

F&eIT Series

Authentication Server

SVR-RDS(FIT)

Micro Authentication Server

SVR-RDS(FIT)L

User's Manual

CONTEC CO.,LTD.

The Check Your Package

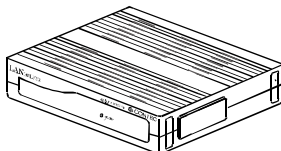
Thank you for purchasing the CONTEC product.

The items making up the SVR-RDS(FIT) and SVR-RDS(FIT)L packages are different.

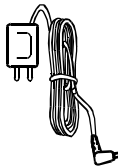
Check, with the following list, that your package is complete. If you discover damaged or missing items, contact your retailer.

Product Configuration List<SVR-RDS(FIT)>

- Main unit (SVR-RDS(FIT))...1
- AC Adapter...1
- Clamp...1
- Cable tie...2
- Wall mount screw...4
- Magnets...4
- Hub joint...1
- External-toothed screw...1
- User's Manual (this booklet)...1



Main unit (SVR-RDS(FIT))



AC Adapter



Cable tie x 2



Magnets x 4



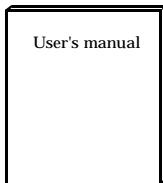
Clamp



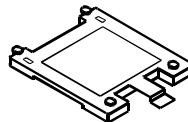
Wall mount screws x 4



External-toothed screw



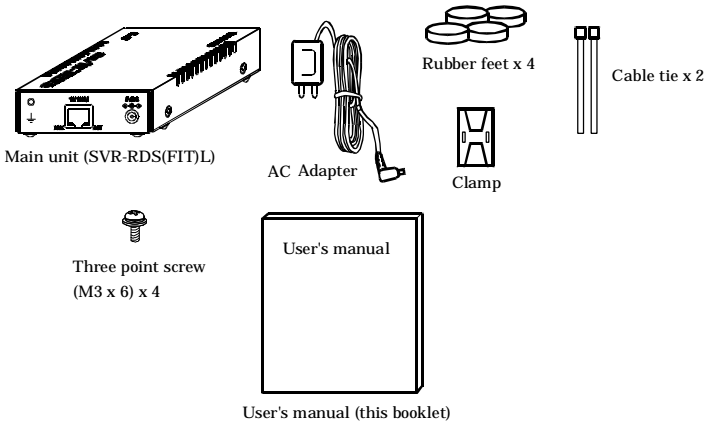
User's manual (this booklet)



Hub joint

Product Configuration < SVR-RDS(FIT)L >

- Main unit (SVR-RDS(FIT)L)...1
- AC Adapter...1
- Rubber feet...4
- Clamp...1
- Cable tie...2
- Three-point screw (M3×6)...1
- User's Manual (this booklet)...1



Copyright

Copyright 2003 CONTEC CO., LTD. ALL RIGHTS RESERVED

No part of this document may be copied or reproduced in any form by any means without prior written consent of CONTEC CO., LTD.

CONTEC CO., LTD. makes no commitment to update or keep current the information contained in this document. The information in this document is subject to change without notice.

All relevant issues have been considered in the preparation of this document. Should you notice an omission or any questionable item in this document, please feel free to notify CONTEC CO., LTD.

Regardless of the foregoing statement, CONTEC assumes no responsibility for any errors that may appear in this document or for results obtained by the user as a result of using this product.

Trademarks

F&eIT, FLEXLAN are registered trademark of CONTEC CO., LTD.

MS, Microsoft, Windows, Windows NT, and MS-DOS are registered trademarks of Microsoft Corporation in the U.S.A. and other countries.

Netscape Navigator is a registered trademark of Netscape Communications.

Other company and product names mentioned herein are generally trademarks or registered trademarks of their respective owners. This document does not use the symbols ™, ®, © etc.

Terminology/Abbreviations

The following terms and abbreviations are used in this manual for convenience.

Full term	Term used in this manual
SVR-RDS(FIT), SVR-RDS(FIT)L	authentication server / CA
FX-DS540-APW, FX-DS540-APP FX-DS540-AP, FX-DS540-APD FX-DS540-APDL, FX-DS540-APL	Access point / AP
A device with the wireless function	User unit / Wireless terminal
Personal computer	PC
User unit / Wireless terminal	UU

Table of contents

The Check Your package.....	i
Copyright.....	iii
Trademarks.....	iii
Terminology/Abbreviations.....	iii

1. BEFORE USING THE PRODUCT	1
------------------------------------	----------

About the SVR-RDS(FIT) or SVR-RDS(FIT)L.....	1
Features	1
Customer Support.....	2
Web Site.....	2
Limited One-Year Warranty.....	2
How to Obtain Service.....	2
Liability.....	2
Safety Precautions	3
Safety Information	3
Handling Precautions.....	3
Environment	5
Inspection.....	5
Storage	6
Disposal.....	6

2. BEFORE SETTING THE NETWORK	7
--------------------------------------	----------

Constructing a network.....	7
Component Locations	8
Setup.....	10
Table Top Installation of SVR-RDS(FIT).....	10
Wall Installation of SVR-RDS(FIT)	11
Attaching Using a Magnet of SVR-RDS(FIT)	12
For stacking SVR-RDS(FIT) on HUB or access point.....	14
Table Top Installation of SVR-RDS(FIT)L.....	16
Cable Installation.....	17
Network Cable Installation.....	17
AC Adapter Connection	18
Ground the SVR-RDS(FIT)/ SVR-RDS(FIT)L	19
Function Overview	20
Authentication Type and Function	20
Backup and restore of the system	20
Setting procedure.....	21

Setup Preparation	23
Connecting to the Web Browser PC.....	24
Connecting to an SVR-RDS(FIT)/ SVR-RDS(FIT)L.....	24
Setup Method.....	25
Login.....	25
Various settings.....	25
Exiting Setup.....	25
Setting to be conducted at first.....	26
1.Login.....	26
2.Setting the system time	26
3.IP Address Setting	27
4.Setting for the authenticator.....	28
5.Starting the authentication server	30
6.Exiting Setup.....	30
Setting user information	31
Registering user information (Authentication Type: EAP-TLS, PEAP(TLS))	31
1.Login.....	31
2.Registering an account and obtaining a certificate	31
3.Validating user information Make registered user information take effect.....	34
4.Exiting Setup.....	34
Registering user information (Authentication Type: PEAP(MS CHAP-V2)).....	35
1.Login.....	35
2.Registering an account and obtaining a certificate	35
3.Validating user information.....	38
4.Exiting Setup.....	38
Registering user information again (Authentication Type: EAP-TLS, PEAP(TLS)).....	39
1.Login.....	39
2.Registering an account and obtaining a certificate again.....	39
3.Validating user information.....	42
4.Exiting Setup.....	42
Registering user information again (Authentication Type: PEAP(MS CHAP-V2))	43
1.Login.....	43
2.Registering an account and obtaining a certificate again.....	43
3.Validating user information.....	46
4.Exiting Setup.....	46
Deleting user information.....	47
1.Login.....	47
2.Deleting an account	47
3.Validating user information.....	48
4.Exiting Setup.....	49

Adding or removing an authenticator	50
Adding an authenticator	50
1.Login.....	50
2.Adding an authenticator	50
3.Validating user information	52
4.Exiting Setup.....	52
Deleting an authenticator.....	53
1.Login.....	53
2.Deleting an authenticator	53
3.Validating user information	54
4.Exiting Setup.....	54
Setting Items	55
Basic Setup.....	56
System time setting.....	57
NTP clients Setup.....	57
Starting or stopping the authentication function	58
Authenticator Setup	58
Authentication Type Setup.....	59
CA certificate (Root CA)	60
User information (User CA).....	61
Initial Setup	61
Password setting.....	62
Back up	62
Restore	62
4. SETTING FOR THE AUTHENTICATOR	63
Setting items (Setup using a web browser)	63
Wireless LAN.....	63
IEEE802.1X.....	64
5. SETTING FOR THE SUPPLICANT	65
Use under Windows XP SP1	65
Authentication Type: EAP-TLS	66
1.Installation of CA certificate.....	66
2.Installation of User CA.....	68
3.Setting the wireless network.....	70
4.Connecting to the wireless network	72
Authentication Type: PEAP(MS CHAP-V2)	74
1.Installation of CA certificate.....	74
2.Setting the wireless network	76
3.Connecting to the wireless network	78

Authentication Type: PEAP(TLS)	80
1.Installation of CA certificate	80
2.Installation of User CA	82
3.Setting the wireless network	84
4.Connecting to the wireless network	86
Use under Windows 2000 SP4.....	88
Authentication Type: EAP-TLS	89
1.Installing the IEEE 802.1X support	89
2.Installation of CA certificate	90
3.Installation of User CA	92
4.Setting the wireless network	94
5.Connection to the wireless network	96
Authentication Type: PEAP(MS CHAP-V2)	97
1.Installing the IEEE 802.1X support	97
2.Installation of CA certificate	98
3.Setting the wireless network	100
4.Connection to the wireless network	103
Authentication Type: PEAP(TLS)	104
1.Installing the IEEE 802.1X support	104
2.Installation of CA certificate	106
3.Installation of User CA	108
4.Setting the wireless network	110
5.Connection to the Wireless Network	114
Use under Windows 2000 SP3.....	115
Installing the IEEE 802.1X support	115
Deleting a certificate.....	116
Deleting a CA certificate.....	116
Deleting an user certificate	117

6. MAINTENANCE 119

Status Display	119
Saving and restoring system information.....	120
Back up	120
Restore.....	122
Upgrading the System.....	124

7. TROUBLESHOOTING 127

When Communication Fails.....	127
When the main body Will Not Start.....	127
Authentication failed	128

Factory Default Settings List.....	129
System setting.....	129
Product Specifications.....	129
Physical Specifications.....	129
Software Specifications.....	129
Environmental Specifications for Installing the main body.....	130
LEDs.....	131
SVR-RDS(FIT)	131
SVR-RDS(FIT)L.....	131
Indicator	131
Input/Output Interface.....	132
Pin Assignment for UTP Port	132
life expectancy of Battery	132
Glossary.....	133

1. Before Using the Product

This chapter provides information you should know before using the product.

About the SVR-RDS(FIT) or SVR-RDS(FIT)L

This product is an authentication server unit for IEEE 802.1X authentication. The product has the functions of a private certification authority (CA) and Remote Authentication Dial-In User Service (RADIUS) server required for authentication. The product supports EAP-TLS, PEAP, a standard authentication protocol conforming to IEEE 802.1X, and allows web browsers to easily issue certificates required for EAP-TLS, PEAP authentication. This product can therefore provide all the functions required for IEEE 802.1X authentication, from issuing certificates to authentication.

Read this manual carefully to use the product correctly.

Features

Common to SVR-RD(FIT) and SVR-RD(FIT)L

- It serves as an authentication server.
- It has CA and RADIUS server function required for authentication server of IEEE 802.1X.
- Easy configuration and management using a WWW browser.
- Supporting EAP-TLS, capable of authentication of each terminal using a public key certificate.
- Supporting PEAP, capable of authentication with a password without using an user certificate.
- CA can be issued up to 200.
- Capable of managing up to ten authenticators. This allows wireless LAN user units to roam in the coverage of up to ten access points.

SVR-RDS(FIT)L

- Compact and lightweight.

SVR-RDS(FIT)

- Flexibility in installation depending on the location, allowing the unit to be even hung on the wall or stacked together with a FLEXLAN DS540 series access point (CONTEC HUB)

Customer Support

CONTEC provides the following support services for you to use CONTEC products more efficiently and comfortably

Web Site

Japanese	http://www.contec.co.jp/
English	http://www.contec.com/
Chinese	http://www.contec.com.cn/

Latest product information

CONTEC provides up-to-date information on products.

CONTEC also provides product manuals and various technical documents in the PDF.

Free download

You can download updated driver software and differential files as well as sample programs available in several languages.

Note! For product information

Contact your retailer if you have any technical question about a CONTEC product or need its price, delivery time, or estimate information.

Limited One-Year Warranty

CONTEC products are warranted by CONTEC CO., LTD. to be free from defects in material and workmanship for up to one year from the date of purchase by the original purchaser.

Repair will be free of charge only when this device is returned freight prepaid with a copy of the original invoice and a Return Merchandise Authorization to the distributor or the CONTEC group office, from which it was purchased.

This warranty is not applicable for scratches or normal wear, but only for the electronic circuitry and original product products. The warranty is not applicable if the device has been tampered with or damaged through abuse, mistreatment, neglect, or unreasonable use, or if the original invoice is not included, in which case repairs will be considered beyond the warranty policy.

How to Obtain Service

For replacement or repair, return the device freight prepaid, with a copy of the original invoice. Please obtain a Return Merchandise Authorization Number (RMA) from the CONTEC group office where you purchased before returning any product.

* No product will be accepted by CONTEC group without the RMA number.

Liability




The obligation of the warrantor is solely to repair or replace the product. In no event will the warrantor be liable for any incidental or consequential damages due to such defect or consequences that arise from inexperienced usage, misuse, or malfunction of this device.

Safety Precautions

Understand the following definitions and precautions to use the product safely.

Safety Information

This document provides safety information using the following symbols to prevent accidents resulting in injury or death and the destruction of equipment and resources. Understand the meanings of these labels to operate the equipment safely.

 DANGER	DANGER indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	WARNING indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	CAUTION indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury or in property damage.

Handling Precautions

DANGER

Do not use the product where it is exposed to flammable or corrosive gas. Doing so may result in an explosion, fire, electric shock, or failure.



CAUTION

- This product contains precision electronic elements and must not be used in locations subject to physical shock or strong vibration.
Otherwise, the products may malfunction, overheat, or cause a failure.
 - Do not use or store this device in high temperature or low temperature surroundings, or do not expose it to extreme temperature changes.
Otherwise, the products may malfunction, overheat, or cause a failure.
 - Do not use or store this device where it is exposed to direct sunlight or near stoves or other sources of heat. Otherwise, the products may malfunction, overheat, or cause a failure.
 - Do not use or store this device near strong magnetic fields or devices emitting electromagnetic radiation. Otherwise, the products may malfunction, overheat, or cause a failure.
 - If an unusual smell or overheat is noticed, unplug the power cable immediately.
 - Be careful not to let the external supply voltage or drive current exceed the rating.
 - Do not place an object that blocks ventilation slits on top of this product or on its sides.
 - The specifications of this product are subject to change without notice for enhancement and quality improvement.
Even when using the product continuously, be sure to read the manual and understand the contents.
 - Do not attempt to modify this device. The manufacturer will bear no responsibility whatsoever for the device if it has been modified.
 - Regardless of the foregoing statements, CONTEC is not liable for any damages whatsoever (including damages for loss of business profits) arising out of the use or inability to use this CONTEC product or the information contained herein.
-

Environment

Use this product in the following environment. If used in an unauthorized environment, the products may overheat, malfunction, or cause a failure.

Operating temperature

0 to 40°C

Humidity

10 to 90%RH (No condensation)

Corrosive gases

None

Floating dust particles

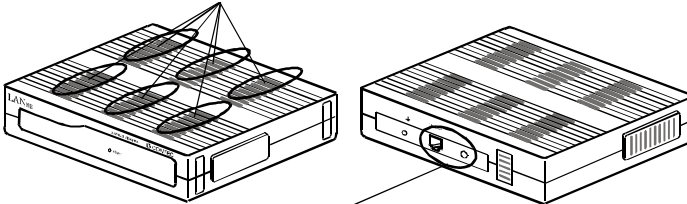
Not to be excessive

Inspection

Inspect the product periodically as follows to use it safely.

< SVR-RDS(FIT) >

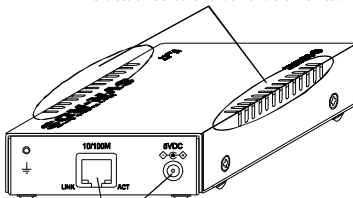
- Front
- The ventilation slits are not covered, and neither dust nor alien substance is attached to the ventilation slits.
- Back



- Check that the connector of the unit and its cable have been plugged correctly.

< SVR-RDS(FIT)L >

- The ventilation slits are not covered, and neither dust nor alien substance is attached to the ventilation slits.



- Check that the connector of the unit and its cable have been plugged correctly.

Storage

When storing this product, keep it in its original packing form.

- (1) Wrap it in the packing material, then put it in the box.
- (2) Store the package at room temperature at a place free from direct sunlight, moisture, shock, vibration, magnetism, and static electricity.

Disposal

When disposing of the product, follow the disposal procedures stipulated under the relevant laws and municipal ordinances.

2. Before setting the network

This chapter describes the adequate information before constructing a network used main body.

Constructing a network

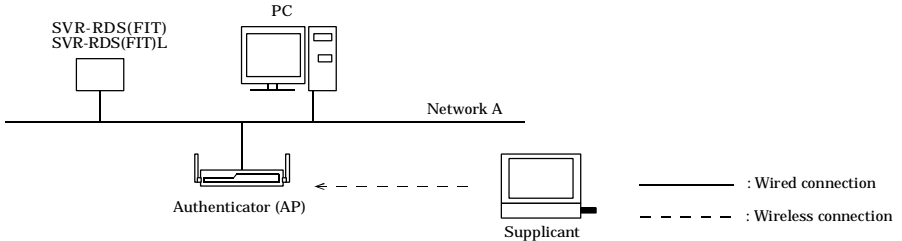


Figure 2.1. Constructing a network

SVR-RDS(FIT) / SVR-RDS(FIT)L

The unit is this product, an IEEE 802.1X compliant authentication server providing the CA (certification authority) and RADIUS server functions.

For the setup method, refer to Chapter 3 settings the main body.

For details on the specifications, see “Product Specifications” in Chapter 8 "Appendix”.

Authenticator

In wireless LAN terminology, an authenticator is an IEEE 802.1X compliant AP.

Capable of managing up to ten authenticators. This allows wireless LAN terminal to roam.

For the setup method, refer to Chapter 4 settings for the authenticator.

For the authenticator corresponding to this product, refer to Chapter 8 Appendix.

Supplicant

A supplicant is a terminal that can issue IEEE 802.1X authentication request.

The terminal requires an OS having the supplicant functions supporting IEEE 802.1X (Windows XP, Windows XP SP1, or Windows 2000 SP3 + IEEE 802.1X, Windows 2000 SP4 support module).

User certificates can be issued up to 200.

For the setup method, refer to Chapter 5 settings for the supplicant

For the supplicant corresponding to this product, refer to Chapter 8 Appendix.

Component Locations

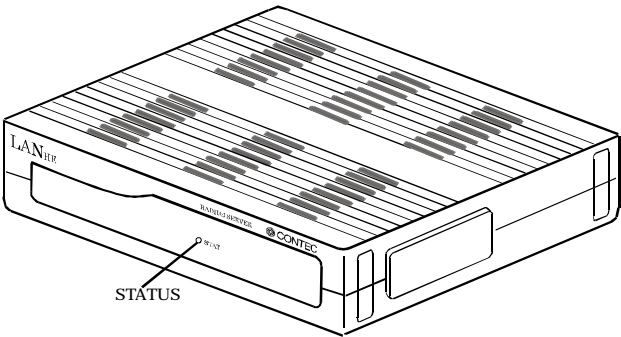


Figure 2.2. SVR-RDS(FIT) (Front)

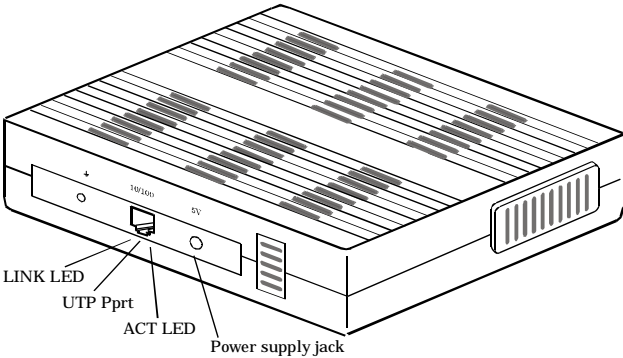


Figure 2.3. SVR-RDS(FIT) (Back)

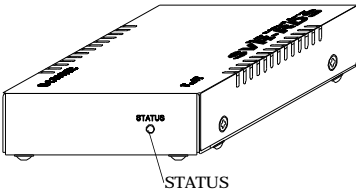


Figure 2.4. SVR-RDS(FIT)L (Front)

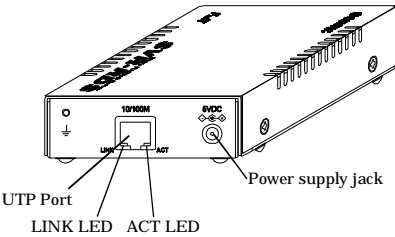


Figure 2.5. SVR-RDS(FIT)L (Back)

LED Indicators

Three LEDs (one on the front and two on the back) indicate power supply, and wired LAN connection status.

Table 2.1. LED Display

Name	Color	Status	Indicator
STATUS	Green / Orange	On in orange	Indicates that the device is operating.
		On in green	Indicates that the device is being started (going to operate after the power switch was turned on).
LINK	Green	On	Indicates that the link has been established.
		Off	Indicates that the link has been disconnected.
ACT	Orange	Flashing	Indicates that LAN data is being transmitted/received.

Connectors

Table 2.2. Connectors

Name of connectors	Name described in main body	Operation / function
UTP Port	10/100M	Connects to a 10BASE-T or 100BASE-TX LAN.
Power supply jack	5VDC	5VDC power supply input jack. Connect the attached AC adapter.



CAUTION

Use the attached AC adapter on the power supply to the main body.

Using the other power supplies may damage.

Setup

Table Top Installation of SVR-RDS(FIT)

If installing on a desktop, place the unit on a stable and flat base and ensure that adequate space is provided for ventilation (5cm).

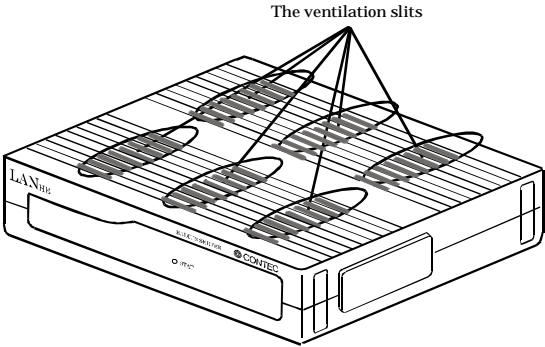
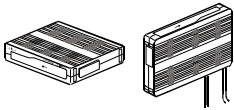


Figure 2.6. The Ventilation Slits

⚠ CAUTION Do not obstruct the ventilation slits. This can cause the temperature inside the product to rise and can damage the components inside.

⚠ WARNING SVR-RDS(FIT) must be installed with the top or side surface face up. If installed with any other surface face up, the SVR-RDS(FIT) can be overheated inside to catch fire.



Wall Installation of SVR-RDS(FIT)

The attached wall mount screws are useful for installing the unit on a wall. Attach the unit to a stable vertical wall and ensure that adequate space is provided for ventilation (5cm).

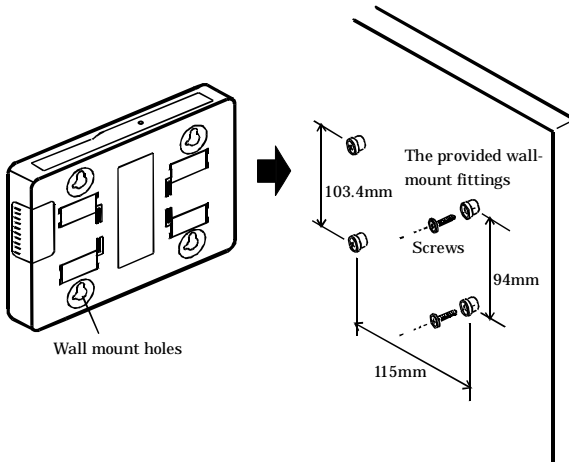


Figure 2.7. Wall Installation

To mount the unit on a wall, obtain the required number of screws (to fit $\phi 3.5$).

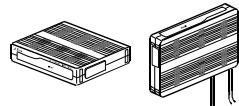
- (1) Use the screws to attach the provided wall-mount fittings to the wall. The dimensions are shown in the figure above. (4 locations)
- (2) Attach the SVR-RDS(FIT) case such that the four wall-mount fittings on the wall insert into the wall-mount holes on the case.
- (3) Slide the SVR-RDS(FIT) unit down to hold it in place.

⚠ CAUTION

Do not obstruct the ventilation slits. This can cause the temperature inside the product to rise and can damage the components inside.

⚠ WARNING

SVR-RDS(FIT) must be installed with the top or side surface face up. If installed with any other surface face up, the SVR-RDS(FIT) can be overheated inside to catch fire.



Attaching Using a Magnet of SVR-RDS(FIT)

The magnet provided with the SVR-RDS(FIT) makes it easy to attach or remove the AP from metal surfaces such as steel partitions or desks.

CAUTION

- Do not place magnets near monitors, floppy disks, or other sensitive objects.
 - Moving the SVR-RDS(FIT) while it is mounted on a steel desk or similar surface can cause paint scratching.
 - Units cannot be stacked if attached by a magnet.
-

Attaching and removing magnets

To mount the unit using a magnet, push the magnet into the magnet mounting hole in the direction of arrow 1 as shown in Figure 2.8. , then insert the entire magnet into the mounting hole.

Next, slide the magnet in the direction of arrow 2 to hold the unit in place.

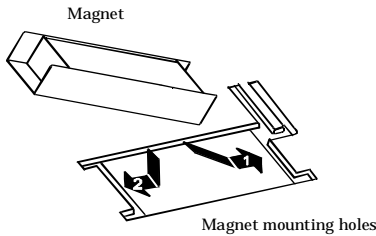


Figure 2.8. Attaching Magnets

To remove, slide the magnet in the direction of arrow 1 in Figure 2.9. , then lift in the direction of arrow 2.

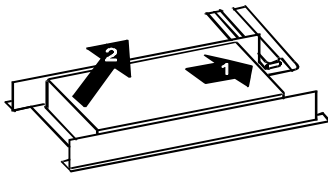


Figure 2.9. Removing Magnets

Mounting on steel desks

The unit can be mounted directly on steel desks. Pull lightly to make sure that the SVR-RDS(FIT) does not come off easily.

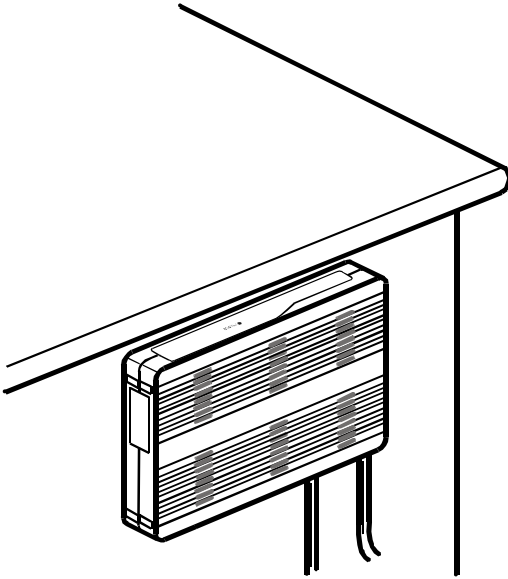
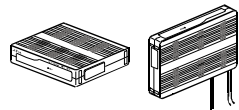


Figure 2.10. Mounting on Steel Desks

WARNING

The SVR-RDS(FIT) must be installed with the top or side surface face up. If installed with any other surface face up, the AP can be overheated inside to catch fire.



For stacking SVR-RDS(FIT) on HUB or access point

For Stacking

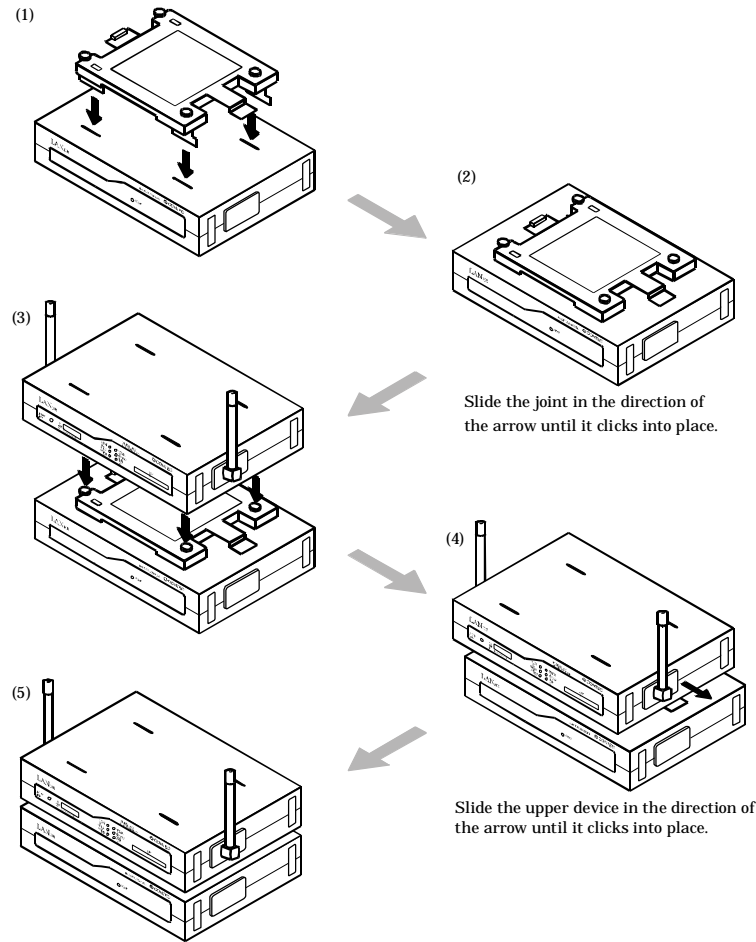


Figure 2.11. How to stack SVR-RDS(FIT) on HUB or Access point

Removing

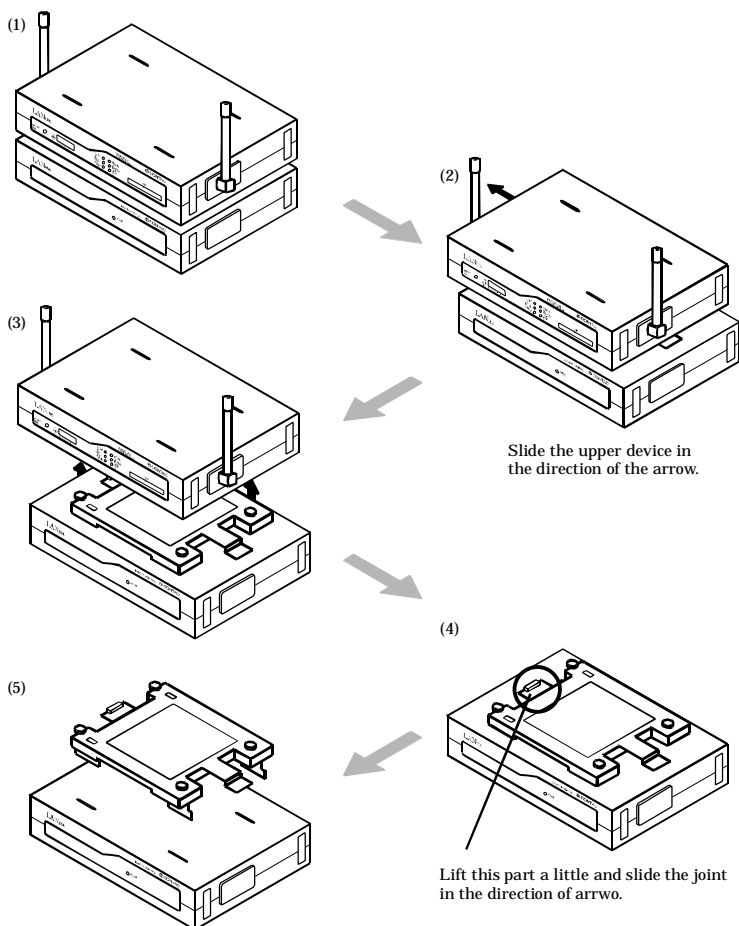


Figure 2.12. How to remove

Table Top Installation of SVR-RDS(FIT)L

Use rubber feet

If installing on a table top , place the unit on a stable and flat base and ensure that adequate space is provided for ventilation (5cm).

