Monitoring Cisco Wireless Accesspoint

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Cisco WAP Wireless-AC/N Dual Radio Access Point with Single Point Setup is a simple yet powerful, high-performance access point. It offers business-class features such as Gigabit Ethernet connectivity, a captive portal for customized guest access, and robust security. The Cisco WAP provides cost-effective 802.11ac wireless connectivity for improved mobility experience to your guests and employees. Key features and benefits:

- Provides 802.11ac wireless connectivity up to three times the 802.11n speed
- Gigabit Ethernet LAN interface with Power over Ethernet (PoE) supports flexible installation
- Captive portal allows for highly secure guest access with customized roles and rights
- Single Point Setup requires no controller for easy deployment of multiple access points
- Works right out of the box with easy installation and simple web-based configuration and wizard

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 Cisco Wireless Access Point is of great importance. To ensure this, eG Enterprise provides a specialized Cisco Wireless Access Point monitoring model.

Chapter 2: How does eG Enterprise Monitor the Cisco Wireless Accesspoint?

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

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

2.1 Managing the Cisco Wireless Accesspoint

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

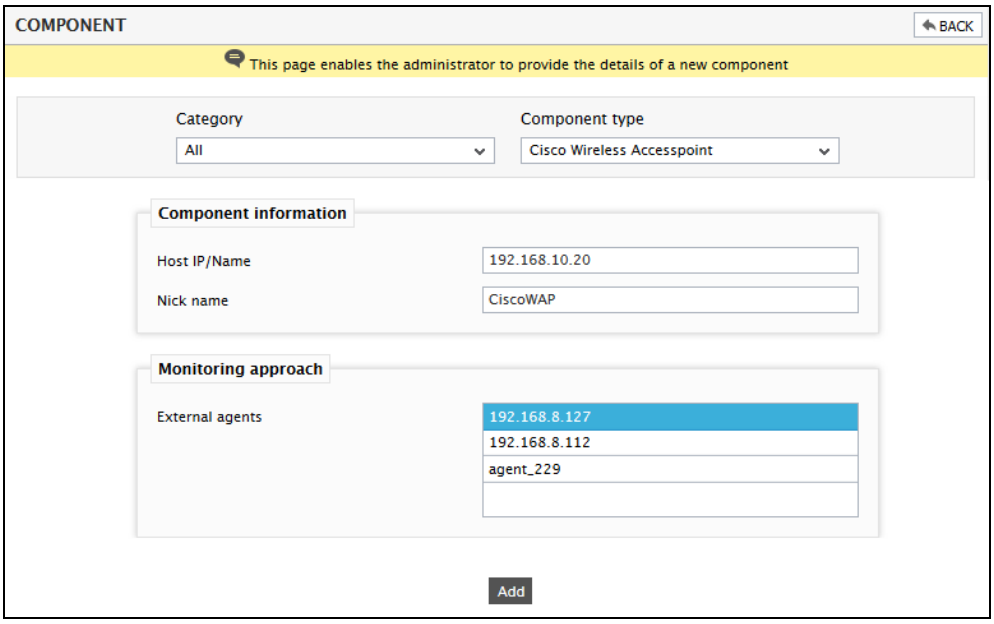

Figure 2.1: Adding the Cisco Wireless Accesspoint

4. Specify the **Host IP** and the **Nick name** of the Cisco Wireless Accesspoint 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 'Cisco Wireless Accesspoint'

Performance		CiscoWAP
Accesspoint Radio	Associated Client	Client Login Status
Device Uptime	Email Alert Status	Log Events
Network Interfaces	TSPEC Accesspoint	TSPEC Associated Client
Virtual Accesspoint	WorkGroup Downstream	WorkGroup Upstream

Configuration		CiscoWAP
Email Alert Details	Interface Details - Advanced	Logging Information
Network Interface Details	Network System Details	Radio Details
System Information	Virtual Accesspoint Details	WPS Details

