

Protokoll

Inbetriebnahmeprotokoll WAMAS

Stumatec · WAMAS Lift & Store 2.8 · SSI LOGIMAT · V 1.0 · 26.10.2026

SSI SCHÄFER

WAMAS®

1 Angaben zur Inbetriebnahme

Angabe	Eintrag
Kunde	Stumatec
System	WAMAS Lift & Store 2.8, zwei SSI LOGIMAT (je mit Firewall ads-tec IRF1401)
Datum / Ort	26.10.2026 / _____
Inbetriebnahme	_____ (SSI SCHÄFER)
Teilnehmende	IT Stumatec: _____ · Key-User: _____

Keine Zugangsdaten

In diesem Protokoll werden **keine** Benutzernamen, Passwörter oder Schlüssel eingetragen. Zugangsdaten werden getrennt im vereinbarten Passwortsafe abgelegt **[auszufüllen]**.

Je Prüfpunkt ankreuzen: **i. O.** (geprüft, in Ordnung), **n. i. O.** (Mangel, unter Bemerkung bzw. Kapitel 6 eintragen), **n. a.** (nicht anwendbar).

2 WAMAS-Server

Nr.	Prüfpunkt	Soll / Eintrag	i. O.	n. i. O.	n. a.	Bemerkung
S1	Hostname	srstulvs101	☐	☐	☐	
S2	IP-Adresse (fest)	10.4.10.21	☐	☐	☐	
S3	Gateway / DNS	10.4.10.1 / 10.4.10.1	☐	☐	☐	
S4	Betriebssystem, Version	[auszufüllen]	☐	☐	☐	
S5	Datenbank (MSSQL 1433 bzw. Oracle 1521)	[auszufüllen]	☐	☐	☐	
S6	WAMAS LS Version / Build	2.8 / [auszufüllen]	☐	☐	☐	
S7	WAMAS-Dienste laufen (BDdeploy 7701)	gestartet	☐	☐	☐	
S8	Uhrzeit synchron (Zeitquelle)	[auszufüllen]	☐	☐	☐	
S9	Windows-Firewall: WAMAS-Ports freigegeben	siehe Kap. 4.2	☐	☐	☐	
S10	Datensicherung vereinbart	[auszufüllen]	☐	☐	☐	
S11	Fernwartung SSI (Weg vereinbart)	[auszufüllen]	☐	☐	☐	

3 Netzwerk und Firewalls der LOGIMATs

Jeder LOGIMAT liegt in einem **LOGIMAT-internen Netz** hinter einer eigenen Firewall. Das **interne Interface (LAN) ist vorkonfiguriert und wird nicht verändert**; angepasst werden nur das externe Interface (WAN), Port-Weiterleitung, Paketfilter und DNS.

Angabe	Firewall FW1 (LOGIMAT 1)	Firewall FW2 (LOGIMAT 2)
Typ	ads-tec IRF1401	ads-tec IRF1401
Seriennummer	AX20416237	[auszufüllen]
MAC-Adresse WAN	00:18:92:08:77:41	00:18:92:08:77:3A
WAN-Adresse (Kundennetz)	10.4.10.104 (DHCP)	10.4.10.197 (DHCP)

Angabe	Firewall FW1 (LOGIMAT 1)	Firewall FW2 (LOGIMAT 2)
LAN (LOGIMAT-intern)	192.168.80.x	192.168.80.x
SPS (PLC)	192.168.80.5	192.168.80.5 [vor Ort prüfen]
IPC LOGIMAT	192.168.80.11 [vor Ort prüfen]	192.168.80.11 [vor Ort prüfen]
LOGIMAT-Bezeichnung in WAMAS	[auszufüllen]	[auszufüllen]
DHCP-Reservierung WAN	☐ eingerichtet (offen)	☐ eingerichtet (offen)
NTP auf der Firewall	☐ eingerichtet (offen)	☐ eingerichtet (offen)

DHCP-Reservierung

WAMAS erreicht die Steuerung über die **WAN-Adresse der Firewall**. Solange diese per DHCP ohne Reservierung vergeben wird, kann sie sich ändern und die Verbindung zum LOGIMAT bricht ab. Reservierung für beide MAC-Adressen (oder feste Adressen) durch die IT Stumatec einrichten lassen.

