GUIDA SULLA CONFIGURAZIONE SICURA

imageRUNNER ADVANCE

Canon

INTRODUZIONE

I moderni dispositivi multifunzione di Canon (MFP) offrono funzionalità di stampa, copia, scansione, invio e fax. Gli 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 fornire 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. Una volta definita, la configurazione finale può essere applicata a un singolo dispositivo o all'intero parco macchine. 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 MFP basata sulle migliori pratiche di settore. Queste impostazioni sono state testate e convalidate 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 e le serie della gamma imageRUNNER ADVANCE, alcune caratteristiche potrebbero differire da un modello all'altro.

Implementazione delle impostazioni di sicurezza MFP 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:

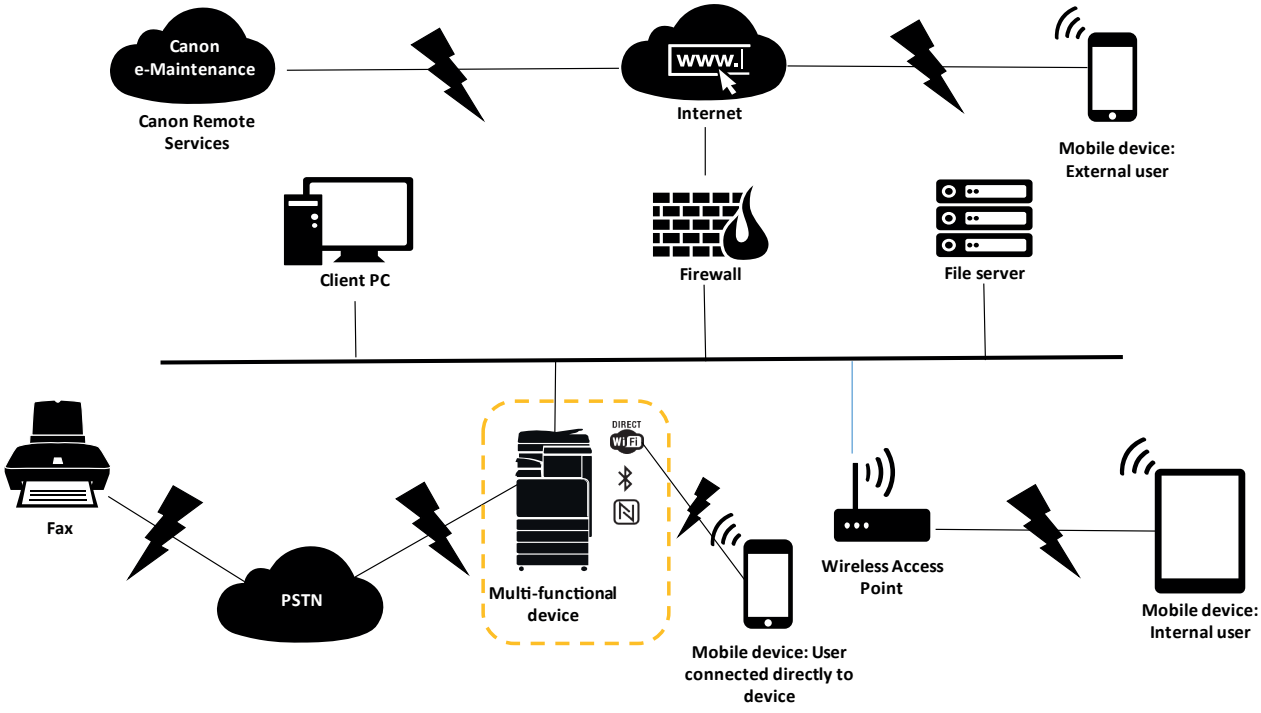
- **L'ambiente tipico di un piccolo ufficio**
- **L'ambiente di ufficio aziendale**

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 quegli utenti che richiedono servizi di stampa al di fuori di un ambiente LAN, è richiesta una connessione sicura, ma questo aspetto non sarà trattato nella presente guida. Tuttavia, occorre prestare attenzione alla sicurezza dei dati in transito tra 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 WiFi. Il dispositivo può anche essere utilizzato per stabilire una connessione WiFi Direct point-to-point con un dispositivo mobile senza che sia richiesta alcuna connessione di rete.

Le opzioni Bluetooth e NFC sono disponibili per diversi modelli di dispositivo e vengono 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 azienda o ambiente di rete.

