OKI

SISTEMI DIGITALI MULTIFUNZIONE A COLORI /
SISTEMI DIGITALI MULTIFUNZIONE

Guida alla Gestione della Modalità di Elevata Sicurezza

ES9455 MFP
ES9465 MFP/ES9475 MFP

Prefazione

Vi ringraziamo per aver acquistato il sistema digitale multifunzione OKI.
Questo manuale illustra le condizioni e le impostazioni richieste per utilizzare i sistemi Digitali Multifunzione in conformità con IEEE Std 2600.1™-2009 *1.
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.

■ 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 tali 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 apparecchiature o beni.
⚠ATTENZIONE	Segnala una situazione di potenziale rischio che, se non evitata, può causare ferite alle persone, danni parziali alla macchina o a beni nelle vicinanze oppure perdite di dati.
Nota	Riporta delle informazioni alli quale fare attenzione quando si utilizza il sistema.

Il manuale riporta, inoltre, le seguenti informazioni che potrebbero aiutare l'utente nell'utilizzo del 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.

❑ Nomi dei modelli e delle serie in questo manuale

All'interno di questo manuale, il nome del modello è stato sostituito con il nome della serie, come indicato di seguito.

Nome del modello	Nome della Serie
ES9455 MFP	ES9455 MFP
ES9465 MFP/ES9475 MFP	Serie ES9475 MFP

❑ Spiegazione per il pannello di controllo e per il pannello a sfioramento

- I dettagli dei menu visualizzati sul pannello a sfioramento possono variare in funzione dell'ambiente operativo configurato e degli accessori opzionali installati.
- Il manuale riporta le schermate inerenti l'utilizzo di carta di formato A/B. Se si utilizza carta di formato LT, le schermate o l'ordine dei pulsanti possono differire.

❑ Opzioni

Per le opzioni e gli accessori disponibili, vedere "Accessori opzionali" nella ***Guida rapida di riferimento*** del sistema.

❑ Marchi di fabbrica

- Il nome ufficiale di Windows XP è Microsoft Windows XP Operating System.
- Il nome ufficiale di Windows Vista è Microsoft Windows Vista Operating System.
- Il nome ufficiale di Windows 7 è Microsoft Windows 7 Operating System.
- Il nome ufficiale di Windows 8 è Microsoft Windows 8 Operating System.
- Il nome ufficiale di Windows Server 2003 è Microsoft Windows Server 2003 Operating System.
- Il nome ufficiale di Windows Server 2008 è Microsoft Windows Server 2008 Operating System.
- Il nome ufficiale di Windows Server 2012 è Microsoft Windows Server 2012 Operating System.
- Microsoft, Windows, Windows NT, i nomi commerciali e i nomi di altri prodotti Microsoft sono marchi di fabbrica di Microsoft Corporation negli USA e negli altri paesi.
- Apple, AppleTalk, Macintosh, Mac, Mac OS, Safari, and TrueType sono marchi di fabbrica di Apple Inc. negli USA e negli altri paesi.
- Adobe, Acrobat, Reader e PostScript sono marchi di fabbrica o marchi di fabbrica depositati di Adobe Systems Incorporated negli USA e negli altri paesi.
- Mozilla, Firefox e il logo Firefox sono marchi di fabbrica o marchi di fabbrica depositati di Mozilla Foundation negli USA e negli altri paesi.
- IBM, AT e AIX sono marchi di fabbrica di International Business Machines Corporation.
- NOVELL, NetWare e NDS sono marchi di fabbrica di Novell, Inc.
- Altri nomi di società o di prodotti riportati nel presente manuale sono marchi di fabbrica delle rispettive aziende.

