SICHERHEITS-LEITFADEN FÜR MULTIFUNKTIONS-SYSTEME

imageRUNNER ADVANCE

Canon

EINFÜHRUNG

Moderne Multifunktionssysteme (MFD) von Canon sind mit Funktionen zum Drucken, Kopieren, Scannen sowie Versenden von E-Mails und optional Faxen ausgestattet. MFD haben sich mittlerweile zu eigenständigen Netzwerkkomponenten entwickelt, die neben einem großen Festplattenspeicher auch eine Reihe von Netzwerkdiensten anbieten.

Wenn ein Unternehmen diese Systeme in seine Infrastruktur eingliedert, sind verschiedene Bereiche im Rahmen der größeren Sicherheitsstrategie zu beachten, damit die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Netzwerksysteme geschützt sind.

Natürlich hat jedes Unternehmen seine eigenen speziellen Sicherheitsanforderungen. Deshalb sorgen wir nicht nur dafür, dass Canon Systeme mit geeigneten Standard-Sicherheitseinstellungen ausgeliefert werden, sondern gehen noch einen Schritt weiter: Wir stellen Ihnen eine Vielzahl von Konfigurationseinstellungen bereit, mit denen Sie das System enger an den Anforderungen Ihrer spezifischen Situation ausrichten können.

Dieses Dokument soll Ihnen als Diskussionsgrundlage dienen, damit Sie gemeinsam mit Canon oder einem Canon Partner die jeweils optimalen Einstellungen für Ihre Umgebung finden. Wir weisen darauf hin, dass nicht jede Gerätehardware den gleichen Funktionsumfang aufweist und eine andere Systemsoftware möglicherweise unterschiedliche Funktionen bietet. Die endgültige Konfigurierung kann dann auf das System oder auch auf die gesamte Geräteflotte angewendet werden. Wenn Sie weitere Informationen oder Unterstützung benötigen, hilft Canon oder ein Canon Partner Ihnen gern weiter.

Zielgruppe dieses Dokuments

Dieses Dokument richtet sich an alle, die sich mit der Konzipierung, Implementierung und Sicherung von Office-Multifunktionssystemen (MFDs) in Netzwerkumgebungen befassen. Also, in erster Linie IT- und Netzwerkspezialisten, IT-Sicherheitsbeauftragte und Kundendienstmitarbeiter.

Umfang und Geltungsbereich

In diesem Leitfaden werden die Konfigurationseinstellungen für zwei typische Netzwerkumgebungen erläutert und vorgestellt, mit denen ein Unternehmen eine MFD-Lösung auf sichere Weise gemäß den bewährten Verfahren umsetzt. Es wird auch erklärt, wie die Syslog-Funktion (ab der Firmwareplattform Version 3.8) Rückmeldungen in Echtzeit vom MFD bereitstellen kann. Diese Einstellungen wurden durch das Sicherheitsteam von Canon erprobt und validiert.

Eventuelle branchenspezifische gesetzliche Bestimmungen, nach denen andere Sicherheitskriterien zu beachten wären, werden in diesem Dokument außer Acht gelassen.

Dieser Leitfaden beruht auf dem standardmäßigen Funktionsumfang der imageRUNNER ADVANCE Plattform der III. Generation oder aktueller Systeme. Die Angaben gelten für alle Modelle und Serien der imageRUNNER ADVANCE Modellreihen, wobei einzelne Funktionen bei bestimmten Modellen abweichen können.

Umsetzen der optimalen MFD-Sicherheit in Ihrer Umgebung

Die sicherheitstechnischen Auswirkungen durch die Einbindung eines Multifunktionssystems in Ihr Netzwerk werden anhand von zwei typischen Szenarien beleuchtet:

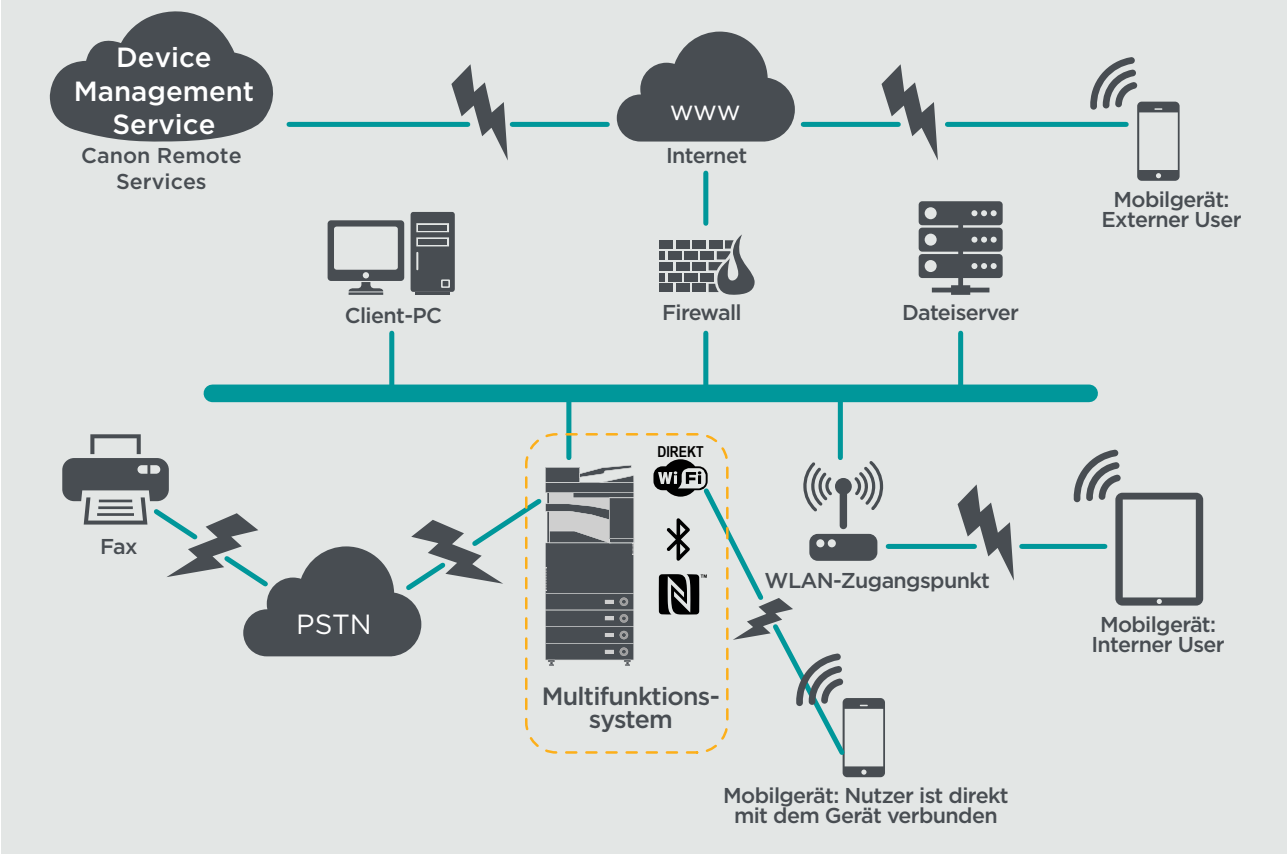
- **Typische Büroumgebung in Kleinunternehmen**
- **Büroumgebung in Großunternehmen**

TYPISCHE BÜROUMGEBUNG IN KLEINUNTERNEHMEN

In der Regel ist diese Umgebung in kleinen Unternehmen zu finden. Die Netzwerktopologie ist nicht segmentiert. Ein oder zwei Multifunktionssysteme dienen zum internen Gebrauch, sind jedoch nicht über das Internet erreichbar.

Mobiles Drucken ist möglich, bei nicht mehr aktuellen Baureihen allerdings nur mit zusätzlichen Lösungskomponenten. Benutzer außerhalb einer LAN-Umgebung, die auf Druckerdienste zugreifen müssen, benötigen eine sichere Verbindung. Diese Verbindung wird in diesem Leitfaden nicht behandelt. Während der Datenübertragung zwischen dem Remote-Gerät und der Druckinfrastruktur müssen die Daten in jedem Fall geschützt werden.

Abbildung 1 Kleines Büronetzwerk



Die neueste Generation der imageRUNNER ADVANCE Modelle lassen sich über die WLAN-Funktion mit einem WLAN verbinden. Auch Punkt-zu-Punkt-Verbindungen (per WiFi Direkt) mit einem Mobilgerät sind ohne Netzwerkverbindung in das Firmennetzwerk möglich.

Mehrere Modelle bieten optionale Bluetooth- und NFC-Funktionen, mit denen eine WiFi-Direkt-Verbindung zu iOS- bzw. Android-Geräten noch komfortabler aufgebaut werden kann.

ÜBERLEGUNGEN ZUR KONFIGURATION

Bei allen Funktionen der imageRUNNER ADVANCE Modelle, die im Folgenden nicht ausdrücklich genannt werden, reichen die Standardeinstellungen für diese Unternehmens- und Netzwerkumgebung aus.

