Epson POS Printer WebAPI Interface Specification

(Application Programming Interfaces (APIs) for device control)

Revision A

TM-m30III
TM-m30III-H
TM-m50II
TM-P20II
TM-P80II

Change Document List

Revision	Date	Notes

Contents

Tables

1. Introduction

"Epson POS Printer WebAPI " (hereafter called "WebAPI") enables developers to make a Solution such as managed print service, print accounting system, etc. WebAPI is based on the HTTP(S) protocol that provides means for the Application to communicate with Epson Imaging Devices. The Browser allows the Application to provide the APIs allow the Application to control Device's functions.

2. Device Configuration

In order to make Services of the Application available, device configuration MUST be completed by the System Integrator using the Application or any other tools in advance. This section helps Application developers configure Devices' settings such as Network Configuration, Administrator Account, Server Connection, and the Access Control.

WebAPI allows the Application to set up Device settings. The Application could send a file described by the Configuration Data Schema to the Device using the /SET API (See the Device Description section and the API section for more information).

Basically, System Integrator can set up selected settings for user as necessary. If the settings are omitted, the default settings in the device are used. However there are several settings in the Device Configuration. The following sections describe Device settings in details.

2.1. Network Environment Settings

Network environment settings are the most fundamental work that is necessary for Devices to join the user's network environment.

WebAPI allows the Application to set up the following fundamental settings related to the network environment. See the Network and Network Security settings in Configuration Data Schema section for more information.

- Wired or Wireless
- IPv4 or IPv6
- Certificate for TLS/SSL
- Date and Time
- SNTP (Optional)
- DNS (Optional)
- IPsec (including IP address or Port filtering) (Optional)
- 802.1X (Optional)

Note: System Integrators should set an IP address for the network environment using connecting Devices with any client directly, in order to make the initial network environment setup on Devices with the factory default settings because IP address in Devices is set to Auto by factory default.

2.2. Administrator Password Settings

Devices have a password for administrators to avoid having some settings changed freely by general users. If the account is set, administrators are only allowed to change the settings with inputting the administrator password.

WebAPI enables administrators to configure the settings using the /SET API. If the password is set to the Device, the Application MUST specify the administrator password in an input parameter of the API.

See the Administration settings in Configuration Data Schema section for more information.

3. Device Description

Device Description is a general concept that encapsulates some aspects of device's properties and functionality such as configuration, device state, job state, and requests. WebAPI defines four data schemas described in the following sub sections. Undefined fields and values on the Data Schemas are reserved for future use.

3.1. Configuration Data Schema

Configuration Data Schema is a set of formats to which the Application MUST conform. It is used when the Application sends data formatted by JSON in order to configure the Device. If there are any unnecessary items to set up for user environment, you can omit the object from the JSON data. All values in Configuration Data Schema are optional.
Note: This schema is used in a request of the /SET API only.

Name	Value type	Value
AdminSettings	object	Administration Settings
ProductSecuritySettings	object	Product Security Settings
SystemSettings	object	System Settings
NetworkSettings	object	Network Settings
NetworkSecuritySettings	object	Network Security Settings
Services	object	Service Settings
Printer Settings	object	Printer Settings

Table 3-1 Configuration Data Schema

3.1.1. Administration Settings

"AdminSettings" consists of one portion "AdminName".

"AdminName" settings can be set as below.

Name	Value type	Value
Name	string	Administrator Name/Contact Information 0 – 255 bytes in UTF-8

Table 3-2 Administration Name Settings

3.1.2. Product Security Settings

"ProductSecurity" consists of one portion "EncryptPassword".

"EncryptPassword" settings can be set as below.

Name	Value type	Value
EncryptPassword	int	Password Encrypt Setting 0 : Disable 1 : Enable

Table 3-3 Encrypt Password Settings

3.1.3. System Settings

"SystemSettings" consists of one portion "DateAndTime".

"DateAndTime" settings can be set as below.

Name	Value type	Value
DateFormat	int	Date Format 0 : MMDDYYYY 1 : YYYYMMDD 2 : DDMMYYYY

TimeFormat	int	Time Format 0 : 12h 1 : 24h
TimeDifference	int	Time Difference UTC -12:45 - +13:45 (in unit of time equal to 15min) -51 – 55 (-1 means -15min, +1 means +15min)
UseTimeServer	int	Use Time Server (SNTP) 0 : Do Not Use 1 : Use
TimeServerAddr	string	Time Server (SNTP) Address IPv4, IPv6, FQDN When “UseTimeServer” is Do Not Use, this item is unnecessary.
UpdateInterval	int	Update Interval(min) 1 – 10080 When “UseTimeServer” is Do Not Use, this item is unnecessary.

Table 3-4 Date and Time Settings

3.1.4. Network Settings

“NetworkSettings” consists of three portions, “Basic”, “WiredLAN”, and “WiFi”.

“Basic” settings can be set as below.