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

Funzionalità imageRUNNER ADVANCE	Descrizione	Nota
Modalità servizio	Consente l'accesso alle impostazioni della modalità servizio	Proteggere con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
Sistema di gestione modalità servizio	Consente l'accesso a diverse impostazioni non standard del dispositivo	Proteggere con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
Sfoglia/Invia SMB	Consente di archiviare e recuperare informazioni da e verso le condivisioni di rete Windows/SMB	Gli amministratori di sistema, di norma, 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 remota	Strumento di configurazione web-based	L'amministratore imageRUNNER ADVANCE deve abilitare il protocollo HTTPS per l'IU remota e disabilitare l'accesso HTTP. Abilita l'uso dell'autenticazione PIN univoca per ciascun dispositivo
SNMP	Integrazione del monitoraggio di rete	Disabilitare la versione 1 e abilitare solo la versione 3
Invia a e-mail e/o IFAX	Invia email dal dispositivo con allegati	Abilita 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	Abilita 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	Abilita SSL Non utilizzare le credenziali di dominio per l'autenticazione con il server LDAP, bensì utilizzare le credenziali specifiche LDAP
Stampa FTP	Carica e scarica documenti da e verso il server FTP incorporato	Attiva l'autenticazione FTP. Tenere presente che il traffico FTP viaggerà sempre in chiaro sulla rete
Invia WebDAV	Scansiona e archivia i documenti su una località remota	Abilita l'autenticazione per le condivisioni WebDAV
PDF crittografato	Protegge i documenti con crittografia	Di norma, i documenti sensibili dovrebbero essere crittografati utilizzando PDF versione 1.6 (AES-128)
Stampa sicura	Il lavoro di stampa viene inviato al dispositivo ma bloccato in coda di stampa fino all'immissione del numero PIN corrispondente	Abilita lavori di stampa protetti da PIN
Browser web incorporato (disponibile dai modelli Generation 3, seconda edizione)	Accesso del browser a Internet	Applica tramite le funzionalità di amministrazione, 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 e NFC (disponibili dai modelli Generation 3)	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

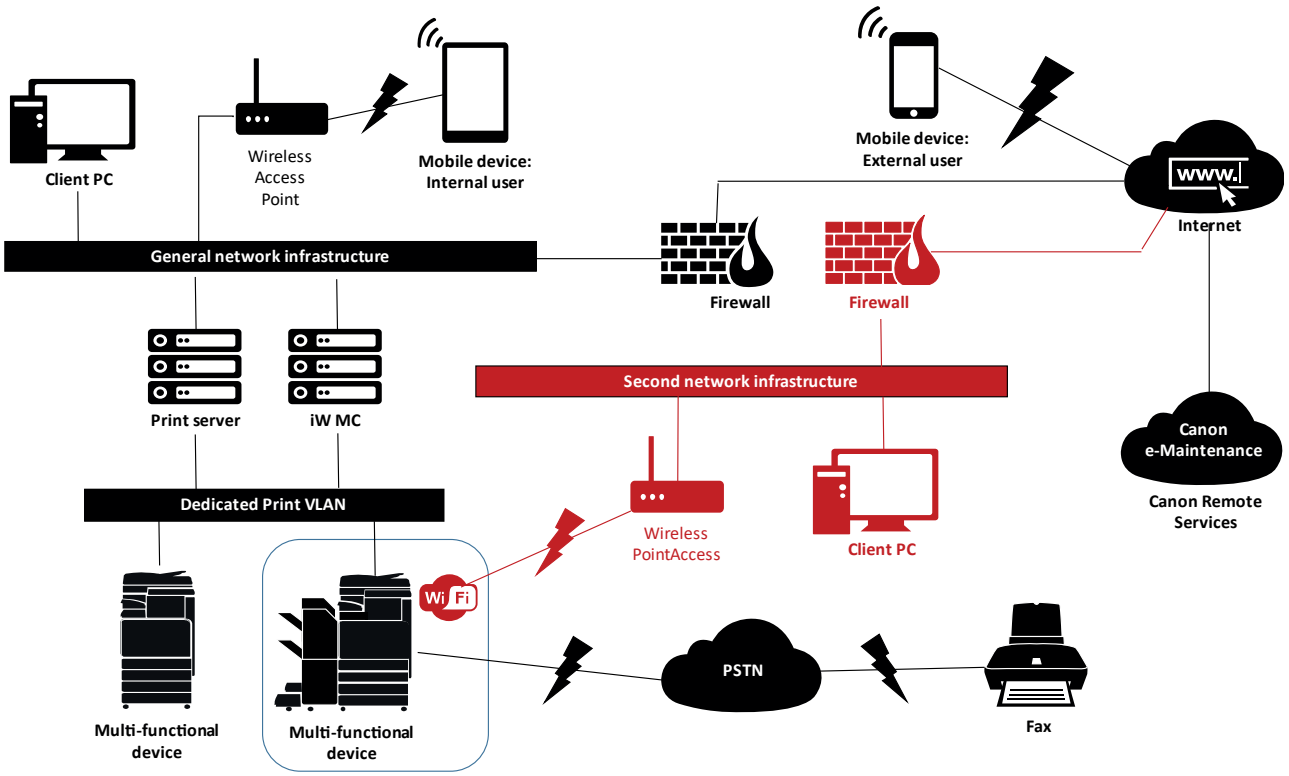
L'AMBIENTE DI UFFICIO AZIENDALE

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

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

Figura 2 Operazioni in un ufficio aziendale



Le connessioni evidenziate in rosso saranno disponibili dai modelli Generation 3, seconda edizione

