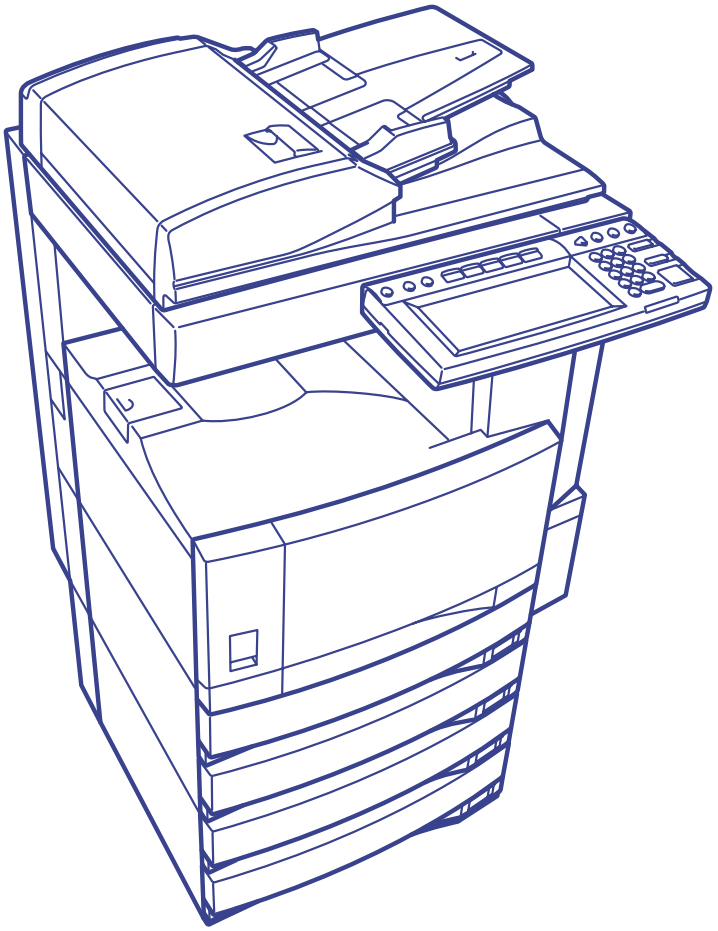
Océ | User Management Guide

im4530 / im3530



For Océ and Imagistics Models

Thank you for selecting an Océ solution for your document production and management needs. The following information will help you get the most productive and reliable use out of your system.

Océ brand supplies are designed for Océ copiers, printers and fax machines to ensure maximum product performance and quality. Substituting other supplies may result in inferior image quality and machine malfunction.
To order supplies call the Océ Supply Line:

1-800-462-6797 (US)
1-866-462-4478 (CAN)
01277 846 146 (UK)

Should your system develop a problem that cannot be remedied by using the maintenance or troubleshooting procedures outlined in this manual, please contact Océ Technical Support by calling:

1-800-243-5556 (US)
1-866-462-4478 (CAN)
08708 500 749 (UK)

For faster service, please have your machine model and serial number available before calling.

Serial Number:

This product was first introduced by Imagistics International Inc. and is now a part of the Océ product line. Please be aware that while some components may still carry the Imagistics name and markings, they are fully compatible with the Océ brand system.

SOFTWARE LICENSE AGREEMENT

INSTALLING OR OTHERWISE USING THIS SOFTWARE PRODUCT CONSTITUTES YOUR ACCEPTANCE OF THE FOLLOWING TERMS AND CONDITIONS (UNLESS A SEPARATE LICENSE IS PROVIDED BY THE SUPPLIER OF APPLICABLE SOFTWARE IN WHICH CASE SUCH SEPARATE LICENSE SHALL APPLY). IF YOU DO NOT ACCEPT THESE TERMS, YOU MAY NOT INSTALL OR USE THIS SOFTWARE, AND YOU MUST PROMPTLY RETURN THE SOFTWARE TO THE LOCATION WHERE YOU OBTAINED IT.

THE SOFTWARE INSTALLED ON THIS PRODUCT INCLUDES NUMEROUS INDIVIDUAL SOFTWARE COMPONENTS, EACH HAVING ITS OWN APPLICABLE END USER LICENSE AGREEMENT (“EULA”). INFORMATION RELATING TO THE EULAS MAY BE FOUND IN AN ELECTRONIC FILE INCLUDED ON THE USER DOCUMENTATION CD-ROM INCLUDED HEREWITH; HOWEVER, ALL SOFTWARE AND DOCUMENTATION DEVELOPED OR CREATED BY OR FOR Océ Imagistics Inc. (“Océ”) ARE PROPRIETARY PRODUCTS OF Océ AND ARE PROTECTED BY COPYRIGHT LAWS, INTERNATIONAL TREATY PROVISIONS, AND OTHER APPLICABLE LAWS.

Grant of License

This is a legal agreement between you, the end-user (“You”), and Océ and its suppliers. This software, fonts (including their typefaces) and related documentation (“Software”) is licensed for use with the system CPU on which it was installed (“System”) in accordance with the terms contained in this Agreement. This Software is proprietary to Océ and/or its suppliers.

Océ and its suppliers disclaim responsibility for the installation and/or use of this Software, and for the results obtained by using this Software. You may use one copy of the Software as installed on a single System, and may not copy the Software for any reason except as necessary to use the Software on a single System. Any copies of the Software shall be subject to the conditions of this Agreement.

You may not, nor cause or permit any third party to, modify, adapt, merge, translate, reverse compile, reverse assemble, or reverse engineer the Software. You may not use the Software, except in accordance with this license. No title to the intellectual property in the Software is transferred to you and full ownership is retained by Océ or its suppliers. Source code of the Software is not licensed to you. You will be held legally responsible for any copyright infringement, unauthorized transfer, reproduction or use of the Software or its documentation.

Term

This license is effective until terminated by Océ or upon your failure to comply with any term of this Agreement. Upon termination, you agree to destroy all copies of the Software and its documentation.

You may terminate this license at any time by destroying the Software and its documentation and all copies.

Disclaimer of Warranty

THIS SOFTWARE IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT. Océ AND ITS SUPPLIERS DISCLAIM ANY WARRANTY RELATING TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE. IF THE SOFTWARE PROVES DEFECTIVE, YOU (AND NOT Océ OR ITS SUPPLIERS) SHALL BE RESPONSIBLE FOR THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. Océ AND ITS SUPPLIERS DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE.

ALL INFORMATION CONTAINED HEREIN THAT IS PROVIDED BY Océ AND ITS AFFILIATES PURSUANT TO A EULA IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED.

Limitation of Liability

IN NO EVENT WILL Océ OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY DAMAGES, WHETHER IN CONTRACT, TORT, OR OTHERWISE (EXCEPT PERSONAL INJURY OR DEATH RESULTING FROM NEGLIGENCE ON THE PART OF Océ OR ITS SUPPLIERS), INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, LOST DATA, LOST SAVINGS OR OTHER INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE, EVEN IF Océ OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, NOR FOR THIRD PARTY CLAIMS.

U.S. Government Restricted Rights

The Software is provided with RESTRICTED RIGHTS. Use, duplication or disclosure by the U.S. Government is subject to restrictions set forth in subdivision (b) (3) (ii) or (c) (i) (ii) of the Rights in Technical Data and Computer Software Clause set forth in 252.227-7013, or 52.227-19 (c) (2) of the DOD FAR, as appropriate. Contractor/Manufacturer is Océ North America, Corporate Printing Division, 100 Oakview Drive, Trumbull CT 06611.

General

You may not sublicense, lease, rent, assign or transfer this license or the Software. Any attempt to sublicense, lease, rent, assign or transfer any of the rights, duties or obligations hereunder is void. You agree that you do not intend to, and will not ship, transmit (directly or indirectly) the Software, including any copies of the Software, or any technical data contained in the Software or its media, or any direct product thereof, to any country or destination prohibited by the United States Government. This license shall be governed by the laws of Japan or, at the election of a Supplier of Océ concerned with a dispute arising from or relating to this Agreement, the laws of the Country designated from time to time by the relevant Supplier of Océ. If any provision or portion of this Agreement shall be found to be illegal, invalid or unenforceable, the remaining provisions or portions shall remain in full force and effect.

YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND THAT YOU UNDERSTAND ITS PROVISIONS. YOU AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. YOU FURTHER AGREE THAT THIS LICENSE AGREEMENT CONTAINS THE COMPLETE AND EXCLUSIVE AGREEMENT BETWEEN YOU AND Océ AND ITS SUPPLIERS AND SUPERSEDES ANY PROPOSAL OR PRIOR AGREEMENT, ORAL OR WRITTEN, OR ANY OTHER COMMUNICATION RELATING TO THE SUBJECT MATTER OF THIS LICENSE AGREEMENT.

Océ North America, Corporate Printing Division, 100 Oakview Drive, Trumbull CT 06611.

TRADEMARKS AND COPYRIGHT

Trademarks

- The official name of Windows 98 is Microsoft Windows 98 Operating System.
- The official name of Windows Me is Microsoft Windows Me Operating System.
- The official name of Windows 2000 is Microsoft Windows 2000 Operating System.
- The official name of Windows XP is Microsoft Windows XP Operating System.
- The official name of Windows Server 2003 is Microsoft Windows Server 2003 Operating System.
- Microsoft, Windows, Windows NT, and the brand names and product names of other Microsoft products are trademarks of Microsoft Corporation in the US and other countries.
- Apple, AppleTalk, Macintosh, Mac, TrueType, and LaserWriter are trademarks of Apple Computer, Inc. in the US and other countries.
- Postscript is a trademark of Adobe Systems Incorporated.
- Netscape is a trademark of Netscape Communications Corporation.
- IBM, AT and AIX are trademarks of International Business Machines Corporation.
- NOVELL, NetWare, and NDS are trademarks of Novell, Inc.
- Other company names and product names in this manual are the trademarks of their respective companies.

Copyright

© 2005 Océ North America, Corporate Printing Division. All rights reserved
Under the copyright laws, this manual cannot be reproduced in any form without prior written permission of Océ. No patent liability is assumed, however, with respect to the use of the information contained herein.

Preface

Thank you for purchasing an im4530 Series or im2830 Series system. This User Management Guide explains the instructions how to manage the equipment with user management functions, such as department management, User Management Setting, and User Authentication for Scan to E-mail.

About This Guide

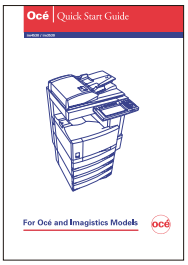
This manual explains describes how to manage this equipment using the functions of “Department Management”, “User Management Setting” and “User Authentication for Scan to E-mail”.

Conventions

- The term “this equipment” in this manual refers to the im4530 Series or im2830 Series.
- The term “e-Filing” in this manual is an abbreviation of “electronic filing”.

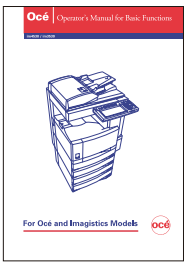
Lineup of Our Manuals

Thank you for purchasing the Océ multifunctional digital systems im4530 Series or im2830 Series.
We have provided you with these manuals for the operation of this equipment. Select and read the manual best suited to your needs.



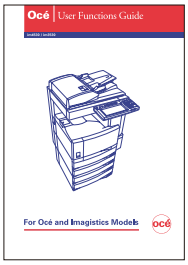
Quick Start Guide

This Quick Start Guide describes the initial setup method of this equipment and accessories of this product such as operator’s manuals and CD-ROMs.



Operator’s Manual Basic Functions

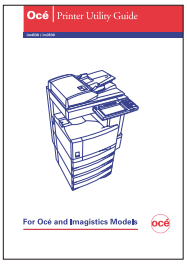
This Operator’s Manual Basic Functions describes how to use the basic functions of this equipment mainly focusing on the copying function. Also this manual contains safety precautions for users to be observed. Be sure to read it first carefully.



User Functions Guide

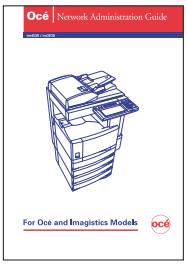
This User Functions Guide describes the functions and settings under the [USER FUNCTIONS] button on the control panel of this equipment.

Other guides are provided by the User Documentation CD-ROM in PDF files:



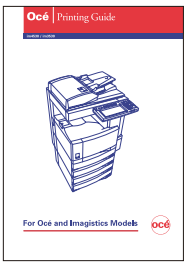
Printer Utility Guide

This Printer Utility Guide explains how to operate and set up the network functions such as the network scanning function and job management, using the Printer Utility (Web-based utility) from client computers.



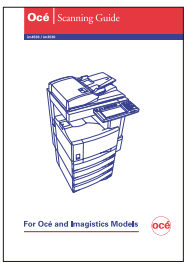
Network Administration Guide

This Network Administration Guide explains the guidelines for setting up network servers to provide various network services, and troubleshooting for network administrators.



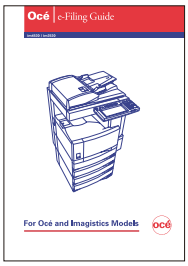
Printing Guide

This Printing Guide explains how to install the client software for printing from Microsoft Windows, Apple Mac OS, and UNIX computers, and print to the equipment.



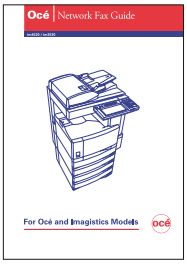
Scanning Guide

This Scanning Guide explains how to operate the scanning function of this equipment.



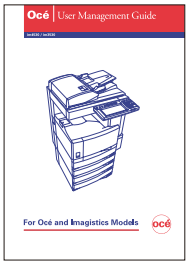
e-Filing Guide

This e-Filing Guide explains how to operate the e-Filing function using the TWAIN driver, File Downloader and e-Filing web utility.



Network Fax Guide

This Network Fax Guide explains how to use the network fax function that enable users to operate fax and internet fax sending from a client computer via network.



User Management Guide

This User Management Guide describes how to manage this equipment using the functions of “Department Management”, “User Management Setting” and “User Authentication for Scan to E-mail”.

To read manuals in PDF (Portable Document Format) files

Viewing and printing this operator’s manual in PDF files require that you install Adobe Reader or Adobe Acrobat Reader on your PC. If Adobe Reader or Adobe Acrobat Reader is not installed on your PC, download and install it from the website of Adobe Systems Incorporated.