Tabelle 1: Überlegungen zur Konfiguration einer Büroumgebung in Kleinunternehmen

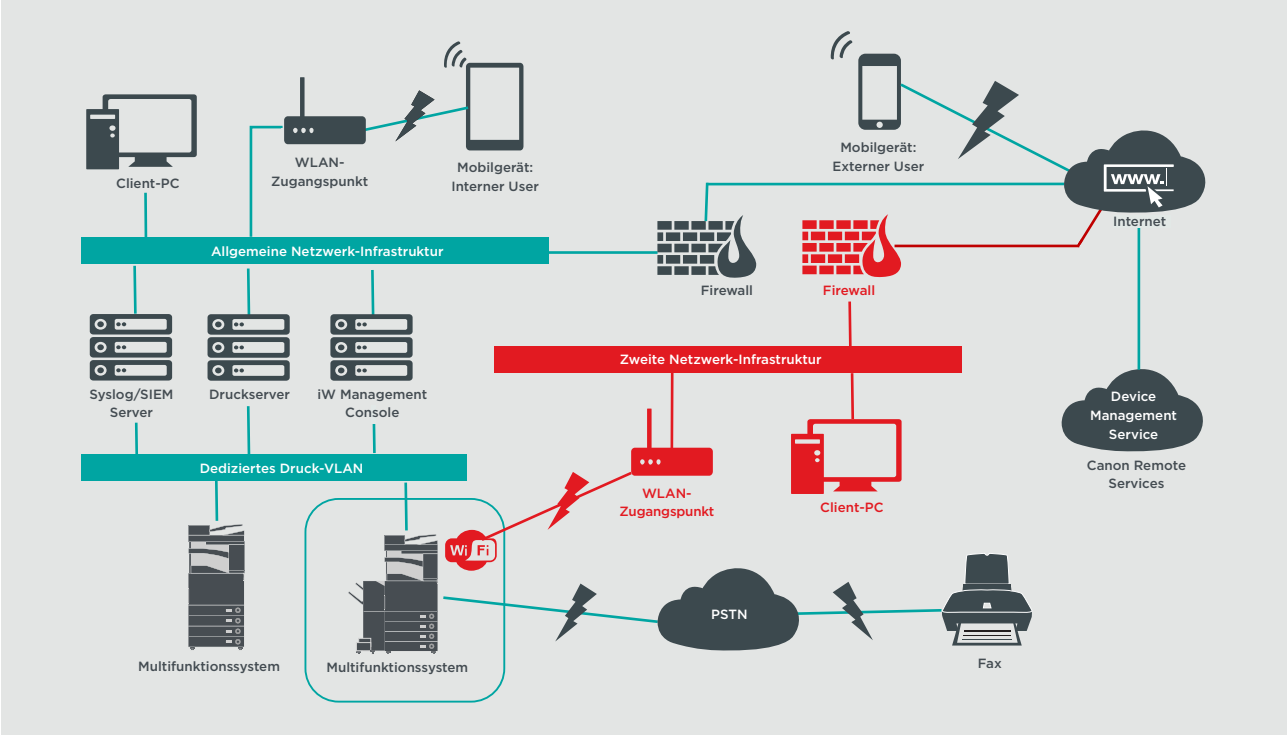
imageRUNNER ADVANCE Funktion	Beschreibung	Überlegung
Kundendienstmodus	Zugriff auf die Kundendienstmodus-Einstellungen	Kennwortschutz mit einem nicht standardmäßigen, nicht leicht erratbaren Kennwort maximaler Länge
Kundendienst-Managementsystem	Erlaubt den Zugriff auf diverse, nicht standardmäßige Einstellungen	Kennwortschutz mit einem nicht standardmäßigen, nicht leicht erratbaren Kennwort maximaler Länge
Durchsuchen/Senden über SMB	Daten auf/aus Windows-/SMB-Netzwerkfreigaben speichern und abrufen	Der Systemadministrator sollte per Richtlinie festlegen, dass die Benutzer auf ihrem Client-Computer keine lokalen Konten erstellen dürfen, mit denen Dokumente über SMB für das imageRUNNER ADVANCE-System freigegeben werden
Remote UI	Webgestütztes Konfigurationstool	Der imageRUNNER ADVANCE Administrator sollte HTTPS für die Fernzugriffs-Nutzeroberfläche aktivieren und den HTTP-Zugriff deaktivieren. Außerdem sollte eine eindeutige PIN-Authentifizierung für die verschiedenen Geräte aktiviert werden
SNMP	Integrierte Netzwerküberwachung	Version 1 ist zu deaktivieren; nur Version 3 sollte aktiviert werden
Senden per E-Mail und/oder Fax	E-Mails als Anhang über das Gerät senden	SSL/TLS aktivieren Vor SMTP-Versand keine POP3-Authentifizierung verwenden SMTP-Authentifizierung verwenden
POP3	Dokumente automatisch aus der Mailbox abholen und drucken	SSL/TLS aktivieren POP3-Authentifizierung aktivieren
Adressbuch/LDAP	Telefonnummer oder Mailadressen als Ziel für eingescannte Dokumente per Adressverzeichnis ermitteln	SSL/TLS aktivieren Authentifizierung beim LDAP-Server nicht mit den Domänen-Benutzerdaten vornehmen, sondern mit LDAP-spezifischen Benutzerdaten
FTP-Druck	Dokumente zum/vom integrierten FTP-Server hoch- und herunterladen	FTP-Authentifizierung aktivieren. FTP-Daten werden stets im Klartext über das Netzwerk übertragen
Senden über WebDAV	Dokumente an einen Remote-Standort scannen und speichern	Authentifizierung für WebDAV-Freigaben aktivieren
Verschlüsseltes PDF	Dokumente verschlüsseln	Vertrauliche Dokumente sollten per Richtlinie mindestens mit PDF-Version 1.6 (AES-128) verschlüsselt werden.
Secure Print	Der Druckauftrag wird an das Gerät gesendet, bleibt jedoch so lange in der Druckerwarteschlange, bis die richtige PIN-Nummer eingegeben wird	PIN-geschützte Druckaufträge
Syslog Ereignismeldung	Das System-Logging-Protokoll ist ein Standard-Industrieprotokoll, mit dem Systemprotokoll- oder Ereignismeldungen an einen bestimmten Server gesendet werden, der als Syslog-Server bezeichnet wird	Es wird empfohlen, die imageRUNNER Syslog-Daten an Ihr vorhandenes Netzwerk-Syslog-Analysetool oder die SIEM-Plattform (Security Event Management System) zu senden.
Systemüberprüfung beim Systemstart	Bietet die Gewissheit, dass die Systemsoftware-Komponenten nicht kompromittiert wurden. Dadurch wird die Systemstartzeit nur minimal verlängert.	Funktion aktivieren
Eingebundener Webbrowser	Browserzugriff auf das Internet	Per Administration sollte ein Web-Proxy zur Inhaltsfilterung festgelegt werden, damit kein Zugriff auf schädliche oder virenverseuchte Inhalte möglich ist. Anlegen von Favoriten deaktivieren
Bluetooth und NFC (ab Geräte-Generation III optional verfügbar)	WiFi-Direkt-Verbindungen	WiFi Direkt aktivieren, damit direkte Verbindungen zu mobilen Geräten aufgebaut werden können. Wenn die MFD-Verbindung zum Netzwerk per WLAN erfolgt, ist WiFi Direkt nicht zulässig.
WLAN	Drahtloser Zugriff	WPA-PSK/WPA2-PSK mit starken Kennwörtern verwenden
IPP	Verbindungen über IP herstellen und Druckaufträge senden	IPP deaktivieren
TPM	Eine Funktion zur Speicherung sicherheitsrelevanter Daten, z. B. Passwörter und Verschlüsselungscode, in der Hardware für maximale Sicherheit	Diese Funktion ist standardmäßig ausgeschaltet. Bei Aktivierung wird die Durchführung eines Backups empfohlen.

BÜROUMGEBUNG IN GROSSUNTERNEHMEN

Diese Umgebung besteht in der Regel aus mehreren Standorten und Büros mit einer segmentierten Netzwerkarchitektur. In einem separaten VLAN befinden sich mehrere Multifunktionssysteme für den internen Gebrauch über mindestens einen Druckserver. Die MFD sind nicht über das Internet erreichbar.

In dieser Umgebung kümmert sich meist ein ständiges Team um die Netzwerk- und Back-Office-Anforderungen sowie um allgemeine Computerfragen. In diesem Leitfaden wird vorausgesetzt, dass die Teammitglieder keine spezielle MFD-Schulung durchlaufen haben.

Abbildung 2 Büronetzwerk in Großunternehmen



Rote Verbindungen: Modelle ab III. Generation

ÜBERLEGUNGEN ZUR KONFIGURATION

Bei allen Funktionen der imageRUNNER ADVANCE Modelle, die im Folgenden nicht ausdrücklich genannt werden, reichen die Standardeinstellungen für diese Unternehmens- und Netzwerkumgebung aus.

Tabelle 2: Überlegungen zur Konfigurierung einer Büroumgebung in Großunternehmen

imageRUNNER ADVANCE Funktion	Beschreibung	Überlegung
Kundendienstmodus	Zugriff auf die Kundendienstmodus-Einstellungen	Kennwortschutz mit einem nicht standardmäßigen, nicht leicht erratbarem Kennwort maximaler Länge
Kundendienst-Managementsystem	Erlaubt den Zugriff auf diverse, nicht standardmäßige Einstellungen	Kennwortschutz mit einem nicht standardmäßigen, nicht leicht erratbarem Kennwort maximaler Länge
Durchsuchen/Senden über SMB	Daten auf/aus Windows-/SMB-Netzwerkfreigaben speichern und abrufen	Der Systemadministrator sollte per Richtlinie festlegen, dass die Benutzer auf ihrem Computer keine lokalen Konten erstellen dürfen, mit denen Dokumente über SMB für das imageRUNNER ADVANCE System freigegeben werden
Remote UI	Webgestütztes Konfigurationstool	In den nachfolgenden anfänglichen Systemkonfigurierungen werden HTTP und HTTPS deaktiviert, sodass die Fernzugriffs-Nutzeroberfläche vollständig deaktiviert wird
SNMP	Integrierte Netzwerküberwachung	Version 1 ist zu deaktivieren; nur Version 3 sollte aktiviert werden
Senden per E-Mail und/oder Fax	E-Mails als Anhang über das Gerät senden	SSL/TLS aktivieren Aktivieren: – Zertifikatsprüfung auf dem SMTP-Server Falls nicht durchführbar: – Diese Funktion ausschließlich in einer Umgebung mit NIDS-Collector (Network Intruder Detection System) verwenden – Vor SMTP-Versand keine POP3-Authentifizierung verwenden – SMTP-Authentifizierung verwenden
POP3	Dokumente automatisch aus der Mailbox abholen und drucken	SSL/TLS aktivieren Aktivieren: – Zertifikatsprüfung auf dem POP3-Server Falls nicht durchführbar: – Diese Funktion ausschließlich in einer Umgebung mit NIDS-Collector (Network Intruder Detection System) verwenden – POP3-Authentifizierung verwenden
Adressbuch/LDAP	Telefonnummer oder E-Mail-Adressen als Ziel für eingescannte Dokumente per Adressverzeichnis ermitteln	SSL/TLS aktivieren Aktivieren: – Zertifikatsprüfung auf dem LDAP-Server Falls nicht durchführbar: – Diese Funktion ausschließlich in einer Umgebung mit NIDS-Collector (Network Intruder Detection System) verwenden – Authentifizierung beim LDAP-Server nicht mit den Domänen-Benutzerdaten vornehmen, sondern mit LDAP-spezifischen Benutzerdaten
IPP	Verbindungen über IP herstellen und Druckaufträge senden	IPP deaktivieren
Senden über WebDAV	Dokumente an einen Remote-Standort scannen und speichern	Authentifizierung für WebDAV-Freigaben aktivieren SSL/TLS aktivieren Nur Dateien zum Hochladen auf den Drucker zulassen, die die richtigen „Druck-Dateinamenerweiterungen“ aufweisen
IEEE802.1X	Authentifizierungsmechanismus für Netzwerkzugriff	Unterstützung für EAPOL v1
Verschlüsseltes PDF	Dokumente verschlüsseln	Vertrauliche Dokumenten sollten per Richtlinie mindestens mit PDF-Version 1.6 (AES-128) verschlüsselt werden.
Verschlüsselter sicherer Druck	Für mehr Schutz beim sicheren Drucken die Datei und das Kennwort während der Übertragung verschlüsseln	Auf der Registerkarte „Printer“ in der Konfigurierung des Client-Druckers einen anderen Benutzernamen festlegen als in den LDAP-/Domänen-Benutzerdaten dieses Benutzers. „Restrict printer jobs“ deaktivieren
Automatische Zertifikatserneuerung	Der automatische Anmeldungsprozess verbessert die Effizienz beim Abrufen und Bereitstellen digitaler Zertifizierungen	Zur Nutzung wird eine Lösung für Netzwerkzertifikate benötigt
Syslog Ereignismeldung	Das System-Logging-Protokoll ist ein Standard-Industrieprotokoll, mit dem Systemprotokoll- oder Ereignismeldungen an einen bestimmten Server gesendet werden, der als Syslog-Server bezeichnet wird	Es wird empfohlen, die imageRUNNER ADVANCE Syslog-Daten an Ihr vorhandenes Netzwerk-Syslog-Analysetool oder die SIEM-Plattform (Security Event Management System) zu senden.
Systemüberprüfung beim Systemstart	Bietet die Gewissheit, dass die Systemsoftware-Komponenten nicht kompromittiert wurden. Dadurch wird die Systemstartzeit nur minimal verlängert	Funktion aktivieren
WLAN	Drahtloser Zugriff	WPA-PSK/WPA2-PSK mit starken Kennwörtern verwenden
WiFi Direkt	zur Herstellung von WiFi-Direkt-Verbindungen	WiFi Direkt deaktivieren
Integrierter Webbrowser	Browserzugriff auf das Internet	Geeignete Einschränkungen festlegen oder Funktion zum Herunterladen von Dateien über den Browser deaktivieren

Die neueste Generation der imageRUNNER ADVANCE-Modelle lassen sich auch dann über die WLAN-Funktion mit einem WLAN verbinden, wenn sie bereits mit einem drahtgebundenen Netzwerk verbunden sind. Dieses Szenario kann dann hilfreich sein, wenn ein Kunde ein System in zwei Netzwerken nutzen möchte. Typisches Beispiel ist eine Schule mit getrennten Netzwerken für Lehrer und Schüler.

Die imageRUNNER ADVANCE Plattform bietet Funktionen, die eine höchst flexible Nutzung ermöglichen. Aufgrund der Vielfalt der Protokolle und Dienste, die dies ermöglichen, ist es wichtig, dass nur die benötigten Funktionen, Dienste und Protokolle aktiviert sind, um die Nutzeranforderungen zu erfüllen. Dies hat sich als gute Sicherheitsmaßnahme in der Praxis bewährt, um die potenziellen Angriffsmöglichkeiten und deren Ausnutzung zu minimieren. Da ständig neue Sicherheitslücken auftauchen, muss man immer wachsam gegenüber Manipulationen sein, entweder im System selbst oder in seiner Peripherie. Wenn man die Möglichkeit hat, die Nutzeraktivitäten zu kontrollieren, kann das hilfreich sein, Angriffe zu erkennen und falls notwendig korrigierend einzugreifen.

Die imageRUNNER ADVANCE Software Plattform ab Version 3.8 bietet gegenüber den seit Jahren bekannten einige zusätzliche Funktionen. Das schließt zum Beispiel die Fähigkeit mit ein, das System per Syslog-Daten und einer Systemüberprüfung beim Rechnerstart in Echtzeit zu überwachen. Der Einsatz dieser Funktionen in Verbindung mit Ihren bestehenden Netzwerk-Sicherheitslösungen, wie z.B. ein Sicherheitsinformations- und Ereignismanagement (SIEM) oder Protokoll-Lösungen, erlauben eine bessere Transparenz sowie die Erkennung von Vorfällen und deren kriminaltechnische Auswertung.

