OKI

MULTIFUNCTIONAL DIGITAL COLOR SYSTEMS /
MULTIFUNCTIONAL DIGITAL SYSTEMS

Operator's Manual for the Latest Functions

Preface

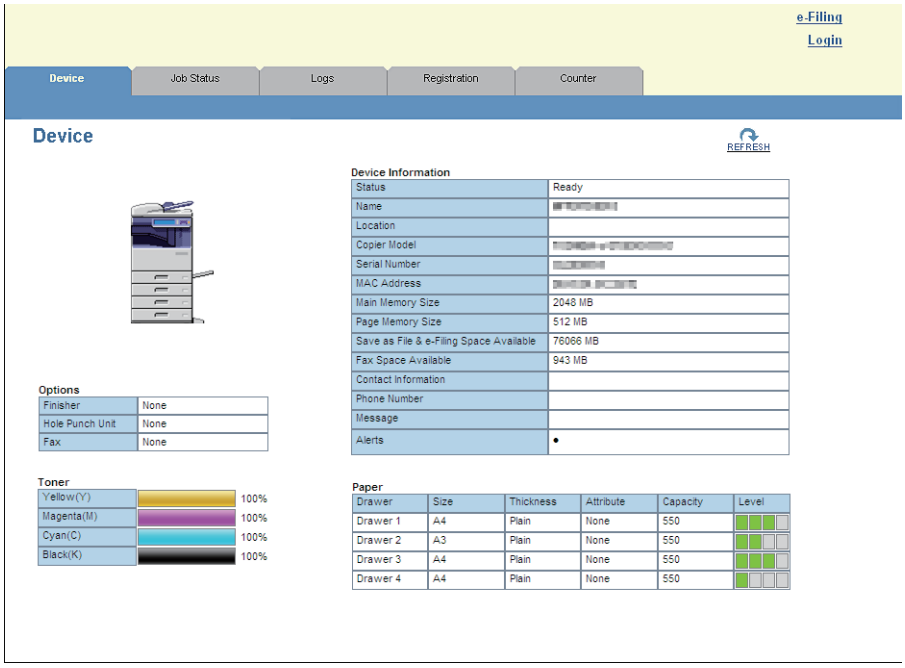
Thank you for purchasing OKI Multifunctional Digital Color Systems.
This manual describes the updated functions.
Read this manual before using your Multifunctional Digital Color Systems. Keep this manual within easy reach, and use it to configure an environment that makes best use of OKI MFP's functions.

■ How to read this manual

Only updated functions and screens for the Top Access Guide are described.
Refer to the corresponding title and page of the TopAccess Guide with this manual for your better understanding.

