Monitoring Ruckus ZoneDirector

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Ruckus Wireless ZoneDirector serves as a central control system for Ruckus ZoneFlex Access Points (APs). ZoneDirector provides simplified configuration and updates, wireless LAN security control, RF management, and automatic coordination of Ethernet-connected and mesh-connected APs.

Using ZoneDirector in combination with Ruckus Wireless ZoneFlex APs allows deployment of a Smart Mesh network, to extend wireless coverage throughout a location without having to physically connect each AP to Ethernet. In a Smart Mesh network, the APs form a wireless mesh topology to route client traffic between any member of the mesh and the wired network. Meshing greatly reduces the cost and time requirements of deploying an enterprise-class WLAN, in addition to providing much greater flexibility in AP placement.

ZoneDirector also integrates network, radio frequency (RF), and location management within a single system. User authentication is accomplished with an integrated captive portal and internal database, or forwarded to existing Authentication, Authorization and Accounting (AAA) servers, such as RADIUS or Active Directory. Once users are authenticated, client traffic is not required to pass through ZoneDirector, thereby eliminating bottlenecks when higher speed Wi-Fi technologies such as 802.11n are used.

Since access point failures, WLAN failures, inefficiencies, and delays can cause prolonged outages and cost an enterprise money and reputation, the continuous operation and good health of the Ruckus ZoneDirector is of great importance. To ensure this, eG Enterprise provides a specialized Ruckus ZoneDirector monitoring model.

Chapter 2: How does eG Enterprise Monitor the Ruckus ZoneDirector?

eG Enterprise is capable of monitoring the Ruckus ZoneDirector in an agentless manner. For this, a single eG agent deployed on a remote Windows host is required. This agent communicates with the Ruckus ZoneDirector via SNMP and periodically monitors the SNMP- MIB of the Ruckus ZoneDirector to pull out the metrics pertaining to its performance. The key pre- requisite for monitoring the Ruckus ZoneDirector is that the target Ruckus ZoneDirector should be SNMP-enabled.

To start monitoring the Ruckus ZoneDirector, you have to manage the component using the eG administrative interface. The following section helps you to manage the Ruckus ZoneDirector in the eG administrative interface.

2.1 Managing the Ruckus ZoneDirector

The eG Enterprise cannot automatically discover the Ruckus ZoneDirector 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 Ruckus ZoneDirector 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 Ruckus ZoneDirector as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

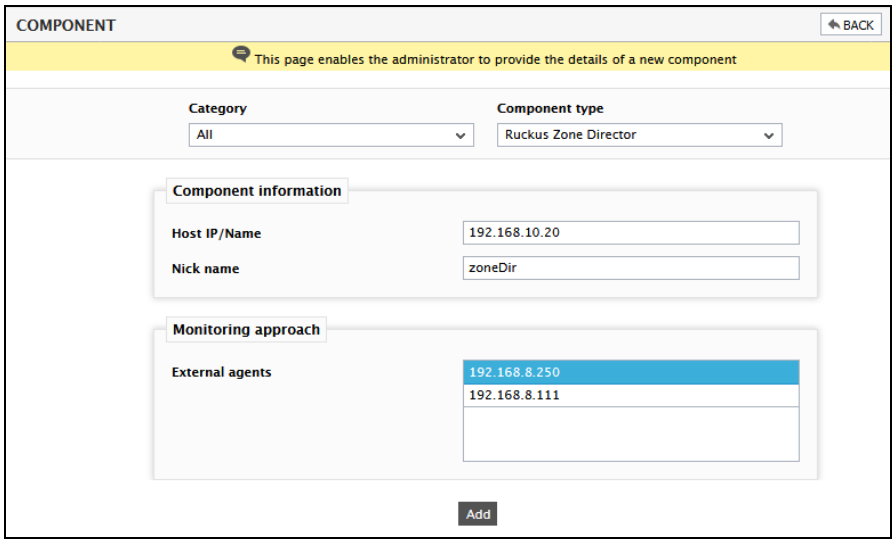

Figure 2.1: Adding the Ruckus ZoneDirector

4. Specify the **Host IP** and the **Nick name** of the Ruckus ZoneDirector 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 'Ruckus Zone Director'

Performance		zoneDir
AccessPoint Details	AccessPoint Radio Details	AccessPoint UpTime Details
CPU Details	Device Details	Ethernet Details
Memory Details	Rogue Device Details	Ruckus UpTime
System Details	WLAN Details	WLAN User Details
ZD Detail Statistics		

Configuration		zoneDir
AccessPoint Details	Ruckus System Details	Ruckus System Ip Details
Ruckus System management	Ruckus User Details	Ruckus WLAN Details

