TOSHIBA

TOSHIBA Barcode Printer

B-SA4T/SX6T/SX8T/852-R Series

Wireless LAN Setting Specification

First Edition:	July 22, 2005
Second Edition:	December 25, 2006
Third Edition:	October 9, 2008

TOSHIBA TEC CORPORATION

TABLE OF CONTENTS

Page

1. SCOPE

This specification applies to the optional wireless LAN module B-SA704-WLAN-QM(-R) for the general purpose bar code printer B-SA4T, B-SX6T, B-SX8T, and B-852-R series (hereinafter referred to as the B-SA4T series).

2. GENERAL DESCRIPTION

In order to incorporate the B-SA704-WLAN-QM(-R) into the B-SA4T series, settings are required. This document explains the specifications of the B-SA704-WLAN-QM(-R) and the connection and setting procedures to the B-SA4T series.

3. SPECIFICATIONS

3.1 HARDWARE SPECIFICATIONS

Item	Specification		
Wired LAN	Ethernet		IEEE802.3 (10BASE-T) IEEE802.3u (100BASE-TX)
	Data transmission speed		10/100 Mbps
	Access method		CSMA/CD
	Communication method		Half duplex, Full duplex
	Number of ports		1 (10BASE-T/100BASE-TX)
Wireless LAN	IEEE802.11a	Data transmission	IEEE802.11a compliant, OFDM
		Channel	Depending on country
		Data transmission speed	54, 48, 36, 24, 18, 12, 9, 6 Mbps (Fixed/Automatic)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	Low-power data communication system (5.150-5.850GHz)
		Power	10 mW/MHz or less
	IEEE802.11b	Data transmission	IEEE802.11b compliant, DSSS
		Channel	Depending on country
		Data transmission speed	11, 5.5, 2, 1 Mbps (Fixed/Automatic)
		Access method	CSMA/CA + ACK(RTS/CTS)
		Wireless category	Low-power data communication system (2.4-2.4835GHz)
		Power	10 mW/MHz or less
	IEEE802.11g	Data transmission	IEEE802.11g compliant, OFDM, DSSS
		Channel	Depending on country
		Data transmission speed	54, 48, 36, 24, 18, 12, 9, 6, 11, 5.5, 2, 1 Mbps (Fixed/Automatic)
		Access method	CSMA/CA+ACK(RTS/CTS)
		Wireless category	Low-power data communication system (2.4-2.4835GHz)
		Power	10 mW/MHz or less
	Antenna		Diversity antenna (Chip)

3.2 SOFTWARE SPECIFICATIONS

Item		Specification
Unit type		<Station>, Access Point Basically, Station should be used.
Operating mode		<Compatible>, Standard, Advanced
Default country code	Japan	Japan
	Other countries	US
Default IP address		192.168.10.21
Default subnet address		255.255.255.0
Default password		tecbcp
Encryption		WEP (64/128/152 bit) or AES, AES-OCB (128 bit) TKIP (only when using WPA, WPA-PSK, WPA2, WPA2-PSK)
Setting change		Browser, telnet
Browser		Microsoft IE5.01 or higher

Protocol		IP(RFC791), ICMP(RFC792), UDP(RFC768)
		TCP(RFC793, 896), ARP(RFC826),
		HTTPD(RFC1866), TELNET
		FTPD(RFC959), DHCP(RFC2131)

3.3 LED INDICATION

<During operation>

LED	Status	Description
LED1 (Red)	ON	In operation
	Flash	At startup
LED2 (Orange)	ON	During connection to the wired LAN (B-SA4T series)
	Flash	During communication with the B-SA4T series
	OFF	During disconnection from the B-SA4T series
LED3 (Orange)	ON	When using the station function: The B-SA704-WLAN-QM has been logging in to an access point. When using the access point function: A user-unit has been logging in.
	Flash	During communication with a device with a wireless LAN connection
	OFF	When using the station function: The B-SA704-WLAN-QM has not logged in to an access point. When using the access point function: A user-unit has not logged in.

<In start-up error mode>

LED	Status	Description
LED2	Flash	Wired LAN error
LED3	Flash	Wireless LAN error

3.4 DIP SW

DIP SW No.	SW	Description
1	INIT	Initializes the B-SA704-WLAN-QM. When this switch is set to ON, LEDs 1-3 continue to flash for about 3 seconds until they stop flashing and stay ON. If this switch is set to OFF during this 3-second period, all AP settings are restored to the default at a next startup.
2	IP LESS	With this switch set to ON, the printer can operate without setting an IP address. However, TELNET, FTP, and WWW browser are not available under this condition.

3.5 LIST OF DEFAULT SETTINGS

The list only includes the items necessary for using the station function.

<Basic setting>

Item	Setting values (The red values indicate the default setting.)
Host name (Max. 1-byte 16 alphanumeric characters)	Blank
DHCP client	Disabled, Enabled
IP address	192.168.10.21
Subnet mask	255.255.255.0
Gateway	0.0.0.0
Structure of access point	Compatible, Unified
Access point type	Normal, Master, Backup
IP of Master AP (Set when using Normal or Backup)	0.0.0.0
IP of Backup AP (Set when using Normal or Master)	0.0.0.0
Country code	US and other 23 countries
Language	English
Password (Max. 1-byte 31 alphanumeric characters, case-sensitive)	tecbcp

<Ethernet>

Item	Setting values (The red values indicate a default setting.)
Port speed	Automatic detection 100 M/full duplex, 100 M/half duplex 10 M/full duplex, 10 M/ half duplex
Link down detection	Disabled, Enabled
Link down condition	LinkStatus, Ping
Ping parameter, IP address	0.0.0.0
Ping parameter, transmission interval (sec.)	60, 1 - 65535
Ping parameter, response time (sec.)	3, 1 - 15
Ping parameter, number of transmission retries	3, 0 - 15

<Wireless LAN>

Item	Setting values (The red values indicate a default setting.)
Interface	Enabled, Disabled
Wireless LAN standards	[IEEE802.11g, IEEE802.11a], IEEE802.11b
Wireless connection mode	Compatible, Standard, Advanced-infrastructure
Unit type	Station, Access point
ESSID (Max. 1-byte 32 alphanumeric characters, case-sensitive)	LocalGroup
Transmission rate	11a: Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M 11g: Auto, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M, 1M, 2M, 5.5M, 11M 11b: Auto, 1M, 2M, 5.5M, 11M
Max. transmission rate	11a: 54M, 6M, 9M, 12M, 18M, 24M, 36M, 48M 11g: 54M, 6M, 9M, 12M, 18M, 24M, 36M, 48M, 1M, 2M, 5.5M, 1M 11b: 11M, 1M, 2M, 5.5M
Transmission power	MAX. 50% (-3 dB), 25% (-6 dB)

<Security>

Item	Setting values (The red values indicate a default setting.)
Encryption	Disabled, WEP, AES, AES-OCB, TKIP
WPA function	Disabled, WPA, WPA-PSK, WPA2, WPA2-PSK
Default key	#1, #2, #3, #4
Size/Key #1 - #4	WEP: Disabled, 64 bit (10 digits), 128 bit (26 digits), 152 bit (32 digits) AES/AES-OCB: Disabled, 128 bit (32 digits)
Key #1 - #4, hexadecimal number (0 - 9, a - f or A - F)	#1: Disabled #2: Disabled #3: Disabled #4: Disabled
AP-ST key size	AES: Disabled, 128 bit (32 digits) TKIP: Disabled, 256 bit (64 digits)

3.6 MAC ADDRESS

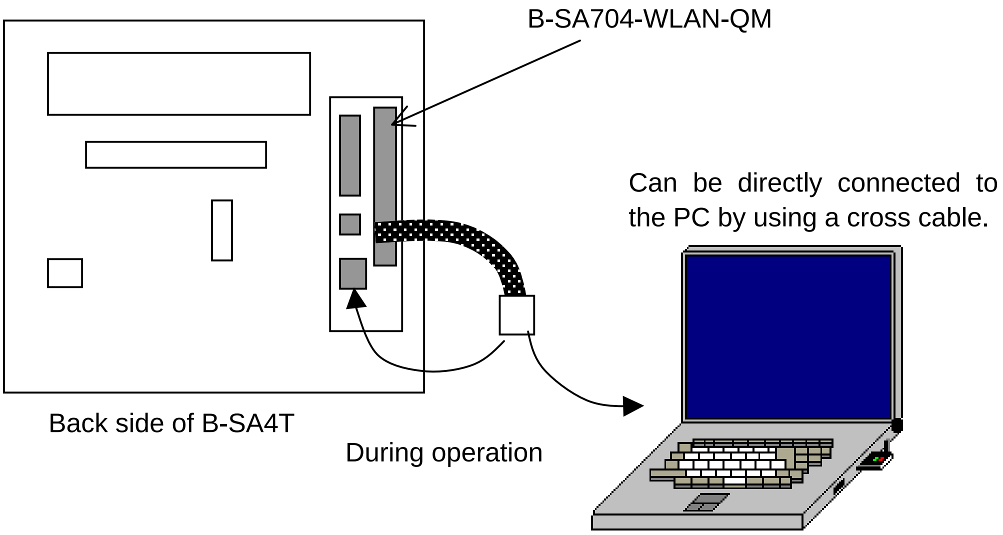
The wireless MAC address is indicated on the top of the wired LAN connecter. This address is required for using the MAC address filtering function of the access point (AP).

192.168.10.21
C:xxxxxxxxxxxx
W:yyyyyyyyyyyy

Please write down the 6-byte MAC address
(12 characters) on the right side of “W:” and keep it.

4. CONNECTION FOR SETTING

4.1 WIRED LAN CONNECTION TO PC



The IP address for the B-SA704-WLAN-QM is 192.168.10.21 (factory default). Please note that the TCP/IP of the PC must be set within the same subnet mask range as the IP address for the B-SA704-WLAN-QM, for example, 192.168.10.10.

For your reference, the default IP address of the B-SA4T is 192.168.10.20.

5. COUNTRY CODE SETTING

*** Toshiba TEC Group confidential**

For the market outside Japan, a specified country code must be set to the B-SA704-WLAN-QM before it reaches an end user because a usable frequency band differs among countries.

The method of setting the country code must not be disclosed to the end users as it relates to laws and regulations. It can be set only by using TELNET.

The program will ask the user to check the country code setting. Using the device with a wrong country code setting may infringe the radio law of an applicable country.

<Setting by using PC>

(1) Disconnect the currently used LAN cable from the B-SA4T series, and re-connect the B-SA4T series to the PC by using a straight LAN cable via a relay connecter.

When the B-SA4T series is connected to the PC via a hub, use a cross cable or a reverse input function of the hub.

(2) Execute telnet by entering “telnet 192.168.10.21” in the MS-DOS prompt and pressing the Enter key.

(3) Enter the password to log in.

(4) ON the top menu, change the county code using the command “=>ctry XX”. “XX” indicates country code.

(5) The change of the country code takes effect after the power is turned off and on again.

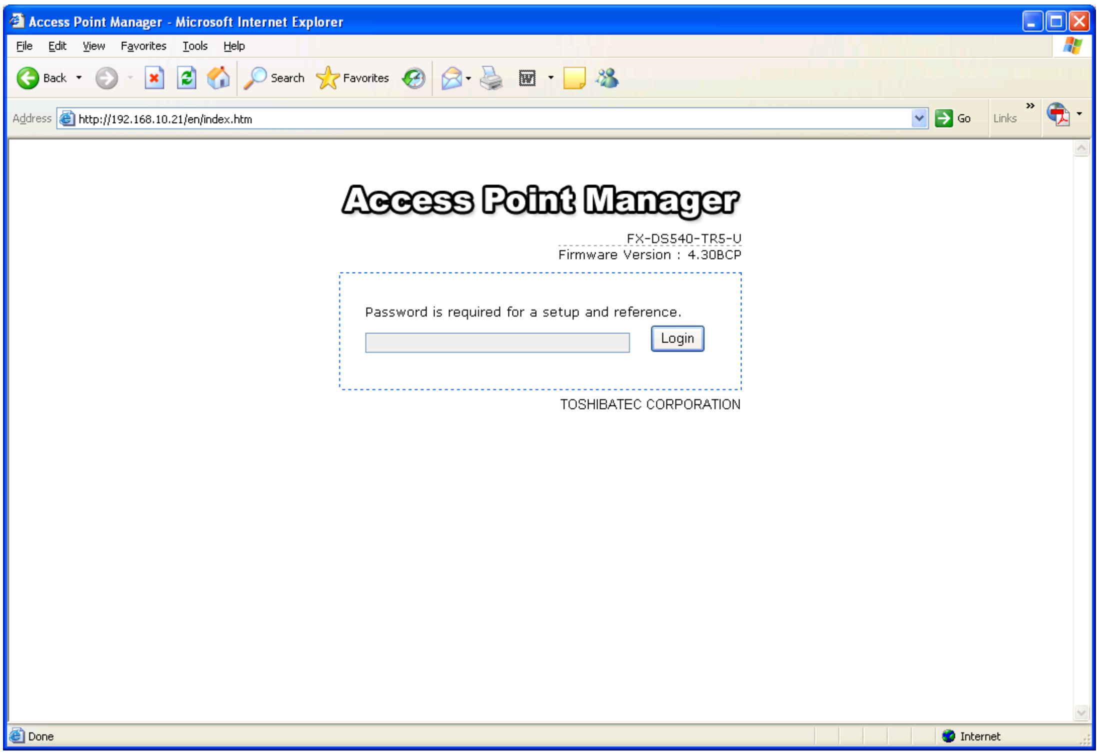
(6) To confirm the setting, enter “=>ctry” in the telnet consol.

	Country code	Country
1	US	United States of America
2	AT	Austria
3	DK	Denmark
4	FR	France
5	GR	Greece
6	IE	Ireland
7	PT	Portugal
8	SE	Sweden
9	GB	United Kingdom of Great Britain and Northern Ireland
10	NO	Norway
11	HU	Hungary
12	AU	Australia
13	CA	Canada
14	BE	Belgium
15	FI	Finland
16	DE	Germany
17	IT	Italy
18	LU	Luxembourg
19	ES	Spain
20	NL	Netherlands
21	CH	Swiss
22	IS	Iceland
23	LI	Liechtenstein
24	NZ	New Zealand

6. WIRELESS LAN SETTINGS

Setting from WEB browser using the factory default

(1) Start the Access Point Manager shown below using the IP address of the B-SA704-WLAN-QM, 192.168.10.21 (factory default). If the Access Point Manager screen does not appear, try it again after disabling the proxy settings.



Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/index.htm
Go Links
Done
Internet

Access Point Manager

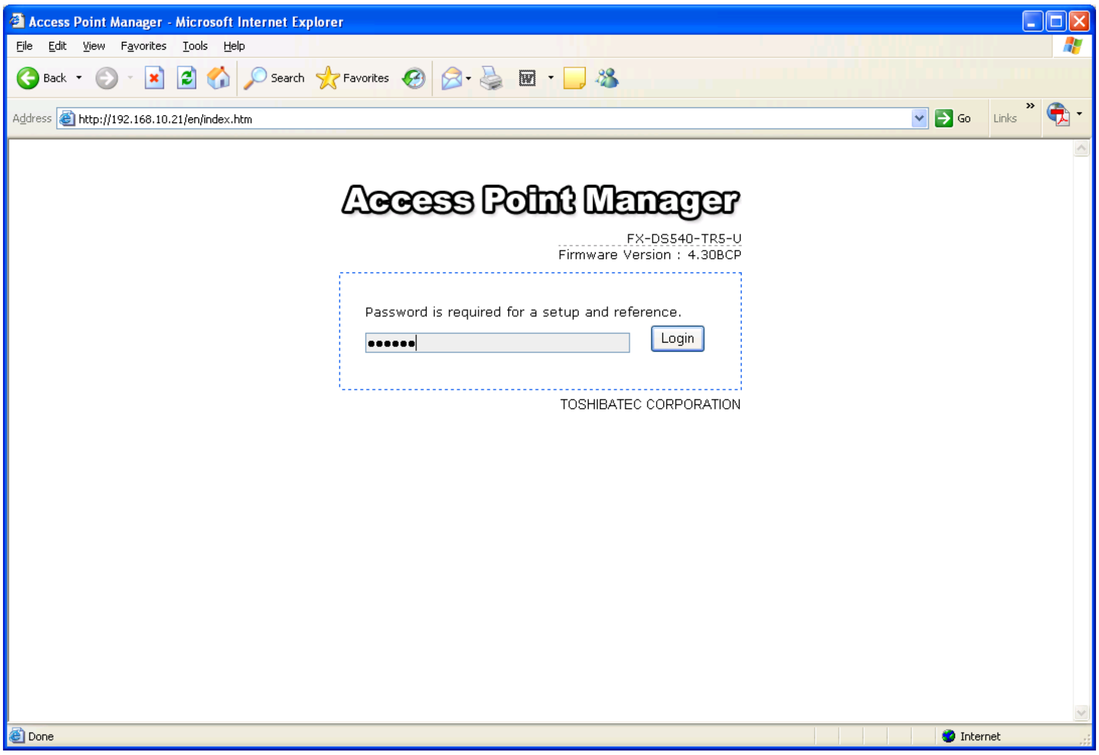
FX-DS540-TR5-U
Firmware Version : 4.30BCP

Password is required for a setup and reference.

Login

TOSHIBATEC CORPORATION

(2) Enter the password (tecbcp) to log in.



Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/index.htm
Go Links
Done
Internet

Access Point Manager

FX-DS540-TR5-U
Firmware Version : 4.30BCP

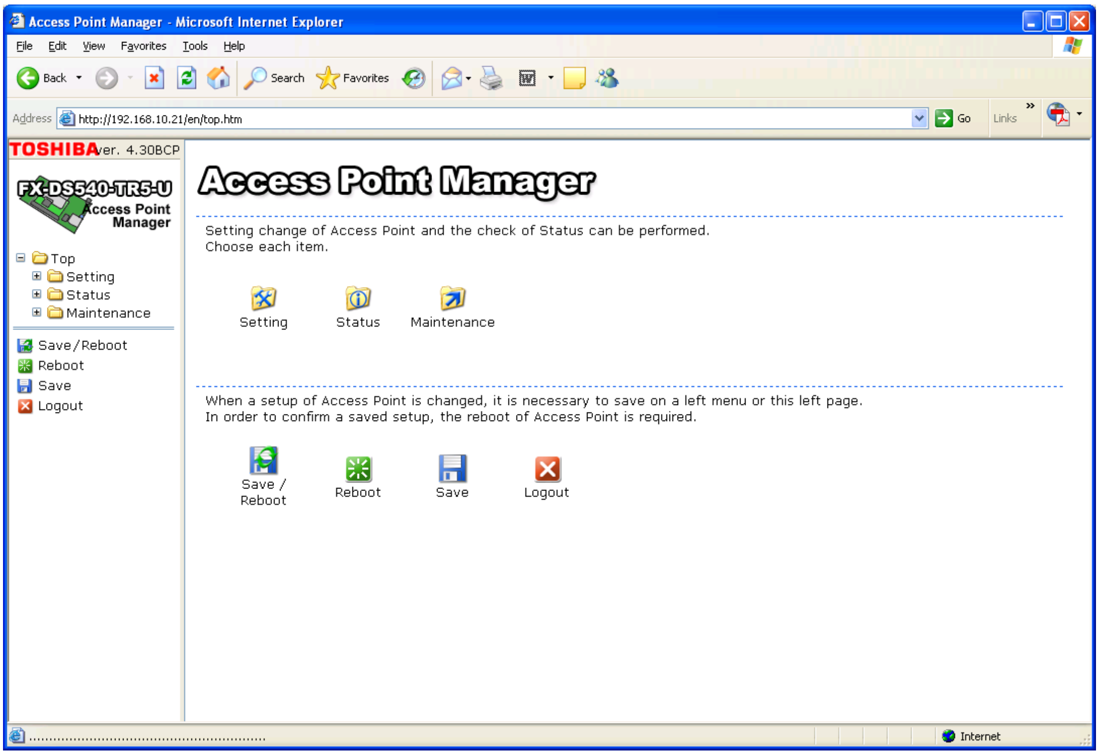
Password is required for a setup and reference.

●●●●●●

Login

TOSHIBATEC CORPORATION

(3) The top menu appears.

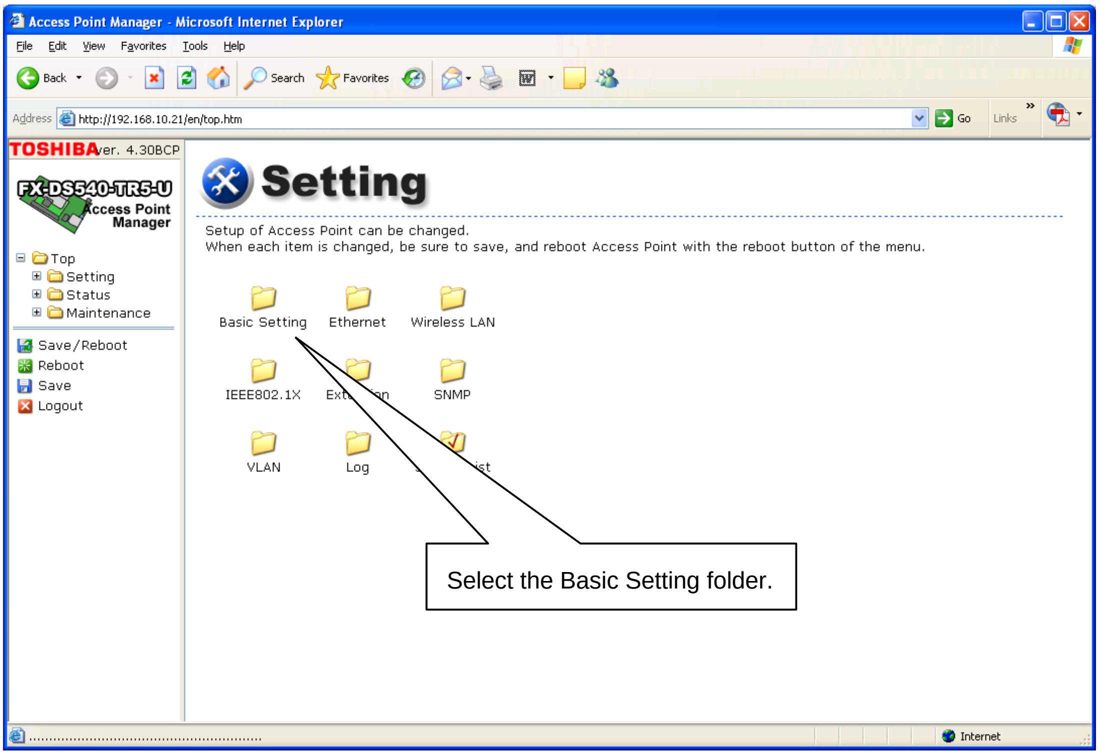

Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Access Point Manager

Setting change of Access Point and the check of Status can be performed.
Choose each item.

When a setup of Access Point is changed, it is necessary to save on a left menu or this left page.
In order to confirm a saved setup, the reboot of Access Point is required.

(4) Click on the Setting icon, then click on the Basic Setting folder.

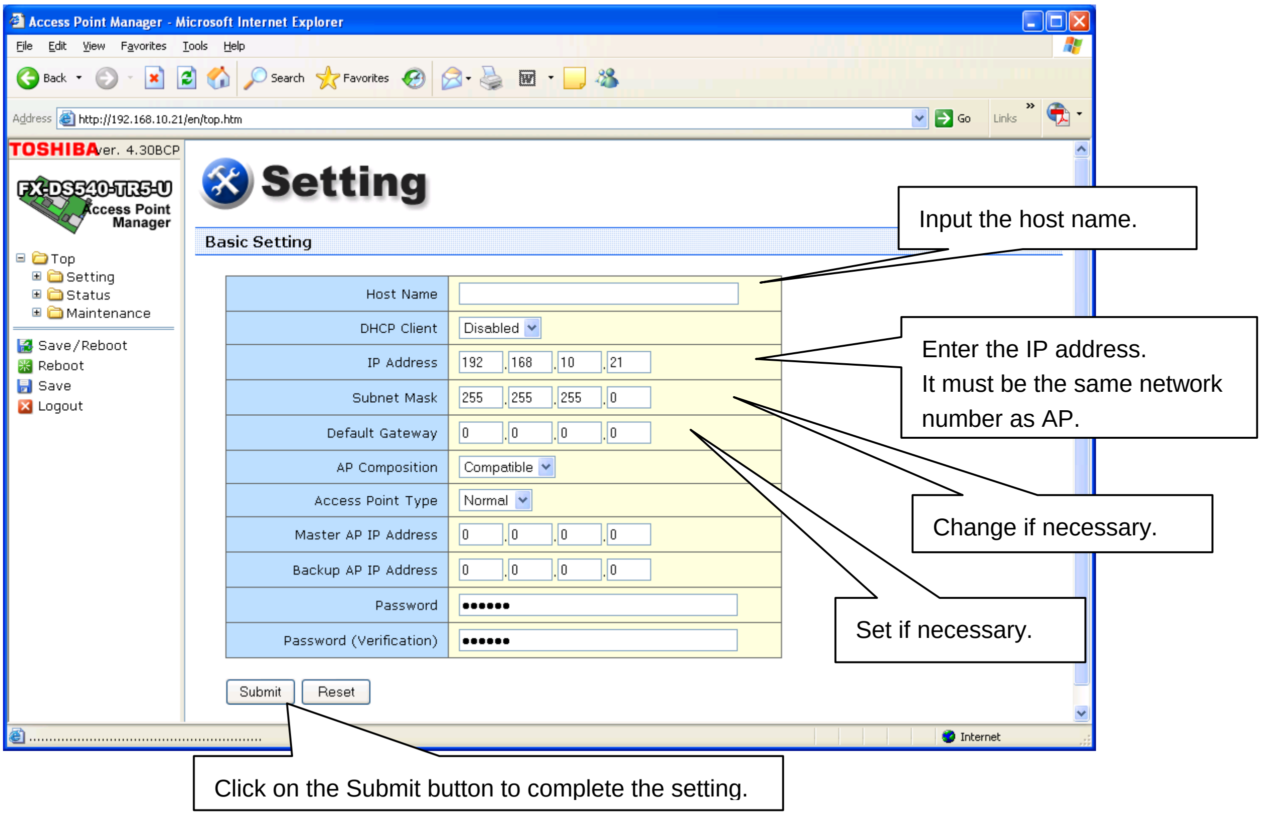

Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

Setup of Access Point can be changed.
When each item is changed, be sure to save, and reboot Access Point with the reboot button of the menu.

Select the Basic Setting folder.

(5) The Basic Setting screen appears.



Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Setting
Internet

Basic Setting

Host Name	
DHCP Client	Disabled
IP Address	192 .168 .10 .21
Subnet Mask	255 .255 .255 .0
Default Gateway	0 .0 .0 .0
AP Composition	Compatible
Access Point Type	Normal
Master AP IP Address	0 .0 .0 .0
Backup AP IP Address	0 .0 .0 .0
Password	••••••
Password (Verification)	••••••

Submit Reset

Input the host name.

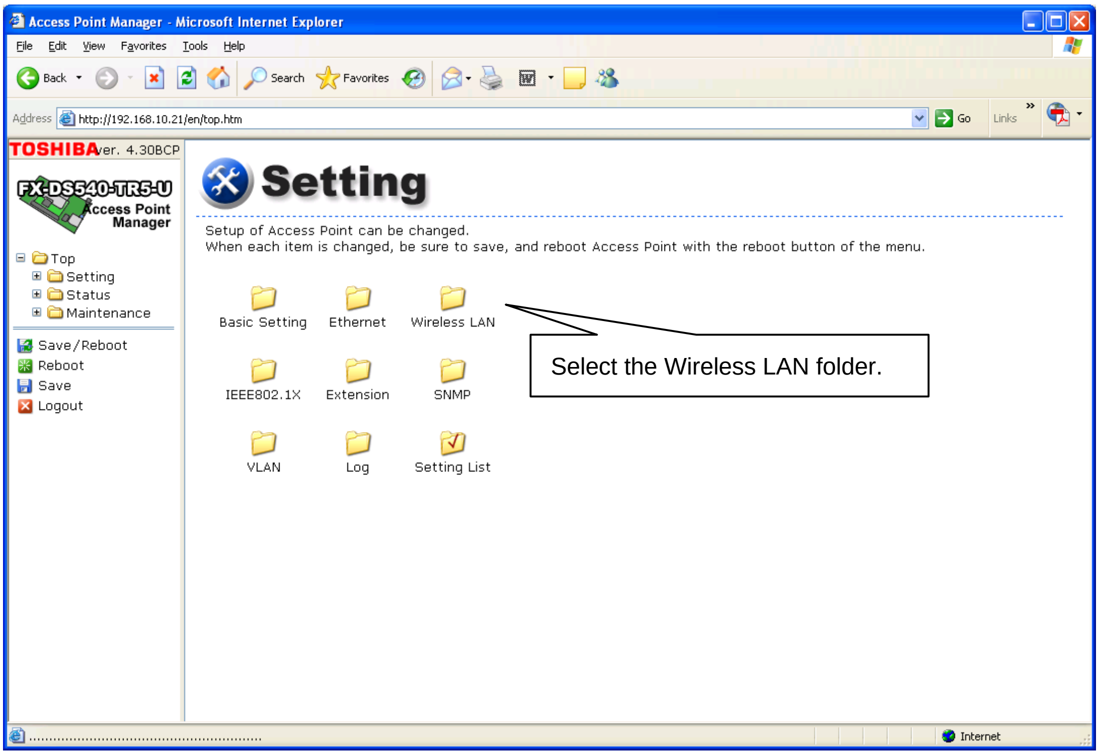
Enter the IP address.
It must be the same network number as AP.

Change if necessary.

Set if necessary.

Click on the Submit button to complete the setting.

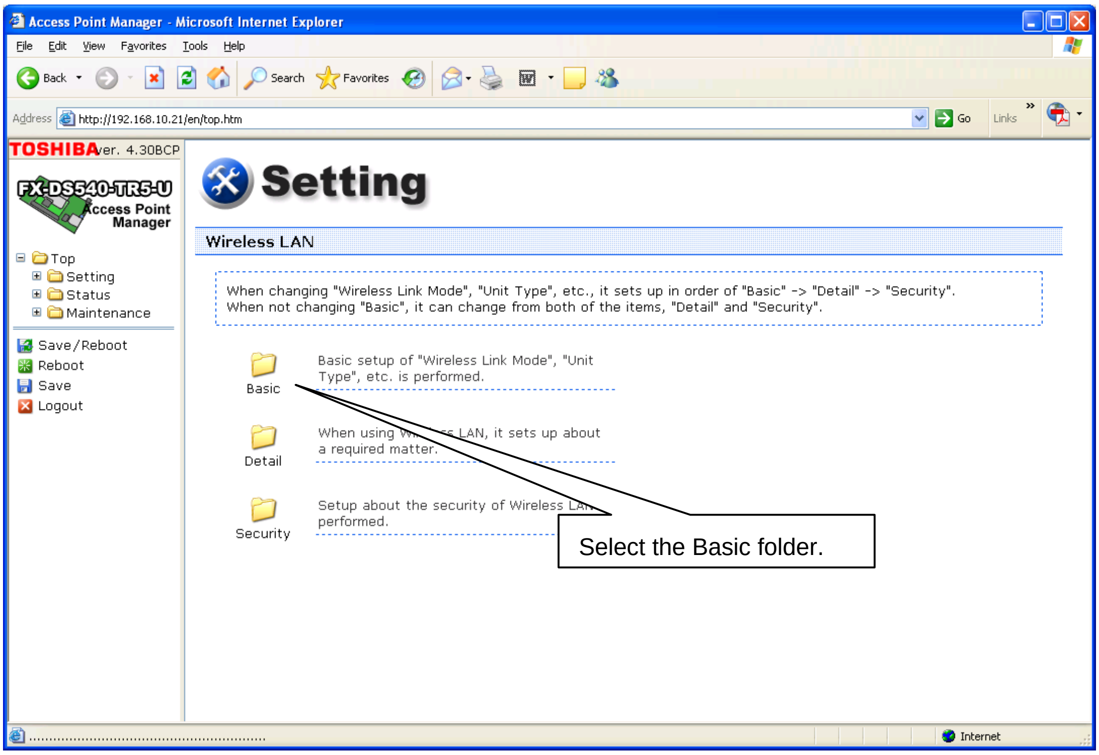
(6) Click on the Wireless LAN folder to make the wireless LAN settings.



Setup of Access Point can be changed.
When each item is changed, be sure to save, and reboot Access Point with the reboot button of the menu.

Select the Wireless LAN folder.

(7) The Wireless LAN setting screen appears. Select the Basic folder.



Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

Wireless LAN

When changing "Wireless Link Mode", "Unit Type", etc., it sets up in order of "Basic" -> "Detail" -> "Security".
When not changing "Basic", it can change from both of the items, "Detail" and "Security".

