TOSHIBA

MULTIFUNKTIONALE DIGITALE FARBSYSTEME /
MULTIFUNKTIONALE DIGITALSYSTEME

Sicherheitseinstellungen Management Anleitung

e-STUDIO2010AC/2510AC
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC
e-STUDIO2518A/3018A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO5518A/6518A/7518A/8518A
e-STUDIO330AC/400AC

Vorwort

Wir danken Ihnen, dass Sie sich für unser Produkt entschieden haben.
Dieses Handbuch beschreibt die Voraussetzungen und Einstellungen des digitalen Multifunktionssystems für die Erfüllung der CC Zertifizierung.
Lesen Sie dieses Handbuch, bevor Sie die Ihr digitales Multifunktionssystem in diesem hohen Sicherheitsmodus benutzen. Lesen Sie die “Sicherheitshinweise” unter “Sicherheitsinformationen”, damit das System in Übereinstimmung mit der CC Zertifizierung betrieben werden kann.
Halten Sie dieses Handbuch griffbereit, damit Sie es jederzeit für die Verwendung des Systems gemäß CC Zertifizierung 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.

❑ Modellserien in diesem Handbuch

In diesem Handbuch werden die einzelnen Modellnamen durch einen Seriennamen ersetzt.

Modellname	Serienname
e-STUDIO2010AC/2510AC	e-STUDIO5015AC Serie
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC	
e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A	e-STUDIO5018A Serie
e-STUDIO5516AC/6516AC/7516AC	e-STUDIO7516AC Serie
e-STUDIO5518A/6518A/7518A/8518A	e-STUDIO8518A Serie
e-STUDIO330AC/400AC	e-STUDIO400AC Serie

❑ Optionales Equipment

Einzelheiten zu den verfügbaren Optionen siehe **Kurzbedienungsanleitung**.

❑ Handelsmarken

Zu den Handelsmarken siehe **Sicherheitsinformationen**.

INHALT

1

HOHER SICHERHEITSMODUS

Dieser Modus schützt das System vor unbefugten Zugriffen und Informationsverlust.
Die folgenden Sicherheitsfunktionen entsprechen der CC Zertifizierung.

- Benutzerverwaltung
- Funktionszuweisungen
- Protokollierung und Suchfunktion
- Kommunikationsfunktion mit TLS1.2
- Integritätsprüfung
- Managementfunktionen wie:
  Systemprotokolle, Kennwörter, Benutzer, Kennwortrichtlinie, Datum & Uhrzeit, Automatische Rückstellung, Sitzungszeitgeber, Ein-/Ausschalten von TLS

Die ISO/IEC15408 Zertifizierung wird einem System (bei installierter Fax-Unit und IPv4-Nutzung) erteilt, wenn die unten aufgeführte Kombination von Betriebssystemen und Browsern in den Systemsprachen Japanisch oder Englisch verwendet werden.

PP Kennzeichen: HCD-PP

OS:	Windows 10
Browser:	Internet Explorer 11
Multifunktionssystem:	e-STUDIO2010AC/2510AC e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC e-STUDIO2018A/2518A/3018A/3518A/4518A/5018A e-STUDIO5516AC/6516AC/7516AC e-STUDIO5518A/6518A/7518A/8518A e-STUDIO330AC/400AC*

* Die Zertifizierung steht bevor (Stand: März, 2020)

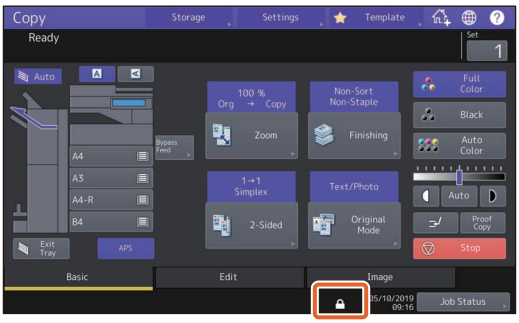
Zum Betrieb des Systems im hohen Sicherheitsmodus gemäß CC Zertifizierung ist eine entsprechende Konfiguration der Systemumgebung wie Daten- und Protokollverschlüsselung sowie Authentifizierung von Server und Client PC erforderlich.
Nur wenn die in diesem Handbuch beschriebenen Bedingungen erfüllt sind, kann das System in Übereinstimmung mit der CC Zertifizierung betrieben werden.

