

Security Guidebook Function List (Label Printers)

Y: Supported -: Not supported



Security Function	CW-C4000 Series	CW-C6000 CW-C6500 Series	CW-C8000 Series	CW-D6000 CW-D6500 Series	CW-D3800 Series
Network Security					
TLS Communication	Y	Y	Y	Y	Y
TLS1.1	Y	Y	Y	Y	Y
TLS1.2	Y	Y	Y	Y	Y
TLS1.3	-	-	Y	-	-
Controlling Protocol Permissions and Exclusions	Y	Y	Y	Y	Y
IPsec/IP Filtering	Y	Y	Y	Y	Y
IKEv1	Y	Y	Y	Y	Y
IKEv2	Y	Y	Y	Y	Y
ESP: AES-CBC-128/AES-CBC-192/AES-CBC-256/3DES	Y	Y	Y	Y	Y
ESP: AES-GCM-128/AES-GCM-192/AES-GCM-256	Y	Y	Y	Y	Y
ESP/AH: SHA-1/MD5	Y	Y	Y	Y	Y
ESP/AH: SHA-256/SHA-384/SHA-512	Y	Y	Y	Y	Y
IEEE802.1X Authentication	Y	Y	Y	Y	Y
EAP-TLS	Y	Y	Y	Y	Y
PEAP-TLS	Y	Y	Y	Y	Y
PEAP/MSCHAPv2	Y	Y	Y	Y	Y
EAP-TTLS	Y	Y	Y	Y	Y
AES128/AES256/3DES/RC4	Y	Y	Y	Y	Y
SNMP	Y	Y	Y	Y	Y
SNMPv1	Y	Y	Y	Y	Y
SNMPv2c	Y	Y	Y	Y	Y
SNMPv3	Y	Y	Y	Y	Y
SMB	-	-	-	-	-
SMB1.0	-	-	-	-	-
SMB2.0	-	-	-	-	-
SMB3.0	-	-	-	-	-
WPA3	Y	-	Y	-	Y
Separation Between Interfaces	Y	Y	Y	Y	Y
Protecting Your Product					
Block USB Connection from Computer	Y*1	-	Y*1	-	Y*1
Disabling the External Interface	-	-	-	-	-
Handling Viruses Introduced by USB Memory	-	-	-	-	-
Print / Scan Security					
Confidential Jobs	-	-	-	-	-
Anti-Copy Pattern	-	-	-	-	-
Watermark	-	-	-	-	-
PDF Encryption	-	-	-	-	-
S/MIME	-	-	-	-	-
AES-128/AES-192/AES-256/3DES	-	-	-	-	-
SHA-1/SHA-256/SHA-384/SHA-512/MD5	-	-	-	-	-
Domain Restrictions	-	-	-	-	-
Support for Long Authentication Passwords	-	-	-	-	-
Restrictions on File Access from PDL	-	-	-	-	-
Secure Printing	Y	Y	Y	Y	Y
Fax Security					
Direct Dialing Restrictions	-	-	-	-	-
Confirmation of Address List	-	-	-	-	-
Dial Tone Detection	-	-	-	-	-
Measures Against Abandoned Faxes	-	-	-	-	-
Transmission Confirmation Report	-	-	-	-	-
Deleting the Backup Data for Received Faxes	-	-	-	-	-
Limit Sending to Multiple Recipients	-	-	-	-	-
User Data Protection					
Storage Security	-	-	-	-	-
Protecting Your Contacts	-	-	-	-	-
Data Handling Processed by a Product	Y	Y	Y	Y	Y
Encryption of Saved Data in HDD/SSD	-	-	-	-	-
Sequential Deletion of Job Data	-	-	-	-	-
Password Encryption	Y	-	Y	-	Y
TPM	-	-	-	-	-
HDD/SSD Mirroring	-	-	-	-	-
Operational Limitation					
Panel Lock	Y	Y	Y	Y	Y
Access Control	-	-	-	-	-
Authenticated Printing / Scanning	-	-	-	-	-
Password Policy	-	-	-	-	-
Audit Log	Y*1	-	Y*1	-	Y*1
Product Security					
Automatic Firmware Updates	-	-	-	-	-
Protection Against Illegal Firmware Updates	Y	Y	Y	Y	Y
Administrator Password Authentication for Network Updating	Y	Y	Y	Y	Y
HTTPS Data Communication Protection	Y*1	-	Y	-	Y*1
Signature Verifying the Authenticity of F/W Update	-	-	Y	-	-
Secure Boot	-	-	Y	-	-
Malware Infiltration Detection	-	-	Y	-	-
Security Measures When You Dispose of Your Product					
Restore Factory Default	Y	Y	Y	Y	Y
Security Certification and Standards					
ISO15408/IEEE2600.2™	-	-	-	-	-

*1 The feature is only available in Europe, the Middle East, and Africa. For details, see the Cybersecurity Enhancement Supplementary Guide or the product manual.