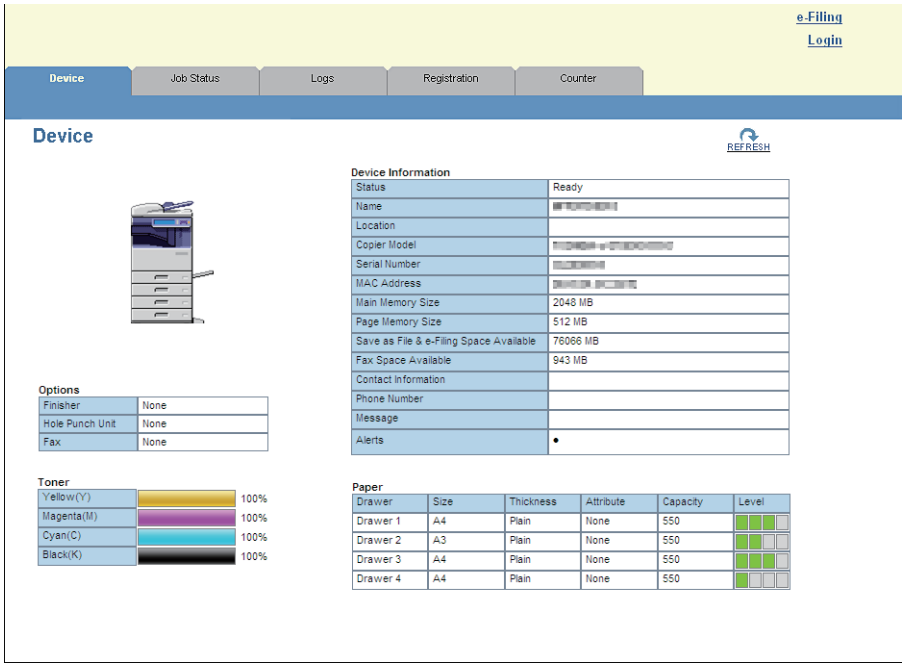
Accessing TopAccess

2 The TopAccess website appears.



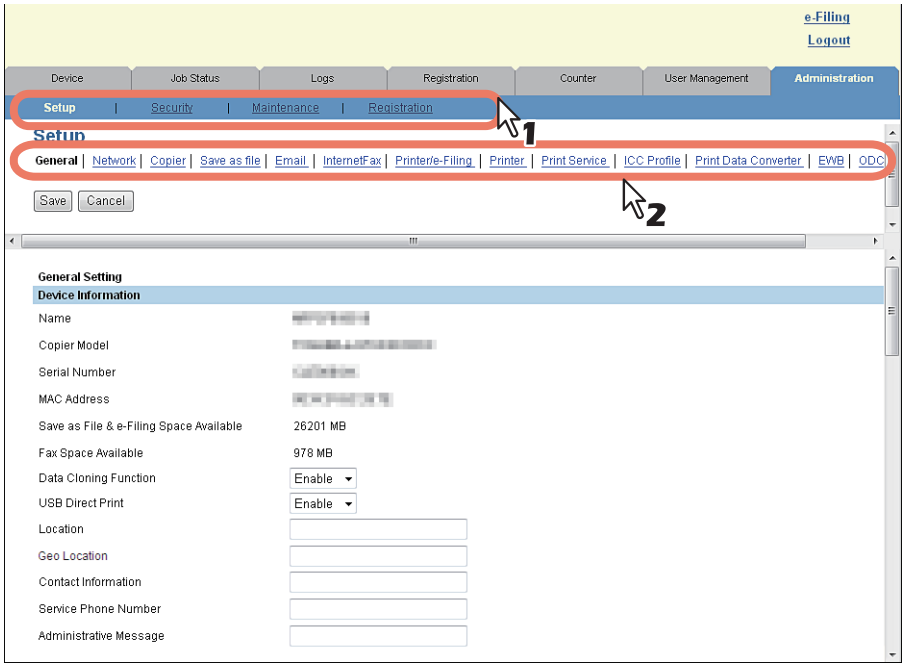
Accessing TopAccess

6 **The TopAccess website appears.**

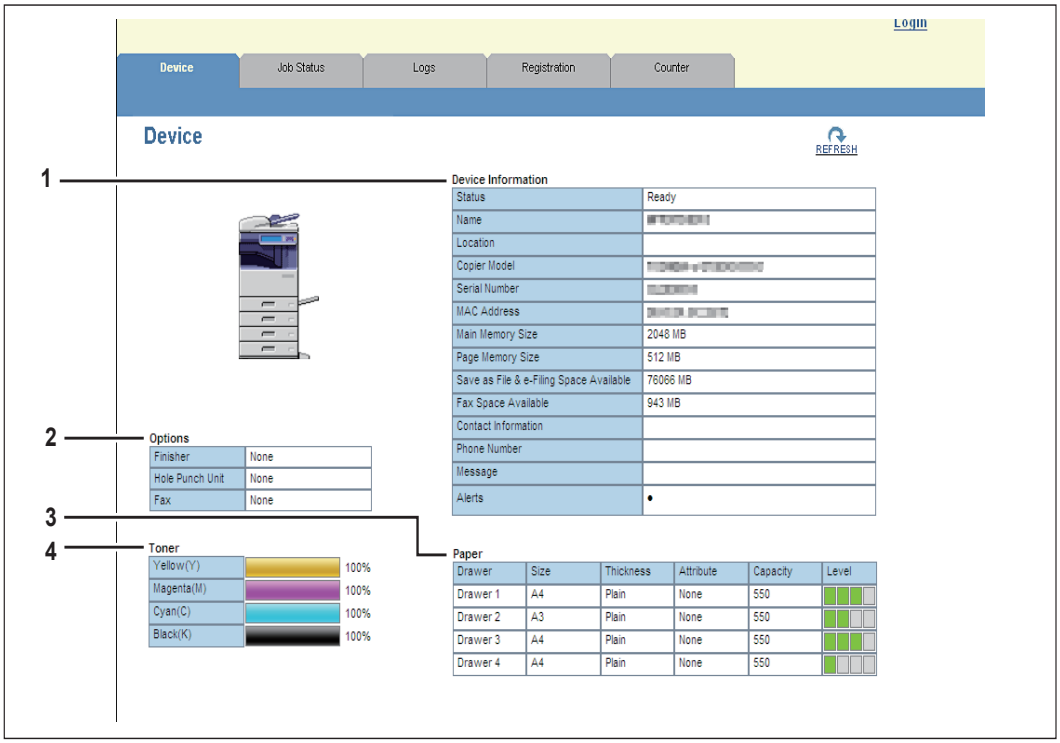


Access Policy Mode

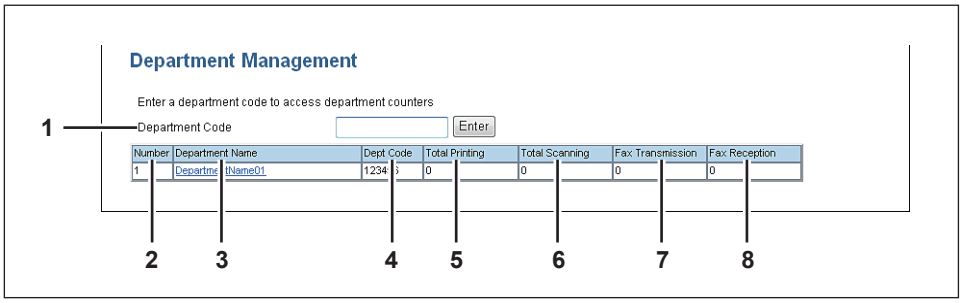
4 **Click the menu and submenu to display the desired page.**



