Power Grids

EDS500 series - Ethernet and DSL Switches
Security Deployment Guideline Release 2
User manual
Revision

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>08/2019</td>
<td>Initial version for Release 2.1</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>7.5</td>
<td>Firmware update via Web Interface</td>
<td>34</td>
</tr>
<tr>
<td>8</td>
<td>Glossary</td>
<td>35</td>
</tr>
</tbody>
</table>
1 Device Description

The EDS500 managed switches have been designed as multilayer switch and multi-purpose communication device specifically for tasks of the process data communication. The devices are employed for the data communication in future-oriented energy networks, for remote meter reading, remote monitoring and control when feeding renewable energy into Smart Grids.

Switching technologies are crucial to network design, as they allow traffic to be sent only where it is needed, using fast, hardware-based methods. A standard switch is known as a layer 2 switch and is commonly found in nearly any LAN. Managed switches require advanced technology and are more expensive, and thus are usually only found in larger LANs or in special network environments.
2 Secure Access

2.1 Secure System Setup

The goal of network security is to provide confidentiality, integrity and authenticity:

- Confidentiality (keeping the data secret from the unintended listeners on the network)
- Integrity (ensuring that the received data is the data was actually sent)
- Authenticity (providing the identity of the endpoint to ensure that the end point is the intended entity to communicate with)

For secure operation of the EDS500 managed switches according this guide, it is necessary to distinguish between two communication channels:

- User data communication
- Device management

The first item describes the possibilities of the EDS500 managed switches to protect the data traffic between two terminal devices against external attacks. The second item describes the possibilities to securely monitor and manage the EDS500 managed switches from a control center.

2.2 Device Management

The EDS500 managed switches support secure protocols and functions by default. This means that the factory setting of the device corresponds to the current ABB cyber security standards.

There can be contradictions between functionality and security if, for example, the control center uses a protocol that is not secure (e.g. SNMP v1).

2.2.1 Telnet used for Configuration

With the help of a Telnet client program the management console can be accessed.

References:
- Details on the Telnet configuration can be found under EDS500 Manual - Part 2: Configuration via Telnet.

Default configuration:
- In default configuration Telnet is disabled.

Recommendation for secure configuration:
- Telnet has to be disabled in a secure configuration.

Disable Telnet:
- <set telnet no enable>

ADVICE

Telnet is considered as unsecure protocol.
Telnet has to be disabled in a secure configuration. Telnet is disabled by default.

2.2.2 SSH used for Configuration

The command line interface (CLI) can be accessed with the help of a SSH client program.
References:
Details on the SSH interface can be found under EDS500 Manual - Part 2: Configuration via SSH.

Default configuration:
In default configuration SSH is enabled.

Recommendation for secure configuration:
SSH is recommended for CLI.

Enable SSH port:
<set system ssh enable>

2.2.3 TFTP used for Configuration

The Trivial File Transfer Protocol (TFTP) is a very simple file transfer protocol. TFTP only supports reading or writing files. The EDS500 managed switches uses TFTP to transfer for example firmware, config files and certificates from and to the device.

References:
Details on the TFTP configuration can be found under EDS500 Manual - Part 2: Configuration via TFTP.

Default configuration:
The TFTP transmission has to be started with the command line interface (CLI) (via serial terminal, Telnet or SSH), via the web interface or via SNMP.

Recommendation for secure configuration:
Do not use TFTP in a secure configurations.
Alternative:
Configure the device via secure web interface.

Disable/enable TFTP port:
The TFTP transmission has to be started with the command line interface (CLI) (via serial terminal, Telnet or SSH), via the web interface or via SNMP.

ADVICE
TFTP is considered as unsecure protocol. TFTP uses transmission in plain text. Transmissions can thus be listened to and manipulated.

Do not use TFTP in a secure configuration.

2.2.4 HTTP and HTTPS used for Configuration

The EDS500 managed switches provide a web-based interface for configuration. The web interface can be uses with common web browsers like Mozilla Firefox, Opera, Apple Safari, Google Chrome or Microsoft Internet Explorer.

The EDS500 series Web server access is protected by authentication and with secure HTTPS communication.

References:
Details on the HTTP and HTTPS configuration can be found under EDS500 Manual - Part 2: Handling in the Web Interface.

Default configuration:
The Web-Server is activated with the configuration HTTP with redirection to HTTPS.
Recommendation for secure configuration:
Use HTTPS only for configuration.

<set system web-server enable only-https>

Commands to configure the web interface
<set system web-server enable [http-and-https | no-https | only-https | redirect-to-https]>
<set system web-server no enable>
<set system web-server port {1-65536}>
<set system web-server secure-port {1-65536}>
<set system web-server session-timeout {...}>

If the web-server is disabled the corresponding ports are closed.

**ADVICE**

HTTP is considered as unsecure protocol.
Enable HTTPS in secure configurations. HTTPS is enabled by default.

2.2.5 SNMP Network Management for configuration

SNMP (Simple Network Management Protocol) is intended for the central monitoring and control of network devices.

The EDS500 managed switches support SNMP in the versions SNMPv1, SNMPv2c and SNMPv3.

References:
Details of the SNMP network management can be found under EDS500 Manual - Part 2: SNMP Network management.

Default configuration:
In the default configuration SNMP is disabled.