Name	Value type	Value
DeviceName	string	Printer Name 2 – 15 characters in ASCII
Location	string	Location 0 – 127 bytes in UTF-8
ObtainIPAddr	int	Obtain IP Address 0 : Auto 1 : Manual
BOOTPSetting	int	Set using BOOTP 0 : Disable 1 : Enable When “ObtainIPAddr” is Manual, this item is unnecessary.
APIPASetting	int	Obtain IP address using Automatic Private IP Addressing(APIPA) 0 : Disable 1 : Enable When “ObtainIPAddr” is set to Manual, this item is unnecessary.
IPAddr	string	IP Address(IPv4) IPv4 format When “ObtainIPAddr” is set to Auto, this item is unnecessary.
SubnetMask	string	Subnet Mask IPv4 format When “ObtainIPAddr” is set to Auto, this item is unnecessary.
DefaultGateway	string	Default Gateway IPv4 format When “ObtainIPAddr” is set to Auto, this item is unnecessary.
DNSServerSetting	int	DNS Server Setting 0 : Auto 1 : Manual
PrimaryDNS	string	Primary DNS Server IPv4 format When “DNSServerSetting” is set to Auto, this item is unnecessary.
SecondaryDNS	string	Secondary DNS Server IPv4 format When “DNSServerSetting” is set to Auto, this item is unnecessary.

DNSHostSetting	int	DNS Host Name Setting 0 : Manual 1 : Auto
DNSDomainSetting	int	DNS Domain Name Setting 0 : Manual 1 : Auto
DNSDomain	string	DNS Domain Name 2 – 249 characters in ASCII When “DNSDomainSetting” is set to Auto, this item is unnecessary.
RegisterToDNS	int	Register the network interface address to DNS 0 : Disable 1 : Enable
ProxyServerSetting	int	Proxy Server Setting 0 : Do Not Use 1 : Use
ProxyServer	string	Proxy Server IPv4 or FQDN format When “ProxyServerSetting” is Do Not Use, this item is unnecessary.
ProxyPort	int	Proxy Server Port Number 0 – 65535 When “ProxyServerSetting” is Do Not Use, this item is unnecessary.
ProxyUserName	string	Proxy Server User Name 0 – 255 bytes in ASCII When “ProxyServerSetting” is Do Not Use, this item is unnecessary.
ProxyPassword	string	Proxy Server Password 0 – 255 bytes in ASCII When “ProxyServerSetting” is Do Not Use, this item is unnecessary.
IPv6Setting	int	IPv6 Setting 0 : Disable 1 : Enable
IPv6PrivacyExtension	int	IPv6 Privacy Extension 0 : Disable 1 : Enable When “IPv6Setting” is set to Disable, this item is unnecessary.
IPv6DHCP	int	IPv6 DHCP Server Setting 0 : Do Not Use 1 : Use When “IPv6Setting” is set to Disable, this item is unnecessary.
IPv6Addr	string	IPv6 Address IPv6 format When “IPv6Setting” is set to Disable, this item is unnecessary.
IPv6DefaultGateway	string	IPv6 Default Gateway IPv6 format When “IPv6Setting” is set to Disable, this item is unnecessary.
IPv6PrimaryDNS	string	IPv6 Primary DNS IPv6 format When “IPv6Setting” is set to Disable, this item is unnecessary.
IPv6SecondaryDNS	string	IPv6 Secondary DNS IPv6 format When “IPv6Setting” is set to Disable, this item is unnecessary.
PowerSaving_WiFi	int	Wi-Fi power saving settings 0 : Disable 1 : Enable

WirelessBand	int	Wireless Band Setting 0 : Auto 1 : 2.4GHz 2 : 5Ghz
IPAddressPrint	int	IP Address Print Setting 0 : Disable 1 : Enable

Table 3-5 Network Basic Settings

"WiredLAN" settings can be set as below.

Name	Value type	Value
LinkSpeed	int	Link Speed & Duplex 0 : Auto (In this mode, the Device can communicate with all of the communication speeds including 1000BASE-T) 1 : 10BASE-T Half 2 : 10BASE-T Full 3 : 100BASE-T Half 4 : 100BASE-T Full
IEEE8023AZ	int	IEEE802.3az setting 0 : Disable 1 : Enable

Table 3-6 Wired LAN Settings

"WiFi" settings can be set as below.

Name	Value type	Value
WiFiEnable	int	Wi-Fi Enable 0 : Disable(Wired LAN Enable) 1 : Enable
ConnectionMode	int	Connection Mode 0 : Infrastructure 1 : Adhoc When "WiFiEnable" is set to Disable, this item is unnecessary.
SSID	string	SSID 1 – 32 characters in ASCII When "WiFiEnable" is set to Disable, this item is unnecessary.
SecuritySetting	int	Security Level 0 : None 1 : WEP64 2 : WEP128 3 : TKIP 4 : AES 5 : WPA None 6 : WEP Unknown 7 : WPA2-Enterprise 9 : Unknown When "WiFiEnable" is set to Disable, this item is unnecessary.
SecurityKey	string	Security Key 0, 5, 8 – 63 characters in ASCII When "WiFiEnable" is set to Disable, this item is unnecessary.