Trusted Platform Module (TPM)

Alle imageRUNNER ADVANCE Systeme verfügen über ein sogenanntes Trusted Platform Modul (TPM), einem nicht manipulierbaren Sicherheitschip nach offenen Standards (imageRUNNER ADVANCE DX Baureihen mit Vertriebsstart 2021 sind mit einem TPM 2.0 Modul ausgestattet). Es ist für die Speicherung von Passwörtern, digitalen Zertifikaten und Verschlüsselungscodes verantwortlich.

Alle aktuellen imageRUNNER ADVANCE Modelle mit Festplatte oder SSD bieten eine vollständige Verschlüsselung des Festplattenspeichers. Der Kryptographische-Schlüssel wird in einem separaten Canon Sicherheits-Chip, der dem US FIPS 140-2 Level 2 Sicherheits-Standard entspricht, auf dem MFP gespeichert - nicht im TPM-Modul.

Standardmäßig ist die TPM-Funktion nicht aktiviert; sie kann aber über das Menü imageRUNNER ADVANCE Zusatzfunktionen aktiviert werden. Es wird dringend empfohlen, im Falle eines Fehlers ein Backup des TPM unmittelbar nach seiner Aktivierung zu sichern. Dabei ist zu beachten, dass es nur einmal auf einen USB-Speicherstick gesichert werden kann.

Für weitere Informationen zum TPM, rufen Sie in Ihrem Webbrowser den folgenden Link auf und geben Sie "Verwenden von TPM" in das Suchfeld ein. Sie erhalten Informationen betreffend:

- TPM aktivieren
- TPM sichern und wiederherstellen

https://oip.manual.canon/USRMA-4796-zz-CS-5700-deDE/

Systemüberprüfung beim Systemstart

Diese Funktionalität ist ein hardwaregesteuerter Mechanismus, mit dem sichergestellt wird, dass alle Teile der Systemsoftware bei imageRUNNER ADVANCE Generation 3 – III. Edition-Systemen und deren Nachfolgemodelle der DX-Serien anhand einer Sicherheitskette überprüft werden, ob sie wie von Canon vorgegeben geladen werden. Sollte ein Betrugs- oder Manipulationsversuch des Systems erkannt werden oder ein Fehler beim Laden auftreten, wird der Startprozess gestoppt und ein Fehlercode angezeigt.

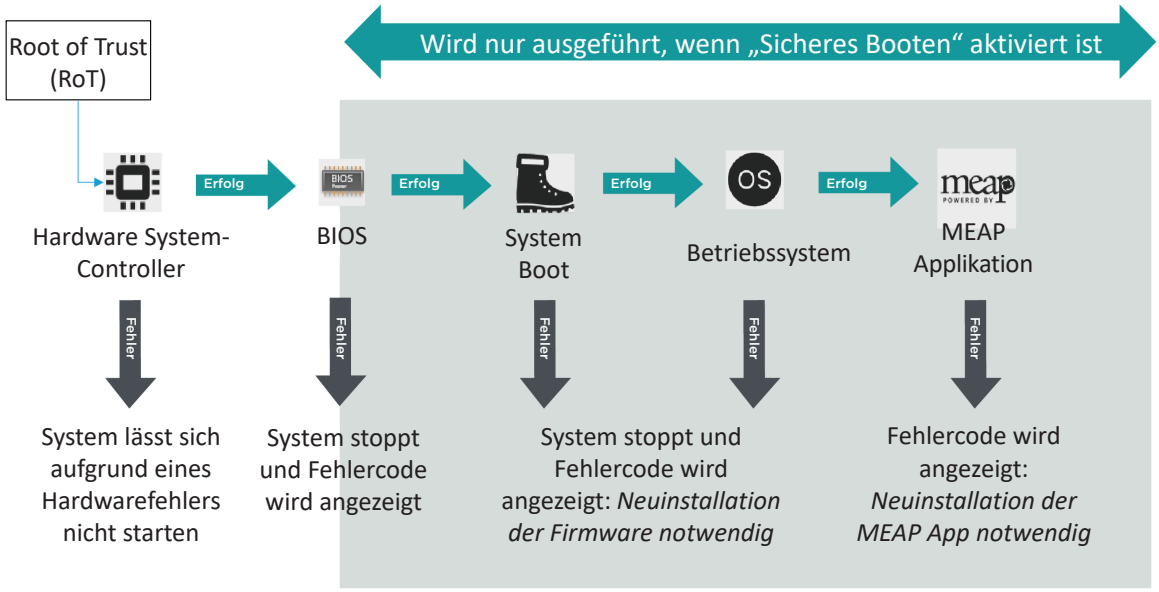


Abbildung 3 Prozess der Systemüberprüfung beim Systemstart

Dieser Vorgang ist für den Benutzer völlig transparent, abgesehen von der Anzeige, dass eine unbeabsichtigte Systemversion geladen wird. Die imageRUNNER ADVANCE Generation 3 – III. Edition und Nachfolgemodelle verfügen über eine Option zur Aktivierung der Systemüberprüfung beim Start. Wir empfehlen diese Option unbedingt zu nutzen.

Sichere Datenlöschung am Ende der Nutzungsdauer

Das Multifunktionssystem verarbeitet beim Kopieren, Scannen, Drucken und Faxen sowie in den Adressbüchern, System- und Jobprotokollen Daten, die letztendlich vertrauliche Informationen enthalten können. Die imageRUNNER ADVANCE Plattform bietet eine sichere Funktion zu Datenlöschung, die nicht nur den Eintrag in der Dateizuordnungstabelle löscht, sondern auch die physikalischen Speichersektoren mit Blinddaten überschreibt und so jegliche Wiederherstellung verhindert.

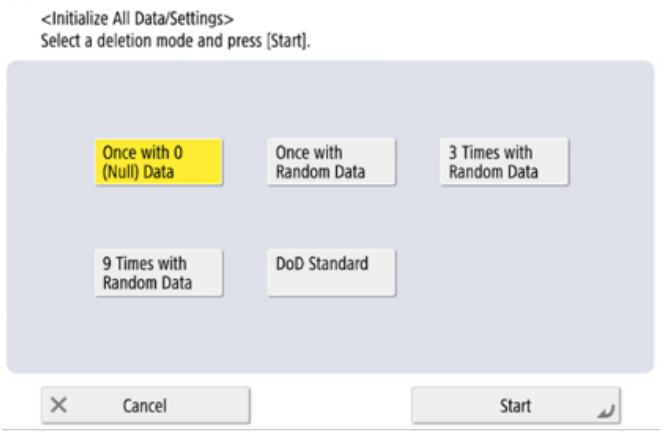


Abbildung A: Optionen zur Datenlöschung bei imageRUNNER ADVANCE Systemen mit Festplatte

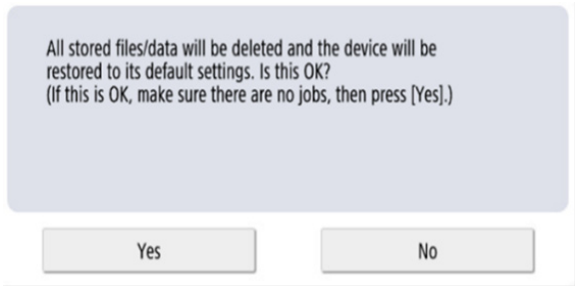


Abbildung B: Initialisierung der gesamten imageRUNNER ADVANCE SSD-Daten

Je nach Modell des Systems wird entweder eine Festplatte (HDD) oder eine Solid-State Disk (SSD) verwendet. Da eine HDD physische Speichermedien nutzt, werden die Daten zur effektiven Löschung mehrmals, in der Regel dreimal, überschrieben. Die SSD-Technologie verwaltet den Speicher jedoch unterschiedlich, da sie Daten gleichmäßig auf den gesamten verfügbaren Speicherplatz verteilt, sodass das mehrmalige Überschreiben nicht erforderlich ist.

SSD-Technologie

Im Gegensatz zu einer HDD ist bei der SSD keine Löschung temporärer Daten im laufenden Betrieb erforderlich, da durch Algorithmen und Ausfallsicherungen gewährleistet ist, dass Daten effizient bereinigt werden und gleichzeitig die Lebensdauer maximiert wird – die Selbständigkeit in puncto Datenverwaltung ist quasi schon eingebaut. Darüber hinaus sind alle Daten auf der SSD permanent verschlüsselt (AES-256). Die Daten werden elektrisch in Festkörperspeicherzellen (Solid-State Memory Cells) abgelegt. Der Vorteil dabei ist die Zugriffsgeschwindigkeit. Doch jede Zelle hat nur eine begrenzte Anzahl von Schreibvorgängen.

"Wear Levelling" – Verschleißnivellierung

Um dem Problem der übermäßigen Nutzung eines bestimmten Speicherblocks zu begegnen, wird ein als "Wear Leveling" bezeichneter Prozess angewendet, der die Anzahl der Schreibvorgänge so gleichmäßig wie möglich verteilt. Dabei werden zwei verschiedene Verfahren angewendet: dynamisches und statisches Wear Levelling.

Bei der dynamischen Verschleißnivellierung werden genutzte Speicherblöcke erkannt, sodass Überschreibungen auf neue, leere Blöcke verschoben werden. Dabei wird ein Zähler hochgesetzt, der dem SSD-Controller die Anzahl der Schreibvorgänge mitteilt. Beim statischen Verfahren werden vorhandene unveränderte Daten in einen neuen Speicherblock verschoben, wodurch die Nutzung gleichmäßiger auf den verfügbaren Speicher verteilt wird. Dadurch soll erreicht werden, dass die Zahl der Überschreibungen gleichmäßig auf alle Speicherblöcke verteilt wird, unabhängig davon, ob sich Daten nur gelegentlich oder ständig ändern. Der "TRIM"-Prozess trägt dazu bei, die Lebensdauer zu verlängern und eine äußerst schnelle Datenzuordnung sicherzustellen.

Je nach imageRUNNER ADVANCE Modell und Festplattentyp werden verschiedene Methoden zur Sicherstellung der Datensicherheit angewandt: Modelle, die einen HDD-Festplattenspeicher verwendeten, verfügten über eine Löschfunktion, um auch temporäre Daten im laufenden Betrieb unwiederbringlich zu tilgen. Das Vorgehen bei SSD-Speicher unterscheidet sich aufgrund der Technologie daher vollständig.

- Der SSD-Verschlüsselungscode wird auf dem einzelnen System im MFD Security Chip gespeichert. Wenn die SSD aus diesem speziellen Gerät entfernt wird, sind die Daten mit **AES 256-Bit** verschlüsselt und können weder gelesen noch geschrieben werden. Eine Löschung temporärer Daten, die die Lebensdauer der SSD reduzieren würde, ist also nicht notwendig.
- Canon MFP Security Chip 2.10 erfüllt den **FIPS 140-2 Level 2** Standard der US-Regierung

Initialisierung aller Daten/Einstellungen

- **Bei SSD beschränkt auf [einmalig mit 0 (Null)-Daten]**
- Eine SSD ist ein Festkörperspeicher, während eine HDD rotierende Magnetplatten verwendet. Aufgrund der Magnetisierung der Platten ist es möglich, dass Daten nach einem einfachen Überschreiben mit einigem Aufwand wieder hergestellt werden können, deshalb empfehlen wir hier eine Löschung durch 3faches Überschreiben gem. DoD-Standard.
- Nach dem Überschreiben mit Nullen ist es bei SSD-Speicher praktisch unmöglich, die geschriebenen Daten zu lesen, da nicht nur die Daten überschrieben werden, sondern auch die Speicher-Zugriffstabelle, ohne die der Speicherort der Daten unbekannt ist.
- Da die gespeicherten Daten verschlüsselt sind, ist es nicht möglich, die Daten per PC oder nach Installation in einem anderen MFD zu lesen oder zu schreiben.

