL) network communications while still being able to utilize non-secure (HTTP and NetWitness Suite Core native) connectivity methods for communication between services that are present on the same system. Administrators can toggle the ports on and off to support only SSL, only non-SSL, or both.

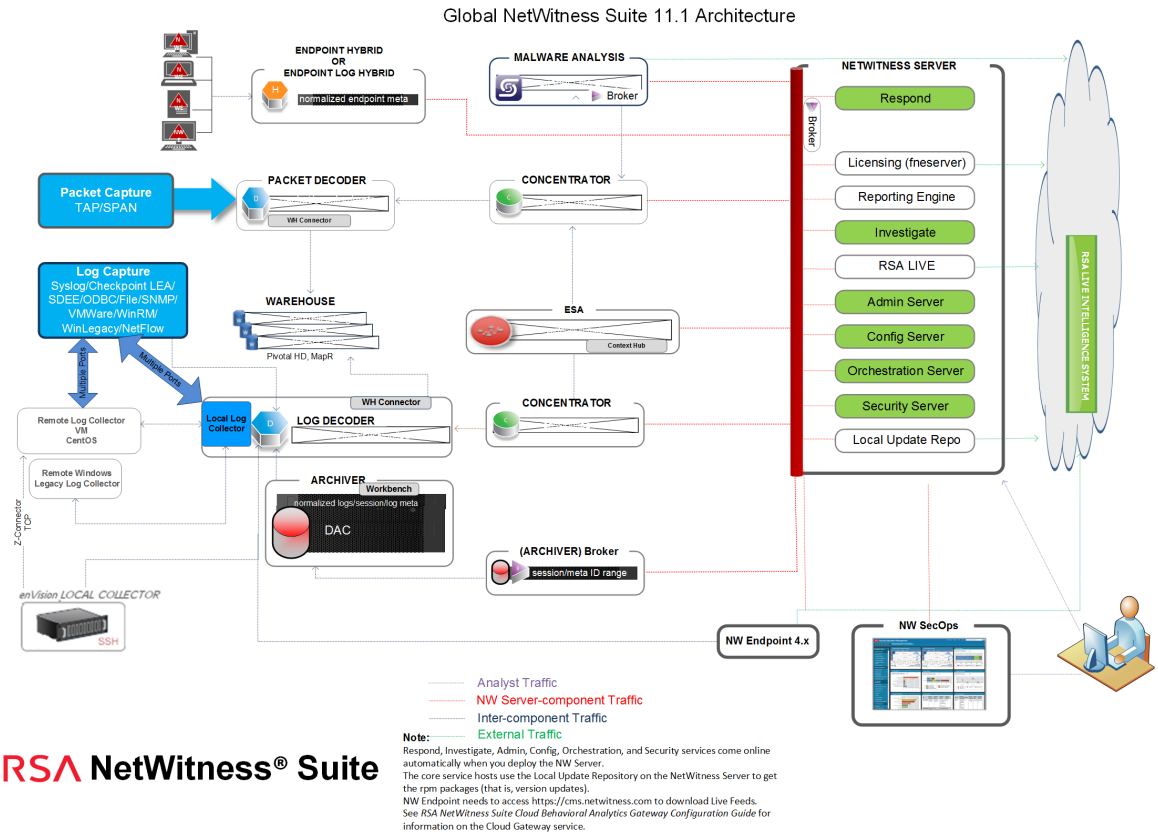
Refer to the following diagram and port table to ensure that all the relevant ports are opened for components in your NetWitness Suite deployment to communicate with each other.

For more information on individual Endpoint Architectural diagrams, see Communication Security Settings at the end of this topic.

NetWitness SuiteNetwork Architecture Diagram

The following diagram illustrates the NetWitness Suite network architecture including all of its component products.

Note: NetWitness Suite core hosts must be able to communicate with the Netwitness Server (Primary Server in a multiple server deployment) through UDP port 123 for Network Time Protocol (NTP) time synchronization.



RSA NetWitness® Suite

Comprehensive List of NetWitness Suite Host and Service Ports

Note: 1.) For ports used in event collection through the Netwitness Logs, see the "The Basics" in the *RSA NetWitness Suite Log Collection Deployment Guide*.

This section contains the port specifications for the following hosts.

NW Server Host	Log Collector Host
Archiver Host	Log Decoder Host
Broker Host	Log Hybrid Host
Concentrator Host	Malware Host
Endpoint Hybrid/Endpoint Log Hybrid Host	Packet Decoder Host
Event Stream Analysis Host	Packet Hybrid Host

NW Server Host

Source Host	Destination Host	Destination Ports	Comments
Admin Work-station	NW Server	TCP 443, 80	nginx - NetWitness UI
Admin Workstation	NW Server	TCP 15671	RabbitMQ Management UI
NW Hosts	NW Server	TCP 15671	RabbitMQ Management UI
Admin Work-station	NW Server	TCP 22	SSH
NW Hosts	NW Server	TCP 4505, 4506	Salt Master Ports
NW Server	NW Server	TCP 50003, 50103, 56003	Broker Ports
NW Server	NW Server	TCP 5671	RabbitMQ-amqp
NW Server	NW Server	UDP 50514	Audit Ports
NW Server	NW Server	TCP 7000, 7003, 7009, 7010	Launch Ports
NW Server	NW Server	TCP 50006, 50106, 56006	NetWitness Appliance Ports
NW Hosts	NW Server	UDP 123	NTP
NW Hosts	NW Server	TCP 27017	MongoDB
NW Server	NW Server	UDP 123	NTP
NW Server	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
NW Server	NW Endpoint	TCP 443, 9443	For NW Endpoint 4.x integrations

Archiver Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Archiver	TCP 15671	RabbitMQ Management UI
Admin Workstation	Archiver	TCP 22	SSH
NW Server	Archiver	TCP 56008 (SSL), 50008 (Non-SSL), 50108 (REST)	Archiver Application Ports
NW Server	Archiver	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Archiver	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
NW Server	Archiver	TCP 514, 6514, 56007 (SSL), 50007 (Non-SSL), 50107 (REST), UDP 514	Workbench Application Ports
Archiver	Archiver	UDP 50514	Audit Data
Archiver	Archiver	UDP 123	NTP
Archiver	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Broker Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Broker	TCP 15671	RabbitMQ Management UI

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Broker	TCP 22	SSH
NW Server	Broker	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
NW Server	Broker	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Broker	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Broker	Broker	UDP 50514	Audit Data
Broker	Broker	UDP 123	NTP
Broker	NW Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Concentrator Host

Source Host	Destination Host	Destination Ports	Comments
Admin Work-station	Concentrator	TCP 15671	RabbitMQ Management UI
Admin Work-station	Concentrator	TCP 22	SSH
NW Server	Concentrator	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
Malware	Concentrator	TCP 56005 (SSL)	Malware
NW Server	Concentrator	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports

Source Host	Destination Host	Destination Ports	Comments
NW Server	Concentrator	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Concentrator	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
Concentrator	Concentrator	UDP 50514	Audit Data
Concentrator	Concentrator	UDP 123	NTP

Endpoint Hybrid or Endpoint Log Hybrid

Source Host	Destination Host	Destination Ports	Comments
Endpoint 11.1 Agent	Endpoint Hybrid or Endpoint Log Hybrid	TCP 443	NGINX HTTPS
Endpoint 11.1 Agent	Log Decoder or Virtual Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windows Log Collection
Endpoint Server	Log Decoder (External)	TCP 50102, 56202, 50202	To forward meta to an external Log Decoder
NW Server	Endpoint Hybrid or Endpoint Log Hybrid	TCP 7050	UI web traffic
Endpoint Hybrid or Endpoint Log Hybrid	NW Server	TCP 5671	Message Bus
Endpoint Server	NW Server	TCP 27017	MongoDB

Endpoint Hybrid or Endpoint Log Hybrid with NetWitness Endpoint 4.4

Source Host	Destination Host	Destination Ports	Comments
NW Console Server (4.4.0.2 or later)	Endpoint Hybrid	TCP 443	NGINX HTTPS
Meta Service	Log Decoder	TCP 50102, 56202, 50202	NGINX HTTPS To forward meta to a Log Decoder Endpoint Hybrid or Endpoint Log Hybrid with NWE 4.4

Event Stream Analysis (ESA) Host

Source Host	Destination Host	Destination Ports	Comments
Admin Work-station	ESA	TCP 15671	RabbitMQ Management UI
Admin Work-station	ESA	TCP 22	SSH
NW Server, ESA Sec-ondary	ESA Primary	TCP 27017	MongoDB
NW Server	ESA Primary	TCP 7005	Context Hub Launch Port - (ESA Primary)
NW Server	ESA	TCP 50030 (SSL)	ESA Application Port
NW Server	ESA	TCP 50035 (SSL)	ESA Application Port
NW Server	ESA	TCP 50036 (SSL)	ESA Application Port
NW Server	ESA	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
ESA	cms.netwitness.com	TCP 443	Live

Source Host	Destination Host	Destination Ports	Comments
ESA	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations
ESA	Active Directory	636 (SSL)/389 (Non-SSL)	
NW Server	ESA	80 (HTTP)/ 443 (HTTPS)(REST)	
ESA Primary	Archer	443 (SSL)/80 (Non-SSL)	
ESA Primary	ESA Primary	TCP 7007	Launch Port
ESA Primary	ESA Primary	UDP 50514	Audit Data
ESA Primary	ESA Primary	UDP 123	NTP

Log Collector Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Collector	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Collector	TCP 22	SSH
Log Collector	Log Event Sources	See *Log Collection Configuration Guide*. (missing or bad snippet)	
Log Event Sources	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Log Collection Ports

Source Host	Destination Host	Destination Ports	Comments
Log Event Sources	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Log Collection FTP/S Ports
NW Server	Log Collector	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Collector	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Collector	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Log Collector	Log Collector	UDP 50514	Audit Data
Log Collector	Log Collector	UDP 123	NTP
Log Collector	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC installations

Log Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Decoder	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Decoder	TCP 22	SSH
Log Decoder	Log Event Sources	See *Log Collection Configuration Guide*. (missing or bad snippet)	

Source Host	Destination Host	Destination Ports	Comments
Log Event Sources	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Decoder	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Decoder	TCP 56002 (SSL), 50002 (Non-SSL), 50102 (REST)	Log Decoder Application Ports
NW End-point	Log Decoder	56202	Log Decoder Application Ports
NW Server	Log Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Decoder	TCP 5671	RabbitMQ (AMQPS) mes-sage bus for all NW hosts.
Log Decoder	Log Decoder	UDP 50514	Audit Data
Log Decoder	Log Decoder	UDP 123	NTP
Log Decoder	Log Col-lector	TCP 6514	
Log Decoder	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Log Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Log Hybrid	TCP 15671	RabbitMQ Management UI
Admin Workstation	Log Hybrid	TCP 22	SSH
Log Collector	Log Event Sources	See *Log Collection Configuration Guide*. (missing or bad snippet)	
Log Event Sources	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Log Collection Ports
Log Event Sources	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Log Collection FTP/S Ports
NW Server	Log Hybrid	TCP 56001 (SSL), 50001 (Non-SSL), 50101 (REST)	Log Collector Application Ports
NW Server	Log Hybrid	TCP 56002 (SSL), 50002 (Non-SSL), 50102 (REST)	Log Decoder Application Ports
NW Endpoint	Log Hybrid	56202	Log Decoder Application Ports
NW Server	Log Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Log Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Log Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.

Source Host	Destination Host	Destination Ports	Comments
Log Hybrid	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Malware Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Malware	TCP 15671	RabbitMQ Management UI
Admin Workstation	Malware	TCP 22	SSH
NW Server	Malware	TCP 60007	Malware Application Ports
NW Server	Malware	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Malware	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
NW Server	Malware	TCP 5432	Postgresql
NW Server	Malware	TCP 56003 (SSL), 50003 (Non-SSL), 50103 (REST)	Broker Application Ports
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Community evaluation / Opswat
Malware	Malware	UDP 50514	Audit Data

Source Host	Destination Host	Destination Ports	Comments
Malware	Malware	UDP 123	NTP
Malware	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Packet Decoder Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Decoder	TCP 15671	RabbitMQ Management UI
Admin Workstation	Packet Decoder	TCP 22	SSH
NW Server	Packet Decoder	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Decoder	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Decoder	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Decoder	Packet Decoder	UDP 50514	Audit Data
Packet Decoder	Packet Decoder	UDP 123	NTP
Packet Decoder	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Packet Hybrid Host

Source Host	Destination Host	Destination Ports	Comments
Admin Workstation	Packet Hybrid	TCP 15671	RabbitMQ Management UI
Admin Workstation	Packet Hybrid	TCP 22	SSH
NW Server	Packet Hybrid	TCP 56004 (SSL), 50004 (Non-SSL), 50104 (REST)	Packet Decoder Application Ports
NW Server	Packet Hybrid	TCP 56005 (SSL), 50005 (Non-SSL), 50105 (REST)	Concentrator Application Ports
NW Server	Packet Hybrid	TCP 56006 (SSL), 50006 (Non-SSL), 50106 (REST)	NetWitness Appliance Ports
NW Server	Packet Hybrid	TCP 5671	RabbitMQ (AMQPS) message bus for all NW hosts.
Packet Hybrid	NFS Server	TCP 111 2049 UDP 111 2049	iDRAC Installations

Note: For the latest architecture and port usage information, see "Network Architecture and Ports" topic in the *Deployment Guides*.

Topics

- Network Encryption

Network Encryption

You can configure RSA NetWitness Suite to send or receive data from external data sources.