Table 3-7 Wired LAN Settings

3.1.5. Network Security Settings

"NetworkSecuritySettings" consists of four portions, settings "SSLTLS", "IPsecIPFiltering", "IEEE8021X" and "CACertificate".

"SSLTLS" consist of two portions, settings "Basic" and "ServerCertificate".
"Basic" settings can be set as below.

Name	Value type	Value
EncryptionStrength	int	Encryption Strength 0 : 80bit 1 : 112bit 2 : 128bit 3 : 192bit 4 : 256bit
RedirectToHTTPS	int	Redirect HTTP to HTTPS 0 : Disable 1 : Enable
TLS1_0	int	TLS1.0 0 : Disable 1 : Enable
TLS1_1	int	TLS1.1 0 : Disable 1 : Enable

Table 3-8 SST/TLS Basic Settings

"ServerCertificate" settings can be set as below.

Name	Value type	Value
UseCert	int	Which Certificate is used for Server Certificate 1 : Self-signed Certificate 2 : CA-signed Certificate
CASignedCert	string	CA-signed Certificate Max 5k bytes in ASCII When "UserCert" is set to "CA-signed Certificate", this item MUST be necessary.
CASignedCertKey	string	Key of CA-signed Certificate Max 5k bytes in ASCII When "UserCert" is set to "CA-signed Certificate", this item MUST be necessary.
CSR	string	CSR Max 5k bytes in ASCII
CSRKey	string	Key of CSR Max 5k bytes in ASCII
CACert1	string	Certificate of CA-signed Certificate issuer Max 5k bytes in ASCII
CACert2	string	Certificate of CACert 1 issuer Max 5k bytes in ASCII
SelfSignedCert	string	Self-signed Certificate Max 5k bytes in ASCII
SelfSignedCertKey	string	Key of Self-signed Certificate Max 5k bytes in ASCII

Table 3-9 SST/TLS Server Certificate Settings

"IPsecIPFiltering" consist of two portions, settings "Basic" and "ClientCertificate".
"Basic" settings can be set as below.

Name	Value type	Value
IPsecFiltering	int	IPsec/IP Filtering 0 : Disable 1 : Enable This item is required to apply the "IPsecIPFiltering Basic Settings" settings to the Device.
AccessControl	int	Access Control 0 : Permit Access 1 : Refuse Access 2 : IPsec When "IPsecFiltering" is set to Enable, this item is required.
IkeVersion	int	IKE Version 1 : IKEv1 2 : IKEv2 When "Access Control" is set to IPsec, this item is required.
AuthMethod	int	Authentication Method 0 : Pre-Shared Key 1 : Certificate When "Access Control" is set to IPsec, this item is required.
PreSharedKey	string	Pre-Shared Key 1 – 127 character in ASCII When "AuthMethod" is set to Pre-Shared Key, this item is required.
LocalIdType	int	ID Type for Local Authentication 1 : Distinguished Name 2 : IP Address 3 : FQDN 4 : Email Address 5 : Arbitrary String When "IkeVersion" is set to 2 (IKEv2), this item is required.
LocalId	string	The string of the ID for Local Authentication. The allowed value depends on the value of LocalIdType. 1 (Distinguished Name) : ASCII 1 – 255 characters (It must contain '='). 2 (IP Address) : IPv4 or IPv6 address. 3 (FQDN) : ASCII (Alphanumeric, dot, hyphen) 1 – 255 characters. 4 (Email Address) : ASCII 1 – 255 characters (It must contain '@' and must not contain '=') 5 (Arbitrary String) : ASCII 1 – 255 characters. When "IkeVersion" is set to 2 (IKEv2), this item is required.
RemoteAuthMethod	int	Authentication Method for Remote Authentication 0 : Pre-Shared Key 1 : Certificate When "IkeVersion" is set to 2 (IKEv2), this item is required.
RemoteIdType	int	ID Type for Remote Authentication 1 : Distinguished Name 2 : IP Address 3 : FQDN 4 : Email Address 5 : Arbitrary String When "IkeVersion" is set to 2 (IKEv2), this item is required.

RemoteId	string	The string of the ID for Remote Authentication. The allowed value depends on the value of LocalIdType. 1 (Distinguished Name) : ASCII 1 – 255 characters (It must contain '='). 2 (IP Address) : IPv4 or IPv6 address. 3 (FQDN) : ASCII (Alphanumeric, dot, hyphen) 1 – 255 characters. 4 (Email Address) : ASCII 1 – 255 characters (It must contain '@' and must not contain '=') 5 (Arbitrary String) : ASCII 1 – 255 characters. When "IkeVersion" is set to 2 (IKEv2), this item is required.
RemotePreSharedKey	string	Pre-Shared Key for Remote Authentication. 1 – 127 character in ASCII When "IkeVersion" is set to 2 (IKEv2), this item is required.
Encapsulation	int	Encapsulation 0 : Transport Mode 1 : Tunnel Mode When "Access Control" is set to IPsec, this item is required.
RemoteGateway	string	Remote Gateway(Tunnel Mode) IPv4 or IPv6 Address When "Encapsulation" is set to Tunnel Mode, this item is required.
SecurityProtocol	int	Security Protocol 0 : ESP 1 : AH When "Access Control" is set to IPsec, this item is required.
IKEv1EncAlgo	int	Encryption Algorithm for IKEv1 1 : AES-CBC-128 2 : AES-CBC-192 3 : AES-CBC-256 7 : 3DES 0 : Any When "IkeVersion" is set to 1 (IKEv1), this item is required.
IKEv2EncAlgo	int	Encryption Algorithm for IKEv2 1 : AES-CBC-128 2 : AES-CBC-192 3 : AES-CBC-256 4 : AES-GCM-128 5 : AES-GCM-192 6 : AES-GCM-256 7 : 3DES 0 : Any When "IkeVersion" is set to 2 (IKEv2), this item is required.
IKEv1AuthAlgo	int	Authentication Algorithm for IKEv1 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When "IkeVersion" is set to 1 (IKEv1), this item is required.
IKEv2AuthAlgo	int	Authentication Algorithm for IKEv2 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When "IkeVersion" is set to 2 (IKEv2), this item is required.

