SYSCON PLANTSTAR
1108 High Street, South Bend, IN 46601
www.plantstar.com

NETWORK SEGREGATION & SECURITY REQUIREMENTS

PlantStar Server Deployment Guide

The required network architecture for your PlantStar MES deployment, and why it matters for the security of your plant.

SYSCON International, Inc. • PlantStar MES • South Bend, Indiana

| Making a difference for PEOPLE in manufacturing

1. Purpose

This document describes the network architecture SYSCON requires for every PlantStar server deployment, and explains the security rationale behind each requirement. It is intended for IT staff, plant managers, and security stakeholders responsible for approving and maintaining the network environment the PlantStar server runs in.

The requirement is simple to state: the PlantStar server must live on its own segregated network segment, it must have outbound internet access for maintenance and support, inbound access must be limited to ports 80/443 only, and no outbound access from PlantStar into the customer's broader network is required or permitted. The sections below unpack what that means in practice and why each element exists.

2. Required Network Architecture

The PlantStar server (APU) should be placed on a dedicated VLAN or subnet that is logically and, where possible, physically isolated from corporate IT systems (ERP, email, file shares, domain controllers) and from plant-floor OT systems that PlantStar does not need to directly reach. Isolation is enforced at the switch and firewall layer, not left to server-level configuration alone.

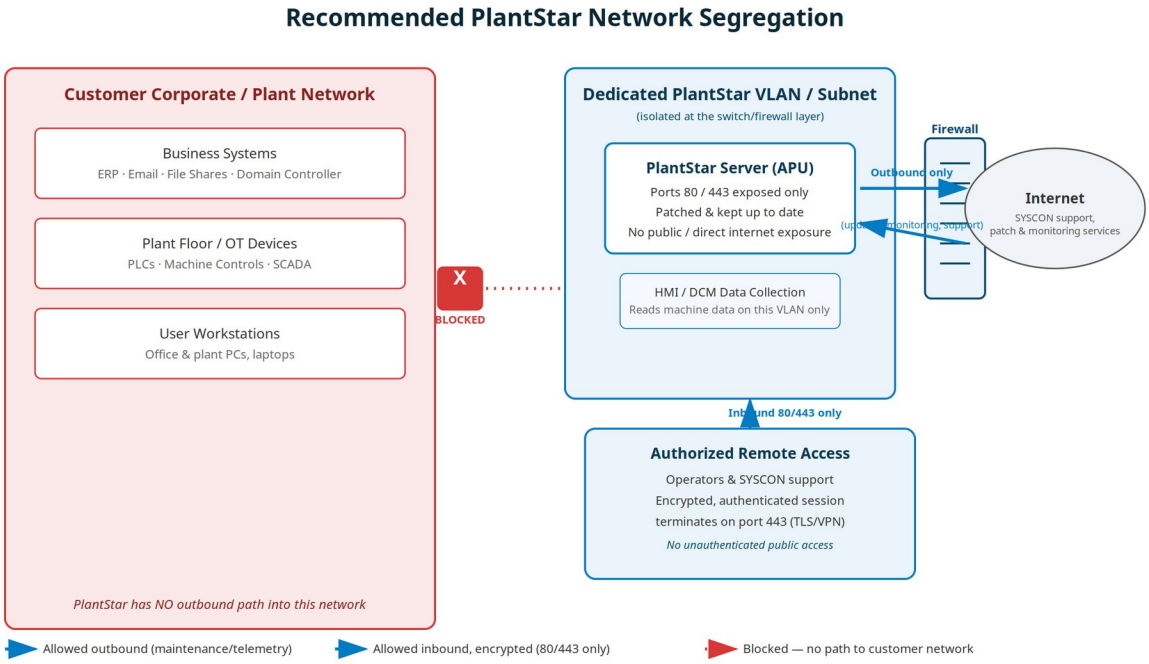

Figure 1: Recommended network segregation for the PlantStar server.

3. Internet Access Requirement

PlantStar depends on reliable outbound internet access to remain current and supportable. SYSCON publishes and maintains the full, current list of required endpoints in the PlantStar Knowledge Base:

kb.syscon-intl.com — What internet access is necessary for your PlantStar 4.0 server?

At a high level, this outbound-only access supports:

- Security and OS patching (Debian package repositories and mirrors, PostgreSQL, Docker, Node.js, and related package sources)
- Remote monitoring and management (RMM agent) so SYSCON can proactively watch server health
- Encrypted support tunnels (WireGuard) that SYSCON support engineers use to reach the server for troubleshooting
- Automated email notifications and alerting (outbound SMTP relay via Mailgun)

If the PlantStar server sits behind a corporate web proxy, contact SYSCON Support (support@syscon-intl.com) before cutover so the required proxy root certificate and configuration can be prepared in advance.

4. Inbound & Outbound Traffic Rules

The firewall rules protecting the PlantStar segment are intentionally narrow. The table and diagram below summarize what is allowed and what is not.