Note: RSA recommends that whenever you have the option to choose between unsecured and secured versions of a communication protocol, you choose the secured version.

NetWitness Suite Web Server Communications

The RSA NetWitness Suite UI or web server which communicates with the Live Service (CMS) over port 443 using the HTTPS protocol.

Note: During installation, the system is engineered to set the default communication protocol to HTTPS over port 443.

Reporting Engine, ESA and Warehouse Connector : External Communication

RSA recommends that you use the secure tcp protocol and enable an SSL connection while configuring Reporting Engine, ESA, Warehouse Connector, Licensing, and Malware.

For more information on Reporting Engine, see "Step 4: Configure Output Actions" topic in the *Host and Services Configuration Guides*.

For more information on Malware external communication, see " Step 1. Configure Malware Analysis Operating Environment" topic in the *Host and Services Configuration Guides*.

For more information on ESA, see " Notification Methods" topic in the *Alerting Using ESA Guide*.

For more information on the Warehouse Connector, see "Configure Warehouse Connector" topic in the *Host and Services Configuration Guides*.

For more information on Licensing, see "Configure NetWitness Suite Notifications" topic in the *Alerting Using ESA Guide*.

Log Collector Service

To help secure communication between the Log Collector service running on the Log Decoder and the event sources, RSA recommends the protocols in the following table

Event Source	Protocol	Resources
File	SFTP, SCP, FTPS	For more information, see " File Collection Protocol Configuration" topic in the *Log Collection Guides*.
ODBC	ODBC	For more information on configuring an ODBC event source, see "ODBC Collection Configuration" topic in the *Log Collection Guides*. **Note:** Note: Depending on the event source, administrators can configure additional progress driver parameter for secure connections. For more information, see Progress document at https://www.progress.com/odbc/resources/documentation/books-and-readme-file. For more information on using a Certificate, see the certificate creation kit at http://openssl.org/. For more information on securing communication with SQL Server, Oracle, and ODBC, see the URLs: http://technet.microsoft.com/en-us/l...QL.105%29.as http://technet.microsoft.com/en-us/l.../cc754431.aspx http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html http://www.psdn.progress.com/progres...92/odr/odr.pdf
Windows	HTTPS	For more information on configuring a Windows event source to use certificates and enable HTTPS, see NetWitness Suite 11.1 Help topic *Windows Collection Configuration Guide*.
Check Point	OPSEC LEA	For more information on configuring a Check Point event source to use certificates, see NetWitness Suite 11.1 Help topic *Check Point Collection Configuration Guide*.
Netflow	Netflow	For more information on configuring a Netflow event source to use certificates, see NetWitness Suite11.1 Help topic *Netflow Collection Configuration Guide*.

Event Source	Protocol	Resources
SDEE	SDEE	For more information on configuring a SDEE event source to use certificates, see NetWitness Suite 11.1 Help topic *SDEE Collection Configuration Guide*.
SNMP	SNMP	For more information on configuring a SNMP event source to use certificates, see NetWitness Suite 11.1 Help topic *SNMP Collection Configuration Guide*.
VMware		For more information on configuring a VMware event source to use certificates, see NetWitness Suite11.1 Help topic *VMware Collection Configuration Guide*.
Legacy Windows and NetApp		For more information on configuring a Legacy Windows event source to use certificates, see NetWitness Suite11.1 Help topic *Legacy Windows and NetApp Collection Configuration Guide*
Amazon Web Services (AWS) Cloud Trail	HTTPS	For more information on configuring an AWS Cloud Trail event source to use certificates, see NetWitness Suite 11.1 Help topic *AWS (CloudTrail) Collection Configuration Guide*.

Note: For more information on enabling SSL for component communications, see Component Authentication.
Enabling HTTPS on REST Interfaces for Core Services

Enabling HTTPS on REST Interfaces for Core Services

To enable HTTPS on REST interfaces:

1. Log in to REST interface.
2. Go to the **rest** > **config** node.

3. Set **SSL** config to **on**.
4. Restart the service.

Data Security Settings

Data security settings are designed to enable the definition of controls to prevent data permanently stored by RSA NetWitness Suite from being disclosed in an unauthorized manner.

Securing Data

To help protect online data, such as current database, log, and configuration files, RSA recommends that you restrict access to the files and database and configure permissions so that only trusted administrators are allowed to access them.

RSA recommends that you back up your sensitive data, encrypt it, and keep it in a secure physical location in accordance with your corporate disaster recovery and business continuity policies.

The backup can be done in the following ways:

- Regular backup of Configuration and Data files – You can back up and restore data and configuration files for the core host and services and all the modules of NetWitness Suite. For more information, see "Back Up and Restore Data for Hosts and Services" topic in the *System Maintenance Guide*.
- Regular backup of critical configuration – You can export configurations using the Export option available on the UI. For example, you can take a backup of critical rules, reports, alerts, ESA rules, dashboards, investigation profiles, meta groups, event sources, global notifications, and so on. For more information, see topics:
  - "Export a Rule, Export an Alert and Export a Report" in the *Reporting Guide*.
  - "Rule Library View and Dashboard" in the *Alerting using ESA Guide*.
  - "Manage Profiles Dialog and Export a Meta Group" in the *Investigation and Malware Analysis Guide*.
  - "Events View and Export Event Sources" in the *Event Source Management Guide*.
  - "Global Notifications Panel Toolbar" in the *System Configuration Guide*.

Data Privacy

Data Privacy is very integral and helps you manage privacy-sensitive data. You can achieve data privacy using the Data Privacy Officer (DPO) role. The DPO can configure NetWitness Suite to limit the exposure of meta data and raw content (packets and logs) using a combination of techniques. The methods available to protect data in NetWitness Suite include:

- Data Obfuscation
- Data Retention Enforcement
- Auditing Logging

For more information, see topics in the Data Privacy Management.

Default Storage Passwords

The default storage passwords for database accounts that store alerts in ESA, Respond Service, and Data Science can be changed. For more information, see "Change Default Storage Passwords" topic in the *Host and Services Configuration Guide*.

Alert System Settings

For instructions on configuring NetWitness Suite to send alerts or notifications, see following topics in the *System Configuration Guide*:

- "Email Configuration Panel"
- "Global Audit Logging Configurations Panel"
- "Global Notifications Panel"

FIPS Compliance

This topic provides information on the Federal Information Processing Standards (FIPS) compliant mode for RSA NetWitness Suite. The FIPS publications are guidelines that set best practices for software and hardware security products for the protection of valuable and sensitive information.

When the FIPS compliant mode is used, products that support one or more FIPS standards can be set into a mode where the product uses FIPS approved algorithms and methods only.

NetWitness Suite supports both FIPS approved and non-FIPS approved functions. In FIPS mode, the product is incapable of using any non-FIPS approved methods.