Tipp

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.



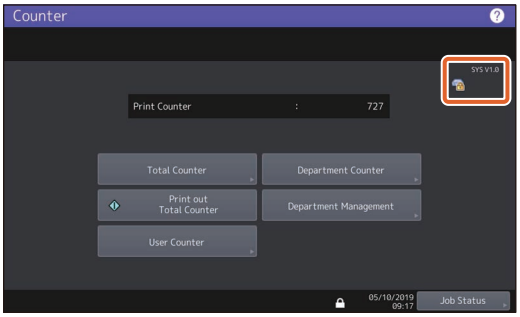
Hinweis

Nachdem Ihr Servicetechniker die Einstellungen des Systems geändert hat, kontrollieren Sie bitte, dass  im Touch Screen angezeigt wird.
Kontrollieren Sie bitte auch anhand der Liste der Anfangswerte, dass die Einstellungen korrekt sind.
📖 S.19 “Tabelle der Voreinstellungen”

Tipp

- Im hohen Sicherheitsmodus sind die Daten auf dem internen Datenträger des Systems verschlüsselt.
  Die Prüfung der jeweiligen Funktion kann oben rechts im [Zähler (Counter)]-Bildschirm des Systems durchgeführt werden.

Der interne Datenträger ist verschlüsselt.	 wird angezeigt. Im hohen Sicherheitsmodus sind die Daten auf dem internen Datenträger verschlüsselt.



- Wenn eine FIPS Festplatte installiert ist, wird deren Status durch ein Symbol im Touch Screen angezeigt.

■ 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 die CC Zertifizierung.

Damit der Sicherheitsstatus gemäß CCC Zertifizierung erhalten bleibt, müssen bei Erstellen eines selbstsignierten Zertifikats "RSA2048" für den öffentlichen Schlüssel und "SHA256", "SHA384" oder "SHA512" für den Signaturalgorithmus verwendet werden.

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 **e-STUDIO 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 Verschlüsselung des internen Datenträgers () nicht angezeigt wird.
- Wenn die angezeigte Systemversion von der tatsächlichen abweicht.

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

- e-Filing
- Unterbrechungskopie
- Netzwerk Fax
- Adressbuchanzeige
- Datei-Downloader
- TWAIN-Treiber
- e-Filing BackUp/Restore Dienstprogramm
- Zeitversetzter Druck
- Deaktivierung der Protokollauthentifizierung
- Mailbox
- E-Mail Empfangsdruck
- POP3 Einstellung deaktivieren
- Daten Backup/Restore

Die automatische Benutzeranmeldung über die 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/TLS zur Kommunikation mit diesem System.

Für den IPP-Druck wird der Port genutzt, der durch Eingabe von "https://[IP-Adresse (IP address)]:[SSL Portnummer (SSL port number)]/Print" in das URL-Feld erzeugt wurde.
(z.B.: https://192.168.1.2:631/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; Universal Drucker 2, Universal PS3 und Universal XPS.

Die Funktion Integritätsprüfung wird automatisch beim Start des Systems ausgeführt. Wenn "Service erforderlich" angezeigt wird, wenden Sie sich bitte an Ihren Servicetechniker.

Für den Betrieb des Systems im hohen Sicherheitsmodus ist ein Syslog-Server erforderlich, der TLS1.2 unterstützt.