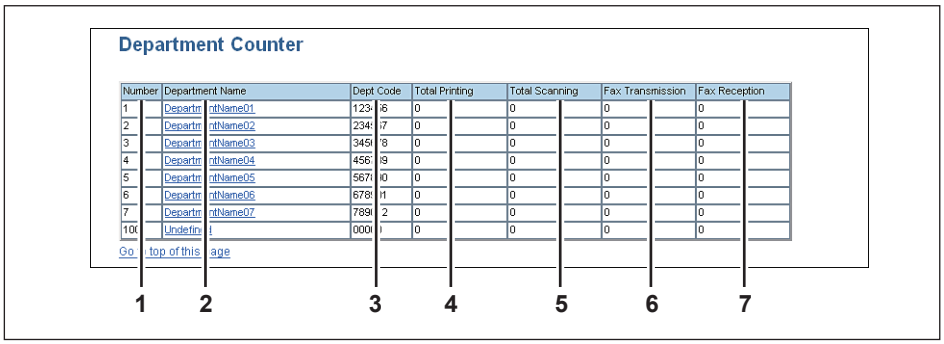
[Device] Item List



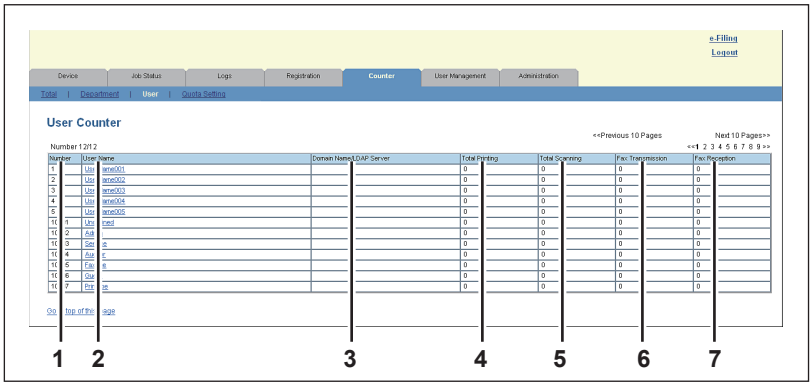
❑ [Department Management] screen



❑ [Department Counter] screen <access policy mode>

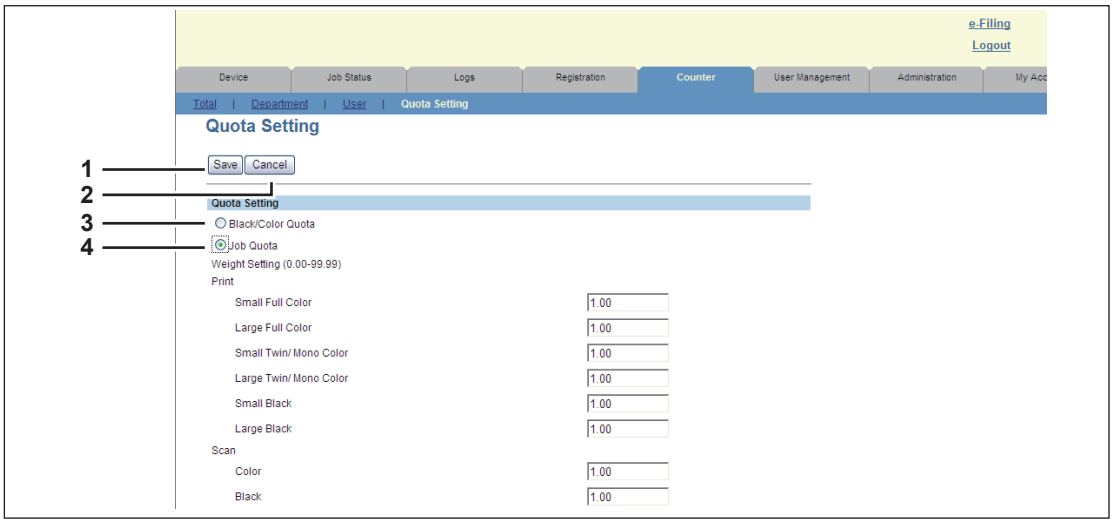


❑ [User Counter] screen <access policy mode>



❑ [Quota Setting] screen <access policy mode>

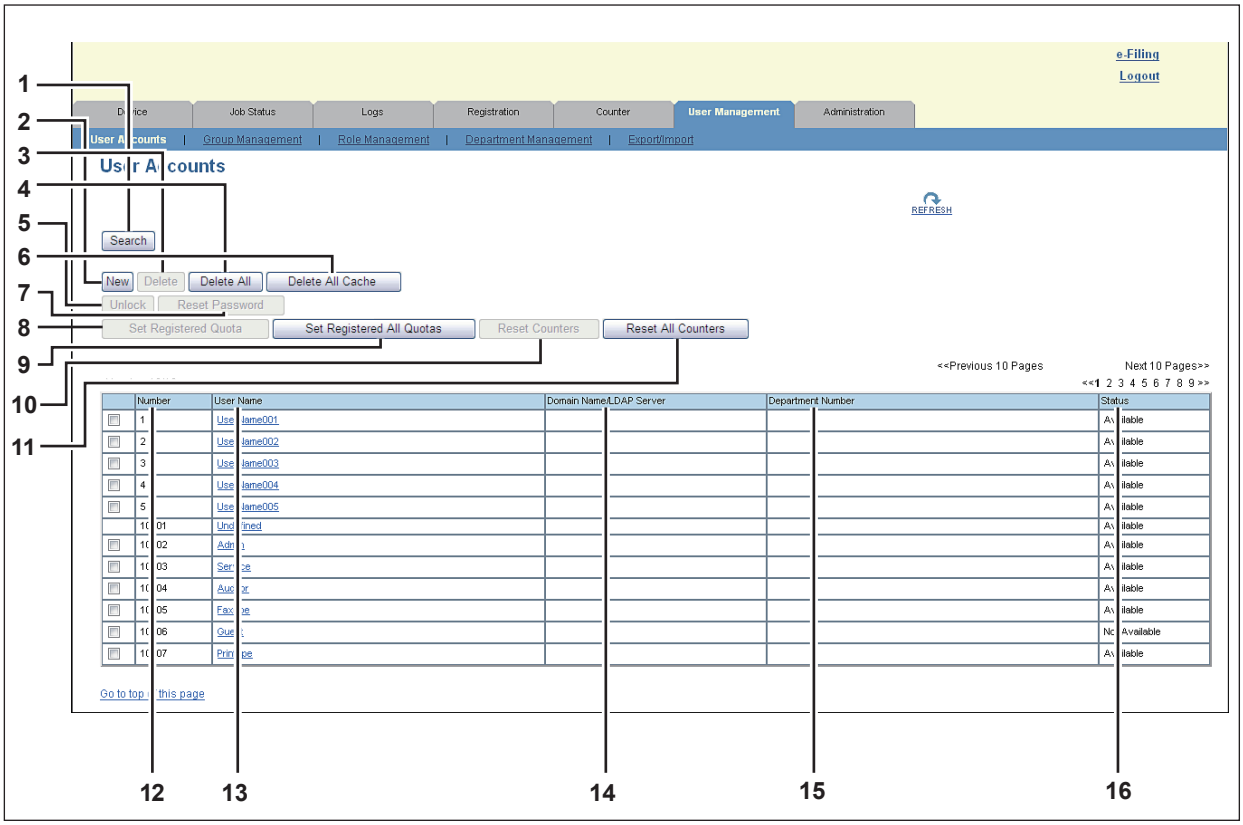
You can make the quota management settings based on either a print count or a job. In job-based quota management, different weights can be assigned to each job when the number of outputs is counted.



	Item name	Description
1	[Save] button	Saves the quota settings.
2	[Cancel] button	Cancels the settings.
3	Black/Color Quota	Performs quota management based on the number of black and color outputs.
4	Job Quota	Assigns weights to each job and calculates the sum total quotas of the print jobs and scan jobs for quota management. Different weights can be assigned to each of the jobs listed below. • Print - Small Full Color - Large Full Color - Small Twin/Mono Color - Large Twin/Mono Color - Small Black - Large Black • Scan - Color - Black
	Tip When assigning a weight to a job, you can enter a value in the range from 0.00 to 99.99. The default value is “1.00”. For example, assuming that a weight assigned to Small Black in Print is 0.50, if the user makes 2 outputs in Small Black, the quota value assigned to the user is decremented by 1.00.	

[User Management] Tab Page Overview

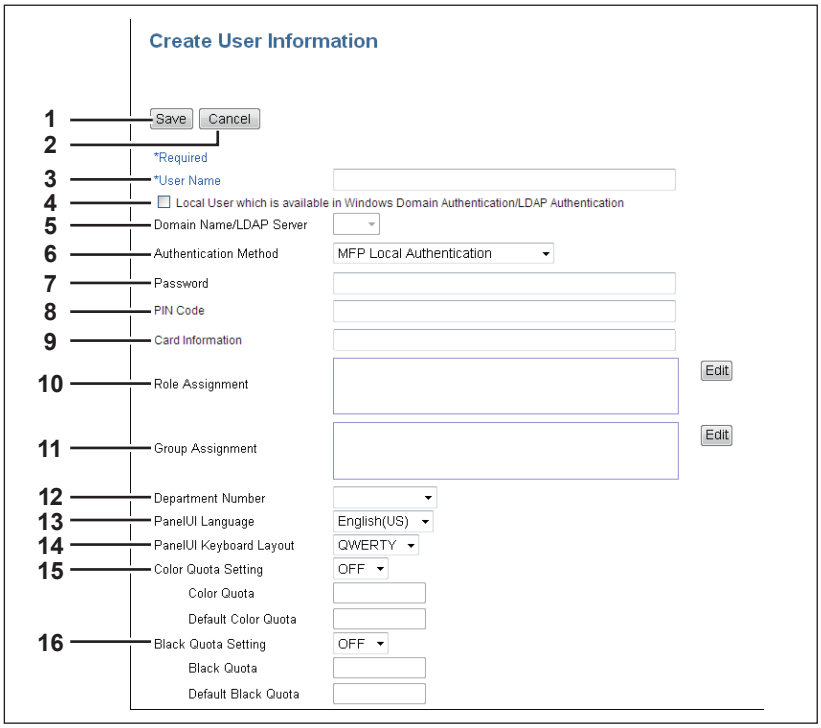
■ [User Accounts] Item list <access policy mode>



	Item name	Description
6	[Delete All Cache] button	Select this to delete all the authentication information to be used when an authentication server failure occurs.
7	[Reset Password] button	Resets the password of the user selected in the user account list. 📖 P.123 “[Enter Password] screen”
8	[Set Registered Quota] button	Initializes the registered quota for the user selected in the user account list.
9	[Set Registered All Quotas] button	Initializes all registered quotas.
10	[Reset Counters] button	Resets counters for the user selected in the user account list.
11	[Reset All Counters] button	Resets counters for all departments.