NetWitness Suite Components working in FIPS mode

The table below lists the NetWitness Suite components that work in FIPS mode. The method you use to activate or deactivate FIPS depends on the type of security library used by your NetWitness Suite services. Your NetWitness Suite services use the security libraries, as mentioned in the following table.

Services	Security Library
Event Stream Analysis (ESA), Malware Analysis, Reporting Engine, NetWitness Suite Host, Respond Service, Context Hub and Endpoint	BSAFE
Broker, Concentrator, Decoder, Log Decoder, Warehouse Connector, Archiver, and Workbench	BSAFE

FIPS 140-2 Certified Cryptographic Modules are enabled for all services that perform cryptographic operations. For the following services, although the FIPS Cryptographic Module is leveraged, the use of FIPS cipher suites is not being enforced:

- NTP: UPD Port 123
- TCP: SSH Port 22
- TCP: Salt API Loopback Port 8000
- CollectD
- Log Collector
- Log Decoder

Note: In 11.0 or later, FIPS is enabled by default for all services, except for Log Collector and Log Decoder. For more information on how to enable FIPS on log Collector and Log Decoder see *RSA NetWitness® Suite 11.0 Release note.*

Note: Security Technical Implementation Guide (STIG) is not supported for version 11.0 or later.

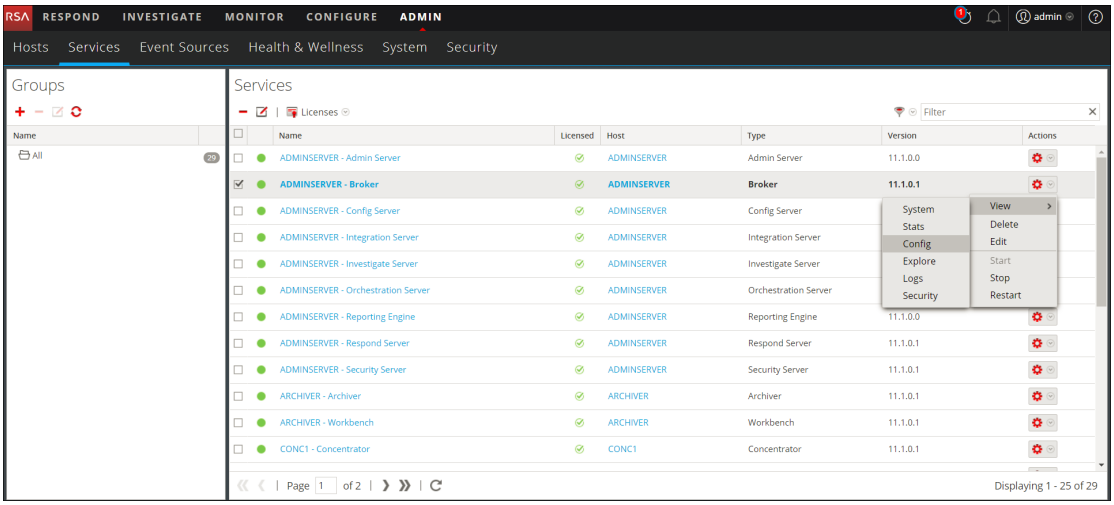
Common Criteria Compliance

This topic provides information on Common Criteria Compliance for RSA NetWitness Suite.To support this requirement, you must ensure that only a secure communication is configured for the core services. To achieve this you must disable the unencrypted ports for the NetWitness core services.

Disabling Unencrypted Ports For NetWitness Core Services

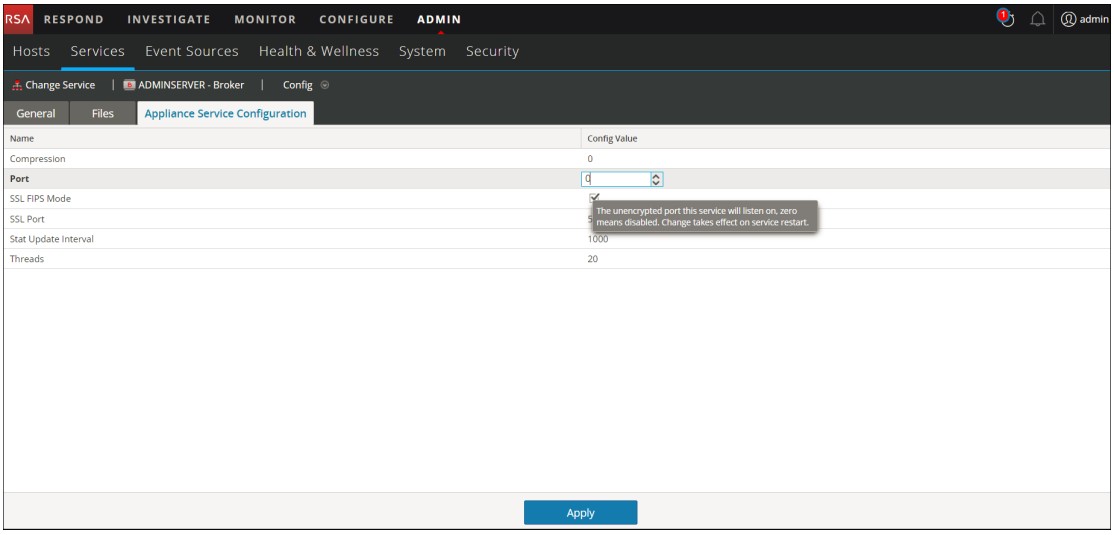
To disable an unencrypted port for a NetWitness core service:

1. Log in to NetWitness Suite UI.
2. Go to **ADMIN** > **Services**.
   The Services page is displayed.
3. Select a core service to configure.
4. Click  and select **View** > **Config**.



5. Select the General tab.
6. In the Port field under the System Configuration section, replace the existing value with **0**.
7. Now click the Appliance Service Configuration tab.

8. In the Port field, replace the existing value with **0**.



9. Click **Apply** and restart the service, if prompted.

Note: After you apply the changes only the SSL port is configured for the service and no unencrypted interfaces are available to interact with the service.

Other Security Considerations

This topic describes various other security configuration settings that are not covered in previous sections.

Changing the RabbitMQ Management Password for Windows Legacy Collectors

For Windows Legacy Log Collectors (WLCs), a default password is used for the "logcollector" username to access the RabbitMQ broker on that machine. RSA recommends that you change the password for WLCs, per the procedure outlined, which involves changing the RabbitMQ password for the Log Collector and for the RabbitMQ broker.

Note: For CentOS, changing the RabbitMQ password is not supported.

If you are using a Log Collector, you may have to initialize the "lockbox". For instructions, see "Step 3: Set Up a Lockbox" topic in the *Log Collection Guides*.

