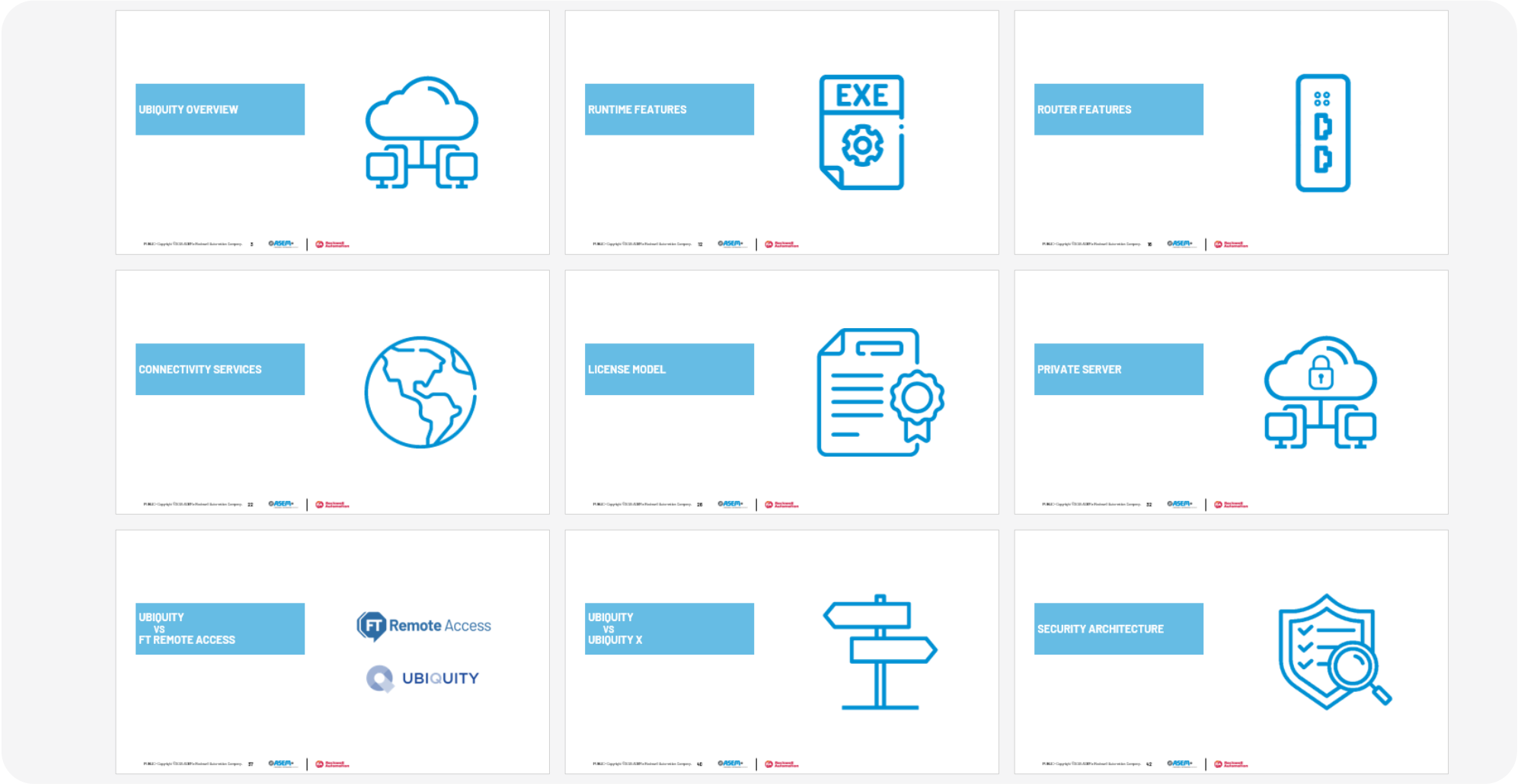
# UBIQUITY

## SECURE REMOTE ACCESS FOR INDUSTRIAL AUTOMATION DEVICES

v28.00 – February 26

A ROCKWELL AUTOMATION COMPANY

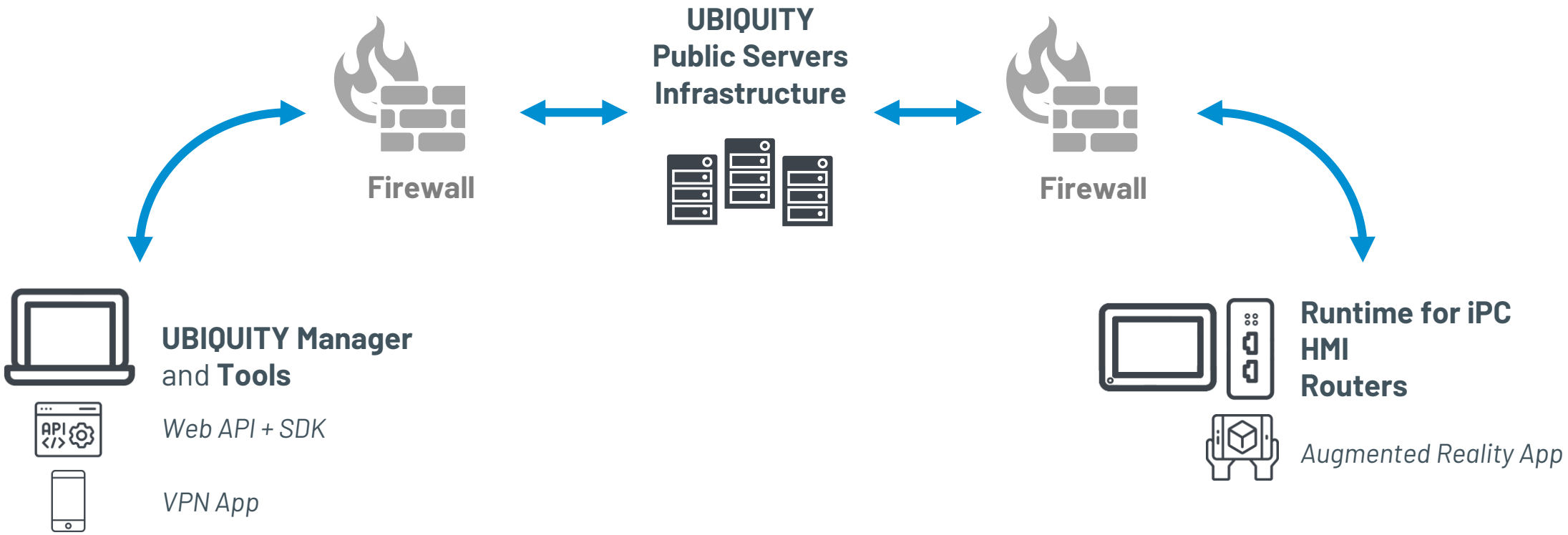
# SUMMARY


UBIQUITY OVERVIEW
RUNTIME FEATURES
EXE
ROUTER FEATURES
CONNECTIVITY SERVICES
LICENSE MODEL
PRIVATE SERVER
UBIQUITY
VS
FT REMOTE ACCESS
FT Remote Access
UBIQUITY
UBIQUITY
VS
UBIQUITY X
SECURITY ARCHITECTURE

