MFMC-GTS-071-0034

Issued: May 24, 2007

Network Security White Paper

ver.F.1.0

Covered Products:

Model SI-P1

Ricoh Company, Ltd.

Notice

T

Version history

Version	Issue Date	Revised item
F.1.0	May. 24, 2007	Initial release

The following terms are used in this document. Please familiarize yourself with them.

Terms:

the products: This refers to the digital multifunction and printing devices covered by this document, as noted in the Model Cross Reference table. “the products” refers to all of these machines collectively.

Host Interface: The physical interface of the Ethernet board on the products.

Model Cross Reference:

cc	Product Code	Brand					
		Ricoh	Savin	Gestetner	Lanier	NRG	infotec
Model SI-P1	G176 G177	Aficio SP 4100N Aficio SP 4110N	MLP31n MLP36n	SP 4100N/P7031n SP 4110N/P7035n	SP 4100N / LP131n SP 4110N / LP136n	SP 4100N SP 4110N	- -

Note: Parts of this document may not apply to some models. For example, printer models do not have scanners. Therefore some uses of RSH (for scanning) do not apply to these models.

Table of contents

1 Introduction

This document describes potential network threats and recommended precautions for them. The products have built-in network services for providing a variety of features for wired and wireless network clients, such as network scanning, printing or faxing, and also client services for accessing network servers running outside the products, such as an LDAP server, Netware server, or Mail server.
This document focuses on how-to protect against potential threats from external attacks.

As the products are designed for use inside an Intranet where network clients and servers are protected by firewalls, the products rely on the Intranet's security policy, like the security provided by other network servers and clients. However, some customers require more strict security levels for network devices, because potential threats from inside the firewalls are increasing, and some configurations even use a secure connection to the Internet as a part of the Intranet.
To satisfy these demands, the products are all evaluated by security scanning applications during development, and also are checked for known vulnerability issues reported by Internet security organizations, such as CERT Coordination Center (CERT/CC : HTTP:// www.cert.org/). Whenever we find security vulnerabilities in the products, we provide appropriate countermeasures.

2 Port Based Network Services and Potential Security Issues

Some server services allow write access from network clients. Because of this, some customers may feel that the products are insecure against viruses, worms, or intruder accesses. The products are secure against such attacks and provide security measures against potential threats to specific services, but some of these measures can make the services unavailable. For example, disabling the LPD port will make the products unavailable for LPR clients.
You should disable all protocols that are not being used. This can be done more quickly using Network Security Levels (described in Appendix H). The Network Security Level function can be used to expedite security configuration. Please refer Appendix H for information about the configuration and a description of each level.

We also recommend using the Access Control function for added security. Access Control is a list of “safe” client host addresses. Once you set up Access Control for specific IP addresses, the products will receive print or scan requests from the specified hosts only. Access Control is applied for LPR printing, RSH/RCP access, HTTP/HTTPS access, FTP printing, TCP raw printing (DIPRINT), SMB printing, IPP printing, and scanning from DeskTopBinder. For information on how to set up access control, please refer Appendix C.

In the following sections, the potential threats and recommended precautions are given for each service. The recommended precautions should be accompanied by a firewall and restricted by Access Control.

2.1. TELNET

2.1.1. Function Overview

The TELNET service provides a virtual terminal service in order to use the maintenance shell (mshell). It is compliant with RFC 854. The mshell uses TCP port 23 and provides a dedicated command interface for the following functions.

- Configuring network settings of the products from remote terminals
- Monitoring device status and settings from remote terminals
- Getting system logs from remote terminals

Unlike shell services for UNIX/Linux, the mshell provides a command interface for configuration purposes only. Access to the file system or kernel, or modifying system files inside the products is not possible.

When logging into the mshell, the user must enter a correct username and password.

2.1.2 Potential threats

1) Destruction, corruption and modification of the file system and kernel.

There is no possibility of destruction, corruption or modification of the file system.

The mshell permits write-access to network parameters only and no one can access the file system or kernel.

2) Possibility of acting as a server for relaying viruses.

There is no possibility that the products will be used by viruses as an open relay server, because unrecognized data is disregarded. Also, neither the local file system nor remote host can be accessed via the mshell.

3) Theft of username and password

Interception of network packets: When accessing the products using TELNET, the username and password are sent in clear text, because the TELNET protocol itself does not support encryption. So if the username and password are intercepted by a packet sniffer, the possibility of unauthorized access and changes being made does exist.

2.1.3 Recommended precautions

The following are suggested precautions against threats to the embedded TELNET service. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the username and password from the default value to something difficult to guess and change it regularly. (Please refer Appendix G)

- The username and password are the same as those used for logging into Web Image Monitor in Administrator mode. So, changing the username and

password for the mshell means changing them for Web Image Monitor's Administrator mode.

Level 2: Close the TELNET port.

- The TELNET port can be completely closed using Web Image Monitor. When TELNET is disabled, the services provided by the mshell will not be available.

2.2. FTP

2.2.1. Function Overview

The FTP (File Transfer Protocol) service provides the function of receiving data with reliability and efficiency. This service is compliant with RFC 959. TCP port 20 is used for FTP-data service and TCP port 21 is used for FTP-control service. The FTP client must be compliant with RFC 959.

The following functions are provided by the FTP service.

- Receiving print jobs from FTP clients
- Providing the following files to FTP clients

File name	Description	Attribute
Syslog	System log information	Read-only
Stat	Printer Status	Read-only
Prnlog	Print log information	Read-only
Info	Printer Information	Read-only
Help	Help	Read-only
Fax application files (hidden)	Fax job log information Fax counter Fax address book	SmartDeviceMonitor for Admin/Client is required to read/ manage these files.

- Receiving firmware files from remote clients.

  RFU requires Machine administrator privileges. When Web Smart Device Monitor is used for RFU, TCP port 10020/10021 are used to send firmware files via the FTP protocol. However, port 21 is used to negotiate the transfer. All 3 ports must be open. It is a proprietary process defined by Ricoh and is extremely difficult to emulate without the knowledge of the specification. However if a strict security policy is to be maintained, that port can be closed via TELNET. (Please refer to Appendix C.)

2.2.2 Potential threats

1) Destruction, corruption and modification of the file system.

There is no possibility of destruction, corruption or modification of the file system.

Although the FTP service permits write-access, any files that are received by the printer are considered to be a print job or firmware data. When the embedded FTP server receives an executable file, the products prints a binary representation (garbage characters) of the data contained in the executable. As for firmware, a dedicated account and password that are disclosed only to Service Technicians is required to input firmware to the printer using the FTP service. In addition, data is verified by checking the header, IDs and the file format

before being used. It is impossible to make a pseudo firmware file to destroy the file system.
2) Possibility of acting as a server for relaying viruses.
There is no possibility that the products will be used by a virus as an open relay server. Although the FTP service permits write-access, all written data are treated as print jobs. Even if someone sent an executable file via the embedded FTP service, the products print the file as garbage data.
4) Theft of username and password.
Interception of network packets: When accessing the products using FTP, the username and the password are sent in clear text because the FTP protocol itself does not support encryption. However, this does not present a major security risk because no changes can be made to the system via FTP. In fact a username and password are not even necessary when logging onto an FTP session except when for updating the firmware. When putting firmware data onto an FTP server, a dedicated account and password are required and they are disclosed to only Service Technicians. There is no possibility of destruction of the file system from someone using a sniffed username and password because it is impossible to make a pseudo firmware file to destroy the file system.
5) Theft of print data
Interception of network packets: Using FTP, print data is sent as clear text. If intercepted by a third party it is easily read.

2.2.3 Recommended precautions

As stated earlier, the suggested precaution against the threats to the embedded FTP service is closing the FTP port if you maintain a strict security policy. The port for this service can be completely closed using Web Image Monitor or the mshell.
Note1: To reduce the likelihood of print data being intercepted, please use SFTP instead of FTP as the printing protocol.

2.3. HTTP

2.3.1. Function Overview

The HTTP (Hypertext Transfer Protocol) service provides web services. This service is compliant with RFC 1945. TCP port 80 is used for the HTTP service.

The following functions are provided by the HTTP server service.

- Configuring machine settings via Web Image Monitor in Administrator mode
- Viewing machine settings and status via Web Image Monitor
- Managing files saved in the Document Server of the products via DeskTopBinder.
- Managing user information and retrieving counter information when using User Management Tool in SmartDeviceMonitor for Admin/Client
- Managing the Product's address book when using Address Management Tool in SmartDeviceMonitor for Admin.
- Printing a job from an IPP client.
- Providing job status to an IPP client.

Note1: When logging into Web Image Monitor in Administrator mode, the user must enter the username and password. It is the same as the username and password used for the mshell.

2.3.2 Potential threats

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system. Because no one can access the file system and executable files cannot be processed on the products web server.

2) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. The web server was developed by Ricoh and does not allow any malicious and executable files to be processed.

3) Theft of username and password

Interception of network packets: When accessing Web Image Monitor, the password is sent with BASE64 encode. In this case, the password is not sent in clear text, but it is not particularly difficult to decode.

Therefore, if the password is intercepted using a packet sniffed and then decrypted, the possibility of unauthorized access and changing of network settings does exist.

4) Theft of print data

Interception of network packets: Using HTTP, print data is sent as clear text. If intercepted by a third party it is easily read.

2.3.3 Recommended precautions

The following are suggested precautions against threats to HTTP service. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the username and password from the default value to something difficult to guess and change them regularly.

- The username and password are the same as those used for logging in to the shell. So, changing the username and password for Web Image Monitor's Administrator mode means changing them for the mshell as well.

Level 2: Forward HTTP requests to HTTPS.

- Whether all, some or none of the HTTP requests received by the MFP are forwarded to HTTPS, depends on the settings. (Please refer to Appendix E.)

Level 3a: Close the HTTP port.

- The HTTP port can be completely closed with mshell. In this case, both Web Image Monitor and IPP (Internet Print Protocol) are unavailable via HTTP. IPP printing provides printer access via HTTP (HTTP://<printer host name or IP address>/printer (or ipp)). If the HTTP port is closed, Web Image Monitor and IPP printing are still available via HTTPS.

Level 3b: Disable web function.

- If it is not needed, Web Image Monitor can be disabled using the mshell. When web is set to 'Down', Web Image Monitor does not activate and the error "503 Service Unavailable" is displayed. Even when not in use, TCP port 80 stays open and is therefore HTTP is available for IPP printing.

Note1: We recommend using HTTPS instead of HTTP for Web Image Monitor and IPP printing.
Note2: If you want to reduce the possibility of print data being intercepted, please use HTTPS instead of HTTP as the printing protocol.

2.4. SNMP v1/v2

2.4.1. Function Overview

SNMP (Simple Network Management Protocol) is used to communicate management information between the network management stations (SNMP manager), such as a PC running a management application, and the agents in the network (SNMP agent), such as printers, scanners, workstations or servers, routers and hubs. The SNMP service is embedded in the products, to provide a method of managing them on the network. This service is compliant with RFC 1157 for SNMP v1 and RFC 1902 for SNMP v2. UDP port 161 is used for SNMP service and UDP port 162 is used for SNMP-trap.

The following functions are available.

- Configuring the settings of the products.
- Monitoring the status of the products.
- Detecting errors affecting the products.
- Communicating with the client PC for Scanning using the TWAIN driver.

Although the SNMP service is not protected by a password, it is protected using unique community names and assigned access rights (read-only, read-write and trap) within those communities. You can only communicate with or configure an agent if it is a member of the same community and if the access rights allow you to get or modify data in the MIBs (Management Information Base) embedded in the products.

Default settings of SNMP community names are follows;

- Read-only: public
- Read-Write: admin

2.4.2. Potential threats and recommended precautions

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system.

SNMP permits write-access to network parameters only and no one can access the file system or kernel.

2) Theft of community name

Interception of network packets: Community names are sent in clear text because of the specification of the protocol. Therefore, if intercepted, the community name is easily read.

3) Possibility of unauthorized parties intercepting device information:

Interception of network packets: The products do not respond with important information such as administrator password even if the SNMP client sends a get request for this information. Therefore security risk is low. However when accessing the products using SNMP, other parameters are sent in clear text. Because the SNMP v1/v2 protocol itself does

not support encryption. So if other parameters are intercepted, there is a possibility of unauthorized parties obtaining device information.

2.4.3. Recommended precautions

The suggested precautions against this threat are as follows. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the community names from the default value to something difficult to guess and change it regularly.

- When the community name settings are changed in the agents, the community name settings in the management utilities must also be changed.

Level 2: Change the setting so that only ‘get’ access using SNMP v1/v2 is allowed (disable ‘set’ access from SNMP v1/v2).

Level 3: Disable the SNMP v1/v2 service

- If it is not absolutely necessary, the SNMP service should be disabled via Web Image Monitor or the mshell.

Level 4: Close the SNMP port

- If it is not absolutely necessary, the SNMP port should be closed via Web Image Monitor or the mshell.

Note1: Please refer Appendix F for details about SNMP settings

Note2: We recommend using the maximum level of security possible. SNMP v3 should always be used in cases where SNMP v1/v2 is not absolutely necessary. Utilities that do not support SNMP v3 will not be able to get device status unless SNMP v1/v2 is enabled. Therefore these utilities will not work correctly if SNMP v1/v2 has been disabled. If your utility does not support SNMP v3 and only requires ‘get’ access to work (doesn’t make any changes to MFP settings), then we recommend security Level 2.

2.5. SHELL (RSH/RCP)

2.5.1. Function Overview

Remote shell (RSH/RCP) services provide the following functions via TCP port 514.

- Printing jobs from RSH/RCP clients.
- Monitoring machine status and settings from RSH/RCP clients.
- Providing the print logs and the system logs to RSH/RCP clients.
- Transferring scan data to the Twain driver.

2.5.2. Potential threats and recommended precautions

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system. Because no one can access the file system or kernel and executable files cannot be processed via the remote shell service

2) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. Although the remote shell service permits write-access, all written data are treated as print jobs. Even if someone sent an executable file via the embedded remote shell service, the products print the file as garbage data.

3) Theft of username and password

Interception of network packets: The RSH protocol has an authentication function. However an account is not necessarily needed to access products via RSH. If the user is concerned about this, the port for remote shell service can be completely closed via Web Image Monitor and mshell.

5) Theft of print data

Interception of network packets: Using RSH/RCP, print data is sent as clear text. If intercepted by a third party it is easily read.

2.5.3. Recommended precautions

As stated above, there are not many threats that apply to the products. However, if you want to maintain a strict security policy, the RSH/RCP service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

Note1: If you want to reduce the possibility of print data being intercepted, please use HTTPS instead of RSH/RCP as the printing protocol.

2.6. LPD

2.6.1. Function Overview

The LPD service is one of the TCP/IP Printing Services known as LPD or LPR. This service is compliant with RFC 1179 and uses TCP port 515 for connection with a RFC 1179 compliant client. The following functions are provided by this service.

- Printing a job from LPR clients
- Monitoring the status of the printer and print queues from LPR clients.
- Deleting print jobs from the print queue by LPR clients.

2.6.2. Potential threats and recommended precaution

1) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. The LPD service treats all received data as print jobs. Even if someone sends an executable file via the embedded LPD service, the products print the file as garbage data.

2) Possibility of successful DoS (Denial of Service) attacks.

There is no possibility of successful DoS attacks.

When the products receive the data that does not meet the protocol specification, the products will stop the LPD service, and the executed application (if any), at regular steps.

3) Theft of username and password

Interception of network packets: LPD does not have an authentication function. However, print data may contain authentication information. This information can be encrypted by the printer driver. Please refer the user manual and driver help for more information about this method.

4) Theft of print data

Interception of network packets: Using LPR, print data is sent as clear text. If intercepted by a third party it is easily read.

