

**OKI**

MULTIFUNKTIONALE DIGITALE FARBSYSTEME

# **Sicherheitseinstellungen Management Anleitung**

---

**ES9466 MFP/ES9476 MFP**



## Vorwort

---

Wir danken Ihnen, dass Sie sich für das digitale Multifunktionssystem oder digitale farbfähige Multifunktionssystem von Oki entschieden haben.

Dieses Handbuch beschreibt die Voraussetzungen und Einstellungen des digitalen Multifunktionssystems für die Kompatibilität mit IEEE Std 2600.1™-2009.

Lesen Sie dieses Handbuch, bevor Sie die Ihr digitales Multifunktionssystem in diesem hohen Sicherheitsmodus benutzen. Lesen Sie die "Sicherheitshinweise" unter "Sicherheitshinformationen", damit das System in Übereinstimmung mit IEEE Std 2600.1™-2009 betrieben werden kann.

Halten Sie dieses Handbuch griffbereit, damit Sie es jederzeit für die Verwendung des Systems gemäß IEEE Std 2600.1™-2009 benutzen können.

### Hinweis

Wenn es Anhaltspunkte gibt oder Sie den Verdacht haben, dass die erhaltenen Kartons geöffnet wurden oder Sie sich über die Verpackung nicht sicher sind, wenden Sie sich bitte an unsere Verkaufsniederlassung bzw. unseren Vertriebspartner.

## ■ Über dieses Handbuch

### □ Symbole in diesem Handbuch

In diesem Handbuch sind wichtige Hinweise durch folgende Symbole gekennzeichnet. Lesen Sie diese Hinweise, bevor Sie das System benutzen.

 **WARNUNG** Diese Gefahrenstufe weist auf eine potenziell gefährliche Situation hin, die - wenn sie nicht behoben wird - tödliche bzw. ernsthafte Verletzungen, erhebliche Schäden oder Feuer im Gerät oder in seiner Umgebung nach sich ziehen kann.

 **VORSICHT** Diese Gefahrenstufe weist auf eine potenziell gefährliche Situation hin, die - wenn sie nicht behoben wird - geringfügige bis mittlere Verletzungen, Teilschäden am Gerät oder in seiner Umgebung sowie Datenverlust nach sich ziehen kann.

### Hinweis

Kennzeichnet Informationen, die Sie bei der Bedienung des Systems beachten sollten.

### Tipp

Beschreibt praktische Tipps zur Bedienung des Systems.



Seiten, auf denen Sie weitere Hinweise finden können. Lesen Sie ggf. auch diese Seiten.

### □ Zielgruppe für dieses Handbuch

Dieses Handbuch richtet sich an Systemadministratoren. Allgemeine Anwender brauchen es nicht zu lesen.

### □ Optionales Equipment

Einzelheiten zu den verfügbaren Optionen siehe *Kurzbedienungsanleitung*.

### □ Handelsmarken

Zu den Handelsmarken siehe *Sicherheitshinformationen*.



# INHALT

---

<b>Vorwort</b> .....	<b>3</b>
Über dieses Handbuch .....	3

## **Kapitel 1 Hoher Sicherheitsmodus**

---

<b>Sicherheitshinweise</b> .....	<b>8</b>
Prüfen des Modus .....	9
Bedingungen .....	10

## **Kapitel 2 BESONDERE FUNKTIONEN**

---

<b>Temporäres Kennwort</b> .....	<b>14</b>
Fälle, in denen ein temporäres Kennwort verwendet wird .....	14
Benutzerhinweise für die Verwendung eines temporären Kennworts .....	14
<b>Halten (Fax)</b> .....	<b>15</b>

## **Kapitel 3 DIE VOREINSTELLUNGEN**

---

<b>Sicherheitshinweise zu den Voreinstellungen</b> .....	<b>18</b>
Systemanmeldung.....	18
Tabelle der Voreinstellungen .....	19



## Hoher Sicherheitsmodus

<b>Sicherheitshinweise .....</b>	<b>8</b>
Prüfen des Modus .....	9
Bedingungen .....	10

## Sicherheitshinweise

---

Dieser Modus schützt das System vor unbefugten Zugriffen und Informationsverlust.