Automatische Zertifikatserneuerung

Bis zur imageRUNNER ADVANCE Systemsoftware-Plattform Version 3.8 musste der Administrator die Aktualisierung der Zertifikatsanmeldung auf allen Systemen von Hand vornehmen.
Das war eine mühsame Aufgabe, da hierfür zu jedem Gerät nacheinander eine Verbindung hergestellt werden musste. Die Zertifikate mussten dann manuell über das jeweilige Remote User Interface (RUI) des Systems installiert werden, was den Vorgang sehr zeitaufwändig machte. Durch die automatische Zertifikatserneuerung, die es ab Version 3.8 gibt, wurde diese Mehrarbeit eliminiert.

Der automatische Anmeldeprozess verbessert die Effizienz beim Abruf der Zertifikate. Er bietet den automatischen Abruf unter Nutzung des Network Device Enrolment Service (NDES) für Microsoft Windows und des Simple Certificate Enrolment Protocol (SCEP).

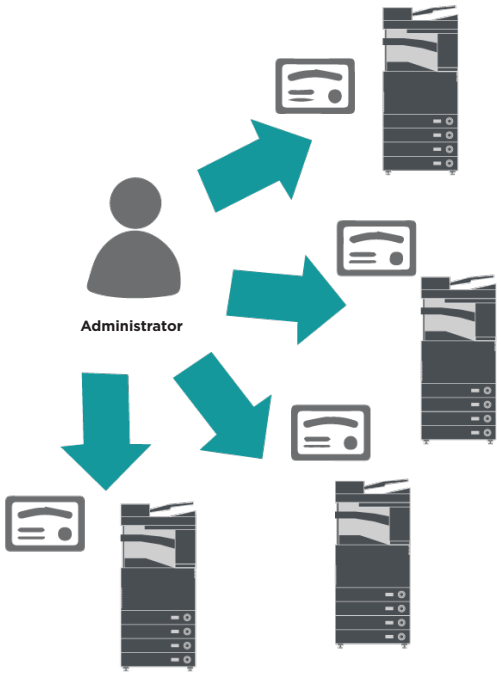


Abbildung 4 Zertifikatsanmeldung

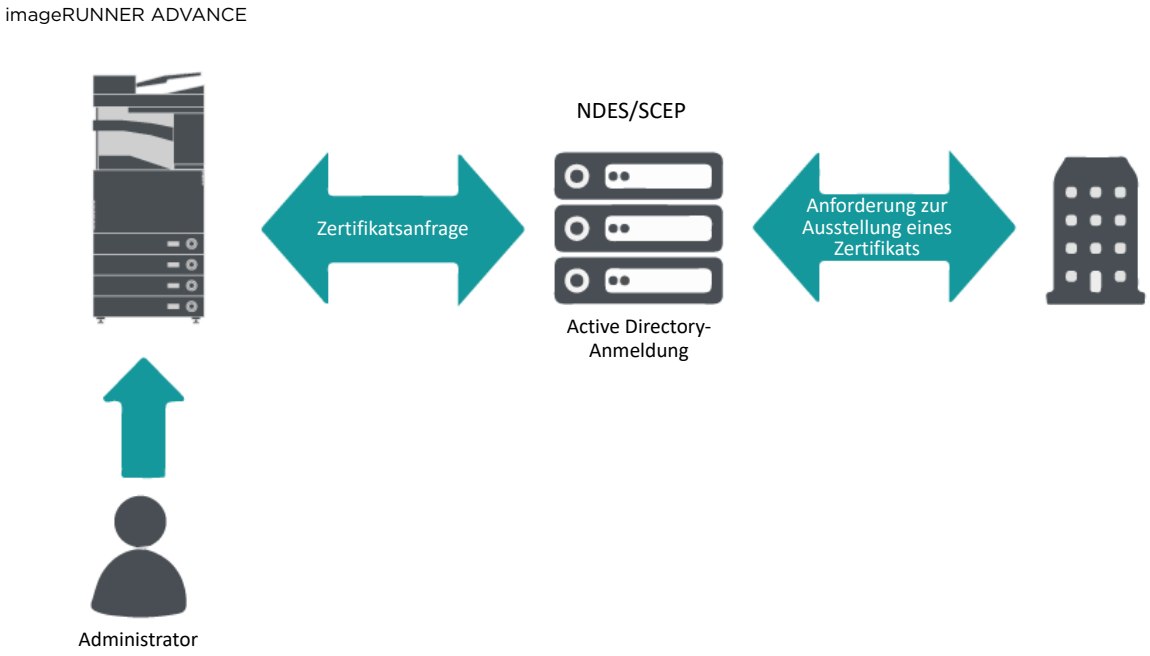


Abbildung 5 Prozess der Zertifikatserneuerung

SCEP ist ein Protokoll, das von der Certificate Authority (CA) herausgegebene Zertifikate unterstützt. NDES gestattet es Netzwerkgeräten, SCEP-Zertifikate abzurufen oder zu aktualisieren.

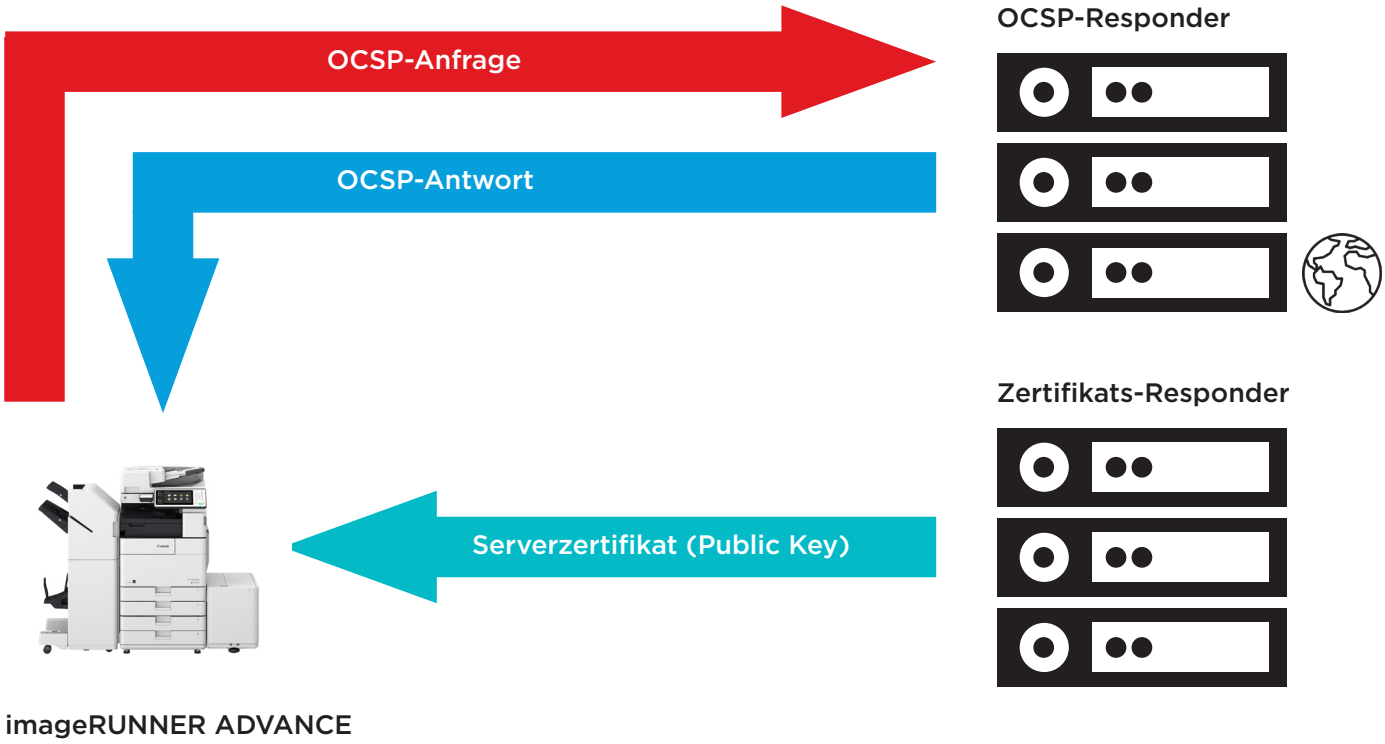
NDES ist ein Rollendienst der Active Directory Certificate Services.

Online Zertifikatsstatus-Protokoll

Es gibt viele Gründe, warum die Stornierung eines digitalen Zertifikats notwendig werden kann. Beispielsweise kann der Private Schlüssel (Private Key) verlorengehen, entwendet oder manipuliert werden oder ein Domänenname kann sich ändern.

Das Online Zertifikatsstatus-Protokoll (Online Certificate Status Protocol–OCSP) ist ein Standard-Internetprotokoll zur Überprüfung des Status eines digitalen X.509-Zertifikats, das über einen Zertifikatsserver bereitgestellt wurde. Durch das Senden einer OCSP-Anfrage an einen OCSP-Responder (in der Regel der Zertifikatsaussteller) mit der Angabe eines speziellen Zertifikats, antwortet der OCSP-Responder mit "gut", "storniert" oder "unbekannt".

Abbildung 6 OCSP-Handshaking-Prozess



Ab imageRUNNER ADVANCE Plattform Version 3.10 bietet OCSP einen Mechanismus in Echtzeit, der die installierten digitalen X.509-Zertifikate überprüft. Frühere Plattformen bieten nur die CRL-Methode (Certificate Revoke List), die sehr ineffizient ist und die Netzwerk-Ressourcen stark belasten.

Sicherheitsinformations- und Ereignismanagement

Die imageRUNNER ADVANCE Technologie unterstützt die Möglichkeit, Echtzeit-Sicherheitsereignisse mithilfe des Syslog-Protokolls auszusenden, das RFC 5424, RFC 5425 und RFC 5426 entspricht.

Dieses Protokoll wird von vielen Gerätetypen zum Sammeln von Echtzeit-Informationen verwendet, um damit potenzielle Sicherheitsgefährdungen zu erkennen.

Um die Erkennung von Bedrohungen und Sicherheitsvorfällen zu erleichtern, muss das Gerät so konfiguriert sein, dass es auf einen SIEM-Server (Security Incident Event Management) eines Drittanbieters verweist.

Die von verschiedenen Netzwerkendgeräten erzeugten Syslog-Informationen können in Echtzeit gesammelt und analysiert werden. Bei Unregelmäßigkeiten können aus diesen dann geeignete Gegenmaßnahmen abgeleitet werden (Abbildung 7). Durch die Verwendung weiterer Lösungen, wie eines SIEM-Servers, können Compliance-Berichte und Untersuchungen von Vorfällen unterstützt werden. In Abbildung 8 wird ein Beispiel gezeigt.

Die neueste Generation der imageRUNNER ADVANCE Systeme bietet Syslog-Funktionen, die es ermöglichen, eine große Anzahl an Ereignissen zu sammeln. Dies kann dazu verwendet werden, um Ereignisse aus verschiedenen Quellen in Beziehung zu setzen und zu analysieren. Dadurch lassen sich Trends oder Abnormalitäten besser erkennen.

Abbildung 7 Erfassung von Syslog-Daten

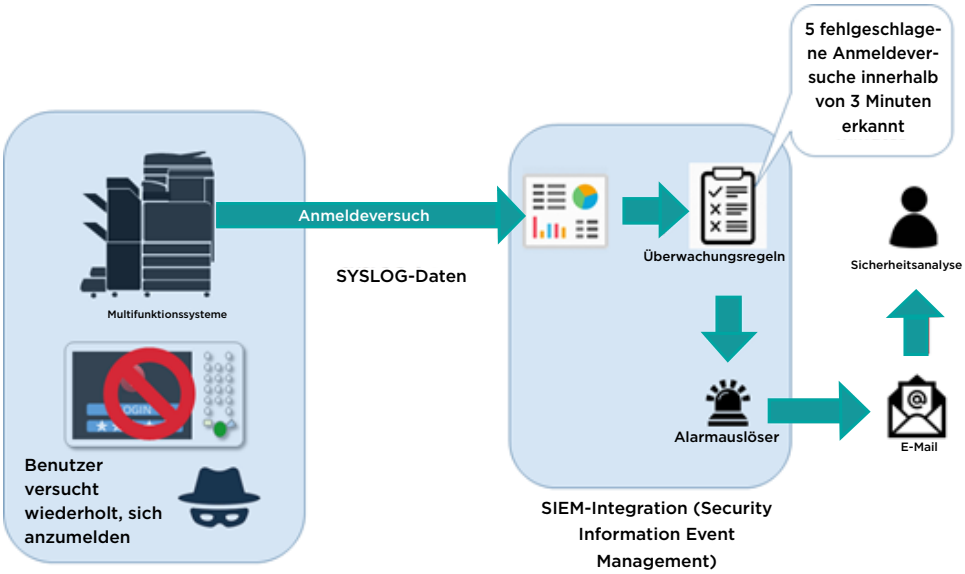


Abbildung 8 Beispiel zur Nutzung von imageRUNNER ADVANCE Syslog-Daten

Zum Herunterladen der Liste der SIEM-Spezifikationen geben Sie folgenden Link in Ihren Webbrowser ein und laden Sie die Datei **„SIEM_spec (imageRUNNER ADVANCE)“**.
https://www.canon.de/support/product-specific-security-measures/

Geräte-Ereignisprotokollierung

Zusätzlich zu den Syslog-Funktionen, die die System-Softwareplattform ab Version 3.8 zur Verfügung stellt, haben die imageRUNNER ADVANCE folgende Protokolle, die auf dem Gerät verwaltet werden können. Diese Protokolle können als CSV über das Remote User Interface (RUI) exportiert werden.

