Com'X 210/510 Hardening Guide

Introduction	2
Additional resources	2
Access Com'X user manual	3
Upgrade Firmware	3
Determine current firmware version	3
Upgrade to latest firmware version	4
Safety Precautions	5
User management	5
Set default administrator password	6
Set default guest password (Com'X 510 only)	6
Disable the Password Reset button	6
Install a private SSL certificate	
	•
Disable enabling of Remote VPN access from cloud services	7
Disable enabling of Remote VPN access from cloud services Port management	7 7
Disable enabling of Remote VPN access from cloud services Port management	7 7 7
Disable enabling of Remote VPN access from cloud services Port management Close unused ports Disable unused services	7 7 7
Disable enabling of Remote VPN access from cloud services Port management Close unused ports Disable unused services Disable replies to ICMP Echo requests (PING)	7 7 7 8
Disable enabling of Remote VPN access from cloud services Port management Close unused ports Disable unused services Disable replies to ICMP Echo requests (PING) Set Secure Publication Transports	7 7
Disable enabling of Remote VPN access from cloud services Port management Close unused ports Disable unused services Disable replies to ICMP Echo requests (PING) Set Secure Publication Transports Configure SMTP (Email settings)	7 7
Disable enabling of Remote VPN access from cloud services Port management Close unused ports Disable unused services Disable replies to ICMP Echo requests (PING) Set Secure Publication Transports Configure SMTP (Email settings) Recommended best practices of unsecure protocols	7 7
Disable enabling of Remote VPN access from cloud services Port management Close unused ports Disable unused services Disable replies to ICMP Echo requests (PING) Set Secure Publication Transports Configure SMTP (Email settings) Recommended best practices of unsecure protocols Disable WiFi Access Point	7 7
Disable enabling of Remote VPN access from cloud services Port management Close unused ports. Disable unused services. Disable replies to ICMP Echo requests (PING) Set Secure Publication Transports. Configure SMTP (Email settings) Recommended best practices of unsecure protocols. Disable WiFi Access Point Apply Modbus TCP/IP Filtering.	7 7



Introduction

Your Schneider Electric product is equipped with security-enabling features. These features arrive in a default state and can be configured for your installation needs. Please note that disabling or modifying settings can impact the overall security robustness of the device and the security of your network.

This guide provides recommendations to better secure your Com'X device. Please use this guide in conjunction with the user manual for the step by step procedure details required for the configuration of specific features and settings.

NOTE: This guide is applicable for Com'X firmware version 6.5 and above.

Additional resources

Document	References
Com'X 200/Com'X 210/Com'X 510 Instruction Sheet	5406AD002 5406AD005 5406AD006 5406AD007
Com'X 510 User Manual	DOCA0098EN DOCA0098FR DOCA0098ES DOCA0098DE DOCA0098PT DOCA0098IT DOCA0098ZH DOCA0098RU
Com'X 210 User Manual	DOCA0036EN DOCA0036FR DOCA0036ES DOCA0036DE DOCA0036PT DOCA0036IT DOCA0036ZH DOCA0036RU
Com'X SSL Certificate Installation Guide	7EN12-0327

Access Com'X user manual

You can download the Com'X 210 and Com'X 510 user manual from the Schneider Electric website.

- Com'X 510 User Manual
- <u>Com'X 210 User Manual</u>

The user manual for Com'X 510 can also be accessed directly on the device.

- 1. Login to the Com'X.
- 2. Select Settings > Links > View Links.
- 3. Click the Com'X 510 User Manual EN document **local** link to download the manual.