Precautions in this manual

To ensure correct and safe use of this equipment, this operator's manual describes safety precautions according to the three levels shown below.
You should fully understand the meaning and importance of these items before reading this manual.

Warning	Indicates a potentially hazardous situation which, if not avoided, could result in death, serious injury, or serious damage, or fire in the equipment or surrounding assets.
Caution	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury, partial damage of the equipment or surrounding assets, or loss of data.
Note	Indicates a procedure you should follow to ensure the optimal performance of the equipment and problem-free copying.

Other than the above, this manual also describes information that may be useful for the operation of this equipment with the following signage:

Tip	Describes handy information that is useful to know when operating the equipment.
🕮	Pages describing items related to what you are currently doing. See these pages as required.

TABLE OF CONTENTS

SOFTWARE LICENSE AGREEMENT 1

TRADEMARKS AND COPYRIGHT 3

Preface 4

About This Guide 4

Conventions 4

Lineup of Our Manuals 4

To read manuals in PDF (Portable Document Format) files 6

Precautions in this manual 7

Chapter 1 Setting up User Management

Enabling Department Management 12

Setting up User Management Setting 15

Enabling User Management Setting 16

Enabling Windows Domain Authentication 17

Enabling LDAP Authentication 21

Enabling MFP Local Authentication 25

Managing User Information 26

How to Login to Touch Panel 43

Setting up User Authentication for Scan to E-mail 48

INDEX 55

1

Setting up User Management

In the User Management tab page, you can enable or disable the department management, configure the User Management Setting, and configure the User Authentication for Scan to E-mail.

Enabling Department Management 12

Setting up User Management Setting 15

Enabling User Management Setting 16
Managing User Information 26
How to Login to Touch Panel 43

Setting up User Authentication for Scan to E-mail 48

Enabling Department Management

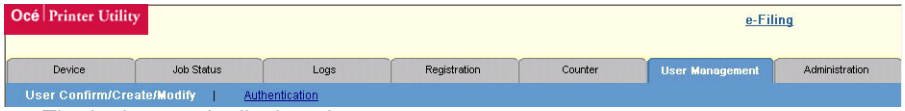
The department management is disabled as the default setting. When you want to manage the counters for every department, enable the department management. If the department management is enabled, the department code input screen will be displayed in the Touch Panel Display when you perform copying, scanning, faxing, and e-Filing box operations to manage the operations separately every department. The printing can be also managed using the department code.

Notes

- To enable the department management, at least one department code must be registered. Before enabling the department management, register the department code that you require.
- Enabling or disabling the department management can be operated in the General sub-menu page in the Setup menu page.
- Enabling or disabling the department management can be operated using the Control Panel. For instructions using the Control Panel, see ***User Functions Guide***.

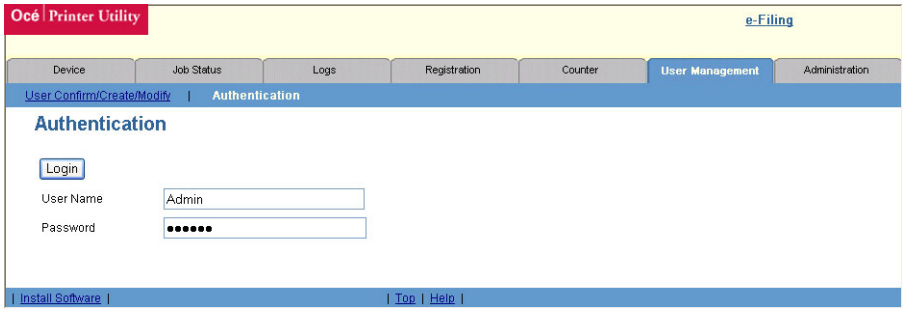
Enabling the department management

1 Click the User Management tab and the Authentication menu.



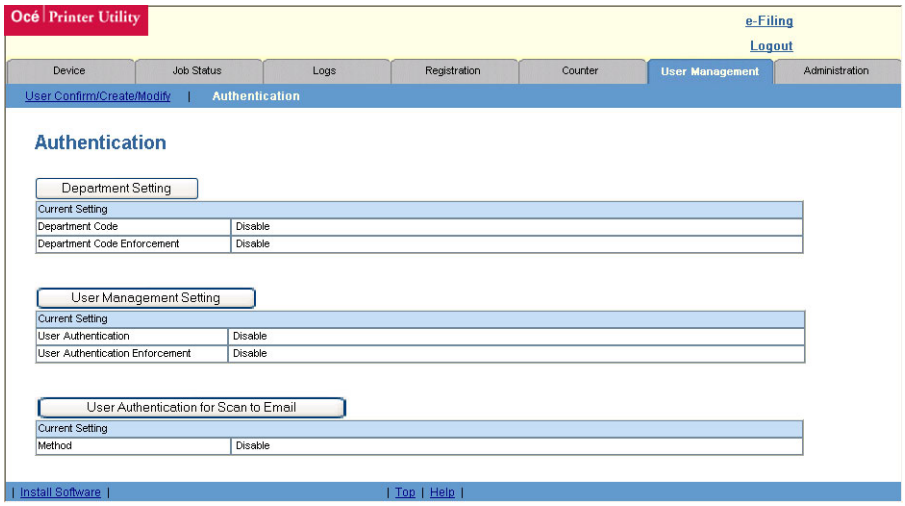
- The login page is displayed.

2 Enter the administrator password and click [Login].



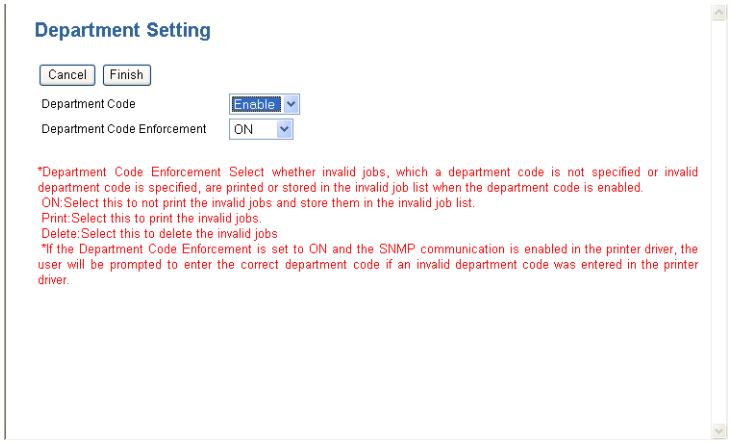
- The Authentication page is displayed.

3 Click [Department Setting].



- The Department Setting page opens.

4 Specify the following items and click [Finish].



- **Department Code**
  Select whether the department management is enabled or disabled.

  Note

  When the User Management Setting is enabled, the Department Code option cannot be disabled.

- **Department Code Enforcement**
  Select whether invalid jobs, which a department code is not specified or invalid department code is specified, are printed or stored in the invalid job list when the department code is enabled.
  ON — Select this to not print the invalid jobs and store them in the invalid job list.
  Print — Select this to print the invalid jobs.
  Delete — Select this to delete the invalid jobs without storing them in the invalid job list.

  Notes

  - If the Department Code Enforcement is set to ON and the SNMP communication is enabled in the printer driver, the user will be prompted to enter the correct department code if an invalid department code was entered in the printer driver.
  - The Department Code Enforcement setting is not applied when the User Management Setting is enabled.

Setting up User Management Setting

When the User Management Setting is enabled, users must enter the user name and password before operating this equipment. Therefore, you can secure the equipment from the unexpected users.

When the User Management Setting is enabled, the following functions will be available.

- The counters for each user can be managed.
- The limitations for each user can be set.
- Up to 10000 users can be registered.
- The user name and password will be required to operate the [COPY], [SCAN], [e-FILING], [FAX], [TEMPLATE], [USER FUNCTIONS], and [JOB STATUS] buttons.
- The user name and password will be required to operate the e-Filing web utility.
- The print jobs can be accepted only from the computer of which the login user name can be attested. (When the Windows Domain Authentication or LDAP Authentication is used, the computer must also join the domain.)
- When the Windows Domain or LDAP Authentication is used, the user information will be registered automatically in the equipment when a user enters the user name and password in the User Authentication screen and then enter the department code.

The following table shows which function will use the User Management Setting.

Operation		Authentication	Remarks
Control Panel	COPY	Yes	
	SCAN	Yes	
	e-FILING	Yes	
	FAX	Yes	
	EXTENSION	No	
	JOB STATUS	Yes	
	ACCESS	No	
	INTERRUPT	Yes	
	TEMPLATE	Yes	
	USER FUNCTIONS	Yes	
Web	Printer Utility	No	
	e-Filing	Yes	
Client Software	Printer Driver N/W-Fax Driver	Yes (User Name Only)	The computer must login the domain.
	Document Monitor	No	
	File Downloader	No	
	TWAIN Driver	No	
	Backup/Restore	No	
	Address Book Viewer	No	

Note

Please remember the following limitations and considerations for the User Management Setting.
- The jobs cannot be printed or deleted from Printer Utility. When you want to print or delete the jobs, please perform the operation from the [JOB STATUS] button on the Control Panel.
- The department codes that any users are registered cannot be deleted. If you want to delete the department codes, make sure that the no user is registered in the department codes that you want to delete.
- When the Windows Domain or LDAP Authentication is enabled, the password setting in the User Information will not be used for the authentication. Do not specify the password for the User Information when the Windows Domain or LDAP Authentication is used.
- When the user's jobs are in progress or the user currently log in the touch panel, the user information cannot be deleted or you cannot reset the user's counters.

Before registering the user information, enable the User Management Setting.
🕮 P.16 "Enabling User Management Setting"
After you enable the User Management Setting, register the user information.
🕮 P.26 "Managing User Information"

Note

When you enable the User Management Setting, the department management will be enabled automatically. However, no department code has been registered, you cannot enable the User Management Setting. In that case, please register the department code before enabling the User Management Setting.

Enabling User Management Setting

This equipment supports the following methods for the User Management Setting.
- **Windows Domain Authentication**
  When your network manages the network users using the Windows Domain, this equipment can be managed using the Windows Domain Authentication.
  When this is configured, users must enter the user name and password that is registered in the Windows Domain to perform any operations on the Control Panel of this equipment.
  🕮 P.17 "Enabling Windows Domain Authentication"
- **LDAP Authentication**
  When your network manages the network users using the LDAP, this equipment can be managed using the LDAP Authentication.
  When this is configured, users must enter the user name and password that is registered in the LDAP server to perform any operations on the Control Panel of this equipment.
  🕮 P.21 "Enabling LDAP Authentication"
- **MFP Local Authentication**
  When you do not have any network authentication systems in your network, you can use the MFP Local Authentication.
  When this is configured, users must enter the user name and password that is registered in the MFP to perform any operations on the Control Panel of this equipment.
  🕮 P.25 "Enabling MFP Local Authentication"

Note

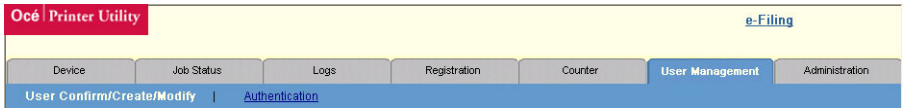
If you want to change the authentication method, please change the domain name and password settings of the User Information as required. It's easy to change the settings of the User Information using the Export/Import function.
🕮 P.36 "Exporting User Information and Counters"
🕮 P.38 "Importing User Information"

Enabling Windows Domain Authentication

To use the Windows Domain Authentication, you must have Windows Domain Authentication system in your network.

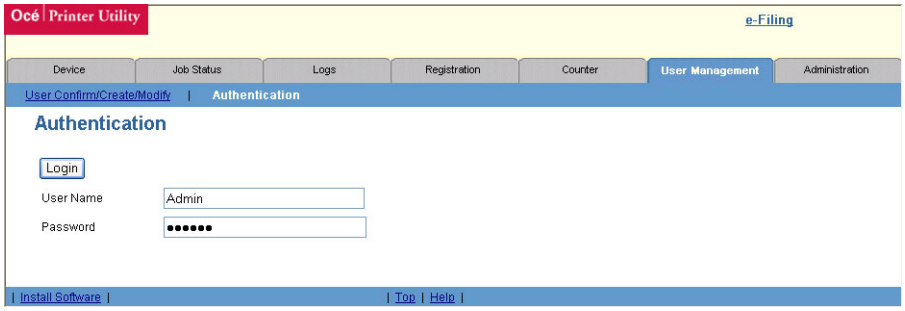
Enabling Windows Domain Authentication

1 Click the User Management tab and the Authentication menu.



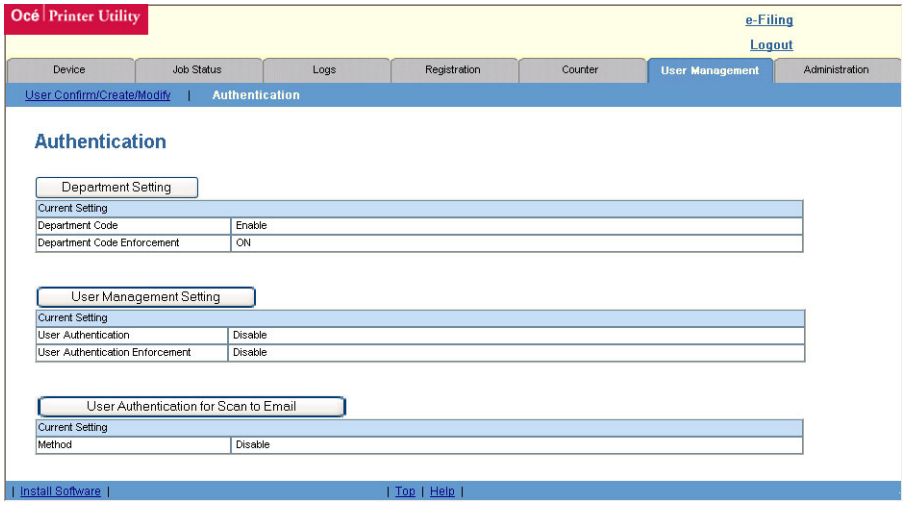
- The login page is displayed.

2 Enter the administrator password and click [Login].



- The Authentication page is displayed.

3 Click [User Management Setting].



- The User Management Setting page opens.

4 Select “Enable” in the “User Authentication” drop down box, and select how invalid jobs are processed in the “User Authentication Enforcement” drop down box. Then click [Next].