Tabelle 3 – Beispiele von Protokollen, die vom MFD verwaltet werden können.

Protokolltyp	Zahl angegeben als „Protokolltyp“ in der CSV-Datei	Beschreibung
Protokoll	4098	Dieses Protokoll enthält Informationen über den Status der Benutzer-Authentifizierung (Login/ Logout und erfolgreiche/ abgelehnte Anmeldungen), die Registrierung/ Änderung/ Löschung von Benutzerangaben, die von der Benutzer-Authentifizierung verwaltet werden, und die Rollenverwaltung (Anlage/ Änderung/ Löschung) mit dem ACCESS MANAGEMENT SYSTEM (Zugangsverwaltungs-System).
Auftragsprotokoll	1001	Dieses Protokoll enthält Daten zur Fertigstellung von Kopier-, Fax-, Scan, Sende- und Druck-Aufträgen
Übertragungsprotokoll	8193	Das Protokoll enthält Informationen zu Übertragungen
Advanced Space-Speicherprotokoll	8196	Dieses Protokoll enthält Informationen zur Speicherung von Dateien in Advanced Space, auf dem Netzwerk (Advanced Space anderer Systeme) und auf Speichermedien
Mailbox-Einsatzprotokoll	8197	Dieses Protokoll enthält Informationen zu Datenoperationen im Postfach, dem Speicher-RX-Posteingang und dem vertraulichen Fax-Eingang
Mailbox-Authentifizierprotokoll	8199	Dieses Protokoll enthält Informationen zum Anmeldestatus im Postfach, dem Speicher-RX-Posteingang und dem vertraulichen Fax-Eingang
Advanced Space-Bearbeitungsprotokoll	8201	Dieses Protokoll enthält Informationen über die Datenbearbeitung in Advanced Space
Systemverwaltungsprotokoll	8198	Dieses Protokoll enthält Informationen zum Starten/Herunterfahren des Systems, zu Änderungen an den Einstellungen, Änderungen an den Einstellungen unter Nutzung der „Device Information Delivery“-Funktion und den Zeiteinstellungen. Außerdem werden Änderungen der Nutzerinformationen oder an sicherheitsrelevanten Einstellungen aufgezeichnet, wenn das System von autorisierten Canon Technikern/ Partnern inspiziert oder repariert wird.
Netzwerk-Authentifizierprotokoll	8200	Dieses Protokoll wird aufgezeichnet, wenn die IPSec-Kommunikation fehlschlägt
Export/Import aller Protokolle	8202	Dieses Protokoll enthält Informationen zum Importieren/ Exportieren von Einstellungen über die „Alle exportieren/ importieren“-Funktion
Mailbox-Backup-Protokoll	8203	Dieses Protokoll enthält Informationen zu Daten-Backups in Nutzer-Posteingängen, im Speicher-RX-Posteingang, vertraulichen Fax-Eingang und Advanced Space, plus alle gespeicherten Daten und das registrierte Formular für die Bildüberlagerungs-Funktion
Anwendungs-/Software-Management-Bildschirm-Einsatzprotokoll	3101	Dies ist ein Einsatzprotokoll für SMS (Service Management Service), Software-Registrierung/ Updates und MEAP-Anwendungsinstaller etc.
Sicherheitsrichtlinien-Protokoll	8204	Dieses Protokoll enthält Informationen zum Status der Sicherheitsrichtlinien-Einstellungen
Gruppenmanagement-Protokoll	8205	Dieses Protokoll enthält Informationen zum Einstellungsstatus (registrieren/ bearbeiten/ löschen) der Nutzergruppen.
Systemwartungs-Protokoll	8206	Dieses Protokoll enthält Informationen zu Firmware-Updates und Datensicherung/Wiederherstellung der MEAP-Anwendung, etc.
Druckauthentifizierungs-Protokoll	8207	Dieses Protokoll enthält Informationen und die Betriebshistorie zu sicheren Druckaufträgen mit der Forced Hold Print-Funktion (erzwungenes Zurückhalten).
Einstellungssynchronisierungs-Protokoll	8208	Dieses Protokoll enthält Informationen zur Synchronisierung der Geräteeinstellungen/Synchronisiereinstellungen für mehrere Canon Multifunktionsdrucker
Protokoll für die Verwaltung von Audit-Protokollen	3001	Dieses Protokoll enthält Informationen zum Starten und Beenden dieser Funktion (Überwachungsprotokoll-Management) sowie zum Exportieren von Protokollen etc.

Protokolle können bis zu 40.000 Einträge enthalten. Sobald die Zahl der Einträge 40.000 überschreitet, werden die ältesten sukzessive gelöscht.

UNTERSTÜTZUNG FÜR REMOTE-GERÄTE

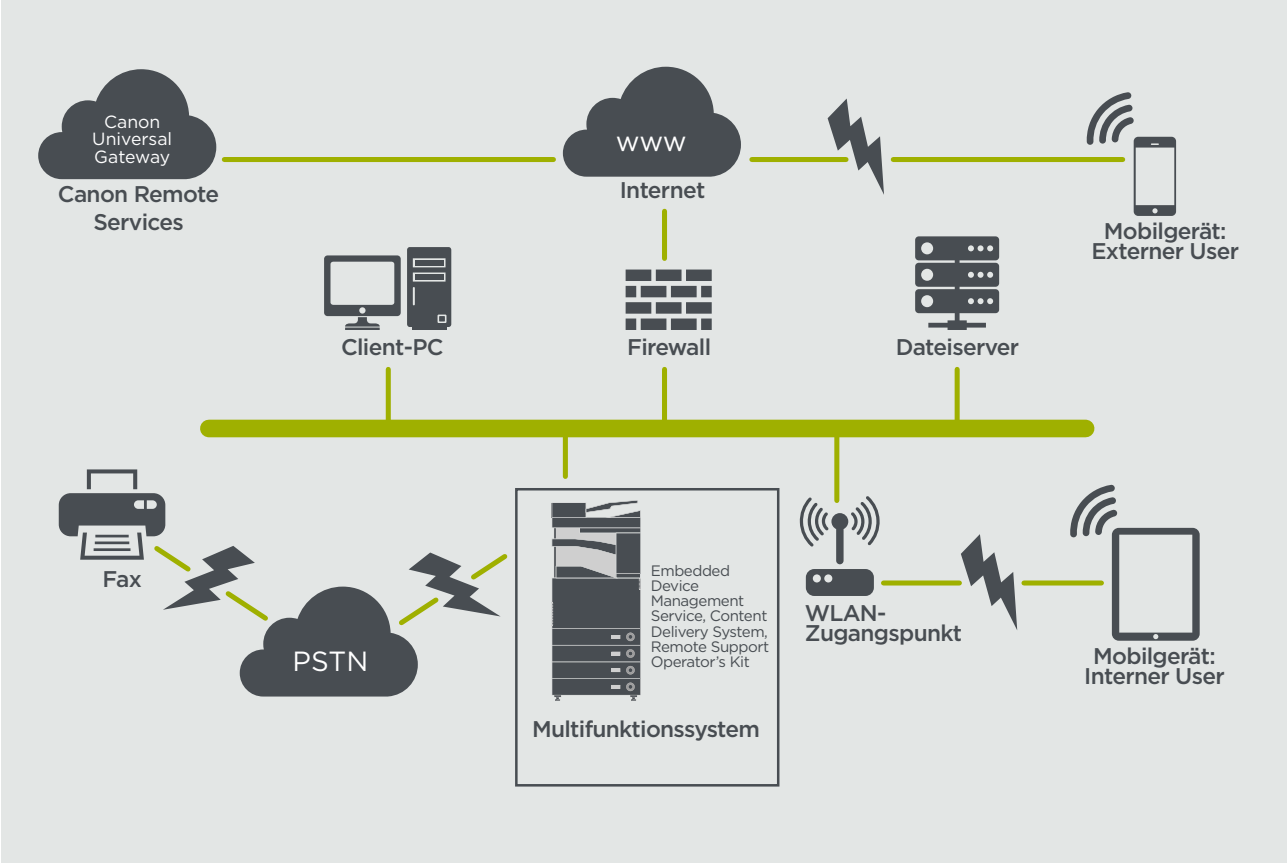
Die imageRUNNER ADVANCE Modelle können kundendienstrelevante Daten übertragen und auch Firmware-Aktualisierungen oder Software-Anwendungen empfangen, sodass Canon oder ein Canon-Partner den jeweils bestmöglichen Service leisten kann. Hierbei werden weder Bilder noch Bild-Metadaten gesendet.

Canon Remote-Services lassen sich auf zwei Arten in einem Unternehmensnetzwerk umsetzen.

Implementierszenario 1: verteilte Verbindung

In dieser Situation kann sich jedes Multifunktionssystem über das Internet mit dem Remote-Service verbinden.

Abbildung 9 verteilte Verbindung



Implementierszenario 2: zentral gesteuerte Verbindung

Im Szenario einer Unternehmensumgebung mit mehreren Multifunktionssystemen müssen diese effizient von zentraler Stelle aus verwaltet werden können. Hierzu zählt auch die Verbindung zu den Remote-Services von Canon. Die verschiedenen Geräte stellen jeweils eine Managementverbindung über einen einzigen iWMC-Verbindungspunkt (iW Management Console) her, was den ganzheitlichen Steuerungsansatz erleichtert. Die Kommunikation zwischen dem DFU-Plug-in (Device Firmware Upgrade) und den Multifunktionssystemen erfolgt über den UDP-Port 47545.

