

Issued: July 15, 2004



Network Security White Paper

ver.C.1.1

Covered Products:

Model C-P2c

Model G-P1

Model J-C2

Model K-P4

Model MT-C2

Model MT-P1

Model TH-C1

Model V-C1

Notice :

THIS DOCUMENT MAY NOT BE REPRODUCED OR DISTRIBUTED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH COMPANY LIMITED. RICOH COMPANY LIMITED RETAINS THE SOLE DISCRETION TO GRANT OR DENY CONSENT TO ANY PERSON OR PARTY.

Copyright © 2004 by Ricoh Company Ltd.

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Company Limited makes no representation or warranties of any kind with regards to the completeness or accuracy of the contents and accepts no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this document.

T

Version history :

Version	Issue Date	Revised item
C.1.0	Jan. 11, 2005	1 st release
C.1.1		

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:

Model Name	Product Code	Brand					
		Ricoh	Savin	Gestetner	Lanier	NRG	infotec
Model C-P2c	G113	Aficio AP410N	MLP28n	P7527n	LP128n	P7527n	-
Model G-P1	G104 G105	Aficio CL4000DN Aficio CL4000HDN	CLP26DN	C7425dn	LP125cx LP126cn	C7425dn C7425hdn	IPC 2525 IPC 2525e
Model J-C2	B202 B178 B180	Aficio 3228C Aficio 3235C Aficio 3245C	C2824 C3528 C4535	DSm428 DSm435 DSm445	LD328c LD335c LD345c	DSm428 DSm435 DSm445	ISC 2428 ISC 2835 ISC 3545
Model K-P4	G116	Aficio AP610N	MLP35	P7535n	LP135n	P7535n	-
Model MT-C2	B163 B228 B140 B142 B141 B143	Aficio 2051 Aficio 2051 SP Aficio 2060 Aficio 2060 SP Aficio 2075 Aficio 2075 SP	4051 4051 SP 4060 4060 SP 4075 4075 SP	DSm651 DSm651 SP DSm660 DSm660 SP DSm675 DSm675 SP	LD151 LD151 SP LD160 LD160 SP LD175 LD175 SP	DSm651 DSm660 DSm675	IS 2151 IS 2160 IS 2175
Model MT-P1	G126	Aficio AP900	MLP75n	P7575	LP175hdn	P7575	-

Model TH-C1	B156 B220	Aficio 3224C Aficio 3232C	C2410 C3210e	DSc424 DSc432	LD124c LD132c	DSc424 DSc432	ISC 1024c ISC 1032c
Model V-C1	B132 B181 B200	Aficio 3260C Aficio Color 5560	C6045 SDC555	DSc460 CS555	LD160c LC155	DSc460 CS555	ISC 4560 ISC 5560

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) does not apply to these models.

Table of contents

- 1 Introduction
- 2 Embedded services and potential security issues
 - 2.1 TELNET
 - 2.2 FTP
 - 2.3 HTTP
 - 2.4 SNMP v1/v2
 - 2.5 SHELL (RSH/RCP)
 - 2.6 LPD
 - 2.7 IPP
 - 2.8 DIPRINT (RAW print)
 - 2.9 SMB
 - 2.10 MDNS
 - 2.11 HTTPS
 - 2.12 SNMP v3
 - 2.13 Others
- 3 Appendix
 - A) The list of services provided with open TCP/UDP ports
 - B) Related Protocols
 - C) The purpose of Access Control
 - C)-1. Web Image Monitor
 - C)-2. mshell
 - D) How to disable services
 - D)-1. Web Image Monitor
 - D)-2. mshell
 - E) HTTP/HTTPS settings
 - F) SNMP v1/v2/v3 settings
 - G) How to change administrator account settings
- 4 Reference List

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 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/](http://www.cert.org/)). Whenever we find security vulnerabilities in the products, we provide appropriate countermeasures.

2 Embedded 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.

To avoid such inconvenience, specifying an Access Control list of “safe” client host addresses is strongly recommended. Once you set up Access Control for specific IP addresses, the products will receive print or scan requests from the specified hosts only. This 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 the mshell. When TELNET is disabled, the services provided by the mshell will no longer be available. A Memory clear by a customer engineer is required in order to start the TELNET service again.

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
Install	Install Shell script	Read-only
Stat	Printer Status	Read-only
Prnlog	Print log information	Read-only
Info	Printer Information	Read-only
Help	Help	Read-only
<i>Fax application files (hidden)</i>	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.

Note1: Only Service Technicians can add firmware to the FTP server. In addition, some of the products do not have this function.

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 product 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 prints 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: If you want to reduce the possibility of print data being intercepted, please use HTTPS 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 prints 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 it 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 it is easily read.

5) Possibility products being seen on the network by unauthorized parties via browsing (ie. 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 (ie. 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 rendezvous. If rendezvous is not being used, this port can be closed.

2.10.2. Potential threats and recommended precaution

1) Possibility of unauthorized parties intercepting information about available services and devices.

The products use MDNS to advertise services and device information.

If you do not want unauthorized parties to be aware of this information, the rendezvous 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 rendezvous 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 secs).

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. Others

TCP port 7443 and 7444 are reserved for a remote service that we will launch in the future. 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.

TCP port 10021 is reserved for communication with a new utility that we will launch in the future. This specification of this service was defined by Ricoh and it is impossible to emulate it without knowledge of the specification. In addition, we will not disclose the information about this 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, that port can be closed via TELNET. (Please refer to Appendix C.)

FTP is used for this service as an underlying layer. Please refer to “2.2 FTP” for the potential threats and recommended precautions for FTP.

TCP port 12701 is reserved for internal use by the product itself. Access from the outside will be rejected.

3. Appendix

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

Protocol	Port Num.	Login	Default Username	Username Changeable	Password	Password Changeable	Note
TELNET	23/TCP	N/A	N/A	N/A	Y	Y	This is the same username and password as are used for Web Image Monitor.
FTP-control	21/TCP	Y	ANONYMOUS	N/A	N/A	N/A	
HTTP	80/TCP	N/A	N/A	N/A	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.
netbios-ns	137/UDP	N/A	N/A	N/A	N/A	N/A	
netbios-dgm	138/UDP						
netbios-ssn	139/TCP						
SNMP	161/UDP	Y	RO: public RW: admin	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.
HTTPS	443/TCP	N/A	N/A	N/A	Y	Y	This is the same username and password as are used for TELNET and HTTP. If no password is input, then only read access is available.
RSH/RCP (shell)	514/TCP	N/A	N/A	N/A	N/A	N/A	
LPD	515/TCP	N/A	N/A	N/A	N/A	N/A	
IPP	631/TCP	Y	ANONYMOUS	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

Protocol	Port Num.	Login	Default Username	Username Changeable	Password	Password Changeable	Note
							password will be required.
MDNS	5353/UDP	N/A	N/A	N/A	N/A	N/A	
future remote service	7443/TCP 7444/TCP	-	-	-	-	-	
DIPRINT	9100/TCP	N/A	N/A	N/A	N/A	N/A	
To be used in the future by a new Ricoh utility	10021/TCP	Y	-	-	-	-	This port is based on FTP and will be used for a utility that will be released in the future.
For machine internal use	12701/TCP	N/A	N/A	N/A	N/A	N/A	Access from the outside will be rejected.

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)
FTP-control	TCP/IP	21/tcp, udp	2) Sending scan data to ScanRouter
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.
NCP	TCP/IP, IPX/SPX	524/tcp, udp	1) Logging in to a Netware server.

Protocol	Protocol Suite	Commonly Used Port Num.	Description of the protocol's function in the Products.
			2) Printing from the Netware environment.
SLP	TCP/IP	427/tcp, udp	1) Serching 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.

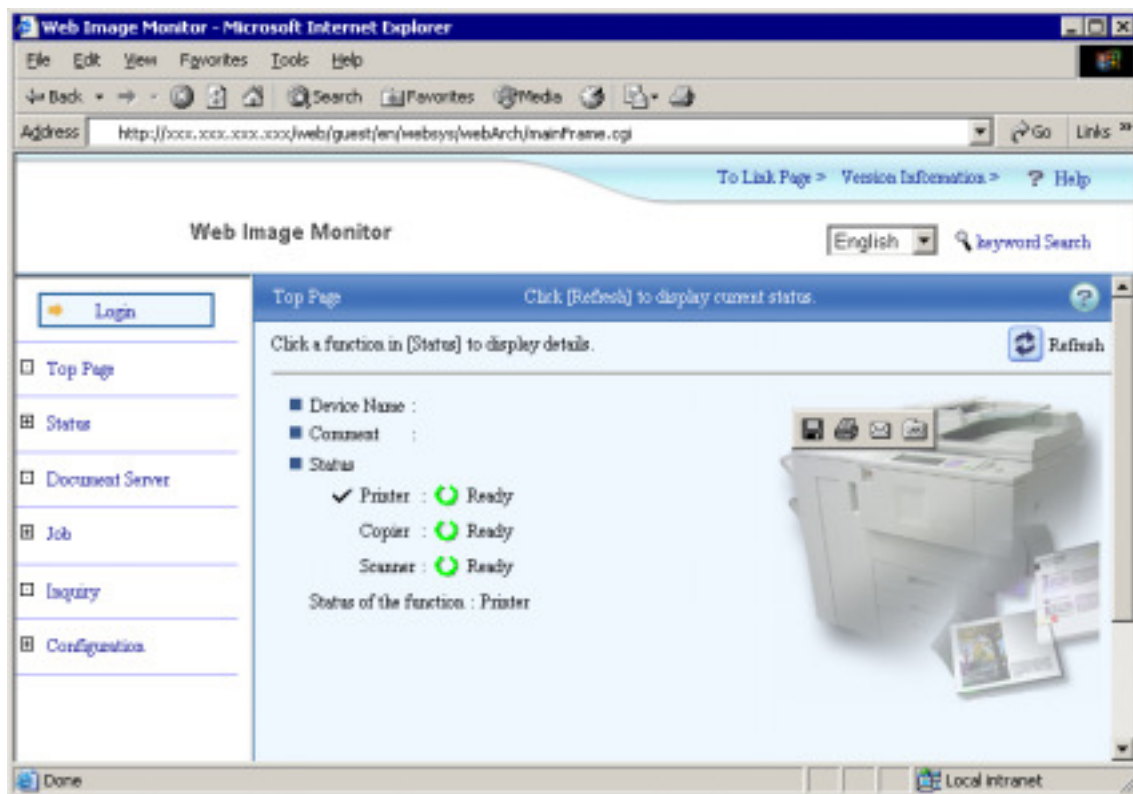
The cannot be applied to TELNET and SmartDeviceMonitor.

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

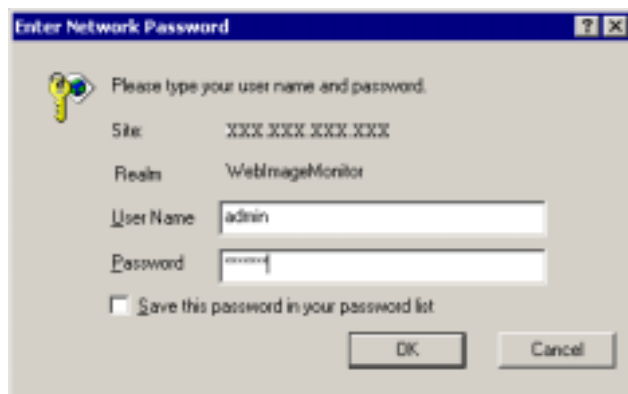
(1) Web Image Monitor can be used for accessing the products. A supported Browser such as Microsoft Internet Explorer and the product's IP address is required. Enter the IP address as shown below.

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

And then click "Login"

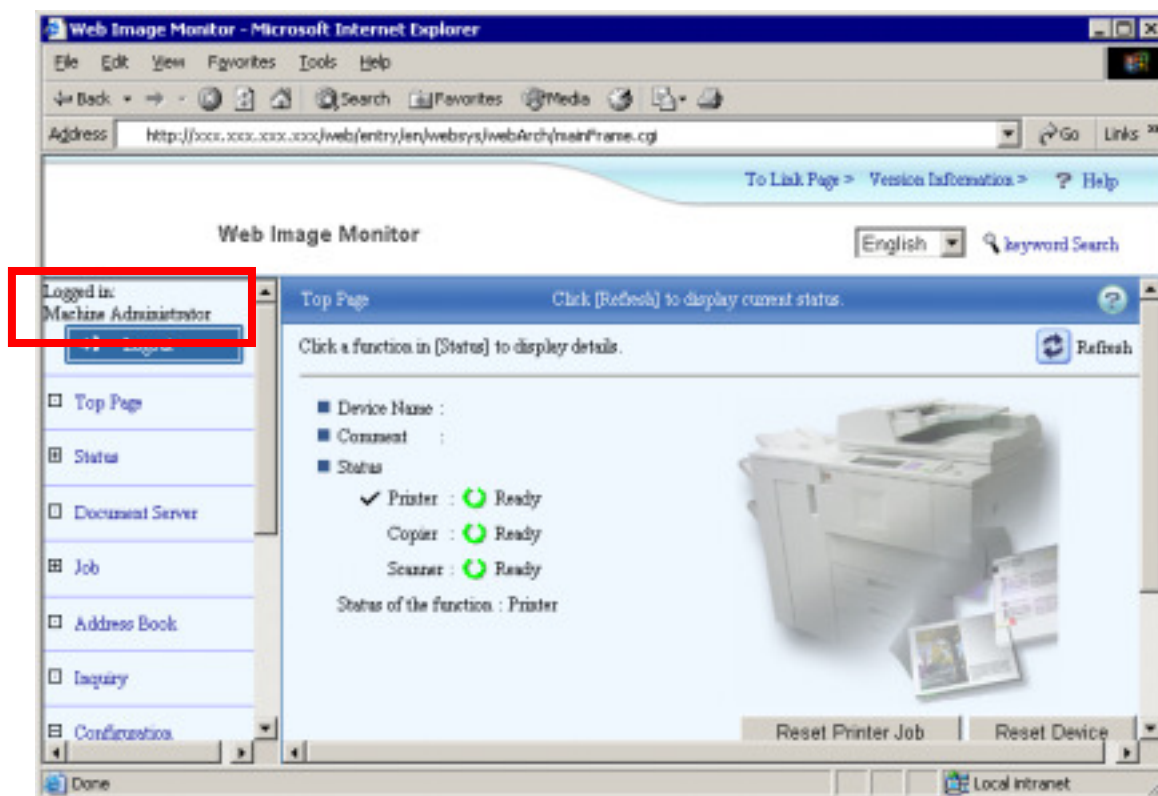


(2) In order to access Administrator mode, a username and password are required.

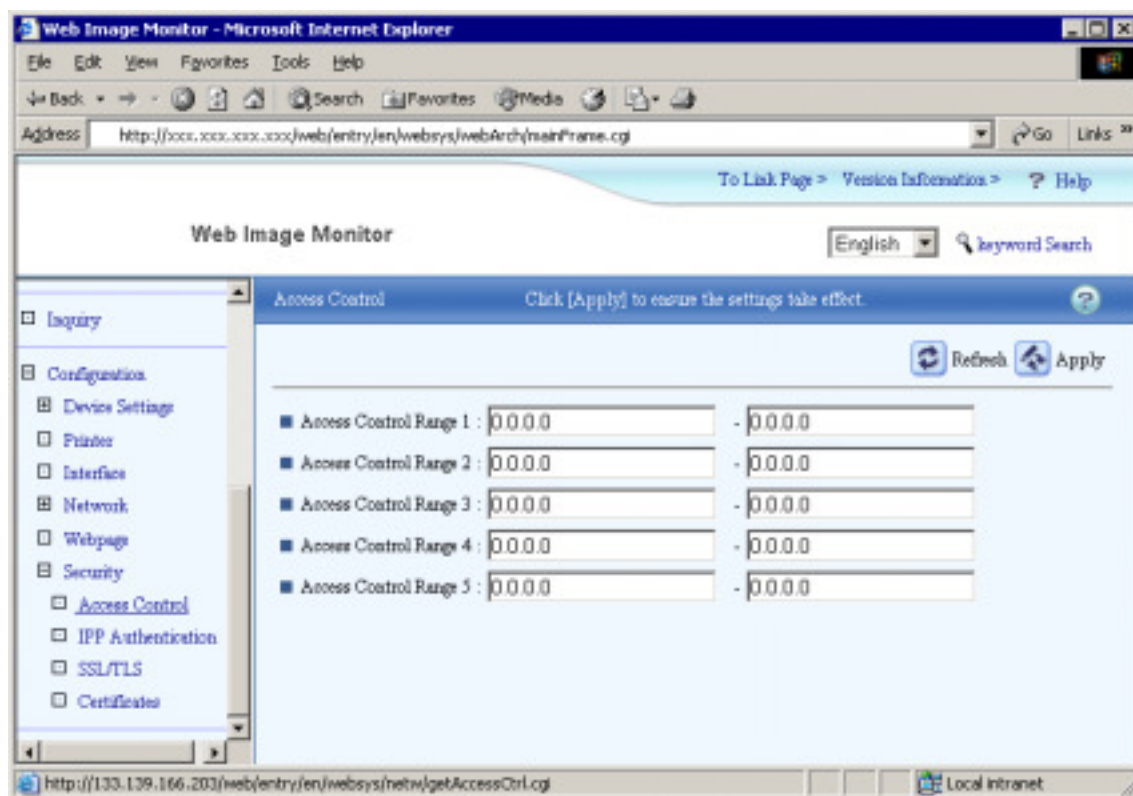


(3) Login to enter Administrator mode.

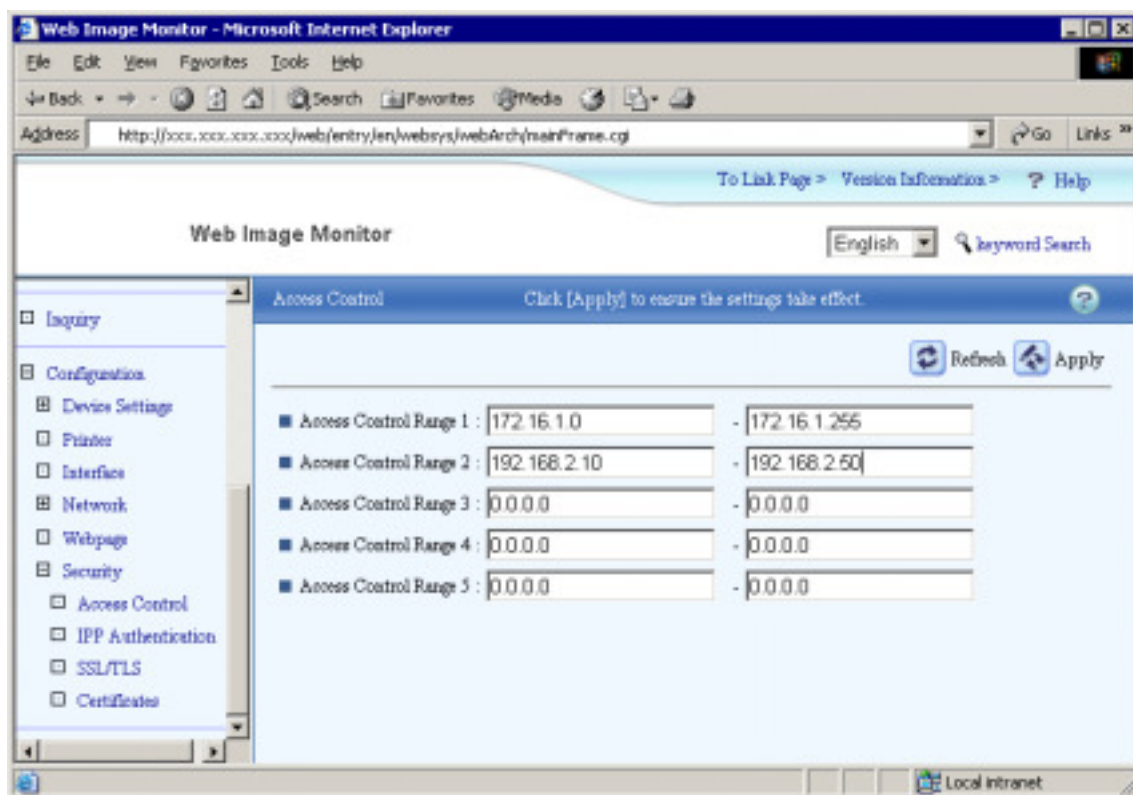
You will know that you are in administrator mode if you can see 'Logged in: Machine Administrator' as shown below.



(4) To open the access control settings, click 'Configuration' -> 'Security' -> 'Access Control'.



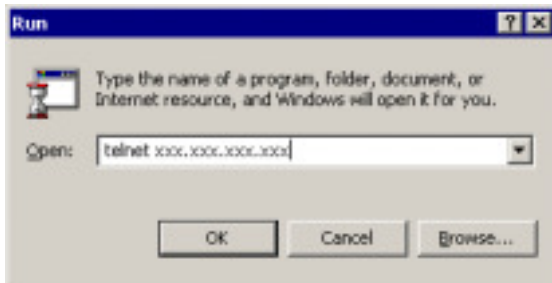
- (5) Input the range of IP addresses that you wish to permit communication with.
Click the 'Apply' button to commit the changes.



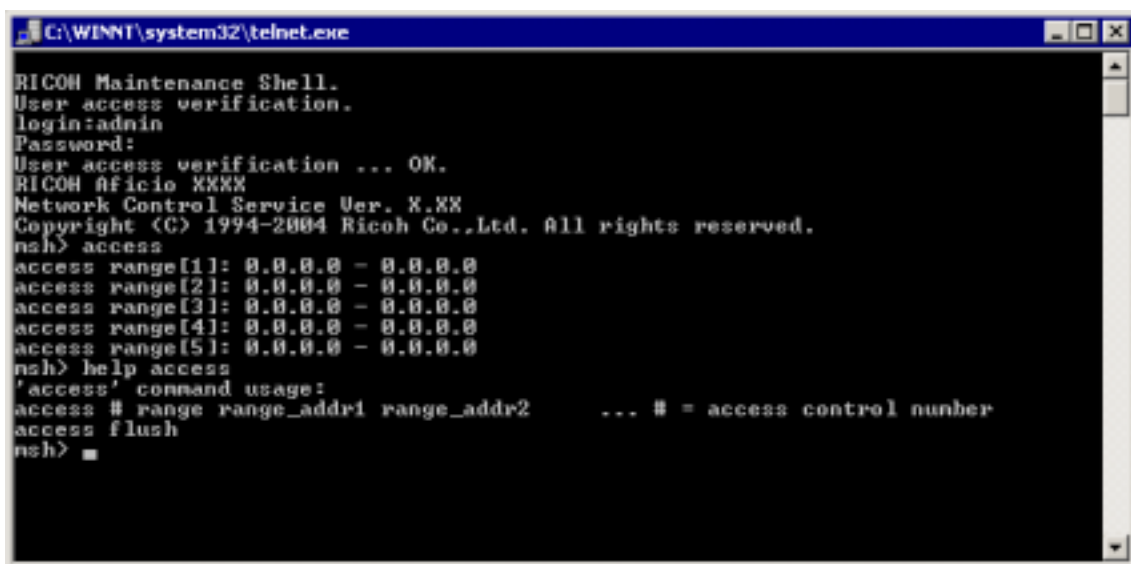
C)-2 The Purpose of Access Control – mshell

The following example is shown using the Windows 2000 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.



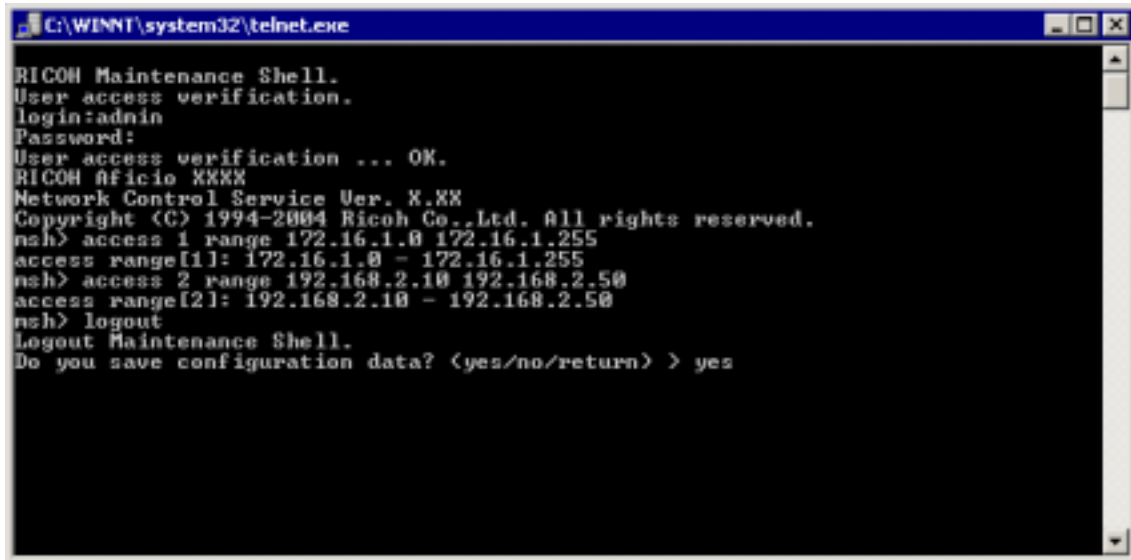
E.g.1 Input the following command to permit only access from 172.16.1.0 to 172.16.2.0

nsh> access 1 range 172.16.1.0 172.16.2.0

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

nsh> 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.



```
C:\WINNT\system32\telnet.exe

RICOH Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
RICOH Aficio XXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2004 Ricoh Co., Ltd. All rights reserved.
nsh> access 1 range 172.16.1.0 172.16.1.255
access range[1]: 172.16.1.0 - 172.16.1.255
nsh> access 2 range 192.168.2.10 192.168.2.50
access range[2]: 192.168.2.10 - 192.168.2.50
nsh> logout
Logout Maintenance Shell.
Do you save configuration data? (yes/no/return) > yes
```

D) How to disable services

The following services can be enabled or disabled by selecting up or down.

TCP/IP, Netware(*1), SMB(*2), Appletalk, LPR, FTP(*3), RSH/RCP, DIPRINT, WEB(Only mshell)(*4), SNMP(*5), IPP(*6), HTTP(Only mshell)(*7), ip1394, scsiprint, TELNET(Only mshell), rendezvous(*8), SSL(*9), NRS(Only mshell)(*10), RFU(Only mshell)(*11), NBT(Only mshell)(*12)

*1; Netware; 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.

*2; SMB; 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.

*3; FTP; 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.

*4; web; Setting web to down, disables the Web Image Monitor. However even if this function is disabled, HTTP Port (80/tcp) will still be open. Therefore if this function is disabled, IPP printing using HTTP Port (80/tcp) is still available.

*5; SNMP; 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.

*6; IPP; Setting IPP to down, disables the IPP printing function but doesn't close IPP Port (631/tcp). Therefore if IPP is down, IPP printing using HTTP (80/tcp) is still available.

*7; HTTP; Setting HTTP to down, closes HTTP Port (80/tcp). Therefore, not only Web Image Monitor but also IPP printing using HTTP port (80/tcp) is disabled.

*8; rendezvous; Setting rendezvous to down makes rendezvous is unavailable and closes the MDNS port (5353/udp).

*9; SSL; Setting SSL to down, closes the HTTPS port. Therefore, Web Image Monitor and IPP printing using HTTPS port (443/tcp) are disabled.

*10; NRS; This was mentioned in section "2.13. Others" as "a remote service that we will launch in the future". To disable NRS, please close ports 7443 and 7444.

*11; RFU; This was mentioned in section "2.13. Others" as "a new utility that we will launch in the future". To disable RFU, please close port 10021.

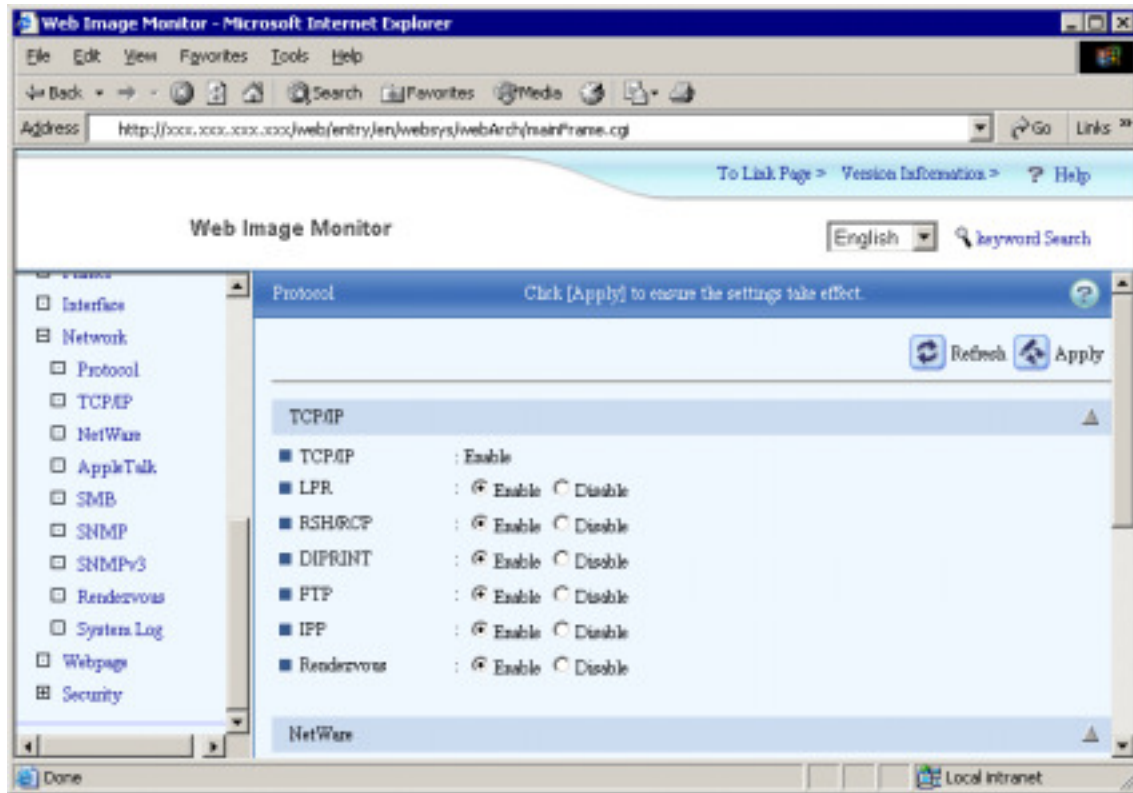
*12; NBT; Setting NBT to down, closes NetBIOS-NS (137/UDP) and NetBIOS-DGM (138/UDP).

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

Steps (1) to (3) are the same as C)-1 (previous section)

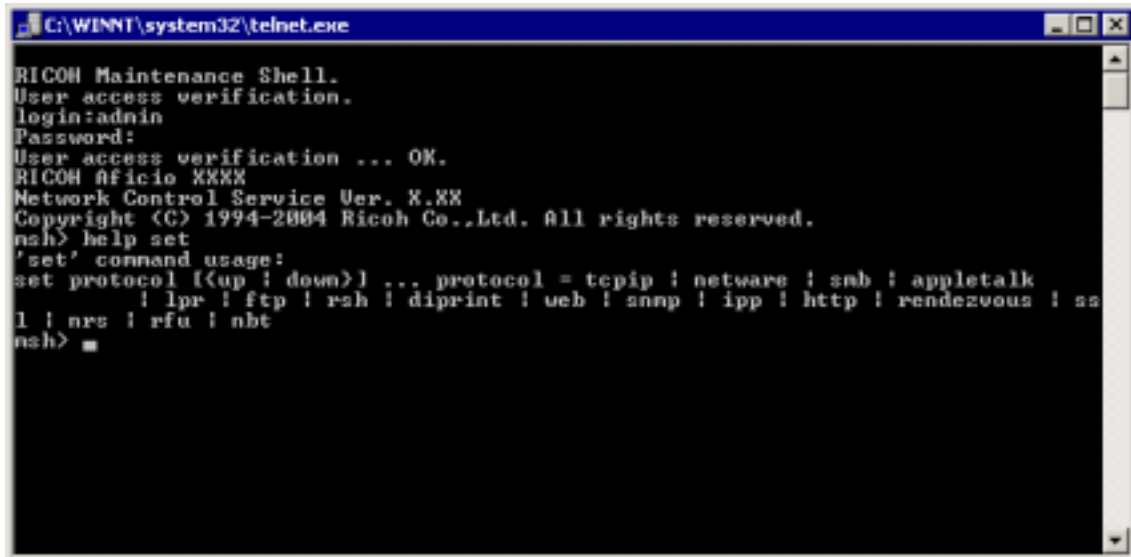
(4) Click 'Configuration' -> 'Network' -> 'Protocol' -> 'Protocol' to access the protocol settings.

By default all protocols are enabled.



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.



```

C:\WINNT\system32\telnet.exe
RICOH Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
RICOH Aficio XXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2004 Ricoh Co.,Ltd. All rights reserved.
nsh> help set
'set' command usage:
set protocol {(up | down)} ... protocol = tcpip | netware | snb | appletalk
        | lpr | ftp | rsh | diprint | ueb | snmp | ipp | http | rendezvous | ss
        | l | ars | rfu | nbt
nsh>

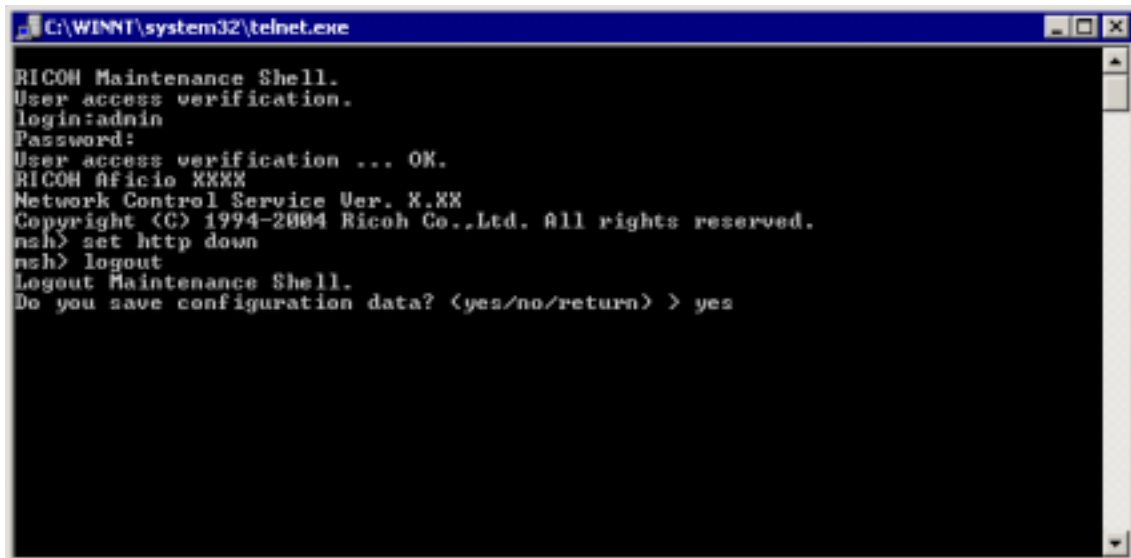
```

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

nsh> 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



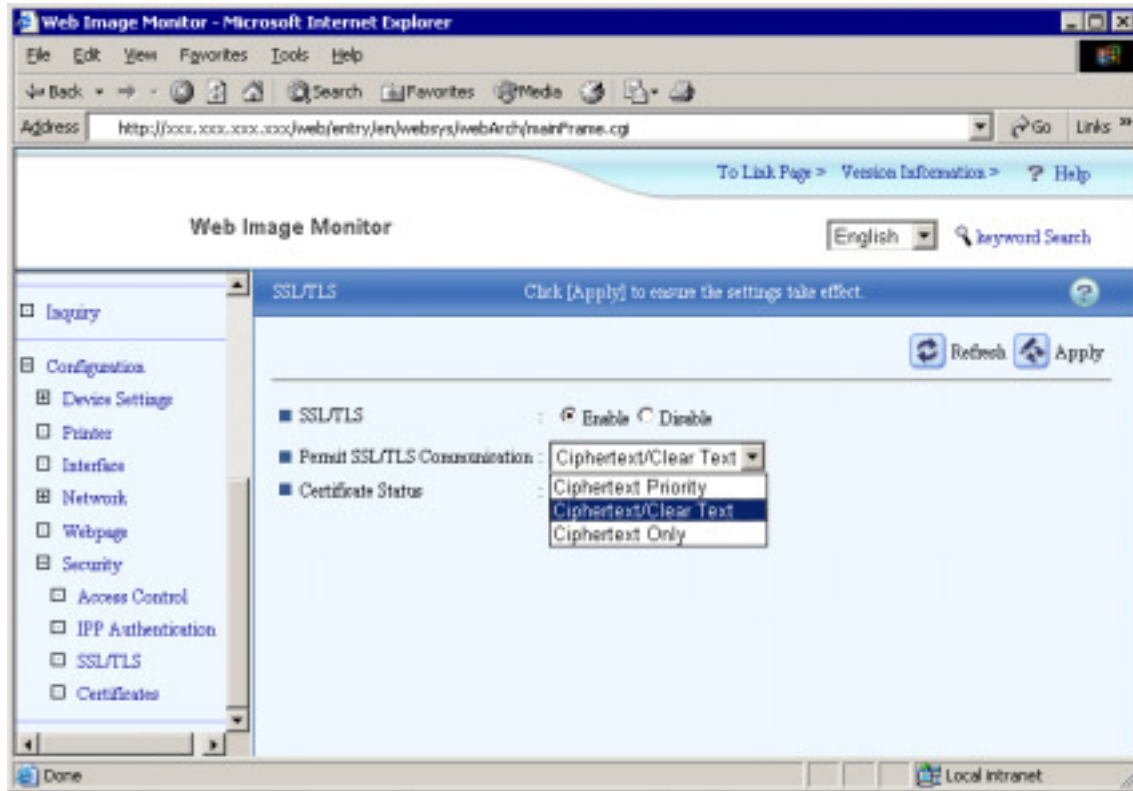
```

C:\WINNT\system32\telnet.exe
RICOH Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
RICOH Aficio XXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2004 Ricoh Co.,Ltd. All rights reserved.
nsh> set http down
nsh> logout
Logout Maintenance Shell.
Do you save configuration data? (yes/no/return) > yes

```

E) SSL settings

To access the SSL/TLS settings, click 'Configuration' -> 'Security' -> 'SSL/TLS'.



- Permit SSL/TLS Communication

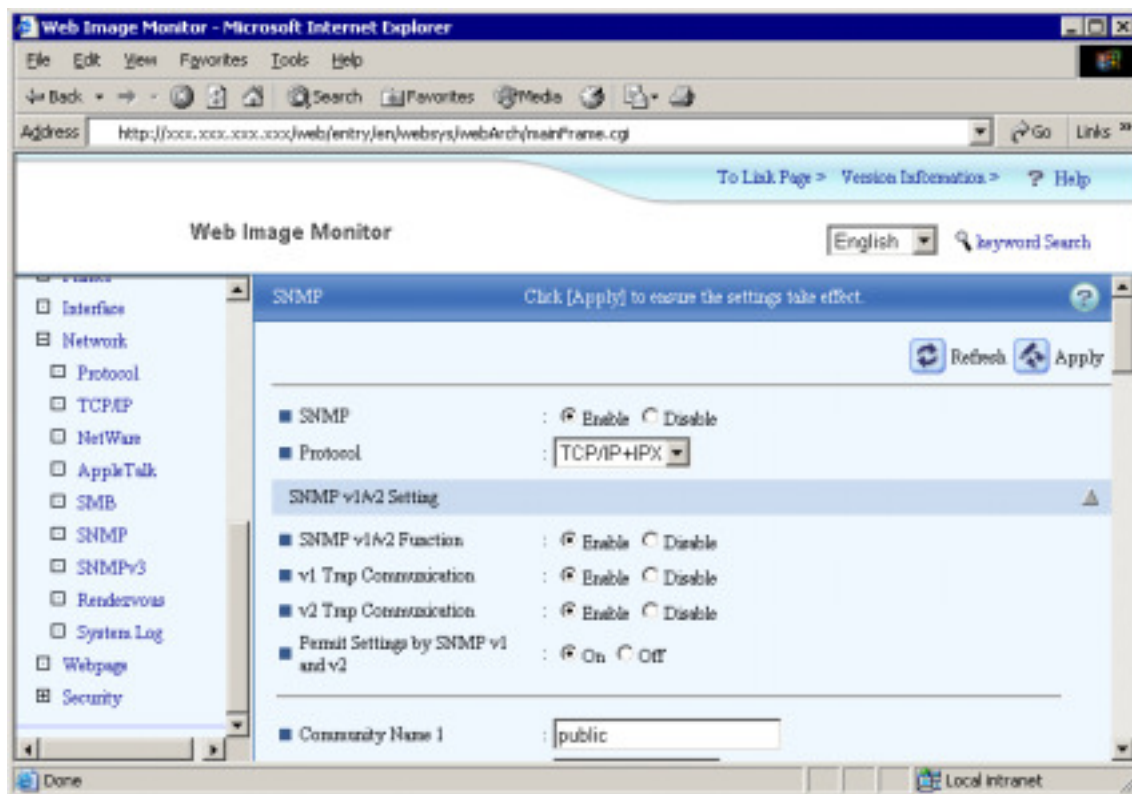
Ciphertext/Clear Text: Permit both HTTPS and HTTP connections. No forwarding of HTTP to HTTPS.

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

1. To access the SNMP (v1/v2) settings, click 'Configuration' -> '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.

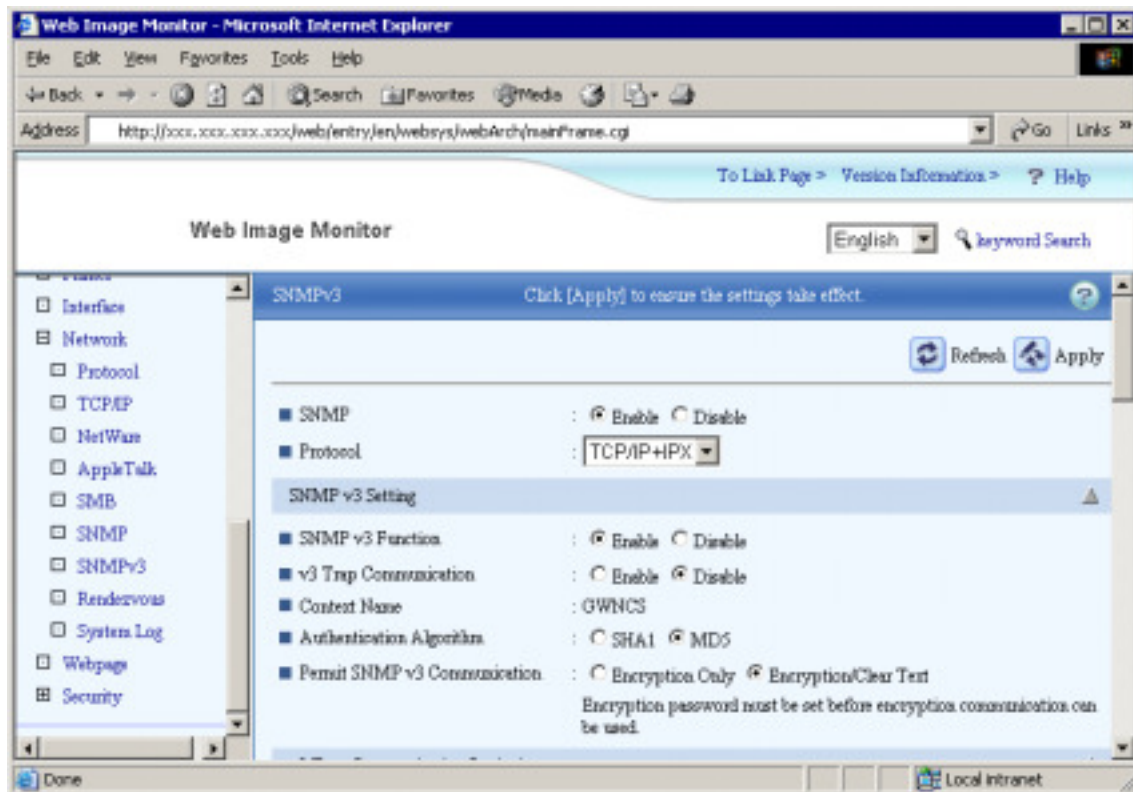
Disable: Does not allow connections using SNMP v1/v2. Because SNMP v1/v2 don't have encryption or authorization, we recommend using 'Disable' for this setting unless absolutely necessary.

-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.

2. To access the SNMP v3 settings, click 'Configuration' -> '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

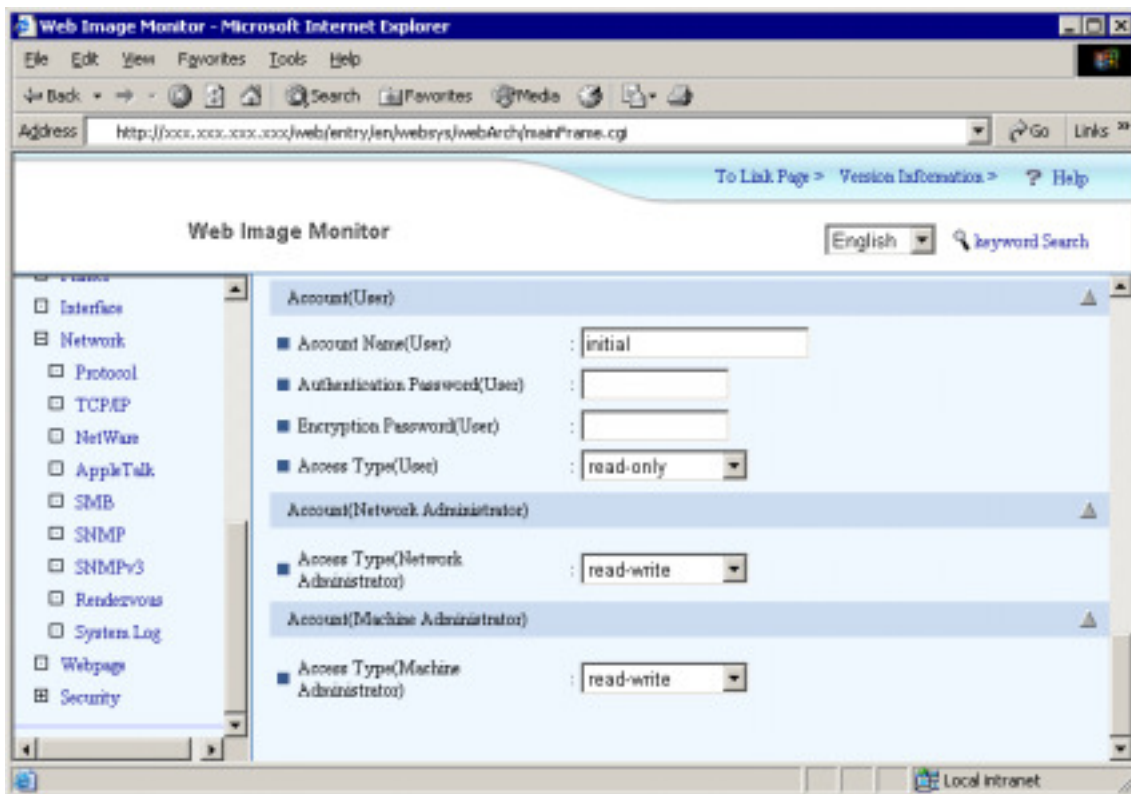
SHA1: Hashes the username and password using the SHA1 hashing algorithm.

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.

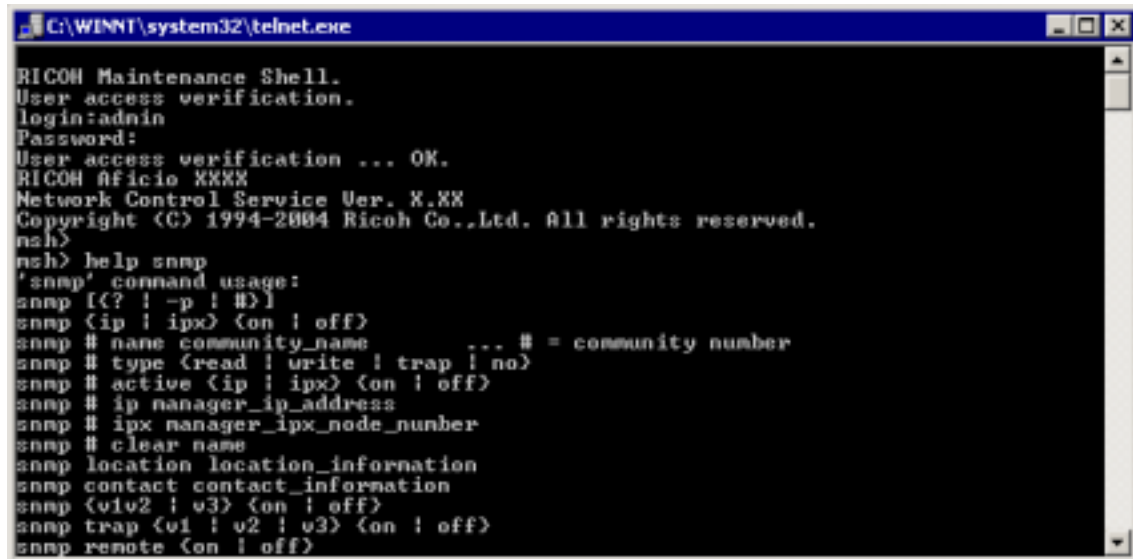
Account Name(User): This is the username that the user will use to login to SNMPv3.

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

You can configure SNMP settings using snmp commands from mshell. These commands can be displayed by typing 'help snmp' in mshell.

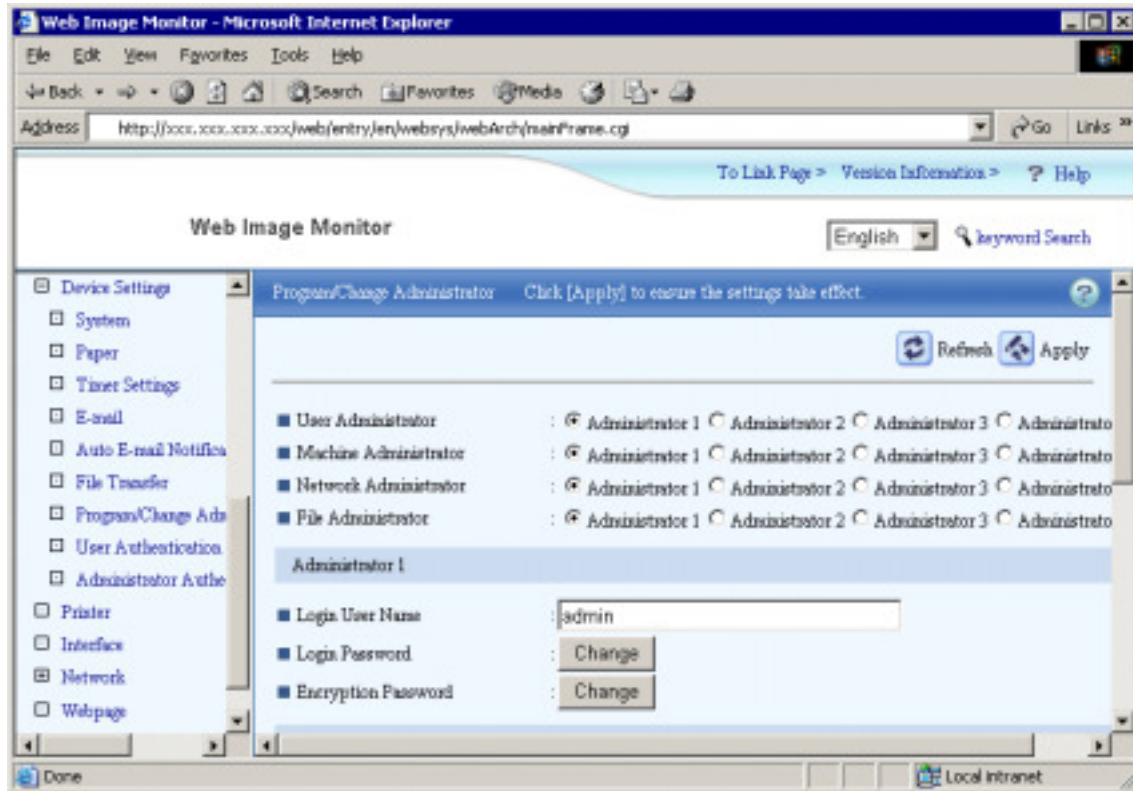


```
C:\WINNT\system32\telnet.exe

RICOH Maintenance Shell.
User access verification.
login:admin
Password:
User access verification ... OK.
RICOH Aficio XXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2004 Ricoh Co.,Ltd. All rights reserved.
msh>
msh> help snmp
'snmp' command usage:
snmp [(? | -p | #)]
snmp (ip | ipx) (on | off)
snmp # name community_name ... # = community number
snmp # type (read | write | trap | no)
snmp # active (ip | ipx) (on | off)
snmp # ip manager_ip_address
snmp # ipx manager_ipx_node_number
snmp # clear name
snmp location location_information
snmp contact contact_information
snmp (v1v2 | v3) (on | off)
snmp trap (v1 | v2 | v3) (on | off)
snmp remote (on | off)
```

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

1. To access settings for the administrator accounts, click 'Configuration' -> '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.

4. Reference list

RFC: [HTTP://www.fags.org/rfcs/](http://www.fags.org/rfcs/)

CVE: [HTTP://cve.mitre.org/](http://cve.mitre.org/)

CERT: [HTTP://www.cert.org/](http://www.cert.org/)

CIAC: [HTTP://www.ciac.org/ciac/](http://www.ciac.org/ciac/)

SecurityFocus: [HTTP://www.securityfocus.com/](http://www.securityfocus.com/)

NESSUS: [HTTP://www.nessus.org/index2.html](http://www.nessus.org/index2.html)