

Configure 802.1X Settings on the WAP351

Objective

IEEE 802.1X authentication allows the WAP device to gain access to a secured wired network. You can configure the WAP device as an 802.1X supplicant (client) on the wired network. The WAP351 can also be configured as an authenticator. An encrypted user name and password can be configured to allow the WAP device to authenticate using 802.1X.

On the networks that use IEEE 802.1X port-based network access control, a supplicant cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information on the WAP device, so that it can supply it to the authenticator.

The objective of this document is to show you how to configure 802.1X Supplicant settings on the WAP351.

Applicable Devices

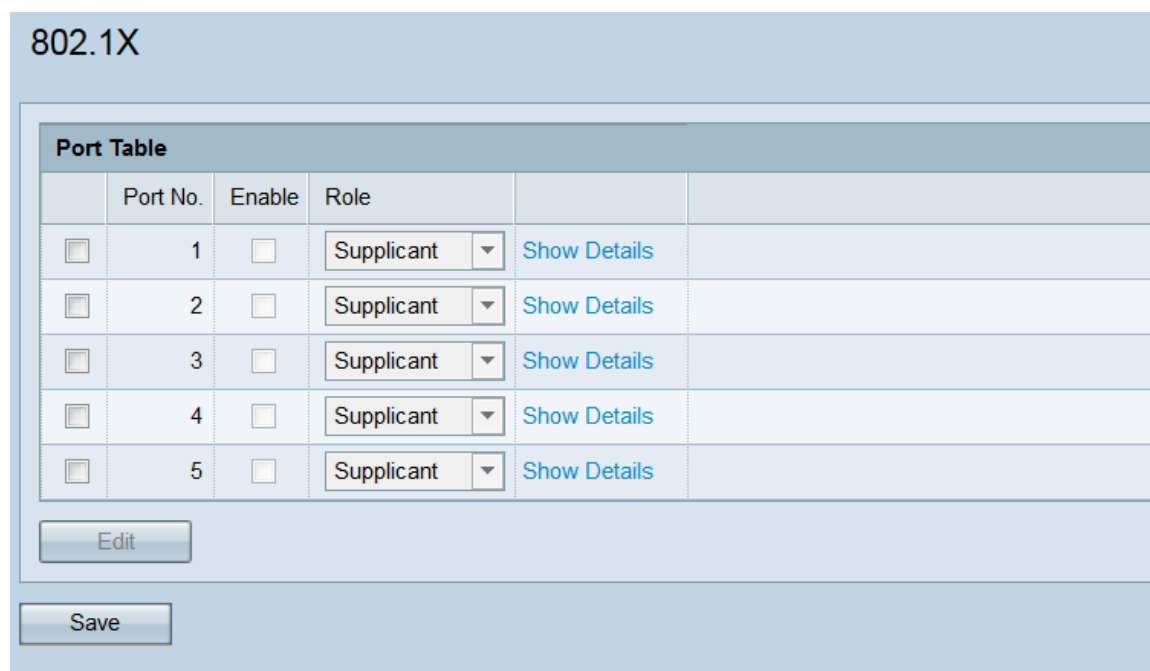
- WAP351

Software Version

- v1.0.1.3

Configuring 802.1X Supplicant Settings

Step 1. Log in to the web configuration utility and choose **System Security > 802.1X**. The *802.1X* page opens.



802.1X

Port Table				
	Port No.	Enable	Role	
<input type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details

Step 2. The *Port Table* shows five LAN interfaces that can be configured for 802.1X authentication. Check the check box(s) corresponding to the port(s) you wish to edit.

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Step 3. Click the **Edit** button. The checked port(s) will now be available for editing.

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Step 4. In the *Enable* field, check the check box(s) of the port(s) that you want to enable 802.1X settings on.

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

Step 5. In the *Role* drop-down list, select whether the corresponding port will be configured as a **Supplicant** or an **Authenticator**. If you chose Supplicant, go the [Supplicant Settings Configuration](#) section. If you chose Authenticator, go to the [Authenticator Settings Configuration](#) section. An Authenticator lies in between the client (Supplicant) wishing to gain access to the network and the RADIUS server itself. It is responsible for handling all communication between the two. A Supplicant provides credentials to an Authenticator in order to gain access to the network. A typical setup on the WAP351 would have the WAN port be a Supplicant (so the WAP can access the network) and have the LAN ports be Authenticators (so the WAP can authorize devices underneath it).