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	Nota
Modalità servizio	Consente l'accesso alle impostazioni della modalità servizio	Proteggere con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
Sistema di gestione modalità servizio	Consente l'accesso a diverse impostazioni non standard del dispositivo	Proteggere con password utilizzando una password non predefinita, non banale e che sfrutti il numero massimo di caratteri disponibili
Sfoglia/Invia SMB	Consente di archiviare e recuperare informazioni da e verso le condivisioni di rete Windows/SMB	Gli amministratori di sistema, di norma, 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 remota	Strumento di configurazione web-based	Le seguenti configurazioni iniziali del dispositivo disabilitano completamente l'IU remota disattivando i protocolli HTTP e HTTPS
SNMP	Integrazione del monitoraggio di rete	Disabilitare la versione 1 e abilitare solo la versione 3
Invia a e-mail e/o IFAX	Invia email dal dispositivo con allegati	Abilita 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	Abilita 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	Abilita 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
Invia WebDAV	Scansiona e archivia i documenti su una località 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 unicamente utilizzando 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
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 Generation 3, seconda edizione)	Accesso del browser a Internet	Applica le restrizioni appropriate o disabilita la possibilità di scaricare file acquisiti tramite il 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 personale e studenti.

SUPPORTO PER DISPOSITIVI REMOTI

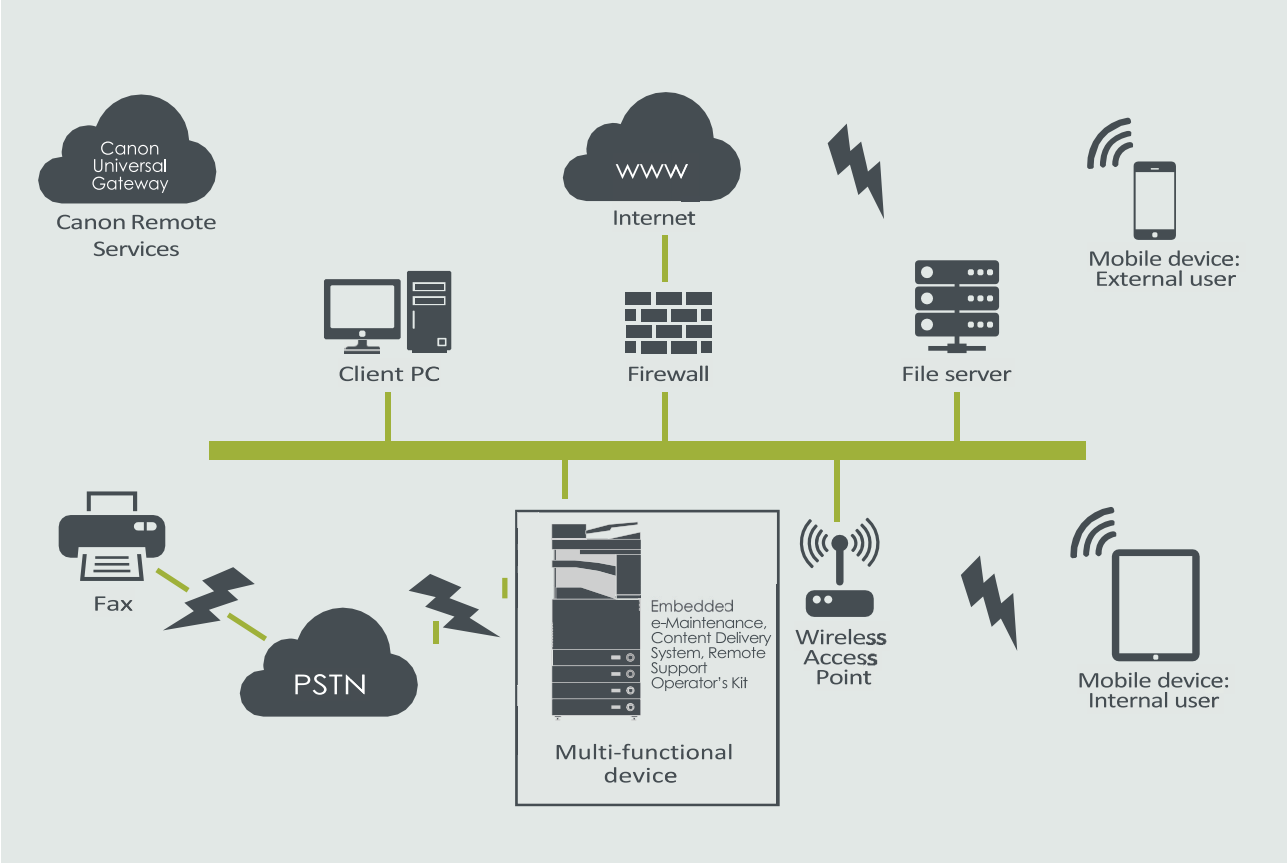
Per consentire a Canon o un partner Canon di fornire un servizio efficiente, imageRUNNER ADVANCE è in grado di trasmettere dati relativi ai servizi e di ricevere aggiornamenti del firmware o software applicativi. Si noti non vengono inviate immagini o metadati immagine.