Figure 2.2: List of tests to be configured for the Cisco Wireless Accesspoint

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

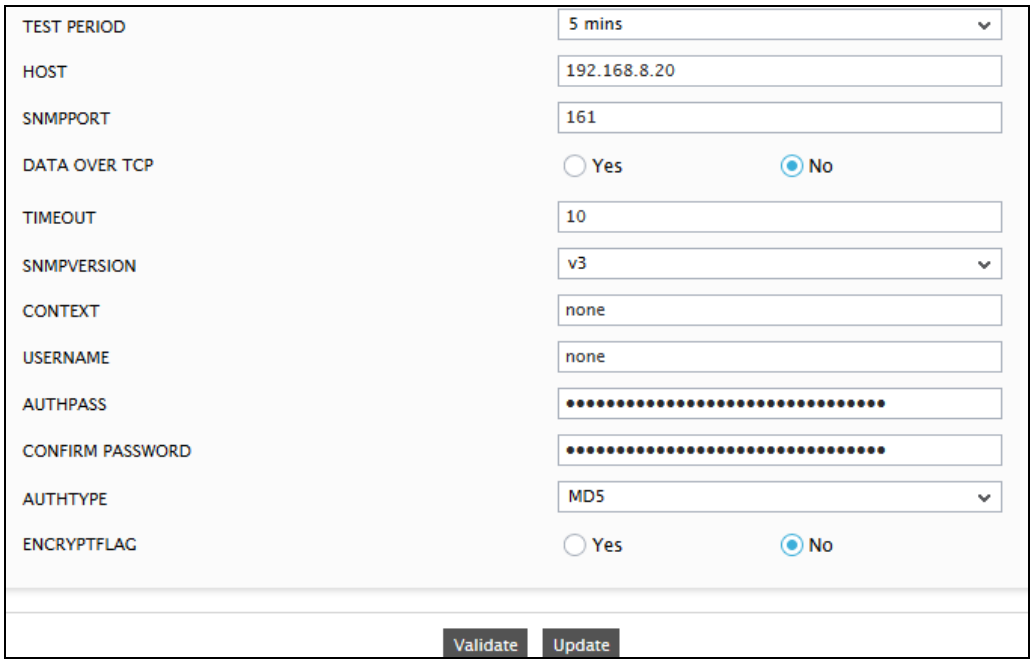

Figure 2.3: Configuring the AccessPoint Radio test

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

Chapter 3: Monitoring the Cisco Wireless Accesspoint

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

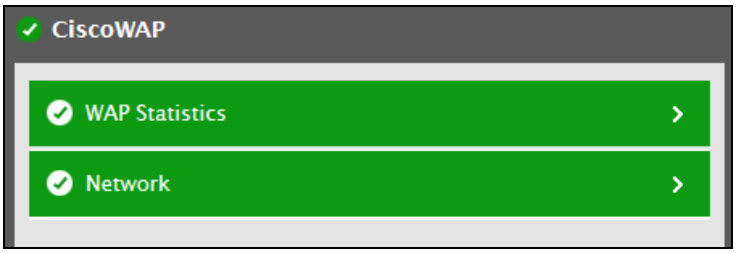

Figure 3.1: The layer model of the Cisco Wireless Accesspoint

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

- What is the administrative status and operational status of each radio on the target access point?
- How well WLAN is utilized by each radio?
- How well data was received / transmitted by each client associated with the access point?
- How many packets were received / transmitted by each client associated with the access point?
- How many packets were dropped by each client during transmission / reception?
- How many users were currently logged in to the network through the target access point?
- How many users logged out of the network through the target access point?
- What is the operational status of the email alert feature?
- How many emails were sent to the user and how many emails failed to be sent to the user?
- How many critical error events were logged in for the target access point?
- How many warning and debug events were logged in for the target access point?
- How many video calls / voice calls were accepted /rejected by the access point?
- How many packets were received / transmitted by each client through traffic stream on the target access point?

- What is the amount of data received / transmitted by each client through traffic stream on the target accesspoint?
- What is the administrative status and operational status of each virtual access point?
- What is the current connection status of each downstream workgroup?
- How many packets were received and transmitted by each downstream workgroup?
- How well data was received and transmitted by each downstream workgroup?
- What is the current connection status of each upstream workgroup?
- How many packets were received and transmitted by each upstream workgroup?
- How well data was received and transmitted by each upstream workgroup?