Die folgenden Sicherheitsfunktionen entsprechen dem Standard IEEE Std 2600.1™-2009.

- Benutzerverwaltung
- Funktionszuweisungen
- Protokollierung und Suchfunktion
- Überschreiben der Festplattendaten nach Ausführung eines Jobs oder nach Einschalten des Systems
- Kommunikation mit TLS
- Integritätsprüfung
- Managementfunktionen wie:  
Systemprotokolle, Kennwörter, Benutzer, Kennwortrichtlinie, Datum & Uhrzeit, Automatische Rückstellung, Sitzungszeitgeber, Ein-/Ausschalten von TLS

Wir haben die ISO/IEC 15408 Zertifizierung für Systemumgebungen mit folgendem Equipment in den Sprachen Japanisch und Englisch bei Anbindung an einen a PC unter Windows 7 mit Internet Explorer Version 9.0 beantragt.

Multifunktionssystem: ES9466 MFP/ES9476 MFP\*

\* Die Zertifizierung steht bevor (Stand: April 2016)

Zum Betrieb des Systems im hohen Sicherheitsmodus gemäß IEEE-Standard 2600.1™-2009 ist eine entsprechende Konfiguration der Systemumgebung wie eine Protokollverschlüsselung sowie Authentifizierung von Server und Client PC erforderlich.

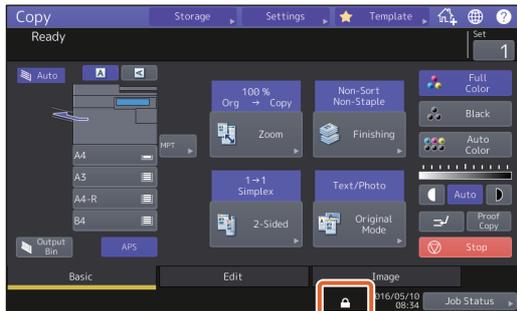
Nur wenn die in diesem Handbuch beschriebenen Bedingungen erfüllt sind, kann das System in Übereinstimmung mit IEEE Std 2600.1™-2009 betrieben werden.

### Tipps

Zu Einzelheiten über die jeweiligen Sicherheitsfunktionen und deren Einstellung siehe **TopAccess-Anleitung**.

## ■ Prüfen des Modus

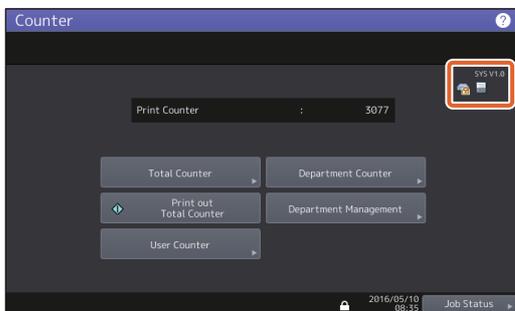
Im hohen Sicherheitsmodus wird  im Touch Screen des Systems angezeigt.



### Tipps

- Im hohen Sicherheitsmodus sind die Daten auf der Festplatte des Systems verschlüsselt. Zusätzlich ist in derartigen Systemen der Data Overwrite Kit (GP-1070) installiert. Die Prüfung der jeweiligen Funktion kann oben rechts im [Zähler (Counter)]-Bildschirm des Systems durchgeführt werden.

Die HDD ist verschlüsselt.	 wird angezeigt. Im hohen Sicherheitsmodus sind die Daten auf der Festplatte des Systems verschlüsselt.
Der Data Overwrite Enabler ist aktiviert.	 zeigt an, dass der Data Overwrite Enabler korrekt funktioniert. Die aktuell ausgeführte Systemversion wird angezeigt. (SYS V1.0)



- Wenn der Data Overwrite Enabler installiert ist, wird der Festplattenbereich für temporäre Daten nach der Abmeldung des Anwenders überschrieben und kann dann für den nächsten Job verwendet werden.