Abbildung 4 zentrale gesteuerte Verbindung

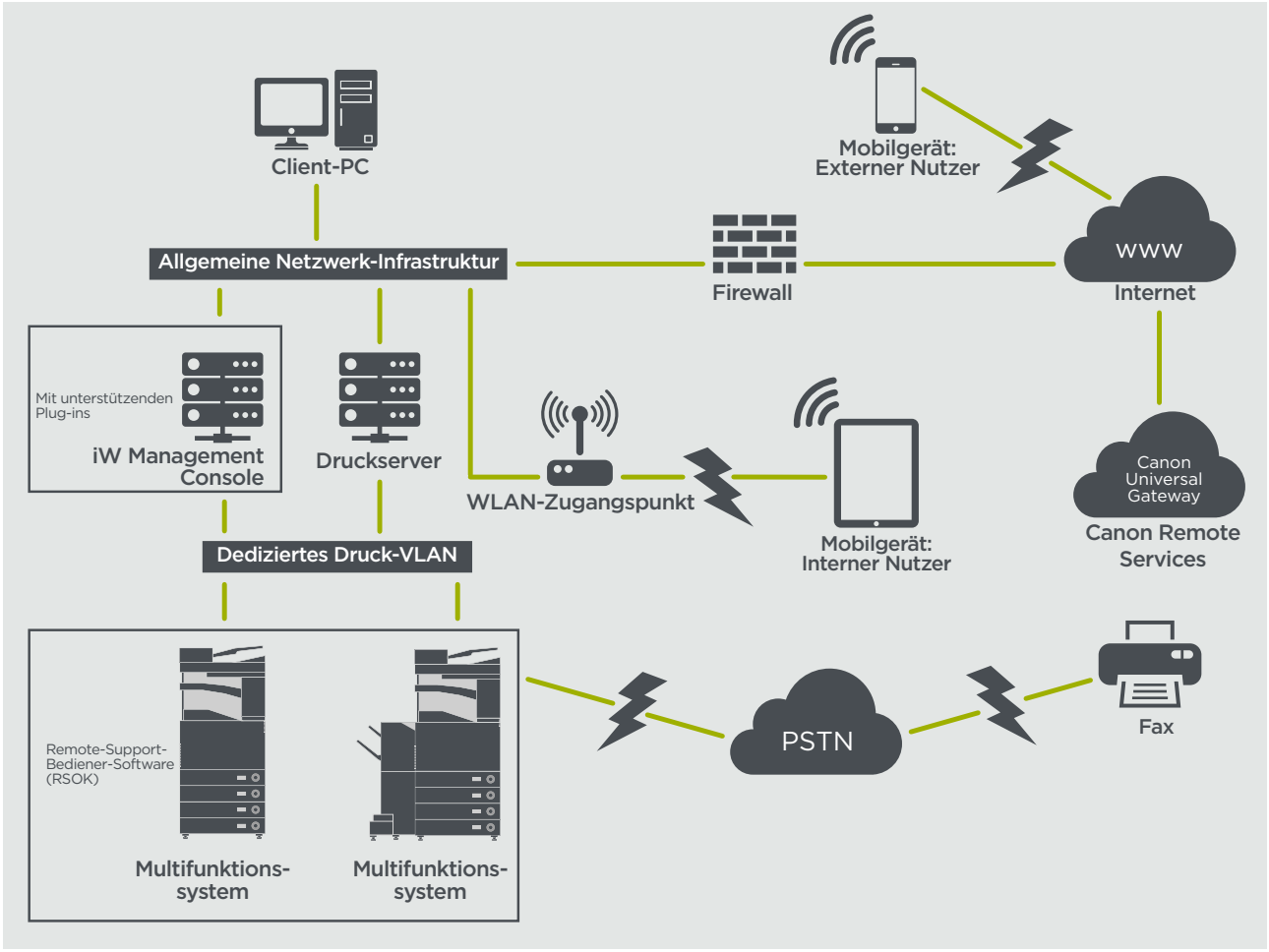


Abbildung
11a. Geräteliste (in diesem Fall ein einziges Gerät) laut Anzeige in der imageWARE Management Console und
11b. Gerätedetails und -einstellungen

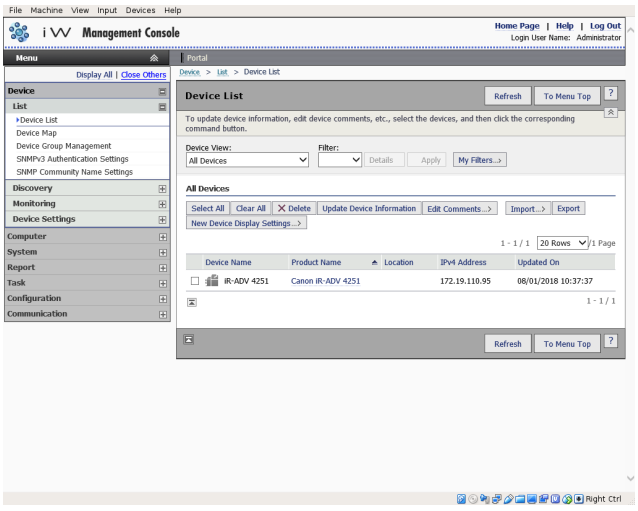


Abbildung 11a

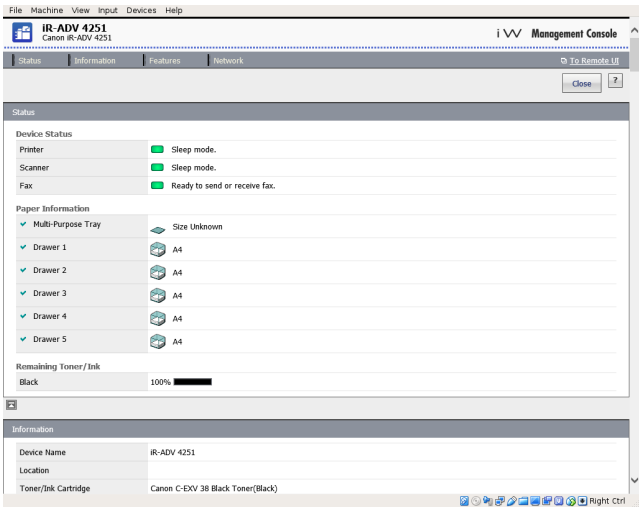


Abbildung 11b

Device Management Service (eMaintenance)

Das Device Management Service-System erfasst automatisch die Gerätezähler zur Fakturierung. Auch die Verbrauchsmaterialverwaltung und die Remote-Geräteüberwachung anhand von Status- und Fehlermeldungen werden automatisch abgewickelt.

Das Device Management Service-System besteht aus einem Server mit Internetanschluss (UGW) sowie einer Multifunktionssystem-Software (eRDS) und/oder einer servergestützten Zusatzsoftware (RDS-Plug-in), mit der die kundendienstrelevanten Gerätedaten erfasst werden. Das eRDS wird als Überwachungsprogramm direkt im imageRUNNER ADVANCE System ausgeführt. Wenn die Überwachungsoption in den Geräteeinstellungen aktiviert ist, ruft das eRDS eigene Gerätedaten ab, die dann an den UGW gesendet werden. Das RDS-Plug-in wird als Überwachungsprogramm auf einem normalen Computer installiert und kann 1 bis 3.000 Geräte überwachen. Das Programm ruft die Daten der einzelnen Geräte über das Netzwerk ab und sendet die Daten an den UGW.

Wie in Tabelle 4 unten gezeigt, bietet die nächste Seite einen Überblick über den Datentransfer, die Protokolle (je nach den Optionen, die beim Design und bei der Implementierung festgelegt wurden) sowie die verwendeten Ports. Kopier-, Druck-, Scan- oder Fax-Bilddaten werden unter keinen Umständen übertragen.

Tabelle 4 Überblick über die Device Management Service-Daten

Beschreibung	Übertragene Daten	Protokoll/Port	Port
Kommunikation zwischen Device Management Service (eRDS oder RDS-Plug-in) und UGW	UGW-Webdienstadresse Adresse/Portnummer des Proxyservers Konto/Kennwort für Proxyserver UGW-Mail-Zieladresse SMTP-Serveradresse Adresse des POP-Servers Angaben zu Gerätestatus, Zähler und Modell Seriennummer Angabe zur Toner-/Tintenrestmenge Angaben zur Firmware Informationen zu Reparaturanfrage Protokollinformationen Kundendienst-Einsatz Kundendienst-Benachrichtigung Papierstau Umweltschutz Zustandsprotokoll	HTTP/HTTPS/SMTP/POP3	TCP/80, TCP/443, TCP/25, TCP/110
Kommunikation zwischen Device Management Service und Gerät (nur RDS-Plug-in; die eRDS-Software ist integriert)		SNMP Canon-proprietär SLP/SLP/HTTPS	UDP/161, TCP/47546, UDP/47545, TCP9007, UDP/427 UDP/11427, TCP/443

Content Delivery System

Das CDS (Content Delivery System) bildet eine Verbindung zwischen dem Multifunktionssystem und dem UGW (Canon Universal Gateway). Hiermit werden Aktualisierungen für die Geräte-Firmware und die Anwendungen bereitgestellt.

Tabelle 5 Überblick über die CDS-Daten

Beschreibung	Gesendete Daten	Protokoll/Port	Port
Kommunikation zwischen MFD und UGW	Seriennummer des Geräts Firmware-Version Sprache Land Angaben zur EULA des Geräts	HTTP/HTTPS	TCP/80 TCP/443
Kommunikation zwischen UGW und MFD	Prüfdatei (binäre Zufallsdaten) zum Testen der Kommunikation Binäre Daten für Firmware oder MEAP-Anwendungen	HTTP/HTTPS	TCP/80 TCP/443

In der Gerätekonfigurierung ist eine bestimmte URL für den CDS-Zugriff voreingestellt. Sollen die Geräte-Firmware und die Anwendungen zentral aus der Infrastruktur heraus verwaltet werden, muss die iWMC mit dem DFU-Plug-in (Device Firmware Upgrade) und dem Device Application Management-Plug-in lokal installiert sein.

Remote-Support-Bediener-Software

Über die Remote-Support-Bediener-Software (RSOK) erhalten Sie den Fernzugriff auf das Bedienfeld des Geräts. Dieses nach dem Server-Client-Prinzip aufgebaute System besteht aus einem VNC-Server auf dem Multifunktionssystem und der VNC-Client-Anwendung „Remote Operation Viewer“ für Microsoft Windows.

Abbildung 12 Einrichtung der Remote-Support-Bediener-Software

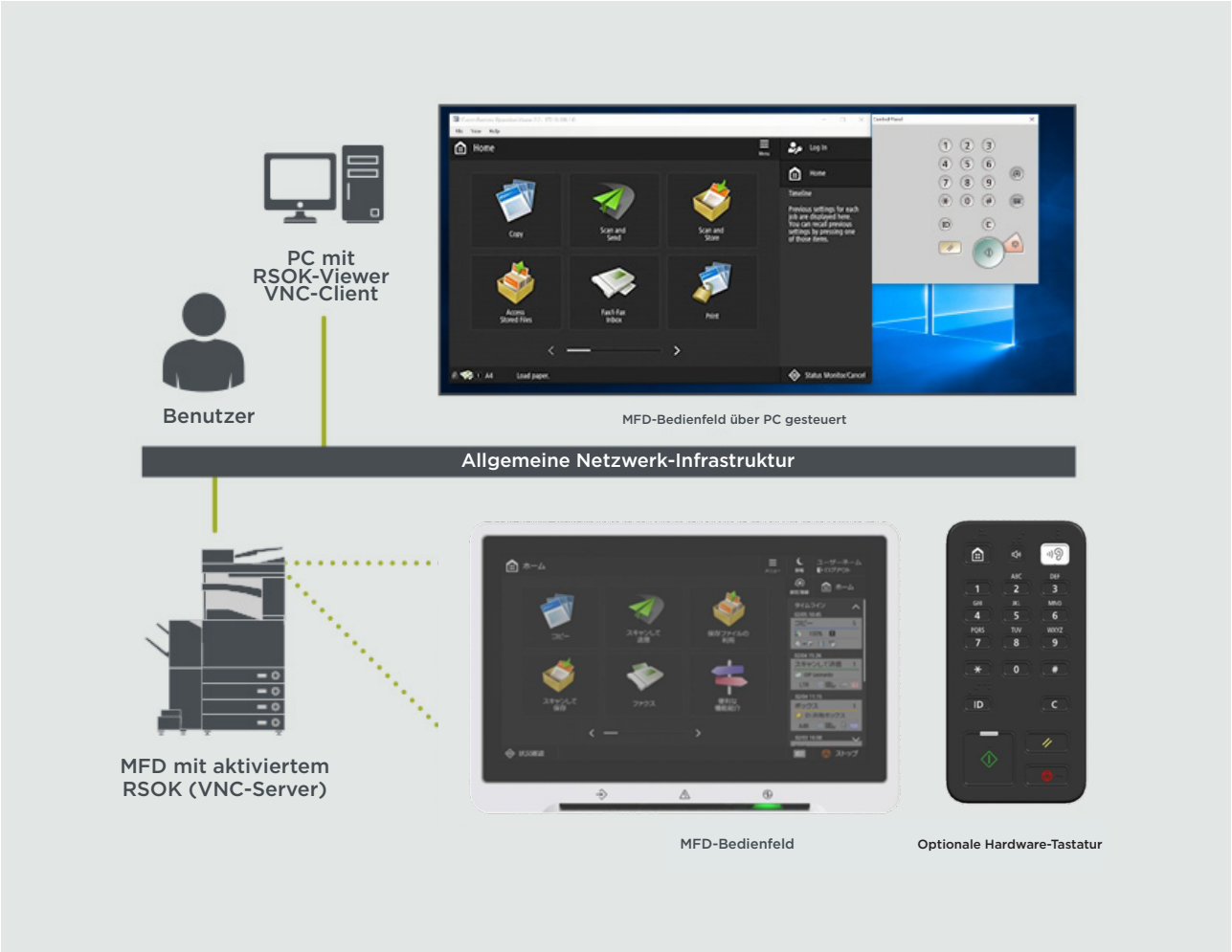


Tabelle 6 Überblick über die RSOK-Daten

Beschreibung	Gesendete Daten	Protokoll/Port	Port
VNC-Kennwortauthentifizierung	Benutzerkennwort	DES-Verschlüsselung	5900
Operation Viewer	Bedienfeld des Geräts – Bildschirmdaten – Bedienung der Hardware-Tasten	Version 3.3 RFB-Protokoll	5900

ANHANG

Canon imageRUNNER ADVANCE – Sicherheitsfunktionen

Die imageRUNNER ADVANCE Plattform lässt sich über die webgestützte Fernzugriffs-Nutzeroberfläche (Remote User Interface, RUI) im Fernverfahren konfigurieren. Diese Nutzeroberfläche umfasst einen Großteil der Konfiguriereinstellungen für das Gerät, kann jedoch bei Bedarf deaktiviert und mit einem Kennwort gegen unbefugten Zugriff geschützt werden.

