

ToolsControl 1.9

Datasheet



Contents

Product Overview	3
ToolsControl Architecture	4
Simplified architecture diagram	4
Ports and firewall configuration	5
External ports (single node and cluster)	5
Internal ports (3-node cluster only)	5
Technical specification	6
Recommended hardware specification	6
Frequently asked questions	6
Operational environment	6
Infrastructure	6
Authentication	7
Data	7
Secure SDLC	8

Product Overview

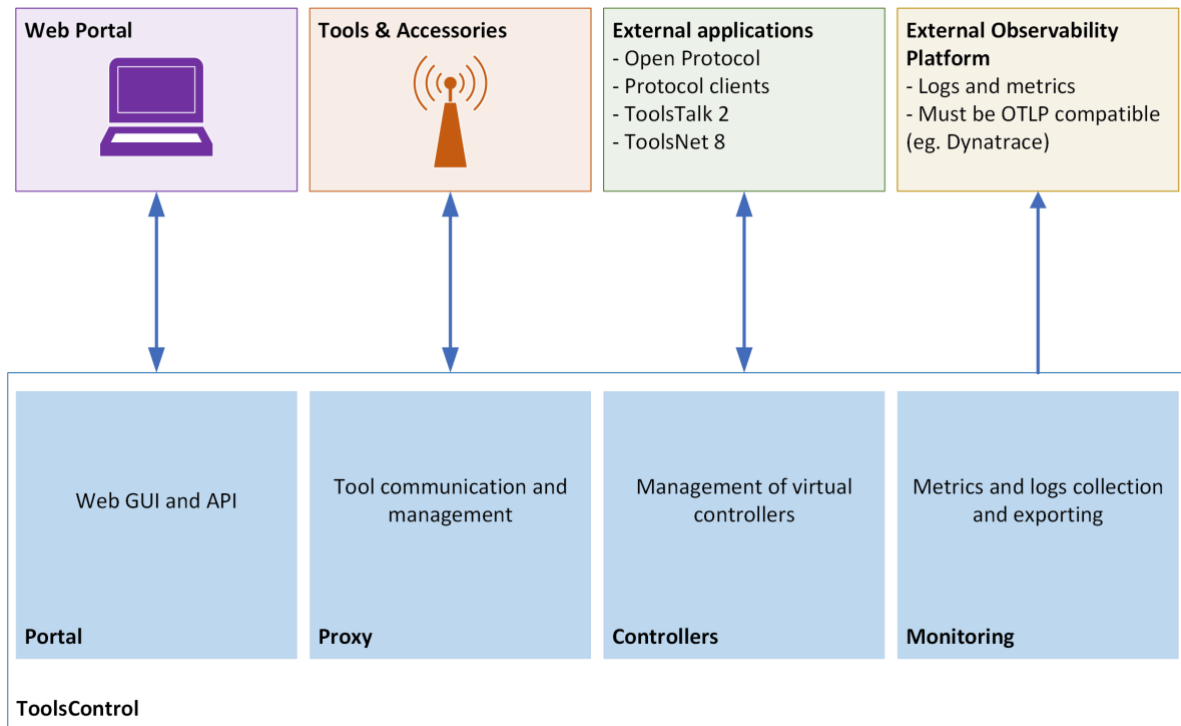
ToolsControl is a collection of applications intended to operate inside a cloud-like environment. The ToolsControl installer includes everything needed to create this environment, to streamline the setup process and provide a turnkey solution that is optimized for the ToolsControl use case. This makes it easy to set up a ToolsControl system without installing and configuring a complete cloud-like environment separately. All that is needed is suitable PC hardware or a system to provision virtual machines (VM's). The ToolsControl system includes tightening controllers that are created on-demand and managed by the ToolsControl Portal and the other services. One such service that is automatically included is a license server that handles all the needed licenses for tools to communicate with controllers via ToolsControl.

The installation methods for ToolsControl nodes include stand-alone PC/server installation and cluster installation. A stand-alone installation means that there is only one ToolsControl node in operation. A cluster installation includes multiple ToolsControl nodes. In general, a typical cluster installation includes three ToolsControl servers.

ToolsControl runs inside a cluster bringing benefits such as failover handling, load balancing, and self-healing. ToolsControl needs no physical devices (controllers) apart from the servers required to run the cluster. The advantages of using ToolsControl contribute to less physical hardware, freeing up floor space for other purposes, and less physical connections, meaning a substantial reduction in power and Ethernet cables.

ToolsControl Architecture

Simplified architecture diagram



The above diagram shows a simplified picture of the ToolsControl architecture with its external interfaces. For correct operation, proper network communication must be ensured between ToolsControl and the external applications and devices. When a network firewall is used, make sure to open the correct protocols and ports. See the next section, *Ports and firewall configuration*, for the relevant port numbers.

Ports and firewall configuration

External ports (single node and cluster)

The following ports must be open for external communication to/from ToolsControl, regardless of if installed as a single node or a cluster. On top of this, any *external applications* must be allowed, like Open Protocol, ToolsNet, OTLP, etc.