---

## ■ Bedingungen

**Befolgen Sie das oben beschriebene Bedienkonzept, da sonst die Datensicherheit nicht gewährleistet ist und ein unbefugter Zugriff auf das System erfolgen kann.**

**Stellen Sie die [MFP Lokale Authentifizierung (MFP Local Authentication)] unter [Authentifizierungsmethode (Authentication Method)] in [Benutzerverwaltung (User Management)] ein. Wenn die [Windows Domain Authentifizierung (Windows Domain Authentication)] oder [LDAP Authentifizierung (LDAP Authentication)] als Benutzerauthentifizierung eingestellt ist, erfüllt das System nicht die Voraussetzung für IEEE Std 2600.1™-2009.**

**Führen Sie in der manuellen Einstellung [VOLL (FULL)] die Integritätsprüfung direkt nach der Installation und danach in regelmäßigen Abständen durch.**

\* Zu Einzelheiten über die Integritätsprüfung siehe *MFP Management-Anleitung*.

**Ändern Sie nicht die Kommunikations-Voreinstellungen des Systems. Die Netzwerk-Kommunikation kann über TLS geschützt werden, sofern dies nicht geändert wird.**

**In einem der folgenden Fälle wenden Sie sich bitte an Ihren Servicetechniker.**

- Wenn das Symbol für die Festplattenverschlüsselung () nicht angezeigt wird.
- Wenn das Symbol für das korrekte Funktionieren des Data Overwrite Enabler () nicht angezeigt wird.
- Wenn die angezeigte Systemversion von der tatsächlichen abweicht.

**Im Modus für hohe Sicherheit können folgende Funktionen nicht benutzt werden.**

- Unterbrechungskopie
- Netzwerk Fax
- Adressbuchanzeige
- Datei-Downloader
- TWAIN-Treiber
- e-Filing BackUp/Restore Dienstprogramm
- Zeitversetzter Druck
- Speichern in e-Filing per Druckertreiber\*

\* Die Funktion kann zwar ausgewählt werden; aber ein Fehler tritt auf und der Job wird gelöscht. Daher wird der Druck nicht ausgeführt. Gelöschte Jobs werden im Fehlerprotokoll aufgezeichnet. Prüfen Sie dies in TopAccess unter [Protokolle (Logs)] oder am System unter [Job Status] - [Protokolle (Log)] - [Drucken (Print)].

- Deaktivierung der Protokollauthentifizierung

**Die automatische Benutzeranmeldung der mit dem System ausgelieferten Clientsoftware steht nicht zur Verfügung. Zur Benutzung der Clientsoftware müssen Sie immer Benutzernamen und Kennwort eingeben.**

**An das System gesendete Daten wie Fax und Internet Fax oder vom Druckertreiber\* empfangene Druckdaten können nur gedruckt werden, wenn ein Anwender mit entsprechenden Benutzerrechten am System angemeldet ist.**

\* Verwenden Sie IPP SSL zur Kommunikation mit diesem System.

**Verwenden Sie für den IPP-Druck den, durch Eingabe von “https://[IP-Adresse IP address]][:SSL Portnummer (SSL port number)]/Print” in das URL-Feld, erzeugten Port.**

(Z.B.: https://192.168.1.2:443/Print)

\* Zu Einzelheiten siehe [IPP-Druck (IPP printing)] unter [Druckertreiber für Windows installieren (Installing Printer Drivers for Windows)] - [Weitere Installationen (Other Installations)] in der **Software Installationsanleitung**.

**Wenn Sie Daten wie etwa Adressbuchdaten importieren, müssen die Daten aus diesem System exportiert worden sein.**

**Verwenden Sie keine Anwendungen, die eine Änderung im Untermenü [ODCA] von [Setup] im Register [Verwaltung (Administration)] von TopAccess erfordert.**

**Aktivieren Sie nicht [Kennwort Authentifizierung für Druckjobs verwenden (Use Password Authentication for Print Job)], wenn Sie mit einem der folgenden Druckertreiber drucken; PCL (PCL6), PS (PostScript) und dem XPS Druckertreiber ausgeliefert.**

**Zur sicheren Benutzung des Systems sind folgende Punkte einzustellen:**

#### **Hinweis**

Führen Sie eine korrekte Einstellung anhand der Liste der Anfangswerte (📖 S.19) durch.