2.6.3. Recommended precaution

As stated above, there are not many threats that apply to the products. However, if a strict security policy is to be maintained, the LPD service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

Note1: If you want to reduce the possibility of print data being intercepted, please use HTTPS instead of LPR as the printing protocol.

2.7. IPP

2.7.1. Function Overview

The IPP (Internet Printing Protocol) service is used for Internet printing from IPP clients. This service is compliant with RFC 2565 and it uses TCP port 631.
The following functions are provided by the IPP service.

- Printing a job from an IPP client.
- Providing job status to an IPP client.

The IPP service has a user authentication function. 10 accounts are available for IPP service and the password can be set for each account. Both “BASIC” and “DIGEST” authentication are supported. “BASIC” authentication is common, but the username and password are sent in clear text. “DIGEST” authentication is more secure with the username and password irreversibly hashed and the popularity of “DIGEST” authentication had been increasing at the time of this writing.
Both authentication methods are selectable in Web Image Monitor and mshell.
IPP authentication can also be disabled. In this case, usernames and passwords are not authenticated (The default setting is “disabled”.).

2.7.2. Potential threats and recommended precaution

1) Possibility of acting as a server for relaying viruses
There is no possibility that the products will be used by a virus as an open relay server. The IPP service treats all received data as print jobs. Even if someone sends an executable file via the embedded IPP service, the products print the file as garbage data.
2) Possibility of successful DoS (Denial of Service) attacks
There is no possibility of successful DoS attacks.
When the products receive data that can carry out a DoS attack, a waiting period is implemented in the reply process of the products. This reduces the system load and stops the service and application at regular steps if data that falls outside of the specification of the protocol is present in the system.
3) Theft of username and password
Interception of network packets: When the client negotiates the connection with the MFP, the MFP can specify whether the connection uses digest-MD5 hashing for the username and password.
4) Theft of print data
Interception of network packets: Using IPP, print data is sent as clear text. If intercepted by a third party it is easily read.

2.7.3. Recommended precaution

As stated above, there are not many threats that apply to the products. However, if you want to maintain a strict security policy, we recommend the following precautions. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Set IPP Authentication to either “BASIC” or “DIGEST” from “Disabled” in Web Image Monitor, the mshell or the operation panel.

- “DIGEST” authentication is more secure than “BASIC” because the username and the password are not sent in clear text.

Level 2: Close the IPP (631/TCP) port.

- If it is not absolutely necessary, the IPP port should be closed via Web Image Monitor or the mshell.

Note1: This only closes the IPP port. The IPP service is still available using HTTP or HTTPS.

Note2: If you want to reduce the possibility of print data being intercepted, please use HTTPS instead of IPP as the printing protocol.

2.8. DIPRINT (RAW print)

2.8.1. Function Overview

The DIPRINT (Direct Print or RAW Print) service is Ricoh Company Ltd's name for port 9100 communication. This service provides direct printing from remote terminals using TCP port 9100.

2.8.2. Potential threats and recommended precaution

1) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. The DIPRINT service treats all received data as print jobs. Even if someone sends an executable file via the embedded DIPRINT service, the products print the file as garbage data.

2) Theft of username and password

Interception of network packets: DIPRINT does not have an authentication function. However, print data may contain authentication information. This information can be encrypted by the printer driver. Please refer the user manual and driver help for more information about this method.

3) Theft of print data

Interception of network packets: Using DIPRINT, print data is sent as clear text. If intercepted by a third party in is easily read.

2.8.3. Recommended precaution

As stated above, there are not many threats that apply to the products. However, if you want to maintain a strict security policy, the DIPRINT port can be changed and the port for this service can be completely closed using Web Image Monitor or the mshell.

Note1: If you want to reduce the possibility of print data being intercepted, please use HTTPS instead of DIPRINT as the printing protocol.

2.9. SMB

2.9.1. Function Overview

The SMB service uses NBT (NetBIOS over TCP/IP) as its base layer.
The NBT service provides the NetBIOS service over TCP/IP instead of NetBEUI. Using this service, a remote host can access network services of the products by the NetBIOS name (Computer Name) instead of IP address. This service uses 3 ports, UDP port 137 for NetBIOS-NS (NetBIOS Name Service), UDP port 138 for NetBIOS-DGM (NetBIOS Datagram Service) and TCP port 139 for NetBIOS-SSN (NetBIOS Session Service). SMB (Server Message Block) over TCP/IP is provided by this service as follows.

- Browsing the print servers from SMB clients
- Printing a job from SMB clients
- Sending job queue information to SMB clients
- Sending notifications of a job completion to SMB clients

2.9.2. Potential threats and recommended precautions

1) Possibility of acting as a server for relaying viruses
There is no possibility that the products will be used by a virus as an open relay server. The SMB service treats all received data as print jobs. Even if someone sends an executable file via the embedded SMB service, the products print the file as garbage data.
2) Possibility of successful DoS (Denial of Service) attacks
There is no possibility of successful DoS (Denial of Service) attacks. Repeated access and disconnection to TCP port 139 is a well known DoS (Denial of Service) attack. The products are protected against this by accepting connections sequentially. And also when the products receive data that can be used to carry out a DoS attack, the connection with the sender will be disconnected.
3) Theft of username and password
Interception of network packets: The SMB protocol has an authentication function. However the products can be accessed using a guest account. All data received via SMB will simply be printed. Therefore this does not present a major security risk because no changes can be made to the system via SMB. However some print data may contain authentication information. The password can be encrypted by enabling the printer driver’s encryption function before sending data to the MFP. Please refer to the user manual and driver help for more information about this function.
4) Theft of print data
Interception of network packets: Using SMB, print data is sent as clear text. If intercepted by a third party in is easily read.

5) Possibility products being seen on the network by unauthorized parties via browsing (i.e. via network neighborhood).
To protect the products from being browsed by unauthorized parties, NetBIOS-NS and NetBIOS-DGM services should be disabled using the mshell.

2.9.3. Recommended precaution

The suggested precautions against this threat are as follows. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Disable NetBIOS-NS and NetBIOS-DGM services using mshell

- If these services are disabled, the products will not be visible to anyone when the network is browsed (i.e. Via network neighborhood).

Level 2: Disable the SMB service

- If it is not absolutely necessary, the SMB service should be disabled via Web Image Monitor or the mshell.

Note1: If you want to reduce the possibility of print data being intercepted, please use HTTPS instead of SMB as the printing protocol.

2.10. MDNS

2.10.1. Function Overview

MDNS (Multicast DNS) is a way of using familiar DNS programming interfaces, packet formats and operating semantics, in a small network where no conventional DNS server has been installed.

The products only use MDNS for Bonjour. If Bonjour is not being used, this port can be closed.

2.10.2. Potential threats and recommended precaution

1) Possibility of unauthorized parties intercepting device information.

The products use MDNS to advertise services and device information.

If you do not want unauthorized parties to be aware of this information, the Bonjour service should be disabled using Web Image Monitor or the mshell.

2.10.3. Recommended precaution

As stated above, there are not many threats that apply to the products. However, if a strict security policy is to be maintained, the MDNS service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell. (If Bonjour is turned off, the MDNS port is closed automatically.)

2.11. HTTPS

2.11.1. Function Overview

HTTPS is HTTP over SSL (Secure Socket Layer). HTTPS provides the same functions as HTTP. HTTPS maintains higher security than HTTP because SSL provides the following features:

- Server authentication/certification. (Protects against server spoofing.)
- Data Encryption. (Protects against wiretap/falsification.)

*About SSL

SSL is a communication technology used for secure connections between 2 hosts. The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. SSL is layered on top of some reliable transport protocol (e.g., TCP). SSL allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.

2.11.2. Potential threats and recommended precaution

1) Destruction, corruption or modification of the file system

There is no possibility of destruction, corruption or modification of the file system. Because no one can access the file system and executable files cannot be processed on the products web server.

2) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. The web server was developed by Ricoh and does not allow any malicious and executable files to be processed.

3) Theft of username and password

When using HTTPS, all data including the username and password is encrypted using SSL. This is safer than sending username and passwords encoded in Base 64 (using the HTTP).

4) Theft of print data

Interception of network packets: Using HTTPS, all data sent over the connection is encrypted. Therefore, even if data is intercepted, it will be extremely difficult for unauthorized parties to read.

2.11.3. Recommended precaution

The following are suggested precautions against threats to the HTTPS service. The levels

described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the user name and password from the default value to something difficult to guess and change them regularly.

- The username and password are the same as the one for logging in to the mshell. So, changing the username and password for Web Image Monitor's Administrator mode means changing them for the mshell as well.

Level 2a: Close the HTTPS port.

- The HTTPS port can be completely closed with mshell. In this case, both Web Image Monitor and IPP (Internet Print Protocol) are unavailable via HTTPS. If the HTTPS port is closed, Web Image Monitor and IPP printing are still available via HTTP.

Level 2b: Disable web function.

- If it is not needed, Web Image Monitor can be disabled using the mshell. When web is set to 'Down', Web Image Monitor does not activate and the error "503 Service Unavailable" is displayed. Even when not in use, TCP port 443 stays open and is therefore HTTPS is available for IPP printing.

2.12. SNMP v3

2.12.1. Function Overview

SNMP v3 provides the same functions as SNMP. SNMP v3 maintains higher security than SNMP v1 and v2 because SNMP v3 has the following features:

- User Authentication
- Data Encryption

2.12.2. Potential threats and recommended precautions

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system.

SNMP only permits write-access to network parameters. No one can access the file system or kernel.

2) Theft of username and password

Interception of network packets: When using SNMP v3, the password is hashed using SHA1 or MD5.

Brute force attack: To protect against brute force attempts at acquiring the SNMP password, the products limit the number of incorrect connection attempts to 100. After 100 attempts, the machine will enter a lockout mode that disables any incoming connection attempts for a specified length of time (60 seconds).

3) Possibility of unauthorized parties intercepting device information:

Interception of network packets: The products do not respond with important information such as administrator password even if the SNMP client sends a get request for this information. Therefore security risk is low. In addition the products encrypt other parameters. (Please refer to Appendix F)

2.12.3. Recommended precaution

The suggested precautions against this threat are as follows. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the usernames and password from the default value and the passwords for each user to something difficult to guess and change it regularly.

Level 2: Encrypt all data.

Level 3: Disable the SNMP v3 service.

- If it is not absolutely necessary, the SNMP v3 service should be disabled via Web Image Monitor or the mshell.

Level 4: Close the SNMP port.

- If it is not absolutely necessary, the SNMP port should be closed via Web Image Monitor or the mshell.

2.13. H323hostcall/SIP

2.13.1. Function Overview

H323/SIP services are used to provide VoIP (Voice over IP) for IP-Fax. The H.323 hostcall service is compliant with ITU-T standards and uses TCP port 1720. The SIP service is compliant with RFC3261 and uses TCP/UDP port 5060.

2.13.2. Potential threats and recommended precautions

1) Possibility of successful DoS (Denial of Service) attacks.
H323hostcall/SIP is only able to maintain a single session. In addition, session's timeout if a recognizable response is not sent within a specified period. Therefore it is unlikely that the service could be stopped via DoS.
2) Theft of username and password
The SIP protocol supports the authentication function. However the products do not support authentication using the SIP protocol. Therefore the username and password are not included with data sent over this protocol.
3) Theft of facsimile data
Interception of network packets: Using IP-Fax, facsimile data is formatted for an ISDN connection and is not encrypted. If intercepted by a third party it can be read.

2.13.3. Recommended precaution

As stated above, there are not many threats that apply to H323hostcall/SIP. However, if a strict security policy is to be maintained, the TCP/UDP port numbers for H323hostcall (1720) and for SIP (5060) can be changed by a customer engineer. However, these services cannot be stopped.

2.14. SSDP

2.14.1. Function Overview

SSDP (Simple Service Discovery Protocol) is used for both advertising services and searching for services on UPnP network. SSDP uses UDP port 1900. If UPnP is not being used, this port can be closed.

2.14.2. Potential threats and recommended precautions

1) The possibility of unauthorized parties intercepting device information.
The products use SSDP to advertise services and search for services. If you do not want to unauthorized parties to be aware of this information, the SSDP service should be disabled using Web Image Monitor or the mshell.

2.14.3. Recommended precaution

If a strict security policy is to be maintained, the SSDP service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

2.15. SFTP (SSH)

2.15.1 Function Overview

The SFTP (“Secure File Transfer Protocol” or “SSH File Transfer Protocol”) service provides the same functions as FTP. SFTP uses an SSH (Secure Shell) session over TCP port 22. The SSH provides the following features:

- Data Encryption. (Protects against interception/falsification).

*Abut SSH

SSH (Secure Shell) is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over unsecured channels. It is intended as a replacement for rlogin, rsh, and rcp. Additionally, ssh provides secure X connections and secure forwarding of arbitrary TCP connections. Ricoh’s implementation of SSH is based on OpenSSH. For information about OpenSSH, please see:
http://www.openssh.com/

2.15.2 Potential threats

1) Destruction, corruption and modification of the file system or kernel:

There is no possibility of destruction, corruption or modification of the file system or kernel. Although the SFTP service permits write-access, any files that are received by the printer are considered to be a print job or firmware data. When the embedded SFTP server receives an executable file, the products print a binary representation (garbage characters) of the data contained in the executable. As for firmware, a dedicated account and password is required to input firmware to the printer using the SFTP service. In addition, data is verified by checking the header, IDs and the file format before being applied as firmware.

2) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. Although the SFTP service permits write-access, any data written to the device (executable or otherwise) is treated as a print job and output as ASCII data.

3) Theft of username, password, and device information

Using SFTP, all data including the username and password is encrypted using DES, 3DES or AES.

4) Theft of print data

Interception of network packets: Using SFTP, all data sent over the connection is encrypted. Therefore, even if data is intercepted, it will be difficult for unauthorized parties to read.

2.15.3 Recommended precaution

The following are suggested precautions against threats to the SFTP service. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the username and password from the default value to something difficult to guess and change them regularly.

- The username and password are the same as those used for logging in to the shell.

Level 2: Close the SSH port.

- SFTP is used over TCP port 22. The SFTP port can be closed with mshell or WebImageMonitor. If closed, both printing and firmware updating are unavailable via SFTP.

2.16. Others

TCP port 7443 and 7444 are reserved for @Remote service. This service accepts only a Ricoh-confidential protocol and it is impossible to emulate it without knowledge of the protocol specification. In addition, we will not disclose the protocol specification to anyone outside of Ricoh Company, Ltd. As just described, there are no threats that apply to the products. However if a strict security policy is to be maintained, those ports can be closed via TELNET. (Please refer to Appendix C.)
HTTPS is used for this service as an underlying layer. Please refer to “2.11 HTTPS” for the potential threats and recommended precautions for HTTPS.

3. Other Network Services

The Previous section dealt mainly with port based network services. This section will describe security related information for non-port based network services.

3.1. Wireless LAN

3.1.1. Overview

WLAN utilizes spread spectrum technology based on radio waves to enable communication between devices in a limited area. This gives users the mobility to move around within a broad coverage area and still be connected to the network. The absence of cables leaves transmissions extremely susceptible to interception. For this reason a variety of security precautions have been incorporated into WLAN specifications.
[SSID only] All data is sent as clear text without any authentication or integrity checking. As wireless data is available to anyone within range, unencrypted data is extremely susceptible tampering and theft.

[WEP]
'WEP' (Wired Equivalent Privacy) is a security standard settled on by IEEE, and adopted as IEEE802.11. Using WEP, data can be encrypted with a shared key (RC4). Access to the network is based on a WEP key configured on the clients and the Access Points. Although WEP provides a degree of security, it does have vulnerabilities. 'WPA' was created to overcome the vulnerabilities in WEP. The products support not only WEP but also WPA.