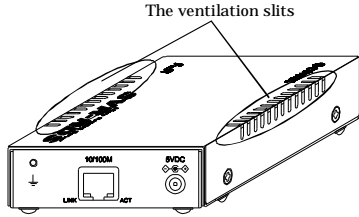


Figure 2.13. The Ventilation Slits



CAUTION

Do not obstruct the ventilation slits. This can cause the temperature inside the product to rise and can damage the components inside.



WARNING

Do not obstruct the ventilation slits. This can cause the temperature inside the product to rise and can be overheated inside to catch fire.

Cable Installation

Network Cable Installation

Connect your network cable to the network connector on the SVR-RDS(FIT)/ SVR-RDS(FIT)L. This model has a single 10BASE-T / 100BASE-TX connector.

10BASE-T or 100BASE-TX connection

⚠ CAUTION

- When connecting this product to a personal computer or hub use a twisted pair cable no more than 100m in length.
- Use UTP cable or STP cable having category 3, 4, or 5 specifications.
- When connecting with a personal computer (NIC) or hub up-link port, use a UTP cross cable (TP-X).

- (1) Connect the UTP cable (straight-through cable) to the UTP port in a hub or bridge.
- (2) Connect the other end of the UTP cable to the UTP port on the SVR-RDS(FIT)/ SVR-RDS(FIT)L.

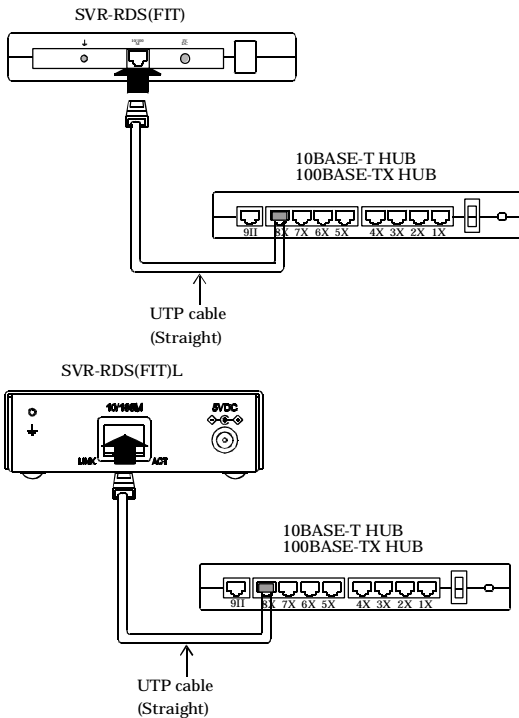



Figure 2.14. 10 BASE-T or 100BASE-TX Connection

AC Adapter Connection

Connect the attached AC adapter to the power jack on the main unit.

**CAUTION**

Use the attached AC adapter on the power supply to the main body.
Using the other power supplies may damage.

Securing the DC jack of the AC adapter

Using the attached clamp and cable tie prevents the DC jack from coming off when the DC cable is loaded.

Stick the clamp onto the SVR-RDS(FIT)/ SVR-RDS(FIT)L main unit. Plug the DC jack of the AC adapter into the connector on the main unit, then fasten the DC cable to the clamp using the cable tie.

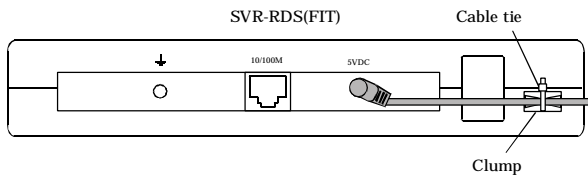


Figure 2.15. DC Jack Clamping Example of AC adapter(SVR-RDS(FIT))

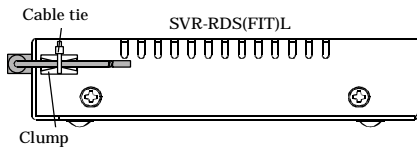
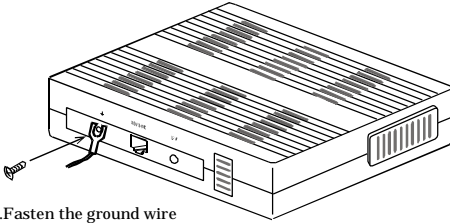


Figure 2.16. DC Jack Clamping Example of AC adapter(SVR-RDS(FIT)L)

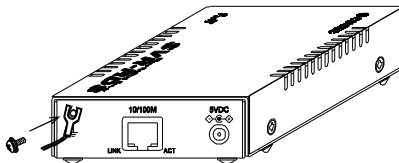
Ground the SVR-RDS(FIT)/ SVR-RDS(FIT)L

Use the attached external-toothed screw (for the SVR-RDS(FIT)) or three-point sems screw (for the SVR-RDS(FIT)L) to connect the ground wire to the ground terminal on the main unit.



1. Fasten the ground wire using the external-toothed screw.

Figure 2.17. Ground the SVR-RDS(FIT)



1. Fasten the groud wire using the three-point screw.

Figure 2.18. Ground the SVR-RDS(FIT)L

Function Overview

Authentication Type and Function

This section summarizes a feature of each authentication type, which is different from the features of the other authentication type.

Authentication Type and Function

Table 2.3. Authentication Type and Function

Type		User certificate	Server certificate	Remarks
EAP-TLS		Required	Required	Conducts authentication using the digital certificates on the client and server, providing the highest level of security.
PEAP	MS CHAP-V2	Not required	Required	Conducts authentication using a password but requiring no digital certificate on the client, making operation and management relatively easy. This protocol can also request both of the client and server to have a digital certificate.
	TLS	Required	Required	

Authentication types supported by Windows by default

Table 2.4. Authentication types supported by Windows by default

Type		Windows XP	Windows XP SP1	Windows 2000 SP3 (Patch required)	Windows 2000 SP4
EAP-TLS		O	O	O	O
PEAP	MS CHAP-V2	x	O	O	O
	TLS	x	O	O	O

O: Supported x: Unsupported

Backup and restore of the system

You can back up configuration information to a data file, such as network settings, user information, and passwords.

The backup of data can be restored on the main unit. On the SVR-RDS(FIT) or SVR-RDS(FIT)L, a backup of data from another unit can be restored.

Setting procedure

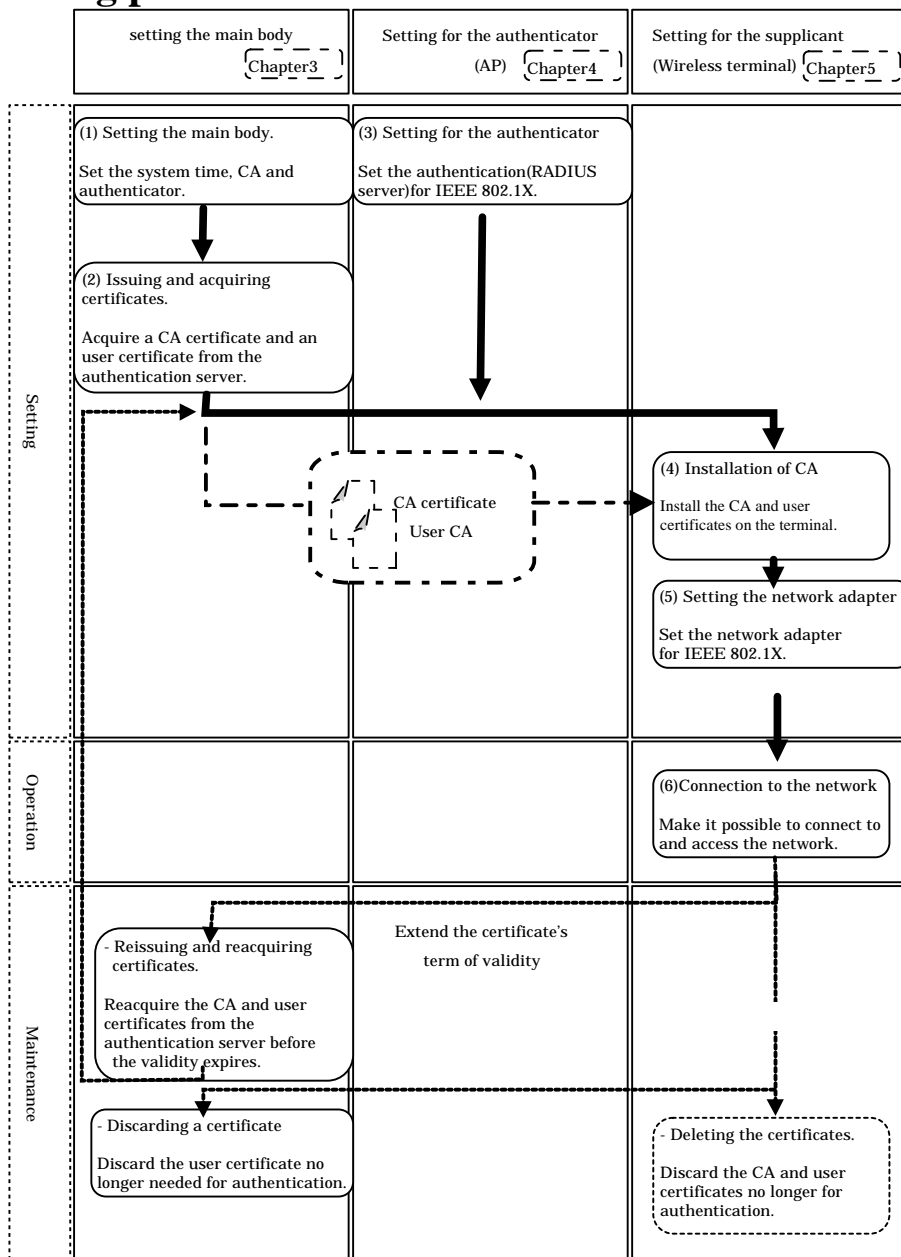


Figure 2.19. Setting procedure

3. Setting the main body

This chapter describes how to setup the SVR-RDS(FIT)/SVR-RDS(FIT)L.

Setup Preparation

You can setup the AP software from a PC running a web browser via the LAN. As this provides a graphical interface, setup using a web browser is much easier than using a terminal.

This product is factory-set to be assigned an IP address of “192.168.1.1” and a network mask of “255.255.255.0”.

You can use this address to connect to the AP from a web browser but this requires that you change the IP address of the PC to be in the same network group as the AP’s IP address (when finished, set the IP address back to its original value).

Supported web browsers (recommended)

- Microsoft Internet Explorer 5.01 or higher
- Netscape Navigator 6 or higher

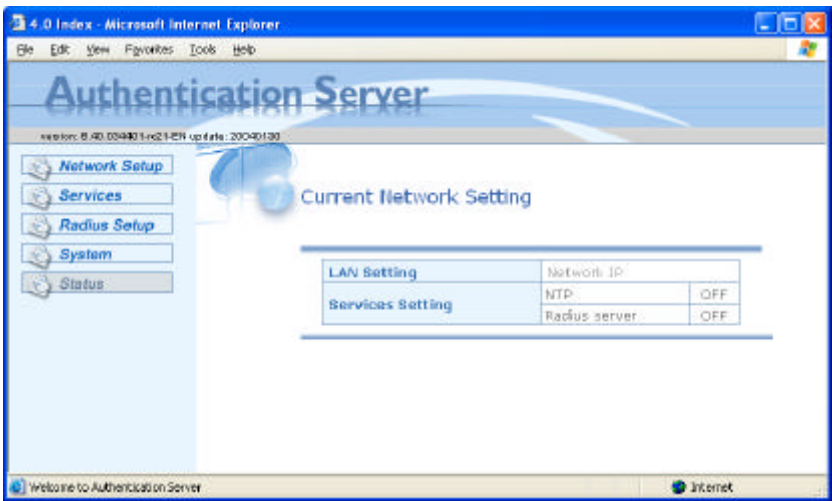


Figure 3.1. Example Browser Setting Screen

Connecting to the Web Browser PC

When using a web browser to setup the AP, you can connect via either a LAN. Use the following procedure to connect the web browser.

- (1) Connect the PC on which you will run the web browser to the same network as the AP.
Alternatively, you can use a UTP cable to connect the PC directly to the AP. In that case, use a crossed-cable.
The connection will not work if you use a standard straight-through cable.

CAUTION

You may not be able to establish a connection if the web browser is setup to use a proxy. In this case, change the setting to not use a proxy.

Remember to change the proxy setting back when you have finished setting up the AP.

Connecting to an SVR-RDS(FIT)/ SVR-RDS(FIT)L

To connect the web browser to the SVR-RDS(FIT)/ SVR-RDS(FIT)L, the IP address of the PC on which you run the web browser must be in the same network group as the IP address of the SVR-RDS(FIT)/ SVR-RDS(FIT)L. The factory default IP address set in the SVR-RDS(FIT)/ SVR-RDS(FIT)L is always in the class C network group starting with [192.168.1.1] and [192.168.1]. Accordingly, set the IP address of the PC to also start with [19.168.1] ([IP 192.168.1.10, MASK 255.255.255.0], for example).

When you have completed setting up the authentication server via your PC, reset the PC's IP address to the original value.

- (1) Start the web browser.
Recommended web browsers are Microsoft Internet Explorer 5.01 or later and Netscape 6.0 or later.
- (2) After starting the web browser, specify the IP address of the main body in the URL field.
For example, if the IP address of the main body is [192.168.1.1], enter the following:

http://192.168.1.1

CAUTION

Manage the set IP address not to be forgotten.

If you forget the IP address, you cannot make changes to the settings for the server unit.

If you cannot access the server unit via the web browser, you cannot even reset the server unit to the factory defaults.

Setup Method

This section describes how to perform setup using a web browser.

Login

When you have completed preparation for setup and connection to the main unit, the authentication server prompts you to enter the password.

Enter the password.

Both of the user name and password are factory-set to “root”.

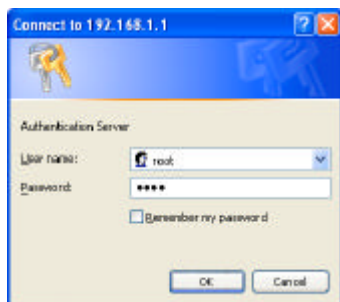


Figure 3.2. Login Screen

Various settings

Make “Settings to Be Made First” followed by other settings as required.

You can make these settings in the same way as when you use the WWW browser to connect to and work with the Internet. To change the setting of an item, edit the form containing that item. Follow the procedure to complete setup to reflect the new settings in the main body.

Exiting Setup

Exit the web browser to disconnect the PC from the server unit.

Setting to be conducted at first

After purchasing the SVR-RDS(FIT) / SVR-RDS(FIT)L, be sure to follow the procedure below to make all of these settings.

1.Login

- (1) Connect to the main body.
For the devices and cables used for connection, see “Setup Preparation” and “Setup Method”.

2.Setting the system time

Select your time zone and set the current time. The system time is referenced to define the validity term of each certificate to be issued and to check the validity term of each certificate used for authentication. Authentication cannot be performed normally unless the system time has been set correctly.

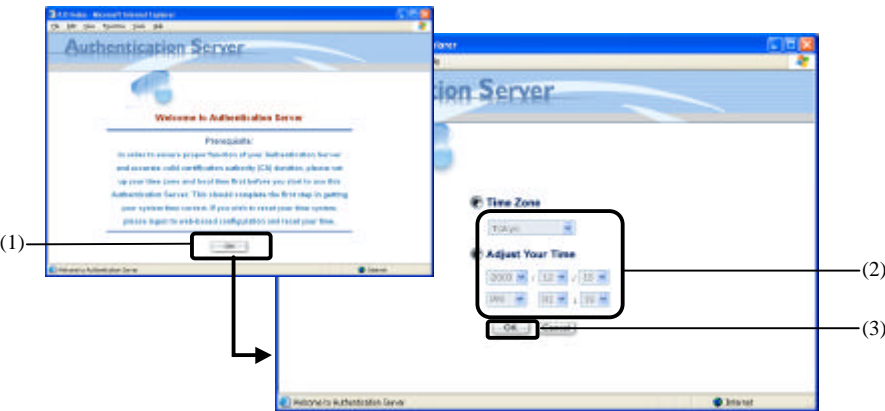


Figure 3.3. System Time Setting Page

- (1) When connecting to the main body, a guide page is displayed. Click on the [OK] button.
- (2) On the system time setting page, set your time zone (Time Zone) and system time (Adjust Your Time).
- (3) Click on the [OK] button and save the setting.
The status page (Current Network Setting) will be displayed shortly.

⚠ CAUTION
After this setting, make sure that the web browser has returned to the status page.
Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

3.IP Address Setting

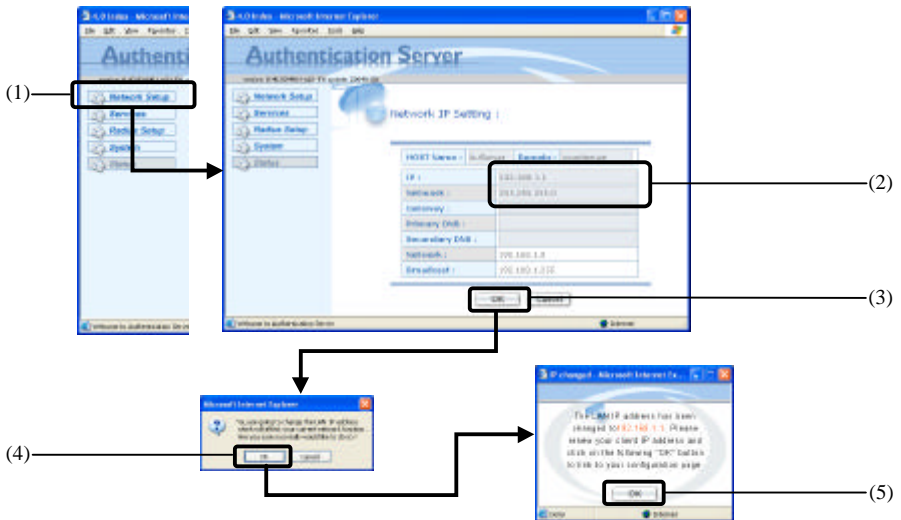


Figure 3.4. NETWORK Setup Screen

- (1) On the menu screen, click on the [Network Setup].
- (2) When network screen (Network IP Setting) is displayed, enter the IP address in [IP] and subnetmask in [Netmask].
- (3) Click on the [OK] button.
- (4) When asked whether to save network settings, click on the [OK] button to save the settings. Saving the settings restarts the main unit automatically.
- (5) Then a confirmation message appears, that lets you reconnect to the network using the renewed IP address. Click on the [OK] button. The web browser shows a post-login page.

4.Setting for the authenticator

Set the information of authenticator, authentication type, CA used for the CA.

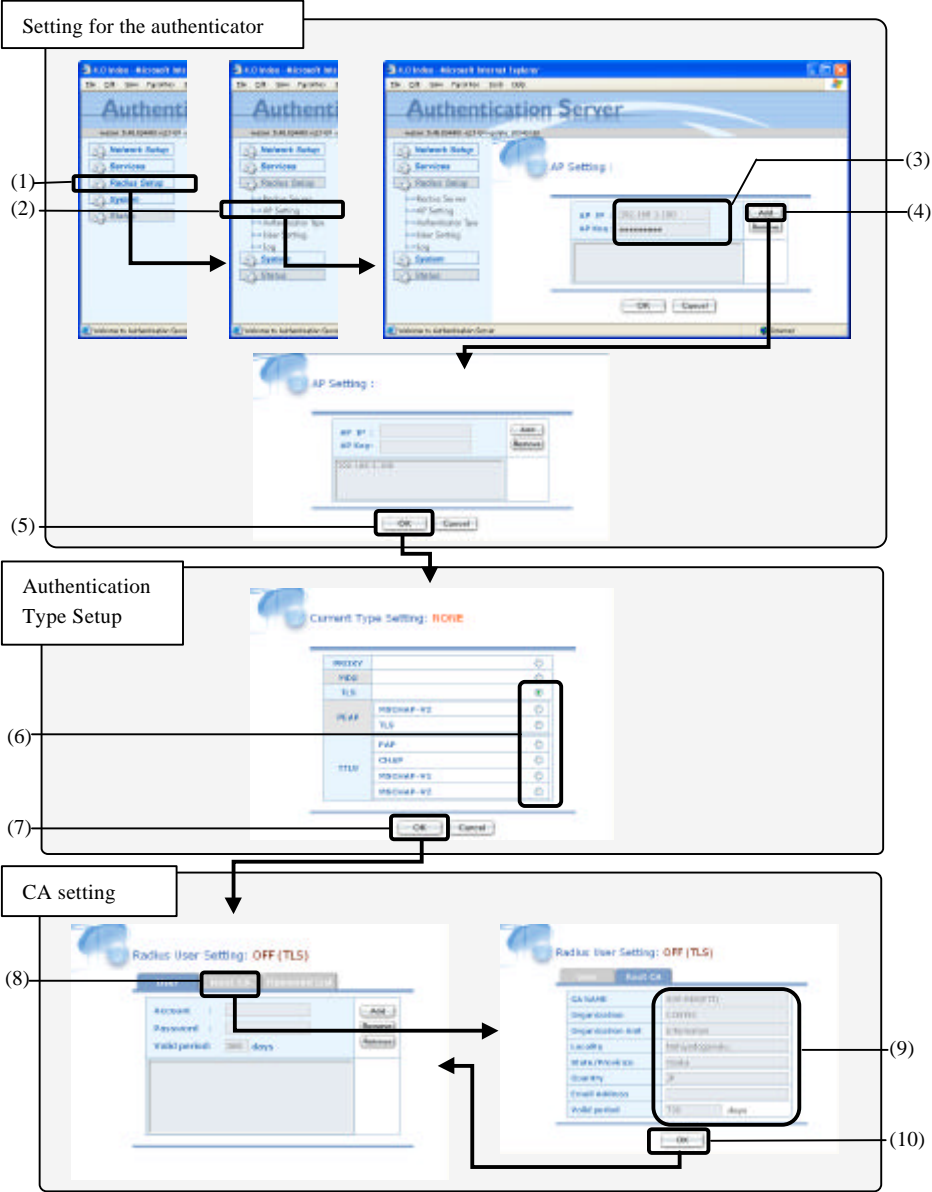


Figure 3.5. Authentication Server Setting Screen

4-1. Registering an authenticator

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [AP Setting].
- (3) Fill out the authenticator registration dialog box (AP Setting) that appears. Refer to the chapter3, “Setting Items” for the settings.

AP IP :	192.168.1.100	Add Remove
AP Key:	*****	

This step sets the following items.
 IP Address: [192.168.1.100]
 Shared Secret: [apkeypass]

Figure 3.6. Authenticator Setting Screen

- (4) Next, click on the [Add] button and save the setup information. Upon completion of saving, the registered IP address appears in the list.
- (5) Click on the [OK] button.

4-2. Authentication Type Setup

- (6) When the authentication type setting page (Current Type Setting) appears, select the type of authentication to be used from the list. Refer to chapter3, “Setting Items” on the Authentication Type. This time, [EAP-TLS] is selected.
- (7) Click on the [OK] button and save the setup information.

4-3. CA setting

- (8) When the setup screen of user information (Radius User Setting: User tab) is displayed, click on the [Root CA] tab.
- (9) Fill out the CA information setting dialog box (Radius User Setting: Root CA tab). Refer to the chapter3, “Setting Items” for the settings.

CA NAME	SVR-RDS(FIT)
Organization	CONTEC
Organization Unit	Information
Locality	Nishiyodogawaku
State/Province	Osaka
Country	JP
Email Address	
Valid period	730 days

This step sets the following items.
 CA Name: [SVR-RDS(FIT)]
 Organization: [CONTEC]
 Organization Unit: [Information]
 Locality: [Nishiyodogawaku]
 State/Province: [Osaka]
 Country: [JP]
 Email Address: Left blank
 Valid period: [730] days

Figure3.7. Radius CA Configuration

- (10) Click on the [OK] button and save the setup information. Saving will be completed after a while, displaying the user information setting dialog box.

⚠ CAUTION

After setting CA information, be sure to check that the web browser has returned to the user information setting dialog box. Turning the power off without returning to the user information setting dialog box may corrupt internal information, possibly causing a failure.

5.Starting the authentication server

Enable the authentication server.

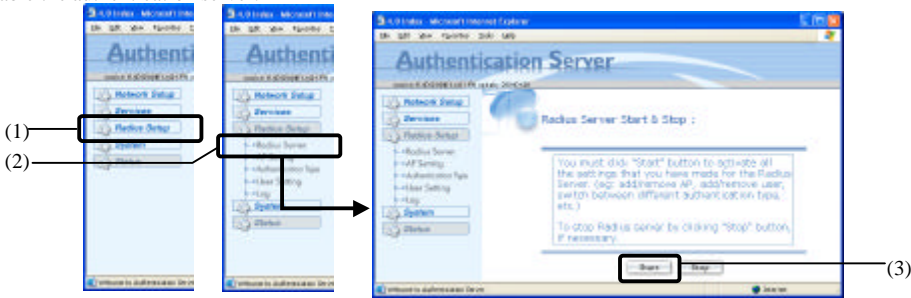


Figure 3.8. Authentication Server Start Up Screen

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [Radius Server].
- (3) Click on the [Start] button on the authentication server on/off page (Radius Server Start & Stop). The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

⚠ CAUTION

After this setting, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

6.Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.

⚠ CAUTION

- Once you have performed CA (certification authority) setup, do not attempt to set up the CA again unless it is required, for example, when the CA certificate has expired. An user certificate is paired with the CA certificate. Once the CA certificate is updated, therefore, authentication fails until the user certificate is reissued. If you open the CA certificate setup page (Root CA) after having set the CA, click on the [CANCEL] button immediately to dismiss the CA certificate setup page.
- The system time plays an important role, for example, when the validity term of each certificate is checked for authentication. If you unplug the power to the server unit and plug it again after setting the system time, check the system time again. The system timer remains battery-backed even while the server unit is off. The system time may not be retained correctly if the battery runs out.

Setting user information

This section describes how to issue the CA and user certificates required for IEEE 802.1X authentication.

Registering user information

(Authentication Type: EAP-TLS, PEAP(TLS))

If you have set the authentication type to EAP-TLS or PEAP(TLS) that use user certificates, take the following steps to set user information.

1.Login

- (1) Connect to the main body.

For the devices and cables used for connection, see “Setup Preparation” and “Setup Method”.

2.Registering an account and obtaining a certificate

Before setting an user account, be sure to check that the system time has been set correctly. The system time is referenced to define the validity term of each certificate to be issued and to check the validity term of each certificate used for authentication. Authentication cannot be performed normally unless the system time has been set correctly.

To set an user account, register the account and issue a CA certificate and an user certificate. The certificates issued here must be retained to be used in Chapter 5 “Setting for the supplicant”.

Once you have installed an issued user certificate, discard it or otherwise manage it confidentially to prevent a leak of secret information. The user certificate contains a private key for authentication. Security is lost if the user certificate is disclosed.