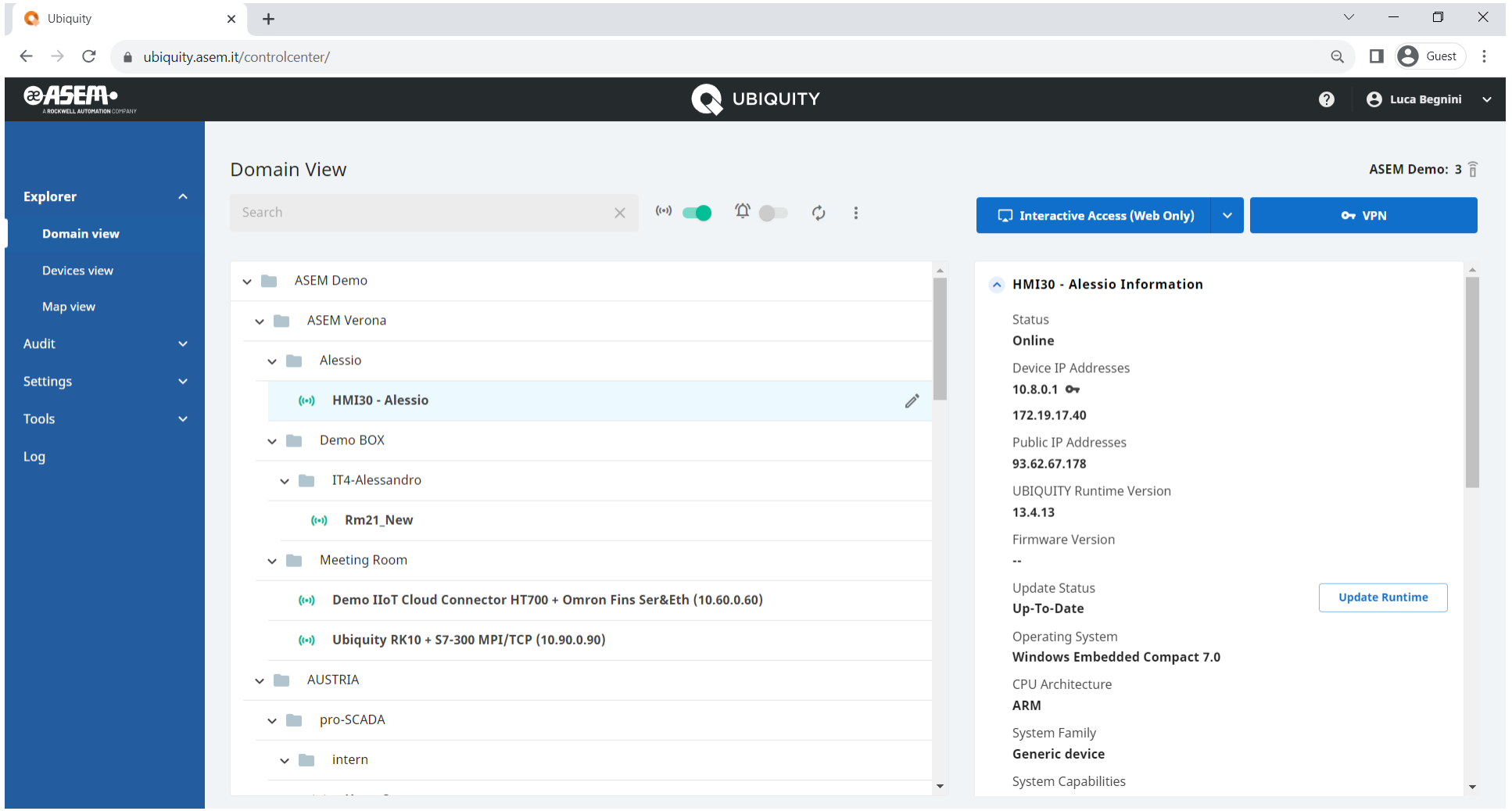
# UBIQUITY OVERVIEW

# OVERVIEW

- UBIQUITY Manager and UBIQUITY Manager Tools
- UBIQUITY Public Server Infrastructure
- Runtime, HMI and Routers



# OVERVIEW: UBIQUITY MANAGER



# OVERVIEW: PUBLIC SERVER INFRASTRUCTURE

## Redundant

7+ Relay servers located distributed all over the world

2+ Access servers in Europe

provides Continuity of Service and High Performances

## Scalable

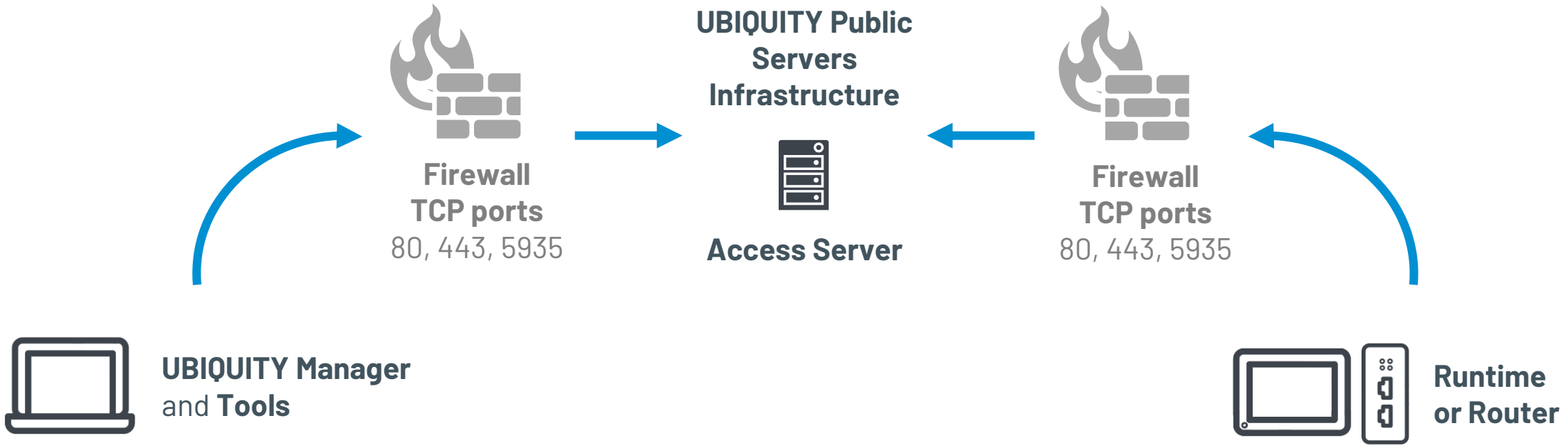
Unlimited Runtimes and devices manageable