[WPA]
'WPA' (WiFi Protected Access) is a subset of IEEE802.11i. It utilizes a key exchange system to constantly change the shared key. Users can select either TKIP or CCMP. If a device does not support WPA2, CCMP may not be selected. TKIP uses RC4 as an encryption algorithm and is intended for use with legacy systems that do not yet support CCMP. In addition to providing key exchange, CCMP uses the AES encryption algorithm which is a stronger than RC4.

Encryption method	WEP	WPA	
		TKIP	CCMP
Encryption algorithm	RC4	RC4	AES
Shared key size	40/104 bit	104 bit	128 bit
Key exchange / refreshing method	- / Not refreshed	Yes / Timely refreshed	

WPA employs four authentication modes: 'WPA-PSK', 'WPA2-PSK', 'WPA (802.1X)' and 'WPA2 (802.1X)'. WPA-PSK/WPA2-PSK is similar to WEP in that a pre-shared key is used to join the network. However, as an encryption key is generated in handshake process, WPA-PSK/WPA2-PSK is more secure than WEP in that point. WPA (802.1X)/WPA2 (802.1X) is much more strict. Only users that can be authenticated by a RADIUS server using EAP are allowed to join the network. Supported EAP authentication types are:

- EAP-TLS
- EAP-TTLS
- PEAP
- LEAP

3.1.2. Potential Threats

1) SSID only (no encryption)

All data (including the SSID) is transmitted in plain text. It is easily readable by anyone within range of the wireless transmission.

2) WEP

WEP provides RC4 encryption of data and is therefore more secure than using only an SSID. However the weaknesses of RC4 encryption are well documented. Note: WPA TKIP uses RC4. However, because the keys are being constantly refreshed, the key will change before an attacker has time to crack it.

3) WPA

In WPA, the encryption key is generated at interval by TKIP or CCMP. The key does not need to be entered manually. As the key is refreshed so often, a brute force attack is almost impossible. Furthermore, CCMP uses AES, which is a stronger encryption method than RC4. As an added precaution, WPA (802.1X) /WPA2 (802.1X) provides user authentication.

3.1.2. Recommended Precaution

The suggested precautions against this threat are as follows. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: General Access Point settings

- Prohibit broadcast of the SSID.
- Prohibit connections that do not have the correct SSID.
- Limit connections to only specific MAC addresses.

* Off course, SSID is just used for the connection identification, not for the security purpose. Therefore, we recommend that user apply the security level below.

Level 2: WEP

* It is more secure if user changes the WEP key regularly.

Level 3: WPA-PSK/WPA2-PSK

Level 4: WPA (802.1X)/WPA2 (802.1X) instead of WPA-PSK/WPA2-PSK.

* Please refer to Appendix I for an explanation of how to configure these settings.

4. Appendix

A) The list of services provided with open TCP/UDP ports

Protocol	Port Num.	Login	Username Changeable	Password	Password Changeable	Note
TELNET	23/TCP	Y	Y	Y	Y	This is the same username and password as are used for Web Image Monitor.
FTP-control	21/TCP	Y	N/A	N/A	N/A	For RFU, administrator privilege is required.
HTTP	80/TCP	Y	Y	Y	Y	This is the same username and password as are used for TELNET. The unauthorized users can only read access is available.
netbios-ns	137/UDP	N/A	N/A	N/A	N/A	
netbios-dgm	138/UDP					
netbios-ssn	139/TCP					
SNMP	161/UDP	Y	Y	N/A	N/A	Although there is no concept of user accounts, it can perform access restrictions using the Community Name. Up to 10 Communities can be registered.
SNMPv3	161/UDP	Y	Y	Y	Y	This is the same username and password as are used for TELNET. If no password is input, then only read access is available.
HTTPS	443/TCP	Y	Y	Y	Y	This is the same username and password as are used for TELNET. If no password is input, then only read access is available.
RSH/RCP (shell)	514/TCP	N/A	N/A	N/A	N/A	
LPD	515/TCP	N/A	N/A	N/A	N/A	

Protocol	Port Num.	Login	Username Changeable	Password	Password Changeable	Note
IPP	631/TCP	Y	Y	Y	Y	Authentication by account/password is not performed by default. In this case all users are ANONYMOUS. When IPP authentication is enabled, a username and password will be required.
H323gatestat	1719/UDP	N/A	N/A	N/A	N/A	If the products are configured to use ‘gatekeeper’, this port is opened so the products can register its information with gatekeeper.
H323hostcall	1720/TCP	N/A	N/A	N/A	N/A	
SSH	22/TCP	Y	Y	Y	Y	SSH is only used for SFTP. For RFU, administrator privilege is required. For SFTP, RFU is not available via Web Smart Device Monitor.
SIP	5060/TCP, UDP	N/A	N/A	N/A	N/A	The SIP protocol supports authentication. However we do not support SIP authentication with our products.
MDNS	5353/UDP	N/A	N/A	N/A	N/A	
@Remote	7443/TCP 7444/TCP	-	-	-	-	
SSDP	1900/UDP	N/A	N/A	N/A	N/A	
DIPRINT	9100/TCP	N/A	N/A	N/A	N/A	
RFU	10021/TCP	Y	-	-	-	This port functions similarly to an FTP port and used for Web Smart Device Monitor.

B) Related Protocols

Protocol	Protocol Suite	Commonly Used Port Num.	Description of the protocol's function in the Products.
IP	TCP/IP	-	-
ICMP	TCP/IP	Protocol Num. 1	-
UDP	TCP/IP	Protocol Num. 17	-
TCP	TCP/IP	Protocol Num. 6	-
FTP-data	TCP/IP	20/tcp, udp	1) Sending scan data to the FTP server. (Scan to FTP) 2) Sending scan data to ScanRouter
FTP-control	TCP/IP	21/tcp, udp	
SMTP	TCP/IP, IPX/SPX	25/tcp, udp	1) Sending scan data to the SMTP server. (Scan to E-mail)
Domain (DNS)	TCP/IP	53/tcp, udp	1) Resolving IP addresses from the server name.
BOOTP DHCP	TCP/IP	67/tcp, udp 68/tcp, udp	1) Getting IP addresses and other network parameters from the DHCP server.
POP	TCP/IP	110/tcp, udp	1) Using POP before SMTP authentication for 'Scan to E-mail'. 2) Receiving internet-fax data.
SNTP	TCP/IP	123/tcp, udp	1) Getting GMT from the NTP server.
NETBIOS-NS	TCP/IP, IPX/SPX, NetBEUI	137/tcp, udp	1) Sending scan data to SMB clients. (Scan to SMB)
NETBIOS-DGM		138/tcp, udp	
NETBIOS-SSN		139/tcp, udp	
IMAP	TCP/IP	143/tcp, udp	1) Getting internet-fax data
SNMP-trap	TCP/IP, IPX/SPX	162/tcp, udp	1) Sending status information to Network Management Server.
LDAP	TCP/IP	389/udp, tcp	1) Searching e-mail addresses from the LDAP server's address book.
syslog	TCP/IP	514/udp	1) Sending system logs to a syslog server.

Protocol	Protocol Suite	Commonly Used Port Num.	Description of the protocol's function in the Products.
NCP	TCP/IP, IPX/SPX	524/tcp, udp	1) Logging in to a Netware server. 2) Printing from the Netware environment.
SLP	TCP/IP	427/tcp, udp	1) Searching for a Netware Server.
IPX	IPX/SPX	-	1) Providing ipx connections
SPX	IPX/SPX	-	1) Providing spx connections
SAP	IPX/SPX	-	1) Broadcasts to availability of print services.
RIP	IPX/SPX	-	1) Broadcasts route information.
APPLETALK	APPLETALK	-	1) Providing appletalk connections.
PAP	APPLETALK	-	1) Providing appletalk printing services
NETBEUI	NETBEUI	-	1) Providing netbeui connections.

Commonly User Port Number: This is meant to be general information. This column contains well-known port numbers commonly used in industry. This is not necessarily the port used by the products.

C) The Purpose of Access Control

The printer will accept communication only from a set range of IP addresses. This can be applied to connections from LPR, RSH/RCP, HTTP, HTTPS, FTP, DIPRINT, SMB, IPP, and DeskTopBinder.

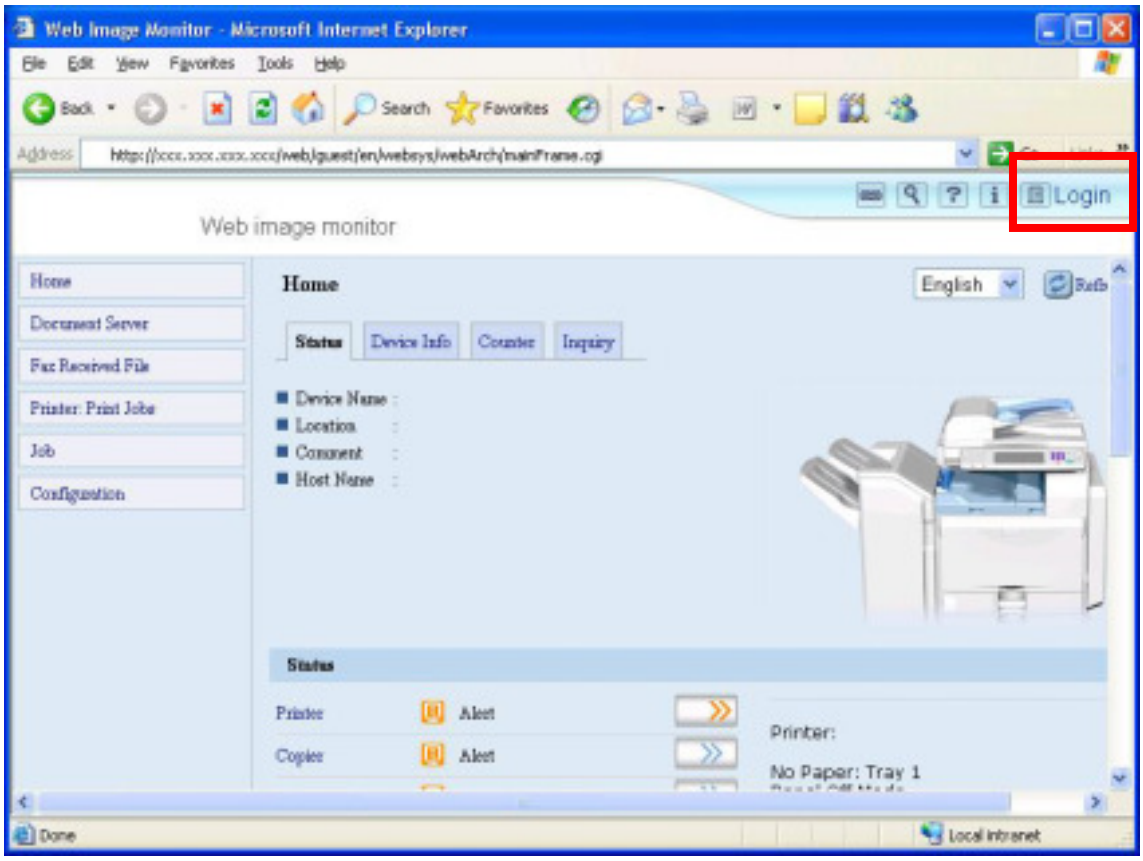
These cannot be applied to TELNET and SmartDeviceMonitor.

C)-1 The Purpose of Access Control – Web Image Monitor

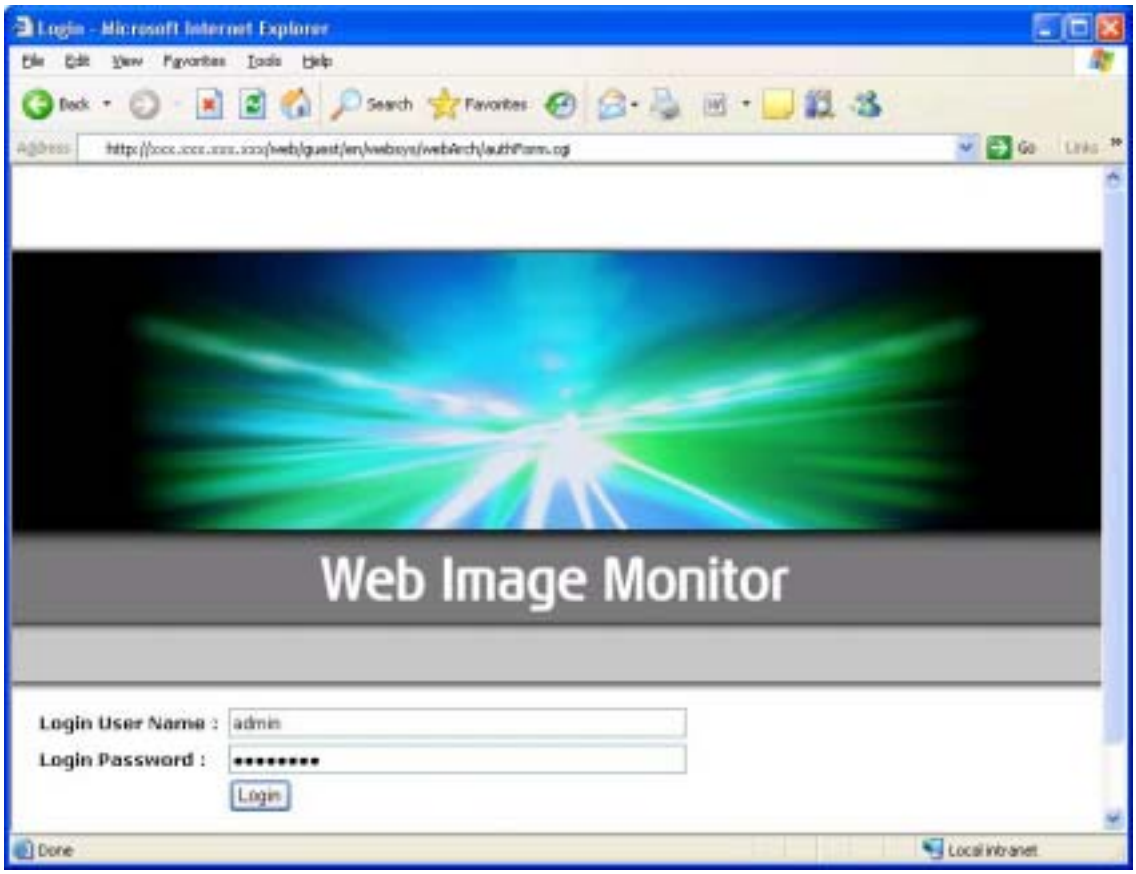
(1) Web Image Monitor can be used for accessing the products. A supported Browser such as Microsoft Internet Explorer and the product's IP address is required. Enter the IP address as shown below.

