GUIDA ALLA CONFIGURAZIONE SICURA

imageRUNNER ADVANCE

Canon

INTRODUZIONE

I dispositivi multifunzione Canon offrono funzionalità di stampa, copia, scansione, invio e fax. Le MFP sono server informatici indipendenti che forniscono una serie di servizi in rete e avanzate capacità di archiviazione su disco rigido.

Nel momento in cui un'organizzazione introduce questi dispositivi nella propria infrastruttura, ci sono diverse aree sulle quali bisogna concentrarsi nell'ambito di una più ampia strategia di sicurezza, orientata a proteggere la riservatezza, l'integrità e la disponibilità dei sistemi in rete.

Chiaramente, le tipologie di implementazione saranno variabili e ciascuna organizzazione avrà i propri requisiti di sicurezza specifici. Parallelamente al nostro impegno congiunto per garantire che i dispositivi Canon vengano forniti con adeguate impostazioni di sicurezza iniziali, desideriamo migliorare ulteriormente tale aspetto fornendo una serie di impostazioni di configurazione per garantire un migliore allineamento del dispositivo con i requisiti specifici dell'azienda.

Questo documento è progettato in modo da fornire informazioni sufficienti per consentirvi di valutare con Canon o un partner Canon le impostazioni più adeguate per il vostro ambiente operativo. È importante notare che non tutto l'hardware dei dispositivi presenta lo stesso livello di capacità, e sistemi software diversi possono fornire funzionalità diverse. Una volta definita, la configurazione finale può essere applicata a un singolo dispositivo o all'intero parco dispositivi. Vi invitiamo a contattare Canon o un partner Canon per ricevere ulteriori informazioni e assistenza.

A chi è destinato questo documento?

Questo documento è destinato a chiunque si occupi della progettazione, dell'implementazione e della sicurezza dei dispositivi multifunzione (MFP) per ufficio all'interno di un'infrastruttura di rete. Le figure interessate possono comprendere specialisti IT e di rete, professionisti della sicurezza IT e personale di assistenza.

Ambito e copertura

La guida illustra e consiglia le impostazioni di configurazione per due ambienti di rete tipici, per consentire alle organizzazioni di implementare in modo sicuro una soluzione MFD basata sulle best practice di settore. Viene inoltre spiegato come utilizzare la funzionalità Syslog (della piattaforma software versione 3.8) per ottenere feedback in tempo reale dal dispositivo MFD. Queste impostazioni sono state testate e validate dal team di sicurezza Canon.

Non formuliamo alcuna ipotesi su specifici requisiti normativi di settore che potrebbero imporre altre valutazioni di sicurezza e che non rientrano nell'ambito di applicazione di questo documento.

Questa guida è stata creata in base al set tipico di funzionalità della piattaforma imageRUNNER ADVANCE e, sebbene le informazioni qui riportate si applichino a tutti i modelli della gamma imageRUNNER ADVANCE, alcune caratteristiche potrebbero differire da un modello all'altro.

Implementazione delle impostazioni di sicurezza più adeguate per il proprio ambiente operativo

Per esplorare le implicazioni di sicurezza associate all'implementazione di un dispositivo multifunzione in una rete aziendale, abbiamo preso in considerazione due scenari tipici:

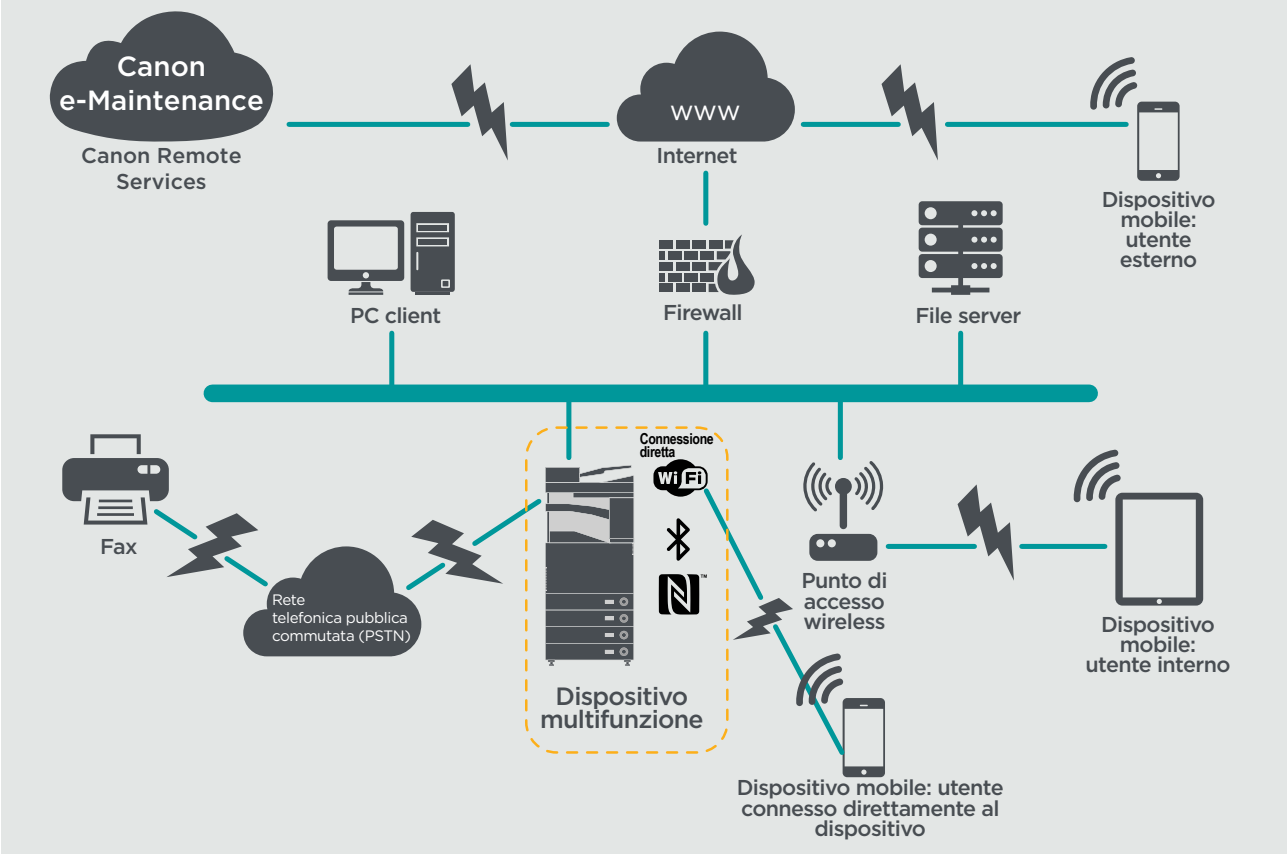
- **L'ambiente di un piccolo ufficio**
- **L'ambiente di ufficio di una grande azienda**

AMBIENTE TIPICO DI UN PICCOLO UFFICIO

In genere si tratta di un ambiente di un piccola impresa con una topologia di rete non segmentata. Utilizza uno o due MFP per applicazioni interne e tali dispositivi non sono accessibili online.

Nonostante siano disponibili funzionalità di stampa mobile, saranno necessari componenti aggiuntivi. Per gli utenti che richiedono servizi di stampa al di fuori di un ambiente LAN, è necessaria una connessione sicura, ma questo aspetto non sarà trattato nella presente guida. Tuttavia, occorre prestare attenzione alla sicurezza dei dati in transito fra il dispositivo remoto e l'infrastruttura di stampa.

Figura 1 Rete di un piccolo ufficio



L'ultima generazione di modelli imageRUNNER ADVANCE fornisce connettività di rete wireless, consentendo al dispositivo di connettersi a una rete Wi-Fi. Il dispositivo può anche essere utilizzato per stabilire una connessione Wi-Fi diretta point-to-point con un dispositivo mobile senza ricorrere ad alcuna connessione di rete aziendale.

Le opzioni Bluetooth e NFC sono disponibili per diversi modelli di dispositivo e possono essere utilizzate per stabilire la connessione WiFi Direct con dispositivi iOS e Android.

NOTE SULLA CONFIGURAZIONE

Si noti che le eventuali funzionalità imageRUNNER ADVANCE non menzionate qui di seguito sono da ritenersi sufficienti nelle impostazioni predefinite per questa specifica tipologia di azienda o ambiente di rete.