Recommendation for secure configuration:
Use SNMPv3 for Network management:
<set system snmp version v3-only>

Commands to activate/deactivate the SNMP agent:
<set system snmp {{enable [read-only | read-write]} | {no enable}}>
<set system snmp enable>
<set system snmp enable read-write>
<set system snmp enable read-only>
<set system snmp no enable>
<set system snmp version {any | v3-only}>
<show system snmp>

**ADVICE**

SNMPv1 and SNMPv2 are considered as unsecure protocols.
SNMPv1 and SNMPv2 have to be disabled in a secure configuration. SNMP is disabled by default. If required enable only SNMPv3.
2.2.6 **Syslog and Device Internal Log**

EDS500 managed switches store information messages in an internal event storage. If there is synchronization with a time server (NTP server), the time stamp with date and time is used, otherwise the current system uptime is used as time stamp.

The event log can be displayed as follows:
- at the command line interface (CLI)
- at the web interface where it is also available as text file

Commands to use the internal device logs

```
<show log>
<clear log>
```

Logged events can be distributed to up to 10 Syslog servers in the network. There the messages can be processed and evaluated.

References:
- Details on the Syslog configuration can be found under EDS500 Manual - Part 2: Syslog and device internal Log.

Default configuration:
- Client mode - n/a

Recommendation for secure configuration:
- Activate ABB CSA events (CSA: Common Security Architecture) if ABB management software is used (SDM600).

Commands to configure Syslog:

```
<set system syslog server {IP address} {{0-7} | abb-security-events}>
<c当地 system syslog server {IP address}>
<show system syslog>
<debug system syslog testmessage {{IP address}}>
```

2.2.7 **IEC 60870-5-104**

For monitoring purposes the EDS500 managed switches can serve a telecontrol central office according to IEC 60870-5-104 as well as IEC 60870-5-101. The functionality is similar to SNMP Network monitoring.

The device can be assigned an ASDU address and be included as station into the telecontrol monitoring according to IEC 60870-5-104 or 60870-5-101. It is possible to monitor the device and interface state and supervise the communication network from the control center.

References:
- Details on the IEC 60870-5-104 configuration can be found under EDS500 Manual - Part 2: IEC 60870-5-101 and IEC 60870-5-104.

Default configuration:
- In default configuration IEC 60870-5-104 and IEC 60870-5-101 is disabled.

Recommendation for secure configuration:
- Use SNMPv3 for monitoring instead of IEC 60870-5-104.

Commands to activate / deactivate an IEC 60870-5-101 / IEC 60870-5-104 interface

```
<set {iec101 | iec104} interface {1 | 2} no shutdown>
<set {iec101 | iec104} interface {1 | 2} shutdown>
```
2.3 User Data Communication

The EDS500 managed switches do not encrypt data communication like VPN. This point of view is also supported by the ISO/IEC 27001 standard. Thus, the devices are intended for use in private networks. For networks in particular with connection to the public Internet, additional configurations are required to increase protection and privacy for the EDS500 Ethernet communication. This requirement could be fulfilled by a secure Virtual Private Network (VPN) configured with external devices.

<table>
<thead>
<tr>
<th>ADVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the use of the EDS500 devices in networks with internet connection, the communication must be additionally secured (e. g. with VPN).</td>
</tr>
</tbody>
</table>

Some EDS500 services are disabled by default. Some are considered insecure, but can still be useful in certain applications. An overview can be found in the next chapters.

The EDS500 managed switches have functions that prevent or mitigate external attacks on the network. These include, for example, the rate limiter and the VLAN function, which intercept packet storms and prevent forwarding to critical subnets by separating the network.

2.3.1 VLAN

Virtual networks allow to transmit different services separated from each other over the same infrastructure. Although the physical topology of a network connects all network elements, setting VLANs can take care that the individual logical topologies are separated from each other. This separation can fulfil among others a security aspect. But also in respect to the performance aspect can the assignment of priorities lead to a preferred transmission of certain data.

The EDS500 managed switches support VLANs according to standard IEEE 802.1Q. According to this, Ethernet frames get an additional VLAN tag that shows the membership to a specific VLAN id.
Figure 1: Using VLANs

References:
Details on the VLAN configuration can be found under EDS500 Manual - Part 2: VLAN Settings.

Default configuration:
In default configuration VLANs are disabled.

Recommendation for secure configuration
Use VLANs to separate the network into work areas.

Commands to configure VLANs on interfaces

- `<set interface {channel...} access-vlan {...}>`
- `<set interface vlan {1-4094} ip-address {{IP address} [{IP address range end}] {subnet mask}} | {unnumbered vlan {vlan-id}}>
- `<set switch {fo1 | fo2} access-vlan {1-4094}>`
- `<set interface {channel...} trunk-vlan {{1-4094} | all}>`
- `<set stp msti {...} [no] vlan {...}>`
<set stp msti {1-4094} vlan {1-4094}>
<set stp msti {1-4094} no vlan {1-4094}>
<set switch {port1 | port2 | port3 | port4} access-vlan {1-4094}>
<set switch port1 access-vlan 10>
<set switch {port1 | port2 | port3 | port4} trunk-vlan {{1-4094} | all}>
<set switch port3 trunk-vlan all>
<set system radius source vlan {1-4094} [dependency {inverse-monitor | monitor}]>
<set system snmp trap-source vlan {1-4094} [dependency {inverse-monitor | monitor}]>
<clear interface {channel...} trunk-vlan {...}>
<clear interface {dsi...} access-vlan>
<clear interface {fastethernet...} access-vlan>
<clear interface {fastethernet...} trunk-vlan {...}>
<clear interface {tunnel...} access-vlan>
<clear interface {tunnel...} trunk-vlan {...}>
<clear interface console source vlan {{1-4094}}>
<clear interface vlan {...} gateway>
<clear interface vlan {...} ip-address {...}>
<clear interface vlan {1-4094} vrrp id>
<clear switch {fo...} access-vlan>
<clear switch {fo...} trunk-vlan {...}>
<clear switch {port...} access-vlan>
<clear switch {port...} trunk-vlan {...}>
<clear system radius source vlan {{1-4094}}>
<clear system snmp trap-source vlan {{1-4094}}>
<clear system syslog source vlan {{1-4094}}>  