Figure 2.2: List of tests to be configured for the Ruckus ZoneDirector

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

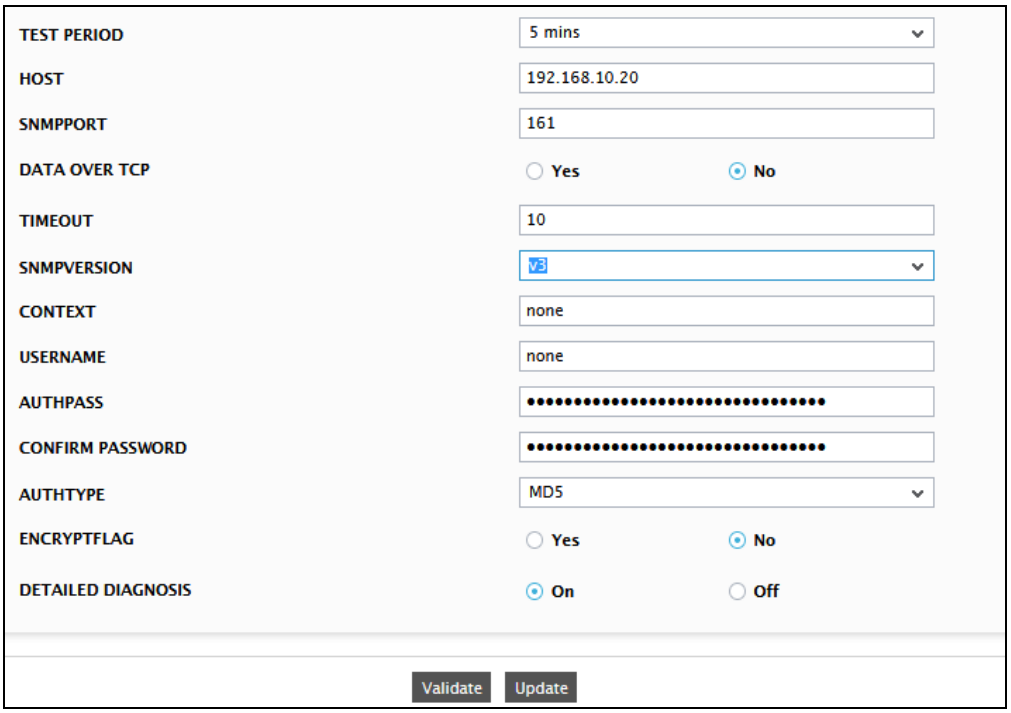

Figure 2.3: Configuring the AccessPoint Details test

7. To know how to configure the tests, refer to **Monitoring the Ruckus ZoneDirector** chapter.
8. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Ruckus ZoneDirector

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

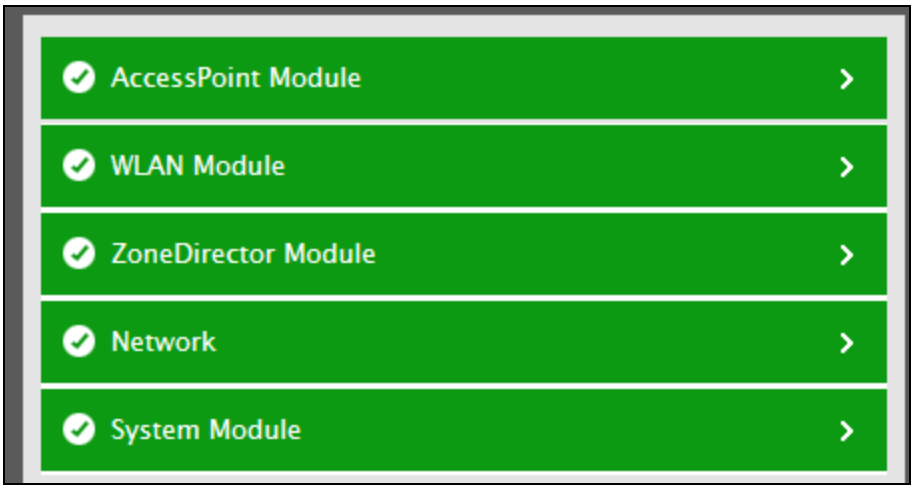

Figure 3.1: The layer model of the Ruckus ZoneDirector

Each layer of Figure 3.1 is mapped to a variety of tests each of which report a wealth of metrics related to the Ruckus ZoneDirector that is being monitored. Using these metrics administrators can find quick and accurate answers to the following queries:

- What is the status of each Access Point?
- How well data is received by and transmitted through each Access Point?
- How well memory is utilized by eeach Access Point?
- What is the rate of unicast and multicast packets transmitted and received by each Access Point?
- Has the Access Point been rebooted?
- What is the uptime of each Access Point?
- How well data is transmitted and received by each radio associated with an Access Point?
- What is the current transmit power status of each radio?
- What is the rate of unicast and multicast packets transmitted and received by each radio associated with each Access Point?

