Monitoring RSA Authentication Manager

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

RSA Authentication Manager is a multi-factor authentication solution that verifies authentication requests and centrally administers authentication policies for enterprise networks. Use Authentication Manager to manage security tokens, users, multiple applications, agents, and resources across physical sites, and to help secure access to network and web-accessible applications, such as SSL-VPNs and web portals.

RSA Authentication Manager provides the following choices for strong authentication:

- RSA SecurID, which protects access using two-factor authentication with hardware and software-based tokens.
- On-demand authentication (ODA), which protects access using two-factor authentication by sending authentication credentials to users upon request through SMS text messaging or e-mail.
- Risk-based authentication (RBA), which protects access by assessing user behavior and matching the device being used to authenticate to assess the risk-level of an authentication attempt.

By leveraging devices that the user already owns, for example, a mobile phone, PC, or laptop, RBA and ODA enable multi-factor authentication with no tokens to manage. Figure 1.1 shows a deployment of the RSA Authentication Manager.

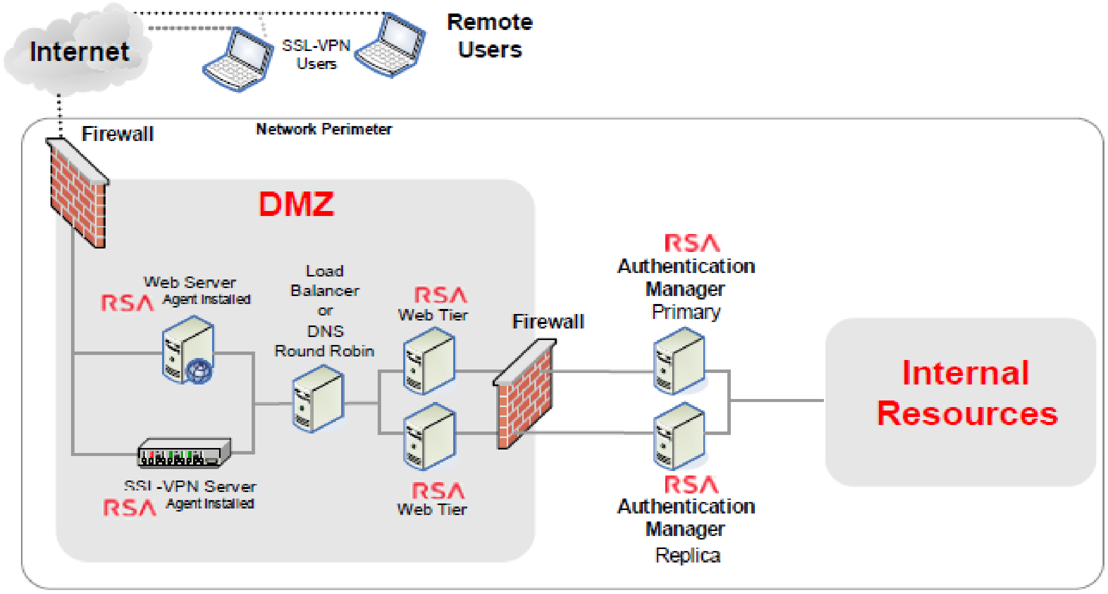


Figure 1.1: The RSA Authentication Manager deployed in an environment

An RSA Authentication Manager deployment may have the following components:

1. **Primary Instance:** The primary instance is the initial Authentication Manager system that you deploy. The main functions of the primary instance include the following:

   - Authenticating users.
   - Enabling administration of Authentication Manager data stored in the internal database. You can perform tasks such as importing and assigning SecurID tokens, enabling risk-based authentication (RBA), adding LDAP identity sources, configuring self-service, generating replica packages, and generating agent configuration files and node secrets.
   - Replicating changes due to administration and authentication activities.
   - Hosting the primary RSA RADIUS server.
   - Handling self-service requests.
   - Maintaining the most up-to-date Authentication Manager database.