HTTP://<<printer host name or IP address>>

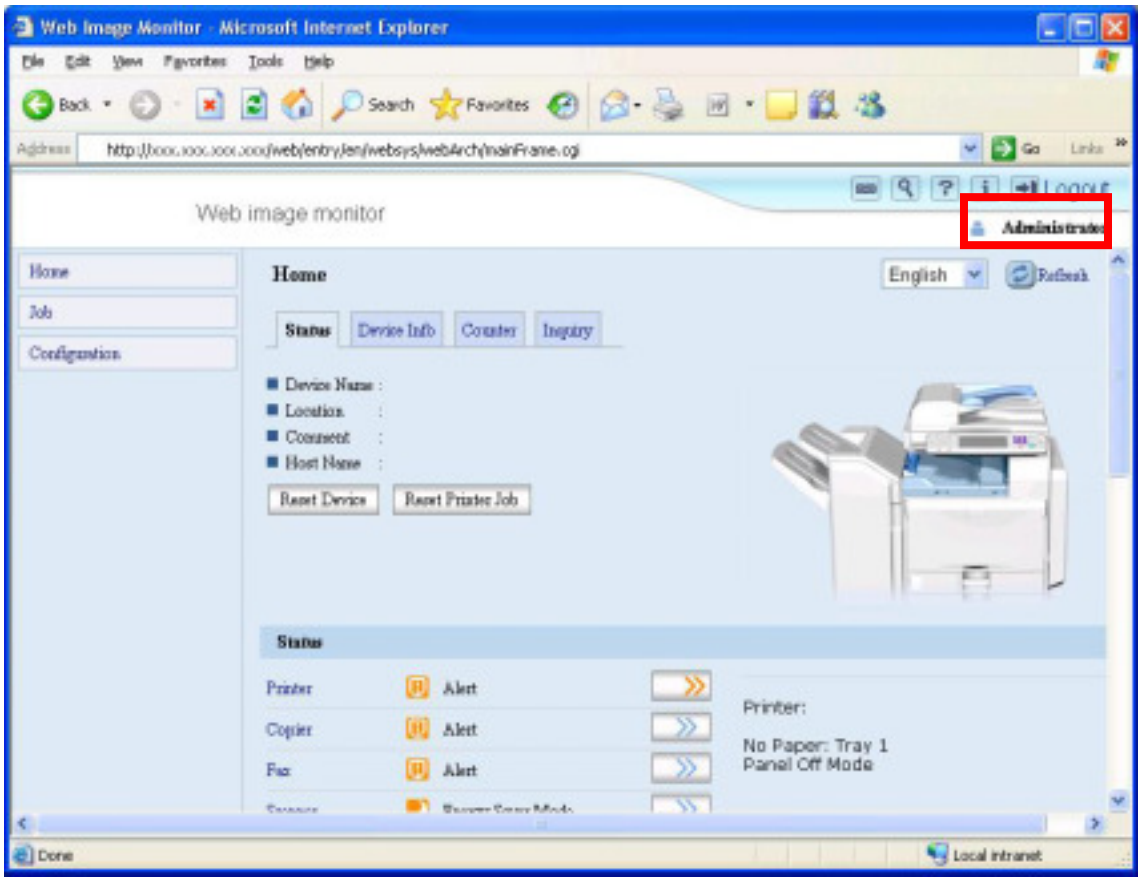
And then click "Login"



(2) In order to access Administrator mode, a username and password are required.



(3) Login to enter Administrator mode.



The 4 administrator types are identified as follows:

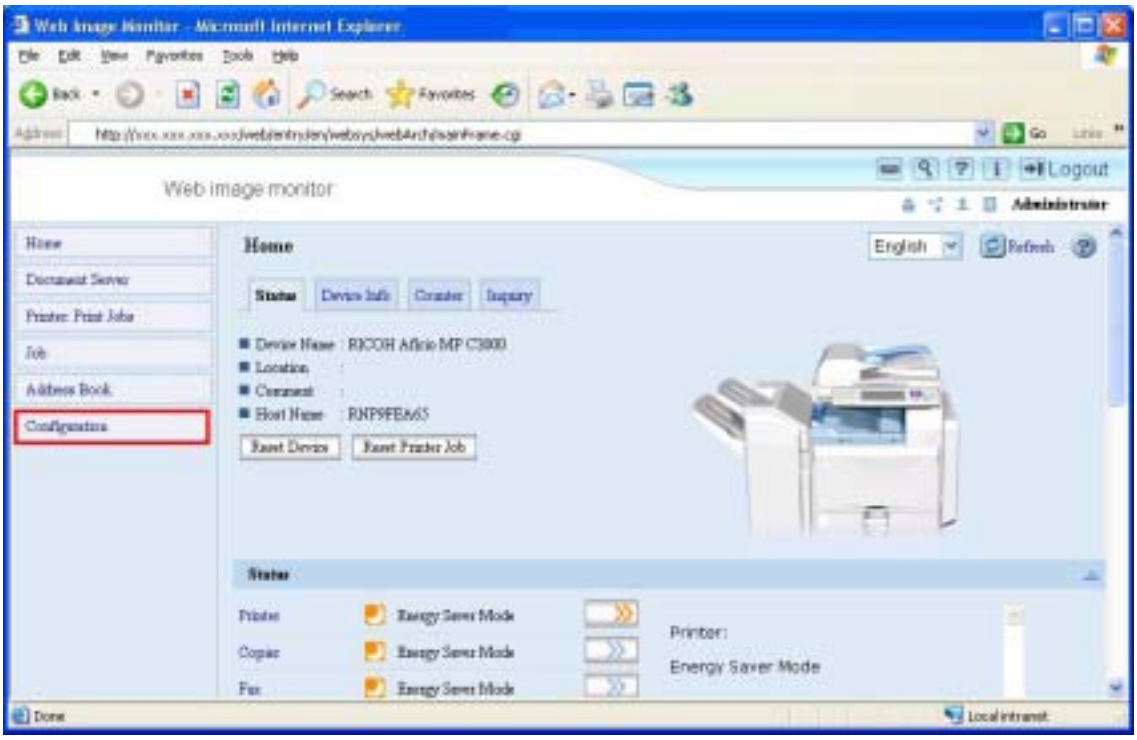
: Machine Administrator

: Network Administrator

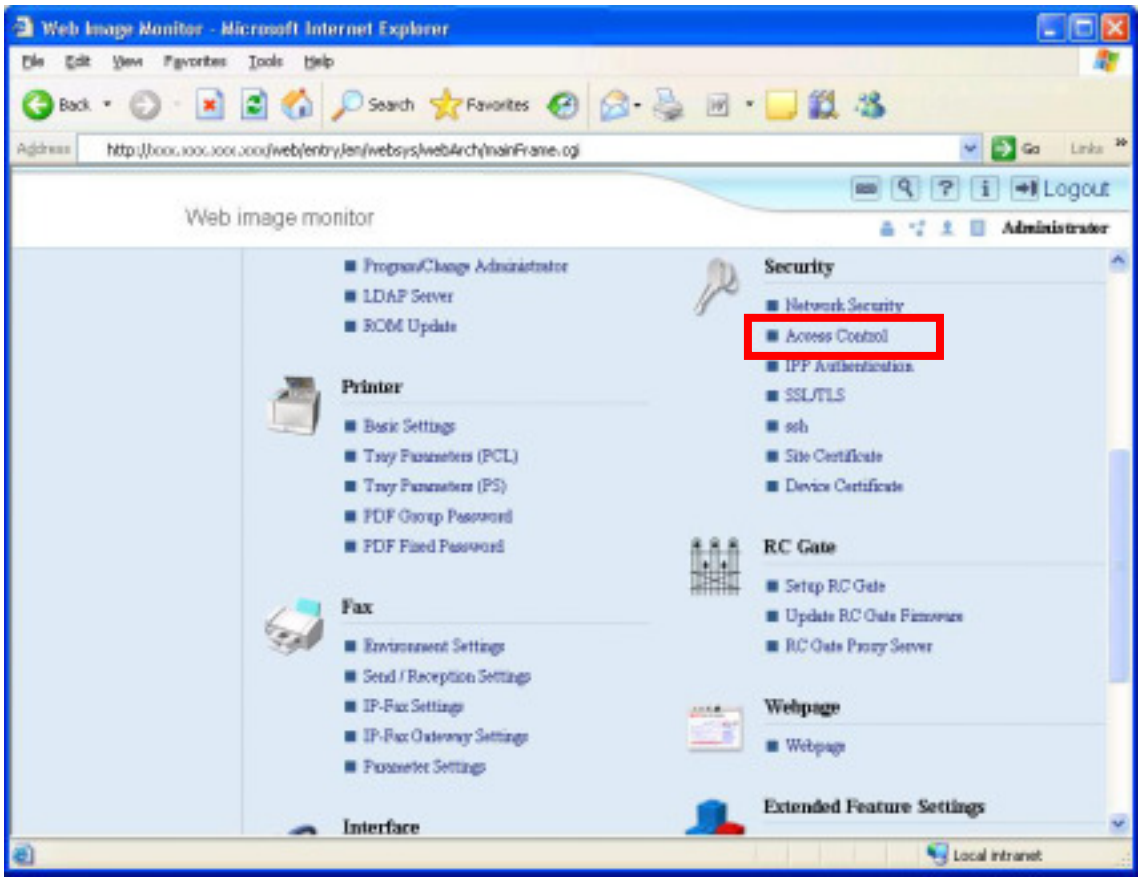
: User Administrator

: File Administrator

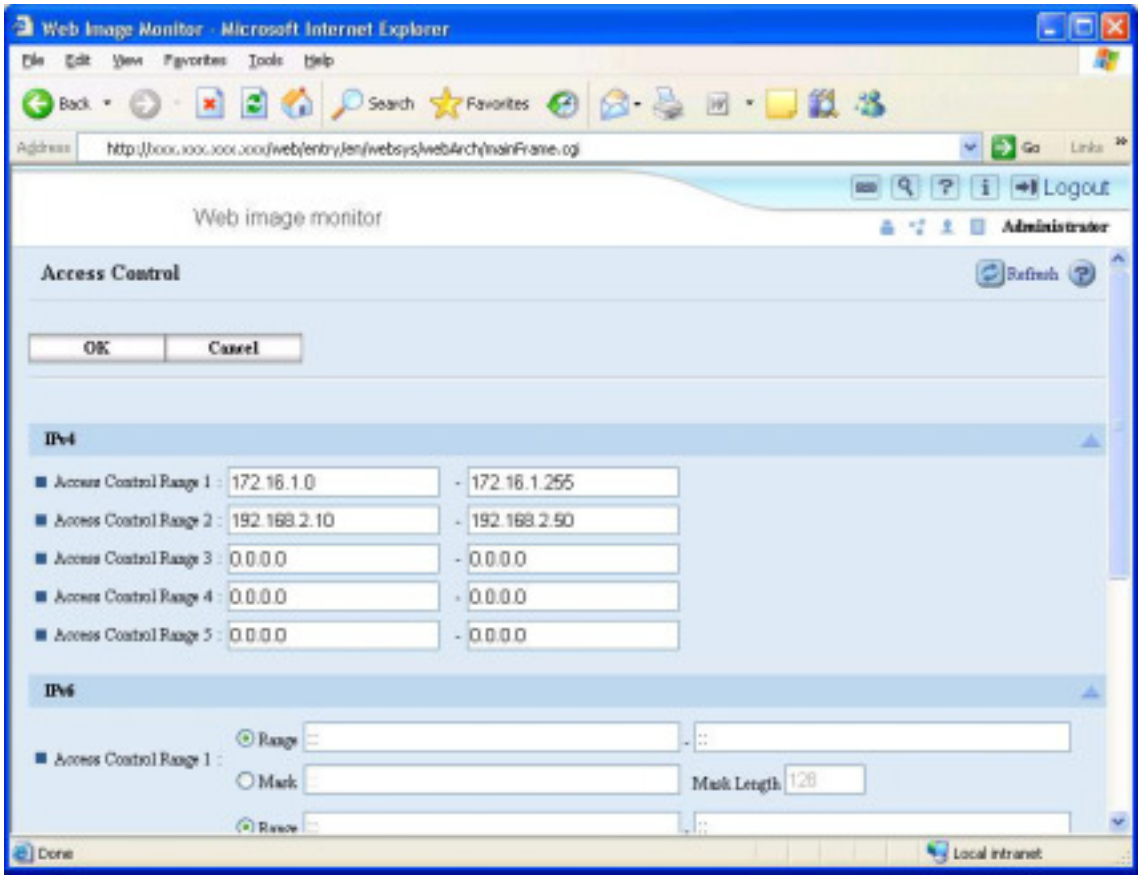
(4) Click ‘Configuration’.



(5) To open the access control settings, click ‘Security’ -> ‘Access Control’.



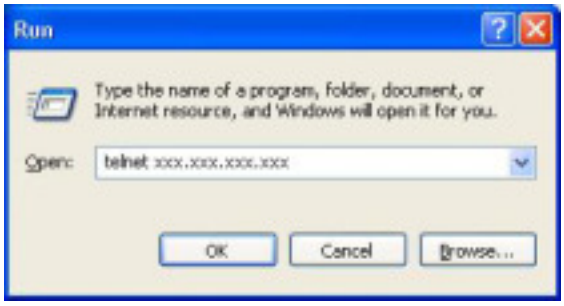
(6) Input the range of IP addresses that you wish to permit communication with.
Click the ‘OK’ button to commit the changes.



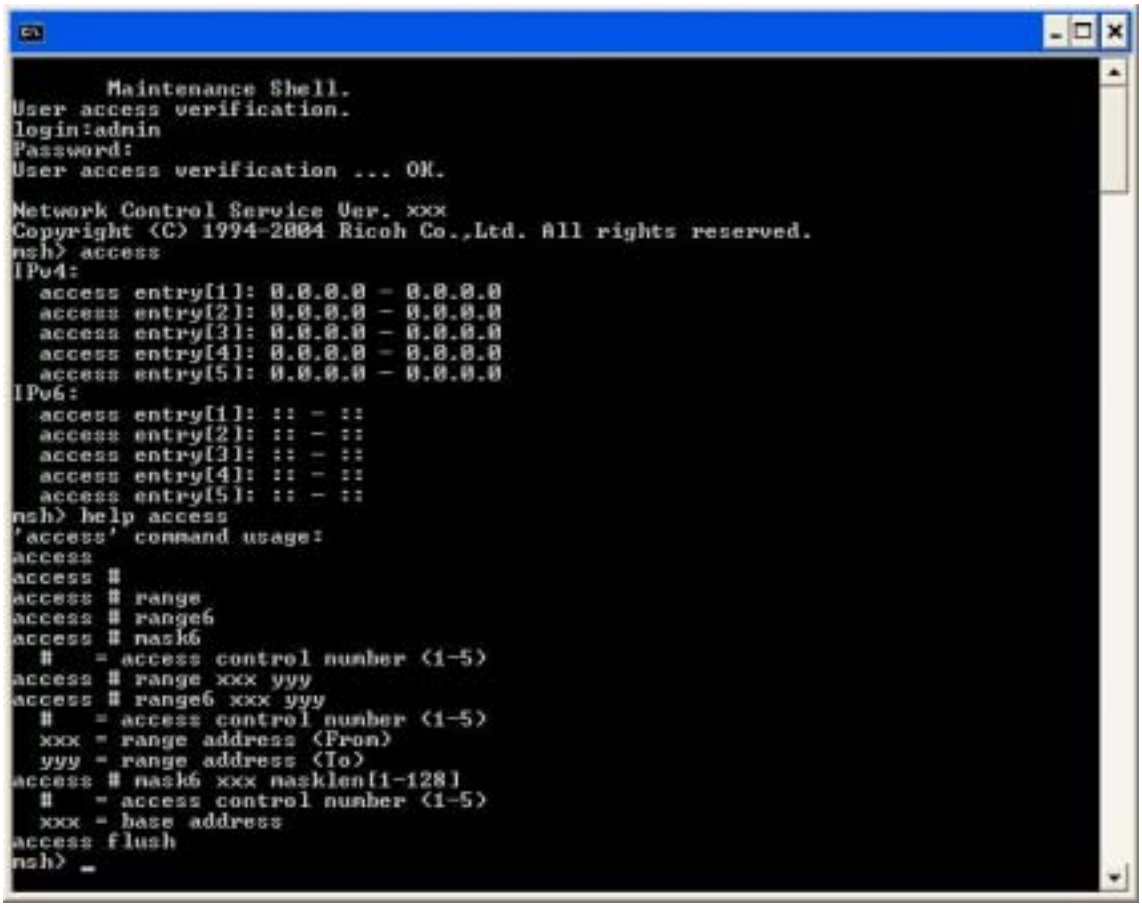
C)-2 The Purpose of Access Control – mshell

The following example is shown using the Windows XP telnet client.

