GUIA DE FORTALECIMENTO MFD

Série imageRUNNER ADVANCE

Canon

INTRODUÇÃO

Os equipamentos multifunções modernos (MFD) da Canon oferecem funcionalidades de impressão, cópia, digitalização, envio e fax. Os MFD são servidores informáticos por direito próprio, oferecendo vários serviços em rede, juntamente com um armazenamento em disco rígido significativo.

Quando uma organização adiciona estes equipamentos à sua infraestrutura, existem várias áreas que devem ser abordadas, como parte da estratégia de segurança mais alargada, a qual deve procurar proteger a confidencialidade, a integridade e a disponibilidade de todos os seus sistemas em rede.

Evidentemente, as implementações serão diferentes e as organizações terão os seus próprios requisitos de segurança específicos. Embora trabalhemos em conjunto para garantir que os equipamentos da Canon são enviados com as definições de segurança iniciais adequadas, pretendemos continuar a suportar esta prática ao oferecer várias opções de configuração para lhe permitir ajustar melhor o equipamento aos requisitos específicos da sua situação.

Este documento foi concebido para fornecer informações suficientes que lhe permitam discutir, em conjunto com a Canon ou com os nossos parceiros, as definições mais adequadas para o seu ambiente. É de notar que nem todo o hardware dos equipamentos tem o mesmo nível de capacidade e software de sistema diferente pode fornecer funcionalidades diferentes. Uma vez escolhida, a configuração final pode ser aplicada ao seu equipamento ou parque. Não hesite em entrar em contacto com a Canon ou com um dos nossos parceiros de forma a obter mais informações e apoio.

A quem se destina este documento?

Este documento destina-se a qualquer pessoa que tenha algum tipo de preocupação com o design, implementação e proteção de equipamentos multifunções (MFD) de escritório numa infraestrutura de rede. Podendo assim estar incluídos especialistas em TI e redes, profissionais de segurança de TI e funcionários de assistência.

Âmbito e cobertura

O guia explica e oferece aconselhamento sobre as definições de configuração para dois ambientes de rede típicos, de forma a que as organizações possam implementar, de forma segura, uma solução de MFD com base nas melhores práticas. O guia explica, igualmente, (a partir da versão 3.8 da plataforma de software do sistema) como a funcionalidade Syslog pode fornecer feedback em tempo real a partir do MFD. Estas definições foram testadas e validadas pela equipa de segurança da Canon.

Não fazemos suposições sobre requisitos regulatórios específicos do setor industrial que possam impor outras considerações de segurança e que estejam fora do âmbito deste documento.

Este guia foi criado com base no conjunto de funcionalidades típico da plataforma imageRUNNER ADVANCE e, embora as informações aqui contidas se apliquem a todos os modelos e séries da gama imageRUNNER ADVANCE, algumas funcionalidades podem diferir entre modelos.

Implementação da segurança adequada de MFD para o seu ambiente

Para explorar as implicações de segurança relativamente à implementação de um equipamento multifunções como parte da sua rede, considerámos dois cenários típicos:

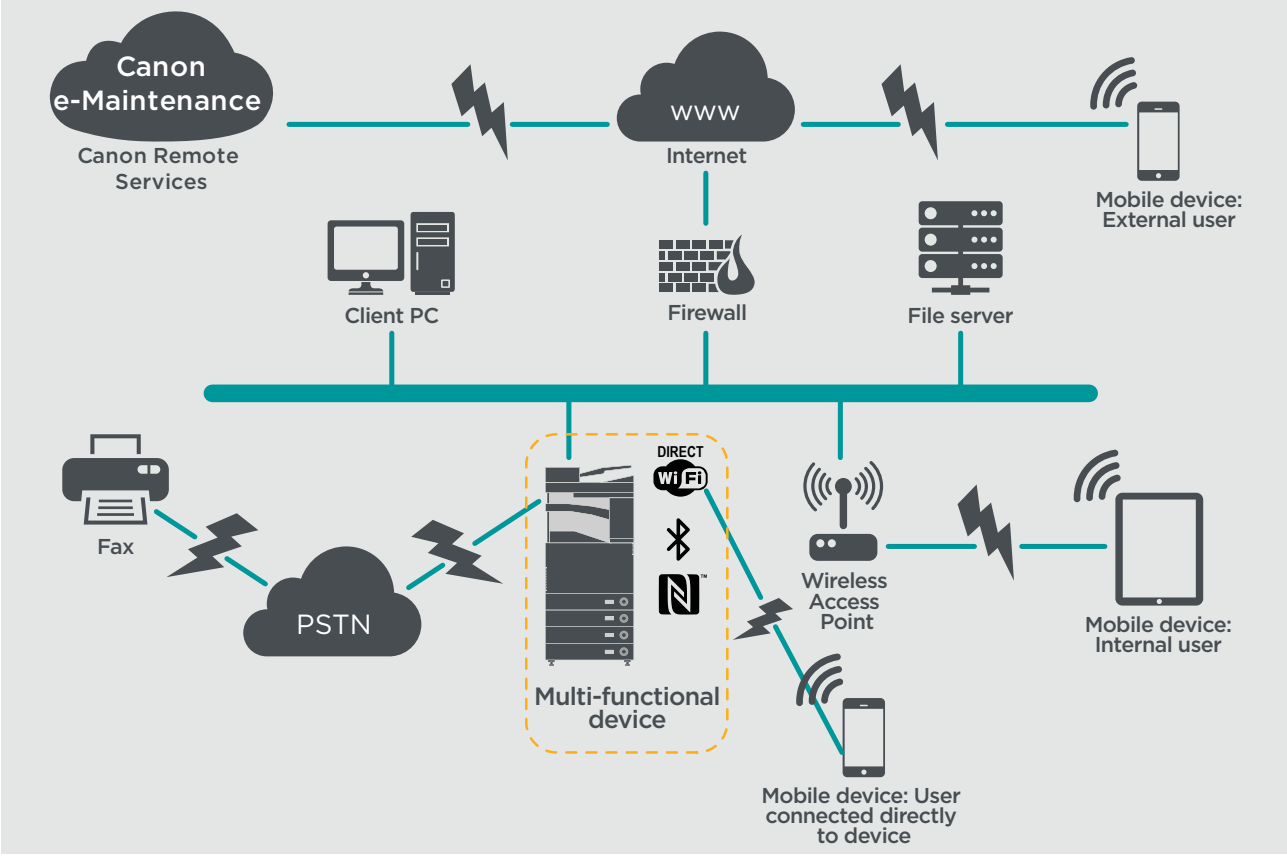
- **Um ambiente típico de pequeno escritório**
- **Um ambiente de escritório empresarial**

AMBIENTE DE PEQUENO ESCRITÓRIO

Normalmente, este é um ambiente típico das pequenas empresas com uma topologia de rede não segmentada. Utiliza um ou dois MFD para a sua utilização interna e estes equipamentos não estão acessíveis na Internet.

Embora a impressão móvel esteja disponível, serão necessários componentes de solução adicionais. Para os utilizadores que precisam de serviços de impressão fora de um ambiente LAN, é necessária uma ligação segura, mas este aspeto não será abordado neste guia. No entanto, deve ser dada atenção à segurança dos dados em trânsito entre o equipamento remoto e a infraestrutura de impressão.

Figura 1 Rede de um pequeno escritório



A mais recente geração de modelos da série imageRUNNER ADVANCE oferece uma conetividade de rede sem fios, permitindo que o equipamento se ligue a uma rede Wi-Fi. Também pode ser utilizada para estabelecer uma ligação Wi-Fi Direct com um dispositivo móvel sem necessidade de uma ligação de rede.

As opções de Bluetooth e de NFC estão disponíveis para vários modelos de equipamentos e são utilizadas apenas para estabelecer a ligação Wi-Fi Direct para dispositivos iOS e Android, respetivamente.

CONSIDERAÇÕES SOBRE A CONFIGURAÇÃO

Tenha em atenção que, a menos que uma funcionalidade da série imageRUNNER ADVANCE esteja mencionada abaixo, esta é considerada suficiente nas predefinições para este ambiente empresarial e de rede.

Tabela 1 Considerações sobre a configuração para um ambiente de pequeno escritório

Funcionalidade da série imageRUNNER ADVANCE	Descrição	Consideração
Modo de serviço	Permite o acesso às definições do modo de serviço	Proteção por palavra-passe com uma palavra-passe diferente da predefinida, que não seja trivial e com um tamanho máximo
Sistema de gestão de serviços	Permite o acesso a várias definições não standard do equipamento	Proteção por palavra-passe com uma palavra-passe diferente da predefinida, que não seja trivial e com um tamanho máximo
Pesquisa/envio através de SMB	Armazenamento e recuperação de e para partilhas de rede SMB/Windows	Os administradores do sistema devem, por política, proibir qualquer utilizador de criar contas locais para utilização na partilha de documentos com a imageRUNNER ADVANCE através de SMB
IU remota	Web-based configuration tool	O administrador do imageRUNNER ADVANCE deve ativar o HTTPS para a IU remota e desativar o acesso HTTP. Ative o uso da autenticação PIN exclusiva para cada equipamento
SNMP	Integração da monitorização da rede	Desative a versão 1 e ative apenas a versão 3
Envie para e-mail e/ou IFAX	Envie e-mails a partir do equipamento com anexos	Ative o SSL Não utilize a autenticação do POP3 antes do envio por SMTP Utilize a autenticação por SMTP
POP3	Obtenha e imprima automaticamente documentos da caixa de correio	Ative o SSL Ative a autenticação do POP3
Livro de endereços/LDAP	Utilize o serviço de diretório para procurar o número indicativo ou os endereços de e-mail para onde enviar as digitalizações	Ative o SSL Não utilize credenciais do domínio para autenticar no servidor LDAP; utilize credenciais LDAP específicas
Impressão FTP	Carregue e transfira documentos de e para o servidor FTP incorporado	Ative a autenticação FTP. Tenha em atenção que o tráfego FTP irá sempre deslocar-se num texto não encriptado ao longo da rede
Envio WebDAV	Digitalize e armazene documentos num local remoto	Ative a autenticação para partilhas WebDAV
PDF encriptado	Encripte documentos	Por norma, os documentos sensíveis apenas devem ser encriptados através da versão em PDF 1.6 (AES-128)
Impressão segura	O trabalho de impressão é enviado para o equipamento, mas bloqueado na fila de impressão até que o número PIN correspondente seja introduzido	Ative os trabalhos de impressão protegidos por código PIN
Notificação de eventos Syslog	O System Logging Protocol é um protocolo standard da indústria utilizado para enviar registos do sistema ou mensagens de eventos para um servidor específico, denominado servidor Syslog	Considere encaminhar os dados Syslog da série imageRUNNER para a sua ferramenta de análise de rede syslog atual ou para a plataforma Security Event Managment (SIEM).
Verificação do sistema no arranque	Garante que os componentes de software do sistema não foram comprometidos. Terá um impacto mínimo no tempo de arranque do sistema	Ative a função
Navegador Web incorporado	Acesso do navegador à Internet	Execute, através da administração, um proxy Web de filtragem de conteúdo de forma a evitar o acesso a conteúdos maliciosos ou virais. Desative a criação de favoritos
Bluetooth e NFC (disponíveis a partir dos modelos Generation 3)	Utilizados para estabelecer uma ligação Wi-Fi Direct	Ative o Wi-Fi Direct para permitir a ligação direta a um dispositivo móvel. O WiFi Direct não pode ser utilizado quando o Wi-Fi é utilizado para se ligar a uma rede
LAN sem fios	Disponibiliza acesso sem fios	Utilize WPA-PSK/WPA2-PSK com palavras-passe fortes
IPP	Ligue e envie trabalhos de impressão através de IP	Desative o IPP

