



Identity-based access control for connected devices.

The missing piece in IT, OT and IoT security. Policy graph, just-in-time access, traffic discovery, WebAccess, traffic mirroring, scoped administration.

Fourteen features of your XoT technology system.

01 Protect without changing the network 03

02 Micro-segmentation inside a subnet 04

03 Policies: access control in XoT 05

04 Just-in-time access 06

05 Access approval 07

06 Policy Graph for security posture 08

07 Policy verification with inline graph 10

08 Traffic Discovery, with AI-written report 11

09 WebAccess 13

10 XoT-Desktop Client 15

11 Scoped administrators 16

12 Traffic Mirroring 17

13 XoT-Bridge 18

14 Secured end to end 19



Put a Lock in front of an asset. The asset keeps its IP, gateway and VLAN.

01 Insert the Lock inline

Between the switch and the device. Nothing is reconfigured on the asset itself.

02 Same address on both sides

The asset keeps its IP, gateway and VLAN. The rest of the network reaches it the way it always has.

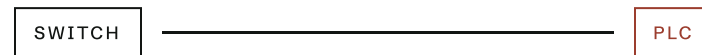
03 Invisible until permitted

From the moment the Lock is in place, only policy-permitted traffic reaches the asset.

Built for legacy OT

Devices that cannot be reconfigured or patched get protection in place. No downtime, no IP changes.

BEFORE



192.168.10.20 · VLAN 10 · reachable by anyone

AFTER



192.168.10.20 · VLAN 10 · policy-permitted only

Fig. 1 Same address, now protected. Only permitted traffic passes the Lock.

Isolate a device or a group in the same subnet, without touching the network design.

01 One Lock per device or group

In front of a single device, or in front of a group that should be treated as one segment.

02 Policy decides who talks to whom

Lock-to-Lock (M2M) connections are permitted per port and protocol. Everything else in the subnet is blocked.

03 No new IPs, no new VLANs

The flat network stays flat. Only the trust model changes.

Stops lateral movement in flat networks

A compromised workstation can no longer reach the PLCs next to it.

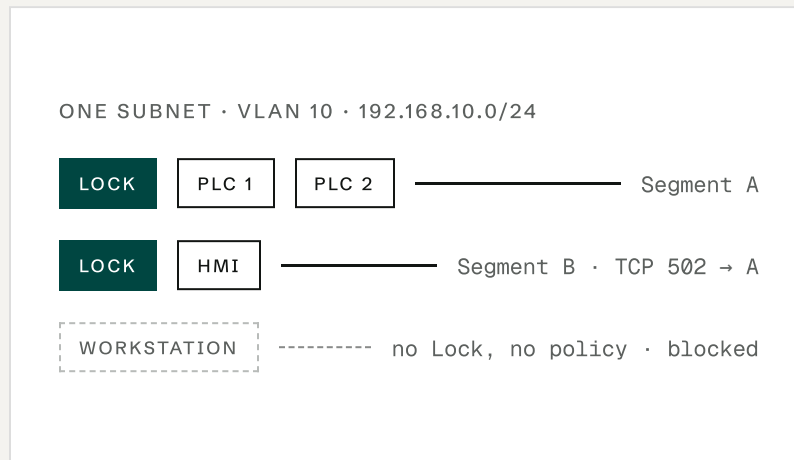


Fig. 2 Policy: HMI → PLC group on TCP 502 only. The workstation shares the subnet but cannot reach any of them.

Who can access what, how, and when. No IP addresses required.

SOURCE

Who

User groups from your identity source, or machines by type and location.

TRAFFIC

How

Permitted ports and protocols only. Everything else is denied.

DESTINATION

What

Assets by type and location. Attributes, not IP addresses.

EXAMPLE POLICY

SUPERUSER · GROUP

REMOTE ACCESS TO PLC

PLC #34 · STOCKHOLM · CELL 34

TCP 502 · Thursday 09.00-13.30 · from EWS client, Stockholm

Just-in-time by design

Policies can be time-limited, scheduled once or recurring, and can require approval by a designated administrator.

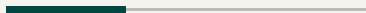


No standing access. Granted by schedule or approval, expiring on its own.

COUNTDOWN

Time-limited from activation

Active for a set duration, then expires automatically. E.g. four hours from activation.



ONE-OFF

A specific window

Active on a specific date, between set start and end times. E.g. a maintenance window.