2.3.2 RIP Configuration

The Routing Information Protocol (RIP) is a distance vector routing protocol that automatically synchronizes the routing tables of connected routers.

EDS500 managed switches support RIP in the versions 1 and 2 including split horizon and triggered updates.

References:
Details of the RIP network management can be found under EDS500 Manual - Part 2: Configure Routing Protocol RIP.

Default configuration:
The default value for RIP is: no rip.

Recommendation for secure configuration:
RIP has to be disabled in a secure configuration.

Disable RIP
<set router no rip>
<show router rip>
2.3.3  Rate Limiting

While QoS/IEEE 802.1p CoS takes care that frames can be prioritized at the place where bandwidth overload happens, it is the task of the rate limiting to limit the incoming or outgoing data rate at an interface in general. It can also be set which frame types should be limited and can be used as broadcast storm control function.

Figure 2: Rate Limiting per port
In estimating the bandwidth, already when feeding in the data stream a later overload situation can be avoided in the further network.

References:
Details on the rate limiting configuration can be found under EDS500 Manual - Part 2: Rate Limiting.

Default configuration:
In default configuration receive-rate-limit and transmit-rate-limit are not set.

Recommendation for secure configuration:
Set the limit according to the applications. Potential overload is thus reduced to the subnetwork.

Commands to configure the Rate limiting:
<set switch {port...} limit-mode {...}>
<set switch {port...} {receive-rate-limit | transmit-rate-limit} {...}>

2.3.4  Access Control and Device Authentication with IEEE 802.1X

The IEEE 802.1X standard offers the possibility to apply an access protection for physical ports in the LAN. A device ("Supplicant") connected to an EDS500 managed switches ("Authenticator") is granted network access only after a successful authentication. The Authenticator (in this case the EDS500 device) does not perform the actual authentication, but instead uses a RADIUS server for this purpose, which must be configured.
Figure 3: Access control with IEEE 802.1X

References:
Details on the Access control can be found under EDS500 Manual - Part 2: Access Control and Device Authentication with IEEE 802.1X.

Default configuration:
By default, 802.1X is activated and every port is unlocked (<set dot1x portcontrol {...} auth-force>).

Recommendation for secure configuration:
Configure 802.1X and force authentication for every port.

Commands to related 802.1X:
<set dot1x [no] enable>
<set dot1x portcontrol {fastethernet0 | fo1 | fo2 | port1 | port2 | port3 | port4} {auth-force | pae-auto | unauth-force}>
<set dot1x mab {port1 | port2 | port3 | port4} [no] enable>
<set dot1x reauthentication port-down [no] allow>
<show dot1x>

**ADVICE**
The setting <set dot1x reauthentication port-down allow> includes the danger that by plugging in an Ethernet switch or something similar between Supplicant and Authenticator potential illegal network access is possible. When using a hub the 802.1X authentication can be recorded.

2.3.5 **Access Lists**

EDS500 managed switches offer 16 access lists that help to classify Ethernet frames. If at least one rule from a list matches an Ethernet frame then the linked action is carried out (forwarding, blocking, change Class-of-Service).
Access lists can either be defined as deny lists (blacklist, allowed is anything outside the specified criteria) or as permit list (whitelist, allowed is everything from the list).

Thus the list functions as a mini firewall or packet filter.

References:
- Details on the Syslog configuration can be found under EDS500 Manual - Part 2: Access Lists.

Default configuration:
- Access lists are disabled.

Recommendation for secure configuration:
- Use access lists to built-up a small firewall.

Commands for access list management:
- `<show access-list>`
- `<show access-list {1-16}>`
- `<access-list {1-16} clear>`
- `<access-list {1-16} clear rule {1-16}>`
- `<access-list {...} ethertype {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} ethertype {arp | ip | {0x0800-0xffff}}>`
- `<access-list {...} ip [...] {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} ip [{destination | source} {IP address} [{subnet mask}]]>`
- `<access-list {...} mac [...] {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} mac {destination | source} {aa-bb-cc-dd-ee-ff | aabb.ccdd.eeff | aabbccddeeef}>`
- `<access-list {...} protocol {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} protocol {tcp | udp | icmp | {0-255}}>`
- `<access-list {...} tcp dst-port {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} tcp dst-port {0-65535}>`
- `<access-list {...} tcp src-port {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} tcp src-port {0-65535}>`
- `<access-list {...} udp dst-port {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} udp dst-port {0-65535}>`
- `<access-list {...} udp src-port {...}>`
- `<access-list {1-16} {deny-rule | permit-rule} {1-16} udp src-port {0-65535}>`

### 2.3.6 L2TP Configuration

The layer-2-tunnel protocol (L2TP) can be used to connect physically not directly connected network nodes on the layer 2 of the OSI layer model.
One device of a L2TP tunnel is configured as L2TP server, the other is configured as L2TP client and establishes a link to the server. Both devices need the local and the remote IP address. The local address is called source IP address, the remote address is the destination IP address. To avoid that the already encapsulated L2TP data traffic is encapsulated again, the tunnel interface should be configured as an access VLAN (untagged) or as one or more trunk VLANs (tagged) where all of them are not associated with the local or remote IP address. Then the tunnel interface has to be activated.