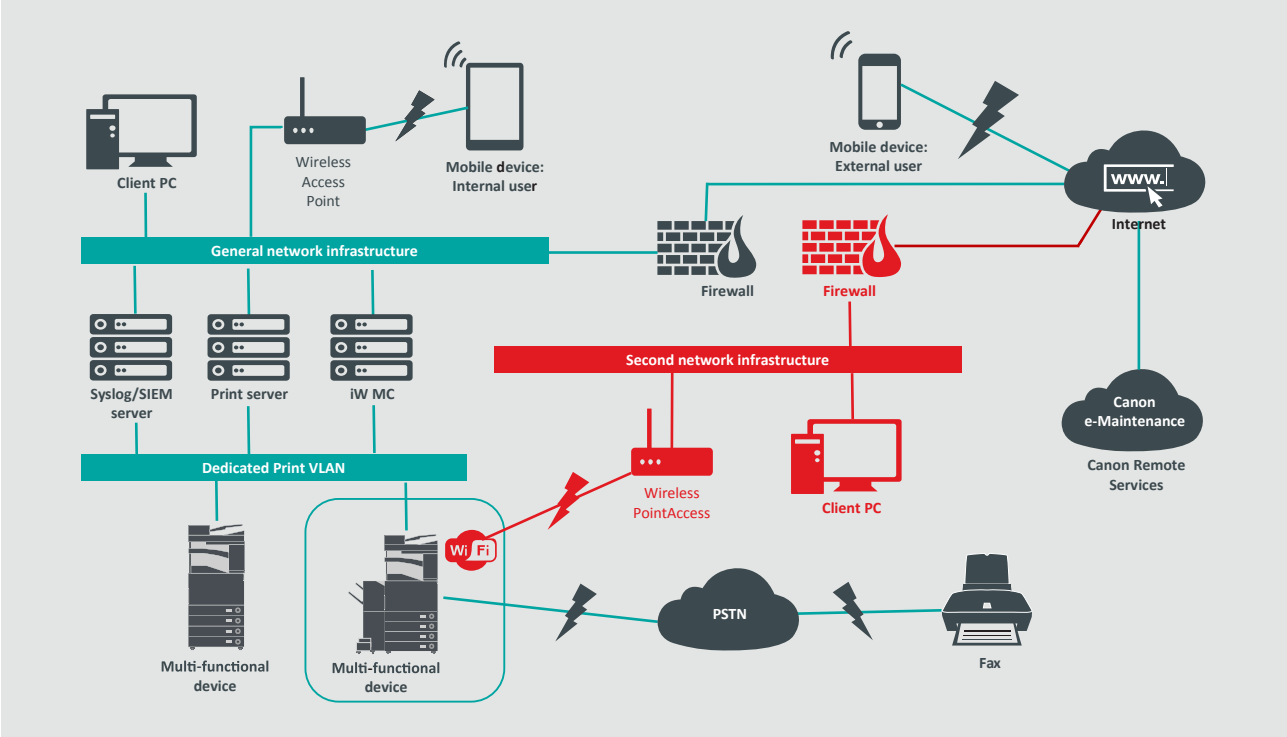
UM AMBIENTE DE ESCRITÓRIO EMPRESARIAL

Normalmente, trata-se de um ambiente com vários locais, vários escritórios e uma arquitetura de rede segmentada. Possui vários MFD implementados numa VLAN separada, a qual é acessível para uso interno através de servidor(es) de impressão. Estes MFD não estão acessíveis a partir da Internet.

Este ambiente terá normalmente uma equipa permanente para apoiar as suas necessidades de rede e back office juntamente com questões informáticas gerais, mas presume-se que não terão formação específica em MFD.

Normalmente, trata-se de um ambiente com vários locais, vários escritórios e uma arquitetura de rede segmentada. Possui vários MFD implementados numa VLAN separada, a qual é acessível para uso interno através de servidor(es) de impressão. Estes MFD não estão acessíveis a partir da Internet.

Figura 2 Trabalho num escritório empresarial



As ligações realçadas a vermelho estarão disponíveis nos modelos Generation 3

CONSIDERAÇÕES SOBRE A CONFIGURAÇÃO

Tenha em atenção que, a menos que uma funcionalidade da série imageRUNNER ADVANCE esteja mencionada abaixo, esta é considerada suficiente nas predefinições para este ambiente empresarial e de rede.

Tabela 2 Considerações sobre a configuração para um ambiente de escritório empresarial

Funcionalidade da série imageRUNNER ADVANCE	Descrição	Consideração
Modo de serviço	Permite o acesso às definições do modo de serviço	Proteção por palavra-passe com uma palavra-passe diferente da predefinida, que não seja trivial e com um tamanho máximo
Sistema de gestão de serviços	Permite o acesso a várias definições não standard do equipamento	Proteção por palavra-passe com uma palavra-passe diferente da predefinida, que não seja trivial e com um tamanho máximo
Pesquisa/envio através de SMB	Armazenamento e recuperação de e para partilhas de rede SMB/Windows	Os administradores de sistemas devem, por norma, impedir que quaisquer utilizadores criem contas locais nos seus equipamentos para a partilha de documentos com a série imageRUNNER ADVANCE através de SMB
IU remota	Web-based configuration tool	Após as configurações iniciais do equipamento, desative totalmente a IU remota ao desativar os protocolos HTTP e HTTPS
SNMP	Integração da monitorização da rede	Desative a versão 1 e ative apenas a versão 3
Envie para e-mail e/ou IFAX	Envie e-mails a partir do equipamento com anexos	Ative o SSL Ative: - Verificação do certificado no servidor SMTP Ou, caso não seja viável: - Utilizar esta funcionalidade apenas num ambiente onde esteja presente uma solução de deteção de intrusão de Rede. Não utilizar a autenticação POP3 antes do envio de SMTP. Utilizar autenticação SMTP
POP3	Obtenha e imprima automaticamente documentos da caixa de correio	Ative o SSL Ative: - Verificação do certificado no servidor POP3 Ou, caso não seja viável: - Utilizar esta funcionalidade apenas num ambiente onde esteja presente uma solução de deteção de intrusão de Rede. Ativar a autenticação POP3
Livro de endereços/LDAP	Utilize o serviço de diretório para procurar o número de telefone ou os endereços de e-mail para onde enviar as digitalizações	Ative o SSL Ative: - Verificação do certificado no servidor LDAP Ou, caso não seja viável: - Utilizar esta funcionalidade apenas num ambiente onde esteja presente uma solução de deteção de intrusão de Rede. Não utilizar credenciais de domínio para autenticar contra o servidor LDAP; Utilizar credenciais específicas LDAP
IPP	Ligue e envie trabalhos de impressão através de IP	Desative o IPP
Envio WebDAV	Digitalize e armazene documentos num local remoto	Ative a autenticação para as partilhas WebDAV. Ative o SSL Faça com que a impressora apenas permita o carregamento de ficheiros que terminem com as "extensões de impressão de ficheiros"
IEEE802.1X	Mecanismo de autenticação de acesso à rede	EAPOL V1 suportado
PDF encriptado	Encripte documentos	Por norma, os documentos sensíveis apenas devem ser encriptados através da versão em PDF 1.6 (AES-128)
Impressão segura encriptada	Aumente a proteção da impressão segura ao encriptar o ficheiro e a palavra-passe durante a transmissão	Durante a configuração da impressora do cliente, altere o nome de utilizador no separador "Impressora" para um nome diferente das credenciais LDAP ou do domínio desse utilizador. Certifique-se de que a opção "restringir os trabalhos da impressora" está desligada
Registo automático de certificados	O processo de registo automático melhora a eficiência da recuperação e implementação da certificação digital	Requer uma solução de certificado de rede para potenciar
Notificação de eventos Syslog	O System Logging Protocol é um protocolo standard da indústria utilizado para enviar registos do sistema ou mensagens de eventos para um servidor específico, denominado servidor Syslog	Considere encaminhar os dados Syslog da série imageRUNNER ADVANCE para a sua ferramenta de análise de rede syslog atual ou para a plataforma Security Event Managment (SIEM)
Verificação do sistema no arranque	Garante que os componentes de software do sistema não foram comprometidos. Terá um impacto mínimo no tempo de arranque do sistema	Ative a função
LAN sem fios	Disponibiliza acesso sem fios	Utilize WPA-PSK/WPA2-PSK com palavras-passe fortes
Wi-Fi Direct	Utilizados para estabelecer uma ligação Wi-Fi Direct	Desative o Wi-Fi Direct
Navegador Web incorporado (disponível nos modelos Generation 3 2nd Edition)	Acesso do navegador à Internet	Aplique restrições adequadas ou desative a capacidade de transferir ficheiros obtidos através do navegador

A mais recente geração de modelos imageRUNNER ADVANCE oferece conetividade de rede sem fios, permitindo que o equipamento se ligue simultaneamente a uma rede Wi-Fi enquanto se encontra ligado a uma rede com fios. Este cenário pode ser útil quando o cliente precisar de partilhar um equipamento entre duas redes. O ambiente escolar é um exemplo típico em que existem redes separadas para funcionários e alunos.