Der Zugriff auf Drucken, Kopieren, Scannen und Faxsendung/-empfang ist durch die Benutzerauthentifizierung eingeschränkt. Alle Benutzer können die Listen der verarbeiteten und angehaltenen Jobs prüfen. Nur das Prüfen der Liste über empfangene Faxjobs erfordert die Zugriffsrechte eines Administrators oder FaxOperators. Je nach zugewiesener Berechtigung können Benutzer Jobs ausdrucken, löschen, pausieren oder die Jobreihenfolge ändern. Verfügen Benutzer über die Rechte eines Administrators oder Benutzers, können sie Jobs erstellen. Verfügen Benutzer über die Rechte eines FaxOperators, können Sie Fax-Sendejobs/Fax-Empfangsjobs erstellen, drucken und löschen. Benutzer können jedoch nur die Fax-Sendejobs ihres eigenen Benutzerkontos drucken und löschen. Verfügen Benutzer über die Rechte eines Benutzers, können sie nur die Jobs ihres eigenen Benutzerkontos drucken und löschen. Verfügen Benutzer über die Rechte eines Administrators, können sie alle Jobs löschen und pausieren sowie die Reihenfolge angehaltener Jobs ändern. Verfügen Benutzer über die Rechte eines AccountManagers oder AddressBookRemoteOperators, ist für sie das Drucken, Löschen, Pausieren und das Ändern der Reihenfolge von Druck-, Kopier- oder Faxjobs nicht verfügbar.

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.
- Es sollte ein zuverlässiger PC als Speicherziel für Scandaten definiert werden.
- Verwenden Sie als Speicherziel nicht MFP LOKAL, da hierfür kein Kennwortschutz eingerichtet werden kann.
- Administratoren sollten die Systemprotokolle regelmäßig exportieren und speichern.
- Aktivieren Sie den E-Mail-Direktdruck nicht mit der Einstellung [Auto].
- Nach dem Upload oder dem Entfernen der CA Zertifizierung muss das System neu gestartet werden.

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.
- Es sollten keine lokalen Ordner des Systems verwendet werden.

Der Administrator sollte kontrollieren, dass eine permanente Kommunikationsverbindung zum Syslog-Server besteht.

Zur Entsorgung des Systems wenden Sie sich bitte an Ihren Servicetechniker, damit die auf dem internen Datenträger gespeicherten Daten vollständig gelöscht werden.

2

BESONDERE FUNKTIONEN

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 Kennworts 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] iim 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.

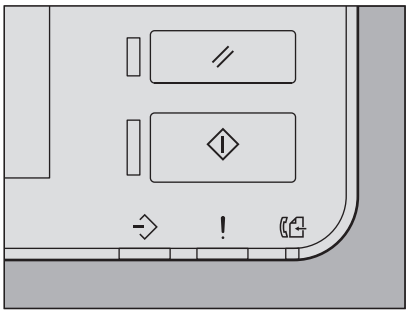
- Remote Scan Treiber
- e-Filing Web Dienstprogramm

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.

Tipp

- Sie können eine Vorschau des empfangenen Faxbildes im Touch Screen prüfen, bevor Sie das Fax ausdrucken. Einzelheiten siehe **GD-1370 Faxanleitung**.
- Wenn sich in der Warteschlange [Halten (Fax) (Hold (Fax))] Jobs befinden, blinkt die Anzeige Faxspeicher.