To change the RabbitMQ password:

1. Change the RabbitMQ password in Log Collector:
   a. Go to the Explore view for the Log Collector service.
   b. Right-click the **event-broker** node and select **config**.
   c. Type the new password in the **amqp_password** field. The password is encrypted by a key that is managed through the lockbox of this Log Collector. This only changes the password on the Log Collector side.

   Note: Most of the settings should not be changed. Ensure you do NOT change the Message Queue User Name "amqp_username" because it is referred to in some certificate checks.
2. Change the RabbitMQ password for the RabbitMQ broker:
   a. Go to the Explore view for the Log Collector service.
   b. Right-click the **event-broker** node and select **properties**.
   c. Select **passwd** in the drop-down list.
   d. In the **Parameters** field, type the old and new password.
   Ensure you remember your old password. If it was never changed, it should be "netwitness" by default.

Example: `Parameters: oldpw=<netwitness> newpw=<YourNewPasswordHere>`

e. Click **Send**.

Hardening the NetWitness Suite Core service

By default, all NetWitness SuiteCore services ship with a default username and password and with SSL turned off. To harden the service, you have to run it with the command line option `-s harden=true`.

Using a Decoder, here's an example command line:

```
NwDecoder -s harden=true -s defaultUsername=<username> -s
defaultPassword=<password>
```

The above command does the following:

1. Removes the default admin account (with caveats, see below).
2. Creates a new account <username> with a password of <password> (thus meeting the password requirements below).
3. Enables SSL on both the native and REST ports.
4. Strengthens default password requirements:
   - /users/config/account.lockout.time = 60
   - /users/config/password.alpha.lowercase.min = 1
   - /users/config/password.alpha.uppercase.min = 1
   - /users/config/password.length.min = 8
   - /users/config/password.numeric.min = 1
   - /users/config/password.symbol.min = 1
5. Sets /rest/config/user.agent.whitelist = Apache-HttpClient/\d\.\d\.\d

   Note: This setting prevents the browsers to connect to the REST port.

The caveat for changing the default user account is that there cannot be an already existing configuration file. This is always true the first time the service is run or before the service is licensed. To harden a service, you must run it before a configuration is written or delete whatever configuration file exists and then harden.

To alter the command line for a service that writes its own upstart script without actually SSHing into the box and modifying the script, there is a new parameter that you can pass to either the /sys shutdown or /decoder reset command (substitute decoder for the actual service name) and this parameter is called "cl" for command line. What you do is pass name=value pairs to the "cl" parameter and those parameters will take affect on the next restart of the service.

Example:

```
/sys shutdown reason="Restart because license was applied"
cl="harden=true default
Username=<username> defaultPassword=<password>"
```

The above command shuts down the service (which should be restarted by Linux upstart) and the command line parameters will be applied on the restart. This command line exactly matches the command line given above for the decoder service. If you want to do a configuration reset, you can use the following:

```
 /broker reset config=true cl="harden=true defaultUsername=<username>
defaultPassword=<password>"
```

This will delete the broker configuration file and create a new default configuration that is automatically hardened with the given default account and credentials. The admin account will not exist when the broker restarts, only the <username> account exists.

NFS Access Controls

By default, the NFS mounts are wide open. To lock them down to a specific address, you must edit the exports file and specify the IP addresses that are allowed to interact with the SAW.

The SAW NFS service is managed from the command line using *mapr-nfsserver*.

```
[root@saw-node1 ~]# service mapr-nfsserver
Usage: /etc/init.d/mapr-nfsserver {start|stop|status|restart|}
[root@saw-node1 ~]# service mapr-nfsserver status
nfsserver (pid 5692 5691) is running...
[root@saw-node1 ~]#
```

If nfs-utils is installed on the node, you can execute a *showmount* on the localhost to see the exposed exports.

```
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr *
/mapr/saw *
[root@saw-node1 ~]#
```

Exports are controlled using the exports file in the */opt/mapr/conf* directory.

```
[root@saw-node1 ~]# cat /opt/mapr/conf/exports
# Sample Exports file
# for non /mapr exports
# <Path> <comma separated cldb addresses=host:port> <exports_control>
# for /mapr exports
# <Path> <exports_control>
#access_control -> order is specific to default
# list the hosts before specifying a default for all
# a.b.c.d,1.2.3.4(ro) d.e.f.g(ro) (rw)
# enforces ro for a.b.c.d & 1.2.3.4 and everybody else is rw
# special path to export clusters in mapr-clusters.conf. To disable
exporting,
# comment it out. to restrict access use the exports_control
#
/mapr (rw)
#to export only certain clusters, comment out the /mapr & uncomment.
# Note: this will cause /mapr to be unexported
#/mapr/clustername (rw)
#to export /mapr only to certain hosts (using exports_control)
#/mapr a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster1 rw to a.b.c.d & ro to e.f.g.h (denied for
others)
#/mapr/cluster1 a.b.c.d(rw),e.f.g.h(ro)
# export /mapr/cluster2 only to e.f.g.h (denied for others)
#/mapr/cluster2 e.f.g.h(rw)
# export /mapr/cluster3 rw to e.f.g.h & ro to others
#/mapr/cluster2 e.f.g.h(rw) (ro)
[root@saw-node1 ~]#
```

To restrict the SAW exports to a certain IP address or group of IPs, you must first edit the exports file and then restart the *mapr-nfsserver service*.

```
[root@saw-node1 ~]# vi /opt/mapr/conf/exports
[root@saw-node1 ~]# cat /opt/mapr/conf/exports | grep ^/mapr
/mapr 10.42.1.87(rw)
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr *
/mapr/saw *
```

```
[root@saw-node1 ~]# service mapr-nfsserver restart
[root@saw-node1 ~]# showmount -e localhost
Export list for localhost:
/mapr 10.42.1.87
/mapr/saw 10.42.1.87
[root@saw-node1 ~]# mount -t nfs -o nolock,tcp localhost:/mapr/saw
/saw
mount.nfs: access denied by server while mounting localhost:/mapr/saw
[root@saw-node1 ~]#
```

Note: Trying to mount the export on the localhost will fail as only a specific host IP is now allowed to use the NFS mount

Secure Deployment and Usage Settings

This topic describes the settings for secure deployment and usage. It is very important to protect all physical, local, and remote access to the RSA NetWitness Suite appliances. It is also important to restrict all access methods to the absolute minimum required to maintain RSA NetWitness Suite.

Note: RSA recommends that you do not set up the test environments to be exact copies of the full production environment. If the test environment is identical to the production environment, you should take the same precautions to protect the test environment as you do in the production environment.

Security Controls Map

This topic describes the security controls map. An RSA NetWitness Suite deployment can consist of the following components:

- Decoder
- Log Decoder
- Concentrator
- Broker
- Log Collector
- Context Hub
- Malware
- ESA
- Archiver
- NetWitness Warehouse
- NetWitness Server
- External Warehouse - Hortonworks
- External CMS Library (Live)
- Endpoint Insights

NetWitness Suite supports integration with products such as RSA NetWitness Endpoint 4.x and RSA Archer.