A plataforma imageRUNNER ADVANCE oferece um ambiente de funcionalidades que permite uma utilização flexível. Com os protocolos e serviços disponíveis para tal, é importante garantir que apenas são ativadas as funcionalidades, serviços e protocolos necessários para satisfazer as necessidades do utilizador. Esta é uma boa prática de segurança que não só irá reduzir a potencial superfície de ataque como também irá impedir a sua exploração. Uma vez que estão constantemente a aparecer novas vulnerabilidades, devemos estar sempre atentos a compromissos, quer intrínsecos quer extrínsecos ao dispositivo. Ter a capacidade de monitorizar a atividade do utilizador é útil para ajudar a identificar e a tomar medidas corretivas quando necessário.

A versão 3.8 da plataforma de software imageRUNNER ADVANCE fornece algumas funcionalidades adicionais àquelas que já se encontram disponíveis há vários anos. Aqui inclui-se a capacidade de monitorizar o equipamento em tempo real utilizando o Syslog e a Verificação do sistema no arranque. A utilização destas caraterísticas em colaboração com as suas soluções de segurança de rede existentes, tais como uma plataforma SIEM ou uma solução de registo, permite uma maior visibilidade e identificação de incidentes e para fins forenses.

Verificação do sistema no arranque

Esta funcionalidade é um mecanismo de hardware concebido para garantir que todas as partes do software do sistema imageRUNNER ADVANCE Generation 3 são verificadas em relação a uma Root of Trust para garantir que o sistema operativo é carregado conforme a Canon pretende. Caso alguém com intenções maliciosas adultere ou tente modificar o sistema, ou caso ocorra um erro ao carregar o sistema, o processo será interrompido e será apresentado um código de erro.

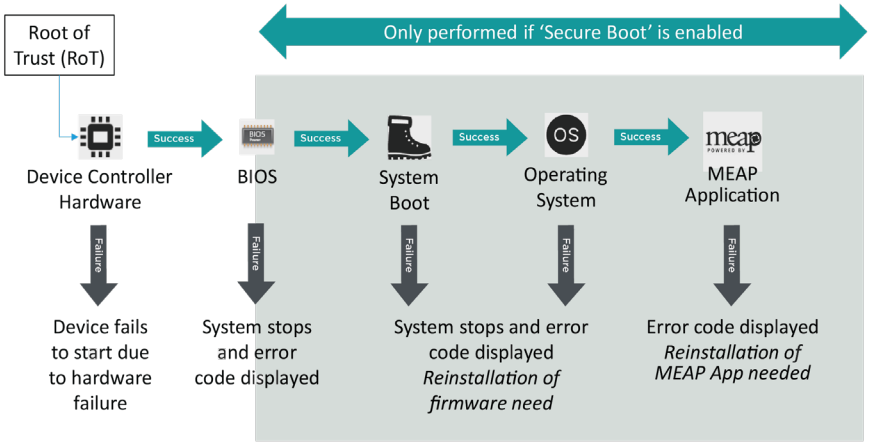


Figura 3 Processo de verificação do sistema no arranque

Este processo é transparente para o utilizador, para além do visor indicar que uma versão não intencional do sistema está a ser carregada. A série imageRUNNER ADVANCE Generation 3 3rd Edition tem uma opção para ativar a verificação do sistema no arranque, a qual deve ser ligada de forma a ativar esta funcionalidade de segurança.

Registo automático de certificados

Nas versões anteriores à versão 3.8 da plataforma de software do sistema imageRUNNER ADVANCE, o administrador tinha de instalar manualmente os certificados de segurança atualizados em cada equipamento. Esta é uma tarefa trabalhosa, uma vez que é necessário ligar a cada equipamento para efetuar uma atualização manual. Adicionalmente, os certificados têm de ser instalados manualmente utilizando a interface de utilizador remota (RUI) do equipamento específico, tornando o processo muito mais demorado. Com o serviço de registo automático de certificados, o qual foi introduzido a partir da versão 3.8 e superior da plataforma, esta sobrecarga foi eliminada.

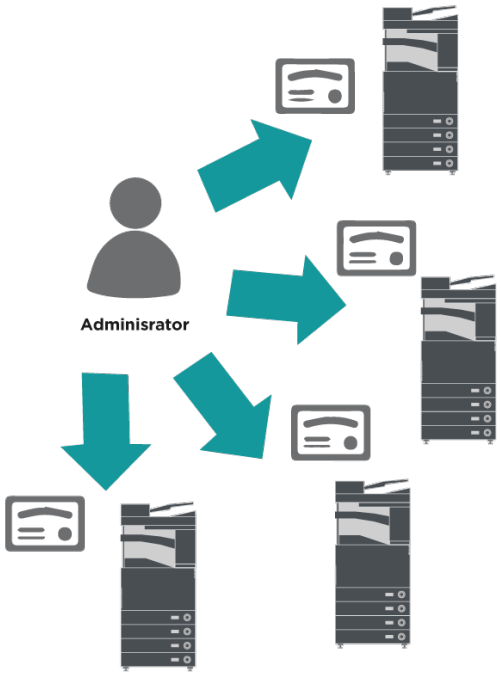


Figura 4 Registo de certificados

O processo de registo automático melhora a eficiência da recuperação do certificado. Este processo fornece a capacidade de recuperar automaticamente certificados utilizando o NDES (Network Device Enrolment Service) para Microsoft Windows e o SCEP (Simple Certificate Enrolment Protocol).

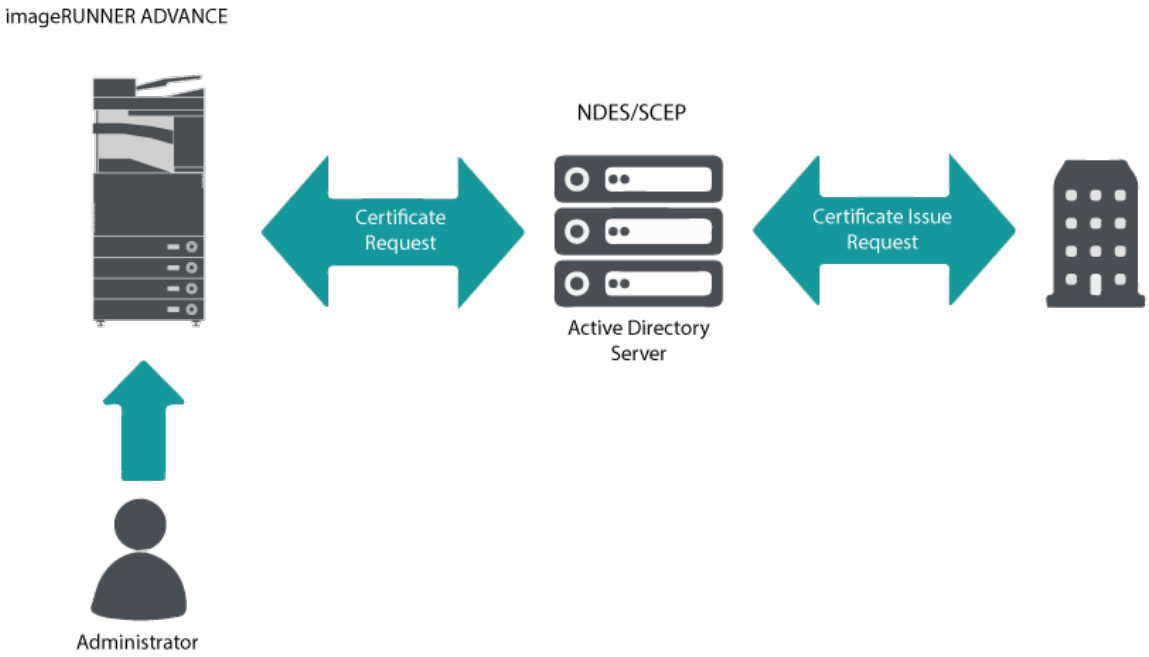


Figura 5 Processo de registo de certificados

O SCEP é um protocolo que suporta certificados emitidos por uma Autoridade de certificação (AC) e o NDES permite que os equipamentos de rede recuperem ou atualizem certificados baseados no SCEP.

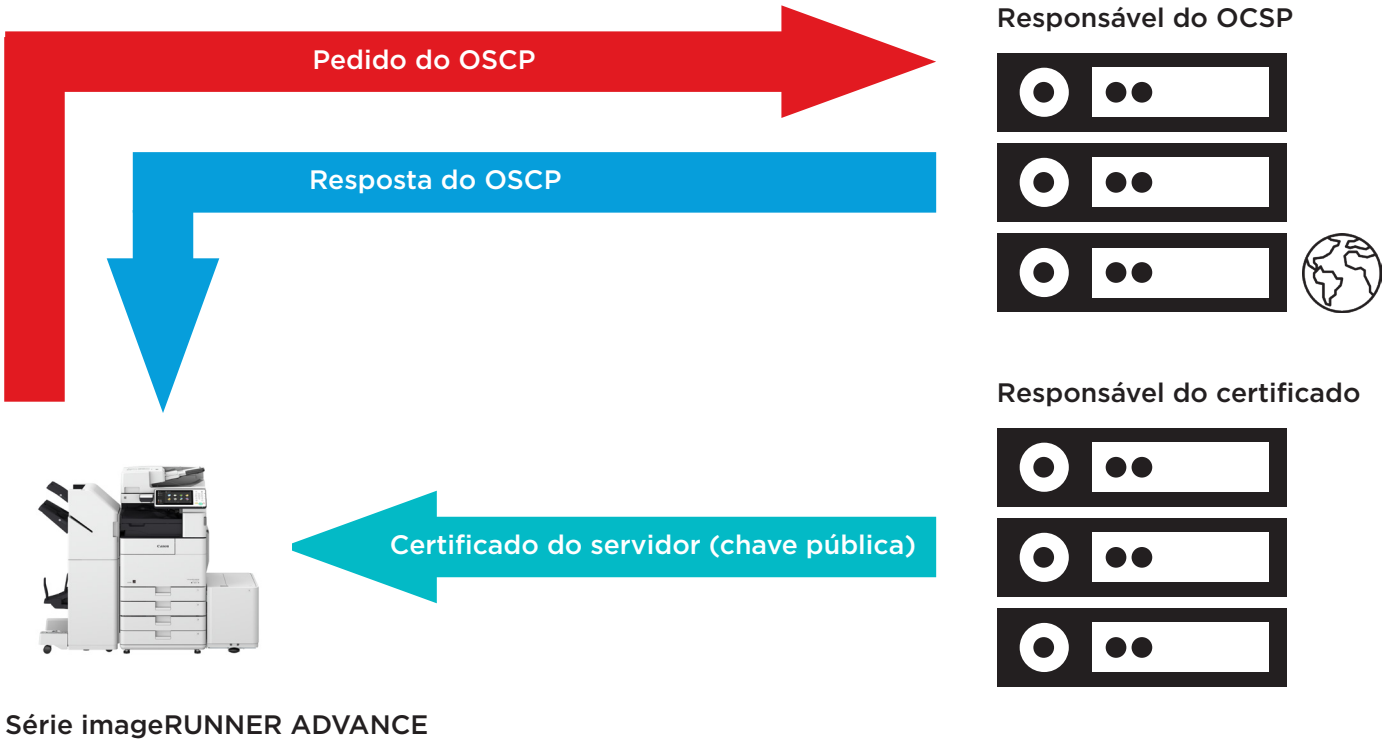
O NDES é um serviço de função dos Serviços de certificados do Active Directory.