2. **Replica Instance:** A replica instance provides deployment-level redundancy of the primary instance. You can view, but not update, administrative data on a replica instance. A replica instance provides the following benefits:

   - Real-time mirror of all user and system data
   - Failover authentication if the primary instance becomes unresponsive
   - Improved performance by load balancing authentication requests to multiple instances
   - Ability to deploy a replica instance at a remote location
   - Ability to recover administrative capabilities through replica promotion if the primary instance becomes unresponsive

3. **Identity Sources:** All users and user groups in your deployment are stored in identity sources. RSA Authentication Manager supports the following as identity sources:

   - LDAP directory servers, either Active Directory, Sun Java System Directory Server, Oracle Directory Server, or OpenLDAP.
   - Active Directory Global Catalogs, when some or all of the Active Directory servers in its Active Directory forest are used as identity sources. In such a case, the Global Catalog is used for runtime activities, for example, looking up and authenticating users, and resolving group membership within the Active Directory forest. The Global Catalog cannot be used to perform administrative functions.

- The Authentication Manager internal database, used for administrative operations, such as enabling users for on-demand authentication and risk-based authentication.

4. **RSA Authentication Agents:** An authentication agent is a software application installed on a machine, such as a domain server, web server, or personal computer, that enables authentication. The authentication agent is the component on the protected resource that communicates with RSA Authentication Manager to process authentication requests. Any resource that is used with SecurID authentication, on-demand authentication (ODA) or risk-based authentication (RBA) requires an authentication agent.

5. **Risk-Based Authentication for a Web-Based Resource:** Risk-based authentication (RBA) protects access to web-based resources and applications. Deploying RBA requires integrating the resource with Authentication Manager. Authentication Manager provides a template to facilitate the integration process. Once integrated, the web-based resource automatically redirects users to Authentication Manager, which does either of the following:

   - Authenticates the user and returns proof of authentication to the resource
   - When the risk level is high, prompts the user to provide further credentials, such as the correct answers to pre-configured security questions, before returning proof of authentication.

   The web-based resource presents the proof of authentication to Authentication Managerfor verification and allows the user access to the resource.

6. **RSA RADIUS Overview:** You can use RSA RADIUS with RSA Authentication Manager to directly authenticate users attempting to access network resources through RADIUS-enabled devices.

7. **Web Tier:** A web tier is a lightweight application server that hosts several Authentication Manager services securely in the network DMZ. Services such as risk-based authentication (RBA), the Cryptographic Token Key Initialization Protocol (CT-KIP) for the dynamic provisioning of software tokens, and the Self-Service Console may be required by users outside of your corporate network. If your network has a DMZ, you can use a web tier to deploy these services in the DMZ.

8. **Self Service:** Self-Service is a web-based workflow system that provides user self-service options and automates the token deployment process.

9. **Load Balancer:** If your deployment includes more than one web tier, you can add a third-party load balancer. The web-tier deployment can be used with a load balancer or you can use round robin DNS.

Owing to its ability to be deployed easily in an environment and provide multi-factor authentication with ease, the RSA Authentication Manager is preferred across most mission critical environments. A second's non-availability of the authentication manager, an overload condition or authentication failure, ineffective caches of the RSA Authentication Manager, and intense response time during authentication process can cause serious harm to not only the performance of the RSA Authentication Manager, but also the services that rely on it. Continuous monitoring of the RSA Authentication Manager and prompt detection and resolution of anomalies is hence imperative. For continuously monitoring the RSA Authentication Manager, the eG Enterprise provides a specialized monitoring model, which is explained in the upcoming topics.