RSA recommends that you access the host on secure client machines within the network. If you must access the host through remote access, RSA recommends that you connect to the network through a secure VPN connection. Only allow remote access to NetWitness Suite hosts for secure maintenance using the Remote Desktop Protocol (RDP) through a secure VPN connection.

Caution: RSA recommends that you deploy the hosts in a secure location, where physical access to the hosts are restricted only to the personnel who manage the hosts.

Secure Enclave

To help protect NetWitness Suite against unauthorized authentication and access by end users or machines, RSA recommends that you deploy NetWitness Suite hosts such as Broker, Concentrator, and Decoder.

You can help create a secure enclave by separating the low security corporate network from the high security network with firewalls. To help create a secure enclave, RSA recommends that you:

- Implement basic physical security elements, policies, procedures, and processes for the low security network.
- Provide access to the hosts within the secure enclave through a secure virtual private network (VPN) tunnel only, such as IPSec tunnel, to establish encryption and authentication of all network traffic to and from the hosts.

Note: The client machines through which you access NetWitness Suite can be present outside of the Secure Enclave.

Secure Deployment Guidelines

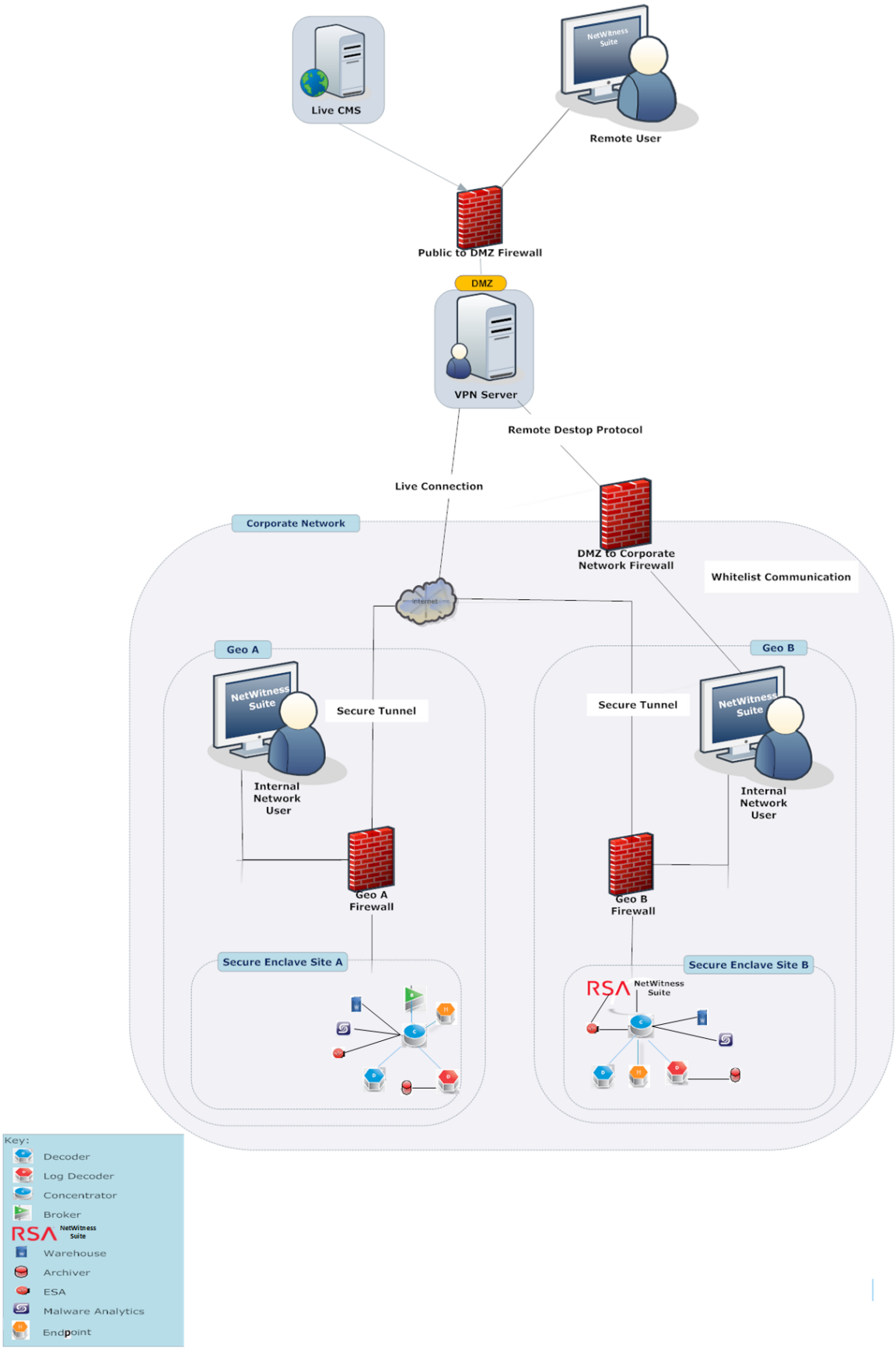
To help ensure a secure deployment, RSA recommends that you:

- Deploy multiple hosts in the corporate network. The multiple hosts in the example are in two geographic locations and include the following components:
  - NetWitness Suite
  - Broker
  - Packet Decoder
  - Log Decoder
  - Concentrator
  - ESA
  - Archiver
  - NetWitness Warehouse
  - Malware Analysis
  - Endpoint
- Ensure that all the components are connected to the same subnetwork.
- Deploy firewalls at each site to ensure the secure transfer of data from an instance of NetWitness Suite at one site to another instance of NetWitness Suite located at a different site.
- Configure firewall rules to control all communication between different sites and other

components in the network as depicted in the previous figure.

- Implement data transfer between sites using a secure tunnel IPSec.

The following figures show the deployment of multiple sites within a corporate network:


Live CMS
NetWitness Suite
Remote User
Public to DMZ Firewall
DMZ
VPN Server
Remote Destop Protocol
Live Connection
Corporate Network
DMZ to Corporate Network Firewall
Whitelist Communication
Internet
Geo A
Geo B
NetWitness Suite
Secure Tunnel
Secure Tunnel
NetWitness Suite
Internal Network User
Internal Network User
Geo A Firewall
Geo B Firewall
Secure Enclave Site A
Secure Enclave Site B
RSA NetWitness Suite
Key:
Decoder
Log Decoder
Concentrator
Broker
RSA NetWitness Suite
Warehouse
Archiver
ESA
Malware Analytics
Endpoint

Firewall Rules

It is important that you use a firewall to restrict network traffic between RSA NetWitness Suite and external systems. RSA NetWitness Suite recommends that you configure firewall rules to help ensure secure communication for the following connections:

- Demilitarized zone (DMZ) to corporate network
- Corporate network to site sub network
- Site to site
- Live CMS to DMZ
- External email server to DMZ

Note: RSA recommends that you restrict access from client hosts to only known IP addresses. For example, if you set up the NetWitness Suite Client UI on IP address 192.168.0.1, configure your firewall to allow only the IP address 192.168.0.1 to connect to the NetWitness Suite host.