(1) Access the products, using the command prompt. Launch the telnet command prompt from the Run menu as shown below.



(2) Open the Maintenance Shell (mshell). A username and password will be required for this. Using the access command input the access control range.



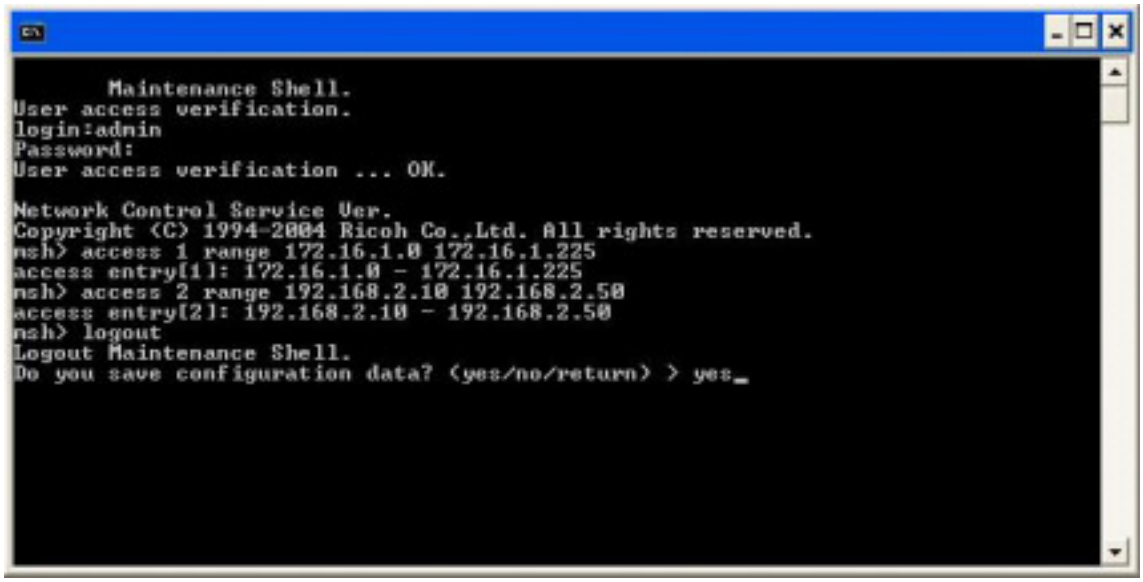
E.g.1 Input the following command to permit only access from 172.16.1.0 to 172.16.2.0

msh> access 1 range 172.16.1.0 172.16.2.0

E.g.2 Input the following command to clear all access ranges.

msh> access flush

(3) If changes have been made, the following question will appear before the user logs out. ‘Do you save configuration data?’ Input ‘yes’ to commit the changes. Input ‘no’ to discard them.



D) How to disable services

The following table describes whether services or ports can be open or close with Web Image Monitor and mshell.

See 'H) Network Security Level Settings' to open or close the services or ports when using Web Image Monitor. Also, see 'D)-2 How to disable services – mshell' to open or close the services or ports when using mshell. Some ports cannot be closed via above settings. See comments in table below.

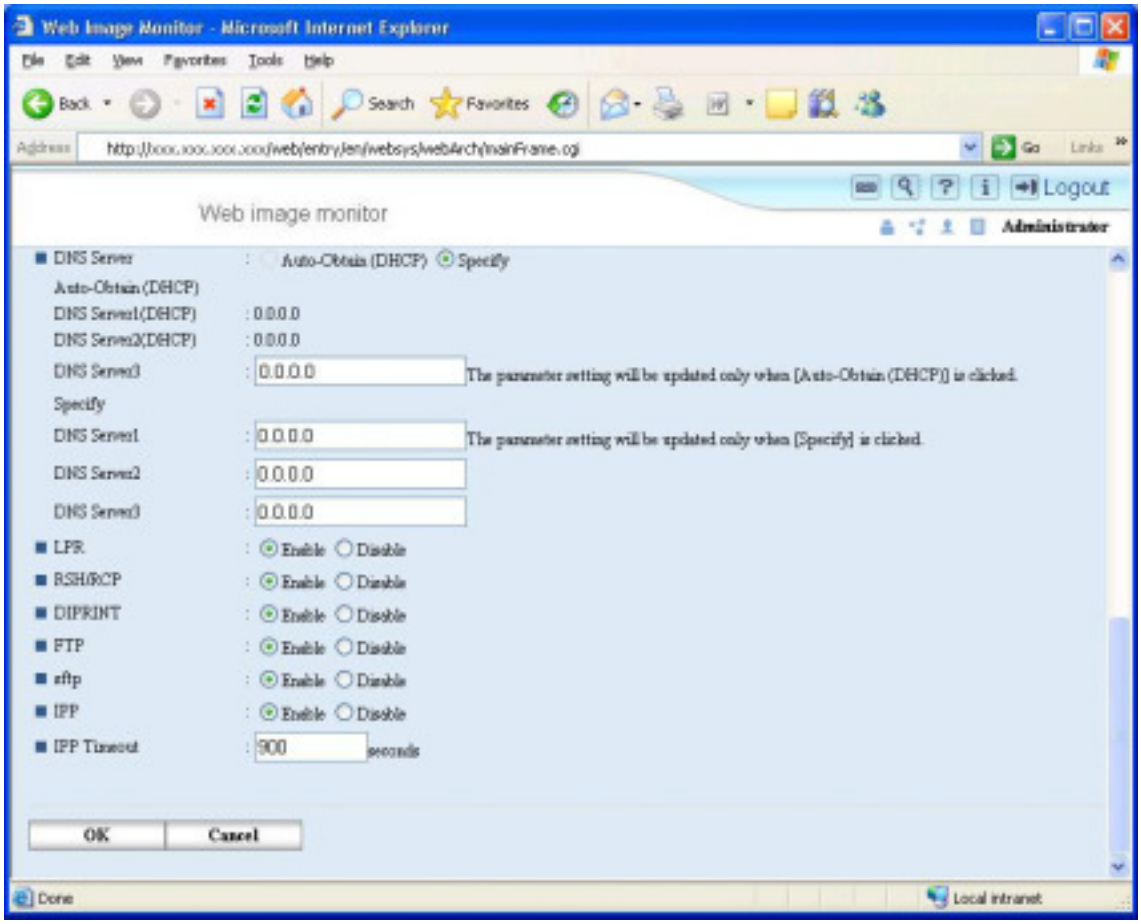
Service/Protocol	Port	Web Image Monitor		mshell		Comment
Netware	-	Y		Y		* Setting Netware to down, disables the IPX/SPX protocol and NCP/IP. Therefore if Netware is down, printing in the IPX/SPX environment and in the pure IP environment is unavailable. LPR in NDPS and iPrint (IPP Printing) are unaffected.
AppleTalk	-	Y		Y		
		IPv4	IPv6	IPv4	IPv6	
TCP/IP	-	Y	Y	Y	Y	* It is not possible to set own TCP/IP version via Web Image Monitor. For example, in order to disable TCP/IPv4, it needs to be connected via TCP/IPv6.
FTP	21	Y	Y	Y	Y	* Setting FTP to down, closes FTP port (21/tcp). The FTP server service will be down but the FTP client function is still available. Therefore if this function is down, Scan to FTP is still available.
SSH/SFTP	22	Y	Y	Y	Y	* If either of ssh or sftp is set to down, this port will be closed.
TELNET	23	Y	Y	-	-	* telnet cannot be disabled via mshell.
SMTP	25	Y	-	-	-	* In order to close this port, set [Configuration] – [E-mail] – [Reception Protocol] to 'POP3' or 'IMAP4'.
HTTP	80	Y	Y	Y	Y	*. 'set web down' does not close this port. In order to close this port via mshell, type 'set http down'. * In order to close this port via Web Image Monitor, it needs to be connected via HTTPS or IPv6.
IPP	631	Y	Y	Y	Y	
NBT	137/138	Y	-	Y	-	* Setting NBT to down, closes NetBIOS-NS (137/UDP) and NetBIOS-DGM (138/UDP)
SMB	139	Y	-	Y	-	* Setting SMB to down, closes NetBIOS-SSN (139/TCP) and NETBEUI service will be down.

						However affects only the server service. The client service is not affected. Therefore, if SMB is down, Scan to SMB can still be used.
SNMP	161	Y	Y	Y	Y	* See 'F)-1 SNMP settings – Web Image Monitor' to close this port. * Setting SNMP to down, closes SNMP port (161/udp). In addition when SNMP is down, the SNMP trap function and SNMP function over IPX/SPX are not available.
SSL	443	Y	Y	Y	Y	*Setting SSL to down, closes HTTPS. * HTTP and HTTPS cannot be closed at the same time from Web Image Monitor.
RSH/RCP	514	Y	Y	Y	Y	
LPR/LPD	515	Y	Y	Y	Y	
H.323	1720	Y	-	-	-	* In order to close this port, set [Configuration] – [Fax] – [IP-Fax Settings] – [Enable H.323] to 'Off' in Web Image Monitor. * This port cannot be closed via mshell.
SSDP	1900	Y	-	Y	-	* Settings SSDP to down makes UPnP is unavailable and closes the SSDP port (1900/UDP)
MDNS	5353	Y	-	Y	-	* In order to close this port, set 'Bonjour' to down.
SIP	5060	Y	-	-	-	* In order to close this port, set [Configuration] – [Fax] – [IP-Fax Settings] – [Enable SIP] to 'Off' in Web Image Monitor * This port cannot be closed via mshell.
@Remote	7443/7444	-	-	Y	-	* In order to disable this service, type 'set nrs down' in mshell.
DIPRINT	9100	Y	Y	Y	Y	* If this port is closed, printing from diprint client is not available.
RFU	10021	-	-	Y	Y	* If this port is closed, remote firmware update will be done via ftp. Then password will be sent in plain text.

D)-1 How to disable services – Web Image Monitor

Steps (1) to (4) are the same as C)-1.

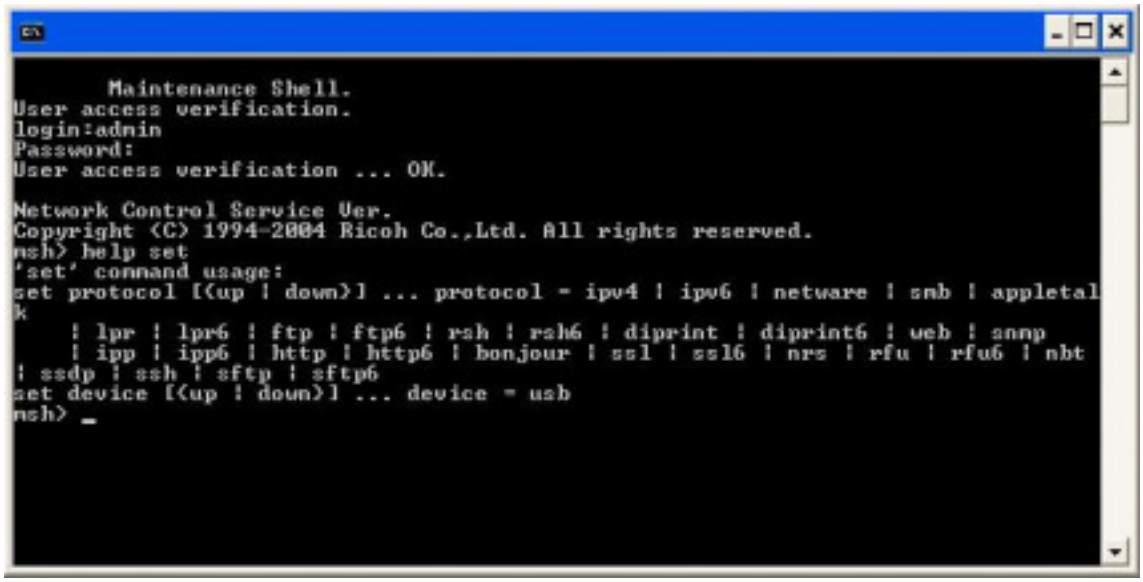
(5) Click ‘Network’ -> ‘IPv4’ to access the IPv4 protocol settings. By default all protocols are enabled. Similarly, by clicking ‘Network’ -> ‘IPv6’, the IPv6 protocols can be enabled or disabled.



D)-2 How to disable services – mshell

(1) The procedure for this is the same as is shown in section C)-2

(2) Using the ‘set’ command, input the access control range.

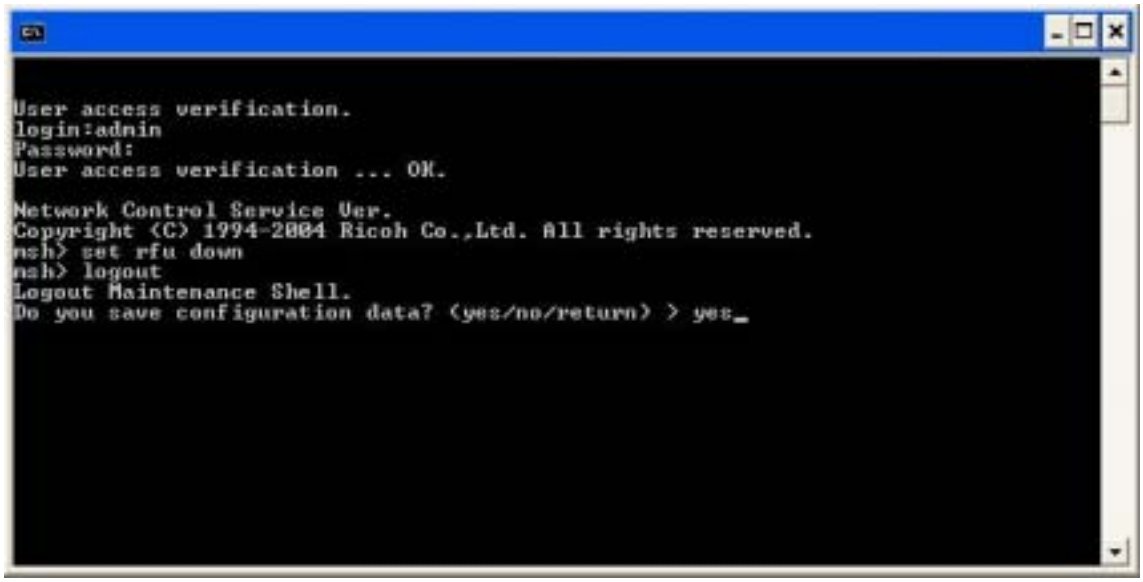


E.g.1 Input the following command to disable the HTTP protocol.

msh> set HTTP down

Note1: TELNET does not appear in the help menu.