802.1X

Port Table					
	Port No.	Enable	Role		
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant Authenticator	Show Details	
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant	Show Details	
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant	Show Details	

Edit

Save

Supplicant Settings Configuration

Step 1. Click on **Show Details** to display the Supplicant settings information.

Port Table			
	Port No.	Enable	Role
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Supplicant Hidden Details
<p>EAP Method: <input type="text" value="MD5"/></p> <p>Username: <input type="text"/> (Range: 1 - 64 Characters)</p> <p>Password: <input type="text"/> (Range: 1 - 64 Characters)</p> <hr/> <p>Certificate File Status <input type="button" value="Refresh"/></p> <p>Certificate File Present: No</p> <p>Certificate Expiration Date: Not Present</p> <hr/> <p>Browse to the location where your certificate file is stored and click the "Upload" button. To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.</p> <p>Certificate File Upload</p> <p>Transfer Method: <input checked="" type="radio"/> HTTP <input type="radio"/> TFTP</p> <p>Filename <input type="button" value="Browse..."/> No file selected.</p> <p><input type="button" value="Upload"/></p>			
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant Show Details

Note: This information may open automatically after you make a selection in the *Mode* field.

Step 2. In the *EAP Method* drop-down list, choose the algorithm that will be used to encrypt usernames and passwords. EAP stands for Extensible Authentication Protocol, and is used as a basis for encryption algorithms.

EAP Method: MD5 (dropdown menu open showing MD5, PEAP, TLS)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: Browse... No file selected.

Upload

The available options are:

- MD5 — The MD5 message-digest algorithm utilizes a hash function to provide basic security. This algorithm is not recommended, as the other two have higher security.
- PEAP — PEAP stands for Protected Extensible Authentication Protocol. It encapsulates EAP and provides higher security than MD5 by using a TLS tunnel to transmit data.
- TLS — TLS stands for Transport Layer Security, and is an open standard that provides high security.

Step 3. In the *Username* field, enter in the username that the WAP device will use when responding to requests from an 802.1X authenticator. The username must be 1 – 64 characters long, and can include alphanumeric and special characters.

EAP Method: MD5 ▼

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

Step 4. In the *Password* field, enter in the password that the WAP device will use when responding to requests from an 802.1X authenticator. The username must be 1 - 64 characters long, and can include alphanumeric and special characters.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

Step 5. The *Certificate File Status* area shows whether an HTTP SSL certificate file exists on the WAP device. The *Certificate File Present* field will show "Yes" if a certificate is present; the default is "No". If a certificate is present, the *Certificate Expiration Date* will show when it expires; otherwise, the default is "Not present". To display the latest information, click the **Refresh** button to get the most current certificate information.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

Step 6. If you do not want to upload an HTTP SSL certificate file, skip to [Step 12](#). Otherwise, select either the **HTTP** or **TFTP** radio buttons in the *Transfer Method* field to choose which protocol you want to use to upload the certificate.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename Browse... No file selected.

Upload

Step 7. If you selected **TFTP**, continue to Step 8. If you selected **HTTP**, click the **Browse...** button to find the certificate file on your PC. Skip to [Step 10](#).

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP
 TFTP

Filename No file selected.

Upload

Step 8. If you selected **TFTP** in the *Transfer Method* field, enter in the filename of the certificate in the *Filename* field.

EAP Method: (Range: 1 - 64 Characters)

Username: (Range: 1 - 64 Characters)

Password: (Range: 1 - 64 Characters)

Certificate File Status

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: (xxx.xxx.xxx.xxx)

Note: The file must end in .pem.

Step 9. Enter the IP address of the TFTP server in the *TFTP Server IPv4 Address* field.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Certificate File Upload

Transfer Method: HTTP TFTP

Filename: certificate.pem (Range: 1 - 256 Characters)

TFTP Server IPv4 Address: 192.0.2.100 (xxx.xxx.xxx.xxx)

Upload

[Step 10](#). Click **Upload**.