IKEv1KeyExcAlgo	int	Key Exchange Algorithm for IKEv1 X : DH Group X (X=1, 2, 5, 14 – 26) 0 : Any When "IkeVersion" is set to 1 (IKEv1), this item is required.
IKEv2KeyExcAlgo	int	Key Exchange Algorithm for IKEv2 X : DH Group X (X=1, 2, 5, 14 – 30) 0 : Any When "IkeVersion" is set to 2 (IKEv2), this item is required.
ESPEncAlgo	int	Encryption Algorithm for ESP 1 : AES-CBC-128 2 : AES-CBC-192 3 : AES-CBC-256 4 : AES-GCM-128 5 : AES-GCM-192 6 : AES-GCM-256 7 : 3DES 0 : Any When "SecurityProtocol" is set to ESP, this item is required.
ESPAuthAlgo	int	Authentication Algorithm for ESP 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When "SecurityProtocol" is set to ESP, this item is required.
AHAuthAlgo	int	Authentication Algorithm for AH 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When "SecurityProtocol" is set to AH, this item is required.
GroupPolicy	array	GroupPolicy can have up to 10 policies and the format of the array content is described in Table 3-11 Format of GroupPolicy.

Table 3-10 IPsecIPFiltering Basic Settings

Name	Value type	Value
EnableGroupPolicy	int	Enables this Group Policy 0 : Disable 1 : Enable This item is required to apply the "GroupPolicy" settings,.
AccessControl	int	Access Control 0 : Permit Access 1 : Refuse Access 2 : IPsec When "EnableGroupPolicy" is set to Enable, this item is required.
IkeVersion	int	IKE Version 1 : IKEv1 2 : IKEv2 When "AccessControl" is set to IPsec, this item is required.
LocalAddr	string	Local Address (Printer) IPv4 or IPv6 Address When "EnableGroupPolicy" is set to Enable, this item is required.

RemoteAddr	string	Remote Address (Host) IPv4 or IPv6 Address When “EnableGroupPolicy” is set to Enable, this item is required.
ChoosingPortMethod	int	Method of Choosing Port 0 : Service Name 1 : Port Number When “EnableGroupPolicy” is set to Enable, this item is required.
ServiceName	array	Service Name String of IPsec target function is input in array. Max 10 [“Any”, “ENPC”, “SNMP”, “LPR”, “RAW”, “IPP”, “WSD”, “WSDiscovery”, “NWScan”, “NWPushScan”, “NWPushScanDiscovery”, “FTPDataLocal”, “FTPControlLocal”, “FTPDataRemote”, “FTPControlRemote”, “CIFSLocal”, “CIFSRemote”, “HTTPLocal”, “HTTPSLocal”, “HTTPRemote”, “HTTPSRemote”, “NBNameLocal”, “NBDatagramLocal”, “NBSessionLocal”, “NBNameRemote”, “NBDatagramRemote”, “NBSessionRemote”] When “ChoosingPortMethod” is set to Server Name, this item is required.
TransportProtocol	int	Transport Protocol 0 : Any Protocol 1 : TCP 2 : UDP 3 : ICMPv4 When “ChoosingPortMethod” is set to Port Number, this item is required.
LocalPort	string	Local Port 0 – 60 characters in ASCII When “TransportProtocol” is set to TCP or UDP, this item is required.
RemotePort	string	Remote Port 0 – 60 characters in ASCII When “TransportProtocol” is set to TCP or UDP, this item is required.
AuthMethod	int	Authentication Method 0 : Pre-Shared key 1 : Certificate When “Access Control” is set to IPsec, this item is required.
PreSharedKey	string	Pre-Shared Key 1 – 127 characters in ASCII When “AuthMethod” is set to Pre-Shared Key, this item is required.
LocalIdType	int	ID Type for Local Authentication 1 : Distinguished Name 2 : IP Address 3 : FQDN 4 : Email Address 5 : Arbitrary String When “IkeVersion” is set to 2 (IKEv2), this item is required.