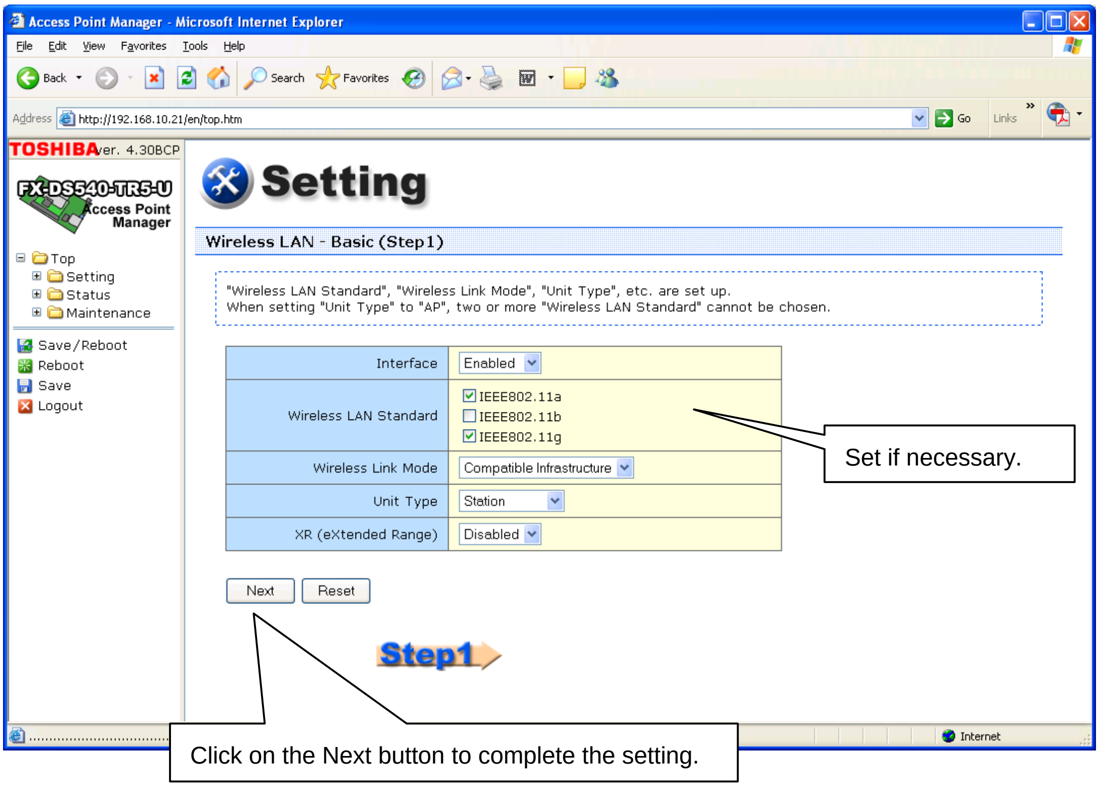
Basic — Basic setup of "Wireless Link Mode", "Unit Type", etc. is performed.

Detail — When using Wireless LAN, it sets up about a required matter.

Security — Setup about the security of Wireless LAN performed.

Select the Basic folder.

(8) The Wireless LAN – Basic setting screen appears.



Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Next
Reset
Step1
Internet

Setting

Wireless LAN - Basic (Step1)

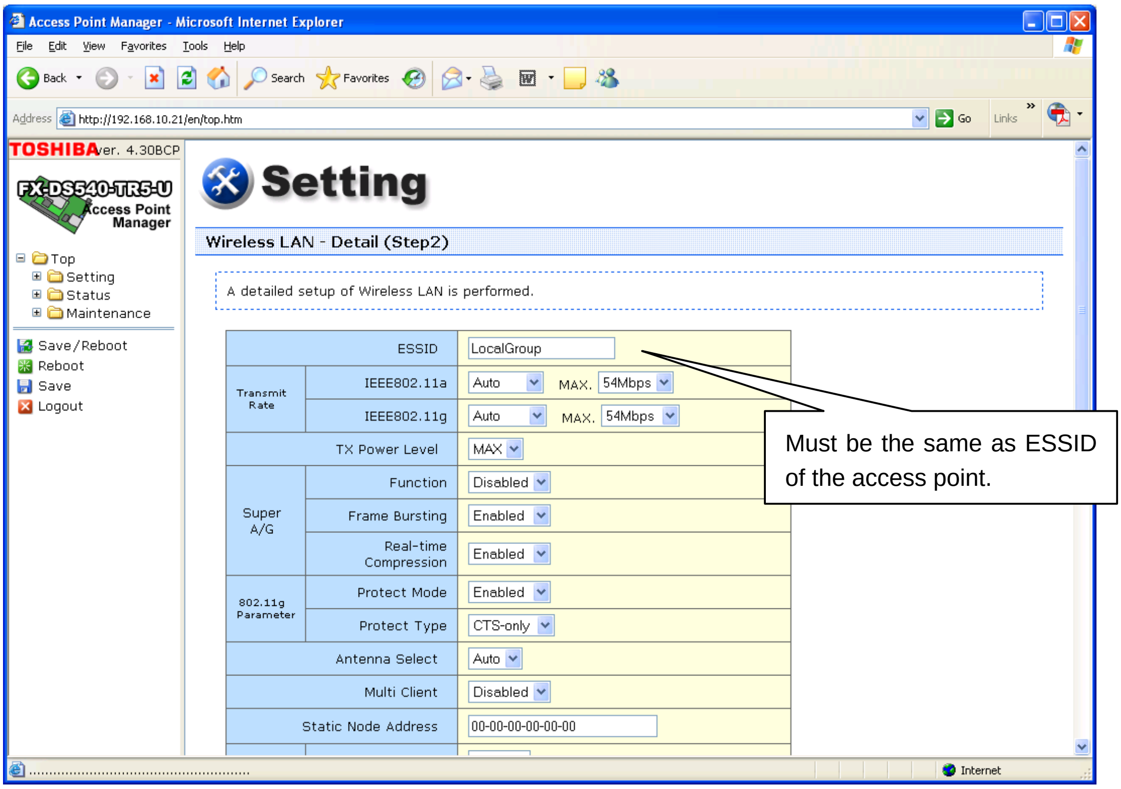
"Wireless LAN Standard", "Wireless Link Mode", "Unit Type", etc. are set up.
When setting "Unit Type" to "AP", two or more "Wireless LAN Standard" cannot be chosen.

Interface	Enabled
Wireless LAN Standard	☑ IEEE802.11a □ IEEE802.11b ☑ IEEE802.11g
Wireless Link Mode	Compatible Infrastructure
Unit Type	Station
XR (eXtended Range)	Disabled

Set if necessary.

Click on the Next button to complete the setting.

(9) The Wireless LAN - Detail screen appears.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TRS-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

Wireless LAN - Detail (Step2)

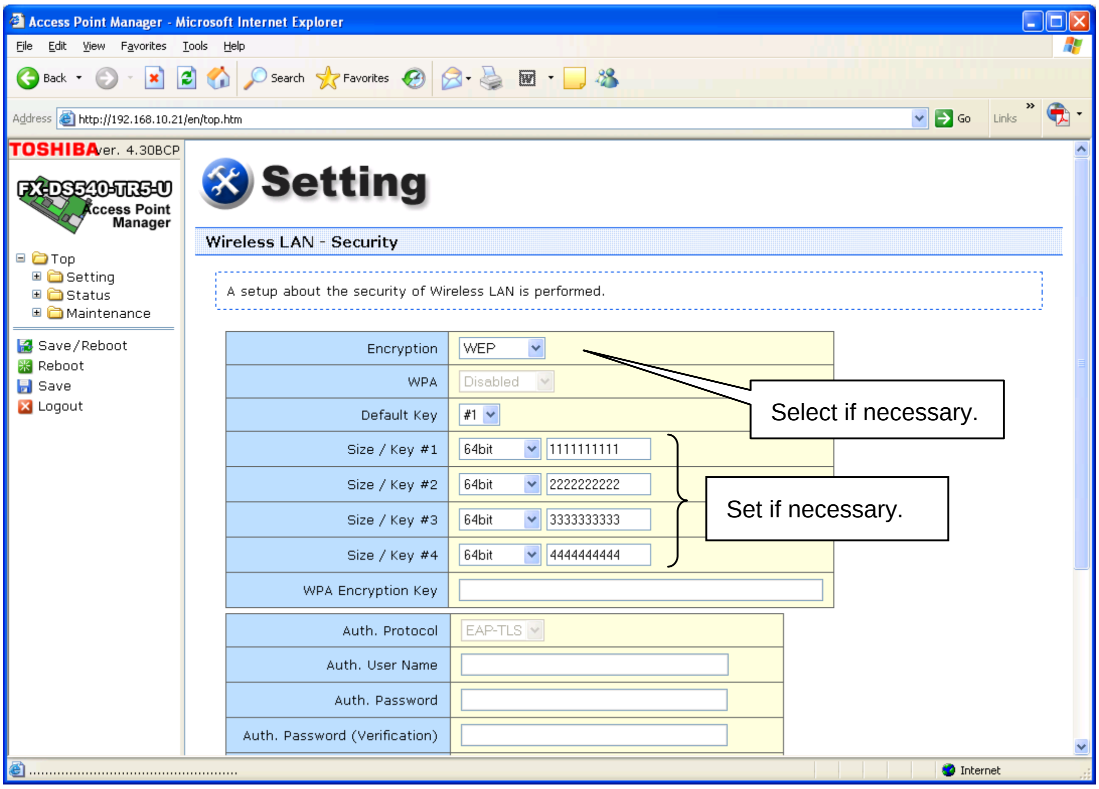
A detailed setup of Wireless LAN is performed.

ESSID		LocalGroup
Transmit Rate	IEEE802.11a	Auto MAX. 54Mbps
	IEEE802.11g	Auto MAX. 54Mbps
TX Power Level		MAX
Super A/G	Function	Disabled
	Frame Bursting	Enabled
	Real-time Compression	Enabled
802.11g Parameter	Protect Mode	Enabled
	Protect Type	CTS-only
Antenna Select		Auto
Multi Client		Disabled
Static Node Address		00-00-00-00-00-00

Must be the same as ESSID of the access point.

Click on the Next button to complete the setting.

(10) The Wireless LAN - Security setting screen appears.
Select an encryption type and set the encryption key if necessary.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TRS-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

Wireless LAN - Security

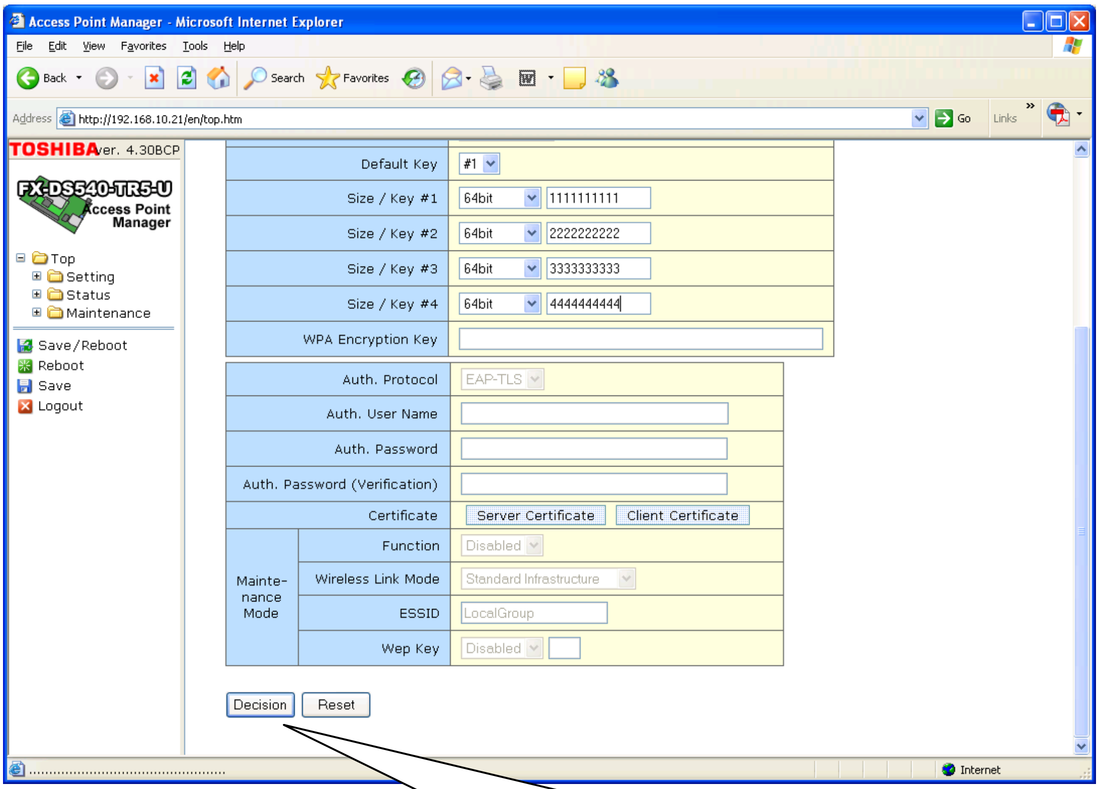
A setup about the security of Wireless LAN is performed.

Encryption	WEP	
WPA	Disabled	
Default Key	#1	
Size / Key #1	64bit	1111111111
Size / Key #2	64bit	2222222222
Size / Key #3	64bit	3333333333
Size / Key #4	64bit	4444444444
WPA Encryption Key		
Auth. Protocol	EAP-TLS	
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		

Select if necessary.

Set if necessary.

(11) Select an encryption type and set the encryption key, if necessary.



Access Point Manager - Microsoft Internet Explorer

Address http://192.168.10.21/en/top.htm

TOSHIBA ver. 4.30BCP

FX-DS540-TR5-U Access Point Manager

- Top
  - Setting
  - Status
  - Maintenance
- Save/Reboot
- Reboot
- Save
- Logout

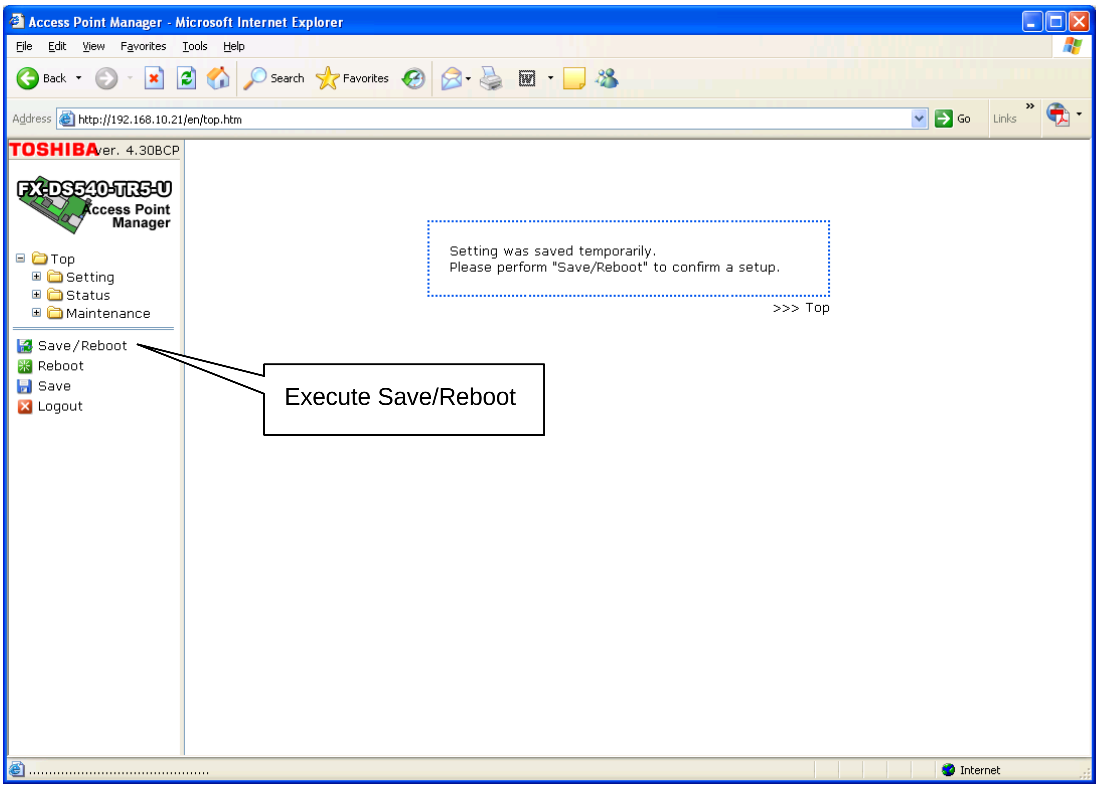
Default Key	#1	
Size / Key #1	64bit	1111111111
Size / Key #2	64bit	2222222222
Size / Key #3	64bit	3333333333
Size / Key #4	64bit	4444444444
WPA Encryption Key		

Auth. Protocol		EAP-TLS
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

Decision Reset

Click on the Decision button to complete the setting.

(12) To make the changes effective, execute Save/Reboot.



Access Point Manager - Microsoft Internet Explorer

Address http://192.168.10.21/en/top.htm

TOSHIBA ver. 4.30BCP

FX-DS540-TR5-U Access Point Manager

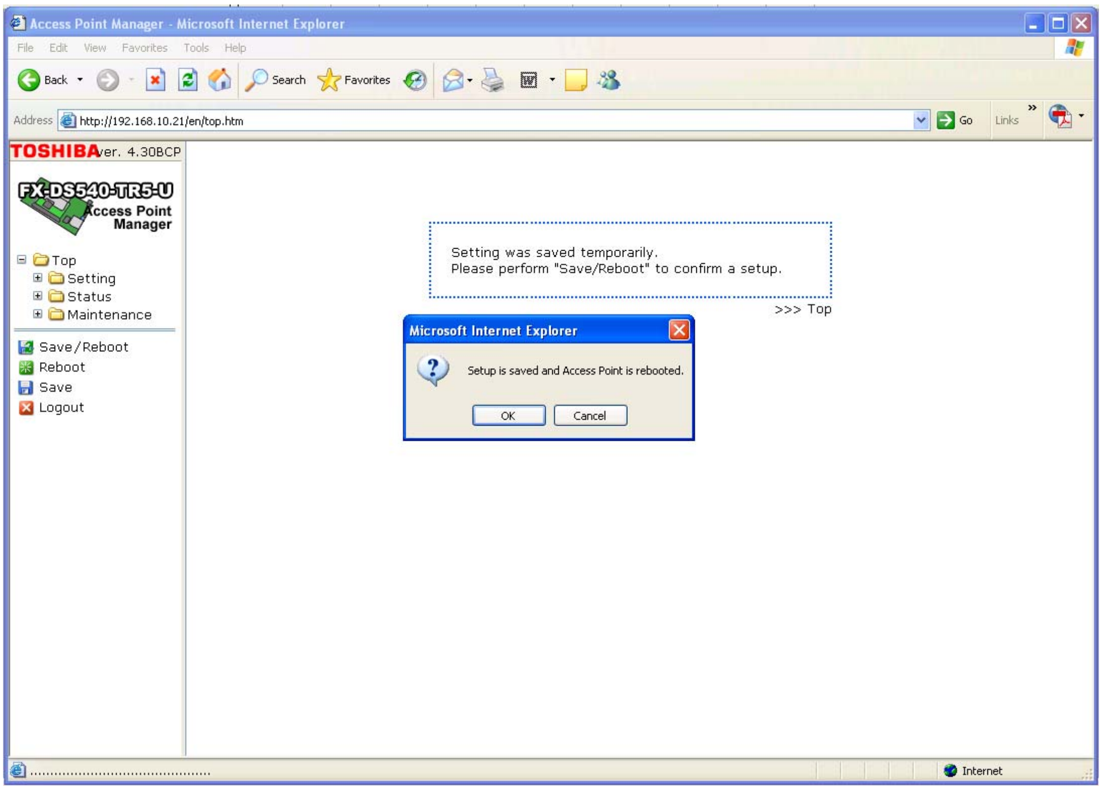
- Top
  - Setting
  - Status
  - Maintenance
- Save/Reboot
- Reboot
- Save
- Logout

Setting was saved temporarily.
Please perform "Save/Reboot" to confirm a setup.

>>> Top

Execute Save/Reboot

(13) The confirmation dialog box appears. Click on the OK button.

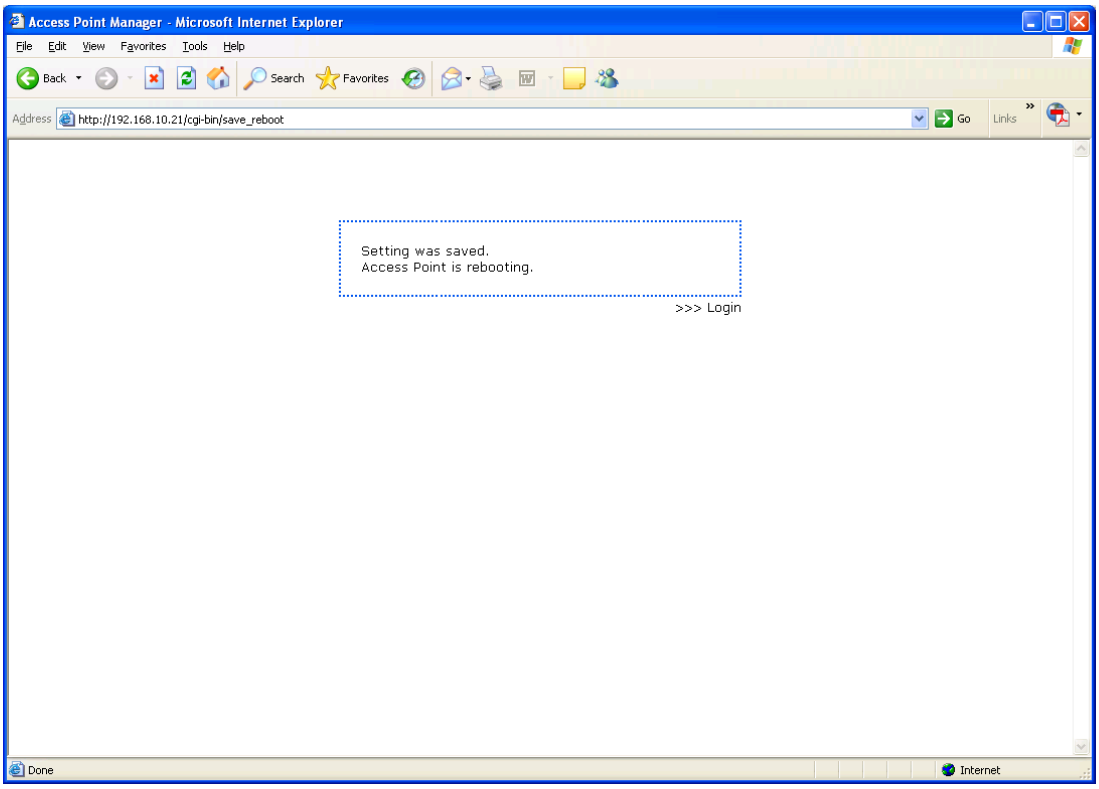


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
>>> Top
Microsoft Internet Explorer
OK
Cancel
Internet

Setting was saved temporarily.
Please perform "Save/Reboot" to confirm a setup.

Setup is saved and Access Point is rebooted.

(14) Execute Save/Reboot.

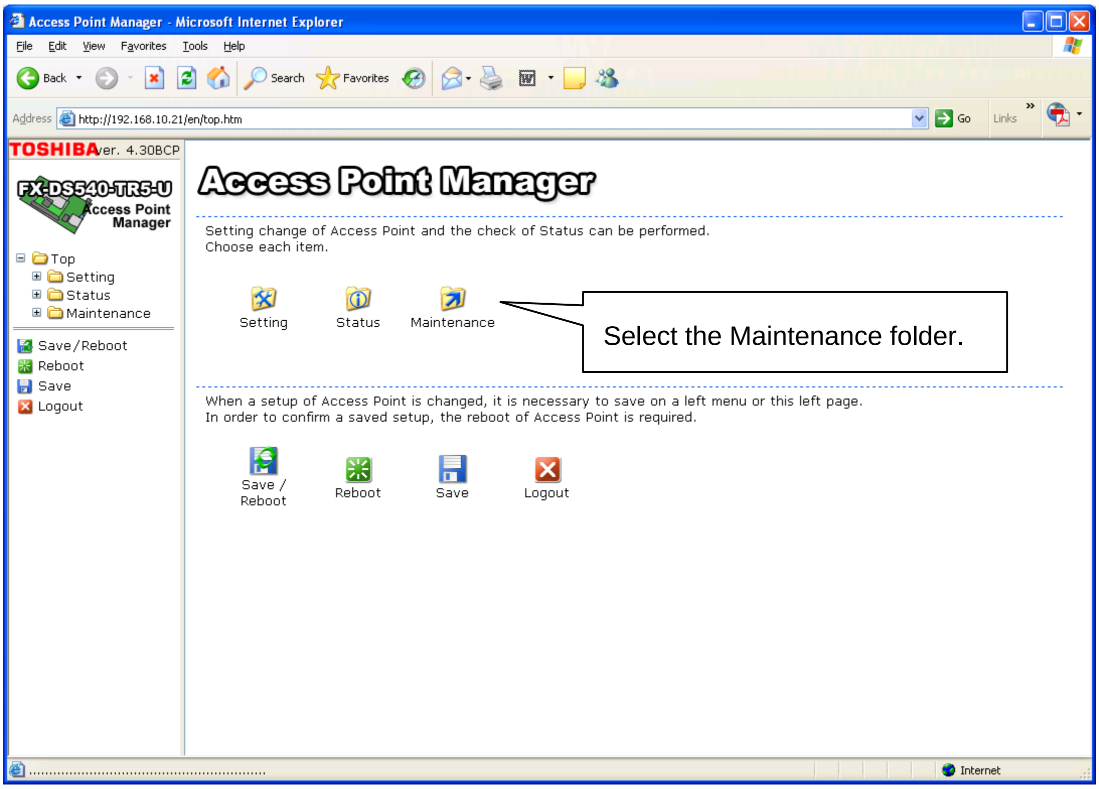


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/cgi-bin/save_reboot
Go Links
>>> Login
Done
Internet

Setting was saved.
Access Point is rebooting.

7. FIRMWARE DOWNLOADING

(1) Click on the Maintenance icon.

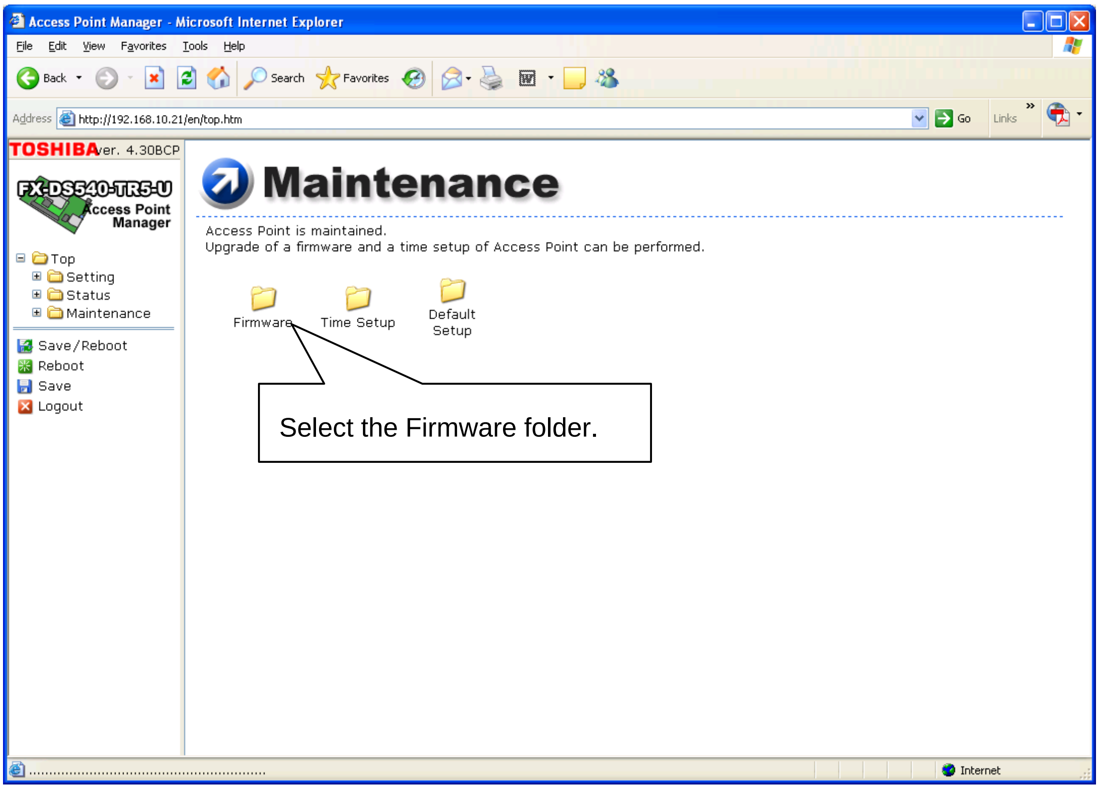


Setting change of Access Point and the check of Status can be performed.
Choose each item.

When a setup of Access Point is changed, it is necessary to save on a left menu or this left page.
In order to confirm a saved setup, the reboot of Access Point is required.

Select the Maintenance folder.

(2) Click on the Firmware folder.

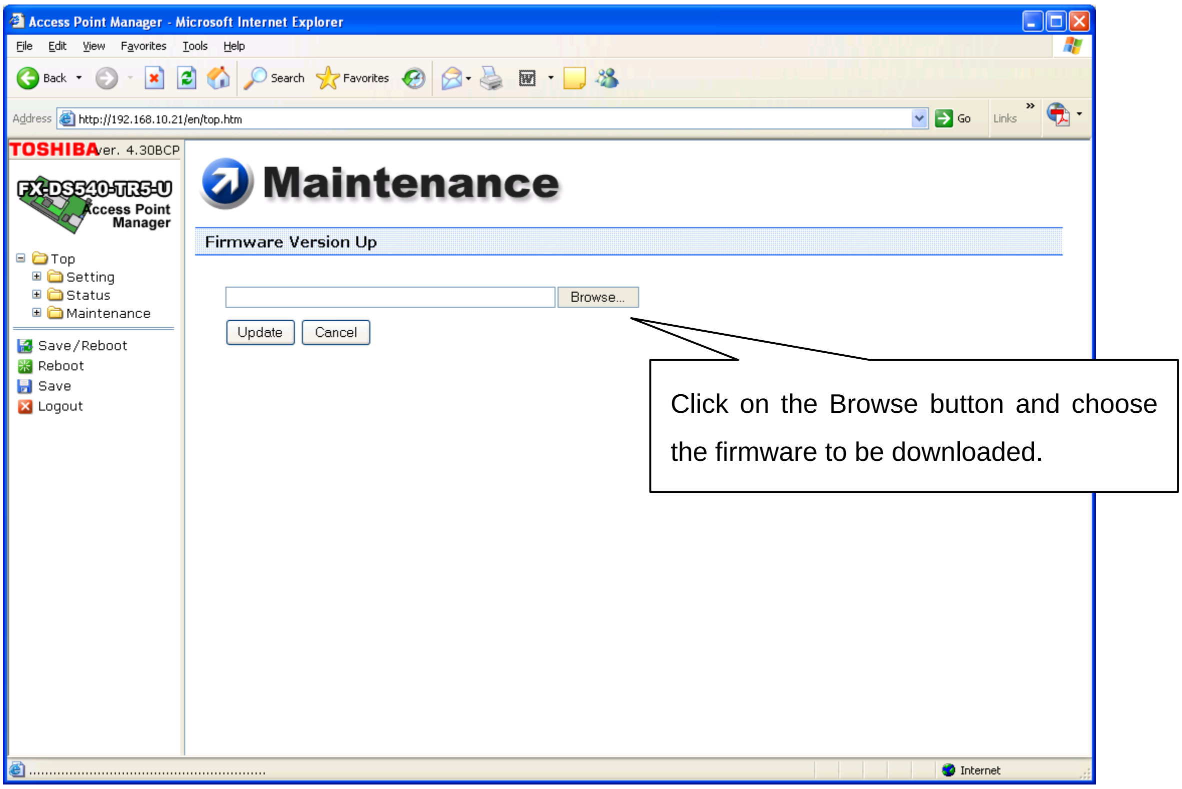


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Maintenance
Firmware
Time Setup
Default Setup
Internet

Access Point is maintained.
Upgrade of a firmware and a time setup of Access Point can be performed.

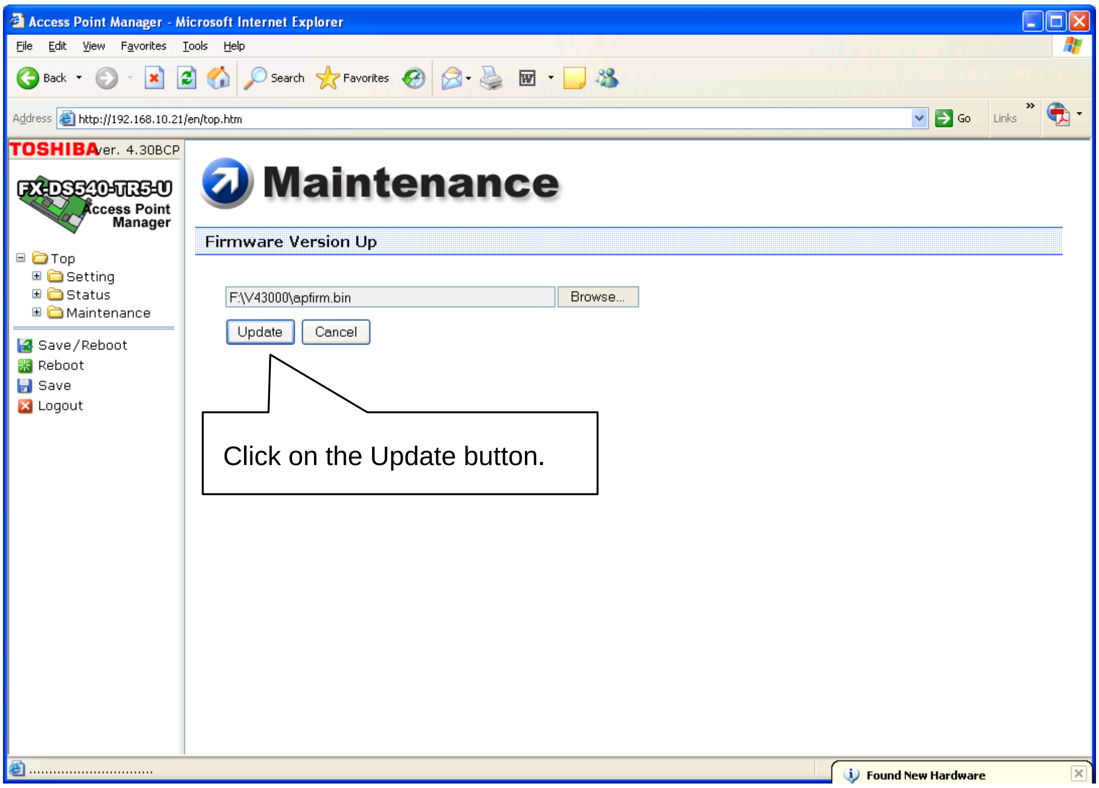
Select the Firmware folder.