Since the Network layer is discussed extensively in *Monitoring Unix and Windows Servers* document, let us now discuss the tests pertaining to the other layers.

3.1 The WAP Statistics 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!

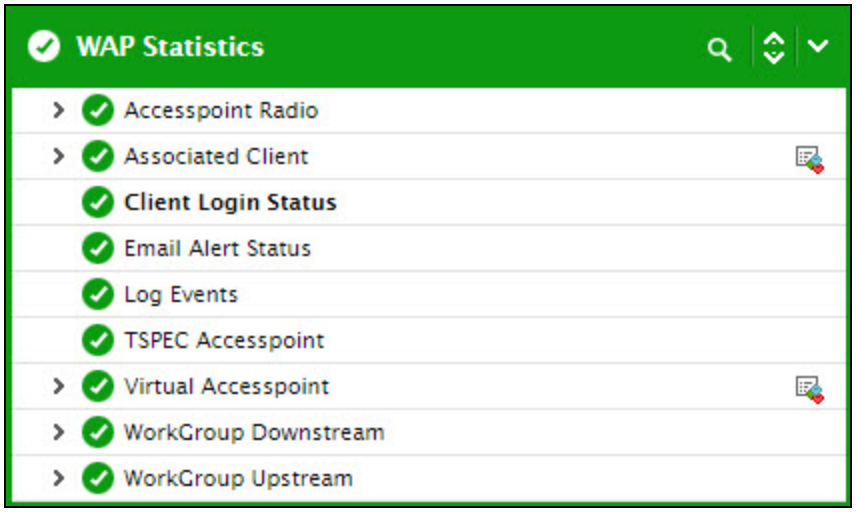

Figure 3.2: The tests mapped to the WAP Statistics layer

3.1.1 Accesspoint Radio Test

This test auto-discovers the radios available in the access points that are associated with the Cisco Wireless Accesspoint and measures the wireless LAN utilized by each radio. This test also reveals the administrative and operational status of each radio.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for each radio controlled by the target Cisco Wireless Accesspoint 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

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

Parameters	Description
	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
Administrative status	Indicates the administrative status of this radio.		The States reported by this measure and their corresponding numeric equivalents are mentioned in the table below: State: Up — Numeric Value: 1 State: Down — Numeric Value: 2 **Note:** By default, this measure reports the above-mentioned **State**s while indicating the administrative status of each radio. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., *1 or 2*.
Operational status	Indicates the current operational status of this radio.		The States reported by this measure and their corresponding numeric equivalents are mentioned in the table below: State: Up — Numeric Value: 1 State: Down — Numeric Value: 0 **Note:** By default, this measure reports the above-mentioned **State**s while

Measurement	Description	Measurement Unit	Interpretation
			indicating the operational status of each radio. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., *0 or 1*.
Channels in used	Indicates the total number of channels used to service this radio.	Number	
WLAN utilization	Indicates the percentage of wireless LAN utilized by this radio.	Percentage	

3.1.2 Associated Client Test

For each client connected to the network via the target Cisco Wireless Accesspoint, this test reveals the authentication status and the amount of data transmitted and received. This test also reports the packets transmitted from and received by each client and also throws light on the amount of data dropped during transmission/reception. Using this test, administrators can determine the client that is tranmitting/receiving the maximum amount of data and figure out if the data/packets transmitted/received is legitimate.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Network:Client* associated with the target Cisco Wireless Accesspoint 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

Parameters	Description
	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 **Yes** option.

Parameters	Description
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
is Authenticated?	Indicates the authentication status of this client on the network associated with the access point.		The values reported by this measure and their corresponding numeric equivalents are mentioned in the table below: Measure Value / Numeric Value: Yes – 1; No – 0 **Note:** By default, this measure reports the above-mentioned **Measure value**s while indicating the authentication