Tabella 1 Note sulla configurazione dell'ambiente di un piccolo ufficio

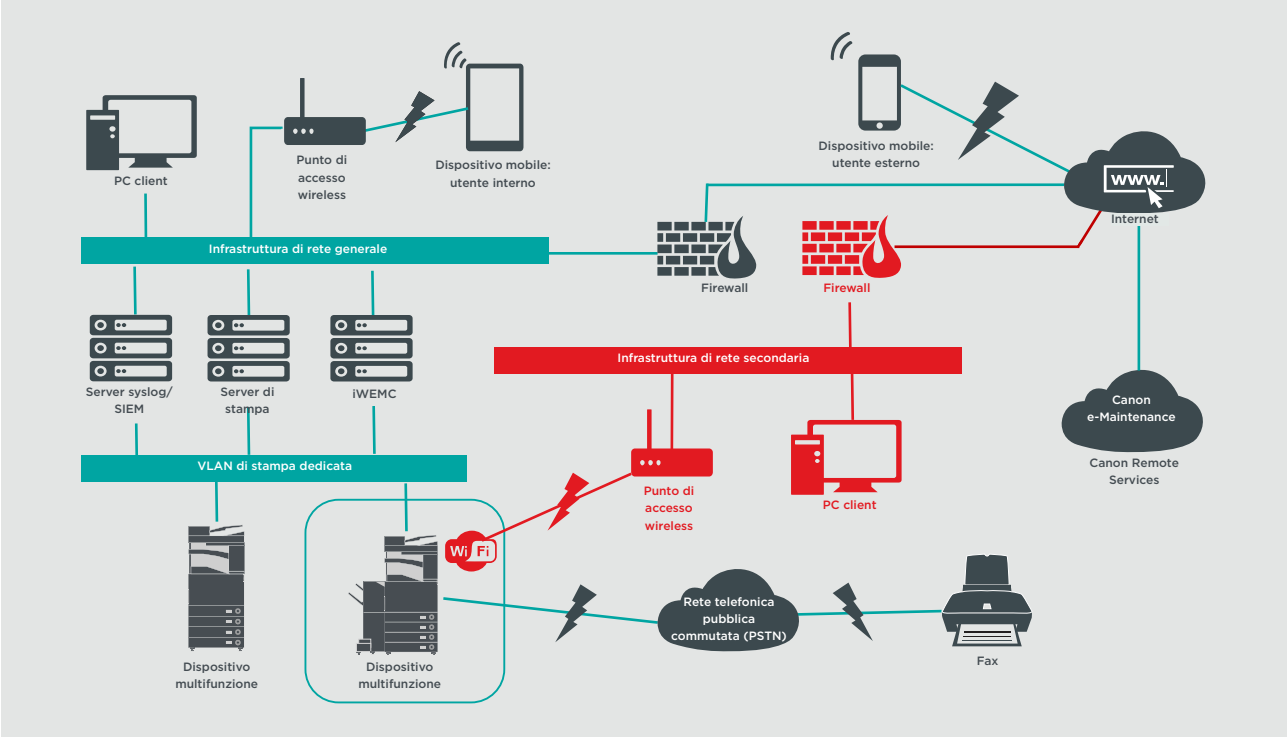
Funzionalità imageRUNNER ADVANCE	Descrizione	Note
Modalità servizio	Consente l'accesso alle impostazioni della modalità servizio	Protezione con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
Sistema di gestione modalità servizio	Consente di accedere a varie impostazione non standard dei dispositivi	Protezione con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
SMB Browsing/Invio SMB	Consente di archiviare e recuperare informazioni da e verso le condivisioni di rete Windows/SMB	Solitamente, gli amministratori di sistema non consentono ad alcun utente di creare account locali sul proprio computer client per l'utilizzo nella condivisione di documenti con imageRUNNER ADVANCE su SMB
Interfaccia utente da remoto	Strumento di configurazione web-based	L'amministratore imageRUNNER ADVANCE deve abilitare il protocollo HTTPS per l'interfaccia utente remota e disabilitare l'accesso HTTP. Abilita l'uso dell'autenticazione PIN univoco per ciascun dispositivo
SNMP	Integrazione del monitoraggio di rete	Disabilitare la versione 1 e abilitare solo la versione 3
Invio a e-mail e/o IFAX	Invia email dal dispositivo con allegati	Abilitazione SSL Non utilizzare l'autenticazione POP3 prima di inviare tramite SMTP Utilizzare l'autenticazione SMTP
POP3	Recupera e stampa automaticamente i documenti dalla casella di posta	Abilitazione SSL Abilita l'autenticazione POP3
Rubrica/LDAP	Utilizza il servizio directory per cercare numeri telefonici privati o indirizzi di posta elettronica a cui inviare le scansioni	Abilitazione SSL Non utilizzare le credenziali di dominio per l'autenticazione con il server LDAP, bensì utilizzare le credenziali specifiche LDAP
Stampa FTP	Caricamento e scaricamento documenti da e verso il server FTP incorporato	Attiva l'autenticazione FTP. Tenere presente che il traffico FTP viaggerà sempre in chiaro sulla rete
Invio WebDAV	Consente di digitalizzare e archiviare i documenti in una posizione remota	Abilita l'autenticazione per le condivisioni WebDAV
PDF crittografato	Protegge i documenti con crittografia	Di norma, i documenti sensibili dovrebbero essere crittografati esclusivamente tramite PDF versione 1.6 (AES-128)
Stampa protetta	Il lavoro di stampa viene inviato al dispositivo, ma rimane bloccato in coda di stampa fino all'immissione del numero PIN corrispondente	Abilita lavori di stampa protetti da PIN
Notifica eventi di Syslog	System Logging Protocol (Syslog) è un protocollo standard di settore che consente di inviare messaggi relativi agli eventi o ai registri del sistema a uno specifico server denominato server Syslog	È consigliabile inviare i dati Syslog di imageRUNNER a uno strumento di analisi Syslog disponibile in rete o a una piattaforma SIEM (Security Event Management System).
Verifica del sistema all'avvio	Garantisce che i componenti software del sistema non siano stati compromessi. Ha un impatto minimo sui tempi di avvio del sistema	Abilita la funzione
Browser web incorporato	Accesso del browser a Internet	Tramite le funzionalità di amministrazione, impone l'uso di un proxy web per il filtraggio dei contenuti e per evitare l'accesso a contenuti dannosi o virali. Disabilita la creazione di preferiti
Bluetooth ed NFC (disponibile a partire dai modelli di terza generazione)	Utilizzato per stabilire una connessione WiFi Direct	Abilita WiFi Direct per consentire la connessione diretta a un dispositivo mobile. WiFi Direct non può essere utilizzato quando si utilizza il WiFi per connettersi a una rete
LAN wireless	Fornisce l'accesso wireless	Utilizzare WPA-PSK/WPA2-PSK con password sicure
IPP	Connette e invia lavori di stampa su IP	Disabilita IPP
TPM	Una funzione che memorizza nell'hardware i dati di sicurezza, come le password e le chiavi di crittografia, al fine di garantire la massima protezione	Questa funzione è disattivata per impostazione predefinita. Quando questa opzione è abilitata, si consiglia di eseguire un backup

L'AMBIENTE DI UFFICIO AZIENDALE

Si tratta in genere di un ambiente multi-sito e multi-ufficio con architettura di rete segmentata. Dispone di più MFD distribuiti su una VLAN separata accessibile per l'utilizzo interno tramite server di stampa. Questi MFD non sono accessibili da Internet.

Questo ambiente dispone generalmente di un team permanente per l'applicazione dei requisiti di rete e di back-office e la risoluzione di problemi informatici generali, tuttavia tale team potrebbe non avere competenze specifiche in materia di MFP.

Figura 2 Operazioni in un ufficio aziendale



Le connessioni evidenziate in rosso saranno disponibili dai modelli di terza generazione

NOTE SULLA CONFIGURAZIONE

Si noti che le eventuali funzionalità imageRUNNER ADVANCE non menzionate qui di seguito sono da ritenersi sufficienti nelle impostazioni predefinite per questa specifica azienda o ambiente di rete.

Tabella 2 Note sulla configurazione dell'ambiente di un piccolo ufficio

Funzionalità imageRUNNER ADVANCE	Descrizione	Note
Modalità servizio	Consente l'accesso alle impostazioni della modalità servizio	Protezione con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
Sistema di gestione modalità servizio	Consente di accedere a varie impostazioni non standard dei dispositivi	Protezione con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
SMB Browsing/Invio SMB	Consente di archiviare e recuperare informazioni da e verso le condivisioni di rete Windows/SMB	Solitamente gli amministratori di sistema non consentono ad alcun utente di creare account locali sul proprio computer per l'utilizzo nella condivisione di documenti con imageRUNNER ADVANCE su SMB
Interfaccia utente da remoto	Strumento di configurazione web-based	Le seguenti configurazioni iniziali del dispositivo disabilitano completamente l'interfaccia utente remota disattivando i protocolli HTTP e HTTPS
SNMP	Integrazione del monitoraggio di rete	Disabilitare la versione 1 e abilitare solo la versione 3
Invio a e-mail e/o IFAX	Invia email dal dispositivo con allegati	Abilitazione SSL Abilita: - Verifica del certificato sul server SMTP O se non è possibile: - Utilizzare questa funzione solo in un ambiente in cui sia presente un sistema di rilevamento delle intrusioni di rete; non utilizzare l'autenticazione POP3 prima dell'invio tramite SMTP; utilizzare l'autenticazione SMTP
POP3	Recupera e stampa automaticamente i documenti dalla casella di posta	Abilitazione SSL Abilita: - Verifica del certificato sul server POP3 O se non è possibile: - Utilizzare questa funzione solo in un ambiente in cui sia presente un sistema di rilevamento delle intrusioni di rete; abilitare l'autenticazione POP3
Rubrica/LDAP	Utilizza il servizio directory per cercare numeri telefonici o indirizzi di posta elettronica a cui inviare le scansioni	Abilitazione SSL Abilita: - Verifica del certificato sul server LDAP O se non è possibile: - Utilizzare questa funzione solo in un ambiente in cui sia presente un sistema di rilevamento delle intrusioni di rete; non utilizzare le credenziali di dominio per l'autenticazione con il server LDAP; utilizzare credenziali specifiche LDAP
IPP	Connette e invia lavori di stampa su IP	Disabilita IPP
Invio WebDAV	Consente di digitalizzare e archiviare i documenti in una posizione remota	Abilita l'autenticazione per le condivisioni WebDAV Abilita SSL Attiva la stampante per consentire il caricamento esclusivo di file che terminano con le "estensioni di stampa dei file"
IEEE802.1X	Meccanismo di autenticazione dell'accesso di rete	EAPOL V1 supportato
PDF crittografato	Protegge i documenti con crittografia	Di norma, i documenti sensibili dovrebbero essere crittografati esclusivamente tramite PDF versione 1.6 (AES-128)
Stampa sicura crittografata	Migliora la protezione Secure Print crittografando il file e la password durante la trasmissione	Configurare il nome utente nella scheda Stampante sulla configurazione della stampante client con un nome utente diverso rispetto alle credenziali di dominio/LDAP dell'utente interessato. Verificare che la funzionalità "Limita lavori stampante" sia disattivata
Registrazione automatica dei certificati	Il processo di registrazione automatica aumenta l'efficienza del recupero dei certificati digitali e della loro distribuzione	Richiede la disponibilità di una soluzione di gestione dei certificati di rete
Notifica eventi di Syslog	System Logging Protocol (Syslog) è un protocollo standard di settore che consente di inviare messaggi relativi agli eventi o ai registri del sistema a uno specifico server denominato server Syslog	È consigliabile inviare i dati Syslog di imageRUNNER ADVANCE a uno strumento di analisi Syslog disponibile in rete o a una piattaforma SIEM (Security Event Management System)
Verifica del sistema all'Avvio	Garantisce che i componenti software del sistema non siano stati compromessi. Ha un impatto minimo sui tempi di avvio del sistema	Abilita la funzione
LAN wireless	Fornisce l'accesso wireless	Utilizzare WPA-PSK/WPA2-PSK con password sicure
WiFi Direct	Utilizzato per stabilire una connessione WiFi Direct	Disabilita WiFi Direct
Browser web incorporato (disponibile dai modelli di terza generazione, seconda edizione)	Accesso del browser a Internet	Applica le restrizioni appropriate o disabilita la possibilità di scaricare file acquisiti tramite browser

L'ultima generazione di modelli imageRUNNER ADVANCE fornisce connettività di rete wireless, consentendo al dispositivo di connettersi a una rete WiFi e simultaneamente a una rete fisica. Questo scenario può essere utile quando il cliente desidera condividere un dispositivo su due reti. Un ambiente scolastico è un tipico esempio in cui sono presenti reti separate, rispettivamente per il personale e gli studenti.

La piattaforma imageRUNNER ADVANCE offre un insieme di funzionalità che consente un uso flessibile. Con i protocolli e i servizi disponibili per raggiungere questo obiettivo, è importante garantire che solo le funzionalità, i servizi e i protocolli richiesti siano abilitati per soddisfare le esigenze dell'utente. Questa è una buona procedura di sicurezza e ridurrà la potenziale superficie di attacco e ne impedirà lo sfruttamento. Dal momento che compaiono costantemente nuove vulnerabilità, dobbiamo sempre stare attenti a comprometterle, sia intrinsecamente che estrinsecamente al dispositivo. Avere la possibilità di monitorare l'attività dell'utente è utile per aiutare a identificare e adottare azioni correttive quando necessario.

La piattaforma software imageRUNNER ADVANCE versione 3.8 fornisce alcune funzionalità aggiuntive rispetto a quelle disponibili già da diversi anni. Queste includono la possibilità di monitorare il dispositivo in tempo reale utilizzando Syslog e la verifica del sistema all'avvio. L'utilizzo di queste funzionalità insieme a soluzioni di sicurezza di rete esistenti, come ad esempio una piattaforma di Security Information Event Management o una soluzione di registrazione, consente una maggiore visibilità e l'identificazione degli incidenti per scopi forensi.

Trusted Platform Module (TPM)

Ogni dispositivo imageRUNNER ADVANCE include un modulo TPM (Trusted Platform Module) che è un chip di sicurezza aperto a prova di manomissione (i modelli imageRUNNER ADVANCE DX sono dotati di TPM 2.0). Consente l'archiviazione di password, certificati digitali e chiavi di crittografia.

Tutti gli attuali modelli imageRUNNER ADVANCE con disco rigido o unità a stato solido forniscono una crittografia completa dell'unità, la cui chiave di crittografia è memorizzata nel Security Chip Canon MFP, conforme allo standard di sicurezza FIPS 140-2 Level 2 (in vigore negli Stati Uniti), e non nel TPM.

Per impostazione predefinita, la funzionalità TPM è disabilitata; tuttavia, può essere abilitata accedendo al menu delle funzioni aggiuntive di imageRUNNER ADVANCE. Si consiglia vivamente di eseguire il backup del TPM in caso di guasto immediatamente dopo l'attivazione. Occorre notare che è possibile eseguire il backup solo una volta su una chiavetta USB.