- In the “User Authentication Enforcement” drop down box, select whether invalid jobs, which an authentication failed, are printed or stored in the invalid job list.
  - **ON** — Select this to not print the invalid jobs and store them in the invalid job list.
  - **Print** — Select this to print the invalid jobs.
  - **Delete** — Select this to delete the invalid jobs without storing them in the invalid job list.

Tip

You can disable the User Management Setting by selecting “Disable” and click [Next].

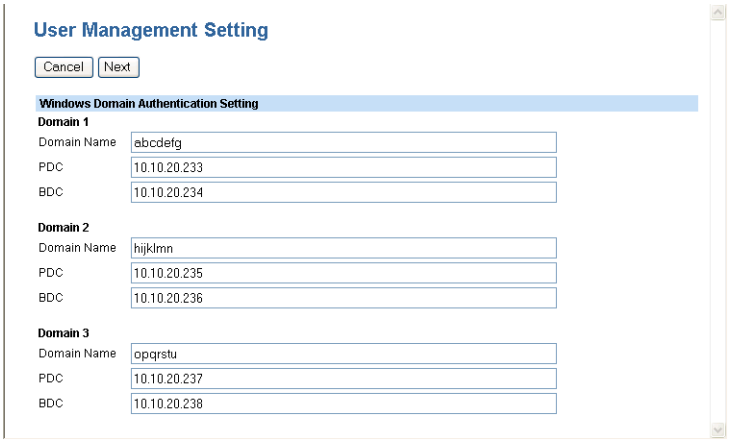
5 Select “Windows Domain Authentication” and click [Next].



Tip

If you want to automatically register user information that is entered by users in the authentication screen on the touch panel, Printer Utility, and e-Filing web utility, check the “Create User Information Automatically” check box.

6 Enter the following items and click [Next].



Domain Name — Enter the domain name in your network.
PDC — Enter the server name or IP address of the Primary Domain Controller.
BDC — Enter the server name or IP address of the Backup Domain Controller as you required.

Notes

- If the wrong primary or backup domain controller is specified, the [ENTER] button in the USER AUTHENTICATION screen on the touch panel is highlighted while this equipment searches for the primary or backup domain controller for 2 to 4 minutes. In that case, correct the primary or backup domain controller setting after the beep will sound and the alert message will be displayed on the touch panel.
- You can specify up to 3 domain names. You must specify at least one domain name to enable the Windows Domain Authentication.

7 Specify the following items and click [Next].

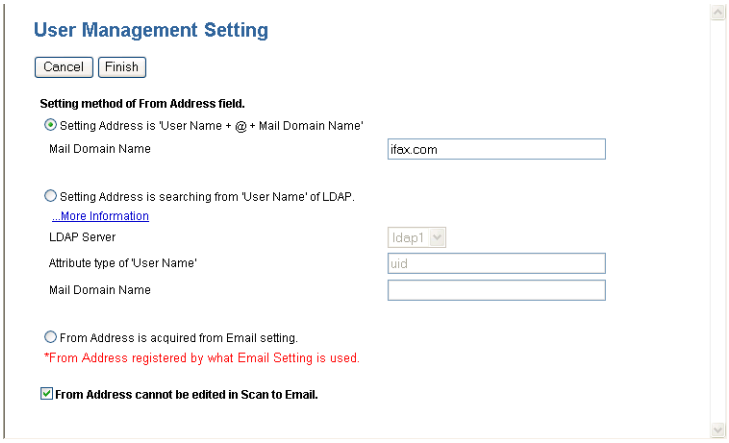


Role Based Access — Select whether the Role Based Access Control is enabled or not.
LDAP Server — Select the LDAP server that manages the Role Based Access Control.

Tips

- When you enable the Role Based Access Control, you must also configure the LDAP server to manage the operation of this equipment using Role Based Access Control. For instructions on how to configure the LDAP server for Role Based Access Control, please see ***Network Administration Guide***.
- The LDAP server to be used for the authentication must be configured in the Directory Service submenu page in the Maintenance menu. When you configure the Active Directory in Windows server, please specify the domain administrator or account operator for the user name.

8 Specify how the From Address is set for Scan to Email.



Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field.
When this is selected, enter the domain name in the “Mail Domain Name” field.
Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address that is searched from the LDAP server.
When this is selected, this equipment will search the user name, which is entered on the Touch Panel Display for the authentication, from the records of the attribute type in the LDAP server that you specify in the “LDAP Server” drop down box and “Attribute type of ‘User Name’” field.
If the user name is found, this equipment sets the From Address as the email address of the user name registered in the LDAP server.
If the user name is not found in the LDAP server, this equipment sets the From Address as the “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field.
When this is selected, select the LDAP server in the “LDAP Server” drop down box, enter the attribute type to search the user name in the “Attribute type of ‘User Name’” field, and the domain name that is used when the user name is not found in the “Mail Domain Name” field.
From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.
From Address cannot be edited in Scan to Email — Check this box if you do not want to allow users to edit the From Address.

9 Click [Finish].

- The Windows Domain Authentication is enabled.

Enabling LDAP Authentication

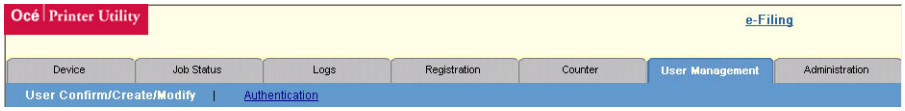
To enable the LDAP Authentication, you must have LDAP directory service in your network.

Notes

- Before enabling the LDAP Authentication, please see “Setting up LDAP Authentication Service” in the ***Network Administration Guide***.
- To enable LDAP with SSL, please see the description for LDAP Session in ***Printer Utility Guide***.

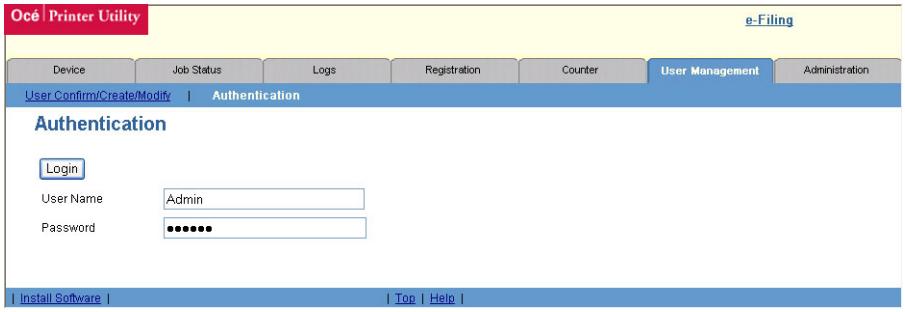
Enabling LDAP Authentication

1 Click the User Management tab and the Authentication menu.



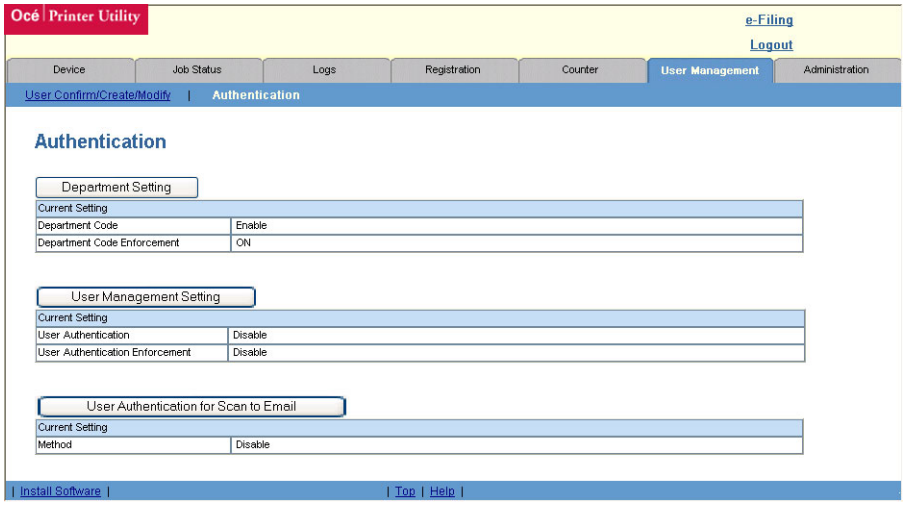
- The login page is displayed.

2 Enter the administrator password and click [Login].



- The Authentication page is displayed.

3 Click [User Management Setting].



- The User Management Setting page opens.

4 Select “Enable” in the “User Authentication” drop down box, and select how invalid jobs are processed in the “User Authentication Enforcement” drop down box. Then click [Next].



- In the “User Authentication Enforcement” drop down box, select whether invalid jobs, which an authentication failed, are printed or stored in the invalid job list.
  - **ON** — Select this to not print the invalid jobs and store them in the invalid job list.
  - **Print** — Select this to print the invalid jobs.
  - **Delete** — Select this to delete the invalid jobs without storing them in the invalid job list.

Tip

You can disable the User Management Setting by selecting “Disable” and click [Next].

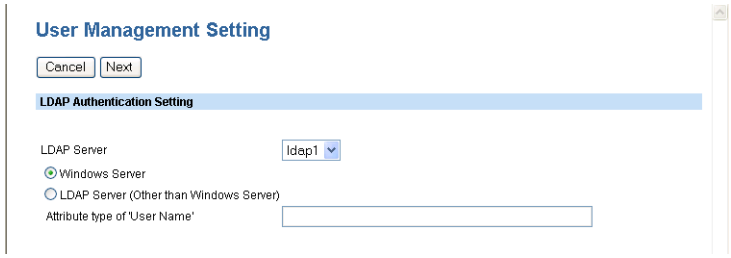
5 Select “LDAP Authentication” and click [Next].



Tip

If you want to automatically register user information that is entered by users in the authentication screen on the touch panel, Printer Utility, and e-Filing web utility, check the “Create User Information Automatically” check box.

6 Select the LDAP server to be used for the authentication and select the type of the LDAP server. Then click [Next].

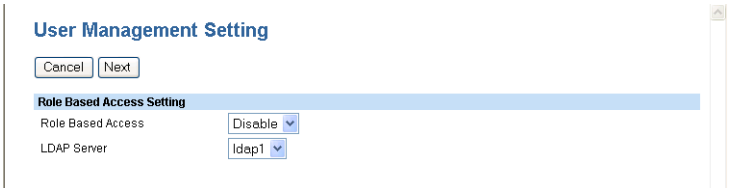


Windows Server — Select this when LDAP is running on Windows server.
LDAP Server (Other than Windows Server) — Select this when the LDAP is running the server other than Windows server. When this is selected, you have to specify the attribute type of ‘User Name’.

Tip

The LDAP server to be used for the authentication must be configured in the Directory Service submenu page in the Maintenance menu.

7 Specify the following items and click [Next].

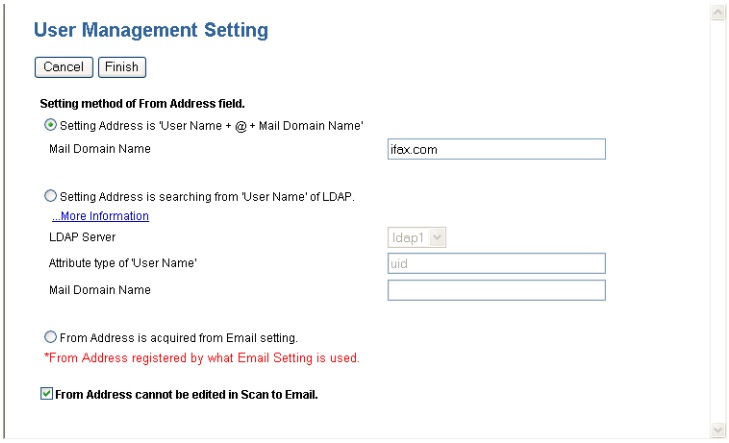


Role Based Access — Select whether the Role Based Access Control is enabled or not.
LDAP Server — Select the LDAP server that manages the Role Based Access Control.

Tips

- When you enable the Role Based Access Control, you must also configure the LDAP server to manage the operation of this equipment using Role Based Access Control. For instructions on how to configure the LDAP server for Role Based Access Control, please see ***Network Administration Guide***.
- The LDAP server to be used for the authentication must be configured in the Directory Service submenu page in the Maintenance menu. When you configure the Active Directory in Windows server, please specify the domain administrator or account operator for the user name.

8 Specify how the From Address is set for Scan to Email.



Note

When the User Authentication for Scan to Email is not enabled, these settings are not used for Scan to Email.

Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field.
When this is selected, enter the domain name in the “Mail Domain Name” field.
Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address that is searched from the LDAP server.
When this is selected, this equipment will search the user name, which is entered on the Touch Panel Display for the authentication, from the records of the attribute type in the LDAP server that you specify in the “LDAP Server” drop down box and “Attribute type of ‘User Name’” field.
If the user name is found, this equipment sets the From Address as the email address of the user name registered in the LDAP server.
If the user name is not found in the LDAP server, this equipment sets the From Address as the “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field.
When this is selected, select the LDAP server in the “LDAP Server” drop down box, enter the attribute type to search the user name in the “Attribute type of ‘User Name’” field, and the domain name that is used when the user name is not found in the “Mail Domain Name” field.
From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.
From Address cannot be edited in Scan to Email — Check this box if you do not want to allow users to edit the From Address.

9 Click [Finish].

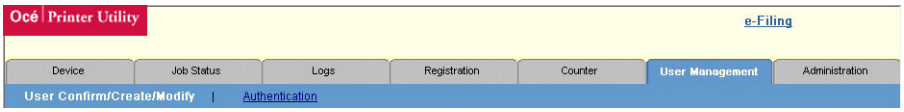
- The LDAP Authentication is enabled.