EAP Method: MD5 ▼

Username: username1 (Range: 1 - 64 Characters)

Password: ●●●●●●●● (Range: 1 - 64 Characters)

Certificate File Status Refresh

Certificate File Present: No

Certificate Expiration Date: Not Present

Browse to the location where your certificate file is stored and click the "Upload" button.
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

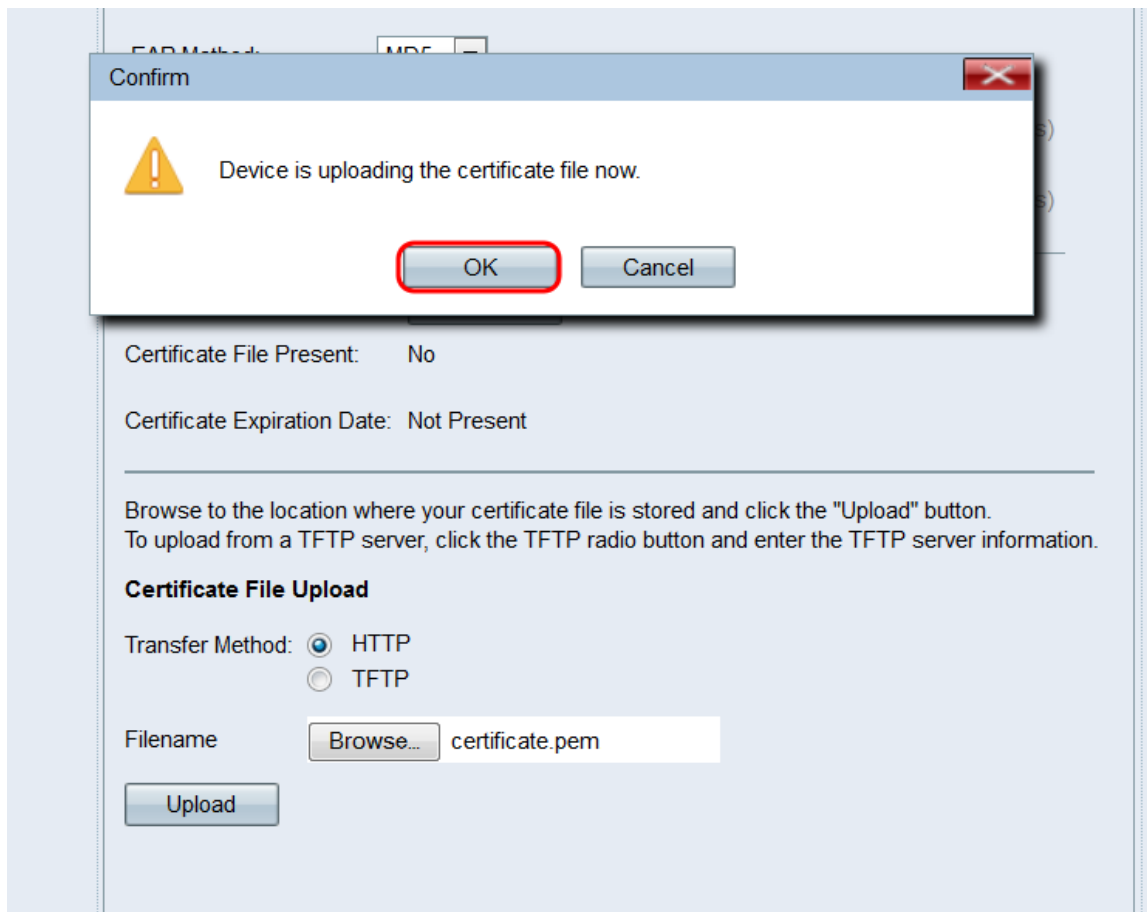
Certificate File Upload

Transfer Method: HTTP
 TFTP

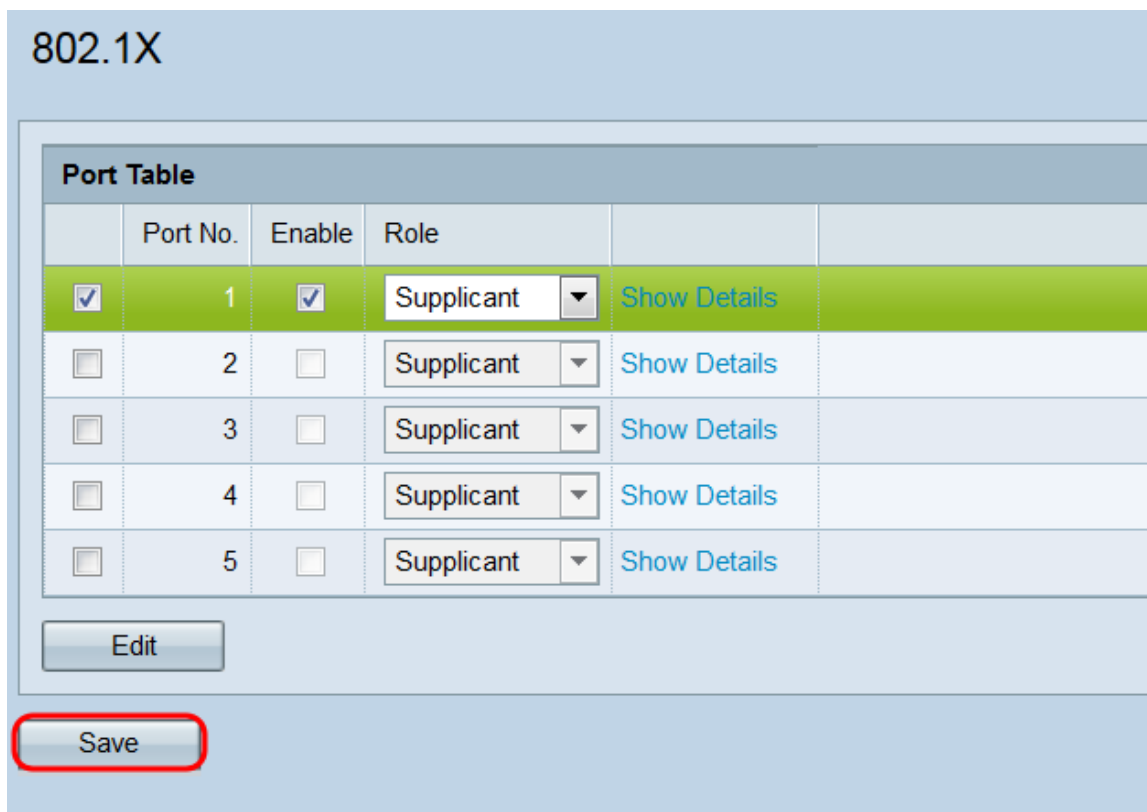
Filename Browse... certificate.pem

Upload

Step 11. A confirmation window appears. Click **OK** to begin the upload.



[Step 12](#). Repeat this section for every port that you want to configure as an 802.1X Supplicant. Then, click **Save**.



[Authenticator Settings Configuration](#)

Step 1. Click on **Show Details** to display the Authenticator settings information.

Port Table																							
Port No.	Enable	Role																					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Authenticator	Hidden Details																				
<input checked="" type="checkbox"/> Use global RADIUS server settings Server IP Address Type: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <table border="1"> <thead> <tr> <th>No.</th> <th>Server IP Address (xxx.xxx.xxx.xxx)</th> <th>Key (Range: 1 - 64 Characters)</th> <th>Authentication Port (Range: 0 - 65535, Default: 1812)</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0.0.0.0</td> <td></td> <td>1812</td> </tr> <tr> <td>2</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>3</td> <td></td> <td></td> <td>1812</td> </tr> <tr> <td>4</td> <td></td> <td></td> <td>1812</td> </tr> </tbody> </table> <input type="checkbox"/> Enable RADIUS Accounting Active Server: Server IP Address-1 Periodic Reauthentication: <input type="checkbox"/> Enable Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)				No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)	1	0.0.0.0		1812	2			1812	3			1812	4			1812
No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)																				
1	0.0.0.0		1812																				
2			1812																				
3			1812																				
4			1812																				
<input type="checkbox"/>	<input type="checkbox"/>	Supplicant	Show Details																				

Note: This information may open automatically after you make a selection in the *Mode* field.