Online Certificate Status Protocol

Existem várias razões pelas quais pode ser necessário revogar um certificado digital. Alguns exemplos podem incluir o facto de a chave privada ter sido perdida, roubada, comprometida ou que o nome de um domínio tenha sido alterado.

O OCSP (Online Certificate Status Protocol) é um protocolo standard de Internet, utilizado para verificar o estado de revogação de um certificado digital X.509 que tenha sido fornecido pelo servidor de certificados. Ao enviar um pedido de OCSP ao respetivo responsável (normalmente, um emissor de certificados) especificando um certificado específico, o responsável do OCSP responderá com "good" (bom), "revoked" (revogado) ou "unknown" (desconhecido).

Figura 6 Processo de "handshake" do OCSP



Com a versão 3.10 da plataforma imageRUNNER ADVANCE, o OCSP fornece um mecanismo em tempo real para verificar os certificados digitais X.509 instalados. As versões anteriores da plataforma apenas suportavam o método CRL (Certificate Revoke List), o qual é pouco eficaz e resulta numa sobrecarga pesada nos recursos da rede.

Informações de segurança e gestão de eventos

A tecnologia da série imageRUNNER ADVANCE suporta a capacidade de enviar eventos de segurança em tempo real utilizando o protocolo Syslog, o qual cumpre as normas RFC 5424, RFC 5425 e RFC 5426.

Este protocolo é utilizado por muitos tipos de equipamentos como forma de recolher informações em tempo real, que podem ser utilizadas para identificar potenciais problemas de segurança.

Para facilitar a deteção de ameaças e incidentes de segurança, o equipamento deve ser configurado para encaminhar para um servidor de Security Incident Event Management (SIEM) externo.

Os eventos syslog produzidos pelo equipamento podem ser utilizados para criar ações através da recolha e análise em tempo real de eventos a partir de uma grande variedade de fontes contextuais de dados (Figura 7). Também pode suportar relatórios de conformidade e investigação de incidentes através da utilização de soluções adicionais, como um servidor SIEM. Pode encontrar um exemplo disto mesmo na figura 8.

A mais recente geração de equipamentos da série imageRUNNER ADVANCE oferece a funcionalidade Syslog que suporta uma gama de eventos que podem ser recolhidos. Isto pode ser utilizado para correlacionar e analisar eventos de várias fontes diferentes de forma a identificar tendências ou anomalias.

Figura 7 Captura de dados do Syslog

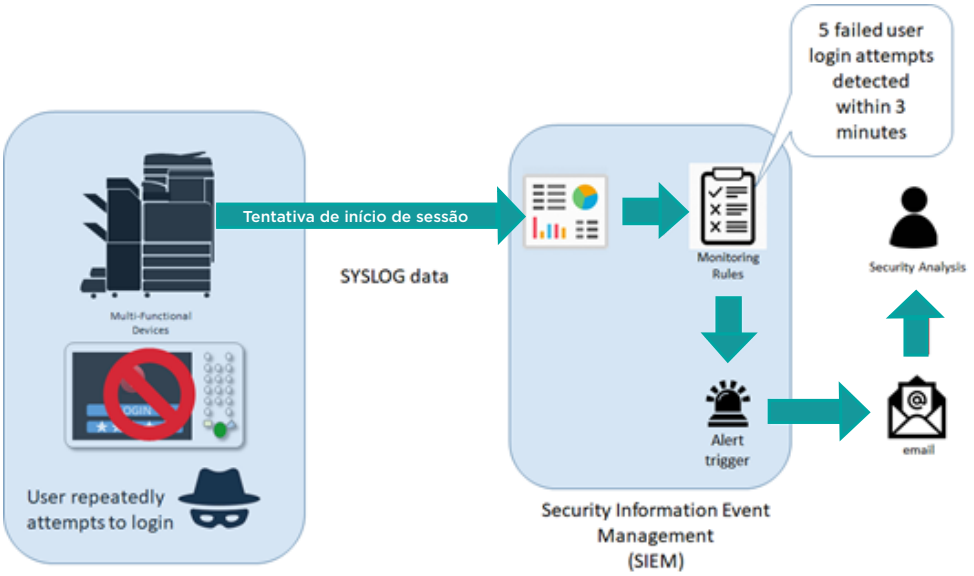


Figura 8 Exemplo de utilização de dados do Syslog da série imageRUNNER ADVANCE

Gestão de registos de equipamentos

Para além da funcionalidade Syslog fornecida pela plataforma de software de sistema versão 3.8, a série imageRUNNER ADVANCE conta com os seguintes registos que podem ser geridos no equipamento. Estes registos podem ser exportados em formato CSV através da Interface de utilizador remota (RUI).

Tabela 3 - Exemplos de ficheiros de registos que podem ser geridos pelo equipamento multifunções.

Tipo de registo	Número indicado como "Log Type" (tipo de registo) no ficheiro CSV	Descrição
Log	4098	Este registo contém informações relacionadas com o estado da autenticação do utilizador (início/encerramento de sessão e êxito/falha da autenticação do utilizador), o registo/alteração/eliminação de informações do utilizador geridas com autenticação do utilizador e a gestão (adição/edição/eliminação) de funções com o SISTEMA DE GESTÃO DE ACESSO
Registo do trabalho	1001	Este registo contém informações relacionadas com a conclusão de trabalhos de cópia/fax/digitalização/envio/impressão
Registo de transmissão	8193	O registo contém informações relacionadas com transmissões
Registo de gravação de espaço avançado	8196	Este registo contém informações relacionadas com a gravação de ficheiros no espaço avançado, na rede (espaço avançado de outros equipamentos) e nos suportes de memória
Registo de operação da caixa de correio	8197	Este registo contém informações relacionadas com as operações realizadas nos dados da caixa de correio, da caixa de entrada RX da memória e da caixa de entrada confidencial de fax
Registo de autenticação da caixa de correio	8199	Este registo contém informações relacionadas com o estado de autenticação da caixa de correio, da caixa de entrada da memória RX e da caixa de entrada confidencial de fax
Registo de operação de espaço avançado	8201	Este registo contém informações relacionadas com as operações de dados no espaço avançado
Registo de gestão de equipamentos	8198	Este registo contém informações relacionadas com o arranque/encerramento do equipamento, alterações efetuadas às definições utilizando a função (definições/registo), alterações efetuadas às definições utilizando a função de fornecimento de informações do equipamento, e a definição de hora do registo de gestão de equipamentos também regista alterações nas informações do utilizador ou nas definições relacionadas com a segurança quando o equipamento é inspecionado ou reparado pelo seu revendedor local autorizado da Canon
Registo de autenticação da rede	8200	Este registo é gravado quando existe uma falha na comunicação IPSec
Registo exportar/importar tudo	8202	Este registo contém informações relacionadas com a importação/exportação das definições utilizando a função Exportar tudo/importar tudo
Registo de cópia de segurança da caixa de correio	8203	Este registo contém informações relacionadas com cópias de segurança de dados nas caixas de entrada do utilizador, na caixa de entrada RX da memória, na caixa de entrada confidencial de fax, no espaço avançado, para além de quaisquer dados detidos e no formulário registado para a função de sobreposição de imagem
Registo de operação do ecrã de gestão de aplicações/software	3101	Este é um registo de operação de SMS (Service Management Service), registo/atualizações de software e programas de instalação de aplicações MEAP, etc.
Registo de política de segurança	8204	Este registo contém informações relacionadas com o estado das programações da política de segurança
Registo de gestão de grupos	8205	Este registo contém informações relacionadas com o estado das programações (registo/edição/eliminação) dos grupos de utilizadores
Registo de manutenção do sistema	8206	Este registo contém informações relacionadas com atualizações de firmware e cópias de segurança/restauro da aplicação MEAP, etc.
Registo de autenticação da impressão	8207	Este registo contém informações relacionadas com o histórico de operações relacionados com os trabalhos de impressão de suspensão forçada
Registo de sincronização das definições	8208	Este registo contém informações relacionadas com a sincronização das definições do equipamento. Sincronização de definições para várias impressoras multifunções da Canon
Registo para gestão de registos de auditoria	3001	Este registo contém informações relacionadas com o início e o fim desta função (a função de gestão de registos de auditoria), bem como a exportação de registos, etc.

Os registos podem conter até 40 000 entradas. Assim que o número de entradas exceder 40 000, as entradas mais antigas são eliminadas primeiro.

