OKI
PRINTING SOLUTIONS

Security Guide

COLOR/MONO

SECURITY

INFORMATION

PREFACE

Every effort has been made to ensure that the information in this document is complete, accurate, and up-to-date. The manufacturer assumes no responsibility for the results of errors beyond its control. The manufacturer also cannot guarantee that changes in software and equipment made by other manufacturers and referred to in this guide will not affect the applicability of the information in it. Mention of software products manufactured by other companies does not necessarily constitute endorsement by the manufacturer.

While all reasonable efforts have been made to make this document as accurate and helpful as possible, we make no warranty of any kind, expressed or implied, as to the accuracy or completeness of the information contained herein.

CONTENTS

NOTES, CAUTIONS AND WARNINGS

NOTE
A note provides additional information to supplement the main text.

CAUTION!

A caution provides additional information which, if ignored, may result in equipment malfunction or damage.

WARNING!

A warning provides additional information which, if ignored, may result in a risk of personal injury.

Specifications subject to change without notice. All trademarks acknowledged.

DOCUMENT SECURITY

Document security can be breached in many ways. Some are obvious and can be remedied quite easily;

> Unattended documents left in a printer's output tray. Even one connected "one-to-one" with a computer.

> Worse still, unattended documents left in a networked printer's output tray, for all to see!

> Personnel possessing confidential documents off-site.

Other security risks may not be so obvious.

As printers and multi-function products become more sophisticated so must the security measures to ensure your valuable data is kept secure.

If left unprotected, access to records can be achieved via a networked machine. On-board storage devices may contain confidential data such as PIN numbers, personnel names and IP addresses as well as raw text.

Your machine has a number of valuable features which, when enabled, reduce the risk of security breaches.

The following chapters guide you through the initial set up and also explain how you use the secure printing features.

GLOSSARY

|	
IP	**Internet Protocol**
MAC Address	**Media Access Control Address**
PIN	**Personal Identification Number**
SSL	**Secure Sockets Layer**
TLS	**Transport Layer Security**
Storage device	**Hard disk drive (HDD) or SD card**

SETTING THE SECURITY

Although, in most cases, it is possible to program your machine via the operator panel, the most effective way is via the web page.

> NOTE
> *Example screenshots are used throughout this manual and as such may not represent the screens displayed for your machine. Some of the features shown on the example screenshots may not be available on your machine.*

ACCESSING THE WEB PAGE

Type the IP address of the machine in the URL field of your browser and then press **Enter**. The machine web page appears. For example: ***http://10.18.207.15***
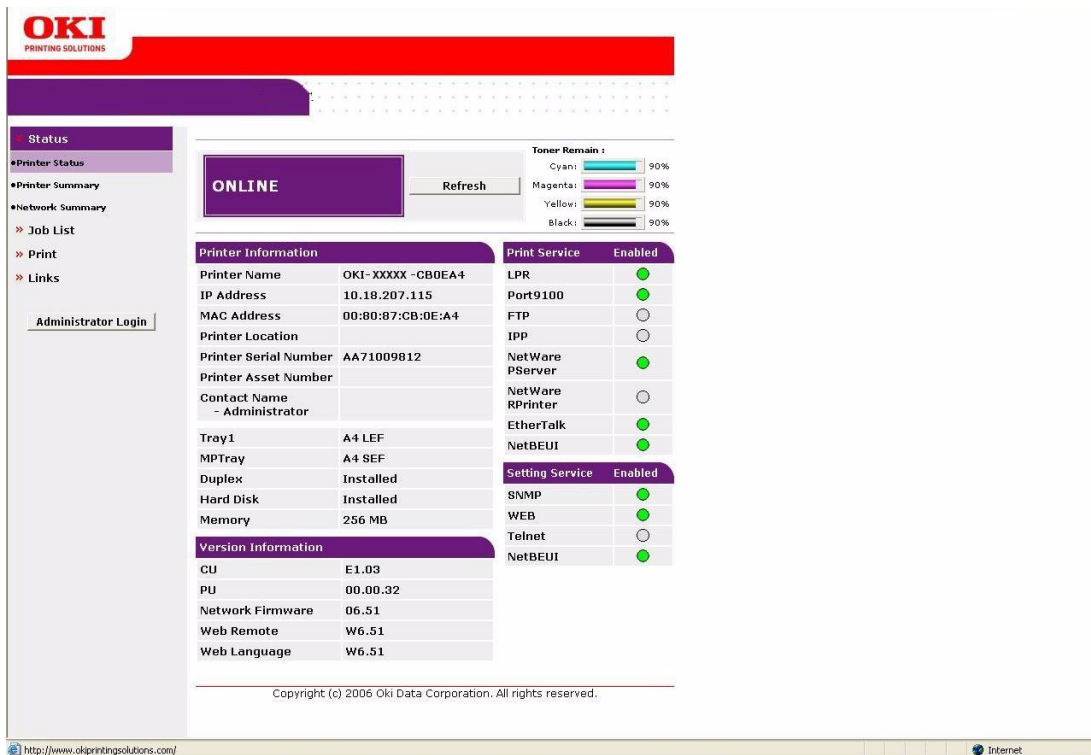
ADJUSTING THE SECURITY SETTINGS

You must log on as the administrator to adjust the security settings.