Unlimited Users and Groups

Unlimited traffic between UBIQUITY Manager and remote systems

# OVERVIEW: PUBLIC SERVER INFRASTRUCTURE AUTHENTICATION

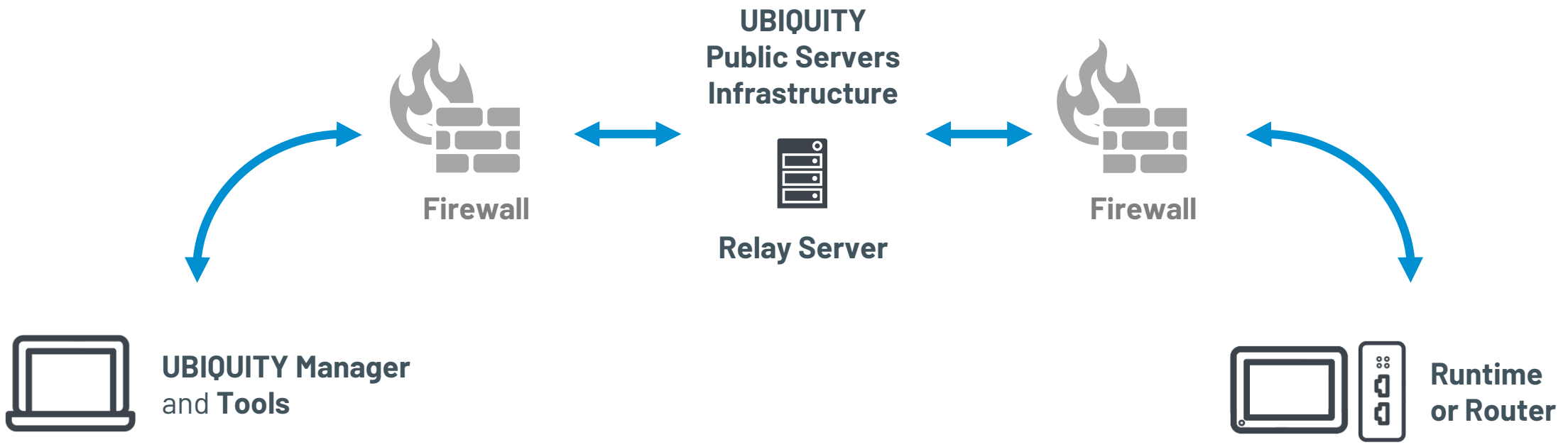
UBIQUITY Manager Tools, Runtime and Routers authenticates to one of the UBIQUITY Access Server using outgoing connections (SSL/TSL) usually allowed by firewall policies



# OVERVIEW: PUBLIC SERVER INFRASTRUCTURE CONNECTION

When UBIQUITY Manager wants to connects to a Runtime/Router:

- Endpoints agree on the Relay Server with best round-trip time
- The secure end-to-end connection will be established with the Relay Server
- Relay Server forward encrypted messages without being able to decrypt them



