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 **6**
Disable enabling of Remote VPN access from cloud services **7**
Port management **7**
Close unused ports 7
Disable unused services 8
Disable replies to ICMP Echo requests (PING) 8
Set Secure Publication Transports **8**
Configure SMTP (Email settings) 9
Recommended best practices of unsecure protocols 10
Disable WiFi Access Point **10**
Apply Modbus TCP/IP Filtering **11**
Enable Warning Banner **12**

Schneider Electric

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

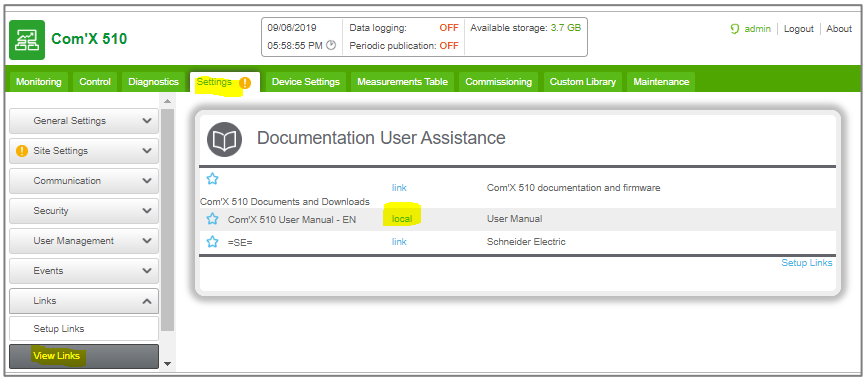
Access Com’X user manual

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

- Com’X 510 User Manual
- Com’X 210 User Manual

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.



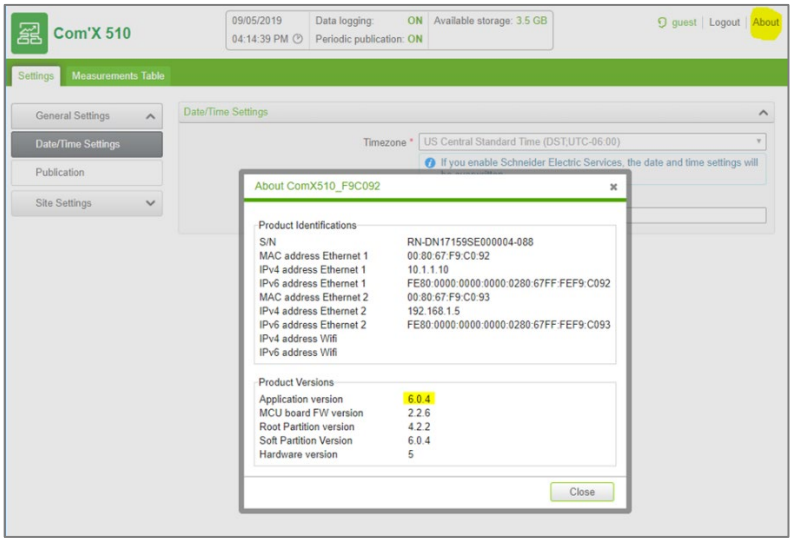
Upgrade Firmware

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**.



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.

⚠WARNING

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

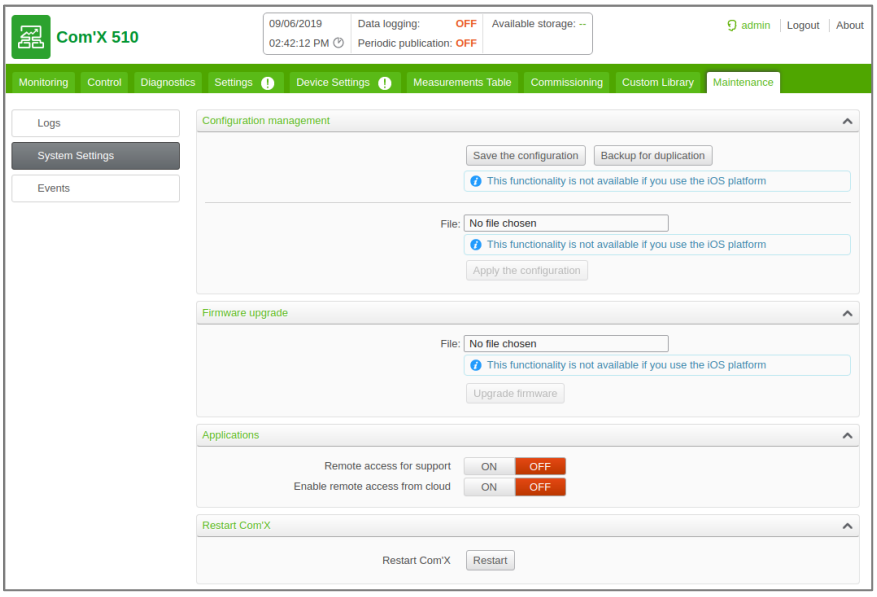
The Com'X comes with a self-signed SSL certificate installed for the HTTPS protocol. It is recommended to install your own certificate signed by a public or private CA.