Measurement	Description	Measurement Unit	Interpretation
			status of each client. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., *0 or 1*.
Received packets	Indicates the number of packets received by this client during the last measurement period.	Packets	Compare the value of these measures across the clients to determine the client that is transmitting / receiving the maximum / least number of packets.
Transmitted packets	Indicates the number of packets transmitted by this client during the last measurement period.	Packets	
Received data	Indicates the amount of data received by this client during the last measurement period.	MB	Compare the value of these measures across the clients to figure out the client that is transmitting / receiving the maximum / least amount of data.
Transmitted data	Indicates the amount of data transmitted by this client during the last measurement period.	MB	
Dropped packets received	Indicates the number of packets dropped during reception by this client during the last measurement period.	Packets	Compare the value of these measures across the clients to figure out the client that dropped the maximum number of packets during transmission / reception.
Packets dropped during transmission	Indicates the number of packets dropped during transmission from this client during the last measurement period.	Packets	
Dropped data received	Indicates the amount of data dropped during reception by this client during the last measurement period.	MB	Compare the value of these measures across the clients to figure out the client that dropped the maximum amount of data during transmission / reception.
Data dropped during	Indicates the amount of	MB	

Measurement	Description	Measurement Unit	Interpretation
transmission	data dropped during transmission from this client during the last measurement period.		
Received TS violate packets	Indicates the number of packets received by this client that exceeds the normal active Traffic Stream (TS) downlink bandwidth for which the client has not been admitted.	Packets	
Transmitted TS violate packets	Indicates the number of packets transmitted from this client that exceeds the normal active Traffic Stream (TS) uplink bandwidth for which the client has not been admitted.	Packets	

3.1.3 Client Login Status Test

This test helps administrators determine the new user logins to the target Cisco Wireless Accesspoint. Using this test, administrators can also figure out the users who had logged out and the users who logged in very recently. This way, administrators can figure out the if there was a sudden suspicious surge in user logins and logouts.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Cisco Wireless Accesspoint being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed

Parameters	Description
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: • **MD5** – Message Digest Algorithm

Parameters	Description
	• **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
Users currently loggedin	Indicates the total number of users currently logged in.	Number	This is a good indicator of the load on the Cisco Wireless Accesspoint. The detailed diagnosis of this measure lists the MAC address, login time, session time and associated SID of the users logged in.
New users	Indicates the number of users who are newly connected since the last measurement period.	Number	A consistent zero value could indicate a connection issue. The detailed diagnosis of this measure lists the MAC address and the associated SID of the users who logged in recently.
Recently loggedout users	Indicates the number of users logged out during the last measurement period.	Number	If all the current users suddenly log out, it indicates a problem condition that requires investigation. The detailed diagnosis of this measure lists the MAC address, login time, logout time, session time and associated SID of the users logged out.

3.1.4 Email Alert Status Test

Generally, events are activities on the target Cisco Wireless Accesspoint that may require attention. In order to take necessary action on the generated events so that the target Cisco Wireless Accesspoint can be run smoothly, these events are recorded as logs. These logs in turn can be sent over to the administrators via email alerts. If the email alerts fail, then the administrators may not be able to take necessary action in time which may result in the failure of the Cisco Wireless Accesspoint. It is therefore necessary to figure out the count of the emails sent round the clock. The **Email Alert Status** test helps administrators in this regard!

This test helps administrators to figure out the operational status of the *Email Alert* feature on the target Cisco Wireless Accesspoint. This test also reports the number of email alerts sent to the user and the number of email alerts that failed to be sent to the user.

Note:

For this test to report metrics, it is essential to enable the *Email Alert* feature on the target Cisco Wireless Accesspoint.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Cisco Wireless Accesspoint 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
Alert feature operation status	Indicates the operational status of the email alert feature.		The values reported by this measure and their corresponding numeric equivalents are mentioned in the table below: Measure Value: Numeric Value Up: 1 Down: 2 **Note:** By default, this measure reports the above-mentioned **Measure value**s while indicating the authentication status of each client. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., 1 *or* 2.
Sent email failed count	Indicates the number of emails that failed to be sent to the user.	Number	This measure will be reported only if the *Alert feature operation status* measure reports an 'Up' status.
Sent email count	Indicates the number of emails that were sent to the user.	Number	This measure will be reported only if the *Alert feature operation status* measure reports an 'Up' status.