Enabling MFP Local Authentication

When no network authentication system is configured in your network, you can enable the MFP Local Authentication.
The MFP Local Authentication uses the account information that is registered in this equipment for the authentication. Therefore, you must register the user account information first before enabling the MFP Local Authentication. This equipment also manages the counters for each user if the MFP Local Authentication is enabled.
P.27 “Creating or modifying user information”
After you register the user information, enable the MFP Local Authentication.
P.25 “Enabling MFP Local Authentication”

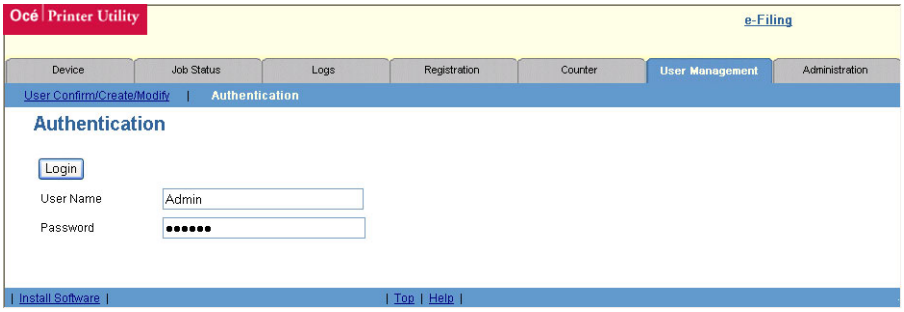
Enabling MFP Local Authentication

1 Click the User Management tab and the Authentication menu.



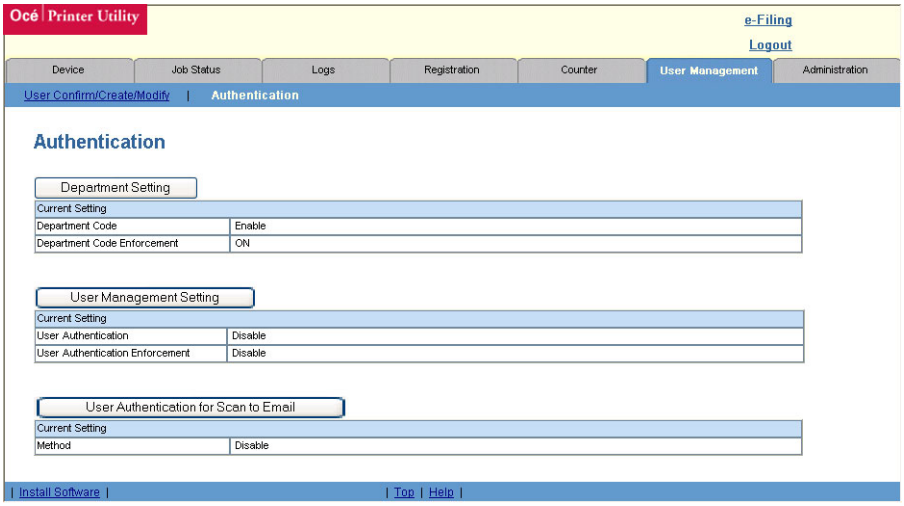
- The login page is displayed.

2 Enter the administrator password and click [Login].



- The Authentication page is displayed.

3 Click [User Management Setting].



- The User Management Setting page opens.

4 Select “Enable” in the “User Authentication” drop down box, and select how invalid jobs are processed in the “User Authentication Enforcement” drop down box. Then click [Next].



- In the “User Authentication Enforcement” drop down box, select whether invalid jobs, which an authentication failed, are printed or stored in the invalid job list.
  - **ON** — Select this to not print the invalid jobs and store them in the invalid job list.
  - **Print** — Select this to print the invalid jobs.
  - **Delete** — Select this to delete the invalid jobs without storing them in the invalid job list.

Tip

You can disable the User Management Setting by selecting “Disable” and click [Next].

5 Select “MFP Local Authentication” and click [Next].



- The MFP Local Authentication is enabled.

Managing User Information

After enabling the User Management Setting, you must register the user information In the User Confirm/Create/Modify page.
In this page, you can do:
📖 P.27 “Creating or modifying user information”
📖 P.29 “Deleting user information”
📖 P.31 “Deleting all user information”
📖 P.32 “Resetting the counters for specific users”
📖 P.34 “Resetting the counters for all users”
📖 P.36 “Exporting User Information and Counters”
📖 P.38 “Importing User Information”

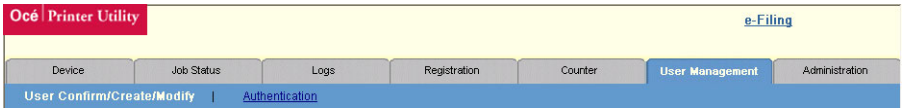
The registered users can view the own user information in the User Confirm/Create/Modify page. Users can also change the own password (only when the Local MFP Authentication is enabled).
📖 P.41 “Viewing the own user information by a user”
📖 P.42 “Changing a password by a user (Local MFP Authentication only)”

Notes

- When the Windows Domain or LDAP Authentication is used and the “Create User Information Automatically” option is enabled when enabling the User Management Setting, the user information can be registered automatically in the equipment when a user enters the user name and password in the User Authentication screen and then enter the department code.
- There is “Undefined” user information that is registered as the default. This user information is used to count the Invalid jobs. You can view the counter information of this user information, but cannot modify or delete this default user information.

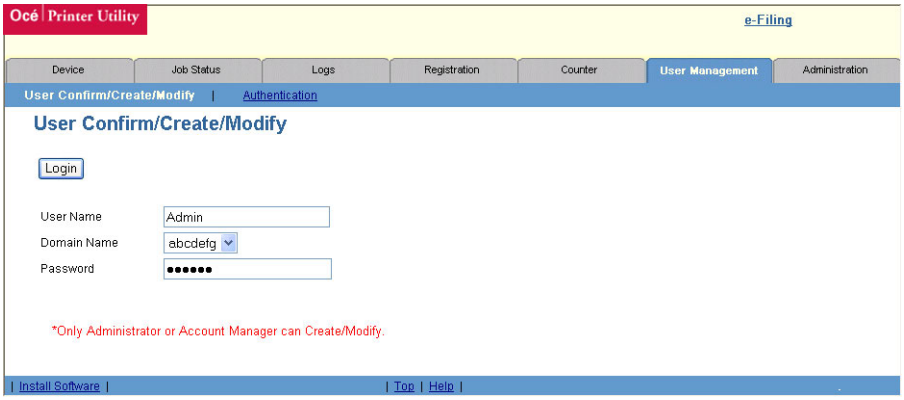
Creating or modifying user information

1 Click the User Management tab.



- The login page is displayed.

2 Enter “Admin” in the “User Name” field, enter the administrator password in the “Password” field, and click [Login].

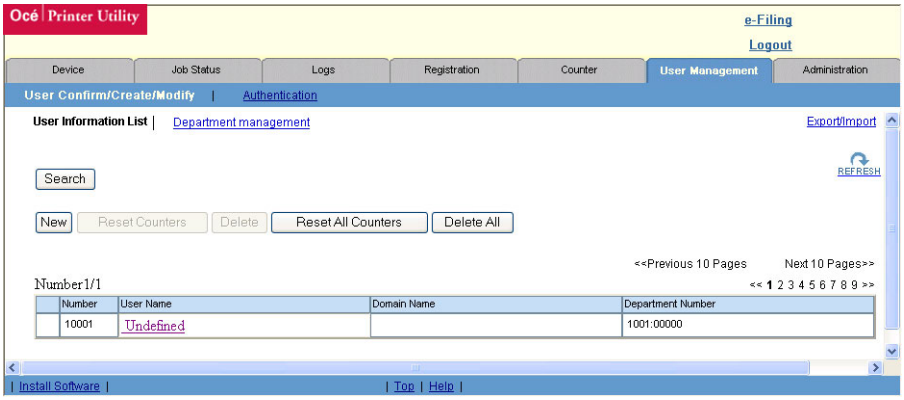


- The User Information List submenu page is displayed.

Tips

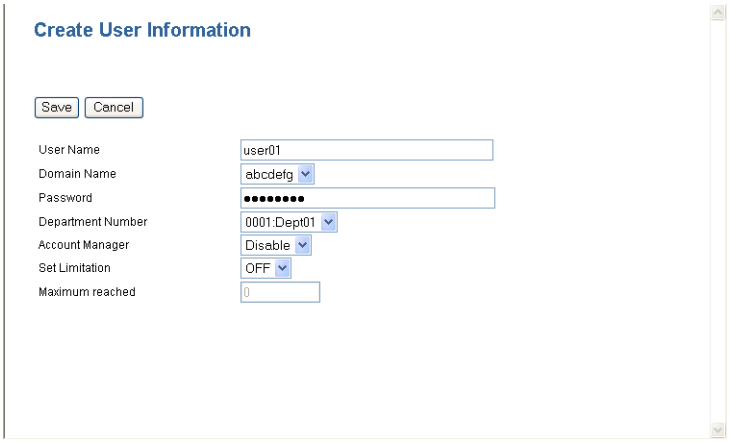
- Users can also login using the user name, domain name (required only when Windows Domain Authentication is enabled), and password that has been set as the Account Manager in the User Information.
- You do not have to select the “Domain Name” field when you log in as the Administrator.

3 Click [New] to create a new user or click the user name link to modify the existing user information.



- The User Information page is opened.

4 Enter the following items and press [Save].



User Name — Enter a login user name. You can enter up to 128 characters.
Domain Name — Select the domain name that this user will login. The domain name that is set while enabling the Windows Domain authentication is used for the authentication.
Password — Enter a login password. You can enter up to 64 characters. You do not have to specify this when the Windows Domain or LDAP authentication is used.
Department Number — Select the department code that the user belongs. The jobs that are performed by the user are counted as the specified department code.
Account Manager — Select whether this user is registered as the Account Manager. The users that are registered as the Account Manager can login to the User Information List submenu page.
Set Limitation — Select whether enabling the limitation of outputs for this user. When you select “ON”, enter the maximum number of outputs for this user in the “Maximum reached” field.
Maximum reached — Enter the maximum number of outputs for this user when the “Set Limitation” option is enabled.

Tips

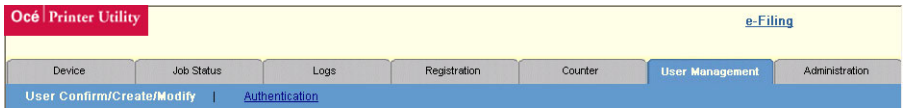
- You can also delete the user information by clicking [Delete].
- You can also reset the counter for this user by clicking [Reset Counters].
- When you editing the existing user information, the counter information of the user is displayed in the page.

Deleting user information

Notes

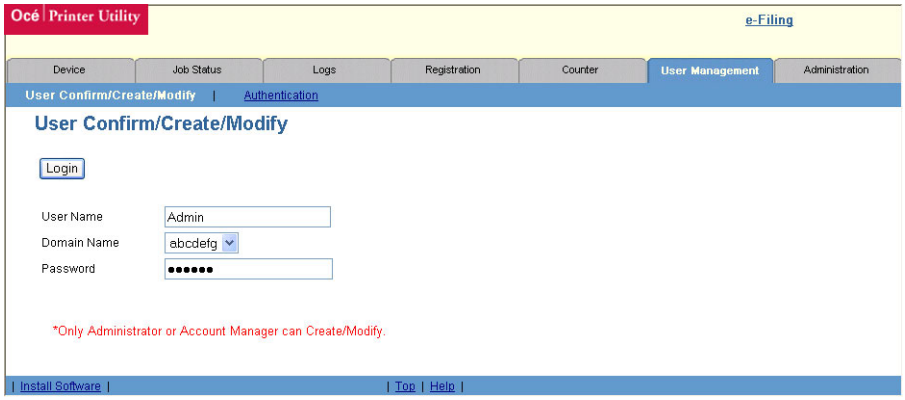
- When the user’s jobs are in progress or the user currently log in the touch panel, the user information cannot be deleted.
- The “Undefined” user information cannot be deleted.

1 Click the User Management tab.



- The login page is displayed.

2 Enter “Admin” in the “User Name” field, enter the administrator password in the “Password” field, and click [Login].

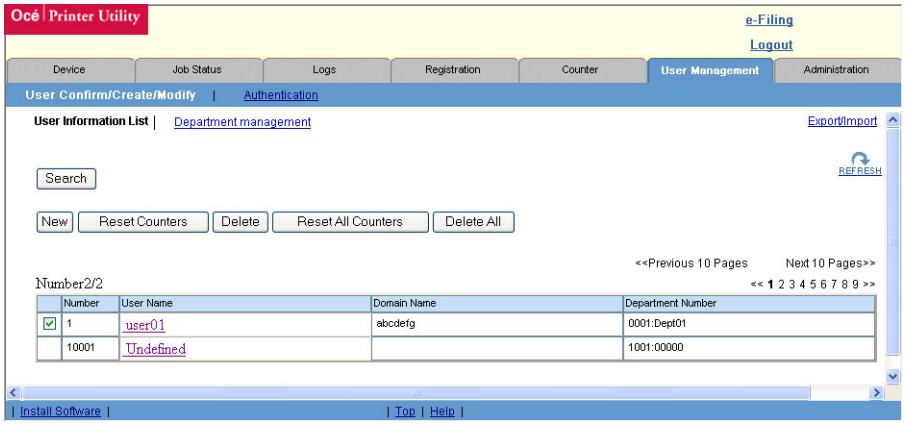


- The User Information List submenu page is displayed.

Tips

- Users can also login using the user name, domain name (required only when Windows Domain Authentication is enabled), and password that has been set as the Account Manager in the User Information.
- You do not have to select the “Domain Name” field when you log in as the Administrator.

3 Check the boxes of users that you want to delete and click [Delete].



- The confirmation dialog box appears.

4 Click [OK] to delete the user information.



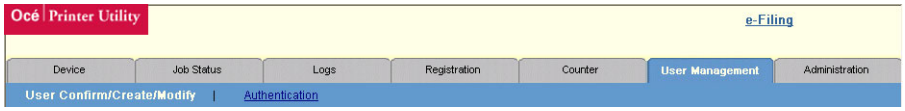
- The selected users are deleted.

Deleting all user information

Notes

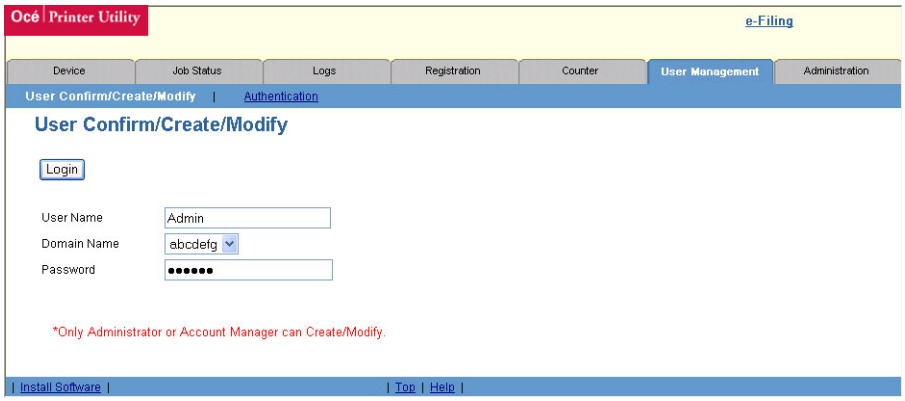
- When the user's jobs are in progress or the user currently log in the touch panel, the user information cannot be deleted.
- The "Undefined" user information cannot be deleted.