(3) Choose the firmware to be downloaded.



Click on the Browse button and choose the firmware to be downloaded.

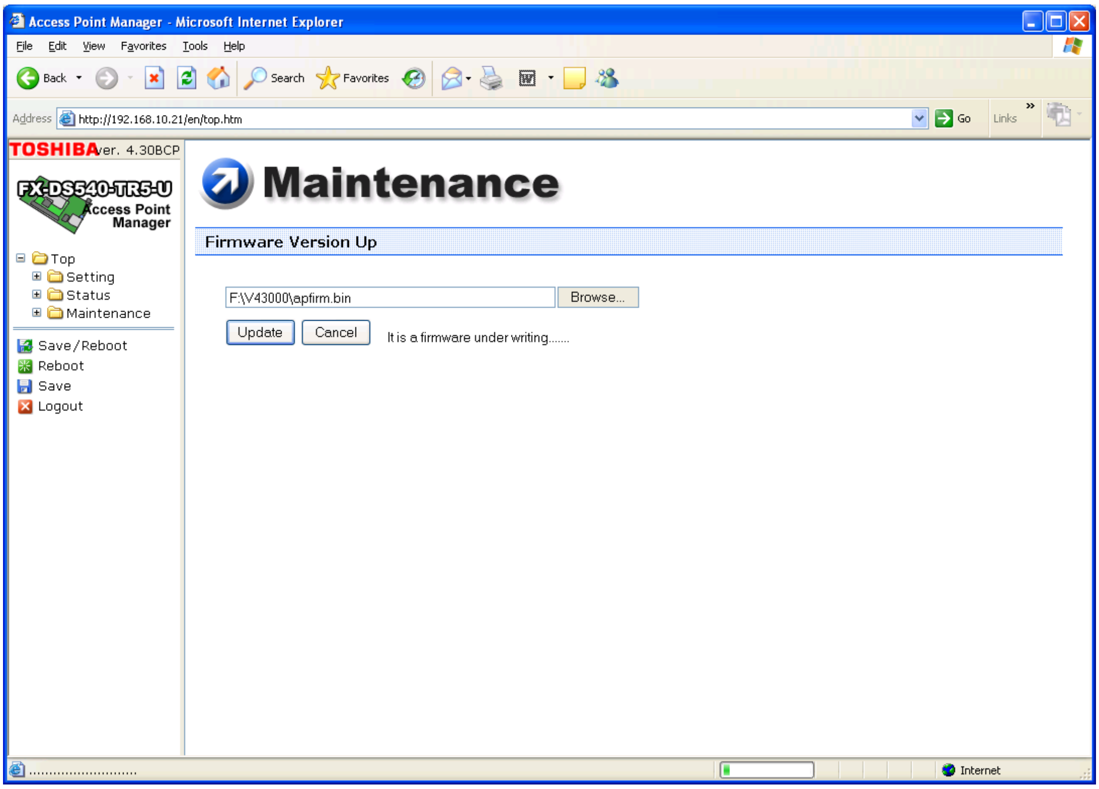
(4) Click on the Update button.



F:\V43000\apfirm.bin

Click on the Update button.

(5) Downloading of the firmware is started.



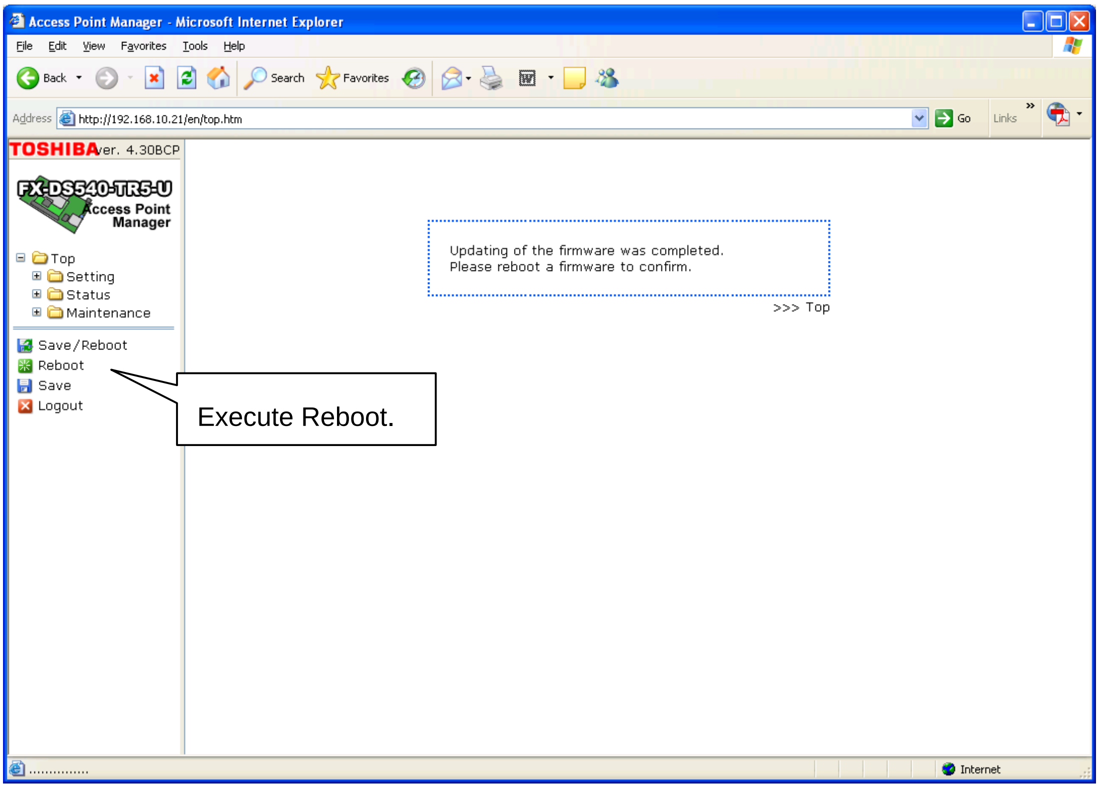
Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Maintenance
Browse...
Update
Cancel
Internet

Firmware Version Up

F:\V43000\apfirm.bin

It is a firmware under writing.......

(6) When the downloading is completed, execute Reboot.

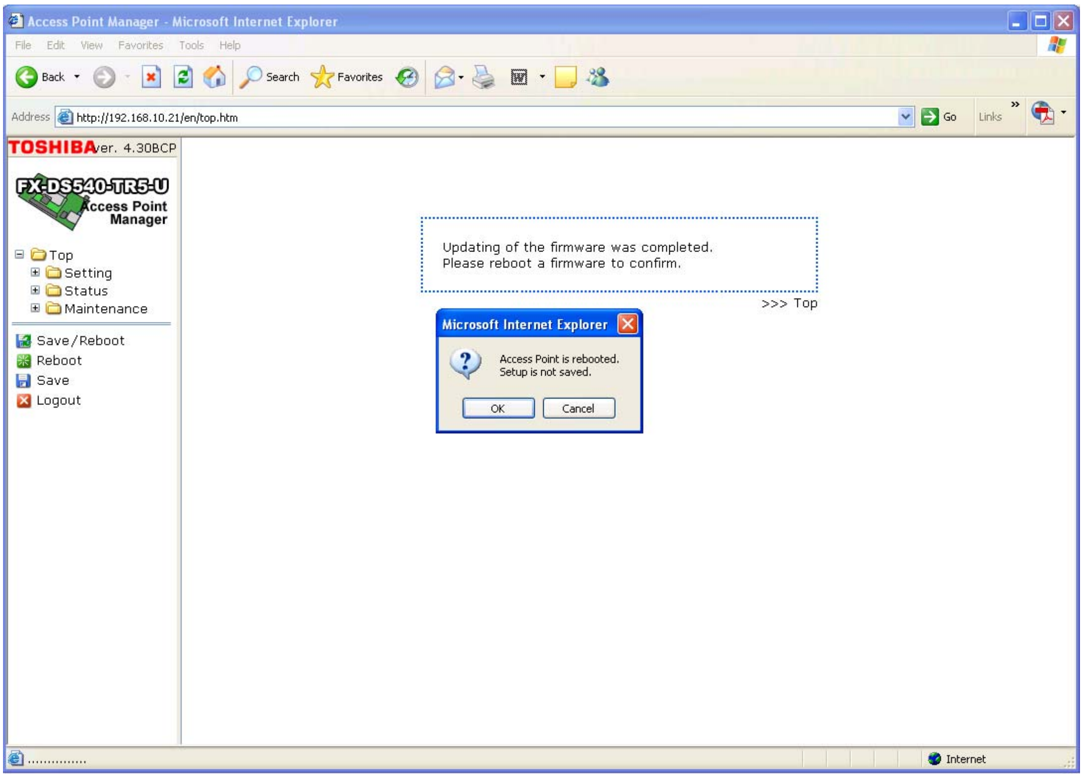


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
>>> Top
Internet

Updating of the firmware was completed.
Please reboot a firmware to confirm.

Execute Reboot.

(7) Click on the OK button on the confirmation dialog box.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
>>> Top
Internet

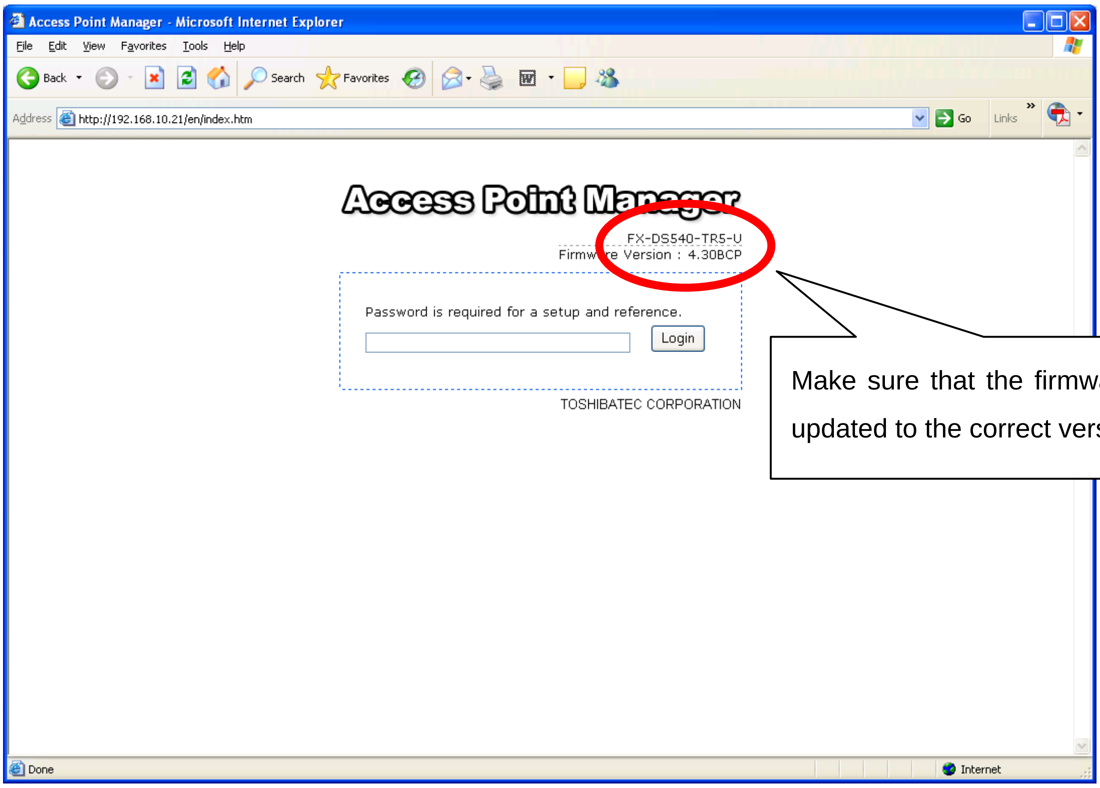
Updating of the firmware was completed.
Please reboot a firmware to confirm.

Microsoft Internet Explorer

Access Point is rebooted.
Setup is not saved.

OK Cancel

(8) The access point is rebooted.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/index.htm
Go Links
Access Point Manager
Login
TOSHIBATEC CORPORATION
Done
Internet

FX-DS540-TR5-U
Firmware Version : 4.30BCP

Password is required for a setup and reference.

Make sure that the firmware has been updated to the correct version.

8. WIRELESS LAN CONNECTION USING ENCRYPTION/ AUTHETICATION

8.1 SYSTEM CONFIGURATION

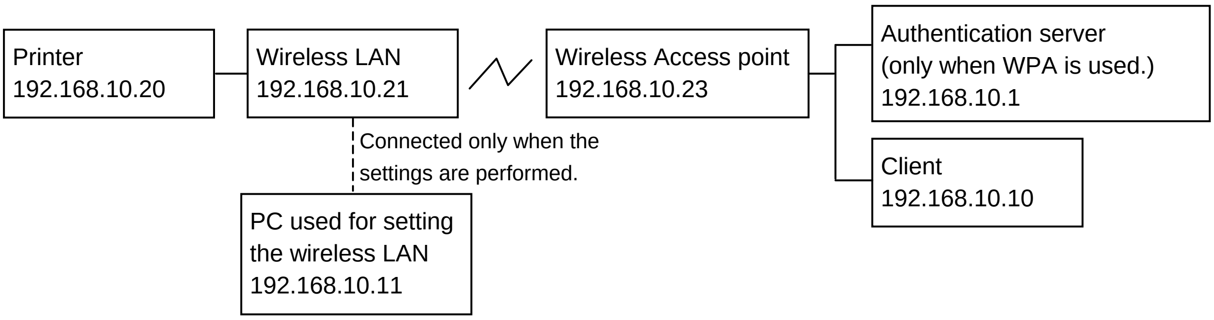
Required devices

- Printer (192.168.10.20)
- Wireless LAN module (192.168.10.21)
- PC (Required to configure the wireless LAN module settings.)
- Access point (192.168.10.23)

[When WPA is used, the following are also required.]

- Authentication server (192.168.10.1)
- Root certificate
- User certificate (Only when a connection is made using EAP-TLS.)

NOTE*: How to obtain a certificate is described separately.*

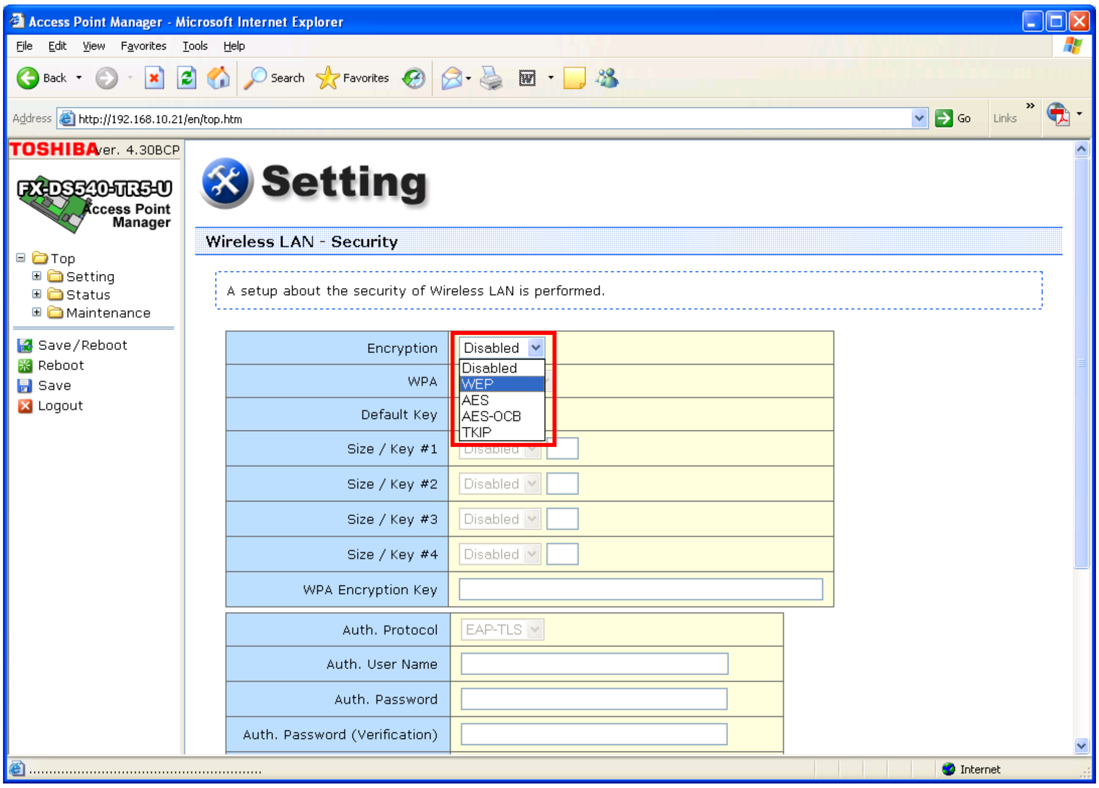


8.2 SETTINGS FOR THE WIRELESS LAN MODULE

<WEP encryption>

(1) Set the security features.

Choose WEP from the Encryption pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Setting
Internet

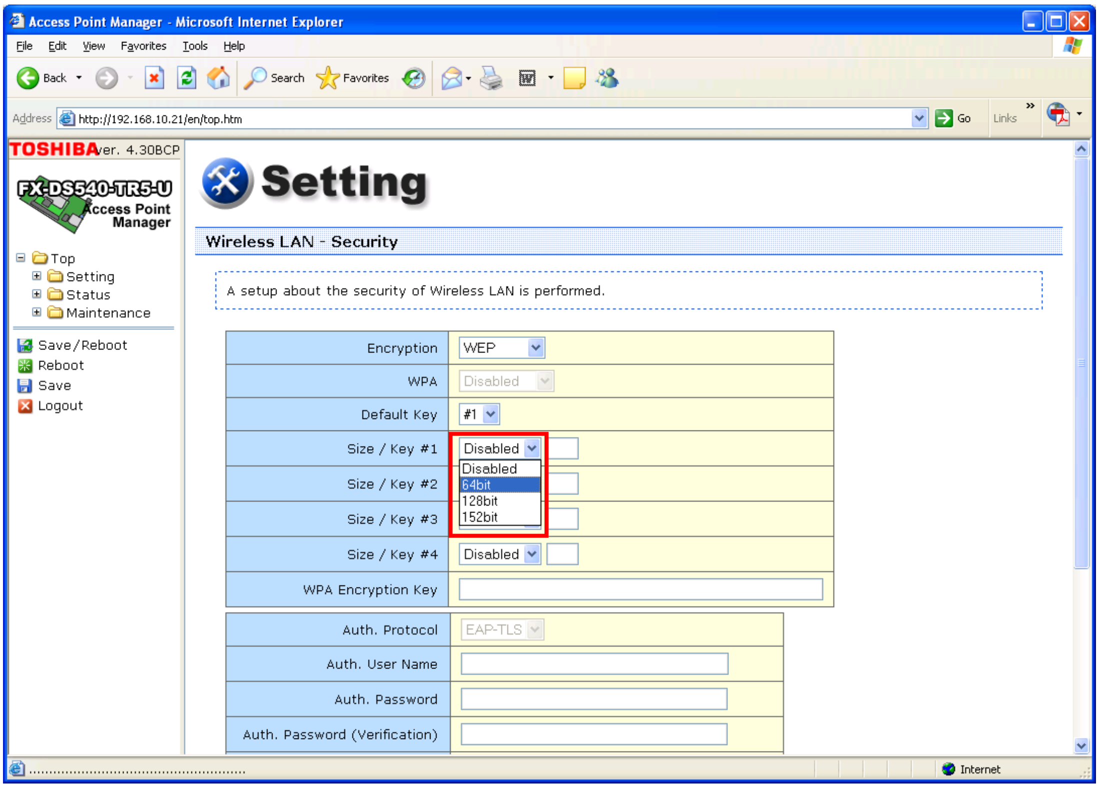
Address http://192.168.10.21/en/top.htm

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	Disabled Disabled WEP AES AES-OCB TKIP
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	
Auth. Password (Verification)	

Set the default key and size/key number. In the following sample screen, #1 is set for the key number and 64 bit for the size.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Setting
Internet

Address http://192.168.10.21/en/top.htm

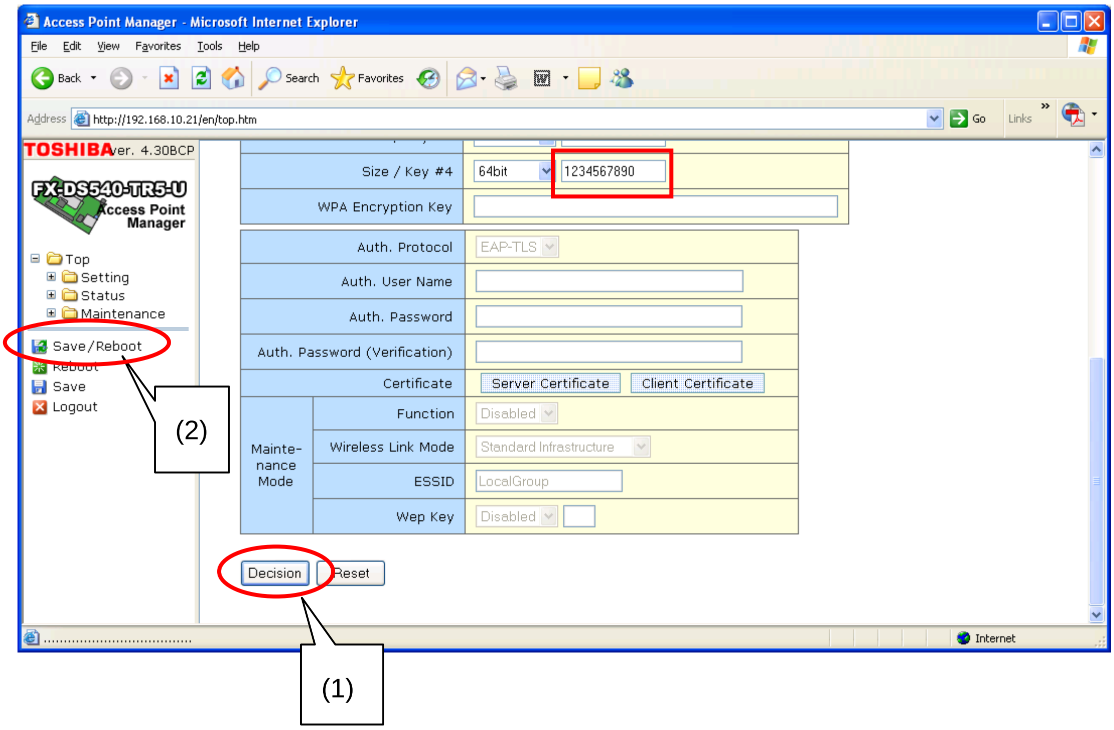
Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	WEP
WPA	Disabled
Default Key	#1
Size / Key #1	Disabled Disabled 64bit 128bit 152bit
Size / Key #2	
Size / Key #3	
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	
Auth. Password (Verification)	

Enter a key with hexadecimal code.

Click on the Decision button (1), then click on Save/Reboot to restart the wireless LAN module (2).

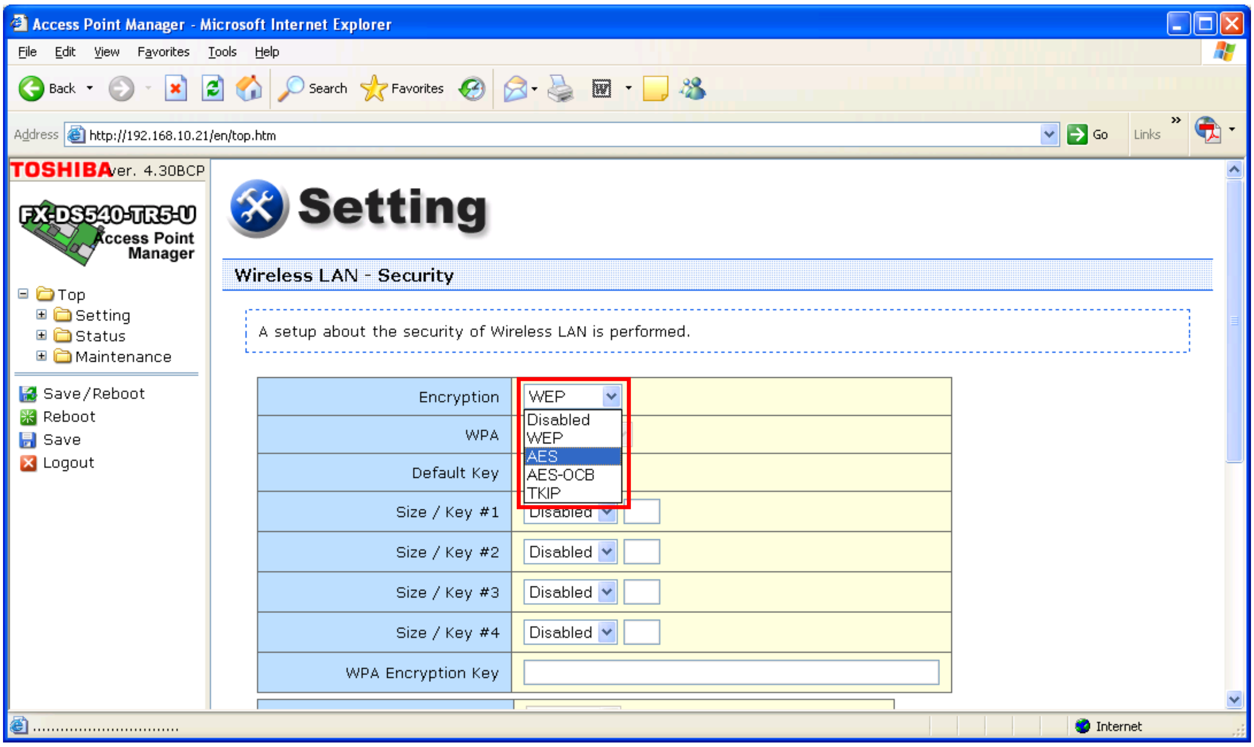


Size / Key #4	64bit	1234567890
WPA Encryption Key		
Auth. Protocol	EAP-TLS	
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate	Server Certificate	Client Certificate
Mainte-nance Mode Function	Disabled	
Wireless Link Mode	Standard Infrastructure	
ESSID	LocalGroup	
Wep Key	Disabled	

<AES encryption with no options>

(1) Set the security features.

Choose AES from the Encryption pull down menu.



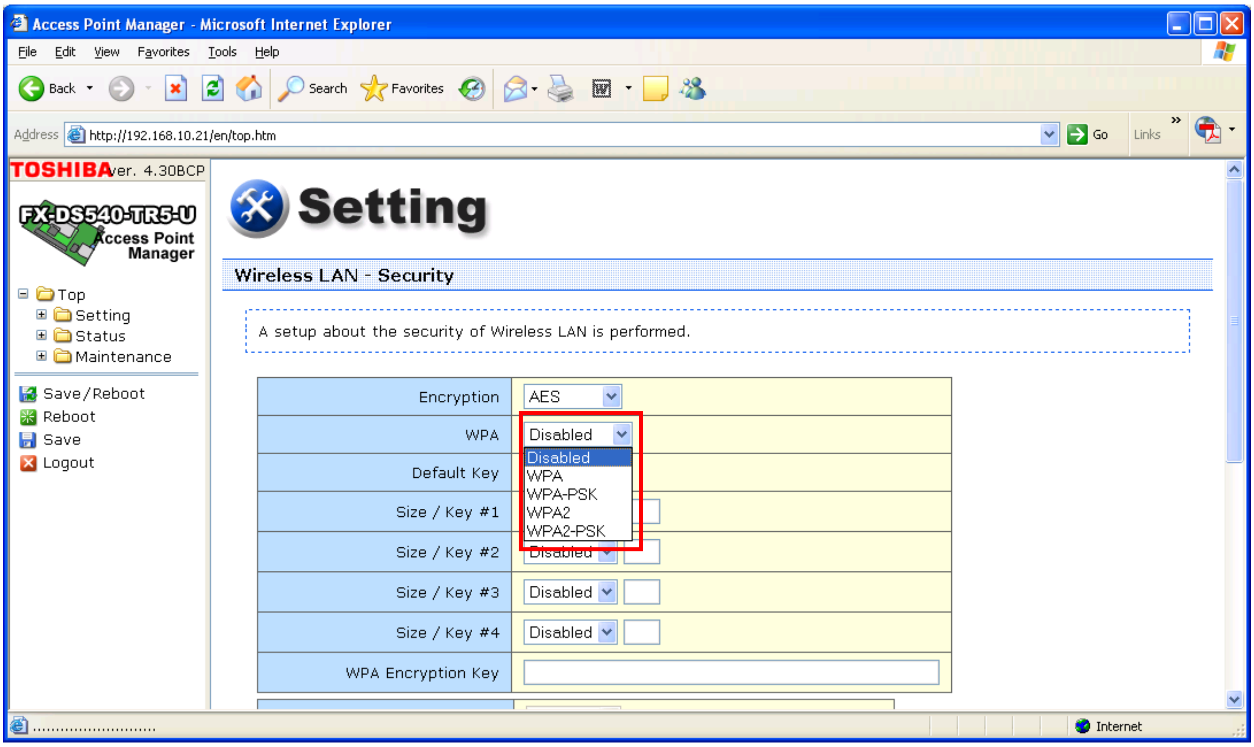
Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	WEP Disabled WEP AES AES-OCB TKIP
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	

Choose Disabled from the WPA pull down menu.



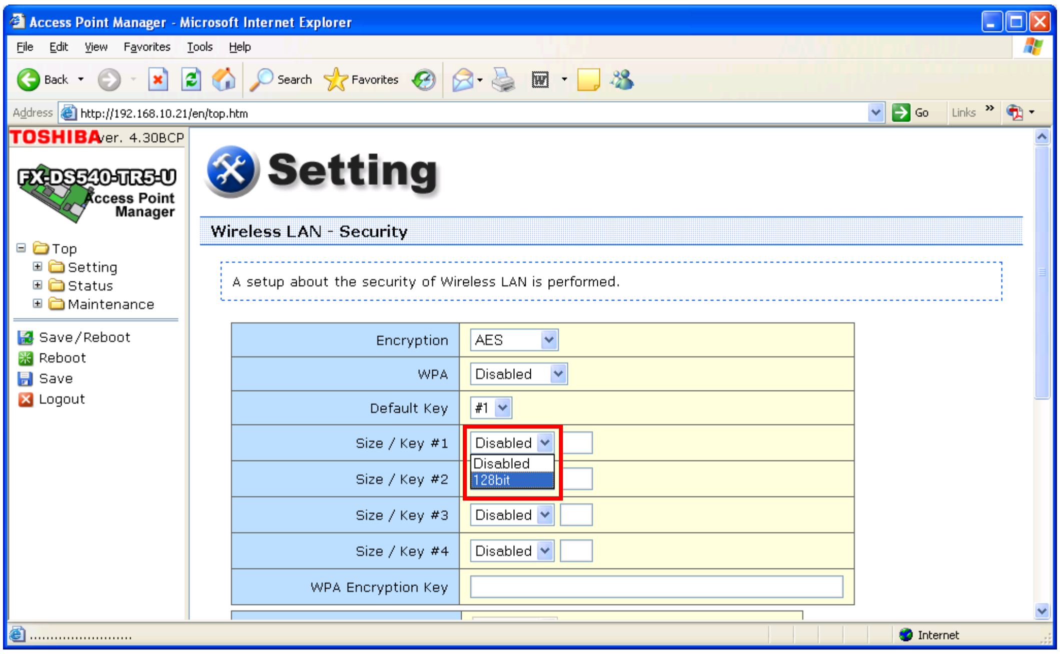
Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	AES
WPA	Disabled Disabled WPA WPA-PSK WPA2 WPA2-PSK
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	

Set the default key and size/key number. In the following sample screen, 1 is set for the key number and 128 bit for the size.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

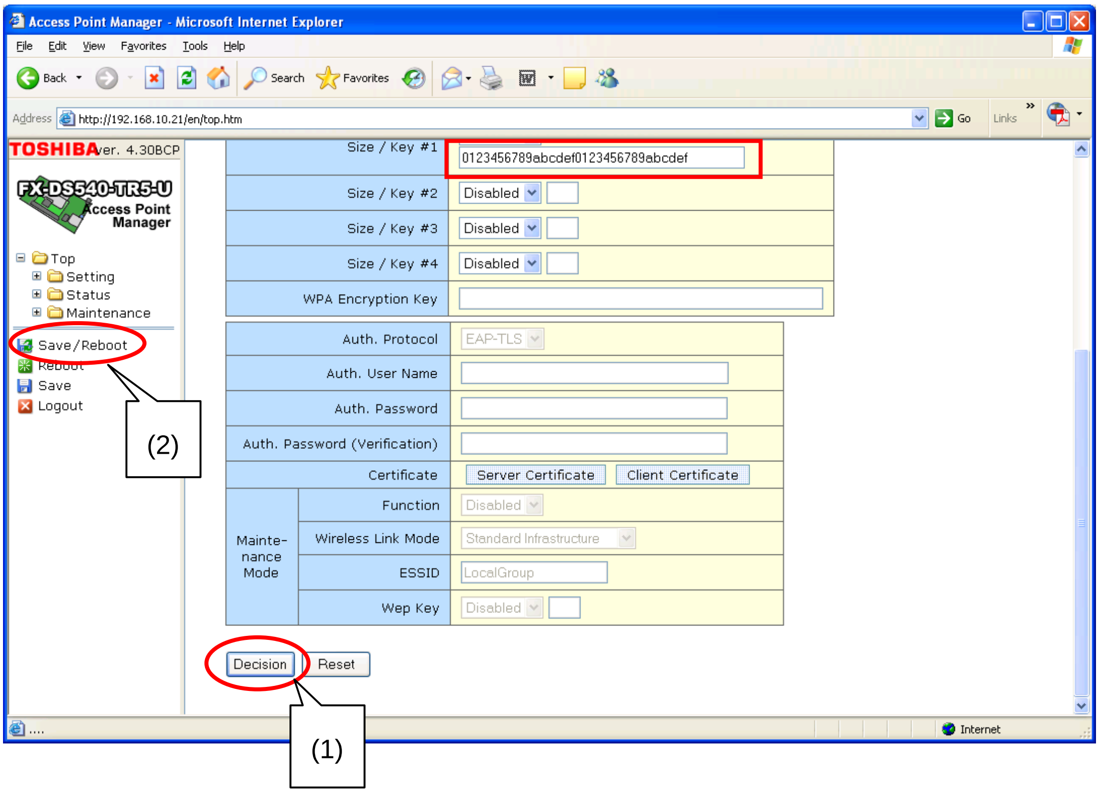
Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	AES
WPA	Disabled
Default Key	#1
Size / Key #1	Disabled Disabled 128bit
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	

Enter a key with hexadecimal code.