Note: The firewall rules should be configured on an external firewall and not on any of the NetWitness Suite host.

RSA recommends that you configure firewall rules as described in the sections below. These recommendations are based on the following assumptions:

- You have a stateful firewall, indicating that only the establishment of TCP ports is considered.
- You specify the direction of communication for the UDP ports because the connections are sessionless.
- You deploy NetWitness Suite as shown in the Security Controls Map.
- The firewall processes the rules top to bottom, finishing with a generic drop of all the packets.

DMZ to Corporate Network

RSA recommends that you:

- Configure whitelist communication from the VPN server in the DMZ to the client machines on which you run RSA NetWitness Suite applications such as NetWitness Suite Web UI.
- Create firewall rules for all the machines from which you intended to remotely access the corporate network through Remote Desktop Protocol (RDP).

Corporate Network to Site

RSA recommends that the firewall at each RSA NetWitness Suite site allow access only from designated client machines through a whitelisted IP address and port.

RSA recommends that you secure the following ports to ensure secure communication between the client machine that is set as the RSA NetWitness Suite Web UI and the NetWitness Suite site:

- TCP 443

For more information, see Communication Security Settings. To help ensure secure communication between the client machines that access the NetWitness Suite UI and a site, you must set up the firewall rules as shown below:

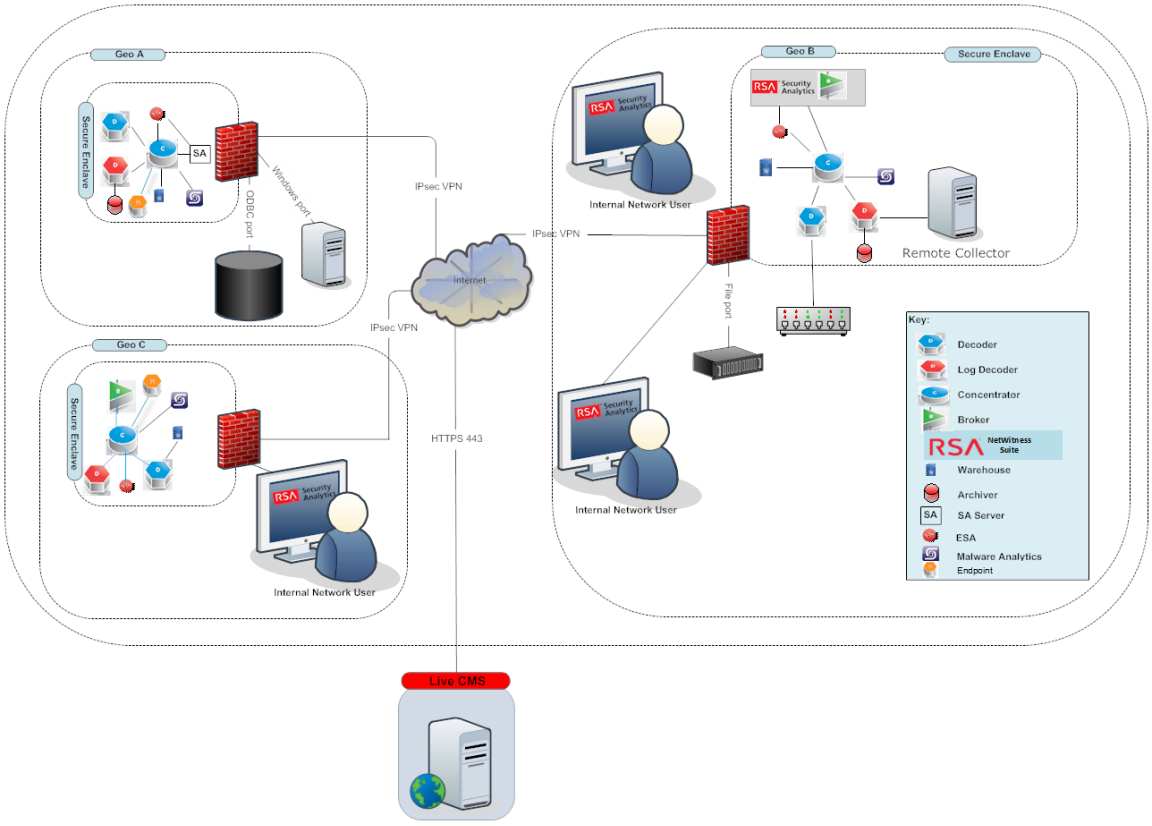
ALLOW $nwclient_IP to $nwsite_IP on port 443/tcp

DROP all from * to *

where **nwclient_IP** is the IP address assigned to the client machine that is set as the NetWitness Suite web UI and **nwsite_IP** is the IP address assigned to the Broker host within which the RSA NetWitness Suite web server is running.

Site to Site

RSA NetWitness Suite may run in multiple sub-networks within your corporate network, called sites. You can configure RSA NetWitness Suite to allow the hosts located in one site to communicate with the hosts in another site.



For this scenario, RSA recommends that you do the following:

- Ensure that the firewall at each RSA NetWitness Suite site allows communication between two sites only through a whitelisted IP address and port. For a graphical depiction of the site-to-site security control map showing the site firewalls, see the above figure.
- NetWitness Suite system update uses port 80. That means NetWitness Server site to another site (where brokers, decoders exist), port 80 should be open.

Live CMS to DMZ

To ensure secure communication between the RSA NetWitness Suite site and Live CMS, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $Live_IP on port 443/tcp

DROP all from * to *

where **nw_site_IP** and **Live_IP** are the IP addresses assigned to the NetWitness Suite site and the Live CMS respectively.

Note: If you are using proxy server with self-signed certificate, you must add exception in proxy server rule to allow traffic between Live CMS server (cms.netwitness.com, port 443) and NetWitness Server.

RSA Download Central to DMZ

To ensure secure communication between the RSA NetWitness Suite site and RSA Download Central, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $rsa_DLC_IP on port 80/tcp

DROP all from * to *

where **nw_site_IP** and **rsa_DLC_IP** are the IP addresses assigned to the NetWitness Suite site and RSA Download Central respectively.

External Email Server to DMZ

To ensure secure communication between the RSA NetWitness Suite site and the External Email Server, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $Email_IP on port 443/tcp

DROP all from * to *

where **nw_site_IP** and **Email_IP** are the IP addresses assigned to the NetWitness Suite site and the external email server respectively.