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.



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)

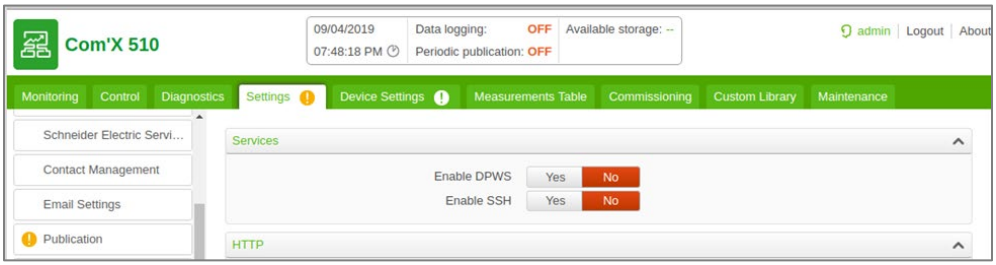
See *Firewall Management* section under *Com'X 510 Settings* chapter for additional information.

Disable unused services

By default, the following services are enabled.

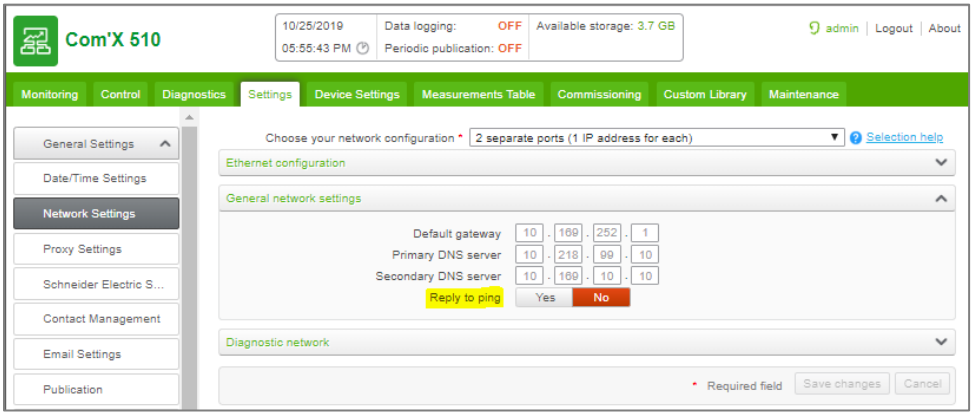
- SSH (Port: 2222): Used for technical support
- DPWS (Port: 5357): Used for device discovery

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.

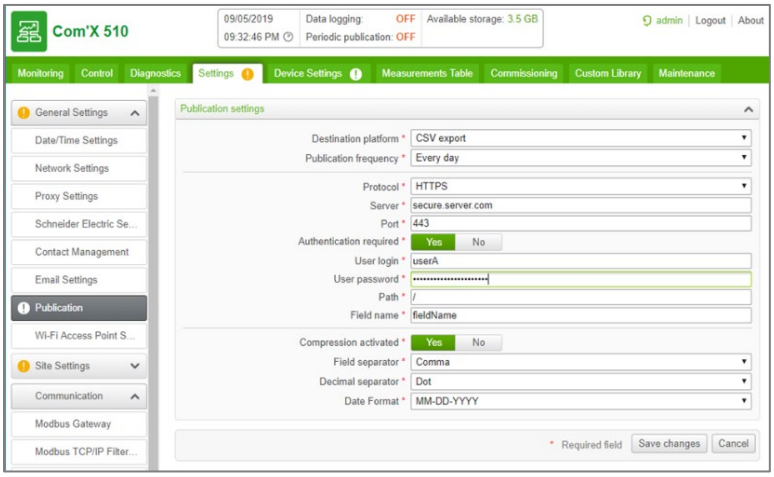


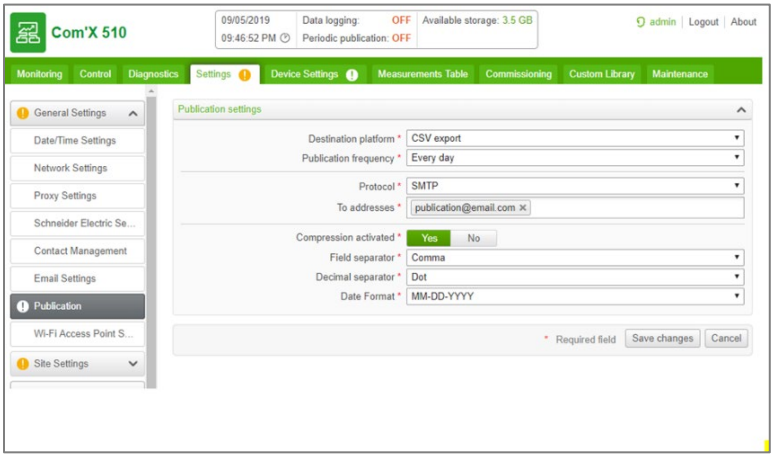
See *Configuring the Ethernet Ports* section under *Com'X 510 Settings* chapter for additional information.

