SISTEMI DIGITALI MULTIFUNZIONE A COLORI

Guida alla Gestione della Modalità di Elevata Sicurezza

ES9466 MFP/ES9476 MFP

Prefazione

Vi ringraziamo per aver acquistato i sistemi digitali multifunzione in B/N o a colori Oki.
Questo manuale illustra le condizioni e le impostazioni richieste per utilizzare i sistemi Digitali Multifunzione in conformità con IEEE Std 2600.1 ™-2009.
Leggere attentamente questa guida prima di utilizzare i sistemi Digitali Multifunzione in modalità di elevata sicurezza.
Per le precauzioni di sicurezza relative all'utilizzo della periferica in conformità con IEEE Std 2600.1™-2009, vedere "Precauzioni di sicurezza" in "Informazioni sulla sicurezza".
Conservare questa guida a portata di mano e consultarla per utilizzare la periferica in conformità con IEEE Std 2600.1 ™-2009.

Nota

Qualora si sospetti che la confezione sia stata aperta o in caso di dubbi sull'imballo, contattare il rivenditore.

■ Suggerimenti per la lettura di questo manuale

❑ Simboli utilizzati nel manuale

Nel manuale si utilizzano i seguenti simboli per evidenziare delle informazioni importanti; leggere attentamente queste informazioni prima di utilizzare il sistema.

⚠AVVERTENZA	Segnala una situazione di potenziale rischio che, se non evitata, potrebbe causare lesioni gravi a persone e danneggiare o incendiare la macchina o gli oggetti circostanti.
⚠ATTENZIONE	Segnala una situazione di potenziale rischio che, se non evitata, può causare ferite alle persone, danni parziali alla macchina o ad oggetti nelle vicinanze oppure perdite di dati.
Nota	Riporta delle informazioni alle quali prestare attenzione quando si utilizza il sistema.
Suggerimento	Segnala informazioni utili sulle modalità di funzionamento del sistema.
🕮	Segnala le pagine contenenti informazioni sull'operazione in corso. Consultare queste pagine all'occorrenza.

❑ Destinatari del manuale

Questo manuale è destinato agli amministratori del sistema. Non è necessario che utenti generici leggano il manuale.

❑ Accessori opzionali

Per le opzioni e gli accessori disponibili, vedere la ***Guida rapida di riferimento del sistema***.

❑ Marchi di fabbrica

Per i marchi di fabbrica, vedere la guida ***Informazioni sulla sicurezza***.

SOMMARIO

1

Il modo elevata sicurezza

Precauzioni di utilizzo del Modo Elevata Sicurezza

Questa modalità operativa protegge le informazioni sensibili dei clienti da accessi non autorizzati al sistema e da divulgazione.
Le funzioni di sicurezza attivate quando si utilizza la periferica in conformità con lo standard IEEE Std 2600.1 TM-2009 sono quelle di seguito elencate.

- Funzione di Impostazione di autenticazione utente
- Funzione di Gestione dei ruoli
- Funzione di raccolta dei log e browsing
- Funzione di sovrascrittura dei dati specificati sul disco fisso al termine dei lavori o all'accensione della periferica
- Funzione di comunicazione con i protocolli TLS
- Funzione di controllo dell'integrità
- Funzioni di gestione come:
  Registro, Password, Utente, Policy password, Data & Ora, Azzeramento automatico, Timer sessione, Abilita/Disabilita TLS

Abbiamo richiesto la certificazione ISO/IEC 15408 per le periferiche sotto elencate utilizzate nella versione Giapponese o Inglese e collegate a PC con installato Windows 7 come sistema operativo e Internet Explorer versione 9.0.
MFP: ES9466 MFP/ES9476 MFP*

* In attesa di certificazione (a Aprile 2016)