- What is the percentage of CPU utilized by the target Ruckus ZoneDirector?
- How well the memory is being utilized by the target Ruckus ZoneDirector?
- How many Access Points are registered with the target Ruckus ZoneDirector?
- How many authorized devices and unauthorized devices are connected to the target Ruckus ZoneDirector?
- What is the current status of each Ethernet port?
- How well data is transmitted through and received from each Ethernet Port?
- What is the rate at which packets were transmitted through and received from each Ethernet port?
- What is the rate at which packets were dropped during transmission and reception on each Ethernet port?
- What is the radio type of each rogue device detected on the target Ruckus ZoneDirector?
- What is the type of each rogue device detected on the target Ruckus ZoneDirector?
- What is the encryption mode of each rogue device?
- What is the uptime of the target Ruckus ZoneDirector?
- Has the target Ruckus ZoneDirector been rebooted recently? If so, when did the reboot happen?
- What is the percentage of CPU and memory utilized by the WLANs of the target Ruckus ZoneDirector?
- How well data is transmitted and received over each WLAN?
- How well packets are received and transmitted over each WLAN?
- How many authentications were successful on each WLAN?
- How many authentications actually failed on each WLAN?
- What is the radio type of each useron each WLAN?
- How well data is transmitted and received by each user over each WLAN?
- How well packets are transmitted and received by each user over each WLAN?
- What is the signal strength of each user?
- How well data is transmitted and received by the target Ruckus ZoneDirector?

- How well packets and multicast packets are transmitted from and received by the target Ruckus ZoneDirector?

3.1 The System Module Layer

Using the tests mapped to this layer, administrators can figure out the memory utilization and CPU utilization of the target Ruckus ZoneDirector and in the process, identify potential resource contentions, if any.

Figure 3.2: The tests mapped to the System Module layer

3.1.1 Memory Details Test

This test monitors the memory utilization of the target Ruckus ZoneDirector and proactively alerts administrators to potential resource contentions, if any.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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

Parameters	Description
	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 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

Parameters	Description
	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 memory	Indicates the total amount of memory allocated to the ZoneDirector.	MB	
Used memory	Indicates the amount of memory that is currently used by the ZoneDirector.	MB	A low value is desired for this measure.
Available memory	Indicates the amount of memory that is available for use on the	MB	A high value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
	ZoneDirector.		
Memory utilization	Indicates the percentage of memory utilized by the ZoneDirector.	Percent	A utilization value close to 100% is indicative of a memory bottleneck at the ZoneDirector.

3.1.2 CPU Details Test

Often excess traffic to a Ruckus ZoneDirector can impose a prohibitive load on the ZoneDirector, choking the CPU and hence making it a bottleneck. Using this test, administrators can figure out the current CPU utilization of the zone director thus enabling them to take remedial actions immediately if the ZoneDirector is found to utilize the CPU resources excessively.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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

Parameters	Description
	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: • DES – Data Encryption Standard • AES – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.

Parameters	Description
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
CPU utilization	Indicates the percentage of CPU utilized by the zone director.	Percent	A very high value could indicate a CPU bottleneck at the zone director.

3.2 The Network Layer

Using the test mapped to this layer, administrators can figure out the uptime of the target Ruckus ZoneDirector and in the process identify when exactly the Ruckus ZoneDirector was restarted.

Figure 3.3: The test mapped to the Network layer

3.2.1 Ruckus UpTime Test

In most network environments, it is essential to monitor the uptime of critical components such as the Ruckus ZoneDirector. By tracking the uptime of the ZoneDirector, administrators can determine what percentage of time the ZoneDirector has been up. Comparing this value with service level targets, administrators can determine the most trouble-prone areas of the infrastructure.

In some environments, administrators may schedule periodic reboots of the ZoneDirector. By knowing that the ZoneDirector has been up for an unusually long time, an administrator may come to know that the scheduled reboot task is not working.