References:
Details on the L2TP configuration can be found under EDS500 Manual - Part 2: Layer-2-Tunnel.

Default configuration:
In default configuration L2TP is disabled.

Recommendation for secure configuration:
When using L2TP additional protective measures (like VPN) are required.

ADVICE
L2TP is considered as unsecure protocol. L2TP is disabled by default.

Commands related to the layer 2 tunnel function
<set interface {tunnel...} role {...}>
<set interface {tunnel...} source-ip {...}>
<set interface tunnel0 trunk-vlan {{1-4094} | all}>
<set interface tunnel0 destination-ip {IP address}>
2.3.7 **IEC 60870-5-101 to IEC 60870-5-104 Converter**

In addition the EDS500 managed switches can be used for the conversion between IEC 60870-5-101 and IEC 60870-5-104.

The EDS500 managed switches feature a converter function for this purpose. The serial interfaces of the modem are connected to one or more telecontrol units. Several telecontrol units can be connected via an existing voice-frequency telegraphy circuit line. Prerequisite is the use of the protocol IEC 60870-5-101 on the telecontrol unit. Each connected telecontrol unit gets an additional IP address in the switch with which one or more IEC 60870-5-104 central offices can connect themselves. The telegram types get translated, as well as the address formats and time stamp. In order to convert, the assignment of an ASDU address (station address) to a link address (IEC 60870-5-101) as well as to a local IP address for the central office (IEC 60870-5-104) has to be configured. No information objects need to be created by configuration, instead they are forwarded transparently.

References:
Details on the IEC 60870-5-104 configuration can be found under EDS500 Manual - Part 2: IEC 60870-5-101 and IEC 60870-5-104.

Default configuration:
In default configuration IEC 60870-5-104 and IEC 60870-5-101 is disabled.

Recommendation for secure configuration:
n/a

Commands to activate / deactivate an IEC 60870-5-101 / IEC 60870-5-104 interface

```
<set {iec101 | iec104} interface {1 | 2} no shutdown>
<set {iec101 | iec104} interface {1 | 2} shutdown>
```

2.4 **TCP/UDP Ports**

To setup an Ethernet firewall the following table summarizes the Ethernet ports used in the EDS500 series. The ports are listed in ascending order. The column “Default state” defines whether a port is open or closed by default. All ports that are closed by default are opened by configuration.

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Default state</th>
<th>Service</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>TCP</td>
<td>closed</td>
<td>Echo</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>TCP</td>
<td>open</td>
<td>SSH</td>
<td>access to CLI</td>
</tr>
<tr>
<td>23</td>
<td>TCP</td>
<td>closed</td>
<td>TELNET</td>
<td>access to CLI</td>
</tr>
<tr>
<td>67</td>
<td>VDP</td>
<td>closed</td>
<td>DHCP</td>
<td>client</td>
</tr>
<tr>
<td>68</td>
<td>VDP</td>
<td>closed</td>
<td>DHCP</td>
<td>relay/server</td>
</tr>
<tr>
<td>69</td>
<td>UDP</td>
<td>n/a</td>
<td>TFTP</td>
<td>client only</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>open</td>
<td>HTTP</td>
<td>only redirect to HTTPs</td>
</tr>
<tr>
<td>161</td>
<td>UDP</td>
<td>closed</td>
<td>SNMP</td>
<td>Supervision client</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>open</td>
<td>HTTPS</td>
<td>Web server for configuration</td>
</tr>
</tbody>
</table>

Table 1: TCP/UDP ports used in EDS500 series
### 2.5 Encryption Algorithm

In EDS500 managed switches encryption and hash algorithms are used to protect the access to the Web server, to access the command line interface (CLI) via SSH, and for SNMPv3 access.

The algorithms are:

- **AES (Advanced Encryption Standard)**, a block cipher based on a symmetric key algorithm to encrypt and decrypt information. NIST has defined AES as succeeding standard of DES. The effective key length for AES varies between 128 and 256 bits, depending on the algorithm.
- **Encryption Algorithm SHA (Secure Hash Algorithm)** a family of cryptographic hash functions published by NIST. In the EDS500 managed switches the SHA-2 variants SHA-256 and SHA-1 are used.
- **DSA (Digital Signature Algorithm)** is a Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiations and the discrete logarithm problem. For the EDS500 managed switches a DSA key length of 1024 bits is used.
- **3DES** is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
- **DES (Data Encryption Standard)**, a block cipher based on a symmetric key algorithm to encrypt and decrypt information. The effective key length of DES is 56 bits.
- **DH (Diffie–Hellman)** key exchange, a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. In the EDS500 managed switches Diffie-Hellman with an effective key length of 768 (DH group 1) and 2048 (DH group 14 = default) bits are used.
- **MD5 (Message-Digest algorithm 5)**, a cryptographic hash function with a 128 bit hash value (see RFC1321 “The MD5 Message-Digest Algorithm” for detailed information). Used in the EDS500 series for HTTP Digest Access Authentication with quality of protection (protection of Web server access).
- **ECDSA (Elliptic Curve Digital Signature Algorithm)** is a variant of the Digital Signature Algorithm which uses elliptic curve cryptography. ECDSA offers the same or better security strength as DSA, while significantly reducing the necessary key size and subsequently computation time. For the EDS500 managed switches the curve NIST P-256 is used (defined by NIST). Other names are Secp256r1 (SEC 2) and prime256v1 (X9.62/SECG).
- **ECDH (Elliptic Curve Diffie–Hellman)** is a variant of the Diffie–Hellman key exchange protocol, which uses elliptic curve cryptography. ECDH offers the same or better security strength as DH, while significantly reducing the necessary key size and subsequently computation time. For the EDS500 managed switches the curve NIST P-256 is used (defined by NIST). Other names are Secp256r1 (SEC 2) and prime256v1 (X9.62/SECG).