宫 Com'X 51	0		09/06/2019 05:58:55 PM 🕐	Data logging: OFF Periodic publication: OFF	Available storag	e: 3.7 GB		🧿 admin Logout About
Monitoring Control	Diagnostics	Settings	Device Settings	Measurements Table	Commissioning	Custom Library	Maintenance	
General Settings	×		ocumenta	tion User Assis	tance			
Communication	~			link	Com'X 510 (locumentation and	firmware	
Security	~	Com'X 510 Doci	uments and Down 0 User Manual - E	loads N local	User Manua	I.		_
User Management	~	☆ =SE=		link	Schneider E	lectric		
Events	~							Setup Links
Links	^	<u> </u>						
Setup Links								
View Links	•							

Upgrade Firmware

Products are hardened to increase security robustness. This is an ongoing process consisting of secure development practices, inclusion of security features and testing at our security test facilities. Keep your device firmware updated with the latest security updates.

Determine current firmware version

Locate the firmware version currently running on your Com'X.

- 1. Login to the Com'X.
- 2. Click About link located on the top right corner of the screen.
- 3. Determine Application version under Product Versions.

© 2019 Schneider Electric. All rights reserved.



Upgrade to latest firmware version

- 1. Determine the latest Com'X firmware version available on se.com.
 - a. Com'X 510 firmware
 - b. Com'X 210 firmware
- 2. Download and unzip the firmware bundle if it is higher than the firmware version on your Com'X device.
- 3. Open the release notes contained in the unzipped bundle.
- 4. Update the firmware if the release notes indicate security updates. The firmware filename begins with *upgrade-Com'X* and has file extension *.sp1*.

NOTE: See Upgrade Firmware section in the User Manual.

Safety Precautions

Installation, wiring, testing and service must be performed in accordance with all local and national electrical codes.

AWARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

- Change default passwords to help prevent unauthorized access to device settings and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, modification of data and logs, interruption of services, or unintended operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTICE

UNAUTHORIZED DATA ACCESS

- Immediately change the default password to a new, secure password.
- Do not distribute the password to unauthorized or otherwise unqualified personnel.

Failure to follow these instructions can result in equipment damage.

User management

A strong password is essential for device security. The Com'X security policy requires the following:

- 8 characters
- 1 uppercase letter
- 1 numeric digit

1 special character

It is recommended to increase the password complexity by increasing the number of characters, special characters, and not repeating characters.

Set default administrator password

Use the default administrator password (admin) when you first log in. After your first login, you will be required to create a new password. Follow the password recommendations when entering the new password.

You can change the default admin password after the initial log-in. See *Changing the Password* section in the user manual for additional information.

Set default guest password (Com'X 510 only)

The default password for the guest account is "guest". It is strongly recommended to change the password after you log in for the first time as an administrator.

NOTE: Only an administrator can change the guest password.

- 1. Log in as administrator.
- 2. Go to Settings > User Management > Users.
- 3. Select guest.
- 4. Follow password recommendations and enter a new password.
- 5. Enter the same password in **Confirm new password**.
- 6. Click Save changes.

Disable the Password Reset button

You can reset the default administrator account password by pressing the backup button. This feature is enabled by default. It is recommended to disable this feature for a Com'X installed in a publicly accessible location.

See *Disabling the Password Reset Button* section in the user manual for additional information.

Install a private SSL certificate

The Com'X comes with a self-signed SSL certificate installed for the HTTPS protocol. It is recommended to install your own certificate signed by a public or private CA.

Refer the *Com'X SSL Certificate Installation Guide* – 7EN12-0327 for information on creating a certificate file that is compliant with Com'X 510/210.

See *Uploading a New Certificate* section under *Settings* chapter in the user manual for additional information

Disable enabling of Remote VPN access from cloud services

By default, the Com'X is set up to connect to cloud services through the Remote Assistance VPN connection via a command from the Schneider Electric cloud. It is recommended to disable this feature and enable it only when remote technical support from Schneider Electric is required.