	Item name	Description
12	Number	Displays the registration number of the user. 10001 to 10007 are assigned to default users.
13	User Name	Displays the user name. Undefined, Admin, Service, Auditor, Faxope, Guest, and Printope are default users. You can check the user information by clicking the user name. 📖 P.124 “[User Information] screen”
14	Domain Name/LDAP Server	Displays the domain name or LDAP server registered in the user information.
15	Department Number	Displays the department number registered in the user information.
16	Status	Displays the user status.

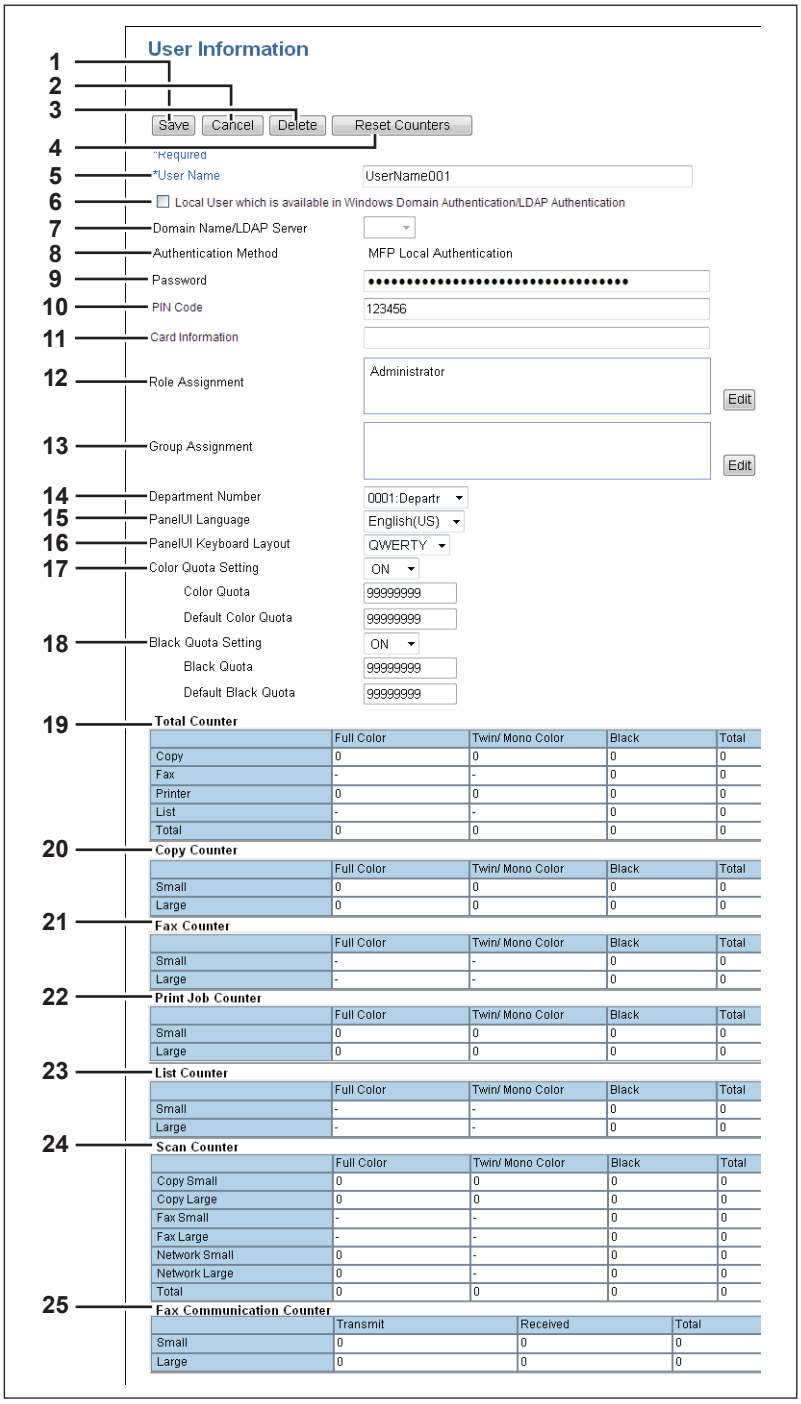
❑ [Create User Information] screen



	Item name	Description
1	[Save] button	Saves the entered user information.
2	[Cancel] button	Cancels creating user information.
3	User Name	Enter the user name. You can enter up to 128 alphanumerical characters and symbols.
4	Local User which is available in Windows Domain Authentication/ LDAP Authentication	Select this to register as a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication.
	Tip The above setting is available only when the [Local User which is available in Windows Domain Authentication/LDAP Authentication] checkbox is selected. 🕮 P.265 “Windows Domain Authentication” 🕮 P.266 “LDAP Authentication”	
5	Domain Name/LDAP Server	Select the domain name or LDAP server.
6	Authentication Method	Select the user authentication method. • **MFP Local Authentication** — Use MFP local authentication on your equipment. • **Windows Domain Authentication** — Use network authentication managed by the Windows domain. • **LDAP Authentication** — Use network authentication managed by LDAP.
7	Password	Enter the password. You can enter up to 64 alphanumerical characters and symbols (! # ( ) * + , - . / : ; = ? @ ? ^ _ ` { | } ~ space).
8	PIN Code	Enter the PIN code for the user authentication.
	Notes • The PIN code is up to 32 figures (0 - 9) long. The minimum length is specified on [User Authentication Setting]. 🕮 P.264 “Setting up User Authentication Setting” • If you change any settings, the changes will be reflected from the next time you log in. • When you use the PIN code for the Windows domain authentication or LDAP authentication, the unique PIN code should be assigned for all users.	
9	Card Information	Enter the information necessary for card authentication.

	Item name	Description
10	Role Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Select from the registered roles. Click the [Edit] button and select roles from the displayed screen. 📖 P.126 “[Role Assignment] screen”
11	Group Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Select from the registered groups. Click the [Edit] button and select groups from the displayed screen. 📖 P.126 “[Group Assignment] screen”
12	Department Number	Select from the registered departments. 📖 P.135 “[Department Management] Item list <access policy mode>”
13	PanelUI Language	Select the display language for the touch panel.
14	PanelUI Keyboard Layout	Select the keyboard pattern displayed on the touch panel.
15	Color Quota Setting	• **OFF** — No color output restriction. • **ON** — Restricts color output.
	Color Quota	Displays the remaining number for color output. The number entered in [Default Color Quota] decreases each time a color page is printed, and color output is prohibited when it reaches 0. You can manually change the remaining number of outputs to a desired value.
	Default Color Quota	Enter the default number assigned for the user. Up to 99,999,999 can be entered.
16	Black Quota Setting	• **OFF** — No monochrome output restriction. • **ON** — Restricts monochrome output.
	Black Quota	Displays the remaining number for monochrome output. The number entered in [Default Black Quota] decreases each time a monochrome page is printed, and monochrome output is prohibited when it reaches 0. You can manually change the remaining number of outputs to a desired value.
	Default Black Quota	Enter the default number assigned for the user. Up to 99,999,999 can be entered.