Protocol	Port Number	Direction	Description of usage
ICMP		In/Out	Ping messages to measure response times connected tools
OSPF		In/Out	Only if using multi-subnet with OSPF routers
TCP	53	Out	DNS resolution, must be allowed to working DNS server
TCP	80	In	Web http. Should be disabled with https redirect in the portal.
UDP	123	In/Out	NTP protocol for time synchronization
TCP	179	In/Out	Only if using multi-subnet with BGP routers
TCP	443	In	Web https
UDP	6677-6678	In/Out	Tool communication (e.g., SRB, STB, TBP, STwrench, MWR)
TCP	8081	In	Bluetooth Gateway web (node IP, not Single IP)
TCP	25000	In	Accessory communication (I/O Hub, CAN Converter, Selector 6)
TCP	61200-61202	In/Out	Tool communication PFS (e.g., ST, STR)
TCP	62000-62030	In/Out	Tool communication (e.g., ITB, ICB, IPB)

Internal ports (3-node cluster only)

The following list of ports must be open between all the nodes in a cluster.

Protocol	Port Number	Description of usage
VRRP		Internal cluster keep-alive messages for failover detection
ICMP		Ping messages to measure response times for cluster nodes
UDP	123	NTP protocol for time synchronization
TCP	2377	Cluster communication
UDP	4787	Cluster communication
TCP	5000	Software library
TCP	7946	Internal cluster communication
UDP	7946	Internal cluster communication
TCP	8081	Bluetooth Gateway web (node IP, not Single IP)
TCP	8082	Internal cluster communication (node IP, not Single IP)

Technical specification

Recommended hardware specification

	Max tools	Max controllers	Type	Disk	CPU	Memory	Cluster network
Small	50	10	Cluster (3 nodes)	SSD 100 GB	4 threads *	6 GB	1 Gbit/s
Medium	100	25	Cluster (3 nodes)	SSD 100 GB	4 threads *	6 GB	1 Gbit/s
Large	200	50	Cluster (3 nodes)	SSD 100 GB	8 threads *	8 GB	1 Gbit/s
Large+	300	100	Cluster (3 nodes)	SSD 150 GB	16 threads **	16 GB	10 Gbit/s
Extra large	500	200	Cluster (3 nodes)	SSD 200 GB	32 threads **	32 GB	10 Gbit/s

* Intel Core i5 @ 1.5 GHz or better

** Intel Xeon @ 2.0 GHz or better

Threads refers to the number of HW threads in the CPU. This is usually 2x the number of cores.

Frequently asked questions

Operational environment

What operating system is required for ToolsControl?	None. ToolsControl uses its own OS. The installer includes everything needed. It is not possible to install ToolsControl on Windows.
What is needed for an installation?	A blank virtual machine or an empty PC without operating system.
What Virtual Machine environments are supported?	VMWare-based, Qemu-based, and HyperV virtual machine environments supported.
I want to install directly on hardware, without VM (bare metal). What is supported?	Only supported on desktop-class PC's. Not supported on server-grade machines (use VM if installing on server, see above).
What is the recommended hardware?	See <i>Recommended hardware specification</i> above.

Infrastructure

What programming languages/frameworks are used by the application?	There are no dependencies, nothing extra needs to be provisioned for ToolsControl to run. Internally, the backend application is written in Go, supported by Gin web framework and Gorm database ORM. Frontend web application is React JS.
--	--

What backend technologies are used? (e.g., MySQL, memcached, nginx, etc.)	There are no dependencies, nothing extra needs to be provisioned for ToolsControl to run. Internally, embedded databases using SQLite. Embedded webserver using gin. Docker Swarm for container orchestration and load balancing. Keepalived for IP redundancy. Prometheus for metrics and OpenTelemetry Collector for logs and metrics. Flexera license server. Traefik proxy. Gluster FS. BIRD router for BGP/OSPF.
What operating systems are used to host the above applications and services?	There are no dependencies, nothing extra needs to be provisioned for ToolsControl to run. Internally, ToolsControl includes Ubuntu Linux 22.04. Custom immutable installation.
Is the application integrated with other internal or external systems?	Typically integrated with MES system over Open Protocol

Authentication

Is there support for multi-factor authentication? If so, what methods?	No
Is there support for federation? If so, how? (e.g., SAML, LDAP, etc.)	Federation of user credentials over LDAP(S)
Is the platform co-tenancy/multi-tenant?	No

Data

What data is stored/processed?	Configuration data is stored. Tightening results are stored and processed, then sent out over TCP/Open protocol message. User authentication logs. Minimal basic user meta data from LDAP.
Is data encrypted in transit?	Internal cluster communication is encrypted. Web traffic is also encrypted (https), communication with Atlas Copco wireless tools is not (raw UDP, Wi-Fi encryption only), communication over Open Protocol is not (raw TCP).
Is data encrypted at rest?	No
Who has access to the data?	Data is available over Open Protocol if enabled. Data can be browsed through the web application if authenticated.
How are backups stored, and for how long?	There is no internal backup storage or automation. Backups need to be actively pulled to external backup storage through the web application or using the REST API.

Secure SDLC

What methodologies do you use for security review? (e.g., automated scans, manual testing, code review, etc.)	Code review, manual and automatic testing, CVE scan using Black Duck
Do you use a third-party to assess security? If so whom, and how regularly?	Black Duck scan for every major and minor release. No major vulnerabilities accepted.
What is your estimated remediation time for a given vulnerability?	Depending on the criticality of the vulnerability. Following Ubuntu LTS security updates, hotfix patches will be released as soon as possible.