EPSON
EXCEED YOUR VISION

Epson Device Admin

Security White Paper

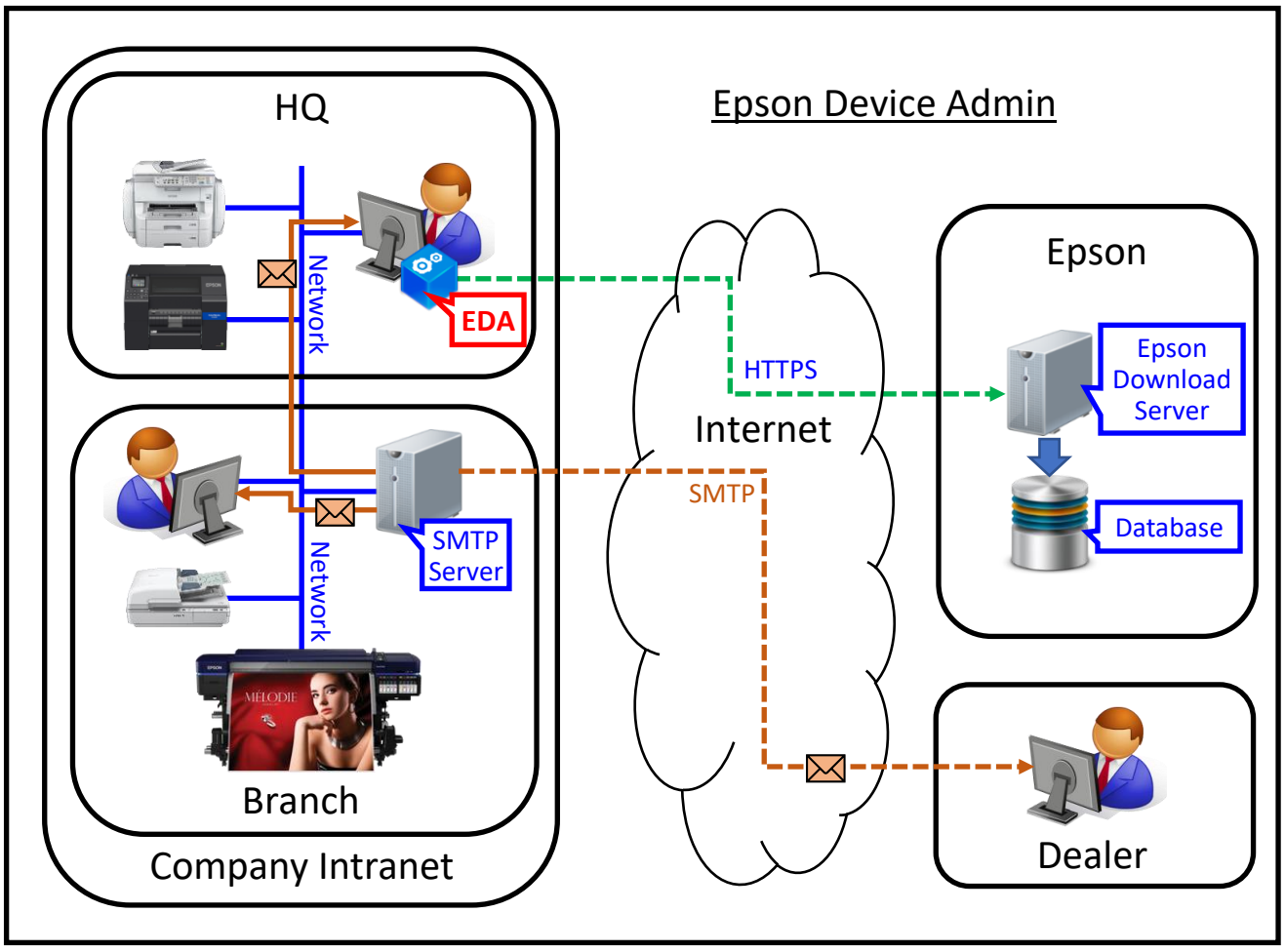
Contents

Epson Device Admin

Overview and Terminology

Epson Device Admin (EDA) is an application that helps you to manage, discover, monitor, and configure devices. The devices can be anywhere in the world if EDA can reach them within the Intranet.

See the chart below for an overview.



EDA needs to access the SMTP server to send emails for its Alert and Report functions. If it can be reached from EDA, the SMTP server does not have to be on the Intranet.