SOMMARIO

Prefazione 1
Suggerimenti per la lettura di questo manuale 1

Capitolo 1 IL MODO ELEVATA SICUREZZA

Precauzioni di utilizzo del Modo Elevata Sicurezza 6
Controllo e verifica della modalità attiva 6
Condizioni operative 7

Capitolo 2 FUNZIONI ESCLUSIVE DEL MODO ELEVATA SICUREZZA

Password temporanea 10
Condizioni quando si utilizza una password temporanea 10
Operazione utente quando si utilizza una password temporanea 10
ATTESA (FAX) 11

Capitolo 3 I VALORI INIZIALI

Precauzioni riguardanti i valori iniziali 14
Login 14
Elenco dei valori iniziali 15

1

IL MODO ELEVATA SICUREZZA

Precauzioni di utilizzo del Modo Elevata Sicurezza 6
Controllo e verifica della modalità attiva 6
Condizioni operative 7

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™-2009 sono quelle di seguito elencate.

- Funzione di Impostazione di autenticazione utente
- Funzione di Gestione dei ruoli
- Funzione di crittografia dei dati scritti sul disco fisso
- 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 SSL o TLS
- Funzione di controllo dell'integrità
- Funzioni di gestione come:
  Registro, Password, Utente, Policy password, Data & Ora, Azzeramento automatico, Timer sessione, Abilita/Disabilita SSL/LTS

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 XP o Vista come sistema operativo e Internet Explorer versione 8.0
ES9455 MFP
ES9465 MFP/ES9475 MFP

Per utilizzare la periferica in conformità con lo standard IEEE Std 2600.1™-2009 in modalità elevata sicurezza è necessario configurare l'MFP in funzione dell'ambiente di utilizzo, configurando ad esempio le impostazioni di crittografia del protocollo o dei dati 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™-2009.

Suggerimenti

- Per maggiori informazioni sulle funzioni di sicurezza e sulle procedure di configurazione, fare riferimento alla Guida di TopAccess.
- Si richiede Hard Disk Kit (GE-1220) quando si utilizza un sistema ES9455 MFP senza hard disk in modalità sicurezza elevata.

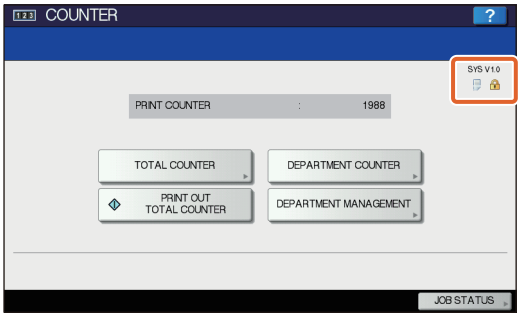
■ Controllo e verifica della modalità attiva

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] visualizzata sul pannello a sfioramento della periferica.

Il disco fisso è criptato.	Viene visualizzata l'icona  . Anche se questa icona non è visualizzata, 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 (V1.0).



- Quando è installato il Kit di sovrascrittura dei dati, lo spazio del disco fisso temporaneamente utilizzato durante l'elaborazione di un lavoro verrà utilizzato per un altro lavoro dopo la sovrascrittura dei dati.

■ Condizioni operative

Selezionare [Autenticazione locale MFP] per [Tipo di autenticazione] in [Autenticazione utente]. Se per l'autenticazione utente si utilizza un server SNTP, un server LDAP o un server DNS, la periferica non potrà più operare in conformità con lo standard IEEE Std 2600.1™-2009.

Quando si collega la periferica da Utility di backup/ripristino eFiling, File Downloader, TWAIN Driver o Addressbook Viewer, immettere ID e password di accesso. La password immessa viene visualizzata con una serie di simboli. Inoltre, se si immette ripetutamente una password errata, verrà bloccato l'accesso all'utente.

Selezionare manualmente [FULL] per eseguire il controllo dell'integrità.

* Per maggiori informazioni sul controllo dell'integrità, vedere la 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 SSL.

Impostare OFF per [TX DA MEMORIA] in [IMPOSTAZIONE] - [AMMINISTRATORE] - [ELENCHI/ RAPPORTI] - [IMPOSTAZIONE RAPPORTO] - [RAPPORTO COMU.].