1 Click the User Management tab.



- The login page is displayed.

2 Enter "Admin" in the "User Name" field, enter the administrator password in the "Password" field, and click [Login].

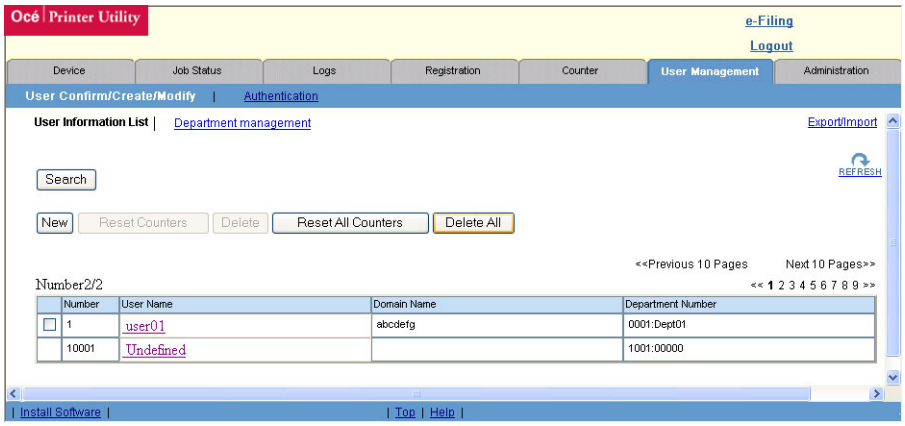


- The User Information List submenu page is displayed.

Tips

- Users can also login using the user name, domain name (required only when Windows Domain Authentication is enabled), and password that has been set as the Account Manager in the User Information.
- You do not have to select the "Domain Name" field when you log in as the Administrator.

3 Click [Delete All].



- The confirmation dialog box appears.

4 Click [OK] to delete all user information.



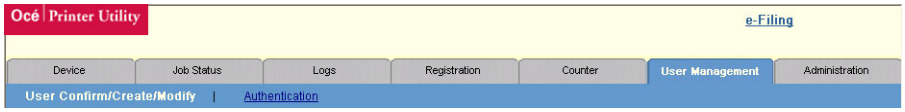
- The counters of selected users are cleared.

Resetting the counters for specific users

Note

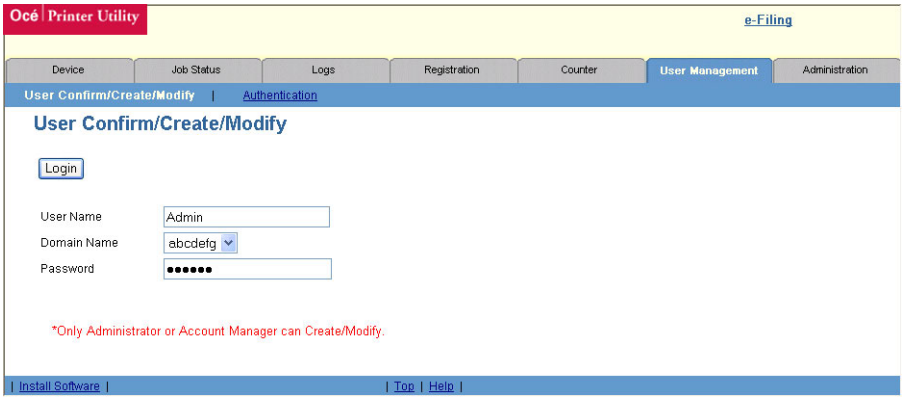
When the user's jobs are in progress or the user currently log in the touch panel, you cannot reset the user's counters.

1 Click the User Management tab.



- The login page is displayed.

2 Enter “Admin” in the “User Name” field, enter the administrator password in the “Password” field, and click [Login].

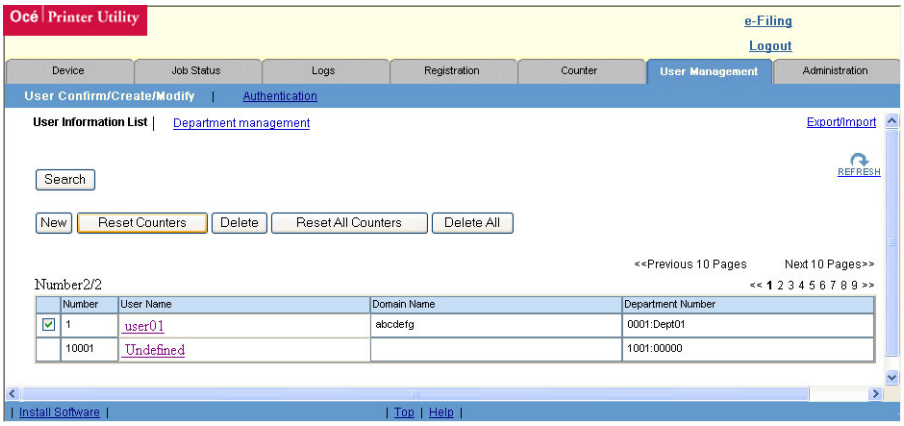


- The User Information List submenu page is displayed.

Tips

- Users can also login using the user name, domain name (required only when Windows Domain Authentication is enabled), and password that has been set as the Account Manager in the User Information.
- You do not have to select the “Domain Name” field when you log in as the Administrator.

3 Check the boxes of users that you want to reset counters and click [Reset Counters].



- The confirmation dialog box appears.

4 Click [OK] to reset the counters.



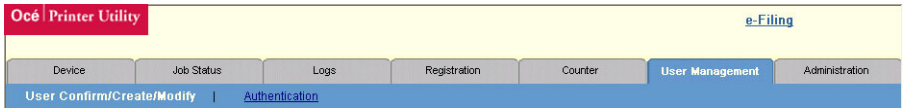
- The counters of selected users are cleared.

Resetting the counters for all users

Note

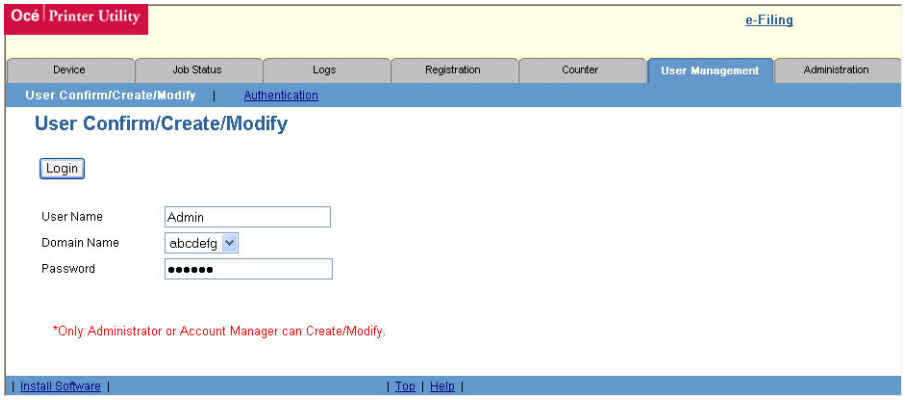
When the user's jobs are in progress or the user currently log in the touch panel, you cannot reset the user's counters.

1 Click the User Management tab.



- The login page is displayed.

2 Enter "Admin" in the "User Name" field, enter the administrator password in the "Password" field, and click [Login].

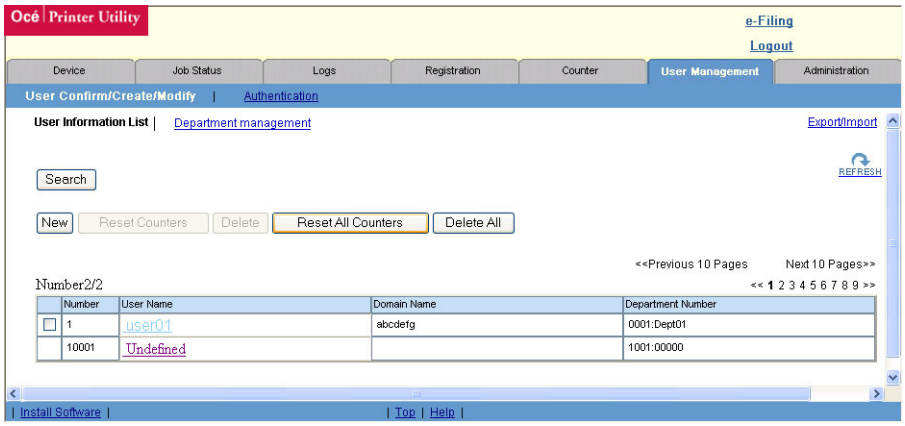


- The User Information List submenu page is displayed.

Tips

- Users can also login using the user name, domain name (required only when Windows Domain Authentication is enabled), and password that has been set as the Account Manager in the User Information.
- You do not have to select the "Domain Name" field when you log in as the Administrator.

3 Click [Reset All Counters].



- The confirmation dialog box appears.

4 Click [OK] to reset all counters.

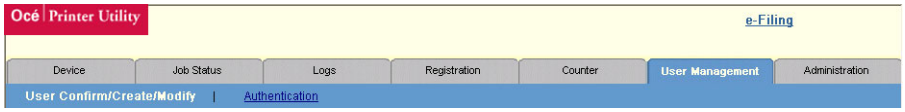


- The counters of selected users are cleared.

Exporting User Information and Counters

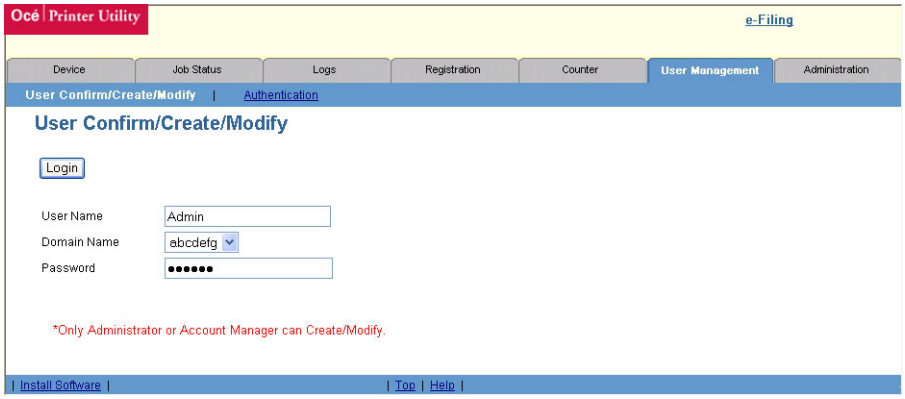
The user information can be exported as a CSV file for use in other equipment.

1 Click the User Management tab.



- The login page is displayed.

2 Enter “Admin” in the “User Name” field, enter the administrator password in the “Password” field, and click [Login].

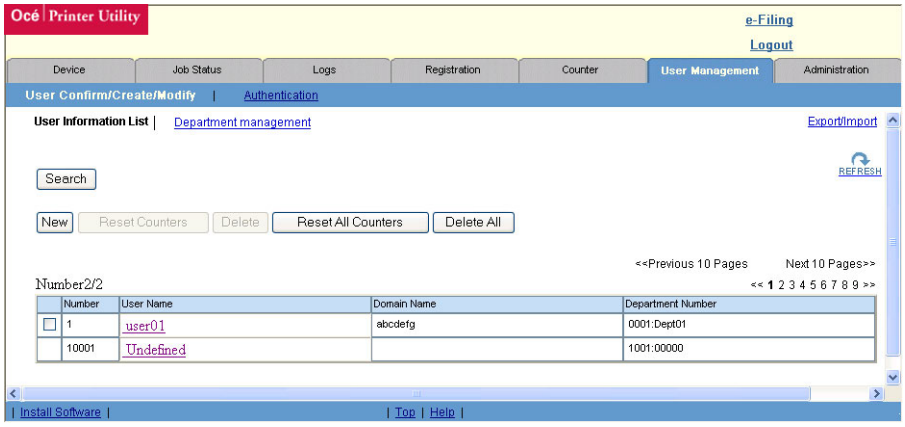


- The User Information List submenu page is displayed.

Tips

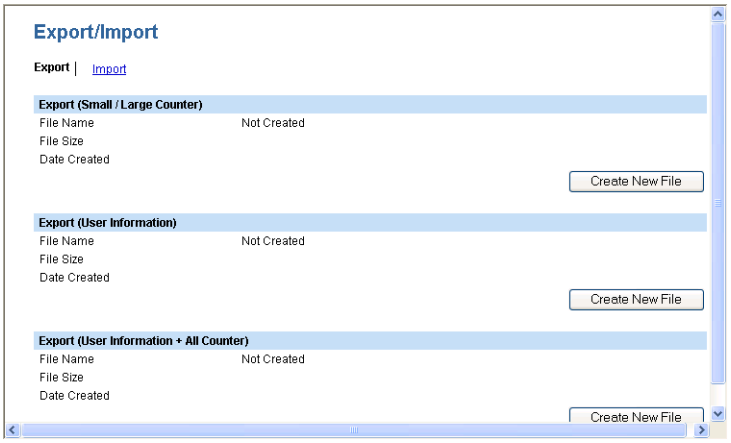
- Users can also login using the user name, domain name (required only when Windows Domain Authentication is enabled), and password that has been set as the Account Manager in the User Information.
- You do not have to select the “Domain Name” field when you log in as the Administrator.

3 Click the “Export/Import” link at the upper right of the page.



- The Export/Import window appears.