SUPORTE PARA EQUIPAMENTOS REMOTOS

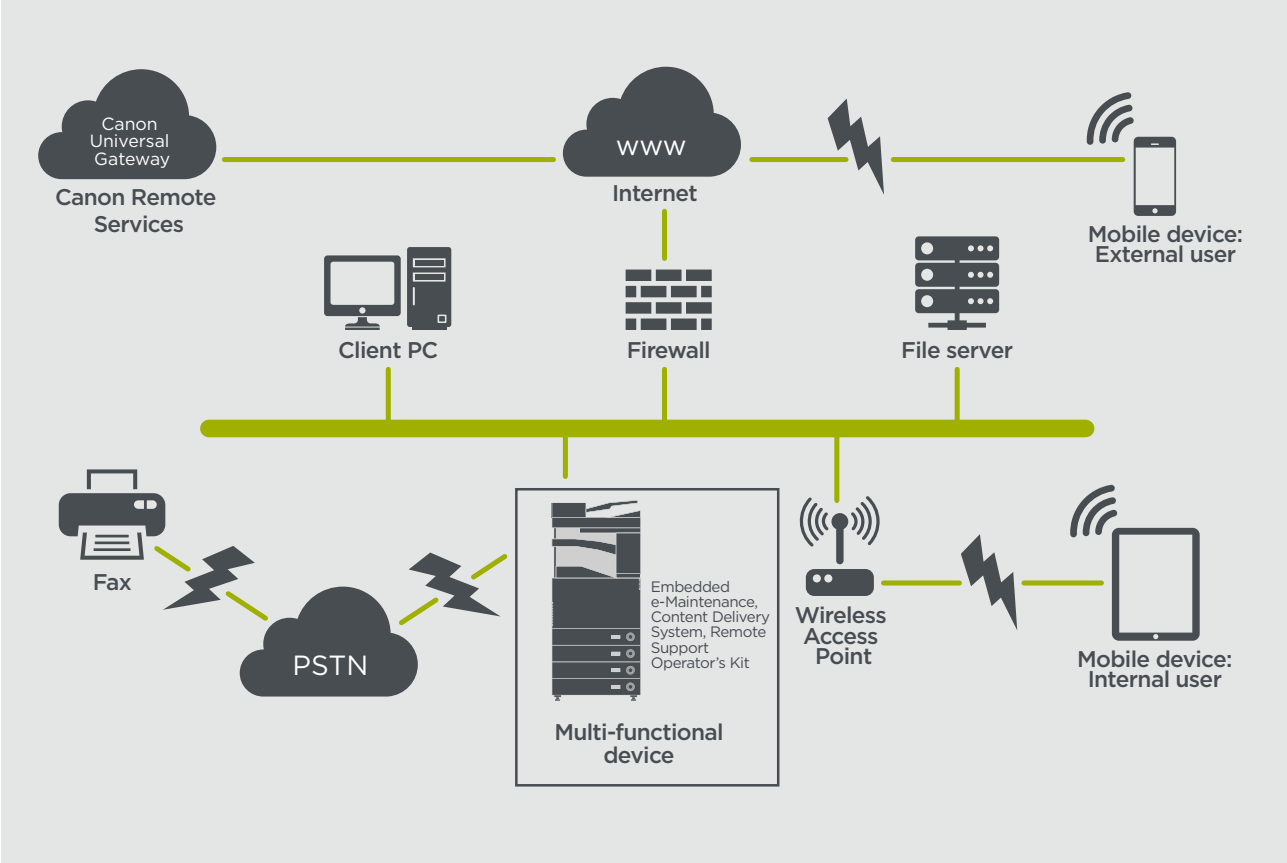
Para que a Canon ou um parceiro da Canon possam prestar um serviço eficiente, a série imageRUNNER ADVANCE é capaz de transmitir dados relacionados com o serviço, bem como receber atualizações de firmware ou aplicações de software. Deve ter-se em consideração que não são enviadas imagens ou metadados de imagens.

Abaixo estão apresentadas duas possíveis implementações dos serviços remotos da Canon na rede de uma empresa.

Cenário de implementação 1: ligação dispersa

Nesta definição, cada MFD permite uma ligação direta ao serviço remoto através da Internet.

Figura 9 Ligação dispersa



Cenário de implementação 2: ligação gerida centralizada

Num cenário de ambiente empresarial, onde se encontram instalados vários MFD, é necessário conseguir gerir estes equipamentos de uma forma eficiente a partir de um ponto central, o que inclui a ligação aos serviços remotos da Canon. Para facilitar o método de gestão holística, os equipamentos individuais estabeleceriam ligações de gestão através de um único ponto de ligação iW Management Console (iWMC). Para a comunicação entre o plug-in de atualização de firmware de equipamentos (DFU) e os equipamentos multifunções, é utilizada a porta UDP 47545.

Figura 10 Ligação gerida centralizada

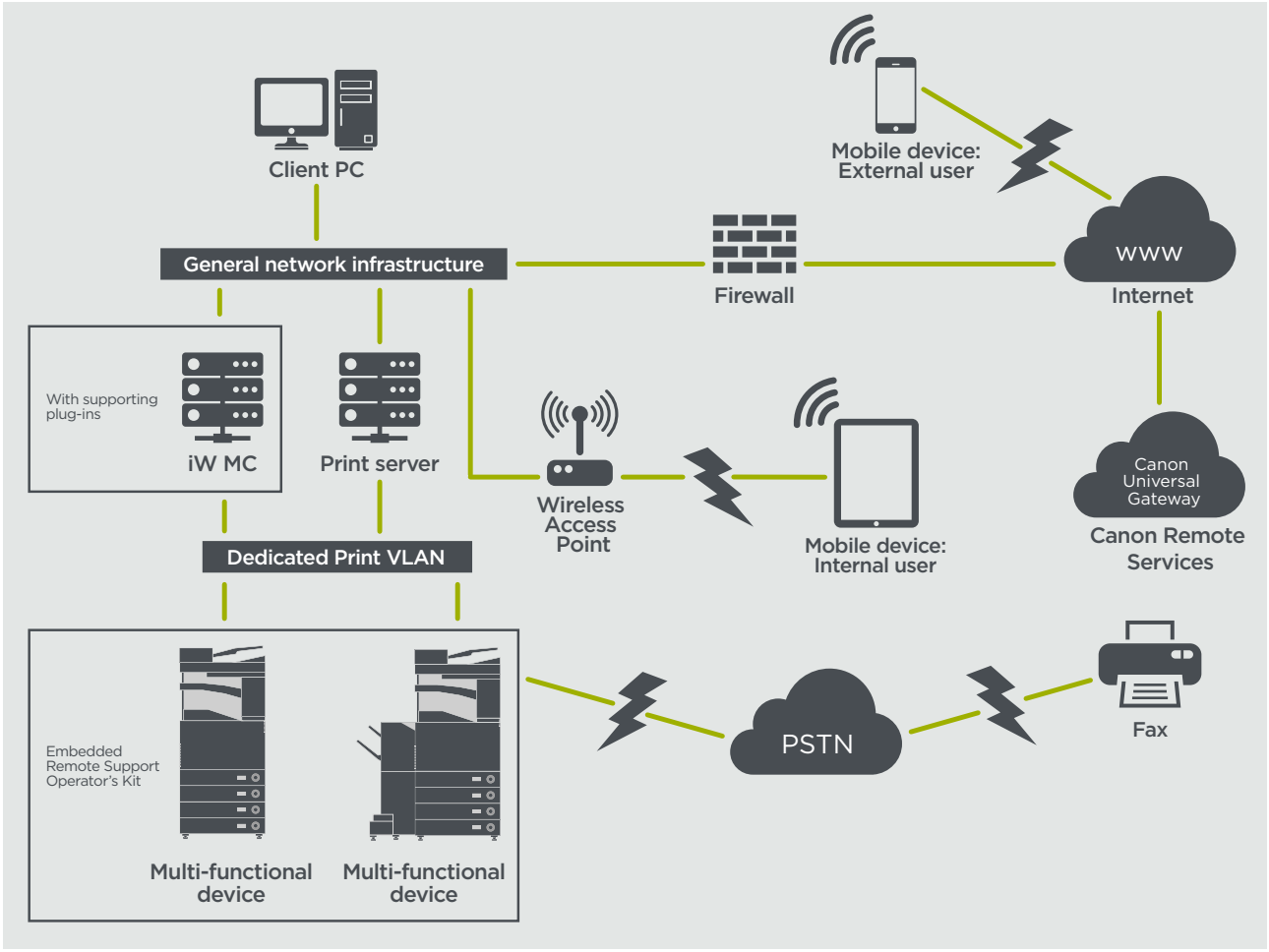


Figura
11a. Lista de equipamentos (neste caso, um único equipamento) conforme relatado no imageWARE Management Console e
11b. Detalhes e definições do equipamento

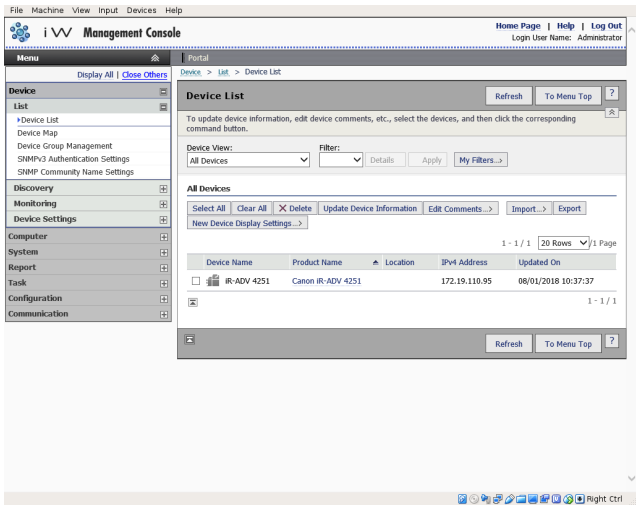


Figura 11a.

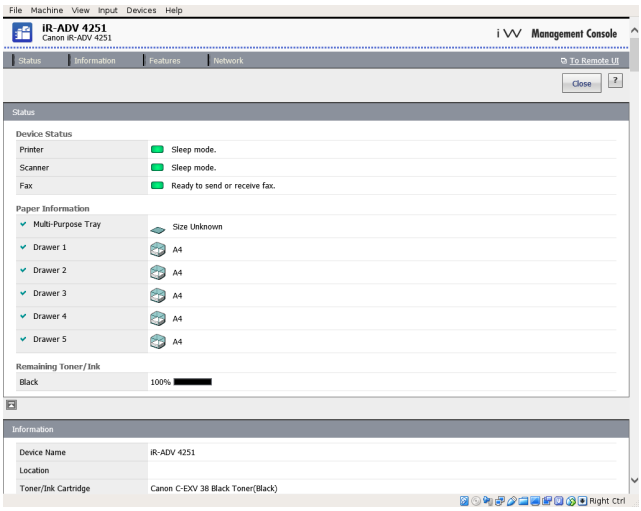


Figura 11b.

e-Maintenance

O sistema e-Maintenance fornece uma forma automatizada de recolher contadores de utilização de equipamentos para fins de faturação, gestão de consumíveis e monitorização remota de equipamentos através de alertas de estado e de erro.