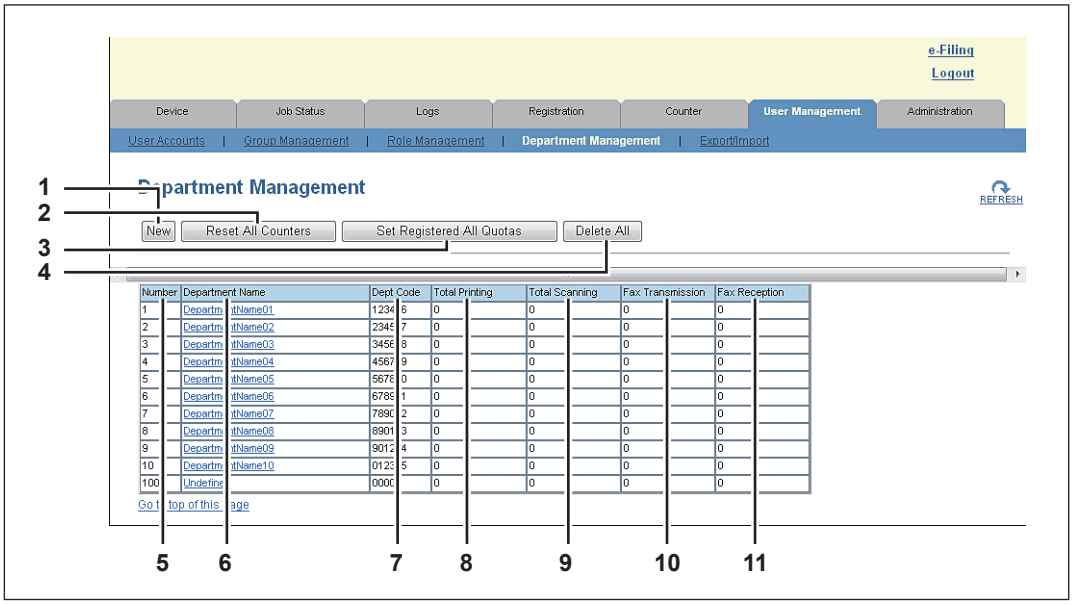
❑ [User Information] screen



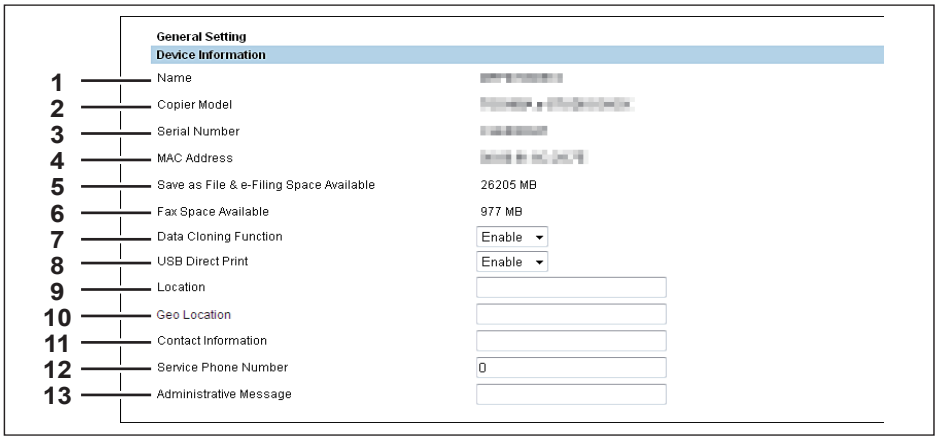
	Item name	Description
6	Local User which is available in Windows Domain Authentication/ LDAP Authentication	Select this to register as a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication.
	Note The above setting is available only when the [Local User which is available in Windows Domain Authentication/LDAP Authentication] checkbox is selected. 📖 P.265 “Windows Domain Authentication” 📖 P.266 “LDAP Authentication”	
7	Domain Name/LDAP Server	Displays the registered domain name or LDAP server. Select this item if you want to change. You can select this item only when the authentication method is [Windows Domain Authentication] or [LDAP Authentication].
8	Authentication Method	Displays the user authentication method. • **MFP Local Authentication** — Use MFP local authentication on your equipment. • **Windows Domain Authentication** — Use network authentication managed by the Windows domain. • **LDAP Authentication** — Use network authentication managed by LDAP.
9	Password	You can change the password only when the authentication method is [MFP Local Authentication].
	Note If you change any settings, the changes will be reflected from the next time you log in.	
10	PIN Code	Displays the PIN code for the user authentication. You can set this item only when the authentication method is [MFP Local Authentication].
	Notes • The PIN code is up to 32 figures (0 - 9) long. The minimum length is specified on [User Authentication Setting]. 📖 P.264 “Setting up User Authentication Setting” • If you change any settings, the changes will be reflected from the next time you log in. • When you use the PIN code for the Windows domain authentication or LDAP authentication, the unique PIN code should be assigned for all users.	
11	Card Information	Enter the information necessary for card authentication.
12	Role Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Displays the registered roles. Click the [Edit] button and select roles from the displayed screen. 📖 P.126 “[Role Assignment] screen”
	Note If you change any settings, the changes will be reflected from the next time you log in.	
13	Group Assignment	This can be configured when [MFP Local Authentication] is selected in [Authentication Method]. Displays the registered groups. Click the [Edit] button and select groups from the displayed screen. 📖 P.126 “[Group Assignment] screen”
	Note If you change any settings, the changes will be reflected from the next time you log in.	
14	Department Number	Displays the registered departments. Select this item if you want to change. 📖 P.135 “[Department Management] Item list <access policy mode>”
15	PanelUI Language	Displays the registered display languages of the touch panel. Select this item if you want to change.
16	PanelUI Keyboard Layout	Displays the registered keyboard patterns for the touch panel. Select this item if you want to change.
17	Color Quota Setting	• **OFF** — No color output restriction. • **ON** — Restricts color output.
	Color Quota	Displays the remaining number for color output. The number entered in [Default Color Quota] decreases each time a color page is printed, and color output is prohibited when it reaches 0. You can manually change the remaining number of outputs to a desired value.
	Default Color Quota	Enter the default number assigned for the user. Up to 99,999,999 can be entered.