No security relevant proprietary algorithms or protocols are used.

---

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Default state</th>
<th>Service</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>514</td>
<td>UDP</td>
<td>n/a</td>
<td>Syslog</td>
<td>client only</td>
</tr>
<tr>
<td>520</td>
<td>UDP</td>
<td>closed</td>
<td>RIP</td>
<td>Routing information protocol</td>
</tr>
<tr>
<td>1701</td>
<td>UDP</td>
<td>closed</td>
<td>L2TP</td>
<td>Layer 2 Tunneling Protocol</td>
</tr>
<tr>
<td>2404</td>
<td>TCP</td>
<td>closed</td>
<td>IEC60870-5-104</td>
<td>Communication protocol</td>
</tr>
<tr>
<td>49833</td>
<td>UDP</td>
<td>closed</td>
<td>UART Tunnel</td>
<td>proprietary protocol (HUTP)</td>
</tr>
</tbody>
</table>

Table 1: TCP/UDP ports used in EDS500 series

All Ports can freely be configured in configuration mode
2.6 Intended Use

Details concerning intended use:
• EDS500 managed switches are intended to be used in private, isolated networks.
• It is not intended to connect the EDS500 managed switches or the EDS500 web server direct to the internet.
• In case the EDS500 managed switches are using public networks, external devices with VPN functionality have to be used.
3 User Authentication

Access to the command line interface (CLI) and the web interface is protected by a two-step authorization concept.

The default value for passwords is "" (empty). It is recommended to set a new password during first login. This reminder will appear as long as no password is not set.

The following sections describe how the device can be protected against unauthorized access.

ADVICE
The web application login (local authentication) is not used for user administration. It is recommended to manage the user administration via Radius which supports various password policies. The local authentication does not support password policies.

3.1 Operation Modes - View (Login) and Configuration (Enable)

The management console of the EDS500 managed switches has a two-level access concept: view mode and operation mode configuration.

Most of the system parameters can be shown in view mode whereas safety critical settings are excluded.

The view mode is accessed with a successful login. Depending on the connection type to the management console (CLI) (serial, Telnet, SSH…) and depending on the user authentication scheme a login name and/or a login password have to be entered.

In operation mode configuration all system parameters can be shown and all commands for system configuration can be executed. The operating mode configuration is accessed at the management console with the command <enable> after login to the command line interface (CLI).

Depending on the set user authentication scheme a login name and/or a login password have to be entered for the operating mode configuration.

The command <disable> terminates operation mode configuration. Afterwards, the device is in view mode.

Figure 5: Access modes
The command <exit> terminates view mode and operating mode configuration and closes the command line interface (CLI).

The prompt at the command line interface (CLI) shows the current access mode:

Prompt for view mode
switch>

The symbol > indicates the login permission (view mode).

Prompt in operation mode configuration
switch#

The symbol # indicates the operation mode configuration.

Entering and exiting operation mode configuration
switch>enable
<enable>
switch#
switch#disable
<disable>
switch>

Depending on the connection type to the command line interface (CLI) (serial, Telnet, SSH...) the operation mode configuration and view mode are automatically terminated after a configurable period (autoLogout and auto-disable).

3.2 Login Mode Password

The login mode determines in what way the user is authenticated.

The default value for loginmode is: password.

Login password and password for the operation mode configuration (enablepass) are not set.

ADVICE
Login and enable passwords shall be enabled in a secure configuration. Login and enable passwords are enabled by default.

Commands to set login and enable passwords
<set system loginmode password>
<set loginpass {...}>
<set enablepass {...}>

3.3 Login Mode RADIUS

As an alternative to the loginmode password that uses a fixed password for authentication, a login is also possible with the help of a (remote) authentication server. User name and password combinations can be verified by a RADIUS server.

To use the login mode radius on a EDS500 device, the RADIUS server that can be reached via the network has to be configured first. If no RADIUS server is configured the login mode
password stays active as a fall-back. After successful login with RADIUS (e.g. via Telnet or SSH) the user is in view mode. If the web interface is used with RADIUS, the user is in operation mode configuration after authentication.

<table>
<thead>
<tr>
<th>ADVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial connections to the command line interface (CLI) via serial connections are not authenticated by RADIUS but always with the login and enable password.</td>
</tr>
</tbody>
</table>

Commands to enable RADIUS

- `<set system loginmode radius>`
- `<set system radius server {IP address} [{server port}] {shared secret}>`

3.4 **Automatic Session Termination**

To avoid that authenticated connections stay open due to a forgotten logout there is an automatic function for logout and disable on EDS500 managed switches.