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

Scenario di implementazione 1: Connessione dispersa

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

Figura 3 Connessione dispersa



Scenario di implementazione 2: Connessione gestita centralizzata

Nello scenario di un ambiente aziendale, in cui sono installati più MFP, bisogna avere la capacità di gestire in modo efficiente questi dispositivi da un punto centralizzato, per esempio tramite la connessione ai servizi remoti di 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 Management Console (iWMC). Per la comunicazione tra il plug-in Device Firmware Upgrade (DFU) e i dispositivi multifunzione, viene utilizzata la porta UDP 47545.

Figura 4 Connessione gestita centralizzata

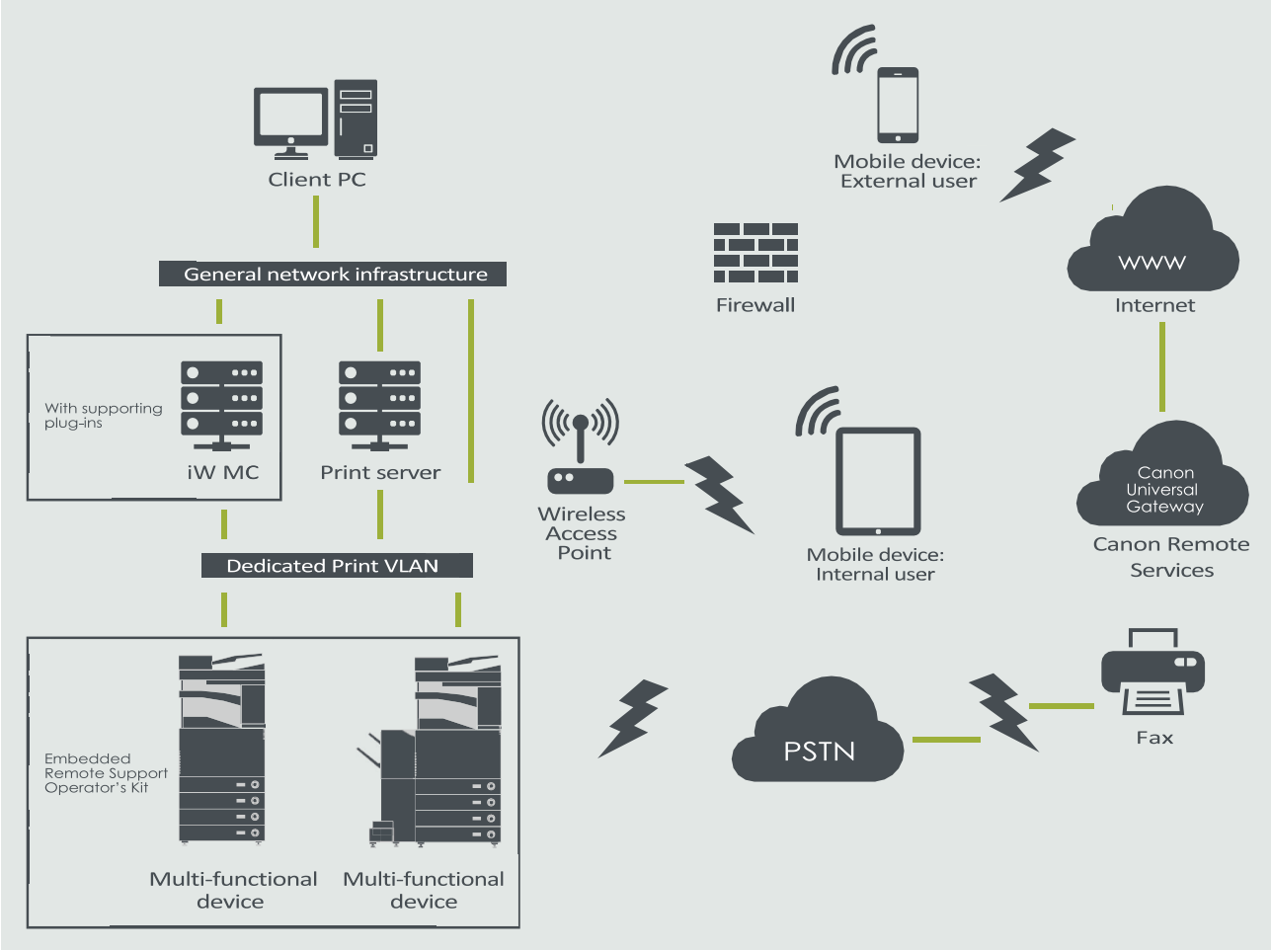
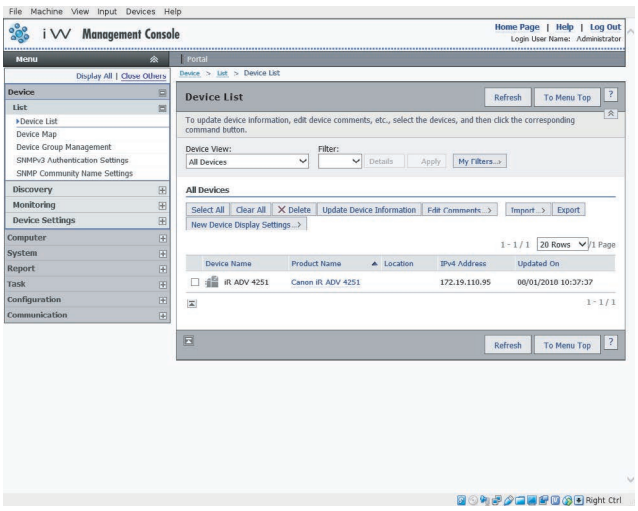
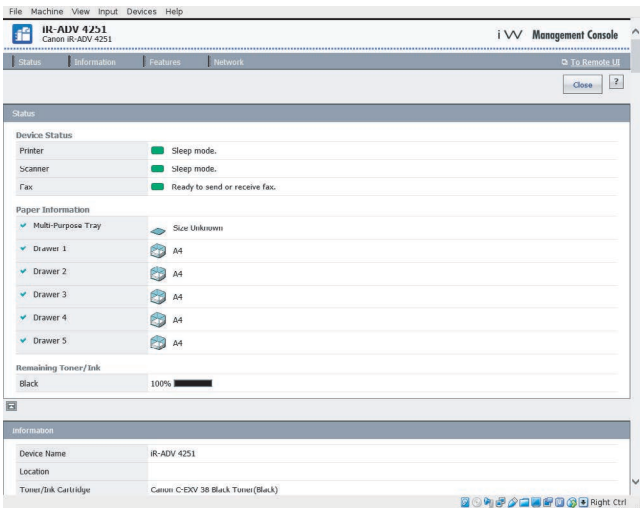