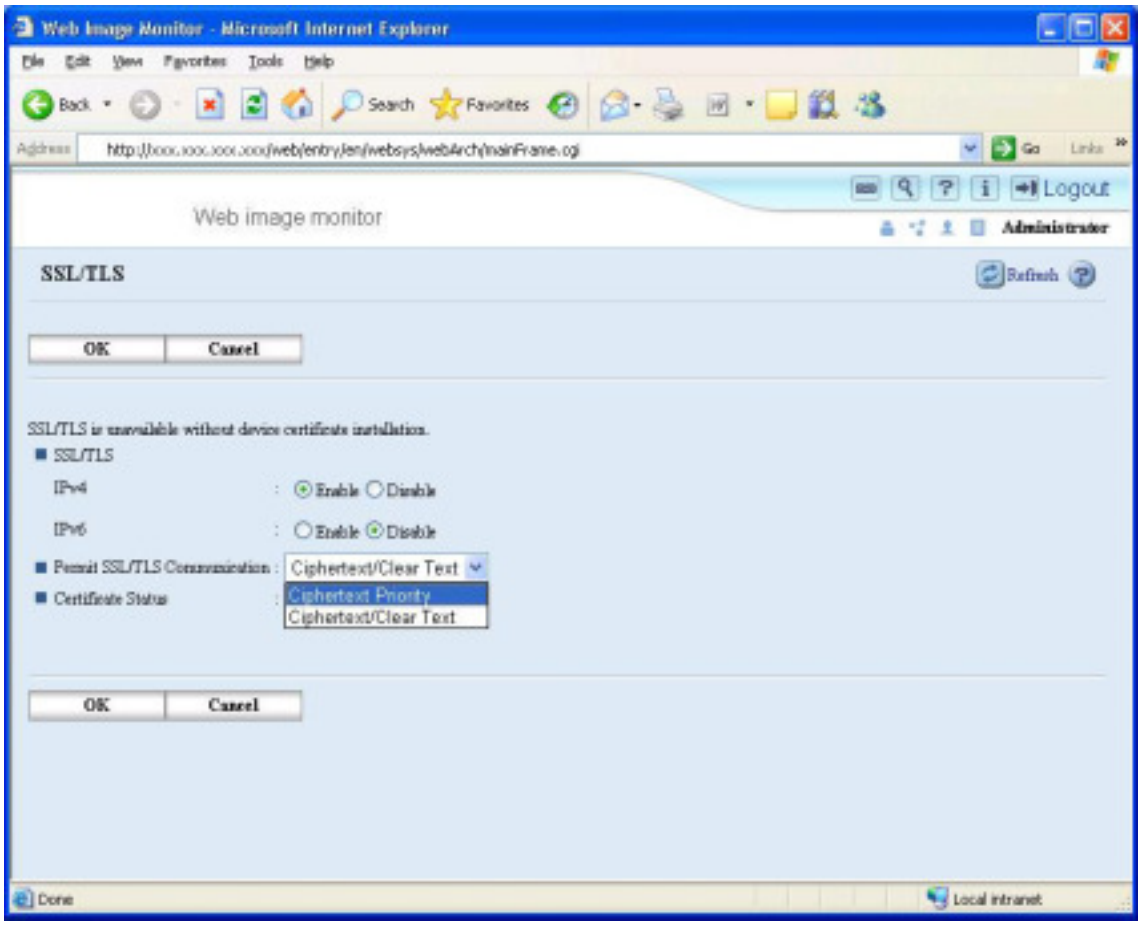
(3) The procedure for this is the same as is shown in section C)-2



E) HTTP/HTTPS settings

Steps (1) to (4) are the same as C)-1.

(5) To access the SSL/TLS settings, click ‘Security’ -> ‘SSL/TLS’.



- Permit SSL/TLS Communication

Ciphertext/Clear Text: Permit both HTTPS and HTTP connections. No forwarding of HTTP to HTTPS.

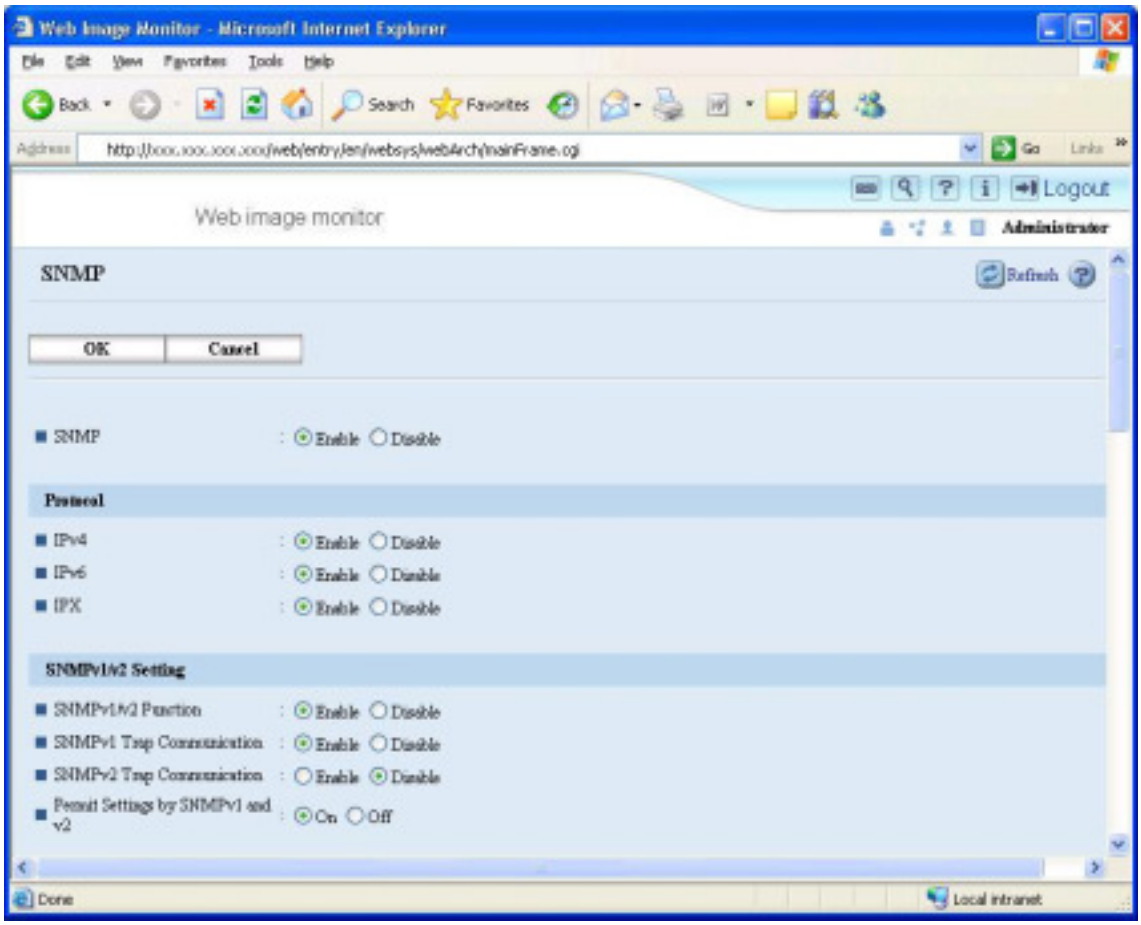
Ciphertext Priority: Any incoming HTTP request that can be forwarded to HTTPS, will be forwarded. With this setting it will be possible to use HTTPS from Internet Explorer, Netscape Navigator, etc. (HTTP will be forwarded) but not using IPP from SmartDeviceMonitor for Client etc. (these requests can not be forwarded). If the request cannot be forwarded to HTTPS, HTTP will be permitted.

Ciphertext Only: Permit only HTTPS connections. All incoming HTTP requests will be forwarded to HTTPS. If the request cannot be forwarded, the connection will be rejected.

F)-1 SNMP settings – Web Image Monitor

Steps (1) to (4) are the same as C)-1.

(5) To access the SNMP (v1/v2) settings, click ‘Network’ -> ‘SNMP’.



- SNMP

(This setting can be configured either from here or from the SNMPv3 settings.)

Enable: Opens the SNMP port

Disable: Closes the port completely. No SNMP communication of any version can be used.

- SNMP v1/v2 Function

Enable: Allows the use of SNMP v1/v2.

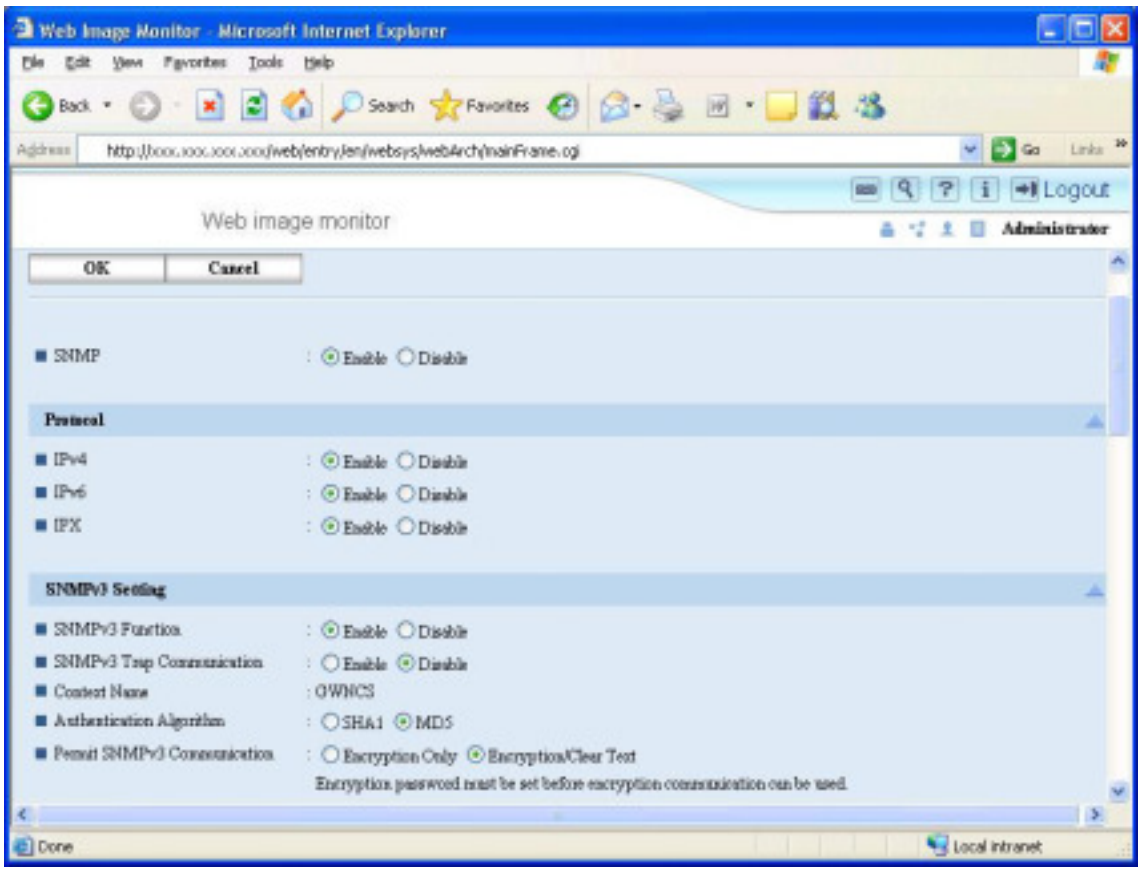
Disable: Does not allow connections using SNMP v1/v2. Because SNMP v1/v2 don’t have encryption or authorization, we recommend using ‘Disable’ for this setting unless absolutely necessary.

-Permit Settings by SNMP v1 and v2

On: This enables SNMP set. It is used to write changes to settings.

Off: This disables SNMP set. Only get will be permitted. Therefore, settings can be read but not changed.

(6) To access the SNMP v3 settings, click ‘Network’ -> ‘SNMP v3’.



-SNMP

(This setting can be configured either from here or from the SNMPv1/v2 settings.)

Enable: Opens the SNMP port

Disable: Closes the port completely. No SNMP communication of any version can be used.

-SNMP v3 Function

Enable: Allows communication using SNMP v3.

Disable: Does not allow communication via SNMP v3.

-Authentication Algorithm

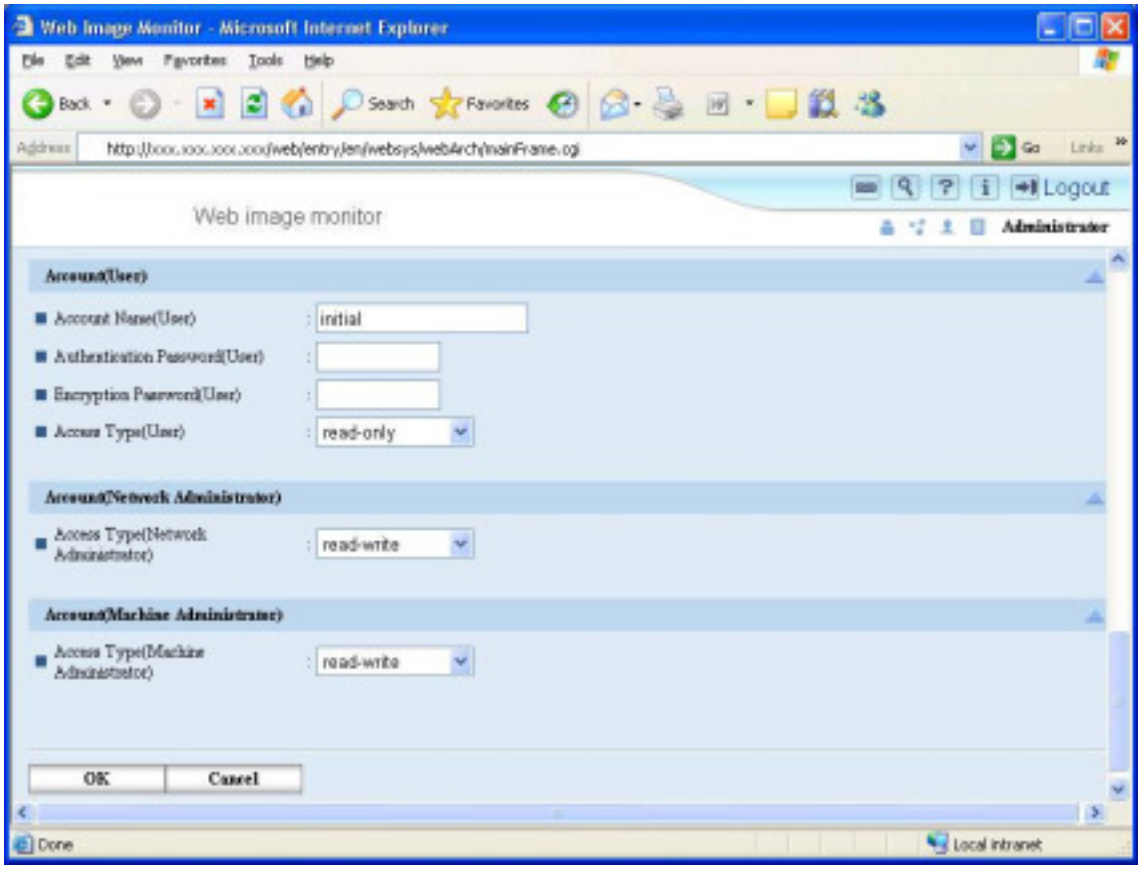
SHA1: Hashes the username and password using the SHA1 hashing algorithm.

MD5: Hashes the username and password using the MD5 hashing algorithm.

-Permit SNMPv3 communication

Encryption Only: The username and password must be encrypted using the hashing algorithm selected above.

Encryption/Clear Text: The username and password can be sent either encrypted or unencrypted.