> *NOTE*
> *The Administrative Settings are blocked by a password. Refer to your user documentation for the factory default settings.*
>
> *It is recommended that the system administrator creates a new password, refer to "Password configuration" on page 15.*

1. Click **Administrator Login.**

2. Enter the correct user name and password.

3. Click **Login**.

   The initial administration entry screen is displayed.

4. Click **Skip** to navigate to the main menu page.
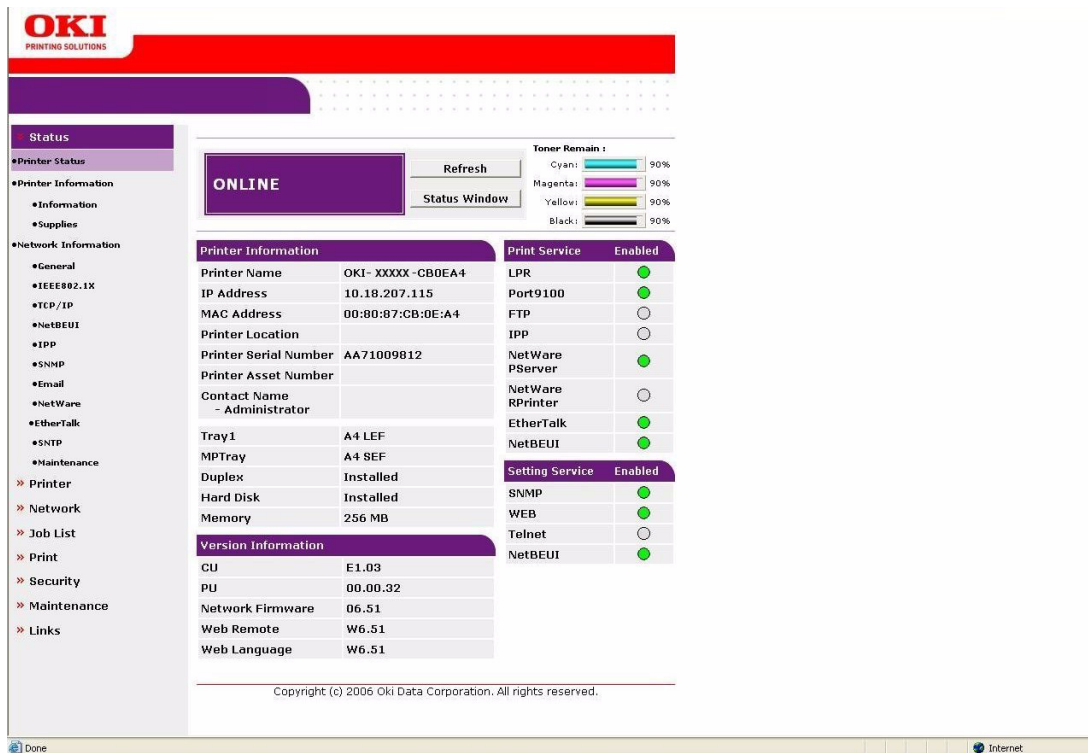
5. From the left hand menu select **Security**.
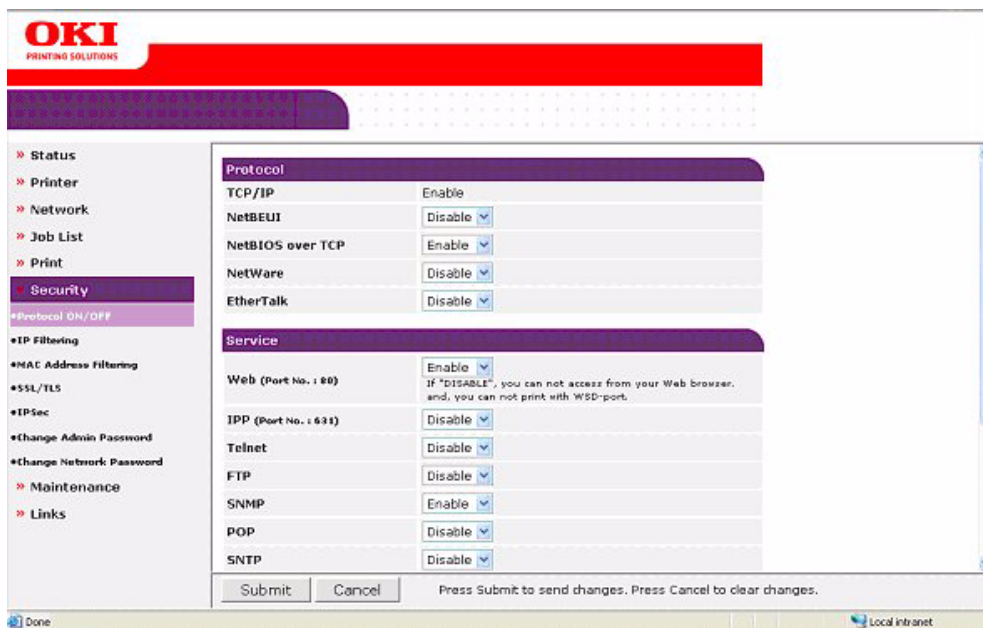
Refer to the following chapters for instructions on how to set your security preferences.