- Verwenden Sie zum Speichern oder Senden von Dateien das verschlüsselte PDF Format mit der Verschlüsselungsstufe 128 bit AES.
- Definieren Sie einen zuverlässigen PC als Speicherziel für Scandaten.
- Verwenden Sie als Speicherziel nicht die ÖFFENTLICHE BOX in e-Filing, da hierfür kein Kennwortschutz möglich ist.
- Verwenden Sie als Speicherziel nicht MFP LOKAL, da hierfür kein Kennwortschutz möglich ist.
- Administratoren sollten die Systemprotokolle regelmäßig exportieren und speichern.

**Der Administrator sollte den Anwendern mitteilen, dass der hohe Sicherheitsmodus für dieses System aktiviert ist und die Anwender über folgende Punkte informieren, damit sie sich entsprechend verhalten können.**

- Das Drucken sollte mit den Druckertreiber-Einstellungen für IPP-Druck durchgeführt werden.
- Es sollte ein zuverlässiger PC als Speicherziel für Scandaten definiert werden.
- Für e-Filing sollte kein freigegebener Ordner verwendet werden.
- Es sollten keine lokalen Ordner des Systems verwendet werden.

**Zur Entsorgung des Systems wenden Sie sich bitte an Ihren Servicetechniker, damit die auf der Festplatte gespeicherten Daten vollständig gelöscht werden.**



## BESONDERE FUNKTIONEN

<b>Temporäres Kennwort</b> .....	<b>14</b>
Fälle, in denen ein temporäres Kennwort verwendet wird .....	14
Benutzerhinweise für die Verwendung eines temporären Kennworts .....	14
<b>Halten (Fax)</b> .....	<b>15</b>

## Temporäres Kennwort

---

Im hohen Sicherheitsmodus wird ein vom Administrator vergebenes, vorläufiges Kennwort als temporäres Kennwort angesehen. Zur weiteren Verwendung des Systems müssen Sie das temporäre Kennwort nach dem ersten Zugriff auf das System durch ein eigenes Kennwort ersetzen.

### Hinweis

Wenn Sie das temporäre Kennwort weiter verwenden, ist die Sicherheitsstufe unzureichend. Speichern Sie so bald wie möglich ein eigenes Kennwort.

## ■ Fälle, in denen ein temporäres Kennwort verwendet wird

Ein temporäres Kennwort wird in folgenden Fällen verwendet:

- Für die erste Systemanmeldung nach der Registrierung durch den Administrator.
- Wenn ein Administrator das Benutzerkennwort zurückgesetzt hat.
- Wenn das Kennwort als Klartext vom Administrator importiert wurde.

### Hinweis

Wenn ein Administrator das Benutzerkennwort zurückgesetzt hat, muss der Anwender darüber informiert werden, sein Kennwort durch ein eigenes zu ersetzen.

### Tipp

Um zu verhindern, dass exportierte Benutzerinformationen verändert werden, sind diese mit Hash versehen. Wird das Kennwort für die exportierten Benutzerinformationen geändert, erfolgt dies unverschlüsselt (in Klartext).

## ■ Benutzerhinweise für die Verwendung eines temporären Kennworts

### Wenn Ihr Kennwort bei einem Zugriff auf das System registriert werden kann.

- Kennwort über das Bedienfeld speichern  
Geben Sie den Benutzernamen und ein temporäres Kennwort im Menü der Benutzeranmeldung ein. Nach Drücken auf [OK] im Bestätigungsbildschirm für das temporäre Kennwort erscheint der Kennwort-Eingabebildschirm. Geben Sie das temporäre Kennwort in [Altes Kennwort (Old Password)] ein. Geben Sie Ihr neues Kennwort in [Neues Kennwort (New Password)] und [Neues Kennwort wiederholen (Retype New Password)] ein und drücken Sie [OK]. Das neue Kennwort ist registriert und Sie können es für die nächste Systemanmeldung benutzen.
- Kennwort in TopAccess speichern  
Wenn Sie über TopAccess auf das System zugreifen, erscheint der Anmeldebildschirm. Geben Sie im Anmeldebildschirm den Benutzernamen und ein temporäres Kennwort ein und drücken Sie [Anmeldung (Login)]. Wenn die Anzeige zur Registrierung erscheint, geben Sie Ihr neues Kennwort in [Neues Kennwort (New Password)] und [Neues Kennwort wiederholen (Retype New Password)] ein und drücken [Speichern (Save)]. Das neue Kennwort ist registriert und Sie können es für die nächste Anmeldung in TopAccess benutzen.