冨 Com'X 510	O9/06/2019 Data logging: OFF Available storage: O admin Logout About 02:42:12 PM (2) Periodic publication: OFF About About About
Monitoring Control Diagnostic	s Settings () Device Settings () Measurements Table Commissioning Custom Library Maintenance
Logs	Configuration management
System Settings	Save the configuration Backup for duplication
Events	This functionality is not available if you use the iOS platform
	File: No file chosen
	This functionality is not available if you use the IOS platform Apply the configuration
	Firmware upgrade
	File: No file chosen
	 This functionality is not available if you use the iOS platform
	Upgrade firmware
	Applications
	Remote access for support ON OFF
	Enable remote access from cloud ON OFF
	Restart Com'X
	Restart ComX Restart

See *Disabling Remote Access from Cloud Services* section under *Com'X 510 Maintenance* chapter for additional information.

Port management

There are certain ports and services that are open by default. It is strongly recommended to disable these ports and unused services when not required.

Close unused ports

By default, the following ports are open on the supported network connections. Disable the following ports when not in use.

- 80 (HTTP) disable for each network connection.
- 502 (Modbus TCP/IP)

See *Firewall Management* section under *Com'X 510 Settings* chapter for additional information.

Disable unused services

By default, the following services are enabled.

- SSH (Port: 2222): Used for technical support
- DPWS (Port: 5357): Used for device discovery

It is recommended to disable services when not required or in use. See *Firewall Management* section under Com'X 510 Settings chapter for additional information.



Disable replies to ICMP Echo requests (PING)

By default, the Com'X is configured to not reply to ICMP Echo requests (Ping). It is recommended to keep it disabled if possible. Disabling "Reply to ping" disables replies for all network connections.

置 Com'X 510	10/25/2019 Data logging: OFF Available storage: 3.7 GB 3 admin Logout 4 content 05:55:43 PM (*) Periodic publication: OFF Image: Content Image: Content </th <th>About</th>	About
Monitoring Control Diagnostics	Settings Device Settings Measurements Table Commissioning Custom Library Maintenance	
General Settings	Choose your network configuration • 2 separate ports (1 IP address for each) • Selection he Ethernet configuration	
Network Settings	General network settings	^
Proxy Settings	Default gateway 10 . 100 . 252 . 1 Primary DNS server 10 . 218 . 600 . 10	
Schneider Electric S	Secondary DNS server 10 106 10 10 Reply to ping Yes No No	
Contact Management	Diagnostic network	~
Email Settings		
Publication	Required field Save changes Cancel	ei j

See Configuring the Ethernet Ports section under Com'X 510 Settings chapter for additional information.

Set Secure Publication Transports

It is recommended to select HTTPS with authentication or SMTP with a connection security mode enabled when configuring publication.

See Publication / Configuring HTTP and HTTPS Transfer Protocols section under Com'X 510 Settings chapter of the user manual for additional information.