Click on the Decision button (1), then click on Save/Reboot to restart the wireless LAN module (2).

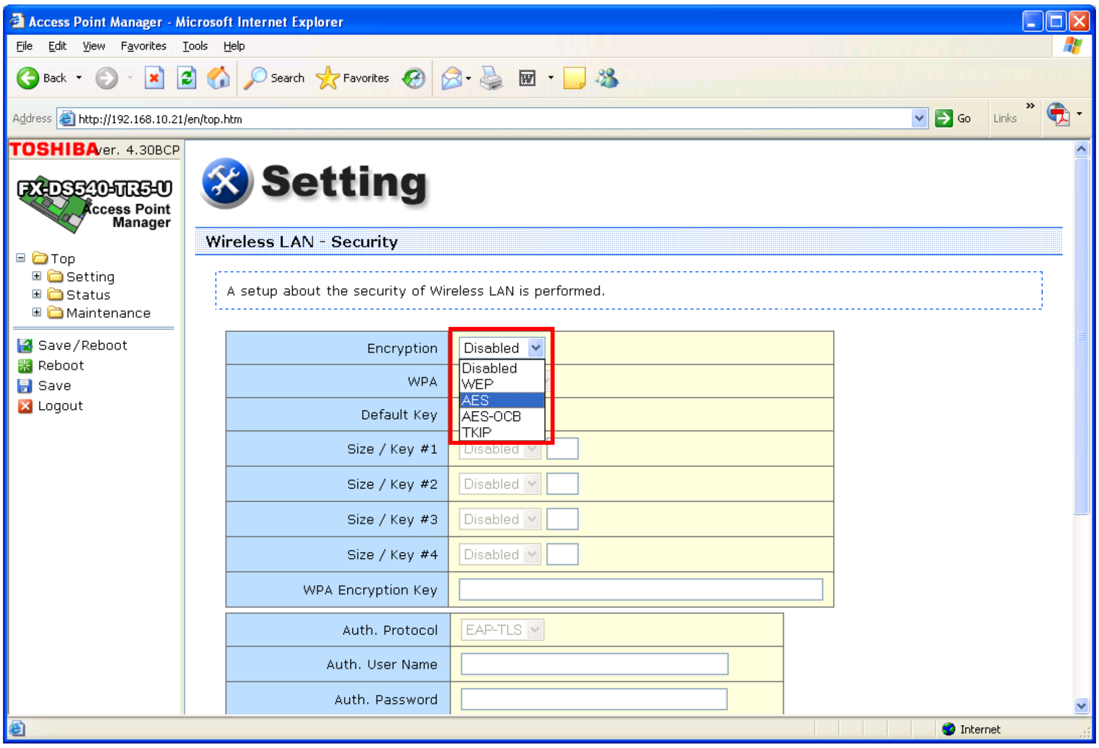

Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
(2)
Decision
Reset
(1)
Internet

Size / Key #1		0123456789abcdef0123456789abcdef
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		EAP-TLS
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

<AES encryption with WPA>

(1) Set the security features and authentication method.

Choose AES from the Encryption pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

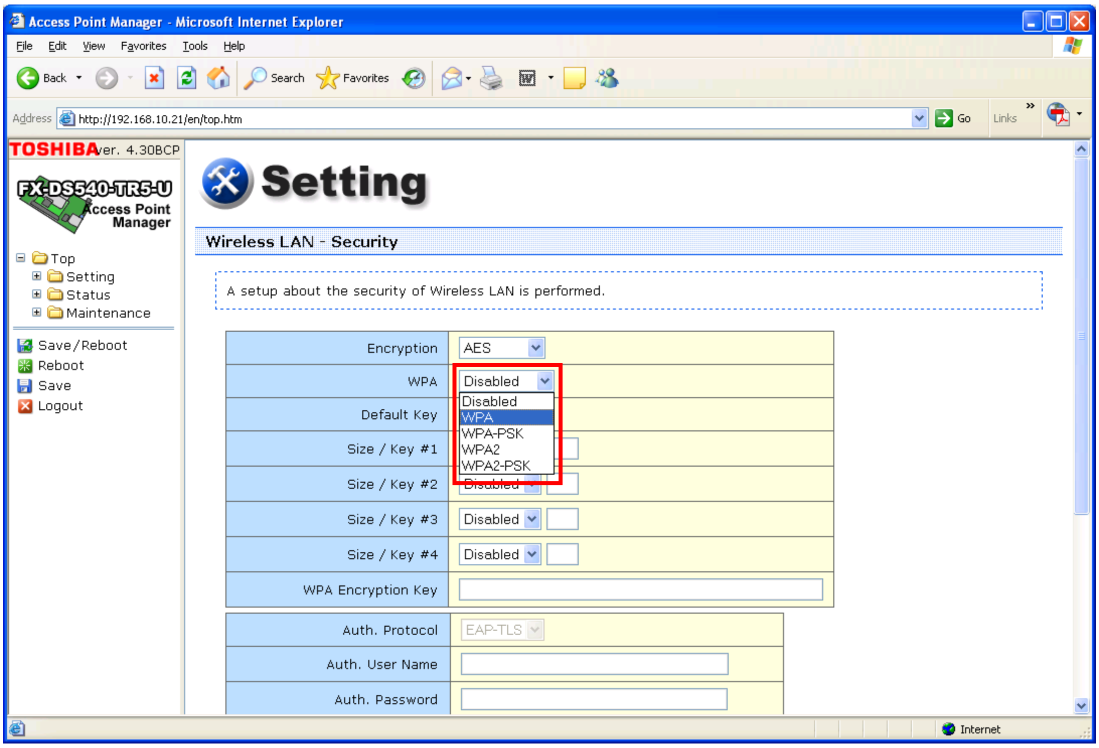
Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	Disabled Disabled WEP AES AES-OCB TKIP
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Choose WPA from the WPA pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

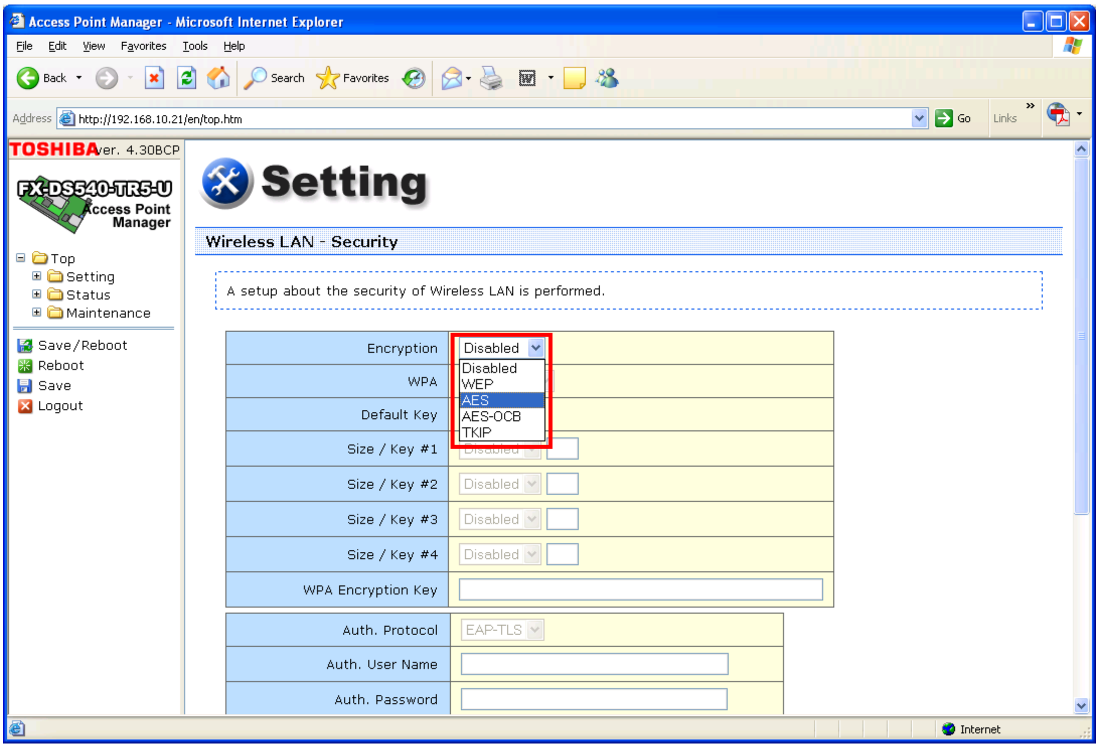
Encryption	AES
WPA	Disabled Disabled WPA WPA-PSK WPA2 WPA2-PSK
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Continued on **<When using WPA>**.

<AES encryption with WPA-PSK>

(1) Set the security features and authentication method.

Choose AES from the Encryption pull down menu.



Access Point Manager - Microsoft Internet Explorer

Address http://192.168.10.21/en/top.htm

TOSHIBA ver. 4.30BCP

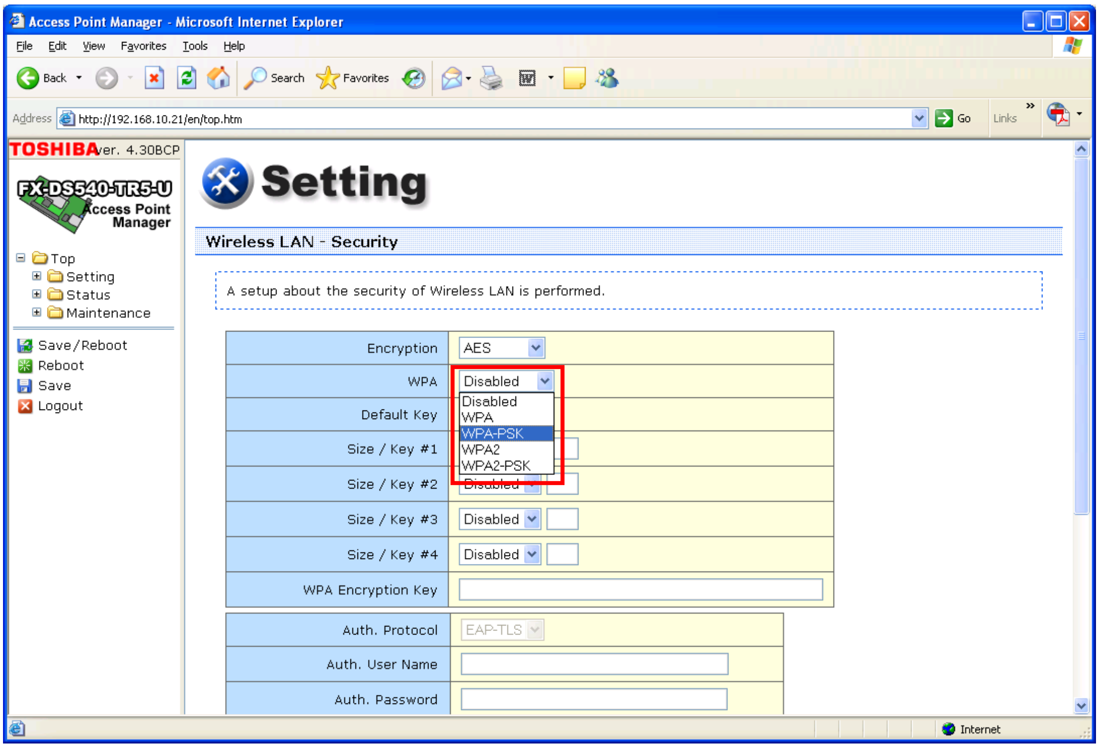
Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	Disabled
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Choose WPA-PSK from the WPA pull down menu.



Access Point Manager - Microsoft Internet Explorer

Address http://192.168.10.21/en/top.htm

TOSHIBA ver. 4.30BCP

Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

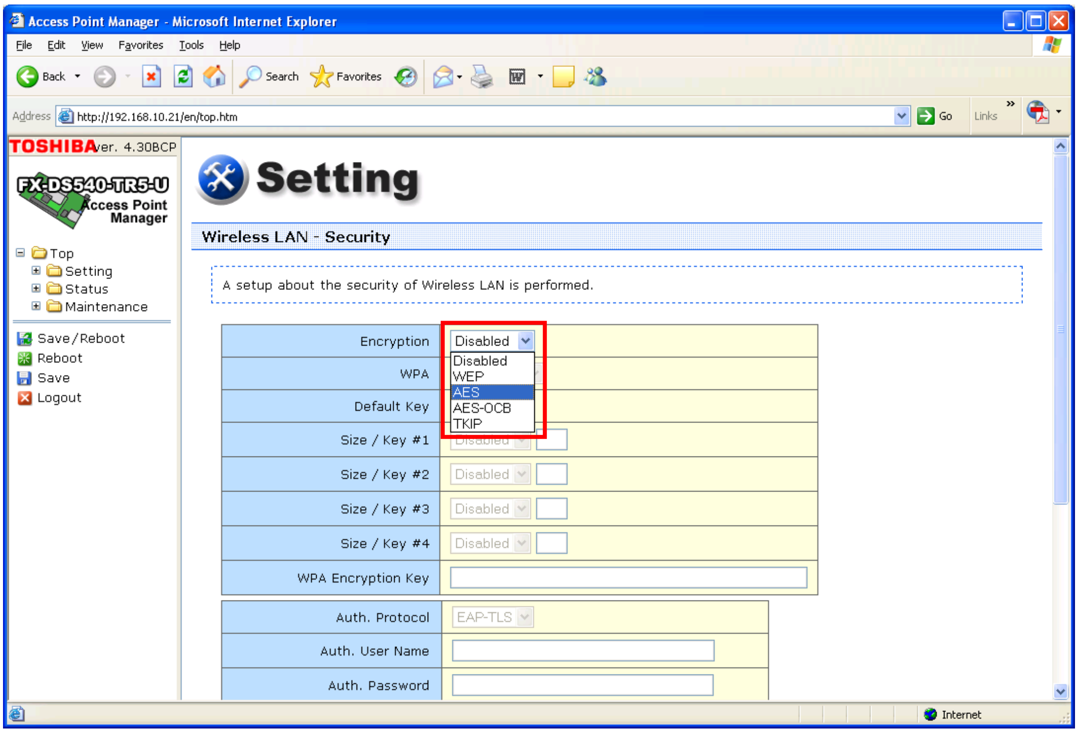
Encryption	AES
WPA	Disabled
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Continued on **<When using WPA-PSK>**.

<AES encryption with WPA2>

(1) Set the security features and authentication method.

Choose AES from the Encryption pull down menu.

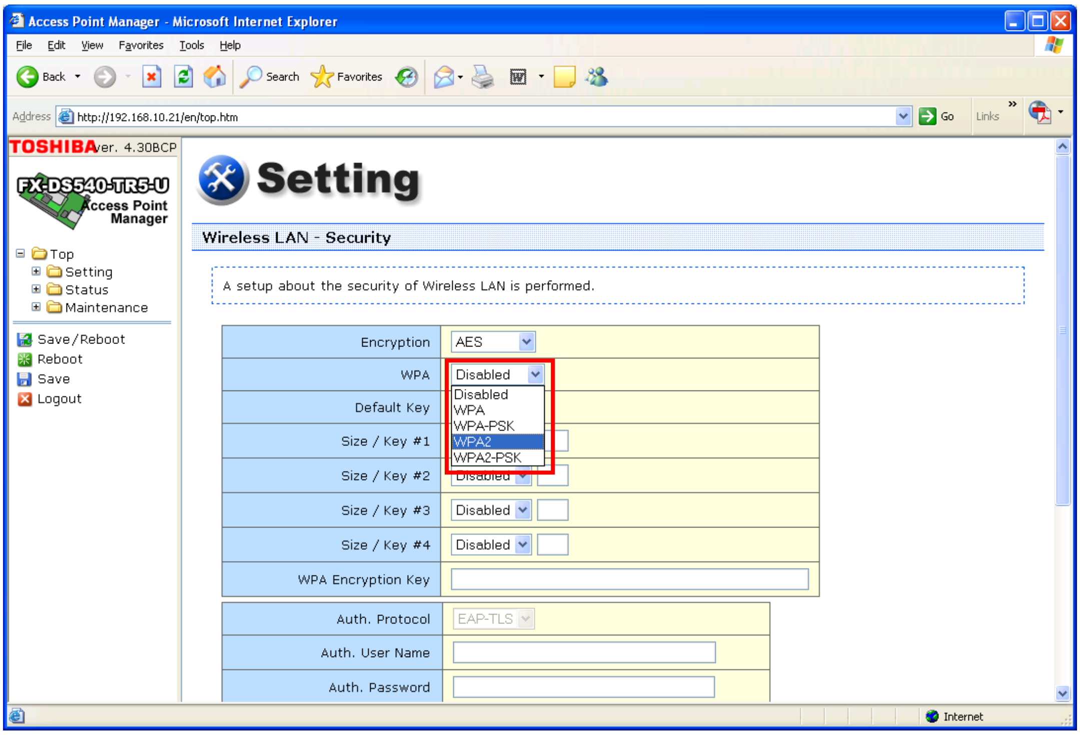

Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Setting
Internet

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	Disabled Disabled WEP AES AES-OCB TKIP
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Choose WPA2 from the WPA pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Setting
Internet

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

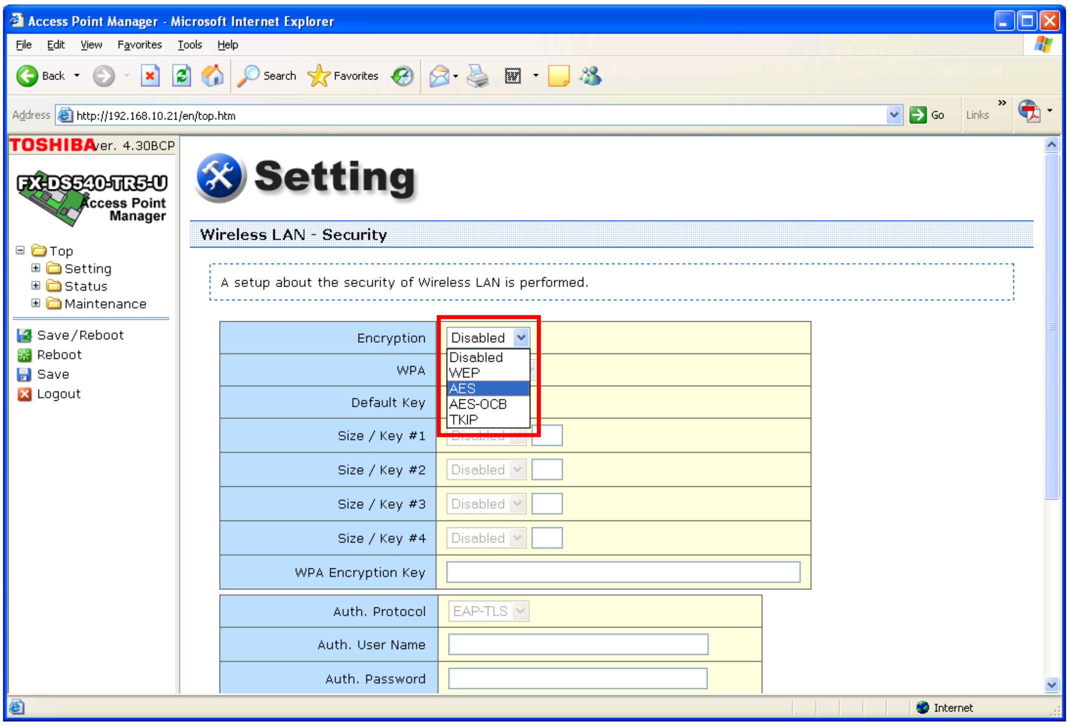
Encryption	AES
WPA	Disabled Disabled WPA WPA-PSK WPA2 WPA2-PSK
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Continued on **<When using WPA2>**.

<AES encryption with WPA2-PSK>

(1) Set the security features and authentication method.

Choose AES from the Encryption pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

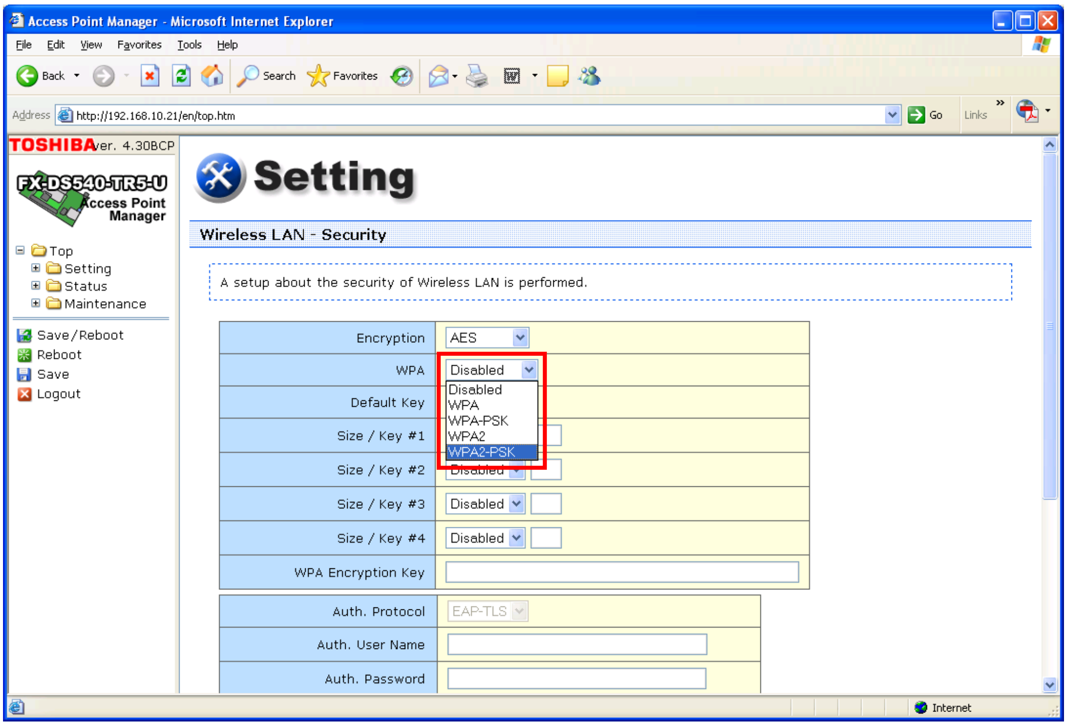
Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	Disabled Disabled WEP AES AES-OCB TKIP
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Choose WPA2-PSK from the WPA pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

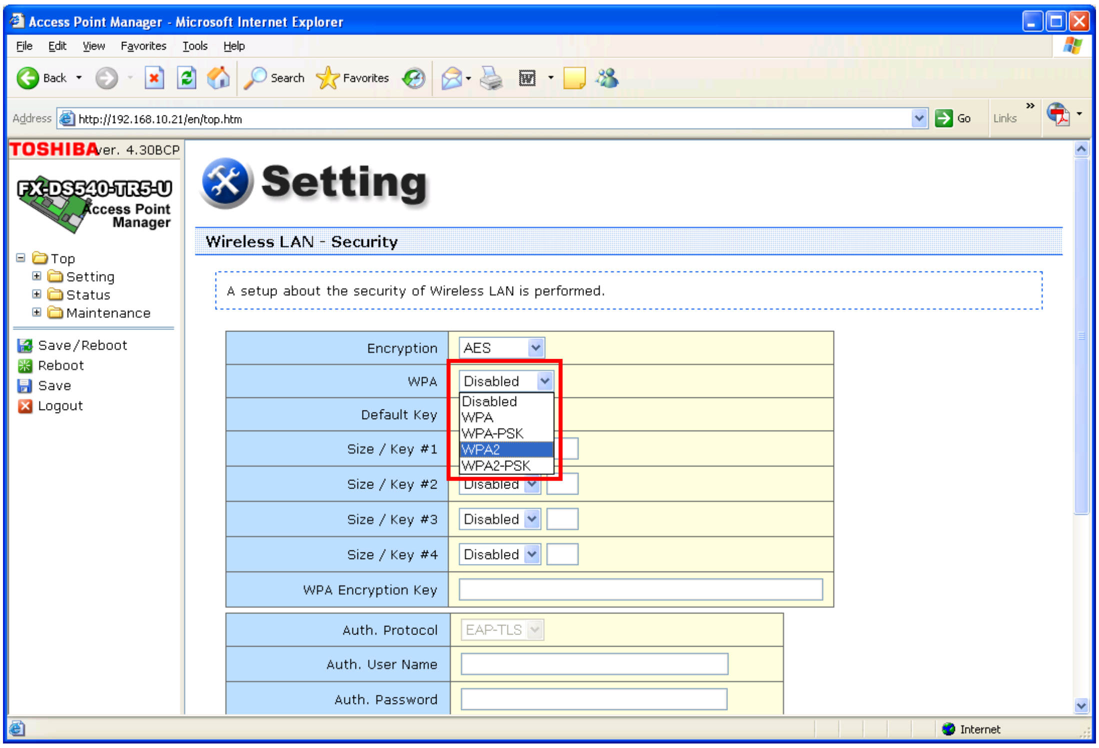
Encryption	AES
WPA	Disabled Disabled WPA WPA-PSK WPA2 WPA2-PSK
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Continued on **<When using WPA2-PSK>**.

<AES-OCB encryption>

(1) Set the security features.

Choose AES-OCB from the Encryption pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

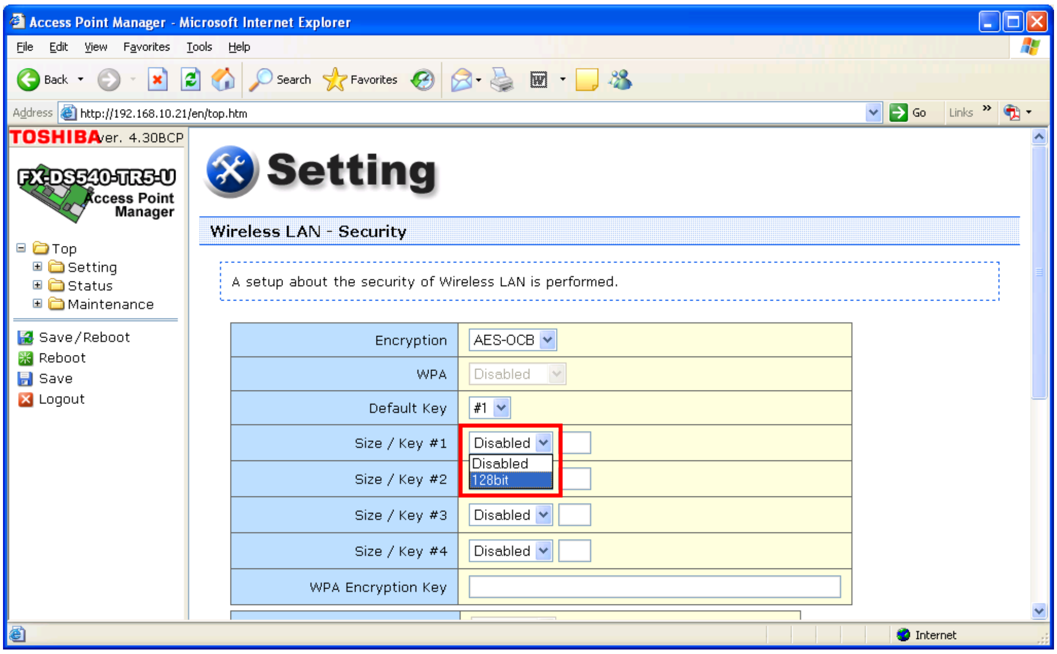
Setting

Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	AES
WPA	Disabled Disabled WPA WPA-PSK WPA2 WPA2-PSK
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	

Set the default key and size/key number. In the following sample screen, 1 is set for the key number and 128 bit for the size.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Setting

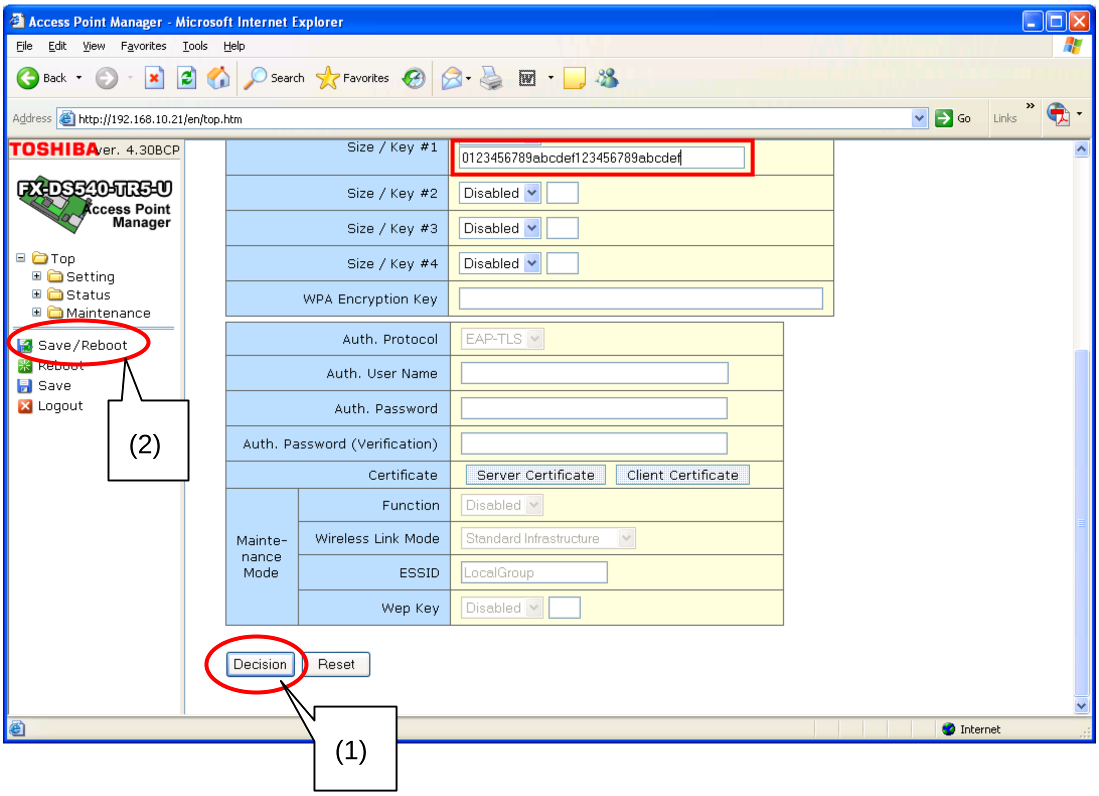
Wireless LAN - Security

A setup about the security of Wireless LAN is performed.

Encryption	AES-OCB
WPA	Disabled
Default Key	#1
Size / Key #1	Disabled Disabled 128bit
Size / Key #2	
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	

Enter a key with hexadecimal code.

Click on the Decision button (1), then click on Save/Reboot to restart the wireless LAN module (2).