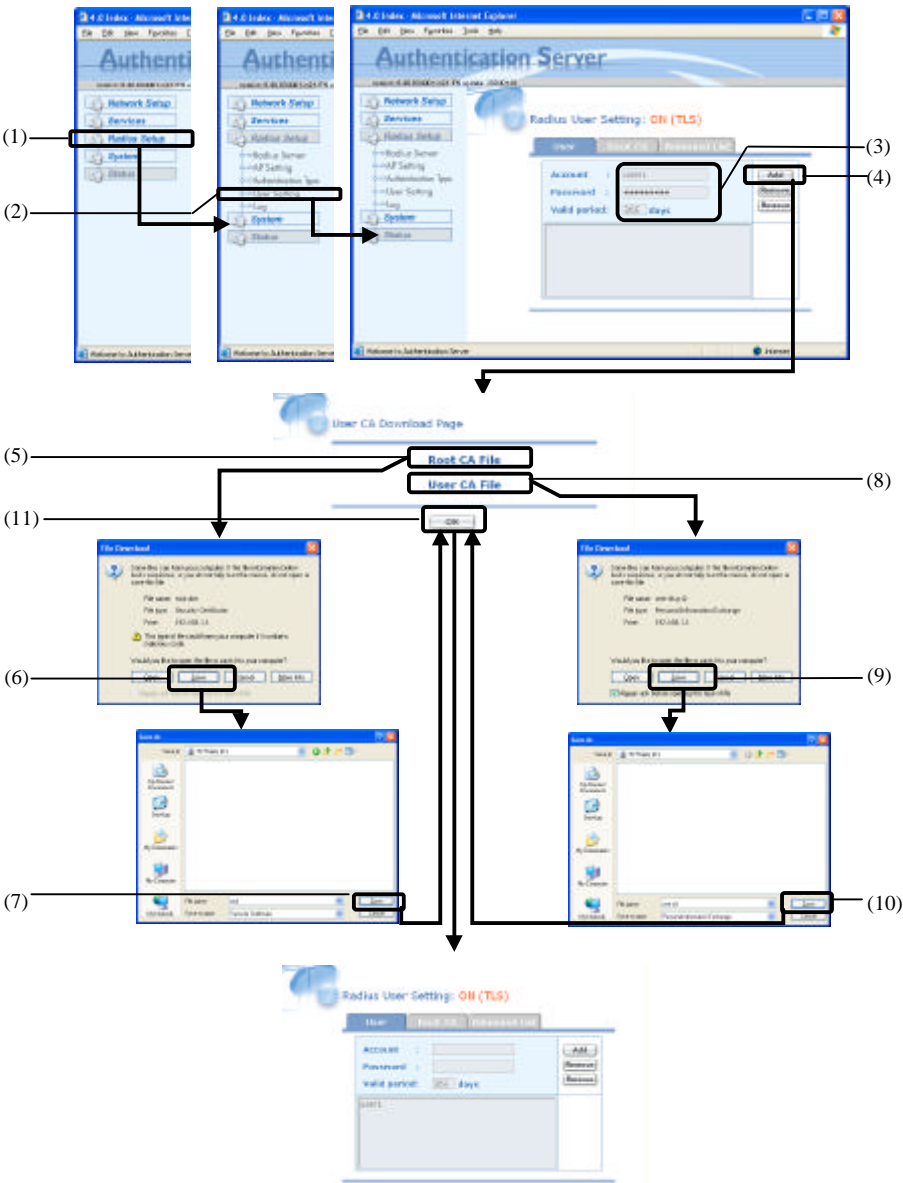


Figure 3.9. Authentication Server Setup Screen (EAP-TLS, PEAP(TLS))

2-1. Registering an user account

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [User Setting].
- (3) Fill out the user information setting dialog box (Radius User Setting: User tab). Manage the account and password not to be forgotten since they are required for installing the user certificate. Refer to chapter3, “Setting Items” for the setup.

This step sets the following items.

Account: [user1]

Password: [user1pass]

Valid period: [365] days

Figure 3.10. Authenticator Setup Screen

- (4) Click on the [Add] button to add the current settings.

2-2. Issuing the CA certificate

Issue (download) the CA certificate. The certificate issued here is used in Chapter 5 “Setting for the supplicant”.

- (5) Click on the [Root CA File] on the User CA Download Page.
- (6) The file download dialog box appears. Click on the [Save] button.
- (7) Specify the destination and file name to save the file to be downloaded and click on the [Save] button.
This example specifies the [root.der] as the file name.

2-3. Issuing the user certificate

Issue (download) the user certificate. The certificate issued here is used in Chapter 5 “Setting for the supplicant”.

- (8) Click on the [User CA File] on the User CA Download Page.
- (9) The file download dialog box appears. Click on the [Save] button.
- (10) Specify the destination and file name to save the file to be downloaded and click on the [Save] button.
This example specifies the [cert-clt.p12] as the file name.

2-4. Completing the issuance of the certificates

- (11) Click on the [OK] button on the User CA Download Page.
The user information setting dialog box (Radius User Setting: User tab) will then appear with the registered account name added to the list.

3. Validating user information

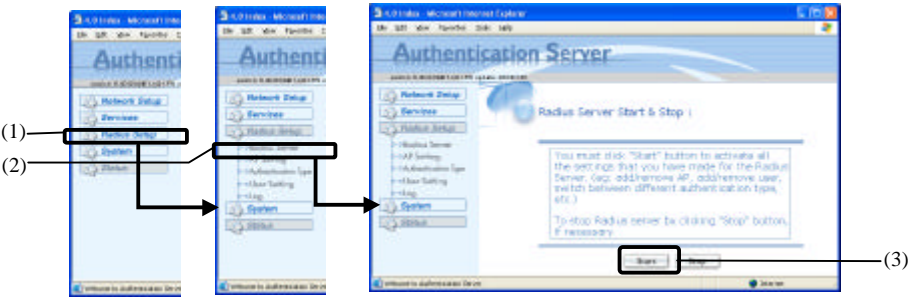


Figure 3.11. Authentication Server On/Off Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [Radius Server].
- (3) When the authentication server on/off page (Radius Server Start & Stop) is displayed, click on the [Start] button.
The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

⚠ CAUTION
After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

4. Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.

⚠ CAUTION
Once you have installed an issued user certificate, discard it or otherwise manage it confidentially to prevent a leak of secret information. The user certificate contains a private key for authentication. Security is lost if the user certificate is disclosed.

Registering user information

(Authentication Type: PEAP(MS CHAP-V2))

If you have set the authentication type to PEAP(MS CHAP-V2) that do not use user certificates, take the following steps to register user information.

1.Login

- (1) Connect to the main body.

For the devices and cables used for connection, see “Setup Preparation” and “Setup Method”.

2.Registering an account and obtaining a certificate

To set an user account, register the account and issue a CA certificate. The certificates issued here must be retained to be used in Chapter 5 “Setting for the supplicant”.

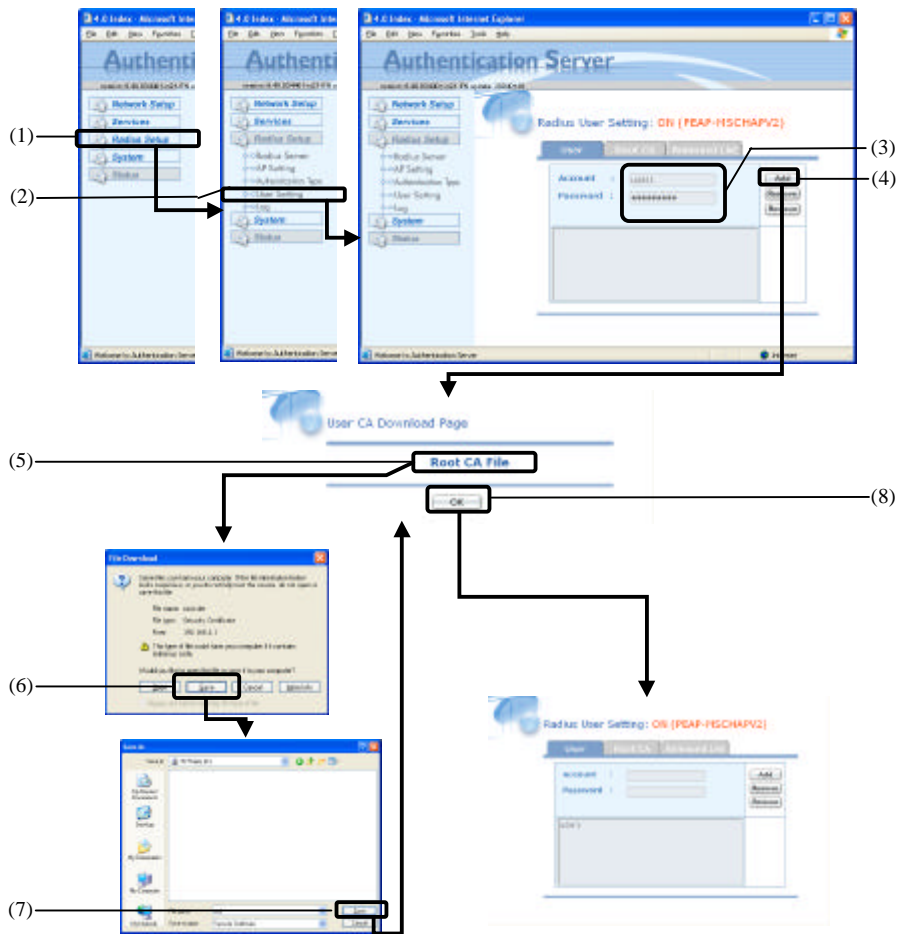


Figure 3.12. Authentication Server Setup Screen (PEAP(MS CHAP-V2))

2-1. Registering an user account

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [User Setting].
- (3) Fill out the user information setting dialog box (Radius User Setting: User tab). Manage the account and password not to be forgotten since they are required for installing the user certificate. Refer to chapter3, “Setting items” on the setup.

This step sets the following items.

Account: [user1]

Password: [user1pass]

Figure 3.13. Authenticator Setup Screen

- (4) Click on the [Add] button to add the current settings.

2-2. Issuing the CA certificate

Issue (download) the CA certificate. The certificate issued here is used in Chapter 5 “Setting for the supplicant”.

- (5) Click on the [Root CA File] on the User CA Download Page.
- (6) The file download dialog box appears. Click on the [Save] button.
- (7) Specify the destination and file name to save the file to be downloaded and click on the [Save] button.

This example specifies the [root.der] as the file name.

2-3. Completing the issuance of the certificates

- (8) Click on the [OK] button on the User CA Download Page.
The user information setting dialog box (Radius User Setting: User tab) will then appear with the registered account name added to the list.

3. Validating user information

Make registered user information take effect.

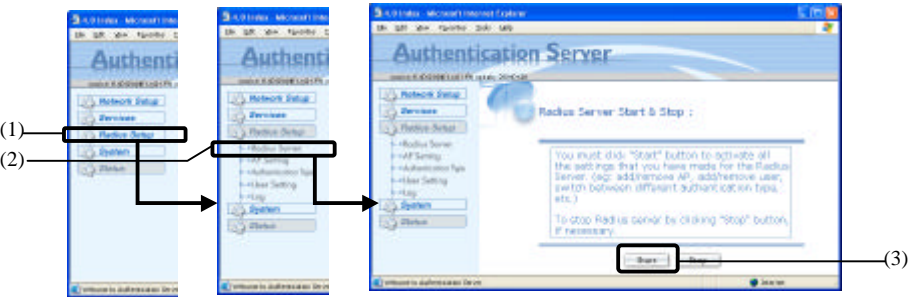


Figure 3.14. Authentication Server On/Off Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [Radius Server].
- (3) Click on the [Start] button on the authentication server on/off page (Radius Server Start & Stop). The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

⚠ CAUTION

After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

4. Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.

Registering user information again

(Authentication Type: EAP-TLS, PEAP(TLS))

A certificate can be reissued when it has expired.

If you have set the authentication type to EAP-TLS or PEAP(TLS) that use user certificates, take the following steps to register user information again.

1.Login

- (1) Connect to the main body.

For the devices and cables used for connection, see “Setup Preparation” and “Setup Method”.

2.Registering an account and obtaining a certificate again

To set an user account, register the account and issue a CA certificate. The certificates issued here must be retained to be used in Chapter 5 “Setting for the supplicant”.

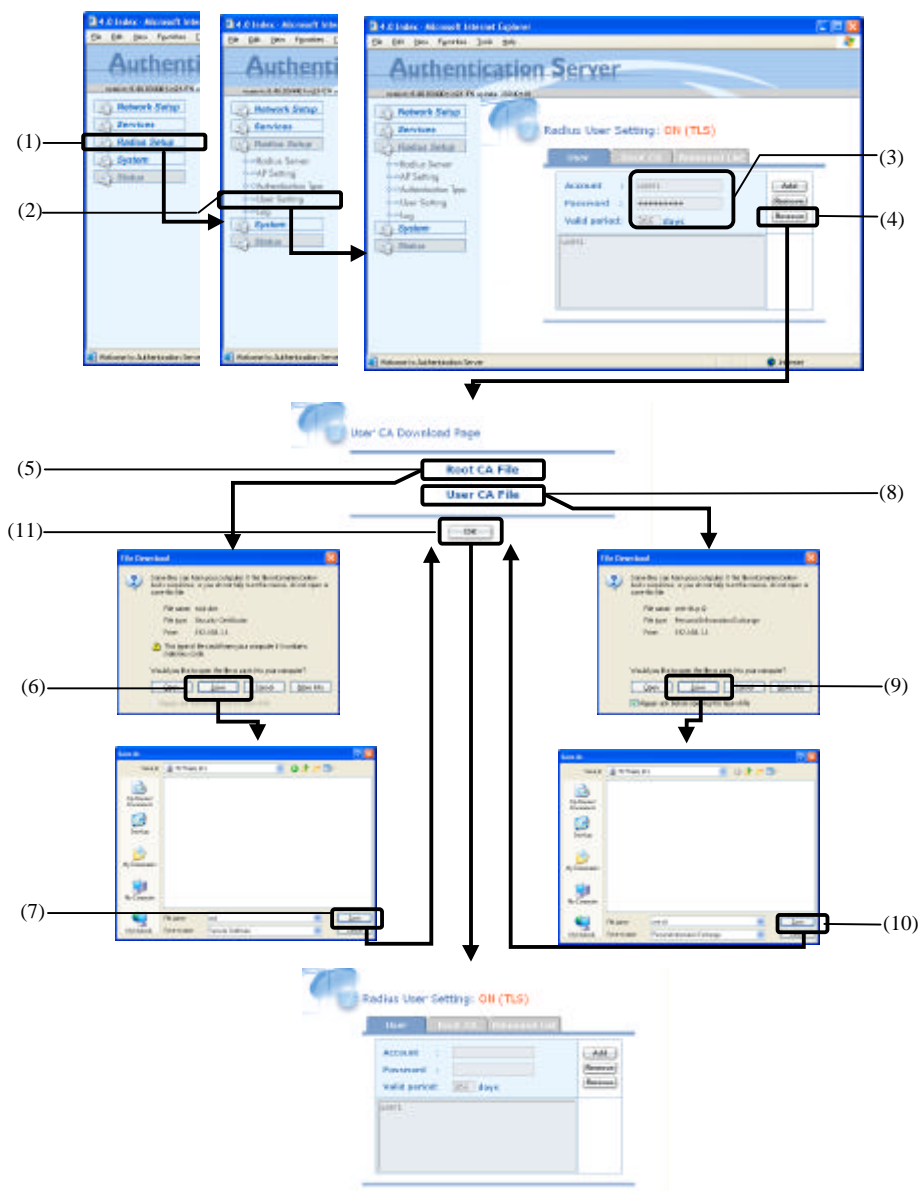


Figure 3.15. Authentication Server Reset Page (EAP-TLS, PEAP(TLS))

2-1. Registering user account again

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [User Setting].
- (3) Fill out the user information setting dialog box (Radius User Setting: User tab). Manage the account and password not to be forgotten since they are required for installing the user certificate. Refer to chapter3, “Setting Items” on the setup.

Account :	<input type="text" value="user1"/>	<input type="button" value="Add"/> <input type="button" value="Remove"/> <input type="button" value="Reissue"/>
Password :	<input type="password" value="*****"/>	
Valid period:	<input type="text" value="365"/> days	
<div>user1</div>		

This step sets the following items.

Account: [user1]
 Password: [user1pass]
 Valid period: [365] days

Figure 3.16. Authenticator Setup Screen

- (4) Click on the [Reissue] button to add the current settings.

2-2. Issuing the CA certificate

Issue (download) the CA certificate. The certificate issued here is used in Chapter 5 “Setting for the supplicant”.

- (5) Click on the [Root CA File] on the User CA Download Page.
- (6) The file download dialog box appears. Click on the [Save] button.
- (7) Specify the destination and file name to save the file to be downloaded and click on the [Save] button.

This example specifies the [root.der] as the file name.

2-3. Issuing the user certificate

Issue (download) the user certificate. The certificate issued here is used in Chapter 5 “Setting for the supplicant”.

- (8) Click on the [User CA File] on the User CA Download Page.
- (9) The file download dialog box appears. Click on the [Save] button.
- (10) Specify the destination and file name to save the file to be downloaded and click on the [Save] button.

This example specifies the [cert-clt.p12] as the file name.

2-4. Completing the issuance of the certificates

- (11) Click on the [OK] button on the User CA Download Page.
 The user information setting dialog box (Radius User Setting: User tab) will then appear with the registered account name added to the list.
- (12) Click on the [Start] button on the user information setting dialog box. The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.



CAUTION

After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

3. Validating user information

Make registered user information take effect.

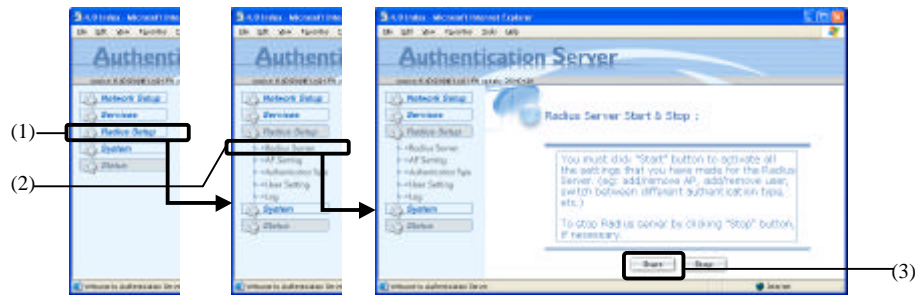


Figure 3.17. Authentication Server On/Off Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [Radius Server].
- (3) Click on the [Start] button on the authentication server on/off page (Radius Server Start & Stop). The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

⚠ CAUTION
After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

4. Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.

⚠ CAUTION
Once you have installed an issued user certificate, discard it or otherwise manage it confidentially to prevent a leak of secret information. The user certificate contains a private key for authentication. Security is lost if the user certificate is disclosed.

Registering user information again

(Authentication Type: PEAP(MS CHAP-V2))

A certificate can be reissued when it has expired.

If you have set the authentication type to PEAP(MS CHAPV2) that do not use user certificates, take the following steps to register user information again.

1.Login

- (1) Connect to the main body.

For the devices and cables used for connection, see “Setup Preparation” and “Setup Method”.

2.Registering an account and obtaining a certificate again

To set an user account, register the account and issue a CA certificate. The certificates issued here must be retained to be used in Chapter 5 “Setting for the supplicant”.

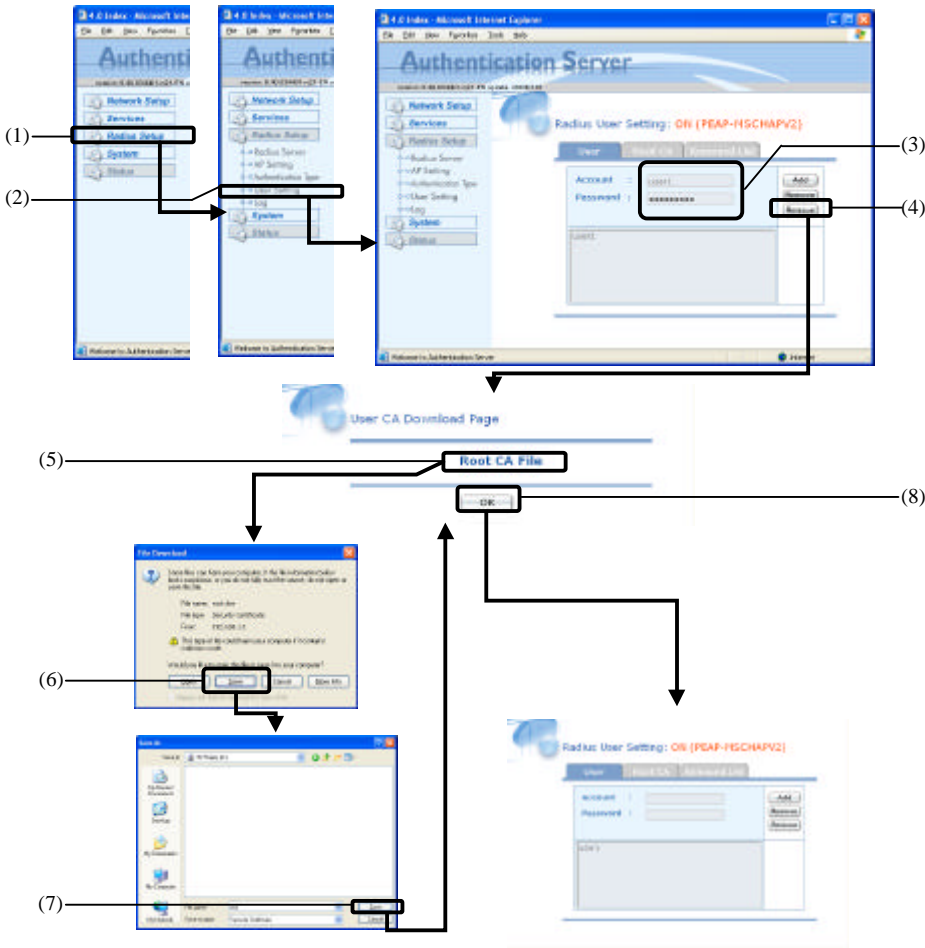


Figure 3.18. Authentication Server Reset Page (PEAP(MS CHAP-V2))

2-1. Registering an user account

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [User Setting].
- (3) Fill out the user information setting dialog box (Radius User Setting: User tab). Manage the account and password not to be forgotten since they are required for installing the user certificate. Refer to chapter3, “Setting Items” on the setup.

This step sets the following items.

Account: [user1]

Password: [user1pass]

Figure 3.19. Authenticator Setup Screen

- (4) Click on the [Reissue] button to add the current settings.

2-2. Issuing the CA certificate

Issue (download) the CA certificate. The certificate issued here is used in Chapter 5 “Setting for the supplicant”.

- (5) Click on the [Root CA File] on the User CA Download Page.
- (6) The file download dialog box appears. Click on the [Save] button.
- (7) Specify the destination and file name to save the file to be downloaded and click on the [Save] button.

This example specifies the [root.der] as the file name.

2-3. Completing the issuance of the certificates

- (8) Click on the [OK] button on the User CA Download Page.
The user information setting dialog box (Radius User Setting: User tab) will then appear with the registered account name added to the list.

3.Validating user information

Make registered user information take effect.

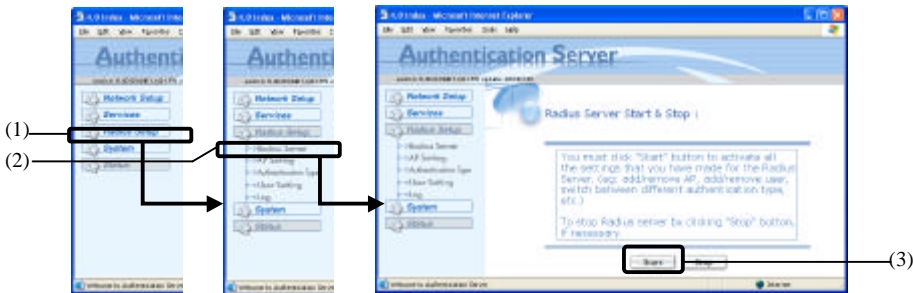


Figure 3.20. Authentication Server On/Off Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [Radius Server].
- (3) Click on the [Start] button on the authentication server on/off page (Radius Server Start & Stop). The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

⚠ CAUTION
After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

4.Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.

Deleting user information

Take the following steps to delete registered user information.

1.Login

- (1) Connect to the main body.

For the devices and cables used for connection, see “Setup Preparation” and “Setup Method”.

2.Deleting an account

You can unregister an user account by deleting it.

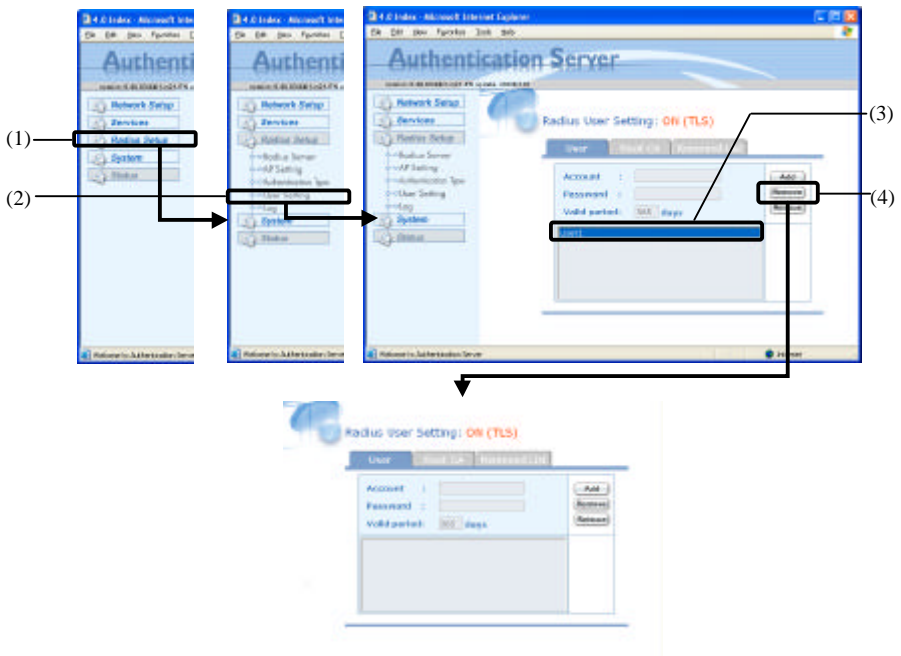


Figure 3.21. Account Deleting Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [User Setting].
- (3) In the user information dialog box (Radius User Setting) that appears, select the user account to be deleted from the list.
- (4) Next, Click on the [Remove] button and delete the information.
Upon completion of deleting, the list is updated with the selected user account deleted.

3.Validating user information

Make registered user information take effect.

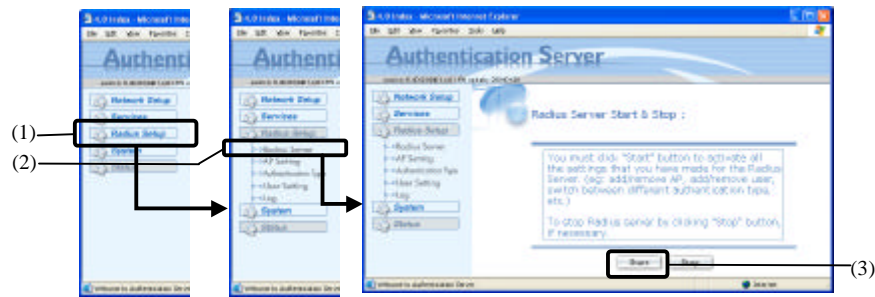


Figure 3.22. Authentication Server On/Off Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [Radius Server].
- (3) Click on the [Start] button on the authentication server on/off page (Radius Server Start & Stop). The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

CAUTION

After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

4.Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.



CAUTION

Once deleted, an account name can no longer be used for registration.

Adding or removing an authenticator

Take the following steps to add or remove an authenticator.

Adding an authenticator

1.Login

- (1) Connect to the main body.
For the devices and cables used for connection, see “Setup Preparation” and “Setup Method”.

2.Adding an authenticator

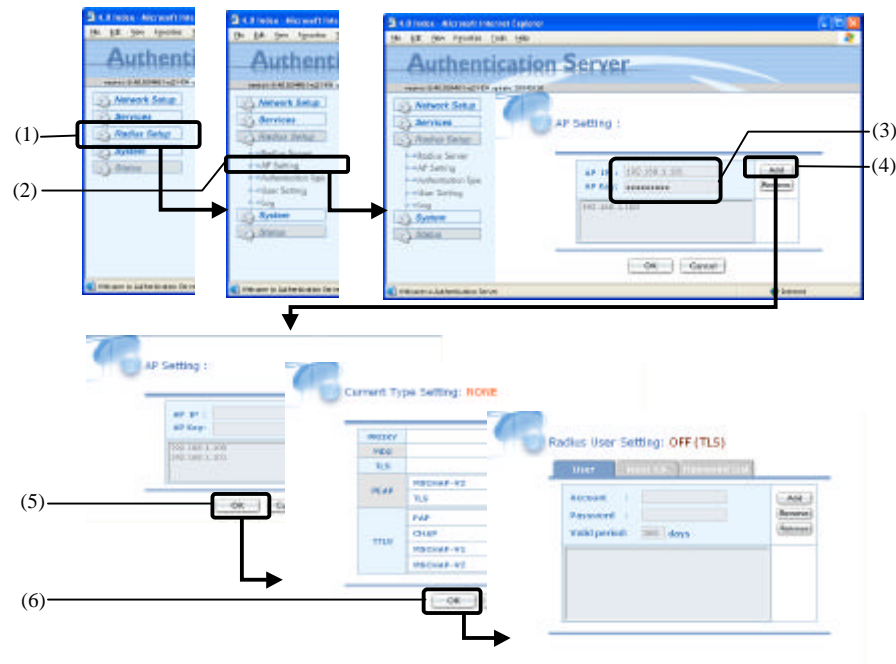
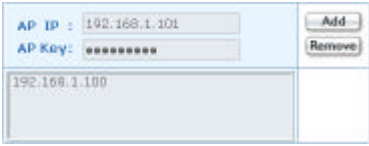


Figure 3.23. Authenticator Adding Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [AP Setting].
- (3) Fill out the authenticator registration dialog box (AP Setting) that appears. Refer to chapter3, “Setting Items” on the setup.



This step sets the following items.
IP Address: [192.168.1.101]
Shared Secret: [apkeypass]

Figure 3.24. Authenticator Setup Screen

- (4) Next, click on the [Add] button and save the setup information. Upon completion of saving, the registered IP address appears in the list.
- (5) Click on the [OK] button.
- (6) When the authentication type setting dialog box (Current Type Setting) is displayed, click on the [OK] button.
- (7) When the user information setting dialog box (Radius User Setting: User tab) is displayed, click on the [Start] button. The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.