General Settings 🔨	Publication settings	
Date/Time Settings	Destination platform * CSV export	,
Network Settings	Publication frequency * Every day	,
Proxy Settings	Protocol * HTTPS	
Schneider Electric Se	Server * secure.server.com Port * 443	
Contact Management	Authentication required * Yes No	
Email Settings	User login * userA User password *	
Publication	Path * //	
Wi-Fi Access Point S	Field name * fieldName	
The Process Form S	Compression activated * Yes No	
Site Settings	Decimal separator * Dot	
Communication	Date Format * MM-DD-YYYY	,
Modbus Gateway		
Modbus TCP/IP Filter	09/05/2019 Data logging: OFF Available storage: 3.5 GB	9 admin Logout Ab
Com'X 510	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09.46.52 PM (*) Periodic publication: OFF OFF Available storage: 3.5 GB cs Settings (*) Device Sortings (*) Measurements Table Commissioning Custom Libra	3 admin Logout Ab any Maintenance
Modbus TCP/IP Filter	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09.46 52 PM Periodic publication: OFF Available storage: 3.5 GB cs Settings Device Settings Measurements Table Commissioning Custom Libra	🤉 admin Logout Ab ary Maintenance
Modbus TCP/IP Filter	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09.46 52 PM Periodic publication: OFF Available storage: 3.5 GB cs Settings Device Settings Measurements Table Commissioning Custom Libra Publication settings Device Settings Measurements Table Commissioning Custom Libra	9 admin Logout Ab ary Maintenanco
Modbus TCP/IP Filter	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09.46:52 PM Periodic publication: OFF Commissioning Custom Libro cs Settings Device Settings Measurements: Table Commissioning Custom Libro Publication settings Destination platform * CSV export Publication frequency * Every day	9 admin Logout Ab ary Maintenanco
Modbus TCP/IP Filter Com'X 510 Com'X 510 General Settings Date/Time Settings Network Settings	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09:46:52 PM Periodic publication: OFF Available storage: 3.5 GB Settings Device Settings Measurements: Table Commissioning Custom Libro Publication settings Destination platform * CSV export Publication frequency * Every day Protocol * SMTP	9 admin Logout Ab ary Maktenanco • •
Modbus TCP/IP Filter Com'X 510 Com'X 510 General Settings Date/Time Settings Network Settings Proxy Settings	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09:46:52 PM Periodic publication: OFF Available storage: 3.5 GB Settings Device Settings Measurements: Table Commissioning Custom Libro Publication settings Destination platform * CSV export Publication frequency * Every day Protocol * [SMTP To addresses * [publication@email.com x]	9 admin Logout Ab ary Maktenance • •
Modbus TCP/IP Filter Com'X 510 Com'X 510 General Settings Date/Time Settings Network Settings Proxy Settings Schneider Electric Se	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09:46:52 PM Periodic publication: OFF Commissioning Custom Libra Publication settings Device Settings ① Measurements Table Commissioning Custom Libra Publication settings Destination platform * CSV export Publication frequency * Every day Protocol * [SMTP] To addresses * [publication@email.com x] Compression activated * Yes No	9 admin Logout Ab ary Maintenanco • •
Modbus TCP/IP Filter Contact Management	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09:46:52 PM Periodic publication: OFF Commissioning Custom Libra Publication settings Device Sostings ① Measurements: Table Commissioning Custom Libra Publication settings Destination platform * CSV export Every day Publication frequency * [SMTP To addresses * [publication@email.com x] Compression activated * Yes No Field separator * [Comma [Comma	9 admin Logout Ab ary Maintenance • • • • •
Modus TCPIIP Filter Control Diagnost General Settings DaterTime Settings Network Settings Proxy Settings Schneider Electric Se Contact Management Email Settings	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09:46:52 PM Periodic publication: OFF Commissioning Custom Libra Publication settings Device Settings ① Measurements Table Commissioning Custom Libra Publication settings Destination platform * CSV export Every day Publication frequency * [Every day Protocol * [SMTP To addresses * [publication@email.com x] Compression activated * Yes No Field separator * Date Format * [Dothoryryr	admin Logout Ab Ab A
Modus TCPIIP Filter Control Disposed General Settings DaterTime Settings Network Settings Proxy Settings Schneider Electric Se Contact Management Email Settings Publication	09/05/2019 Data logging: OFF Available storage: 3.5 GB 09:46:52 PM Periodic publication: OFF Commissioning Custom Libra Publication settings Device Settings ① Measurements: Table Commissioning Custom Libra Publication settings Destination platform * CSV export Every day Publication frequency * [SMTP To addresses * [publication@email.com x] Compression activated * Yes No Field separator * Comma Decimal separator * Det Date Format * MM-DD-YYYY Date Format * MM-DD-YYYY	admin Logout Ab Ab A

Configure SMTP (Email settings)

See *Email Settings* section under Com'X 510 Settings chapter of the user manual for additional information.



Recommended best practices of unsecure protocols

The table below lists risks and best practices associated with unsecure protocols. It is highly recommended to follow these best practices.

Unsecure protocols	Best Practices
SMTP	 For publication: Select SMTP with either SSL/TLS or SMART TLS configured for publication.
НТТР	 For network configuration: Disable HTTP. Select HTTPS for network connections. For publication: Do not select HTTP. Select HTTPS with authentication.
FTP	 For publication: Do not use FTP. Select either HTTPS with authentication or SMTP with either SSL/TLS or SMART TLS configured for publication.
Modbus TCP/IP	 For Modbus device communications: Limit access to Modbus Communications by use of Modbus TCP/IP Filtering. Disable the Modbus port for each network interface when not in use.