The latest versions of EDA and necessary firmware are stored in the Epson Download Server's Database. EDA needs to access the Internet to download these files from the Epson Download Server.

Epson Device Admin

This document is intended to provide information about various aspects of security so that you can feel secure using EDA. The user is responsible for building and maintaining the optimum security environment to use EDA, while Epson's role is limited to providing information.

Be sure to use the latest version of EDA to ensure the optimum security.

Device Registration

EDA provides two ways to register devices. The first is Discovery in the Device menu. This function discovers devices on the network and registers all of the found devices. The second is Add in the Device menu. This function allows you to specify and find the device you want to register.
Unless otherwise stated, the information in this chapter applies to both of these methods.
This chapter explains the network protocols used to discover devices. When EDA finds devices that can be registered, it automatically starts collecting data from the found devices; this process is explained in the Data Collection chapter. EDA adds the found devices to its device list and stores the updated device list and all of the data collected in its database.

Network Protocols

The following tables provide the network protocols and ports used by EDA to discover devices.

Discovery function

Protocol	Port	IN/OUT	Description
SLP (UDP)	427	OUT	Discovers devices using multicast.
ENPC (UDP)	3289	OUT	Discovers devices using multicast.

Add function

Protocol	Port	IN/OUT	Description
DNS (UDP)*1	53	OUT	Converts the host name to an IP address.
NBNS (UDP)*1	137	OUT	Converts the host name to an IP address.
LLMNR (UDP)*1	5355	OUT	Converts the host name to an IP address.
ICMP	N/A	OUT	Checks if the target device is active.

*1: These are used only when Host Name is specified to add a device to the device list.

See the Appendix for the complete list of network protocols and ports used by EDA.

Security

The Discovery function searches for devices using the specified IP Addresses, IP Address Ranges, and Network Addresses, as well as the same network segment as the computer on which EDA is running. EDA does not search other network addresses.

Data Collection

EDA offers several functions that collect data from devices, such as Discovery, Update Device Information, Alerts, and Reports.
Unless otherwise stated, the information in this chapter applies to all of the above.

Network Protocols

The following table provides the network protocols and ports used by EDA to collect device data.

Protocol	Port	IN/OUT	Description
DNS (UDP)*1	53	OUT	Converts the host name to an IP address.
NBNS (UDP)*1	137	OUT	Converts the host name to an IP address.
LLMNR (UDP)*1	5355	OUT	Converts the host name to an IP address.
ENPC (UDP)	3289	OUT	Collects device data.
SNMP (UDP)	161	OUT	Collects device data.
IS (TCP)*2	1865	OUT	Collects device data.

*1: These are used only when Host Name is specified to add a device to the device list.
*2: This is used only for scanners.

See the Appendix for the complete list of network protocols and ports used by EDA.

Data Collected

The type of device data that is collected by EDA depends on the model, accessories, configuration, usage status, and the EDA function that is being used.
See the Appendix for more information about the device data collected by EDA.

Security

EDA collects device data only from the devices registered in EDA's device list and stores the collected device data in its database. It does not collect any data from non-registered devices or computers.
EDA does not collect user's data, such as images of prints, copies, scans, or sent/received faxes.

Configuration

EDA provides two ways to configure devices. The first is to configure one device at a time. The second is to apply a configuration template to multiple devices in a batch.
Unless otherwise stated, the information in this chapter applies to both of these methods.

Network Protocols

The following table provides the network protocols and ports used by EDA to configure devices.

Protocol	Port	IN/OUT	Description
DNS (UDP)*1	53	OUT	Converts the host name to an IP address.
NBNS (UDP)*1	137	OUT	Converts the host name to an IP address.
LLMNR (UDP)*1	5355	OUT	Converts the host name to an IP address.
ENPC (UDP)	3289	OUT	Collects/updates device settings.
SNMP (UDP)	161	OUT	Collects/updates device settings.
HTTPS (TCP)	443	OUT	Collects/updates device settings.
LPR (TCP)*2	9100	OUT	Collects/updates device settings.

*1: These are used only when Host Name is specified to add a device to the device list.
*2: This is used only for label printers.

See the Appendix for the complete list of network protocols and ports used by EDA.

Security

EDA can configure only the devices specified by the user from EDA's device list. It does not configure any unspecified devices or devices not registered in EDA's device list.

Email

EDA can email alert notifications using the Alerts functions and reports using the Reports functions.
Unless otherwise stated, the information in this chapter applies to both of these methods.
EDA uses the specified SMTP server, which does not have to be in the user's Intranet, to send email.