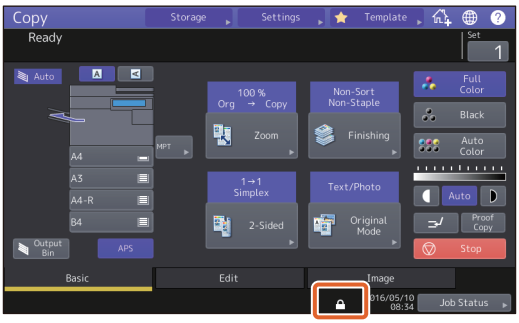
Per utilizzare la periferica in conformità con lo standard IEEE Std. 2600.1TM-2009 in modalità di elevata sicurezza é necessario configurare l'MFP in funzione dell'ambiente di utilizzo, configurando ad esempio le impostazioni di crittografia del protocollo oppure le impostazioni necessarie per consentire solo il collegamento di PC server o client autorizzati.
Si tenga presente che se non si osservano le condizioni indicate in questa guida non sarà possibile utilizzare la periferica in conformità con lo standard IEEE Std. 2600.1 TM-2009.

Suggerimento

Per maggiori informazioni sulle funzioni di sicurezza e sulle procedure di configurazione, fare riferimento alla ***Guida di TopAccess***.

■ Controllo della modalità

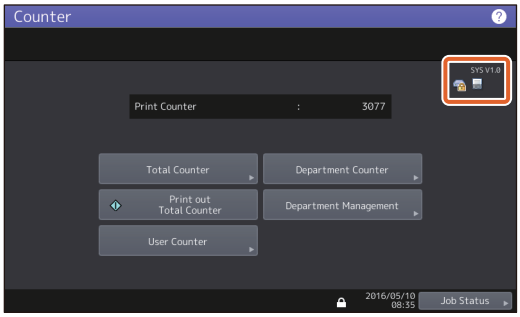
Quando si utilizza la periferica in modalità di elevata sicurezza, sul pannello a sfioramento verrà visualizzato .



Suggerimenti

- Quando è abilitata questa modalità di utilizzo della periferica, il disco fisso è criptato. Inoltre, sulla periferica deve essere installato anche il kit opzionale di sovrascrittura dei dati (GP-1070).
  Per controllare l'operatività di ogni funzione, fare clic nell'area in alto a destra sulla schermata [Contatore (Counter)] visualizzata sul pannello a sfioramento della periferica.

Il disco fisso è criptato.	Viene visualizzata l'icona. Il disco fisso verrà comunque criptato se sulla periferica è attiva la modalità elevata sicurezza.
Il kit di sovrascrittura dei dati funziona correttamente.	La comparsa dell'icona indica che il kit di sovrascrittura dei dati funziona correttamente. Viene visualizzata la versione del sistema. (SYS V1.0)



- Se è installato il kit di sovrascrittura dei dati, lo spazio del disco fisso temporaneamente utilizzato durante l'elaborazione del lavoro verrà utilizzato per un altro lavoro dopo la sovrascrittura dei dati quando l'utente si scollega.

■ Condizioni operative

Attenersi alle istruzioni operative di cui sopra per evitare che informazioni sensibili non siano protette da divulgazione e accessi non autorizzati al sistema.

Accertarsi di selezionare [Autenticazione MFP locale (MFP Local Authentication)] per [Metodo di autenticazione (Authentication Method)] in [Gestione utente (User Management)]. Se per l'autenticazione utente si utilizza una [Autenticazione dominio Windows (Windows Domain Authentication)] o [Autenticazione LDAP (LDAP Authentication)], la periferica non potrà più operare in conformità con lo standard IEEE Std 2600.1 ™-2009.

Selezionare manualmente [FULL] per eseguire un controllo dell'integrità in fase di installazione e periodicamente.

* Per maggiori informazioni sul controllo dell'integrità, fare riferimento alla ***Guida alla gestione del sistema multifunzione***.

Non modificare i valori predefiniti delle impostazioni di comunicazione della periferica. Se non si applicano modifiche ai valori predefiniti, la comunicazione in rete può essere protetta mediante TLS.

Nei seguenti casi, contattare il tecnico dell'assistenza.

- Se l'icona che indica che il disco fisso è criptato () non è visualizzata.
- Se l'icona che indica che il kit di sovrascrittura dei dati funziona correttamente () non è visualizzata.
- La versione visualizzata non coincide con quella reale.