Disable WiFi Access Point

The USB Wi-Fi key can be used as a temporary communication medium during the commissioning phase. This allows you to use a laptop or a tablet to configure the Com'X. The Wi-Fi access point is enabled by default. It is recommended to disable the Wi-Fi access point and enable it only for the required duration when needed.

See *Wi-Fi Access Point Settings* section under *Com'X 510 Settings* chapter of the user manual for additional information.

窑 Com'X 510	09/04/2019 Data logging: OFF Available storage: ① admin Logout 05:59:22 PM ⑦ Periodic publication: OFF Periodic publication: OFF Periodic publication: OFF Periodic publication: OFF	Abou
Monitoring Control Diagnost	tcs Settings () Device Settings () Measurements Table Commissioning Custom Library Maintenance	
0 General Settings	Access Point Settings	^
Date/Time Settings	Enable Wi-Fi access point Yes No	
Network Settings	Session duration 1 hour	۳
Proxy Settings	Required field Save changes Can	cel
Schneider Electric Servi		
Contact Management		
Email Settings		
Publication		
Wi-Fi Access Point Sett		
Site Settings		

It is recommended to ensure only secure protocols are used when connecting over the WiFi Access Point. Do not rely only on WiFi encryption.

Apply Modbus TCP/IP Filtering

Modbus TCP/IP filtering allows the administrator to create a whitelist and assign the level of access IP addresses have to the Com'X and its downstream devices. When enabled, the default access level is **Read** for any Modbus TCP/IP client, not in the filtered list. Setting the **Default Access** field to **None** blocks all Modbus TCP/IP clients not in the filtered list.

Modbus TCP/IP Filtering is disabled by default making the Modbus TCP/IP server accessible from any IP addresses. It is strongly recommended to enable Modbus TCP/IP Filtering and manage the access level of each Modbus client connecting to the Com'X.

See *Configuring Modbus TCP/IP Filtering* section of the user manual for additional information.

2 Com'X 510	09/04/2019 07:49:19 PM 🕑	Data logging: Periodic publ	OFF Available storage:	🧿 admin Logi	out Ab
onitoring Control Diagnostics Settings	Device Setting	is 🌖 Me			
Wi-Fi Access Point Sett					
Site Settings	P/IP Filtering				^
Site Information		Apply Filt	ering Yes No		
Data Logging		14/5-1	An empty octet field is treated right most octet and be contig	d as a wildcard. Empty fields must begin with t guous.	the
Communication	10	1 2	Read		
Modbus Gateway	10.	1.2.	3 Full		
inclusion of a characteristic and a characteristic			Read		
Modbus TCP/IP Filtering			Read		٠
Modbus Serial			Read		
Advanced Ethernet Sott			Read		٠
Advanced Enemet Sett			Read		٠
Zigbee Settings			Read		•
Security			Read		*
			Read		•
Firewall Management			Read		-
Certificates			Read		
Licer Management			Read		
Oser Management			Read		
Users			Read		*
Group Settings					
Events		Default Ac	cess None		•
Event Settings					

Enable Warning Banner

Enable the Com'X Warning Banner to all users attempting to access your computer system if required by your network security policy.

See *Warning Banner Settings* section under *Com'X 510 Settings* chapter of the user manual for additional information.

December 2 and the second	HTTPS	~
Proxy Settings		
Schneider Electric Serv	Modbus TCP/IP	~
Contact Management	Network Access	~
Email Settings	Default admin reset	~
Publication	Account Lockout Policy	~
Wi-Fi Access Point Sett	Warning Banner Settings	^
Site Settings	Enable warning banner Yes No	
	Place warning banner text here.	
Communication 🗸		
Security	Warning banner text	//
Firewall Management		