Per ulteriori informazioni relative al TPM, indirizza il browser Web al link seguente e inserisci **Utilizzo del TPM** nella casella di ricerca. Questo fornirà informazioni relative a:

- Attivazione del TPM
- Backup e ripristino del TPM

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Verifica del sistema all'avvio

Questa funzionalità è un meccanismo hardware espressamente progettato per garantire che tutti i componenti del software imageRUNNER ADVANCE di terza generazione, edizione III, vengano verificati in base a una fonte di attendibilità per garantire che il sistema operativo venga caricato come previsto da Canon. Se un malintenzionato dovesse manomettere o cercare di modificare il sistema, o si verifica un errore durante il caricamento del sistema, il processo si arresta e viene visualizzato un codice di errore.

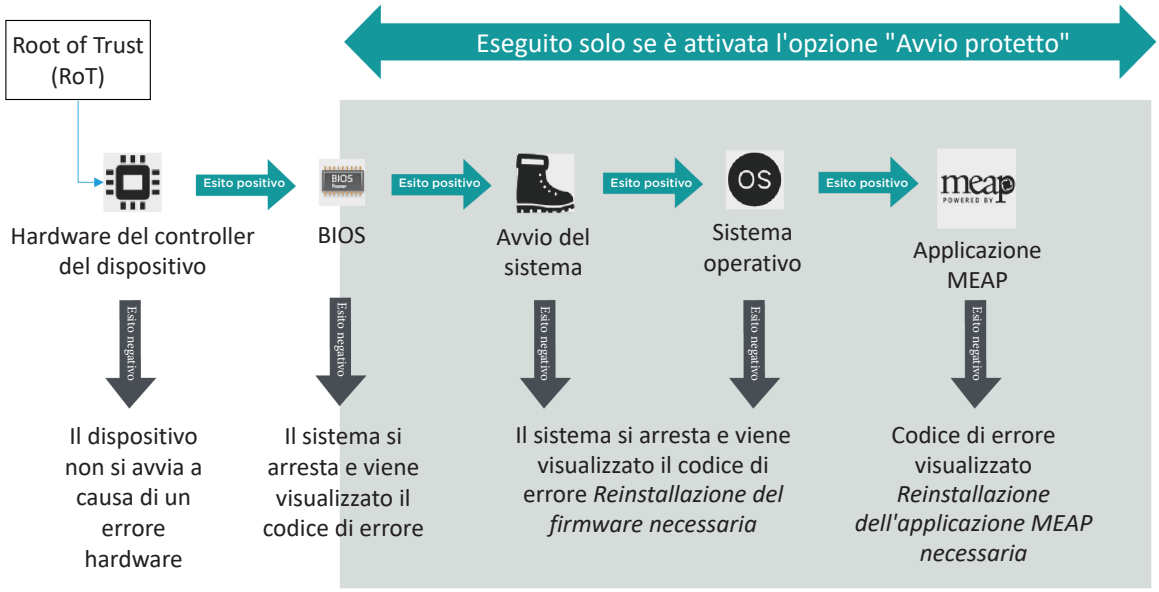


Figura 3 Processo di verifica del sistema all'avvio

Questo processo è trasparente all'utente, a parte il fatto che viene visualizzato un messaggio per indicare il caricamento di una versione imprevista del sistema. Il software imageRUNNER ADVANCE di terza generazione, edizione III, offre la possibilità di abilitare l'opzione Verifica del sistema all'avvio, che deve essere attivata per abilitare questa funzionalità di sicurezza.

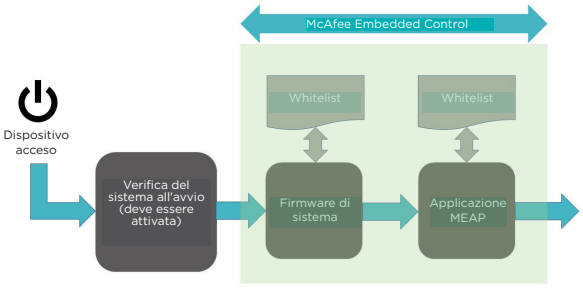


Figura 4 Processo di avvio del dispositivo, dall'inizio e durante l'esecuzione

McAfee Embedded Control

Con l'aggiunta di McAfee Embedded Control, a partire dalla piattaforma 3.9, i modelli imageRUNNER ADVANCE di terza generazione, edizione III, dispongono di un ulteriore livello di protezione dei dispositivi. A seconda della gravità, le modifiche non autorizzate al firmware di sistema dell'ambiente MEAP possono determinare l'arresto del dispositivo con un codice di errore o la registrazione dell'evento nel registro di audit, che verrà analizzato dall'amministratore.

Con l'aggiunta di McAfee Embedded Control, a partire dalla piattaforma 3.9, un ulteriore livello di file di programma non inclusi nella whitelist viene considerato non autorizzato al fine di impedirne l'esecuzione. Questo consente di impedire a worm, virus, spyware e altro malware di compromettere il dispositivo. Quando è abilitato, nel registro di audit è disponibile una registrazione di tutte le esecuzioni bloccate. Caratteristiche di McAfee Embedded Control:

- Previene la manomissione del software durante l'esecuzione, attraverso l'implementazione di una "whitelist" fornita da McAfee
- Arresta il sistema con un codice di errore o registra l'evento nel registro di audit, che verrà analizzato dall'amministratore, a seconda della gravità
- McAfee Embedded Control è una funzionalità standard dei modelli di terza generazione, edizione III
- È disattivato per impostazione predefinita: per avviare il servizio è necessario attivare Verifica del sistema all'avvio e McAfee Embedded Control
- Quando questo servizio è abilitato, i tempi di riscaldamento si allungano (fino a 60 secondi)
- Se per un dispositivo è attivato l'Avvio rapido, McAfee Embedded Control non funziona anche se l'opzione Verifica del sistema all'avvio è abilitata

McAfee Embedded Control verifica il valore contenuto nella whitelist prima dell'esecuzione del modulo, quindi controlla il valore generato dall'esecuzione del modulo durante il funzionamento. Se i due valori corrispondono, il controllo ha esito positivo, in caso contrario la verifica non viene superata e l'esecuzione del modulo non riesce. Se la verifica ha esito negativo, accade quanto segue:

(a) Il processo di verifica del firmware inizia all'avvio dell'esecuzione del modulo registrato nella whitelist. Se la verifica non viene superata, l'esecuzione viene bloccata e viene visualizzato un codice di errore (E614-xxxx).

(b) Se viene rilevato un tentativo di eseguire un modulo software non elencato, l'esecuzione si arresta e l'evento viene registrato nel registro di audit.

(c) Se viene rilevato un tentativo di riscrivere o eliminare un modulo software registrato incluso nella whitelist, il tentativo viene bloccato e il codice di errore viene salvato nel registro di audit

(d) La convalida della whitelist stessa viene eseguita all'avvio. Se viene rilevata una manomissione della whitelist, l'esecuzione viene bloccata e viene visualizzato un codice di errore. Il codice di errore visualizzato dipende dalla posizione del modulo software in cui è stata rilavata la manomissione. Esempio di codice di errore: E614-xxxx per il firmware, E602-xxxx per l'applicazione MEAP.

(e) La whitelist viene aggiornata come necessario quando viene aggiornato il firmware di sistema o quando vengono installate applicazioni MEAP autorizzate. Per garantire la coerenza, quando il modulo software viene aggiornato vengono aggiornati anche la whitelist e il registro delle transazioni in cui viene registrata la cronologia delle modifiche della whitelist.

Tutte le attività registrabili correlate ai processi di Verifica del sistema all'avvio e McAfee Embedded Control vengono elencate nel registro di gestione dei dispositivi e possono essere notificate in tempo reale a un amministrazione della sicurezza, attraverso l'integrazione con un sistema SIEM.

Cancellazione sicura dei dati

Il dispositivo multifunzione gestisce i dati per eseguire i lavori di copia, scansione, stampa e fax, nonché le rubriche, i registri di sistema e la cronologia dei lavori che potrebbero contenere anche informazioni sensibili. La piattaforma imageRUNNER ADVANCE fornisce una funzione di cancellazione sicura dei dati per garantire che non solo la voce della tabella di allocazione dei file per i dati eliminati venga rimossa, ma anche che i settori che memorizzano i dati vengano sovrascritti con dati fittizi che impediscono qualsiasi recupero.

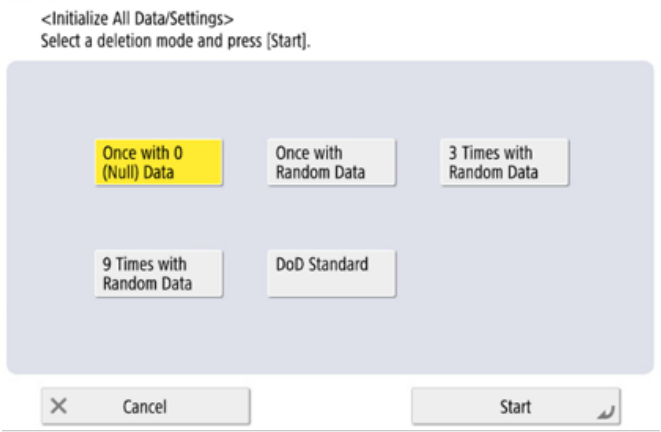


Figura 5: opzioni di sovrascrittura dei dati per imageRUNNER ADVANCE dotato di unità HDD

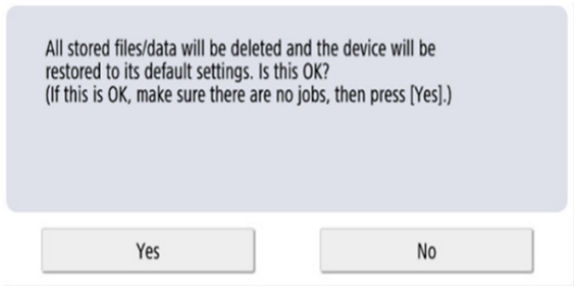


Figura 6: inizializzazione di tutti i dati SSD per imageRUNNER ADVANCE

A seconda del modello specifico del dispositivo, viene utilizzato un disco rigido (HDD) o un'unità di memoria a stato solido (SSD). Poiché un HDD utilizza un piatto fisico rotante su cui vengono registrati i dati, è necessario effettuare una serie di sovrascritture, in genere tre, per garantire che i dati vengano effettivamente sovrascritti. Tuttavia, la tecnologia SSD gestisce l'archiviazione in modo diverso, distribuendo l'allocazione della memoria in modo uniforme su tutto lo spazio disponibile, rendendo inutile la necessità di sovrascrivere i dati più volte.

Tecnologia SSD

A differenza di un'unità HDD, con un'unità SSD non dovrebbe essere necessario eseguire la manutenzione, in quanto l'autosufficienza è stata incorporata secondo progetto utilizzando algoritmi e dispositivi di sicurezza per garantire che i dati vengano eliminati in modo efficiente, massimizzando la durata di vita. I dati vengono memorizzati elettricamente in celle di memoria a stato solido, con un vantaggio in termini di velocità di accesso, ma con il problema del numero limitato di scritture di ogni cella.

Livellamento dell'usura

Per contrastare il problema dell'usura eccessiva di un particolare blocco di memoria, viene utilizzato un processo noto come livellamento dell'usura per garantire che il numero di scritture si mantenga il più possibile uniforme. Vengono utilizzati due principi di livellamento dell'usura: il livellamento dinamico e il livellamento statico.

Il livellamento dinamico assegna i blocchi di memoria in modo tale che le riscritture siano riposizionate su blocchi vuoti nuovi. Un contatore di usura viene quindi incrementato per consentire al controller SSD di tenere traccia dell'usura. Il livellamento statico adotta l'approccio di spostare i dati esistenti non modificati in un nuovo blocco di memoria, distribuendo così l'usura in modo più uniforme sullo spazio disponibile. Il principio è quello di distribuire il numero di riscritture in modo uniforme su tutti i blocchi di memoria, indipendentemente dal fatto che i dati cambino solo occasionalmente o costantemente. Il processo "TRIM" contribuisce a prolungare la vita utile e a garantire una mappatura dei dati ad alta velocità.