### Wenn das Kennwort bei einem Zugriff auf das System nicht registriert werden kann.

Mit folgenden Dienstprogrammen können Sie nicht mit temporärem Kennwort auf das System zugreifen. Daher kann auch kein neues Kennwort registriert werden. Registrieren Sie ein neues Kennwort über das Bedienfeld oder in TopAccess, bevor Sie diese Dienstprogramme verwenden.

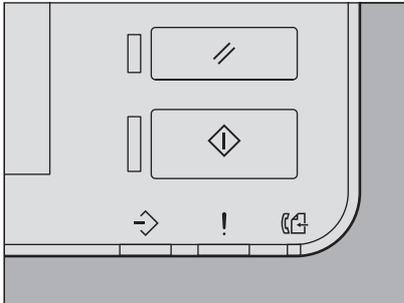
- Remote Scan Treiber
- e-Filing Web Dienstprogramm

## Halten (Fax)

Im Modus für hohe Sicherheit werden empfangene Emails, die ein Fax, Internetfax oder Bilddaten enthalten, nicht automatisch ausgedruckt. Diese Jobs werden in der Warteschlange [Halten (Fax) (Hold (Fax))] gespeichert und können nur von Anwendern gedruckt werden, die über die Berechtigung [Fax Empfangsdruck (Fax Received Print)] verfügen.

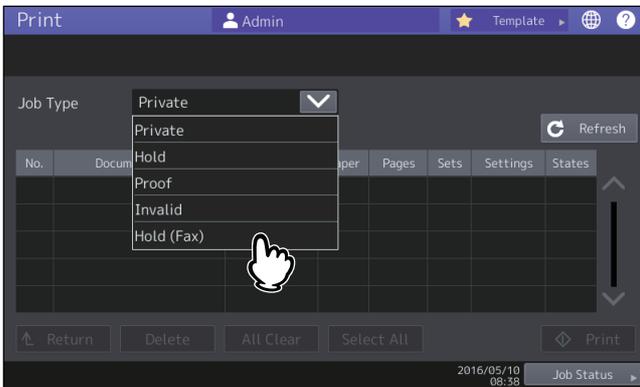
### Tipps

Wenn sich in der Warteschlange [Halten (Fax) (Hold (Fax))] Jobs befinden, blinkt die Anzeige DATEN IM SPEICHER.



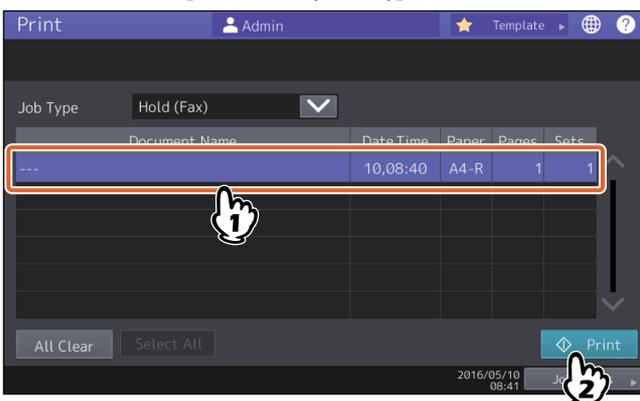
### Jobs in der Warteschlange Halten (Fax) drucken

- 1 **Melden Sie sich mit Benutzerrechten für [Faxempfang drucken (Fax Received Print)] am System an.**
- 2 **Drücken Sie [Druckmodus (Print Mode)] in der Home-Anzeige.**
- 3 **Wählen Sie [Halten (Fax) (Hold (Fax))].**



- Alle Jobs in der Warteschlange [Halten (Fax) (Hold (Fax))] werden angezeigt.

- 4 **Wählen Sie den gewünschten Job oder drücken Sie [Alle Wählen (Select All)] und drücken Sie anschließend [Drucken (Print)].**



- Der Job wird ausgegeben und anschließend aus der Warteschlange [Halten (Fax) (Hold (Fax))] gelöscht.