3.1.5 Log Events Test

Generally, events are activities on the target Cisco Wireless Accesspoint that may require attention. Often administrators have to figure out the problematic events generated on the target accesspoint so that necessary action can be taken before end users are affected. The **Log Events** test helps administrators in this regard!

This test monitors the events logged in for the target Cisco Wireless Accesspoint and reports the count of the critical, warning, alert and error events.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Cisco Wireless Accesspoint 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
Info	Indicates the number of Info events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.
Debug	Indicates the number of debug events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.
Notice	Indicates the number of notice events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.
Warning	Indicates the number of warning events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.
Error	Indicates the number of error events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.
Critical	Indicates the number of critical events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.
Alert	Indicates the number of alert events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.

Measurement	Description	Measurement Unit	Interpretation
Emergency	Indicates the number of emergency events generated on the Cisco Wireless Accesspoint.	Number	The detailed diagnosis of this measure lists the time stamp at which the log event was logged on, the file location and the message.

3.1.6 TSPEC Accesspoint Test

Sometimes, the quality of real-time applications like VoIP and video streaming over Wireless Local Area Network (WLAN) can be poor because of an unstable wireless link. This is the reason why there is a need to prioritize network traffic by enabling Quality of Service (QoS).

Traffic Specification (TSPEC) is sent from a QoS-capable wireless client that requests for a certain amount of network traffic from the Wireless Access Point (WAP) for the traffic stream (TS) it represents. The WAP then decides whether the request is acceptable or not and provides its decision to the client. The client can start the high-priority communication only when the WAP approves it. This prevents any kind of collision and congestion of the wireless link and thus keeps the communication quality good. The **TSPEC Accesspoint** test helps administrators track the voice and video communication via the target Cisco Wireless Accesspoint.

By closely monitoring the voice and video communication, this test helps administrators identify the number of voice and video calls that were approved and rejected by the target Cisco Wireless Accesspoint.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Cisco Wireless Accesspoint 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

Parameters	Description
	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 **Yes** option.

Parameters	Description
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
Accepted voice	Indicates the number of voice calls (traffic streams) accepted by the Cisco Wireless accesspoint.	Number	
Rejected voice	Indicates the number of voice calls (traffic streams) rejected by the Cisco Wireless accesspoint.	Number	
Accepted video	Indicates the number of video calls (traffic streams) accepted by the Cisco Wireless	Number	

Measurement	Description	Measurement Unit	Interpretation
	accesspoint.		
Rejected video	Indicates the number of video calls rejected (traffic streams) by the Cisco Wireless accesspoint.	Number	

3.1.7 TSPEC Associated Client Test

Traffic Specification (TSPEC) is sent from a QoS-capable wireless client that requests for a certain amount of network traffic from the Wireless Access Point (WAP) for the traffic stream (TS) it represents. In environments where the target Cisco Wireless Accesspoint is installed, it is necessary to track the amount of data sent to and from each client through the traffic stream. The **TSPEC Associated Client** test helps administrators in this regard!

For each wireless client on the target Cisco Wireless Accesspoint, this test helps administrators determine the amount of data transmitted / received. The count of packets transmitted / received through each client is also tracked and reported.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for each client on the target Cisco Wireless Accesspoint 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

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

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
Packets received	Indicates the number of packets received by this client through traffic stream.	Packets	Compare the value of these measures across the clients to figure out the client who has transmitted / received the maximum number of packets through traffic stream.
Packets transmitted	Indicates the number of packets transmitted from this client through traffic stream.	Packets	
Data received	Indicates the amount of data received by this client through traffic stream.	MB	Compare the value of these measures across the clients to figure out the client who has transmitted / received the maximum amount of data through traffic stream.
Data transmitted	Indicates the amount of data transmitted from this client through traffic stream.	MB	

3.1.8 Virtual Accesspoint Test

Virtual Access Points (VAPs) simulate multiple access avenues in one physical WAP device; VAPs are similar to Ethernet VLANs. Each VAP can be enabled or disabled independently and is identified by a user - configured Service Set Identifier (SSID).

For each Virtaul Access Point configured on the target Cisco Wireless Accesspoin, this test reports the administrative status and operational status. By comparing the operational state across the VAPs, administrators can figure out the VAP that is not operational for a considerable time period.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for each virtual accesspoint on the target Cisco Wireless Accesspoint 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.

