

FIREWALL UND KOMMUNIKATIONSMATRIX E-CONNECT

Version: 1.5



Inhaltsverzeichnis

1.	Einleitung	1
2.	Firewall und Kommunikationsmatrix e-connect	2
2.1.	Tabellarische Übersicht Firewall und Kommunikationsmatrix	2
2.2.	Allgemeine Protokolle und Ports	4

Sehr geehrte Nutzer,

die folgende Tabelle zeigt Vorgaben, welche in der Firewall und Antivirensoftware berücksichtigt werden müssen, damit eine reibungslose Kommunikation zwischen den einzelnen e-connect-Softwarekomponenten möglich ist.

Bitte beachten Sie, dass e-connect für Microsoft Windows 10 (64Bit) und Windows 11 getestet und freigegeben wurde.

Für die Installation der Software werden erhöhte Benutzerrechte (Administrator) benötigt.

Die Software selbst kann im Benutzerkontext genutzt werden.

Bei Fragen oder Anregungen wenden Sie oder Ihr Systembetreuer sich an support@dampsoft.de.

Vielen Dank

Ihr e-connect-Team

Hinweis!

Bitte nehmen Sie die Einstellungen der Firewall und Antivirensoftware am Tag der Installation von e-connect vor dem Installationstermin vor, um eventuelle Ausfallzeiten zu minimieren und eine reibungslose Installation zu ermöglichen. Ziehen Sie dazu Ihren Systembetreuer hinzu.

2.1. Tabellarische Übersicht Firewall und Kommunikationsmatrix

Hinweis!

Das Kartenterminal in Ihrem Netzwerk muss mit dem Rechner, auf dem der TIC installiert ist, einwandfrei kommunizieren können. In den Einstellungen der lokalen Firewall auf diesem Rechner müssen die im TIC unter „PROXY-PORT“ angezeigten Ports freigeschaltet werden. In der Regel sind dies UDP/TCP-Ports zwischen 5052 und 5057. Wenn Sie die Windows-Firewall nutzen, wird diese Regel automatisch während der Installation gesetzt.

Komponente	Sichtweise	Service	Port	Protokoll	Kommentar	eingehend	ausgehend	Quelle	Ziel
TIC	Richtung Internet	VPN-Verbindung TI-GW	60000 - 60100	UDP	Verbindung zum VPN-Endpunkt für Verbindung zum TI-GW	N/A	Ja	Lokaler Client	213.95.83.58 - Produktivumgebung (PU) 213.95.83.11 - Referenzumgebung (RU)
		TIC-Self-UPDATE-Server	443	TCP	Kommunikation zum Update-Server der TIC-Installationen	N/A	Ja	Lokaler Client	https://client.ti-gateway.de
	Im LAN der Einsatzumgebung	Kommunikation mit Kartenleser	4742 <small>(im Client-Modul und Kartenleser konfigurierbar)</small>	TCP/UPD	Kommunikation zwischen TIC installierten Computer zum Kartenleser	Ja	Ja	Lokaler Client	Kartenleser
		Kommunikation mit Kartenleser	Default 5052 - 5059 <small>(im Client-Modul konfigurierbar)</small>	TCP	Kommunikation zwischen Konnektor und Kartenlesegerät (via TI-GW VPN - Tunnel)	Ja	Ja	Lokaler Client	vKonnektor via TI-GW VPN
		Kommunikation mit Kartenleser	443	TCP	Kommunikation zwischen TIC und Kartenleser für das RemotePIN+ Feature	Ja	Ja	Lokaler Client	Kartenleser
		Kommunikation mit vKonnektor	8443	TCP	Aufruf der Verwaltungsoberfläche des vKonnektors	N/A	Ja	Lokaler Client	https://xxx.xxx.xxx.xxx:8443

Komponente	Sichtweise	Service	Port	Protokoll	Kommentar	eingehend	ausgehend	Quelle	Ziel
KIM-Client-Modul 1.5	Im LAN der Einsatzumgebung	Verzeichnisdienst	636	TCP	LDAP-Proxy des vKonnektors zum TI-Verzeichnisdienst	Nein	Ja	Lokaler Client	vKonnektor via TI-GW VPN
		SMTP-Port	Im Client-Modul konfigurierbar	TCP	SMTP-Port über den Client auf den SMTP-Proxy des CMs zugreifen	Ja	Nein	Lokaler Client	Lokaler Client
		POP3-Port	Im Client-Modul konfigurierbar	TCP	POP3-Port über den Client auf den SMTP-Proxy des CMs zugreifen	Ja	Nein	Lokaler Client	Lokaler Client
		Admin UI (Web)	Default 9443 (Im Client-Modul konfigurierbar)	TCP	Administration des KIM 1.5 CMs über ein Web UI	Ja	Nein	Lokaler Client	Lokaler Client
	Richtung Internet	KIM-Self-UPDATE-Server	443	TCP	Kommunikation zum Update-Server der KIM-Installationen	Nein	Ja	Lokaler Client	https://cm.rise-kim.de/

2.2. Allgemeine Protokolle und Ports

Komponente	Sichtweise	Service	Port	Protokoll	Kommentar	eingehend	ausgehend	Quelle	Ziel
DNSSec			53	TCP/UDP		Nein	Ja		
HTTP			80	TCP		Nein	Ja		
HTTPS			443	TCP		Nein	Ja		
IKE			500	UDP		Nein	Ja		
NAT-Traversal			4500	UDP		Nein	Ja		
HTTPS			8443	TCP		Nein	Ja		