	Item name		Description
18	Black Quota Setting		• **OFF** — No monochrome output restriction. • **ON** — Restricts monochrome output.
		Black Quota	Displays the remaining number for monochrome output. The number entered in [Default Black Quota] decreases each time a monochrome page is printed, and monochrome output is prohibited when it reaches 0. You can manually change the remaining number of outputs to a desired value.
		Default Black Quota	Enter the default number assigned for the user. Up to 99,999,999 can be entered.
19	Total Counter		Displays the total counter.
20	Copy Counter		Displays the number of pages printed by copy operations.
21	Fax Counter		Displays the number of pages printed by fax reception.
22	Print Job Counter		Displays the number of pages printed by print operations and E-mail reception (Internet Fax reception).
23	List Counter		Displays the number of pages printed by system page print operations.
24	Scan Counter		Displays the number of pages scanned by scan operations.
25	Fax Communication Counter		Displays the communication record.

■ [Department Management] Item list <access policy mode>

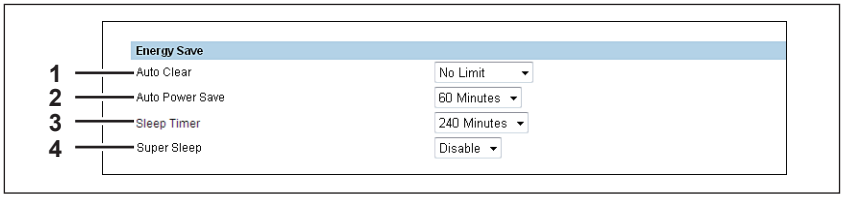


❑ Setting up Device Information



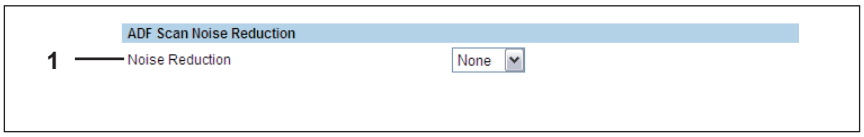
Item name		Description
10	Geo Location	Enter the latitude and longitude in that order with a comma between them. Enter the precise values if required. Up to 64 characters can be entered including ! $ % & ' ( ) * : + ; [, - =] . ~. (e.g. geo:00.00,90.00)
11	Contact Information	Enter the name of the person who is responsible for this equipment. This is displayed in the [Device] tab page that appears first when accessing the TopAccess website for users.
12	Service Phone Number	Enter the telephone number of the person who is responsible for servicing this equipment. This is displayed in the [Device] tab page that appears first when accessing the TopAccess website for users.
13	Administrative Message	Enter the message to the users about this equipment. This is displayed in the [Device] tab page that appears first when accessing the TopAccess website for users.

❑ Setting up Energy Save



	Item name	Description
3	Sleep Timer	Select how long your equipment can remain inactive before being entering Sleep mode.

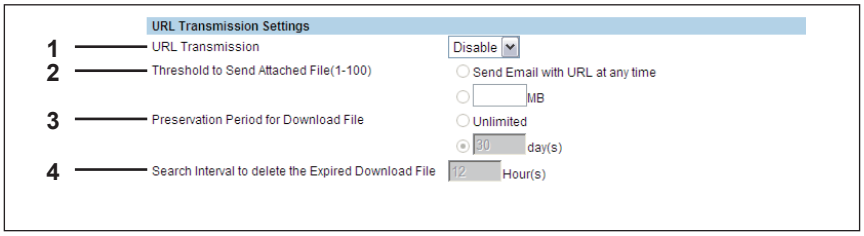
❑ Setting up ADF Scan Noise Reduction



	Item name	Description
1	Noise Reduction	Use this setting if streaks are conspicuous on images when originals are scanned with the Reversing Automatic Document Feeder. • **None** — Select this not to perform noise reduction. • **Low/Middle/High** — Select this to specify the noise reduction level. [High] is the most effective.
	Note Colored characters become faint if the noise reduction level is set to [High].	

❑ Setting up URL Transmission Settings

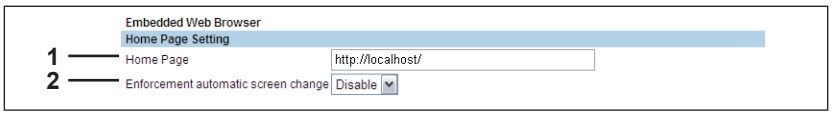
You can set to provide a URL (link) to the saving directory of the file instead of attaching it before sending a scanned image by email. This function is available only if the hard disk is installed.



	Item name	Description
1	URL Transmission	Select whether to enable or disable the function to provide a URL to the saving directory of the scanned data. • **Enable** — Provides a URL to the saving directory. • **Disable** — Sends the data as attachments.
	Tips • The scanned data is stored in MFP Local. • If a URL to the saving directory is provided, its link and the preservation period are stated in the email.	
2	Threshold to Send Attached File (1-100)	Select the maximum size of an attached file. The allowable range is between 1 MB and 100 MB. Select [Send Email with URL at any time] if you want to provide a URL to the saving directory of the file, regardless of the file size. If a maximum size is specified, any file whose size is smaller than the specified one is attached to an email message. On the other hand, if a file exceeds the specified maximum size, a URL to the saving directory is provided.
3	Preservation Period for Download File	Select the preservation period of the file if a URL to the saving directory is provided. If you do not want to impose any limits on the preservation period, select [Unlimited]. If you prefer to automatically delete download files regularly, select a period until the data is deleted.
	Tip If the data cannot be stored in MFP Local because it is full, this results in an error. Delete the stored files regularly. If you want to delete them manually, all scanned data in the shared folder is deleted. 📖 P.310 “Deleting the data from local folder”	
4	Search Interval to delete the Expired Download File	Selects the interval of monitoring the expiration of the specified preservation period.