O sistema e-Maintenance consiste num servidor voltado para a Internet (UGW) e num software de equipamento multifunções incorporado (eRDS) e/ou software adicional baseado em servidor (plug-in de RDS) para recolher informações relacionadas com o funcionamento do equipamento. O eRDS é um programa de monitorização executado dentro da imageRUNNER ADVANCE. Se a opção de monitorização estiver ativada nas definições do equipamento, o eRDS obtém as suas próprias informações do equipamento e envia-as para o UGW. O plug-in de RDS é um programa de monitorização instalado num PC geral e pode monitorizar entre 1 e 3000 equipamentos. Obtém as informações de cada equipamento através da rede e envia-as para o UGW.

Conforme apresentado na Tabela 4 abaixo, a próxima página exibe os dados transferidos, os protocolos (dependendo das opções selecionadas durante o design e a implementação) e as portas utilizadas. Em nenhum momento são transferidos quaisquer dados de imagem de cópia, impressão, digitalização ou fax.

Tabela 4 Visão geral dos dados de e-Maintenance

Descrição	Dados tratados	Protocolo/Porta	Porta
Comunicação entre o e-Maintenance (plug-in de eRDS ou RDS) e UGW	Endereço de serviço Web UGW Endereço do servidor proxy/número da porta da conta proxy/palavra-passe Endereço de e-mail de destino do UGW Endereço do servidor SMTP Endereço do servidor POP Estado do equipamento, contador e informações do modelo Número de série Informações sobre o toner/tinteiro restante Informações de firmware Informação sobre pedido de reparação Informações de registos Chamada de assistência Alarme de assistência Papel encravado Ambiente Registo de condição	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Comunicação entre o e-Maintenance e o equipamento (apenas plug-in de RDS, uma vez que o eRDS se trata de um software incorporado)		SNMP Propriedade da Canon SLP/SLP/HTTPS	UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Content Delivery System

O Content Delivery System (CDS) estabelece uma ligação entre os MFD e o Canon Universal Gateway (UGW). Este fornece atualizações de firmware e de aplicações do equipamento.

Tabela 5 Visão geral dos dados do Content Delivery System

Descrição	Dados enviados	Protocolo/Porta	Porta
Comunicação entre os MFD e o UGW	Número de série do equipamento Versão de firmware Idiomas País Informações relacionadas com o EULA do equipamento	HTTP/HTTPS	TCP/80 TCP/443
Comunicação entre o UGW e o MFD	Ficheiro de teste (dados aleatórios binários) para teste de comunicação Dados binários de firmware ou da aplicação MEAP	HTTP/HTTPS	TCP/80 TCP/443

Um URL de acesso ao CDS específico está predefinido na configuração do equipamento. Caso seja necessário fornecer firmware de equipamentos e gestão de aplicações centralizados a partir da infraestrutura, será necessária uma instalação local do iWMC com o plug-in de atualização de firmware de equipamentos (DFU) e o plug-in de gestão de aplicações de equipamentos.

Kit do operador de suporte remoto

O kit do operador de suporte remoto (RSOK) fornece o acesso remoto ao painel de controlo do equipamento. Este sistema do tipo servidor-cliente é composto por um servidor de VNC executado nos MFP e na aplicação do cliente Visualizador de Operações Remotas de VNC para Microsoft Windows.

Figura 12 Instalação do kit do operador de suporte remoto (RSOK)

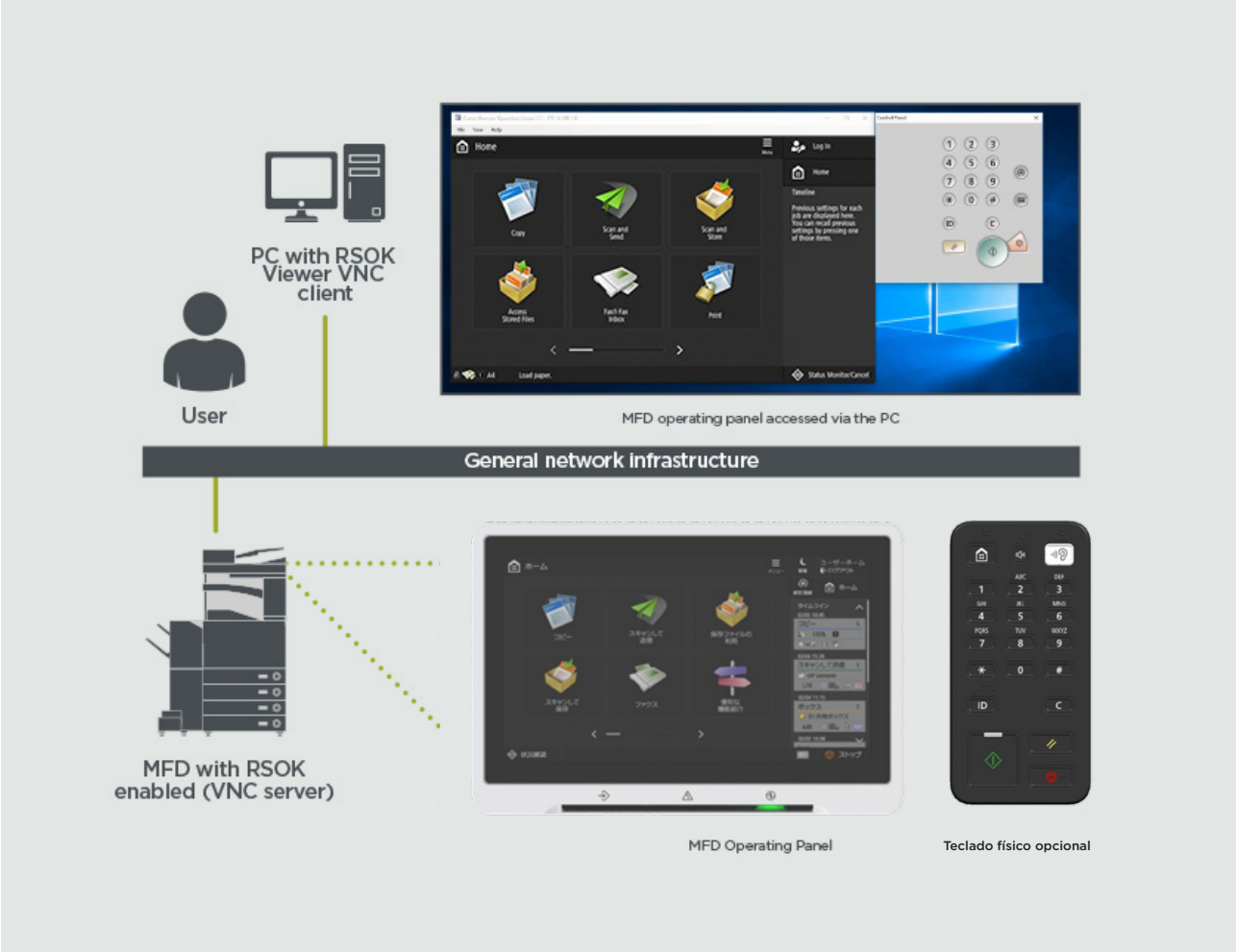


Tabela 6 Visão geral dos dados do kit do operador do suporte remoto

Descrição	Dados enviados	Protocolo/Porta	Porta
Autenticação da palavra-passe do VNC	Palavra-passe do utilizador	Encriptação DES	5900
Visualizador de operações	Painel de controlo do equipamento - dados no ecrã - operação da chave de hardware	Versão 3.3 do protocolo RFB	5900

ANEXO

Funcionalidades relacionadas com a segurança da Canon imageRUNNER ADVANCE

A plataforma imageRUNNER ADVANCE oferece uma configuração remota através de uma interface de serviços Web conhecida como Interface de utilizador remota (RUI). Esta interface concede acesso a muitas das definições de configuração do equipamento e pode ser desativada se não for dada permissão e se não for protegida por palavra-passe para evitar o acesso não autorizado.

Embora a maioria das definições do equipamento esteja disponível através da RUI, é necessário utilizar o painel de controlo do equipamento para definir itens que não possam ser definidos utilizando esta interface. A nossa recomendação é desativar quaisquer serviços não utilizados e reforçar os controlos nos que o assim o requeiram. Para fornecer flexibilidade e suporte, o Kit do operador de serviço remoto (RSOK) concede acesso remoto ao painel de controlo do equipamento. Esta ação é baseada na tecnologia VNC que consiste num servidor (os MFD) e um cliente (um PC da rede). Está disponível um visualizador de cliente específico para PC da Canon que concede acesso simulado às teclas do painel de controlo, quando necessário.

Esta secção apresenta uma visão geral das principais funcionalidades relacionadas com a segurança da série imageRUNNER ADVANCE e das respetivas definições de configuração.

Os Manuais do utilizador online interativos estão disponíveis em https://oip.manual.canon/, fornecendo detalhes que não abrangem apenas as funcionalidades relacionadas com a segurança. Comece por selecionar o tipo de produto adequado (por exemplo, imageRUNNER ADVANCE DX), clique no ícone de pesquisa e introduza os seus critérios de pesquisa. Abaixo estão apresentadas algumas áreas gerais que vale a pena ter em conta.

Gestão do equipamento

Para reduzir a fuga de informações pessoais ou o uso não autorizado, são necessárias medidas de segurança constantes e eficazes. Através da designação de um administrador para gerir as definições do equipamento, a gestão de utilizadores e as definições de segurança podem ser restringidas apenas aos que estão autorizados para tal.

Aceda ao seu navegador Web, introduza a ligação abaixo e insira **configuração do administrador** na caixa de pesquisa. Ao fazê-lo, receberá informações relacionadas com:

- Gestão básica do equipamento
- Limitação de riscos por negligência, erro do utilizador e utilização indevida
- Gestão de equipamentos
- Gestão de configurações e definições do sistema

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

Standard IEEE P2600

Vários modelos da série imageRUNNER ADVANCE estão em conformidade com o IEEE P2600, que é um standard global de segurança de informações para periféricos multifunções e impressoras.

A ligação abaixo descreve os requisitos de segurança definidos no standard IEEE 2600 e como as funções do equipamento satisfazem esses requisitos.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

Autenticação IEEE 802.1X

Quando existe um requisito para se ligar a uma rede 802.1X, o equipamento deve autenticar-se para garantir que se trata de uma ligação autorizada.