4 Click [Create New File] of which you want to export.

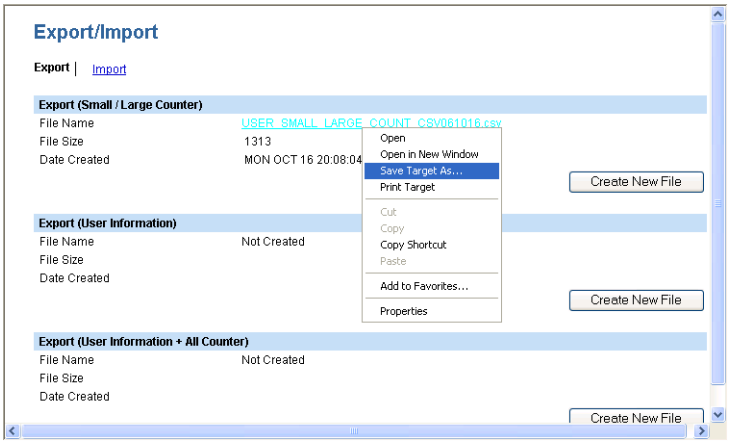


Export (Small/Large Counter) — Click [Create New File] of this area to export the counter information only.
Export (User Information) — Click [Create New File] of this area to export the user information only.
Export (User Information + All Counter) — Click [Create New File] of this area to export the counter information and user information.

Tip

If you previously exported user information data, the exported file link and information are displayed in the page. You can click the link to save the previously exported file.

5 Right-click the File Name link and select [Save Target As...].

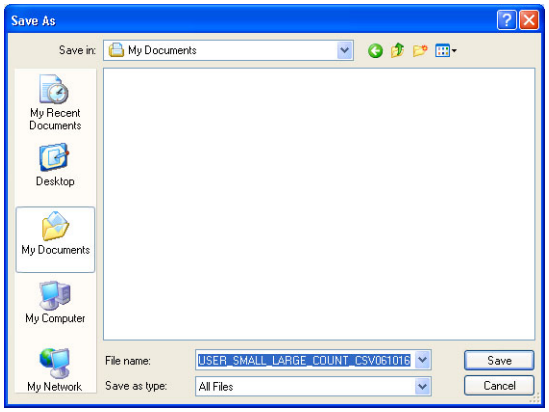


- The Save As dialog box appears.

Note

If the File Name link is not displayed or not updated, close the window and try again. Creating a new file may take a few minutes.

6 Select the file location and select “All Files” in the “Save as type” drop down box. Then click [Save].



- The CSV file that contains the user information data is saved in a selected location.

Importing User Information

You can import user information from a file that has been exported from another device such as cm4531 Series, im8530Series, im4530 Series, and im2830 Series. The imported file must be the comma delimited CSV file and created in the suitable format for the user information data.

Notes

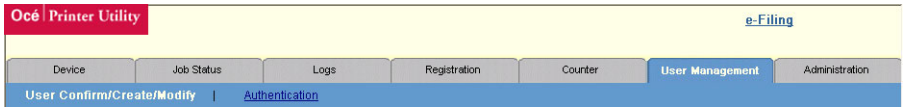
- Before importing the user information data, please confirm that there is no print job, no scan job, and no fax job. The user information data cannot be imported if there are any jobs that have been processed. If importing the user information data takes a long time, perform restoring the data after the equipment turns in a Sleep/Auto Shut Off mode. It may take a long time when there are too many user information or the data includes the too long user name or domain name.
- Before importing the CSV file, please confirm that all required data for each item is entered in the CSV file. The required items vary depending on the authentication type.
  * Yes = Required, No = Not Required

Items	Win-dows Domain	LDAP	Local	Supplements
UserId	Yes	Yes	Yes	
Username	Yes	Yes	Yes	
Password	No	No	Yes	The value must be deleted for Windows Domain or LDAP.
Domainname	Yes	No	No	The value must be deleted for LDAP or Local.
Department Code	Yes	Yes	Yes	
Access Manager	No	No	No	When the value is blank, the value is set to “0”. 0 = Disable, 1 = Enable
Rolebase	No	No	No	When the value is blank, the value is set to “0”. 0 = Disable, 1 = Enable

Items	Windows Domain	LDAP	Local	Supplements
Set Limitation	No	No	No	When the value is blank or invalid value is entered, the value is set to “OFF”.
Maximum reached	No	No	No	

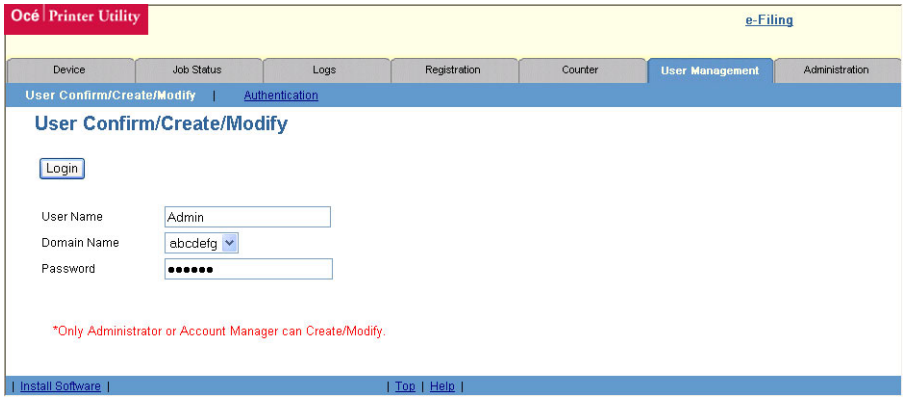
- When user sends a print job while importing the user information, the alert message will be displayed to tell that the equipment cannot receive the print job. When this equipment receives a fax while importing the user information, this equipment cannot start receiving the fax so that it continues ringing.

1 Click the User Management tab.



- The login page is displayed.

2 Enter “Admin” in the “User Name” field, enter the administrator password in the “Password” field, and click [Login].

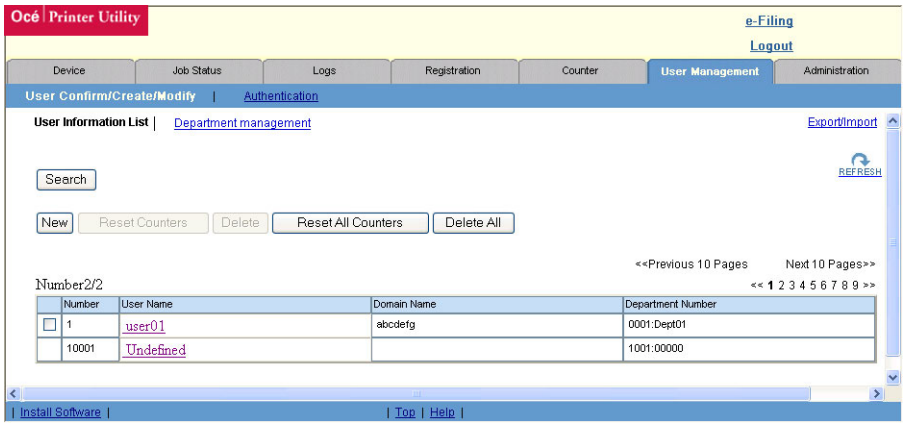


- The User Information List submenu page is displayed.

Tips

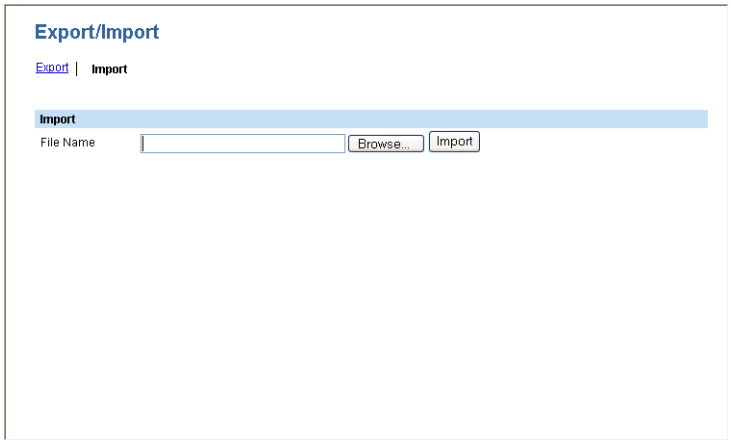
- Users can also login using the user name, domain name (required only when Windows Domain Authentication is enabled), and password that has been set as the Account Manager in the User Information.
- You do not have to select the “Domain Name” field when you log in as the Administrator.

3 Click the “Export/Import” link at the upper right of the page.



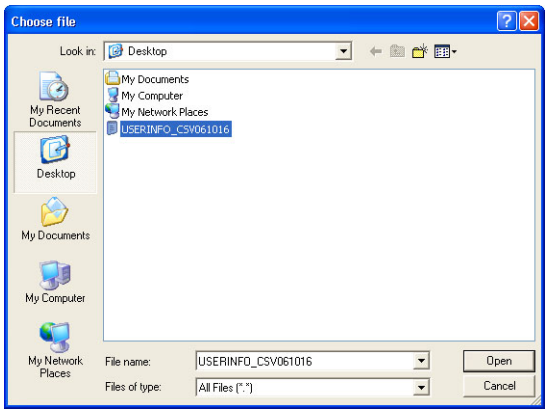
- The Export/Import window appears.

4 Click Import menu and click [Browse...].

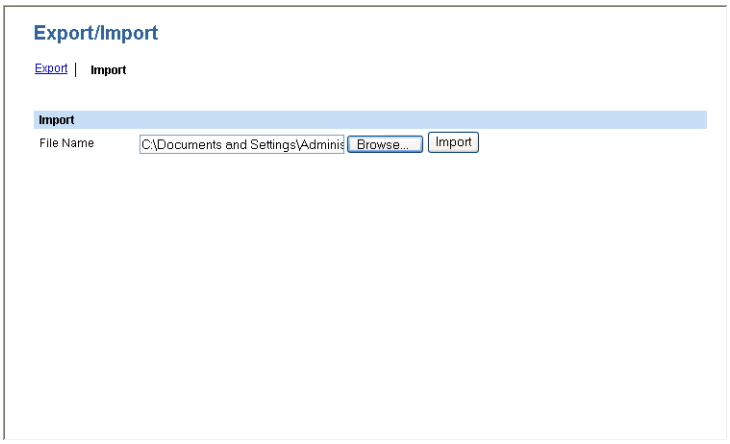


- The Choose file dialog box appears.

5 Select the CSV file that contains user information data and click [Open].



6 Click [Import].

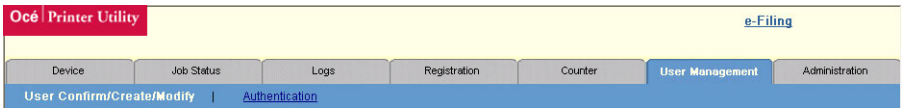


- The data is imported to the User Information list page.

Viewing the own user information by a user

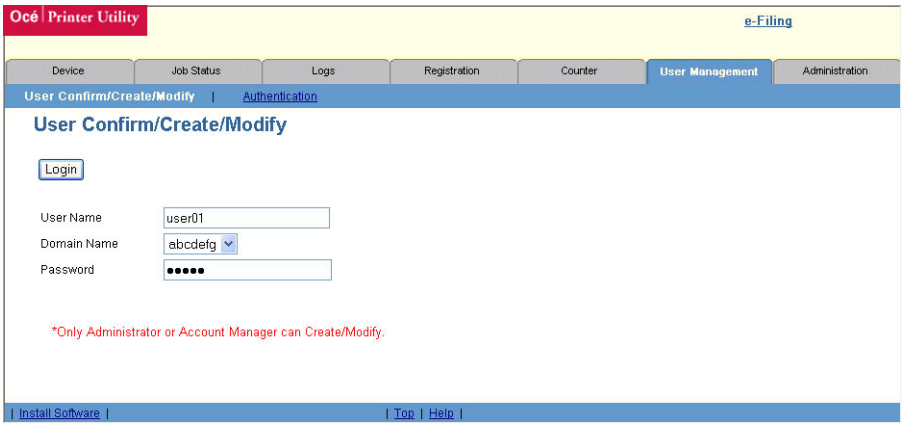
Users can view the own user information by login the User Confirm/Create/Modify page. When the Role Based Access Control is enabled, users can also confirm the functions to be allowed.

1 Click the User Management tab.

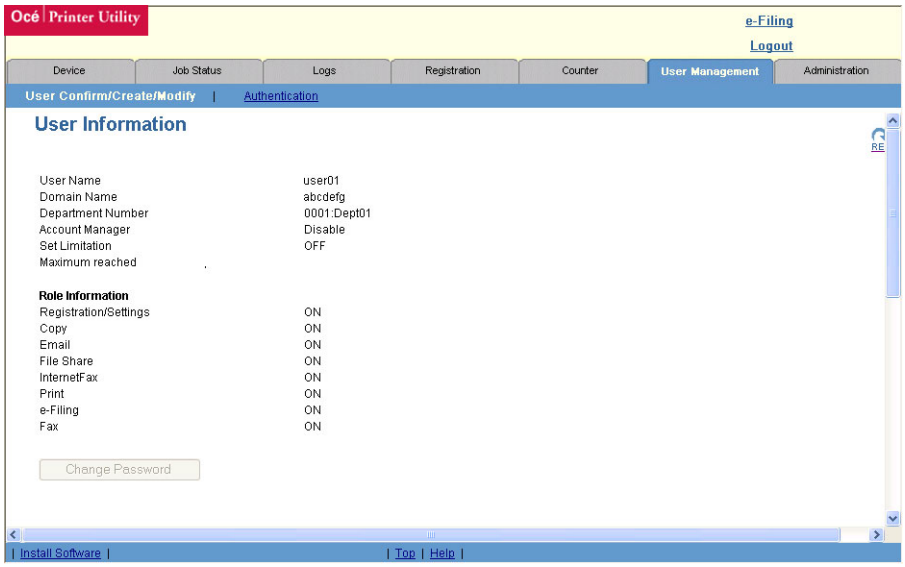


- The login page is displayed.

2 Enter your user name in the “User Name” field, select a domain name (required only when Windows Domain Authentication is enabled), enter the your password in the “Password” field, and click [Login].