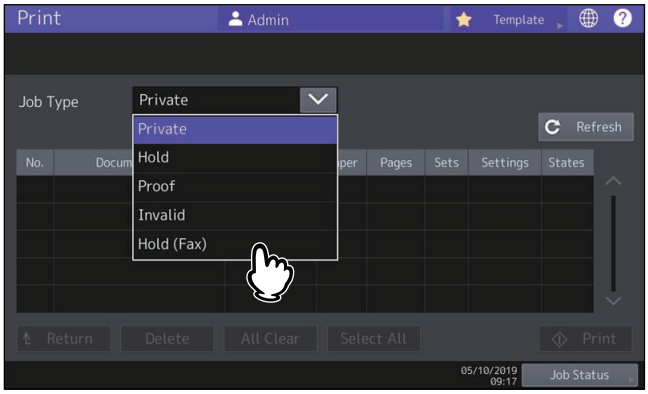


■ Jobs in der Warteschlange Halten (Fax) drucken

1 Melden Sie sich mit Benutzerrechten für [Faxempfang drucken (Fax Received Print)] am System an.

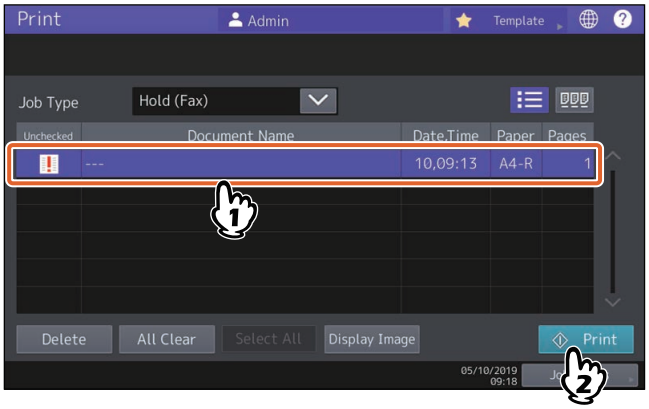
2 Drücken Sie [Druckmodus (Print Mode)] in der Home-Anzeige.

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.

3

DIE VOREINSTELLUNGEN

Sicherheitshinweise zu den Voreinstellungen

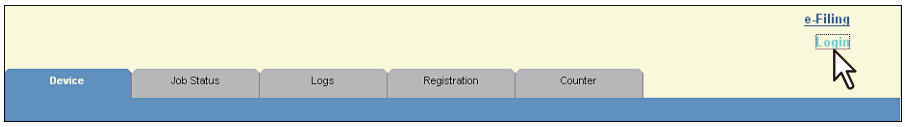
Die Voreinstellungen und die einstellbaren Positionen unterscheiden sich im Modus mit hoher Sicherheit vom normalen Sicherheitsmodus. Diese Unterschiede sind nachfolgend beschrieben.
Zur Erfüllung der CC Zertifizierung müssen gemäß diesem Kapitel, die Anfangswerte auf den hohen Sicherheitsmodus geändert werden und müssen unverändert erhalten bleiben.

Hinweis

- Zu den Anfangseinstellungen und die einstellbaren Positionen im normalen Sicherheitsmodus siehe **TopAccess-Anleitung** und **e-STUDIO 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 **e-STUDIO Management-Anleitung**.

■ Systemanmeldung

- Die Register [Benutzerverwaltung (User Mangagement)] und [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 [Anwender Funktionen (User Function)] des Systems als Anwender mit Administratorrechten an.

■ Tabelle der Voreinstellungen

Home-Anzeige:
[User Funktion-Anwender- (User Functions -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		
e-Filing	Aktiviert	Die Einstellung muss auf “Deaktiviert” geändert werden.
Speichern unter FTP	Deaktiviert	
Speichern auf USB Medium	Deaktiviert	
Speichern unter SMB	Deaktiviert	
Speichern unter Netware	Deaktiviert	
iFax Sendung	Aktiviert	
Fax Sendung	Aktiviert	
Netzwerk iFax	Deaktiviert	
Netzwerk Fax	Deaktiviert	
Web-Dienste Scan	Deaktiviert	
Twain Scan	Deaktiviert	
Adressbuchgebrauch einschränken durch Administrator / AddressbookRemoteOperator		
Benutzung nur durch Administrator / AddressbookRemoteOperator		
Energie sparen		
Autom. Löschen *	45 Sek.	Diese Voreinstellung entspricht dem normalen Sicherheitsmodus; sie kann nicht auf AUS geändert werden.
Startseite Einstellung		
Portnummer	990	
SSL/TLS aktivieren	Aktiviert	

* Die Einstellung kann im Touch Screen des Systems im Register [ADMIN] unter [User Funktion -Anwender- (User Functions -User-)] geändert werden.

Untermenü [Netzwerk (Network)]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
IPv6		
IPv6 aktivieren	Aktiviert	Die Einstellung muss auf “Deaktiviert” geändert werden.
SMB		
SMB Server-Protokoll	Deaktiviert	
HTTP		
SSL/TLS* aktivieren	Aktiviert	
WSD		
SSL/TLS aktivieren	Aktiviert	
Web-Dienste Druck	Deaktiviert	
Web-Dienste Scan	Deaktiviert	
SMTP Server		
SMTP-Server	Deaktiviert	
FTP-Server		
FTP-Server	Deaktiviert	
SSL/TLS aktivieren	Aktiviert	
SMTP-Client		
SSL/TLS aktivieren	Mit importierten CA Zertifikat(en) prüfen	
Authentifizierung	AUTO	Achten Sie darauf, dass in Ihrer Systemumgebung entweder “CRAM-MD5”, “Digest-MD5”, “Kerberos” oder “NTLM (IWA)” angewendet wird.
POP3-Client		
POP3-Client aktivieren	Aktiviert	Die Einstellung muss auf “Deaktiviert” geändert werden.
SSL/TLS aktivieren	Mit importierten CA Zertifikat(en) prüfen	
FTP Client		
SSL/TLS Einstellung	Mit importierten CA Zertifikat(en) prüfen	
Bonjour		
Bonjour	Deaktiviert	
SNMP		
SNMP V1/V2	Deaktiviert	
SNMP V3	Aktiviert	
SLP		
SLP	Deaktiviert	

