OmniFab 2022

Machine Insight

User Guide

Network and Hardware Requirements

1 Overview

This document describes the requirements regarding for system and network of the OmniFab Machine Insight solution. Key components of the solution are:

> The Global Control or Global Connect, both part of the Messer cutting machines
> The Messer Exchange Server (MXS, only mandatory for machines with Global Control)
> The Messer Cloud infrastructure reachable via the Internet (Messer Cloud)
> The customer back-office workplaces

2 Hardware Requirements

The Messer Exchange Server (MXS) is only needed when Machine Insight should be used together with a machine with Global Control. It is optional for machines with Global Connect. If the Global Connect machines is not connected to the Messer Cloud through a MXS all MXS related network configurations need to be applied to the cutting machine. It can be deployed as follows:

> Hardware: MCS provides a hardware appliance including all software

> Virtual Machine: Customer provides a Virtual Machine (VM), e.g. VMware

Hardware Requirements:

For options Hardware and Virtual Machine the following requirements must be met.

CPU: >= Intel i3 (64 bit); 2 cores minimum

Main memory: >= 4 GB

Disk space: >= 100 GB

Network Requirements:

10 MBit LAN interface; 100 MBit recommended

3 Messer Exchange Server

For the two options above, Hardware and Virtual Machine, the MXS software environment is created as part of the installation procedure. All software will be provided by Messer. The software is based on the CentOS Linux distribution and will be managed and updated by Messer including security fixes and new functional features.

We recommend that the Messer Exchange Server will be deployed as a virtual machine in the customers' data center.

4 Network Topology and Requirements

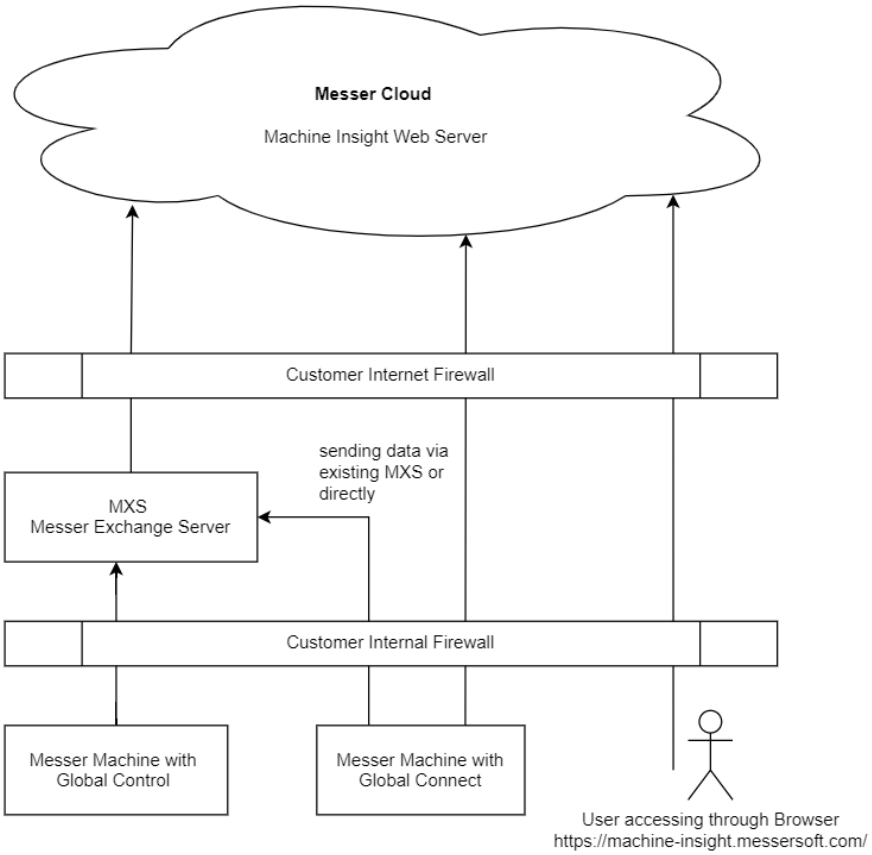
The network topology must allow for the following connections:

> Messer Cutting Machine Global Control → Messer Exchange Server (MXS)

> Messer Exchange Server → Messer Cloud

> Machine Insight Users → Messer Cloud

The following diagram illustrates the core network topology along the following three connections as shown in the diagram above:



The requirements for the network connectivity are described in the following sections.

4.1 Network interfaces

We assume that the MXS is configured as having only one network interface, no matter whether hardware or a virtual machine is used.

4.2 IP Address

The IP address of the MXS must be static or the router DHCP rules must be adjusted to always assign the same IP address to the MXS MAC.

4.3 Network Connection (Messer Cutting Machine GC → MXS)

Requirements:

> The Ethernet network MUST support at least 10 MBit/s.

> The MXS MUST be reachable from all cutting machines via TCP and UDP protocols as specified below.

> The Messer Cutting Machine GC MUST have access to the Network Time Protocol (NTP) to be able to synchronize its time to produce accurate data collections with correct timestamps.