A timeout can be set for the access to the management console via serial connections, Telnet connections, SSH connections and the Web-interface.

A serial connection to a management console gets only terminated if a login password is set and the value for idle-logout timeout does not equal 0.

The default value for the automatic termination of the operation mode configuration after inactivity is 600 seconds.

The default value for the automatic termination of the view mode is 1200 seconds.

Commands to set the automatic logout / disable

- `<set interface {console...} idle-logout {...}>`
- `<set interface {console...} idle-disable {...}>`
- `<set telnet idle-disconnect {...}>`
- `<set system web-server session-timeout {...}>`
- `<set system ssh idle-disconnect {...}>`
Secure Web server access

For secure access, the EDS500 series web server supports Hypertext Transfer Protocol Secure (HTTPS). HTTPS is a combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server. Detailed information about HTTPS could be found in RFC2818 “HTTP Over TLS”.

For the identification the EDS500 series web server uses as default self-signed public key certificates not issued by a certification authority (CA). The default self-signed certificates are created at startup depending on the configuration. In addition the EDS500 series web server supports the upload of external generated HTTPS certificates. This allows to use trusted certificates issued by a certification authority (CA).

Client authentication with user certificates is not supported by the EDS500 series. The authentication of the user is ensured by a user name and a password.

ADVICE

For security reasons, the web client has to be closed after each working session. This prevents the usage of supplied user names and passwords by unauthorized persons.

The following chapters describe configuration, access and certificate handling for the secured EDS500 series web server.

4.1 Web Server User Authentication

After a successful connection with a web browser to the EDS500 series web server, the server requests a user name and password for log-in.

Examples for this kind of log-in dialog are shown in the next figure. The Example is from the Google Chrome Browser.

![Log-in Dialog Example](image-url)
4.2 HTTPS Web Server Access

To access the EDS500 series web server via HTTPS the URL given in the Web client must begin with “https://” followed by the IP address of the EDS500 devices. The following figure shows an example.

The default Web server certificates used by the EDS500 series are self-signed and not issued by a certification authority (CA). As result an actual web client shows a warning messages concerning the missing CA, if the Web server is accessed with HTTPS. To avoid this warning message a trusted external certificate must be configured and uploaded to the EDS500 series.

If the Web server is configured for HTTPS a standard access is not possible anymore. In case of a standard access the Web server redirects the access to the secure pages of the EDS500 series web server.

If the web server is not configured for HTTPS, a secure access is possible as well. There are no restrictions in this case besides the possible warning message from the self-signed certificate.
5 Certificate Management

For secure webserver (HTTPS) functionality the EDS500 managed switches requires a compatible combination of EC key (Elliptic Curve key) and certificate.

In delivery state each EDS500 managed switches has stored its EC key (device key) and its certificate (device certificate - self-signed) generated from the EC key. This combination is valid and can be used for the HTTPS functionality.

The usage of the devices' EC key and the devices' certificate (self-signed) is the easiest way for a HTTPS connection. However, the certificate of each individual device must be downloaded and integrated into the browser. That can be very complex when managing a large number of browsers and workstations.

The EC key and certificate can also be generated externally and loaded onto the device. This enables the use of customer generated keys (external key) and/or certificates (external certificates).

Every combination of device and external keys and certificates have their advantages.
- Device EC key and device certificate (default state)
- Device EC key and external certificate (CSR)
- External EC key and device certificate
- External EC key and external certificate (CSR or external generated)

The latter combination allows two possibilities. The following chapter describes the combinations and list.

Generally it should be noted that the activation of certificates takes place directly after the upload via the web interface. A restart of the device is not necessary.

5.1 Host Key Type

The EDS500 managed switches supports only EC (Elliptic curve) keys.

This key is standardized by the name:
- Secp256r1 (SEC 2)
- prime256v1 (X9.62/SECG)
- NIST P-256 (NIST)

The key length has to be 256 bit.

5.2 Combination of Key and Certificate

From a technical point of view, the device allows five different ways of using or generating keys and certificates. Depending on requirements of cyber security and the operating comfort, the following options are available.
EC key

The first decision is if the preinstalled key on the device or an external key shall be used. This decision usually depends on the guidelines of the companies. The key pre-installed in the device complies with ABB’s minimum cyber security requirements. According to this, the key is unique and the private part is not read out. However, some companies need to use their own keys and this is supported by the EDS500 managed switches. How to upload keys to the device is described in the next chapter.

At this point it should be mentioned that the key, especially the private part, must never be transmitted over an insecure connection. This should also be avoided over supposedly secure connections.

**ADVICE**

Private keys must be protected against access by third parties under all circumstances.

The device EC key is not deleted when using an external EC key. It remains in the device, but is inactive.

Certificate

Certificates can be generated in the device based on the current EC Key. As soon as the device has a valid EC key (external or device), it automatically generates a valid certificate (self-signed). This certificate can be downloaded and added to the used browser.
Certificate Management

Combination of Key and Certificate

1. Certificate
2. External Certificate
3. Certificate Signing Request
4. EC key
5. Device
6. Browser
7. PEM format
8. UPLOAD
9. DOWNLOAD

a) Use default key and self-signed certificate of device

EDS500

EC key

device

Certificate
device / Self-signed

download

Browser

b) Use external EC key and self-signed function of device.