This test helps administrators to monitor the uptime of the Ruckus ZoneDirector.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Ruckus ZoneDirector being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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

Parameters	Description
	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 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
Has the system been rebooted?	Indicates whether the ZoneDirector has been rebooted or not.		If this measure shows 1, it means that the ZoneDirector was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this ZoneDirector was rebooted.
Uptime during the last measure period	Indicates the time period that the ZoneDirector has been up since the last time this test ran.	Secs	If the ZoneDirector has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the ZoneDirector was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the ZoneDirector was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period – the smaller the measurement period, greater the accuracy.
Total uptime of the system	Indicates the total time that the ZoneDirector has been up since its last reboot.		This measure displays the number of years, months, days, hours, minutes and seconds since the last reboot. Administrators may wish to be alerted if a ZoneDirector has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

3.3 The WLAN Module Layer

Using the tests associated with this layer, administrators can figure out the radio type of each user accessing the WLANs of the Ruckus ZoneDirector, the data transmitted and received by each user etc. Administrators can also figure out the data transmitted and received through each WLAN and in the process figure out the WLAN that is transmitting the maximum/minimum amount of data.

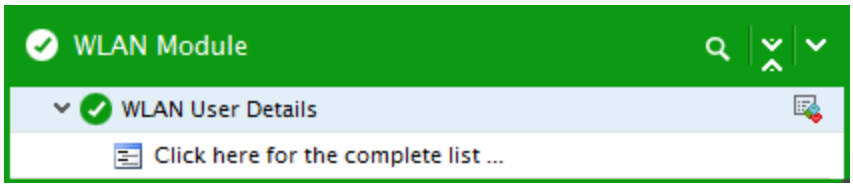

Figure 3.4: The tests mapped to the WLAN Module layer

3.3.1 WLAN Details Test

This test reveals performance measures pertaining to the WLANs that are connected to the Ruckus ZoneDirector. Using the authentication related statistics reported by this test, administrator is able to isolate authentication failures and take immediate actions before the performance of the WLAN lags.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for every WLAN connected to the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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.

Parameters	Description
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:

Parameters	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
Authorized client devices	Indicates the number of authorized client devices accessing this WLAN.	Number	
Data transmitted	Indicates the rate at which data was transmitted over this WLAN.	MB/sec	
Data received	Indicates the rate at which data was received over this WLAN.	MB/sec	
Packets transmitted	Indicates the rate at which the packets were transmitted over this WLAN.	Packets/sec	
Packets received	Indicates the rate at which the packets were received over this WLAN.	Packets/sec	
Transmitted data on	Indicates the rate at which	MB/sec	

Measurement	Description	Measurement Unit	Interpretation
LAN	data was transmitted from this WLAN to the Ruckus ZoneDirector over LAN .		
Received data on LAN	Indicates the rate at which data was received by this WLAN from the Ruckus ZoneDirector over LAN .	MB/sec	
Total authentication	Indicates the total number of authentications performed by this WLAN.	Number	
Success authentication	Indicates the number of authentications that were performed successfully by this WLAN.	Number	A high value of this measure indicates that more number of authorized clients are accessing the network.
Failed authentication	Indicates the number of authentications that failed.	Number	Ideally, the value of this parameter should be low.
Percentage of failed authentication	Indicates the percentage of number of authentications performed by this WLAN.	Percent	A significant increase in the value of this measure is a cause for concern.

3.3.2 WLAN User Details Test

This test auto-discovers the WLAN users who are logged in on the WLANs that are under control of the Ruckus ZoneDirector and reveals the radio type to which each user is associated with. For each user, this test measures the rate at which the packets were transmitted/received, the rate at which the data was transmitted/received, and the rate at which the error packets transmitted/received. In addition, this test reports the number of times the transmission was retried by each user and the amount of data retransmitted by each user after transmission failure. In the process, administrator can also detect the Signal- to- Noise ratio for each user and the strength of signals transmitted/received by each user.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for each user on the WLANs that are under control of the target Ruckus ZoneDirector being monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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.

Parameters	Description
	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 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**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG

Parameters	Description
	agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Radio type	Indicates the type of radio to which this user is associated with.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** Radio11a: 0 Radio11b: 1 Radio11g: 2 Radio11ng: 3 Radio11na: 4 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the Radio type of this user. The graph of this measure however, represents the type of a rogue device using the numeric equivalents only - 0 and 4. The detailed diagnosis of this measure provides you the Access point mac

Measurement	Description	Measurement Unit	Interpretation
			address and service set ID (SSID) of the WLAN user.
Packets transmitted	Indicates the rate at which the packets were transmitted by this user.	Packets/sec	
Packets received	Indicates the rate at which the packets were received by this user.	Packets/sec	
Data transmitted	Indicates the rate at which the data was transmitted by this user.	MB/sec	
Data received	Indicates the rate at which the data was received by this user.	MB/sec	
Transmitted packets dropped	Indicates the rate at which the packets were dropped during transmission.	Packets/sec	Ideally, the value of this measure should be zero.
Received packets dropped	Indicates the rate at which the packets were dropped during reception.	Packets/sec	Ideally, the value of this measure should be zero.
Transmitted error packets	Indicates the rate at which the error packets were transmitted by this user.	Packets/sec	Ideally, the values of these measures should be zero. A higher value results in unreliable connection and affects throughput.
Received error packets	Indicates the rate at which the error packets were received by this user.	Packets/sec	
Transmitted retries	Indicates the number of times the transmission was retried by this user after transmission failure.	Number	
Transmitted retry data	Indicates the rate at which the data was retransmitted by this user after transmission failure.	MB/sec	
Signal noise ratio	Indicates the Signal-to-	dB	Ideally, the value of this measure