Direction	Traffic	Rule	Status
Inbound	TCP 80 / 443	Only path into the PlantStar server; used for the encrypted web UI and secure remote access	ALLOWED
Inbound	All other ports	No other inbound service is exposed	BLOCKED
Inbound	Unsolicited public traffic	No public access by default; connections are encrypted and authenticated	BLOCKED
Outbound	Customer LAN / OT network	PlantStar does not need, and should not have, a path back into other customer systems	NOT REQUIRED
Outbound	Internet (defined	Patch repositories,	ALLOWED

	endpoints)	monitoring/RMM, SYSCON support tunnel, outbound email relay	

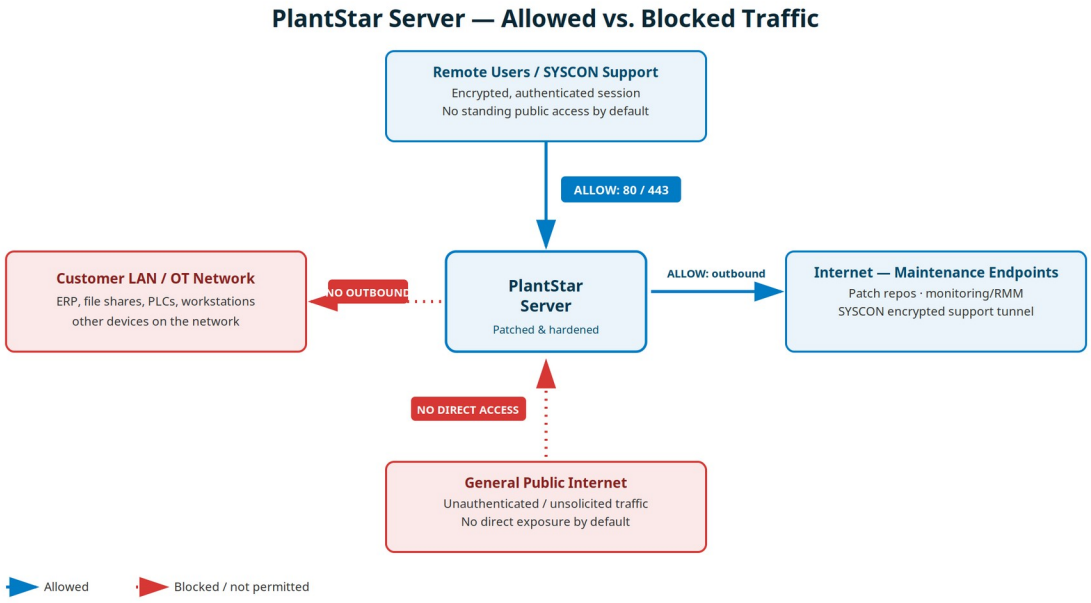

Figure 2: Allowed vs. blocked traffic paths for the PlantStar server.

5. Why This Matters — Security Rationale

Network Segregation Limits Blast Radius

Placing PlantStar on its own segment means that if any single device on the broader plant or corporate network were ever compromised, that compromise cannot pivot laterally into the MES environment — and, just as importantly, if any component in the PlantStar segment were ever affected, it has no network path back into corporate IT or OT systems to spread further. Segregation turns a potential plant-wide incident into a contained one.

No Outbound Path to the Customer Network Removes an Entire Attack Surface

Because PlantStar never needs to initiate connections into the customer's LAN, that path is closed entirely rather than merely restricted. An attacker who gained a foothold on the PlantStar server would find no route to pivot toward ERP systems, domain controllers, file shares, or plant controllers. Removing unnecessary trust relationships is a foundational security control, not an incidental benefit.

A Minimal Inbound Footprint Reduces What Must Be Defended

Exposing only ports 80/443 — and nothing else — means there are only two doors to lock, monitor, and patch instead of dozens. Every open port is a potential entry point; PlantStar's design deliberately minimizes that surface. There is no public access by default, and every remote

session that does reach the server is encrypted and authenticated, so traffic cannot be read or tampered with in transit and unauthenticated parties cannot connect at all.

Controlled Outbound Access Enables Security, Not Just Convenience

The server's limited outbound access exists specifically to keep it secure over time: it is how OS and application security patches are retrieved, how SYSCON's monitoring detects problems before they become incidents, and how support engineers reach the server through an encrypted tunnel rather than an ad-hoc, less secure workaround. Blocking this access would leave the server unpatched and unsupported — a greater risk than the narrowly-scoped access itself.

Defense in Depth

None of these controls stand alone. Network segregation, a minimal inbound footprint, encrypted transport, and disciplined patching work together: if one layer is ever bypassed, the others continue to limit impact. This layered approach is standard practice for any system — like an MES — that bridges IT networks and industrial operations, and it is the same principle recommended by frameworks such as NIST SP 800-82 (Guide to Industrial Control Systems Security) and IEC 62443 for segmenting OT/ICS environments from general-purpose networks.

6. Summary of Requirements

Deploy PlantStar on a dedicated, segregated network segment

- Isolated from corporate IT and unrelated OT systems at the switch/firewall layer

Allow only inbound TCP 80/443 to the PlantStar server

- No other inbound ports or services are required
- No public access by default; connections are encrypted and authenticated

No outbound access is required from PlantStar into the customer network

- This path should remain closed

Allow outbound internet access to SYSCON-published endpoints

- Required for patching, monitoring, and encrypted support access
- See the PlantStar Knowledge Base for the current, complete endpoint list

Keep the server patched and up to date

- SYSCON maintains the server's OS and application patch level as part of ongoing support

7. Questions or Proxy / Firewall Changes

If your organization needs to place the PlantStar server behind a corporate proxy, or if planned firewall changes could affect any of the access described above, contact SYSCON Support at support@syscon-intl.com before making changes so the transition can be coordinated without an interruption in support or monitoring.