RECURRING

Repeats automatically

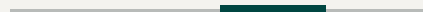
Repeats on a schedule and is closed outside each window. Thursdays 09.00-13.30, every week.



ON APPROVAL

Request-driven

Granted per request by an administrator, then expires. Detailed on the next slide.



Zero standing privileges

Whether scheduled or approved per request, access is closed by default and expires on its own, drastically reducing the attack surface.



Just-in-time access with human oversight.

ADMIN

Create policy

Assets are marked requestable for selected users.

USER

Request access

Reason and time slot, or hours from approval.

APPROVER

Review request

Gets an e-mail with the request and its reason. Rejections are sent back with a reason.

USER

Session active

Policy activates; tunnel open for the approved window.

USER

Session ends

Expires at end time or is ended early by the approver.

Requested, approved, time-limited, closed

Requester and approvers are notified by e-mail on every state change and before requests or sessions expire. Never open longer than needed.



Who can reach what, through which policy, read from the saved configuration.

01 Ask in both directions

Who can reach a specific device, or what can this user or group reach.

02 Get the answer as a graph

Every path is drawn: user → group → policy → asset. Nothing is inferred.

03 Verify your security posture

Spot over-privileged users, unexpected paths and forgotten policies. Show auditors the evidence (NIS2, IEC 62443).

Shows every policy in the system

Active, scheduled and inactive policies are all drawn. Nothing is hidden.

WHO CAN REACH WHAT · EXAMPLE

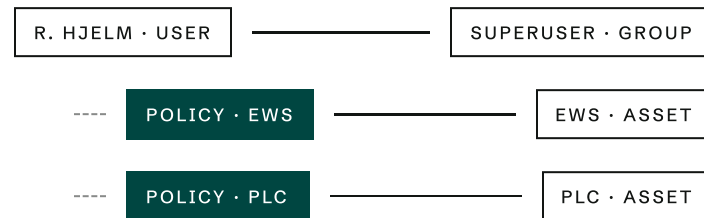


Fig. 3 One user, one group, two policies, two assets. Four real examples on the next slide.

Four questions an auditor asks, each answered with one picture.

QUESTION

What does Rikard Hjelm have access to?

Two assets, EWS and PLC, both through the SuperUser group.

QUESTION

Who can access the EWS system?

Seven users through two policies, including all consultants.

QUESTION

Who can access SCADA?

Two user groups and the EWS client. Every path and policy in one view.

QUESTION

What can the Consultant group access?

PLC, SCADA HMI and EWS, all via Consultant Access.

Preview what a policy would match, before anything is saved or enforced.

The same graph runs while you build a policy. Access Overview shows what it would match if saved as configured.

01 Every user the source group resolves to

02 Every asset the type and location match

03 Updates live as you change a field

SOURCE · DESTINATION · ACCESS OVERVIEW

CONSULTANTS

DRAFT POLICY

PLC

7 users resolved · 3 assets matched

Not saved. Not enforced. Drawn from what the fields currently match.

Fig. 4 Access Overview draws the graph while you fill in the policy.

See what a protected asset really talks to. Then write the policy that permits exactly that.

01 Capture on the Lock

Every flow through a Lock is recorded at the 5-tuple level and sent to the XMS.

02 Read it in the XMS

Grouped per protected device: which hosts it talks to, on which ports, and how much data.

03 Let AI write the report

Export the flows to an AI tool for a plain-language report and suggested policies.

From unknown to least privilege

Start with a temporary any-to-any policy, discover the real traffic, then replace it with scoped policies.

XMS FLOW LIST · GROUPED PER PROTECTED DEVICE

PLC → 10.2.0.5 : 502/tcp · 1.2 GB

PLC → 10.2.0.9 : 123/udp · 3 MB

HMI → 10.2.0.5 : 443/tcp · 640 MB

Sensor → 10.2.1.4 : 1883/tcp · 12 MB

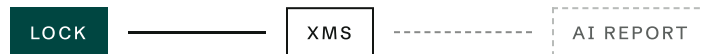


Fig. 5 Any-to-any while discovering; scoped policies when done.

Export the flows from the XMS and get a report you can hand to the asset owner.

01 Flow map per Lock

Which protected devices talk to which hosts, ports and protocols.
Drawn, not listed.

02 Aggregated flows

One row per source, destination and service, with volumes and packet counts.

03 Findings and suggestions

Plain-language observations, and least-privilege policies ready to create in the XMS.

Bring your own AI. Not part of XoT.