LocalId	string	The string of the ID for Local Authentication. The allowed value depends on the value of LocalIdType. 1 (Distinguished Name) : ASCII 1 – 255 characters (It must contain '='). 2 (IP Address) : IPv4 or IPv6 value. 3 (FQDN) : ASCII(Alphanumeric, dot, hyphen) 1 – 255 characters. 4 (Email Address) : ASCII 1 – 255 characters (It must contain '@' and must not contain '=') 5 (Arbitrary String) : ASCII 1 – 255 characters. When "IkeVersion" is set to 2 (IKEv2), this item is required.
RemoteAuthMethod	int	Authentication Method for Remote Authentication 0 : Pre-Shared Key 1 : Certificate When "IkeVersion" is set to 2 (IKEv2), this item is required.
RemoteIdType	int	ID Type for Remote Authentication 1 : Distinguished Name 2 : IP Address 3 : FQDN 4 : Email Address 5 : Arbitrary String When "IkeVersion" is set to 2 (IKEv2), this item is required.
RemoteId	string	The string of the ID for Remote Authentication. The allowed value depends on the value of LocalIdType. 1(Distinguished Name) : ASCII 1 – 255 characters (It must contain '='). 2(IP Address) : IPv4 or IPv6 value. 3(FQDN) : ASCII(Alphanumeric, dot, hyphen) 1 – 255 characters. 4(Email Address) : ASCII 1 – 255 characters (It must contain '@' and must not contain '=') 5(Arbitrary String) : ASCII 1 – 255 characters. When "IkeVersion" is set to 2 (IKEv2), this item is required.
RemotePreSharedKey	string	Pre-Shared Key for Remote Authentication. 1 – 127 character in ASCII When "IkeVersion" is set to 2 (IKEv2), this item is required.
Encapsulation	int	Encapsulation 0 : Transport Mode 1 : Tunnel Mode When "Access Control" is set to IPsec, this item is required.
RemoteGateway	string	Remote Gateway (Tunnel Mode) IPv4 or IPv6 When "Encapsulation" is set to Tunnel Mode, this item is required.
SecurityProtocol	int	Security Protocol 0 : ESP 1 : AH When "Access Control" is set to IPsec, this item is required.
IKEv1EncAlgo	int	Encryption Algorithm for IKEv1 1 : AES-CBC-128 2 : AES-CBC-192 3 : AES-CBC-256 7 : 3DES 0 : Any When "IkeVersion" is set to 1 (IKEv1), this item is required.

IKEv2EncAlgo	int	Encryption Algorithm for IKEv2 1 : AES-CBC-128 2 : AES-CBC-192 3 : AES-CBC-256 4 : AES-GCM-128 5 : AES-GCM-192 6 : AES-GCM-256 7 : 3DES 0 : Any When “IkeVersion” is set to 2 (IKEv2), this item is required.
IKEv1AuthAlgo	int	Authentication Algorithm for IKEv1 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When “IkeVersion” is set to 1 (IKEv1), this item is required.
IKEv2AuthAlgo	int	Authentication Algorithm for IKEv2 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When “IkeVersion” is set to 2 (IKEv2), this item is required.
IKEv1KeyExcAlgo	int	Key Exchange Algorithm for IKEv1 X : DH Group X (X=1, 2, 5, 14 – 26) 0 : Any When “IkeVersion” is set to 1 (IKEv1), this item is required.
IKEv2KeyExcAlgo	int	Key Exchange Algorithm for IKEv2 X : DH Group X (X=1, 2, 5, 14 – 30) 0 : Any When “IkeVersion” is set to 2 (IKEv2), this item is required.
ESPEncAlgo	int	Encryption Algorithm for ESP 1 : AES-CBC-128 2 : AES-CBC-192 3 : AES-CBC-256 4 : AES-GCM-128 5 : AES-GCM-192 6 : AES-GCM-256 7 : 3DES 0 : Any When “SecurityProtocol” is set to ESP, this item is required.
ESPAuthAlgo	int	Authentication Algorithm for ESP 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When “SecurityProtocol” is set to ESP, this item is required.
AHAuthAlgo	int	Authentication Algorithm for AH 1 : SHA-1 2 : SHA-256 3 : SHA-384 4 : SHA-512 5 : MD5 0 : Any When “SecurityProtocol” is set to AH, this item is required.

Table 3-11 Format of GroupPolicy

"ClientCertificate" settings can be set as below.

Name	Value type	Value
ClientCert	string	Client Certificate Max 5k bytes in ASCII
ClientCertKey	string	Key of Client Certificate Max 5k bytes in ASCII
CSR	string	CSR Max 5k bytes in ASCII
CSRKey	string	Key of CSR Max 5k bytes in ASCII
CACert1	string	Certificate of Client Certificate issuer Max 5k bytes in ASCII
CACert2	string	Certificate of CACert1 issuer Max 5k bytes in ASCII

Table 3-12 IPsecIPFiltering Client Certificate Settings

"IEEE8021X" consist of two portions, settings "Basic" and "ClientCertificate".
"Basic" settings can be set as below.