- The MXS SHOULD be used as a NTP time server in cases where the machines are not allowed to directly connect to the Internet or cannot synchronize time otherwise.

> The Messer Cutting Machine GC SHOULD have access to the Domain Name System (DNS).

- This is particularly useful if machines inside the customer network are addressable via DNS and contributes to the reliability of the installation in case IP addresses change.

> The Messer Cutting Machine GC SHOULD have access to the Avahi Zeroconf service running on MXS (mDNS).

- This allows the data collection software on the Messer Cutting Machine GC to automatically detect the MXS IP address during installation.

Firewall rules:

Mandatory:

> Machine → MXS : udp/123 NTP (allow)

Remark: Only needed in case the MXS is used as a time server. But time synchronization is needed in all cases on a cutting machine.

> Machine → MXS: tcp/80 HTTP (allow)

> Machine → MXS: tcp/8443 HTTPS (allow)

> Machine → MXS: tcp/5672 AMQP (allow)

> Machine → MXS: tcp/5671 AMQPS (allow)

Optional:

> MXS → Machine : udp/5353 IP multicast mDNS/Avahi/Zeroconf (allow, not needed for Global Connect)

> Machine → Network : udp/53 DNS (allow)

4.4 Network Connection (MXS → Messer Cloud / Internet)

Requirements:

> Network MUST support at least 10 MBit/s.

> The MXS MUST have access to the DNS and be able to query DNS entries.

> The MXS MUST have access to the Network Time Protocol (NTP) to be able to synchronize its time to produce accurate data collections with correct timestamps.

> The MXS MUST be able to reach the Internet directly or via an HTTP(S) proxy to retrieve software updates.

> Data from the MXS to a Messer Cloud will be sent via the AMQPS protocol (TLS-based strong encryption).

The protocol ensures strong mutual authentication and end-to-end encryption with strong ciphers based on TLS.

Details of which data will be sent is subject to detailed discussion and customer consent.

Firewall rules:

Mandatory:

> MXS→ Network: udp/123 NTP (allow)

> MXS→ Network: udp/53 DNS (allow)

> MXS→ Network: tcp/80 HTTP (allow)
  - alternatively via HTTP(S) proxy
> MXS→ Network: tcp/443 HTTPS (allow)
  - alternatively via HTTP(S) proxy
> MXS→ Network: tcp/5671 AMQPS (allow)

Optional and recommended:

Diagnostics information:

> MXS→ Network: tcp/5044 (allow)
  - This needed to send diagnostic messages of the MXS software to Messer (e.g. remaining disk space, logs of software updates, key software performance indicators, connected machines).
> MXS→ Network: tcp/9000 (allow)
  - This is needed to reconfigure the components that sends diagnostic information above.

4.5 Network Connection (Back-office PCs → Messer Cloud)

Requirements:

> The Messer Cloud must be reachable from back-office PCs via HTTPS (application data) and HTTP (only for redirects and static data like images).
> Access is necessary for:
  - All office PCs / laptops who want to access the OF MI Web applications .
  - All clients who would like to connect to the Messer Cloud in order to (programmatically) retrieve data via REST protocol over HTTPS (TLS encryption).

Firewall rules:

Mandatory:

> Backoffice → Network: tcp/80 HTTP (allow)
> Backoffice → Network: tcp/443 HTTPS (allow)
> Backoffice → Network: udp/53 DNS (allow)
  - Remark: Our applications make use of HTTP headers that require the Web server to be addressed by DNS, not IP addresses

5 Glossary

Term	Meaning
AMQP	Advanced Message Queuing Protocol (Wikipedia)
AMQPS	Advanced Message Queuing Protocol Secure (TLS-based)
DNS	Domain Name Service
OF MI	OmniFab Machine Insight
TLS	Transport Layer Security (Wikipedia)
MXS	Messer Exchange Server
VM	Virtual Machine

6 Technical Annex

The MXS is a Linux-based component that serves as an IoT gateway for data from MCS cutting machines to the MCS Cloud deployment where the Machine Insight Web application is hosted. The operating system is CentOS (www.centos.org) which is derived from the commercial Red Hat Enterprise Linux (RHEL, www.redhat.com, division of IBM).

The MXS appliance is designed to be maintenance-free (from the perspective of the customers) and will receive selected software updates for security and functional enhancement when triggered by MCS. This is done by the MXS querying an update server (provided by MCS) in regular time intervals and requesting, downloading and incorporating configuration changes when they are made available.

The MXS holds certificate-based customer credentials that enable strongly secured and authenticated communication channels downstream to the Web as well as general and customer-specific configuration.

The MXS ensures that machines never need to be connected to the Internet directly. Only the communication from the cutting machines to the MXS is needed to make the overall system work. This allows customers to implement flexible security measures based on network filters and firewalls.

The MXS is designed to reside in a firewall-separated part of the customer-site subnet so that it will passively receive data from MCS machines. The MXS acts as a server and the communication will always be established from the machine to the MXS. The MXS will never actively initiate a connection to a machine.

The MXS can run as a hardware component or a a virtual machine (VM) in both cases.