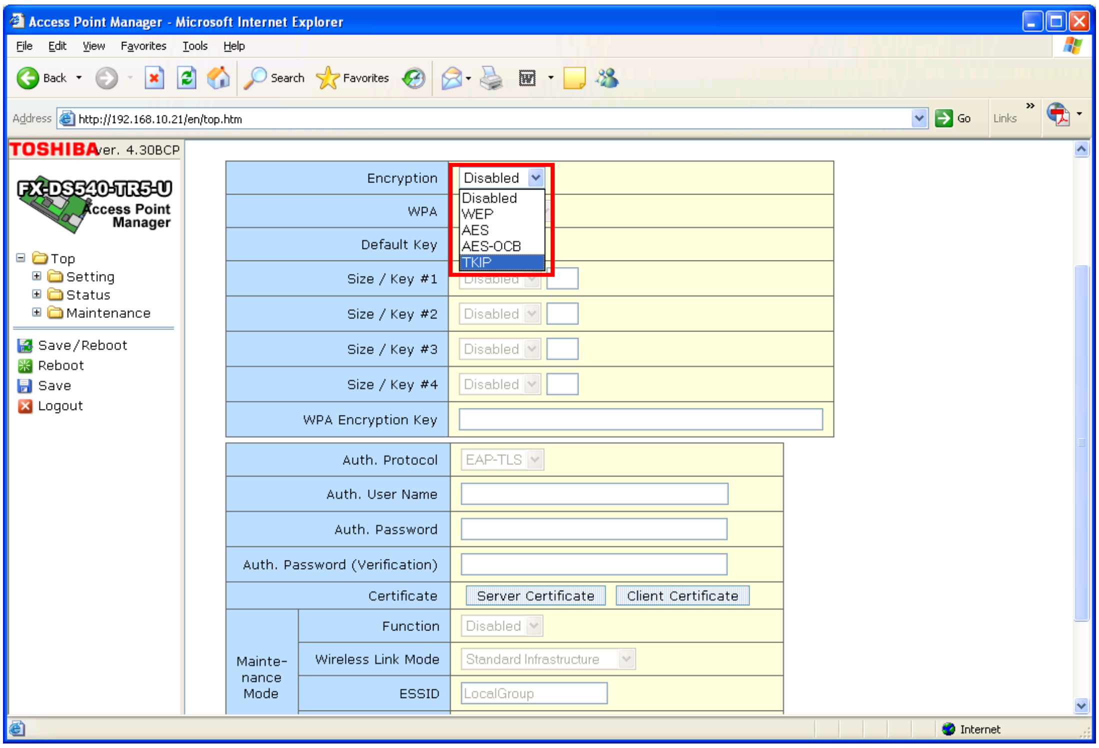


Size / Key #1		0123456789abcdef123456789abcdef
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		EAP-TLS
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

<TKIP encryption with WPA>

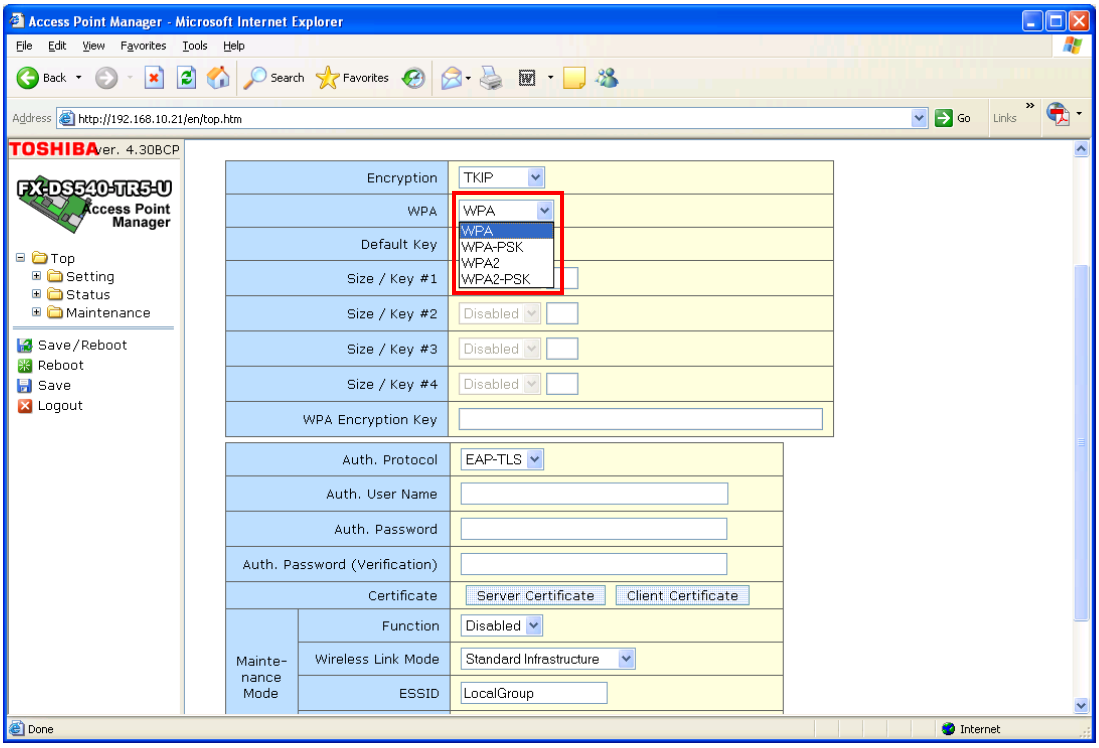
(1) Set the security features and authentication method.

Choose TKIP from the Encryption pull down menu.



Encryption	Disabled
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	
Auth. Password (Verification)	
Certificate	Server Certificate Client Certificate
Mainte-nance Mode Function	Disabled
Mainte-nance Mode Wireless Link Mode	Standard Infrastructure
Mainte-nance Mode ESSID	LocalGroup

Choose WPA from the WPA pull down menu.



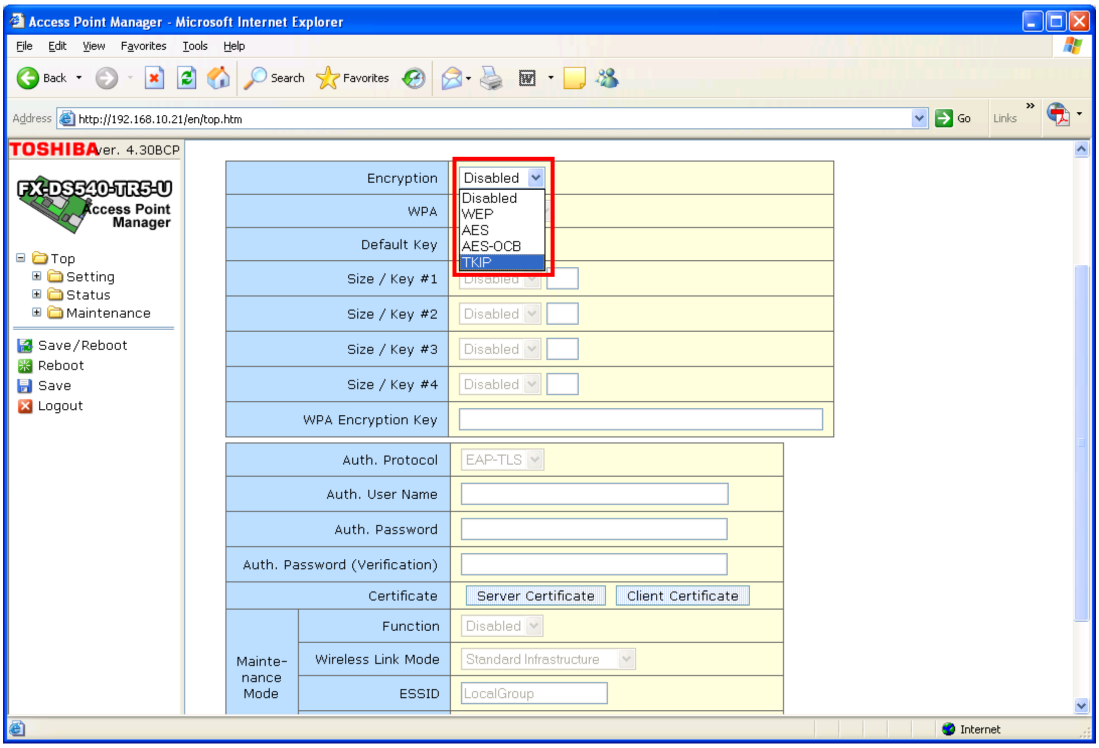
Encryption	TKIP
WPA	WPA
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	
Auth. Password (Verification)	
Certificate	Server Certificate Client Certificate
Mainte-nance Mode Function	Disabled
Mainte-nance Mode Wireless Link Mode	Standard Infrastructure
Mainte-nance Mode ESSID	LocalGroup

Continued on **<When using WPA>**.

<TKIP encryption with WPA-PSK>

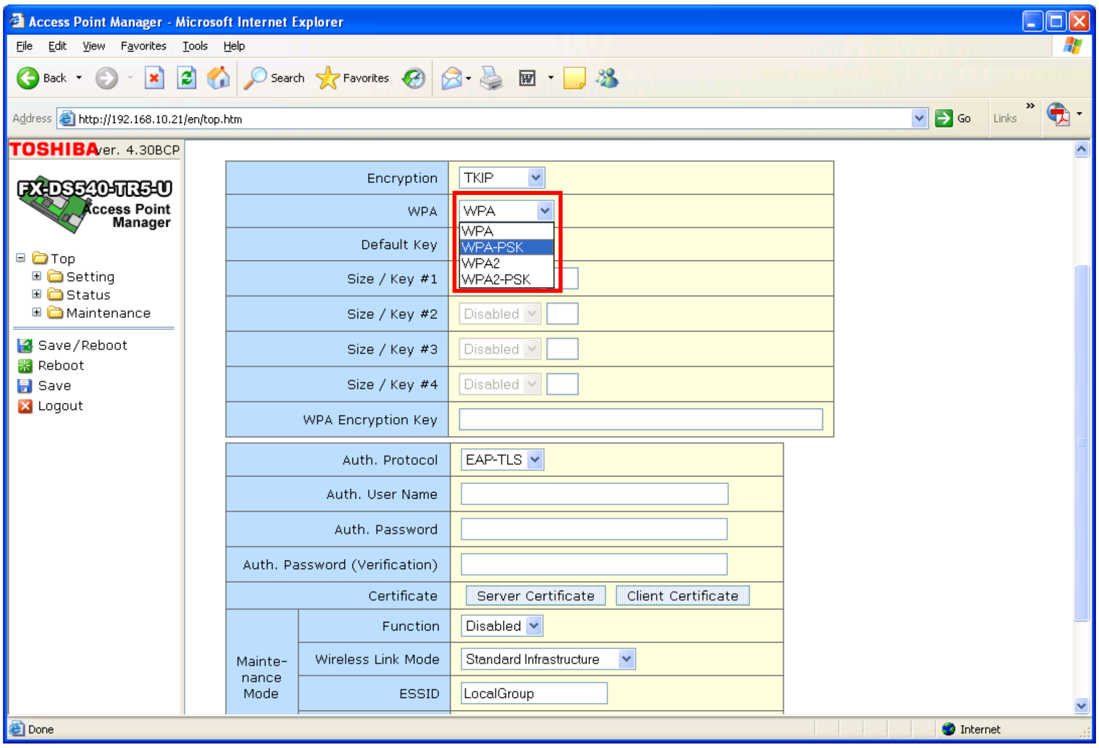
(1) Set the security features and authentication method.

Choose TKIP from the Encryption pull down menu.



Encryption	Disabled
WPA	
Default Key	
Size / Key #1	Disabled
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	
Auth. Password (Verification)	
Certificate	Server Certificate Client Certificate
Mainte-nance Mode: Function	Disabled
Mainte-nance Mode: Wireless Link Mode	Standard Infrastructure
Mainte-nance Mode: ESSID	LocalGroup

Choose WPA-PSK from the WPA pull down menu.



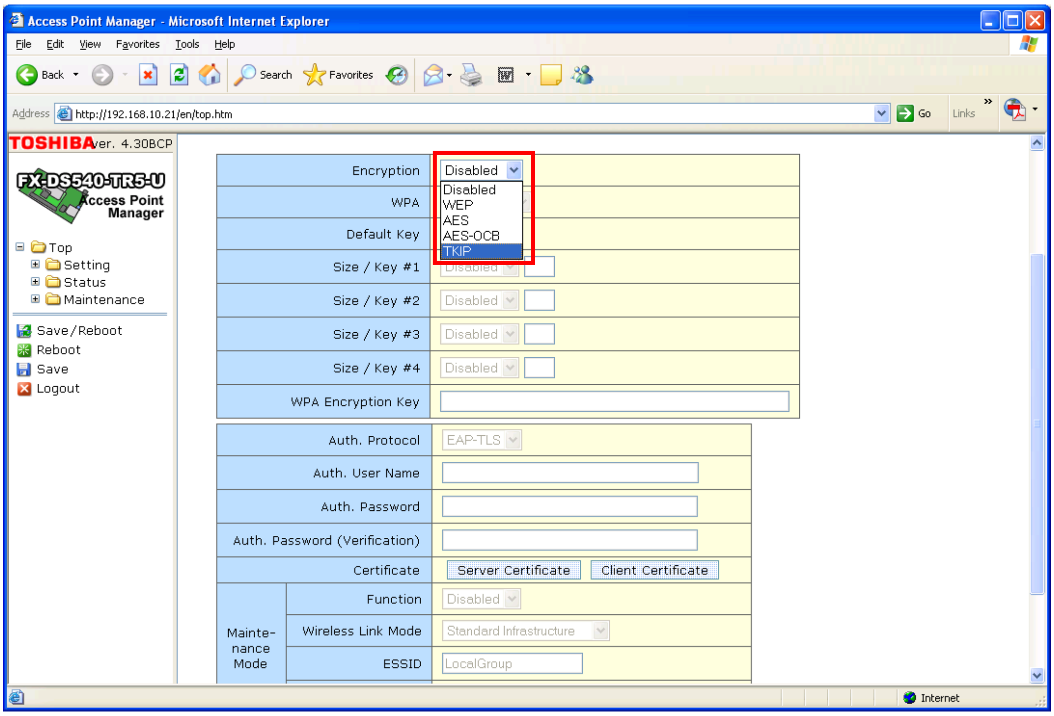
Encryption	TKIP
WPA	WPA
Default Key	
Size / Key #1	
Size / Key #2	Disabled
Size / Key #3	Disabled
Size / Key #4	Disabled
WPA Encryption Key	
Auth. Protocol	EAP-TLS
Auth. User Name	
Auth. Password	
Auth. Password (Verification)	
Certificate	Server Certificate Client Certificate
Mainte-nance Mode: Function	Disabled
Mainte-nance Mode: Wireless Link Mode	Standard Infrastructure
Mainte-nance Mode: ESSID	LocalGroup

Continued on **<When using WPA-PSK>**.

<TKIP encryption with WPA2>

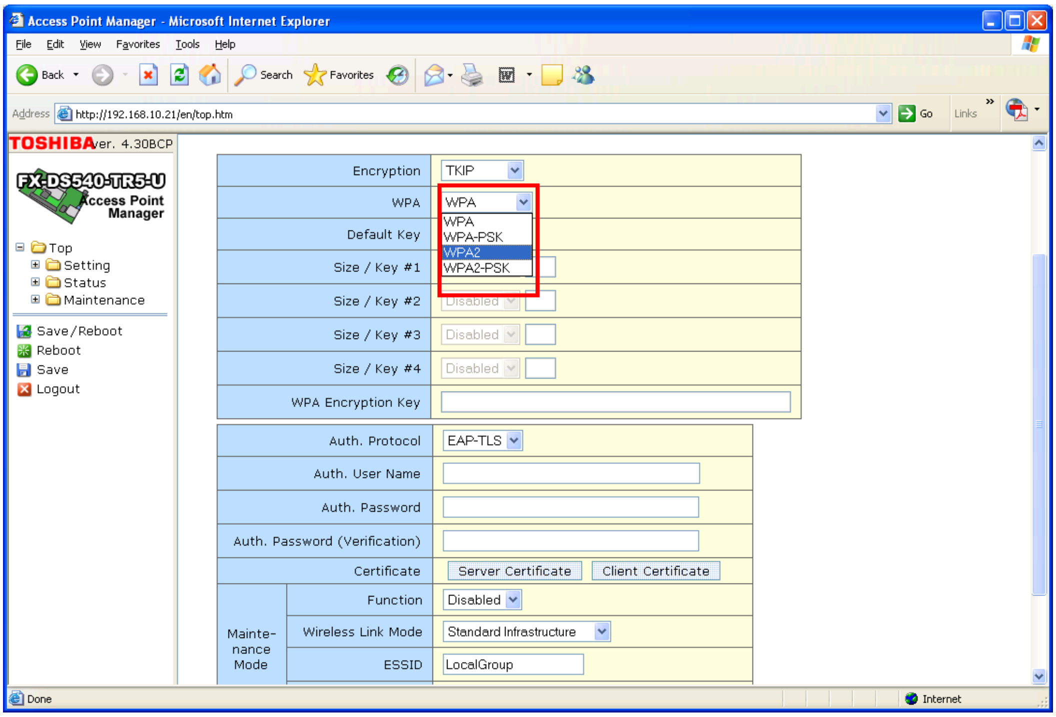
(1) Set the security features and authentication method.

Choose TKIP from the Encryption pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

Encryption		Disabled Disabled WEP AES AES-OCB TKIP
WPA		
Default Key		
Size / Key #1		Disabled
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		EAP-TLS
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup

Choose WPA2 from the WPA pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Done
Internet

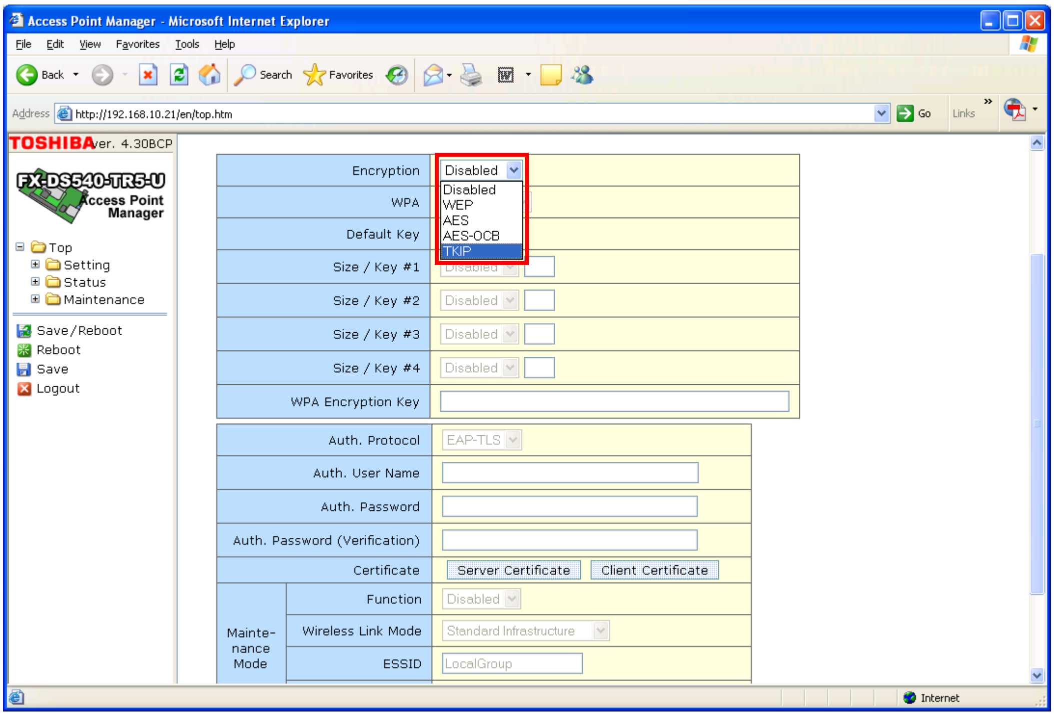
Encryption		TKIP
WPA		WPA WPA WPA-PSK WPA2 WPA2-PSK
Default Key		
Size / Key #1		
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		EAP-TLS
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup

Continued on **<When using WPA2>**.

<TKIP encryption with WPA2-PSK>

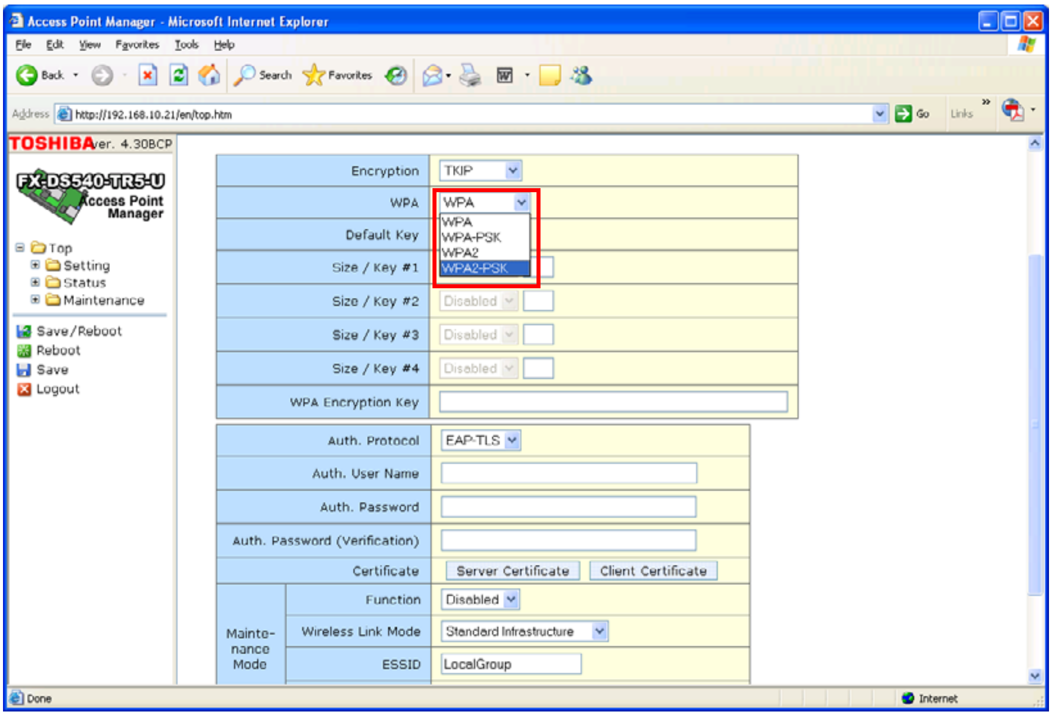
(1) Set the security features and authentication method.

Choose TKIP from the Encryption pull down menu.



Encryption		Disabled
WPA		
Default Key		
Size / Key #1		Disabled
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		EAP-TLS
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup

Choose WPA2-PSK from the WPA pull down menu.



Encryption		TKIP
WPA		WPA
Default Key		
Size / Key #1		
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		EAP-TLS
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup

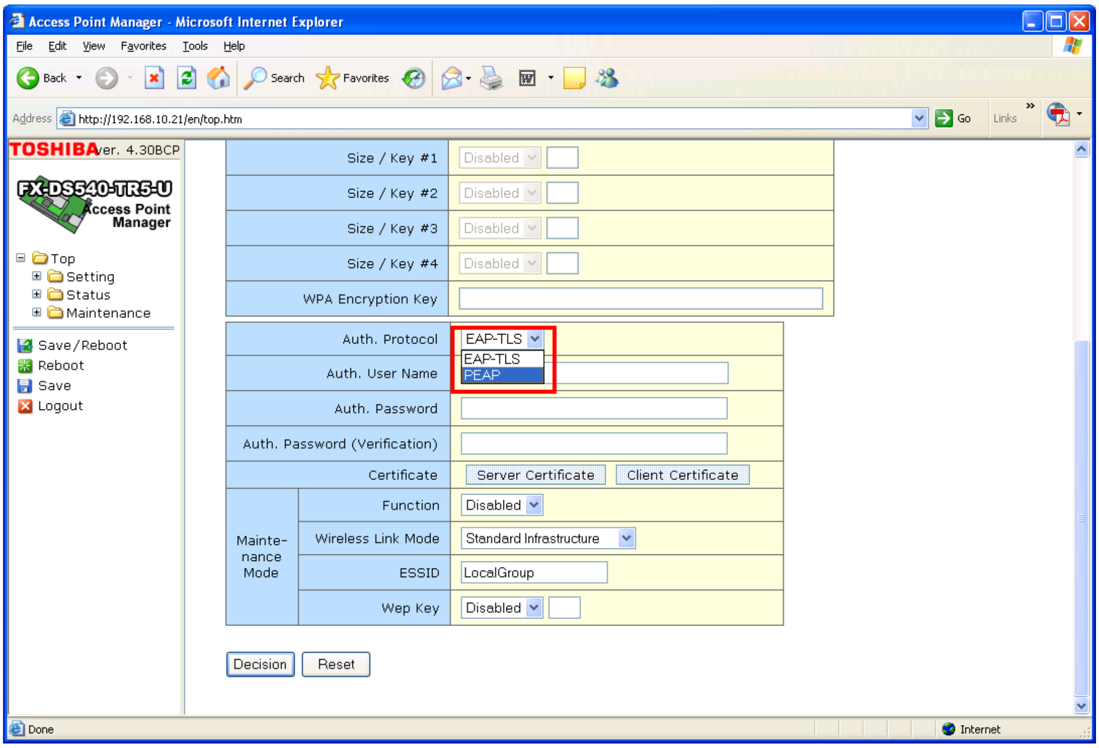
Continued on **<When using WPA2-PSK>**.

<When using WPA> <When using WPA2>

(2) Set the authentication method.

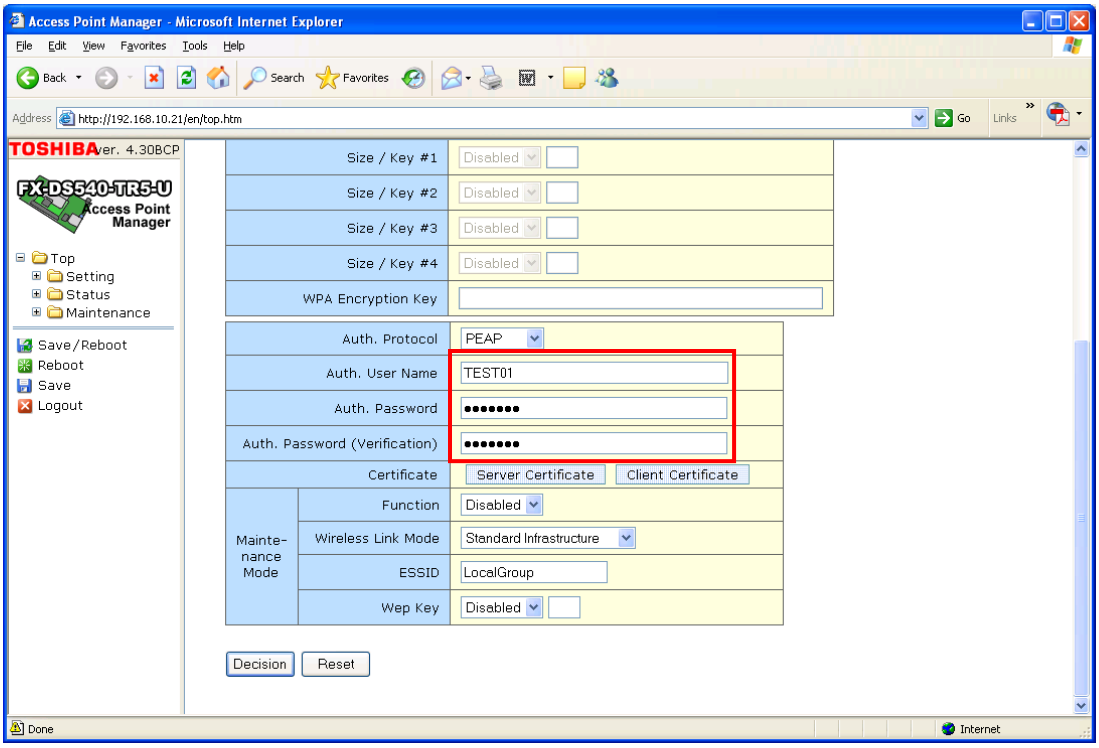
[In the case of Protected EAP (PEAP)]

Choose PEAP from the Auth. Protocol pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Decision
Reset
Done
Internet

Size / Key #1		Disabled
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		EAP-TLS EAP-TLS PEAP
Auth. User Name		
Auth. Password		
Auth. Password (Verification)		
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

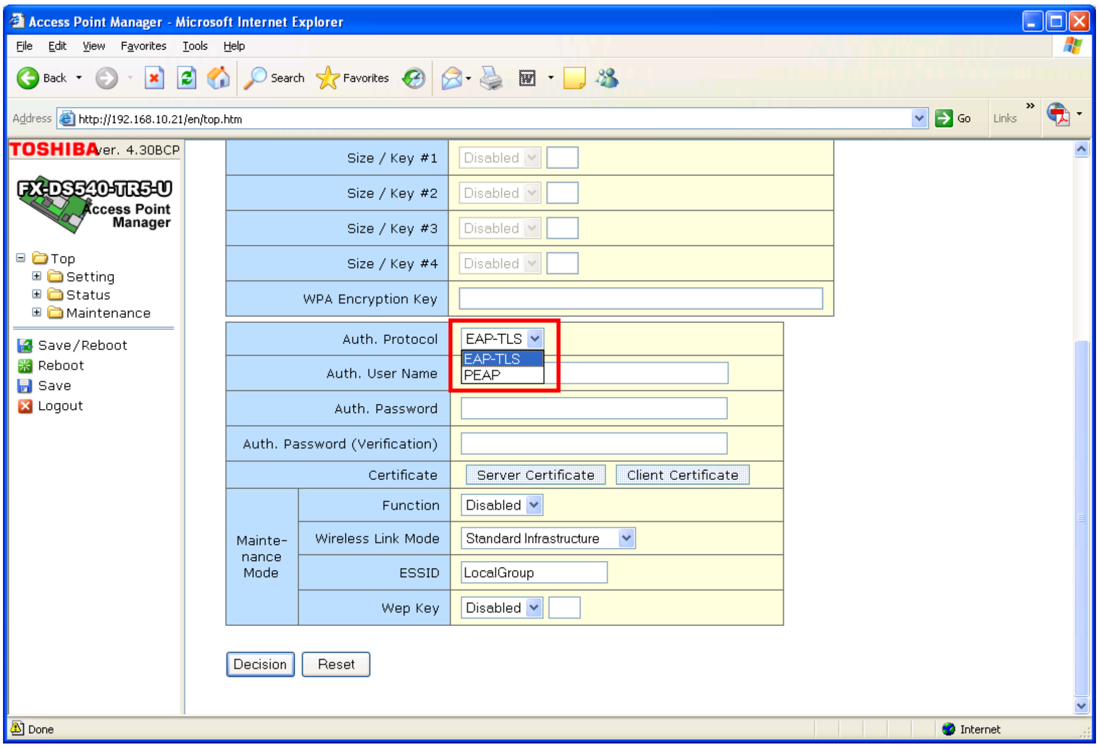
Enter the authentication user name and password.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Decision
Reset
Done
Internet

Size / Key #1		Disabled
Size / Key #2		Disabled
Size / Key #3		Disabled
Size / Key #4		Disabled
WPA Encryption Key		
Auth. Protocol		PEAP
Auth. User Name		TEST01
Auth. Password		●●●●●●●
Auth. Password (Verification)		●●●●●●●
Certificate		Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

[In the case of EAP-TLS]

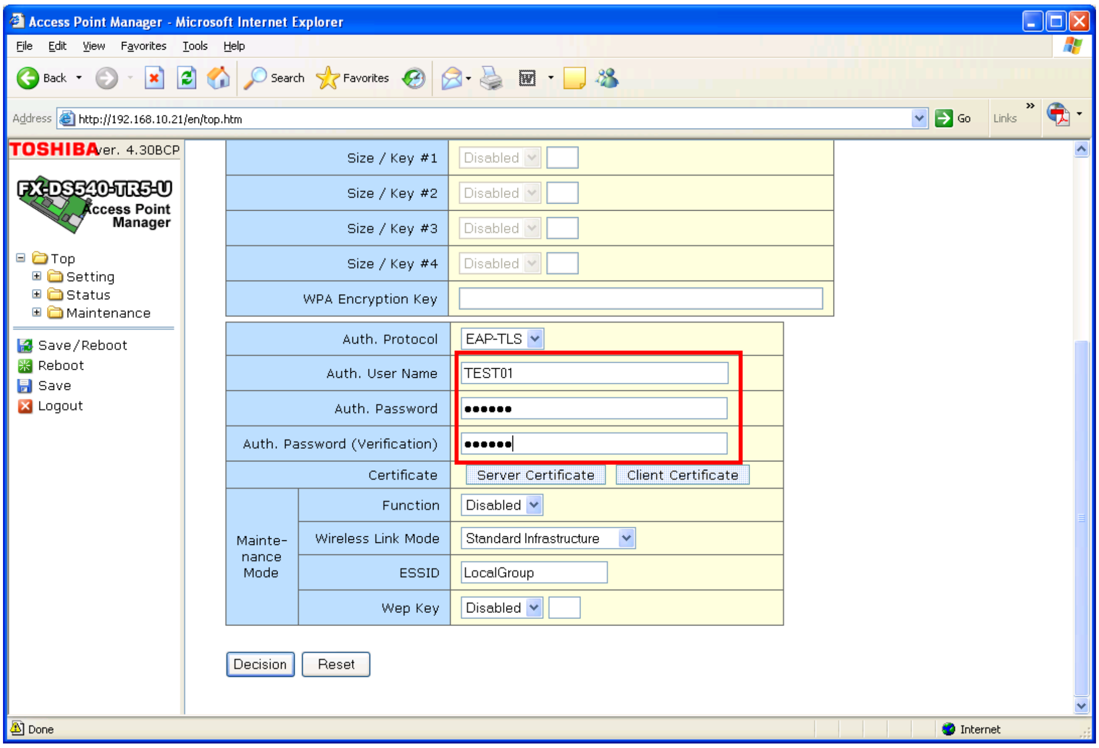
Choose EAP-TLS from the Auth. Protocol pull down menu.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TRS-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Done
Internet

	Size / Key #1	Disabled
	Size / Key #2	Disabled
	Size / Key #3	Disabled
	Size / Key #4	Disabled
	WPA Encryption Key	
	Auth. Protocol	EAP-TLS EAP-TLS PEAP
	Auth. User Name	
	Auth. Password	
	Auth. Password (Verification)	
	Certificate	Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

Decision Reset

Enter the authentication user name and the password.