CAUTION

After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

3. Validating user information

Make registered user information take effect.

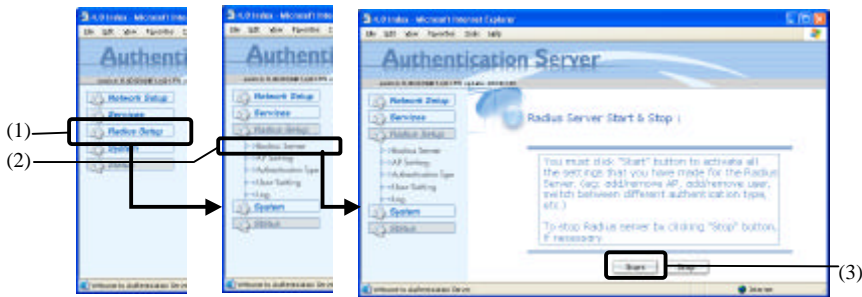


Figure 3.25. Authentication Server On/Off Page

- (1) Click on the [Radius Setup] on the menu screen,
- (2) Next, click on the [Radius Server].
- (3) Click on the [Start] button on the authentication server on/off page (Radius Server Start & Stop). The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

⚠ CAUTION
After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

4. Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.

Deleting an authenticator

1.Login

- (1) Connect to the main body.
See “Setup Method” for details.

2.Deleting an authenticator

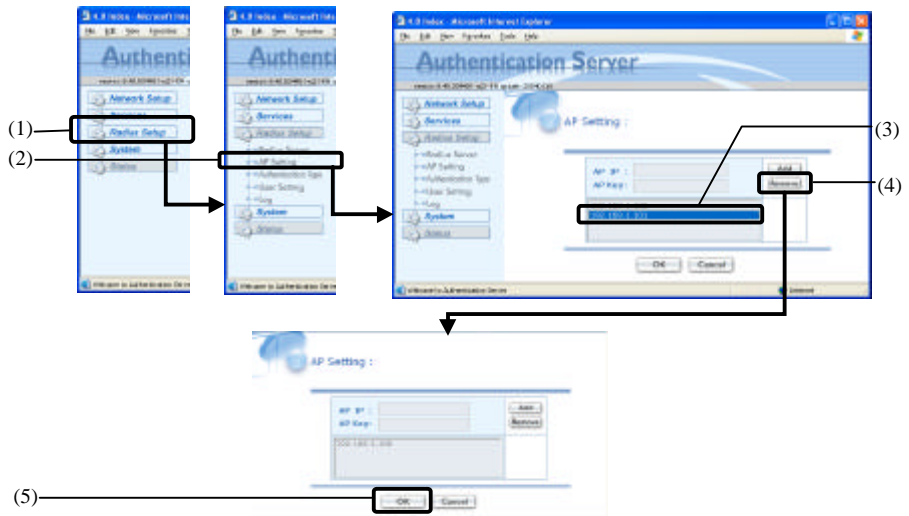


Figure 3.26. Authenticator Deleting Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [AP Setting].
- (3) When the authenticator registration page (AP Setting) appears, select the authenticator to be deleted from the list.
- (4) Click on the [Remove] button and delete the information.
Upon completion of saving, the list is updated with the selected IP address deleted.
- (5) Click on the [OK] button.

3.Validating user information

Make registered user information take effect.

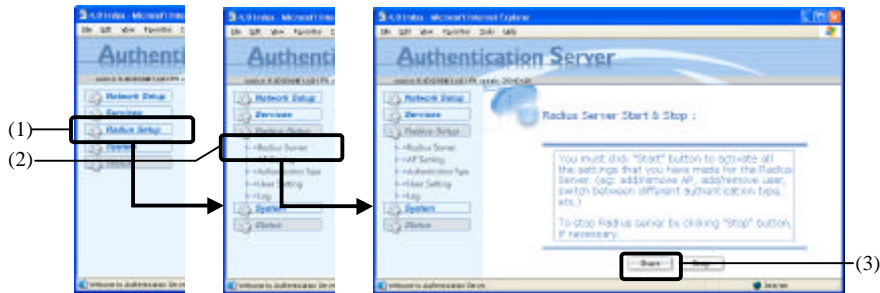


Figure 3.27. Authentication Server On/Off Page

- (1) Click on the [Radius Setup] on the menu screen.
- (2) Next, click on the [Radius Server].
- (3) Click on the [Start] button on the authentication server on/off page (Radius Server Start & Stop). The web browser changes to the status page (Current Network Setting) after a while, indicating that the new settings have taken effect.

⚠ CAUTION

After clicking on the [Start] button, make sure that the web browser has returned to the status page. Turning the power off without returning the web browser to the status page may corrupt internal information, possibly causing a fault.

4.Exiting Setup

- (1) Exit the web browser to disconnect the PC from the server unit.

Setting Items

Setting items are listed in the following table.

Table 3.1. Setting Items List

Setting Items		Setting	Remarks
Network Setup		O	Makes basic network settings. See "Basic Setup" for details.
Services	Set Time	O	Sets the system time. See "Setting the system time" for details.
	Network Time Adjustment	O	Sets NTP clients. See "NTP clients Setup" for details.
Radius Setup	AP Setting		Registers authenticators. See "Authenticator Setup" for details.
	Authentication Type		Sets the Authentication Type. See "Authentication Type Setup" for details.
	User Setting	Root CA	Registers CA certificates. See "CA certificates" for details.
		User	Registers user accounts and issues certificates. See "User certificate" for details.
	Log		—
System	Reset		Resets the system to its factory defaults. See "Initial Setup" for details.
	Password		Sets password. See "Password Setting" for details.
	Upgrade		For details, refer to the document supplied with upgrade data.
	Backup		Backs up data. See "Backup" for details.
	Restore		Restores the backup of data. See "Restore" for details.
Status		O	Displays the current setting states. See "Status" for details.

O: Supported —: Unsupported



CAUTION

Some of the setting items are not supported by the server unit.
Do not select or set any of the unsupported items. Doing so may result in a fault.

Basic Setup

This section describes the setting items on the [Network Setup].

HOST Name :	AuServer	Domain :	yourdomain
IP :	192.168.1.1		
Netmask :	255.255.255.0		
Gateway :			
Primary DNS :			
Secondary DNS :			
Network :	192.168.1.0		
Broadcast :	192.168.1.255		

Figure 3.28. Basic Setup Screen

IP Address

Sets the IP address of the AP. The IP address and subnet mask are factory-set to “192.168.1.1” and “255.255.255.0”, respectively. Always set the IP address. When setting via a LAN using a browser running on the other PC, the network group of the PC must be the same as the network group of the main body.

Subnet mask(Netmask)

If using a subnet, specify the subnet mask.

Default gateway

Specify the IP address of the router for the network to which this product belongs.

This item can be omitted when no router exists.

DNS (Primary DNS/Secondary DNS)

Set the DNS server IP.

HOST Name

Naming the SVR-RDS(FIT) or SVR-RDS(FIT)L makes it easy to identify it on the network. The host name can be a string of up to 30 single-byte alphanumeric characters beginning with a letter.

Domain Name

Specify the Domain Name. You can enter a string of up to 30 single-byte alphanumeric characters.

CAUTION

Manage the set IP address not to be forgotten. If you forget the IP address, you cannot make changes to the settings for the server unit.

System time setting

This section describes the [Set Time] setting items on the [SERVICES] page.



Figure 3.29. System time setting screen

Time Zone

Set your locality. For Japan, for example, select “Tokyo”.

Adjust Your Time

Adjust your current day and time.

⚠ CAUTION

The system time plays an important role, for example, when the validity term of each certificate is checked for authentication. If you unplug the power to the server unit and plug it again after setting the system time, check the system time again. The system timer remains battery-backed even while the server unit is off. The system time may not be retained correctly if the battery runs out.

NTP clients Setup

This section describes the [Network Time Adjustment] setting items on the [SERVICES] page.



Figure 3.30. NTP clients Setup

NTP Server IP

Specify the NTP Server IP or host name. If specifying the host name, you can enter a string of up to 128 single-byte alphanumeric characters.

Enabling the NTP server (Enable)

Enter the NTP server.

Clicking on the [Enable] button makes in inquiry to the NTP server.

Disabling the NTP server (Diable)

Disable the NTP server.

Starting or stopping the authentication function

This section describes the [Radius Server] setting items on the [Radius Setting].

After setting an authenticator, authentication type, CA and user information, make the settings take effect.

Authenticator Setup

This section describes the [AP Setting] setting items on the [Radius Setting].

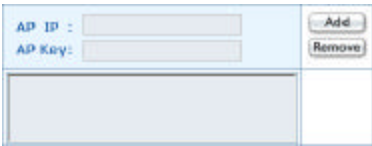
The image shows a web-based form for authenticator setup. It has a light blue header area with two input fields: 'AP IP : ' and 'AP Key: '. To the right of these fields are two buttons: 'Add' and 'Remove'. Below the input fields is a large, empty rectangular box, likely for a list of configured authenticators.

Figure 3.31. Authenticator Setup Screen

IP Address (AP IP)

Sets the IP address of the authenticator.

Shared secret (AP Key)

Set the shared secret value between the server unit and the authenticator. You can enter a string of up to 64 single-byte alphanumeric characters.

This setting must be identical to the IEEE 802.1X shared secret setting for the authenticator.

Authentication Type Setup

This section describes the [Authentication Type] setting items on the [Radius Setting].

PROXY		<input type="radio"/>
MD5		<input type="radio"/>
TLS		<input type="radio"/>
PEAP	MSCHAP-V2	<input type="radio"/>
	TLS	<input type="radio"/>
TTLS	PAP	<input type="radio"/>
	CHAP	<input type="radio"/>
	MSCHAP-V1	<input type="radio"/>
	MSCHAP-V2	<input type="radio"/>

Figure 3.32. Authentication Type Setup Screen

Authentication Type

Select the type of authentication to be used for IEEE 802.1X authentication.

Table 3.2. CA Setting Items

Setting Items		Setting
PROXY		—
MD5		—
TLS		O
PEAP	MS CHAP-V2	O
	TLS	O
TTLS	PAP	—
	CHAP	—
	MS CHAP-V1	—
	MS CHAP-V2	—

O: Supported —: Unsupported

CA certificate (Root CA)

This section describes the setting items accessible by selecting [Radius Setup], [User Setting], and the [Root CA] tab.

CA NAME	
Organization	
Organization Unit	
Locality	
State/Province	
Country	
Email Address	
Valid period	730 days

Figure 3.33. CA certificate (Root CA) Setup Screen

CA Name

Set the CA Name. You can enter a string of 2 to 60 single-byte alphanumeric characters which can include a hyphen “-”, underscore “_”, period “.”, and left and right parentheses “(” “)”.

Organization

Set the name of organization or business. You can enter a string of up to 64 single-byte alphanumeric characters.

Organization Unit

Set the Organization Unit. You can enter a string of up to 64 single-byte alphanumeric characters.

Locality

Set the Locality. You can enter a string of up to 128 single-byte alphanumeric characters.

State/Province

Set the State/Province. You can enter a string of up to 128 single-byte alphanumeric characters.

Country

Specify the country name. For Japan, for example, enter uppercase letters “JP”.

Email Address

Set the Email Address. You can enter a string of 60 single-byte alphanumeric characters which can include “-”, “_”, “.”, “@”.

Valid period

Set the CA Valid period. A number of up to 9999 is acceptable using single-byte numeric characters.

⚠ CAUTION

- Once you have performed CA (certification authority) setup, do not attempt to set up the CA again unless it is required, for example, when the CA certificate has expired. An user certificate is paired with the CA certificate. Once the CA certificate is updated, therefore, authentication fails until the user certificate is reissued. When the CA or user certificate is reissued, the old one is made invalid.
 - When the certificate expires, authentication fails, rejecting access to the network.
-

User information (User CA)

This section describes the setting items accessible by selecting [Radius Setting], [User Setting], and the [User] tab.

Figure 3.34. User information (Root CA) Setup Screen (EAP-TLS, PEAP(TLS))

Figure 3.35. User information (Root CA) Setup Screen (PEAP(MS CHAP-V2))

Account

Set the user account name. A number of up to 16 is acceptable using single-byte numeric characters, "-", "_".

The character string entered here is required when you install the user certificate on the PC.

Password

Set the password as the secret key for the account. A number of up to 16 is acceptable using single-byte numeric characters, "-", "_".

Valid period (Authentication Type: EAP-TLS, PEAP(TLS))

Set the CA Valid period. A number of up to 9999 is acceptable using single-byte numeric characters.

⚠ CAUTION

Manage the account and password not to be forgotten since they are required for installing a certificate on a supplicant or for connection to the network.

When the certificate expires, authentication fails, rejecting access to the network.

Initial Setup

This section describes the [Reset] setting items on the [System].

[RESET] resets the setting items to their defaults.

Password setting

This section describes the [Password] setting items on the [System].




Old Password :

New Password :

Re-Confirm New Password :

Figure 3.36. Password Setup Screen

Sets the password. You can enter a string of 1 to 8 single-byte alphanumeric characters. The default factory setting is [root].

 **CAUTION**

Manage the set password not to be forgotten. You cannot set up the authentication server if you forget the password.

Back up

This section describes the [Backup] items on the [System].



☐ Network

☐ Services

☐ Password

Figure 3.37. Backup Item Selectors

Back up information set for the system. The items of information selected by the check boxes will be backed up.

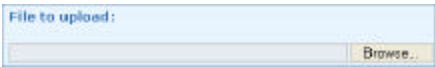
Refer to “Restore” to load the backup of information to the system.

Table 3.3. Backup Item List

Setting items	Description
Network	Backs up the items of Basic Setup (Network Setup, Services/Network Time Adjustment).
Services	Backs up the Radius Setup items.
Password	Backs up the System-Password items.

Restore

This section describes the [Restore] setting items on the [System].



File to upload:

Figure 3.38. Restore Data Selectors

Reload a backup of information to the system.

4. Setting for the authenticator

This chapter describes the items to be set with extra care when the SVR-RDS(FIT) or SVR-RDS(FIT)L is used in combination with an AP in the FLEXLAN DS540 series as an authenticator. For details on setting up the AP, refer to its manual.

Setting items (Setup using a web browser)

Wireless LAN

WEP function

Select this item to [Enable] to enable the IEEE 802.1X functions.

Enter an appropriate value (such as 64bit/1111111111) in [size/key #1] and select [#1] as the [default key].

IEEE802.1X

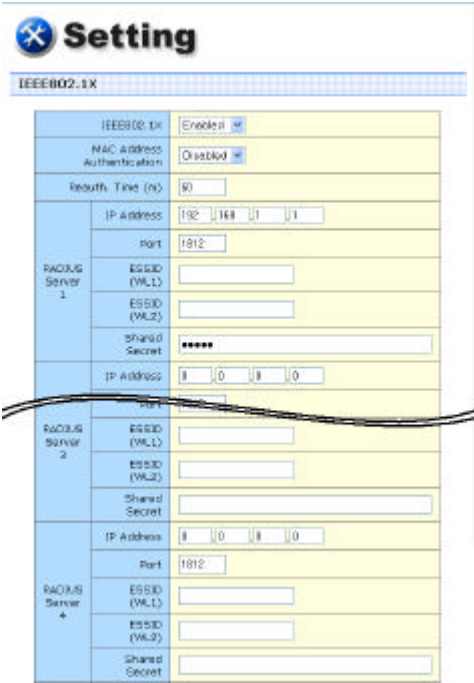


Figure 4.1. IEEE802.1X setting screen

The setup table may differ depending on the version of the AP.

IEEE802.1X function

Select this item to “Enable” to enable the IEEE 802.1X functions.

Re-authentication interval

Set the Re-authentication interval.

IP address

Set the IP address of the SVR-RDS(FIT)/SVR-RDS(FIT)L.

Port No.

Set “1812” as the port number of the server unit.

Shared Secret

Set the shared secret value between the server unit and the AP.

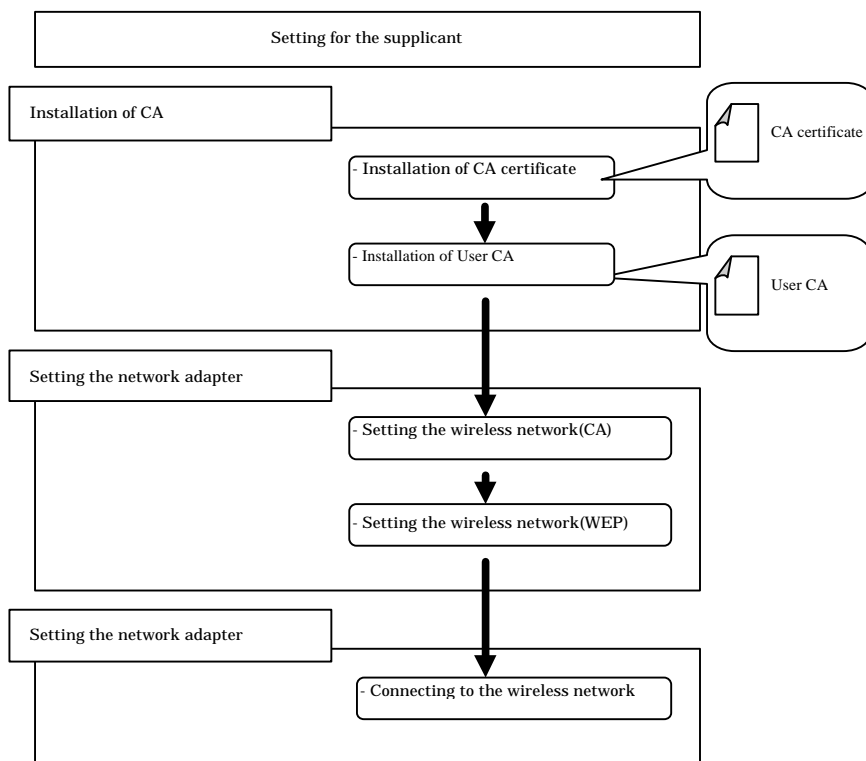
This setting must be identical to the “CA Setting” shared secret setting for the AP.

5. Setting for the supplicant

This chapter assumes the use of a wireless card (FX-DS540-PCC) in the FLEXLAN DS540 series as a supplicant used in combination with the SVR-RDS(FIT)/SVR-RDS(FIT)L. For details on setting up the PC, refer to the manual for the OS in use.

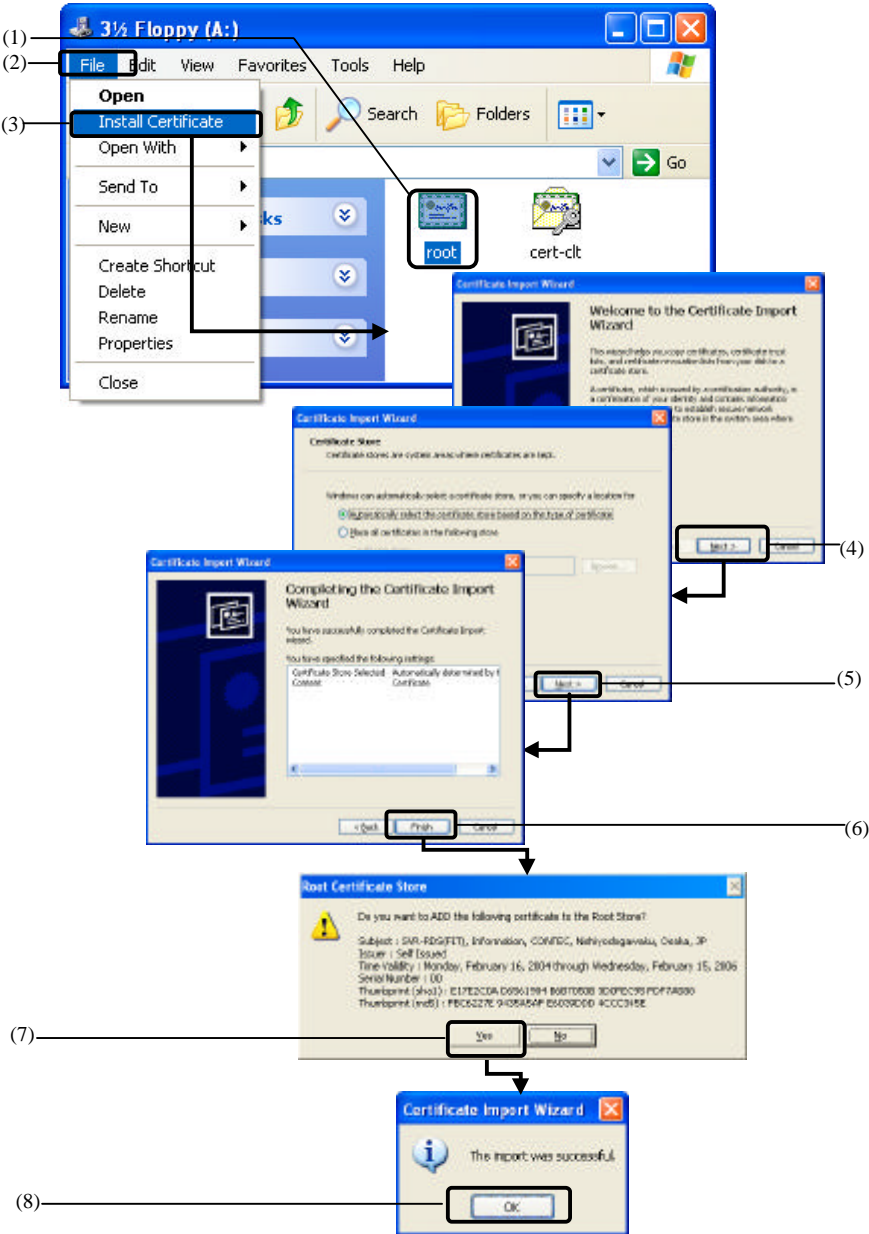
When using a single PC with other users, take into account the possibility of the use of a certificate by any other use sharing the PC.

Use under Windows XP SP1



Authentication Type: EAP-TLS

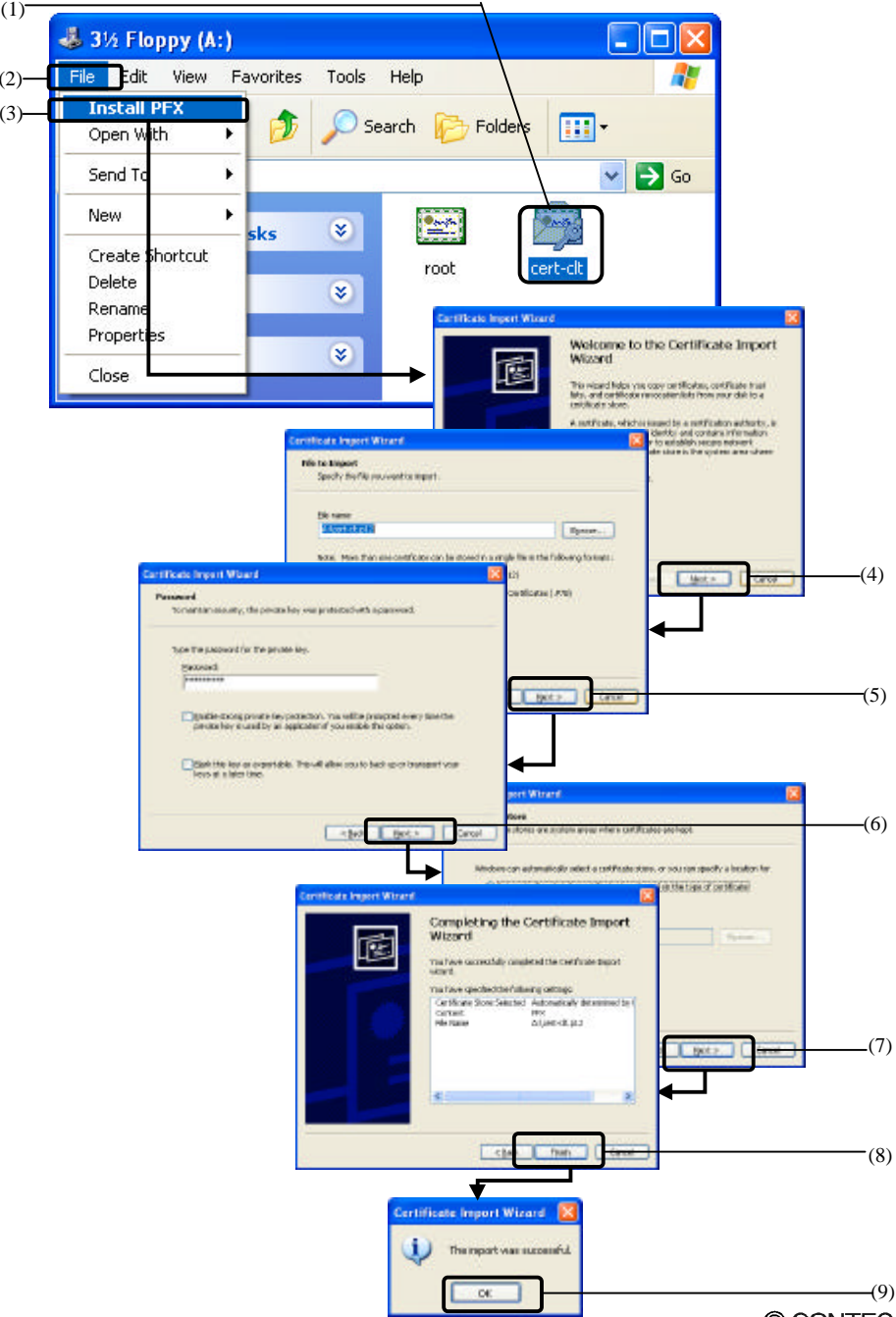
1.Installation of CA certificate



- (1) Select the CA certificate (root.der) issued by the server unit.
- (2) Select [File].
- (3) Select [Install Certificate] to start installing the CA certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button.
- (5) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (6) When [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (7) When the [Root Certificate Store] dialog box appears, click on the [Yes] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

The CA certificate has now been installed.

2.Installation of User CA



- (1) Select the user certificate (cert-clt.p12) issued by the server unit.
- (2) Select File].
- (3) Select Install PFX] to start installing the user certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the Next] button.
- (5) When the [File to Import] dialog box that appears, click on the Next] button.
- (6) When the [Password] dialog box appears, enter the [Password:] set when the user certificate was acquired, as the private key password, then click on the Next] button.
Usually, leave [Enable strong private key protection.] and [Mark this key as exportable.] unchecked.
- (7) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the Next] button.
- (8) When the [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (9) When the [Certificate Import Wizard] shows the message [The import was successful.], click on the [OK] button.

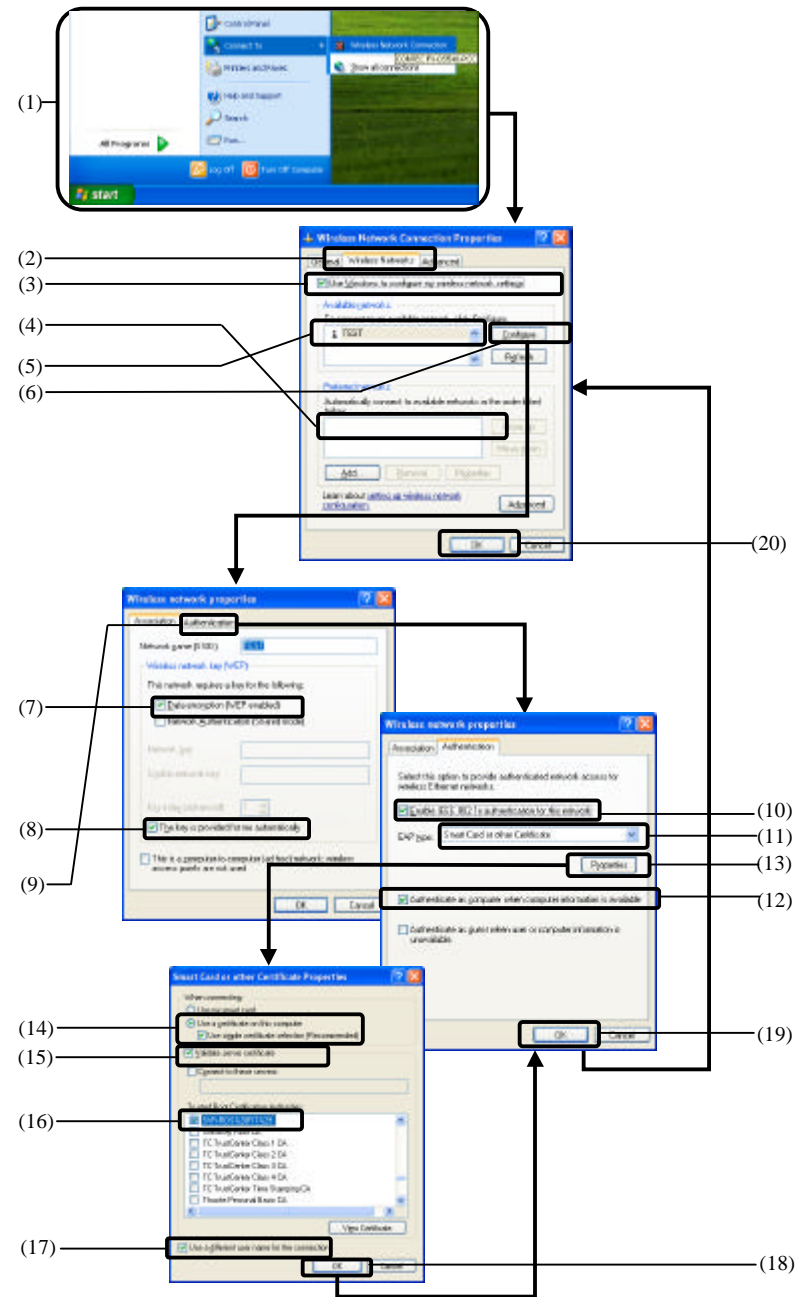
The user certificate has now been installed.