A seconda del modello imageRUNNER ADVANCE, diverse opzioni di configurazione possono essere utilizzate per impostare quando viene eseguita una sovrascrittura e il metodo di sovrascrittura. I modelli che usavano l'archiviazione HDD in precedenza fornivano una funzione di cancellazione completa dei dati per eliminare completamente i dati.

- L'unità SSD è una chiave di crittografia memorizzata nel dispositivo specifico; se rimossa dal dispositivo specifico, i dati vengono crittografati utilizzando **AES a 256 bit** e non possono essere letti/scritti
- Il Security Chip Canon MFP 2.10 è conforme a **FIPS 140-2 Level 2** (standard governativi statunitensi)

Inizializza tutti i dati/impostazioni

- **Limitato a [una volta con 0 (null) dati]**
- L'unità SSD è a stato solido e l'unità HDD utilizza dischi magnetici rotanti.
- Inoltre, dopo aver eseguito la scrittura una volta con 0 dati, è praticamente impossibile leggere i dati scritti perché la tabella di accesso viene riscritta, la posizione dei dati è sconosciuta.
- Poiché i dati memorizzati sono crittografati, non è possibile leggere/scrivere dati su un PC o dopo l'installazione su un altro chip MFP.

Registrazione automatica dei certificati

Nelle versioni della piattaforma software di sistema imageRUNNER ADVANCE anteriori alla 3.8, l'amministratore deve installare manualmente i certificati di sicurezza aggiornati su ciascun dispositivo.
L'aggiornamento manuale è un'attività complicata, che richiede la connessione di ciascun dispositivo uno dopo l'altro. I certificati devono essere installati manualmente tramite un'interfaccia utente remota (RUI, Remote User Interface) specifica, che prolunga notevolmente la durata del processo. Il servizio di registrazione automatica dei certificati introdotto a partire dalla versione 3.8 della piattaforma elimina completamente questo lavoro di overhead.

Il processo di registrazione automatica aumenta l'efficienza del recupero dei certificati. Offre la possibilità di recuperare automaticamente i certificati utilizzando Network Device Enrolment Service (NDES) per Microsoft Windows e Simple Certificate Enrolment Protocol (SCEP).

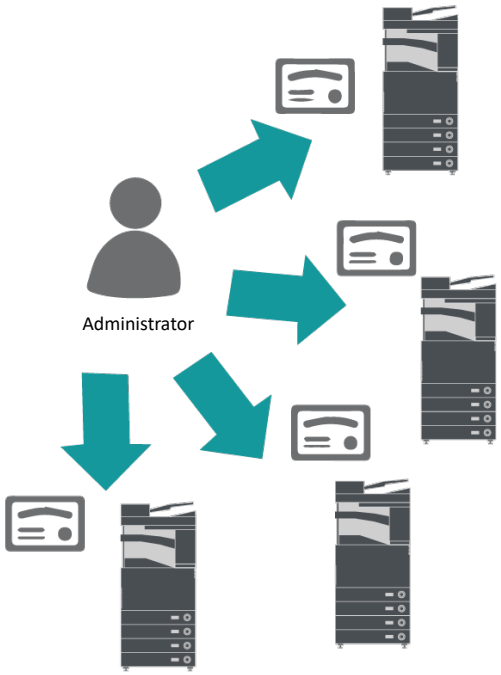


Figura 7 Registrazione dei certificati

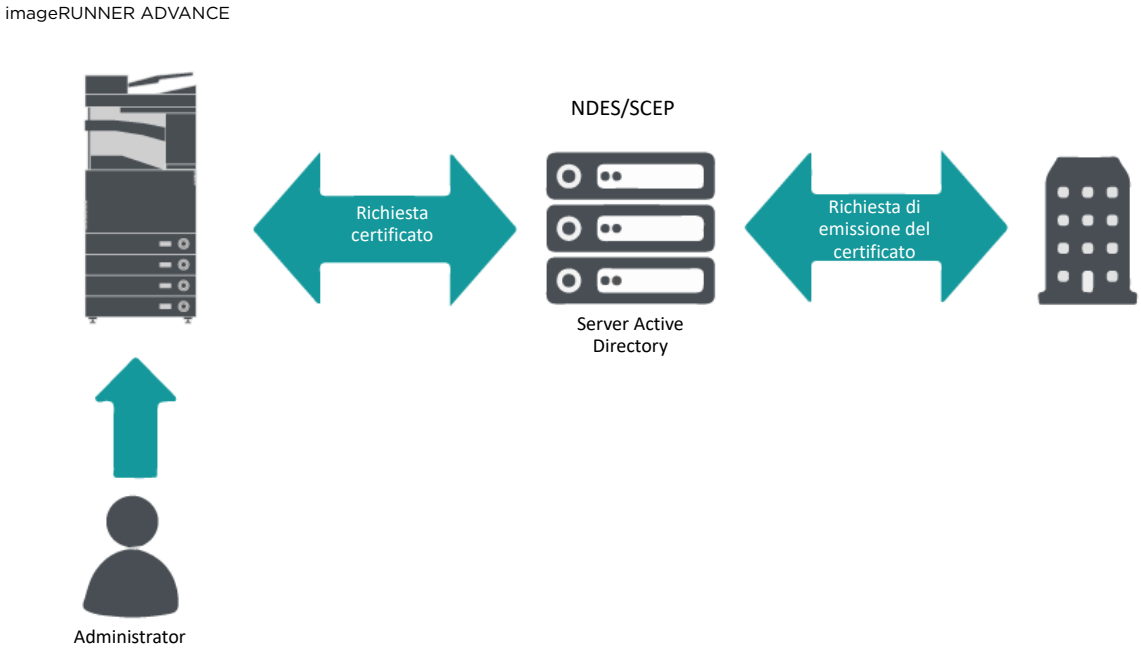


Figura 8 Processo di registrazione dei certificati

SCEP è un protocollo che supporta i certificati emessi da un'autorità di certificazione (CA, Certificate Authority), mentre NDES consente ai dispositivi di rete di recuperare o aggiornare i certificati tramite SCEP.

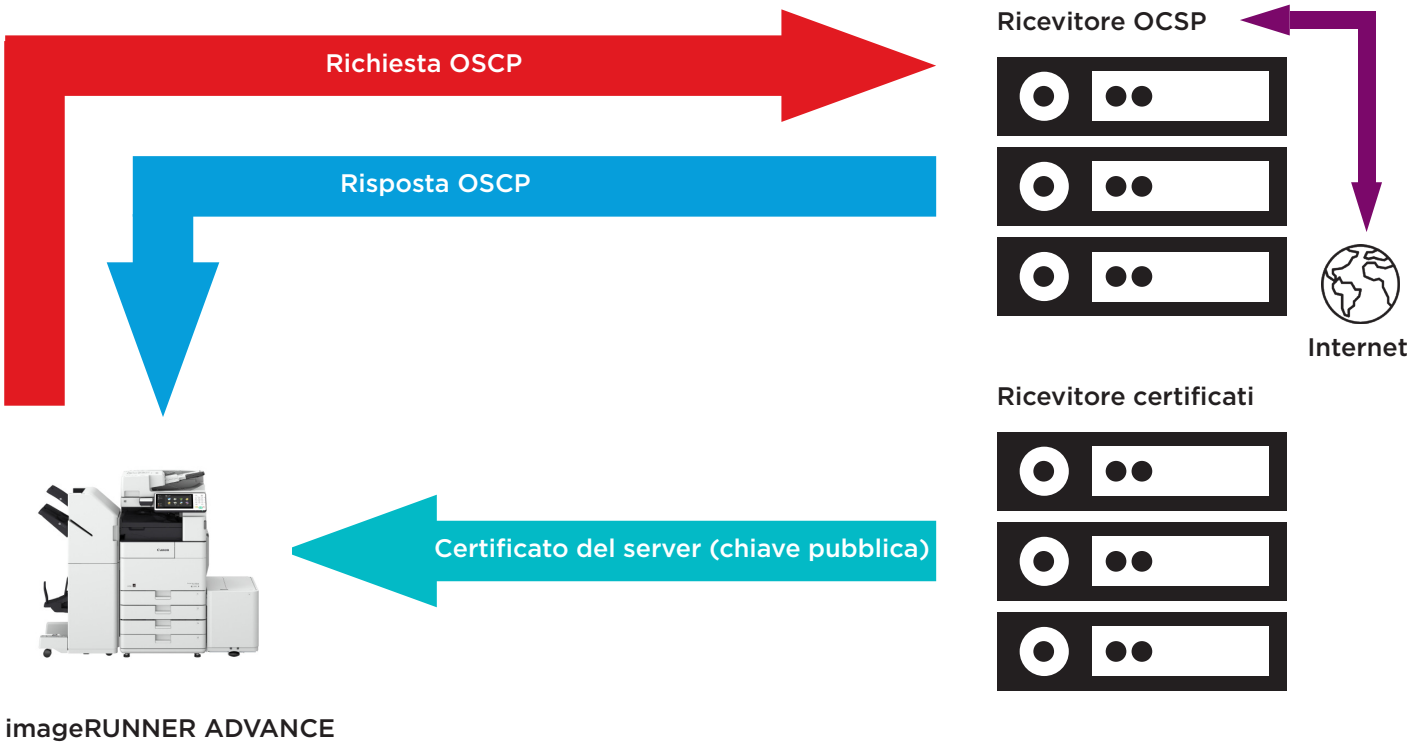
NDES è un servizio di Servizi certificati Active Directory.

Online Certificate Status Protocol

Esistono diversi motivi per cui potrebbe essere necessario revocare un certificato digitale. Ad esempio, la chiave privata è stata smarrita, rubata, compromessa o il nome di un dominio è stato modificato.

L'Online Certificate Status Protocol (OCSP) è un protocollo Internet standard che viene utilizzato per verificare lo stato di revoca di un certificato digitale X.509 fornito dal Certificate Server. Inviando una richiesta OCSP al ricevitore OCSP (in genere, un emittente di certificati) specificando un determinato certificato, il ricevitore OCSP risponderà con "in regola", "revocato" o "sconosciuto".

Figura 9 Processo di negoziazione OCSP



Con imageRUNNER ADVANCE dalla versione 3.10 della piattaforma, OCSP fornisce un meccanismo in tempo reale per verificare i certificati digitali X.509 installati. Le versioni precedenti della piattaforma supportavano solo il metodo Certificate Revoke List (CRL), che è inefficiente e comporta un pesante sovraccarico sulle risorse di rete.

Gestione di informazioni ed eventi di sicurezza

La tecnologia imageRUNNER ADVANCE supporta il push degli eventi di sicurezza in tempo reale tramite il protocollo Syslog, conforme a RFC 5424, RFC 5425 e RFC 5426.

Questo protocollo viene utilizzato da una vasta gamma di dispositivi diversi per raccogliere in tempo reale informazioni che possono essere utilizzate per identificare potenziali problemi di sicurezza.

Per semplificare il rilevamento delle minacce e degli incidenti di sicurezza, il dispositivo deve essere configurato in modo da puntare a un server SIEM (Security Incident Event Management) di terze parti.

Gli eventi Syslog generati dal dispositivo possono essere utilizzati per creare azioni attraverso la raccolta e l'analisi di eventi in tempo reale da una vasta gamma di origini dati contestuali (Figura 7). Supporta inoltre la generazione di report di conformità e l'esecuzione di indagini sugli incidenti tramite l'uso di soluzioni aggiuntive, come un server SIEM. Nella Figura 8 è illustrato un esempio.

L'ultima generazione di dispositivi imageRUNNER ADVANCE fornisce funzionalità Syslog in grado di supportare una vasta gamma di eventi che è possibile raccogliere. Tali funzionalità possono essere utilizzate anche per correlare e analizzare eventi da numerose origini diverse.