Measurement	Description	Measurement Unit	Interpretation
	Noise Ratio for this user.		should be high.
Signal strength	Indicates the signal strength of this user.	dBm_negative	Ideally, the value of this measure should be high. Since stronger signal strength results in more reliable communication and higher speeds.

3.4 The ZoneDirector Module Layer

Figure 3.5: The tests mapped to the ZoneDirector Module layer

3.4.1 ZD Detail Statistics Test

This test measures performance statistics pertaining to the packet transmission in the target ZoneDirector. Using these statistics, administrator can detect the load handled by the ZoneDirector and can also figure out the number of packets that were failed during transmission. In the process, this test proactively alerts administrator to processing bottlenecks on the ZoneDirector. This enables administrator to take swift actions to retransmit the failed packets before it causes performance lag.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection

Parameters	Description
	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 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

Parameters	Description
	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
Packets transmitted	Indicates the rate at which the packets were transmitted from the ZoneDirector.	Packets/sec	
Packets received	Indicates the rate at which the packets were received by the ZoneDirector.	Packets/sec	
Data transmitted	Indicates the amount of data transmitted from the ZoneDirector per second.	MB/sec	
Data received	Indicates the amount of data received by the	MB/sec	

Measurement	Description	Measurement Unit	Interpretation
	ZoneDirector per second.		
Transmitted fail packets	Indicates the number of packets that failed per second during transmission.	Packets/sec	Ideally, the value of this measure should be zero.
Transmitted retry packets	Indicates the rate at which the packets were retried after transmission failure.	Packets/sec	
Multicast packets transmitted	Indicates the rate at which the multicast packets were transmitted from the ZoneDirector.	Packets/sec	
Multicast packets received	Indicates the rate at which the multicast packets were received by the ZoneDirector.	Packets/sec	

3.4.2 ZD WLAN Detail Statistics Test

Using this test, administrators can figure out how well the WLANs utilize the CPU and memory resources of the Ruckus ZoneDirector and can take remedial actions immediately if the WLANs are found to utilize the CPU and memory resources of the ZoneDirector excessively.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection

Parameters	Description
	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 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

Parameters	Description
	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
CPU utilization	Indicates the percentage of CPU utilized by the WLAN.	Percent	An unusually high value or a consistent increase in this value is indicative of abnormal CPU usage which requires further investigation.
Memory utilization	Indicates the percentage of memory utilized by the WLAN.	Percent	A significant increase in this value could be a cause for some serious concern, as it indicates a gradual, but steady erosion of valuable memory resources.

3.4.3 Rogue Device Details Test

A rogue device is an unauthorized device that is connected to an organization's network but does not have permission to access and operate in the network. The rogue devices can be broken down into two categories:

- Access point (AP) -based rogue devices - Wireless access points (WAP) installed in the network without authorization
- Computer-based rogue threats, or rogue peers - end user computers that are connected to the network without permission

The rogue device can impose significant threats to the network and is able to create a conduit for theft of confidential system information. The rogue device potentially allows unchallenged access to the network by any wireless user or client in the physical vicinity and also floods the network with useless data. This way, the rogue devices undermine the security of the network, create a denial of service to the authorized users and potentially damage the organization. It is, therefore, vital for administrator to detect and control the rogue devices connected to the network before they cause serious damage to the network. This is where the **Rogue Device Details** test helps administrator!

For each rogue device connected to the network, this test reveals the radio type, the number of channels associated with it, the type of device, the encryption mode and strength of the signals.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for each rogue device that accesses the network in an unauthorized way

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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.