Step 2. Check the *Use global RADIUS Server Settings* checkbox if you want the port to use the global RADIUS settings during authentication. If you want the port to use a different RADIUS server (or servers), uncheck this checkbox; otherwise, skip to [Step 8](#).

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	0.0.0.0		1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

Note: For more information, see the article [Configuring Global RADIUS Server Settings on the WAP131 and WAP351](#).

Step 3. In the *Server IP Address Type* field, select the radio button for the IP version that the RADIUS server uses. The available options are **IPv4** and **IPv6**.

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	0.0.0.0		1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Note: You can toggle between the address types to configure IPv4 and IPv6 RADIUS address settings, but the WAP device contacts only the RADIUS server or servers with the address type that you select in this field. It is not possible to have multiple servers use different address types in one configuration.

Step 4. In the *Server IP Address 1* or *Server IPv6 Address 1* field, enter either an IPv4 or IPv6 address for the RADIUS server depending on the address type you chose in Step 3.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1		1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Note: The address entered in this field will designate the port's primary RADIUS server. Addresses entered in subsequent fields (*Server IP Address 2* through *4*) will designate the backup RADIUS servers that will be tried in sequence if authentication fails with the primary server.

Step 5. In the *Key* field, enter the shared secret key corresponding to the primary RADIUS server that the WAP device uses to authenticate to the RADIUS server. You can use from 1 to 64 standard alphanumeric and special characters. Repeat this step for each subsequent RADIUS server you have configured for the port in the *Key 2* through *4* fields.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Note: The keys are case sensitive and must match the key configured on the RADIUS server.

Step 6. In the *Authentication Port* field, enter the port that the WAP will use to connect to the RADIUS server. Repeat this step for each backup RADIUS server you have configured in the *Authentication Port 2 through 4* fields. The default is 1812.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2			1812
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Step 7. Check the **Enable RADIUS Accounting** checkbox to enable tracking and measuring of the resources a user has consumed (system time, amount of data transmitted, etc.).

Checking this checkbox will enable RADIUS accounting for the primary and backup servers.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••••••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

Step 8. In the *Active Server* drop-down list, choose one of the configured RADIUS servers to be set as the active server. This setting lets the WAP immediately try to contact the active server, rather than trying to contact each server in sequence and choosing the first one available.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••~••••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: Server IP Address-1 ▼

Periodic Reauthentication: Enable

Reauthentication Period: 3600 sec. (Range: 300 - 4294967295, Default: 3600)

Step 9. In the *Periodic Reauthentication* field, check the **Enable** checkbox to turn on EAP reauthentication. If you do not want to enable EAP reauthentication, skip to [Step 11](#).

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••••	1812
2	192.0.2.2	••••••••	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

Step 10. If you checked the **Enable** checkbox in the *Periodic Reauthentication* field, enter the EAP reauthentication period in seconds in the *Reauthentication Period* field. The default is 3600. The valid range is 300 – 4294967295 seconds.

Use global RADIUS server settings

Server IP Address Type: IPv4
 IPv6

No.	Server IP Address (xxx.xxx.xxx.xxx)	Key (Range: 1 - 64 Characters)	Authentication Port (Range: 0 - 65535, Default: 1812)
1	192.0.2.1	••••••~	1812
2	192.0.2.2	••~	2500
3			1812
4			1812

Enable RADIUS Accounting

Active Server: ▼

Periodic Reauthentication: Enable

Reauthentication Period: sec. (Range: 300 - 4294967295, Default: 3600)

[Step 11](#). Repeat this section for every port that you want to configure as an 802.1X Authenticator. Then, click **Save**.

802.1X

Port Table

	Port No.	Enable	Role	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	Authenticator ▼	Show Details
<input type="checkbox"/>	2	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	3	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	4	<input type="checkbox"/>	Supplicant ▼	Show Details
<input type="checkbox"/>	5	<input type="checkbox"/>	Supplicant ▼	Show Details

Edit

Save