## DIE VOREINSTELLUNGEN

<b>Sicherheitshinweise zu den Voreinstellungen .....</b>	<b>18</b>
Systemanmeldung.....	18
Tabelle der Voreinstellungen .....	19

## Sicherheitshinweise zu den Voreinstellungen

---

Die Voreinstellungen und die einstellbaren Positionen unterscheiden sich im Modus mit hoher Sicherheit vom normalen Sicherheitsmodus. Diese Unterschiede sind nachfolgend beschrieben.

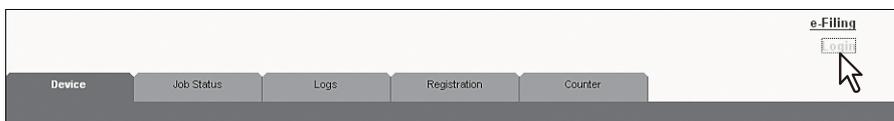
Zur Erfüllung von IEEE Std 2600.1™-2009 müssen, gemäß diesem Kapitel, die Anfangswerte auf den hohen Sicherheitsmodus geändert werden und müssen unverändert erhalten bleiben.

### Hinweise

- Zu den Anfangseinstellungen und die einstellbaren Positionen im normalen Sicherheitsmodus siehe **TopAccess-Anleitung** und **MFP Management-Anleitung**.
- Sichern Sie alle Systemeinstellungen und Benutzerdaten, bevor Sie eine “Initialisierung” des Systems durchführen und dadurch alle Einstellungen zurücksetzen. Einzelheiten siehe **TopAccess-Anleitung** und **MFP Management-Anleitung**.

## ■ Systemanmeldung

- Die Register [Benutzerverwaltung (User Management)] und [Administration (Administration)] werden in TopAccess nur angezeigt, wenn die Systemanmeldung mit Administratorrechten erfolgt. Öffnen Sie TopAccess, klicken Sie oben rechts auf “Login” und geben Sie Benutzername und Kennwort ein.



- Melden Sie sich im Register [Admin] in den [Einstellung (Setting)] des Systems als Anwender mit Administratorrechten an.

## ■ Tabelle der Voreinstellungen

### Home-Anzeige:

- [Einstellung -Benutzer- (Setting -User-)] Menü
- [Admin] Register
- [Listen/Berichte (List/Report)] Menü
- [Berichteinstellungen (Report Setting)] Menü

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
[Komm. Bericht (Comm. Report)]		
Speich. Send	AUS	Ändern Sie diese Einstellung nicht auf "EIN".

\* Die oben stehenden Menüs können nicht mit TopAccess geöffnet werden.

### TopAccess:

- Register [Administration]
- Menü [Setup]
- Untermenü [Allgemein (General)]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
Geräte-Informationen		
USB-Direktdruck	Deaktiviert	
Funktionen		
Speichern unter FTP	Deaktiviert	
Speichern auf USB Medium	Deaktiviert	
Speichern unter SMB	Deaktiviert	
Speichern unter Netware	Deaktiviert	
Netzwerk iFax	Deaktiviert	
Netzwerk Fax	Deaktiviert	
Web Services Scan	Deaktiviert	
Twain Scan	Deaktiviert	
Adressbuchgebrauch einschränken durch Administrator / AddressbookRemoteOperator		
Benutzung nur durch Administrator / AddressbookRemoteOperator		
Energiesparmodus		
Autom. Löschen *	45 Sek.	Diese Voreinstellung entspricht dem normalen Sicherheitsmodus; sie kann nicht auf AUS geändert werden.

\* Die Einstellung kann im Touch Screen des Systems im Register [ADMIN] unter [Einstellung -Benutzer- (Setting -User-)] geändert werden.

Untermenü [Netzwerk (Network)]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
SMB		
SMB Server-Protokoll	Deaktiviert	
HTTP		
SSL*	Aktiviert	
WSD		
SSL	Aktiviert	
Web-Dienste Druck	Deaktiviert	
Web-Dienste Scan	Deaktiviert	
SMTP Server		
SMTP-Server	Deaktiviert	
FTP-Server		
FTP-Server	Deaktiviert	
SSL	Aktiviert	
SMTP-Client		
SSL	Mit importierten CA Zertifikat(en) prüfen	Die Sicherheitseinstellung ist "Mit importierten CA Zertifikat(en) prüfen" oder "Alle Zertifikate ohne CA akzeptieren".
Authentifizierung	AUTO	Achten Sie darauf, dass in Ihrer Systemumgebung entweder "CRAM-MD5", "Digest-MD5", "Kerberos" oder "NTLM (IWA)" angewendet wird.
POP3-Client		
SSL aktivieren	Mit importierten CA Zertifikat(en) prüfen	
FTP Client		
SSL Einstellung	Mit importierten CA Zertifikat(en) prüfen	
Bonjour		
Bonjour	Deaktiviert	
SNMP		
SNMP V1/V2	Deaktiviert	
SNMP V3	Aktiviert	
SLP		
SLP	Deaktiviert	
Syslog Einstellung		
SSL aktivieren	Mit importierten CA Zertifikat(en) prüfen	