Syslog Server to Site

If you have enabled the syslog port, to ensure secure communication between the RSA NetWitness Suite site and the Syslog Server, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $Syslog_IP on port 514/udp

DROP all from * to *

where **nw_site_IP** and **Syslog_IP** are the IP addresses assigned to the NetWitness Suite site and the syslog server respectively.

SNMP Server to Site

If you have enabled the SNMP port, to ensure secure communication between the RSA NetWitness Suite site and the SNMP Server, set up the firewall rules as shown below:

ALLOW $nw_site_IP to $SNMP_IP on port 1610/SNMP

DROP all from * to *

where **nw_site_IP** and **SNMP_IP** are the IP addresses assigned to the NetWitness Suite site and the SNMP server respectively.

Secure Deployment Settings

The following table shows the security controls that RSA recommends putting in place to help secure the deployment.

Default Deployment Setting	Secure Deployment Settings	Pros of Secure Deployment Settings	Cons of Secure Deployment Settings	Instructions on how to configure secure deployment settings
HTTPS is enabled by default between the NetWitness Suite client and the server	For the best possible security between the client and the server, use certificates from CA.	Provides a high level of protection for the communication between client and server by avoiding tampering, spoofing, and man-in-the middle attacks.	May have impact on performance	For instructions on installing external certificates, see SSL Certificate Guidance for NetWitness Suite

Secure Maintenance

This topic describes some common solutions to help ensure secure maintenance.

Security Patch Management

All security patches for RSA NetWitness Suite originate at RSA and are available for you via the NetWitness Suite User Interface. For more information, see "Manage NetWitness Suite Updates" topic in the *System Maintenance Guide* .

The following table lists the third-party components for which patches are needed.

Third-party Component for which patch is needed	Frequency of Patch	EMC Respons-ibility (Y/N)	Customer Responsibility (Y/N)	Reference to instructions for Applying Patch
NetWitness Suite Hosts	Monthly and Quarterly	Y	Y	Based on EMC RSA recom-mendations

Note: From 2016 onwards, security patches will be part of the product release only and will not be shipped out separately.

Virus Scanning

RSA recommends that you:

- Deploy anti-virus client software on the deployed servers in accordance with your enterprise requirements.
- Run anti-virus and anti-malware tools with the most current definition files on the deployed servers.
- Scan all files/drivers before uploading on the deployed server.
- Follow best practices for patch management and regularly review available patches for all anti-virus and anti-malware software.

Ongoing Monitoring and Auditing

As with any critical infrastructure component, RSA NetWitness Suite recommends that you constantly monitor your system and perform periodic and random audits (for example, configuration, permissions, and security logs). You should ensure that the configurations and user access settings match your company policies and needs. For more information, see "Global Audit Logging Configurations Panel" topic in the *System Configuration Guide*.

Hardware Replacement

If RSA NetWitness Suite hardware fails or is faulty, order a replacement by contacting RSA Customer Support. While awaiting a replacement, the Redundant Array of Independent Disks (RAID) configuration is designed to ensure that there is no data loss due to a hardware failure.

The RAID configuration on NetWitness Suite:

- Hosts are RAID 1.
- Direct Attach Capacity (DAC) disk shelves is RAID 5.

Physical Security Controls Recommendations

This topic describes physical security controls.

Recommendations

Physical security controls help to enable the protection of resources against unauthorized physical access and physical tampering. RSA recommends that the physical devices and servers for RSA NetWitness Suite are deployed in a secure data center leveraging the organization's best practices for physically securing a data center, server rack, and/or server.

Supporting Users

This topic describes well-defined policies around help desk procedures for your RSA NetWitness Suite installation.

It is important to have well-defined policies around help desk procedures for your RSA NetWitness Suite installation. RSA recommends that your help desk administrators understand the importance of password strength and the sensitivity of data, such as user logon names and passwords. Creating an environment where an end user is frequently asked for this kind of sensitive data increases the opportunity for social engineering attacks. Train end users to provide, and help desk administrators to request, the least amount of information needed in each situation.

Preventing Social Engineering Attacks

Fraudsters frequently use social engineering attacks to trick unsuspecting employees or individuals into divulging sensitive data that can be used to gain access to protected systems. RSA recommends that you use the following guidelines to help reduce the likelihood of a successful social engineering attack:

- Help desk administrators should only ask for User IDs over the phone when receiving help desk calls. Help desk administrators should never ask for user passwords.
- The help desk telephone number should be well known to all users.
- Help desk administrators should perform an action to authenticate the user's identity before performing any administrative action on a user's behalf. For example, ask users one or more questions to which only they know the answer.
- If help desk administrators need to initiate contact with a user, they should not request any user information. Instead, users should be instructed to call the help desk back at a well-known help desk telephone number to ensure that the original request is legitimate.

Confirming User Identities

It is critical that your help desk administrators verify end users' identities before performing any help desk operations on their behalf. RSA recommends that you verify user identity using the following methods:

- Call the end user back on a phone owned by the organization and on a number that is already stored in the system.

Caution: Be wary of using mobile phones for identity confirmation, even if they are owned by the company because mobile phone numbers are often stored in locations that are vulnerable to tampering or social engineering.

- Send the user an email to a company email address. If possible, use encrypted email.
- Work with the employee's manager to verify the user's identity.
- Verify the identity in person.
- Use multiple open-ended questions from employee records. For example, "Name one person in your group" or "What is your badge number?" Avoid yes or no questions.

Advice for Your Users

RSA recommends that you instruct your users to do the following:

- Never give passwords to anyone.
- Change passwords at regular intervals.
- Inform your users of what information requests to expect from help desk administrators.
- Always log off from the web interface when finished.
- Always lock their desktops when stepping away from their computers.
- Regularly close their browser and clear their cache of data.

Note: Consider regular training to communicate this guidance to users.

Appendix A: Customer Provided Certificates

The following procedure takes effect when you update to NetWitness Suite 11.1. The procedure tells you how to replace the internally generated NetWitness Suite web server certificate (NGINX front-door) with a customer issued certificate. This enables client browsers to establish a trusted SSL connection.

Caution: Files the cert and key files must be `.pem` format. All the files must have same name and permissions as the original files generated by NetWitness Suite.

1. Rename your certificate files and save them in for NGINX.
   - Rename the customer provided `cert.pem` certificate pem file to `web-server-cert.pem`.
   - Rename the customer provided `key.pem` key pem file to `web-server-key.pem`.
   - Rename customer provided `cert.chain` certificate chain file to `web-server-cert.chain`.
   - Rename `cert.p7b` certificate p7b file to `web-server-cert.p7b`.
2. SSH to the NW Server.
3. Replace the existing NetWitness Suite generated `/etc/pki/nw/web/web-server-cert.pem`, `/etc/pki/nw/web/web-server-key.pem`, `/etc/pki/nw/web/web-server-cert.chain` and `/etc/pki/nw/web/web-server-cert.p7b` files with the files you renamed in step 1.
4. Restart NGINX service.
   `service nginx restart.`