Nel modo di elevata sicurezza, le funzioni seguenti non possono essere utilizzate.

- Interruzione copia
- Fax di rete
- AddressBook Viewer
- File Downloader
- Driver TWAIN
- Utility di backup/ripristino e-Filing
- Stampa programmata
- Archiviazione e-Filing da un driver di stampa*
  * È possibile selezionare questa funzione, tuttavia viene generato un errore e il lavoro viene cancellato. La stampa non verrà dunque eseguita. Quando un lavoro viene cancellato, tale lavoro verrà registrato nel registro degli errori. Controllare sulla scheda [Registri (Logs)] in TopAccess oppure [Stato lavori (Job Status)] - [Registro (Log)] - [Stampa (Print)] sulla periferica.
- Disabilitazione autenticazione login

La funzione di login automatico nel software client fornito con la periferica non è disponibile. Immettere nome utente e password quando si utilizza il software client.

I dati inviati alla periferica con Fax/stampante Internet fax o ricevuti con un driver di stampa*, possono essere elaborati solo in caso di autentificazione di un utente con privilegi di stampa.

* Utilizzare i protocolli IPP SSL per comunicare con la stampante.

Durante la stampa IPP, usare la porta creata inserendo “https://[Indirizzo IP (IP Address)]:[Numero porta SSL (SSL Port Number)]/[Stampa (Print)] nel campo [URL].

(es. https://192.168.1.2:443/Print)

* Per maggiori informazioni, vedere [Stampa IPP (IPP printing)] in [Installazione dei driver di stampa per Windows (Installing printer drivers for Windows)] - [Altre installazioni (Other Installations)] nella ***Guida all'installazione dei software***.

Quando si importano dei dati, come ad esempio una rubrica, accertarsi di utilizzare i dati esportati con la periferica.

Non utilizzare applicazioni che necessitano modifiche del menu secondario [ODCA] nel menu [Impostazioni (Setup)] nella schermata [Amministrazione (Administration)] sotto la voce TopAccess.

Non abilitare l'opzione [Usa autent.con psw per il lavoro di stampa(Use Password Authentication for Print Job)] quando si stampa attraverso uno dei seguenti driver di stampa: Stampante PCL (PCL6), PS (PostScript) e XPS.

Per utilizzare questa periferica in piena sicurezza, accertarsi di impostare le seguenti voci:

Nota

Impostare le voci correttamente attenendosi all'elenco dei valori iniziali (📖 P.19).

- Utilizzare il formato PDF criptato quando si salva o si invia un file e il livello di crittografia dovrà essere 128 bit AES.
- Specificare un PC remoto affidabile come destinazione di archiviazione dei dati di scansione.
- Non utilizzare [CASELLA PUBBLICA (PUBLIC BOX)] in e-Filing poiché a questo tipo di casella non è possibile assegnare una password.
- Non utilizzare [MFP LOCALE (MFP LOCAL)] poiché non è possibile assegnare una password.
- L'amministratore deve esportare e archiviare i registri su base regolare.

L'amministratore deve spiegare agli utenti che questa periferica utilizza la modalità di elevata sicurezza; deve inoltre illustrare loro le voci seguenti in modo tale da informarli adeguatamente.

- Stampare utilizzando le impostazioni del driver di stampa della stampa IPP.
- Specificare un PC remoto affidabile come destinazione di archiviazione dei dati di scansione.
- Non utilizzare una cartella condivisa in e-Filing.
- Non utilizzare cartelle locali di questa periferica.

Quando si smaltisce un MFP, contattare il tecnico dell'assistenza per assicurarsi di eliminare completamente i dati presenti nel disco fisso.

2

FUNZIONI ESCLUSIVE

Password temporanea

In modalità elevata sicurezza, una password assegnata a caso dall'amministratore per consentire l'accesso a un utente, viene considerata come password temporanea. Per utilizzare la periferica, occorre registrare una password personale dopo aver eseguito l'accesso con quella temporanea.

Nota

L'utilizzo della password temporanea non garantisce un livello di sicurezza sufficiente. Registrare la propria password personale quanto prima possibile.