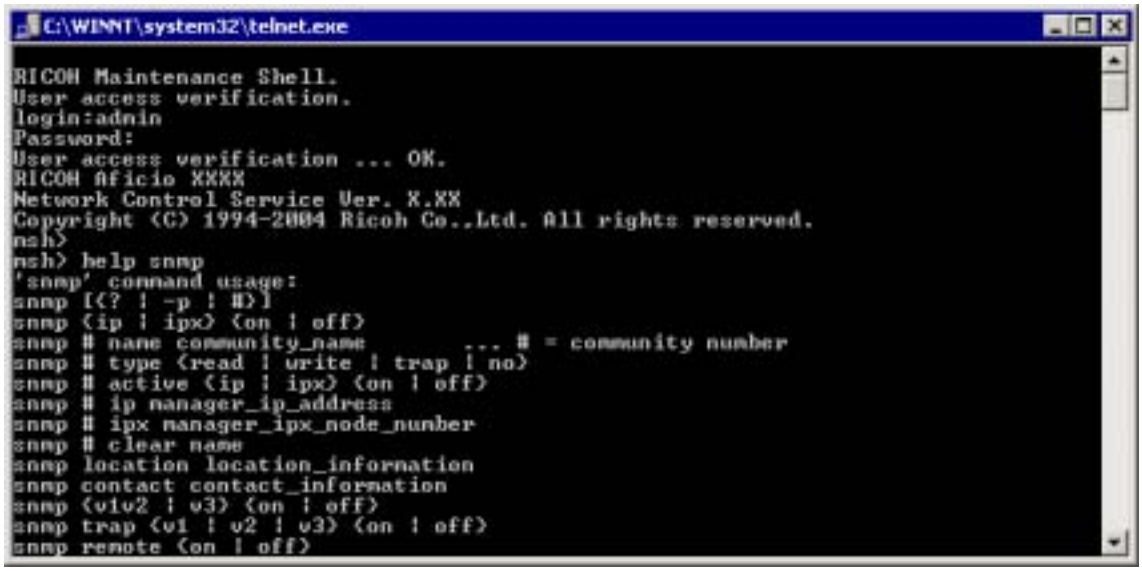
There are 3 different types of accounts that can be used for SNMPv3 connections. Only the User account can be fully configured here. For information about fully configuring the Machine and Network Administrator accounts, please refer to Appendix G.

Account Name (User): This is the username that the user will use to login to SNMPv3.
Authentication Password (User): This is the password that the user will use to login to SNMPv3.
Encryption Password (User): This is the key used for SHA1 or MD5 hashing of the username and password.

F)-2 SNMP settings – mshell

(1) The procedure for this is the same as is shown in section C)-2.

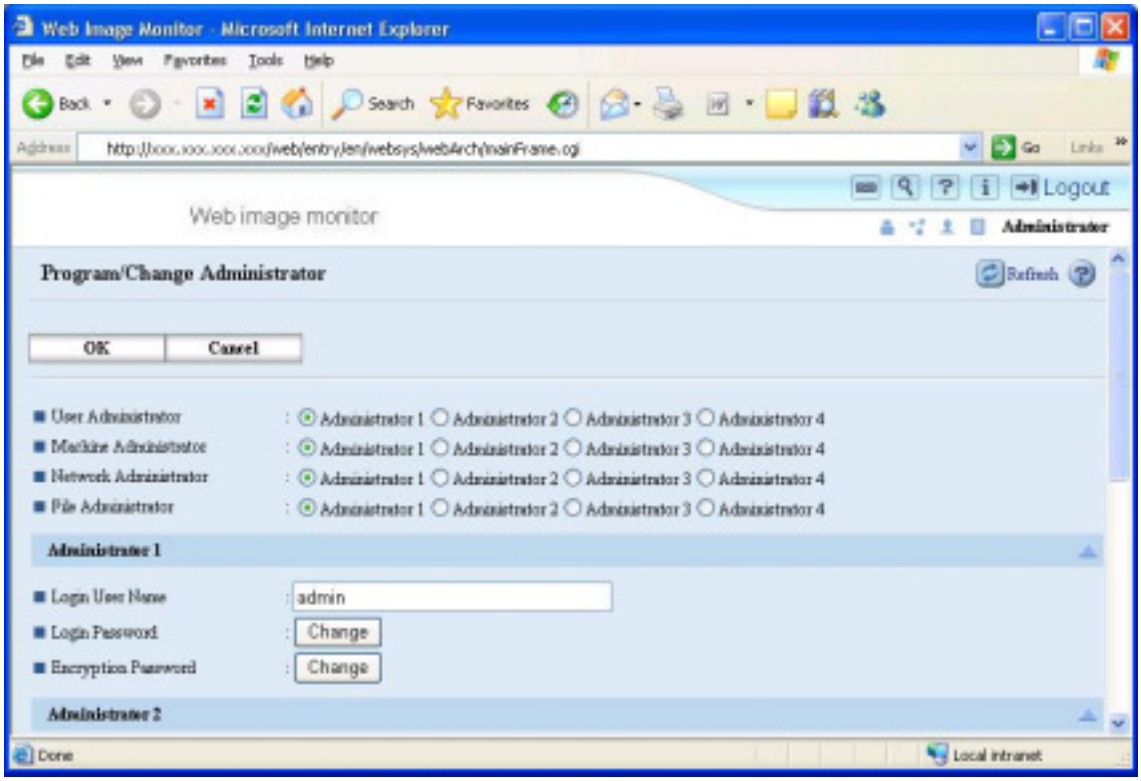
(2) You can configure SNMP settings using snmp commands from mshell. These commands can be displayed by typing ‘help snmp’ in mshell.



G) How to change administrator account settings – Web Image Monitor

Steps (1) to (4) are the same as C)-1.

(5) To access settings for the administrator accounts, click ‘Device Settings’ -> ‘Program/Change Administrator’.



You can change MFP Administrator account settings from here.

These settings affect the Administrator logins for TELNET, Web Image Monitor and SNMP v3.

H) Network Security Level settings

H)-1. How to configure

Network Security Levels are settings-profiles designed to meet different levels of security in customer environments. The advantage to the Network Security Level settings is that they make the task of configuration easier. Customers can use the Network Security levels as is, or modify them to suit their needs. There are 3 levels to choose from:

[Level 0], [Level 1], [Level 2], and [User Settings]

[Level 2] – maximum security.

[Level 1] – moderate security for use in an office LAN.

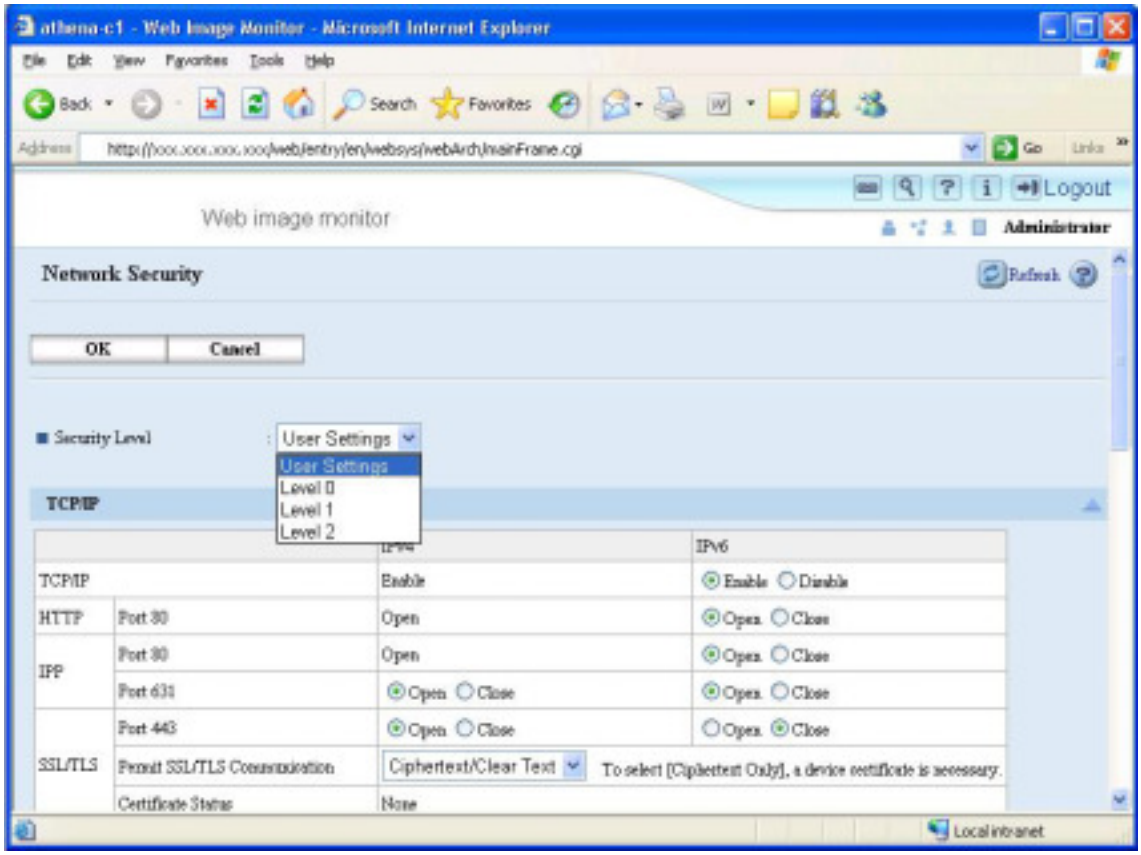
[Level 0] – basic security for closed environments.

[User Settings] – manually defined settings.

Configuration of the Network Security Level setting:

Steps (1) to (4) are the same as C)-1.

(5) To access the Network Security Level setting, click ‘Security’ -> ‘Network Security’.



H)-2. Description of levels

	Setting		Network Security Level		
			Level 0	Level 1	Level 2
Interface	IEEE 1394 SBP-2		Enabled	Enabled	Disabled
	Bluetooth		Enabled	Enabled	Disabled
	IP over 1394		Enabled	Enabled	Enabled
TCP/IP	TCP/IP		Enabled	Enabled	Enabled
	HTTP/HTTPS	Port 80	Port open	Port open	Port open*1
		Port 443	Port open	Port open	Port open
		Port 7443/7444	Port open	Port open	Port open
	IPP	Port 80	Port open	Port open	Port open *1
		Port 443	Port open	Port open	Port open
		Port 631	Port open	Port open	Port closed
	SSL	Encryption Mode	Ciphertext Priority	Ciphertext Priority	Ciphertext Only *2
	DIPRINT	Port 9100	Port open	Port open	Port closed
	LPR	Port 515	Port open	Port open	Port closed
	FTP	Port 21	Port open	Port open	Port open
	SSH/SFTP	Port 22	Port open	Port open	Port open
	RFU	Port 10021	Port open	Port open	Port open
	RSH/RCP	Port 514	Port open	Port open	Port closed
	SNMP	Port	Port open	Port open	Port open
		SNMP v1/v2 (Read)	Enabled	Enabled	Disabled
		SNMP v1/v2 (Write)	Enabled	Disable	Disabled
		SNMP v3	Enabled	Enabled	Enabled
		SNMP v3 with Encrypt	Automatic	Automatic	Ciphertext Only
	TELNET	Port 23	Port open	Port closed	Port closed
	SSDP (UPnP)	Port 1900	Port open	Port open	Port closed
	mDNS	Port 5353	Port open	Port open	Port closed
	NBT	Port 137/138	Port open	Port open	Port closed
	SMB	Port 139	Port open	Port open	Port closed
Netware	Netware		Enabled	Enabled	Disabled
AppleTalk	AppleTalk		Enabled	Enabled	Disabled

*1: The port is open but cannot be used to access the web service because the SSL setting is Ciphertext Only.

*2: If the SSL setting is Ciphertext Only, the products will still accept IPP jobs using port 80.

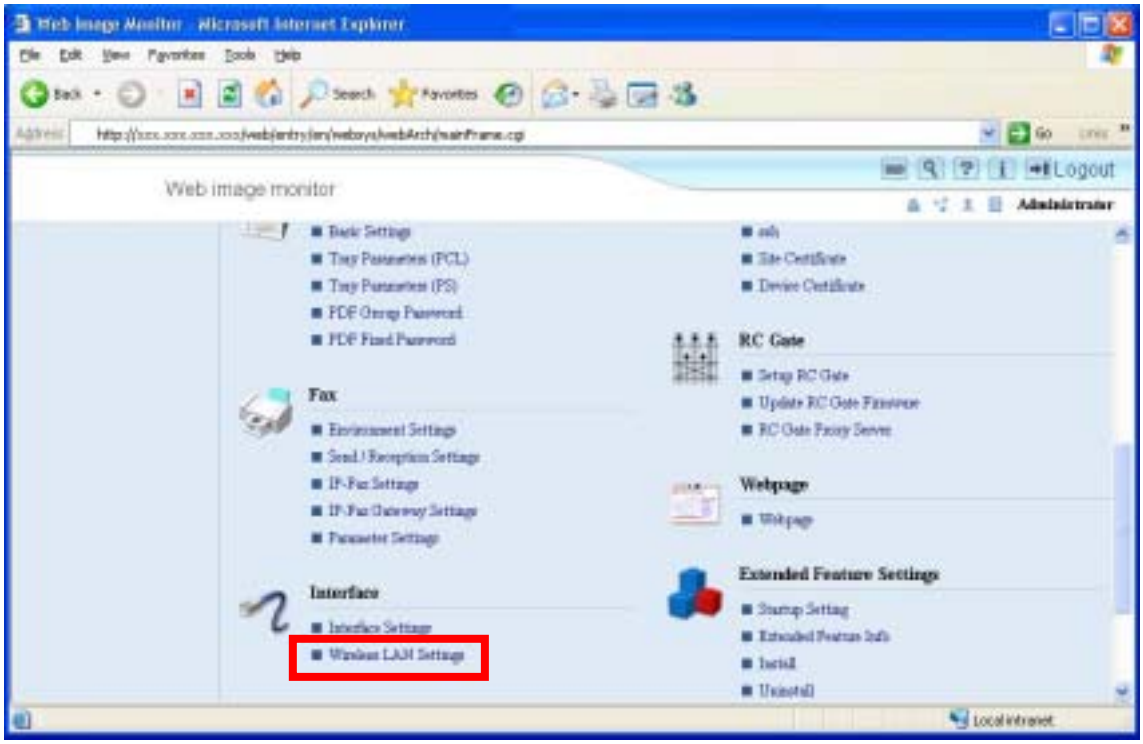
I) Wireless LAN settings

WEP, WPA-PSK/WPA2-PSK, and WPA (802.1X)/WPA2 (802.1X) can be configured via the operation panel, telnet, or Web Image Monitor. However, the WPA (802.1X)/WPA2 (802.1X) certificate settings can only be configured in Web Image Monitor.

I – 1) Wireless LAN settings – Web Image Monitor

Steps (1) to (4) are the same as C)-1.

(5) Click 'Interface' -> 'Wireless LAN Settings'.



- Change Interface

Ethernet: Enable Ethernet

IEEE802.11b: Enable IEEE802.11b

[IEEE802.11b Settings]

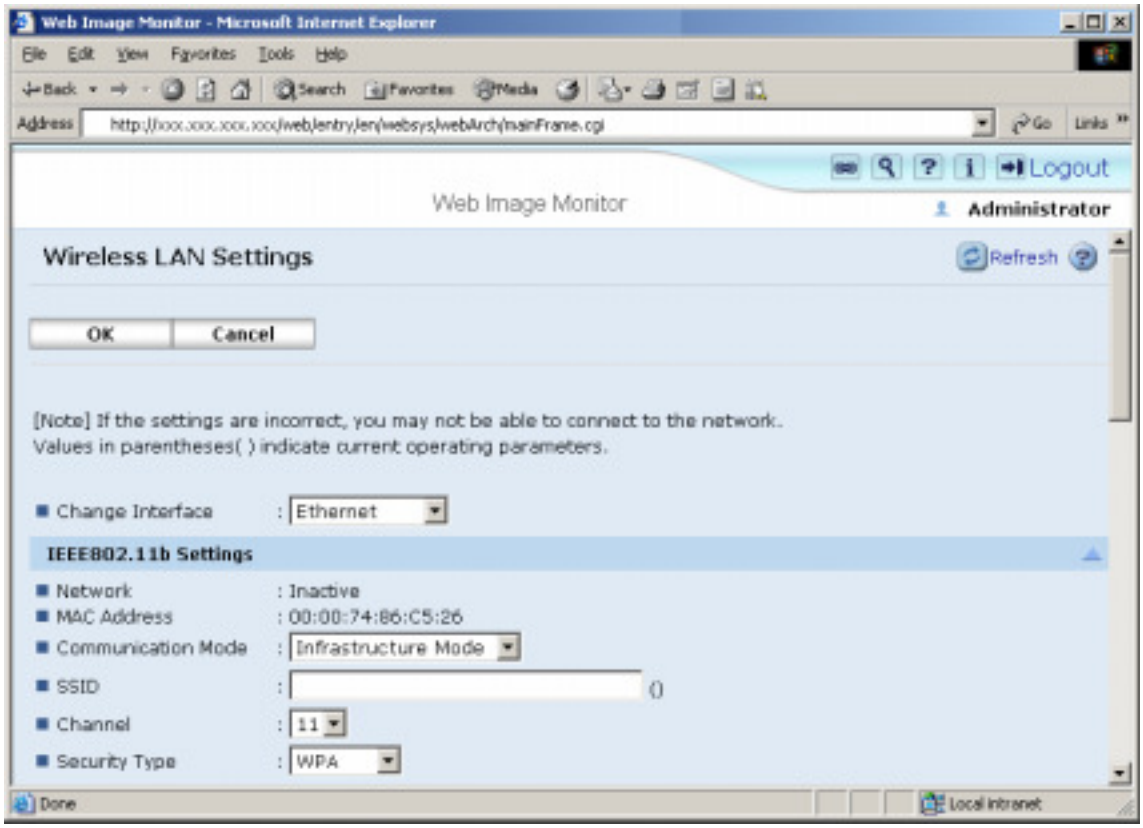
- Network

Enable: IEEE802.11b is enabled

Disable: IEEE802.11b is disabled

- MAC Address

Displays the MAC Address of the Wireless LAN board.



- Communication Mode

802.11 Ad-hoc Mode: Ad-hoc connection using SSID.

Ad-hoc Mode: Ad-hoc connection without using SSID.

Infrastructure Mode: Communicates using an access point and SSID.

- Channel

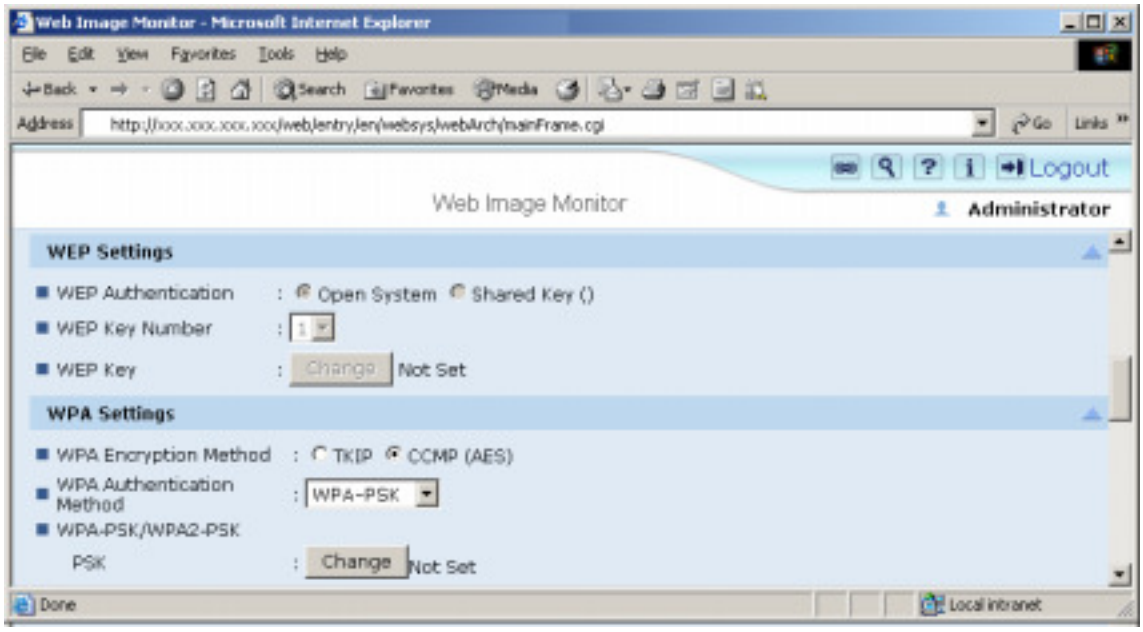
Sets the radio frequency used. If Infrastructure mode is being used, this setting is unimportant as the channel defined by the access point will be used automatically.

- Security Type

Inactive: No encryption of data.

WEP: Uses WEP security.

WPA: Uses WPA security.



[WEP]

WEP settings can only be configured if ‘WEP’ is selected in ‘IEEE802.11b Settings’ -> ‘Security Type’.

- WEP Authentication

Open System: Anyone with the correct SSID can join the network.

Note: As the system uses a WEP key, simply joining the network is not enough to be able to receive or send readable communications.

Shared Key: WEP key required to join the network.

- WEP key number

Up to 4 WEP keys can be saved in the MFP. Select one of them.

- WEP Key

Set the WEP key used for WEP encryption. If 64-bit key is used, 10 hexadecimal characters or 5 alphanumeric characters need to be entered. If a 128-bit key is used, 26 hexadecimal characters or 13 alphanumeric characters need to be entered.

[WPA]

WPA settings can only be configured if ‘WPA’ is selected in ‘IEEE802.11b Settings’ -> ‘Security Type’.

- WPA Encryption Method

TKIP: Uses TKIP.

CCMP: Uses CCMP.

- WPA Authentication Method

WPA : Uses WPA (802.1X).

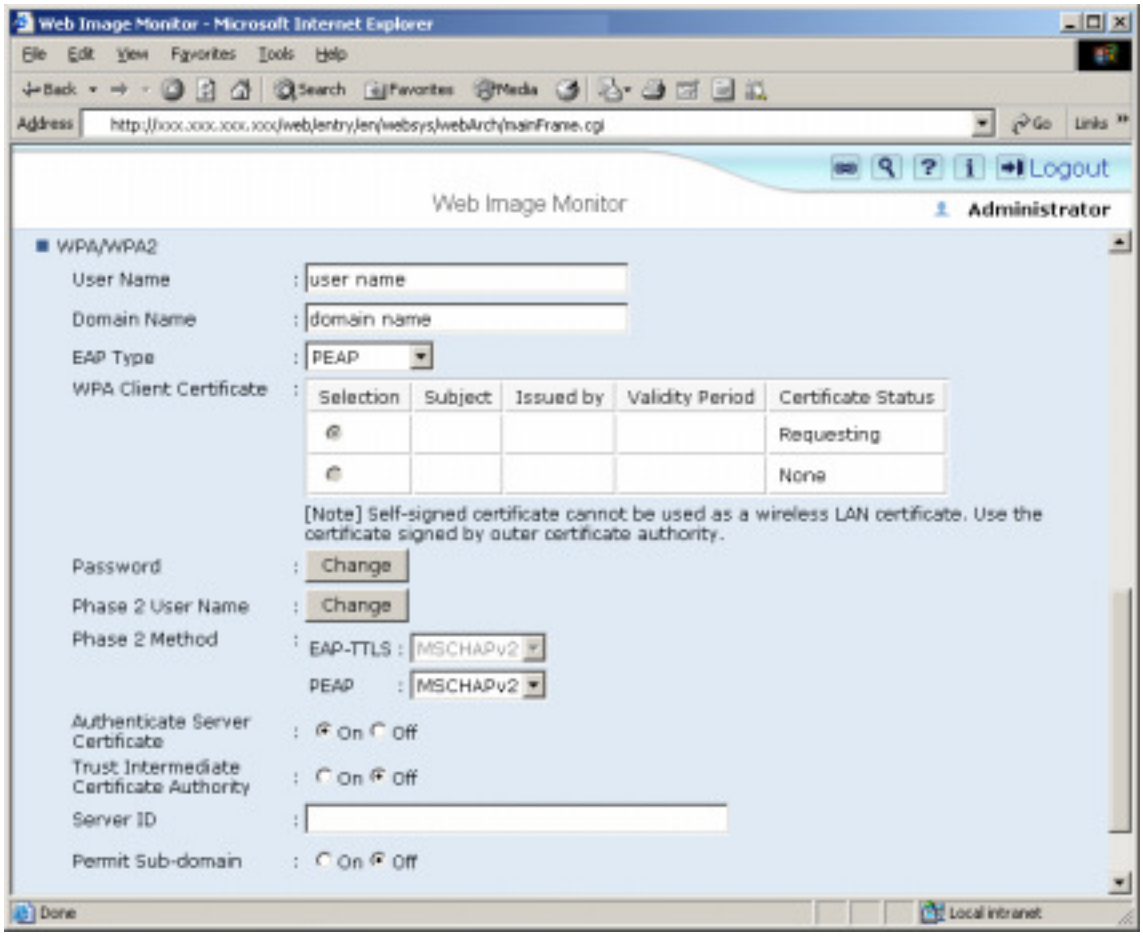
WPA2: Uses WPA2 (802.1X)

WPA-PSK: Uses WPA-PSK.

WPA2-PSK: Uses WPA2-PSK.

- WPA-PSK/WPA2-PSK

PSK: Sets the pre-shared key used.



- WPA/WPA2

User Name: This is the username used for EAP authentication on the Radius server.

Domain Name: This is the domain name used for the authentication on the Radius server.

- EAP Type: EAP-TLS, LEAP, EAP-TTLS, or PEAP

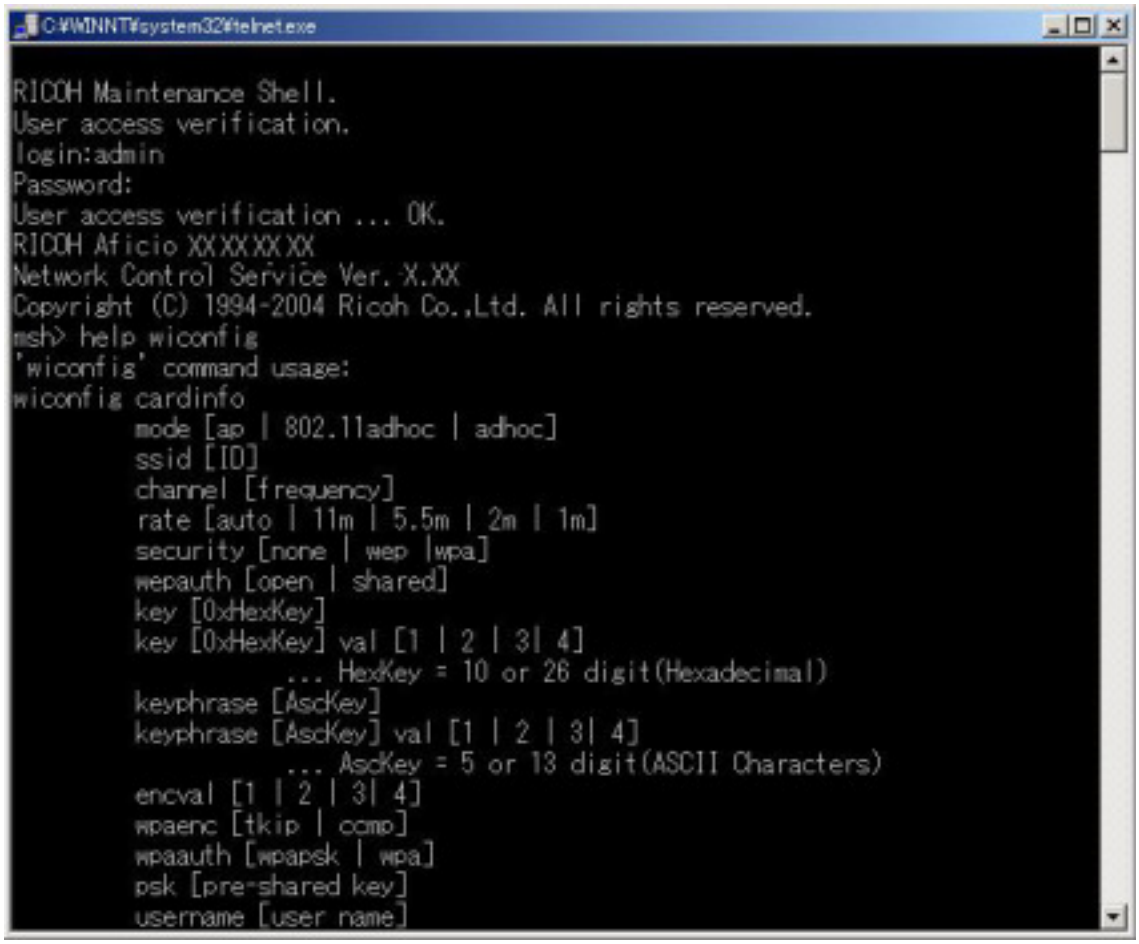
- WPA Client Certificate: WPA/WPA2 802.1X certificate.
- Password: This is the password used for EAP authentication on the Radius server.
- Phase 2 User Name: This is the user name used in phase 2 of EAP-TTLS and PEAP.
- Phase 2 Methods (EAP-TTLS): If EAP-TTLS is selected as the EAP type, a Phase2 authentication method must be selected.
Select from CHAP, MSCHAP, MSCHAPv2, PAP, or MD5
- Phase 2 Methods (PEAP): If PEAP is selected as the EAP type, a Phase2 authentication method must be selected.
Select from MSCHAPv2 or TLS.

- Authentication Server Certificate: Select whether the Radius Server is required to send a certificate to connecting WPA (802.1x) client.
- Trust Intermediate Certificate Authority: Select whether the certificate provided by the Radius Server must be signed by a trusted CA.
- Server ID: This is the CN (or the DC) of server certificate.
- Permit Sub-domain : Select whether the server certificate is permitted for the sub-domain of server ID.

I – 2) **Wireless LAN settings – mshell**

(1) The procedure for this is the same as is shown in section C)-2

(2) Configure Wireless LAN settings using ‘wiconfig’ commands from mshell. For a list of commands, type ‘help wiconfig’ in mshell.


C:¥WINNT¥system32¥telnet.exe
RICOH Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
RICOH Aficio XXXXXXXX
Network Control Service Ver.X.XX
Copyright (C) 1994-2004 Ricoh Co.,Ltd. All rights reserved.
msh> help wiconfig
'wiconfig' command usage:
wiconfig cardinfo
mode [ap | 802.11adhoc | adhoc]
ssid [ID]
channel [frequency]
rate [auto | 11m | 5.5m | 2m | 1m]
security [none | wep |wpa]
wepauth [open | shared]
key [0xHexKey]
key [0xHexKey] val [1 | 2 | 3| 4]
... HexKey = 10 or 26 digit(Hexadecimal)
keyphrase [AscKey]
keyphrase [AscKey] val [1 | 2 | 3| 4]
... AscKey = 5 or 13 digit(ASCII Characters)
encval [1 | 2 | 3| 4]
wpaenc [tkip | ccmp]
wpaauth [wpapsk | wpa]
psk [pre-shared key]
username [user name]

5. Reference list

RFC: HTTP://www.faqs.org/rfcs/

CVE: HTTP://cve.mitre.org/

CERT: HTTP://www.cert.org/

CIAC: HTTP://www.ciac.org/ciac/

SecurityFocus: HTTP://www.securityfocus.com/

NESSUS: HTTP://www.nessus.org/index2.html