EDS500

EC key

external

Certificate

device / self-signed

Certificate

signing request

upload

Browser

Figure 7: Device key (a) or external key (b) with self-signed certificates

The certificates generated in this way are device-specific. This means that this certificate is only valid for this device and not for other EDS500 managed switches. If several EDS500 managed switches are used, all certificates must be downloaded from the devices and integrated into the browser.

The trust in self-signed certificates is legitimated by the fact that they are signed directly by the device. However, for several reasons it may be necessary to use CA-signed certificates (e.g. security guideline, handling ...).

External certificates can be created in two ways: Via a certificate signing request (CSR) or via an external program (via external program only, if private key exists externally). In the case of the CSR method, a .csr file is downloaded from the device. This file is signed with a CA and results in a device-specific .crt file. This .crt file is the actual certificate and have to be uploaded to the device. It replaces the device certificate. In the case of the usage of an external program a .crt file can directly be generated from the EC key and a CA.

External certificates have the advantage that they not only trust themselves, they additionally trust all higher-level certificates (e.g. CA certificates). That gives you the possibility to establish a HTTPS connection to all EDS500 managed switches in a network with just one high-level certificate. The circumstance of integrating each individual certificate from all devices into the browser is eliminated.
CA certificates can be created by yourself as well as purchased from an authentication authority.

Combinations and their characteristics

- **Device EC key and self-signed certificate**
  - Default working
  - Out of the box
  - Each certificate must be integrated in the browser

- **External EC key and self-signed certificate**
  - Use of custom keys
  - Each certificate must be integrated in the browser
  - EC key upload is a security risk

- **Device EC key and CA-signed certificate (CSR)**
  - Browser needs only one high-level certificate
  - Automation possible

- **External EC key and CA-signed certificate (CSR)**
  - Browser needs only one high-level certificate
  - Time-consuming setup of the device
  - EC key upload is a security risk

- **External EC key and CA-signed certificate (external generated)**
  - Browser needs only one high-level certificate
  - EC key upload is a security risk
  - Compatibility of EC key and certificate is not guaranteed by the device.
c) Device EC key, CSR and external CA-signed certificate.

**Figure 8:** Device key (c), external key - CSR (d) or external key - non CSR with CA-signed certificates (e)
5.3 **Step-by-step instruction**

6 System Hardening

ABB strives to improve the security and robustness of its products by performing security testing and hardening. EDS500 series has been systematically hardened, e.g. unused services have been removed and unused ports closed. Furthermore EDS500 series has been thoroughly tested at ABB’s dedicated, independent security test center using state-of-the-art commercial and open-source security testing tools. Security testing and hardening are integral parts of the development process.
7 Patch management

7.1 General Information

This chapter describes the patch management for the EDS500 series and how to keep the system up to date.

The firmware is updated by transferring a firmware image to the device. It can be downloaded with the help of the command line (Telnet, SSH, serial terminal) as well as with the help of the integrated web interface, scripts or a management program. It is mandatory that there is an IP connection to the device.

ADVICE
During a firmware update the power supply must not be interrupted or a reboot must not be triggered as this could leave the device in an inoperable state.

Three categories of updates are available for the EDS500 series:
• Patches (cyber security updates)
• Bug fixes (available for the latest minor release)
• Minor/Major releases (new functions)

Most of the cyber security issues can be solved by patches (e.g. OS patches, fixes in protocols).

Partly minor/major release change is required (e.g. new encryption, new OS versions, new cyber security functions).

7.2 Release Policy

The release policy of the EDS500 series is as follows:
• Patches based on security vulnerability on request.
• Bug fix releases on request (typically every 6-10 weeks).
• Project specific developments are tested as beta version and will be released with the next minor or major release.
• Two minor/major releases per year with functional improvements.

7.3 Update Policy

The Update Policy of the EDS500 series is as follows:

Patch: Updates in cyber security functions
• No changes in configuration
• Test recommendation in the release note

Bug fix: Error corrections
• No changes in configuration
• Functional test of corrected function is recommended

Minor release:
• New device and for new cyber security functions
• Automatic update of configurations if required
• Functional test of updated/new function is recommended

Major release:
• New device and for new cyber security functions
• Automatic update of configurations
• Functional test of updated/new function is recommended

7.4 Recommendation by ABB

We recommend to implement cyber security patches as soon as possible.

<table>
<thead>
<tr>
<th>ADVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firmware update via Command Line Interface (CLI) is considered as unsecure because TFTP must be used.</td>
</tr>
<tr>
<td>Use Firmware update via web interface for secure operation.</td>
</tr>
</tbody>
</table>

We recommend firmware updates via web interface because firmware updates via Command Line Interface (CLI) use the unsecure TFTP protocol.

Information are available at:
• Cyber security alerts and notifications
• ABB Inside: Internal announced findings and solutions
• solutions.abb/eds500: Official Information for end customers

Bug fixes have to be implemented only if it is relevant for the running system.

Annual minor/major release updates are recommended:
• At least minor release update
• Major release updates shall be considered

7.5 Firmware update via Web Interface

The page for firmware update can be reached with the link "Firmware" in the navigation bar. JavaScript has to be activated in the browser to use the update function.