NOTE
High level instructions are given, for more details refer to the information on screen.

PROTOCOL ON/OFF

To set up the security protocol:

1. From the left hand panel select **Protocol ON/OFF**.
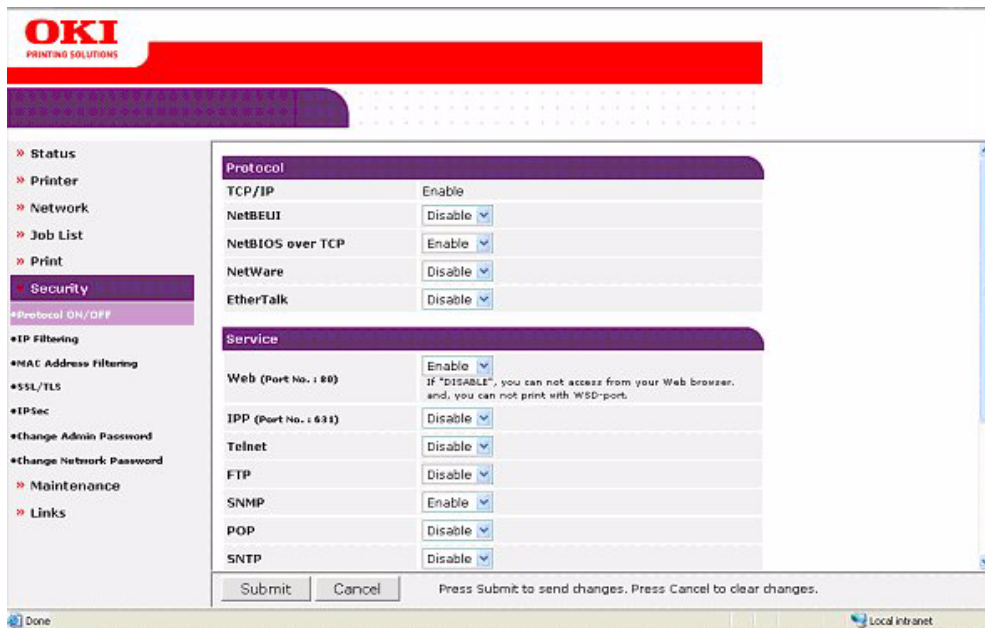

2. From the drop down menus select **ENABLE** / **DISABLE** as appropriate.

3. Input the port numbers as appropriate.

4. Click **Submit** to save the changes or **Cancel** to exit.

PANEL LOCKOUT

To activate the lockout facility on the printer control panel:

1. From the left hand panel select **Panel Lockout**.
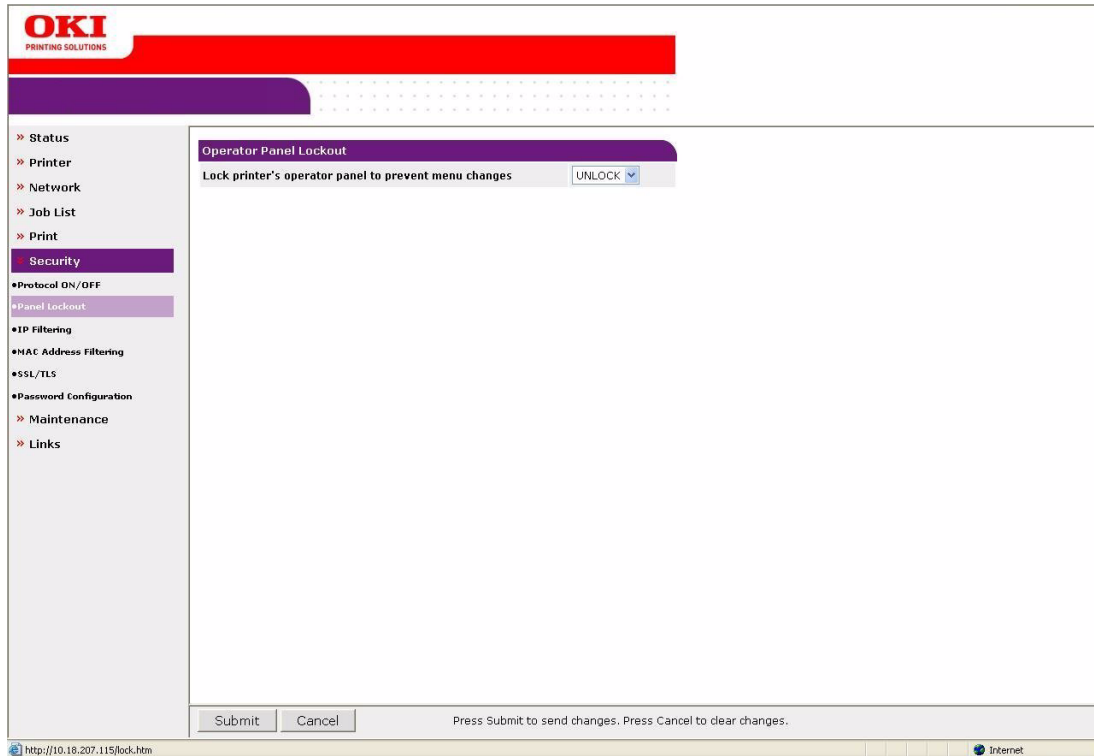
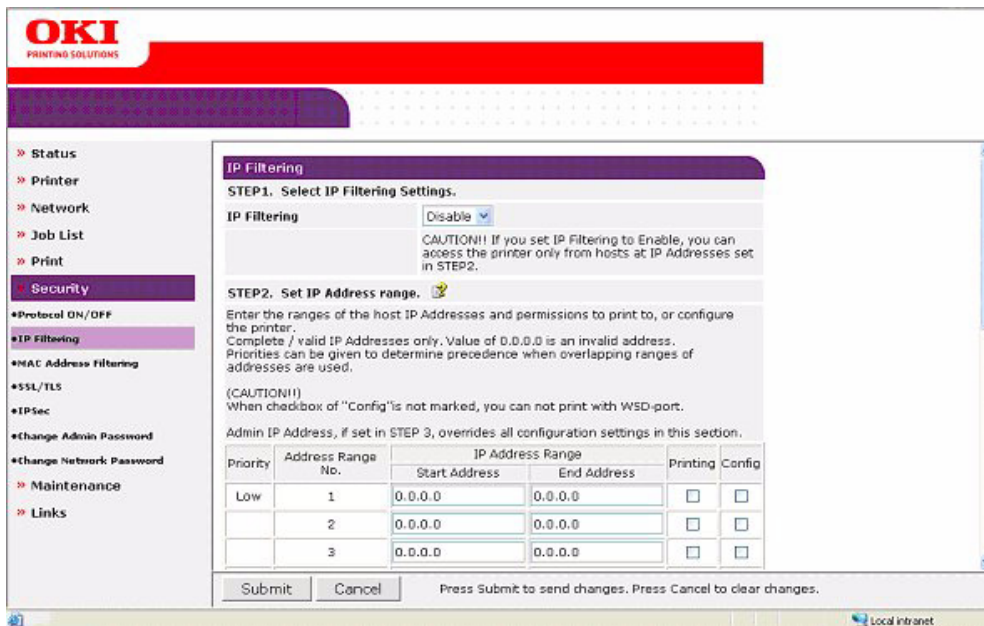2. From the drop down menu select **LOCK**.
3. Click **Submit** to save the changes or **Cancel** to exit.

IP FILTERING

To enable IP filtering:

1. From the left hand panel select **IP Filtering.**

2. From the drop down menu select **ENABLE**.

3. Input the range of host IP addresses and set permissions in the main table.

4. Click **Submit** to save the changes or **Cancel** to exit.

MAC ADDRESS FILTERING

To enable MAC address filtering:

1. From the left hand panel select **MAC Address Filtering**.

2. From the drop down menu select **ENABLE**.

3. From the second drop down menu select **ACCEPT**.

4. Input the MAC addresses in the main table.

5. Click **Submit** to save the changes or **Cancel** to exit.

SSL/TLS

To enable SSL/TLS encryption:

1. From the left hand panel select **SSL/TLS**.
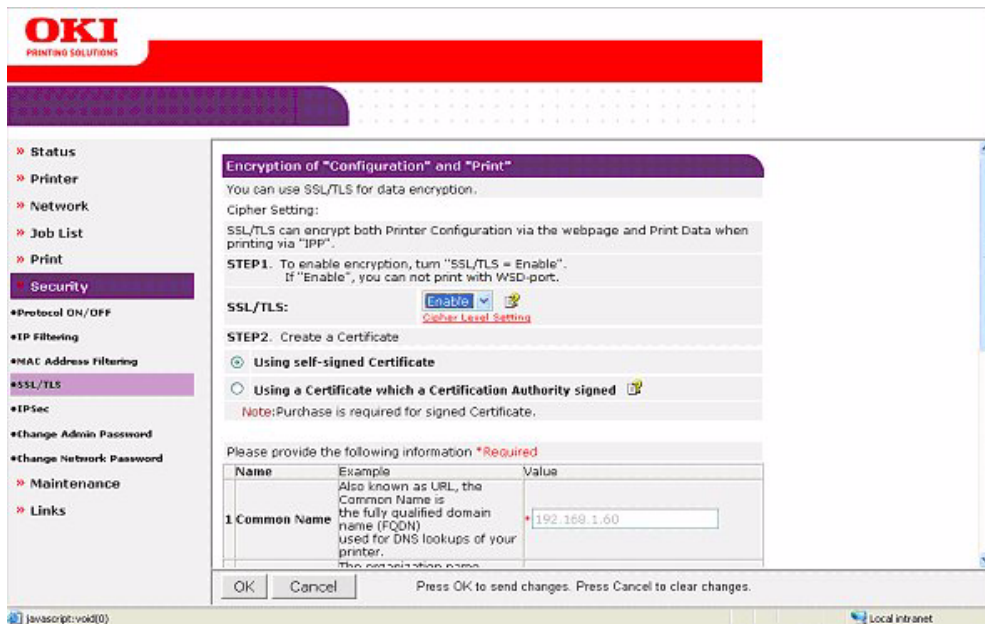
2. From the drop down menu select **ENABLE**.

> *NOTE*
> *Click icon for an explanation of the options available.*

3. Click the **Cipher Level Setting** link.

4. Select the level setting from the drop down menu options:

> **>** Strong

> **>** Standard

> **>** Weak

5. Click **OK** to confirm.

6. Select the required option from Step 2: **Create a Certificate**.
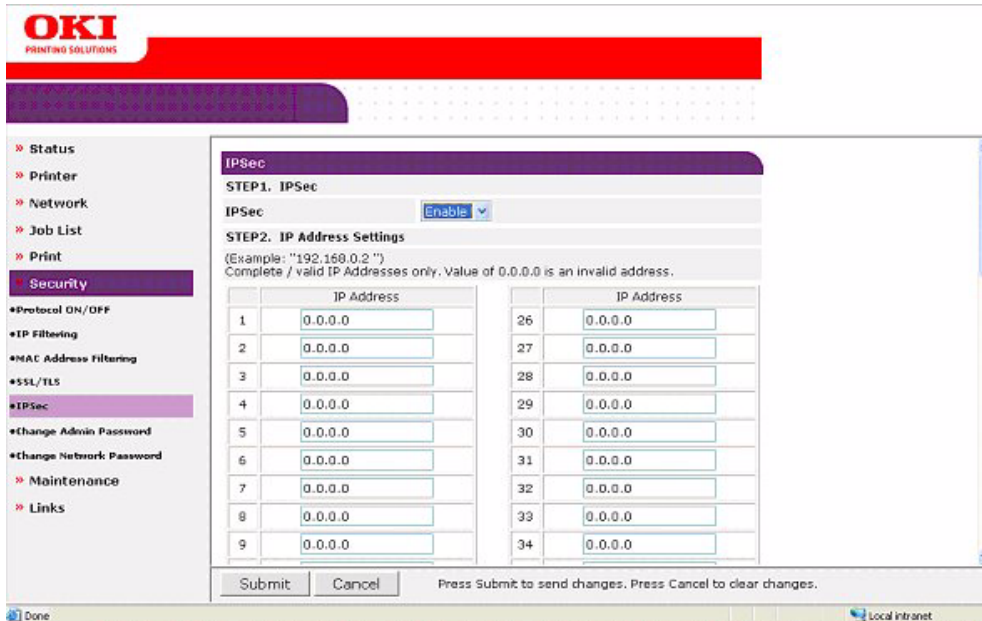
> *NOTE*
> *Click icon for an explanation of the options available.*

7. Input the required information into the main table.

8. If required, update the following information:

> **>** Key Exchange Method

> **>** Key Size

9. Click **OK** to save the changes or **Cancel** to exit.

IPSEC

To enable IPSec encryption:

1. From the left hand panel select **IPSec**.

2. From the drop down menu select **ENABLE**.

3. Enter valid IP Addresses in the **STEP2. IP Address Settings** table.

4. Update the **Phase 1 Proposal Settings** as required.

5. Enter the **Pre-Shared Key Settings** (max. 64 characters).

6. Update the **Key PFS Settings** as required.

7. Update the **Phase 2 Proposal Settings** as required.

8. Click **Submit** to save the changes or **Cancel** to exit.

PASSWORD CONFIGURATION

To change the administrator password:

1.   From the left hand panel select **Admin Password**.
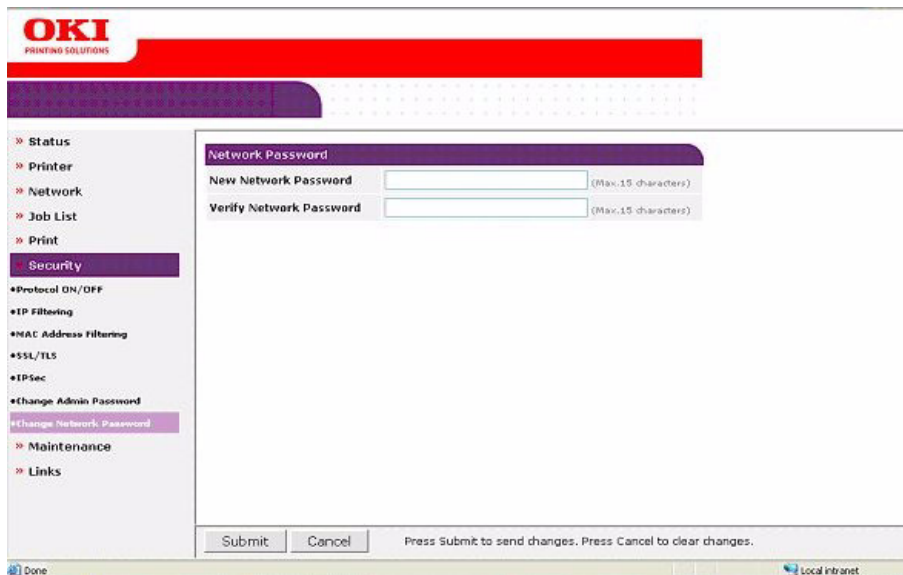
2.   Enter your new password.
3.   Enter your new password again to confirm.
4.   Click **Submit** to save the changes or **Cancel** to exit.

To change the network password:

1.   From the left hand panel select **Change Network Password**.

2.   Enter your new password.
3.   Enter your new password again to confirm.

> *NOTE*
> *Maximum 15 characters.*

4.   Click **Submit** to save the changes or **Cancel** to exit.

USING THE PRINTER SECURITY FEATURES

> *NOTE*
> *Example screenshots are used throughout this manual and as such may not represent the screens displayed for your machine. Some of the features shown on the example screenshots may not be available on your machine.*

SECURE PRINTING

Secure printing allows you to print confidential documents on machines that are shared with other users in a network environment.

The document does not print until a PIN (Personal Identification Number) is entered through the control panel. You must go to the machine and enter the PIN.

This feature requires a storage device option to be fitted to your machine and enabled in the printer driver.

If there is not enough space for the spooled data, a "Disk Full" message displays, and only one copy prints.

> *NOTE*
> *1. The secure printing feature may not be available from within some PC applications.*
>
> *2. This feature is not supported on Mac OS X.*

If your application software has a collate print option, turn it off otherwise secure printing will not work.

There are three parts in secure printing:

> "Sending the document" on page 17

> "Printing the document" on page 18

> "Deleting a secure print document" on page 19

> *NOTE*
> *The menu buttons on your machine's control panel vary depending on the model.*
>
> *For illustration purposes we will demonstrate the Printing and Deleting procedures using the **+/-** and **Enter** buttons; your machine may have **Up/Down** and **Return** arrow buttons instead however the procedure is identical.*
>
> *If your machine has a touch screen and numerical keypad buttons, the principle is basically the same; press the **Print** button to access the print menu options. There are on-screen instructions to guide you through the process.*

SENDING THE DOCUMENT

1. If using the PCL driver, in the **Setup** tab choose any saved driver settings you wish to use.

2. In the driver's **Job Options** tab, click **Secure Print.**

   The Job PIN (Personal Identification Number) window opens.
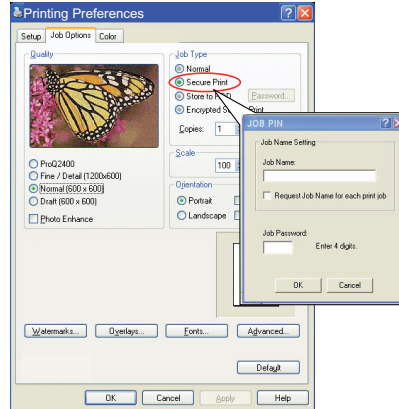
3. If the PIN window does not open, click the **PIN** button.