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
Syslog Einstellung		
Syslog aktivieren	Aktiviert	
SSL/TLS aktivieren	Mit importierten CA Zertifikat(en) prüfen	
Schweregrad - Fehler	Aktiviert	
Schweregrad - Warnung	Aktiviert	
Schweregrad - Information	Aktiviert	
Standort - Sicherheit/ Autorisierung	Aktiviert	
Standort - Lokale Nutzung0	Aktiviert	
Standort - Lokale Nutzung1 (Auftragsprotokoll)	Aktiviert	

* Die Einstellung kann im Touch Screen des Systems im Register [ADMIN] unter [User Funktion -Anwender- (User Functions -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/TLS aktivieren	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)]

Position	Anfangswert für den hohen Sicherheitsmodus	Anmerkungen
Richtlinie für Benutzer		
Minimale Kennwortlänge	8 (Stellen)	Stellen Sie ein Kennwort von mindestens 15 Stellen mit alphanumerischen Zeichen (inkl. Buchstaben mi deutschen Umlauten und französischen Unterhäkchen), Symbolen (! # ( ) * + , - . / : ; = ? @ $ ^ _ ` { | } ~ \) und einer Leerstelle ein.
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)	Stellen Sie ein Kennwort von mindestens 15 Stellen mit alphanumerischen Zeichen (inkl. Buchstaben mi deutschen Umlauten und französischen Unterhäkchen), Symbolen (! # ( ) * + , - . / : ; = ? @ $ ^ _ ` { | } ~ \) und einer Leerstelle ein.
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, Sicheres PDF, SNMPv3, Klonen und Sicherer Empfang		
Minimale Kennwortlänge	8 (Stellen)	Stellen Sie ein Kennwort von mindestens 15 Stellen mit alphanumerischen Zeichen (inkl. Buchstaben mi deutschen Umlauten und französischen Unterhäkchen), Symbolen (! # ( ) * + , - . / : ; = ? @ $ ^ _ ` { | } ~ \) und einer Leerstelle ein.
Voraussetzungen anwenden	Aktiviert	
Sperreinstellung	Aktiviert	(Identisch mit normalem Sicherheitsmodus)
Anzahl Wiederholungen	3 (mal)	
Sperrzeit	2 (Minuten)	

4

ANHANG

Liste der Zielereignisse für Überwachung und Protokollierung, welche an den Syslogserver gesendet werden

Die folgenden Informationen werden an den Syslogserver gesendet. Erfolg oder Fehler können im Ergebnisfeld geprüft werden.

- Registrierungsdatum
- Internes Protokollaufzeichnungsdatum
- Code
- Meldung
- Benutzername
- Domainname