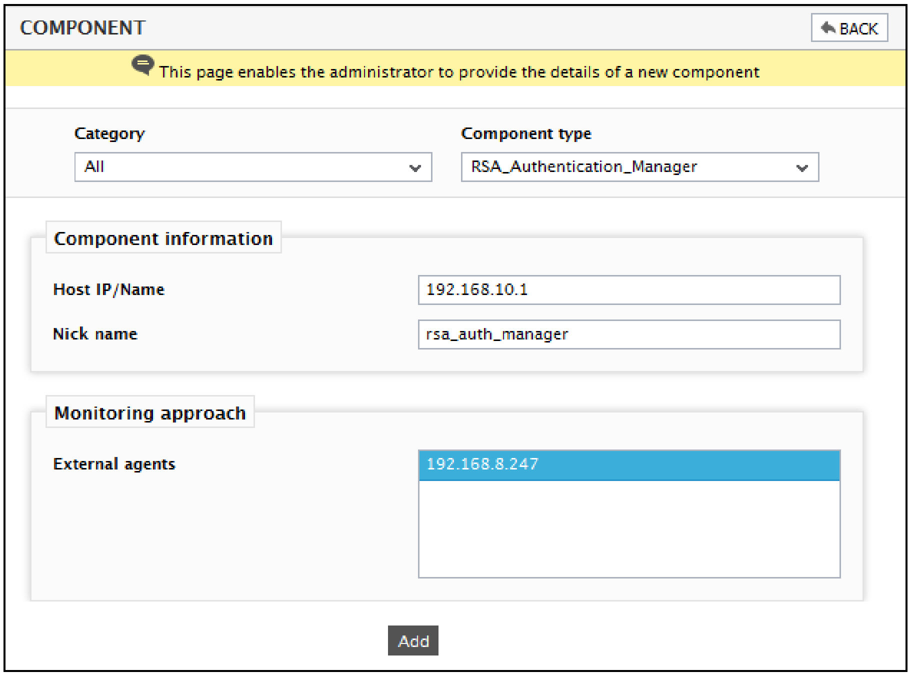
Chapter 2: How to Monitor RSA Authentication Manager Using eG Enterprise?

eG Enterprise is capable of monitoring the RSA Authentication Manager in an agentless manner. All that is required for this is a single eG agent deployed on a remote Windows host. This agent communicates with the authentication manager via SNMP and periodically monitors SNMP-MIB of the authentication manger to pull out the metrics pertaining to its performance. The key pre-requisite for monitoring the authentication manager is ensuring that the authentication manager is SNMP-enabled. To start monitoring the authentication manager, first you have to manage the component using the eG administrative interface. The steps for achieving this are explained in the below section.

2.1 Managing the RSA Authentication Manager

The eG Enterprise cannot automatically discover the RSA Authentication Manager so that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a RSA Authentication Manager component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select RSA Authentication Manager as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: RSA_Authentication_Manager

Component information

Host IP/Name: 192.168.10.1

Nick name: rsa_auth_manager

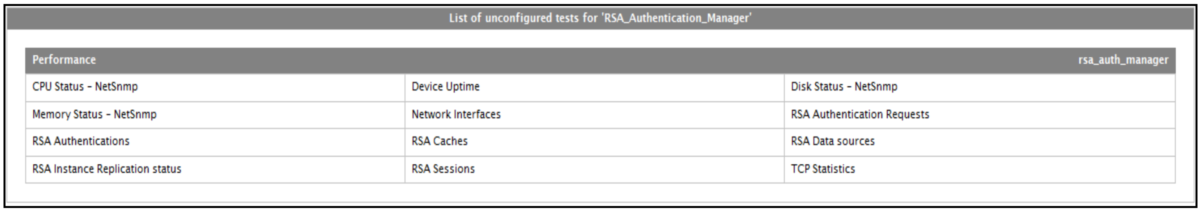
Monitoring approach

External agents: 192.168.8.247

Figure 2.1: Adding the RSA Authentication Manager

4. Specify the **Host IP** and the **Nick name** of the RSA Authentication Manager appliance in Figure 2.1. Then, click the **Add** button to register the changes.

5. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).