Einige wenige Einstellungen sind nicht über die RUI erreichbar, sondern müssen über das Bedienfeld am Gerät selbst festgelegt werden. Wir empfehlen, alle nicht benötigten Dienste zu deaktivieren und nur die unbedingt notwendigen Steuerelemente zu aktivieren. Über das Remote-Support-Bedienerkit (RSOK) erhalten Sie den flexiblen Fernzugriff auf das Bedienfeld des Geräts. Dem liegt die VNC-Technologie zugrunde, bestehend aus einem Server (dem MFD) und einem Client (Netzwerk-PC). Der spezielle Client-PC-Viewer von Canon simuliert die Schaltflächen und benötigten Tasten im Bedienfeld.

In diesem Abschnitt finden Sie die wichtigsten imageRUNNER ADVANCE Sicherheitsfunktionen und ihre Konfiguriereinstellungen.

Interaktive Online-Handbücher sind hier verfügbar: https://oip.manual.canon/ Hier finden Sie Einzelheiten nicht nur zu den Sicherheitsfunktionen. Wählen Sie zunächst den zutreffenden Produkttyp (z.B. imageRUNNER ADVANCE DX) aus, klicken Sie dann auf das Suchsymbol und geben Sie Ihre Suchkriterien ein. Unten finden Sie einige allgemeine Bereiche, die Sie beachten sollten.

Verwalten des Geräts

Nur ständige, effektive Sicherheitsmaßnahmen verhindern den Verlust personenbezogener Daten oder die unbefugte Nutzung. Ein Administrator kann die Nutzerverwaltung und die Sicherheitseinstellungen auf befugte Personen beschränken.

Geben Sie den untenstehenden Link in Ihren Webbrowser ein und geben Sie **Konfigurieren des grundlegenden Verwaltungssystems** in das Suchfeld ein. Sie erhalten Informationen betreffend:

- Grundlegende Verwaltung des Geräts
- Begrenzung der Risiken durch Nachlässigkeit, Benutzerfehler und Missbrauch
- Systemverwaltung
- Verwaltung der Systemkonfigurierung und der Einstellungen

https://oip.manual.canon/USRMA-4709-zz-CS-3700-deDE/

IEEE P2600 Standard

Mehrere imageRUNNER ADVANCE Modelle entsprechen der globalen Datensicherheitsnorm IEEE P2600 für multifunktionale Peripheriegeräte und -drucker.

Unter dem nachfolgenden Link werden die in der Norm IEEE 2600 definierten Sicherheitsanforderungen und die Einhaltung dieser Anforderungen durch die Gerätefunktionen beschrieben (in englischer Sprache).
http://ug.oipsrv.net/USRMA-0945-zz-CS-deDE/contents/CT0305_admin_0095.html#345_h1_01

IEEE-802.1x-Authentifizierung

Wenn eine Verbindung zu einem 802.1x-Netzwerk erforderlich ist, muss sich das Gerät authentifizieren, sodass die Verbindung autorisiert wird.

Geben Sie den untenstehenden Link in Ihren Webbrowser ein und geben Sie **802.1X** in das Suchfeld ein.
https://oip.manual.canon/USRMA-4709-zz-CS-3700-deDE/

Anwenden einer Sicherheitsrichtlinie für das Gerät

Bei den neuesten imageRUNNER ADVANCE Modellen lassen sich mehrere Gerätesicherheits-Einstellungen (die Sicherheitsrichtlinie) als Batch über die Fernzugriffs-Nutzeroberfläche verwalten. Die Einstellungen können mit einem separaten Kennwort geschützt werden, sodass nur der Sicherheitsadministrator die Einstellungen bearbeiten kann.

Geben Sie den untenstehenden Link in Ihren Webbrowser ein und geben Sie **System mit einer Sicherheitsrichtlinie ausstatten** in das Suchfeld ein. Sie erhalten Informationen betreffend:

- Kennwortschutz für die Einstellungen in der Sicherheitsrichtlinie
- Konfigurieren der Einstellungen in der Sicherheitsrichtlinie
- Einstellungen in der Sicherheitsrichtlinie

https://oip.manual.canon/USRMA-4709-zz-CS-3700-deDE/

Nutzerverwaltung

Wenn besonders hohe Sicherheit und Effizienz gefordert sind, können die Kunden auf die in tegrierten Funktionen zugreifen oder eine Druckmanagement-Lösung wie uniFLOW heranziehen.

Weitere Informationen zu unseren Druckmanagement-Lösungen erhalten Sie bei Ihrem zuständigen Vertriebspartner sowie in der uniFLOW Produktbroschüre.

Konfigurieren der Netzwerksicherheitseinstellungen

Selbst befugte Benutzer verursachen mitunter unvorhergesehene Verluste als Wegbereiter für Angriffe durch Dritte mit böswilligen Absichten, z.B. Sniffing, Spoofing und Manipulation der Daten während der Übertragung im Netzwerk. Zum Schutz Ihrer wichtigen und wertvollen Daten vor diesen Angriffen unterstützt das Gerät zahlreiche Funktionen, die die Datensicherheit und -vertraulichkeit erhöhen.

Geben Sie den untenstehenden Link in Ihren Webbrowser ein und geben Sie **Konfiguration der Netzwerk-Sicherheitseinstellungen** in das Suchfeld ein. Sie erhalten Informationen betreffend:

- Unberechtigten Zugriff verhindern
- Mit einem WLAN verbinden
- Die Netzwerkumgebung einrichten

https://oip.manual.canon/USRMA-4709-zz-CS-3700-deDE/

Verwaltung der Daten der Festplatte/SSD

Auf der Festplatte des Geräts befinden sich das Betriebssystem, die Konfiguriereinstellungen und die Auftragsdaten. Die meisten Modelle bieten die vollständige Festplattenverschlüsselung (nach FIPS 140-2). Die Festplatte wird dabei mit dem jeweiligen Gerät gekoppelt, sodass sie nicht von unbefugten Benutzern ausgelesen werden kann. Ein vorbereitender Canon MFP-Sicherheitschip wurde im Rahmen des Cryptographic Module Validation Program (CMVP) der USA und Kanada zertifiziert. Eine weitere Zertifizierung erfolgte nach dem "Japan Cryptographic Module Validation Program" (JCMVP).

Geben Sie den untenstehenden Link in Ihren Webbrowser ein und geben Sie **Daten auf der Festplatte verwalten** in das Suchfeld ein.

https://oip.manual.canon/USRMA-4709-zz-CS-3700-deDE/

Informationen zur Datenbereinigung bei Produkten mit SSD-Technologie finden Sie mit Ihrem Webbrowser unter dem folgenden Link. Geben Sie im Suchfeld **Initialisieren aller Daten/Einstellungen** ein.

https://oip.manual.canon/USRMA-5493-zz-CS-5800-deDE/

ÜBERBLICK ÜBER DIE EINSTELLUNGEN IN DER SICHERHEITSRICHTLINIE

Die imageRUNNER ADVANCE Modelle der 3. Generation und ihre Nachfolgemodelle bringen die Einstellung von Sicherheitsrichtlinien und den Sicherheitsadministrator als neue Funktionen mit. Bei diesen Modellen muss sich zunächst der Administrator anmelden und dann (sofern konfiguriert) ein weiterer Sicherheitsadministrator mit einem eigenen Kennwort.

Die nachfolgende Tabelle zeigt die verfügbaren Einstellungen.

1. Schnittstelle	Anmerkungen
Richtlinie für drahtlose Verbindungen	
Verbot der Nutzung direkter Verbindungen	<Use Wi-Fi Direct> ist auf <Off> eingestellt. Der Zugriff auf das Gerät über mobile Geräte ist nicht möglich.
Verbot der WLAN-Nutzung	<Select Wired/Wireless LAN> ist auf <Wired LAN> eingestellt. Kabellose Verbindungen zum Gerät über ein WLAN oder einen Zugriffspunkt sind nicht möglich.
USB-Richtlinie	
Verbot der Nutzung von USB-Geräten	<Use as USB Device> ist auf <Off> eingestellt. Wenn die Verwendung als USB-Gerät untersagt ist, können Sie nicht über einen (per USB verbundenen) Computer auf die Druck- oder Scanfunktionen zugreifen.
Verbot der Nutzung von USB-Speichermedien	<Use as USB Storage Device> ist auf <Off> eingestellt. USB-Speichergeräte können nicht genutzt werden. Die nachfolgenden Kundendienstfunktionen stehen jedoch auch dann zur Verfügung, wenn <Prohibit use as USB storage device> auf <ON> eingestellt ist. • Firmware-Aktualisierung per USB-Stick (über den Download-Modus) • Kopieren der Sublog-Daten vom Gerät auf USB (LOG2USB) • Kopieren des Berichts vom Gerät auf USB (RPT2USB)
Netzwerkkommunikations-Betriebsrichtlinie Bitte beachten: Diese Einstellungen gelten selbst dann nicht für die Kommunikation mit IEEE-802.1x-Netzwerken, wenn das Kontrollkästchen aktiviert ist: [Überprüfen Sie stets das Serverzertifikat bei Verwendung von TLS]	
Überprüfen Sie stets die Signaturen für SMS/ WebDAV-Serverfunktionen.	Unter <SMB Server Settings> sind die Optionen <Require SMB Signature for Connection> und <Use SMB Authentication> auf <On> eingestellt, unter <WebDAV Server Settings> ist die Option <Use TLS> auf <On> eingestellt. Wenn das Gerät als SMB-Server oder WebDAV-Server fungiert, werden die Signaturen des digitalen Zertifikats im Rahmen der Kommunikation überprüft.
Überprüfen Sie stets das Serverzertifikat bei Verwendung von TLS.	<Confirm TLS Certificate for WebDAV TX>, <Confirm TLS Certificate for SMTP TX>, <Confirm TLS Certificate for POP RX>, <Confirm TLS Certificate for Network Access> und <Confirm TLS Certificate Using MEAP Application> sind auf <On> eingestellt, und <CN> ist mit einem Häkchen versehen. Unter <SIP Settings> > <TLS Settings> sind außerdem die Optionen <Verify Server Certificate> und <Verify CN> auf <On> eingestellt. Im Rahmen der TLS-Kommunikation werden digitale Zertifikate und ihre CN (Common Name) überprüft.
Verbot der Klartext-Authentifizierung für Serverfunktionen.	• Unter <FTP Print Settings> ist die Option <Use FTP Printing> auf <Off> eingestellt. • Unter <E-Mail/I-Fax Settings> > <Communication Settings> ist die Option <Allow TLS (SMTP RX)> auf <Always TLS> eingestellt, und unter <Network> ist die Option <Dedicated Port Authentication Method> auf <Mode 2> eingestellt. • Unter <WebDAV Server Settings> ist die Option <Use TLS> auf <On> eingestellt. Wenn das Gerät als Server fungiert, sind Funktionen mit Klartextauthentifizierung nicht verfügbar. Ist die Klartextauthentifizierung untersagt, kommt TLS zum Einsatz. Darüber hinaus können Sie bestimmte Anwendungen oder Serverfunktionen (z.B. FTP), die lediglich die Klartext-Authentifizierung unterstützen, nicht nutzen. Der Zugriff auf das Gerät über die Geräteverwaltungs-Software oder den Treiber ist eventuell nicht möglich.
Verbot der Nutzung von SNMPv1	Unter <SNMP Settings> ist die Option <Use SNMPv1> auf <Off> eingestellt. Wenn die Verwendung von SNMPv1 untersagt ist, können Sie eventuell die Gerätedaten nicht aus dem Druckertreiber oder der Management-Software abrufen oder dort festlegen.
Richtlinie zur Portnutzung	
Beschränkung des LPD-Ports	Portnummer 515 <LPD Print Settings> ist auf <Off> eingestellt. Der LPD-Druck ist nicht möglich.
Beschränkung des RAW-Ports	Portnummer 9100 <RAW Print Settings> ist auf <Off> eingestellt. Der RAW-Druck ist nicht möglich.
Beschränkung des FTP-Ports	Portnummer 21 Unter <FTP Print Settings> ist die Option <Use FTP Printing> auf <Off> eingestellt. Der FTP-Druck ist nicht möglich.
Beschränkung des WSD-Ports	Portnummer 3702, 60000 Unter <WSD Settings> sind die Optionen <Use WSD>, <Use WSD Browsing> und <Use WSD Scan> auf <Off> eingestellt. Die WSD-Funktionen können nicht genutzt werden.
Beschränkung des BMLinkS-Ports	Portnummer 1900 (Im Raum Europa nicht verwendet)