Name	Value type	Value
EnableIEEE8021X	int	IEEE802.1X(Wired LAN) 0 : Disable 1 : Enable EnableIEEE802.1X is effective against IEEE802.1X working on the wired LAN. If you want to enable WPA2-Enterprise ((EEE802.1X(Wi-Fi)), the following WiFiEnable MUST be set to 1 (Enable) and SecuritySetting MUST be set to 7 (WPA2-Enterprise).
EAPType	int	EAP Type 0 : EAP-TLS 1 : PEAP-TLS 2 : PEAP/MSCHAPv2
UserID	string	User ID 0 – 128 bytes in ASCII
Password	string	Password 1 – 128 bytes in ASCII When "EAPType" is not set to PEAP/MSCHAPv2, this item is unnecessary.
ServerID	string	Server ID 0 – 128 bytes in ASCII
EnableCertValidate	int	Enables Certificate validation 0 : Disable 1 : Enable
AnonymousName	string	Anonymous Name 0 – 128 bytes in ASCII When "EAPType" is EAP-TLS, this item is unnecessary.
EncryptionStrength	int	Encryption Strength 1 : Medium 2 : High
WiFiEnable	int	Wi-Fi Enable 0 : Disable(Wired LAN Enable) 1 : Enable Same as WiFiEnable of NetworkSettings > WiFi
ConnectionMode	int	Connection Mode 0 : Infrastructure 1 : Adhoc Same as ConnectionMode of NetworkSettings > WiFi

SSID	string	SSID 1 – 32 characters in ASCII Same as SSID of NetworkSettings > WiFi
SecuritySetting	int	Security Level 0 : None 1 : WEP64 2 : WEP128 3 : TKIP 4 : AES 5 : WPA None 6 : WEP Unknown 7 : WPA2-Enterprise 9 : Unknown Same as SecruitySetting of NetworkSettings > WiFi

Table 3-13 IEEE802.1X Basic Settings

"ClientCertificate" settings can be set as below.

Name	Value type	Value
ClientCert	string	Client Certificate for identification of Device Max 5k bytes in ASCII
ClientCertKey	string	Key of Client Certificate Max 5k bytes in ASCII
CSR	string	CSR Max 5k bytes in ASCII
CSRKey	string	Key of CSR Max 5k bytes in ASCII
CACert1	string	Certificate of Client Certificate issuer Max 5k bytes in ASCII
CACert2	string	Certificate of CACert1 issuer Max 5k bytes in ASCII

Table 3-14 IEEE802.1X Client Certificate Settings

"CACertificate" settings can be set as below.

Name	Value type	Value
CACert1	string	CA Certificate 1 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert2	string	CA Certificate 2 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert3	string	CA Certificate 3 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert4	string	CA Certificate 4 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert5	string	CA Certificate 5 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert6	string	CA Certificate 6 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert7	string	CA Certificate 7 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert8	string	CA Certificate 8 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert9	string	CA Certificate 9 for peer verification. (Root certificate) Max 5k bytes in ASCII
CACert10	string	CA Certificate 10 for peer verification. (Root certificate) Max 5k bytes in ASCII

Table 3-15 CA Certificate Settings

3.1.6. Service Settings

“Services” consists of four portions, "Protocol", "MSNetwork, "NetworkScan" and "WiFiDirect".

“Protocol” settings can be set as below.

Name	Value type	Value
UseBonjour	int	Use Bonjour 0 : Do Not Use 1 : Use
BonService		Use Bonjour 0 : Do Not Use 1 : Use
BonPProtocol		Top Priority Protocol 0 : IPP 1 : Port9100
WideAreaBonjour		Wide-Area Bonjour 0 : Disable 1 : Enable
EnableiBeaconTransmission	int	Enable iBeacon Transmission 0 : Disable 1 : Enable
EnableUPnP	int	Enable UPnP 0 : Disable 1 : Enable
EnableSLP	int	Enable SLP 0 : Disable 1 : Enable
EnableWSD	int	Enable WSD 0 : Disable 1 : Enable
WSDPrintTimeout	int	WSD Printing Timeout(sec) 3 - 3600 When "EnableWSD" is set to Disable, this item is unnecessary.
WSDScanTimeout	int	WSD Scanning Timeout(sec) 3 - 3600 When "EnableWSD" is set to Disable, this item is unnecessary.
EnableWSDSecurePrint	int	WSD Secure Print 0 : Disable 1 : Enable
EnableLLTD	int	Enable LLTD 0 : Disable 1 : Enable
EnableLLMNR	int	Enable LLMNR 0 : Disable 1 : Enable
AllowLPRPrint	int	Allow LPR Port Printing 0 : Not Allowed 1 : Allowed
LPRPrintTimeout	int	LPR Printing Timeout(sec) 0 - 3600 When "AllowLPRPrint" is set to Not Allowed, this item is unnecessary.
AllowRAWPrint	int	Allow RAW(Port9100) Printing 0 : Not Allowed 1 : Allowed
RAWPrintTimeout	int	RAW(Port9100) Printing Timeout(sec) 0 - 3600 When "AllowRAWPrint" is set to Not Allowed, this item is unnecessary.