4. In the Job PIN window, enter a *name* for this print job.

   The name may be up to 16 alpha-numeric characters.

5. If you would like a prompt at the machine for the job name, click the **Request...** check box below the name entry.

6. Enter a number from 0000 to 9999 in the **PIN** box.

   Your PIN must be unique on this machine. Each user should be allocated a PIN by the system administrator.

7. Click **OK** to accept your changes.

   NOTE
   Leave the number of copies set to one. You can increase the copy count from the operator panel when you print the document.

   ---

8. Click **OK** to close the **Printer Properties** window.

9. Print your document.

   The print job will be sent to the machine, but will not print at this time.

PRINTING THE DOCUMENT

> *NOTE*
> *The menu buttons on your machine's control panel will vary depending on the model.*
>
> *For illustration purposes we will demonstrate the following procedure using the **+/-** and **Enter** buttons; your machine may have **Up**/**Down** and **Return** arrow buttons instead however the procedure is identical.*
>
> *If your machine has a touch screen and numerical keypad buttons, the principle is basically the same; press the **Print** button to access the print menu options. There are on-screen instructions to guide you through the process.*

Your secure print job is printed using the control panel on the front of the machine.

1. When the machine is idle, use the **+/-** buttons to select the PRINT JOB menu, then press **ENTER**.

2. Select ENCRYPTED/STORED JOB.

3. Use the **+/-** buttons to enter your PIN. Press **ENTER** after each digit.

4. If necessary, use the **+/-** buttons to highlight the PRINT option.

5. Press **ENTER** to confirm you wish to print the document.

6. Use the **+/-** buttons to select the number of collated copies you require.

7. Press **ENTER** to print your document.

> *NOTE*
> *It is also possible to print and delete secure documents remotely from your PC using the Storage Device Manager utility.*

DELETING A SECURE PRINT DOCUMENT

> *NOTE*
> *The menu buttons on your machine's control panel will vary depending on the model.*
>
> *For illustration purposes we will demonstrate the following procedure using the **+/-** and **Enter** buttons; your machine may have **Up**/**Down** and **Return** arrow buttons instead however the procedure is identical.*
>
> *If your machine has a touch screen and numerical keypad buttons, the principle is basically the same; press the **Print** button to access the print menu options. There are on-screen instructions to guide you through the process.*

If you change your mind about printing a secure document, you can delete it from the machine's storage device without printing it first.

1. Follow steps 1 to 3 in the above procedure for printing the document.

2. Use the **+/-** buttons to highlight the DELETE option and press **ENTER**.

3. If necessary, use the **+/-** buttons to highlight the YES choice, and press **ENTER** to confirm the deletion.

   Your document is deleted from the machine's storage device without printing.

> *NOTE*
> *It is also possible to print and delete secure documents remotely from your PC using the Storage Device Manager utility.*

STORE TO STORAGE DEVICE

This feature allows print jobs to be created on the PC and stored on the machine's storage device for printing on demand. This is good for forms, generic memos, letterhead, stationery, etc.

If you use this feature for standard forms, for example, you can walk up to the machine at any time and print off your forms without having to re-send them from the PC.

This feature works in exactly the same way as the secure printing feature described earlier in this chapter, and is available only in the Windows PostScript and PCL drivers. The difference with job spooling is that the document is not automatically deleted from the machine's storage device after printing. It remains there for future use until you delete it from the Printer Control Panel or from your PC with the Storage Device Manager utility.

> *NOTE*
> *1. If this choice does not appear in the driver screens, or if it is greyed out, check to ensure that the storage device is enabled in the printer driver.*
>
> *2. This feature is not supported on Mac OS X.*

Like the secure printing feature, there are three activities in job spooling:

> Sending the document

> Printing the document

> Deleting a stored document

SENDING THE DOCUMENT

Follow the same procedures as described in the section "Sending the document" on page 17 for sending a secure document, except that on the **Job Options** tab in step 2, click:

> **Store to HDD** if you have a hard disk drive installed

> **Store to SD** if you have an SD card installed
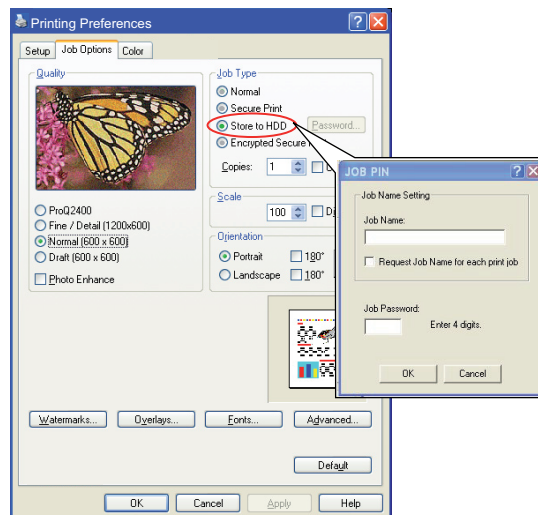
PRINTING THE DOCUMENT

Follow the same procedures as described in "Printing the document" on page 18 for printing a secure document. In this case the document will not be deleted from the storage device after it has been printed.

DELETING A STORED DOCUMENT

Follow the procedure as described in for deleting a secure print document.

Like secure print documents, any other documents stored on the machine's storage device can also be deleted remotely from the PC using the Storage Device Manager utility.

ENCRYPTED SECURE PRINTING

Security over the network is an increasing concern for some organisations. Encrypted secure printing allows you to send, store and print confidential documents on machines that are shared with other users in a network environment.

Encrypting your documents before sending them to your machine will prevent unauthorised personnel accessing confidential or sensitive information.

Print jobs are encrypted immediately before transmission to the machine, where they are stored in an encrypted format on the storage device. The documents will remain stored and unprinted until an authorised user authenticates the print job; decryption only happens when the job is actually printing.

This feature requires a storage device to be installed in your machine and enabled in the printer driver.

NOTE
1. *The secure printing feature may not be available from within some PC applications.*

2. *This feature is not supported on Mac OS X.*

If your application software has a collate print option, turn it off otherwise encrypted printing may not work.

As deletion is automatic, there are only two activities in encrypted secure printing:

> Sending the document

> Printing the document

SENDING THE DOCUMENT

1. If using the PCL driver, in the **Setup** tab choose any saved driver settings you wish to use.

2. In the driver's **Job Options** tab, click **Encrypted Secure Print.**

The Encrypted Secure Print window opens.
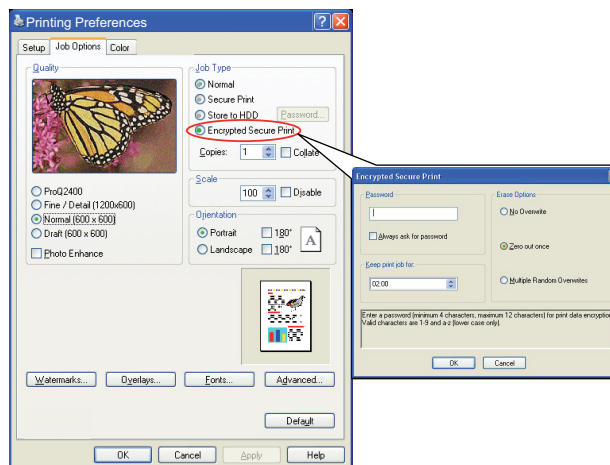
3. In the Encrypted Secure Print window, enter a *Password* for this print job:

   The password must be between 4 and 12 alpha-numeric characters. Numbers 1 to 9 and letters a to z are all valid.

4. If you would like a prompt at the machine for the job password, click the **Always ask for password** checkbox below the password entry.

5. Select the required erase option for your print job÷.

   If you have a hard disk installed, select from the following options:

   > **No overwrite**: deletes the job from the hard disk but doesn't overwrite with data. This option is faster but less secure as the print data may be recovered.

   > **Zero out once**: deletes the job from the hard disk and overwrites with zeros. This option is more secure than "No overwrite" but it may still be possible to reconstruct the print job from the hard disk.

   > **Multiple Random Overwrites**: deletes the job from the hard disk and overwrites it three times. This option is the slowest but the most secure.

   If you have an SD Card installed, select from the following options:

   > **No overwrite**: deletes the job from the SD card but doesn't overwrite with data. This option is faster but less secure as the print data may be recovered.

   > **Zero out once**: deletes the job from the SD card and overwrites with zeros. This option is more secure than "No overwrite".

6. Select the **Auto Erase Time-out** period.

   Specify a period of time (hours:minutes) during which the print job is stored in the machine's storage device. When this period expires, the print job is automatically erased from the storage device.

7. Click **OK** to accept your changes.

8. Click **OK** to close the Printer Properties window.

9. Print your document.

PRINTING THE DOCUMENT

Follow the same procedures as described in the section "Printing the document" on page 18 for printing a secure document.

In this case you will enter your password, and the document will be erased from the storage device depending on the options you specified in Sending the document, step 5 "Select the required erase option for your print job:." on page 22 when sending the document to print.

07087001 iss.4