Zielereignis für Überwachung		An den Syslogserver gesendetes Protokoll		
		Code	Ergebnis	Meldung
Start der Überwachung	Einschalten des Systems	D801	—	Eingeschaltet
Ende der Überwachung	Ausschalten des Systems	D800	—	Ausgeschaltet
Jobende	Ende des Druckjobs	4000	OK	job:Print jobId:6
	Ende des Scanjobs	2D01	OK	job:FTPStore jobId:8 to:
		2C00	OK	job:EmailSend jobId:33 to:
	Ende des Kopierjobs	4000	OK	job:Copy jobId:11
	Ende des Fax-Sendejobs	0000	OK	job:FaxSend jobId:9 to:1
	Ende des Fax-Empfangsjobs	0000	OK	job:FaxReceive jobId:10 from:1
Fehler der Benutzerauthentifizierung	Anmeldefehler	6001	NG	Fehler bei Benutzeranmeldung
Fehler der Benutzeridentifizierung				
Fehler der Benutzeridentifizierung	Anmeldefehler (Druckjob)	4041	NG	job:Print jobId:29
Anwendung der Verwaltungsfunktionen	Hinzufügen eines Benutzers	7174	OK	Aktualisieren von Benutzerinformationen Neu erstellter Benutzer
		7129	NG	Import von Benutzerinformationen fehlgeschlagen
	Festlegung oder Änderung einer Benutzer-ID	7175	OK	Aktualisieren von Benutzerinformationen Ändern von Benutzerinformationen
		717D	OK	Aktualisieren von Benutzerinformationen Rollen-/Gruppenzuweisung geändert
		7129	NG	Import von Benutzerinformationen fehlgeschlagen
	Löschen eines Benutzers	7176	OK	Aktualisieren von Benutzerinformationen Benutzer entfernt

Zielereignis für Überwachung			An den Syslogserver gesendetes Protokoll		
			Code	Ergeb-nis	Meldung
Anwendung der Verwaltungsfunktionen	Ändern von Ein-stellungen	Anzahl Wiederholungen der Kennworteingabe	7184	OK	Bearbeiten von Sicherheitseinstellungen
		Sperrzeit	7184	OK	Bearbeiten von Sicherheitseinstellungen
		Status der Kontosperre	7175	OK	Aktualisieren von Benutzerinformationen Ändern von Benutzerinformationen
		Informationen zur Kennwortrichtlinie	7184	OK	Bearbeiten von Sicherheitseinstellungen
		Automatische Abmeldezeit	7182	OK	Bearbeiten von Systemeinstellungen
		Adressbuch-registrierung	7160	OK	Neuer Kontakt hinzugefügt
		Adressbuchänderung	7166	OK	Adressbuch bearbeitet
		Löschen des Adressbuchs	7170	OK	Kontakt entfernt
		Netzwerkeinstellung	7183	OK	Bearbeiten von Netzwerkeinstellungen
Änderung von Berechtigungen einer Benutzergruppe	Änderung von Berechtigungen		717B	OK	Aktualisieren von Gruppeninformationen Ändern von Gruppeninformationen
Änderung der Systemzeit	Korrektur der Systemzeit		718A	OK	Bearbeiten von Datum & Uhrzeit
Fehler bei Sitzungskonsolidierung	Fehler bei TLS-Sitzungskonsolidierung		80C1	NG	Aufbau der TLS-Sitzung fehlgeschlagen (falscher MAC empfangen)
			80C5	NG	Aufbau der TLS-Sitzung fehlgeschlagen (Handshake-Fehler)

Hinweis

Falls für “Jobende” andere Codes als die in der Liste vorkommen, wird im Ergebnisfeld “NG” angezeigt.

Versionsliste der erhaltenen CC-Zertifizierungen

Die folgende Tabelle enthält die Versionen mit erlangter CC-Zertifizierung in Kombination mit der entsprechenden Bedienungsanleitung und den Optionen für das jeweilige Modell. Bitte kontrollieren Sie die Identifikationsnummer der jeweiligen Anleitung sowie die auf dem Typenschild und auf der Verpackung des Systems angegebenen Informationen.