Parameters	Description
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 should time out in this text box. The default is 10 seconds.

Parameters	Description
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
Administrative status	Indicates the current administrative status of this virtual accesspoint.		The values reported by this measure and their corresponding numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Up – 1 Down – 0 **Note:** By default, this measure reports the above-mentioned **Measure value**s while indicating the administrative status of this virtual accesspoint. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., *0 or 1*.
Operational status	Indicates the current operational status of this virtual accesspoint.		The values reported by this measure and their corresponding numeric equivalents are mentioned in the table below:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>0</td></tr></table> **Note:** By default, this measure reports the above-mentioned **Measure value**s while indicating the operational status of this virtual accesspoint. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., *0 or 2*. By comparing the operational state across the VAPs, administrators can figure out the VAP that is not operational for a considerable time period.

3.1.9 WorkGroup Downstream Test

This test auto-discovers the downstream workgroups and for each downstream workgroup, this test reports the current connection status and the amount of data transmitted/received. This test also reports the number of packets transmitted and received by each downstream workgroup. Using this test, administrators can figure out the downstream workgroup that is transmitting/receiving the maximum number of packets and maximum amount of data.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for each downstream workgroup on the target Cisco Wireless Accesspoint 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**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current connection status of this downstream workgroup.		The values reported by this measure and their corresponding 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>Connected</td><td>1</td></tr><tr><td>Disconnected</td><td>2</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure values while indicating the connection status of this workgroup. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., 1 or 2.</td></tr>
<tr><td>Received packets</td><td>Indicates the number of packets received by this downstream workgroup.</td><td>Packets</td><td rowspan="2">Compare the value of these measures across the downstream workgroups to figure out the downstream workgroup that has transmitted / received the maximum number of packets.</td></tr>
<tr><td>Transmitted packets</td><td>Indicates the number of packets transmitted through this downstream workgroup.</td><td>Packets</td></tr>
<tr><td>Received data</td><td>Indicates the amount of data received by this downstream workgroup.</td><td>MB</td><td rowspan="2">Compare the value of these measures across the downstream workgroup to figure out the downstream workgroup that has transmitted / received the maximum amount of data.</td></tr>
<tr><td>Transmitted data</td><td>Indicates the amount of data transmitted through this downstream workgroup.</td><td>MB</td></tr>
</table>

3.1.10 WorkGroup Upstream Test

This test auto-discovers the upstream workgroups and for each upstream workgroup, this test reports the current connection status and the amount of data transmitted/received. This test also reports the number of packets transmitted and received by each upstream workgroup. Using this test, administrators can figure out the upstream workgroup that is transmitting/receiving the maximum number of packets and maximum amount of data.

Target of the test : A Cisco Wireless Accesspoint

Agent deploying the test : An external agent

Outputs of the test : One set of results for each upstream workgroup on the target Cisco Wireless Accesspoint 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**.

Parameters	Description
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current connection status of this upstream workgroup.</td><td></td><td>The values reported by this measure and their corresponding numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Connected</td><td>1</td></tr><tr><td>Disconnected</td><td>2</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure values while indicating the connection status of this workgroup. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents - i.e., 1 or 2.</td></tr>
<tr><td>Received packets</td><td>Indicates the number of packets received by this upstream workgroup.</td><td>Packets</td><td rowspan="2">Compare the value of these measures across the upstream workgroups to figure out the upstream workgroup that has transmitted / received the maximum number of packets.</td></tr>
<tr><td>Transmitted packets</td><td>Indicates the number of packets transmitted through this upstream workgroup.</td><td>Packets</td></tr>
<tr><td>Received data</td><td>Indicates the amount of data received by this upstream workgroup.</td><td>MB</td><td rowspan="2">Compare the value of these measures across the upstream workgroups to figure out the upstream workgroup that has transmitted / received the maximum amount of data.</td></tr>
<tr><td>Transmitted data</td><td>Indicates the amount of data transmitted through this upstream workgroup.</td><td>MB</td></tr>
</table>

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.