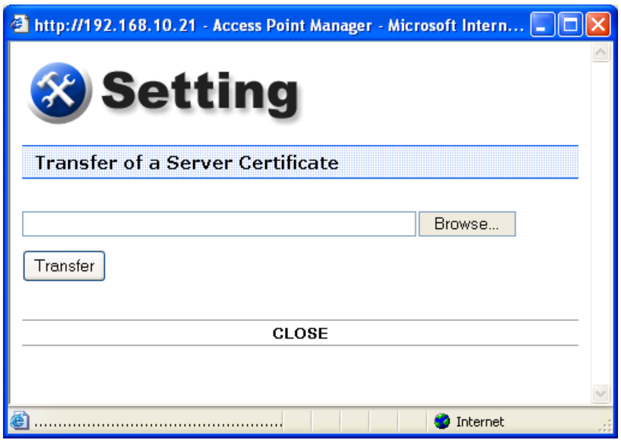

Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TRS-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Done
Internet

	Size / Key #1	Disabled
	Size / Key #2	Disabled
	Size / Key #3	Disabled
	Size / Key #4	Disabled
	WPA Encryption Key	
	Auth. Protocol	EAP-TLS
	Auth. User Name	TEST01
	Auth. Password	••••••
	Auth. Password (Verification)	••••••
	Certificate	Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

Decision Reset

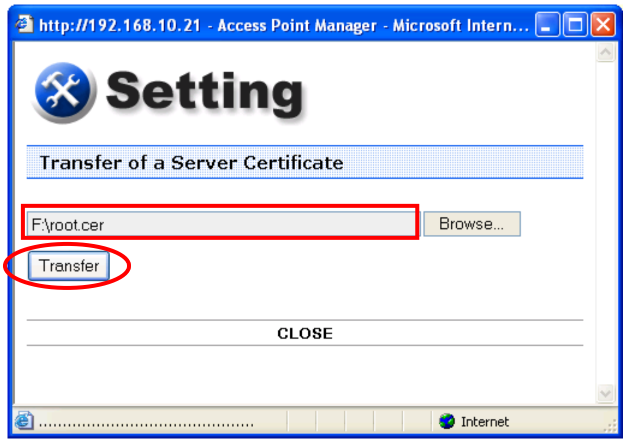
(3) Send the certificate.

Click on the Server Certificate button. The following screen will appear.



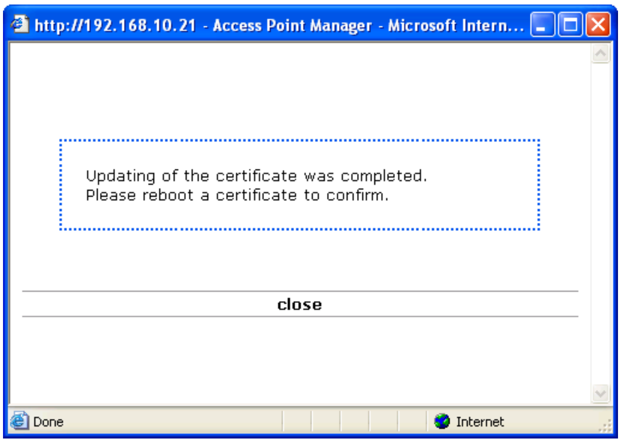
http://192.168.10.21 - Access Point Manager - Microsoft Intern...
Setting
Transfer of a Server Certificate
Browse...
Transfer
CLOSE
Internet

Specify the root certificate and click on the Transfer button.



http://192.168.10.21 - Access Point Manager - Microsoft Intern...
Setting
Transfer of a Server Certificate
F:\root.cer
Browse...
Transfer
CLOSE
Internet

When the transfer is successfully completed, the following screen appears.

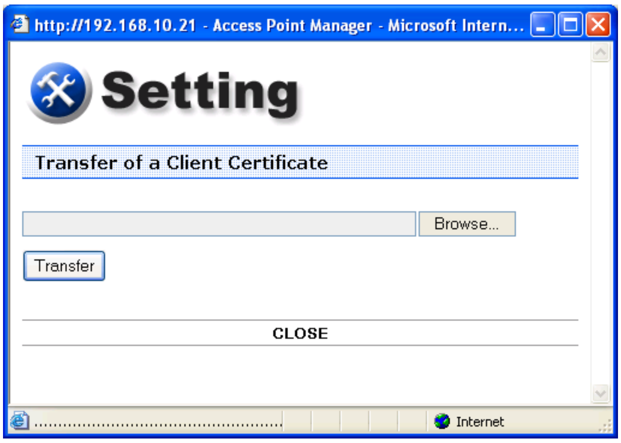


Updating of the certificate was completed.
Please reboot a certificate to confirm.

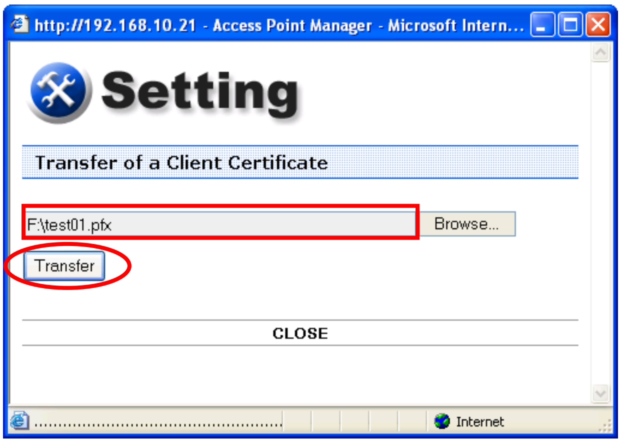
http://192.168.10.21 - Access Point Manager - Microsoft Intern...
close
Done
Internet

[In the case of EAP-TLS]

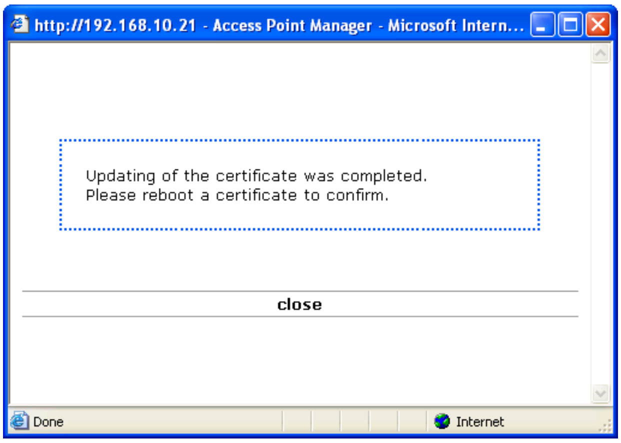
Click on the Client Certificate button. The following screen will appear.


http://192.168.10.21 - Access Point Manager - Microsoft Intern...
Setting
Transfer of a Client Certificate
Browse...
Transfer
CLOSE
Internet

Specify the user certificate and click on the Transfer button.


http://192.168.10.21 - Access Point Manager - Microsoft Intern...
Setting
Transfer of a Client Certificate
F:\test01.pfx
Browse...
Transfer
CLOSE
Internet

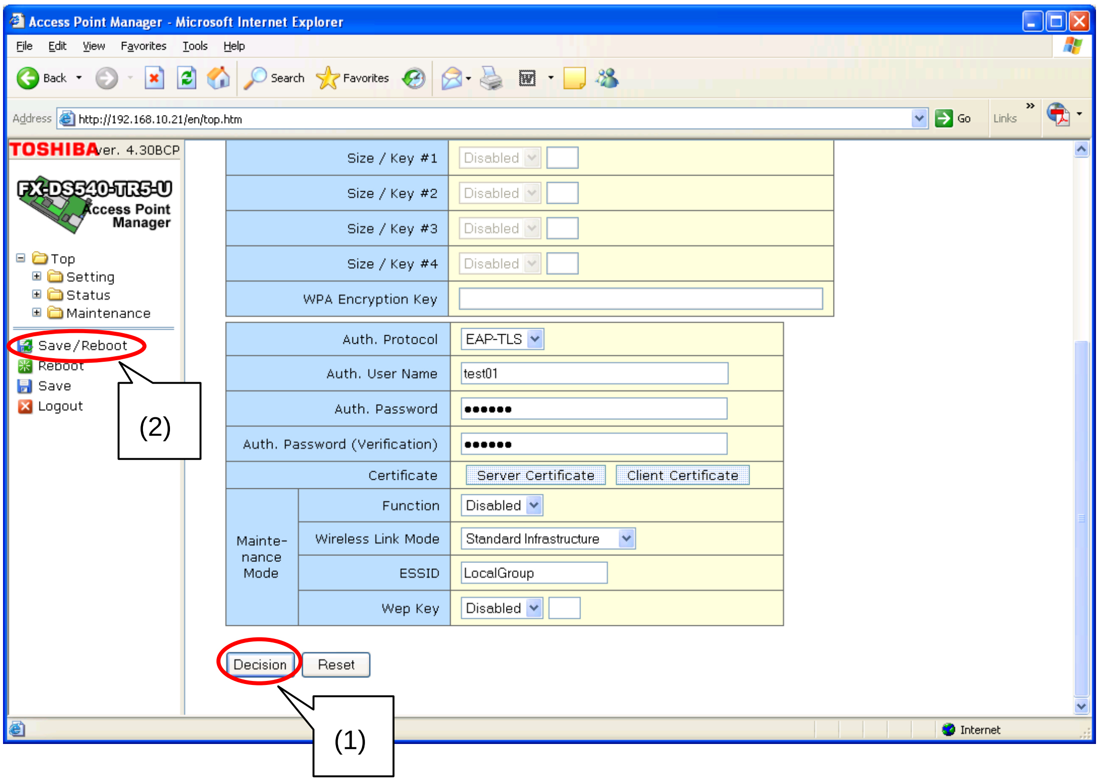
When the transfer is successfully completed, the following screen appears.


http://192.168.10.21 - Access Point Manager - Microsoft Intern...

Updating of the certificate was completed.
Please reboot a certificate to confirm.

(4) Save and reboot

Temporarily save the settings by clicking on the Decision button, then click on Save/Reboot to save the settings and restart the wireless LAN module.

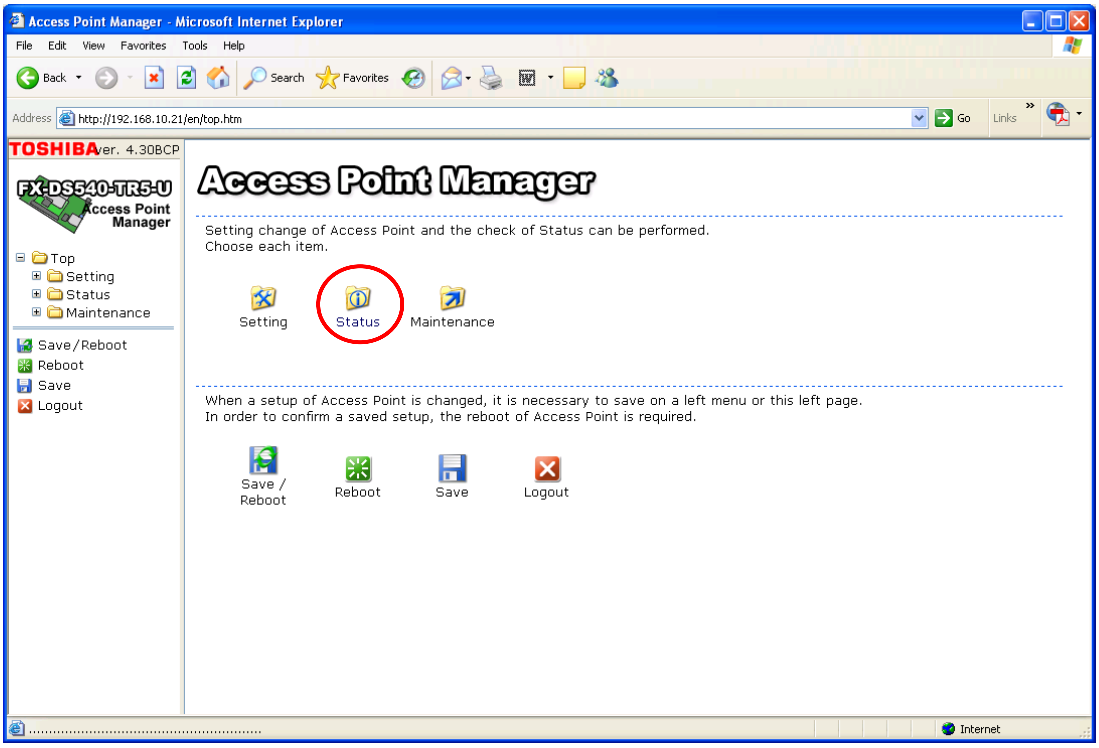


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
(2)
Decision
Reset
(1)
Internet

	Size / Key #1	Disabled
	Size / Key #2	Disabled
	Size / Key #3	Disabled
	Size / Key #4	Disabled
	WPA Encryption Key	
	Auth. Protocol	EAP-TLS
	Auth. User Name	test01
	Auth. Password	••••••
	Auth. Password (Verification)	••••••
	Certificate	Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

(5) Confirmation of settings

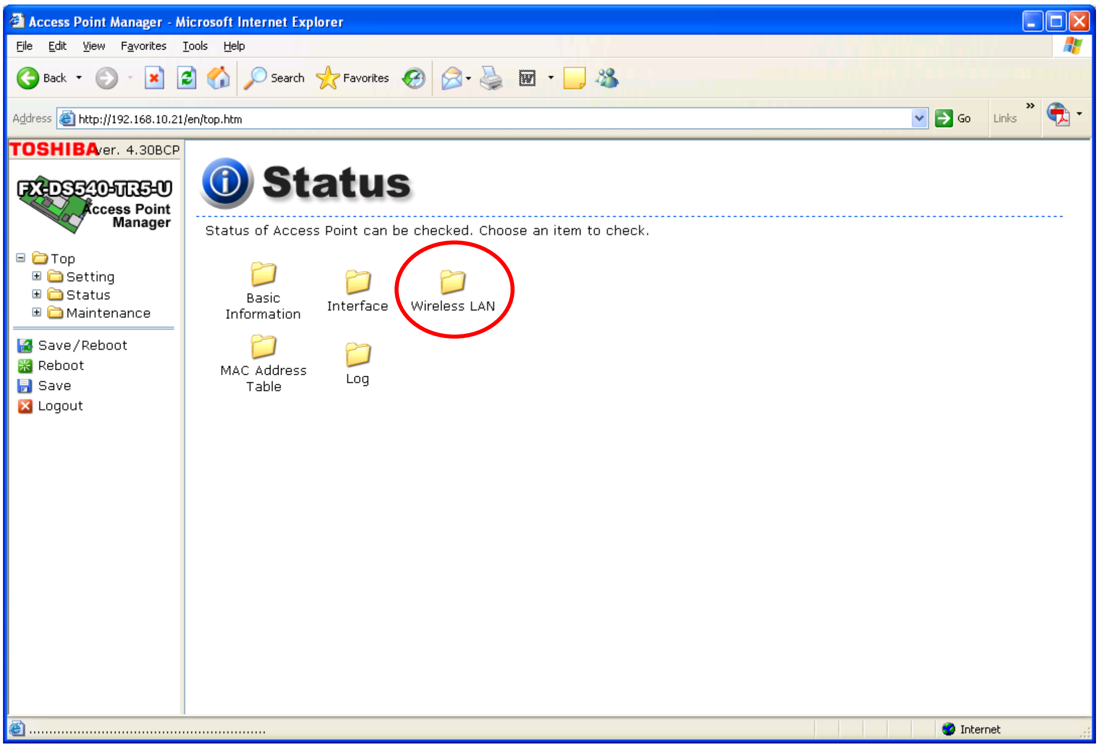
After following steps (1) to (3) and logging in the access point manager, click on the Status icon.



Setting change of Access Point and the check of Status can be performed.
Choose each item.

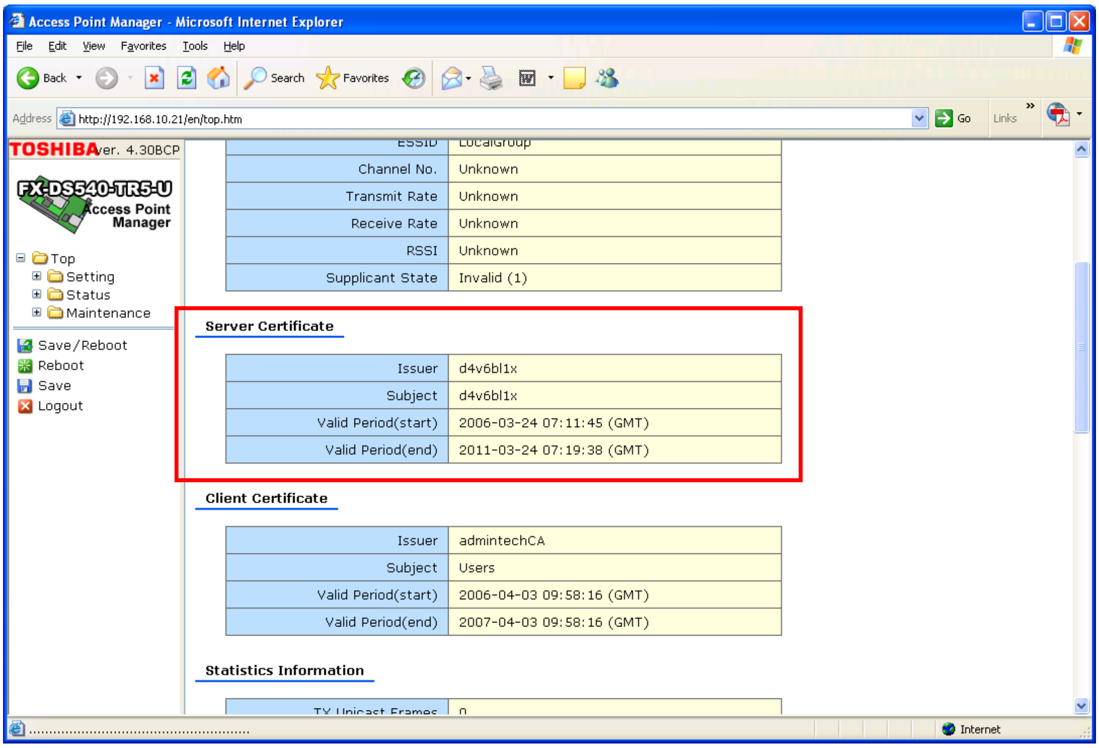
When a setup of Access Point is changed, it is necessary to save on a left menu or this left page.
In order to confirm a saved setup, the reboot of Access Point is required.

Then, click on the Wireless LAN folder.


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Status
Basic Information
Interface
Wireless LAN
MAC Address Table
Log
Internet

Status of Access Point can be checked. Choose an item to check.

Confirm that the information of the server certificate is displayed.



Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

ESSID	LocalGroup
Channel No.	Unknown
Transmit Rate	Unknown
Receive Rate	Unknown
RSSI	Unknown
Supplicant State	Invalid (1)

Server Certificate

Issuer	d4v6bl1x
Subject	d4v6bl1x
Valid Period(start)	2006-03-24 07:11:45 (GMT)
Valid Period(end)	2011-03-24 07:19:38 (GMT)

Client Certificate

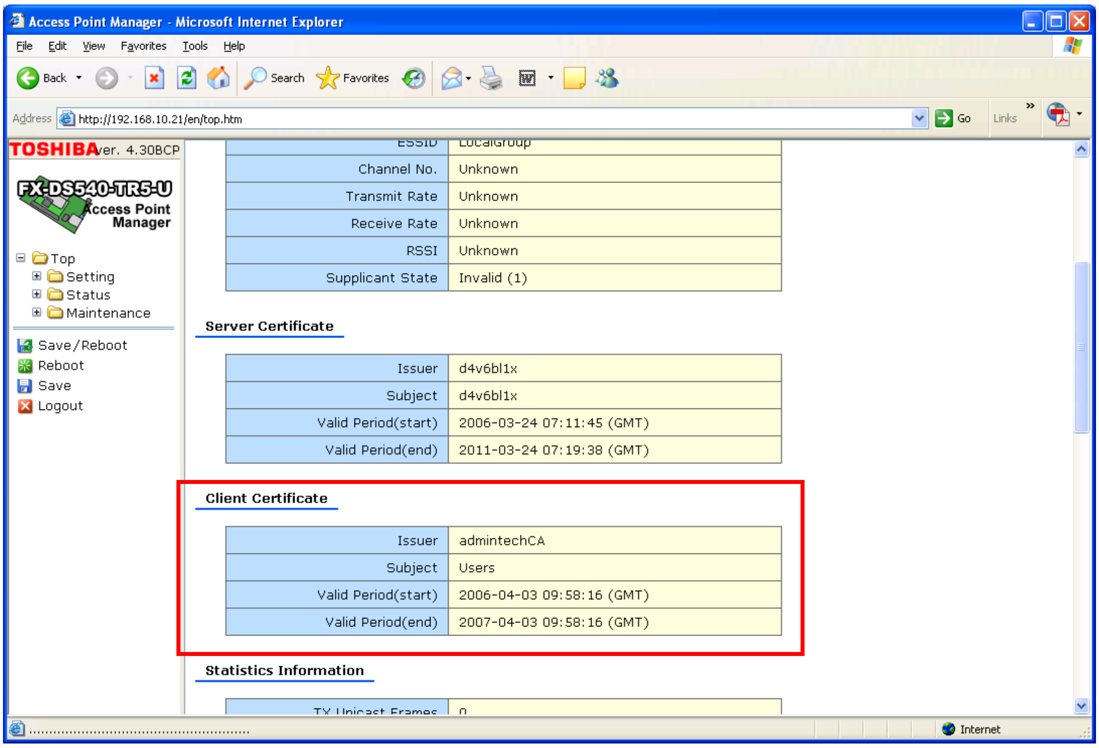
Issuer	admintechCA
Subject	Users
Valid Period(start)	2006-04-03 09:58:16 (GMT)
Valid Period(end)	2007-04-03 09:58:16 (GMT)

Statistics Information

TX Unicast Frames	0

[In the case of EAP-TLS]

Confirm that the information of the client certificate is displayed.



Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
Internet

ESSID	LocalGroup
Channel No.	Unknown
Transmit Rate	Unknown
Receive Rate	Unknown
RSSI	Unknown
Supplicant State	Invalid (1)

Server Certificate

Issuer	d4v6bl1x
Subject	d4v6bl1x
Valid Period(start)	2006-03-24 07:11:45 (GMT)
Valid Period(end)	2011-03-24 07:19:38 (GMT)

Client Certificate

Issuer	admintechCA
Subject	Users
Valid Period(start)	2006-04-03 09:58:16 (GMT)
Valid Period(end)	2007-04-03 09:58:16 (GMT)

Statistics Information

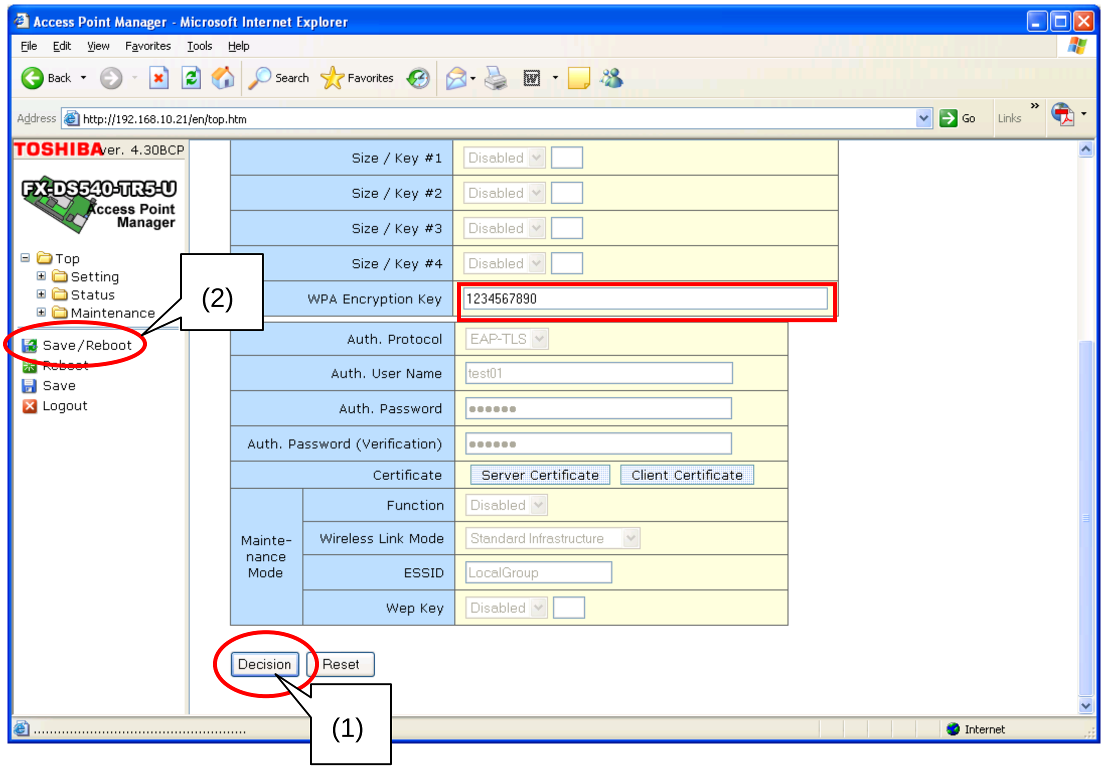
TX Unicast Frames	0

<When using WPA-PSK> <When using WPA2-PSK>

(1) Setting the encryption key

Set a WPA encryption key with 1-byte 8 to 63 characters.

Then, click on the Decision button (1), and click on Save/Reboot to restart the wireless LAN module (2).


Access Point Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.10.21/en/top.htm
Go Links
TOSHIBA ver. 4.30BCP
FX-DS540-TR5-U Access Point Manager
Top
Setting
Status
Maintenance
Save/Reboot
Reboot
Save
Logout
(2)
Decision
Reset
(1)
Internet

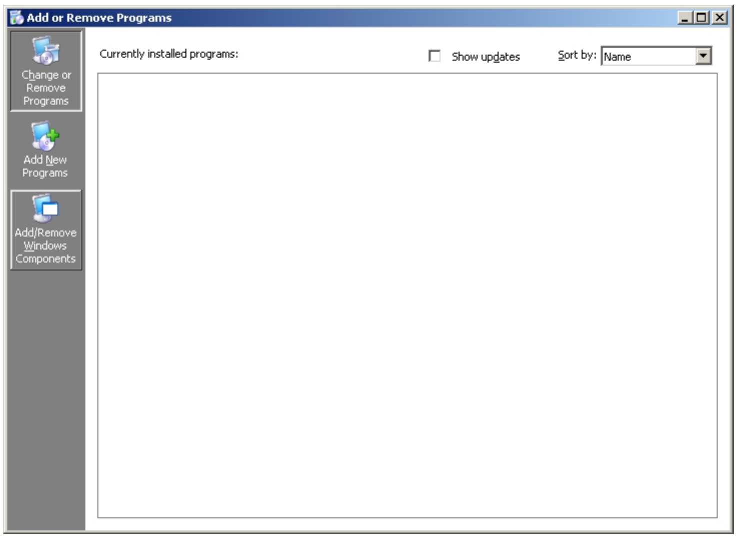
	Size / Key #1	Disabled
	Size / Key #2	Disabled
	Size / Key #3	Disabled
	Size / Key #4	Disabled
	WPA Encryption Key	1234567890
	Auth. Protocol	EAP-TLS
	Auth. User Name	test01
	Auth. Password	●●●●●●
	Auth. Password (Verification)	●●●●●●
	Certificate	Server Certificate Client Certificate
Mainte-nance Mode	Function	Disabled
	Wireless Link Mode	Standard Infrastructure
	ESSID	LocalGroup
	Wep Key	Disabled

8.3 SETTINGS FOR THE SERVER

Settings for the server in the case Protected EAP (PEAP) or EAP-TLS is used:
The OS of the server is supposed to be Windows Server 2003 Enterprise.

- Installation of various components

Open the Add or Remove Programs screen and click on the Add/Remove Windows Components button.

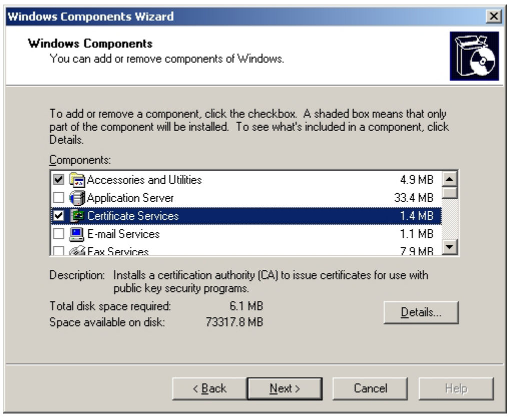


Add or Remove Programs

Currently installed programs: □ Show updates Sort by: Name

When the Windows Components Wizard screen appears, check the check box for the Certificate Services.

Note: A confirmation dialog box confirming an installation may appear, but continue.



Windows Components Wizard

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

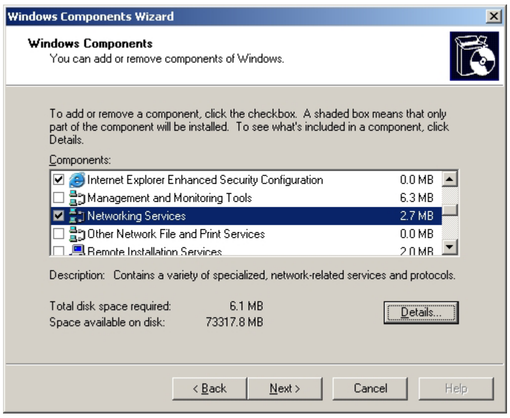
Components:

☑	Accessories and Utilities	4.9 MB
□	Application Server	33.4 MB
☑	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
□	Fax Services	7.9 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 6.1 MB
Space available on disk: 73317.8 MB

Choose Networking Services, and click on the Details button.



Windows Components Wizard

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

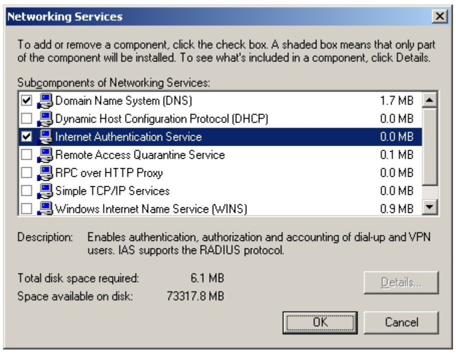
Components:

☑	Internet Explorer Enhanced Security Configuration	0.0 MB
□	Management and Monitoring Tools	6.3 MB
☑	Networking Services	2.7 MB
□	Other Network File and Print Services	0.0 MB
□	Remote Installation Services	2.0 MB

Description: Contains a variety of specialized, network-related services and protocols.

Total disk space required: 6.1 MB
Space available on disk: 73317.8 MB

Check the check box for the Internet Authentication Service, and click on the OK button.



Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Networking Services:

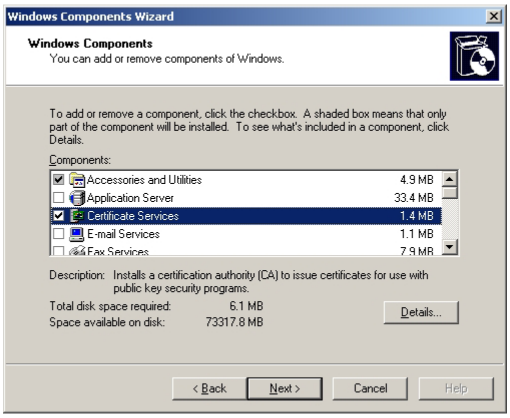
☑	Domain Name System (DNS)	1.7 MB
□	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☑	Internet Authentication Service	0.0 MB
□	Remote Access Quarantine Service	0.1 MB
□	RPC over HTTP Proxy	0.0 MB
□	Simple TCP/IP Services	0.0 MB
□	Windows Internet Name Service (WINS)	0.9 MB

Description: Enables authentication, authorization and accounting of dial-up and VPN users. IAS supports the RADIUS protocol.

Total disk space required: 6.1 MB

Space available on disk: 73317.8 MB

Click on the Next button to continue.



Windows Components Wizard

Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑	Accessories and Utilities	4.9 MB
□	Application Server	33.4 MB
☑	Certificate Services	1.4 MB
□	E-mail Services	1.1 MB
□	Fax Services	7.9 MB

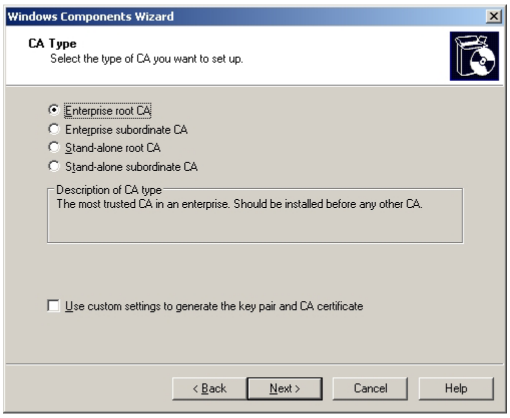
Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 6.1 MB

Space available on disk: 73317.8 MB

Choose the Enterprise root CA when asked the CA type, and click on the Next button.

Note: The Active Directory needs to be installed in advance.



Windows Components Wizard

CA Type

Select the type of CA you want to set up.