■ Condizioni quando si utilizza una password temporanea

Una password utente temporanea può essere utilizzata nei seguenti casi:

- La prima volta che si effettua il login alla periferica dopo essere stati registrati dall'amministratore.
- Quando l'amministratore azzera la password utente.
- Quando la password delle informazioni utente importata da un amministratore è scritta in chiaro.

Nota

Quando l'amministratore reimposta le password deve informare e richiedere agli utenti di sostituire la password con una personale.

Suggerimento

Per prevenire l'alterazione delle informazioni utente esportate da una periferica, la password è criptata. Se si modifica la password per le informazioni utente esportate, verrà utilizzato un testo in chiaro per la password.

■ Operazione utente quando si utilizza una password temporanea

Quando è possibile registrare la password personale durante l'accesso.

- Registrazione della propria password sul pannello di controllo
  Immettere il nome utente e una password temporanea nel menu [Autenticazione utente (User Authentication)]. Premere [OK] sulla schermata di conferma della password temporanea per visualizzare la schermata di immissione password. Immettere la password temporanea nel campo [Vecchia password (Old Password)]. Digitare la nuova password nel campo [Nuova password (New Password)] e nel campo [Conferma password (Retype New Password)], quindi premere [OK]. La nuova password viene registrata e può essere utilizzata per il login alla periferica.
- Registrazione della propria password in TopAcess.
  Quando si accede alla periferica da TopAccess, si apre la schermata di login. Sulla schermata di login immettere nome utente e password temporanea, quindi premere [Login]. Quando si apre la schermata di registrazione, digitare la nuova password nei campi [Nuova password (New Password)] e [Conferma password (Retype New Password)], quindi premere [Salva (Save)]. La nuova password viene registrata e può essere utilizzata per il login a TopAccess.

Quando non è possibile registrare la password personale durante l'accesso.

Con i programmi di utility sotto elencati, si verifica un errore se si tenta di accedere alla periferica con una password temporanea. Di conseguenza, non è neppure possibile registrare una nuova password. Prima di utilizzare queste utility occorre registrare una nuova password personale sul pannello di controllo o in TopAccess.

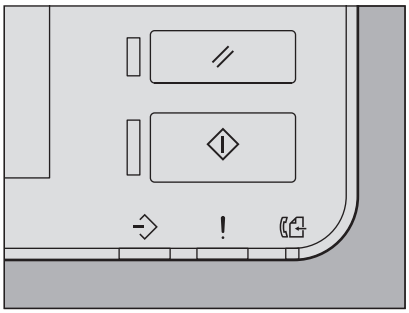
- Driver Remote Scan
- Utility web e-Filing

Attesa (Fax)

Quando è attiva la modalità elevata sicurezza non è possibile la stampa automatica dei Fax, degli Internet Fax o degli allegati e-mail. Questi lavori vengono inviati alla coda [Attesa (Fax) (Hold (Fax))] e potranno essere stampati solo da un utente che accede alla periferica con privilegi di [Stampa fax ricevuti (Fax Received Print)].

Suggerimento

Se nella coda [Attesa (Fax) (Hold (Fax))] vi sono dei lavori, l'indicatore DATI IN MEMORIA (DATA IN MEMORY) lampeggia.

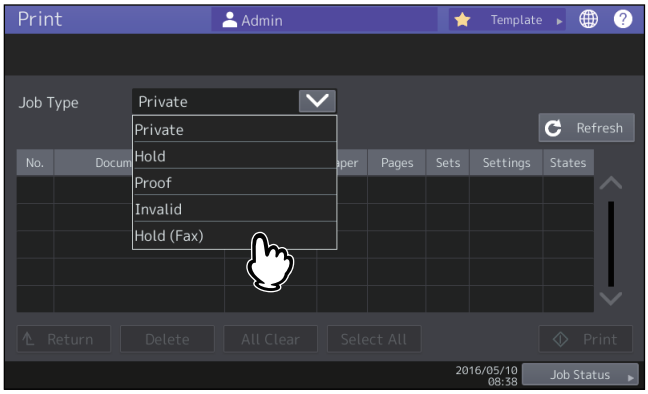


Stampa di un lavoro presente nella coda Attesa (Fax) (Hold (Fax))