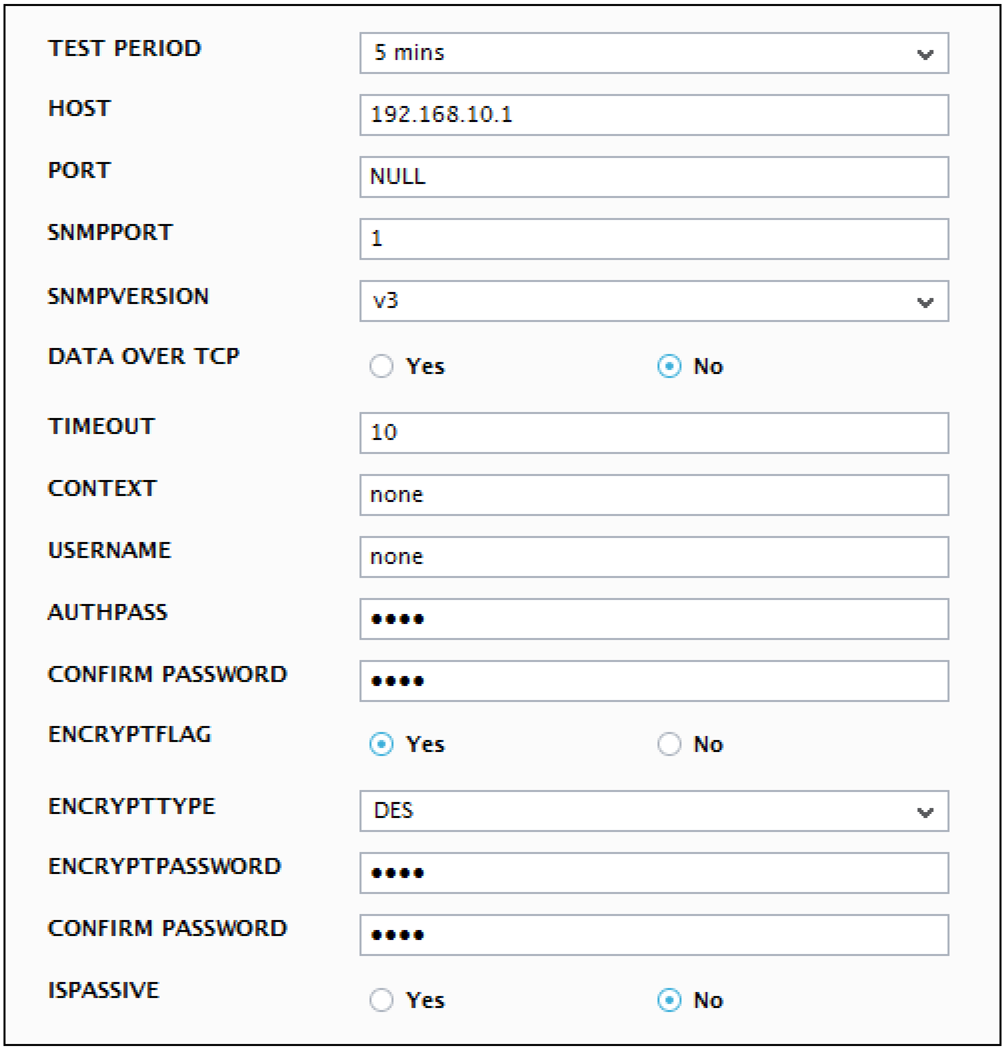


List of unconfigured tests for 'RSA_Authentication_Manager'

Performance		rsa_auth_manager
CPU Status - NetSnmp	Device Uptime	Disk Status - NetSnmp
Memory Status - NetSnmp	Network Interfaces	RSA Authentication Requests
RSA Authentications	RSA Caches	RSA Data sources
RSA Instance Replication status	RSA Sessions	TCP Statistics

Figure 2.2: List of tests to be configured for the RSA Authentication Manager

6. Click on any test in the list of unconfigured tests. For instance, click on the **RSA Authentications** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.



TEST PERIOD	5 mins	
HOST	192.168.10.1	
PORT	NULL	
SNMPPORT	1	
SNMPVERSION	v3	
DATA OVER TCP	○ Yes	● No
TIMEOUT	10	
CONTEXT	none	
USERNAME	none	
AUTHPASS	••••	
CONFIRM PASSWORD	••••	
ENCRYPTFLAG	● Yes	○ No
ENCRYPTTYPE	DES	
ENCRYPTPASSWORD	••••	
CONFIRM PASSWORD	••••	
ISPASSIVE	○ Yes	● No

Figure 2.3: Configuring the RSA Authentications test

7. To know how to configure the tests, refer to **Monitoring the RSA Authentication Manager** chapter.

8. Next, try to signout of the eG administrative interface, now you will be prompted to configure the **Device Uptime** and **Network Interfaces** tests. Refer to *Monitoring Cisco Router* document for the details on configuring these tests.