● Enterprise root CA

○ Enterprise subordinate CA

○ Stand-alone root CA

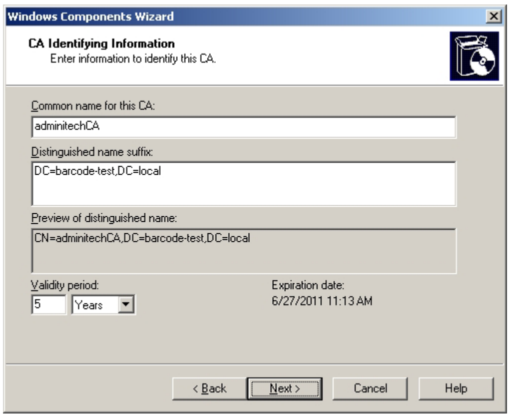
○ Stand-alone subordinate CA

Description of CA type

The most trusted CA in an enterprise. Should be installed before any other CA.

□ Use custom settings to generate the key pair and CA certificate

Enter a common name for the CA, and click on the Next button.



CA Identifying Information

Enter information to identify this CA.

Common name for this CA: adminitechCA

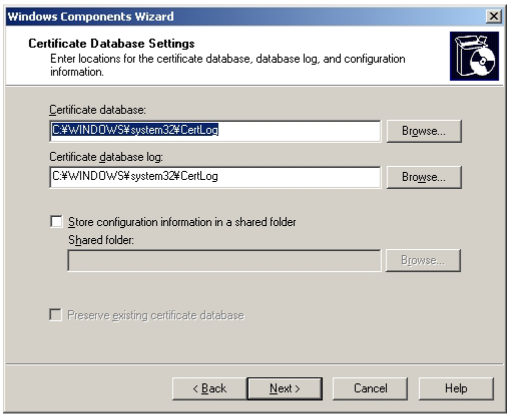
Distinguished name suffix: DC=barcode-test,DC=local

Preview of distinguished name: CN=adminitechCA,DC=barcode-test,DC=local

Validity period: 5 Years

Expiration date: 6/27/2011 11:13 AM

Click on the Next button without changing any database settings.



Certificate Database Settings

Enter locations for the certificate database, database log, and configuration information.

Certificate database: C:¥WINDOWS¥system32¥CertLog

Certificate database log: C:¥WINDOWS¥system32¥CertLog

☐ Store configuration information in a shared folder

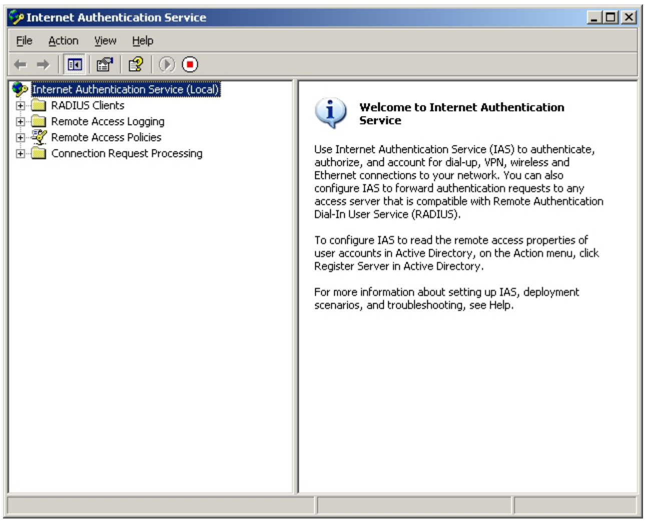
Shared folder:

☐ Preserve existing certificate database

Now, the installation of the component is completed.
At this point, issuing a server certificate is possible.
Issue a certificate for the wireless LAN module and the server, respectively.

- Setting the RADIUS server and access policy

Click on the Start menu, All programs, and Management tool, then start the Internet Authentication Service.


Internet Authentication Service
File Action View Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

Welcome to Internet Authentication Service

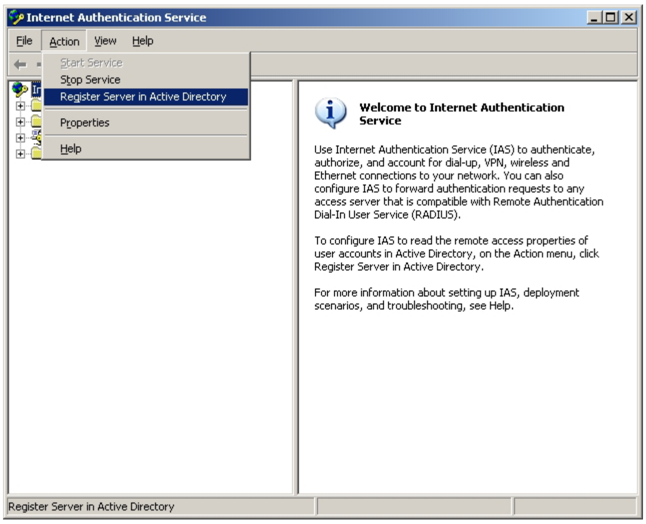
Use Internet Authentication Service (IAS) to authenticate, authorize, and account for dial-up, VPN, wireless and Ethernet connections to your network. You can also configure IAS to forward authentication requests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).

To configure IAS to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.

For more information about setting up IAS, deployment scenarios, and troubleshooting, see Help.

Choose the Register Server in Active Directory from the Action menu.

Note: The Active Directory needs to be installed in advance.


Internet Authentication Service
File Action View Help
Start Service
Stop Service
Register Server in Active Directory
Properties
Help
Register Server in Active Directory

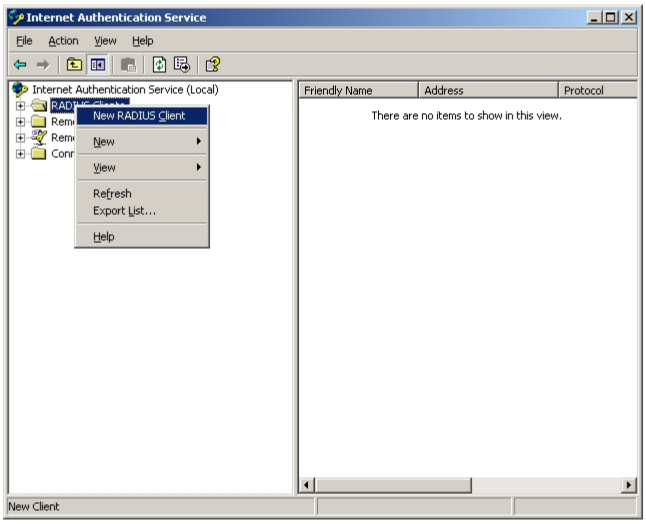
Welcome to Internet Authentication Service

Use Internet Authentication Service (IAS) to authenticate, authorize, and account for dial-up, VPN, wireless and Ethernet connections to your network. You can also configure IAS to forward authentication requests to any access server that is compatible with Remote Authentication Dial-In User Service (RADIUS).

To configure IAS to read the remote access properties of user accounts in Active Directory, on the Action menu, click Register Server in Active Directory.

For more information about setting up IAS, deployment scenarios, and troubleshooting, see Help.

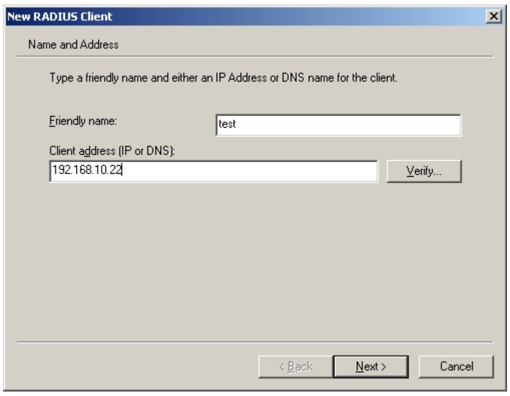
Right-click on the RADIUS Client and choose the New RADIUS Client.



There are no items to show in this view.

New Client

Enter a Friendly name and Client address, then click on the Next button.

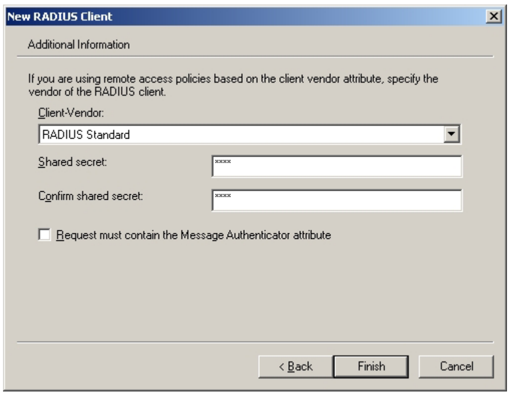


Type a friendly name and either an IP Address or DNS name for the client.

Friendly name: test

Client address (IP or DNS): 192.168.10.22

Choose the RADIUS Standard for the Client Vendor, enter a Shared secret, then click on the Finish button.



If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.

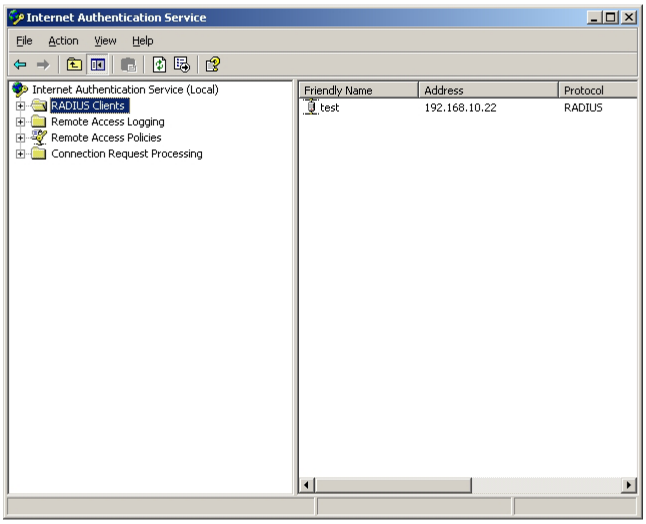
Client-Vendor: RADIUS Standard

Shared secret: ****

Confirm shared secret: ****

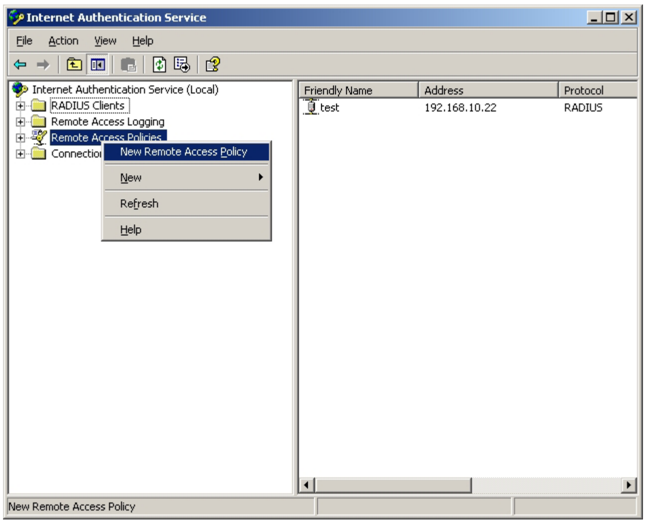
□ Request must contain the Message Authenticator attribute

The following screen is displayed.


Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing

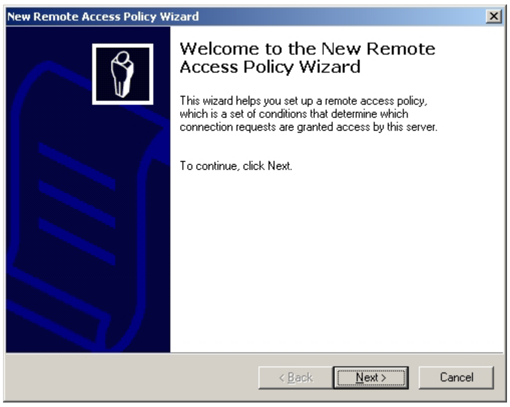
Friendly Name	Address	Protocol
test	192.168.10.22	RADIUS

Right-click on the Remote Access Policy and choose the New Remote Access Policy.



Friendly Name	Address	Protocol
test	192.168.10.22	RADIUS

Click on the Next button.

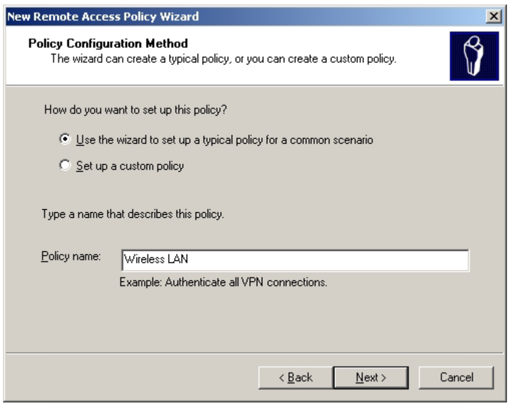


Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.

Enter a Policy name and click on the Next button.



New Remote Access Policy Wizard

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

● Use the wizard to set up a typical policy for a common scenario

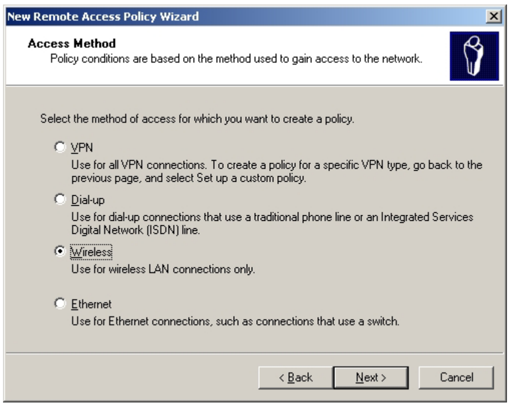
○ Set up a custom policy

Type a name that describes this policy.

Policy name: Wireless LAN

Example: Authenticate all VPN connections.

Choose Wireless for the access method and click on the Next button.



New Remote Access Policy Wizard

Access Method

Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

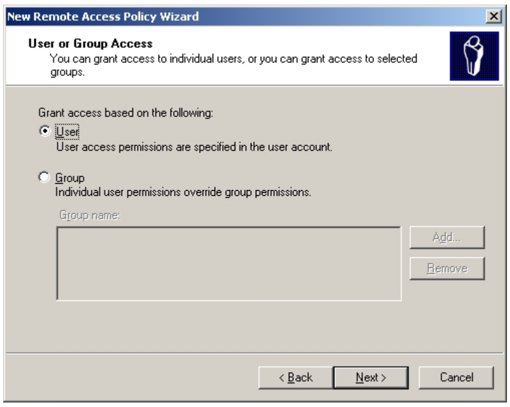
○ VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

○ Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

● Wireless
Use for wireless LAN connections only.

○ Ethernet
Use for Ethernet connections, such as connections that use a switch.

Choose User, and click on the Next button.



New Remote Access Policy Wizard

User or Group Access

You can grant access to individual users, or you can grant access to selected groups.

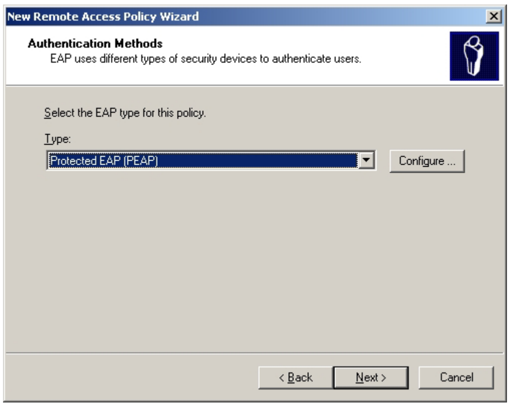
Grant access based on the following:

● User
User access permissions are specified in the user account.

○ Group
Individual user permissions override group permissions.

Group name:

Choose the Protected EAP (PEAP) for the EAP type, and click on the Configure button.



New Remote Access Policy Wizard

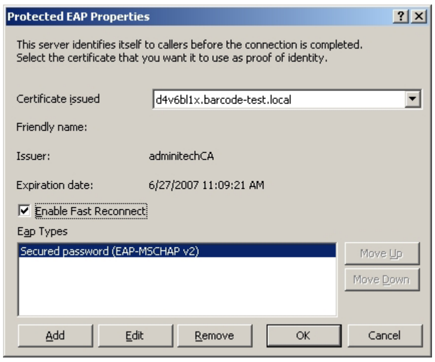
Authentication Methods

EAP uses different types of security devices to authenticate users.

Select the EAP type for this policy.

Type: Protected EAP (PEAP)

Check the check box for the Enable Fast Reconnect, and click on the OK button.



Protected EAP Properties

This server identifies itself to callers before the connection is completed. Select the certificate that you want it to use as proof of identity.

Certificate issued: d4v6bl1x.barcode-test.local

Friendly name:

Issuer: adminitechCA

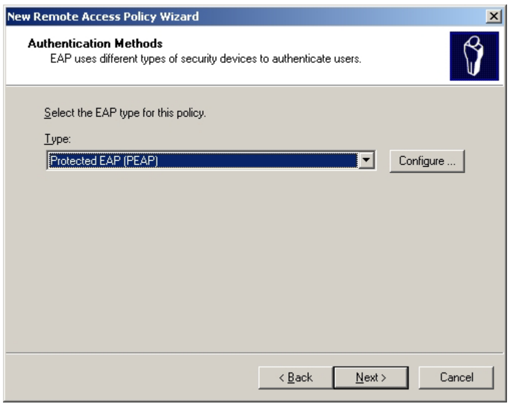
Expiration date: 6/27/2007 11:09:21 AM

☑ Enable Fast Reconnect

Eap Types

Secured password (EAP-MSCHAP v2)

Click on the Next button to finish creating a new remote access policy.



New Remote Access Policy Wizard

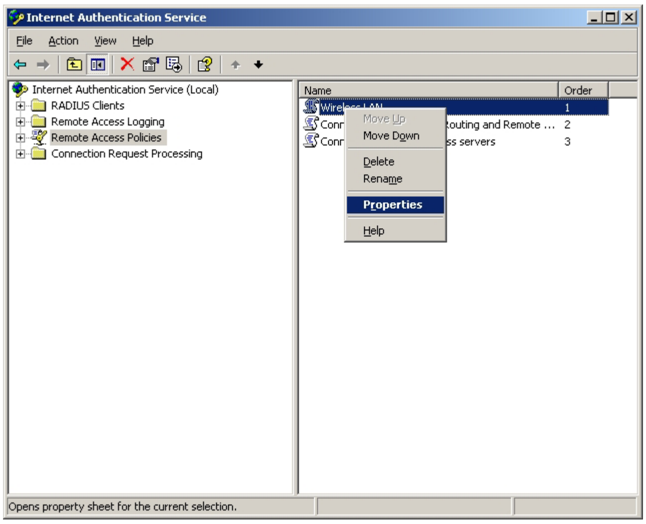
Authentication Methods

EAP uses different types of security devices to authenticate users.

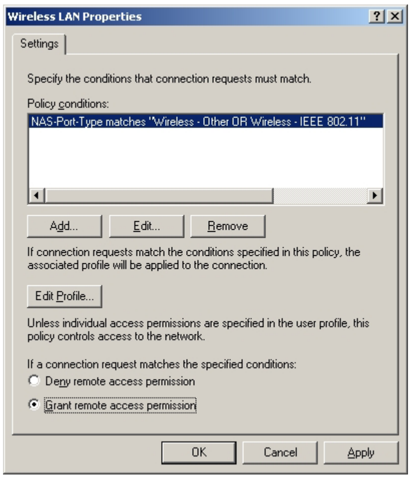
Select the EAP type for this policy.

Type: Protected EAP (PEAP)

Right-click on the created access policy and choose Properties.



Choose Grant remote access permission, and click on the Edit Profile button.



Wireless LAN Properties

Settings

Specify the conditions that connection requests must match.

Policy conditions:

NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"

Add... Edit... Remove

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

Edit Profile...

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

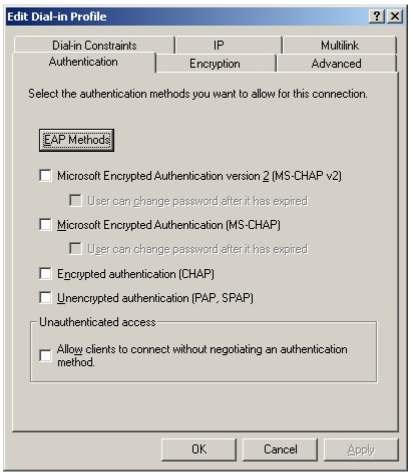
If a connection request matches the specified conditions:

○ Deny remote access permission

● Grant remote access permission

OK Cancel Apply

Choose the Authentication tab and click on the EAP Method button.



Edit Dial-in Profile

Dial-in Constraints | IP | Multilink | Authentication | Encryption | Advanced

Select the authentication methods you want to allow for this connection.

EAP Methods

□ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

□ Encrypted authentication (CHAP)

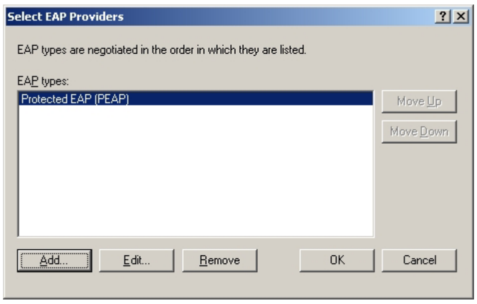
□ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

□ Allow clients to connect without negotiating an authentication method.

OK Cancel Apply

Click on the Add button.

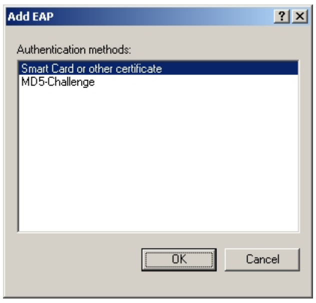

Select EAP Providers

EAP types are negotiated in the order in which they are listed.

EAP types:

Protected EAP (PEAP)

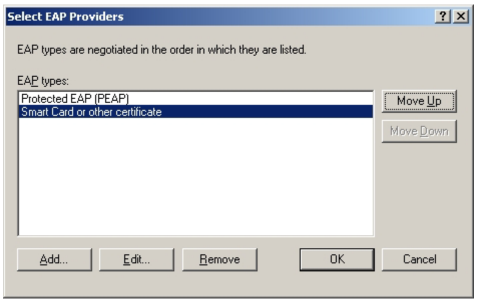
Choose Smart Card or other certificate and click on the OK button.


Add EAP

Authentication methods:

Smart Card or other certificate
MD5-Challenge

Click on the OK button.

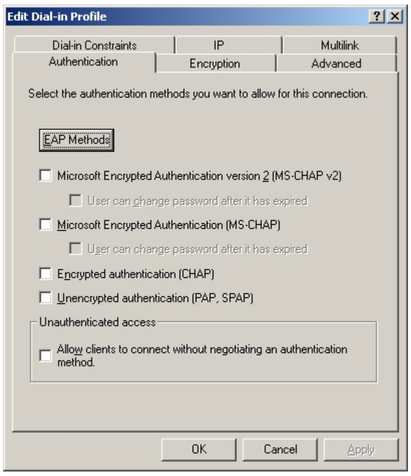

Select EAP Providers

EAP types are negotiated in the order in which they are listed.

EAP types:

Protected EAP (PEAP)
Smart Card or other certificate

Click on the OK button.


Edit Dial-in Profile

Select the authentication methods you want to allow for this connection.

☐ Microsoft Encrypted Authentication version 2 (MS-CHAP v2)

☐ User can change password after it has expired

☐ Microsoft Encrypted Authentication (MS-CHAP)

☐ User can change password after it has expired

☐ Encrypted authentication (CHAP)

☐ Unencrypted authentication (PAP, SPAP)

Unauthenticated access

☐ Allow clients to connect without negotiating an authentication method.

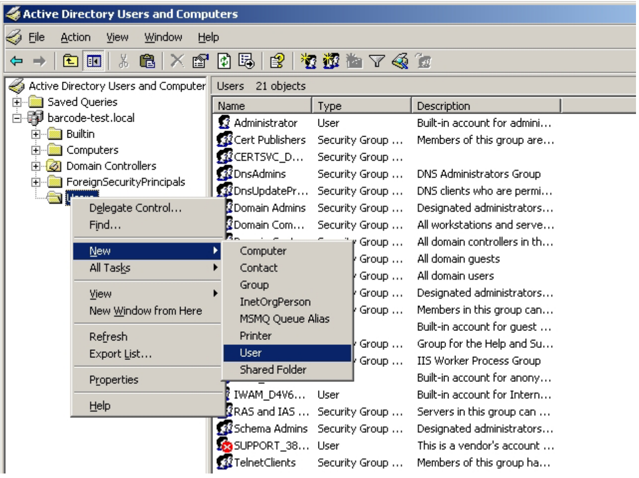
Now, the RADIUS server and access policy settings are completed.

- Creating a user

  The following procedures describe how to create a user for PEAP certificate and for EAP-TLS certificate, respectively.

  Click on the Start menu, All programs, and Management tool, then start the Active Directory Users and Computers.

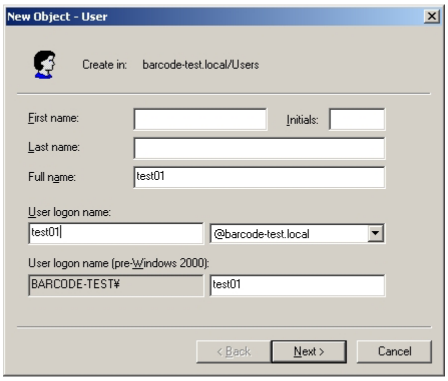
  Right-click on the User folder under the domain controller to be used, choose New, then User.



Users 21 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
CERTSVC_D...	Security Group ...	
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Com...	Security Group ...	All workstations and serve...
	Group ...	All domain controllers in th...
	Group ...	All domain guests
	Group ...	All domain users
	Group ...	Designated administrators...
	Group ...	Members in this group can...
		Built-in account for guest ...
	Group ...	Group for the Help and Su...
	Group ...	IIS Worker Process Group
		Built-in account for anony...
IWAM_D4V6...	User	Built-in account for Intern...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...

  Enter a Full name and the User logon name, then click on the Next button.



Create in: barcode-test.local/Users

First name:

Initials:

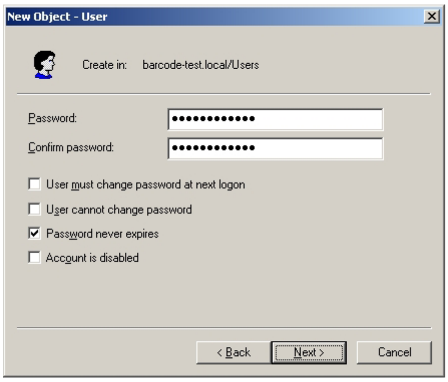
Last name:

Full name: test01

User logon name: test01 @barcode-test.local

User logon name (pre-Windows 2000): BARCODE-TEST¥ test01

  Enter a password and click on the Next button.



Create in: barcode-test.local/Users

Password: ••••••••••••

Confirm password: ••••••••••••

□ User must change password at next logon

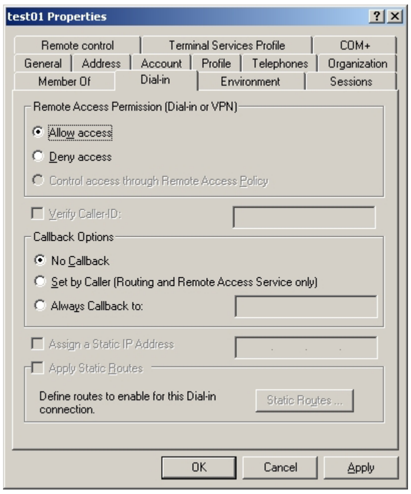
□ User cannot change password

☑ Password never expires

□ Account is disabled

  Now, creating a user is completed.

Right-click on the created user and choose Properties.
Click on the Dial-in tab and choose Allow access.



Remote Access Permission (Dial-in or VPN)

● Allow access

○ Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

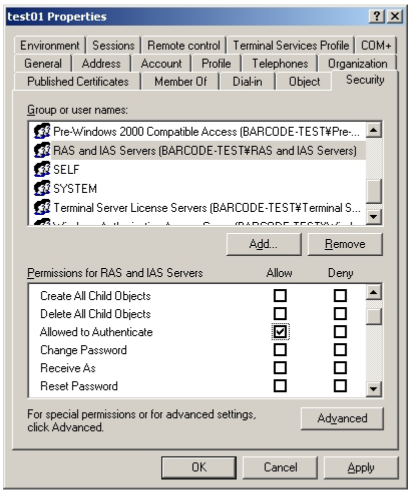
○ Always Callback to:

□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Click on the Security tab, and choose RAS and IAS Server, and check the check box for Allow to Authenticate.



Group or user names:

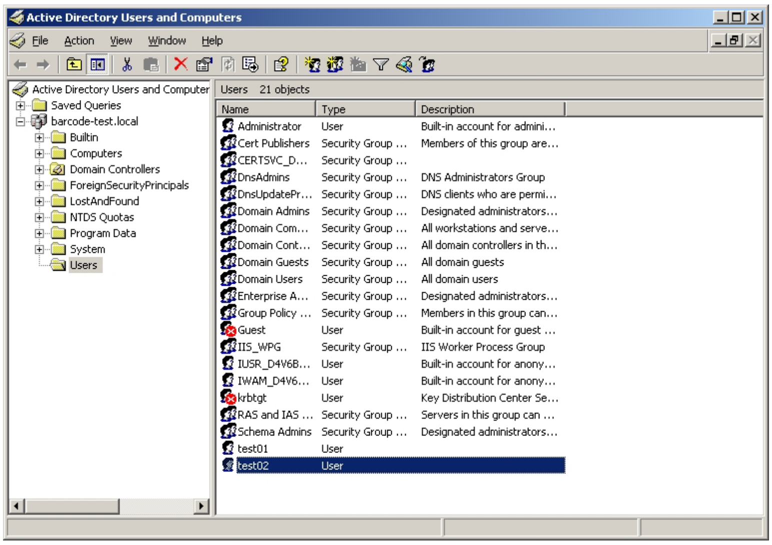
- Pre-Windows 2000 Compatible Access (BARCODE-TEST¥Pre-...
- RAS and IAS Servers (BARCODE-TEST¥RAS and IAS Servers)
- SELF
- SYSTEM
- Terminal Server License Servers (BARCODE-TEST¥Terminal S...

Permissions for RAS and IAS Servers	Allow	Deny
Create All Child Objects	□	□
Delete All Child Objects	□	□
Allowed to Authenticate	☑	□
Change Password	□	□
Receive As	□	□
Reset Password	□	□

For special permissions or for advanced settings, click Advanced.

Click on the OK button to close the Properties screen.

Repeat the above-mentioned procedures one more time to create another user.



- Active Directory Users and Computer
  - Saved Queries
  - barcode-test.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - NTDS Quotas
    - Program Data
    - System
    - Users

Users 21 objects

Name	Type	Description
Administrator	User	Built-in account for admini…
Cert Publishers	Security Group …	Members of this group are…
CERTSVC_D…	Security Group …	
DnsAdmins	Security Group …	DNS Administrators Group
DnsUpdatePr…	Security Group …	DNS clients who are permi…
Domain Admins	Security Group …	Designated administrators…
Domain Com…	Security Group …	All workstations and serve…
Domain Cont…	Security Group …	All domain controllers in th…
Domain Guests	Security Group …	All domain guests
Domain Users	Security Group …	All domain users
Enterprise A…	Security Group …	Designated administrators…
Group Policy …	Security Group …	Members in this group can…
Guest	User	Built-in account for guest …
IIS_WPG	Security Group …	IIS Worker Process Group
IUSR_D4V6B…	User	Built-in account for anony…
IWAM_D4V6…	User	Built-in account for anony…
krbtgt	User	Key Distribution Center Se…
RAS and IAS …	Security Group …	Servers in this group can …
Schema Admins	Security Group …	Designated administrators…
test01	User	
test02	User	

Now, creating users is completed.

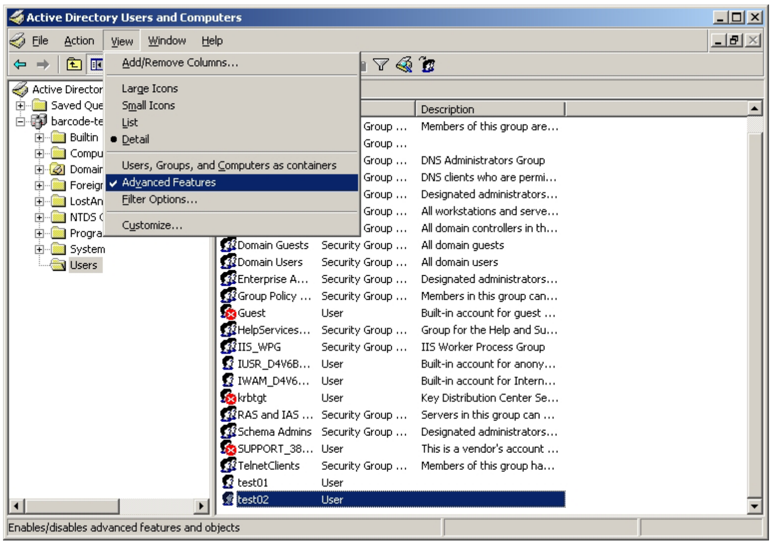
At this point, it is possible to log in the server from the client using the user name.

Log in the server using the user for EAP-TLS, and issue a user certificate.

- Setting the user

This section describes how to set the user for EAP-TLS.

