Authentication and Access Control Methods

Limiting Access to Print Devices and Documents

Canon offers several authentication options designed so that only approved users can access the imageRUNNER ADVANCE DX, imagePRESS, and imagePRESS Lite devices and their functions, such as print, copy, scan, and send features. These options include embedded[1] methods CAC/PIV/SIPR and RSA Secure ID Token utilizing existing federal agency identity infrastructure. Additionally, the standard Access Management System allows administrators to limit device and/or application features based on the user's role within the organization.

With a long history of advanced print security solutions, Canon's technologies can help you to include print and document management in your Zero Trust strategy.

CAC/PIV/SIPR: Two-factor authentication, FIPS 140-2 validated. Help protect device access and document distribution with optional supported solutions Authorized Send (ASEND), Advanced Authentication (AA CAC), uniFLOW, and FedRAMP® (moderate level) authorized Canon Office Cloud.

RSA SecurID Token: Supported by Authorized Send (ASEND) and Advanced Authentication (AA), utilize your agency-provided RSA SecurID token to access the Canon device and document distribution features.

	Authorized Send (ASEND)	Advanced Authentication (AA)	uniFLOW (Server Based)	Canon Office Cloud
CAC/PIV/SIPR	√	√	√	√
RSA SecurID Token	√	√	-	-
Active Directory	√	√	√	√
PIN Code	-	-	√	√
Proximity Card	-	-	√	√
Product Type	Device Embedded	Device Embedded	Server-based	FedRAMP (moderate level) ATO Cloud-based
Device Lockdown	-	√	√	√
Scan to Self/ Email/Folder	√	N/A	√	√
Scan to SharePoint/ OneDrive	√	N/A	√	FedRAMP authorized destinations
Scan to Teams	-	N/A	√	√
Secured Print[2]	N/A	√	√	√
Role Based Access Control	√	N/A	√	√
Scan to RightFax Server[3]	Optional	N/A	√	Optional-Hybrid Mode
Print from Cloud Storage	√	N/A	√	Not allowed by FedRAMP

[1] Additional cost for solutions referenced in chart.

[2] Authorized Send: MFP driver based Secure Print with PIN per job only; Advanced Authentication: with AA defined authentication.

[3] Scan to RightFax Server requires additional components to enable.

SUPPORTED CANON DEVICES

imageRUNNER ADVANCE Color MFP	imageRUNNER ADVANCE B/W MFP	imagePRESS Lite
C355iF/C255iF	715iF II/715iFZ II/615iF II/615iFZ II/525iF II/525iFZ II	C170/C165
C356iF II/C256iF II	715iF III/715iFZ III/615iF III/615iFZ III/525iF III/525iFZ III	C270/C265
C356iF III/C256iF III	DX 717iF/717iFZ/617iF/617iFZ/527iF/527iFZ	**imagePRESS**
DX C357iF/C257iF	DX 719iF/719iFZ/619iF/619iFZ/529iF/529iFZ	V900/800/700
DX C359iF/359iF	4551i/4545i/4535i/4525i	
C475iF III/C475iFZ III	4551i II/4545i II/4535i II/4525i II	**Supported Smart Cards & Readers**
DX C477iF/C477iFZ	4551i III/4545i III/4535i III/4525i III	All CCID 1.0/CCID 1.1 Compliant Readers
DX C568iF/C568iFZ/C478iF/C478iFZ	DX 4751i/4745i/4735i/4725i	GemPC Twin/GemPC USB SL
C3530i/C3525i	DX 4845i/4835i/4825i	GemPC USB SW/GemPC USB TR
C3530i II/C3525i II	DX 4945i/4935i/4925i	Omnikey 3121
C3530i III/C3525i III	6575i/6565i/6555i	Omnikey 3021
DX C3730i/C3725i	6575i II/6565i II/6555i II	Identiv Cloud 2700F
DX C3835i/C3830i/C3826i	6575i III/6565i III/6555i III	Identiv Cloud 2700R
DX C3935i/C3930i /C3926i	DX 6000i	Identiv SCR 3310 V2
C5560i/C5550i/C5540i/C5535i	DX 6780i/6765i/6755i	Identiv SCR 3311
C5560i II/C5550i II/C5540i II/C5535i II	DX 6870i/6860i/6855i	Identiv SCR 331
C5560i III/C5550i III/C5540i III/C5535i III	DX 6980i	**Supported Smart Cards**
DX C5760i/C5750i/C5740i/C5735i	8505i/8595i/8585i	SafeNet
DX C5870i/C5860i/C5850i/C5840i	8505i II/8595i II/8585i II	Giesecke & Devrient (G&D)
C7580i/C7570i/C7565i	8505i III/8595i III/8585i III	Gemalto
C7580i II/C7570i II/C7565i II	DX 8705i/8795i/8786i	HID Global
C7580i III/C7570i III/C7565i III	DX 8905i/ 8995i/ 8986i	Oberthur
DX C7780i/C7770i/C7765i		

Supported RSA Secure ID Authentication Methods
Username and RSA Token (as passcode)
AD Username and AD Password + RSA Token as passcode
Username and RSA Token (as Passcode) (RSA then associates the username with the AD Account)

For more information please visit usa.canon.com/federal-government.

Canon does not warrant that the use of its features will prevent malicious attacks, or prevent misuse of devices or data or other security issues. Some security features may impact functionality/performance; you may want to test these settings in your environment. Canon products offer certain security features, yet many variables can impact the security of your devices and data. Canon does not warrant that use of its features will prevent security issues. Nothing herein should be construed as legal or regulatory advice concerning applicable laws; customers must have their own qualified counsel determine the feasibility of a solution as it relates to regulatory and statutory compliance.

The authors of this content are not engaged in the rendering of professional advice or services including, without limitation, legal or regulatory advice or services. Individuals and organizations should perform their own research and conduct their own due diligence concerning the products and suggestions discussed herein. Canon U.S.A., Inc. does not make any warranties concerning the accuracy or completeness of the opinions, data, and other information contained in this content and, as such, assumes no liability for any errors, omissions, or inaccuracies therein, or for an individual's or organization's reliance on such opinions, data, or other information.

Canon, imageRUNNER, imagePRESS, and MEAP are registered trademarks of Canon Inc. in the United States and may also be registered trademarks or trademarks in other countries. All other referenced product names and marks are trademarks of their respective owners. Specifications and availability subject to change without notice. Not responsible for typographical errors.

usa.canon.com