9. Finally, signout of the eG administrative interface.

Chapter 2: Monitoring the RSA Authentication Manager

eG Enterprise offers a specialized monitoring model that monitors the RSA Authentication Manager inside-out, and promptly alerts administrators to issues affecting its performance, so that the required remedial action can be taken before its too late.

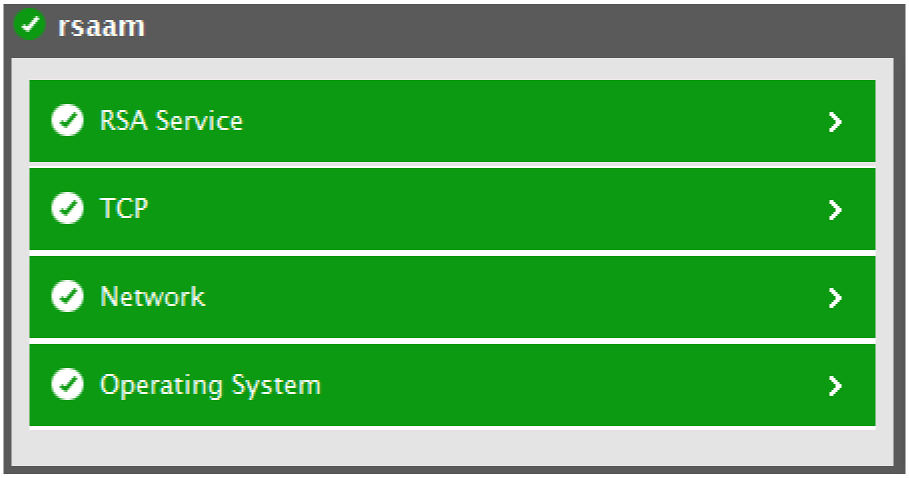


Figure 2.4: The layer model of the RSA Authentication Manager

Each layer of Figure 2.4 is mapped to a variety of tests each of which report a wealth of metrics related to the RSA Authentication Manager that is being monitored. Using these metrics administrators can find quick and accurate answers to the following queries:

- What is the rate at which authentication requests were serviced by the target RSA Authentication Manager?
- What is the rate at which the authentication requests were serviced successfully?
- What is the rate at which the authentication requests failed to be processed?
- What is the average time taken by the RSA Authentication Manager to process the authentication requests and responses?
- How many authentications were provided by the RSA Authentication Manager?
- How many authentication were actually successful and how many failed?
- What is the percentage of authentications that failed?
- How many new PIN authentications were provided by the RSA Authentication Manager?
- What is the total size of each cache of the RSA Authentication Manager?

- How many times the cache was flushed?
- How well the authentication requests were serviced from the cache?
- How many authentication requests were processed by each identity source?
- How many authentication requests failed processing for each identity source?
- How many connection were active for each identity source?
- What is the average time taken by each identity source to respond to requests?
- What is the current status of the Replica instance of the RSA Authentication Manager?
- How many sessions were currently active on the RSA Authentication Manager?

The **Operating System**, **Network** and **TCP** layers of the RSA Authentication Manager monitoring model is similar to that of a Windows server model. Since the tests pertaining to these layers have been dealt with in the *Monitoring Unix and Windows Servers* document, let us now focus on the **RSA Service** layer in the forthcoming section.

2.2 The RSA Service Layer

Using this layer, administrators can determine the status of the Replica instance on the RSA Authentication Manager and the number of active sessions on the RSA Authentication Manager. Using the tests pertaining to this layer, administrators can figure out the authentication requests that failed and the rate of successful authentication requests. In addition, administrators can figure out the identity source that failed to authenticate the requests and the cache that is servicing most of the authentication requests.