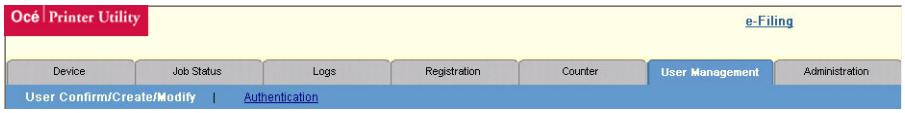
3 **The User Information page is displayed.**



Changing a password by a user (Local MFP Authentication only)

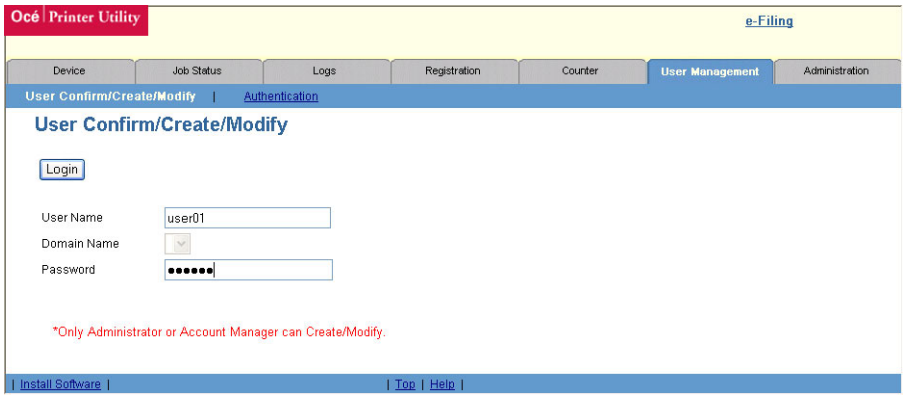
When the Local MFP Authentication is enabled, not only an administrator or account managers but also each registered user can change the password himself.

1 **Click the User Management tab.**



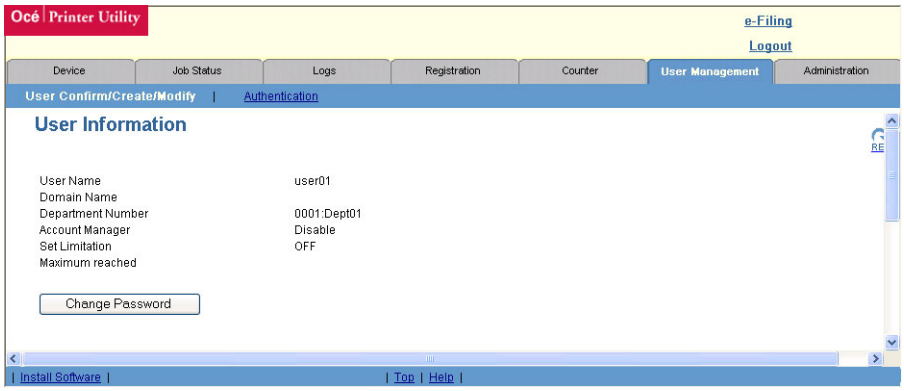
- The login page is displayed.

2 **Enter your user name in the “User Name” field, enter the your password in the “Password” field, and click [Login].**



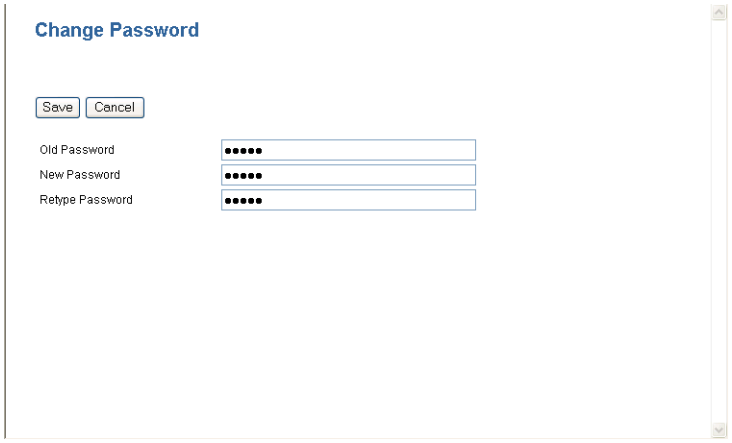
- The User Information page is displayed.

3 Click [Change Password].



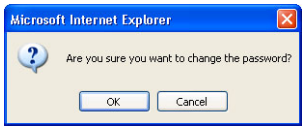
- The Change Password window appears.

4 Enter the following items and click [Save].



Old Password — Enter your login password.
New Password — Enter a new login password. You can enter up to 64 characters.
Retype Password — Enter a new login password again.

5 Click [OK].



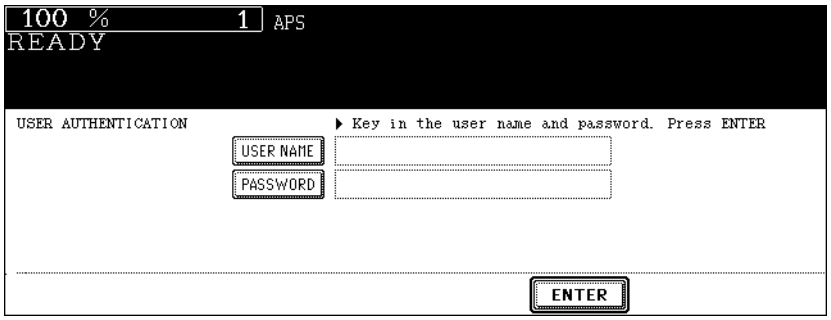
- The password is changed.

How to Login to Touch Panel

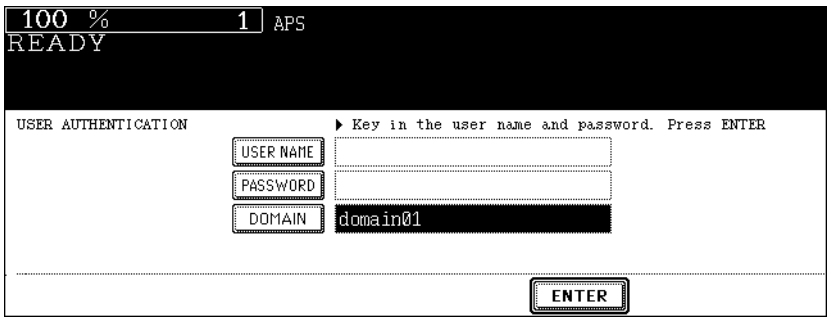
In the user management function, the users of the equipment can be limited or the past record of each user can be managed. When the equipment is managed under this function, turn the power of the equipment ON and enter the information required (e.g. user name, password) to use the equipment. The menu for entering user information also appears when you pressed the [ACCESS] button on the control panel or automatic function clear has worked. Enter the information following the procedure below.

1 The menu for user authentication appears.

MFP local Authentication, LDAP Authentication

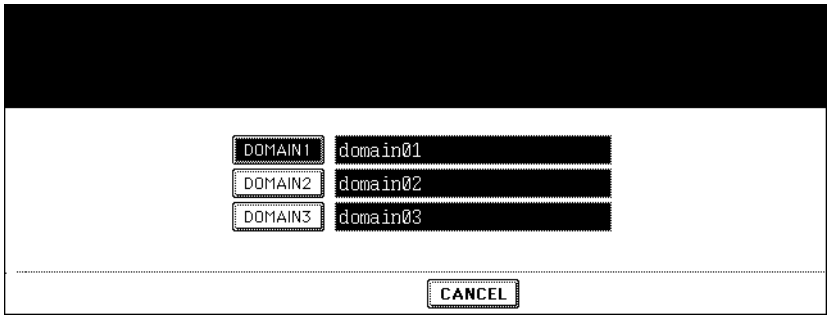


Windows Domain Authentication

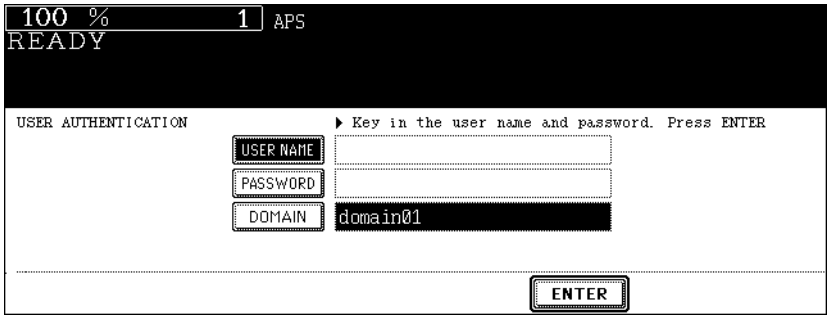


- The domain name previously set by the network administrator is displayed in [DOMAIN].

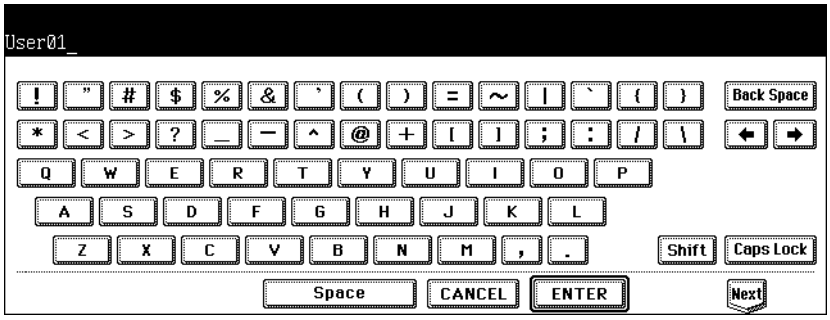
If the preferred domain name is not displayed in [DOMAIN], press the [DOMAIN] button and then select the preferred domain name.



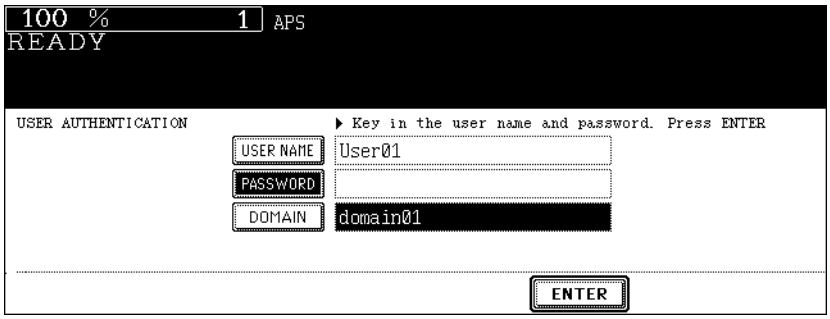
2 Press the [USER NAME] button.



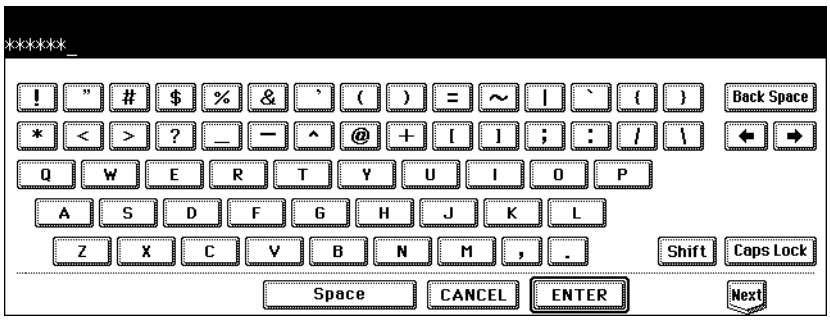
3 **Enter the user name (maximum 128 letters) and then press the [ENTER] button.**



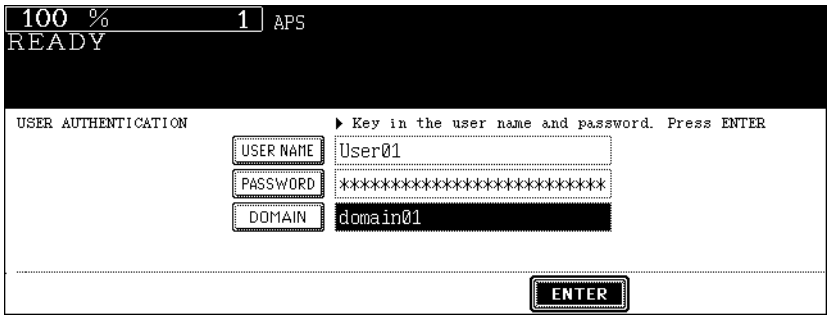
4 **Press the [PASSWORD] button.**



5 **Enter the password (maximum 64 letters) and then press the [ENTER] button.**



6 Press the [ENTER] button.



The menu will switch and the equipment will be ready to be used.

- If the user information is incorrectly entered, the menu will not switch. In this case, press the [FUNCTION CLEAR] button and then enter it again.

Note

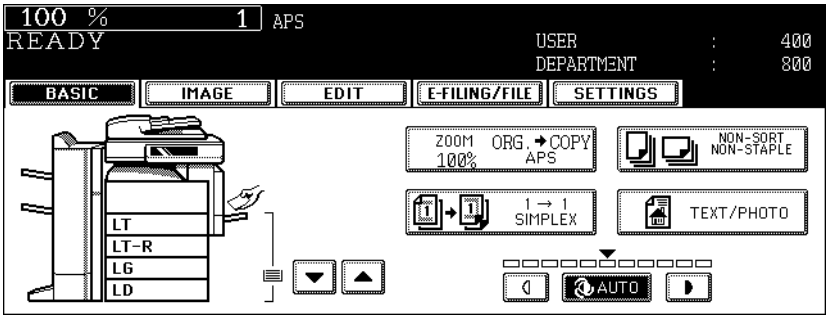
When the Windows Domain or LDAP authentication is used, the Entering the Department Code screen will be displayed if the entered user information is not registered in the equipment. In that case, the user information will be automatically registered when you enter the department code.

Displaying the available number of copies

How many copies the user and the department have remaining is displayed, respectively. The number appears for 5 seconds on the upper right of the screen.

USER: Available number of copies for the user

DEPARTMENT: Available number of copies for the department



Note

The display differs depending on the management setting of this equipment.

When copying is finished

When you finish all operations, press the [ACCESS] button to prevent unauthorized use of the equipment. The display returns to the one for entering user information.

Setting up User Authentication for Scan to E-mail

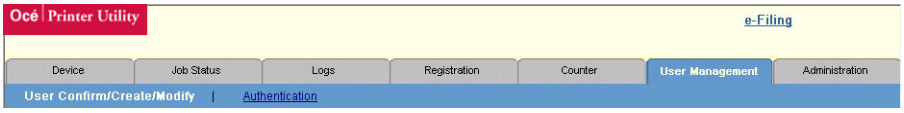
When the User Authentication for Scan to Email is enabled, users must enter the user name and password before performing Scan to E-mail.
You can select either the SMTP or LDAP for User Authentication for Scan to Email.
P.48 “Enabling User Authentication for Scan to Email (SMTP)”
P.50 “Enabling User Authentication for Scan to Email (LDAP)”

Note

When the User Authentication for Scan to Email is enabled, the Email Notification may not be sent to the administrator. Please make sure to set the login name and password in the SMTP Client settings.