CAUTION

Once you have installed an issued user certificate, discard it or otherwise manage it confidentially to prevent a leak of secret information. The user certificate contains a private key for authentication. Security is lost if the user certificate is disclosed.

3.Setting the wireless network



3-1. Selecting the wireless network to connect to

- (1) Select a network card from [Wireless Network Connection] under [Connection].
- (2) When, the [Wireless Network Connection Properties] dialog box appears, select the [Wireless Networks] tab.
- (3) Check [Use Windows to configure my wireless network settings].
- (4) If the [Preferred networks:] list contains the ESSID of the desired authenticator, delete it.
- (5) Select the ESSID of authenticator from the [Available networks:].
- (6) Click on the [Configure] button.

3-2. Association tab setting

- (7) In the [Wireless network properties] dialog box, select the [Association] tab, check [Data encryption (WEP enabled)].
- (8) Check the [The key is provided for me automatically].
- (9) Click on the [Authentication] tab.

3-3. Authentication tab setting

- (10) Check the [Enable IEEE802.1X authentication for this network].
- (11) Select [Smart Card or other Certificate] in the [EAP type:] field.
- (12) Check the [Authenticate as computer when computer information is available]. Leave [Authenticate as guest when user or computer information is unavailable] unchecked.
- (13) Click on the [Properties] button.

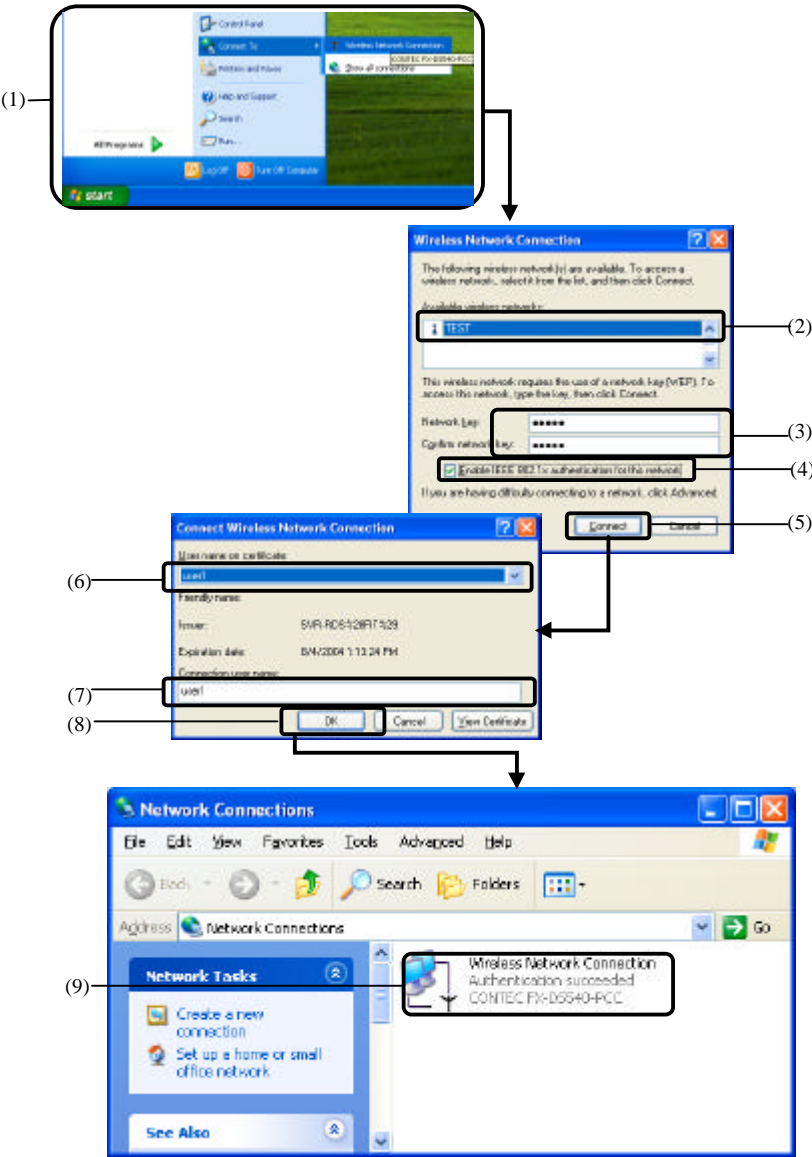
3-4. Selecting the CA certificate

- (14) In the [Smart Card or other Certificate Properties] dialog box, select [Use a certificate on this computer] and check [Use simple certificate selection (recommended)].
- (15) Check [Validate server certificate].
- (16) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (17) To use an account different from the user name entered to login to Windows, check [Use a different user name for the connection].
- (18) Click on the [OK] button.

3-5. Exiting Setup

- (19) In the [Wireless network properties] dialog box, click on the [OK] button.
- (20) In the [Wireless Network Connection Properties] dialog box, click on the [OK] button.

4.Connecting to the wireless network



4-1. Selecting the wireless network to connect to

- (1) Select a network card from [Wireless Network Connection] under [Connection].
- (2) When the [Wireless Network Connection] dialog box appears, select the wireless network to connect to from the [Available wireless networks:] list.
- (3) Enter an appropriate value (such as 11111) in [Network key:] and [Confirm network key]. The entered value is not used because the network key is distributed from the AP.
- (4) In Windows XP SP1, check [Enable IEEE 802.1X authentication for this network].
- (5) Then, click on the [Connect] button.

4-2. Selecting the user CA

- (6) When the [Connect Wireless Network Connection] dialog box appears, select the account name on the user certificate issued for the main unit from the [User name on certificate:].
- (7) Enter the same name as the user name on the certificate.
- (8) Click on the [OK] button.

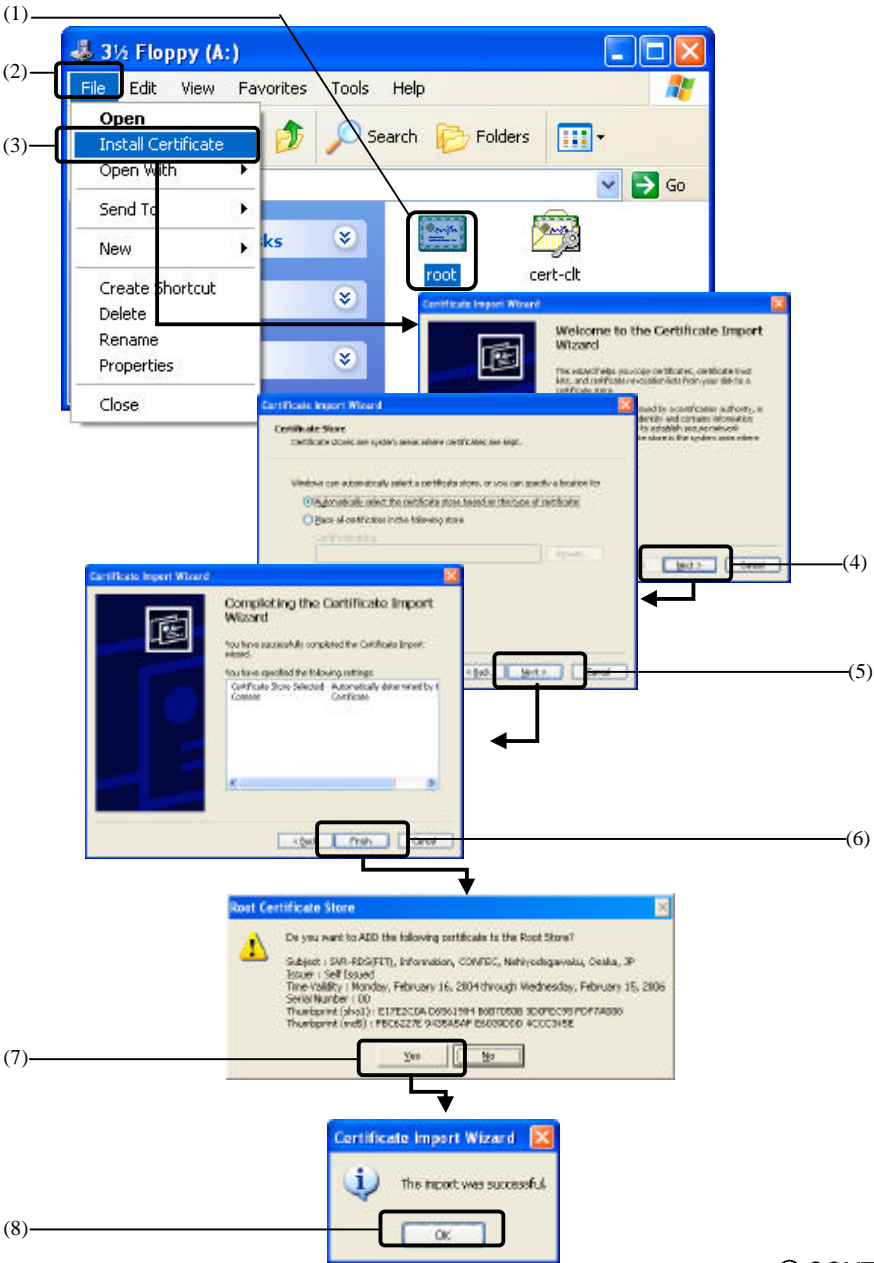
4-3. Successful authentication

- (9) You can confirm successful authentication by invoking [Network Connections] from the Control Panel and checking [Authentication succeeded] displayed under [Wireless Network Connection].

You have now finished connection to the wireless network, capable of accessing the network.

Authentication Type: PEAP(MS CHAP-V2)

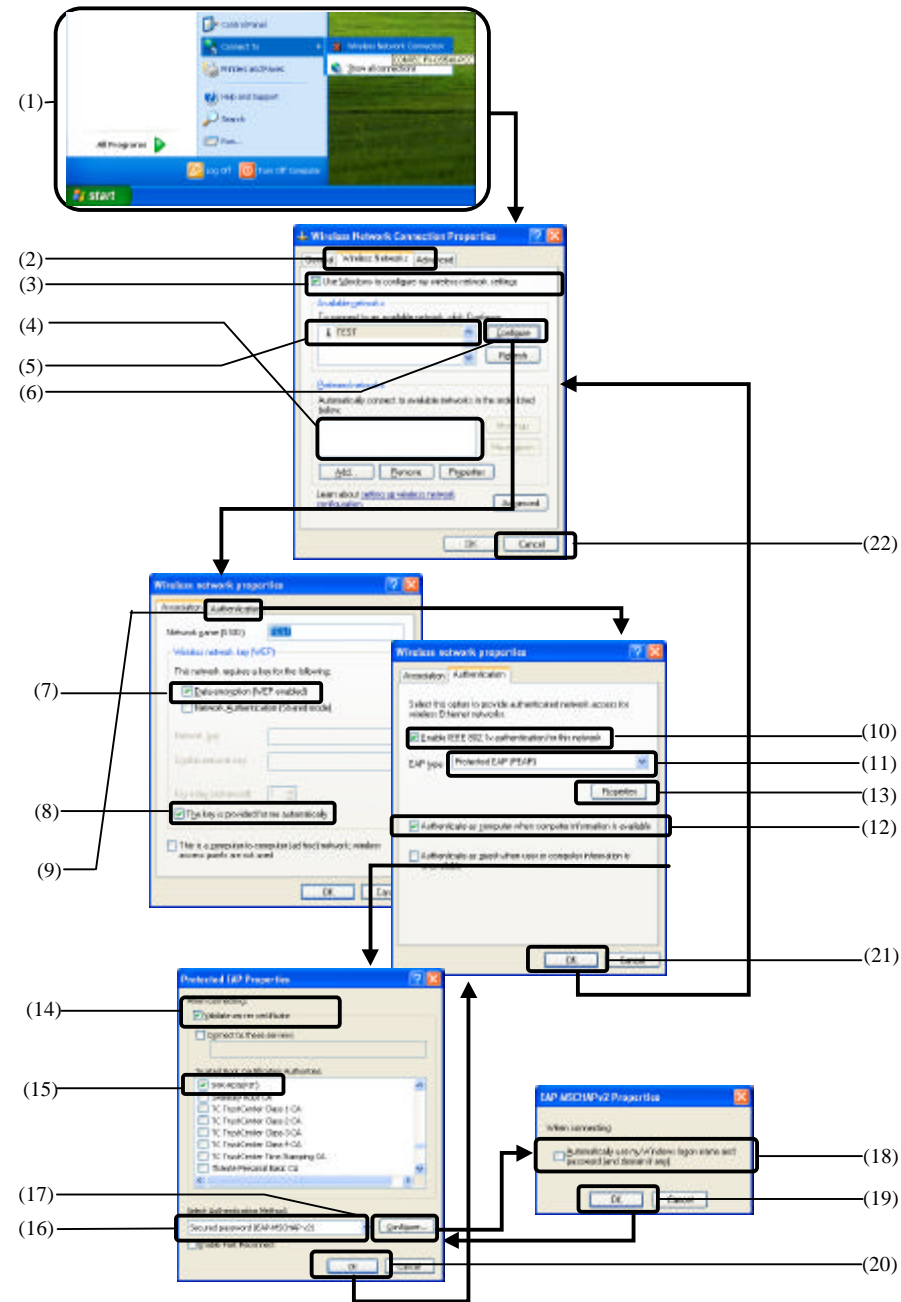
1.Installation of CA certificate



- (1) Select the CA certificate (root.der) issued by the server unit.
- (2) Select [File].
- (3) Select [Install Certificate] to start installing the CA certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button.
- (5) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (6) When [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (7) When the [Root Certificate Store] dialog box appears, click on the [Yes] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

The CA certificate has now been installed.

2.Setting the wireless network



2-1. Selecting the wireless network to connect to

- (1) Select a network card from [Wireless Network Connection] under [Connection].
- (2) When, the [Wireless Network Connection Properties] dialog box appears, select the [Wireless Networks] tab.
- (3) Check [Use Windows to configure my wireless network settings].
- (4) If the [Preferred networks:] list contains the ESSID of the desired authenticator, delete it.
- (5) Select the ESSID of authenticator from the [Available networks:].
- (6) Click on the [Configure] button.

2-2. Association tab setting

- (7) In the [Wireless network properties] dialog box, select the [Association] tab, check [Data encryption (WEP enabled)].
- (8) Check the [The key is provided for me automatically].
- (9) Click on the [Authentication] tab.

2-3. Authentication tab setting

- (10) Check the [Enable IEEE 802.1X authentication for this network].
- (11) Select [Protected EAP (PEA)] in the [EAP type:] field.
- (12) Check the [Authenticate as computer when computer information is available]. Leave [Authenticate as guest when user or computer information is unavailable] unchecked.
- (13) Click on the [Properties] button.

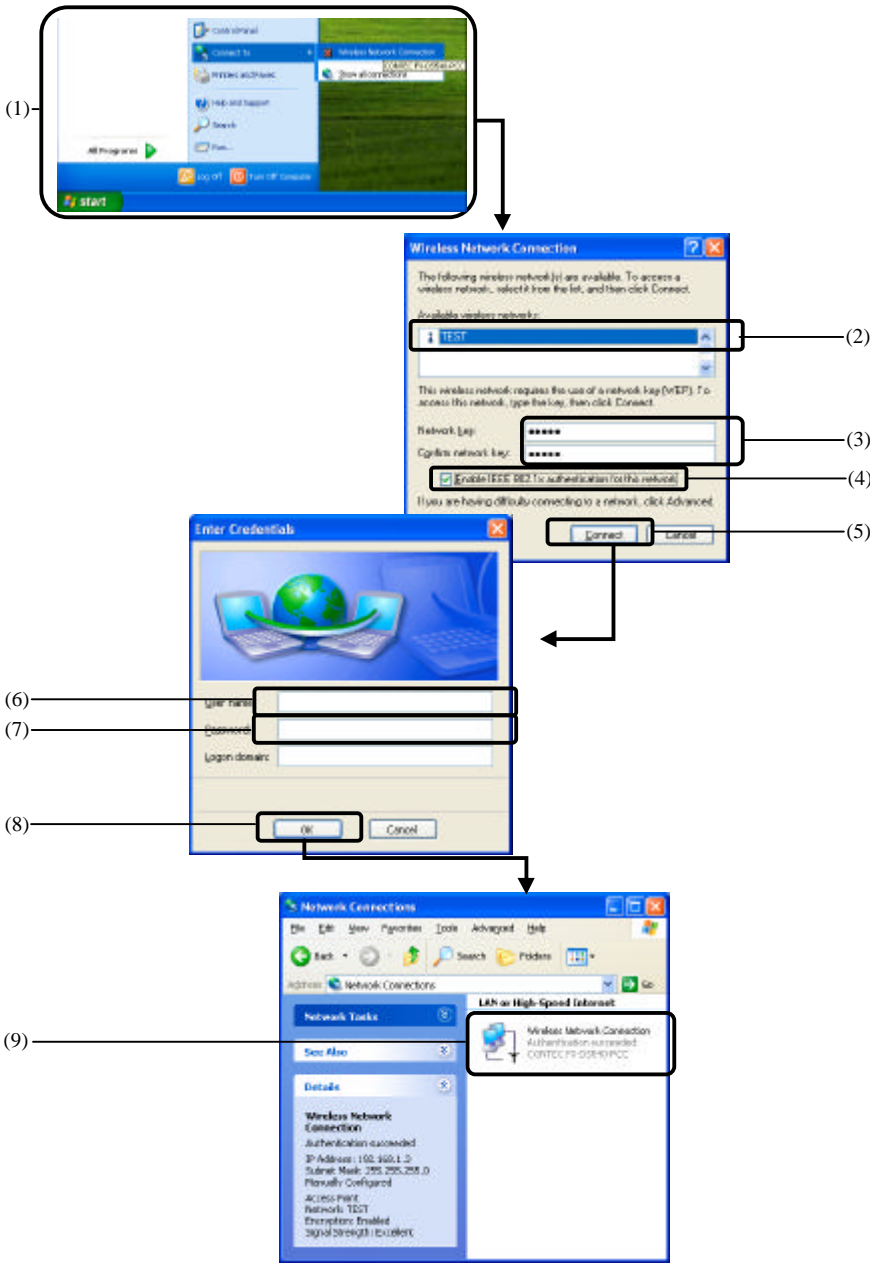
2-4. Selecting the CA certificate

- (14) In the [Protected EAP Properties] dialog box, check [Validate server certificate].
- (15) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (16) Select [Secured password (EAP-MSCHAPv2)] from [Select Authentication Method:].
- (17) Click on the [Configure] button.
- (18) [EAP MSCHAPv2 Properties] dialog box is displayed.
To use an account different from the user name entered to login to Windows, check [Automatically use my Windows logon name and password (and domain if any)].
- (19) Click on the [OK] button.

2-5. Exiting Setup

- (20) In the [Protected EAP Properties] dialog box, click on the [OK] button.
- (21) In the [Wireless network properties] dialog box, click on the [OK] button.
- (22) In the [Wireless Network Connection Properties] dialog box, click on the [OK] button.

3.Connecting to the wireless network



3-1. Selecting the wireless network to connect to

- (1) Select a network card from [Wireless Network Connection] under [Connection].
- (2) When the [Wireless Network Connection] dialog box appears, select the wireless network to connect to from the [Available wireless networks:] list.
- (3) Enter an appropriate value (such as 11111) in [Network key:] and [Confirm network key:]. The entered value is not used because the network key is distributed from the AP.
- (4) In Windows XP SP1, check [Enable IEEE 802.1X authentication for this network].
- (5) Then, click on the [Connect] button.

3-2. Entering qualification information

- (6) When the [Enter Credentials] dialog box appears, enter the account name set for the main unit in the [User name:] field.
- (7) In the [Password:] field, enter the password associated with the account set for the main unit.
- (8) Click on the [OK] button.

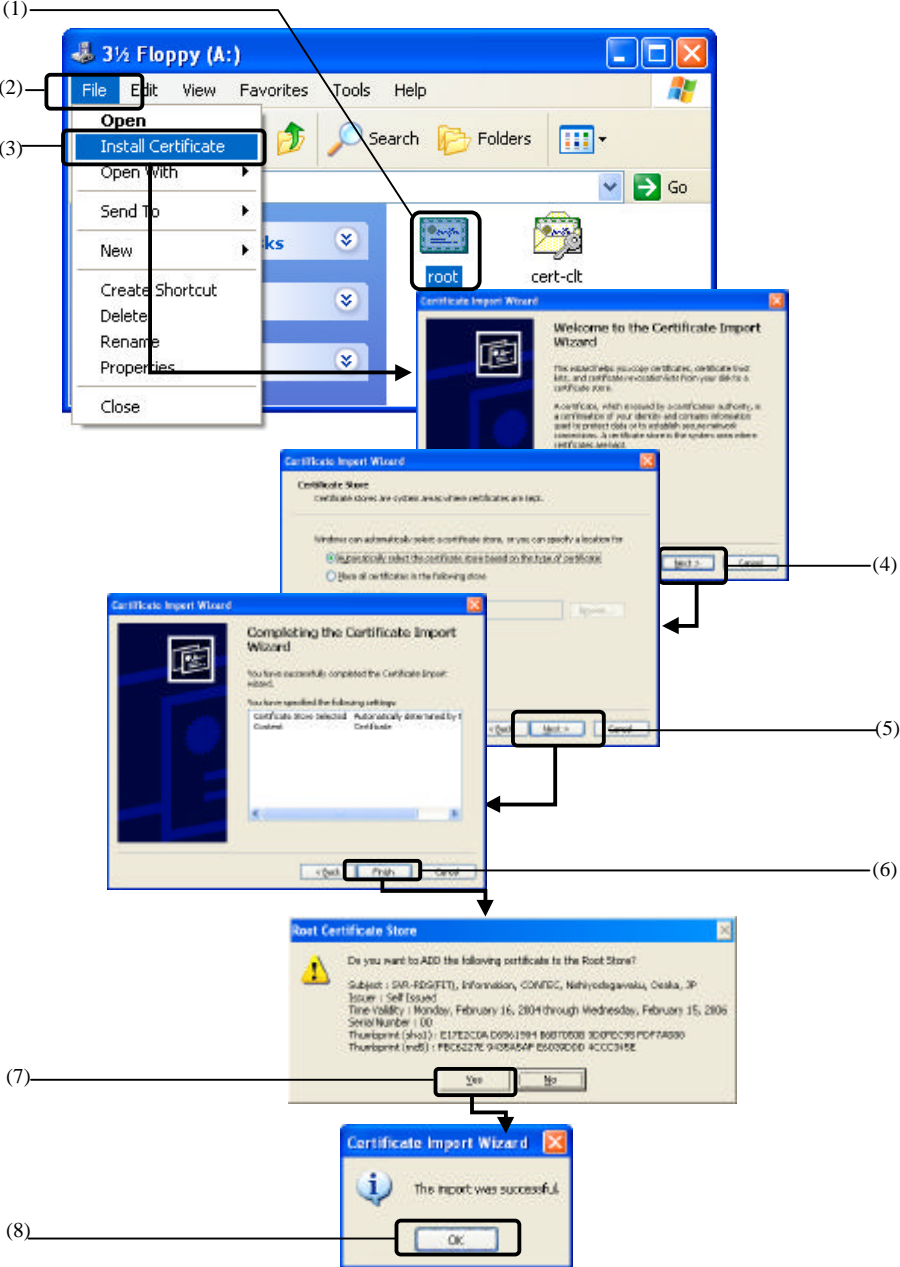
3-3. Successful authentication

- (9) You can confirm successful authentication by invoking [Network Connections] from the Control Panel and checking [Authentication succeeded] displayed under [Wireless Network Connection].

You have now finished connection to the wireless network, capable of accessing the network.

Authentication Type: PEAP(TLS)

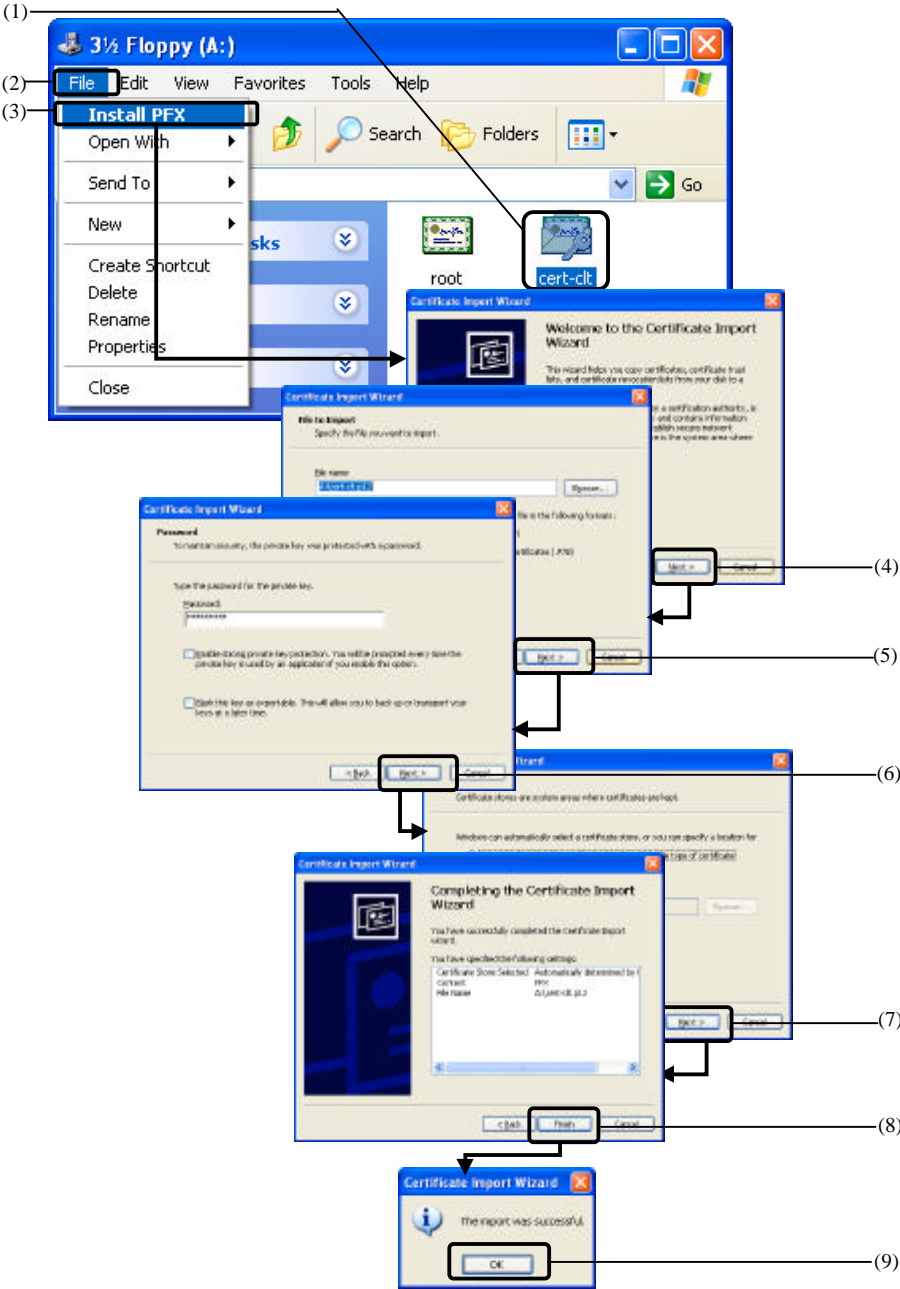
1.Installation of CA certificate



- (1) Select the CA certificate (root.der) issued by the server unit.
- (2) Select [File].
- (3) Select [Install Certificate] to start installing the CA certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button.
- (5) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (6) When [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (7) When the [Root Certificate Store] dialog box appears, click on the [Yes] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

The CA certificate has now been installed.

2.Installation of User CA



- (1) Select the user certificate (cert-clt.p12) issued by the server unit.
- (2) Select [File].
- (3) Select [Install PFX] to start installing the user certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button.
- (5) When the [File to import] dialog box that appears, click on the [Next] button.
- (6) When the [Password] dialog box appears, enter the [Password:] set when the user certificate was acquired, as the private key password, then click on the [Next] button.
Usually, leave [Enable strong private key protection.] and [Mark this key as exportable.] unchecked.
- (7) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (8) When the [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (9) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

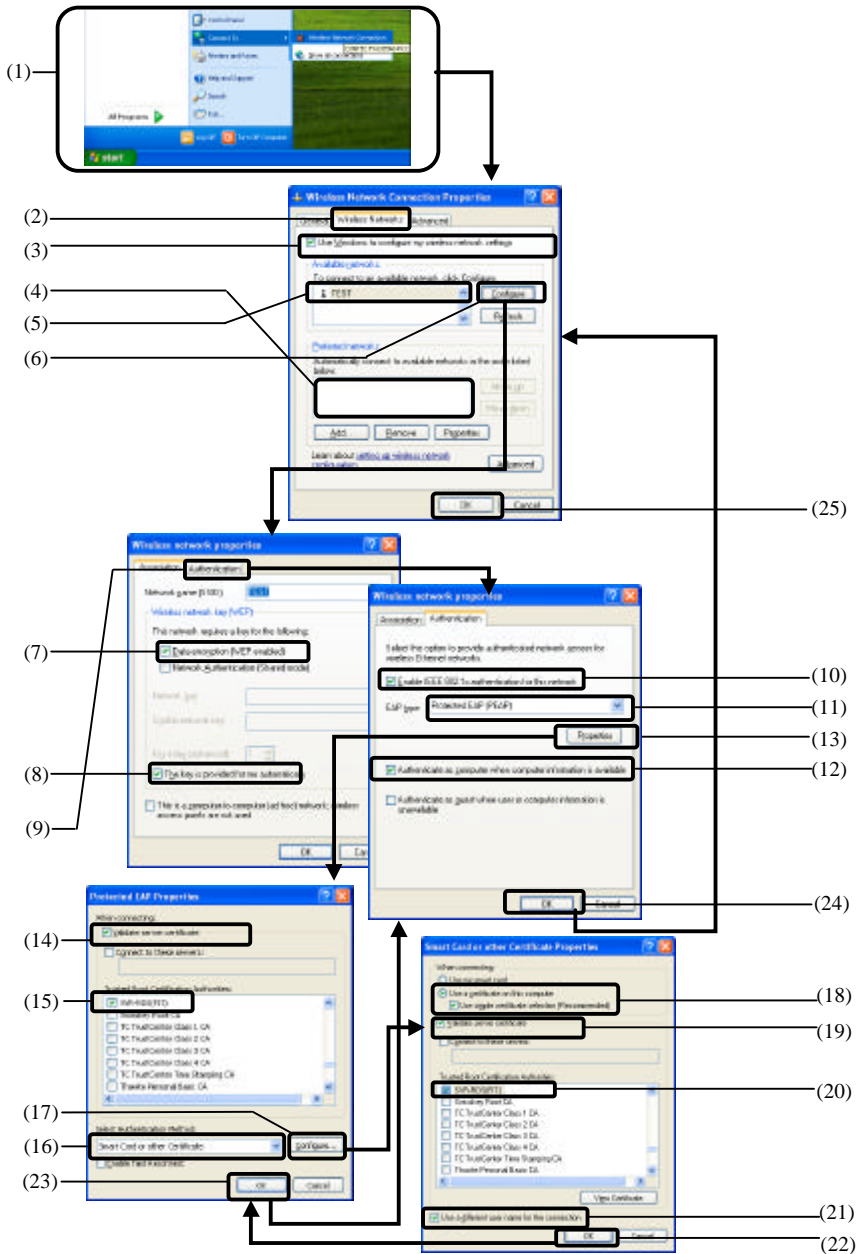
The user certificate has now been installed.