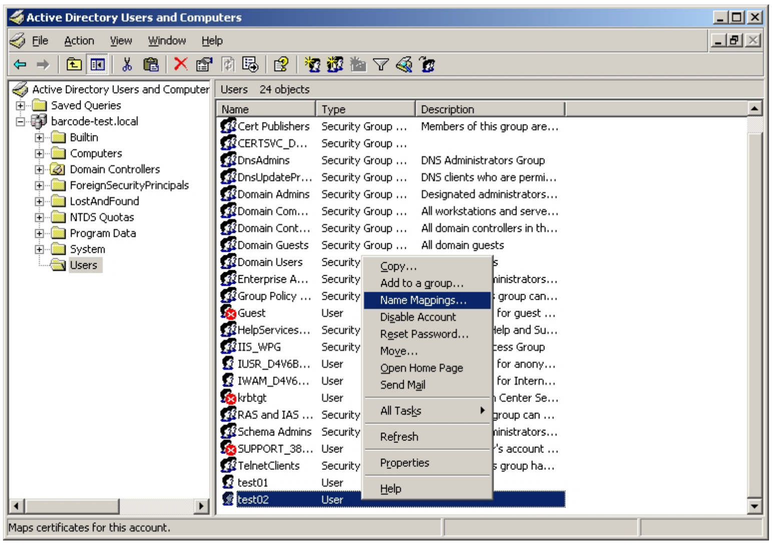
Click on the View menu and check Advanced Features.



Name	Type	Description
	Group ...	Members of this group are...
	Group ...	
	Group ...	DNS Administrators Group
	Group ...	DNS clients who are permi...
	Group ...	Designated administrators...
	Group ...	All workstations and serve...
	Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise A...	Security Group ...	Designated administrators...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_D4V6B...	User	Built-in account for anony...
IWAM_D4V6...	User	Built-in account for Intern...
krbtgt	User	Key Distribution Center Se...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...
test01	User	
test02	User	

Enables/disables advanced features and objects

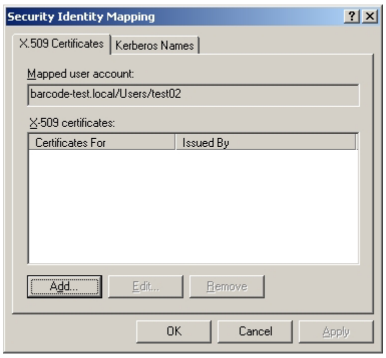
Right-click on the User for EAP-TLS and choose Name Mappings.



Name	Type	Description
Cert Publishers	Security Group ...	Members of this group are...
CERTSVC_D...	Security Group ...	
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Com...	Security Group ...	All workstations and serve...
Domain Cont...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security	s
Enterprise A...	Security	inistrators...
Group Policy ...	Security	group can...
Guest	User	for guest ...
HelpServices...	Security	elp and Su...
IIS_WPG	Security	ess Group
IUSR_D4V6B...	User	for anony...
IWAM_D4V6...	User	for Intern...
krbtgt	User	Center Se...
RAS and IAS ...	Security	group can ...
Schema Admins	Security	inistrators...
SUPPORT_38...	User	's account ...
TelnetClients	Security	group ha...
test01	User	
test02	User	

Maps certificates for this account.

Click on the Add button, choose the created user certificate, then click on the OK button.

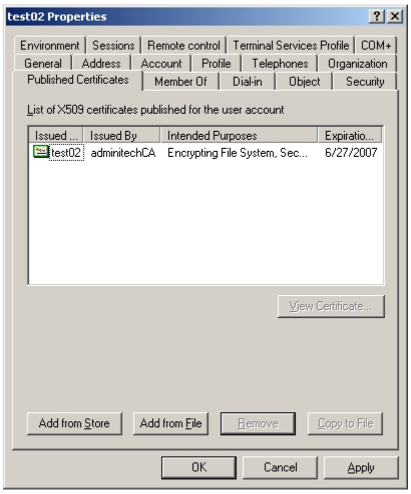


Mapped user account:
barcode-test.local/Users/test02

X.509 certificates:

Certificates For	Issued By

Make sure that the certificate information is displayed on the Properties screen.



List of X509 certificates published for the user account

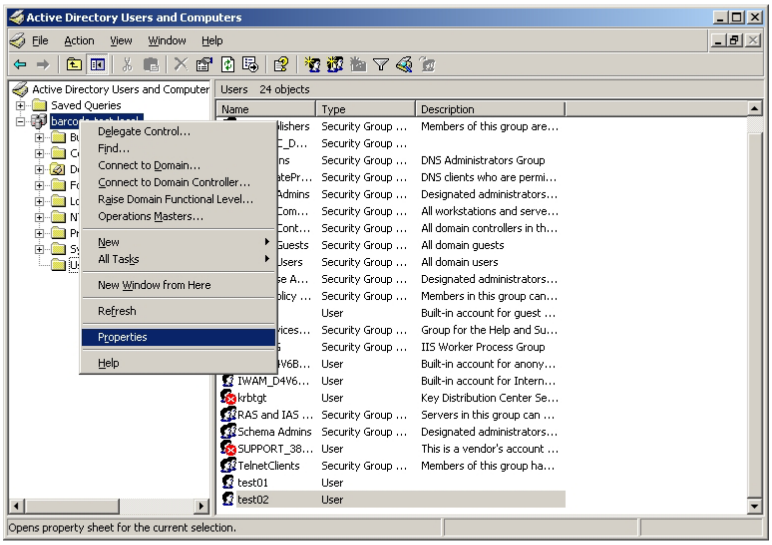
Issued ...	Issued By	Intended Purposes	Expiratio...
test02	adminitechCA	Encrypting File System, Sec...	6/27/2007

Now, the settings of the user for EAP-TLS are completed.

- Setting the group policy

Click on the Start menu, All programs, and Management tool, then start the Active Directory Users and Computers.

Right-click on the domain controller to be used and choose Properties.

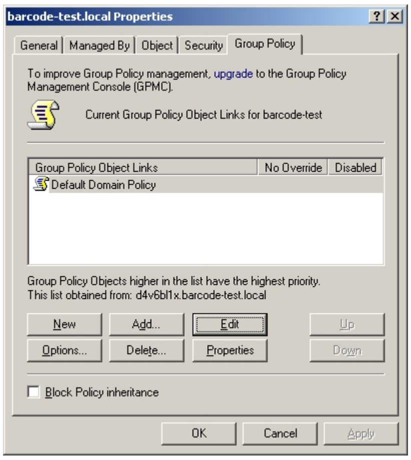


Users 24 objects

Name	Type	Description
lishers	Security Group ...	Members of this group are...
_D...	Security Group ...	
ns	Security Group ...	DNS Administrators Group
tePr...	Security Group ...	DNS clients who are permi...
Admins	Security Group ...	Designated administrators...
om...	Security Group ...	All workstations and serve...
ont...	Security Group ...	All domain controllers in th...
uests	Security Group ...	All domain guests
Users	Security Group ...	All domain users
e A...	Security Group ...	Designated administrators...
licy ...	Security Group ...	Members in this group can...
	User	Built-in account for guest ...
ices...	Security Group ...	Group for the Help and Su...
	Security Group ...	IIS Worker Process Group
V6B...	User	Built-in account for anony...
IWAM_D4V6...	User	Built-in account for Intern...
krbtgt	User	Key Distribution Center Se...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...
test01	User	
test02	User	

Opens property sheet for the current selection.

Choose the Group Policy tab and click on the Edit button.



To improve Group Policy management, upgrade to the Group Policy Management Console (GPMC).

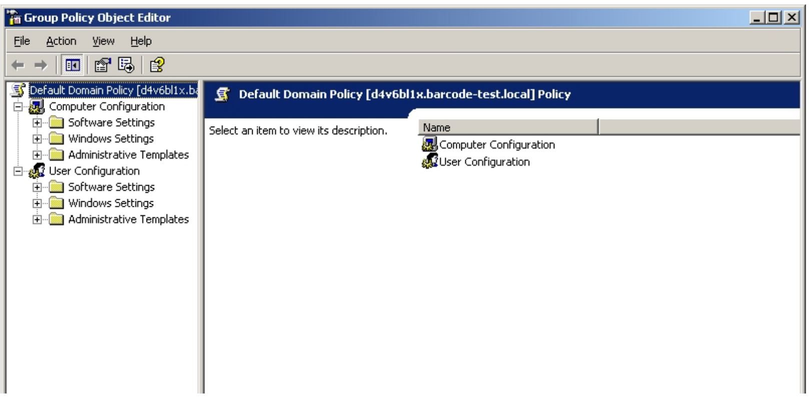
Current Group Policy Object Links for barcode-test

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: d4v6bl1x.barcode-test.local

□ Block Policy inheritance

The Group Policy Object Editor starts.

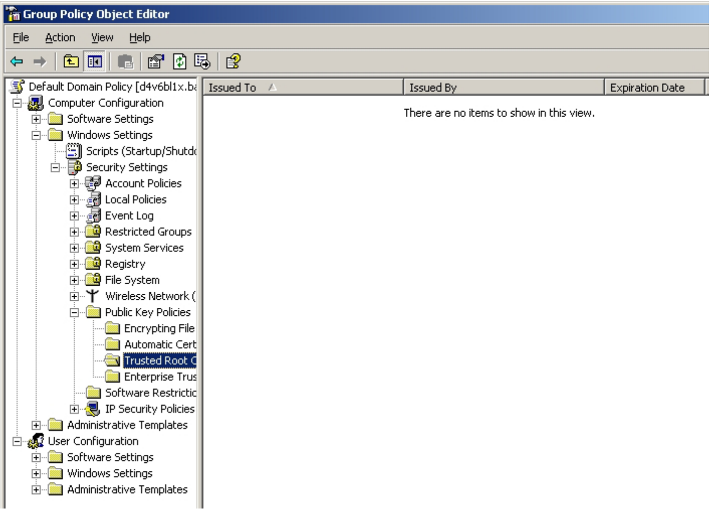


Default Domain Policy [d4v6bl1x.barcode-test.local] Policy

Select an item to view its description.

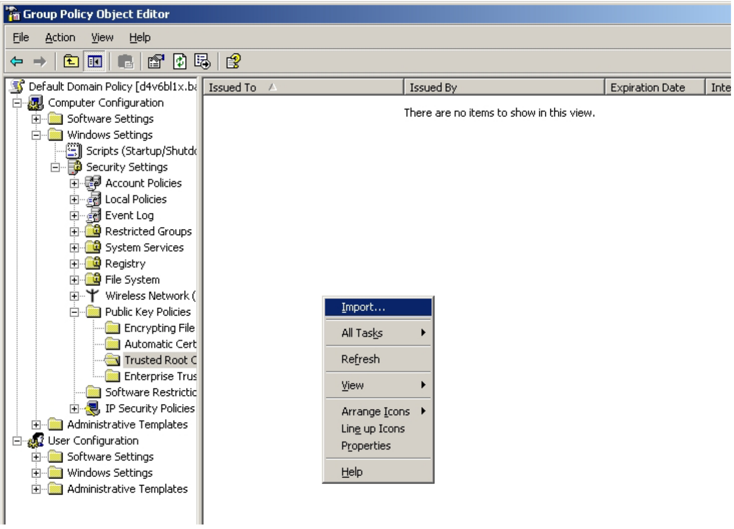
Name
Computer Configuration
User Configuration

Choose Computer Configuration, Windows Settings, Public Key Policies, and the Trusted Root Certificate, in that order.



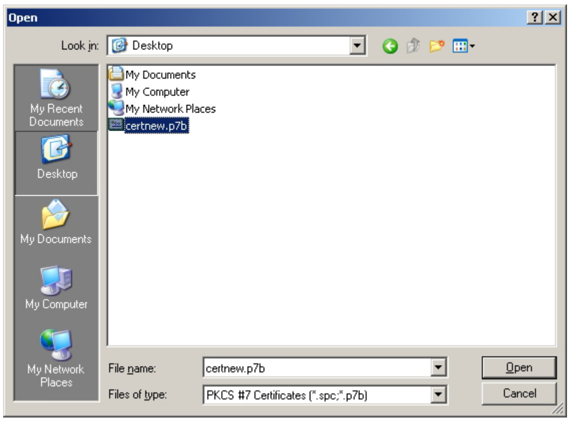
There are no items to show in this view.

Right-click on the view on the right side and click on Import.



There are no items to show in this view.

Choose the obtained server certificate.



File name: certnew.p7b

Files of type: PKCS #7 Certificates (*.spc;*.p7b)

Now, the settings of the group policies are completed.

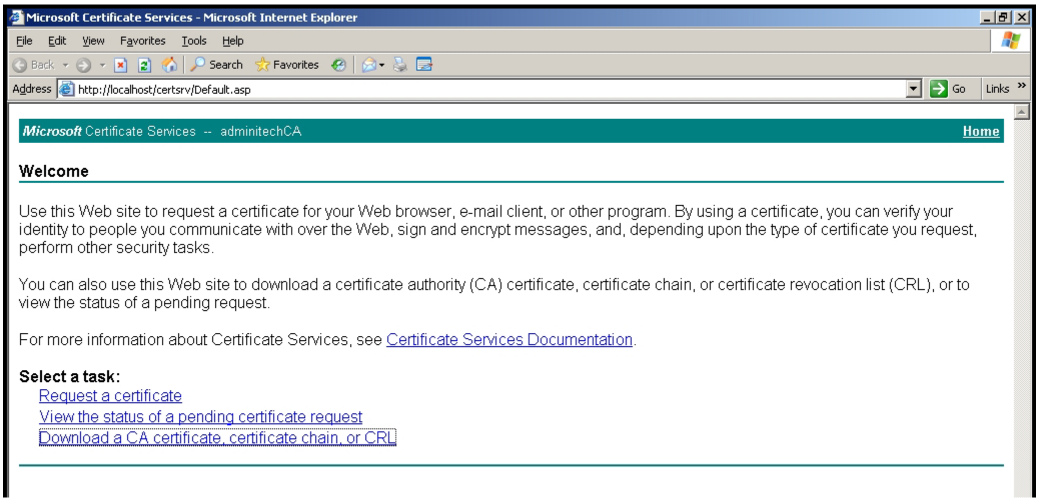
8.4 OBTAINING A CERTIFICATE

Server Certificate

Access the following Microsoft Certificate Services at the following URL:

http://localhost/CertSrv/

The following screen will be displayed.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/certsrv/Default.asp
Go Links
Microsoft Certificate Services -- adminitechCA
Home

Welcome

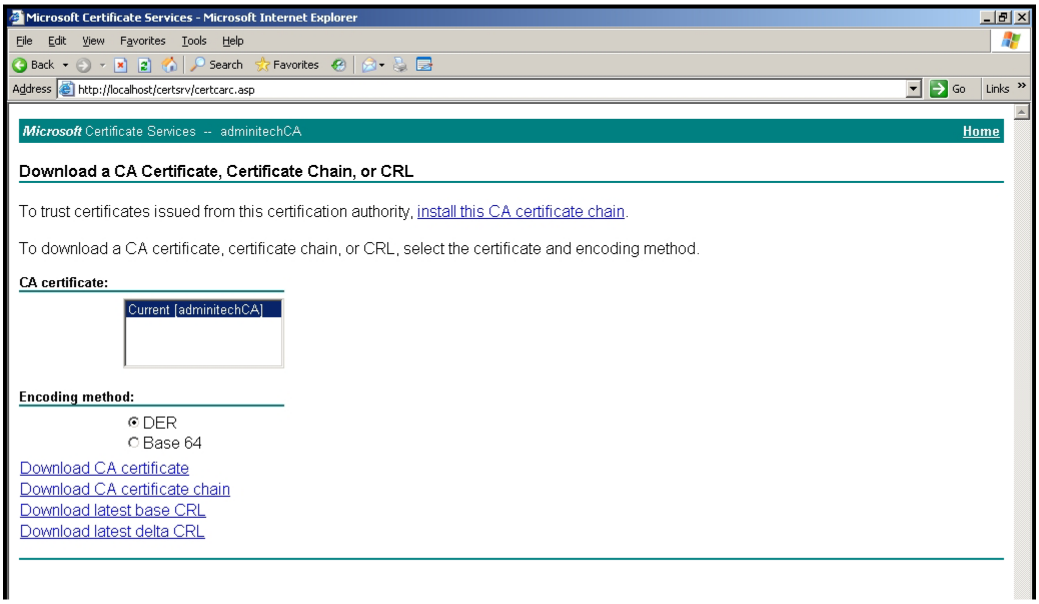
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

Click on Download a CA Certificate, Certificate Chain, or CRL.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/certsrv/certcarc.asp
Go Links
Microsoft Certificate Services -- adminitechCA
Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [adminitechCA]

Encoding method:

● DER
○ Base 64

- Download CA certificate
- Download CA certificate chain
- Download latest base CRL
- Download latest delta CRL

Certificate to be used for the wireless LAN module:

Download from the “Download CA certificate”. Server certificate .cer

Certificate to be used for the server:

Download from the “Download CA certificate chain”.

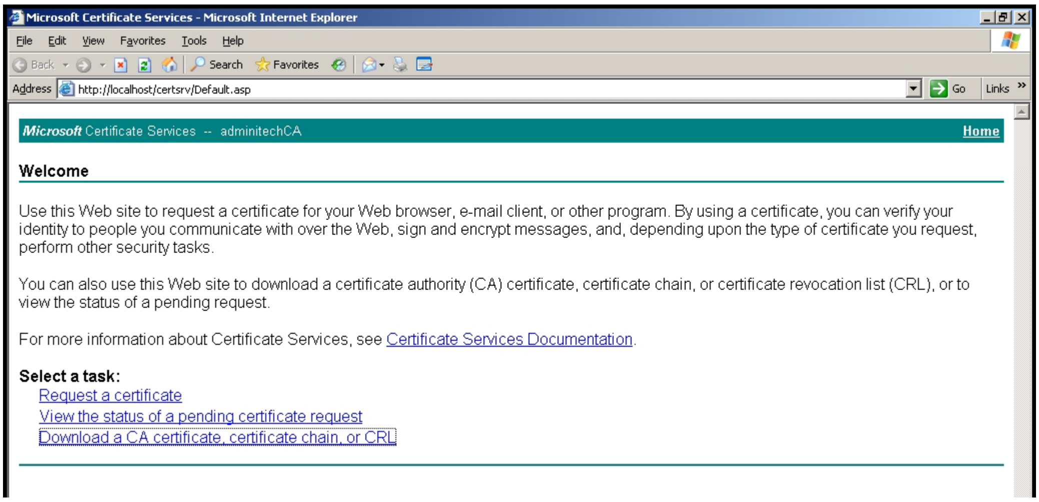
How to obtain a certificate

User certificate

Access the Microsoft Certificate Services at the following URL from the client:

http://(server IP)/CertSrv/

The following screen will be displayed.



Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/certsrv/Default.asp
Go Links
Microsoft Certificate Services -- adminitechCA
Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

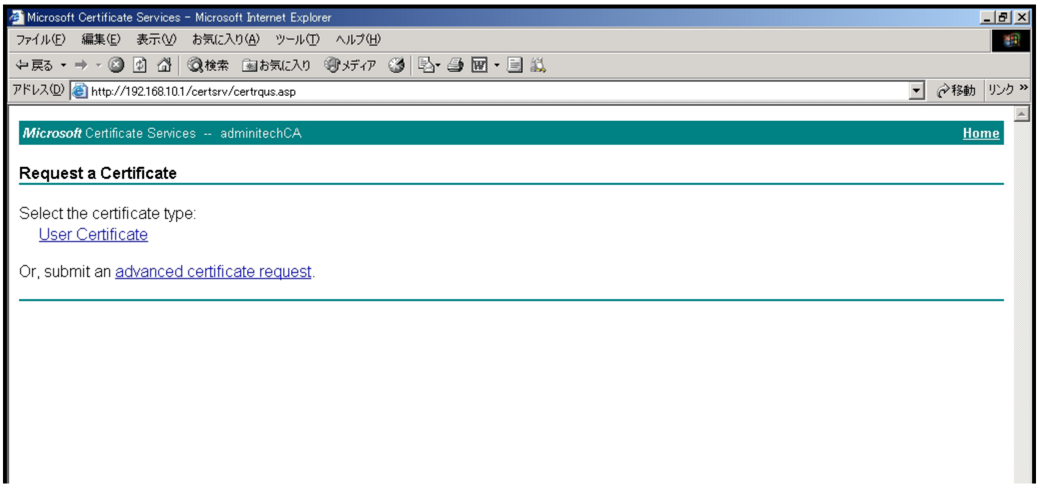
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Click on Request a certificate.



Microsoft Certificate Services - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り メディア
アドレス(D) http://192.168.10.1/certsrv/certrqus.asp
移動 リンク
Microsoft Certificate Services -- adminitechCA
Home

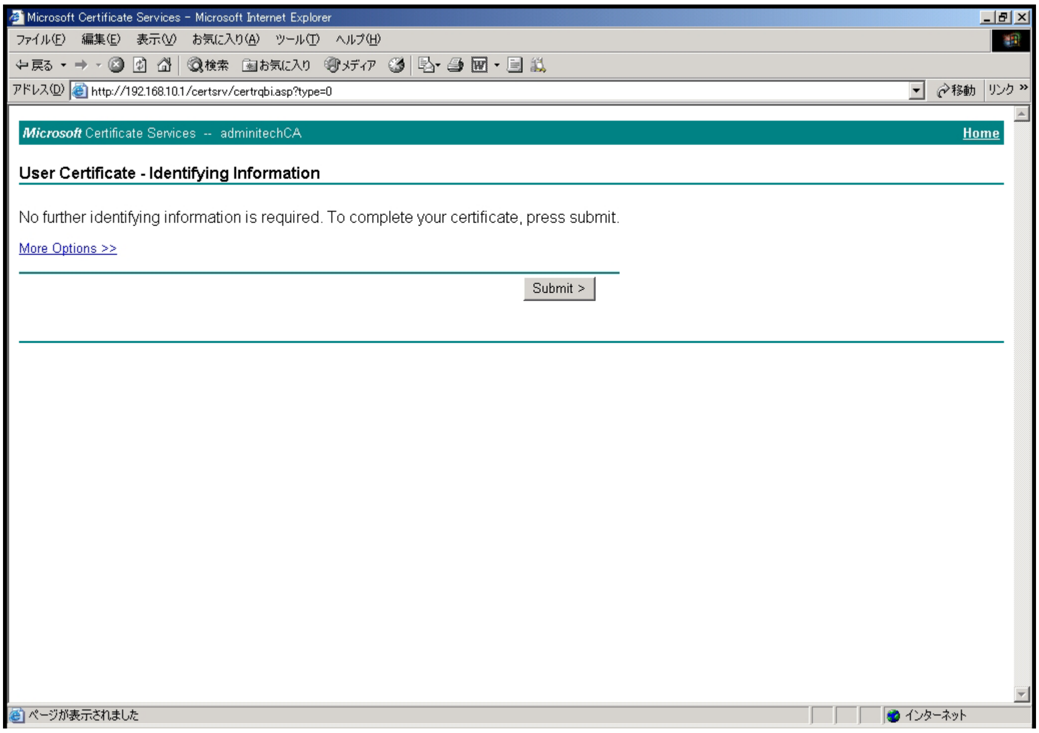
Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

Click on User Certificate.

Click on the Submit button.


Microsoft Certificate Services - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り メディア
アドレス(D)
移動 リンク
Home
ページが表示されました
インターネット

http://192.168.10.1/certsrv/certrqbi.asp?type=0

Microsoft Certificate Services -- adminitechCA

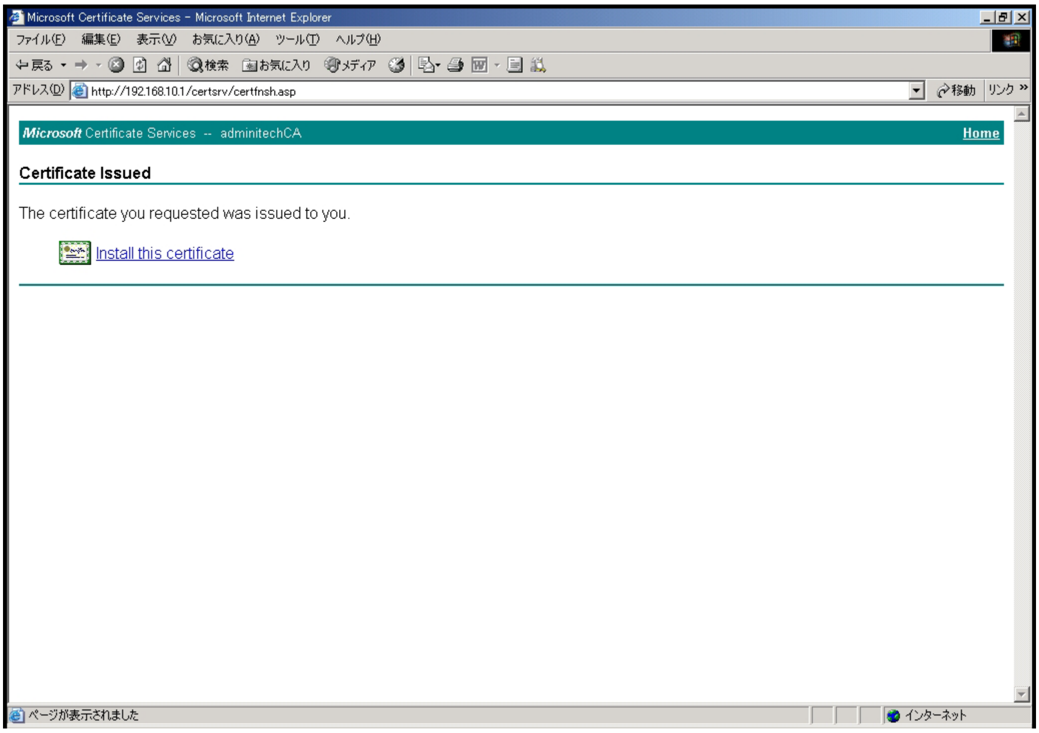
User Certificate - Identifying Information

No further identifying information is required. To complete your certificate, press submit.

More Options >>

Submit >

Click on Install this certificate to install the certificate.


Microsoft Certificate Services - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)
戻る 検索 お気に入り メディア
アドレス(D)
移動 リンク
Home
ページが表示されました
インターネット

http://192.168.10.1/certsrv/certfnsh.asp

Microsoft Certificate Services -- adminitechCA

Certificate Issued

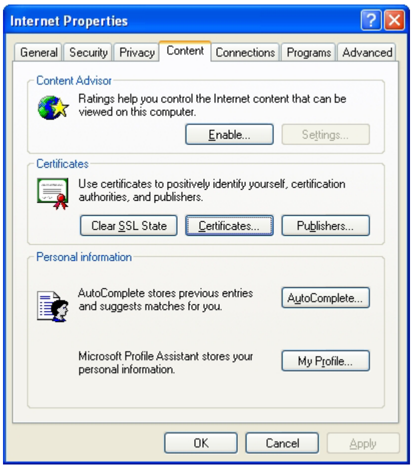
The certificate you requested was issued to you.

Install this certificate

Next, export the certificate.

Choose Internet Option from the Tool menu of the Internet Explorer.

Click on the Content tab, and the following screen is displayed.



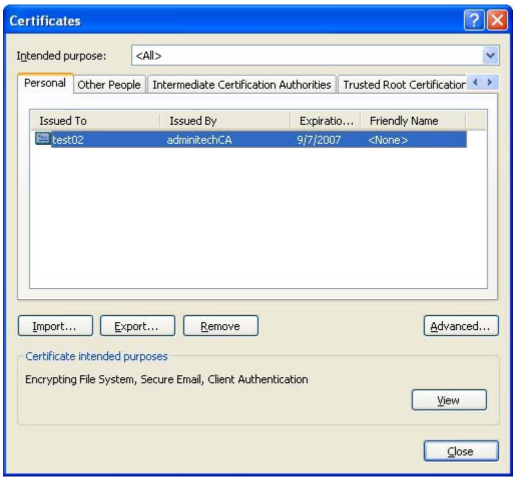
Ratings help you control the Internet content that can be viewed on this computer.

Use certificates to positively identify yourself, certification authorities, and publishers.

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Click on the Certificates button.


Certificates
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification
Import...
Export...
Remove
Advanced...
Certificate intended purposes
View
Close

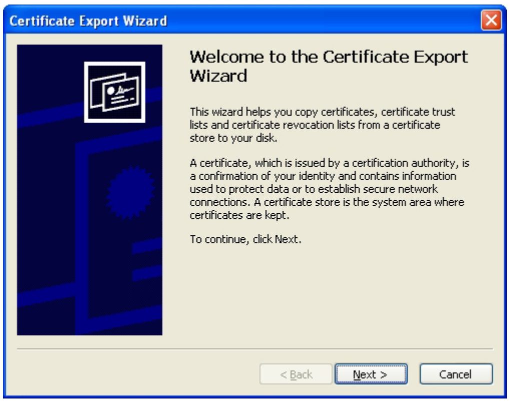
Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
test02	adminitechCA	9/7/2007	<None>

Encrypting File System, Secure Email, Client Authentication

Choose the certificate installed in the previous procedures, then click on the Export button.

The Certificate Export Wizard window appears.　Click on the Next button.



Welcome to the Certificate Export Wizard

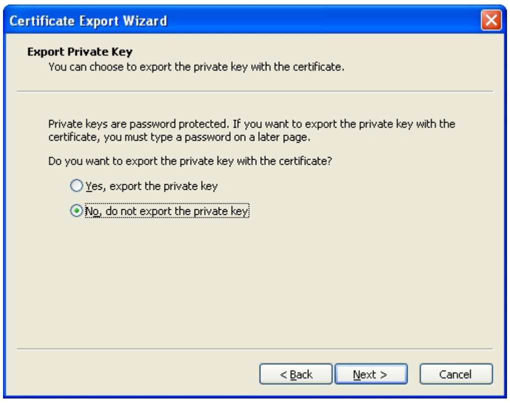
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

[User certificate used by the server]

Choose No, do not export the private key, then click on the Next button.



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

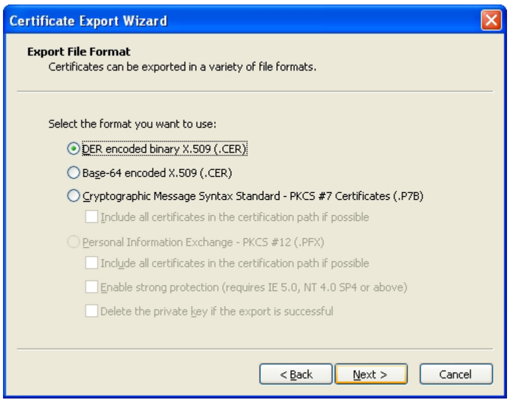
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Click on the Next button without changing any settings.



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

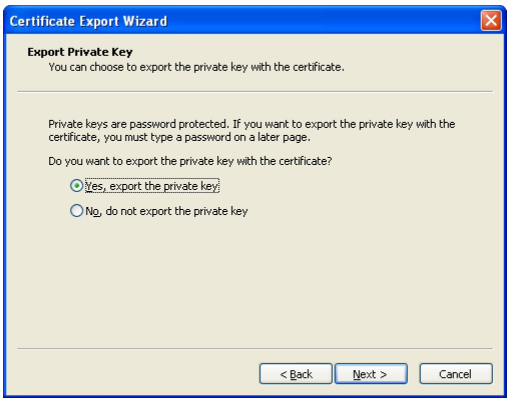
□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

[User certificate used by the wireless LAN module]

Choose Yes, export the private key, then click on the Next button.



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

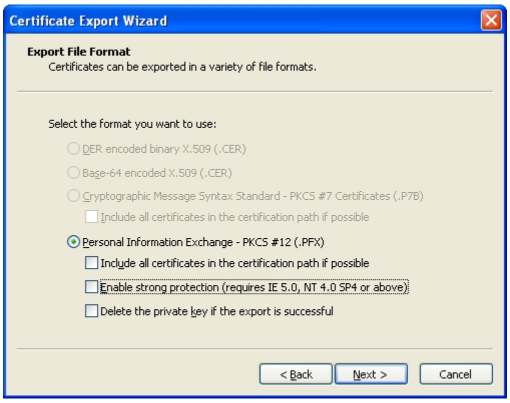
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Remove the check from the Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above), then click on the Next button.

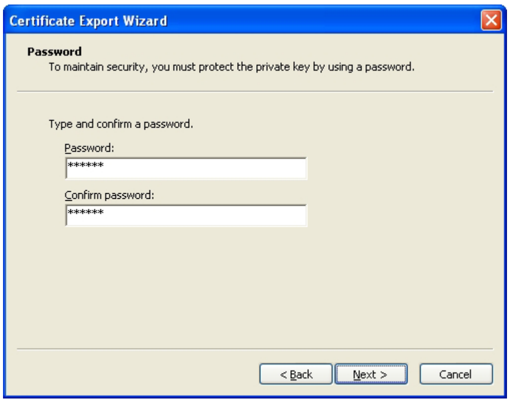


Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)
○ Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
● Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
□ Delete the private key if the export is successful

Enter the same password with the one that is used for the wireless LAN module.



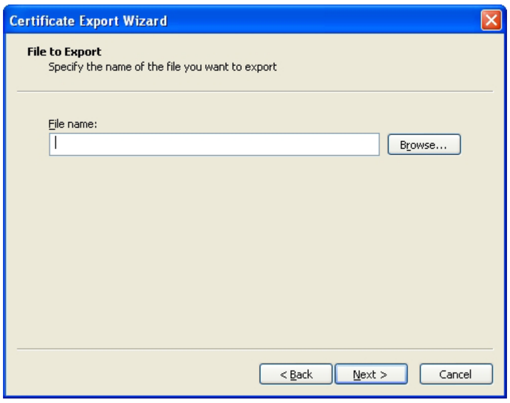
Password
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: ******

Confirm password: ******

Enter a file name and click on the Next button to export the file.



File to Export
Specify the name of the file you want to export

File name: