Network Security White Paper
for
Digital Multifunction and Printing Devices

NOTICE

THIS DOCUMENT SHALL NOT BE REPRODUCED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION AND DISTRIBUTED WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH CORPORATION. WHICH CONSENT RICOH CORPORATION MAY GRANT OR DENY IN ITS SOLE DISCRETION.

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 and for the benefit of such companies. Ricoh does not grant or intend to grant hereby any right to such trademarks or property to any third parties. No such use, or the use of any trade name, or web site is intended to convey endorsement or other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Corporation 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 performances, 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.

Technology Solutions Center
Ricoh Corporation
Version: 1.7
June 2007

Version History
1.1 – January 2004
1.2 – July 2004
1.3 – June 2005
1.4 – November 2005
1.5 – December 2005
1.6 – August 2006
1.6.1 – January 2007
1.6.2 – March 2007

Table of Contents

1 Introduction

This document describes potential internal and external network threats and the recommended precautions for preventing them.

The products have built-in network services that provide a variety of features for network clients (e.g. network scanning, printing or faxing), and client services for accessing network servers running outside the products (e.g. LDAP server, NetWare servers, or Mail servers).

The products are designed for use inside an Intranet where network clients and servers are protected by firewalls, and they rely on the Intranet's security policy. However, some customers require stricter security for network devices, due to increasing threats from inside the firewalls. 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.

For more information, see the information posted in our online Knowledge Base at: http://www.ricoh-usa.com/support/knowledgebase.asp.

> **NOTE**
> This document generally assumes a secure network environment, which is sufficiently protected from unwanted outside intrusion. If the network environment is not secure, it may be possible for intruders to perform malicious acts, such as transmitting viruses and the unauthorized launching of applications. These and other acts may cause serious network damage.

1.1 Terms

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

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

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

1.2 Target Audience

1. All end-users - The information contained in the document can be distributed to end-users as long as the restrictions outlined on the cover page are followed.
   - The main target readers are IT Administrators.
2. The support and marketing staff of Ricoh Sales companies including Ricoh family group companies and their subsidiaries.
3. Technical support personnel (CEs) of dealers.

1.3 Model Cross Reference

Network Security WP Version(s)	Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
1.1	B070	Aficio 2090	4090	9002	LD090
1.1	B071	Aficio 2105	4105	10512	LD0105
1.1	B079	Aficio 2035	4035	3532	LD035
1.1	B082	Aficio 2045	4045	4532	LD045
1.1	B089	Aficio 2022	4022	DSm622	LD122
1.1	B093	Aficio 2027	4027	DSm627	LD127
1.1	B121	Aficio 2015	4015	DSM615	LD115
1.1	B122	Aficio 2018	4018	DSM618	LD118
1.1	B123	Aficio 2018D	4018D	DSM618d	LD118D
1.1	B129	Aficio 1515	3515	DSm415	LD015
1.1	B130	Aficio 1515MF	3515MF	DSm415pf	LD015spf
1.1	B135	Aficio 2035e	4035e	DSm635	LD135
1.1	B138	Aficio 2045e	4045E	DSm645	LD145
1.1	B147	Aficio 2232c	C3224	DSc332	LD232c
1.1	B149	Aficio 2238c	C3828	DSc338	LD238c
1.1	B168	Aficio 1515F	3515F	DSm415f	LD015f
1.1	B169	Aficio 2013PS		DSm415p	LD015sp
1.1	B182	Aficio 2035eSP	4035Esp	DSm635sp	LD135
1.1	B183	Aficio 2045eSP	4045Esp	DSm645sp	LD145
1.1	B190	Aficio 2228c	C2820	DSc328	LD228c
1.1	G091	AP600N	MLP32	P7132N	LP032
1.4	B205	Aficio 3025/SP/SPF/SPi/P	8025/sp/ spf/spi/P	DSm725/sp/ spf/spi/p	LD225/SP
1.4	B209	Aficio 3030/SP/SPF/SPi/P	8030/sp/ spf/spi/P	DSm730/sp/ spf/spi/p	LD230
1.4	B264	Aficio 3035/SP/SPF/Spi/G	8035/sp/ spf/spi/34g	DSm735/sp/ spf/spi/G	LD235
1.4	B265	Aficio 3045/SP/SPF/Spi/G	8045/sp/ spf/spi/g	DSm745/sp/ spf/spi/G	LD245
1.4	G130	Aficio CL7200	CLP128	C7528n	LP332c
1.4	G131	Aficio CL7300	CLP135	C7535ND	LP335c
1.5	B132	Aficio 3260c	C6045	DSc460	LD160c
1.5	B140	Aficio 2060	4060	DSm660	LD160
1.5	B141	Aficio 2075	4075	DSm675	LD175
1.5	B142	Aficio 2060SP	4060sp	DSm660sp	LD160 SP
1.5	B143	Aficio 2075SP	4075sp	DSm675sp	LD175 SP
1.5	B156	Aficio 3224c	C2410	DSC424	LD124C
1.5	B163	Aficio 2051	4051	DSm651	LD151
1.5	B178	Aficio 3235C	C3528	DSc435	LD335c
1.5	B180	Aficio 3245C	C4535	DSc445	LD345c
1.5	B200	Aficio 5560	SDC555	CS555	LC155
1.5	B202	Aficio 3228C	C2824	DSC428	LD328c
1.5	B228	Aficio 2051SP	4051sp	DSm651sp	LD151 SP
1.5	G094	AP400	MLP25	P7325	LP025 / LP026

Network Security WP Version	Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
1.5	G095	AP400N	MLP25N	P7325N	LP025N/LP026N
1.5	G104	Aficio CL4000DN	CLP26DN	C7425dn	LP126cn
1.5	G106	CL7100	CLP35	C7435n	LP235c
1.5	G108	CL1000N	CLP831	P7431cn	LP031c
1.5	G112	AP410	MLP28	P7527	LP128
1.5	G113	AP410N	MLP28N	P7527N	LP128N
1.5	G116	AP610N	MLP35N	P7535N	LP135N
1.5	G126	AP900	MLP75n	P7575	LP175hdn
1.6	B222	MP C3500	C3535	DSc535	LD435c
1.6	B224	MP C4500	C4540	DSc545	LD445c
1.6	B229	Aficio 615c	SGC 1506	GS 106	LD215cg
1.6	B230	Aficio MP C2500	C2525	DSc525	LD425c
1.6	B234	Aficio MP9000	8090	DSm790	LD190
1.6	B235	Aficio MP1100	8110	DSm7110	LD1110
1.6	B236	Aficio MP1350	8135	DSm7135	LD1135
1.6	B237	Aficio MP C3000	C3030	DSc530	LD430c
1.6	B246	Aficio MP 5500	8055	DSm755	LD255
1.6	B248	Aficio MP 6500	8065	DSm765	LD265
1.6	B249	Aficio MP 7500	8075	DSm775	LD275
1.6	B250	Aficio MP 5500 SP	8055 SP	DSm755 SP	LD255 SP
1.6	B252	Aficio MP 6500 SP	8065 SP	DSm765 SP	LD265 SP
1.6	B253	Aficio MP 7500 SP	8075 SP	DSm775 SP	LD275 SP
1.6.1	G133	Aficio SP C811DN	CLP240D	C7640nD	LP440c
1.6.1	G147	Aficio SP 8100DN	MLP145	P7245	LP145n
1.6.1	G148	Aficio SP 9100DN	MLP175n	P7675	LP275hdn
1.6.1	G160	Aficio SP C410DN	CLP27DN	C7526dn	LP226cn
1.6.1	G161	Aficio SP C411DN	CLP31DN	C7531dn	LP231cn
1.6.2	B245	Aficio MP 1500	-	DSm715	LD315
1.6.2	B276	Aficio MP 1600	9016	DSm716	LD316
1.6.2	B277	Aficio MP 2000	9021d	DSm721d	LD320
1.6.2	B284	Aficio MP 161F	816f	DSm416f	LD016f
1.6.2	B288	Aficio MP 161SPF	816mf	DSm416pf	LD016SPF
1.6.2	B291	Aficio MP 3500G	8035eg	DSm735eg	-
1.6.2	B292	Aficio MP 161	816	DSm416	LD016
1.6.2	B295	Aficio 4500G	8045eg	DSm745eg	-
1.6.2	B296	Aficio MP 3500	8035e	DSm735e	LD335
1.6.2	B297	Aficio MP 4500	8045e	DSm 745e	LD345
1.6.2	D007	Aficio MP 2510	8025e	DSm725e	LD325
1.6.2	D008	Aficio MP 3010	8030e	DSm730e	LD330
1.7	G176	Aficio SP 4100N	MLP31n	P7031n	LP131n
1.7	G177	Aficio SP 4110N	MLP36n	P7035n	LP136n

2 Embedded Services and Potential Security Issues

Some server services (Telnet, FTP, etc.) allow write access from network clients. This may make some customers feel that the products are insecure against viruses, worms, or intruder access. 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 an inconvenience, specify an Access Control list of "safe" client host addresses. Once an Access Control is in place for specific IP addresses, the products will only receive print or scan requests from the specified hosts Access Control is applied for LPD printing, RCP/RSH access, HTTP/HTTPS access (where supported), FTP printing, TCP raw printing (DIPRINT), SMB printing, IPP printing, and scanning from DeskTopBinder. For information access control set up, refer to section 4 (page 25).

It is best to disable all protocols not in use. Use the Network Security Level function, described in Appendix D (page 50), to perform a quick security configuration.

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, which allows access to 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 password.

> **NOTE**
> To request the default MSHELL password, contact Ricoh technical support.
> **Phone #:** 1-800- RICOH 38 (1-800-742-6438)
> **Hours:** Monday - Friday (excluding holidays) 8:00 AM to 8:00 PM EST.

2.1.2 Potential Threats

Destruction, corruption and modification of the file system and kernel: Not possible. MSHELL only permits write-access to network parameters and no one can access the file system or kernel.

Possibility of acting as a server for relaying viruses: None. Viruses cannot use the products 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.

Theft of username and password: Possible. When accessing the MSHELL, the username and password are sent in clear text because the Telnet protocol itself does not support encryption. So, if a packet sniffer intercepts the credentials, the possibility of unauthorized access exists.

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 them regularly.

- Since the username and password are the same as those for Web Image Monitor's Administrator mode, changing them for MSHELL means changing them for Web Image Monitor's Administrator mode.

Level 2: Close the TELNET port via Web Image Monitor. When TELNET is disabled, the services provided by the mshell will not be available.

- To disable TELNET via Web Image Monitor, login as the Administrator and then follow this click path: **Configuration** (left hand toolbar) → **Network Security** (under the header labeled *Security*) → **Scroll down to Telnet → Click Disable**.

2.2 FTP

2.2.1 Function Overview

The FTP (File Transfer Protocol) protocol is compliant with RFC 959 and enables the sending and receiving of data files over the Internet with reliability and efficiency. Transmission Control Protocol (TCP) port 20 is used for FTP-data and TCP port 21 is used for FTP-control service. Any FTP client software (e.g., FTP Commander) used must also be compliant with RFC 959.

The FTP service provides the following functions:

- Enables the reception of print jobs from FTP clients.
- Provides the files listed in the following table to 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
Fax application files (hidden)	Fax job log information Fax counter Fax address book	SmartDeviceMonitor for Admin/Client is required to read/ manage these files.

Table 1: Files Provided to FTP Clients

- Receiving firmware files from remote clients.
  - Remote Firmware Update (RFU) requires Machine administrator privileges.
  - When Web Smart Device Monitor is used for RFU, TCP port 10020/10021 sends firmware files via the FTP protocol. However, port 21 is used to negotiate the transfer. All 3 ports must be open.
  - RFU is a proprietary process defined by Ricoh and is extremely difficult to emulate without the knowledge of the specification. However, to maintain a strict security policy, close the port via MSHELL. (See section 5.2 – page 34.)

NOTE
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

Destruction, corruption and modification of the file system: Not possible. 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.

Possibility of acting as a server for relaying viruses: None. 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.

Theft of password: Possible. When accessing the FTP service, the user name and 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, only Service Technicians have a password and dedicated account for making firmware updates. There is no possibility of file system destruction by someone using a sniffed account and password, because it is impossible to make a pseudo firmware file to destroy the file system.

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.

2.3 HTTP

2.3.1 Function Overview

The HTTP (Hypertext Transfer Protocol) service provides web services. This service is compliant with RFC 1945 and generally uses TCP port 80. Some applications however, use a variety of ports for various connections.

The following web functions and connections are provided by the HTTP 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.

NOTE
Users must enter a password during Web Image Monitor Administrator mode login. The default password is the same as the default password for MSHELL.

2.3.2 Potential threats

Destruction, corruption and modification of the file system: Not Possible. No one can access the file system and executable files cannot be processed on the product's web server.

Possibility of acting as a server for relaying viruses: None. Viruses cannot use the products as an open relay server, because unrecognized data is disregarded. The web server was developed by Ricoh and will not process any malicious, executable files.

Theft of username and password: Possible. Interception of network packets: When accessing Web Image Monitor, the username and password are sent with BASE64 encryption. In this case, they are not sent in clear text, but are not difficult to decrypt either. Therefore, if the username and password are intercepted using a packet sniffer and then decrypted, there is a possibility of unauthorized access and network setting changes.

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

2.3.3 Recommended Precautions

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

Level 1: Change the password from the default value to something difficult to guess and change it regularly. Since the password is the same as the one for Web Image Monitor's Administrator mode, changing it for MSHELL means changing it for Web Image Monitor's Administrator mode as well.

Level 2: Forward HTTP requests to HTTPS. Depending on the settings, all, some, or none of the HTTP requests received by the MFP will be sent to HTTPS.

Level 3: Disable web function. If not needed, disable Web Image Monitor (WIM) using MSHELL. When set to 'Down', WIM does not activate and error "503 Service Unavailable" is displayed. Even when not in use, TCP port 80 stays open.

Level 4: Close the HTTP port. The HTTP port can be closed via MSHELL. When HTTP is set to 'Down', Web Image Monitor does not activate and the IPP (Internet Print Protocol) function that allows a printer calls via HTTP (e.g., HTTP://<printer host name or ip address>/), is unavailable. Printer calls via IPP (e.g., IPP://<printer host name or ip address>/), is available.

NOTES

- It is best to use HTTPS instead of HTTP for Web Image Monitor and IPP printing (if available).
- To reduce the possibility of print data interception, use HTTPS instead of HTTP as the printing protocol.

2.4 SNMP v1/v2

2.4.1 Function Overview

SNMP (Simple Network Management Protocol) communicates network management information between the network management stations (SNMP manager), e.g. a PC running a management application, and network agents (SNMP agent), e.g. printers, scanners, workstations or servers, and hubs. The SNMP service is embedded in the products to provide network management. SNMP is compliant with RFC 1157 for SNMP v1 and RFC 1902 for SNMP v2. UPD port 161 is used for SNMP service and UDP port 162 is used for SNMP-trap. The following functions are provided:

- Configuring the settings of the products.
- Monitoring the status of the products.
- Detecting the errors of the products.
- Communication with client PC for scanning via the TWAIN driver.

SNMP service is not protected by a password, but it is protected using unique community names and assigned access (read-only, read-write, trap) within those communities. Communication with, or configuration of, an agent is allowed only if it is a member of the same community and the access rights allow modification of the MIBs (Management Information Base) data embedded in the products.

NOTE

Below are the default SNMP community settings.

- **Community Name 1:** Public
  - Access type: Read-only
- **Community Name 2:** Admin
  - Access Type: Read-write

2.4.2 Potential threats

Destruction, corruption and modification of the file system: None. SNMP only permits write-access to network parameters, and no one can access the file system or kernel.

Theft of community name: Possible. Interception of network packets: Community names are sent in clear text because of the specification of the protocol, so it is readable if intercepted.

Possibility of unauthorized parties intercepting device information: Unlikely. 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, so the security risk is low. However, when accessing the products via SNMP, other parameters are sent in clear text, because the SNMP v1/v2 protocol does not support encryption. So, if other parameters are intercepted, it is a possible for unauthorized parties to obtain device information.

2.4.3 Recommended Precautions

Below are the suggested precautions to minimize the risk of the threats in Section 2.4.2. 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.

> **NOTE:** If the community name settings are changed in the agents, they must also be changed in the management utilities.

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. Unless absolutely necessary, the SNMP port should be closed via Web Image Monitor or the mshell.

NOTES

- Please refer to Appendix C (page 40) for details about SNMP settings.
- Use the highest security level possible. Use SNMP v3, if SNMP v1/v2 is not necessary.
  - Utilities that do not support SNMP v3 cannot get device status unless SNMP v1/v2 is enabled. So, these utilities will not work correctly with SNMP v1/v2 disabled.
  - If a utility does not support SNMP v3 and only requires 'get' access to work (makes no changes to MFP settings), we recommend using 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 print and system logs to RSH/RCP clients.
- Transferring scan data to the Twain driver.

2.5.2 Potential Threats

Destruction, corruption and modification of the file system: Not possible. No one can access the file system or kernel and executable files cannot be processed via the remote shell service.

Possibility of acting as a server for relaying viruses: None. Unrecognized data is disregarded. Although the remote shell service permits write-access, all written data is treated as a print job. Even if someone sent an executable file via the embedded remote shell service, the products print the file as garbage data.

Theft of user name: Possible. The user name is sent in clear text when using the remote shell service. If the user is concerned about this, the port for remote shell service can be completely closed via Web Image Monitor and MSHELL.

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.

> **NOTE**
> To reduce the possibility of print data interception, use HTTPS instead of RSH/RCP as the printing protocol.

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.

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 from LPR clients,
- Monitoring the status of the printer and print queues of LPR clients,
- Deleting print jobs from print queues of LPR clients.

2.6.2 Potential Threats

Destruction, corruption and modification of the file system: Not possible. No one can access the file system via the LPR service.

Possibility of successful DoS (Denial of Service) attacks: None. When the products receive data that does not meet the protocol specification, the products will stop the LPD service, and the executed application (if any), at regular steps.

Possibility of acting as a server for relaying viruses: None. LPD treats all data as a print job. If an executable file is sent via LPD, the products print the file as garbage data.

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

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 Precautions

To maintain a strict security policy, disable the LPD service and the port for the service using Web Image Monitor or the MSHELL.

> **NOTE**
> To reduce the possibility of print data interception, 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 or TCP port 80. 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 user name and password are sent in clear text. "Digest" authentication is more secure with the user name and password irreversibly encrypted. 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

Destruction, corruption and modification of the file system: Not Possible. The file system cannot be accessed via the IPP service in the products.

Possibility of successful DoS (Denial of Service) attacks: None. 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 at regular steps if data that falls outside of the protocol specification is present in the system.

Possibility of acting as a server for relaying viruses: None. LPD treats all data as a print job. If an executable file is sent via LPD, the products print the file as garbage data.

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.

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 Precautions

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). Take the appropriate action for your security policy.

Level 1: Set IPP Authentication to either "basic" or "digest" from "disabled" in Web Image Monitor, MSHELL or the operation panel. "Digest" authentication is more secure than "basic" because the username and password are encrypted.

Level 2: Close the IPP (631/TCP) port. If not necessary, close the IPP port via Web Image Monitor or MSHELL. However, using HTTP://<printer host name or IP address>/ (an IPP function) is available.

NOTES

- This only closes the IPP port. The IPP service is still available via HTTP or HTTPS.
- To reduce the chance of print data interception, 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's name for port 9100 communication. This service uses TCP port 9100 to direct print from remote terminals.

2.8.2 Potential threats

Possibility of acting as a server for relaying viruses: None. 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.

Theft of username and password: Interception of network packets: DIPRINT does not have an authentication function. However, print data may contain authentication information. The printer driver can encrypt this information. Please refer the user manual and driver help for more information about this method.

There are not many threats in this service because all written data is treated as a print job. Even if someone sent an executable file via the embedded remote shell service, the products would print the file as garbage data.

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 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 DIPRINT port can be changed and the port for this service can be completely closed using Web Image Monitor or MSHELL.

> **NOTE**
> To reduce the possibility of print data interception, please use HTTPS instead of DIPRINT as the printing protocol.

2.9 NBT

2.9.1 Function Overview

The NBT stands for NetBIOS over TCP/IP. The products provide the NetBIOS (Network Basic Input/Output System) service over TCP/IP instead of NetBEUI (NetBIOS Extended User Interface) so remote hosts 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 provides the following services:

- 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.

> **NOTE**
> For information on the SMB service, please see Appendix C.2 (page 42).

2.9.2 Potential Threats

Possibility of browsing the network by unauthorized parties: Possible. To prevent unauthorized browsing of the products, disable the SMB service using Web Image Monitor or MSHELL.

Possibility of successful DoS (Denial of Service) attacks: None. Repeated access and disconnection to TCP port 139 is a well known DoS attack. The products are protected against this by accepting the connections sequentially. When the products receive data that can carry out a DoS attack, the connection with the sender will be disconnected.

Possibility of acting as a server for relaying viruses: None. LPD treats all data as a print job. If an executable file is sent via LPD, the products print the file as garbage data.

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.

2.9.3 Recommended Precautions

If the NetBIOS Session service (139/TCP) is not necessary, disable it using Web Image Monitor (set SMB to disable) or the MSHELL (set SMB to 'Down'). When SMB is disabled, SMB over NetBEUI is also disabled. There is no method to disable only NetBIOS Session Service (139/TCP) without disabling SMB over NetBEUI. UDP port 137 and 138 cannot be closed even if SMB is disabled.

2.10 Authentication Service

2.10.1 Function Overview

This proprietary Ricoh service is sometimes referred to internally as uA/uD Service. ScanRouter, and other Ricoh document solutions products, use it to authenticate connections to resources, such as in-trays and management utilities. It acts as an intermediary between clients trying to connect to a ScanRouter server and an external directory service being used by ScanRouter, etc. for authentication.

2.11 Others

2.11.1 @Remote

TCP port 7443 and 7444 are reserved for the @Remote service. Those ports cannot be closed. However, there are no threats that apply to the products because this service accepts only a Ricoh-confidential protocol and it is impossible to emulate without knowledge of the protocol specification.

> **NOTE**
> Closing the ports via Telnet (Mshell) further strengthens network security. Please see section 4.2 (page 29) for more information on disabling the ports using Telnet.

In addition, we do not disclose the protocol specification to anyone outside of Ricoh Corporation. HTTP is used for this service as an underlying layer. Please refer to section 2.3 HTTP (page 11) for the potential threats and recommended precautions.

3 Services provided with open TCP/UDP ports

Protocol	Port Num.	Login	Username Changeable	Password	Password Changeable	Note
Telnet	23/TCP	N/A	N/A	Y	Y	This is the same password as Web Image Monitor.
FTP-control	21/TCP	Y	N/A	N/A	N/A	
HTTP	80/TCP	N/A	N/A	Y	Y	This is the same password as Telnet. Not entering a password allows read access only.
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.
HTTPS	443/TCP	N/A	N/A	Y	Y	This is the same password as Telnet and HTTP. Not entering a password allows read access only.
RSH/RCP (shell)	514/TCP	N/A	N/A	N/A	N/A	
LPD	515/TCP	N/A	N/A	N/A	N/A	
IPP	631/TCP	Y	Y	Y	Y	Authentication by account/password is not performed by default. All users are ANONYMOUS. When IPP authentication is enabled, a username and password will be required.
DIPRINT	9100/TCP	N/A	N/A	N/A	N/A	

3.1 Related Protocols

Protocol	Protocol Suite	Commonly Used Port Number	Description of the protocol's function in 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	Sending scan data to the SMTP server. (Scan to E-mail)
DOMAIN (DNS)	TCP/IP	53/TCP, UDP	Resolving IP addresses from the server name.
BOOTP DHCP	TCP/IP	67/TCP, UDP 68/TCP, UDP	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	Getting GMT from the NTP server.
NetBIOS-NS	TCP/IP, IPX/SPX, NetBEUI	137/TCP, UDP	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	Getting internet-fax data
SNMP-TRAP	TCP/IP, IPX/SPX	162/TCP, UDP	Sending status information to Network Management Server.
LDAP	TCP/IP	389/UDP, TCP	Searching e-mail addresses from the LDAP server's address book.
SYSLOG	TCP/IP	514/UDP	Sending system logs to a syslog server.
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	Searching for a Netware Server.

Protocol	Protocol Suite	Commonly Used Port Number	Description of the protocol's function in Products.
IPX	IPX/SPX	-	Providing IPX connections
SPX	IPX/SPX	-	Providing SPX connections
SAP	IPX/SPX	-	Broadcasts to availability of print services.
RIP	IPX/SPX	-	Broadcasts route information.
APPLETALK	APPLETALK	-	Providing APPLETALK connections.
PAP	APPLETALK	-	Providing APPLETALK printing services
NetBeui	NETBEUI	-	Providing NetBEUI connections.

4 Purpose of Access Control

The products only accept communication from a set range of IP addresses. This can be applied to connections from LPR, RCP/RSH, HTTP, HTTPS (where supported), FTP, DIPRINT, SMB, IPP, and DeskTopBinder. It cannot be applied to Telnet, a web browser, or SmartDeviceMonitor.

4.1 Web Image Monitor Access Control

Web Image Monitor can access the products, using a supported browser such as Microsoft Internet Explorer. The product's IP address is required.

1. Enter the IP address in the address field using the following form: *http://printer host name or IP address* (e.g. http://172.16.121.40) and click on **Go** or press Enter. This opens the page shown in Figure 4.1 below.
2. In the upper right-hand corner, click **Login**, which opens a login page (Figure 4.2).

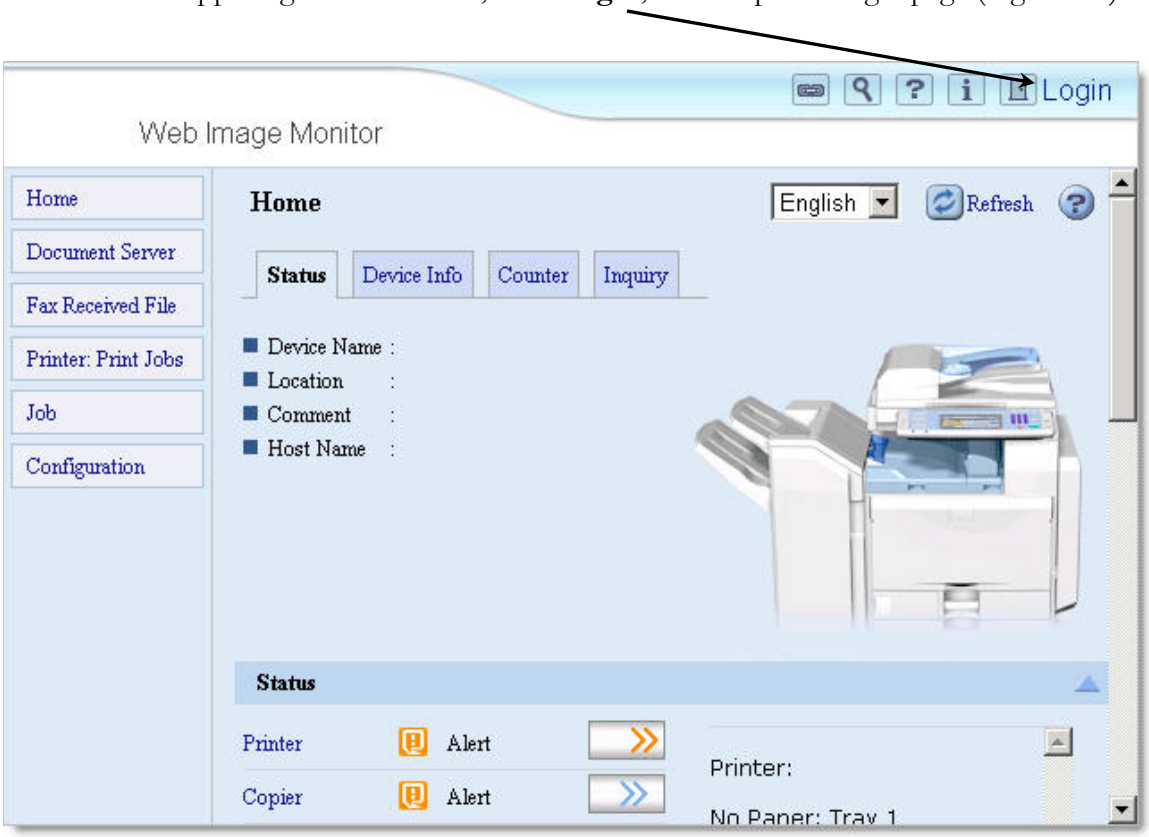


Figure 4.1: Web Image Monitor Main Screen

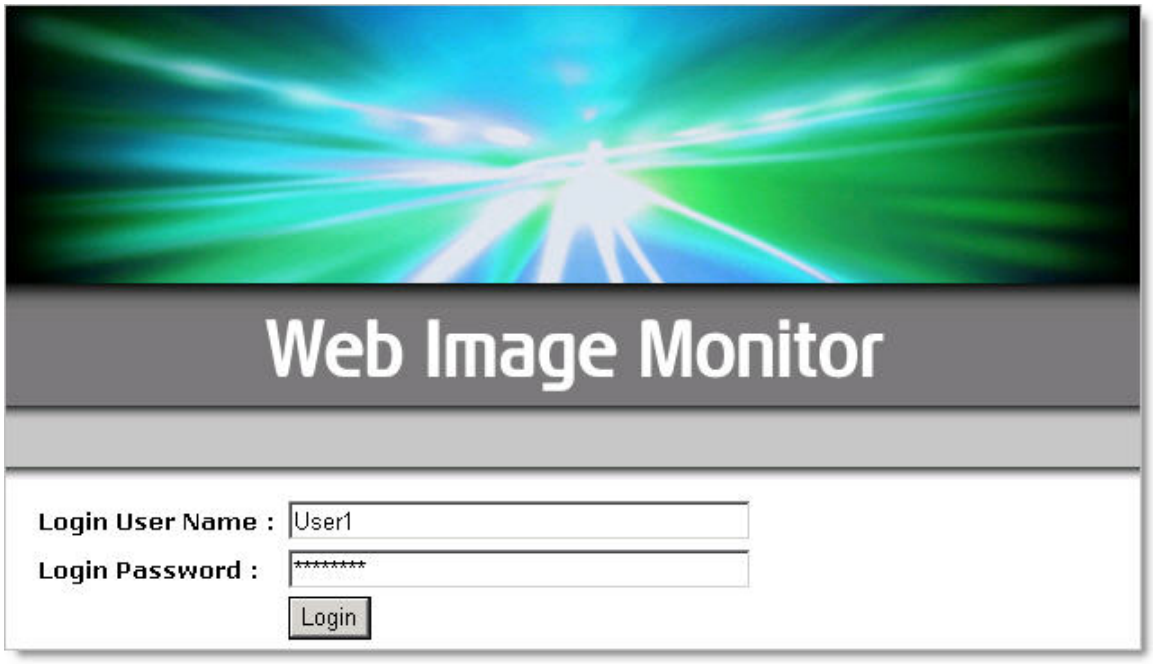


Figure 4.2: Web Image Monitor Login Page

1. Access to Administrator mode requires a password. Login to enter Administrator mode.
2. If the login was successful, the word **Administrator** in the upper right-hand corner. See Figure 4.3.

NOTE
The login process may differ slightly depending on the machine in use.

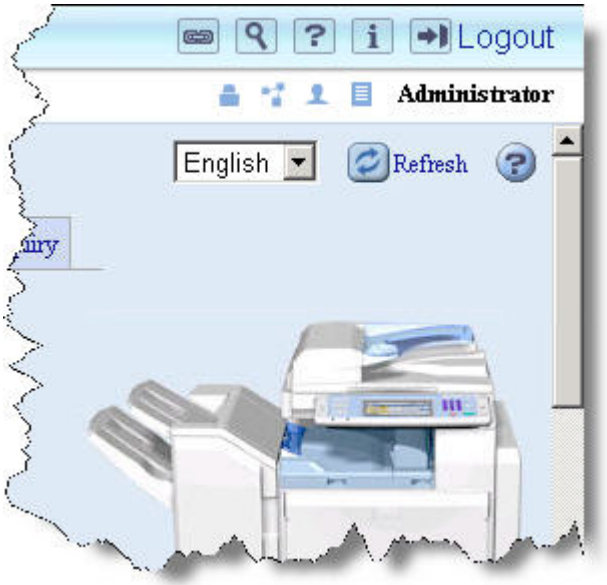
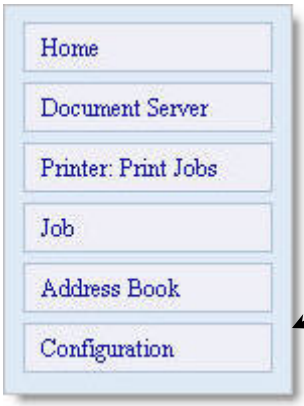


Figure 4.3: Administrator Main Screen



5. On the left-hand toolbar click on **Configuration** to expand the Configuration menu.
6. Under the Security heading, click **Access Control** (Figure 4.5).

Figure 4.4: Toolbar

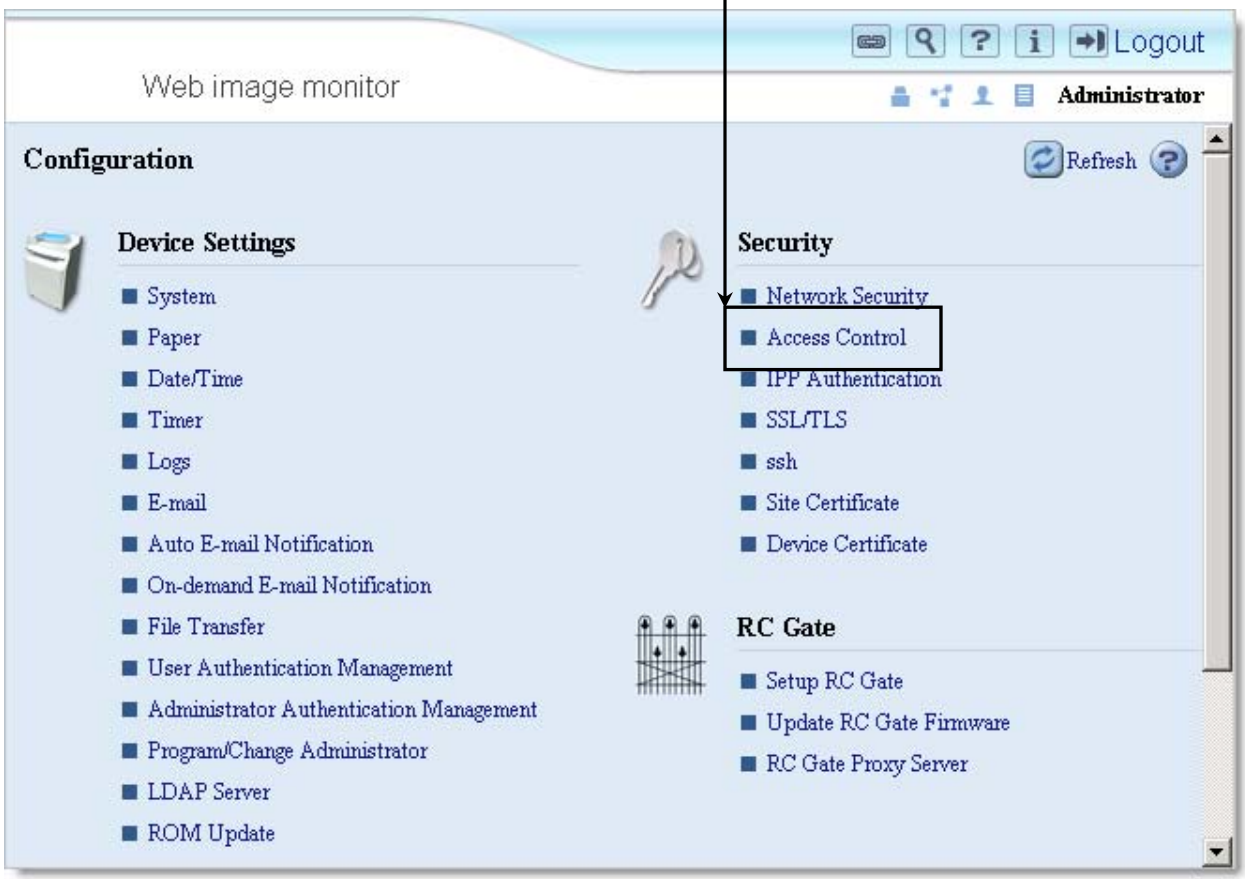


Figure 4.5: Web Image Monitor Configuration Screen

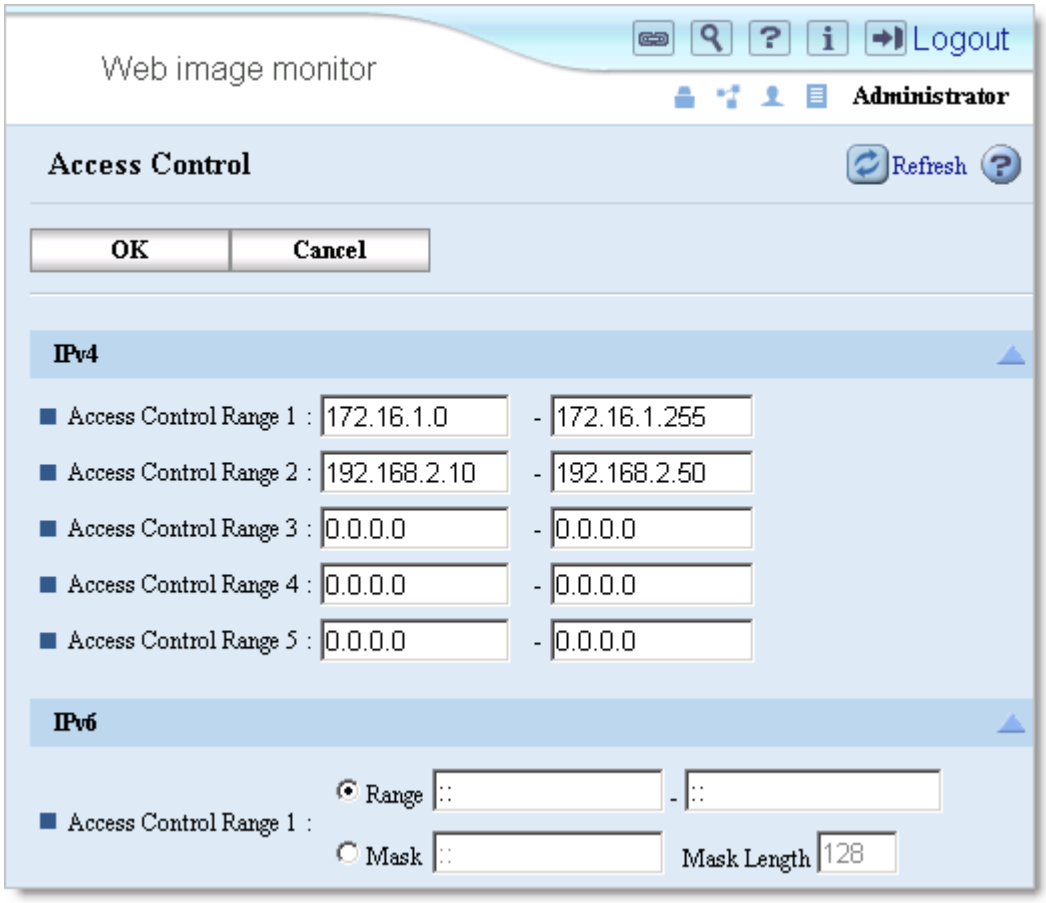


Figure 4.5: Access Control Panel

7. In the Access Control fields (Figure 4.5), enter the range of allowed IP addresses for communication.
8. Click **OK** to save the settings. The products now accept communications from the specified IP addresses only.

4.1.1 Administrator Icons

The icons below identify the four administrator types.

- Machine Administrator
- Network Administrator
- User Administrator
- File Administrator

4.2 TELNET/Maintenance Shell (MSHELL)

Access the products using a Telnet (Mshell) client. Below is the Telnet (Mshell) access procedure.

1. On the Windows taskbar, click **Start**.
2. On the start menu, click **Run**, and enter the following:
   telnet XXX.XX.XXX.XX (e.g. telnet 123.45.678.90). See Figure 4.7.

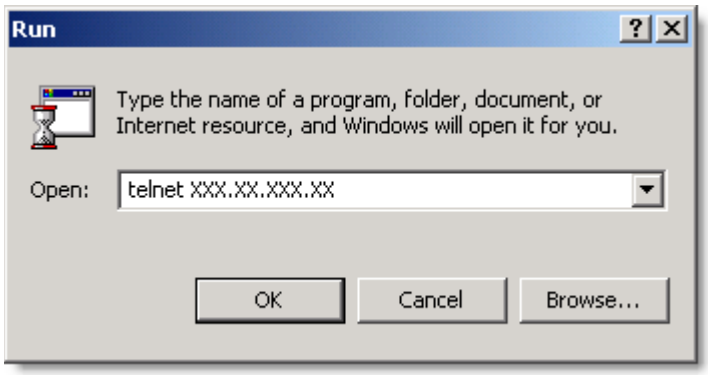


Figure 4.7: Run Telnet Command

3. Click **OK** to open the telnet client. It will go directly to the Telnet (Mshell) login.
4. To access MSHELL enter the login and password.
5. At the msh> prompt, type **access** and press **Enter**.

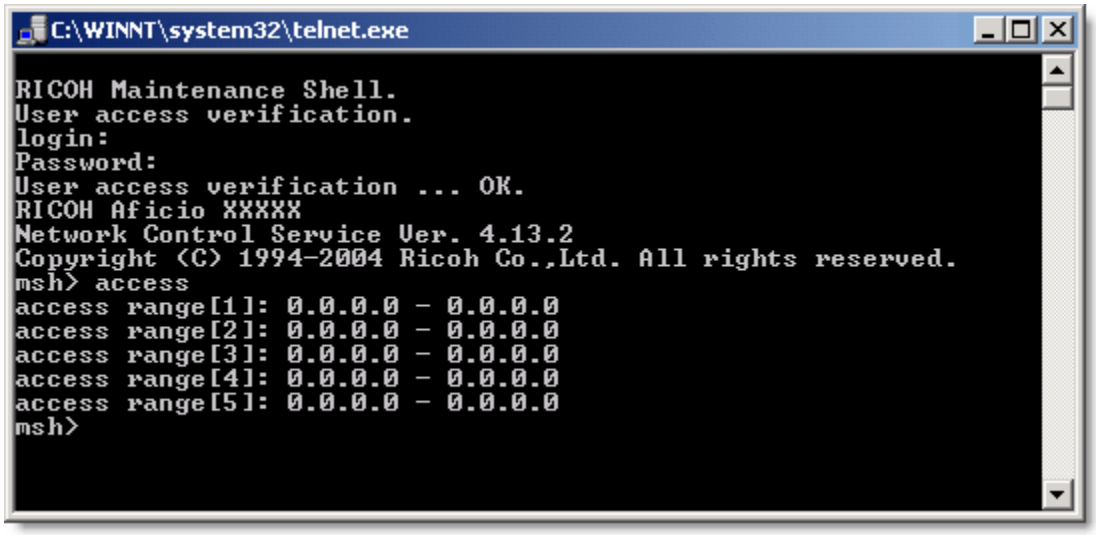


Figure 4.8: MSHELL

6. Enter the following command to set the IP access ranges: **msh>access 1 range XXX.XXX.XXX.XXX YYY.YYY.YYY.YYY** (e.g. entering 176.16.1.0 176.16.1.255 will allow access to IP addresses 176.16.1.0 thru 176.16.1.255)

NOTE
The command: **msh> access flush** will clear all access ranges.

7. After the access ranges are set, type **logout** and press **Enter**.
8. MSHELL will ask whether or not to save the configuration data (Figure 4.9).
9. Enter **yes** to commit the changes or **no** to discard them.

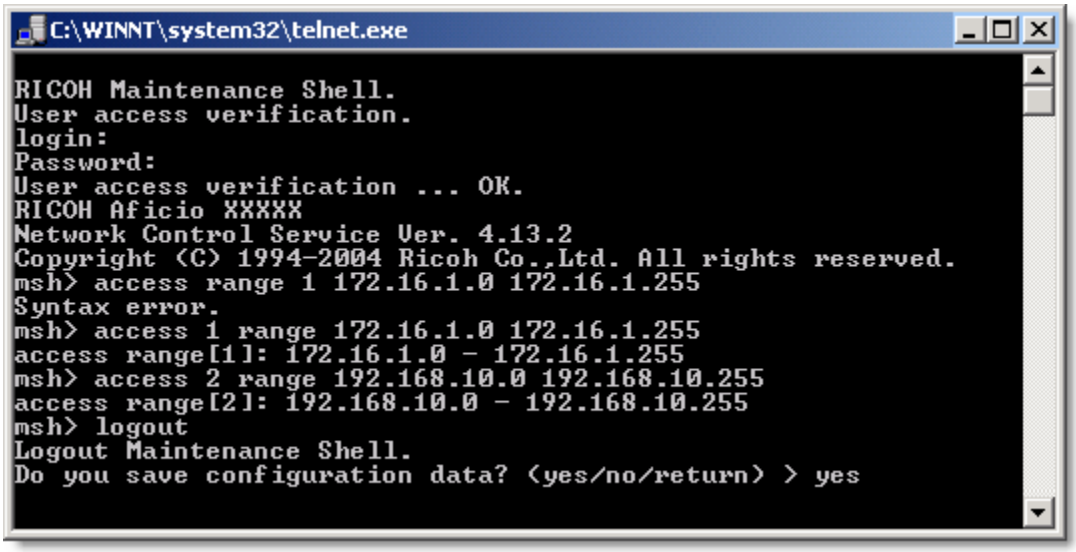


Figure 4.9: MSHELL Logout

5 Service Settings

The following services can be enabled or disabled via Web Image Monitor or MSHELL. The table below lists each service, along with the port(s) used and the interface used when disabling a particular service.

Service/Protocol	Port	Web Image Monitor		mshell		Comment
Netware	-	Y		Y		Setting Netware to **down** disables the IPX/SPX protocol and NCP/IP. So, if Netware is down, printing in the IPX/SPX environment and in the pure IP environment is unavailable. o LPR in NDPS and iPrint (IPP Printing) are unaffected.
AppleTalk	-	Y		Y		
		IPv4	IPv6	IPv4	IPv6	
TCP/IP	-	Y	Y	Y	Y	TCP/IP cannot be set via Web Image Monitor (e.g. 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 (meaning Scan to FTP will continue to function, if in use).
SSH/SFTP	22	Y	Y	Y	Y	Setting either SSH or SFTP down will close this port (22).
TELNET	23	Y	Y	-	-	Telnet cannot be disabled via mshell.
SMTP	25	Y	-	-	-	To close this port, set the e-mail reception protocol to POP3 or IMAP4 in WIM via this path: Configuration → E-mail → Reception Protocol.
HTTP	80	Y	Y	Y	Y	*Via mshell*: Use the **set http down** command to close this port. The **set web down** command does not close this port. *Via Web Image Monitor:* In order to close the port, the device must be connected via HTTPS or IPv6.
IPP	631	Y	Y	Y	Y	Setting IPP to down disables the IPP printing function but doesn't close the IPP Port (631/TCP). Therefore if IPP is down, IPP printing using HTTP (80/TCP) is still available.
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, this only affects the server service. The client service is not affected. Therefore, if SMB is down, Scan to SMB will still function.

SNMP	161	Y	Y	Y	Y	Setting SNMP to down closes the 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. ***Note:*** 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	-	-	-	*Via WIM:* To close the port, follow this path: Configuration → FAX → IP Fax Settings → Set Enable H.323 radio button to **Off**. *Via mshell:* This port cannot be closed via mshell.
SSDP	1900	Y	-	Y	-	Setting SSDP to down makes UPnP unavailable and closes the SSDP port (1900/UDP)
MDNS	5353	Y	-	Y	-	Set Bonjour to down to close this port.
SIP	5060	Y	-	-	-	*Via WIM:* To close the port, follow this path: Configuration → Fax → IP-Fax Settings → Swith Enable SIP to **Off**. *Via mshell:* This port cannot be closed via mshell.
@Remote	7443/7444	-	-	Y	-	*Via mshell:* To disable, use the **set nrs down** command.
DIPRINT	9100	Y	Y	Y	Y	If this port is closed, printing from diprint client is not possible.
RFU	10021	-	-	Y	Y	If this port is closed, remote firmware update will be done via ftp. ***Note:*** If RFU is performed via FTP, the password will be unencrypted and sent in plain text.

5.1 Disabling Services thru Web Image Monitor

Refer to section 4.1: Web Image Monitor Access Control (page 25) for the Administrator login procedure. The following steps detail the process for disabling services.

1. On the left-hand toolbar click on **Configuration** to open the Configuration page.
2. Under the Security heading, click **Network Security**.

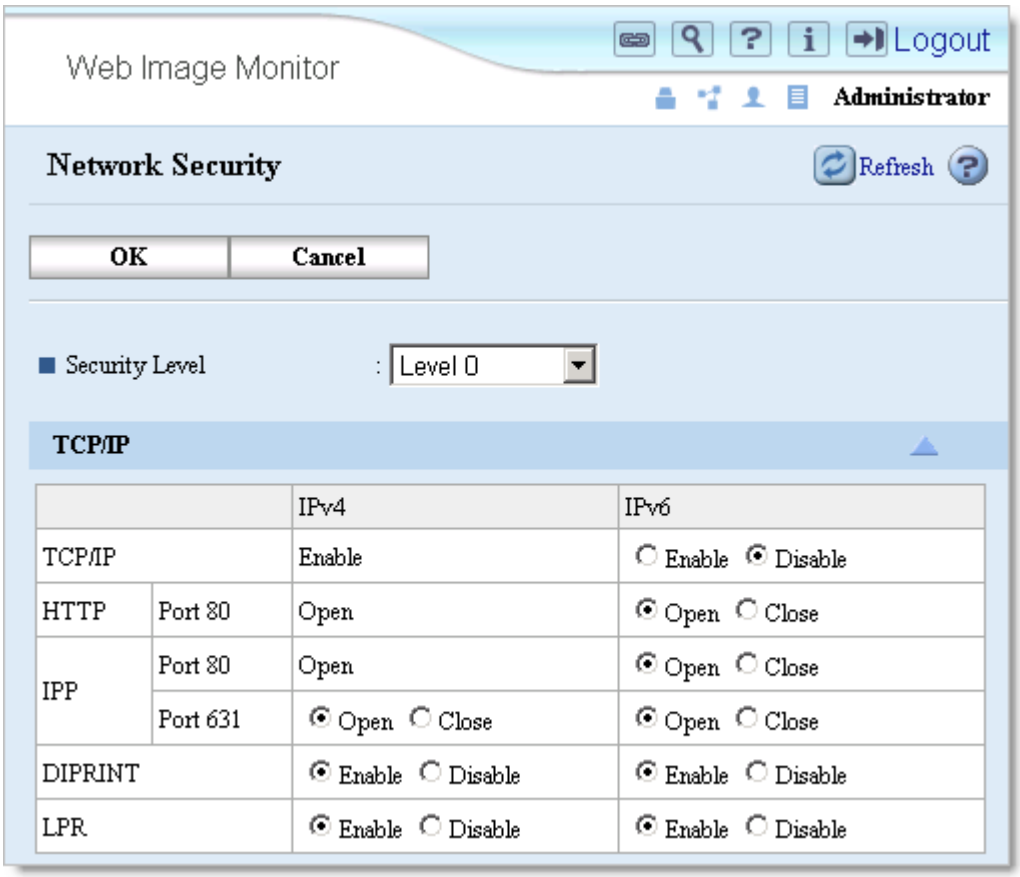


Figure 5.1: Network Security Configuration Menu

3. Select **Disable** (Figure 5.1) to stop any unwanted services.
4. Click **OK** to save changes.

> **NOTE**
> The default setting enables all protocols.

5.2 Disabling Services thru MSHELL

Refer to steps 1-4 of Section 4.2 for the MSHELL (page 29) login procedure. The following steps detail the process for disabling services.

1. At the **msh>** prompt, enter **set XXX down** to disable the service; e.g. enter set http down to disable HTTP (Figure 5.2).

> **NOTE**
> The parameters in the following screen capture show the set command usage and protocols.

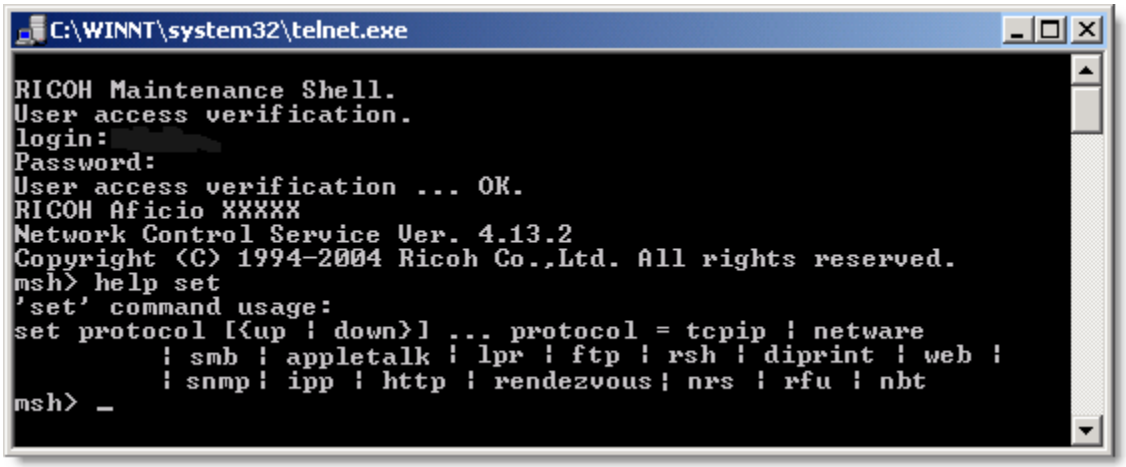


Figure 5.2: Disabling Services thru MSHELL

2. Close your MSHELL session by entering **logout** at the **msh>** prompt. Close Telnet by entering **quit**.

6 Summary and References

This document covered potential threats to network security and the recommended precautions to protect the products. Please use the information in this document as a guideline for appropriate actions to take to ensure the security of your networked devices.

The following websites are provided as reference so you can learn more about network security:

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

Appendix A

The material in Appendix A only applies to the models listed in the Cross Reference table below.

Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
B070	Aficio 2090	4090	9002	LD090
B071	Aficio 2105	4105	10512	LD0105
B079	Aficio 2035	4035	3532	LD035
B082	Aficio 2045	4045	4532	LD045
B089	Aficio 2022	4022	DSm622	LD122
B093	Aficio 2027	4027	DSm627	LD127
B121	Aficio 2015	4015	DSM615	LD115
B122	Aficio 2018	4018	DSM618	LD118
B123	Aficio 2018D	4018D	DSM618d	LD118D
B129	Aficio 1515	3515	DSm415	LD015
B130	Aficio 1515MF	3515MF	DSm415pf	LD015spf
B135	Aficio 2035e	4035e	DSm635	LD135
B138	Aficio 2045e	4045E	DSm645	LD145
B147	Aficio 2232c	C3224	DSc332	LD232c
B149	Aficio 2238c	C3828	DSc338	LD238c
B168	Aficio 1515F	3515F	DSm415f	LD015f
B169	Aficio 2013PS		DSm415p	LD015sp
B182	Aficio 2035eSP	4035Esp	DSm635sp	LD135
B183	Aficio 2045eSP	4045Esp	DSm645sp	LD145
B190	Aficio 2228c	C2820	DSc328	LD228c
G091	AP600N	MLP32	P7132N	LP032
G094	AP400	MLP25	P7325	LP025 / LP026
G095	AP400N	MLP25N	P7325N	LP025N/LP026N
G106	CL7100	CLP35	C7435n	LP235c
G108	CL1000N	CLP831	P7431cn	LP031c

A.1 FTP Potential Threats

Possibility of acting as a server for relaying viruses: Possible. It is possible to access other hosts through the products by using the PORT command. This is known as an "FTP bounce attack" (see: HTTP://cgi.nessus.org/plugins/dump.php3?id=10081 for more information). To prevent this type of attack, close the FTP port.

Possibility of successful DoS (Denial of Service) attack: Possible. There is a possibility of coming under hostile DoS attack when using the PASV command (see: HTTP://cgi.nessus.org/plugins/dump.php3?id=10085 for more information). If the FTP server continues to receive the PASV command, other FTP connection requests will be refused. In order to recover the status of the products, rebooting is required. To prevent this vulnerability, close the FTP port.

A.2 HTTPS Potential Threats

Possibility of attacker taking advantage of a heap corruption error in OpenSSL: Possible. This results in a crash which causes a DoS (Denial of Service), or disables secure communications (HTTPS). (see: cgi.nessus.org/plugins/dump.php3?id=11875 for more information). To prevent this vulnerability, close the HTTPS port.

Appendix B

The material in Appendix B only applies to the models listed in the Cross Reference table below.

Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
B132	Aficio 3260c	C6045	DSc460	LD160c
B140	Aficio 2060	4060	DSm660	LD160
B141	Aficio 2075	4075	DSm675	LD175
B142	Aficio 2060SP	4060sp	DSm660sp	LD160 SP
B143	Aficio 2075SP	4075sp	DSm675sp	LD175 SP
B156	Aficio 3224c	C2410	DSC424	LD124C
B163	Aficio 2051	4051	DSm651	LD151
B178	Aficio 3235C	C3528	DSc435	LD335c
B180	Aficio 3245C	C4535	DSc445	LD345c
B200	Aficio 5560	SDC555	CS555	LC155
B202	Aficio 3228C	C2824	DSC428	LD328c
B205	Aficio 3025/SP/SPF/SPi/P	8025/sp/ spf/spi/P	DSm725/sp/ spf/spi/p	LD225/SP
B209	Aficio 3030/SP/SPF/SPi/P	8030/sp/ spf/spi/P	DSm730/sp/ spf/spi/p	LD230
B222	MP C3500	C3535	DSc535	LD435c
B224	MP C4500	C4540	DSc545	LD445c
B228	Aficio 2051SP	4051sp	DSm651sp	LD151 SP
B229	Aficio 615c	SGC 1506	GS 106	LD215c
B230	Aficio MP C2500	C2525	DSc525	LD425c
B234	Aficio MP 9000	8090	DSm790	LD190
B235	Aficio MP 1100	8110	DSm7110	LD1110
B236	Aficio MP 1350	8135	DSm7135	LD1135
B237	Aficio MP C3000	C3030	DSc530	LD430c
B246	Aficio MP 5500	8055	DSm755	LD255
B248	Aficio MP 6500	8065	DSm765	LD265
B249	Aficio MP 7500	8075	DSm775	LD275
B250	Aficio MP 5500 SP	8055 SP	DSm755 SP	LD255 SP
B252	Aficio MP 6500 SP	8065 SP	DSm765 SP	LD265 SP
B253	Aficio MP 7500 SP	8075 SP	DSm775 SP	LD275 SP
B264	Aficio 3035/SP/SPF/Spi/G	8035/sp/ spf/spi/34g	DSm735/sp/ spf/spi/G	LD235
B265	Aficio 3045/SP/SPF/Spi/G	8045/sp/ spf/spi/g	DSm745/sp/ spf/spi/G	LD245
G104	Aficio CL4000DN	CLP26DN	C7425dn	LP126cn
G106	CL7100	CLP35	C7435n	LP235c
G108	CL1000N	CLP831	P7431cn	LP031c
G112	AP410	MLP28	P7327	LP128
G113	AP410N	MLP28N	P7327N	LP128N
G116	AP610N	MLP35N	P7535N	LP135N
G126	AP900	MLP75n	P7575	LP175hdn
G130	Aficio CL7200	CLP128	C7528n	LP332c
G131	Aficio CL7300	CLP135	C7535n	LP335c
G176	Aficio SP 4100N	MLP31n	P7031n	LP131n
G177	Aficio SP 4110N	MLP36n	P7035n	LP136n

B.1 MDNS

B.1.1 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. It uses UDP port 5353. The products only use MDNS for Apple's Bonjour application. If Bonjour is not being used, port 5353 can be closed.

B.1.2 Potential threats and recommended precaution

Destruction, corruption and modification of the file system: Possible. It may be possible for unauthorized parties to access available services and device information while Bonjour and MDNS are being used.

Possibility of successful Dos (Denial of Service) attacks: The possibility of a successful attack of this type is considered small at this time.

B.1.3 Recommended precautions

To maintain a strict security policy, close the MDNS port (5353/udp) via Web Image Monitor or the MSHELL. (If Apple's Bonjour application is turned off, the MDNS port is closed automatically.)

B.2 HTTPS

B.2.1 Function Overview

HTTPS is HTTP over SSL (Secure Socket Layer). HTTPS provides the same functions as HTTP. This service is compliant with RFC 1945 and generally uses TCP port 80. Some applications however, use a variety of ports for various connections.

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.)
- Username and password encryption during transmission to server.

NOTE
SSL is a communication technology used for secure connections between two 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.

B.2.2 Potential Threats

Destruction, corruption or modification of the file system: Not possible. No one can access the file system and the products web server cannot process executable files.

Possibility of acting as a server for relaying viruses: None. The web server was developed by Ricoh, and will not process any malicious and executable files.

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

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.

B.2.3 Recommended precautions

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 password from the default value to something difficult to guess and change it regularly. The password is the same as the one for logging in to the MSHELL, so changing the password for Web Image Monitor's Administrator mode means changing it for the MSHELL.

Level 2: Disable web function. If not needed, disable Web Image Monitor 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.

Level 3: Close the HTTPS port. Use MSHELL to completely close the HTTPS port. 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.

Appendix C

The material in Appendix C only applies to the models listed in the Cross Reference table below.

Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
B132	Aficio 3260c	C6045	DSc460	LD160c
B140	Aficio 2060	4060	DSm660	LD160
B141	Aficio 2075	4075	DSm675	LD175
B142	Aficio 2060SP	4060sp	DSm660sp	LD160 SP
B143	Aficio 2075SP	4075sp	DSm675sp	LD175 SP
B156	Aficio 3224c	C2410	DSC424	LD124C
B163	Aficio 2051	4051	DSm651	LD151
B178	Aficio 3235C	C3528	DSc435	LD335c
B180	Aficio 3245C	C4535	DSc445	LD345c
B200	Aficio 5560	SDC555	CS555	LC155
B202	Aficio 3228C	C2824	DSC428	LD328c
B205	Aficio 3025/SP/SPF/SPi/P	8025/sp/ spf/spi/P	DSm725/sp/ spf/spi/p	LD225/SP
B209	Aficio 3030/SP/SPF/SPi/P	8030/sp/ spf/spi/P	DSm730/sp/ spf/spi/p	LD230
B222	MP C3500	C3535	DSc535	LD435c
B224	MP C4500	C4540	DSc545	LD445c
B228	Aficio 2051SP	4051sp	DSm651sp	LD151 SP
B229	Aficio 615c	SGC 1506	GS 106	LD215c
B230	Aficio MP C2500	C2525	DSc525	LD425c
B234	Aficio MP 9000	8090	DSm790	LD190
B235	Aficio MP 1100	8110	DSm7110	LD1110
B236	Aficio MP 1350	8135	DSm7135	LD1135
B237	Aficio MP C3000	C3030	DSc530	LD430c
B246	Aficio MP 5500	8055	DSm755	LD255
B248	Aficio MP 6500	8065	DSm765	LD265
B249	Aficio MP 7500	8075	DSm775	LD275
B250	Aficio MP 5500 SP	8055 SP	DSm755 SP	LD255 SP
B252	Aficio MP 6500 SP	8065 SP	DSm765 SP	LD265 SP
B253	Aficio MP 7500 SP	8075 SP	DSm775 SP	LD275 SP
B264	Aficio 3035/SP/SPF/Spi/G	8035/sp/ spf/spi/34g	DSm735/sp/ spf/spi/G	LD235
B265	Aficio 3045/SP/SPF/Spi/G	8045/sp/ spf/spi/g	DSm745/sp/ spf/spi/G	LD245
G104	Aficio CL4000DN	CLP26DN	C7425dn	LP126cn
G112	AP410	MLP28	P7327	LP128
G113	AP410N	MLP28N	P7327N	LP128N
G116	AP610N	MLP35N	P7535N	LP135N
G126	AP900	MLP75n	P7575	LP175hdn
G130	Aficio CL7200	CLP128	C7528n	LP332c
G131	Aficio CL7300	CLP135	C7535n	LP335c
G176	Aficio SP 4100N	MLP31n	P7031n	LP131n
G177	Aficio SP 4110N	MLP36n	P7035n	LP136n

C.1 SNMP v3

C.1.1 Function Overview

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

- User Authentication
- Data Encryption

C.1.2 Potential Threats

Destruction, corruption and modification of the file system: None. SNMP only permits write-access to network parameters. No one can access the file system or kernel.

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

Brute force attack: Unlikely. 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).

Possibility of products being seen on the network by unauthorized parties via browsing (e.g. via network neighborhood): Protect the products against unauthorized browsing by disabling the NetBIOS-NS and NetBIOS-DGM services via mshell.

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.

C.1.3 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 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.

C.2 SMB

C.2.1 Function Overview

The SMB service uses NBT (NetBIOS over TCP/IP) as its base layer. For more details on the NBT function, see section 2.9 (page 20).
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

C.2.2 Potential threats and recommended precautions

Possibility of acting as a server for relaying viruses: None. 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.

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 prints, minimizing the security risk since no system changes can be via SMB. However, some print data may contain authentication information. Enabling the printer driver's encryption function before sending data to the MFP can encrypt the password. Please refer to the user manual and driver help for more information about this function.

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.

C.2.3 Recommended precaution

The suggested precautions against this threat are below. The levels 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.

- Disabling these services will prevent the products from appearing on the network (i.e. Via network neighborhood).

Level 2: Disable the SMB service.

- If it is not necessary, disable the SMB service via Web Image Monitor or the mshell.

> **NOTE**
> Use HTTPS instead of SMB as the printing protocol to reduce the possibility of print data interception by a third party.

C.2.4 Disabling NBT/SMB

NBT/SMB: Setting NBT to down closes NetBIOS-NS (137/UDP) and NetBIOS-DGM (138/UDP).

C.3 Other Embedded Services

TCP port 10021 is reserved for communication with a new utility that will launch in the future. Ricoh defined this specification and it is impossible to emulate without knowledge of the specification. In addition, no one outside of Ricoh will have any information about the specification. There are no threats that apply to the products, but to maintain a strict security policy, port 10021 can be closed via TELNET. FTP is used for this service as an underlying layer. Please refer to section 2.2 FTP (page 9) 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.

C.4 Additional Services Provided with open TCP/UDP Ports

Protocol	Port Num.	Login	Default Username	Username Changeable	Password	Password Changeable	Note
MDNS	5353/UDP	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 is for a future utility.
For machine internal use	12701/TCP	N/A	N/A	N/A	N/A	N/A	Access from the outside will be rejected.

Figure C.1: Additional Services

C.5 HTTP/HTTPS settings

Refer to section 4.1: Web Image Monitor Access Control (page 25) for the Administrator login procedure. Below is an overview of the SSL/TLS settings.

1. To access the SSL/TLS settings, click **Configuration → SSL/TLS** (under Security heading).

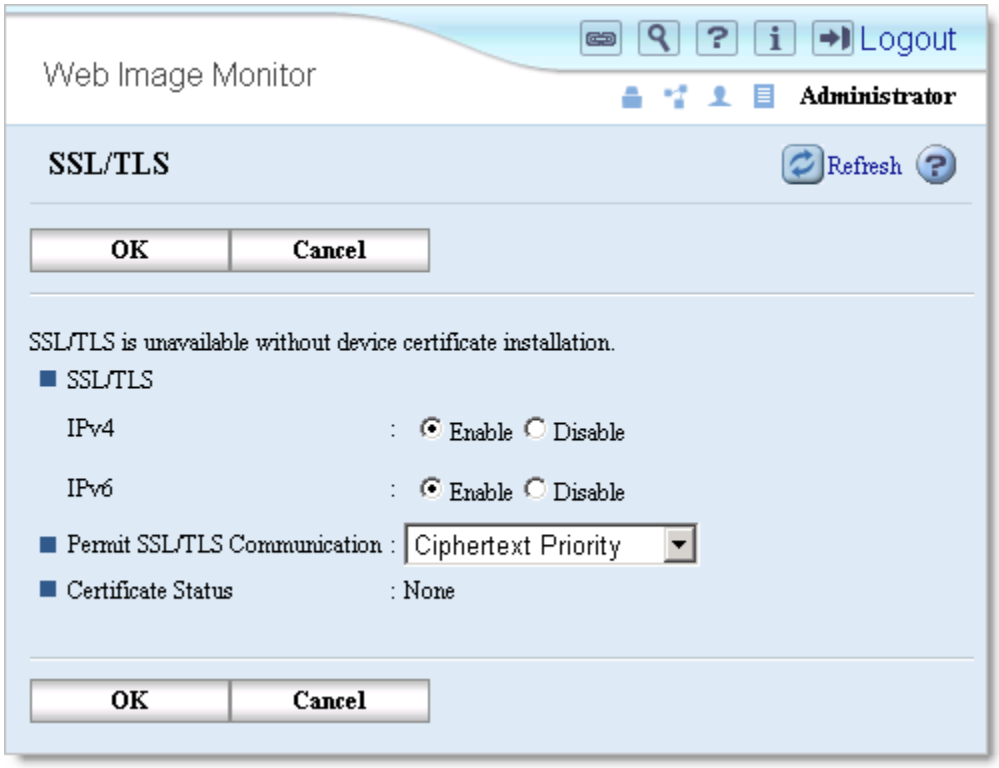


Figure C.2: SSL/TLS Settings

3. Enable SSL/TLS Communication for IPv4 and IPv6 (Figure C.2).
4. From the Permit SSL/TLS Communication drop-down box, select the desired Ciphertext option.

Settings Overview:

- **Ciphertext/Clear Text:** Permit both HTTPS and HTTP connections. No forwarding of HTTP to HTTPS.
- **Ciphertext Priority:** Forwards incoming HTTP requests to HTTPS, if possible. This setting allows HTTPS use in Internet Explorer, Netscape Navigator, etc. (HTTP will be forwarded). However, it is still not possible to use IPP from SmartDeviceMonitor for Client etc. (these requests cannot be forwarded). HTTP is permitted if it is not possible to forward the request to HTTPS.
- **Ciphertext Only:** Only permits HTTPS connections. Forwards all incoming HTTP request to HTTPS. It will reject the connection for any request it cannot forward.

C.6 SNMP v1/v2 Settings

Refer to section 4.1: Web Image Monitor Access Control (page 25) for the Administrator login procedure. Below is an overview of the available SNMP v1/v2 settings.

1. To access the SNMP v1/v2 settings, click **Configuration → Network → SNMP**.

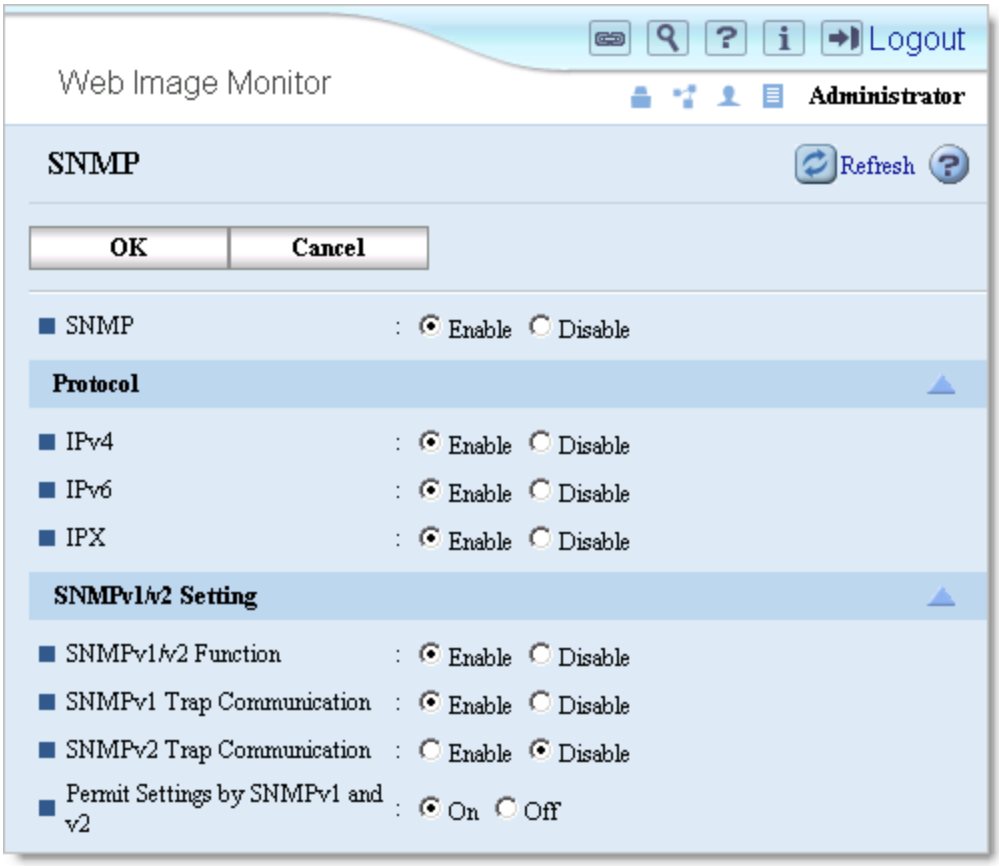


Figure C.3: SNMP Settings

Settings Overview:

SNMP: (This can also be enabled/disabled from SNMPv3 settings).

- Enable: Opens the SNMP port
- Disable: Closes the port completely. No version of SNMP communication can be used.

SNMP v1/v2 Function:

- Enable: Allows the use of SNMP v1/v2.
- Disable: Does not allow connections via SNMP v1/v2. Since SNMP v1/v2 does not have encryption or authorization, it is best to use 'Disable' for this setting unless necessary.

Permit Settings by SNMP v1 and v2:

- On: This enables SNMP set. It is used to write changes to settings.
- Off: Disables SNMP set. Settings can be read but not changed.

C.7 SNMP v3 Settings

Refer to section 4.1: Web Image Monitor Access Control (page 25) for the Administrator login procedure. Below is an overview of the available SNMP v3 settings.

1. To access the SNMP v3 settings, click **Configuration → Network → SNMP v3**.

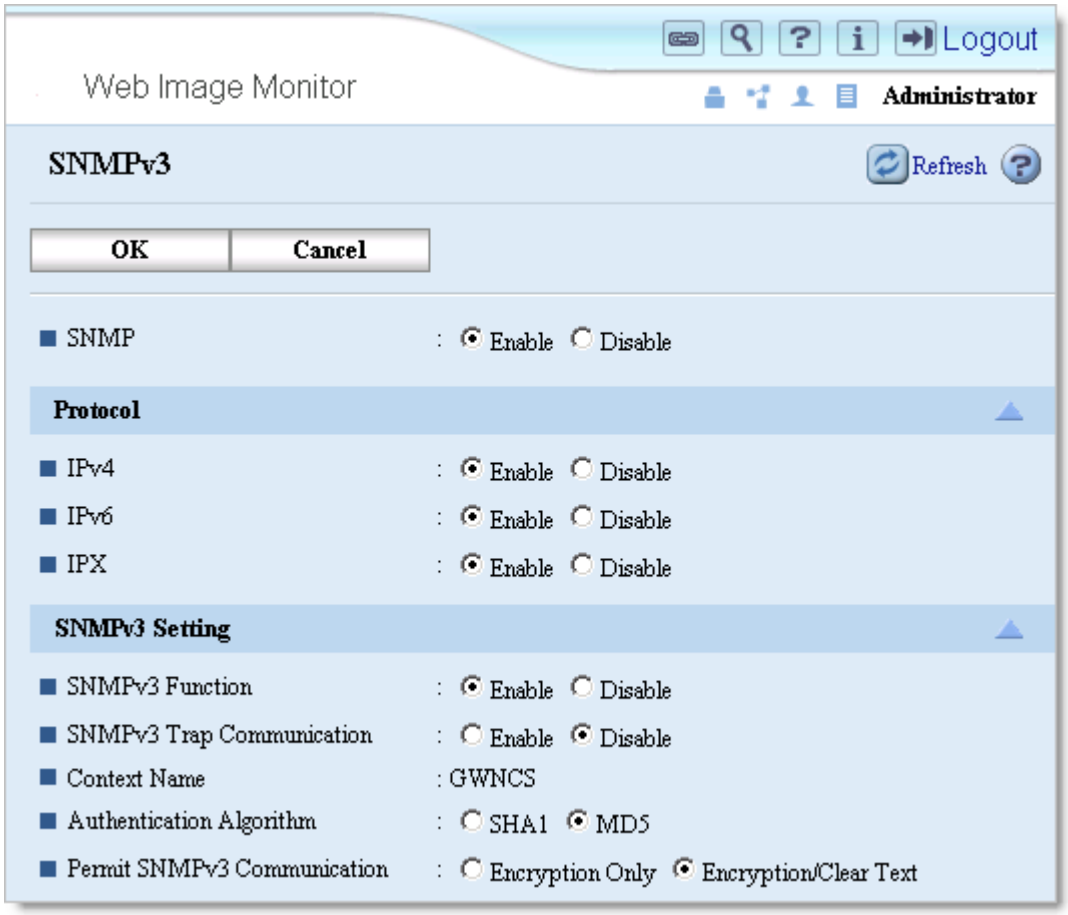


Figure C.4: SNMP v3 Settings

Settings Overview:

SNMP: (This can also be enabled/disabled from SNMPv1/v2 settings.)

- Enable: Opens the SNMP port
- Disable: Closes the port completely. No version of SNMP communication 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: Must encrypt the username and password using the hashing algorithm selected above.
- Encryption/Clear Text: Send encrypted or unencrypted username and password.

C.7.1 SNMP v3 Account Settings

There are 3 different account types for SNMPv3 connections. Only the User account can be fully configured in Web Image Monitor. For information about fully configuring the Machine and Network Administrator accounts, please refer to Section C.9 (page 49).

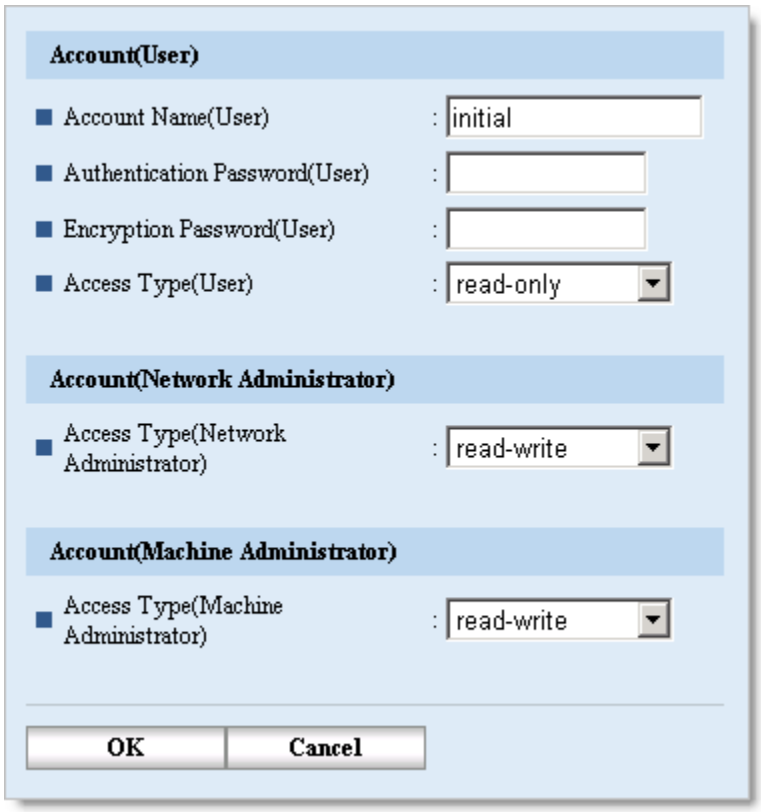


Figure C.5: SNMP v3 Account Types

Settings Overview:

Account Name (User): Username for SNMP v3 login.
Authentication Password (User): Password used for SNMPv3 login.
Encryption Password (User): Key used for SHA1 or MD5 hashing of the username and password.

C.8 SNMP Settings in MSHELL

Refer to section 4.2: MSHELL (page 24) for the Administrator login procedure. Below is the process for configuring the SNMP settings in MSHELL.

Configure the SNMP settings in MSHELL using SNMP commands. Display the commands by typing **help snmp** in MSHELL (Figure C.6).

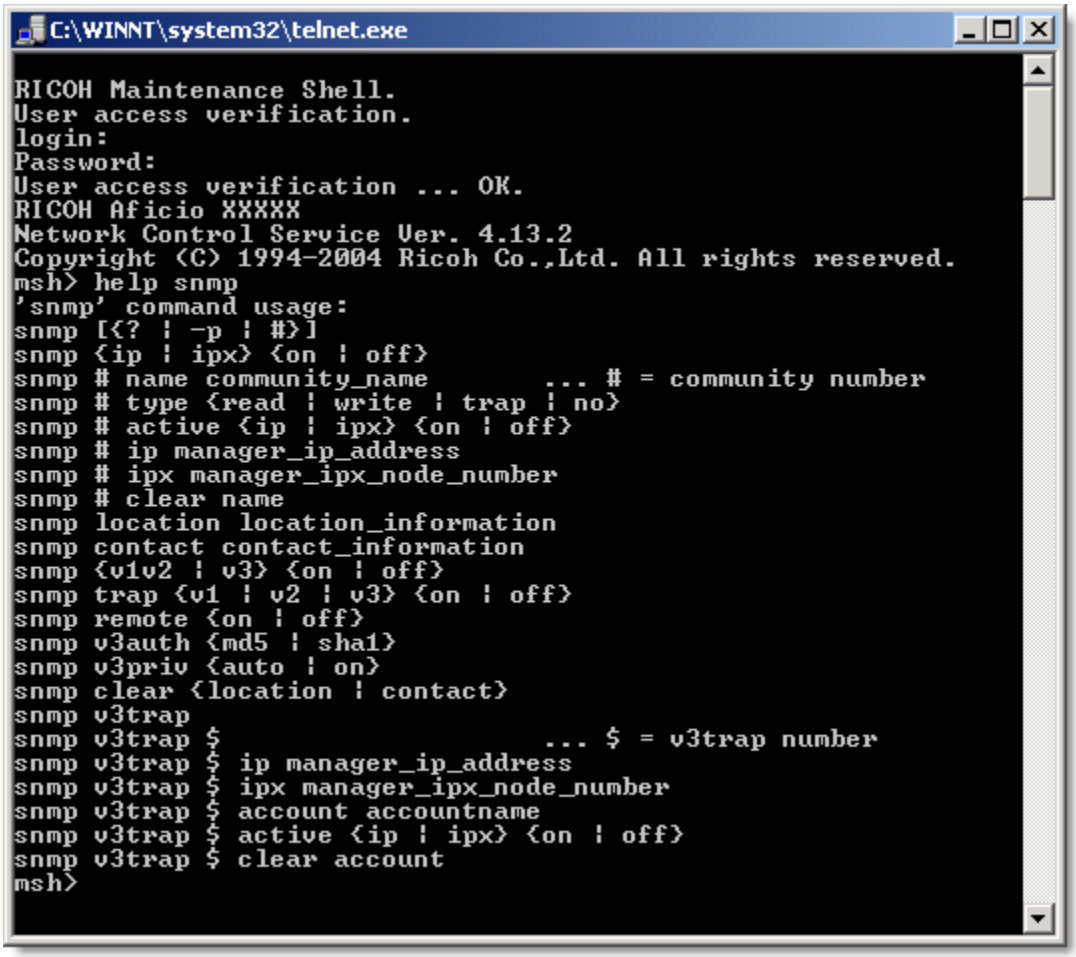


Figure C.6: SNMP Commands

EXAMPLE

To turn off SNMP v3 off, type **snmp v3 off**, and press enter.

C.9 Changing Administrator Settings in Web Image Monitor

Refer to section 4.1: Web Image Monitor Access Control (page 25) for the Administrator login procedure. The following is the procedure for modifying the Administrator settings.

1. To access administrator settings click **Configuration → Device Settings → Program/Change Administrator**.

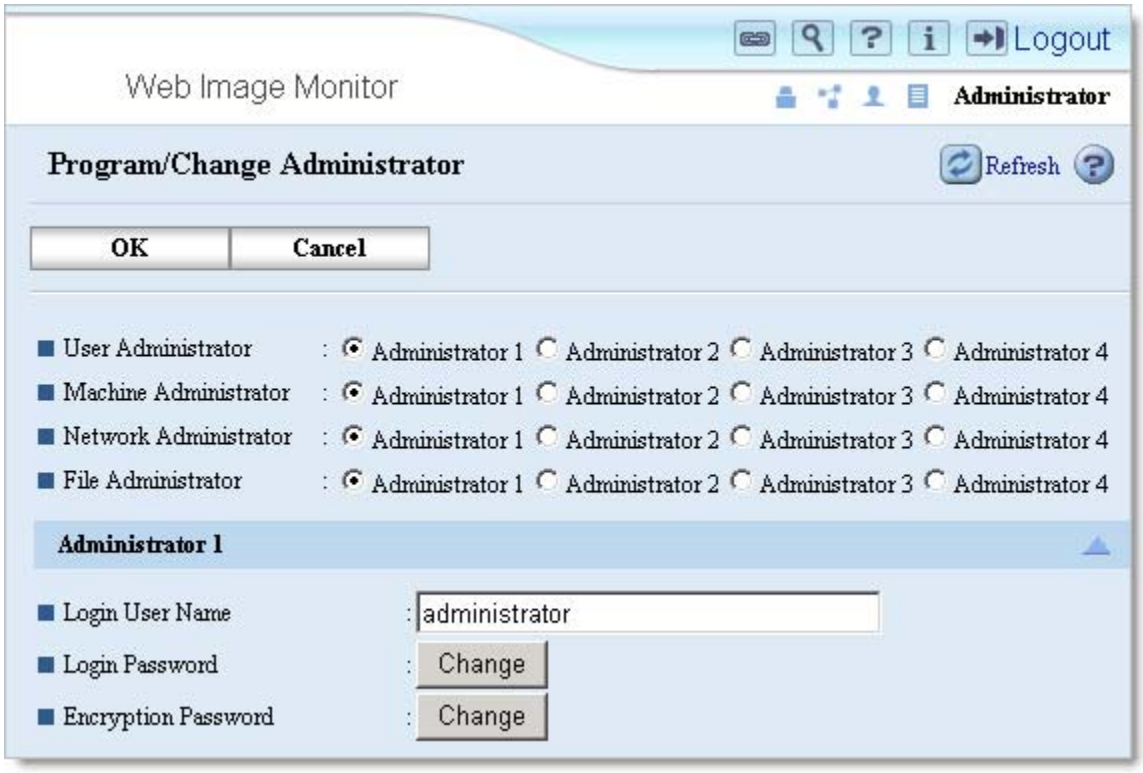


Figure C.7: Administrator Settings

It is possible to change MFP Administrator account settings from this screen.

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

Appendix D

The material in Appendix D only applies to the models listed in the Cross Reference table below.

Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
B205	Aficio 3025/SP/SPF/SPi/P	8025/sp/ spf/spi/P	DSm725/sp/ spf/spi/p	LD225/SP
B209	Aficio 3030/SP/SPF/SPi/P	8030/sp/ spf/spi/P	DSm730/sp/ spf/spi/p	LD230
B222	MP C3500	C3535	DSc535	LD435c
B224	MP C4500	C4540	DSc545	LD445c
B229	Aficio 615c	SGC 1506	GS 106	LD215c
B230	Aficio MP C2500	C2525	DSc525	LD425c
B234	Aficio MP 9000	8090	DSm790	LD190
B235	Aficio MP 1100	8110	DSm7110	LD1110
B236	Aficio MP 1350	8135	DSm7135	LD1135
B237	Aficio MP C3000	C3030	DSc530	LD430c
B245	Aficio MP 1500	-	DSm715	LD315
B246	Aficio MP 5500	8055	DSm755	LD255
B248	Aficio MP 6500	8065	DSm765	LD265
B249	Aficio MP 7500	8075	DSm775	LD275
B250	Aficio MP 5500 SP	8055 SP	DSm755 SP	LD255 SP
B252	Aficio MP 6500 SP	8065 SP	DSm765 SP	LD265 SP
B253	Aficio MP 7500 SP	8075 SP	DSm775 SP	LD275 SP
B264	Aficio 3035/SP/SPF/Spi/G	8035/sp/ spf/spi/34g	DSm735/sp/ spf/spi/G	LD235
B265	Aficio 3045/SP/SPF/Spi/G	8045/sp/ spf/spi/g	DSm745/sp/ spf/spi/G	LD245
B276	Aficio MP 1600	9016	DSm716	LD316
B277	Aficio MP 2000	9021d	DSm721d	LD320
B284	Aficio MP 161F	816f	DSm416f	LD016f
B288	Aficio MP 161SPF	816mf	DSm416pf	LD016SPF
B291	Aficio MP 3500G	8035eg	DSm735eg	-
B292	Aficio MP 161	816	DSm416	LD016
B295	Aficio 4500G	8045eg	DSm745eg	-
B296	Aficio MP 3500	8035e	DSm735e	LD335
B297	Aficio MP 4500	8045e	DSm 745e	LD345
D007	Aficio MP 2510	8025e	DSm725e	LD325
D008	Aficio MP 3010	8030e	DSm730e	LD330
G130	Aficio CL7200	CLP128	C7528n	LP332c
G131	Aficio CL7300	CLP135	C7535n	LP335c
G176	Aficio SP 4100N	MLP31n	P7031n	LP131n
G177	Aficio SP 4110N	MLP36n	P7035n	LP136n

D.1 H.323/SIP

D.1.1 Function Overview

H.323/SIP are protocols used for multimedia conferencing, including voice, video, and data conferencing. 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.

D.1.2 Potential threats

Possibility of successful DoS (Denial of Service) attacks: Unlikely. H323hostcall/SIP can only maintain a single session. In addition, a session will timeout if a recognizable response is not sent within a specified period. This makes service disruption via DoS attacks unlikely.

Theft of username and password: None. The SIP protocol supports the authentication function. However, the products do not support authentication using the SIP protocol, so they are not included with data sent over this protocol.

Theft of facsimile data: Possible. 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.

D.1.3 Recommended precautions

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

D.2 Additional Services Provided with open TCP/UDP Ports

Protocol	Port Num.	Login	Default Username	Username Changeable	Password	Password Changeable	Note
H.323 gatestat	1719/UDP	N/A	N/A	N/A	N/A	N/A	If configured to use 'gatekeeper', this port is opened so the product can register its information with gatekeeper.
H.323	1720/TCP	N/A	N/A	N/A	N/A	N/A	
SIP	5060/TCP, UDP	N/A	N/A	N/A	N/A	N/A	The SIP protocol supports authentication, but our products do not.

D.3 Network Security Level settings

D.3.1 Overview

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. Three security levels, plus one custom level, are available for customers to use as is, or modify to suit their needs.

- **Level 0** – Low/Open. All ports open and settings enabled.
- **Level 1** – Medium. SNMP v1/v2 (write) Disabled, and Port 23 Closed. All other settings enabled and ports open.
- **Level 2** – High. See chart on page 40 for details.
- **User Settings** – Manually defined settings (Default setting).

D.3.2 Network Security Level Configuration

Refer to section 4.1: Web Image Monitor Access Control (page 25) for the Administrator login procedure.

1. To access the Network Security Level settings, click: **Configuration → Security → Network Security**.
2. Make any desired changes to the security levels from the drop-down box.

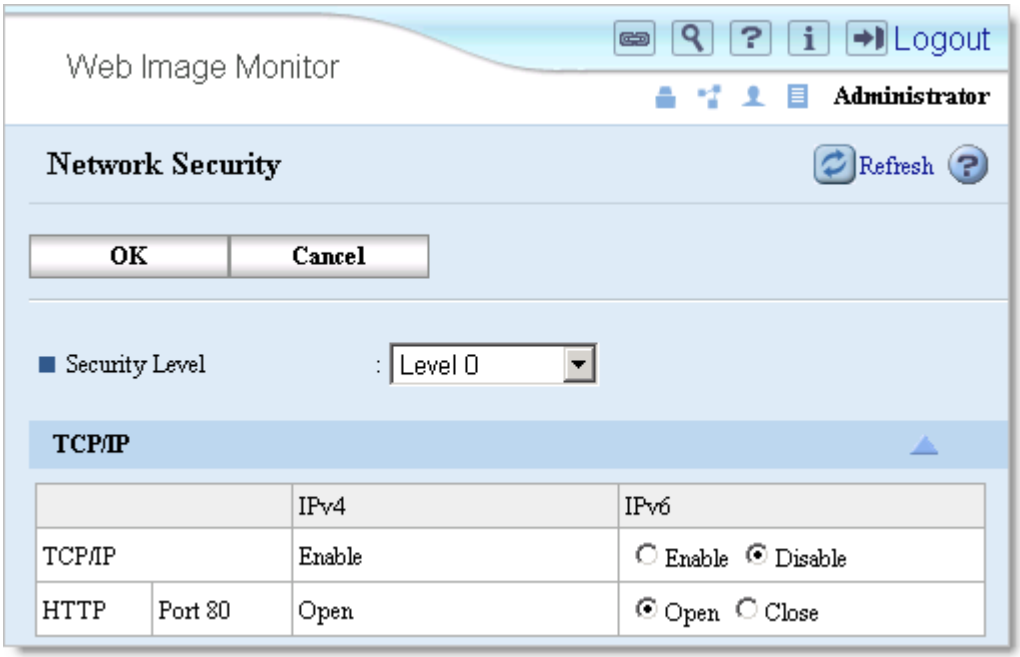


Figure D.1: Security Levels

D.3.3 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
	Ricoh Original	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 accept IPP jobs using port 80.

Appendix E

The material in Appendix E only applies to the models listed in the Cross Reference table below.

Product Code	Ricoh Corp Model Name	Savin (USA) Model Name	Gestetner Model Name	Lanier Model Name
B222	MP C3500	C3535	DSc535	LD435c
B224	MP C4500	C4540	DSc545	LD445c
B229	Aficio 615c	SGC 1506	GS 106	LD215c
B230	Aficio MP C2500	C2525	DSc525	LD425c
B234	Aficio MP 9000	8090	DSm790	LD190
B235	Aficio MP 1100	8110	DSm7110	LD1110
B236	Aficio MP 1350	8135	DSm7135	LD1135
B237	Aficio MP C3000	C3030	DSc530	LD430c
B245	Aficio MP 1500	-	DSm715	LD315
B246	Aficio MP 5500	8055	DSm755	LD255
B248	Aficio MP 6500	8065	DSm765	LD265
B249	Aficio MP 7500	8075	DSm775	LD275
B250	Aficio MP 5500 SP	8055 SP	DSm755 SP	LD255 SP
B252	Aficio MP 6500 SP	8065 SP	DSm765 SP	LD265 SP
B253	Aficio MP 7500 SP	8075 SP	DSm775 SP	LD275 SP
B276	Aficio MP 1600	9016	DSm716	LD316
B277	Aficio MP 2000	9021d	DSm721d	LD320
B284	Aficio MP 161F	816f	DSm416f	LD016f
B288	Aficio MP 161SPF	816mf	DSm416pf	LD016SPF
B292	Aficio MP 161	816	DSm416	LD016
G176	Aficio SP 4100N	MLP31n	P7031n	LP131n
G177	Aficio SP 4110N	MLP36n	P7035n	LP136n

E.1 SSDP

E.1.1 Function Overview

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

E.1.2 Potential threats and recommended precautions

Unauthorized parties intercepting device information: The products use SSDP to advertise and search for services. To prevent unauthorized parties from intercepting this information, disable SSDP via Web Image Monitor or the MSHELL. Please see Section 5.1 (page 33) and 5.2 (page 34) for information on how to disable services.

E.1.3 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. Please see Section 5.1 (page 33) and 5.2 (page 34) for information on how to disable services.

E.2 SFTP (SSH)

E.2.1 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 Data Encryption, which protects against interception/falsification of data.

SSH (Secure Shell) is a program used to log into another computer over a network, execute commands in a remote machine, and/or 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.

E.2.2 Potential threats

Destruction, corruption and modification of the file system or kernel:
Not possible. Although the SFTP service permits write-access, any files that are received by the printer are considered 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.

Possibility of acting as a server for relaying viruses:
None. 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.

Theft of username, password, and device information:
Using SFTP, all data including the username and password is encrypted using DES, 3DES or AES.

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

E.2.3 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 for the MSHELL login.

Level 2: Close the SSH port.
- SFTP uses TCP port 22, which can be closed via MSHELL or Web Image Monitor. If closed, both printing and firmware updates are unavailable via SFTP.

E.3 Wireless LAN

E.3.1 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 while maintaining a network connection. Since the absence of cables leaves transmissions extremely susceptible to interception, there is a variety of security precautions incorporated into WLAN specifications.

E.3.2 Wireless Protocols/Communication Methods

SSID (Service Set IDentifier) 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 (Wired Equivalent Privacy)
WEP 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 (WiFi Protected Access)
WPA 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 Refresh	

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, since an encryption key is generated in handshake process, WPA-PSK/WPA2-PSK is more secure than WEP. WPA (802.1X)/ WPA2 (802.1X) is even stricter. Only users that can be authenticated by a RADIUS server using EAP (Extensible Authentication Protocol) can join the network.

The supported EAP authentication types are:

- EAP-TLS – EAP Transport Layer Security
- EAP-TTLS – EAP Tunneled Transport Layer Security
- PEAP – Protected EAP
- LEAP – Lightweight EAP

E.3.2 Potential Threats

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.

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, but the constant key refresh will change the key before an attacker has time to crack it.

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.

E.3.3 Recommended Precaution

To guard against the potential threats in section E.3.2, choose from one of the four security levels below (Level 1 is the least secure). Please take the appropriate action for your security policy.

***Please refer to E.6 (page 61) for Security Level configuration instructions.**

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.

RECOMMENDATION: Since SSID is used only for connection identification, and not network security, we recommend using Security Level 2.

Level 2: WEP
- To further enhance security, change the WEP on a regular basis.

Level 3: WPA-PSK/WPA2-PSK

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

E.4 SSH/SFTP Network Security Settings

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. Three security levels, plus one custom level, are available for customers to use as is, or modify to suit their needs.

*** For more information on the Network Security levels, see Appendix D - Page 51**

	Setting		Network Security Level		
TCP/IP	SSH/SFTP	Port 22	Level 0	Level 1	Level 2
			Port open	Port open	Port open

E.5 Additional Services Provided with open TCP/UDP Ports

Protocol	Port Number	Login	Username Changeable	Password	Password Changeable	Note
SNMPv3	161/UDP	Yes	Yes	Yes	Yes	Same username/password as TELNET. If no password is input, then only read access is available.
SSH	22/TCP	Yes	Yes	Yes	Yes	• Used only for SFTP. • For RFU, administrator privilege is required. • For SFTP, RFU is not available via Web Smart Device Monitor.
@Remote	7443/TCP 7444/TCP	-	-	-	-	
SSDP	1900/UDP	N/A	N/A	N/A	N/A	
RFU	10021/TCP	Yes	-	-	-	This port functions similarly to an FTP port and used for Web Smart Device Monitor.

E.6 Services that can be Disabled

- **RFU:** Port 21/10020/10021 must be open in order to use RFU via Web Smart Device Monitor. Each port can be closed via MSHELL.
- **SSDP:** Setting SSDP to down makes UPnP unavailable and closes the SSDP port (1900/UDP)
- **SSH/SFTP:** Settings SFTP to down makes SFTP is unavailable and closes the SFTP port (22/TCP)

E.7 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.

E.7.1 Wireless LAN settings – Web Image Monitor

Refer to section 4.1: Web Image Monitor Access Control (page 25) for the Administrator login procedure. Below is an overview of the available Wireless LAN settings.

1. To access administrator settings click Configuration in the left-hand toolbar.
2. Under the Interface heading, click Wireless LAN Settings.

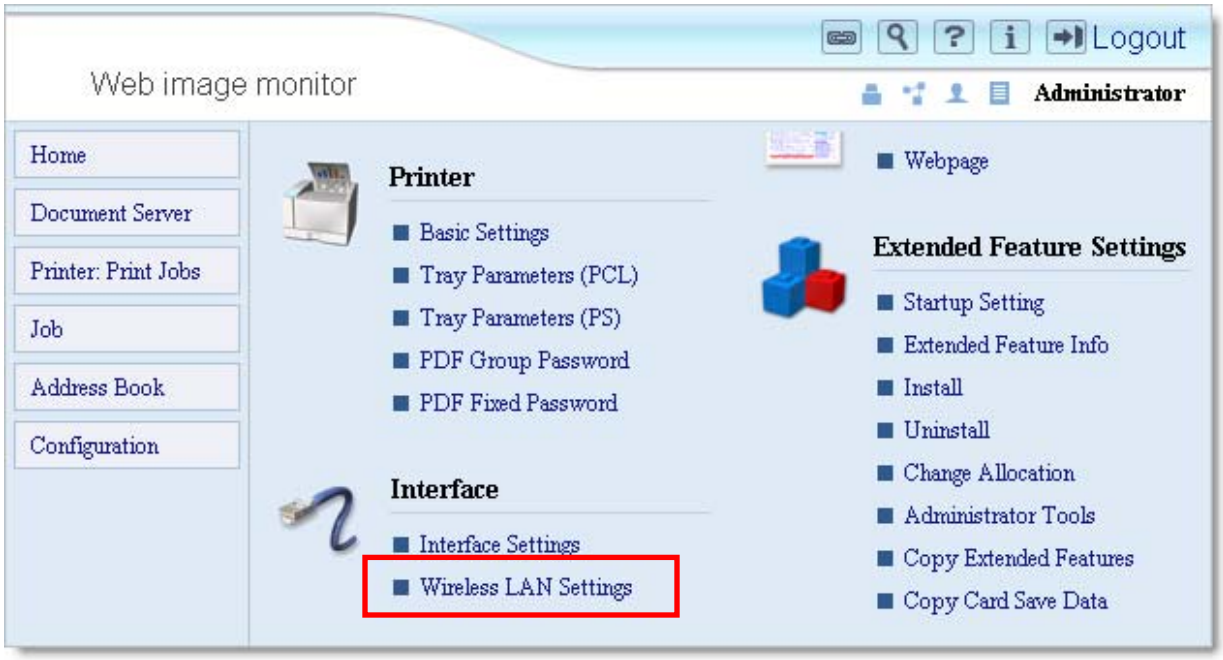


Figure E.1: Web Image Monitor Configuration Page

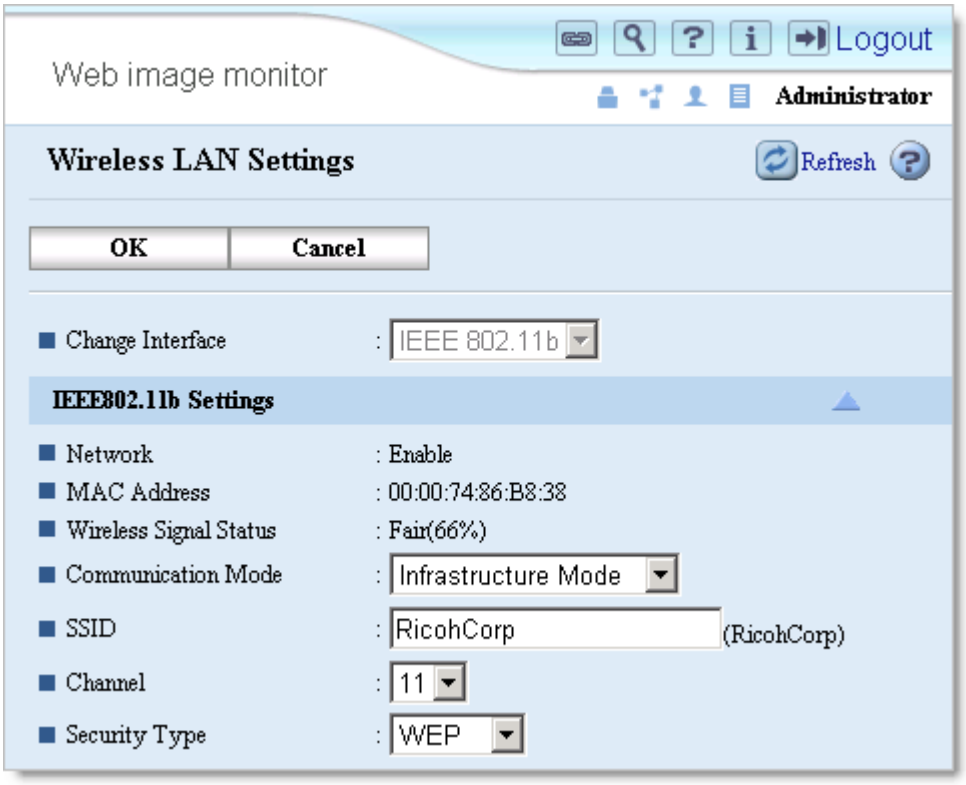


Figure E.2: Wireless LAN Settings

Below is a breakdown of the options available from the Wireless LAN Settings page.

Change Interface

- Ethernet: Enable Ethernet
- IEEE802.11b: Enable IEEE802.11b

E.7.2 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

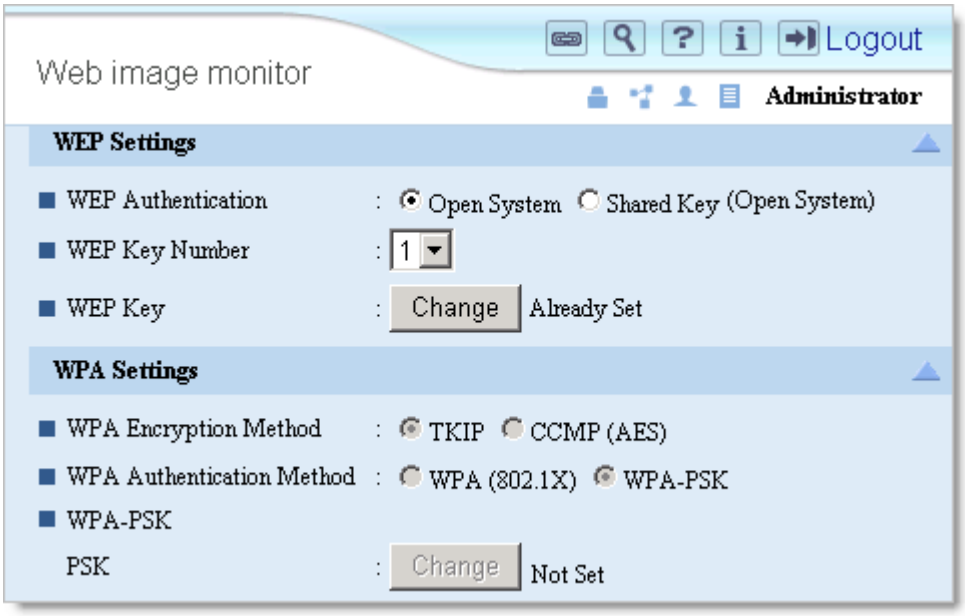


Figure E.3: WEP Settings

E.7.3 WEP Settings

WEP settings can only be configured if "WEP" is selected as the Security Type in the IEEE802.11b Settings (see Figure E.2).

WEP Authentication

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

> **NOTE**
> Since the system uses a WEP key, simply joining the network is not enough to be able to receive 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.

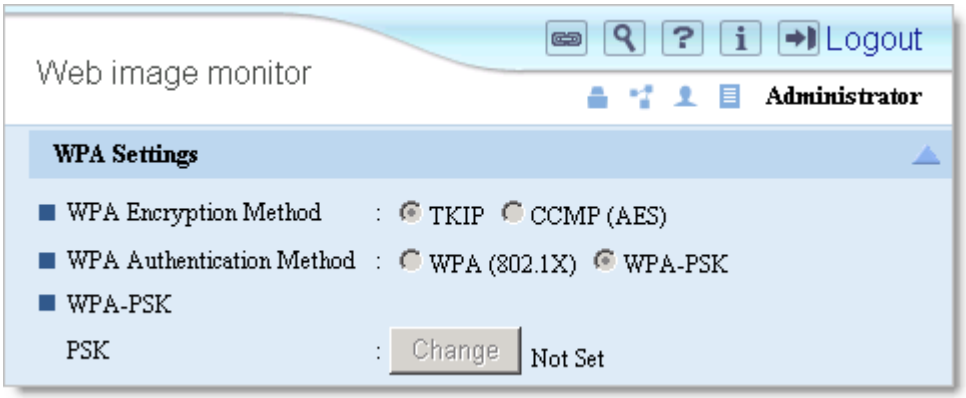


Figure E.4: WPA Settings

E.7.4 WPA Settings

WPA settings can only be configured if "WPA" is selected as the Security Type in the IEEE802.11b Settings (See Figure E.2).

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.

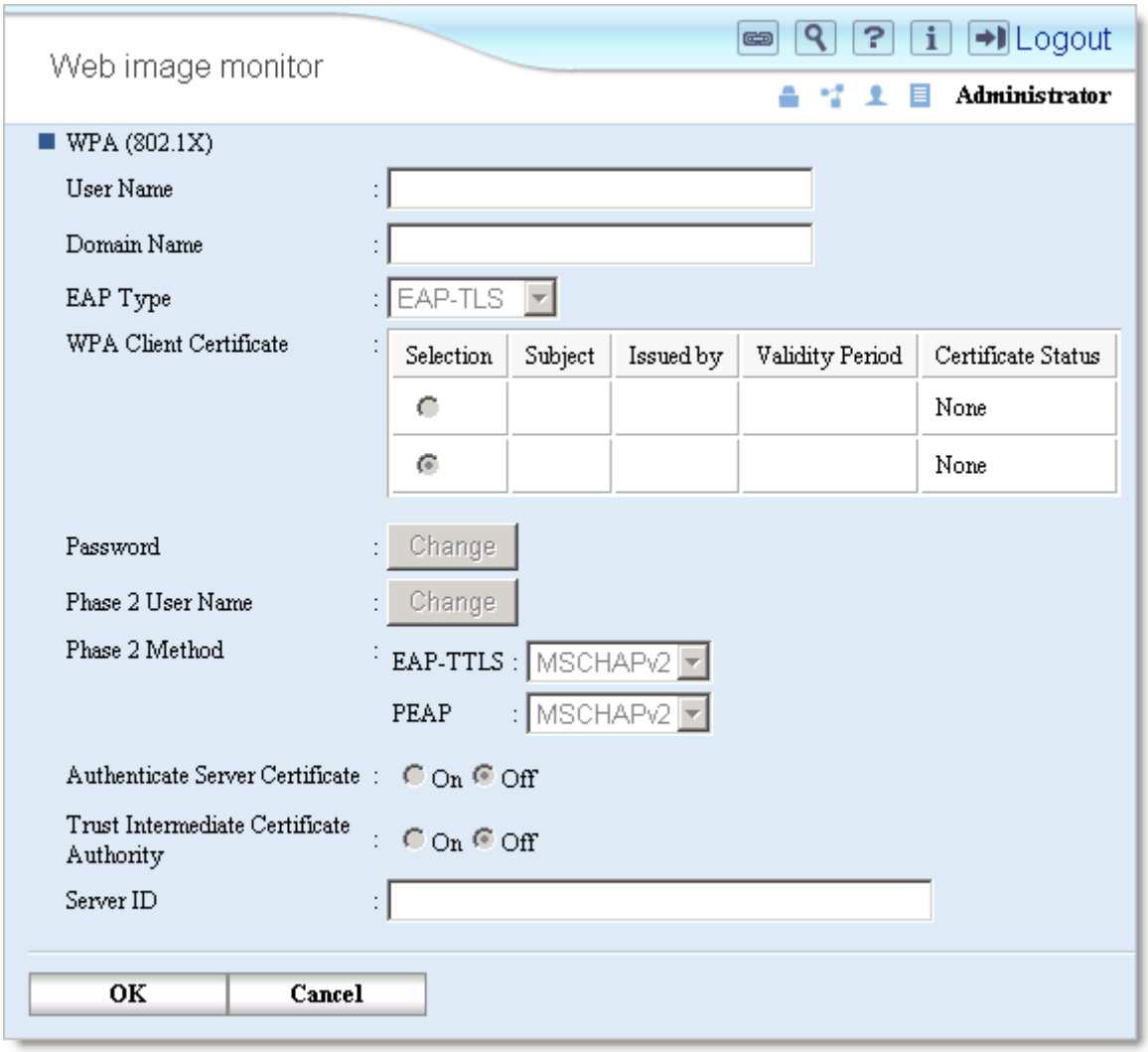


Figure E.5: WPA (802.1X) Settings

E.7.5 WPA/WPA2

User Name: This is the username used for EAP (Extensible Authentication Protocol) 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
- 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
- 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: Determines whether or not a trusted CA (certificate authority) must sign the Radius Server certificate.

Server ID: This is the CN (Common Name), or DC (Domain Controller) of the server certificate.

Permit Sub-domain: Select whether the server certificate is permitted for the sub-domain of server ID.

E.7.6 Wireless LAN settings – MSHELL

Refer to steps 1-4 of Section 4.2 for the MSHELL (page 29) login procedure. The following steps detail the process for disabling services.

1. Enter the phrase **help wiconfig** for a list of the MSHELL commands (see Figure E.6).
2. Configure Wireless LAN settings using 'wiconfig' commands from MSHELL.

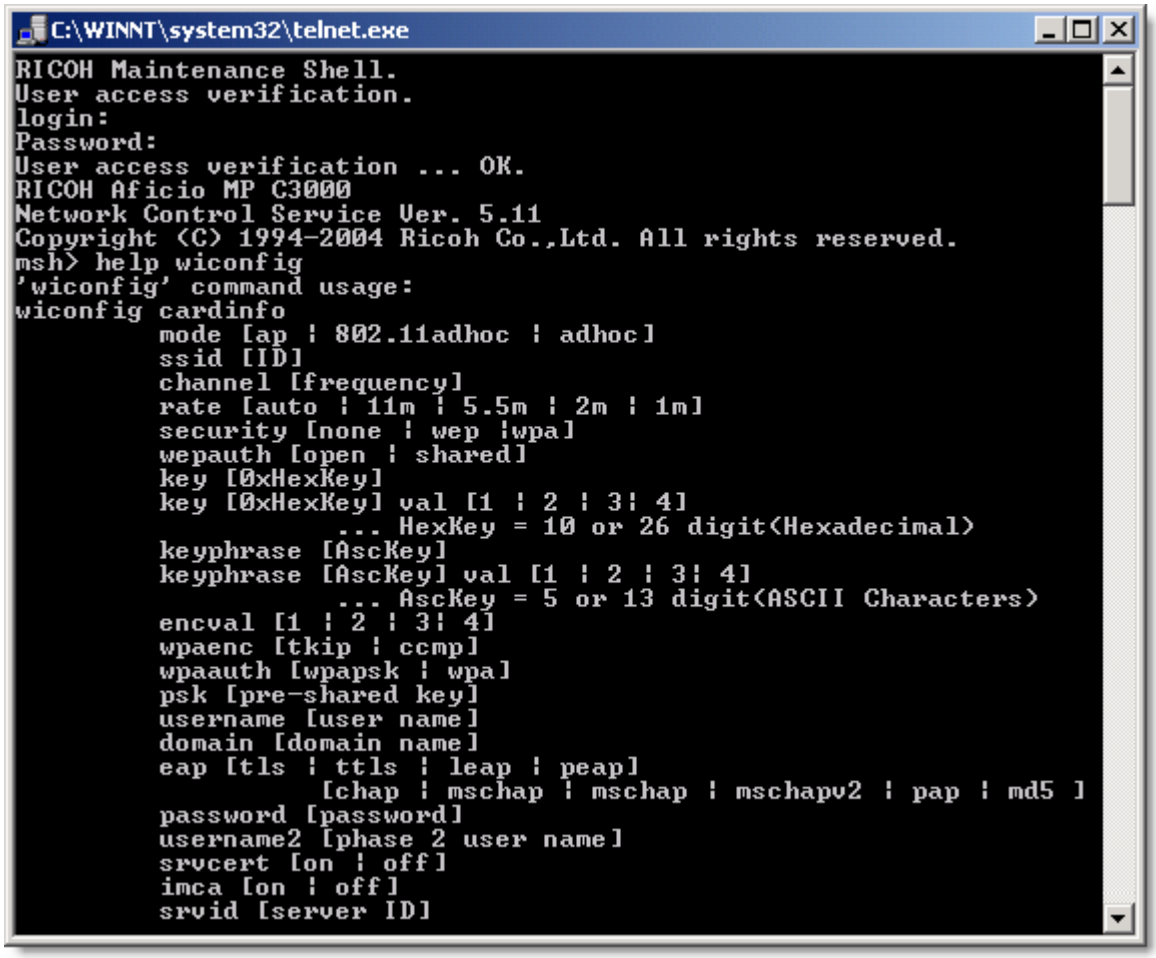


Figure E.6: MSHELL LAN Settings