Quando è attivo il Modo Elevata Sicurezza, non si possono utilizzare le seguenti funzioni.

- Interruzione copia
- Fax di rete
- Stampa programmata
- Archiviazione e-Filing da un driver di stampa*
  * Si può selezionare la funzione ma 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] in TopAccess oppure [STATO LAVORI] - [REGISTRO] - [STAMPA] 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.

Tutti i dati inviati alla periferica, ad esempio i dati fax e Internet Fax stampati o ricevuti da un driver di stampa*, possono essere stampati solo se l'utente che effettua il login dispone di privilegi di stampa.

* Utilizzare i protocolli IPP SSL o SSL di Stampa WS per la comunicazione con la stampante.

Quando si esegue la stampa IPP, utilizzare la porta creata digitando “https://indirizzo IP]:[SSL numero porta]/Print” nel campo URL.

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

* Per maggiori informazioni, vedere [Stampa IPP] in [Installazione dei driver di stampa] - [Altre installazioni] nella guida all'installazione del software.

Non utilizzare applicazioni che richiedono modifiche delle impostazioni nel menu secondario [ODCA] del menu [Setup] nella scheda [Amministrazione] di TopAccess.

Per utilizzare in sicurezza la periferica, si consiglia di osservare le seguenti raccomandazioni.

- 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 in e-Filing poiché a questo tipo di casella non è possibile assegnare una password.
- Non utilizzare MFP LOCALE poiché non è possibile assegnare una password.
- Quando si stampa un Rapporto di InternetFax, non selezionare “Stampa immagine 1ª pagina" per evitare che venga stampata la copia dell'originale.
- Utilizzare SMP Submission in [Print Share].
- Disabilitare [Abilita Raw TCP] e [Abilita LPD] in Print Service.
- L'amministratore deve esportare e archiviare i registri su base regolare.
- Selezionare [Disabilita] in [Scansione Twain].

2

FUNZIONI ESCLUSIVE DEL MODO ELEVATA SICUREZZA

Password temporanea 10
Condizioni quando si utilizza una password temporanea 10
Operazione utente quando si utilizza una password temporanea 10
ATTESA (FAX) 11

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. Premere [OK] sulla schermata di conferma della password temporanea per visualizzare la schermata di immissione password. Immettere la password temporanea nel campo [VECCHIA PASSWORD]. Digitare la nuova password nel campo [NUOVA PASSWORD] e nel campo [CONFERMA NUOVA PASSWORD], quindi premere [OK]. La nuova password viene registrata e può essere utilizzata per il login alla periferica.
- Registrazione della propria password in TopAccess
  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] e [CONFERMA NUOVA PASSWORD], quindi premere [SALVA]. 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.

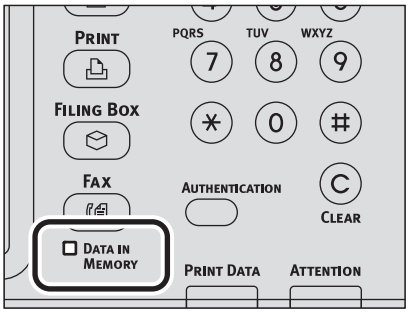
- Driver Remote Scan
- Utility web e-Filing
- Utility di Backup/Ripristino e-Filing
- File Downloader
- Driver TWAIN
- AddressBook Viewer

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)] e potranno essere stampati solo da un utente che accede alla periferica con privilegi di [Stampa fax ricevuto].

Suggerimento

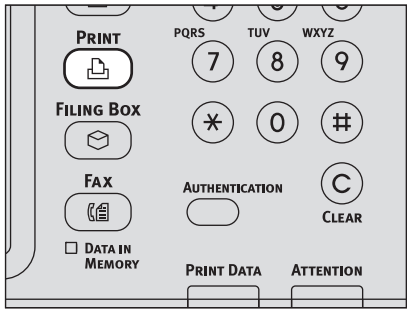
Se nella coda [ATTESA (FAX)] vi sono dei lavori, l'indicatore DATI IN MEMORIA lampeggia.