Serie	Bedienungsanleitung		SYS-Version	Erforderliche Option	
	Name	Identifikationsnummer		FAX-Karte	FIPS-Festplatten Kit
e-STUDIO5015AC Serie, e-STUDIO5018A Serie	Kurzbedienungsanleitung	OME17004400	V1.0 *1	Für U.S.A.: GD-1370NA *2 Für Europa: GD-1370EU *2	GE-1230 *3
	Sicherheitsinformationen	OME17005600			
	Kopierfunktion-Anleitung	OME17006000			
	Scanfunktion-Anleitung	OME17006600			
	e-STUDIO Management-Anleitung	OME17007400			
	Software Installationsanleitung	OME17007200			
	Druckfunktion-Anleitung	OME17007000			
	TopAccess-Anleitung	OME17007600			
	Anleitung zur Software Fehlerbehebung	OME17006200			
	Anleitung zur Hardware Fehlerbehebung	OME17004800			
	Sicherheitseinstellungen Management Anleitung	OME170078B0			
	Papiermedien-Anleitung	OME17004600			
	Spezifikationsanleitung	OME17005800			
	Faxanleitung GD-1370	OME17008000			
e-STUDIO7516AC Serie, e-STUDIO8518A Serie	Kurzbedienungsanleitung	OME17005000			
	Sicherheitsinformationen	OME170056A0			
	Kopierfunktion-Anleitung	OME170060A0			
	Scanfunktion-Anleitung	OME170066A0			
	e-STUDIO Management-Anleitung	OME170074A0			
	Software Installationsanleitung	OME170072A0			
	Druckfunktion-Anleitung	OME170070A0			
	TopAccess-Anleitung	OME170076A0			
	Anleitung zur Software Fehlerbehebung	OME170062A0			
	Anleitung zur Hardware Fehlerbehebung	OME17005400			

Serie	Bedienungsanleitung		SYS-Version	Erforderliche Option	
	Name	Identifikationsnummer		FAX-Karte	FIPS-Festplatten Kit
e-STUDIO7516AC Serie, e-STUDIO8518A Serie	Sicherheitseinstellungen Management Anleitung	OME170078B0	V1.0 *1	Für U.S.A.: GD-1370NA *2 Für Europa: GD-1370EU *2	GE-1230 *3
	Papiermedien-Anleitung	OME17005200			
	Spezifikationsanleitung	OME170058A0			
	Faxanleitung GD-1370	OME170080A0			
e-STUDIO400AC Serie	Kurzbedienungsanleitung	OME19001200	V1.0 *1	Für U.S.A.: GD-1370NA-N*4 Für Europa: GD-1370EU *2	GE-1230 *3
	Sicherheitsinformationen	OME170056B0			
	Kopierfunktion-Anleitung	OME170060B0			
	Scanfunktion-Anleitung	OME170066C0			
	e-STUDIO Management-Anleitung	OME170074D0			
	Software Installationsanleitung	OME170072C0			
	Druckfunktion-Anleitung	OME170070C0			
	TopAccess-Anleitung	OME170076D0			
	Anleitung zur Software Fehlerbehebung	OME170062B0			
	Anleitung zur Hardware Fehlerbehebung	OME19001400			
	Sicherheitseinstellungen Management Anleitung	OME170078C0			
	Papiermedien-Anleitung	OME19001300			
	Spezifikationsanleitung	OME170058C0			
	Faxanleitung GD-1370	OME170080D0			

*1 Zum Prüfen der SYS-Version siehe 📖 S.9 “Prüfen des Modus”.
*2 Die Version der FAX-Karte muss “H625TA10” lauten. Zur Prüfung dieser Version siehe **TopAccess-Anleitung**.
*3 Bitten Sie Ihren Service-Techniker, das System so einzustellen, dass der Modellname des interne Datenträgers im Touch Screen angezeigt wird. Kontrollieren Sie anschließend, dass “MQ01ABU032BW”, der ID-Code für die installierte GE-1230, angezeigt wird.
*4 Die Version der FAX-Karte muss “H625TA12” lauten. Zur Prüfung dieser Version siehe **TopAccess-Anleitung**.

e-STUDIO2010AC/2510AC
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC
e-STUDIO2518A/3018A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO5518A/6518A/7518A/8518A
e-STUDIO330AC/400AC

MULTIFUNKTIONALE DIGITALE FARBSYSTEME /
MULTIFUNKTIONALE DIGITALSYSTEME

Sicherheitseinstellungen Management Anleitung

e-STUDIO2010AC/2510AC
e-STUDIO2515AC/3015AC/3515AC/4515AC/5015AC
e-STUDIO2518A/3018A/3518A/4518A/5018A
e-STUDIO5516AC/6516AC/7516AC
e-STUDIO5518A/6518A/7518A/8518A
e-STUDIO330AC/400AC

Toshiba Tec Corporation

1-11-1, OSAKI, SHINAGAWA-KU, TOKYO, 141-8562, JAPAN

Ver03 F 2020-04