AllowRAWCustomPrint	int	Allow RAW(Custom) Printing 0 : Not Allowed 1 : Allowed
RAWCustomPortNumber	int	Port number of custom RAW. 1024 - 65535
RAWCustomPrintTimeout	int	RAW(Custom) Printing Timeout(sec) 0 - 3600 When "AllowRAWCustomPrint" is Not Allowed, this item is unnecessary.
EnableIPP	int	Enable IPP 0 : Disable 1 : Enable
AllowNonSecure	int	Allow Non-secure Communication 0 : Not Allowed 1 : Allowed When "EnableIPP" is set to Disable, this item is unnecessary.
IPPTimeout	int	IPP Printing Timeout(sec) 3 - 3600 When "EnableIPP" is set to Disable, this item is unnecessary.
PINCodeRequired		Require PIN Code when using IPP printing 0 : No 1 : Yes When "EnableIPP" is set to Disable, this item is unnecessary.
EnableFTPServer	int	Enable FTP Server 0 : Disable 1 : Enable
FTPTimeout	int	FTP Communication Timeout(sec) 0 - 3600 When "EnableFTPServer" is set to Disable, this item is unnecessary.
EnableSNMPv1	int	Enable SNMPv1/v2c 0 : Disable 1 : Enable
EnableSNMPv1Only	int	Enable SNMPv1 0 : Disable 1 : Enable
EnableSNMPv2cOnly	int	Enable SNMPv2c 0 : Disable 1 : Enable
AccessAuthority	int	Access Authority 0 : Read Only 1 : Read/Write When "EnableSNMPv1" is set to Disable, this item is unnecessary.
ReadOnlyCommunity	string	Community Name(Read Only) 0 - 32 characters in ASCII When "EnableSNMPv1" is set to Disable, this item is unnecessary.
ReadWriteCommunity	string	Community Name(Read/Write) 0 - 32 characters in ASCII When "EnableSNMPv1" is set to Disable, this item is unnecessary.
AllowAccessFromEpsonTools	int	Allow Access by Epson Tools 0 : Not Allowed 1 : Allowed
EnableSNMPv3	int	Enable SNMPv3 0 : Disable 1 : Enable

UserName	string	User Name 1 - 32 bytes in UTF-8 When "EnableSNMPv3" is set to Disable, this item is unnecessary.
AuthAlgorithm	int	Authentication Algorithm 0 : MD5 1 : SHA-1 When "EnableSNMPv3" is set to Disable, this item is unnecessary.
AuthPassword	string	Authentication Password 8 - 32bytes in ASCII When "EnableSNMPv3" is set to Disable, this item is unnecessary.
EncryptAlgorithm	int	Encryption Algorithm 0 : DES 1 : AES128 When "EnableSNMPv3" is set to Disable, this item is unnecessary.
EncryptPassword	string	Encryption Password 8 - 32 bytes in ASCII When "EnableSNMPv3" is set to Disable, this item is unnecessary.
ContextName	string	Context Name 0 - 32 bytes in UTF-8 When "EnableSNMPv3" is set to Disable, this item is unnecessary.
EnableEPOSPrint	int	Enable ePOS-Print 0 : Disable 1 : Enable
EPOSPrtDeviceID	string	Device ID 1 - 30 characters A-Z, a-z, 0-9, -, _, .

Table 3-16 Protocol Settings

"WiFiDirect" settings can be set as below.

Name	Value type	Value
DisableWiFiD	int	Used to change the availability of the Wi-Fi Direct settings on the Panel 0 : Disable (Locked) 1 : Enable (Unlocked)
WiFiDirectEnable	int	Enable or Disable Wi-Fi Direct 0 : Disable 1 : Enable
ObtainIPAddr	int	Obtain Method of IP Address 0 : Auto 1 : Manual
IPAddr	string	IP Address(IPv4) IPv4 format(ex. "127.0.0.1") When "ObtainIPAddr" is Auto, this item is unnecessary.
Password	string	Password 8 - 22 characters in ASCII.
SSID	string	SSID 10 - 22 characters in ASCII. It must contain "DIRECT-" at the begining.

Table 3-17 WiFi Direct Settings

3.1.7. Printer Settings

"PrinterSettings" consists of the "PrinterBasic".

"PrinterBasic" settings can be set as below.

Name	Value type	Value
PaperReduction	int	Setting for Paper Reduction 0 : Max 1 : Recommended 2 : Nothing
PrintSpeed	int	Setting for Print Speed 0 - 12
PrintDensity	int	Setting for Print Density 1 : 70% 2 : 75% 3 : 80% 4 : 85% 5 : 90% 6 : 95% 7 : 100% 8 : 105% 9 : 110% 10 : 115% 11 : 120% 12 : 125% 13 : 130%
CommandExecution	int	Setting for Comannd Execution during offline 0 : Disable 1 : Enable
PowerSaveFunc	int	Setting for Power saving function for USB 0 : Enable Power Saving 1 : Disable Power Saving
Buzzer	int	Setting for Buzzer 0 : Disable 1 : Enable
ErrorOccur	int	Number of rings when an error occurs 0 : Does not ring 1 : Ring once 65535 : Endless
AutoPaperCut	int	When automatic paper cut activates 0 : Does not ring 1 : Ring once
PaperEnd	int	When paper end occurrs 0 : Does not ring 1 : Ring once
BatteryLevel	int	When battery level changed 0 : Does not ring 1 : Ring once
SpecifiedPulse1	int	When specified pulse 1 (2 pin) occurs 0 : Does not ring 1 : Ring once
SpecifiedPulse2	int	When specified pulse 2 (5 pin) occurs 0 : Does not ring 1 : Ring once