Parameters	Description
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 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

Parameters	Description
	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**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Radio type	Indicates the radio type of this rogue device.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Radio11bg</td><td>0</td></tr>
<tr><td>Radio11a</td><td>1</td></tr>
<tr><td>Radio11ng</td><td>2</td></tr>
<tr><td>Radio11na</td><td>3</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the Radio type of this rogue device. The graph of this measure however, represents the type of a rogue device using the numeric equivalents only - 0 and 3.
</td></tr>
<tr><td>Channel</td><td>Indicates the number of channels associated with this rogue device.</td><td>Number</td><td></td></tr>
<tr><td>Rogue type</td><td>Indicates the type of this rogue device.</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>AP</td><td>1</td></tr>
<tr><td>Ad-hoc</td><td>2</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the type of this rogue device. The graph of this measure however, represents the type of a rogue device using the numeric equivalents only - 1 and 2.
</td></tr>
<tr><td>Encryption mode</td><td>Indicates the encryption mode of this rogue device.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Open</td><td>0</td></tr>
<tr><td>Encrypted</td><td>1</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the encryption mode of this rogue device. The graph of this measure however, represents the encryption mode of a rogue device using the numeric equivalents only - 0 and 1.
</td></tr>
<tr><td>Signal strength</td><td>Indicates the signal strength of this rogue device.</td><td>dBm_negative</td><td>Ideally, the value of this measure should be low.</td></tr>
</table>

3.4.4 Device Details Test

This test reveals statistics about the access points registered with the Ruckus ZoneDirector and the number of authorized and unauthorized devices connected to the ZoneDirector. Using these details, administrator can detect load on the ZoneDirector and also find out the number of users who utilize the network bandwidth of the organization without permission. This way, administrator can be proactively alerted to overload condition, if any and breach in network security before anything untoward happen.

shared by the unauthorized attackers.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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 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:

Parameters	Description
	• **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**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total accesspoints	Indicates the total number of access points registered with the ZoneDirector.	Number	Use the detailed diagnosis of this measure to know the details about all the access points that were added to the ZoneDirector.
Total authorized devices	Indicates the total number of authorized devices connected to the ZoneDirector.	Number	
Total unauthorized devices	Indicates the total number of unauthorized devices connected to the ZoneDirector.	Number	Ideally, the value of this measure should be zero.

3.4.5 ZD WLAN Detail Statistics Test

Using this test, administrators can figure out how well the WLANs utilize the CPU and memory resources of the Ruckus ZoneDirector and can take remedial actions immediately if the WLANs are found to utilize the CPU and memory resources of the ZoneDirector excessively.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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.

Parameters	Description
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 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

Parameters	Description
	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
CPU utilization	Indicates the percentage of CPU utilized by the WLAN.	Percent	An unusually high value or a consistent increase in this value is indicative of abnormal CPU usage which requires further investigation.
Memory utilization	Indicates the percentage of memory utilized by the WLAN.	Percent	A significant increase in this value could be a cause for some serious concern, as it indicates a gradual, but steady erosion of valuable memory resources.

3.4.6 Ethernet Details Test

The Ruckus ZoneDirector is provided with two Ethernet ports that are used to establish connection between the ZoneDirector and Access Points (APs). Each Ethernet port can be connected to a separate AP. Availability and operability of the ports are important for active and healthy

communication between the ZoneDirector and the APs. If the ports are down due to overloaded requests or huge number of packets are dropped at the ports, then the functionality and reliability of the ports become questionable. This brings all traffic a near halt and directly affects the communication between the ZoneDirector and the APs. To avoid such eventualities, administrator should keep track on traffic flowing through the ports so as to ensure reliable communication between the ZoneDirector and the APs.

This test auto-discovers the Ethernet ports on the ZoneDirector and reveals the current state of each port. In the process, this test reports the amount of data received/transmitted per second, the count of packets transmitted/received per second and the number of packets dropped per second during transmission/reception of packets through each port. In addition, this test also sheds lights on the utilization of each port.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for the every Ethernet port available on the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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

Parameters	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

Parameters	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

Measurement	Description	Measurement Unit	Interpretation
Ethernet status	Indicates the current status of this Ethernet port.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** Up / 1 Down / 2 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current state of this port. The graph of this measure however, represents the status of a resource using the numeric equivalents only - 1 and 2.
Packets transmitted	Indicates the rate at which the packets were transmitted through this port.	Packets/Sec	
Packets received	Indicates the rate at which the packets were received through this port.	Packets/Sec	
Data transmitted	Indicates the rate at which	MB/Sec	

Measurement	Description	Measurement Unit	Interpretation
	the data was transmitted through this port.		
Data received	Indicates the rate at which the data was received through this port.	MB/Sec	
Transmitted packets dropped	Indicates the number of packets dropped per second during transmission through this port.	Packets/Sec	
Received packets dropped	Indicates the number of packets dropped per second during reception through this port.	Packets/Sec	
Ethernet utilization	Indicates the utilization percentage of this port.	Percent	A value close to 100 is a cause for concern.