Network Protocols

The following table provides the network protocols and ports used by EDA to send email.

Protocol	Port	IN/OUT	Description
SMTP (TCP)	25*1	OUT	Sends email. STARTTLS encryption is available. Authenticates users using SMTP Auth.
POP3 (TCP)	110	OUT	Authenticates users using POP before SMTP.

*1: This port number is the default and can be changed. Port 587 is commonly used for STARTTLS. Be sure to use the same port number that the SMTP Server uses.

See the Appendix for the complete list of network protocols and ports used by EDA.

Security

SMTP is the protocol used to send emails without encryption, and STARTTLS encryption is disabled by default on EDA.
When STARTTLS encryption is enabled, EDA performs an unencrypted check to see if the email server supports STARTTLS. If it is supported, emails are sent to the server using SSL/TLS encryption. If it is not supported, emails are sent without encryption. Emails reach their recipients by passing through several servers and the above process is applied to each instance of communication between the servers. Although there is no way to guarantee that all of the communications between the servers are encrypted, emails sent by EDA only contain information about devices and do not contain any sensitive, personal, or confidential information.

You can select 'SMTP Auth' and 'POP before SMTP' methods for the email server to only allow authenticated users to send emails.

See the SSL/TLS section in the Appendix for more information on SSL/TLS.

Software Updates

Network Protocols

The following table provides the network protocols and ports used by EDA to update its own software.

Protocol	Port	IN/OUT	Description
HTTPS (TCP)	443 or 8080*1	OUT	Checks if a new version of EDA is available on the Epson Download Server. Downloads the new version of EDA from the Epson Download Server.

*1: When a proxy server is not specified, port 443 is used.
When a proxy server is manually specified, port 8080 is the default but can be changed.
When the system's proxy server is specified, its port number is used.

See the Appendix for the complete list of network protocols and ports used by EDA.

Security

The Epson Download Server always provides the latest version of EDA. When "Check for software update at startup" for EDA is enabled, EDA checks if a new version is available during startup and prompts the user to perform an update when one is available. When the user agrees, the EDA file is downloaded by HTTPS, and EDA will run the update.

Any data transmitted over the Internet between the client (EDA) and the server (Epson Download Server) is secured. See the SSL/TLS section in the Appendix for more information on HTTPS.

Firmware Updates

Network Protocols

The following table provides the network protocols and ports used by EDA to update the firmware of a device.

Protocol	Port	IN/OUT	Description
HTTPS (TCP)*1	443 or 8080*2	OUT	Checks if a new version of the firmware is available on the Epson Download Server. Downloads the new version of the firmware from the Epson Download Server.
HTTP (TCP)*3	80	OUT	Updates the firmware of a device.
HTTPS (TCP)*3	443	OUT	Updates the firmware of a device.
SNMP (UDP)	161	OUT	Collects device data.

*1: Firmware can be downloaded from the Epson Download Server or loaded from the local PC.
This protocol is not used when firmware is loaded from the local PC.
*2: When a proxy server is not specified, port 443 is used.
When a proxy server is manually specified, port 8080 is the default but can be changed.
When the system's proxy server is specified, its port number is used.
*3: The protocol used depends on the target model.

See the Appendix for the complete list of network protocols and ports used by EDA.

Security

The Epson Download Server always provides the latest version of the firmware. When "Check for software update at startup" for firmware is enabled, EDA checks if a new version is available during startup. When you click Check Updates in the Devices menu, EDA checks if a new version is available immediately. When a new version of the firmware for the device is available, EDA displays the new icon to the left of the firmware version for the device. When the user selects to download the firmware, the firmware file is downloaded by HTTPS, and EDA sends the file to the target device. After receiving the file, the device thoroughly scans the file. Once the device has confirmed that the file is the correct module provided by Epson, the device updates its firmware and reboots. EDA then collects device data, including the firmware version, from the device to confirm that the firmware update has been completed successfully.

Any data transmitted over the Internet between the client (EDA) and the server (Epson Download Server) is secured. See the SSL/TLS section in the Appendix for more information on HTTPS.

Status Sheet Printing

Network Protocols

The following table provides the network protocols and ports used by EDA to print status sheets for the device.

Protocol	Port	IN/OUT	Description
SNMP (UDP)	161	OUT	Prints status sheets for a device.

Security

EDA can print status sheets only for the devices specified by the user from EDA's device list. It does not print status sheets for any unspecified devices or devices not registered in EDA's device list.