Figura
5a. Elenco dispositivi (in questo caso un singolo dispositivo) come riportato sulla Management Console imageWARE
5b. Dettagli e impostazioni del dispositivo





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 consumabili e del monitoraggio dei dispositivi remoti tramite avvisi di stato e di errore.

Il sistema e-Maintenance consiste in un server con connessione in rete (UGW) e un software incorporato nel dispositivo multifunzione (eRDS) e/o un software aggiuntivo server-based (plug-in RDS) 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 cui è associato e le invia al server UGW. Il plug-in RDS è un programma di monitoraggio che viene installato in un PC generico e può monitorare da 1 a 3.000 dispositivi. Ottiene le informazioni da ogni dispositivo tramite rete e le invia invia al server UGW.

La tabella riportata alla 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 immagine relativi a copia, stampa, scansione o fax.

Tabella 3 Descrizione dei dati associati alla funzionalità e-Maintenance

Descrizione	Dati gestiti	Protocollo/porta	Porta
Comunicazione tra eMaintenance (plug-in eRDS o RDS) e UGW	Indirizzo del servizio web UGW Indirizzo del server proxy/numero di porta Account proxy/password Indirizzo di destinazione mail UGW 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 sulla richiesta di riparazione Informazioni sulla registrazione Chiamata di servizio Allarme di servizio Inceppamento Ambiente Registro delle condizioni	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Comunicazione tra eMaintenance e il dispositivo (solo plug-in RDS, poiché eRDS è un software incorporato)		SNMP Proprietà di 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 MFP e Canon Universal Gateway (UGW). Fornisce il firmware del dispositivo e aggiornamenti applicativi.

Tabella 4 Descrizione dei dati associati al Content Delivery System

Descrizione	Dati inviati	Protocollo/porta	Porta
Comunicazione tra MFP e UGW	Numero di serie del dispositivo Versione firmware Lingua Paese Informazioni relative al dispositivo EULA	HTTP/HTTPS	TCP/80 TCP/443
Comunicazione tra UGW e MFP	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 iWMC con il pug-in Device Firmware Upgrade (DFU) e il plug-in Device Application Management.

Remote Operator Software Kit

Il Remote Operator Software Kit (RSOK) fornisce accesso remoto al pannello di controllo del dispositivo. Questo sistema tipo server-client consiste in un server VNC eseguito su MFP e l'applicazione client Remote Operation Viewer VNC Microsoft Windows.