Figura 10 Acquisizione dei dati di Syslog

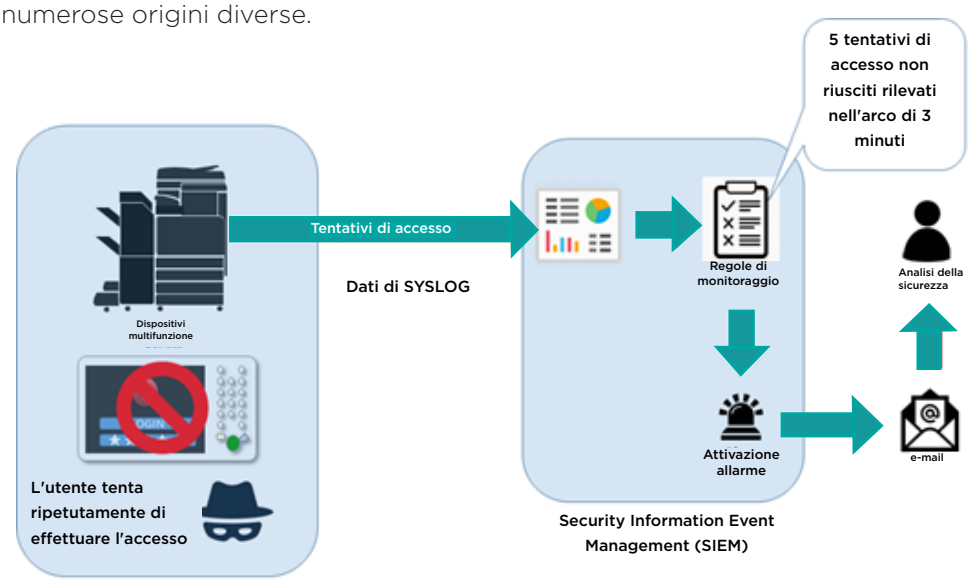


Figura 11 Esempio di utilizzo dei dati di Syslog in imageRUNNER ADVANCE

Per l'elenco delle destinazioni operative SIEM, indirizza il browser Web al link seguente e scarica **"SIEM_spec (imageRUNNER ADVANCE)"**.
https://www.canon-europe.com/support/product-specific-security-measures/

Gestione dei registri dei dispositivi

Oltre alla funzionalità Syslog fornita dalla versione 3.8 della piattaforma software di sistema, imageRUNNER ADVANCE include i registri seguenti, che possono essere gestiti sul dispositivo. Tali registri possono essere esportati in un file in formato CSV tramite l'interfaccia utente remota (RUI, Remote User Interface).

Tabella 3 - Esempi di file di registro gestibili tramite il dispositivo multifunzione.

Tipo di registro	Numero indicato come "Tipo di registro" nel file CSV	Descrizione
Registro	4098	Questo registro contiene informazioni relative allo stato di autenticazione dell'utente (accesso/disconnessione ed esito positivo/negativo dell'autenticazione utente), alla registrazione/modifica/eliminazione delle informazioni sull'utente gestite tramite autenticazione utente e la gestione (aggiunta/modifica/eliminazione) dei ruoli tramite il sistema di gestione dell'accesso
Registro lavori	1001	Questo registro contiene informazioni relative al completamento dei lavori di copia/fax/scansione/invio/stampa
Registro di trasmissione	8193	Questo registro contiene informazioni relative alle trasmissioni
Registro dei salvataggi in Advanced Space	8196	Questo registro contiene informazioni relative al salvataggio dei file in Advanced Space, in rete (Advanced Space di altri sistemi) e su supporti di memoria
Registro delle operazioni nella casella di posta	8197	Questo registro contiene informazioni relative alle operazioni eseguite sui dati della casella di posta, della casella di memoria RX e della casella fax riservata
Registro delle autenticazioni nella casella di posta	8199	Questo registro contiene informazioni relative allo stato di autenticazione della casella di posta, della casella di memoria RX e della casella fax riservata
Registro delle operazioni in Advanced Space	8201	Questo registro contiene informazioni relative alle operazioni sui dati in Advanced Space
Registro di gestione dei sistemi	8198	Questo registro contiene informazioni relative all'avvio/arresto dei sistemi, alle modifiche apportate alle impostazioni tramite (Impostazioni/Registrazione), alle modifiche apportate alle impostazioni tramite la funzione di recapito delle informazioni sui dispositivi e alle impostazioni di data/ora. Nel registro di gestione dei sistemi vengono registrate anche le modifiche apportate alle informazioni dell'utente o alle impostazioni correlate alla sicurezza, quando il sistema viene ispezionato o riparato da un rivenditore Canon autorizzato della zona
Registro di autenticazione della rete	8200	In questo registro vengono memorizzati i messaggi di errore delle comunicazioni IPSec
Registro di Esporta/Importa tutto	8202	Questo registro contiene informazioni relative all'importazione/esportazione delle impostazioni tramite la funzione Esporta/Importa tutto
Registro di backup della casella di posta	8203	Questo registro contiene informazioni relative ai backup dei dati delle caselle di posta degli utenti, della casella di memoria RX e della casella fax riservata, di Advanced Space e su tutti i dati memorizzati, oltre che del modulo registrato per la funzione di sovrapposizione delle immagini
Registro delle operazioni eseguite nelle schermate di gestione di applicazioni e software	3101	È un registro di operazioni per SMS (Service Management Service), registrazioni/aggiornamenti software, programmi di installazione delle applicazioni MEAP e così via
Registro delle politiche di sicurezza	8204	Questo registro contiene informazioni relative allo stato di configurazione delle impostazioni relative alle politiche di sicurezza
Registro di gestione dei gruppi	8205	Questo registro contiene informazioni relative allo stato di configurazione (registrazione/modifica/eliminazione) dei gruppi di utenti
Registro di manutenzione del sistema	8206	Questo registro contiene informazioni relative ad aggiornamenti del firmware, backup/ripristino dell'applicazione MEAP e così via
Registro delle stampa con autenticazione	8207	Questo registro contiene informazioni e la cronologia delle operazioni relative ai lavori di stampa con sospensione forzata
Registro delle impostazioni di sincronizzazione	8208	Questo registro contiene informazioni relative alla sincronizzazione delle impostazioni del sistema. Impostazioni di sincronizzazione per più stampanti multifunzione Canon
Registro per la gestione del registro di audit	3001	Questo registro contiene informazioni relative all'avvio e all'arresto di questa funzione (funzione di gestione del registro di audit), oltre all'esportazione dei registri e così via

Questo registro contiene fino a 40.000 record. Quando sono presenti più di 40.000 record, vengono eliminati per primi i record meno recenti.

SUPPORTO PER DISPOSITIVI REMOTI

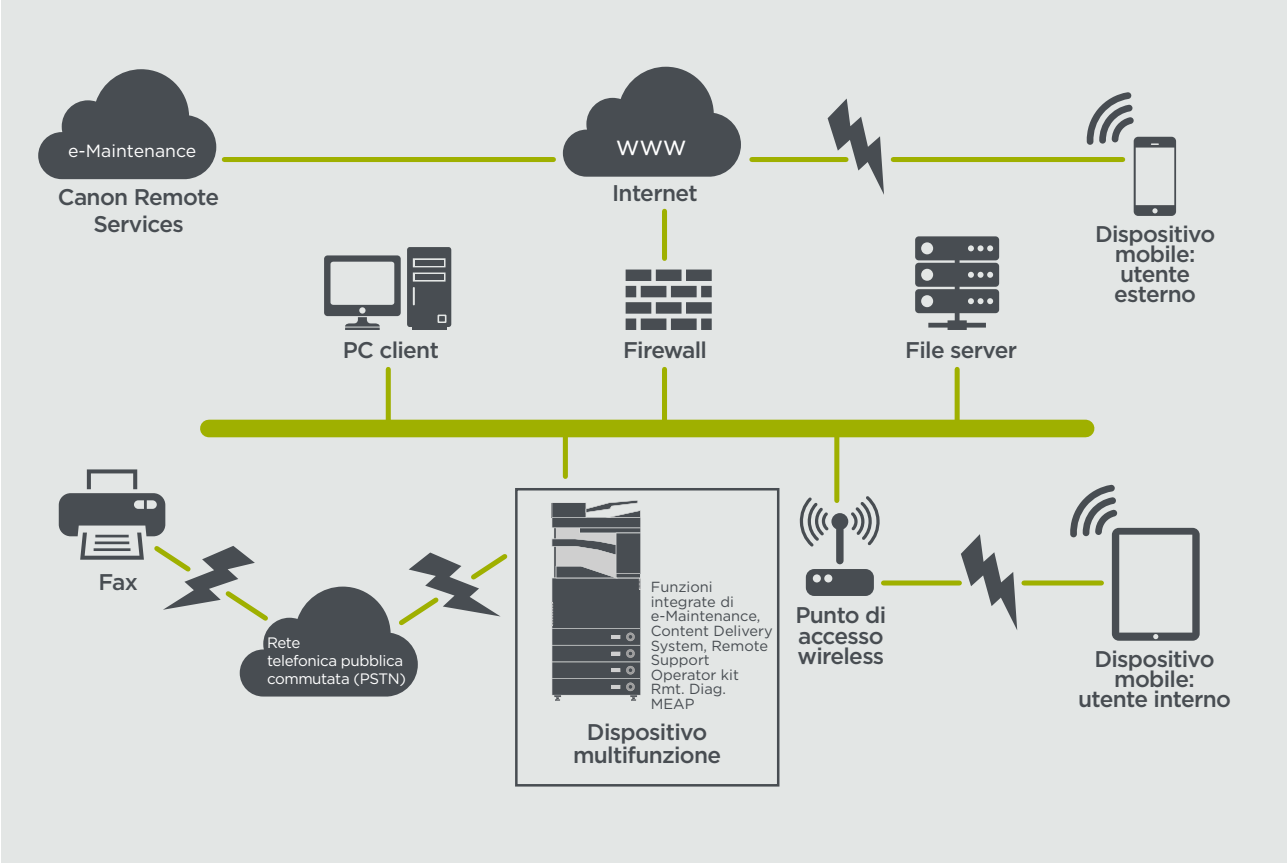
Per consentire a Canon o a un suo partner di fornire un servizio efficiente, imageRUNNER ADVANCE è in grado di trasmettere dati relativi ai servizi e di ricevere aggiornamenti del firmware o del software applicativo. Si noti che non vengono inviate immagini o metadati di immagini.

Di seguito sono mostrate due possibili implementazioni dei servizi remoti Canon in una rete aziendale.

Scenario di implementazione 1: connessioni distribuite

In questa configurazione, ciascun MFD consente la connessione diretta al servizio remoto tramite Internet.

Figura 12 Connessione distribuita



Scenario di implementazione 2: connessione gestita centralizzata

Nello scenario di un ambiente aziendale, in cui sono installati più MFD, bisogna avere la capacità di gestire in modo efficiente questi dispositivi da una posizione centralizzata, ad esempio tramite la connessione ai servizi remoti Canon. Per favorire un approccio orientato alla gestione olistica, i singoli dispositivi devono essere in grado di stabilire le connessioni di gestione tramite un singolo punto di connessione iW Enterprise Management Console (iWEMC). Per la comunicazione tra la funzione di gestione firmware in iWEMC e i dispositivi multifunzione, viene utilizzata la porta UDP 47545.