CAUTION

Once you have installed an issued user certificate, discard it or otherwise manage it confidentially to prevent a leak of secret information. The user certificate contains a private key for authentication. Security is lost if the user certificate is disclosed.

3.Setting the wireless network



3-1. Selecting the wireless network to connect to

- (1) Select a network card from [Wireless Network Connection] under [Connection].
- (2) When the [Wireless Network Connection Properties] dialog box appears, select the [Wireless Networks] tab.
- (3) Check [Use Windows to configure my wireless network settings].
- (4) If the [Preferred networks:] list contains the ESSID of the desired authenticator, delete it.
- (5) Select the ESSID of authenticator from the [Available networks:].
- (6) Click on the [Configure] button.

3-2. Association tab setting

- (7) In the [Wireless network properties] dialog box, select the [Association] tab, check [Deta encryption (WEP enabled)].
- (8) Check the [The key is provided for me automatically].
- (9) Click on the [Authentication] tab.

3-3. Authentication tab setting

- (10) Check the [Enable IEEE802.1X authentication for this network].
- (11) Select [Protected EAP (PEAP)] in the [EAP type:] field.
- (12) Check the [Authenticate as computer when computer information is available]. Leave [Authenticate as guest when user or computer information is unavailable] unchecked.
- (13) Click on the [Properties] button.

3-4. Selecting the CA certificate

- (14) Check [Validate Server Certificate].
- (15) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (16) In the [Smart Card or other Certificate Properties] dialog box, select [Use a certificate on this computer] and check [Use simple certificate selection (recommended)].
- (17) Click on the [Configure] button.

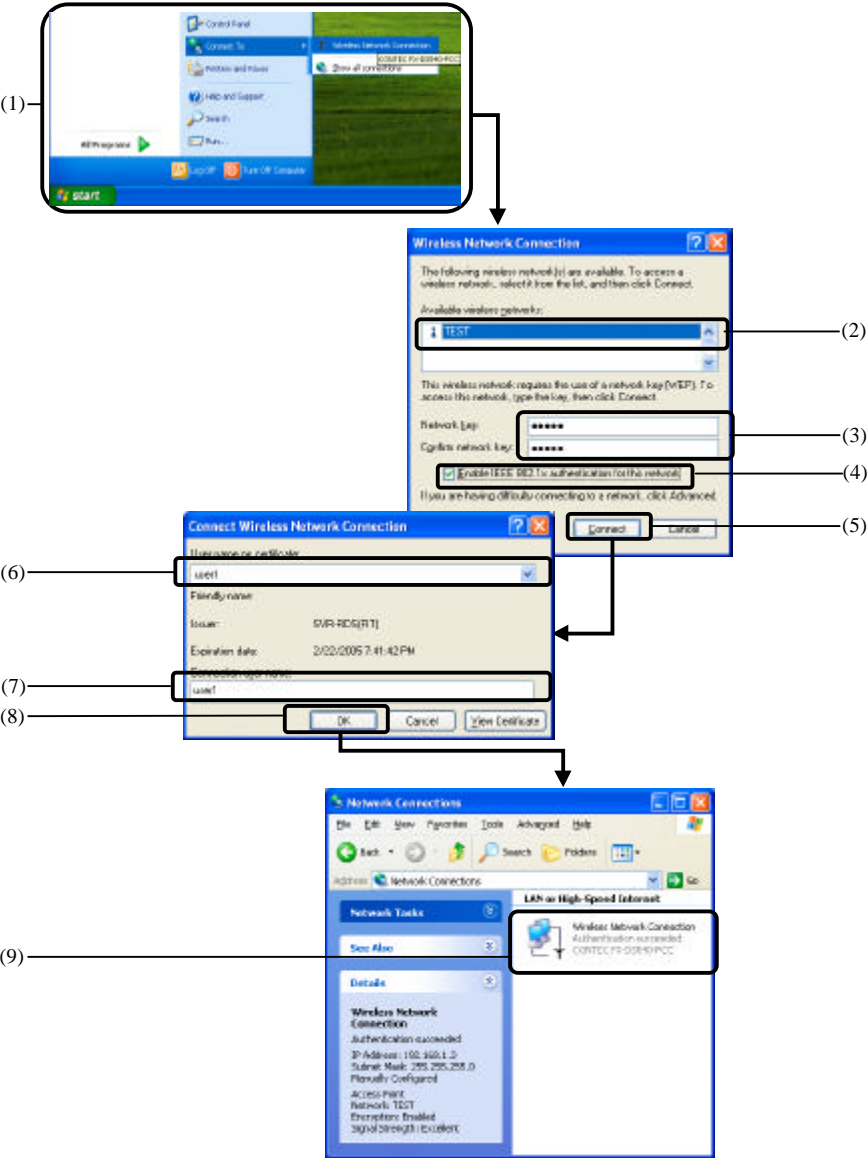
3-5. Selecting the CA certificate for TLS authentication

- (18) In the [Smart Card or other Certificate Properties] dialog box, select [Use a certificate on this computer] and check [Use simple certificate selection (Recommended)].
- (19) Check [Validate server certificate].
- (20) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (21) To use an account different from the user name entered to login to Windows, check [Use a different user name for this connection].
- (22) Click on the [OK] button.

3-6. Exiting Setup

- (23) In the [Protected EAP Properties] dialog box, click on the [OK] button.
- (24) In the [Wireless network properties] dialog box, click on the [OK] button.
- (25) In the [Wireless Network Connection Properties] dialog box, click on the [OK] button.

4.Connecting to the wireless network



4-1. Selecting the wireless network to connect to

- (1) Select a network card from [Wireless Network Connection] under [Connection].
- (2) When the [Wireless Network Connection] dialog box appears, select the wireless network to connect to from the [Available wireless networks:] list.
- (3) Enter an appropriate value (such as 11111) in [Network key:] and [Confirm network key:]. The entered value is not used because the network key is distributed from the AP.
- (4) In Windows XP SP1, check [Enable IEEE 802.1X authentication for this network].
- (5) Then, click on the [Connect] button.

4-2. Selecting the user CA

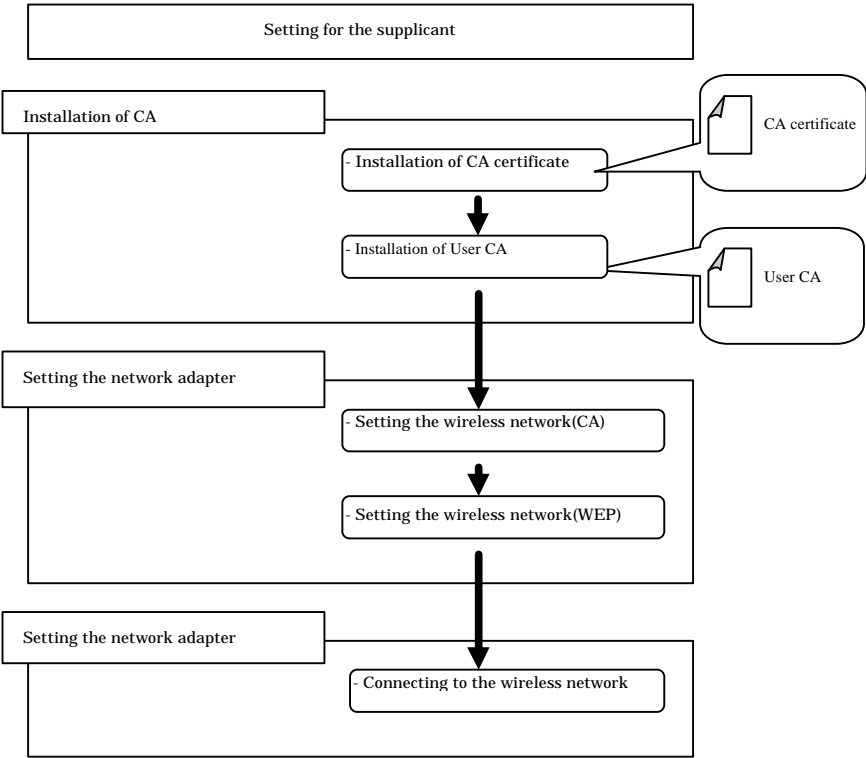
- (6) When the [Connect Wireless Network Connection] dialog box appears, select the account name on the user certificate issued for the main unit from the [User name on certificate:].
- (7) Enter the same name as the user name on the certificate.
- (8) Click on the [OK] button.

4-3. Successful authentication

- (9) You can confirm successful authentication by invoking [Network Connections] from the Control Panel and checking [Authentication succeeded] displayed under [Wireless Network Connection].

You have now finished connection to the wireless network, capable of accessing the network.

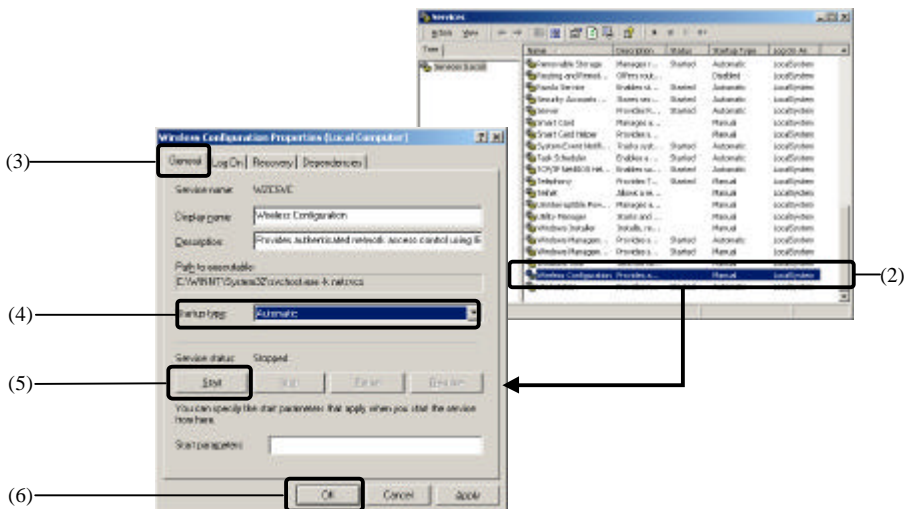
Use under Windows 2000 SP4



Authentication Type: EAP-TLS

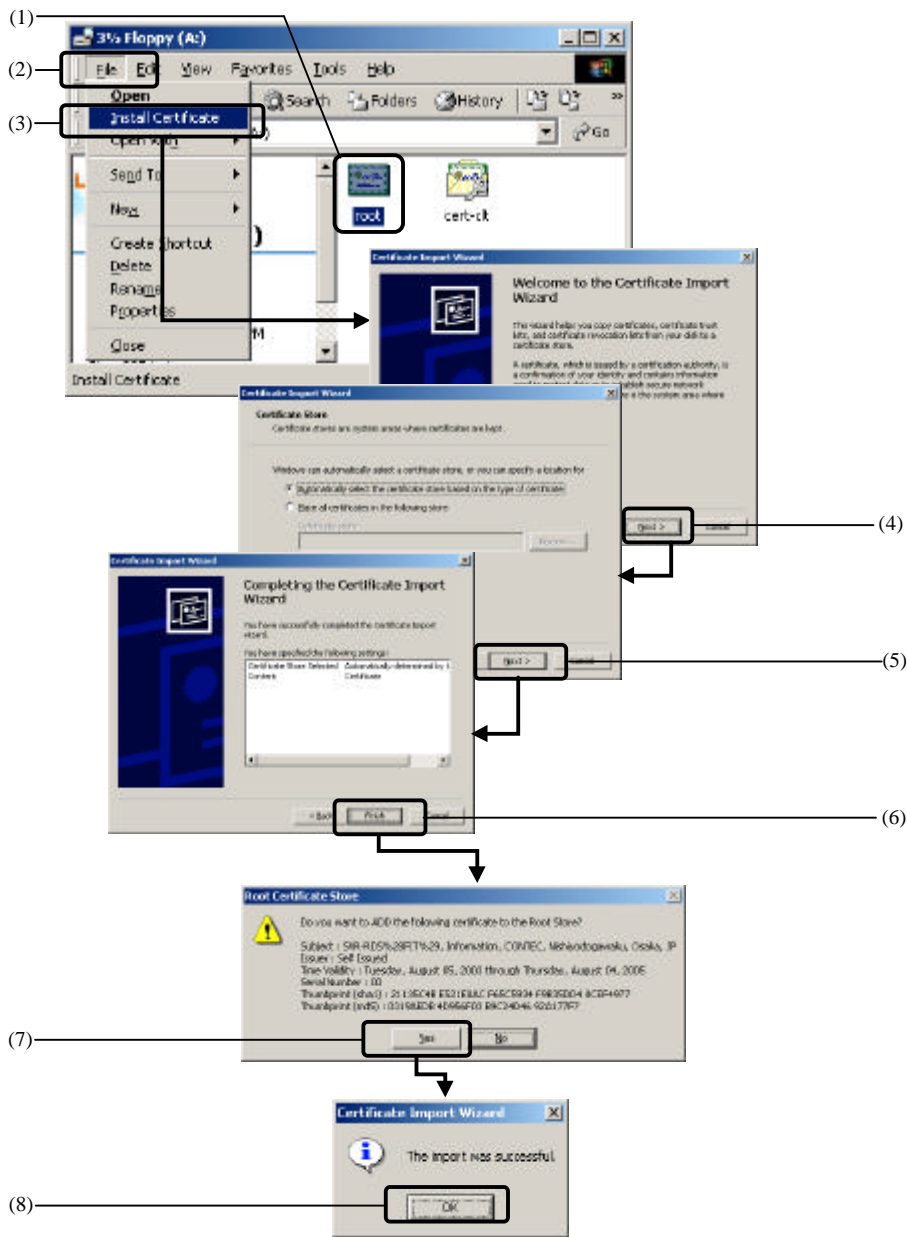
1.Installing the IEEE 802.1X support

To use IEEE 802.1X authentication under Windows 2000 SP4, “Start” the IEEE 802.1X authentication function (Wireless Configuration service) in the Windows 2000 SP4 environment. This section describes how to “start” the Wireless Configuration service.



- (1) Select [Administrative Tools] from [Control Panel]. Next, select [SERVICES].
- (2) Select [Wireless Configuration].
- (3) When [Wireless Configuration Properties (Local Computer)] appears, select [General] tab.
- (4) Select [Automatic] in the [Startup type:] field.
- (5) Click on the [Start] button in the [Service status:].
- (6) Click on the [OK] button.

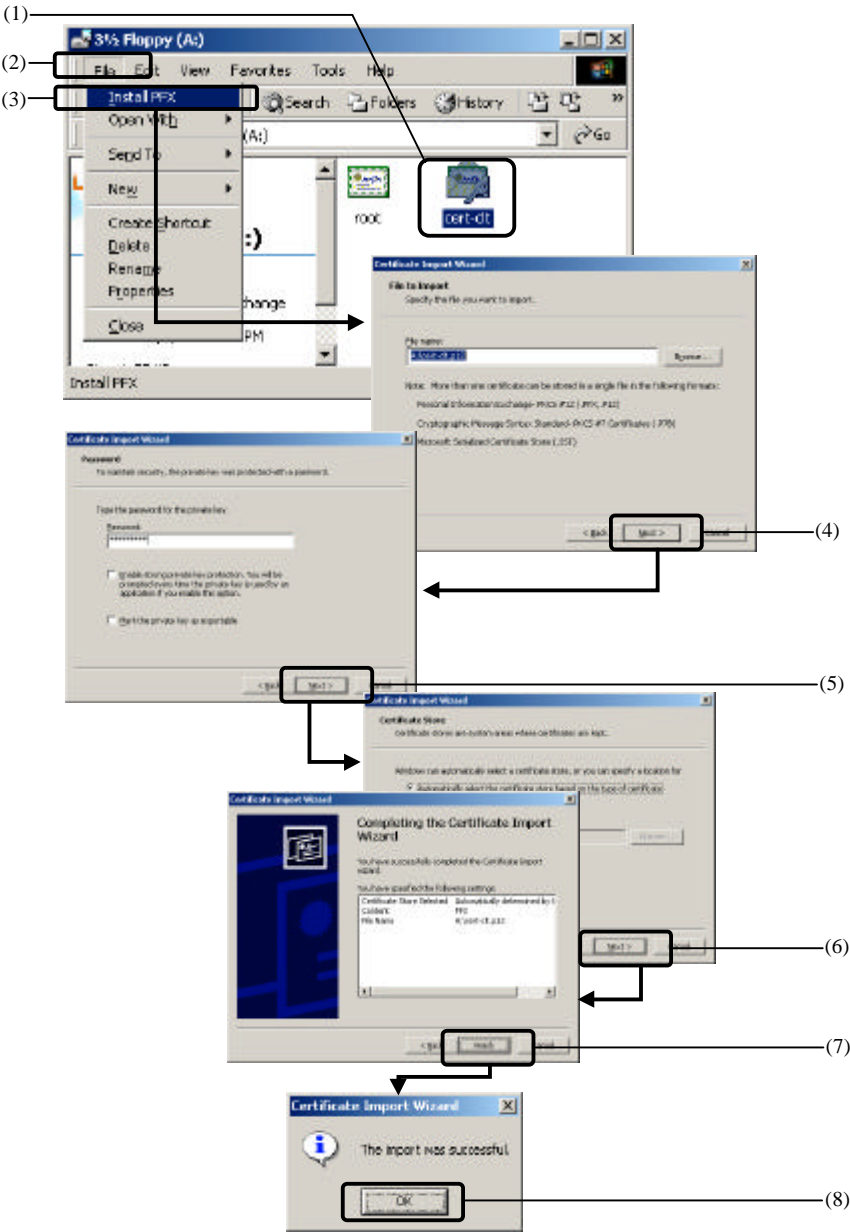
2.Installation of CA certificate



- (1) Select the CA certificate (root.der) issued by the server unit.
- (2) Select [File].
- (3) Select [Install Certificate] to start installing the CA certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button.
- (5) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (6) When [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (7) When the [Root Certificate Store] dialog box appears, click on the [Yes] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

The CA certificate has now been installed.

3.Installation of User CA



- (1) Select the user certificate (cert-clt.p12) issued by the server unit.
- (2) Select [File].
- (3) Select [Install PFX] to start installing the user certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button. When the [File to Import] dialog box that appears, click on the [Next] button.
- (5) When the [Password] dialog box appears, enter the [Password:] set when the user certificate was acquired, as the private key password, then click on the [Next] button.
Usually, leave [Enable strong private key protection] and [Mark the key as exportable] unchecked.
- (6) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (7) When the [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

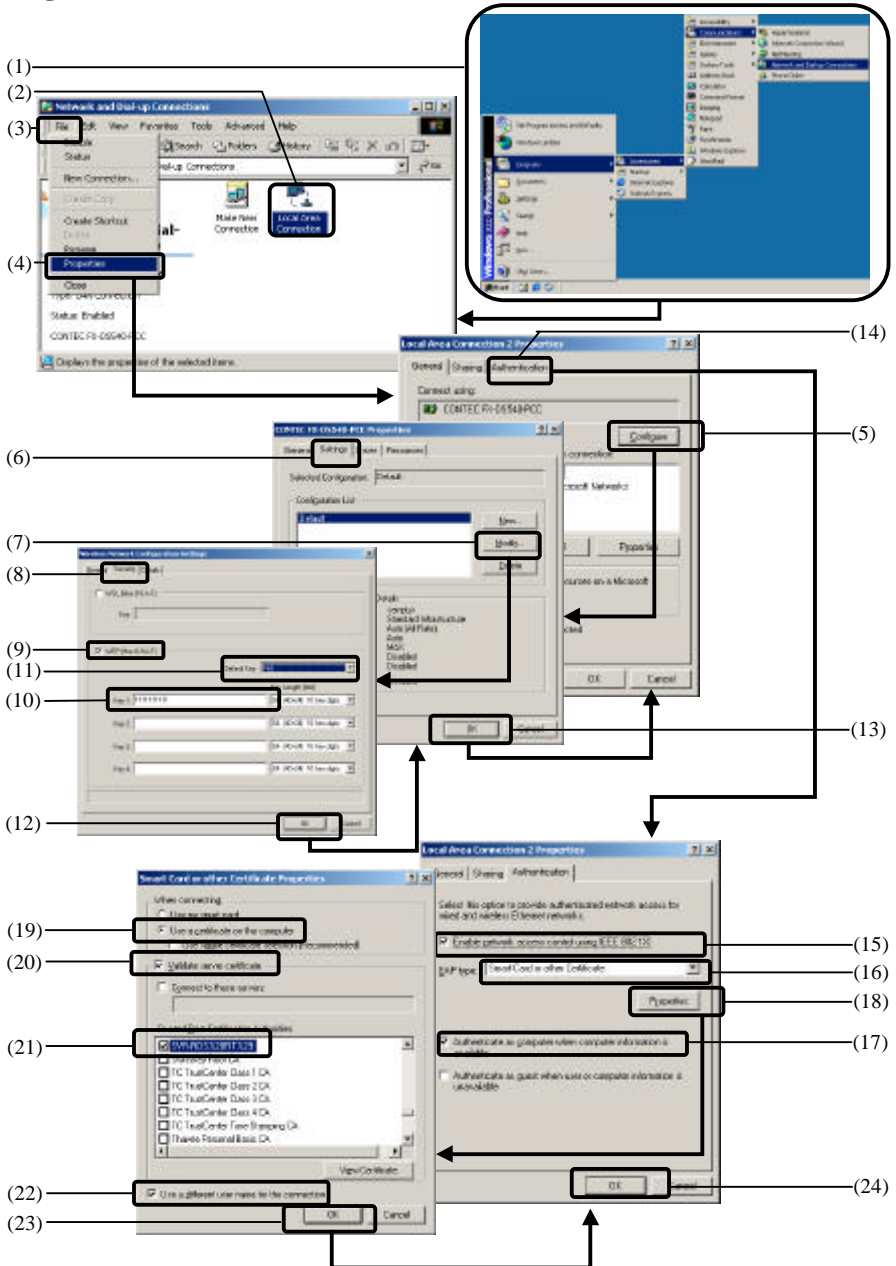
The user certificate has now been installed.



CAUTION

Once you have installed an issued user certificate, discard it or otherwise manage it confidentially to prevent a leak of secret information. The user certificate contains a private key for authentication. Security is lost if the user certificate is disclosed.

4.Setting the wireless network



4-1. Setting the wireless network (WEP)

Make settings to enable the WEP to be used for IEEE 802.1X.

This section assumes the use of the FX-D540-PCC in the FLEXLAN DS540 series as an example.

- (1) Invoke [Network and Dial-up Connections].
- (2) Open the Local Area Connection Properties dialog box for a desired local area connection.
- (3) Select the [File].
- (4) Select the [Properties].
- (5) When the [Local Area Connection Properties] dialog box appears, select the [General] tab and click on the [Configure] in the [Connect using:] field.
- (6) When the [CONTEC FX-DS540-PCC Properties] dialog box appears, select the [Settings] tab.
- (7) Select the setup information from the [Configuration List] and click on the [Modify].
- (8) When the [Wireless Network Configuration settings] dialog box appears, select the [Security] tab.
- (9) Check the [WEP].
- (10) Enter the appropriate size (Ex. 64) and key (Ex. 1111111111) in the [Key#1:] field.
- (11) Select the [First] in the [Default Key:] field.
- (12) Click on the [OK] button.
- (13) When the [CONTEC FX-DS540-PCC Properties] dialog box appears, click on the [OK] button.

4-2. Authentication tab setting

- (14) When the [Local Area Connection Properties] dialog box appears, select the [Authentication] tab.
- (15) Check the [Enable network access control using IEEE802].
- (16) Select [Smart Card or other Certificate] in the [EAP type:] field.
- (17) Check the [Authenticate as computer when computer information is available].
- (18) Click on the [Properties] button.

4-3. Selecting the CA certificate

- (19) In the [Smart Card or other Certificate Properties] dialog box, select [Use a certificate on this computer].
- (20) Check [Validate Server Certificate].
- (21) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (22) To use an account different from the user name entered to login to Windows, check [Use different user name for this connection].
- (23) Click on the [OK] button.

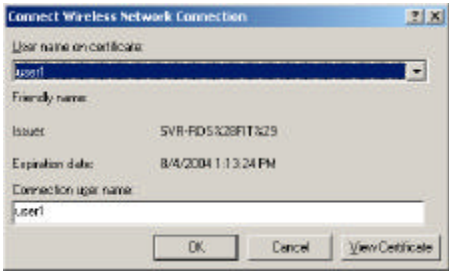
4-4. Exiting Setup

- (24) In the [Local Area Connection Properties] dialog box, click on the [OK] button.

5.Connection to the wireless network

When you have made the above settings in this chapter correctly, IEEE 802.1X authentication is started to complete connection to the network by the following procedure.

- (1) The [Connect Wireless Network Connection] dialog box appears, prompting you to confirm the certificate used for IEEE 802.1X authentication. Select the user certificate (the account name defined when the user certificate was issued) in the “User name on certificate:” list, then click on the [OK] button.

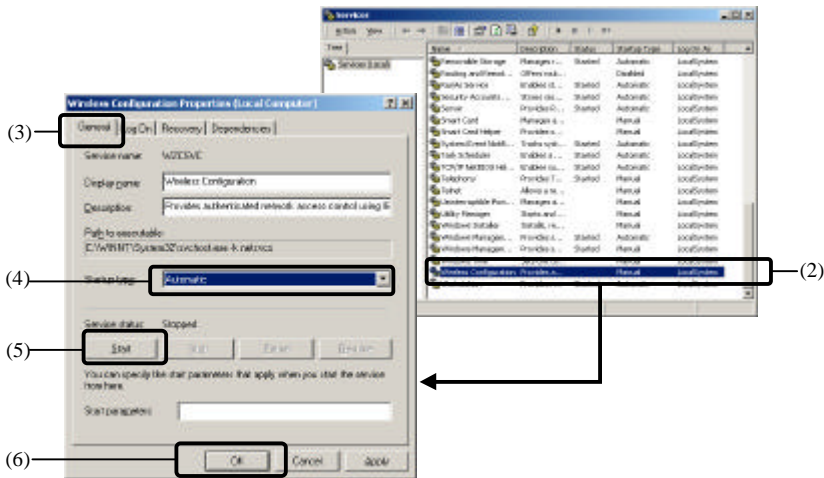


You have now finished connection to the wireless network, capable of accessing the network.