Embedded Web Server

Network Protocols

The following table provides the network protocols and ports used by EDA to launch the Embedded Web Server for a device.

Protocol	Port	IN/OUT	Description
HTTPS (TCP)	443	OUT	Launches the Embedded Web Server for a device.

Security

EDA can launch the Embedded Web Server only for a device specified by the user from EDA's device list. It does not launch the Embedded Web Server for any unspecified devices or devices not registered in EDA's device list.

LDAP

Network Protocols

The following table provides the network protocols and ports used by EDA to retrieve user information from the LDAP server.

Protocol	Port	IN/OUT	Description
LDAP (TCP)	389*1	OUT	Retrieves the Epson Print Admin Serverless user information from the LDAP server. STARTTLS and SSL/TLS encryption is available.

*1: This port number is the default and can be changed. The default port 389 is commonly used for STARTTLS, and port 636 is commonly used for SSL/TLS. Be sure to use the same port number that the LDAP server uses.

Security

You can specify the LDAP settings, including the port number, server address, and authentication method, on EDA.
No encryption is the default setting for the LDAP connection, but SSL/TLS and STARTTLS can be selected for secure communication.
When SSL/TLS is selected, all communication between EDA and the LDAP server is encrypted with SSL/TLS if the server supports SSL/TLS. If it does not, no communication is made.
When STARTTLS is selected, EDA performs an unencrypted check to see if the LDAP server supports STARTTLS. If it is supported, all subsequent communication between EDA and the LDAP server is encrypted with SSL/TLS. If it is not supported, communication between EDA and the LDAP server is not encrypted.

In addition to Anonymous authentication method, you can also select Simple and Kerberos authentication methods for the LDAP server that allow only authenticated users to access the system.

See the SSL/TLS section in the Appendix for more information on SSL/TLS.

Database

Network Protocols

The following table provides the network protocols and ports used by EDA to access its own database.

Protocol	Port	IN/OUT	Description
HTTPS (TCP)	10015*1	N/A	Accesses EDA's database on the same computer.

*1: This port number is the default and can be changed only during installation.
If other programs are using this port, select another available port to avoid port conflict.

The protocol and port are used only on the same computer and there is no incoming/outgoing communication.

Security

EDA uses the SQLite database to save various kinds of data, such as device list, group/view settings, collected device data, Alerts settings, email alert history, configuration history, configuration templates, Reports settings, report archives, and all of the settings in the Options menu.
Downloaded firmware is temporarily saved in the database and removed after the firmware update is complete.
EDA's Backup/Restore functions are to backup/restore the entire database, which is useful when you need to move EDA from one computer to another.
EDA creates its database on the same computer and EDA uses the above network protocol and port to access its database on the same computer. There is no incoming/outgoing communication.

Epson Download Server

URLs

The following table provides the URLs for the Epson Download Server for EDA to update itself or firmware.

URL	IP Address	Description
https://download.ebz.epson.net/...	N/A	Allows EDA to check if a new version of EDA or firmware is available. Provides EDA with one of the following URLs for download.
https://download2.ebz.epson.net/... https://download3.ebz.epson.net/... https://download4.epson.biz/...	N/A	Allows EDA to download the newest version of EDA or firmware.

IP addresses for the URLs above are dynamically assigned by Akamai Technologies for optimum performance. The IP address ranges are undefined.

Appendix

Data Collected

The following table provides the data collected from devices by EDA.

Category	Data Item
Device	Manufacturer
	Model
	IP address
	MAC address
	Serial number
	Firmware version
Usage	Status
	Error/warning code
	Page counters for the combinations of color/mono and simplex/duplex for each paper size.
	Page counters for each function.
	Scanner counters.
	Amounts remaining for the following consumables: Ink, toner, maintenance unit, OPC, transfer unit, transfer belt, fuser, and other parts
	Replacements for the following consumables: Ink, toner, maintenance unit, OPC, transfer unit, transfer belt, fuser, and other parts
	Settings for the network, print, scan, fax, power, and finisher.
	Other device specific miscellaneous counters and settings.

The type of device data in the table above that is collected by EDA depends on the model, accessories, configuration, usage status, and the EDA function that is being used.

Network Protocols and Ports

The following table provides the complete list of network protocols and ports used by EDA.