Figura 13 Connessione gestita centralizzata

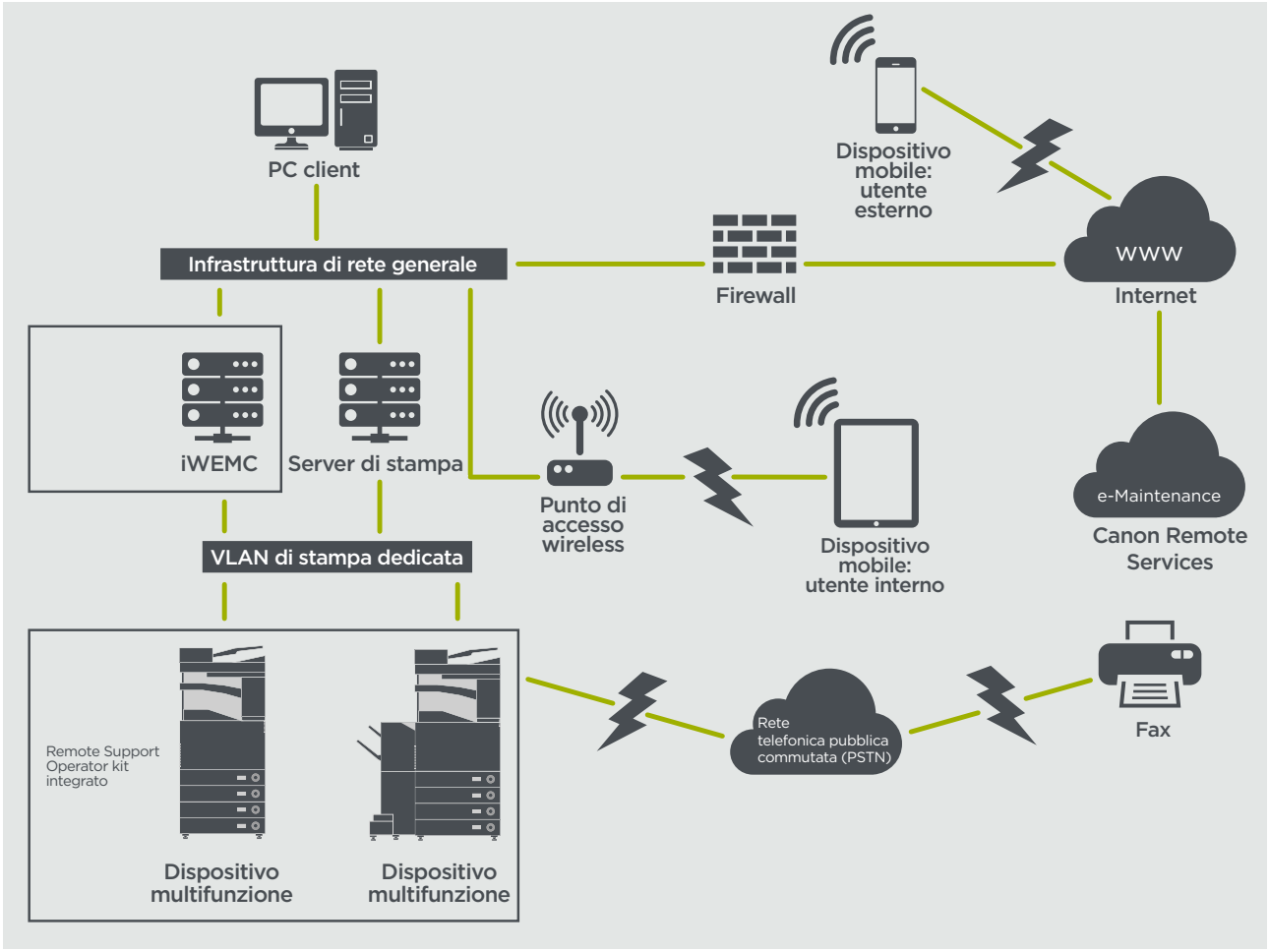
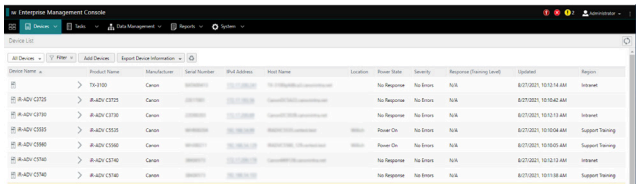


Figura
14a. Elenco dispositivi (in questo caso un singolo dispositivo) come riportato nella iW Enterprise Management Console
14b. Dettagli e impostazioni del dispositivo



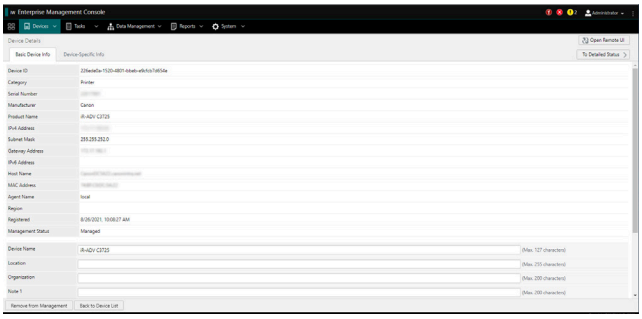


Figura 14a

Figura 14b

e-Maintenance

Il sistema e-Maintenance fornisce un metodo automatizzato per la raccolta dei dati sull'utilizzo dei dispositivi ai fini della fatturazione, della gestione dei materiali di consumo e del monitoraggio dei dispositivi remoti tramite avvisi di stato e di errore.

Il sistema e-Maintenance è costituito da un server con connessione in rete (UGW2) e un software incorporato nel dispositivo multifunzione (eRDS) e/o un software aggiuntivo server-based (CDCA) e/o MEAP (Rmt. Diag. MEAP) per raccogliere informazioni relative all'utilizzo dello specifico dispositivo. L'eRDS è un programma di monitoraggio che viene eseguito all'interno di imageRUNNER ADVANCE. Se l'opzione di monitoraggio è abilitata nelle impostazioni del dispositivo, l'eRDS riceve le informazioni sul dispositivo a cui è associato e le invia al server UGW2. Canon Data Collection Agent (CDCA) è un programma di monitoraggio che viene installato in un PC generico e può monitorare da 1 a 1000 dispositivi. Ottiene le informazioni da ogni dispositivo tramite la rete e le invia al server UGW2. Rmt. Diag. MEAP è un'applicazione MEAP che invia informazioni sul dispositivo al sistema e-Maintenance tramite e-mail o comunicazione HTTPS e può gestire fino a 31 dispositivi.

Come riportato nella Tabella 4 qui sotto, la pagina successiva mostra i dati trasferiti, i protocolli (in base alle opzioni selezionate durante la progettazione e l'implementazione) e le porte utilizzate. In nessuna circostanza vengono trasferiti dati di immagini relativi a copia, stampa, scansione o fax.

Tabella 4 Descrizione dei dati associati alla funzionalità e-Maintenance

Descrizione	Dati gestiti	Protocollo/Porta	Porta
	Indirizzo del servizio web UGW2 Indirizzo del server proxy/numero di porta Account proxy/password Indirizzo di destinazione della posta UGW2 Indirizzo del server SMTP Indirizzo del server POP Stato del dispositivo, contatore e informazioni sul modello Numero di serie Informazioni sul toner/inchiostro rimanente Informazioni sulle richieste di riparazione Informazioni di registrazione Richiesta di assistenza Allarme di servizio Inceppamento Ambiente Registro delle condizioni	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Comunicazione tra eMaintenance (UGW2) e dispositivi (solo CDCA o Rmt. Diag. MEAP, poiché eRDS è un software incorporato)		SNMP Proprietario Canon SLP/SLP/HTTPS	UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Content Delivery System

Il Content Delivery System (CDS) stabilisce una connessione tra MFD e Canon Universal Gateway 2 (UGW2). Fornisce il firmware del dispositivo e aggiornamenti applicativi.

Tabella 5 Descrizione dei dati associati al Content Delivery System

Descrizione	Dati inviati	Protocollo/Porta	Porta
Comunicazione tra MFD e UGW2	Numero di serie del dispositivo Versione del firmware Lingua Paese Informazioni relative al dispositivo EULA	HTTP/HTTPS	TCP/80 TCP/443
Comunicazione tra UGW2 e MFD	File di test (dati binari casuali) per la verifica della comunicazione Dati binari del firmware o dell'applicazione MEAP	HTTP/HTTPS	TCP/80 TCP/443

Uno specifico URL di accesso CDS è preimpostato nella configurazione del dispositivo.
Se è necessario fornire una gestione centralizzata del firmware del dispositivo e delle applicazioni nell'infrastruttura, sarà richiesta un'installazione locale di iWEMC con funzionalità firmware e di gestione delle applicazioni.

Kit dell'operatore addetto all'assistenza remota

Il kit dell'operatore addetto all'assistenza remota (RSOK) fornisce accesso remoto al pannello di controllo del dispositivo. Questo sistema tipo server-client consiste in un server VNC eseguito su MFD e l'applicazione client Remote Operation Viewer VNC Microsoft Windows.

Figura 15 Configurazione kit dell'operatore addetto all'assistenza remota (RSOK)

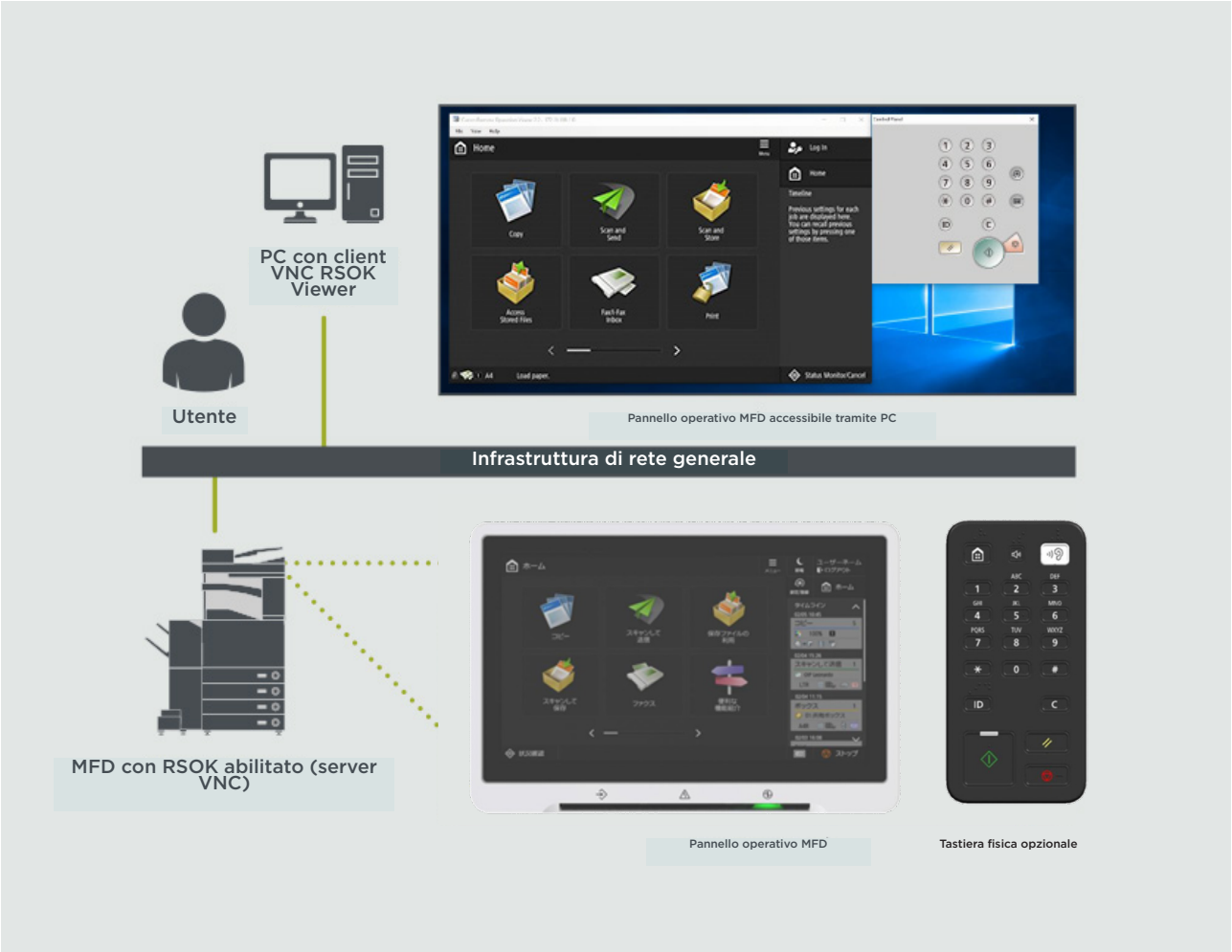


Tabella 6 Descrizione kit dell'operatore addetto all'assistenza remota (RSOK)

Descrizione	Dati inviati	Protocollo/Porta	Porta
Autenticazione con password VNC	Password utente	Crittografia DES	5900
Operation Viewer	Pannello di controllo del dispositivo - dati sullo schermo - funzionamento della chiave hardware	Versione 3.3 protocollo RFB	5900

APPENDICE

Funzionalità relative alla sicurezza di Canon imageRUNNER ADVANCE

La piattaforma imageRUNNER ADVANCE fornisce funzionalità di configurazione remota attraverso un'interfaccia di servizi Web nota come interfaccia utente remota (RUI). Questa interfaccia consente di accedere a molte delle impostazioni di configurazione del dispositivo e può essere disabilitata e protetta da password per prevenire l'accesso non autorizzato.