The report is produced by an external, third-party AI tool of your choice. XoT only exports the plain flow data; the AI model, on-prem or hosted, is yours.

EXAMPLE REPORT · GENERATED BY AN EXTERNAL AI
TOOL

Page 1 · summary and flow map

Page 2 · aggregated flows and findings

3RD-PARTY TOOL · NOT XoT



Browser-based access to protected assets. Nothing to install on the user's device.

01

Log in

Browser to the WebAccess server. Same IdP, MFA and credentials as the XMS.

02

Private desktop

A per-user Debian container starts on demand and is streamed to the browser.
No plugins.

03

Session PKI

Fresh certificates from the XMS, valid for this session only, used by the Desktop Client inside the container.

04

Tunnel to the Lock

Ticket, Access Request and WireGuard tunnel, exactly as a regular client. Full policy enforcement.

Session recording

Every WebAccess session can be screen-recorded, giving a full audit trail of what was done on protected assets.

Session-scoped by design

When the session ends, the container and its credentials are discarded. Nothing remains on the device.



HTTPS to WebAccess. WireGuard from the container to the Lock.

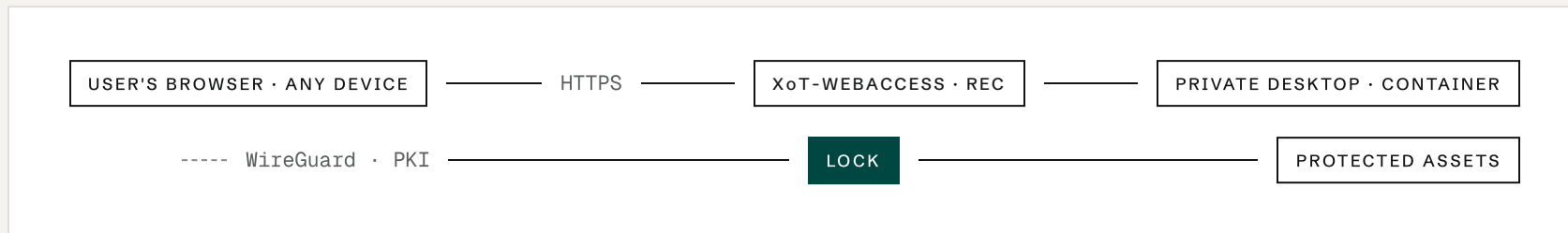


Fig. 6 Browser to WebAccess over HTTPS with the XMS IdP. From the container, a PKI-authenticated WireGuard tunnel to the Lock, with the same ticket, Access Request and policy as any client.

One client for every user. Your identity provider for login, your choice of key storage.

01 Installed once, then it just works

Points at your XMS, or is pre-configured via Intune/MDM. Tunnels come up as soon as a policy is active.

02 Logs in through your IdP

Password, MFA, or whatever your identity provider requires. Users and groups from LDAP or Entra ID.

03 Private key stored where you decide

The key signs the challenge-response that runs inside every tunnel, twice a minute.

Headless for servers

The same client runs as a system service with no GUI. Same authentication, tunnels and policies.

WHERE THE USER'S PRIVATE KEY LIVES

File-based key

Stored as a file on the PC. Quick to roll out, nothing extra to buy.

Device TPM

Sealed in the computer's TPM. Bound to that device, cannot be copied.

Hardware key

On a YubiKey or smart card. Possession + PIN. Highest assurance.

CONVENIENCE

ASSURANCE

All three work with the same policies, tickets and tunnels. The choice is per user or group, not per system.



Each administrator manages only their own site or customer. One XMS, delegated administration.

01 A scope is a slice of the XMS

Locks, assets and policies that belong to one site or customer.

02 Full control inside the scope

Enroll Locks, create assets and policies, for their own scope only.

03 Read-only outside it

Other scopes and global settings can be viewed but not changed.
Only the super admin manages everything.

Built for MSPs and multi-site organisations

One XMS serves many customers or sites, with strict separation of who may change what.

