webdyn
Flexitron group

WebdynSunPM
Application Note

Cybersecurity mechanisms

Table of contents

Cybersecurity mechanisms

1 Objective

This document outlines the main cybersecurity mechanisms available in WebdynSunPM to protect access to the product, remote data exchanges, and commands sent via SMS.

It is intended for operators, integrators, and IT teams who need to integrate the gateway into a secure architecture.

2 Summary

WebdynSunPM combines several security mechanisms:

- access to the local web server protected by authentication;
- an SMS command encryption mechanism;
- support for secure protocols for remote file transfers: SFTP, WebDAV over HTTPS, and MQTTS;
- certificate management for TLS connections, particularly for cloud integrations;
- configuration settings that restrict the use of unencrypted protocols.

3 Compliance with EN 18031-1

WebdynSunPM complies with the applicable requirements of the EN 18031-1 standard, which defines common security requirements for radio equipment connected to the Internet.

The mechanisms described in this note contribute to this compliance, including access authentication, communication protection, the use of secure protocols, certificate management, and the reduction of exposure to unencrypted protocols.

4 Access to the local web server

The local web interface is protected by a username and password. The password cannot be left blank and can be changed from the configuration interface.

During the initial setup, the product detects that it is the first time you are logging in and allows you to set the access password. For subsequent logins, you must enter the old password to change it.

Recommended best practices:

- set a unique password for each device or location;
- limit the distribution of the password to authorized individuals;
- change the password during initial setup and after any major maintenance work;
- Avoid reusing a common password across the entire system.

5 Encrypted SMS commands

WebdynSunPM supports an encrypted SMS format identified by the prefix `xen2`.

This mechanism protects commands sent via SMS when an SMS password is configured. The product uses this password to decrypt the received content before executing the command.

The `xen2` format is based on:

- AES-256-GCM for message encryption and authentication;
- PBKDF2-HMAC-SHA256 to derive the key from the password;
- a 16-byte random seed;
- a 12-byte random seed;

- a 16-byte authentication tag;
- standard Base64 encoding;
- automatic splitting into multiple SMS messages when the message exceeds the maximum size for a single SMS.

If the message cannot be decrypted or if cryptographic authentication fails, the command is not forwarded to the application engine.

6 Secure file transfer with SFTP

WebdynSunPM can exchange its configuration files, commands, logs, alerts, scripts, certificates, and data via a remote server.

For file transfers, SFTP is the recommended protocol when the remote server supports it. It provides an SSH-based encrypted channel and prevents credentials and files from being exposed in plain text over the network.

The SFTP server must support a profile compatible with the WebdynSunPM client, specifically:

Category	Required parameter
Host Key Algorithm	`ssh-rsa`
Key exchange	`diffie-hellman-group-exchange-sha256`
Encryption	`aes128-ctr` or `aes256-ctr`
Integrity	`hmac-sha2-256` or `hmac-sha2-512`
Compression	`none`

The server must also be configured with an account dedicated to the hub. It is recommended to limit this account to the strictly necessary directory, disable interactive shell access if possible, and restrict network access to the server.

7 WebDAV over HTTPS

WebdynSunPM can use WebDAV over HTTPS to exchange files with a remote server.

HTTPS encrypts the connection and protects the credentials used for server authentication. When the infrastructure supports it, HTTPS should be used in place of an unencrypted connection.

Recommended best practices:

- use a valid and up-to-date server certificate;
- Avoid using expired or self-signed certificates in production, unless explicitly permitted by IT policy;
- restrict WebDAV account permissions to the directories used by the hub;
- Verify that the expected directories exist on the server side before deployment.

8 MQTTS and cloud integrations

WebdynSunPM supports secure MQTT server types, including MQTTS and variants designed for cloud integrations.

MQTTS adds a TLS layer to the MQTT protocol. Depending on the type of server configured, the connection may use:

- a certificate of certification authority;
- a client certificate;

- a client private key;
- a configured TLS version, with TLS 1.2 as the baseline for secure configurations;
- settings specific to cloud environments such as AWS IoT or Azure IoT.

When MQTTS is available on the monitoring platform side, it should be preferred over unencrypted MQTT.

9 Unencrypted protocols

The product still allows you to configure certain unencrypted protocols to ensure compatibility with existing environments.

These protocols should be avoided in exposed or shared deployments. FTP and MQTT without TLS can expose credentials and application data on the network. They should only be used in isolated, controlled environments that are explicitly permitted by the client's security policy.

10 Deployment Recommendations

For a secure deployment:

- use SFTP or WebDAV over HTTPS for file transfers;
- use MQTTS for MQTT communication;
- use accounts dedicated to WebdynSunPM on remote servers;
- limit the permissions for these accounts to what is strictly necessary;
- store and renew certificates in accordance with the client's IT policy;
- enable SMS encryption when SMS commands are used;
- set passwords specific to the site or equipment;
- restrict network access to administrative interfaces and remote servers.