1 Accedere alla periferica come utente con privilegi di [Stampa fax ricevuti (Fax Received Print)]

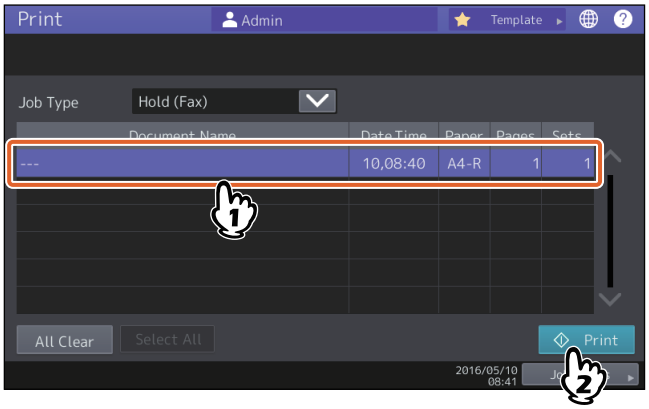
2 Premere [Print Mode] sul pannello di controllo.

3 Selezionare [Attesa (Fax) (Hold (Fax))].



- Verranno visualizzati tutti i lavori presenti nella coda [Attesa (Fax) (Hold (Fax))].

4 Selezionare il lavoro desiderato oppure scegliere [Sel. tutto (Select All)] e premere [Stampa (Print)].



- I lavori stampati verranno cancellati dalla coda [Attesa (Fax) (Hold (Fax))].

3

I VALORI INIZIALI

Precauzioni riguardanti i valori iniziali

Per utilizzare la periferica in modo sicuro, i valori iniziali e i valori selezionabili per il modo elevata sicurezza possono essere diversi da quelli configurabili in modalità sicurezza normale. Questo manuale illustra solo i valori iniziali e le voci di impostazioni che differiscono da quelli della modalità sicurezza normale.

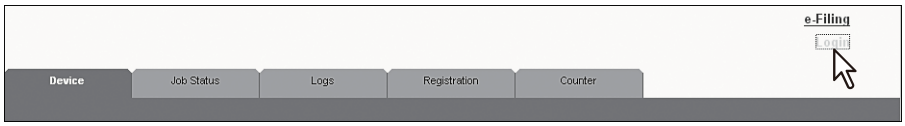
Per utilizzare la periferica in conformità con lo standard IEEE Std 2006.1™-2009; accertarsi di modificare i valori iniziati per la modalità di elevata sicurezza elencati nel presente capitolo, seguendo le istruzioni descritte nelle note prima dell'utilizzo e non cambiarle.

Note

- Per i valori predefiniti e i valori configurabili nel modo sicurezza normale, vedere la ***Guida di TopAccess*** e la ***Guida alla gestione del sistema multifunzione***.
- Per reimpostare tutte le impostazioni eseguendo la “Inizializzazione” della periferica, eseguire il backup delle impostazioni del sistema e dei dati utente prima di eseguire l'inizializzazione. Per maggiori informazioni, vedere la ***Guida di TopAccess*** e la ***Guida alla gestione del sistema multifunzione***.

■ Login

- Quando un utente esegue il login con privilegi di amministratore, in TopAccess vengono visualizzate le schede [Gestione utente (User Management)] e [Amministrazione (Administration)]. Aprire TopAccess, fare clic su “[Login]” in alto a destra, quindi immettere nome utente e password di login.



- Per accedere come utente con privilegi di amministratore, accedere alla scheda [Amministr. (Admin)] nel modo [Impostazione (Setting)].

■ Elenco dei valori iniziali

Schermata Home:
Menu [Impostazione -User- (Setting -User-)]
Scheda [Amministr. (Admin)]
Menu [Elenco/Rapporto (List/Report)]
Menu [Impostazione rapporto (Report Setting)]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
[Rapporto COMUN. (COMM. Report)]		
TX memoria (Memory Tx)	OFF	Non modificare l'impostazione su “ON”.