Set Secure Publication Transports

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

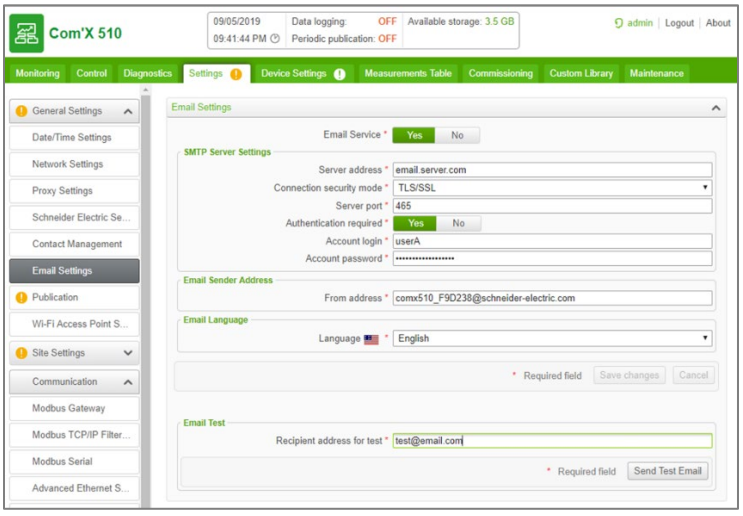
See *Publication / Configuring HTTP and HTTPS Transfer Protocols* section under *Com'X 510 Settings* chapter of the user manual for additional information.





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

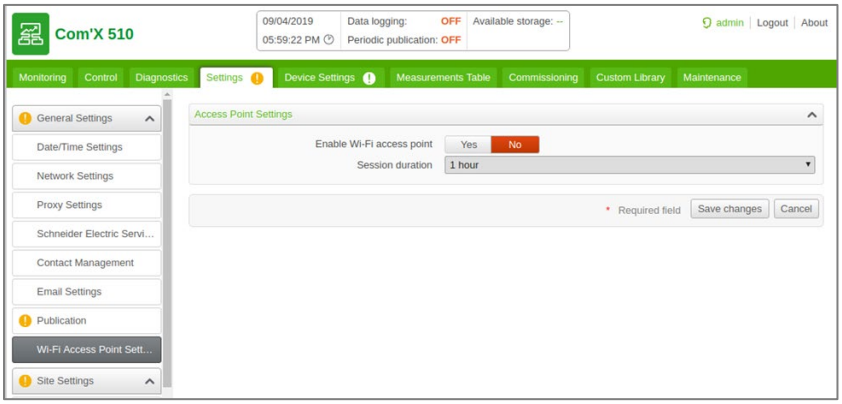
The table below lists risks and best practices associated with unsecure protocols. It is highly recommended to follow these best practices.

Unsecure protocols	**Best Practices**
SMTP	For publication: • Select SMTP with either • SSL/TLS or SMART TLS • configured for publication.
HTTP	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.



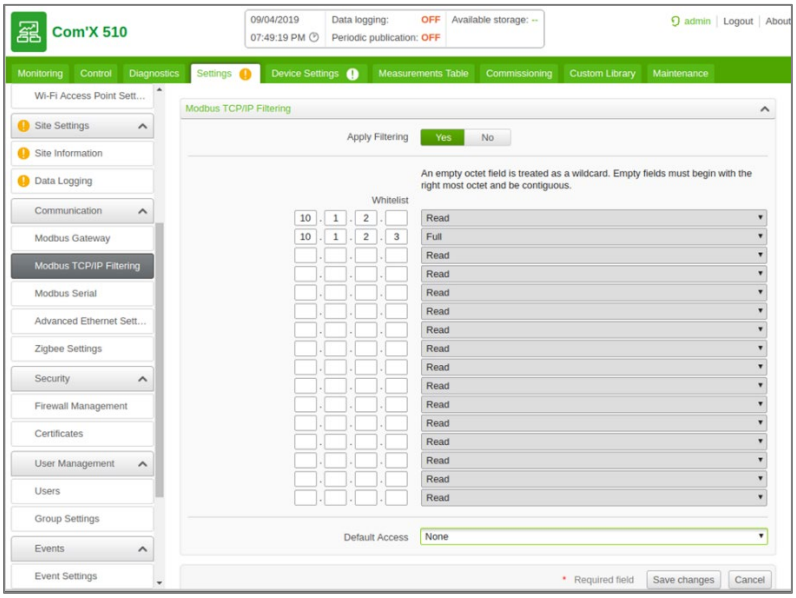
It is recommended to ensure only secure protocols are used when connecting over the WiFi Access Point. Do not rely only on WiFi encryption.

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.



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.