4 Ports

4.1 Port-Weiterleitungen an den Firewalls

Port (TCP)	Dienst	Weiterleitung an	Von	FW1 getestet	FW2 getestet
2011	NGKP (WAMAS ↔ SPS)	SPS 192.168.80.5	WAMAS-Server	☐	i. O. (getestet vor 26.10.)
2012	NGKP (WAMAS ↔ SPS)	SPS 192.168.80.5	WAMAS-Server	☐	☐
3389	RDP (Fernwartung IPC)	IPC 192.168.80.11	SSI-Support	☐	☐
5900	VNC (Bedienung SPS-Panel)	SPS 192.168.80.5	SSI-Support	☐	☐

NGKP-Ports

WAMAS spricht mit der LOGIMAT-Steuerung über NGKP auf TCP-Ports im Bereich 2000–3000; 2011–2020 werden genutzt, wenn WAMAS und SPS in verschiedenen Netzen liegen. Welche Seite die Verbindung aufbaut, ist in den SSI-Unterlagen nicht belegt (**zu verifizieren**).

4.2 Freigaben zum WAMAS-Server (Kundennetz)

Von	Ports (TCP)	i. O.	n. i. O.	n. a.
Desktop-/Touch-Clients	7701; 8300–8302, 8501, 8503, 8600; 9443, 11000, 11005, 11010; 30010–30013, 30021, 30023, 30040–30043; 8445, 8446, 8453, 31011, 31012, 61616	☐	☐	☐
Browser	8080, 8081, 18002, 30044, 30046, 8161	☐	☐	☐
Mobile-Geräte	8088, 30042, 30043, 30013, 61616	☐	☐	☐
WAMAS-Server → Datenbank	1433 bzw. 1521	☐	☐	☐
ERP ↔ WAMAS	projektspezifisch [auszufüllen]	☐	☐	☐

Quelle: SSI-Portliste WAMAS LS 2.7/2.8 (Netzwerk-Kommunikation und Ports V 1.0, Firewall-Checkliste); Portnummern sind konfigurierbar und gegen die BDeploy-Instanz zu prüfen.

5 Funktionstests

Nr.	Test	LOGIMAT 1	LOGIMAT 2	n. a.	Bemerkung
F1	WAN-Adresse der Firewall vom WAMAS-Server erreichbar	☐	☐	☐	
F2	NGKP-Verbindung aufgebaut, LOGIMAT in WAMAS online	☐	☐	☐	
F3	Anmeldung am Touch-Client, Dashboard erscheint	☐	☐	☐	
F4	Tablar anfordern und retournieren	☐	☐	☐	
F5	Testbuchung Einlagern und Entnehmen, Bestand korrekt	☐	☐	☐	
F6	RDP auf IPC über Port 3389	☐	☐	☐	
F7	VNC auf SPS über Port 5900	☐	☐	☐	
F8	Desktop-Client: Anmeldung, Übersicht Tablare, DI002	☐	☐	☐	
F9	Testdruck Beleg / Etikett (Sprache nur Deutsch ger)	☐	☐	☐	
F10	Uhrzeit Server, IPC und Firewall stimmen überein	☐	☐	☐	
F11	Verbindung nach Neustart der Firewall wieder aufgebaut	☐	☐	☐	

6 Offene Punkte

Nr.	Offener Punkt	Verantwortlich	Termin	erledigt
1	DHCP-Reservierung (oder feste Adresse) für FW1 und FW2	IT Stumatec		☐
2	NTP auf beiden Firewalls einrichten (Zeitquelle [auszufüllen])	SSI / IT Stumatec		☐
3	IPC-Adresse 192.168.80.11 bestätigen	SSI		☐
4	Port 2011/2012 an FW1, Port 2012 an FW2 testen	SSI		☐
5	Seriennummer FW2 eintragen	SSI		☐
6				☐

7 Bestätigung

Mit der Unterschrift bestätigen die Parteien die Prüfung gemäss Checkliste. Offene Punkte werden wie oben vereinbart nachbearbeitet.

	Stumatec	SSI SCHÄFER
Name		
Rolle / Funktion		
Ort, Datum		
Unterschrift		