Upload directly in the browser
➢ Select the firmware image on the local computer.
➢ Click on the "Upgrade" to start the process.
## Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td><strong>Active Directory</strong></td>
</tr>
<tr>
<td>AES</td>
<td><strong>Advanced Encryption Standard</strong></td>
</tr>
<tr>
<td>ARP</td>
<td><strong>Address Resolution Protocol</strong></td>
</tr>
<tr>
<td>ASDU</td>
<td><strong>Application Service Data Unit</strong></td>
</tr>
<tr>
<td>CA</td>
<td><strong>Certificate Authority</strong></td>
</tr>
<tr>
<td>CLI</td>
<td><strong>Command Line Interface</strong></td>
</tr>
<tr>
<td>DEA</td>
<td><strong>Data Encryption Algorithm</strong></td>
</tr>
<tr>
<td>DES</td>
<td><strong>Data Encryption Standard</strong></td>
</tr>
<tr>
<td>DH</td>
<td><strong>Diffie–Hellman key exchange</strong></td>
</tr>
<tr>
<td>DSL</td>
<td><strong>Digital Subscriber Line</strong></td>
</tr>
<tr>
<td>EC</td>
<td><strong>Elliptic Curve</strong></td>
</tr>
<tr>
<td>HTTP</td>
<td><strong>Hypertext Transfer Protocol</strong></td>
</tr>
<tr>
<td>IEC</td>
<td><strong>International Electrotechnical Commission</strong></td>
</tr>
<tr>
<td>IEEE</td>
<td><strong>Institute of Electrical and Electronics Engineers</strong></td>
</tr>
<tr>
<td>L2TP</td>
<td><strong>Layer 2 Tunneling Protocol</strong></td>
</tr>
<tr>
<td>LAN</td>
<td><strong>Local Area Network</strong></td>
</tr>
<tr>
<td>NIST</td>
<td><strong>National Institute of Standards and Technology</strong></td>
</tr>
<tr>
<td>NTP</td>
<td><strong>Network Time Protocol</strong></td>
</tr>
<tr>
<td>OSI</td>
<td><strong>Open Systems Interconnection Model</strong></td>
</tr>
<tr>
<td>RADIUS</td>
<td><strong>Remote Authentication Dial-In User Service</strong></td>
</tr>
<tr>
<td>RIP</td>
<td><strong>Routing Information Protocol</strong></td>
</tr>
<tr>
<td>SHA</td>
<td><strong>Secure Hash Algorithms</strong></td>
</tr>
<tr>
<td>SNMP</td>
<td><strong>Simple Network Management Protocol</strong></td>
</tr>
<tr>
<td>SNTP</td>
<td><strong>Simple Network Time Protocol (according to RFC 4330)</strong></td>
</tr>
<tr>
<td>SSH</td>
<td><strong>Secure Shell</strong></td>
</tr>
<tr>
<td>STP</td>
<td><strong>Spanning Tree Protocol</strong></td>
</tr>
<tr>
<td>TDEA</td>
<td><strong>Triple Data Encryption Algorithm</strong></td>
</tr>
<tr>
<td>TFTP</td>
<td><strong>Trivial File Transfer Protocol</strong></td>
</tr>
<tr>
<td>UART</td>
<td><strong>Universal Asynchronous Receiver-transmitter</strong></td>
</tr>
<tr>
<td>UDP</td>
<td><strong>User Datagram Protocol</strong></td>
</tr>
<tr>
<td>VLAN</td>
<td><strong>Virtual Local Area Network</strong></td>
</tr>
<tr>
<td>VPN</td>
<td><strong>Virtual Private Network</strong></td>
</tr>
<tr>
<td><strong>VRRP</strong></td>
<td>Virtual Router Redundancy Protocol</td>
</tr>
</tbody>
</table>
Note:

The specifications, data, design or other information contained in this document (the "Brochure") - together: the "Information" - shall only be for information purposes and shall in no respect be binding. The Brochure does not claim to be exhaustive. Technical data in the Information are only approximate figures. We reserve the right at any time to make technical changes or modify the contents of this document without prior notice. The user shall be solely responsible for the use of any application example or information described within this document. The described examples and solutions are examples only and do not represent any comprehensive or complete solution. The user shall determine at its sole discretion, or as the case may be, customize, program or add value to the ABB products including software by creating solutions for the end customer and to assess whether and to what extent the products are suitable and need to be adjusted or customized.

This product is designed to be connected to and to communicate information and data via a network interface. It is the users sole responsibility to provide and continuously ensure a secure connection between the product and users or end customers network or any other network (as the case may be). The user shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB AG is not liable for any damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB AG shall be under no warranty whatsoever whether express or implied and assumes no responsibility for the information contained in this document or for any errors that may appear in this document. ABB AG's liability under or in connection with this Brochure or the files included within the Brochure, irrespective of the legal ground towards any person or entity, to which the Brochure has been made available, in view of any damages including costs or losses shall be excluded. In particular ABB AG shall in no event be liable for any indirect, consequential or special damages, such as – but not limited to – loss of profit, loss of production, loss of revenue, loss of data, loss of use, loss of earnings, cost of capital or cost connected with an interruption of business or operation, third party claims. The exclusion of liability shall not apply in the case of intention or gross negligence. The present declaration shall be governed by and construed in accordance with the laws of Switzerland under exclusion of its conflict of laws rules and of the Vienna Convention on the International Sale of Goods (CISG).

ABB AG reserves all rights in particular copyrights and other intellectual property rights. Any reproduction, disclosure to third parties or utilization of its contents - in whole or in part - is not permitted without the prior written consent of ABB AG.

© Copyright ABB 2019
All rights reserved
Visit us

ABB AG
Power Grids
P.O. Box 10 03 51
68128 Mannheim, Germany
solutions.abb/eds500