Figura 6 Configurazione Remote Operator Software Kit (RSOK)

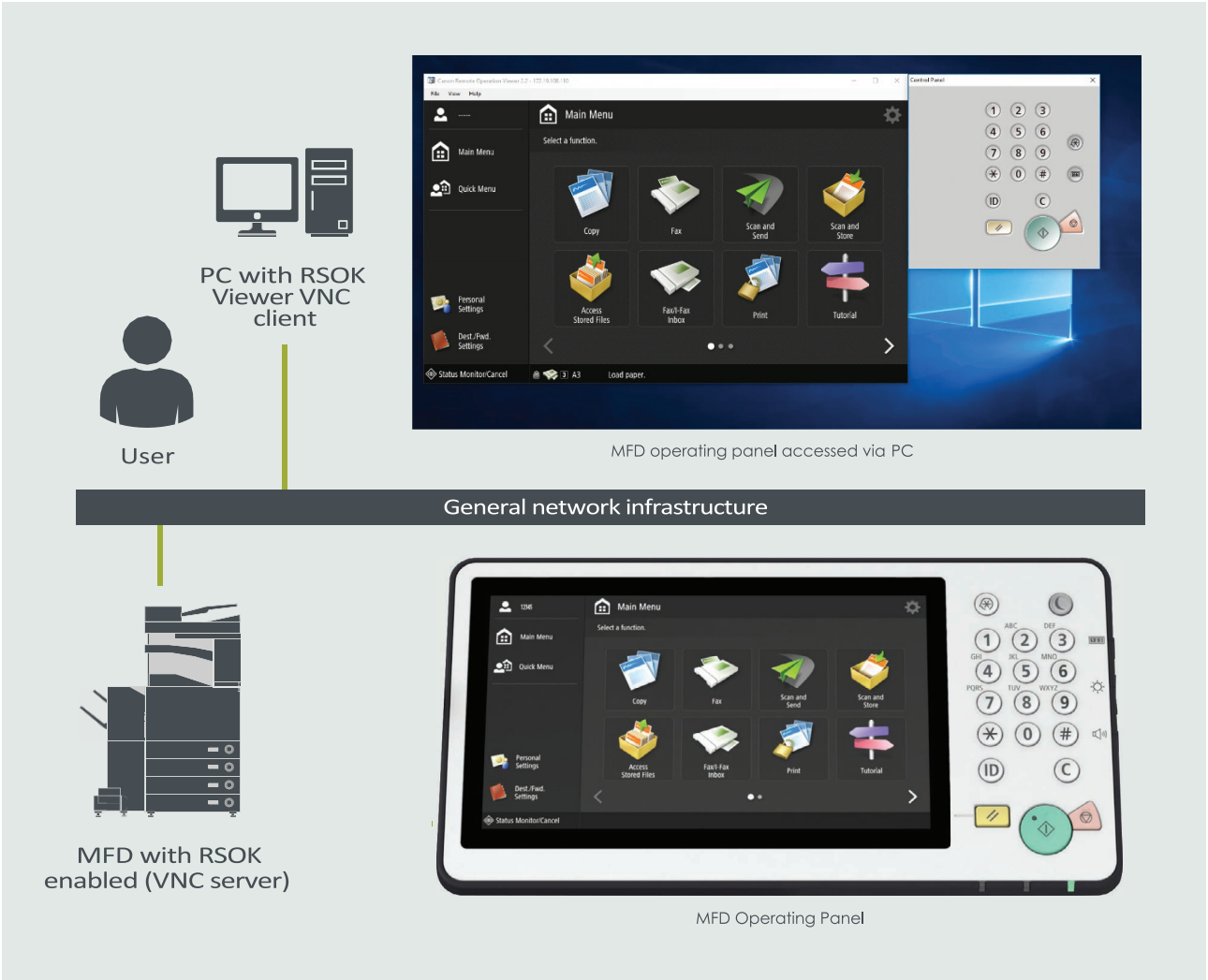


Tabella 5 Descrizione Remote Operator Software Kit (RSOK)

Descrizione	Dati inviati	Protocollo	Porta
Autenticazione con password VNC	Password utente	DES crittografia	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. Pertanto si consiglia di disabilitare tutti i servizi non utilizzati. Per fornire flessibilità e supporto, il Remote Operator Software Kit (RSOK) fornisce accesso remoto al pannello di controllo del dispositivo. Il processo si basa sulla tecnologia VNC, che consiste in un server (il dispositivo) e un client (un PC della rete). È disponibile uno specifico visualizzatore per PC client Canon, che fornisce accesso simulato ai pulsanti del pannello di controllo.

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

Gestione della macchina

Per ridurre il rischio di perdita di informazioni personali o l'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.

I link qui di seguito descrivono:

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

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0001.html
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0037.html

Standard IEEE P2600

Diversi 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.

Il link qui di seguito descrivono i metodi di autenticazione disponibili e le impostazioni di configurazione.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0036.html#296_h1_01

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 l'IU remota. È possibile utilizzare una password separata, che consente unicamente all'amministratore della sicurezza di modificare le impostazioni.