Authentication Type: PEAP(MS CHAP-V2)

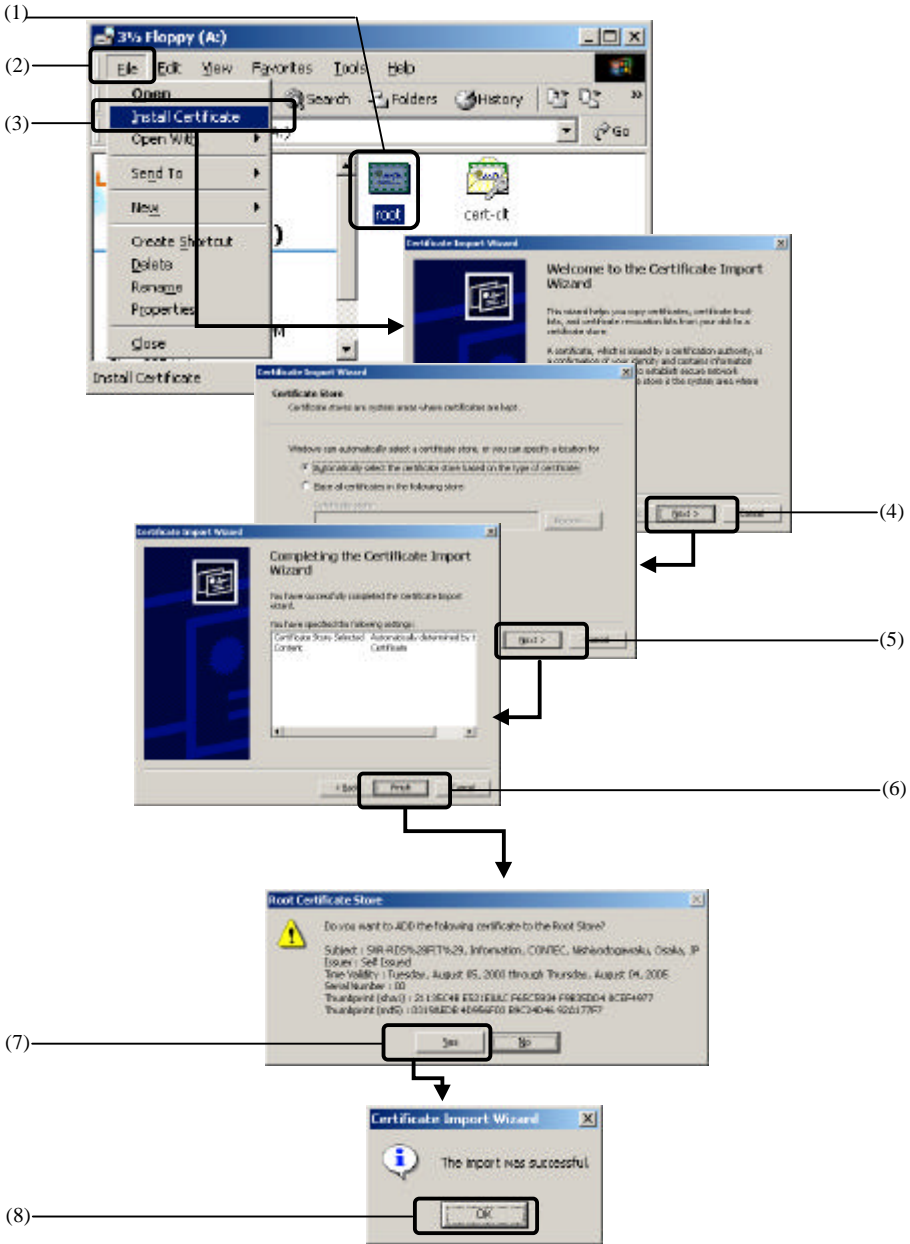
1.Installing the IEEE 802.1X support

To use IEEE 802.1X authentication under Windows 2000 SP4, “Start” the IEEE 802.1X authentication function (Wireless Configuration service) in the Windows 2000 SP4 environment. This section describes how to “start” the Wireless Configuration service.



- (1) Select [Administrative Tools] from [Control Panel]. Next, select [SERVICES].
- (2) Select [Wireless Configuration].
- (3) When [Wireless Configuration Properties (Local Computer)] appears, select [General] tab.
- (4) Select [Automatic] in the [Startup type:] field.
- (5) Click on the [Start] button in the [Service status:].
- (6) Click on the [OK] button.

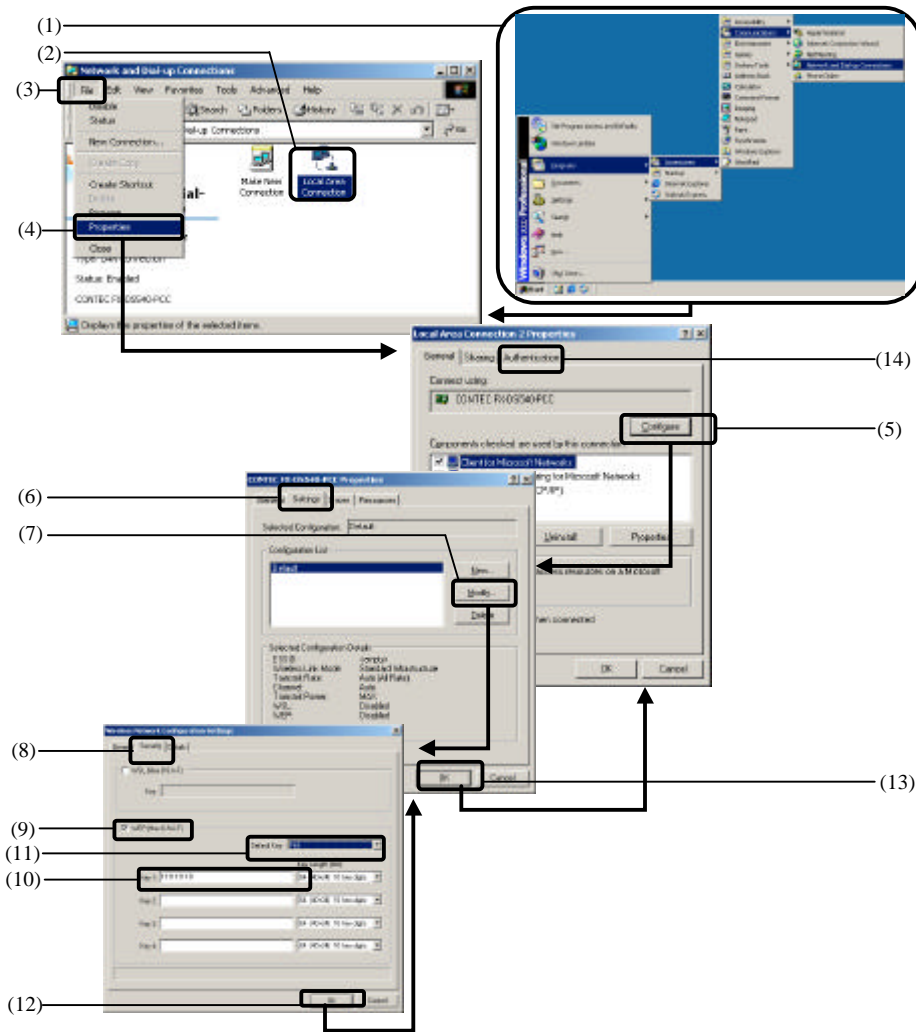
2.Installation of CA certificate



- (1) Select the CA certificate (root.der) issued by the server unit.
- (2) Select [File].
- (3) Select [Install Certificate] to start installing the CA certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button.
- (5) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (6) When [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (7) When the [Root Certificate Store] dialog box appears, click on the [Yes] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

The CA certificate has now been installed.

3.Setting the wireless network

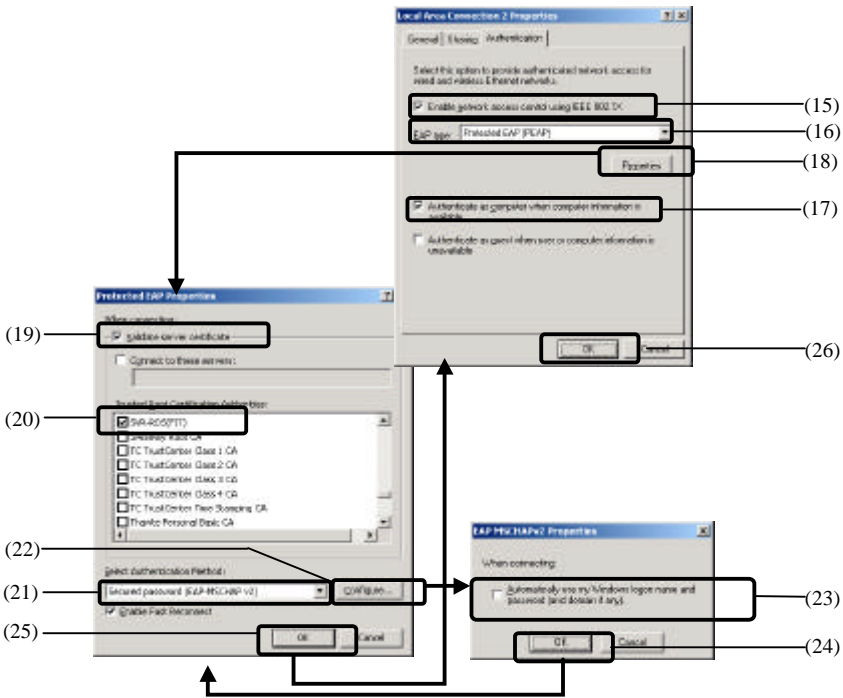


3-1. Setting the Wireless Network (WEP)

Make settings to enable the WEP to be used for IEEE 802.1X.

This section assumes the use of the FX-D540-PCC in the FLEXLAN DS540 series as an example.

- (1) Invoke [Network and Dial-up Connections].
- (2) Open the Local Area Connection dialog box for a desired local area connection.
- (3) Select the [File].
- (4) Select the [Properties].
- (5) When the [Local Area Connection Properties] dialog box appears, select the [General] tab and click on the [Configure] in the [Connect using:] field.
- (6) When the [CONTEC FX-DS540-PCC Properties] dialog box appears, select the [Settings] tab.
- (7) Select the setup information from the [Configuration List] and click on the [Modify].
- (8) When the [Wireless Network Configuration settings] dialog box appears, select the [Security] tab.
- (9) Check the [WEP].
- (10) Enter the appropriate size (Ex. 64) and key (Ex. 1111111111) in the [Key#1:] field.
- (11) Select the [First] in the [Default Key:] field.
- (12) Click on the [OK] button.
- (13) When the [CONTEC FX-DS540-PCC Properties] dialog box appears, click on the [OK] button.
- (14) When the [Local Area Connection Properties] dialog box appears, select the [Authentication] tab.



3-2. Authentication tab setting

- (15) Check the [Enable network access control using IEEE802].
- (16) Select [Smart Card or other Certificate] in the [EAP type:] field.
- (17) Check the [Authenticate as computer when computer information is available].
- (18) Click on the [Properties] button.

3-3. Selecting the CA certificate

- (19) In the [Protected EAP Properties] dialog box, check [Validate server certificate].
- (20) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (21) Select [Secured password (EAP-MSCHAPv2)] from [Select Authentication Method:].
- (22) Click on the [Configure] button.
- (23) [EAP MSCHAPv2 Properties] dialog box is displayed.

To use an account different from the user name entered to login to Windows, check [Automatically use my Windows logon name and password (and domain if any)].

- (24) Click on the [OK] button.

3-4. Setup completion

- (25) In the [Protected EAP Properties] dialog box, click on the [OK] button.
- (26) When the [Local Area Connection Properties] dialog box appears, click on the [OK] button.

4.Connection to the wireless network

When you have made the above settings in this chapter correctly, IEEE 802.1X authentication is started to complete connection to the network by the following procedure.



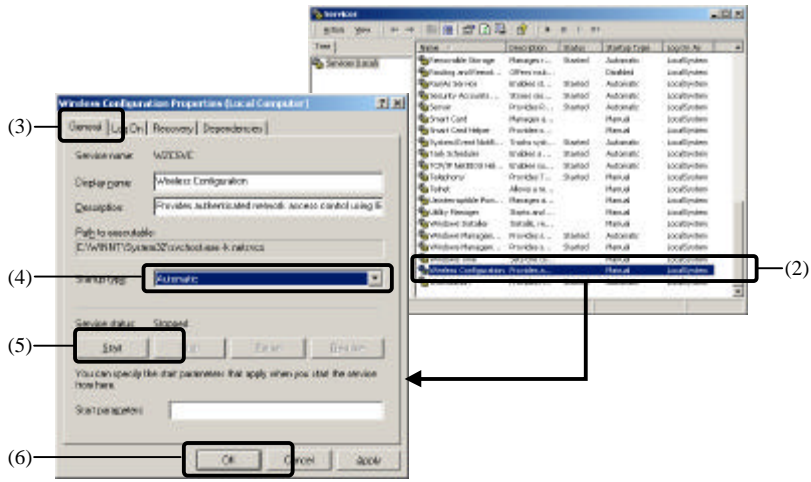
- (1) When the [Enter Credentials] dialog box appears, enter the account name set for the main unit in the [User name:] field.
- (2) In the [Password:] field, enter the password associated with the account set for the main unit.
- (3) Click on [OK] button.

You have now finished connection to the wireless network, capable of accessing the network.

Authentication Type: PEAP(TLS)

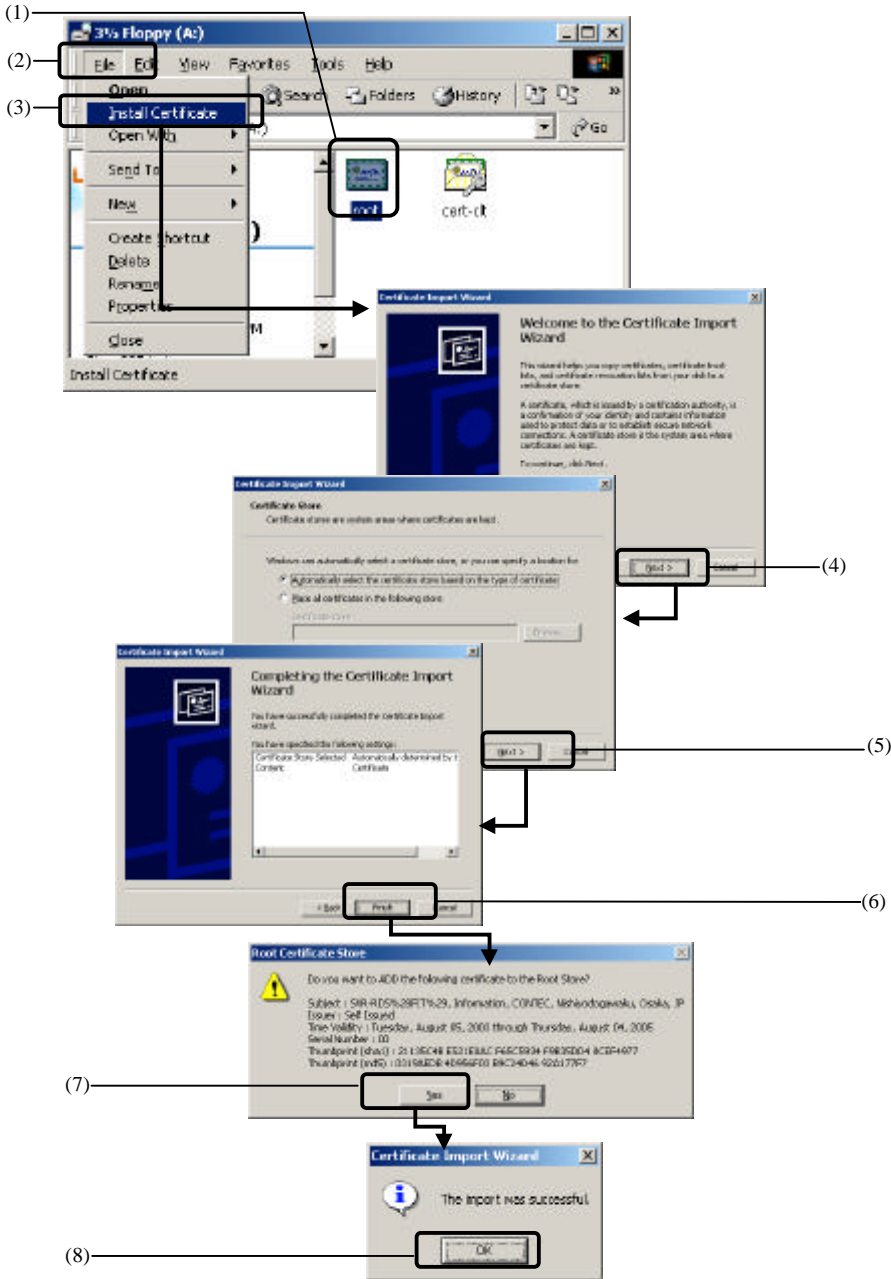
1.Installing the IEEE 802.1X support

To use IEEE 802.1X authentication under Windows 2000 SP4, “Start” the IEEE 802.1X authentication function (Wireless Configuration service) in the Windows 2000 SP4 environment. This section describes how to “start” the Wireless Configuration service.



- (1) Select [Administrative Tools] from [Control Panel]. Next, select [SERVICES].
- (2) Select [Wireless Configuration].
- (3) When [Wireless Configuration Properties (Local Computer)] appears, select [General] tab.
- (4) Select [Automatic] in the [Startup type:] field.
- (5) Click on the [Start] button in the [Service status:].
- (6) Click on the [OK] button.

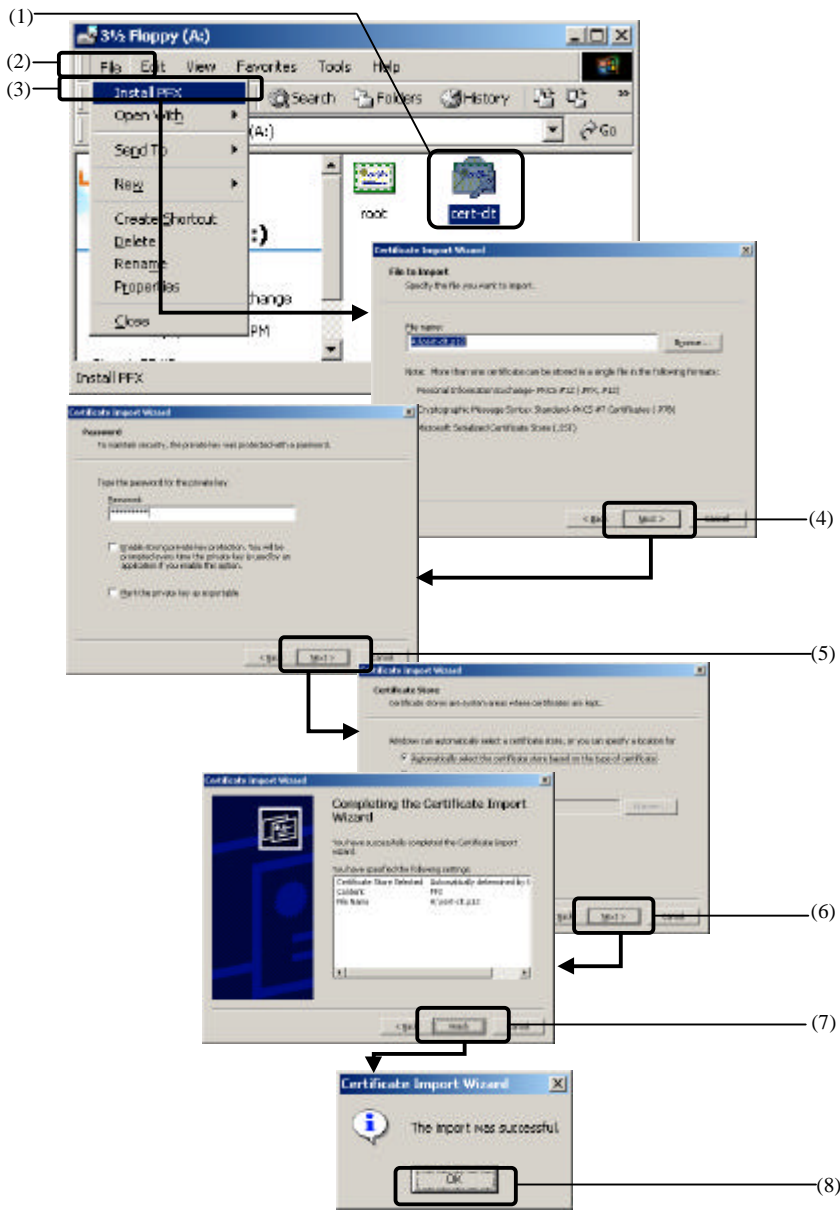
2.Installation of CA certificate



- (1) Select the CA certificate (root.der) issued by the server unit.
- (2) Select [File].
- (3) Select [Install Certificate] to start installing the CA certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button.
- (5) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (6) When [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (7) When the [Root Certificate Store] dialog box appears, click on the [Yes] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

The CA certificate has now been installed.

3.Installation of User CA



- (1) Select the user certificate (cert-clt.p12) issued by the server unit.
- (2) Select [File].
- (3) Select [Install PFX] to start installing the user certificate.
- (4) The [Certificate Import Wizard] is invoked with the [Welcome to the Certificate Import Wizard] dialog box. Click on the [Next] button. When the [File to import] dialog box that appears, click on the [Next] button.
- (5) When the [Password] dialog box appears, enter the [Password:] set when the user certificate was acquired, as the private key password, then click on the [Next] button.
Usually, leave [Enable strong private key protection] and [Mark this key as exportable] unchecked.
- (6) When the [Certificate Store] dialog box appears, check [Automatically select the certificate store based on the type of certificate] and click on the [Next] button.
- (7) When the [Completing the Certificate Import Wizard] dialog box appears, click on the [Finish] button.
- (8) When the Certificate Import Wizard shows the message [The import was successful.], click on the [OK] button.

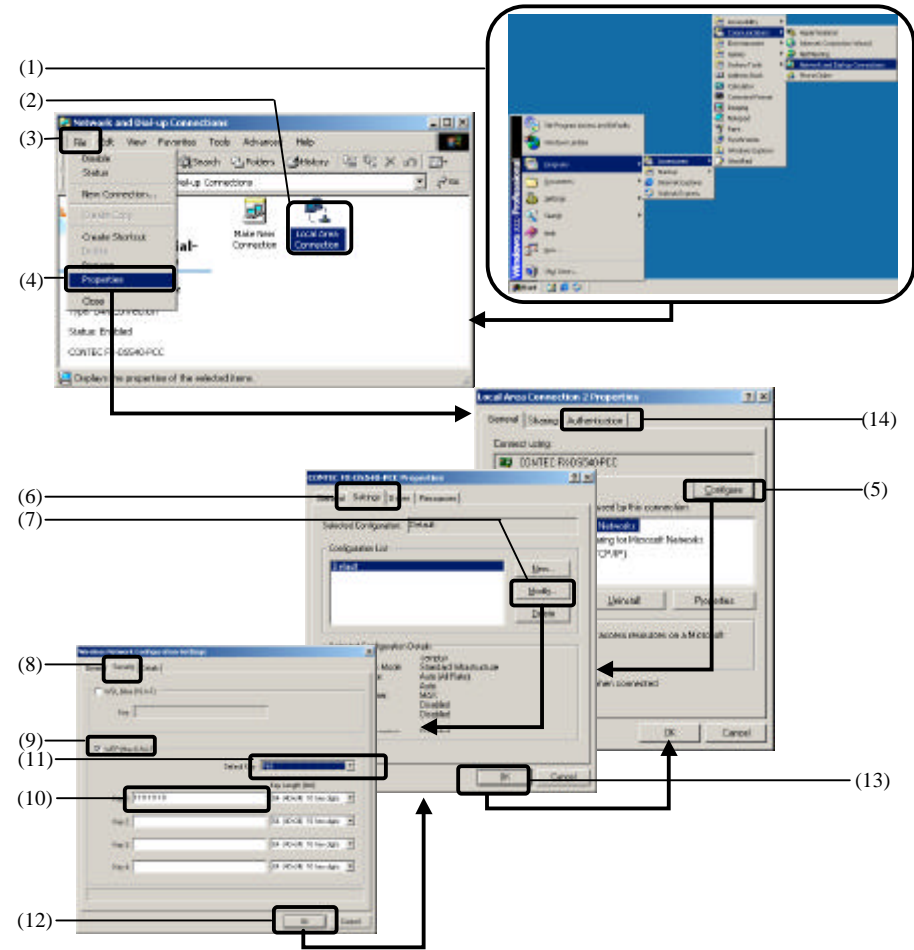
The user certificate has now been installed.



CAUTION

Once you have installed an issued user certificate, discard it or otherwise manage it confidentially to prevent a leak of secret information. The user certificate contains a private key for authentication. Security is lost if the user certificate is disclosed.

4.Setting the wireless network

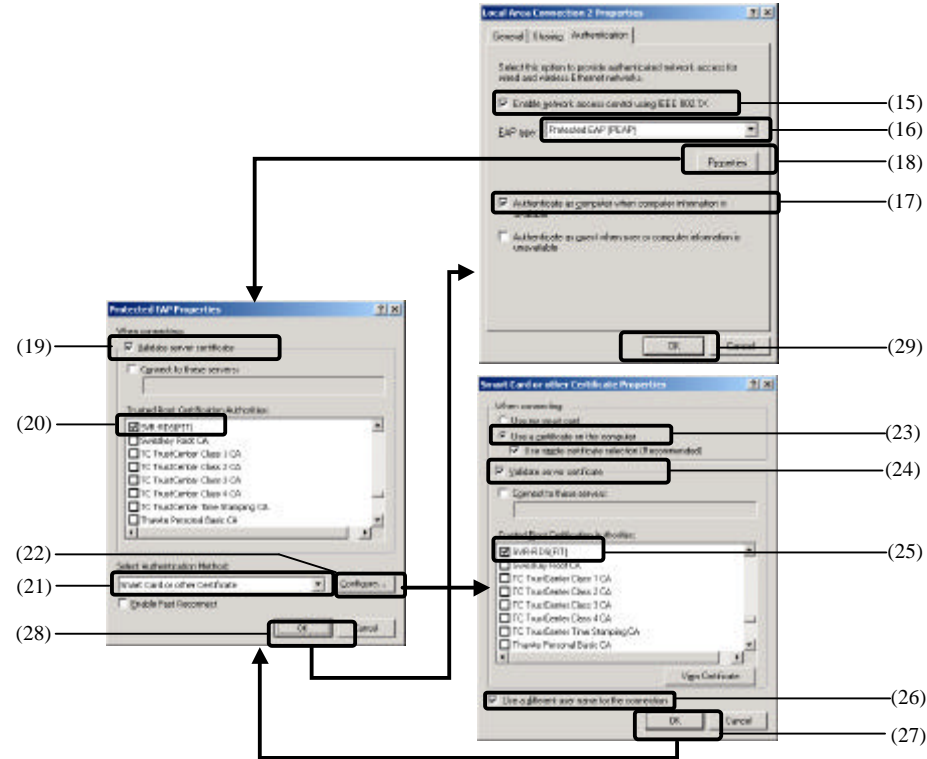


4-1. Setting the wireless network (WEP)

Make settings to enable the WEP to be used for IEEE 802.1X.

This section assumes the use of the FX-DS540-PCC in the FLEXLAN DS540 series as an example.

- (1) Invoke [Network and Dial-up Connections].
- (2) Open the Local Area Connection Properties dialog box for a desired local area connection.
- (3) Select the [File].
- (4) Select the [Properties].
- (5) When the [Local Area Connection Properties] dialog box appears, select the [General] tab and click on the [Configure] in the [Connect using:] field.
- (6) When the [CONTEC FX-DS540-PCC Properties] dialog box appears, select the [Settings] tab.
- (7) Select the setup information from the [Configuration List] and click on the [Modify].
- (8) When the [Wireless Network Configuration settings] dialog box appears, select the [Security] tab.
- (9) Check the [WEP].
- (10) Enter the appropriate size (Ex. 64) and key (Ex. 1111111111) in the [Key#1:] field.
- (11) Select the [First] in the [Default Key:] field.
- (12) Click on the [OK] button.
- (13) When the [CONTEC FX-DS540-PCC Properties] dialog box appears, click on the [OK] button.
- (14) When the [Local Area Connection Properties] dialog box appears, select the [Authentication] tab.



4-2. Authentication tab setting

- (15) Check the [Enable network access control using IEEE802.1X].
- (16) Select [Smart Card or other Certificate] in the [EAP type:] field.
- (17) Check the [Authenticate as computer when computer information is available].
- (18) Click on the [Properties] button.

4-3. Selecting the CA certificate

- (19) Check [Validate server certificate].
- (20) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (21) In the [Smart Card or other Certificate Properties] dialog box, select [Use a certificate on this computer] and check [Use simple certificate selection (recommended)].
- (22) Click on the [Configure] button.

4-4. Selecting the CA certificate for TLS authentication

- (23) In the [Smart Card or other Certificate Properties] dialog box, select [Use a certificate on this computer].
- (24) Check [Validate server certificate].
- (25) Select that name from the [Trusted Root Certificate Authorities:] list which was entered as [CA name] for CA certificate configuration of the server unit.
- (26) To use an account different from the user name entered to login to Windows, check [Use different user name for this connection].
- (27) Click on the [OK] button.

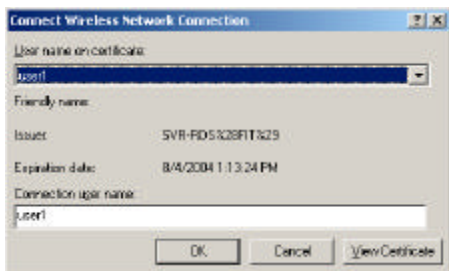
4-5. Exiting Setup

- (28) In the [Protected EAP Properties] dialog box, click on the [OK] button.
- (29) When the [Local Area Connection Properties] dialog box appears, click on the [OK] button.

5.Connection to the Wireless Network

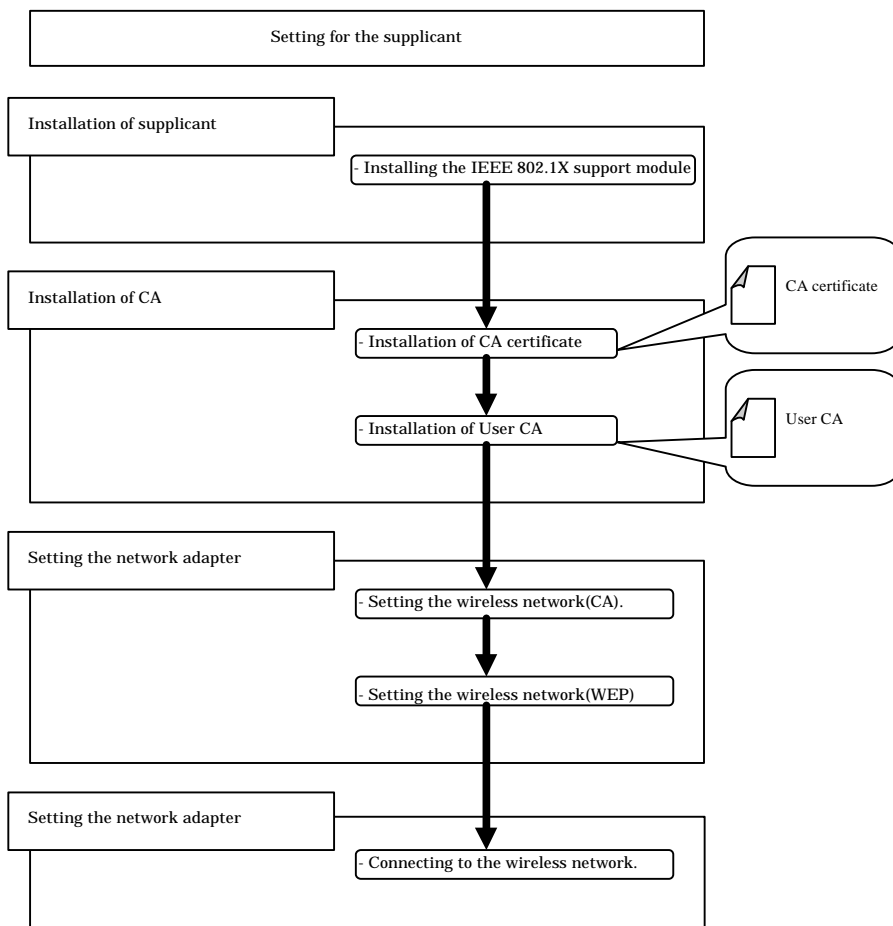
When you have made the above settings in this chapter correctly, IEEE 802.1X authentication is started to complete connection to the network by the following procedure.