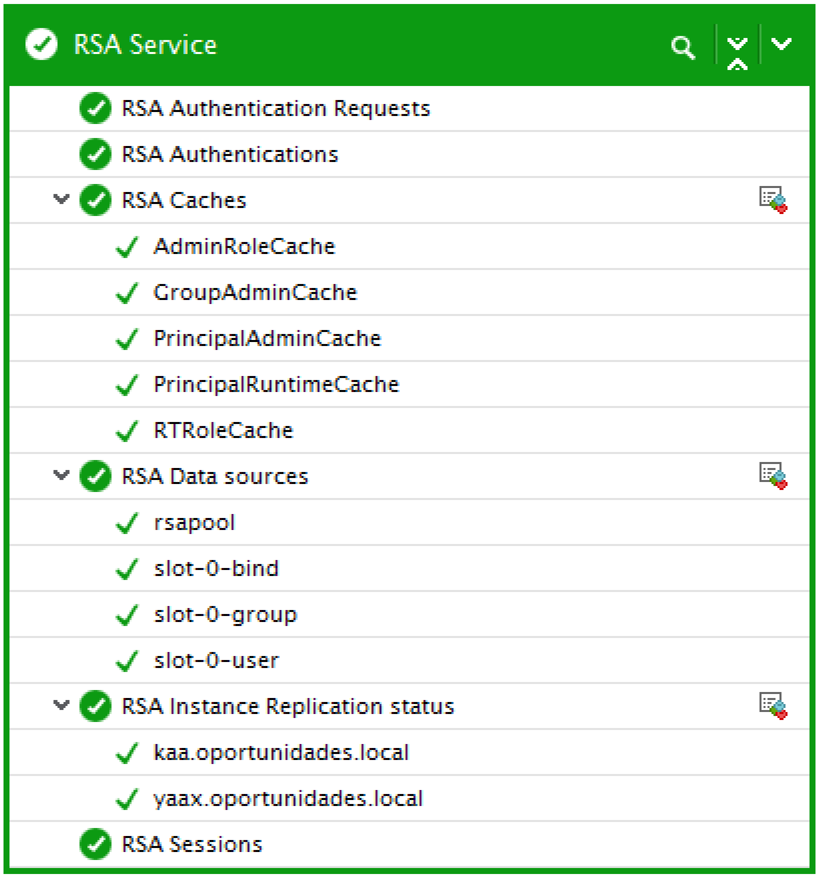


Figure 2.5: The tests mapped to the RSA Service layer

2.2.1 RSA Authentications Requests Test

This test helps administrators to figure out the rate at which the authentication requests were processed by the target RSA Authentication Manager and in the process reveals the rate at which the authentication requests were successful and the authentication requests that failed. In addition, this test reveals the average time taken to process the authentication requests and responses. This way, administrators are alerted to overload condition and the processing bottlenecks, if any.

Target of the test : A RSA Authentication Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the RSA Authentication Manager being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the

Parameter	Description
	Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Average total request	Indicates the rate at which the authentication requests were serviced by the target	Requests/Sec	

Measurement	Description	Measurement Unit	Interpretation
	RSA Authentication Manager.		
Average successful request	Indicates the rate at which the authentication requests were serviced successfully.	Requests/Sec	A high value is desired for this measure.
Average failed request	Indicates the rate at which the authentication requests failed.	Requests/Sec	Ideally, the value of this measure should be zero. A consistently high value for this measure is a cause of concern and requires the administrators to further investigate the real reason.
Average packet processed	Indicates the rate at which the packets were processed by the RSA Authentication Manager.	Packets/Sec	
Average time to process the req/res	Indicates the average time taken by the RSA Authentication Manager to process authentication requests and responses.	Milliseconds	A low value is desired for this measure. A high value of this measure indicates that the appliance took too long to process the authentication requests and responses.

2.2.2 RSA Authentications Test

Using the unique multi-factor authentication, the RSA Authentication Manager verifies security pins, security tokens and the user’s identity for servicing authentication requests. This way, the RSA Authentication Manager guarantees that only authorized users are granted permission to access the enterprise's network.