I link qui di seguito descrivono:

- 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

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0002.html

Gestione degli utenti

I clienti che richiedono un livello più elevato di sicurezza ed efficienza possono utilizzare le funzionalità integrate o utilizzare 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 derivanti da 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 le seguenti funzionalità per migliorare sicurezza e segretezza.

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0028.html

Gestione dei dati sul disco rigido

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 a FIPS 140-2) tramite l'associazione al dispositivo specifico per prevenirne la lettura da parte di utenti non autorizzati. Un chip di sicurezza Canon MFP preparatorio è certificato come modulo crittografico ai sensi del Cryptographic Module Validation Program (CMVP), istituito da Stati Uniti e Canada, e del Japan Cryptographic Module Validation Program (JCMVP).

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0092.html

DESCRIZIONE DELLE IMPOSTAZIONI DELLA POLITICA DI SICUREZZA

Le tre generazioni di modelli imageRUNNER ADVANCE introducono le impostazioni della politica di sicurezza e le funzioni riservate all'amministratore della sicurezza. Ciò richiede il corretto accesso dell'amministratore e, se configurato, l'accesso di un amministratore della sicurezza aggiuntivo con una password separata.

La tabella seguente riporta le impostazioni disponibili.

1. Interfaccia	Note
Politica di connessione wireless	
Vieta l'uso della connessione diretta	<Usa Wi-Fi Direct> è impostato su <Off>. Non è possibile accedere alla macchina da dispositivi mobili.
Vieta l'uso della LAN wireless	<Seleziona LAN cablata/wireless> è impostato su <LAN cablata>. Non è possibile stabilire una connessione wireless con la macchina tramite un router LAN wireless o un punto di accesso.
Politica USB	
Vieta l'uso come dispositivo USB	<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	<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 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].	
Verificare sempre le firme per le funzioni SMS/server WebDAV	In <Impostazioni server SMB>, le opzioni <Richiedi firma SMB per connessione> e <Usa autenticazione SMB> sono impostate su <On> e <Usa TLS> in <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	<Conferma certificato TLS per WebDAV TX>, <Conferma certificato TLS per SMTP TX>, <Conferma certificato TLS per POP RX>, <Conferma certificato TLS per accesso alla rete> e <Conferma certificato TLS con applicazione MEAP> sono tutti impostati su < On> e un segno di spunta viene aggiunto a <CN>. Inoltre, le opzioni <Verifica certificato server> e <Verifica CN> in <Impostazioni SIP>> <Impostazioni TLS> sono impostate su <On>. Durante la comunicazione TLS, viene eseguita la verifica per i certificati digitali e i loro nomi comuni
Vieta l'autenticazione con testo in chiaro per le funzioni server	• <Usa stampa FTP> in <Impostazioni stampa FTP> è impostato su <Off> • <Consenti TLS (SMTP RX)> in <Impostazioni e-mail/I-Fax> <Impostazioni comunicazione> è impostato su <Sempre TLS>, <Metodo di autenticazione porta dedicata> in <Rete> è impostato su <Modalità 2>, • <Usa TLS> in <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 sarà possibile utilizzare applicazioni o funzioni server, come FTP, che supportano solo l'autenticazione con testo in chiaro. Potrebbe non essere possibile accedere alla macchina dal software o driver di gestione del dispositivo
Vieta l'uso di SNMPv1	In <Impostazioni SNMP>, <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 porta: 515 <Impostazioni stampa LPD> è impostato su <Off>. Non è possibile eseguire la stampa LPD.
Limita porta RAW	Numero porta 9100 <Impostazioni stampa RAW> è impostato su <Off>. Non è possibile eseguire la stampa RAW.
Limita porta FTP	Numero porta 21 In <Impostazioni stampa FTP>, <Usa stampa FTP> è impostato su <Off>. Non è possibile eseguire la stampa FTP.