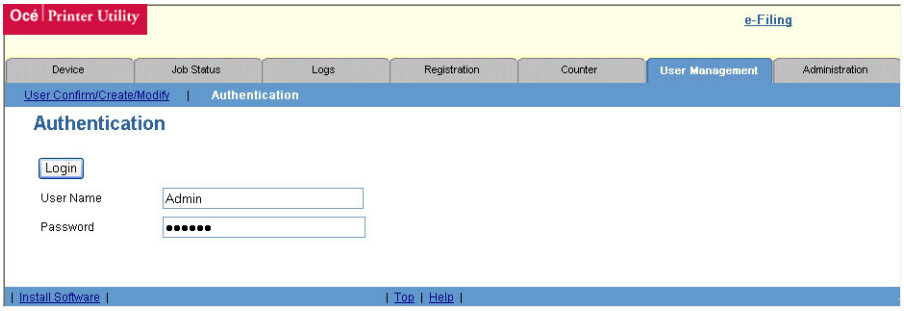
Enabling User Authentication for Scan to Email (SMTP)

1 Click the User Management tab and the Authentication menu.



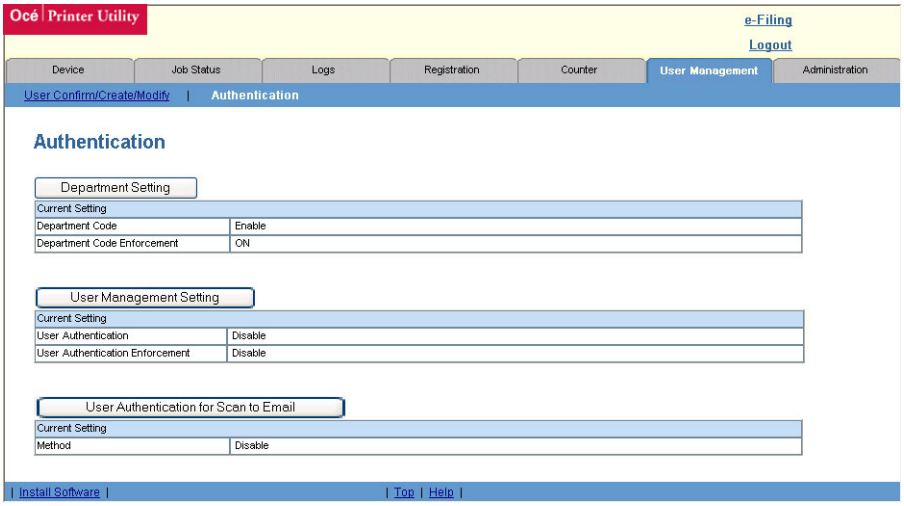
- The login page is displayed.

2 Enter the administrator password and click [Login].



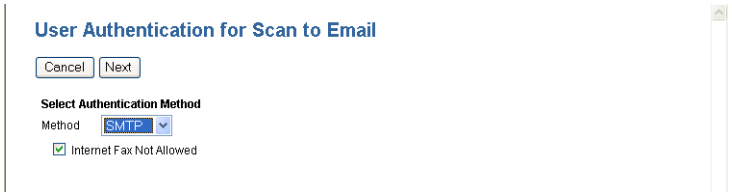
- The Authentication page is displayed.

3 Click [User Authentication for Scan to Email].



- The User Authentication for Scan to Email page opens.

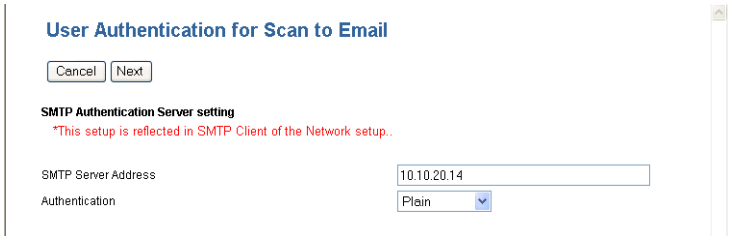
4 Select “SMTP” in the “Method” drop down box and click [Next].



Tips

- This equipment can set the authentication for Scan to Email, but cannot set the authentication for Internet Fax transmission. If you do not want to allow users to perform the Internet Fax transmission, check the “Internet Fax Not Allowed” check box. When you check on this box, users no longer perform the Internet Fax transmission.
- When you want to disable the User Authentication for Scan to Email, select “Disable” in the “Method” and click [Next].

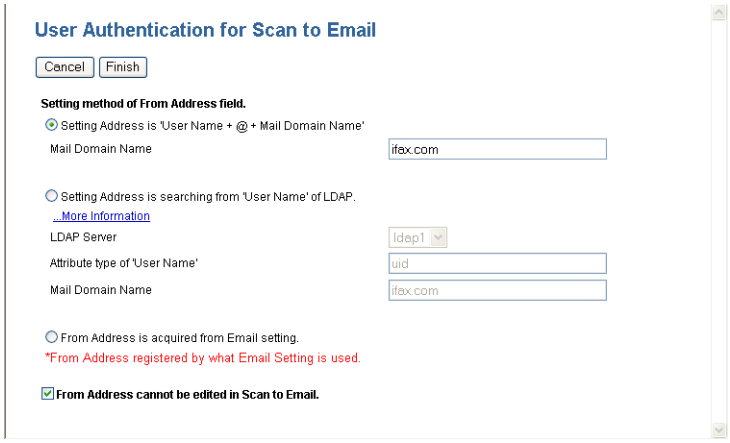
5 Enter the IP address or FQDN (Fully Qualified Domain Name) of the SMTP server and select the authentication type in the “Authentication” drop down box. Then click [Next].



Tip

If you have set the SMTP Client settings in the Network setup page, the setting values of the SMTP Client settings in the Network setup page are reflected in these settings.

6 Specify how the From Address is set for Scan to Email.



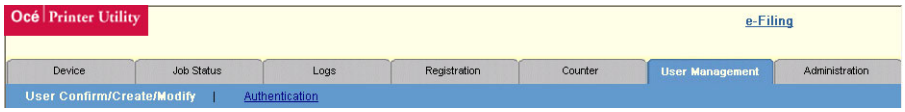
Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field. When this is selected, enter the domain name in the “Mail Domain Name” field.
Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address that is searched from the LDAP server.
When this is selected, this equipment will search the user name, which is entered on the Touch Panel Display for the authentication, from the records of the attribute type in the LDAP server that you specify in the “LDAP Server” drop down box and “Attribute type of ‘User Name’” field.
If the user name is found, this equipment sets the From Address as the email address of the user name registered in the LDAP server.
If the user name is not found in the LDAP server, this equipment sets the From Address as the “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field.
When this is selected, select the LDAP server in the “LDAP Server” drop down box, enter the attribute type to search the user name in the “Attribute type of ‘User Name’” field, and the domain name that is used when the user name is not found in the “Mail Domain Name” field.
From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.
From Address cannot be edited in Scan to Email — Check this box if you do not want to allow users to edit the From Address.

7 Click [Finish].

- The User Authentication for Scan to Email is enabled.

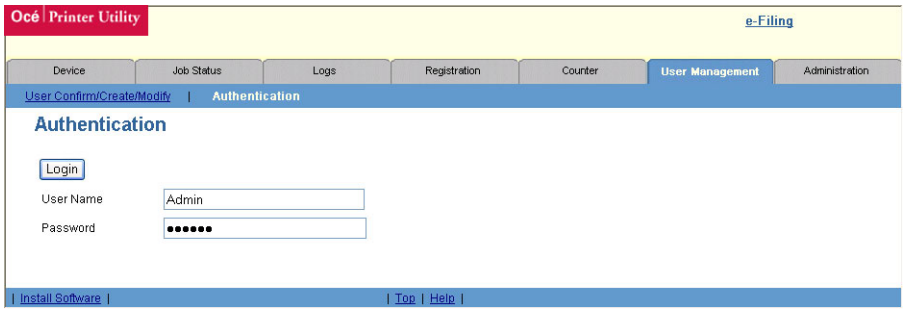
Enabling User Authentication for Scan to Email (LDAP)

1 Click the User Management tab and the Authentication menu.



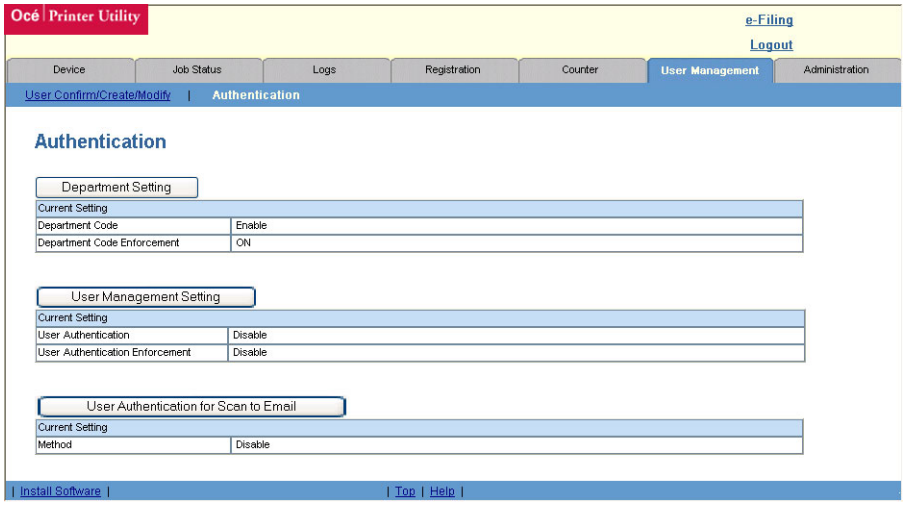
- The login page is displayed.

2 Enter the administrator password and click [Login].



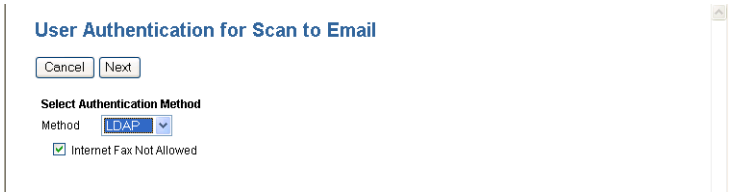
- The Authentication page is displayed.

3 Click [User Authentication for Scan to Email].



- The User Authentication for Scan to Email page opens.

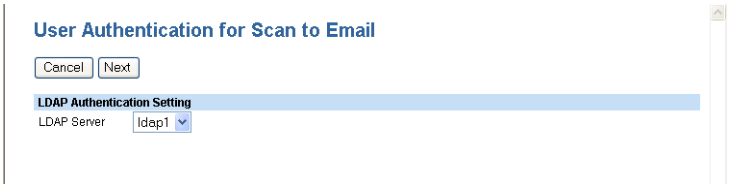
4 Select “LDAP” in the “Method” drop down box and click [Next].



Tips

- This equipment can set the authentication for Scan to Email, but cannot set the authentication for Internet Fax transmission. If you do not want to allow users to perform the Internet Fax transmission, check the “Internet Fax Not Allowed” check box. When you check on this box, users no longer perform the Internet Fax transmission.
- When you want to disable the User Authentication for Scan to Email, select “Disable” in the “Method” and click [Next].

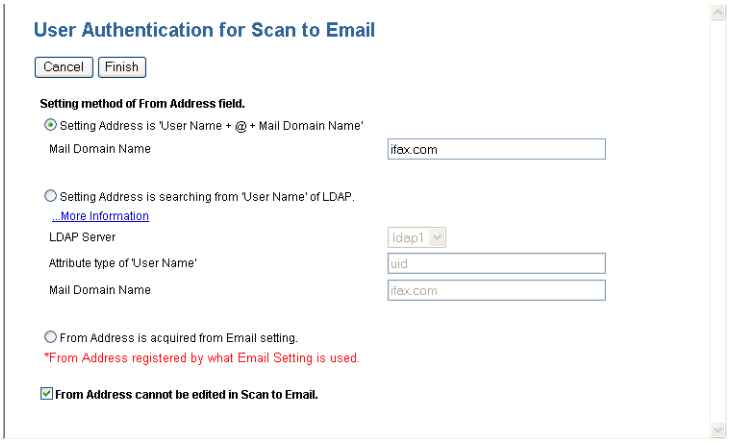
5 Select the LDAP server to be used for the authentication and click [Next].



Tip

The LDAP server to be used for the authentication must be configured in the Directory Service submenu page in the Maintenance menu.

6 Specify how the From Address is set for Scan to Email.



Setting Address is 'User Name + @ + Mail Domain Name' — Select this to set the From Address as “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field. When this is selected, enter the domain name in the “Mail Domain Name” field.

Setting Address is searching from 'User Name' of LDAP — Select this to set the From Address as the email address that is searched from the LDAP server.

When this is selected, this equipment will search the user name, which is entered on the Touch Panel Display for the authentication, from the records of the attribute type in the LDAP server that you specify in the “LDAP Server” drop down box and “Attribute type of ‘User Name’” field.

If the user name is found, this equipment sets the From Address as the email address of the user name registered in the LDAP server.

If the user name is not found in the LDAP server, this equipment sets the From Address as the “User Name@Mail Domain Name”, whose “User Name” is the user name that is entered on the Touch Panel Display for the authentication, and “Mail Domain Name” is the domain name that is entered in the “Mail Domain Name” field.

When this is selected, select the LDAP server in the “LDAP Server” drop down box, enter the attribute type to search the user name in the “Attribute type of ‘User Name’” field, and the domain name that is used when the user name is not found in the “Mail Domain Name” field.

From Address is acquired from Email setting — Select this to set the From Address as the email address set in the Email setting.

From Address cannot be edited in Scan to Email — Check this box if you do not want to allow users to edit the From Address.

7 Click [Finish].

- The User Authentication for Scan to Email is enabled.

INDEX

A

Account Manager 29

B

BDC 19

D

Department Code 13
Department Code Enforcement 14
Department Number 29
Domain Name 19

L

LDAP Authentication 16
LDAP authentication 44

M

Maximum reached 29
MFP Local Authentication 16, 26
MFP local Authentication 44

P

PDC 19

R

Role Based Access 19, 23

S

Set Limitation 29

U

User Authentication Enforcement 18, 22, 26
User Authentication for Scan to Email 48, 51
User Management Setting 17, 21, 25

W

Windows Domain Authentication 16, 44

Printing for Professionals

Océ

100 Oakview Drive, Trumbull, CT 06611

©Océ 2007