\* Die Einstellung kann im Touch Screen des Systems im Register [ADMIN] unter [Einstellung -Benutzer- (Setting -User-)] geändert werden.

Untermenü [Drucker (Printer)]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
Allgemeine Einstellung		
Einschränkung für Druckjobs	Nur Halten	

Untermenü [Druckdienst (Print Service)]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
Raw TCP-Print		
Raw-TCP	Deaktiviert	
LPD-Druck		
LPD	Deaktiviert	
IPP Druck		
SSL	Aktiviert	
FTP Druck		
FTP-Druck	Deaktiviert	

Untermenü [ODCA]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
Netzwerk		
Port aktiviert	Deaktiviert	

Menü [Sicherheit (Security)]

Untermenü [Authentifizierung (Authentication)]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
Einstellung der Benutzerauthentifizierung		
Benutzer Authentifizierung	Aktiviert	Die Einstellung kann nicht auf "Deaktiviert" geändert werden.
Benutzerauthentifizierung entsprechend der Funktion	Deaktiviert	Ändern Sie diese Einstellung nicht auf "Aktiviert".
Kennwort Authentifizierung für Druckjobs verwenden	Deaktiviert	Ändern Sie diese Einstellung nicht auf "Aktiviert".
Gastanwender	Nicht markiert (Deaktiviert)	Diese Voreinstellung entspricht dem normalen Sicherheitsmodus; sie kann nicht auf "Aktiviert" geändert werden.
Authentifizierung Typ	Lokale MFP-Authentifizierung	
Authentifizierung mit PIN Code	Deaktiviert	Ändern Sie diese Einstellung nicht auf "Aktiviert".
Freigegebene Benutzerverwaltung	Deaktiviert	Ändern Sie diese Einstellung nicht auf "Aktiviert".

Untermenü [Kennwortrichtlinie (Password Policy)]

<b>Position</b>	<b>Anfangswert für den hohen Sicherheitsmodus</b>	<b>Anmerkungen</b>
Richtlinie für Benutzer		
Minimale Kennwortlänge	8 (Stellen)	
Voraussetzungen anwenden	Aktiviert	
Sperreinstellung	Aktiviert	(Identisch mit normalem Sicherheitsmodus)
Anzahl Wiederholungen	3 (mal)	
Sperrzeit	2 (Minuten)	
Verfügbarer Zeitraum	Deaktiviert	(Identisch mit normalem Sicherheitsmodus)
Ablauftag(e)	90 (Tage)	
Richtlinie für Administrator, Auditor		
Minimale Kennwortlänge	8 (Stellen)	
Voraussetzungen anwenden	Aktiviert	
Sperreinstellung	Aktiviert	(Identisch mit normalem Sicherheitsmodus)
Anzahl Wiederholungen	3 (mal)	
Sperrzeit	2 (Minuten)	
Verfügbarer Zeitraum	Deaktiviert	(Identisch mit normalem Sicherheitsmodus)
Ablauftag(e)	90 (Tage)	
Richtlinie für e-Filing Boxen, Vorlagengruppen, Vorlagen, SicherePDF, SNMPv3, Klonen und Sicherer Empfang		
Minimale Kennwortlänge	8 (Stellen)	
Zu erfüllende Anforderungen	Aktiviert	
Sperreinstellung	Aktiviert	(Identisch mit normalem Sicherheitsmodus)
Anzahl Wiederholungen	3 (mal)	
Sperrzeit	2 (Minuten)	



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

[www.oki.com/printing/](http://www.oki.com/printing/)