Limita porta WSD	Numero porta 3702, 60000 In <Impostazioni WSD>, le opzioni <Usa WSD>, <Usa navigazione WSD> e <Usa scansione WSD> sono tutte impostate su <Off>. Non è possibile utilizzare le funzioni WSD
Limita porta BMLinkS	Numero porta 1900 Non usato nella regione europea
Limita porta IPP	Numero porta 631 Non sarà possibile utilizzare Mopria, AirPrint e IPP se luso della porta IPP è soggetto a restrizioni
Limita porta SMB	Numero porta: 137, 138, 139, 445 In <Impostazioni server SMB>, <Usa server SMB> è impostato su <Off>. Non è possibile utilizzare la macchina come server SMB.
Limita porta SMTP	Numero porta 25 In <Impostazioni e-mail/I-Fax>> <Impostazioni comunicazione>, <SMTP RX> è impostato su <Off>. La ricezione SMTP non è possibile.
Limita porta dedicata	Numero porta: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547 Non sarà 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 porta 5900 <Impostazioni operazioni in remoto> è impostato su <Off>. Non è possibile utilizzare le funzioni operazioni in remoto.
Limita porta SIP (IP Fax)	Numero porta: 5004, 5005, 5060, 5061, 49152) <Usa Intranet> in <Impostazioni Intranet>, <Usa NGN> in <Impostazioni NGN> e <Usa gateway VoIP> in <Impostazioni gateway VoIP> sono tutti impostati su <Off>. Non è possibile utilizzare la funzione fax IP.
Limita porta mDNS	Numero porta 5353 In <Impostazioni mDNS>, le opzioni <Usa IPv4 mDNS> e <Usa IPv6 mDNS> sono impostate su <Off> <Usa Mopria> è impostato su <Off>. Non è possibile cercare nella rete o eseguire impostazioni automatiche usando mDNS. Inoltre, non è possibile stampare usando Mopria™ o AirPrint
Limita porta SLP	Numero porta 427 In <Impostazioni multicast discovery>, <Risposta> è impostato su <Off>. Non è possibile cercare nella rete o eseguire impostazioni automatiche usando SLP.
Limita porta SNMP	Numero 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 <Impostazioni SNMP>, le opzioni <Usa SNMPv1> e <Usa SNMPv3> sono impostate su <Off>

2. Autenticazione	Note
Politica operativa di autenticazione	
Vieta utenti ospiti	• <Impostazioni spazio avanzato>> <Gestione autenticazione> è impostato su <On> • <Impostazioni visualizzazione schermata di accesso> è impostato su <Visualizza quando il dispositivo viene avviato> • <Limita il lavoro da dispositivo remoto senza autorizzazione utente> è impostato su <On> Non è possibile per gli utenti non registrati accedere alla macchina. Anche i lavori di stampa inviati da un computer vengono annullati.
Forza l'impostazione della disconnessione automatica	Questa impostazione serve per disconnettersi dal pannello di controllo. Questo parametro non si applica ad altri metodi di disconnessione (intervallo regolabile 10 sec - 9 minuti) <Tempo di ripristino automatico> è abilitato. L'utente viene disconnesso automaticamente se non viene eseguita alcuna operazione per un determinato periodo di tempo. Selezionare [Tempo fino alla disconnessione] sulla schermata di configurazione della IU remota.
Politica operativa sulle password	
Vieta la memorizzazione nella cache della password per i server esterni	Questa impostazione non si applica alle password che l'utente salva esplicitamente, come password per rubriche o simili <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	<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	<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 dipartimentale/PIN casella di posta, autenticazione PIN o stampa sicura ecc. Soglia di blocco: Impostabile tra 1 e 10 volte Periodo di blocco: Impostabile tra 1 e 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. Eseguire sempre il backup delle chiavi TPM quando TPM è abilitato. Fare riferimento al manuale utente per i dettagli 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	• <Salva registro operazioni> è impostato su <On> • <Visualizza registro lavori> è impostato su <On> • <Recupera registro lavori con software di gestione> in <Visualizza registro lavori> è impostato su <Consenti> • <Salva registro di controllo> è impostato su <On> • <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 <Impostazioni SNTP>, <Usa SNTP> è impostato su <On>. È richiesta la sincronizzazione dell'ora tramite SNTP. Inserire un valore per [Nome server] sulla schermata di configurazione della IU remota.

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. • <Gestisci i file con errori di inoltro> è impostato su <Off> • <Usa blocco memoria fax> è impostato su <On> • <Usa blocco memoria I-Fax> è impostato su <On> • <Tempo di blocco memoria> è impostato su <Off> • <Visualizza stampa durante l'archiviazione dal driver di stampa> in <Imposta/registra fax in arrivo riservati> è impostato su <Off> • <Impostazioni per tutte le caselle di posta>> <Stampa durante l'archiviazione dal driver di stampa> è impostato su <Off> • <Impostazioni sicurezza casella>> <Visualizza stampa durante l'archiviazione dal driver di stampa> è impostato su <Off> • <Vieta lavoro da utente sconosciuto> è impostato su <On> e <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 <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	<Utilizza impostazioni di inoltro> è impostato su <Off>. Non è possibile inoltrare automaticamente i fax.

6. Memorizzazione	Note
Forza la cancellazione completa dei dati	<Eliminazione completa dei dati dal disco rigido> è impostato su <On>

Canon Inc.
canon.com

Canon Europe
canon-europe.com

Italian edition

Canon Italia Spa
Strada Padana Superiore, 2/B
20063 Cernusco sul Naviglio MI
Tel 02 82481
Fax 02 82484600
Pronto Canon 848800519
canon.it

Canon (Svizzera) SA
Richtistrasse 9
8304 Wallisellen
Canon Helpdesk
Tel. +41 (0)848 833 835
canon.ch