3.5 The AccessPoint Module Layer

Using the tests mapped to this layer, administrators may be able to figure out the status of the access points, the memory and CPU utilization of each access point and the data transmitted to and from the access points. The radios associated with each access point is also discovered and the data transmitted to and from each radio is monitored. The uptime of each acess point is also monitored and irregularities detected with ease!

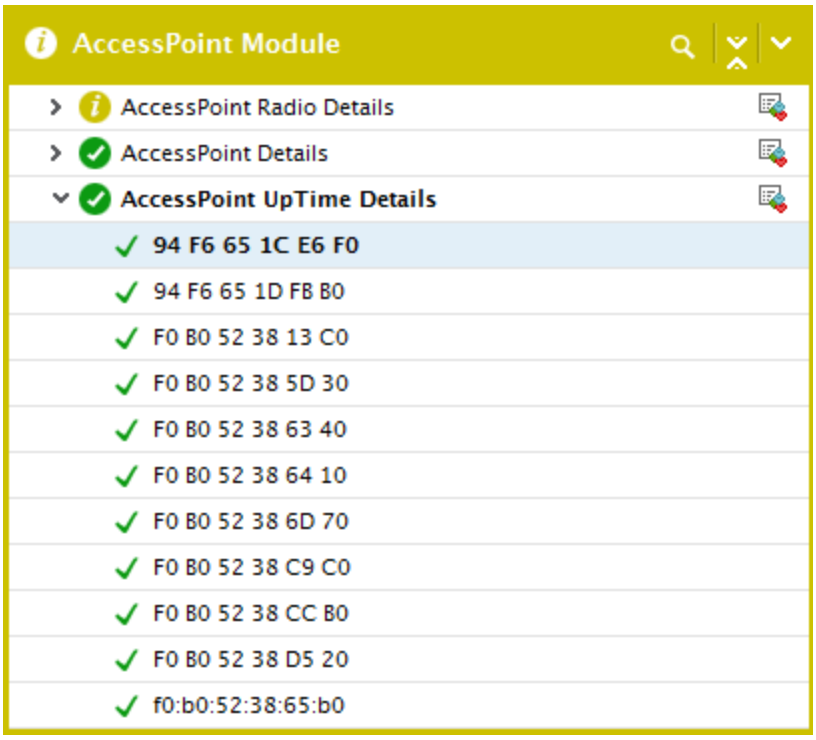

Figure 3.6: The tests mapped to the AccessPoint Module layer

3.5.1 AccessPoint Details Test

The Ruckus ZoneDirector controls multiple access points that are registered with it. In a wireless local area network (WLAN), an access point is a station that transmits and receives data (sometimes referred to as a transceiver). The access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each access point can serve multiple users within a defined network area. If multiple access points are not available for the users to connect, then the users may not be able to connect to the WLAN. This would cause sever hardship to the users and therefore, it becomes necessary to monitor the access points round the clock. The **AccessPoint Details** test helps administrators in this regards!

This test auto discovers the access points controlled by the ZoneDirector and reveals the total number of radios and authorized devices that are associated with each access point. In the process, this test reports current status, CPU utilization and memory utilization of each access point. This test also sheds light on the amount of data transmitted and received over the LAN and the number of unicast packets and multicast packets that are transmitted and received over the LAN.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for every access point controlled by the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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.

Parameters	Description
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 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**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

Parameters	Description
	• The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total radios	Indicates the total number of radios in this access point.	Number	Use the detailed diagnosis of this measure to know about MAC address of each radio available in the access points.
Total authorized devices	Indicates the total number of authorized client devices associated with this access point.	Number	
Accesspoint status	Indicates the current operational status of this access point.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** Disconnected: 0 Connected: 100 Approval Pending: 2 Provisioning: 4 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current status of this access point. The graph of this measure however, represents the current status of this access point using the numeric equivalents only.
CPU utilization	Indicates the percentage	Percent	

Measurement	Description	Measurement Unit	Interpretation
	of CPU utilized by this access point.		
Memory utilization	Indicates the percentage of memory utilized by this access point.	Percent	
Data Transmitted	Indicates the rate at which the data was transmitted from this access point.	MB/sec	
Data received	Indicates the rate at which the data was received by this access point.	MB/sec	
Transmitted data on LAN	Indicates the rate at which the data was transmitted from this access point over LAN.	MB/sec	
Received data on LAN	Indicates the rate at which the data was received by this access point over LAN.	MB/sec	
Transmitted packets on LAN	Indicates the rate at which the packets were transmitted from this access point over LAN.	Packets/sec	
Received packets on LAN	Indicates the rate at which the packets were received by this access point over LAN.	Packets/sec	
Transmitted unicast packets on LAN	Indicates the rate at which the unicast packets were transmitted from this access point over LAN.	Packets/sec	
Received unicast packets on LAN	Indicates the rate at which the unicast packets were received by this	Packets/sec	