- (1) The [Connect Wireless Network Connection] dialog box appears, prompting you to confirm the certificate used for IEEE 802.1X authentication. Select the user certificate (the account name defined when the user certificate was issued) in the [User name on certificate:] list, then click on the [OK] button.



You have now finished connection to the wireless network, capable of accessing the network.

Use under Windows 2000 SP3



Installing the IEEE 802.1X support

For IEEE 802.1X authentication in a Windows 2000 SP3 environment, patch it with [the IEEE 802.1X authentication module](#).

Install the IEEE 802.1X authentication patch module (*1) for Windows 2000 obtained from Microsoft Corporation.

After installing the patch module, please refer to “Use under Windows 2000 SP4”.

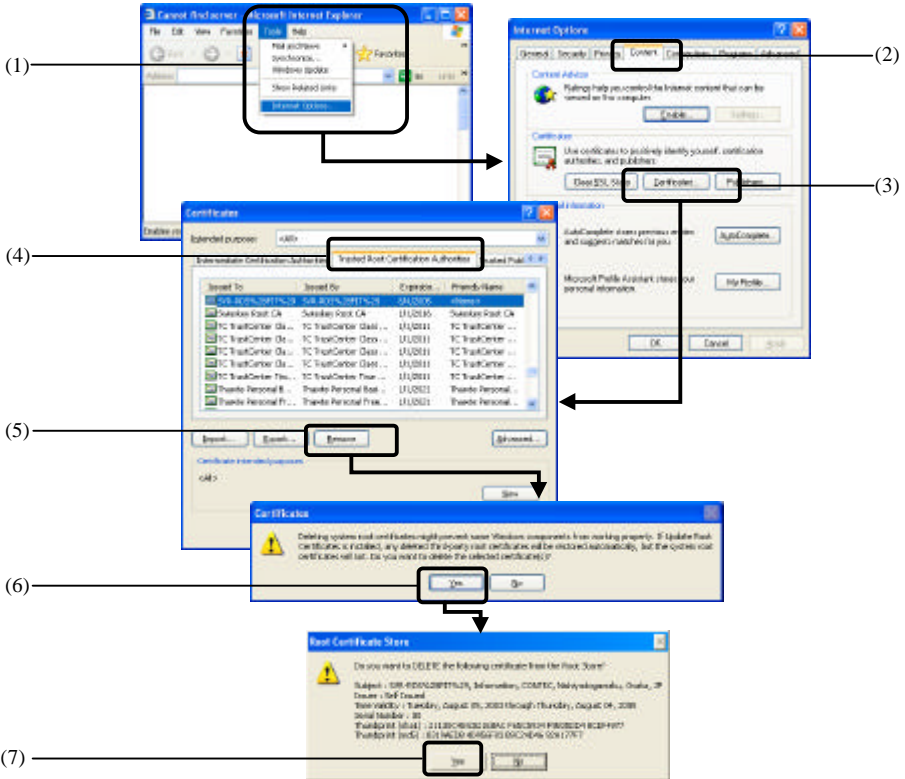
(*1) The IEEE 802.1X authentication module for Windows 2000 is available at the download center of Microsoft Corporation. (The latest version is Q313664 as of April, 2003.).

For information on this module, contact Microsoft Corporation as the supplier.

Deleting a certificate

This section describes how to delete a certificate no longer needed, for example, when the certificate has expired.

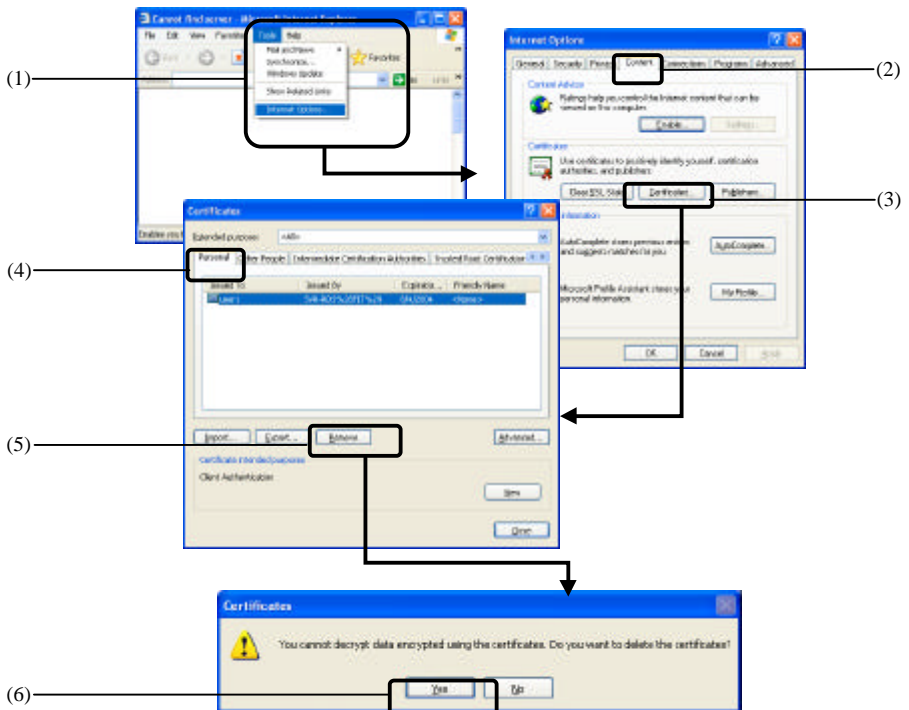
Deleting a CA certificate



- Invoke the Microsoft Internet Explorer and then select the [Internet Options] from the Tools menu.
- When the [Internet Options] dialog box appears, select the [Content] tab.
- Click on the [Certificates] button in the [Certificates].
- When the [Certificates] dialog box appears, select the [Trusted Root Certificate Authorities] tab.
- Select the certificate to be deleted from the list, then click on the [Remove] button.
- A warning message for deleting system root certificates appears. Selecting [Yes] deletes the certificate. Selecting [No] cancels the deletion of the certificate.
- [Root Certificates Store] dialog box appears. Selecting [Yes] deletes the certificate. Selecting [No] cancels the deletion of the certificate.

The CA certificate has now been deleted.

Deleting a user certificate



- (1) Invoke the Microsoft Internet Explorer and then select the [Internet Options] from the Tools menu.
- (2) When the [Internet Options] dialog box appears, select the [Content] tab.
- (3) Click on the [Certificates] button in the [Certificates].
- (4) Select the [Personal] tab in the [Certificates] dialog box.
- (5) Select the certificate to be deleted from the list, then click on the [Remove] button.
- (6) A warning message for deleting system root certificates appears. Selecting [Yes] deletes the certificate. Selecting [No] cancels the deletion of the certificate.

The user certificate has now been deleted.

6. Maintenance

Status Display

You can display a list of the server unit status information.

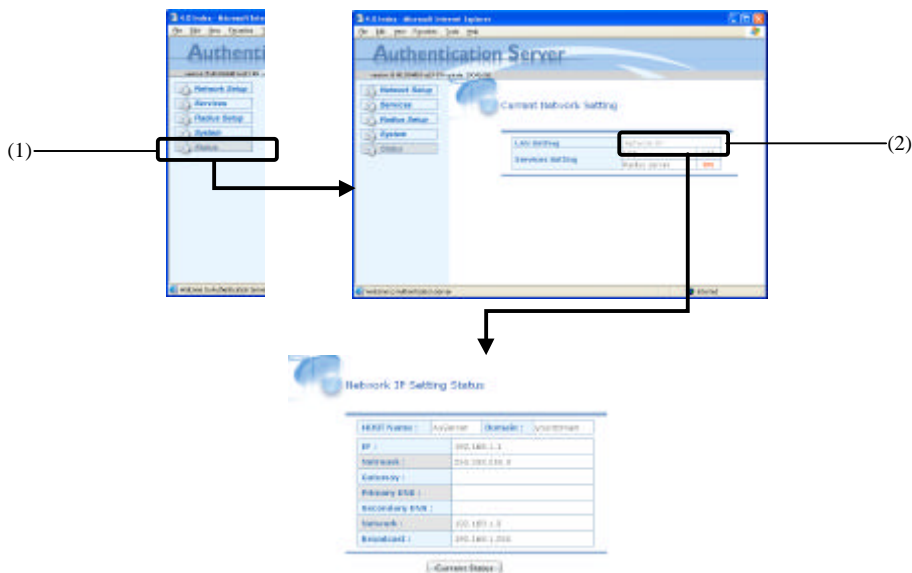


Figure 6.1. Status Display Screen

- (1) Click on the [Status] on the menu page.
- (2) Current Network Setting is displayed.
When clicking on the [Network IP], Network IP Setting Status on the basic setup is displayed.

Saving and restoring system information

You can back up setup information and restore the backup.

Between SVR-RDS(FIT) or SVR-RDS(FIT)L units, the backup of system information can be restored from one unit to another.

Back up

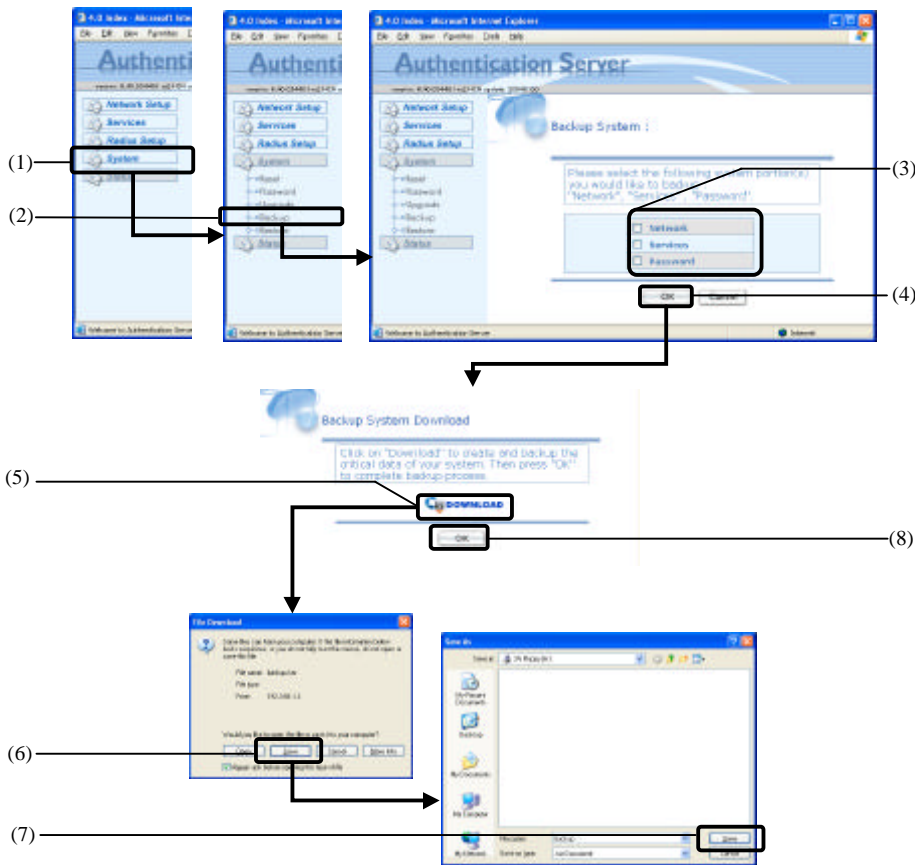


Figure 6.2. Back Up Screen

- (1) Click on the [System] on the menu screen.
- (2) Next, click on the [Backup].
- (3) When the backup page (Backup System) is displayed, check the items you want to back up.



Figure 6.3. Backup Item Selectors

- (4) Click on the [OK] button.
- (5) When the Backup System Download dialog box appears, click on the [DONWLOAD] button.
- (6) When the [File Download] dialog box appears, click on the [Save] button.
- (7) When the [Save As] dialog box appears, click on the [Save] button.
This time, the [backup.tar] is specified as the file name.
Downloading the file will be started. Wait until it is completed.
- (8) After downloading, click on the [OK] button on the [File Download] dialog box.

The backup information has now been saved.

CAUTION

The backup information file contains important information such as certificate data. Keep the obtained backup information file under strict control for confidentiality.

Restore

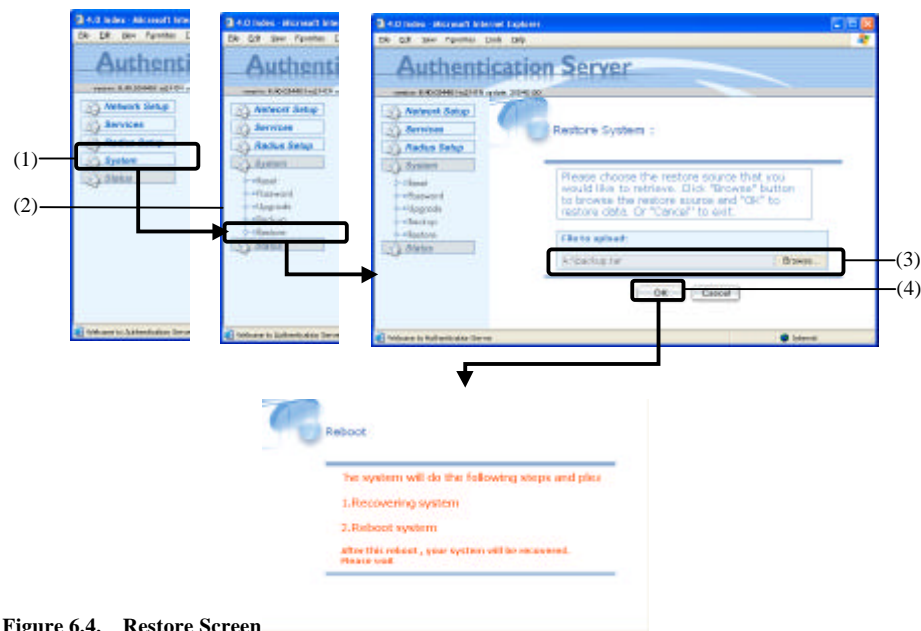


Figure 6.4. Restore Screen

- (1) Click on the [System] on the menu screen.
- (2) Click on the [Restore].
- (3) When the restore page (Restore System) is displayed, specify the backup file containing the information to be restored.

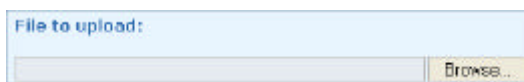


Figure 6.5. Restore Data Selectors

- (4) Click on the [OK] button.
Restoring the backup of information is started and the system is automatically restarted with the restored information.

The restore has now been completed.

Upgrading the System

The SVR-RDS(FIT)/ SVR-RDS(FIT)L may be upgraded to resolve any bugs found in the software or to add new functions. Contact CONTEC via our web site for details of the latest system data.

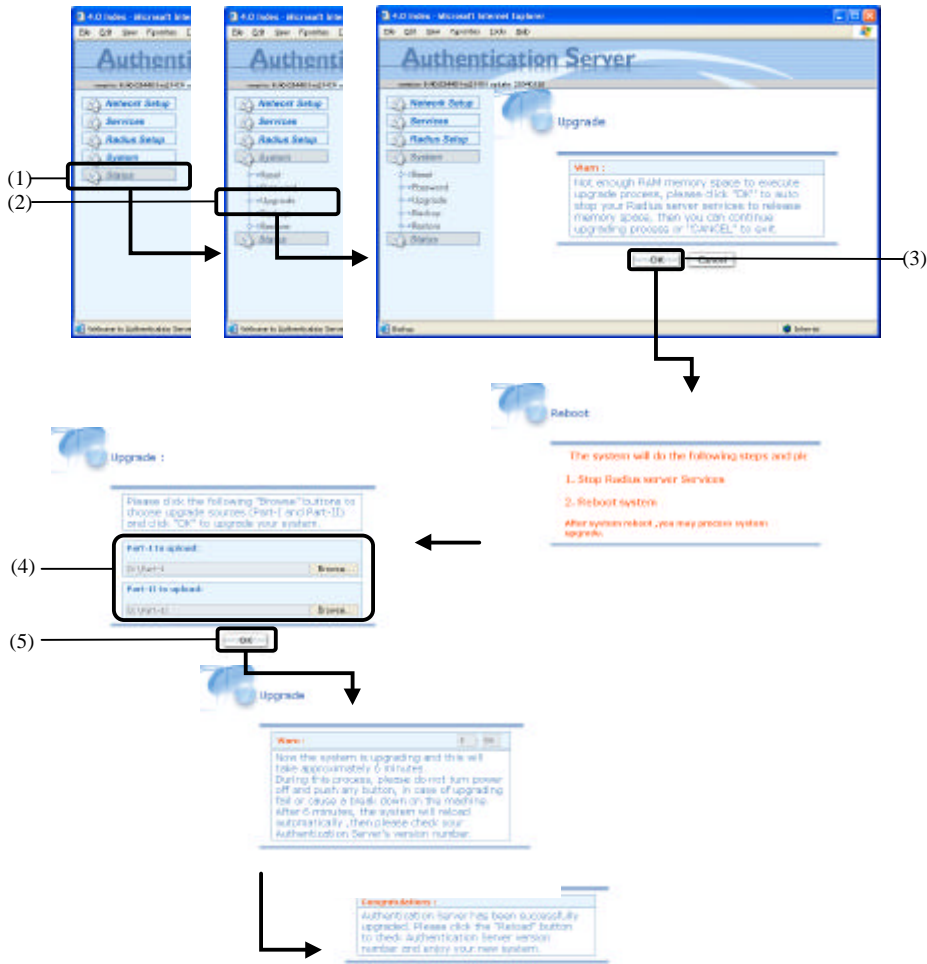
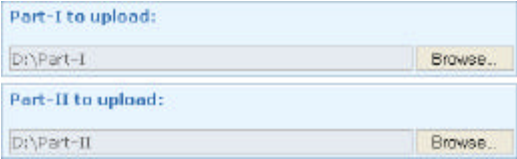


Figure 6.6. Version Up Screen

- (1) Click on the [System] on the menu screen.
- (2) Next, click on the [Upgrade].
- (3) The warning message (Upgrade - Warn) appears when the authentication server function is active. Clicking on the [OK] button brings up the Reboot message and stops the authentication server function. The warning message and Reboot message are not displayed with the authentication server function left inactive.



This step sets the following items.
Part-I to upload: [D: part-I]
Part-II to upload: [D: part-II]

Figure 6.7. Version Up Data Selectors

- (4) When prompted to specify the upgrade data file, specify the location of the upgrade data provided by CONTEC in the [Part-I to upload] and [Part-II to upload] fields.
- (5) Click on the [OK] button.
The message of upgrading (Upgrade - Warn) appears, incrementing the counter until the end of upgrading. The upgrade completion message (Upgrade - Congratulations) will be displayed upon completion of upgrading.

⚠ CAUTION —
After clicking on the [OK] button, be sure to check that the upgrade completion message (Upgrade - Congratulations) is displayed. Turning the power off before the upgrade completion message appears may corrupt internal information, possibly causing a fault.

The version up has now been completed.

⚠ CAUTION —
Upgrading the system initializes setup information, discarding the changes made so far. You should back up the required items of information before upgrading and restore them after that.

7. Troubleshooting

This chapter describes common problems that may occur with this product and what to do about them. If any problems occur that are not described here, check to confirm that the re-occur, then contact the store where you purchased the product.

When Communication Fails

Check hardware

- Check that the LAN cables are connected correctly.
- Check that the AC Adapter is connected correctly.

Check software

- Check that the IP address and subnet mask of the server unit have been set.
- Check if communication has been restricted by a proxy-based security function.
- Check if the IP address of the authentication server at the destination is wrong.
- Make sure that the IP address of the PC in use for setup of the server unit and its IP address belong to the same network group.
- Check that the web browser in use supports frames (HTML 4.0), such as Microsoft Internet Explorer 5.01 or later or Netscape 6 or later.
- No web browser can be used for communication if the TCP/IP protocol has not been installed on the PC attempted to be used for setup of the server unit.

When the main body Will Not Start

Check the status LED

- Make sure that the STATUS LED is on in green or orange. If the STATUS LED is off, check that the AC adapter has been connected to the power supply jack and a wall outlet.
- Make sure that the STATUS LED is on in orange. If the STATUS LED remain on in green even a sufficient period of time (at least 5 to 10 minutes) after the AP is turned on, the system in the server unit may be malfunctioning.

Authentication failed

Checking the server unit

- Check whether the IP address of the AP has been set as a CA setting item.
- Check whether the shared secret value set as a CA setting item is identical to that set for the AP.
- Check whether the IP address of the AP has been set as a CA setting item.
- Check whether the certificate of the AP has been set. as a CA setting item.
- Check whether the user certificate installed on the PC to be authenticated has been registered as an user certificate setting item.

Checking the AP settings

- Check that the IEEE 802.1X function as an IEEE 802.1X setting item has been enabled.
- Check whether the IP address as an IEEE 802.1X setting item has been set to the IP address of the server unit.
- Check whether the port number as an IEEE 802.1X setting item has been set to 1812.
- Check whether the shared secret value is the same as that set for the server unit.

Checking the settings of the PC to be authenticated

- Make sure that the OS in use supports IEEE 802.1X.
- Check that the IEEE 802.1X function has been enabled.
- Check that the wireless LAN has been configured correctly.
- Check that the user certificate issued by the server unit has been installed. To check the user certificate, select the “Content” tab in the “Internet Options” dialog box, then click on the [Certificates...] button. Select the “Personal” tab to check the certificate.
- Check if the user certificate issued by the server unit has expired.
- Check that the CA certificate issued by the server unit has been installed. To check the CA certificate, select the “Content” tab in the “Internet Options” dialog box, then click on the [Certificates...] button. Select the “Trusted root certificate authority” tab and check the certificate.
- Check if the CA certificate issued by the server unit has expired.

8. Appendix

Factory Default Settings List

System setting

Table 8.1. System setting

Specification		SVR-RDS(FIT)	SVR-RDS(FIT)L
IP address		192.168.1.1	
Netmask		255.255.255.0	
Login	User Name	root	
	Password	root	

Product Specifications

Physical Specifications

Table 8.2. Physical Specifications

Specification		SVR-RDS(FIT)	SVR-RDS(FIT)L
LAN unit	Ethernet standard	IEEE802.3(10BASE-T) IEEE802.3u(100BASE-TX)	
	Data transmission speed	10/100Mbps	
	Access method	CSMA/CD	
	Communication type	Half Duplex, Full Duplex	
	Number of ports	1(10BASE-T/100BASE-TX)	
External Dimensions (mm)		255(W) × 165(D) × 37(H)	80(W) × 115(D) × 25(H)
Weight		480g	150g

Software Specifications

Table 8.3. Software Specifications

Specification	SVR-RDS(FIT)	SVR-RDS(FIT)L
Protocols	IP(RFC791), ICMP(RFC792), UDP(RFC768), TCP(RFC793, 896), ARP(RFC826)	
Maximum number of APs to be registered	10 stand	
Maximum number of certificates to be issued	200 sheet	
Authentication type	EAP-TLS, PEAP	
Certified web browser	Microsoft Internet Explorer 5.01 or higher. Netscape Navigator 6 or higher.	
Certified APs	FX-DS540-APW, FX-DS540-AP, FX-DS540-APP, FX-DS540-APD, FX-DS540-APDL, FX-DS540-APL	
Certified supplicants	Windows XP, Windows XP SP1, Windows 2000 SP4, Windows 2000 SP3 (Patch required)	

Environmental Specifications for Installing the main body

Table 8.4. Environmental Specifications (Environmental Specs)

Specification	SVR-RDS(FIT)	SVR-RDS(FIT)L
DC power supply	5VDC \pm 5% 0.24A(Max.) (AC adapter bundled)	
Operating temperature	0 to 40°C	
Operating humidity	10 to 90%RH (non condensation)	
Airborne dust	Not extreme	
Corrosive gases	None	

Table 8.5. AC Adapter Environmental Conditions (Environmental Specs)

Specification	AC Adapter
AC supply voltage	100 to 240VAC 0.3A
AC supply frequency	47 to 63Hz
DC supply voltage	5VDC \pm 5% 2.0A(Max.)
Operating temperature	0 to 40°C
Operating humidity	10 to 90%RH (non condensation)
Airborne dust	Not extreme
Corrosive gases	None

LEDs

SVR-RDS(FIT)

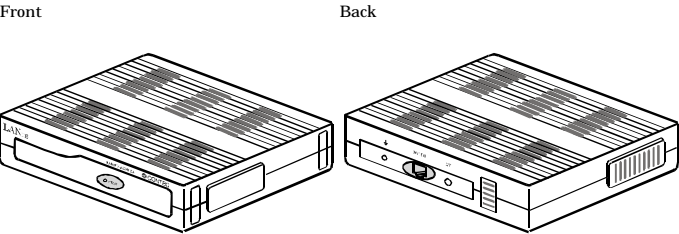


Figure 8.1. Front/back (SVR-RDS(FIT))

SVR-RDS(FIT)L

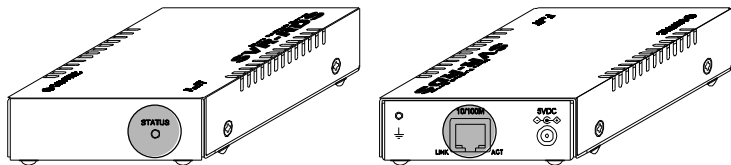


Figure 8.2. Front/back (SVR-RDS(FIT)L)

Indicator

Table 8.6. LED Indicator

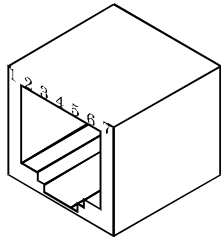
Name	Color	Status	Indicator
STATUS	Green / Orange	On in orange	Indicates that the device is operating.
		On in green	Indicates that the device is being started (going to operate after the power switch was turned on)
LAN	Green	On	Indicates operation at 100 Mbps
		Off	Indicates operation at 10 Mbps
	Orange	Flashing	Indicates that LAN data is being transmitted/received.

Input/Output Interface

Pin Assignment for UTP Port

Table 8.7. UTP Port Pin Assignments

Pin No	Signal
1	TD +
2	TD -
3	RD +
4	Not used
5	Not used
6	RD -
7	Not used
8	Not used



life expectancy of Battery

The SVR-RDS(FIT)/SVR-RDS(FIT)L contains a battery for the internal clock. The internal clock is used to check the validity term of each certificate. If the battery is dead, a certificate may be regarded as having expired, failing in authentication. If this product shows a wrong date while being used and the problem persists even after resetting the system time, contact your retailer or the CONTEC Information Center. The new battery has a lifetime of about five years (at the time of room temperature) after replacement with the server unit turned off. The battery is not consumed with the server unit turned on.

Glossary

AP(Access Point)

Access point. In the FLEXLAN DS540 series, the access point serves as a bridge between a wired network and a wireless network and provides IP tunneling; it is indispensable for the versatility and scalability of the wireless network.

Authenticator

Indicates an AP in a wireless LAN in IEEE 802.1X terminology.

IEEE(Institute of Electrical Electronics Engineers)

"I-triple-E," involved in a wide range of fields from communications and computer to medicine and biology, with primary activities related to publishing articles and sponsoring conferences, but also recommending and setting of standards. The organization sponsoring Committee 802, which is responsible for LAN related matters.

IEEE802.11/ IEEE802.11a

The wireless LAN standard established by the

IEEE802.1X

A standard set by IEEE to specify an authentication protocol.

LAN(Local Area Network)

A network configured from mutual connections between computers within a limited area. Also called an "intranet" or "business or regional data communications network."

Supplicant

Usually indicates client software for authentication in IEEE 802.1X terminology.

Public key

A key used to encrypt data by means of public key encryption, released to the remote party

Public key encryption; asymmetric encryption

A cryptographic system that uses two keys -- a public key and a private or secret key. In public key encryption, the sender passes the public key used for encrypting data to the receiver. The encrypted data is decrypted with the corresponding private key. Only the private key holder can therefore decrypt that data. Public key encryption is also called asymmetric encryption because it uses two different keys for encryption and decryption.

Shared Secret

A private key used between the authentication server and the AP.

CA:Certification Authority

Indicates the authority issuing the certificate.

Private key

The public key encrypts data, and a corresponding private key decrypts it. The private key must be managed confidentially not to be leaked to any third party.

Roaming

This term has the same meaning as roaming for a portable phone or PHS. The AP is in the role commonly called the 'antenna/base station' for the phone or PHS, and the user unit is in the role of the phone itself.

User Unit

In the FLEXLAN-DS540 series, this refers to the FX-DS540-PCC or a device with the FX-DS540-PCC built in.

SVR-RDS(FIT) SVR-RDS(FIT)L User's Manual

CONTEC CO.,LTD.

March 2004 Edition

3-9-31, Himesato, Nishiyodogawa-ku, Osaka 555-0025, Japan

Japanese <http://www.contec.co.jp/>

English <http://www.contec.com/>

Chinese <http://www.contec.com.cn/>

No part of this document may be copied or reproduced in any form by any means without prior written consent of CONTEC CO., LTD. [02032004]

[09162003]

Management No. A-46-747

[03242004_rev2]

Parts No. LYCP301