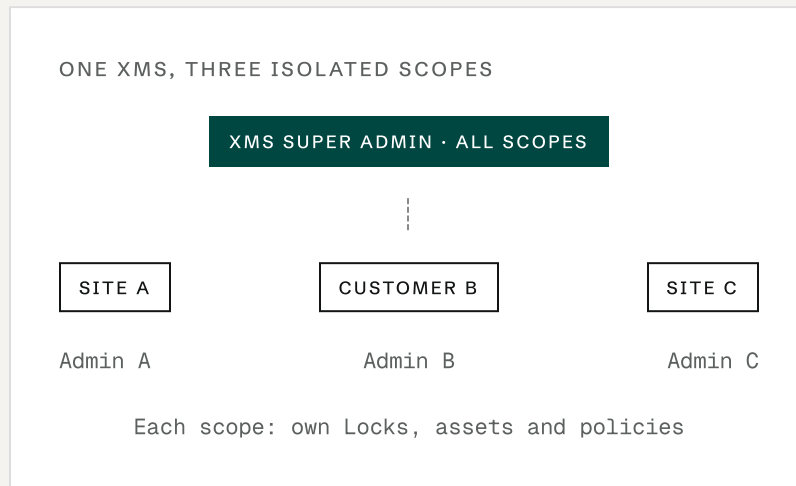


Fig. 7 No management rights across scopes.

Every packet passing the Lock, copied to your monitoring tools for deep analysis.

01 The entire packet is mirrored

Headers and payload, exactly as they passed the Lock. Not a summary or a flow record.

02 Delivered to your receiver

SIEM, IDS/IPS or a recording server on your network gets the copy in real time.

03 Built for deep analysis

Deep packet inspection, forensics and OT protocol anomaly detection on real traffic.

Complements Traffic Discovery

Discovery shows the 5-tuple picture in the XMS; mirroring gives your security tools the full packets.

WHAT THE LOCK DOES WITH EACH PACKET



Original traffic forwarded. Full packet copy mirrored.

Fig. 8 Original traffic is forwarded; a full copy is mirrored.

Reach Locks behind firewalls without opening a single inbound port.

01 Outbound only

Clients from outside and Locks from inside both connect out to the Bridge. No inbound firewall rules, anywhere.

02 One entry point, hundreds of Locks

Deployed in the cloud or a DMZ with a public IP. Adding a Lock never means touching the firewall again.

03 Never sees your data

Forwards the WireGuard tunnel without decrypting it. Its own PKI identity; every client authenticates to it.

Made for Remote Access

Bridge and Software Lock are the same software in different modes.

HOW THE BRIDGE CONNECTS BOTH SIDES

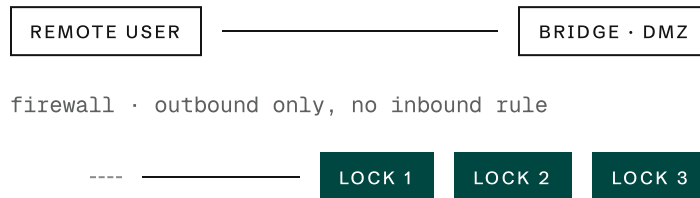


Fig. 9 Client tunnel ends at the Bridge; a second WireGuard tunnel runs on to the Lock. Ticket tries the Lock directly first, Bridge when it is not reachable.

Every component has a cryptographic identity. Every connection is authenticated and encrypted.

01 PKI identities for everything

Locks, clients, Bridge and XMS each hold a certificate from the built-in CA or your own. No shared secrets.

02 WireGuard for all access traffic

Mutual PKI authentication in the Access Request, then a WireGuard tunnel. Challenge-response twice a minute.

03 Secure MQTT for management

Certificate-secured MQTT session to the XMS on port 443. Policies, tickets and telemetry travel only there.

Zero trust, cryptographically proven

Nothing is trusted because of where it sits on the network. Identity is proven at every step.

TWO CHANNELS, ONE PKI

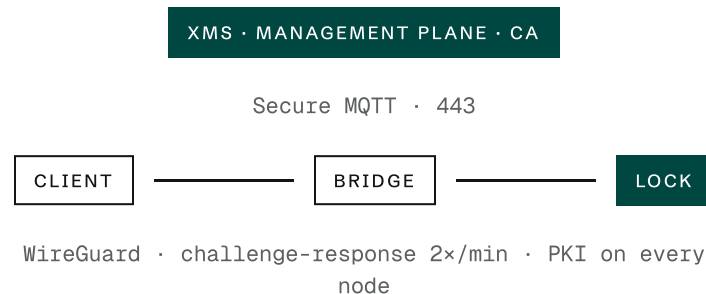


Fig. 10 Management over Secure MQTT; access traffic over WireGuard. PKI certificate identity on every component.



XoT TECHNOLOGY · DELIVERED BY XERTIFIED

Everything connected can be exposed. Until now.