Aceda ao seu navegador Web, introduza a ligação abaixo e insira **802.1X** na caixa de pesquisa.
https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

Implementação de uma política de segurança no equipamento

Os últimos modelos imageRUNNER ADVANCE permitem a gestão de segurança em lotes de múltiplos equipamentos, da política de segurança, através da RUI. Pode ser utilizada uma palavra-passe separada, permitindo apenas que o administrador de segurança modifique as definições.

Aceda ao seu navegador Web, introduza a ligação abaixo e insira **Implementação de uma política de segurança no equipamento** na caixa de pesquisa. Ao fazê-lo, receberá informações relacionadas com:

- Utilização de uma palavra-passe para proteger as programações da política de segurança
- Configuração das programações da política de segurança
- Itens de programação da política de segurança

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

Gestão de utilizadores

Os clientes que necessitam de um nível mais elevado de segurança e eficiência podem utilizar a funcionalidade incorporada ou utilizar uma solução de gestão de impressão como o uniFLOW.

Para obter mais informações sobre as nossas soluções de gestão de impressão, contacte os nossos representantes locais ou consulte o folheto do produto uniFLOW.

Configuração das definições de segurança da rede

Os utilizadores autorizados podem incorrer em prejuízos inesperados derivados de ataques de terceiros mal-intencionados, como sniffing, spoofing e adulteração de dados à medida que estes fluem percorrem uma rede. Para proteger as suas informações importantes e valiosas destes ataques, o equipamento suporta várias funcionalidades para aumentar a segurança e a privacidade.

Aceda ao seu navegador Web, introduza a ligação abaixo e insira **Configuração das definições de segurança da rede** na caixa de pesquisa. Ao fazê-lo, receberá informações relacionadas com:

A ligação abaixo apresenta:

- Prevenção do acesso não autorizado
- Ligação a uma LAN sem fios
- Configuração do ambiente de rede

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

Gestão de dados do disco rígido

A unidade de disco rígido do equipamento é utilizada para armazenar o sistema operativo do equipamento, as definições de configuração e as informações do trabalho. A maioria dos modelos de equipamentos fornece encriptação de todo o conteúdo do disco (em conformidade com a norma FIPS 140-2), emparelhando-a com o equipamento específico, impedindo que este seja lido por utilizadores não autorizados. Um chip de segurança MFP da Canon é certificado como um módulo criptográfico no âmbito do Módulo Criptográfico (CMVP) estabelecido pelos EUA e pelo Canadá, bem como do Programa de Validação de Módulo Criptográfico do Japão (JCMVP).

Aceda ao seu navegador Web, introduza a ligação abaixo e insira **Gestão de dados do disco rígido** na caixa de pesquisa.

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

VISÃO GERAL DE PROGRAMAÇÕES DA POLÍTICA DE SEGURANÇA

A terceira geração dos modelos imageRUNNER ADVANCE apresenta as programações da política de segurança e o utilizador de administração de segurança. Isto requer o início de sessão com êxito do Administrador e, se estiver configurado, um início de sessão adicional do Administrador de segurança com uma palavra-passe adicional.

A tabela abaixo apresenta as definições disponíveis.

1. Interface	Notas
Política de ligação sem fios	
Proibir a utilização de ligação direta	<Use Wi-Fi Direct> (Utilizar Wi-Fi Direct) está definido como <Off> (Desligado) Não é possível aceder ao equipamento a partir de dispositivos móveis
Proibir o uso de LAN sem fios	<Select Wired/Wireless LAN> (Selecionar LAN com/sem fios) está definido como <Wired LAN> (LAN com fios) Não é possível estabelecer uma ligação sem fios com o equipamento através de um router ou ponto de acesso LAN sem fios
Política USB	
Proibir a utilização como dispositivo USB	<Use as USB Device> (Utilizar como dispositivo USB) está definido como <Off> (Desligado) Quando a utilização como dispositivo USB estiver proibida, não poderá utilizar as funções de impressão ou de digitalização de computadores ligados através de USB
Proibir a utilização como dispositivo de armazenamento USB	<Use USB Storage Device> (Utilizar dispositivo de armazenamento USB) está definido como <Off> (Desligado) Não é possível utilizar dispositivos de armazenamento USB No entanto, as seguintes funções de serviço ainda funcionam inclusive se a opção "Proibir a utilização como dispositivo de armazenamento USB" esteja LIGADA • Atualização de firmware por unidade USB (a partir do modo de transferência) • Cópia de dados do Sublog do dispositivo para USB (LOG2USB) • Cópia do relatório do dispositivo para USB (RPT2USB)
Política operacional de comunicação de rede Nota: estas definições não se aplicam à comunicação com redes IEEE 802.1X, mesmo que a caixa de verificação esteja selecionada como [Verificar sempre o certificado de servidor ao utilizar TLS]	
Verificar sempre as assinaturas das funções do servidor SMS/WebDAV	Em <SMB Server Settings> (Definições do servidor SMB), as opções <Require SMB Signature for Connection> (Necessária assinatura do SMB para ligação) e <Use SMB Authentication> (Utilizar autenticação do SMB) estão definidas como <On> (Ligado) e <Use TLS> (Utilizar TLS) em <WebDAV Server Settings> (Definições do servidor WebDAV) está definido como <On> (Ligado) Quando o equipamento é utilizado como um servidor SMB ou WebDAV, as assinaturas de certificados digitais são verificadas durante a comunicação
Verificar sempre o certificado de servidor ao utilizar TLS	<Confirm TLS Certificate for WebDAV TX> (Confirmar certificado do TLS para WebDAV TX), <Confirm TLS Certificate for SMTP TX> (Confirmar certificado do TLS para SMTP TX), <Confirm TLS Certificate for POP RX> (Confirmar certificado do TLS para POP RX), <Confirm TLS Certificate for Network Access> (Confirmar certificado do TLS para acesso à rede) e <Confirm TLS Certificate Using MEAP Application> (Confirmar certificado do TLS para utilizar a aplicação MEAP) estão todos definidos como <On> (Ligado), sendo adicionada uma marca de verificação a <CN> (CN) Além disso, as opções <Verify Server Certificate> (Verificar certificado do servidor) e <Verify CN> (Verificar CN) em <SIP Settings> (Definições do SIP) > <TLS Settings> (Definições do TLS) estão definidas como <On> (Ligado) Durante a comunicação TLS, a verificação é realizada para certificados digitais e respetivos nomes comuns
Proibir a autenticação de texto não encriptado para funções de servidor	• <Use FTP Printing> (Utilizar impressão do FTP) em <FTP Print Settings> (Definições de impressão do FTP) está definido como <Off> (Desligado) • <Allow TLS (SMTP RX)> [Permitir TLS (SMTP RX)] em <e-Mail/I-Fax Settings> (Definições de e-mail/I-Fax) <Communication Settings> (Definições de comunicação) está definido como <Always TLS> (Sempre TLS), <Dedicated Port Authentication Method> (Método de autenticação de porta dedicada) em <Network> (Rede) está definido como <Mode 2> (Modo 2), • <Use TLS> (Utilizar TLS) em <WebDAV Server Settings> (Definições do servidor WebDAV) está definido como <On> (Ligado) Ao utilizar o equipamento como servidor, as funções que utilizam autenticação de texto simples não estão disponíveis O TLS será utilizado se a autenticação de texto não encriptado estiver proibida. Além disso, não poderá utilizar aplicações ou funções de servidor, como o FTP, que suportam apenas autenticação de texto não encriptado Pode não ser possível aceder ao equipamento a partir do software ou controlador de gestão de equipamentos
Proibir a utilização de SNMPv1	Em <SNMP Settings> (Definições do SNMP), <Use SNMPv1> (Utilizar SNMPv1) está definido como <Off> (Desligado) Pode não ser possível recuperar ou definir as informações do equipamento a partir do controlador da impressora ou do software de gestão se a utilização de SNMPv1 estiver proibida
Política de utilização de portas	
Restringir porta do LPD	Porta número: 515 <LPD Print Settings> (Definições de impressão do LPD) definidas como <Off> (Desligado) Não é possível efetuar a impressão LPD
Restringir porta de RAW	Porta número 9100 <RAW Print Settings> (Definições de impressão de RAW) definidas como <Off> (Desligado) Não é possível efetuar a impressão de RAW
Restringir porta do FTP	Porta número 21 Em <FTP Print Settings> (Definições de impressão do FTP), <Use FTP Printing> (Utilizar impressão do FTP) está definido como <Off> (Desligado) Não é possível efetuar a impressão do FTP
Restringir porta do WSD	Porta número 3702, 60000 Em <WSD Settings> (Definições do WSD) as opções <Use WSD> (Utilizar WSD), <Use WSD Browsing> (Utilizar opção de pesquisa no WSD) e <Use WSD Scan> (Utilizar opção de digitalização no WSD) estão todas definidas para <Off> (Desligado) Não é possível utilizar as funções do WSD
Restringir porta do BMLinkS	Porta número 1900 Não utilizado na região europeia
Restringir porta do IPP	Porta número 631 Não será possível utilizar Mopria, AirPrint e IPP se a porta IPP estiver restrita