La maggior parte delle impostazioni del dispositivo è disponibile tramite la RUI, tuttavia è necessario utilizzare il pannello di controllo del dispositivo per impostare elementi che non possono essere configurati utilizzando questa interfaccia. Consigliamo di disattivare tutti i servizi non utilizzati e di rafforzare i controlli su quelli necessari. Per fornire flessibilità e supporto, il kit dell'operatore addetto all'assistenza remota (RSOK) fornisce accesso remoto al pannello di controllo del dispositivo. Il processo si basa sulla tecnologia VNC, che consiste in un server (il dispositivo multifunzione) e un client (un PC della rete). È disponibile uno specifico visualizzatore per PC client Canon, che fornisce un accesso simulato ai pulsanti del pannello di controllo dove necessario.

Questa sezione offre una panoramica delle principali funzionalità relative alla sicurezza di imageRUNNER ADVANCE e delle rispettive impostazioni di configurazione.

I manuali dell'utente interattivi online sono disponibili sul sito https://oip.manual.canon/ e forniscono dettagli che riguardano non solo le funzionalità relative alla sicurezza. Inizia selezionando il tipo di prodotto appropriato (come imageRUNNER ADVANCE DX), fai clic sull'icona di ricerca e inserisci i criteri di ricerca. Di seguito sono riportate alcune aree generali che meritano di essere prese in considerazione.

Gestione della macchina

Per ridurre il rischio di perdita di informazioni personali o uso non autorizzato, sono necessarie misure di sicurezza costanti ed efficaci. Con la designazione di un amministratore per la gestione delle impostazioni del dispositivo, la gestione degli utenti e l'accesso alle configurazioni di sicurezza possono essere limitati alle persone autorizzate.

Indirizza il browser al link seguente e inserisci **configurazione amministratore** nella casella di ricerca. Questo fornirà informazioni relative a:

- Gestione di base del dispositivo
- Limitazione dei rischi per negligenza, errore dell'utente e uso improprio
- Gestione del dispositivo
- Gestione della configurazione e delle impostazioni del sistema

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Standard IEEE P2600

Molti modelli imageRUNNER ADVANCE sono conformi allo standard IEEE P2600, che è uno standard globale in materia di sicurezza delle informazioni per periferiche e stampanti multifunzione.

Il link seguente descrive i requisiti di sicurezza definiti nello standard IEEE 2600 e in che modo le funzioni del dispositivo soddisfano questi requisiti.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

Autenticazione IEEE 802.1X

Quando è necessario connettersi a una rete 802.1X, il dispositivo deve essere autenticato per verificare che si tratti di una connessione autorizzata.

Indirizza il browser al link seguente e inserisci **802.1X** nella casella di ricerca.
https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Applicazione di una politica di sicurezza alla macchina

Gli ultimi modelli imageRUNNER ADVANCE consentono di gestire in batch più impostazioni di sicurezza del dispositivo e la relativa politica di sicurezza, tramite la RUI. È possibile utilizzare una password separata, che consente unicamente all'amministratore della sicurezza di modificare le impostazioni.

Indirizza il browser al link seguente e inserisci **applicazione di una politica di sicurezza alla macchina** nella casella di ricerca. Questo fornirà informazioni relative a:

- Utilizzo di una password per proteggere le impostazioni relative alla politica di sicurezza
- Configurazione delle impostazioni della politica di sicurezza
- Elementi di configurazione della politica di sicurezza

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Gestione degli utenti

I clienti che richiedono un livello più elevato di sicurezza ed efficienza possono utilizzare le funzionalità integrate oppure una soluzione di gestione della stampa come uniFLOW.

Per ulteriori dettagli sulle nostre soluzioni di gestione dei servizi di stampa, contattare i nostri rappresentanti locali o consultare la brochure del prodotto uniFLOW.

Configurazione delle impostazioni di sicurezza della rete

Gli utenti autorizzati possono subire perdite impreviste dovute ad attacchi di malintenzionati, quali sniffing, spoofing e manomissione dei dati mentre transitano su una rete. Per proteggere le informazioni personali importanti e sensibili da questi attacchi, la macchina supporta diverse funzionalità per migliorare sicurezza e privacy.

Indirizza il browser al link seguente e inserisci **configurazione delle impostazioni di sicurezza della rete** nella casella di ricerca. Questo fornirà informazioni relative a:

Il link riportato di seguito descrive:

- Prevenzione degli accessi non autorizzati
- Connessione a una LAN wireless
- Preparazione dell'ambiente di rete

https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Gestione dei dati sul disco rigido/unità a stato solido

L'unità disco rigido del dispositivo viene utilizzata per ospitare il sistema operativo del dispositivo, le impostazioni di configurazione e le informazioni sul lavoro. La maggior parte dei modelli di dispositivo fornisce la crittografia completa del disco (conformemente allo standard FIPS 140-2)

tramite l'associazione al dispositivo specifico, al fine di prevenirne la lettura da parte di utenti non autorizzati. Un chip di sicurezza preliminare Canon MFP è certificato come modulo di crittografia sia nell'ambito del Cryptographic Module Validation Program (CMVP) in vigore negli Stati Uniti e in Canada, sia la certificazione JCMVP (Japan Cryptographic Module Validation Program).

Indirizza il browser al link seguente e inserisci **gestione dei dati sul disco rigido** nella casella di ricerca.
https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

Per informazioni relative alla pulizia dei dati con prodotti che utilizzano la tecnologia SSD, indirizza il browser al link seguente e inserisci **Inizializza tutti i dati** nella casella di ricerca.
https://oip.manual.canon/USRMA-5487-zz-CS-5800-enGB/

DESCRIZIONE DELLE IMPOSTAZIONI DELLA POLITICA DI SICUREZZA

Nella terza generazione dei modelli imageRUNNER ADVANCE sono state introdotte le impostazioni della politica di sicurezza e le funzioni riservate all'amministratore della sicurezza. Ciò richiede l'accesso corretto da parte dell'amministratore e, se configurato, l'accesso di un amministratore della sicurezza aggiuntivo con una password separata.

Nella tabella seguente sono riportate le impostazioni disponibili.

1. Interfaccia	Note
Politica di connessione wireless	
Vieta l'uso della connessione diretta	<Wi-Fi Direct/Usa Wi-Fi Direct> è impostato su <Off> Non è possibile accedere al sistema da dispositivi mobili
Vieta l'uso della LAN wireless	<Select Wired/Wireless LAN/Seleziona LAN cablata/wireless> è impostato su <Wired LAN/LAN cablata> Non è possibile stabilire una connessione wireless con il sistema tramite un router LAN wireless o un punto di accesso
Politica USB	
Vieta l'uso come dispositivo USB	< Use as USB Device/Usa come dispositivo USB> è impostato su <Off> Non è possibile utilizzare le funzioni di stampa o scansione da PC collegati tramite USB quando è vietato l'uso come dispositivo USB
Vieta l'uso come dispositivo di archiviazione USB	<Use USB Storage Device/Usa come dispositivo di archiviazione USB> è impostato su <Off> Non è possibile utilizzare dispositivi di archiviazione USB Tuttavia, le seguenti funzioni di servizio funzionano anche se "Vieta uso come dispositivo di archiviazione USB" è impostato su ON • Aggiornamento del firmware tramite chiavetta USB (dalla modalità download) • Copia dei dati del registro secondario da dispositivo a USB (LOG2USB) • Copia del report da dispositivo a USB (RPT2USB)
Politica operativa della comunicazione di rete Nota: queste impostazioni non si applicano alla comunicazione con le reti IEEE 802.1X, anche se è stata selezionata la casella corrispondente a [Verificare sempre il certificato del server quando si utilizza TLS]	
Verifica sempre le firme per le funzioni SMS/server WebDAV	In <USB Storage Device/Impostazioni server SMB>, le opzioni <Require SMB Signature for Connection/Richiedi firma SMB per connessione> e <Use SMB Authentication/Usa autenticazione SMB> sono impostate su <On> e <Use TLS/Usa TLS> in <WebDAV Server Settings/Impostazioni server WebDAV> è impostato su <On> Quando la macchina viene utilizzata come server SMB o server WebDAV, le firme digitali dei certificati vengono verificate durante la comunicazione
Verifica sempre il certificato del server quando si utilizza TLS	<Confirm TLS Certificate for WebDAV TX/Conferma certificato TLS per WebDAV TX>, <Confirm TLS Certificate for SMTP TX/Conferma certificato TLS per SMTP TX>, < Confirm TLS Certificate for POP RX/Conferma certificato TLS per POP RX>, <Confirm TLS Certificate for Network Access/Conferma certificato TLS per accesso alla rete> e <Confirm TLS Certificate Using MEAP Application/Conferma certificato TLS con applicazione MEAP> sono tutti impostati su < On> e un segno di spunta viene aggiunto a <CN> Inoltre, le opzioni <Verify Server Certificate/Verifica certificato server> e <SIP Settings/Verifica CN> in <SIP Settings/Impostazioni SIP> <TLS Settings/Impostazioni TLS> sono impostate su <On> Durante la comunicazione TLS, viene eseguita la verifica per i certificati digitali e i relativi nomi comuni
Vieta l'autenticazione con testo in chiaro per le funzioni server	• <Use FTP Printing/Usa stampa FTP> in <FTP Print Settings/Impostazioni stampa FTP> è impostato su <Off> • <Allow TLS (SMTP RX)/Consenti TLS (SMTP RX)> in <E-Mail/I-Fax Settings/Impostazioni e-mail/I-Fax> <Communication Settings/Impostazioni comunicazione> è impostato su <Always TLS/Sempre TLS>, <Dedicated Port Authentication Method/Metodo di autenticazione porta dedicata> in <Network/Rete> è impostato su <Mode 2/Modalità 2>, • < Use TLS/Usa TLS> in <WebDAV Server Settings/Impostazioni server WebDAV> è impostato su <On> Quando si utilizza la macchina come server, le funzioni che utilizzano l'autenticazione con testo semplice non sono disponibili TLS verrà utilizzato se l'autenticazione con testo in chiaro è proibita. Inoltre, non è possibile utilizzare applicazioni o funzioni server, come FTP, che supportano solo l'autenticazione con testo in chiaro Potrebbe non essere possibile accedere al sistema dal software o driver di gestione del dispositivo
Vieta l'uso di SNMPv1	In <SNMP Settings/Impostazioni SNMP>, <Use SNMPv1/Usa SNMPv1> è impostato su <Off> Potrebbe non essere possibile recuperare o impostare le informazioni sul dispositivo dal driver di stampa o dal software di gestione se l'uso di SNMPv1 è vietato
Politica di utilizzo della porta	
Limita porta LPD	Numero di porta: 515 <LPD Print Settings/Impostazioni stampa LPD> è impostato su <Off> Non è possibile eseguire la stampa LPD
Limita porta RAW	Numero di porta: 9100 <RAW Print Settings/Impostazioni stampa RAW> è impostato su <Off> Non è possibile eseguire la stampa RAW
Limita porta FTP	Numero di porta: 21 In <IFTP Print Settings/Impostazioni stampa FTP>, <FTP Print Settings/Impostazioni stampa FTP> è impostato su <Off> Non è possibile eseguire la stampa FTP
Limita porta WSD	Numero di porta: 3702, 60000 In <Use FTP Printing/Usa stampa FTP>, le opzioni <Use WSD/Usa WSD>, <Use WSD Browsing/Usa navigazione WSD> e <Use WSD Scan/Usa scansione WSD> sono tutte impostate su <Off> Non è possibile utilizzare le funzioni WSD
Limita porta BMLinkS	Numero di porta: 1900 Non usato nella regione europea