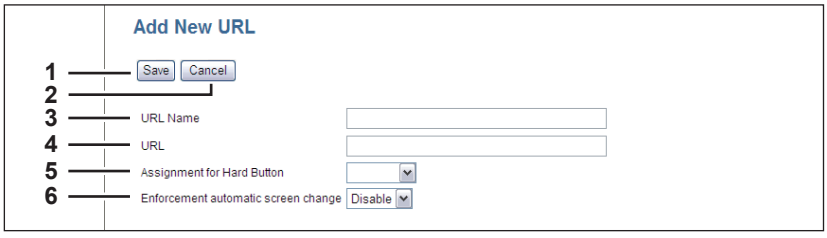
■ Embedded Web Browser settings

❑ Setting up Home Page Setting



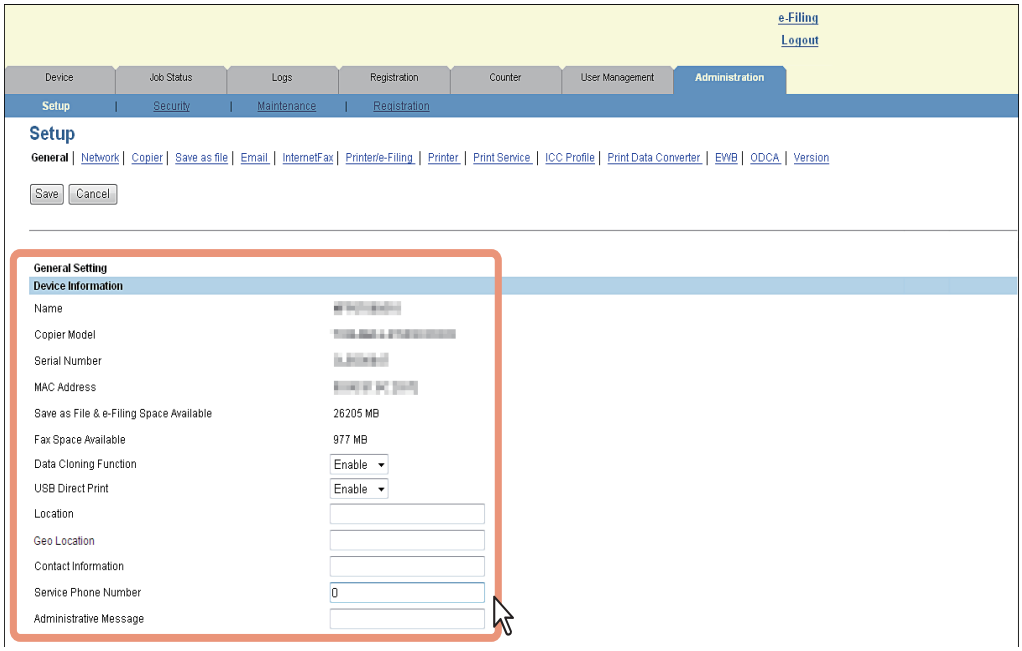
	Item name	Description
2	Enforcement automatic screen change	Specify whether or not the screen is automatically changed to [JOB STATUS] when a job cannot be performed due to paper empty or toner empty, etc. while the EBW screen is displayed. • **Enable** — Select this to change the screen to [JOB STATUS]. • **Disable** — Select this not to change the screen.

❑ [Add New URL] screen

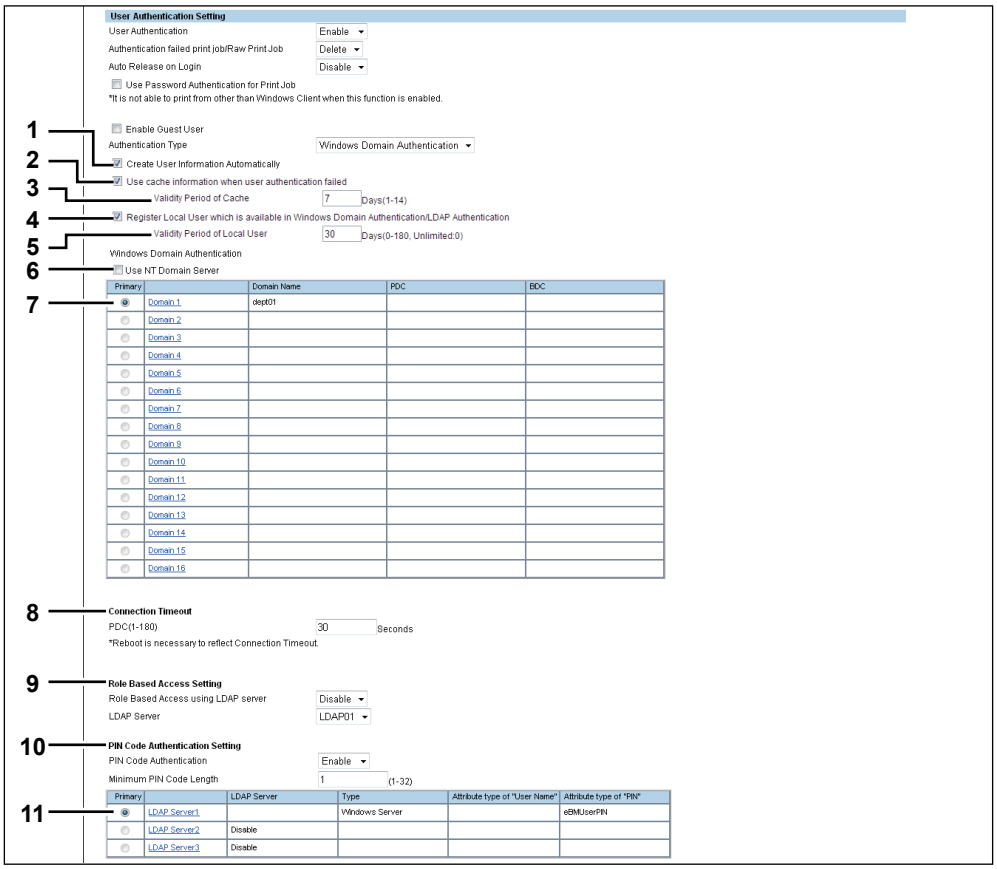


	Item name	Description
6	Enforcement automatic screen change	Specify whether or not the screen is automatically changed to [JOB STATUS] when a job cannot be performed due to paper empty or toner empty, etc. while the EBW screen is displayed.