If the RSA Authentication Manager is rendered unavailable for a while or is unable to process authentications owing to an overload condition or network malfunction, then, the authentication failure may increase rapidly. This may in turn may stall operations of the RSA Authentication Manager and lead to unauthorized user access on the enterprise's network exposing critical data. Added to this, valid users may also be denied access. Authentication failures may directly impact the security of the enterprise's network which leads to data loss and may pave way for malicious attacks on the enterprise's network. To avert such issues, administrators should continuously track the authentications processed by the RSA Authentication Manager, and capture abnormalities before users start complaining. The **RSA Authentications** test helps the administrators in this regard!

This test accurately pinpoints the total number of authentications processed by the RSA Authentication Manager, and the number of authentications that were processed successfully and those that failed. In addition, this test also reports the number of new PIN authentications and security token authentications that were processed.

Target of the test : A RSA Authentication Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the RSA Authentication Manager being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An

Parameter	Description
	item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data

Parameter	Description
	traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total authentication	Indicates the total number of authentications that were processed during the last measurement period.	Number	A high value of this measure could indicate a potential overload condition.
Successful authentication	Indicates the number of authentications that were processed successfully during the last measurement period.	Number	A high value is desired for this measure.
Failed authentication	Indicates the number of authentications that failed during the last measurement period.	Number	Ideally, the value of this measure should be zero. A non-zero value for this measure is a cause of concern and requires further investigation.
Failure authentication pct	Indicates the percentage of authentications that failed on the target RSA Authentication Manager.	Percent	
New pin authentication	Indicates the number of new PIN authentications that were processed during the last measurement period.	Number	
Next token code authentication	Indicates the number of token code authentications that were processed during the last measurement period.	Number	

2.2.3 RSA Caches Test

Cache that is right-sized and well-used can significantly enhance performance of the RSA Authentication Manager! The cache is said to be effectively utilized only if it is able to service the maximum number of requests to the RSA Authentication Manager; this greatly reduces direct disk accesses and related overheads, and thus improves performance. On the contrary, ineffective cache usage can be the key contributor to a slowdown or degradation in performance, as it increases disk accesses. To understand how the caches are utilized and to promptly capture abnormalities in cache usage, administrators have to continuously monitor the size of each cache. If the cache is not updated for a prolonged time period, then the requests served by the cache may contain obsolete entities. This may cause old policies and data of user group to be pushed to the end users, which in turn may pose a serious security thread to the enterprise's data.

This test monitors each cache of the RSA Authentication Manager and reports its usage - both in terms of size and its request serving ability. In the process, the test proactively alerts administrators to the under-utilization and improper size of the cache, and helps them quickly initiate corrective measures.

Target of the test : A RSA Authentication Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each cache of the RSA Authentication Manager being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameter	Description
	is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameter	Description
	- **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Cache size	Indicates the total size of this cache.	MB	
Cache hit ratio	Indicates the percentage of authentication requests that were successfully retrieved from this cache.	Percentage	A high value is desired for this measure.
Cache flush count	Indicates the number of times this cache was flushed.	Number	Cache is flushed to remove old information from memory. When the cache is flushed, each selected object is refreshed from the database the next time it is accessed. Cache contents are refreshed every 10 minutes. Depending on cache settings, database replicated changes to cached data may take up to 10 minutes to display on all instances after a change occurs on the primary.

Measurement	Description	Measurement Unit	Interpretation
			If you do not want to wait for the automatic 10-minute refresh, you can flush the cache on each individual instance.

2.2.4 RSA Data Sources Test

An identity source is a repository that contains user and user group data. Each user and user group in a deployment is associated with an identity source. An identity source can store data in the internal database (which is installed within the RSA Authentication Manager), or one or more LDAP directories. If the internal database is used as an identity source, then, all users, applications, user group, policy, and token data are stored in the internal database. If the RSA Authentication Manager is integrated with identity sources such as Microsoft Active Directory, Sun Java System Directory Server or Oracle Directory Server, only the user and user group data reside in the external identity source. The policy and token data associated with the user and user group are stored only in the internal database. Each type of identity source manages and accesses data differently for processing the authentication requests. By continuously monitoring the identity sources, administrators can easily figure out the identity source that is currently experiencing processing bottlenecks thereby affecting the performance of the RSA Authentication Manager. The **RSA Data Sources** test helps administrators to figure out such identity sources so that the real reason behind processing bottlenecks can be analyzed and rectified at the earliest.