Limita porta IPP	Numero di porta: 631 Non sarà possibile utilizzare Mopria, AirPrint e IPP se l'uso della porta IPP è soggetto a restrizioni
Limita porta SMB	Numero di porta: 137, 138, 139, 445 In < SMB Server Settings/Impostazioni server SMB>, <Use SMB Server/Usa server SMB> è impostato su <Off> Non è possibile utilizzare la macchina come server SMB
Limita porta SMTP	Numero di porta: 25 In <E-Mail/I-Fax Settings/Impostazioni e-mail/I-Fax> <ICommunication Settings/Impostazioni comunicazione>, <SMTP RX> è impostato su <Off> La ricezione SMTP non è possibile
Limita porta dedicata	Numero di porta: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547 Non è possibile utilizzare le funzioni o applicazioni di copia remota, invio fax in remoto, scansione remota o stampa remota se la porta dedicata è soggetta a restrizioni
Limita porta software dell'operatore remoto	Numero di porta: 5900 <Remote Operation Settings/Impostazioni operazioni in remoto> è impostato su <Off> Non è possibile utilizzare le funzioni operazioni in remoto
Limita porta SIP (IP Fax)	Numero di porta: 5004, 5005, 5060, 5061, 49152 <Use Intranet/Usa Intranet> in < Intranet Settings/Impostazioni Intranet>, <Use NGN/Usa NGN> in <NGN Settings/Impostazioni NGN> e <Use VoIP Gateway/Usa gateway VoIP> in <VoIP Gateway Settings/Impostazioni gateway VoIP> sono tutti impostati su <Off> Non è possibile utilizzare la funzione fax IP
Limita porta mDNS	Numero di porta: 5353 In <mDNS Settings/Impostazioni mDNS>, le opzioni <Use IPv4 mDNS/Usa IPv4 mDNS> e <Use IPv6 mDNS/Usa IPv6 mDNS> sono impostate su <Off> <Use Mopria/Usa Mopria> è impostato su <Off> Non è possibile cercare nella rete o eseguire impostazioni automatiche tramite mDNS, e nemmeno stampare tramite Mopria™ o AirPrint
Limita porta SLP	Numero di porta: 427 In <Multicast Discovery Settings/Impostazioni multicast discovery>, <Response/Risposta> è impostato su <Off> Non è possibile cercare nella rete o eseguire impostazioni automatiche usando SLP
Limita porta SNMP	Numero di porta: 161 Potrebbe non essere possibile recuperare o impostare le informazioni sul dispositivo dal driver di stampa o dal software di gestione se l'uso della porta SNMP è soggetto a restrizioni. In <SNMP Settings/Impostazioni SNMP>, le opzioni <Use SNMPv1/Usa SNMPv1> e <SNMPv3/Usa SNMPv3> sono impostate su <Off>

2. Autenticazione	Note
Politica operativa di autenticazione	
Vieta utenti ospiti	• <Advanced Space Settings/Impostazioni spazio avanzato> <Authentication Management/Gestione autenticazione> è impostato su <On> • <Login Screen Display Settings/Impostazioni visualizzazione schermata di accesso> è impostato su <Display When Device Operation Starts/Visualizza quando il dispositivo viene avviato> • <Restrict Job from Remote Device without User Auth/Limita il lavoro da dispositivo remoto senza autorizzazione utente> è impostato su <On> Gli utenti non registrati non possono accedere al sistema I lavori di stampa inviati da un computer vengono annullati
Forza l'impostazione della disconnessione automatica	Questa impostazione consente di disconnettersi dal pannello di controllo Non si applica agli altri metodi di disconnessione (valori consentiti: da 10 secondi a 9 minuti) <Auto Reset Time/Tempo di reimpostazione automatica> è abilitato L'utente viene disconnesso automaticamente se non viene eseguita alcuna operazione per un periodo di tempo specificato Selezionare [Tempo fino alla disconnessione] nella schermata di configurazione dell'interfaccia utente remota
Politica operativa sulle password	
Vieta memorizzazione nella cache della password di autenticazione	Questa impostazione non si applica alle password che l'utente salva esplicitamente, come le password per le rubriche e così via <Prohibit Caching of Authentication Password/Vieta memorizzazione nella cache della password di autenticazione> è impostato su <On> Gli utenti dovranno inserire una password ogni volta che accedono a un server esterno
Visualizza avviso quando la password predefinita è in uso	< Display Warning When Default Password Is in Use/Visualizza avviso quando la password predefinita è in uso> è impostato su <On> Verrà visualizzato un messaggio di avviso ogni volta che viene utilizzata la password predefinita di fabbrica della macchina
Vieta l'uso della password predefinita per l'accesso remoto	<Allow Use of Default Password for Remote Access/Consenti l'uso della password predefinita per l'accesso remoto> è impostato su <Off> Non è possibile utilizzare la password predefinita di fabbrica quando si accede alla macchina da un computer
Politica in materia di impostazioni della password (la politica non si applica alla gestione degli ID dipartimentali o PIN)	
Imposta il numero minimo di caratteri per la password	Numero minimo di caratteri impostabili tra 1 e 32
Imposta il periodo di validità della password	Periodo di validità impostabile tra 1 e 180 giorni
Vieta l'uso di 3 o più caratteri consecutivi identici	
Forza l'uso di almeno 1 carattere maiuscolo	
Forza l'uso di almeno 1 carattere minuscolo	
Forza l'uso di almeno 1 cifra	
Forza l'uso di almeno 1 simbolo	
Politica di blocco	
Abilita il blocco	Non si applica a ID reparto/PIN casella di posta, autenticazione PIN o stampa protetta e così via Soglia di blocco: è possibile impostare da 1 a 10 volte Periodo di blocco: è possibile impostare da 1 a 60 minuti

3. Chiave/certificato	Note
Vieta l'uso della crittografia debole	Si applica a IPSec, TLS, Kerberos, S/MIME, SNMPv3 e LAN wireless Potrebbe non essere possibile comunicare con dispositivi che supportano solo la crittografia debole
Vieta l'uso di chiavi/certificati con crittografia debole	Si applica a IPSec, TLS e S/MIME Se si utilizza una chiave/certificato con crittografia debole per TLS, verrà modificato nella chiave/nel certificato preinstallato. Non sarà possibile stabilire una comunicazione se si utilizza una chiave o un certificato con crittografia debole per funzioni diverse da TLS
Usa TPM per memorizzare password e chiave	Disponibile solo per dispositivi con TPM installato. Esegui sempre backup delle chiavi TPM se TPM è abilitato Per informazioni dettagliate, consultare il manuale dell'utente Importante quando le impostazioni TPM sono abilitate: • Accertarsi di modificare la password "Amministratore" rispetto al valore predefinito, per impedire a una terza parte diversa dall'amministratore di eseguire il backup della chiave TPM. Se una terza parte acquisisce la chiave di backup TPM, non sarà possibile ripristinare la chiave TPM • Per ragioni di sicurezza, la chiave TPM può essere sottoposta a backup una sola volta. Se le impostazioni TPM sono abilitate, accertarsi di eseguire il backup della chiave TPM su un dispositivo di memoria USB, e conservarlo in un luogo sicuro per evitare lo smarrimento o furti • Le funzioni di sicurezza fornite da TPM non garantiscono una protezione completa dei dati e dell'hardware

4. Registro	Note
Forza la registrazione del registro di controllo	• <Save Operation Log/Salva registro operazioni> è impostato su <On> • <Display Job Log/Visualizza registro lavori> è impostato su <On> • <Retrieve Job Log with Management Software/Recupera registro lavori con software di gestione> in <Display Job Log/Visualizza registro lavori> è impostato su <Allow/Consenti> • <Save Audit Log/Salva registro di controllo> è impostato su <On> • <Retrieve Network Authentication Log/Recupera registro autenticazioni in rete> è impostato su <On> I registri di controllo vengono sempre compilati quando questa impostazione è abilitata
Forza impostazioni SNTP	Inserisci l'indirizzo del server SNTP In <SNTP Settings/Impostazioni SNTP>, <Use SNTP/Usa SNTP> è impostato su <On> È necessaria la sincronizzazione a tempo tramite SNTP Immettere un valore per [Nome server] nella schermata di impostazione dell'interfaccia utente remota
Analisi dei registri Syslog	Abilitare i dettagli di destinazione Syslog quando si utilizza un server Syslog o SIEM • <Username and password/Nome utente e password> • <SMB server name/Nome server SMB> • <Destination pathPercorso di destinazione> • <Perform export time/Tempo di esportazione>

5. Lavoro	Note
Politica di stampa	
Vieta la stampa immediata dei lavori ricevuti	I lavori ricevuti verranno archiviati nella memoria fax/I-Fax se è vietata la stampa immediata dei lavori ricevuti • <Handle Files with Forwarding Errors/Gestisci i file con errori di inoltro> è impostato su <Off> • <Use Fax Memory Lock/Usa blocco memoria fax> è impostato su <On> • <Use I-Fax Memory Lock/Usa blocco memoria I-Fax> è impostato su <On> • <Memory Lock End Time/Tempo di blocco memoria> è impostato su <Off> • <Display Print When Storing from Printer Driver/Visualizza stampa durante l'archiviazione dal driver di stampa> in <Set/Register Confidential Fax Inboxes/Imposta/registra fax in arrivo riservati> è impostato su <Off> • <Settings for All Mail Boxes/Impostazioni per tutte le caselle di posta> <Print When Storing from Printer Driver/Stampa durante l'archiviazione dal driver di stampa> è impostato su <Off> • <Box Security Settings/Impostazioni sicurezza casella> <Display Print When Storing from Printer Driver/Visualizza stampa durante l'archiviazione dal driver di stampa> è impostato su <Off> • <Prohibit Job from Unknown User/Vieta lavoro da utente sconosciuto> è impostato su <On> e <Forced Hold/Sospensione forzata> è impostato su <On> La stampa non viene eseguita immediatamente, anche quando vengono eseguite operazioni di stampa
Politica di Invio/Ricezione	
Consenti l'invio solo agli indirizzi registrati	In <Limit New Destination/Limita nuova destinazione>, le opzioni <Fax>, <E-Mail>, <I-Fax> e <File> sono impostate su <On> È possibile inviare solo alle destinazioni registrate nella Rubrica
Forza la conferma del numero di fax	Gli utenti devono inserire nuovamente un numero di fax per la conferma quando inviano un fax
Vieta l'inoltro automatico	<Use Forwarding Settings/Utilizza impostazioni di inoltro> è impostato su <Off> Non è possibile inoltrare automaticamente i fax

6. Archiviazione	Note
Forza la cancellazione completa dei dati	<Hard Disk Data Complete Deletion/Eliminazione completa dei dati dal disco rigido> è impostato su <On>

Per le specifiche complete di imageRUNNER ADVANCE, consultare il sito web del prodotto all'indirizzo https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Italian edition v2.0