Beschränkung des IPP-Ports	Portnummer 631 Wenn der IPP-Port eingeschränkt ist, können Mopria, AirPrint und IPP nicht genutzt werden.
Beschränkung des SMB-Ports	Portnummer 137, 138, 139, 445 Unter <SMB Print Settings> ist die Option <Use SMB Printing> auf <Off> eingestellt. Das Gerät kann nicht als SMB-Server genutzt werden.
Beschränkung des SMTP-Ports	Portnummer 25 Unter <E-Mail/I-Fax Settings> > <Communication Settings> ist die Option <SMTP RX> auf <Off> eingestellt. Der SMTP-Empfang ist nicht möglich.
Beschränkung des dedizierten Ports	Portnummer: 9002, 9006, 9007, 9011–9015, 9017–9019, 9022, 9023, 9025, 20317, 47545–47547 Wenn der dedizierte Port eingeschränkt ist, können Sie die Remote-Kopier-, Remote-Fax-, Remote-Scan- oder Remote-Druckfunktionen, die Remote-Anwendungen und vieles mehr nicht nutzen.
Beschränkung des Remotebetrieb-Software-Ports	Portnummer 5900 <Remote Operation Settings> ist auf <Off> eingestellt. Die Remote-Bedienfunktionen können nicht genutzt werden.
Beschränkung des SIP (IP-Fax)-Ports	Portnummer 5004, 5005, 5060, 5061, 49152 Die Optionen <Use Intranet> unter <Intranet Settings>, <Use NGN> unter <NGN Settings> sowie <Use VoIP Gateway> unter <VoIP Gateway Settings> sind auf <Off> eingestellt. Das IP-Fax kann nicht genutzt werden.
Beschränkung des mDNS-Ports	Portnummer 5353 Unter <mDNS Settings> sind die Optionen <Use IPv4 mDNS> und <Use IPv6 mDNS> auf <Off> eingestellt. <Use Mopria> ist auf <Off> eingestellt. Es ist nicht möglich, das Netzwerk zu durchsuchen oder automatische Einstellungen vorzunehmen. Bei Verwendung von mDNS kann man außerdem nicht über Mopria™ oder AirPrint drucken.
Beschränkung des SLP-Ports	Portnummer 427 Unter <Multicast Discovery Settings> ist die Option <Response> auf <Off> eingestellt. Sie können das Netzwerk nicht mit SLP durchsuchen und keine automatische Einstellungen vornehmen.
Beschränkung des SNMP-Ports	Portnummer 161 Wenn der SNMP-Port eingeschränkt ist, können Sie eventuell die Gerätedaten nicht aus dem Druckertreiber oder der Management-Software abrufen oder dort festlegen. Unter <SNMP Settings> sind die Optionen <Use SNMPv1> und <Use SNMPv3> auf <Off> eingestellt.

2. Authentifizierung	Anmerkungen
Authentifizierungs-Betriebsrichtlinie	
Verbot von Gastnutzern	• <Advanced Space Settings> > <Authentication Management> ist auf <On> eingestellt. • <Login Screen Display Settings> ist auf <Display When Device Operation Starts> eingestellt. • <Restrict Job from Remote Device without User Auth.> ist auf <On> eingestellt. Nicht-registrierte Nutzer können sich am Gerät nicht einloggen. Druckjobs, die von einem PC aus versandt wurden, werden ebenfalls abgebrochen.
Zwangseinstellung der automatischen Abmeldung	Diese Einstellung gilt für die Abmeldung beim Bedienfeld, nicht jedoch für andere Abmeldeverfahren (zulässige Werte: 10 Sekunden bis 9 Minuten). <Auto Reset Time> ist aktiviert. Der Nutzer wird automatisch abgemeldet, wenn innerhalb eines festgelegten Zeitraums keine Aktionen durchgeführt werden. Wählen Sie im Einstellungsbildschirm der Fernzugriffs-Nutzeroberfläche die Option [Time Until Logout].
Kennwort-Betriebsrichtlinie	
Verbot des Zwischenspeicherns von Kennwörtern für externe Server	Diese Einstellung gilt nicht für Kennwörter, die der Benutzer ausdrücklich speichert, wie Kennwörter für Adressbücher und einige mehr. <Prohibit Caching of Authentication Password> ist auf <On> eingestellt. Beim Zugriff auf einen externen Server müssen die Benutzer stets ein Kennwort eingeben.
Warnmeldung bei Verwendung von Standardkennwort	<Display Warning When Default Password Is in Use> ist auf <On> eingestellt. Sobald das werkseitige Gerätekennwort verwendet wird, erfolgt eine Warnmeldung.
Verbot der Verwendung von Standardkennwort für Fernzugriff	<Allow Use of Default Password for Remote Access> ist auf <Off> eingestellt. Beim Zugriff auf das Gerät von einem Computer aus ist das werkseitige Kennwort nicht zulässig.
Richtlinie für Kennwort-Einstellungen (nicht für Abteilungs-ID-Verwaltung oder PIN)	
Vorgeschriebene Mindestanzahl an Zeichen für Kennwort	Zulässige Werte für die Mindest-Zeichenanzahl: 1 bis 32
Eingeschränkte Gültigkeitsdauer des Kennworts	Zulässige Werte für den Gültigkeitszeitraum: 1 bis 180 Tage
Verbot von 3 oder mehr identischen aufeinanderfolgenden Zeichen	
Vorgeschriebene Verwendung von mind. einem Großbuchstaben	
Vorgeschriebene Verwendung von mind. einem Kleinbuchstaben	
Vorgeschriebene Verwendung von mind. einer Ziffer	
Vorgeschriebene Verwendung von mind. einem Satzzeichen	
Sperrrichtlinie	
Ermöglichen einer Sperrung	Gilt nicht für Abteilungs-ID/Mailbox-PIN, PIN-Authentifizierung oder Authentifizierung für sicheres Drucken und einige mehr. Sperrschwelle – zulässige Werte: 1 bis 10 Mal Sperrdauer – zulässige Werte: 1 bis 60 Minuten
3. Schlüssel / Zertifikat	**Anmerkungen**

Verbot einer schwachen Verschlüsselung	Gilt für IPSec, TLS, Kerberos, S/MIME, SNMPv3 und WLAN. Die Datenübertragung mit Geräten, die lediglich die schwache Verschlüsselung unterstützen, ist eventuell nicht möglich.
Verbot von Schlüssel/ Zertifikat mit schwacher Verschlüsselung	Gilt für IPSec, TLS und S/MIME. Ein Schlüssel-/Zertifikatspaar mit schwacher Verschlüsselung für TLS wird durch das vorinstallierte Schlüssel-/Zertifikatspaar ersetzt. Bei anderen Funktionen (außer TLS) ist eine Datenübertragung mit einem Schlüssel-/Zertifikatspaar mit schwacher Verschlüsselung nicht möglich.
Verwendung von TPM zur Speicherung von Kennwort und Schlüssel	Nur für Geräte, auf denen TPM installiert ist. Machen Sie stets eine Sicherheitskopie der TPM-Schlüssel, wenn TPM aktiviert ist. Einzelheiten erfahren Sie im Nutzerhandbuch. Wichtiger Hinweis bei aktivierten TPM-Einstellungen: • Ändern Sie den Standardwert für das „Administrator"-Kennwort, sodass Dritte den TPM-Schlüssel nicht sichern können. Wenn ein Dritter den TPM-Sicherungsschlüssel erlangt, können Sie den TPM-Schlüssel nicht wiederherstellen. • Zur Erhöhung der Sicherheit kann der TPM-Schlüssel nur ein einziges Mal gesichert werden. Wenn die TPM-Einstellungen aktiviert sind, sichern Sie den TPM-Schlüssel in jedem Fall auf einem USB-Speichergerät, und bewahren Sie dieses Speichergerät an einem sicheren Ort vor Verlust und Diebstahl geschützt auf. • Die Sicherheitsfunktionen der TPM können keinen hundertprozentigen Schutz der Daten und der Hardware garantieren.

4. Protokoll	Anmerkungen
Erzwungene Aufzeichnung des Prüfprotokolls	• <Save Operation Log> ist auf <On> eingestellt. • <Display Job Log> ist auf <On> eingestellt. • <Retrieve Job Log with Management Software> unter <Display Job Log> ist auf <Allow> eingestellt. • <Save Audit Log> ist auf <On> eingestellt. • <Retrieve Network Authentication Log> ist auf <On> eingestellt. Wenn diese Einstellung aktiviert ist, werden die Prüfprotokolle stets festgehalten.
Erzwungene SNTP-Einstellungen	Geben Sie die Adresse des SNTP-Servers ein. In <SNTP Settings> ist <Use SNTP> auf <On> eingestellt. Zeitsynchronisierung via SNTP ist erforderlich. Geben Sie einen Wert für [Server Name] im Einstellungsbildschirm der Fernzugriffs-Nutzeroberfläche ein.
Berichte zur Syslog-Protokollierung	Bei der Nutzung eines Syslog-Servers oder SIEM sollten die Syslog-Zielinformationen aktiviert werden • <Benutzername und Kennwort> • <SMB-Servername> • <Zielpfad> • <Zeitpunkt des Exports>

5. Job	Anmerkungen
Druckrichtlinie	
Verbot des sofortigen Drucks von empfangenen Jobs	Wenn der sofortige Druck der empfangenen Aufträge untersagt ist, werden diese Aufträge im Fax-/I-Fax-Speicher abgelegt. • <Handle Files with Forwarding Errors> ist auf <Off> eingestellt. • <Use Fax Memory Lock> ist auf <On> eingestellt. • <Use I-Fax Memory Lock> ist auf <On> eingestellt. • <Memory Lock End Time> ist auf <Off> eingestellt. • <Display Print When Storing from Printer Driver> ist in <Set/Register Confidential Fax Inboxes> auf <Off> eingestellt. • <Settings for All Mail Boxes> > <Print When Storing from Printer Driver> ist auf <Off> eingestellt. • <Box Security Settings> > <Display Print When Storing from Printer Driver> ist auf <Off> eingestellt. • <Prohibit Job from Unknown User> sowie <Forced Hold> sind auf <On> eingestellt. Der Druck wird selbst dann nicht sofort gestartet, wenn ein Druckvorgang ausgeführt wird.
Sende-/Empfangsrichtlinie	
Versand nur an registrierte Adressen	Unter <Limit New Destination> sind die Optionen <Fax>, <E-Mail>, <I-Fax> und <File> auf <On> eingestellt. Der Versand ist nur an Ziele möglich, die im Adressbuch eingetragen sind.
Erzwungene Bestätigung der Faxnummer	Beim Senden einer Faxnachricht müssen die Benutzer die Faxnummer ein zweites Mal zur Bestätigung eingeben.
Verbot der automatischen Weiterleitung	<Use Forwarding Settings> ist auf <Off> eingestellt. Faxnachrichten können nicht automatisch weitergeleitet werden.

6. Speicherung	Anmerkungen
Erzwungene Komplettlöschung von Daten	<Hard Disk Data Complete Deletion> ist auf <On> eingestellt.

Die gesamten technischen Daten der imageRUNNER ADVANCE finden Sie auf dieser Webseite:
https://www.canon.de/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Deutschland GmbH
Europark Fichtenhain A10
D-47807 Krefeld
Canon Helpdesk
Tel.: +49 2151 3450
Fax: +49 2151 345 102
canon.de

Canon Austria GmbH
Oberlaaer Straße 233
A-1100 Wien
Canon Helpdesk
Tel. (01) 360 277 4567
canon.at

Canon (Schweiz) AG
Richtistrasse 9
CH-8304 Wallisellen
Tel. +41 (0) 848 833 835
canon.ch

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

German edition v1.0