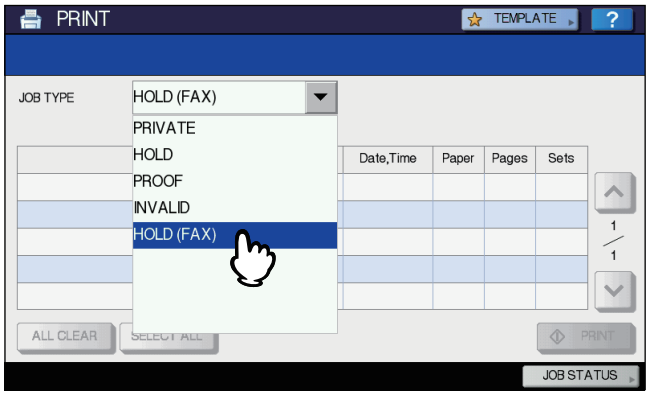
Stampa di un lavoro presente nella coda ATTESA (FAX)

1 Accedere alla periferica come utente con privilegi di [Stampa fax ricevuto].

2 Premere [STAMPA] sul pannello di controllo.

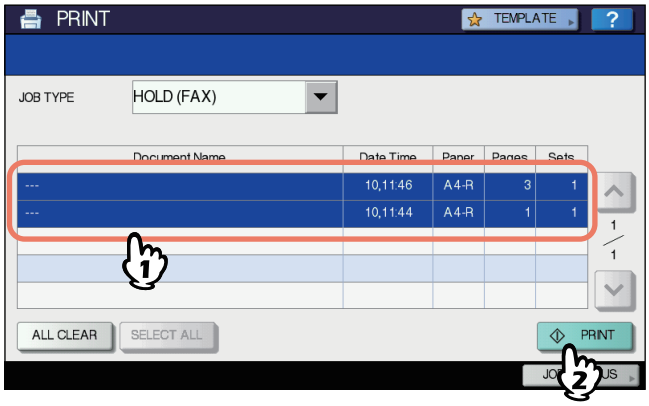


3 Selezionare [ATTESA (FAX)].



- Verranno visualizzati tutti i lavori presenti nella coda [ATTESA (FAX)].

4 Selezionare il lavoro desiderato oppure scegliere [SEL. TUTTO] e premere [STAMPA].



- I lavori stampati verranno cancellati dalla coda [ATTESA (FAX)].

3

I VALORI INIZIALI

Precauzioni riguardanti i valori iniziali 14
Login 14
Elenco dei valori iniziali 15

Precauzioni riguardanti i valori iniziali

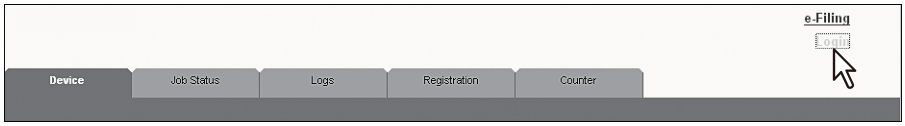
Per utilizzare la periferica in modo sicuro, i valori iniziali e i valori selezionabili per il modo elevata sicurezza possono essere diversi da quelli configurabili in modalità sicurezza normale. Questo manuale illustra solo i valori iniziali e le voci di impostazioni che differiscono da quelli della modalità sicurezza normale.
Per utilizzare la periferica in conformità con IEEE Std 2600.1™-2009, non modificare le impostazioni iniziali descritte in questa guida.

Nota

- 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] e [Amministrazione]. 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 [AMMINISTRATORE] nel modo [IMPOSTAZIONE].