Protocol	Port	IN/OUT	Description
DNS (UDP)[*1]	53	OUT	Converts the host name to an IP address.
NBNS (UDP)[*1]	137	OUT	Converts the host name to an IP address.
LLMNR (UDP)[*1]	5355	OUT	Converts the host name to an IP address.
ICMP	N/A	OUT	Checks if the target device is active.
SLP (UDP)	427	OUT	Discovers devices using multicast.
ENPC (UDP)	3289	OUT	Discovers devices using multicast. Collects device data. Collects/updates device settings. ENPC is an Epson proprietary protocol and stands for Epson Network Peripheral Control.
SNMP (UDP)	161	OUT	Collects device data. Collects/updates device settings. Prints status sheets for a device.
IS (TCP)[*2]	1865	OUT	Collects device data. IS is an Epson proprietary protocol and stands for Internet Scan.
HTTPS (TCP)	443	OUT	Collects/updates device settings. Launches the Embedded Web Server for a device.
LPR (TCP)[*3]	9100	OUT	Collects/updates device settings.
SMTP (TCP)	25[*4]	OUT	Sends email. STARTTLS encryption is available. Authenticates users using SMTP Auth.
POP3 (TCP)	110	OUT	Authenticates users using POP before SMTP.
HTTPS (TCP)[*5]	443 or 8080[*6]	OUT	Checks if a new version of EDA or firmware is available on the Epson Download Server. Downloads the new version of EDA or firmware from the Epson Download Server.
HTTP (TCP)[*7]	80	OUT	Updates the firmware of a device.
HTTPS (TCP)[*7]	443	OUT	Updates the firmware of a device.
LDAP (TCP)	389[*8]	OUT	Retrieves the Epson Print Admin Serverless user information from the LDAP server. STARTTLS and SSL/TSL encryption is available.
HTTPS (TCP)	10015[*9]	N/A	Accesses EDA's database on the same computer.

Appendix

*1: These are used only when Host Name is specified to add a device to the device list.
*2: This is used only for scanners.
*3: This is used only for label printers.
*4: This port number is the default and can be changed. Port 587 is commonly used for STARTTLS. Be sure to use the same port number that the SMTP server uses.
*5: Firmware can be downloaded from the Epson Download Server or loaded from the local PC.
This protocol is not used when firmware is loaded from the local PC.
*6: When a proxy server is not specified, port 443 is used.
When a proxy server is manually specified, port 8080 is the default but can be changed.
When the system's proxy server is specified, its port number is used.
*7: The protocol used depends on the target model.
*8: This port number is the default and can be changed. The default port 389 is commonly used for STARTTLS, and port 636 is commonly used for SSL/TLS. Be sure to use the same port number that the LDAP server uses.
*9: This port number is the default and can be changed only during installation.
If other programs are using this port, select another available port to avoid port conflict.

Encryption Algorithms

The following table provides the list of encryption algorithms used by EDA.

Algorithms	Symmetric/ Asymmetric	Key Length	Description
AES	Symmetric	128 bits	Encrypts confidential data, mainly password information, for network communication.
AES	Symmetric	256 bits	Encrypts PRDF files and firmware files. Encrypts various kinds of password information in the Options menu to store data in the EDA database.
RC4	Symmetric	128 bits	Encrypts the EDA database. This algorithm is used to maintain compatibility with older versions of EDA.
Triple DES	Symmetric	168 bits	Encrypts the password information in the configuration file. This algorithm is used to maintain compatibility with older versions of EDA.

SSL/TLS

Other than email, only HTTPS is used for all EDA communication over the Internet, which is to download new versions of EDA and firmware from the Epson Download Server. HTTPS is the secure version of HTTP (Hypertext Transfer Protocol). The 'S' at the end of HTTPS stands for 'Secure'. HTTPS is often used for online banking or shopping to protect confidential information. HTTPS uses a Secure Socket Layer (SSL) also known as Transport Layer Security (TLS). SSL/TLS is the standard security technology for establishing an encrypted link between a client and a server. For EDA's HTTPS over the Internet, the client is EDA and the server is the Epson Download Server. All of the data transmitted using HTTPS is secure, protected, and guaranteed.

EDA can be configured to use SSL/TLS for email and LDAP communication as well.

EDA 4.18 and later versions support up to TLS 1.3, and EDA 4.17 supports up to TSL 1.2.

Network Traffic

The amount of network traffic for a full data collection is roughly up to 80 KB per device, depending on the model, accessories, configuration, agent type, and usage status. The performance depends on the network environment.

Trademarks

- EPSON and EXCEED YOUR VISION are registered trademarks of Seiko Epson Corporation.
- Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.
- Other product names may be trademarks or registered trademarks of their respective owners.