Measurement	Description	Measurement Unit	Interpretation
	access point over LAN.		
Transmitted mutlicast packets on LAN	Indicates the rate at which the multicast packets were transmitted from this access point over LAN.	Packets/sec	
Received multicast packets on LAN	Indicates the rate at which the multicast packets were received by this access point over LAN.	Packets/sec	

3.5.2 AccessPoint Radio Details Test

This test auto-discovers the radios available in the access points that are associated with the Ruckus ZoneDirector and measures the resource utilization and data transmitted and received by each radio. This test also reveals the rate at which the packets were transmitted and received and the rate at which the failed transmitted packets were retransmitted. Besides, this test reports the number of authentications that were performed successfully and the number of authentications that failed.

Using these statistics, administrators can easily figure out the reasons behind the bottle-neck condition in the radios, can isolate the transmission failures and authentication related issues and can fix those issues quickly.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for each radio available in the access points that are controlled by the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.

Parameters	Description
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 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

Parameters	Description
	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
Resource utilization	Indicates the percentage of resource utilized by this radio.	Percent	A utilization value close to 100% is a cause for concern.
Data Transmitted	Indicates the rate at which the data was transmitted from this radio.	MB/sec	
Data received	Indicates the rate at which the data was received by this radio.	MB/sec	
Packets transmitted	Indicates the rate at which the packets were	Packets/sec	

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>transmitted from this radio.</td><td></td><td></td></tr>
<tr><td>Packets Received</td><td>Indicates the rate at which the packets were received by this radio.</td><td>Packets/sec</td><td></td></tr>
<tr><td>Multicast packets transmitted</td><td>Indicates the rate at which the multicast packets were transmitted from this radio.</td><td>Packets/sec</td><td></td></tr>
<tr><td>Multicast packets transmitted</td><td>Indicates the rate at which the multicast packets were received by this radio.</td><td>Packets/sec</td><td></td></tr>
<tr><td>Failed transmitted packets</td><td>Indicates the rate at which the packets were failed during transmission.</td><td>Packets/sec</td><td></td></tr>
<tr><td>Retry transmitted packets</td><td>Indicates the rate at which the packets were retransmitted by this radio after transmission failure.</td><td>Packets/sec</td><td></td></tr>
<tr><td>Success authentication</td><td>Indicates the number of authentications that were performed successfully by this radio.</td><td>Number</td><td></td></tr>
<tr><td>Failed authentication</td><td>Indicates the number of authentications that failed.</td><td>Number</td><td>Ideally, the value of this measure should be zero.</td></tr>
<tr><td>Transmit power of radio</td><td>Indicates the current transmit power status of this radio.</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>Full</td><td>0</td></tr><tr><td>Half</td><td>1</td></tr><tr><td>Quarter</td><td>2</td></tr><tr><td>Eighth</td><td>3</td></tr></table>
Note:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>By default, this measure reports the Measure Values listed in the table above to indicate the current transmit power status of this radio. The graph of this measure however, represents the current transmit power status using the numeric equivalents only.</td></tr>
<tr><td>Power management status</td><td>Indicates the current power management status of this radio.</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>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>0</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current power management status of this radio. The graph of this measure however, represents the current power management status of this radio using the numeric equivalents only.</td></tr>
</table>

3.5.3 Access Point UpTime Test

In most wireless network environments, it is essential to monitor the uptime of critical components such as the Access Points (APs) in the infrastructure. By tracking the uptime of the access point, administrators can determine what percentage of time the access point has been up. Comparing this value with service level targets, administrators can determine the most trouble-prone areas of the infrastructure.

In some environments, administrators may schedule periodic reboots of the access point. By knowing that the access point has been up for an unusually long time, an administrator may come to know that the scheduled reboot task is not working.

This test included in the eG agent monitors the uptime of the access point.

Target of the test : A Ruckus ZoneDirector

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Access Point (AP) that is connected to the target Ruckus ZoneDirector being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default 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*.

Parameters	Description
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 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
Has the system been rebooted?	Indicates whether this access point has been rebooted or not.		If this measure shows 1, it means that the AP was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this AP was rebooted.
Uptime during the last measure period	Indicates the time period that this access point has been up since the last time this test ran.	Secs	If the AP has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the AP was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the AP was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period – the smaller the measurement period, greater the accuracy.
Total uptime of the system	Indicates the total time that this access point has been up since its last reboot.		This measure displays the number of years, months, days, hours, minutes and seconds since the last reboot. Administrators may wish to be alerted if a AP has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

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.