This test auto-discovers the identity sources in the target RSA Authentication Manager and reveals how well the authentication requests were processed. In addition, this test helps administrators figure out the identity source on which maximum authentication requests failed and the identity source that took too long to respond to the authentication requests. In the process, this test also throws light on the identity source that is active and busy processing the requests.

Target of the test : A RSA Authentication Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each identity source of the RSA Authentication Manager being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the

Parameter	Description
	Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total requests	Indicates the total number of authentication requests that were processed for	Number	A high value of this measure could indicate a potential overload.

Measurement	Description	Measurement Unit	Interpretation
	this identity source during the last measurement period.		
Request rate	Indicates the rate at which the authentication requests are serviced successfully for this identity source.	Requests/Sec	A high value is desired for this measure.
Failed requests	Indicates the number of authentication requests that failed for this identity source during the last measurement period.	Number	Ideally the value of this measure should be zero. Comparing the value of this measure against all the identity sources would reveal the identity source that failed to authenticate the maximum number of requests .
Average response time	Indicates the time taken by this identity source to respond to the authentication requests received.	Milliseconds	Ideally, the value of this measure should be low. Compare the value of this measure to figure out the identity source that takes too long to authenticate the requests.
Active connections	Indicates the number of connections that are currently active on this identity source.	Number	A high value is desired for this measure. A high value of this measure indicates that the identity source is busy processing the requests.

2.2.5 RSA Instance Replication Status Test

A deployment of the RSA Authentication Manager includes a primary instance, and one or more replica instances. The primary instance is the Authentication Manager appliance that you deployed initially. The replica instances are added to the deployment to provide deployment-level redundancy of the primary instance. This redundant deployment protects the appliance against unexpected failures and hardware disasters, facilitates scheduled maintenance, and ensures availability of all authentication services. In the deployment, the primary instance handles all administration and user authentication operations and replicates the operation log data on every replica instance. This way, the replica instance is synchronized with the primary instance. Whenever the primary instance is under maintenance, or down or failed, administrators may want the replica instance to take over quickly from the primary instance. If the replica instance is unresponsive or unable to take over the primary instance quickly, then, there may be too much of non-sync between the primary instance and the replica instance. This in turn may cause delay in authentication operations and result in data loss and performance lag. To avoid such eventualities, administrators should monitor the status of the replica instance periodically. The **RSA Instance Replication Status** test aids administrators in this exercise!

This test auto- discovers the replica instances in the target RSA Authentication Manager deployments, and accurately reveals the current status of each replica instance.

Target of the test : A RSA Authentication Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for every replication instance of the RSA Authentication being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify

Parameter	Description
	the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test

Parameter	Description
	should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Replication status</td><td>Indicates the current replication status of this replica instance.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Healthy</td><td>100</td></tr>
<tr><td>Out of Sync</td><td>99</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current replication status of this instance. The graph of this measure however, represents the replication status of the instance using the numeric equivalents only - 100 and 99.</td></tr>
</table>

2.2.6 RSA Sessions Test

By tracking the number of sessions to the RSA Authentication Manager, administrators can figure out the load on the appliance. If the appliance is overloaded with sessions, it may actually degrade the authentication request processing capability. In such situations, administrators may want to track the session utilization on the appliance to figure out the real cause of the overload condition. This is where the **RSA Sessions** test helps the administrators!

This test accurately reports the number of sessions that were currently active on the appliance. This way, this test alerts administrators to take remedial action before overload condition occurs.

Target of the test : A RSA Authentication Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the RSA Authentication Manager being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the

Parameter	Description
	SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such

Parameter	Description
	environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active sessions	Indicates the number of sessions that were currently active on the appliance.		This measure sheds light on the current load condition of the appliance.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.