4 In the General submenu page, set the General settings as required.



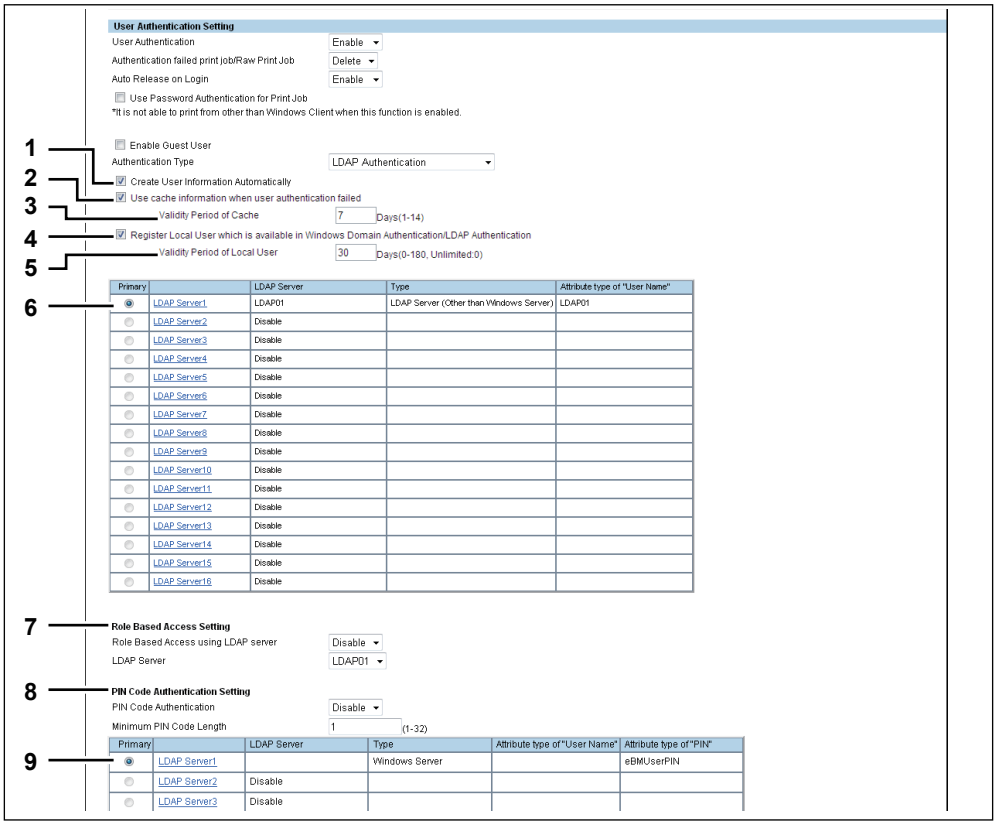
Windows Domain Authentication



	Item name	Description
2	Use cache information when user authentication failed	Either of the following data is saved according to the authentication method. Password, Card number, Domain name, PIN code, HomeDirectry information or RBAC information.
	Tip The cache information will be updated if user authentication succeeds with the authentication server. However, if a user is authenticated with the cache information, it is not updated.	
3	Validity Period of Cache	Enter the number of days to maintain the cache information. 1 to 14 days can be set from the latest update.
4	Register Local User which is available in Windows Domain Authentication/LDAP Authentication	Select this to register a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication.
5	Validity Period of Local User	Enter the number of valid days for local users. Up to 180 days can be set from the user creation day. If 0 is set, the number of valid days will be indefinite.
6	Use NT Domain Server	Select this check box if you are managing the domain using the NT domain controller.
7	Domain 1 - Domain 16	Specify the domain you want to use for Windows domain authentication. Click one of the domains and specify the following items in the displayed screen to register the domain. **Domain Name** — Enter the domain name. **PDC** — Enter the server name or IP address of the Primary Domain Controller (PDC). You can enter up to 128 alphanumerical characters and symbols. **BDC** — Enter the server name or IP address of the Backup Domain Controller (BDC) as required. You can enter up to 128 alphanumerical characters and symbols.
	Note If the wrong primary or backup domain controller is specified, the [OK] 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.	

	Item name	Description
8	Connection Timeout	Enter the timeout period for quitting communication when no response is received from the PDC or BDC server. Specify within the range from 1 to 180 seconds.
9	Role Based Access Setting	Configure role based access using an LDAP server. **Role Based Access using LDAP server** — Select whether enable or disable role based access. [Disable] is set as the default. **LDAP Server** — Select the LDAP server that manages the Role Based Access Control.
10	PIN Code Authentication Setting	**PIN Code Authentication** — Select the PIN code authentication method. • **Disable** — Select this no to use the PIN code authentication. Use the user name and password for authentication. • **Enable** — Select this to use the PIN code authentication. Instead of the PIN code, it is possible to use the user name and password for authentication. **Minimum PIN Code Length** — Enter a figure that specifies the minimum digits for the PIN code.
11	LDAP Server1 - LDAP Server3	Set the following items for LDAP Server1 when you use the PIN Code authentication: **Windows Server** — Select this when LDAP is running on a Windows server. **LDAP Server (Other than Windows Server)** — Select this when the LDAP is running on a server other than a Windows one. **Attribute type of "User Name"** — Enter the attribute type of “User Name” for “LDAP Server (Other than Windows Server)”. **Attribute type of "PIN"** — Enter the attribute type of “PIN” for the PIN code authentication. When you use more than one LDAP server, select LDAP Server2 and/or LDAP Server3 and set up the LDAP server as necessary. See the settings for LDAP Server1.
	Tip If [Windows Server] is selected as an LDAP server for the PIN code or IC card authentication with [Create User Information Automatically] enabled, the following attribute type of user name is used. - If Kerberos is selected to access the LDAP server: sAMAccountName - If Digest-MD5, CRAM-MD5, Login, Plain or Simple Bind is selected to access the LDAP server: displayName	

LDAP Authentication



	Item name	Description
2	Use cache information when user authentication failed	Either of the following data is saved according to the authentication method. Password, Card number, Domain name, PIN code, HomeDirectry information or RBAC information.
	Tip The cache information will be updated if user authentication succeeds with the authentication server. However, if a user is authenticated with the cache information, it is not updated.	
3	Validity Period of Cache	Enter the number of days to maintain the cache information. 1 to 14 days can be set from the latest update.
4	Register Local User which is available in Windows Domain Authentication/LDAP Authentication	Select this to register a local user who can log in with MFP Local Authentication using the cache information for an MFP managed with external authentication.
5	Validity Period of Local User	Enter the number of valid days for local users. Up to 180 days can be set from the user creation day. If 0 is set, the number of valid days will be indefinite.
6	LDAP Server1 - LDAP Server16	Select the LDAP server you want to use for LDAP authentication. Click one of the LDAP servers and specify the following items in the displayed screen to register the LDAP server. **Windows Server** — Select this when LDAP is running on a Windows server. **LDAP Server (Other than Windows Server)** — Select this when the LDAP is running on a server other than a Windows one.
7	Role Based Access Setting	Configure role based access using an LDAP server. **Role Based Access using LDAP server** — Select whether enable or disable role based access. [Disable] is set as the default. **LDAP Server** — Select the LDAP server that manages the Role Based Access Control.
8	PIN Code Authentication Setting	**PIN Code Authentication** — Select the PIN code authentication method. • **Disable** — Select this no to use the PIN code authentication. Use the user name and password for authentication. • **Enable** — Select this to use the PIN code authentication. Instead of the PIN code, it is possible to use the user name and password for authentication. **Minimum PIN Code Length** — Enter a figure that specifies the minimum digits for the PIN code.
9	LDAP Server1 - LDAP Server3	Set the following items for LDAP Server1 when you use the PIN Code authentication: **Windows Server** — Select this when LDAP is running on a Windows server. **LDAP Server (Other than Windows Server)** — Select this when the LDAP is running on a server other than a Windows one. **Attribute type of "User Name"** — Enter the attribute type of “User Name” for “LDAP Server (Other than Windows Server)”. **Attribute type of "PIN"** — Enter the attribute type of “PIN” for the PIN code authentication. When you use more than one LDAP server, select LDAP Server2 and/or LDAP Server3 and set up the LDAP server as necessary. See the settings for LDAP Server1.
	Tip If [Windows Server] is selected as an LDAP server for the PIN code or IC card authentication with [Create User Information Automatically] enabled, the following attribute type of user name is used. - If Kerberos is selected to access the LDAP server: sAMAccountName - If Digest-MD5, CRAM-MD5, Login, Plain or Simple Bind is selected to access the LDAP server: displayName	

Oki Data Corporation
4-11-22 Shibaura, Minato-ku,Tokyo
108-8551, Japan

www.okiprintingsolutions.com

45686131EE