* Con TopAccess non è possibile utilizzare i menu sopra riportati.

TopAccess:
Scheda [Amministrazione (Administration)]
Menu [Impostazioni (Setup)]
Menu secondario [Generale (General)]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
Informazioni sul dispositivo		
Stampa diretta USB (USB Direct Print)	Disabilita (Disable)	
Funzioni (Functions)		
Salva come FTP (Save as FTP)	Disabilita (Disable)	
Salva su supporto USB (Save to USB Media)	Disabilita (Disable)	
Salva come SMB (Save as SMB)	Disabilita (Disable)	
Salva come Netware (Save as Netware)	Disabilita (Disable)	
iFax di rete (Network iFax)	Disabilita (Disable)	
Fax di rete (Network Fax)	Disabilita (Disable)	
Servizi web di scansione (Web Services Scan)	Disabilita (Disable)	
Scansione Twain (Twain Scanning)	Disabilita (Disable)	
Restrizione amministratore uso rubrica /AddressbookRemoteOperator (Restriction on Address Book operation by administrator / AddressbookRemoteOperator)		
Può essere utilizzata dall'amministratore /Solo AddressbookRemoteOperator (Can be operated by Administrator / AddressbookRemoteOperator only)		
Risparmio Energetico (Power Save)		
Azzeramento automatico (Auto Clear)*	45 secondi	Il valore iniziale è uguale a quello della modalità Sicurezza Normale; non si può selezionare il tasto OFF.

* Si può modificare il valore sulla scheda [AMMINISTR. (ADMIN)] nel modo [Impostazione -User- (Setting -User-)] sul pannello a sfioramento della periferica.

Menu secondario [Rete (Network)]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
SMB		
Protocollo server SMB (SMB Server Protocol)	Disabilita (Disable)	
HTTP		
Abilita SSL (Enable SSL)*	Abilita (Enable)	
WSD		
Abilita SSL (Enable SSL)	Abilita (Enable)	
Servizi web di stampa (Web Services Print)	Disabilita (Disable)	
Servizi web di scansione (Web Services Scan)	Disabilita (Disable)	
Server SMTP (SMTP Server)		
Abilita server SMTP (Enable SMTP Server)	Disabilita (Disable)	
Server FTP (FTP Server)		
Abilita server FTP (Enable FTP Server)	Disabilita (Disable)	
Abilita SSL (Enable SSL)	Abilita (Enable)	
Client SMTP (SMTP Client)		
Abilita SSL (Enable SSL)	Verifica con certificato CA importato	L'impostazione sicura è “Verificare con il certificato importato (Verify with imported CA certification(s))” oppure “Accetta tutti i certificati senza CA (Accept all certificates without CA)”.
Autenticazione (Authentication)	AUTO	Controllare che all'ambiente in uso sia applicato “CRAM-MD5”, “Digest-MD5”, “Kerberos” o “NTLM (IWA)”.
Client POP3		
Abilita SSL (Enable SSL)	Verificare con il certificato importato (Verify with imported CA certification(s))	
Client FTP (FTP Client)		
Impostazione SSL (SSL Setting)	Verificare con il certificato importato (Verify with imported CA certification(s))	
Bonjour		
Abilita Bonjour (Enable Bonjour)	Disabilita (Disable)	
SNMP		
Abilita SNMP V1/V2 (Enable SNMP V1/V2)	Disabilita (Disable)	
Abilita SNMP V3 (Enable SNMP V3)	Abilita (Enable)	
SLP		
Abilita SLP (Enable SLP)	Disabilita (Disable)	
Impostazione Syslog (Syslog Setting)		
Abilita SSL (Enable SSL)	Verifica con certificato CA importato	

* Si può modificare il valore sulla scheda [AMMINISTR. (ADMIN)] nel modo [Impostazione -User- (Setting -User-)] sul pannello a sfioramento della periferica.