Restringir porta do SMB	Porta número: 137, 138, 139, 445 Em <SMB Server Settings> (Definições do servidor SMB), <Use SMB Server> (Utilizar servidor SMB) está definido como <Off> (Desligado) Não é possível utilizar o equipamento como um servidor SMB
Restringir porta do SMTP	Porta número 25 Em <e-Mail/I-Fax Settings> (Definições de e-mail/I-Fax)> <Communication Settings> (Definições de comunicação), <SMTP RX> (RX SMTP) está definido como <Off> (Desligado) A receção através do SMTP não é possível
Restringir porta dedicada	Porta número: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547 Não poderá utilizar as funções de cópia remota, fax remoto, digitalização remota ou impressão remota, ou aplicações, etc. se a porta dedicada estiver restrita
Restringir a porta de software do operador remoto	Porta número 5900 <Remote Operation Settings> (Definições de operação remota) está definido como <Off> (Desligado) Não é possível utilizar as funções de operação remota
Restringir porta do SIP (IP Fax)	Porta número: 5004, 5005, 5060, 5061, 49152) <Use Intranet> (Utilizar Intranet) em <Intranet Settings> (Definições de Intranet), <Use NGN> (Utilizar NGN) em <NGN Settings> (Definições de NGN) e <Use VoIP Gateway> (Utilizar gateway VoIP) em <VoIP Gateway Settings> (Definições de gateway VoIP) estão todos definidos como <Off> (Desligado) Não é possível utilizar um IP Fax
Restringir porta do mDNS	Porta número 5353 Em <mDNS Settings> (Definições do mDNS), as opções <Use IPv4 mDNS> (Utilizar mDNS IPv4) e <Use IPv6 mDNS> (Utilizar mDNS IPv6) estão definidas como <Off> (Desligado) A opção <Use Mopria> (Utilizar o Mopria) está definida como <Off> (Desligado) Não é possível pesquisar na rede ou executar definições automáticas utilizando o mDNS. Também não é possível imprimir utilizando o Mopria™ ou o AirPrint
Restringir porta do SLP	Porta número 427 Em <Multicast Discovery Settings> (Definições de deteção Multicast), <Response> (Resposta) está definido como <Off> (Desligado) Não é possível pesquisar na rede ou executar definições automáticas utilizando o SLP
Restringir porta do SNMP	Porta número 161 Pode não ser possível recuperar ou definir as informações do equipamento a partir do controlador da impressora ou do software de gestão se a porta SNMP estiver restrita Em <SNMP Settings> (Definições SNMP), as opções <Use SNMPv1> (Utilizar SNMPv1) e <Use SNMPv3> (Utilizar SNMPv3) estão definidas como <Off> (Desligado)

2. Autenticação	Notas
Política operacional de autenticação	
Proibir utilizadores convidados	• <Advanced Space Settings>> (Definições avançadas de espaço) <Authentication Management> (Gestão de autenticação) está definido como <On> (Ligado) • <Login Screen Display Settings> (Definições de visualização do ecrã de início de sessão) está definido como <Display when Device Operation starts> (Apresentar aquando do arranque do equipamento) • <Restrict Job from Remote Device without User Auth> (Restringir trabalho do equipamento remoto sem autorização do utilizador) está definido como <On> (Ligado) Não é possível que os utilizadores não registados iniciem sessão no equipamento. Os trabalhos de impressão enviados a partir de um computador também são cancelados
Forçar a definição do fim de sessão automático	Esta definição destina-se a terminar sessão a partir do painel de controlo, não se aplicando a outros métodos para terminar sessão (intervalo configurável de 10 segundos - 9 minutos) <Auto Reset Time> (Duração de reposição automática) está ativado. O utilizador termina a sessão automaticamente se não forem efetuadas operações durante um período de tempo especificado Selecionar [Time until Logout] (Tempo até terminar sessão) no ecrã de programação da IU remota
Política operacional de palavra-passe	
Proibir o caching de palavra-passe para servidores externos	Esta definição não se aplica a palavras-passe que o utilizador guarda explicitamente, como palavras-passe de livros de endereços, etc. <Prohibit Caching of Authentication Password> (Proibir o caching de palavra-passe de autenticação) está definido como <On> (Ligado) Os utilizadores terão sempre de introduzir uma palavra-passe ao acederem a um servidor externo
Mostrar aviso quando a palavra-passe predefinida estiver a ser utilizada	<Display Warning When Default Password is in use> (Mostrar aviso quando a palavra-passe predefinida estiver a ser utilizada) está definido como <On> (Ligado) Será apresentada uma mensagem de aviso sempre que for utilizada a palavra-passe predefinida de fábrica do equipamento
Proibir a utilização da palavra-passe predefinida para acesso remoto	<Allow Use of Default Password for Remote Access> (Permitir a utilização da palavra-passe predefinida para acesso remoto) está definido como <Off> (Desligado) Não é possível utilizar a palavra-passe predefinida de fábrica ao aceder ao equipamento a partir de um computador
Política de definições de palavra-passe (a política não se aplica à gestão de ID de departamento ou ao PIN)	
Definir o número mínimo de carateres para a palavra-passe	Número mínimo de carateres que pode ser definido entre 1 e 32
Definir o período de validade da palavra-passe	Período de validade definido entre 1 e 180 dias
Proibir a utilização de 3 ou mais carateres consecutivos idênticos	
Forçar a utilização de, pelo menos, 1 caráter em maiúsculas	
Forçar a utilização de, pelo menos, 1 caráter em minúsculas	
Forçar a utilização de, pelo menos, 1 dígito	
Forçar a utilização de, pelo menos, 1 símbolo	
Política de bloqueio	
Ativar o bloqueio	Não se aplica à ID de departamento/PIN da caixa de correio, PIN ou autenticação de impressão segura, etc. Limite de bloqueio: pode ser definido entre 1 e 10 vezes Período de bloqueio: pode ser definido entre 1 e 60 minutos

3. Chave/certificado	Notas
Proibir a utilização de encriptação fraca	Aplica-se a IPSec, TLS, Kerberos, S/MIME, SNMPv3 e LAN sem fios Talvez não consiga estabelecer ligação com os equipamentos que suportem apenas encriptação fraca
Proibir a utilização de chave/certificado com encriptação fraca	Aplica-se a IPSec, TLS e S/MIME Se utilizar uma chave/certificado com encriptação fraca para TLS, passará a usar uma chave/certificado pré-instalado. Não poderá ligar-se se estiver a utilizar uma chave/certificado com encriptação fraca para funções que não as de TLS
Utilize o TPM para guardar a palavra-passe e a chave	Apenas disponível para equipamentos com TPM instalado. Faça sempre uma cópia de segurança das chaves de TPM quando a opção TPM estiver ativada. Consulte o manual do utilizador para obter mais informações Importante quando as definições de TPM estão ativadas: • Certifique-se de que altera a palavra-passe de "Administrador" a partir do valor predefinido, para evitar que terceiros que não o administrador possam fazer uma cópia de segurança da chave de TPM. Se um terceiro utilizar a chave de cópia de segurança de TPM, não poderá restaurar a chave de TPM • Para fins de segurança avançada, a chave de TPM só pode ser criada uma vez. Se as definições de TPM estiverem ativadas, certifique-se de que faz uma cópia de segurança da chave de TPM num dispositivo de memória USB e de que o guarda num local seguro para evitar perdas ou roubos • As funções de segurança fornecidas pelo TPM não garantem a proteção completa dos dados e do hardware

4. Registo	Notas
Forçar a gravação do registo de auditoria	• < Save Operation Log> (Guardar registo de operação) está definido para <On> (ligado) • <Display Job Log> (Apresentar registo de trabalhos) está definido como <On> (Ligado) • <Retrieve Job Log with Management Software> (Recuperar registo de trabalhos com software de gestão) em <Display Job Log> (Apresentar registo de trabalhos) está definido como <Allow> (Permitir) • <Save Audit Log> (Guardar registo de auditoria) está definido como <On> (Ligado) • <Retrieve Network Authentication Log> (Recuperar registo de autenticação de rede) está definido como <On> (Ligado) Os registos de auditoria são sempre registados quando esta definição está ativada
Forçar definições do SNTP	Introduzir endereço do servidor SNTP Em <SNTP Settings> (Definições do SNTP), <Use SNTP> (Utilizar SNTP) está definido como <On> (Ligado). É necessária a sincronização de tempo através do SNTP. Introduzir um valor para [Nome do servidor] no ecrã de programação da IU remota
Gravação de registo no Syslog	Ativar os detalhes de destino do Syslog ao utilizar um servidor Syslog ou SIEM • <Username and password> (Nome de utilizador e palavra-passe) • <SMB Server name> (Nome do servidor SMB) • <Destination path> (Caminho de destino) • <Perform export time> (Executar hora de exportação)

5. Trabalho	Notas
Políticas de impressão	
Proibir a impressão imediata de trabalhos recebidos	Os trabalhos recebidos serão armazenados na memória de fax/I-Fax se a impressão imediata de trabalhos recebidos estiver proibida • <Handle Files with Forwarding Errors> (Processar ficheiros com erros de encaminhamento) está definido como <Off> (Desligado) • <Use Fax Memory Lock> (Utilizar bloqueio de memória de fax) está definido como <On> (Ligado) • <Use I-Fax Memory Lock> (Utilizar bloqueio de memória de I-Fax) está definido como <On> (Ligado) • <Memory Lock End Time> (Hora de fim do bloqueio da memória) está definido como <Off> (Desligado) • <Display Print when Storing from Printer Driver> (Exibir impressão ao armazenar a partir do controlador da impressora) em <Set/Register Confidencial Fax Inboxes> (Definir/Registar caixa de entrada de faxes confidenciais) está definido como <Off> (Desligado) • <Settings for All Mail boxes> > (Definições para todas as caixas de correio) <Print When Storing from Printer Driver> (Imprimir ao armazenar a partir do controlador da impressora) está definido como <Off> (Desligado) • <Box Security Settings>> (Definições de segurança da caixa) <Display Print when Storing from Printer Driver> (Exibir impressão ao armazenar a partir do controlador da impressora) está definido como <Off> (Desligado) • <Prohibit Job from Unknown User> (Proibir trabalho de utilizador desconhecido) está definido como <On> (Ligado) e <Forced Hold> (Suspensão forçada) está definido como <On> (Ligado). A impressão não ocorre imediatamente, mesmo quando as operações de impressão são executadas
Política de envio/receção	
Permitir o envio apenas para endereços registados	Em <Limit New Destination> (Limitar novo destino), as opções <Fax>, <E-mail>, <I-Fax> e <File> (Ficheiro) estão definidas como <On> (Ligado) Só é possível enviar para destinos registados no Livro de endereços
Forçar confirmação do número de fax	Os utilizadores devem inserir novamente um número de fax para confirmação ao enviar um fax
Proibir o encaminhamento automático	<Use Forwarding Settings> (Utilizar definições de encaminhamento) está definido como <Off> (Desligado) Não é possível encaminhar faxes automaticamente

6. Armazenamento	Notas
Forçar eliminação completa dos dados	<Hard Disk Data Complete Deletion> (Eliminação completa dos dados do disco rígido) está definido como <On> (Ligado)

Para obter as especificações completas da série imageRUNNER ADVANCE, consulte o website do produto que se encontra em https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Portugal, S.A.
Rua Alfredo da Silva, 14
Alfragide 2610-016
Amadora
Tel: 214 704 000
Fax: 214 704 002
canon.pt

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Portuguese edition v1.0
Canon Portugal S.A., 2020