■ Elenco dei valori iniziali

Scheda [Amministrazione]
Menu [Setup]
Menu secondario [Generale]

Funzioni		
Salva come FTP	Disabilita	
Network iFax	Disabilita	
Network Fax	Disabilita	
Servizi web di scansione	Disabilita	
Scansione Twain	Abilita	Il valore iniziale è uguale a quello della modalità Sicurezza Normale; controllare comunque che sia impostato OFF.
Restrizione operativa della Rubrica attivata dall'amministratore		
Solo Amministratore		
Risparmio energia		
Azzeramento automatico*	45 secondi	Il valore iniziale è uguale a quello della modalità Sicurezza Normale; non è comunque possibile selezionare OFF.

* Si può modificare il valore sulla scheda [AMMINISTRATORE] nel modo [IMPOSTAZIONE] sul pannello a sfioramento della periferica.

Menu secondario [Rete]

Servizio di rete HTTP		
Abilita SSL*	Abilita	
Client SMTP		
Abilita SSL	Verifica con certificato CA importato	L'impostazione sicura è "Verifica con certificato CA importato" oppure "Accetta tutti i certificati senza CA".
Autenticazione	AUTO	Controllare che all'ambiente in uso sia applicato "CRAM-MD5", "Digest-MD5", "Kerberos" o "NTLM (IWA)".
Server SMTP		
Abilita server SMTP	Disabilita	
Servizio di rete POP3		
Abilita SSL	Verifica con certificato CA importato	
Client FTP		
Abilita SSL	Verifica con certificato CA importato	
Server FTP		
Abilita SSL	Abilita	
Servizio di rete SNMP		
Abilita SNMP V1/V2	Disabilita	
Abilita SNMP V3	Abilita	
Impostazione servizi web		
Abilita SSL	Abilita	
Servizi web di scansione	Disabilita	

* Si può modificare il valore sulla scheda [AMMINISTRATORE] nel modo [IMPOSTAZIONE] sul pannello a sfioramento della periferica.

Menu secondario [Stampante]

Impostazioni generali		
Restrizione per lavoro di stampa	Solo Attesa	

Menu secondario [Servizio di stampa]

Stampa IPP		
Abilita SSL	Abilita	
Stampa FTP		
Abilita stampa FTP	Disabilita	

Menu secondario [ODCA]

Rete		
Abilita porta	Disabilita	

Menu [Sicurezza]

Menu secondario [Autenticazione]

Impostazione Autenticazione utente		
Autenticazione utente	Abilita	Non è possibile impostare "Disabilita".
Tipo di autenticazione	Autenticazione locale MFP	
Abilita utente guest	Nessun segno di spunta (Disabilita)	Il valore iniziale è uguale a quello della modalità Sicurezza Normale; non è possibile impostare su "Abilita".

Menu secondario [Policy password]

Policy per gli utenti		
Lunghezza password minima	8 (cifre)	
Requisiti da applicare	Abilita	
Impostazione blocco	Abilita	(Come nel Modo sicurezza normale)
Numero di ritentativi	3 (volte)	
Tempo di blocco	2 (minuti)	
Periodo disponibile	Disabilita	(Come nel Modo sicurezza normale)
Giorno/i alla scadenza	90 (giorni)	
Policy per Amministratore, Auditor		
Lunghezza password minima	8 (cifre)	
Requisiti da applicare	Abilita	
Impostazione blocco	Abilita	(Come nel Modo sicurezza normale)
Numero di ritentativi	3 (volte)	
Tempo di blocco	2 (minuti)	
Periodo disponibile	Disabilita	(Come nel Modo sicurezza normale)
Giorno/i alla scadenza	90 (giorni)	
Policy per caselle e-Filing, gruppi di modelli, modelli, PDF protetto, SNMPv3, clonazione, ricezione sicura		
Lunghezza password minima	8 (cifre)	
Requisiti da applicare	Abilita	
Impostazione blocco	Abilita	(Come nel Modo sicurezza normale)
Numero di ritentativi	3 (volte)	
Tempo di blocco	2 (minuti)	

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

www.okiprintingsolutions.com

45686114EE