Menu secondario [Stampante (Printer)]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
Impostazione generale (General Setting)		
Restrizione per lavoro di stampa (Restriction for Print Job)	Solo Stampa trattenuta (Only Hold)	

Menu secondario [Servizio di stampa (Print Service)]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
Stampa Raw TCP (Raw TPC Print)		
Abilita TCP Raw (Enable Raw TCP)	Disabilita (Disable)	
Stampa LPD (LPD Print)		
Abilita LPD (Enable LPD)	Disabilita (Disable)	
Stampa IPP (IPP Print)		
Abilita SSL (Enable SSL)	Abilita (Enable)	
Stampa FTP (FTP Print)		
Abilita stampa FTP (Enable FTP Printing)	Disabilita (Disable)	

Menu secondario [ODCA]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
Rete (Network)		
Abilita porta (Enable Port)	Disabilita (Disable)	

Menu [Sicurezza (Secuity)]
Menu secondario [Autenticazione (Authentication)]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
Impostazione autenticazione utente (User Authentication Setting)		
[Autenticazione utente (User Authentication)]	Abilita (Enable)	Non è possibile impostare “[Disabilita (Disable)]”.
Autenticazione utente in base alla funzione (User Authentication According to Function)	Disabilita (Disable)	Non modificare l'impostazione su “Abilita (Enable)”.
Usa autent.con psw per il lavoro di stampa (Use Password Authentication for Print Job)	Disabilita (Disable)	Non modificare l'impostazione su “Abilita (Enable)”.
Abilita utente guest (Enable Guest User)	Nessun segno di spunta [Disabilita (Disable)]	Il valore iniziale è uguale a quello della modalità Sicurezza Normale; non è possibile impostare “[Abilita (Enable)]”.
Tipo di autenticazione (Authentication Type)	Autenticazione MFP locale (MFP Local Authentication)	
Autenticazione con codice PIN (PIN Code Authentication)	Disabilita (Disable)	Non modificare l'impostazione su “Abilita (Enable)”.
Gestione utente condivisa (Shared User Management)	Disabilita (Disable)	Non modificare l'impostazione su “Abilita (Enable)”.

Menu secondario [Policy password (Password Policy)]

Voci	Valori iniziali per la modalità di elevata sicurezza	Note
Policy per gli utenti (Policy for Users)		
Lunghezza password minima (Minimum Password Length)	8 (cifre)	
Requisiti da applicare (Requirements to Apply)	Abilita (Enable)	
Impostazione di blocco (Lockout Setting)	Abilita (Enable)	(Come nel Modo sicurezza normale)
Numero di ritentativi (Number of Retry)	3 (volte)	
Durata blocco (Lockout Time)	2 (minuti)	
Periodo disponibile (Available Period)	Disabilita (Disable)	(Come nel Modo sicurezza normale)
Giorno/i alla scadenza (Expiration day(s))	90 (giorni)	
Criteri per amministratore, revisore (Policy for Administrator, Auditor)		
Lunghezza password minima (Minimum Password Length)	8 (cifre)	
Requisiti da applicare (Requirements to Apply)	Abilita (Enable)	
Impostazione di blocco (Lockout Setting)	Abilita (Enable)	(Come nel Modo sicurezza normale)
Numero di ritentativi (Number of Retry)	3 (volte)	
Durata blocco (Lockout Time)	2 (minuti)	
Periodo disponibile (Available Period)	Disabilita (Disable)	(Come nel Modo sicurezza normale)
Giorno/i alla scadenza (Expiration day(s))	90 (giorni)	
Criteri per Caselle e-Filing,Gruppi modelli, Modelli, PDF Protetto, SNMPv3, Clonazione, Ricezione sicura (Policy for e-Filing Boxes, Template Groups, Templates, SecurePDF, SNMPv3, Cloning, Secure Receive)		
Lunghezza password minima (Minimum Password Length)	8 (cifre)	
Requisiti da applicare (Requirements to Apply)	Abilita (Enable)	
Impostazione di blocco (Lockout Setting)	Abilita (Enable)	(Come nel Modo sicurezza normale)
Numero di ritentativi (Number of Retry)	3 (volte)	
Durata blocco (Lockout Time)	2 (minuti)	

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

www.oki.com/printing/

46568674EE
Ver00 F Issued in Nov. 2016