Table 3-18 Printer Basic Settings

4. APIs

This section describes the WebAPIs that are exposed to the Application in order for them to operate Devices. The APIs enable the Application to take advantage of the device features such as configure device settings.

4.1. Request

All of the APIs use the Request-Line on the HTTP request message as below.

Elements	Allowed value
Method	POST
Request-URI	Identifies a resource on each API described on subsequent subsections. It may contain a query string in the URI according to each API specification. (e.g. /SET?admin_password=xxxxxx)
HTTP-Version	"HTTP/1.1"
Request Header fields	Comply with RFC 2616. If the message body contains the content, the HTTP client MUST identify the Content-Type depending on the data as below. Content-Type: **application/json; charset=UTF-8**

Table 4-1 Request Message

Here's an example HTTP request.

----- begin ---

1:POST /PRESENTATION/ADVANCED/SETTING/SET?admin_password=xxxxxxx HTTP/1.1

*Method, *Request-URI, *Query String, *HTTP-Version

2:Host: 192.0.2.1

3:Connection: keep-alive

4:Content-Length: 2078

5:Content-Type: application/json

*Content-Type

6:User-Agent: Mozilla/5.0

8:

9:{

"NetworkSettings":{

"Basic":{

"PrinterName":"ISVPrinter",

"Location":"building",

"obtainIPAddr":1,

"BOOTPSettings":0,

"APIPASettings":0,

"IPAddr":"192.168.1.100",

"SubnetMask":"255.255.255.0",

"DefaultGateway":"192.168.1.1",

……

}

*Message Body (JSON)

----- end ---

4.2. Response

All of the APIs use the Status-Line on the HTTP response message as below.

Elements	Allowed value
HTTP-Version	"HTTP/1.1"
Status-Code and Reason-Phrase	"200" OK "400" Bad Request "404" Not Found "500" Internal Server Error
Response Header fields	Comply with RFC 2616. If Status-Code is 200 OK, the Device returns the following fields. Pragma: no-cache Cache-Control: no-cache Content-Type: **application/json; charset=UTF-8**

Table 4-2 Response Message

Here's an example HTTP response.

----- begin ---

1:HTTP/1.1 200 OK

*HTTP-Version, *Status-Code, *Reason-Phrase

2:Pragma: no-cache

3:Cache-Control: no-cache

4:Connection: keep-alive

5:Content-Length: 893

6:Content-Type: application/json; charset=UTF-8

*Content-Type

7:

8:{

"result":"success"

}

*Message Body (JSON)

----- end ---

4.3. Error response

Errors are returned from APIs in the following format by JSON in a 200 (OK) response.

Name	Value type	Value
result	string	Indicates the error reason defined by each API.

Table 4-3 API Error Response

4.4. Basic API

The Basic APIs enable the Application to provide some features such as configure device settings.

4.4.1. /SET

This API is used to configure device settings related to the entire features provided by the Device, for example, network environment, Access Control, certificate for security communication, admin account, etc.
The Application MUST call the /SET API to configure device settings using the configuration data formatted by JSON including an Access Token of WebAPI.
This is an HTTP POST request.

Note: The Application can set all fields supported by the Device in Configuration Data Schema using this API regardless of the selected Platform Version. If the Application sets fields that the Device does not support, the Device ignores those fields.

4.4.1.1. Input

The /SET API has input parameters as below.

Query String	Comments
admin_password	If an account of administrators is set to the Device, a password for the account MUST be set.

The message body should contain the configuration data by JSON.

Message Body	Comments
Configuration Data (JSON)	JSON data which is created based on the Configuration Data Schema. See the Configuration Data Schema section for more information.

Table 4-4 Input of /SET

4.4.1.2. Return

The /SET API returns JSON including following data.

Name	Value type	Value
result	string	Indicate the API acceptance result.

Table 4-5 Return value of /SET

Example:

```
{
  "result":"success"
}
```

4.4.2. /GET

This API is used to get device settings related to the entire features provided by the Device.
Either admin_password or access_token must be present.

4.4.2.1. Input

The /GET API has input parameters as below.

Query String	Comments
admin_password	A password of the administrator account if it is set to the Device,

4.4.2.2. Return

The /GET API returns JSON including the following data.

Name	Value
	Indicate the API acceptance result.
Configuration Data (JSON)	JSON data which is created based on the Configuration Data Schema. See the Configuration Data Schema section for more information.

Table 4-6 Return value of /GET

<Left Blank>