# UBIQUITY OVERVIEW: RUNTIME FOR IPCS


## CROSS-PLATFORM APPLICATION

Installable on third-party iPC

pre-installed on all ASEM's iPC

Available from WinCE up to Win10 and Linux Ubuntu22

## INTERACTIVE ACCESS

allows interactive access to remote systems with audit


## VPN ACCESS

Secure access to the device and to the automation subnet

# UBIQUITY OVERVIEW: HMIS

## EMBEDDED OPERATOR INTERFACE

Ubiquity Runtime Embedded

Can provide physical network separation

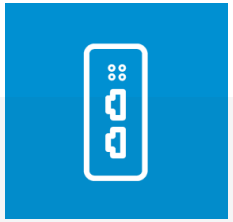
## INTERACTIVE ACCESS

allows interactive access to remote systems with audit


## VPN ACCESS

Secure access to the device and to the automation subnet

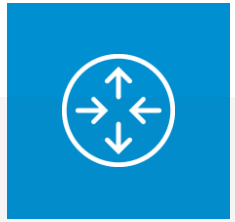
# UBIQUITY OVERVIEW: ROUTERS



## ROUTER APPLIANCE

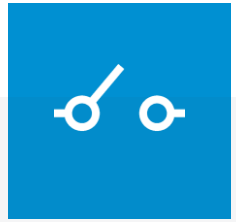
Ubiquity Runtime embedded

Provide physical network separation



## NETWORKING CAPABILITIES

Routing, NAT, Internet Sharing and can provide Wifi/4G connection



## EMBEDDED I/O

Remote access management via digital I/O


## VPN ACCESS

Secure access to the device and to the automation subnet

# RUNTIME FEATURES

# RUNTIMES FEATURES: INTERACTIVE ACCESS

## REMOTE DESKTOP

VNC-like feature with
remote input lock and multi-monitor support

Allow to chat with remote users
with conversation log *

## TASK MANAGER

Allow to check RAM and CPU usage
of process running on the remote system

Process termination

Remote System Reboot

## FILE TRANSFER

Allow to transfer files
to/from remote systems

## MULTICLIENT SUPPORT

A remote system
manages multiple
concurrent connections

* chat is currently available only on Runtime for Wiindows and on ASEM HMI25/30/40

# RUNTIMES FEATURES: VPN

## VPN TO THE DEVICE

Optimized for industrial communications

The VPN Server it's at Runtime level
not on the Server Infrastructure

## IP CONFLICT RESOLUTION

Conflicts are solved
by UBIQUITY VPN virtual adapter
with the use of metric


## DATA LINK - LAYER 2

No routing rules required

No default gateway required

Service PC gets a real remote subnet IP

Supports broadcast messages

## FIREWALL and ROUTING RULES

VPN traffic can be filtered by Firewall rules
with a set of predefined rules ready-to-use

VPN traffic can be routed
by static routing rules

# RUNTIMES FEATURES: ADVANCED

## VPN TO THE SUBNET

VPN can be established
with the automation's subnet
to reach PLC, Drives
of the machine/plant

## INTERNET SHARING

Provide internet access
to devices of automation's subnet

Filtered by MAC-Address

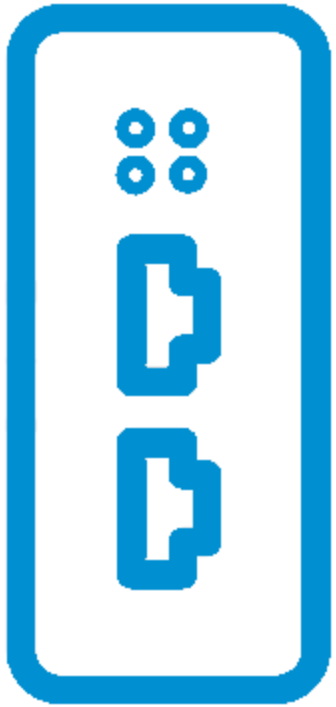
## USB PASS-THROUGH

Allow to access a remote device
connected to the remote system
via USB port

## SERIAL PASS-THROUGH

Allow to access a remote device
connected to the remote system
via Serial port

# ROUTER FEATURES



# UBIQUITY ROUTERS: WHY?

- if a **physical network separation** between the automation subnet and customer/internet subnet is required
- if a wired connection is not available, so a **Cellular or Wi-Fi connection** is needed
- if the **Runtime cannot be installed**, like operator panels with proprietary OS or managed by others

# UBIQUITY ROUTERS: KEY FEATURES

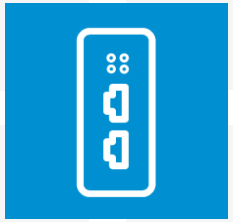
## NETWORKING CAPABILITIES

VPN and Advanced features
provided by the UBIQUITY Runtime
+
Routing and NAT

## EASE OF MANAGEMENT

Configuration via USB Memory
or via System Manager

Remote firmware upgrade



## PROTECTION

Protection against
unauthorized domain change

## SECURITY INCREASE

Embedded I/O allows
to physically accept and check
the Remote Connection

# UBIQUITY ROUTERS

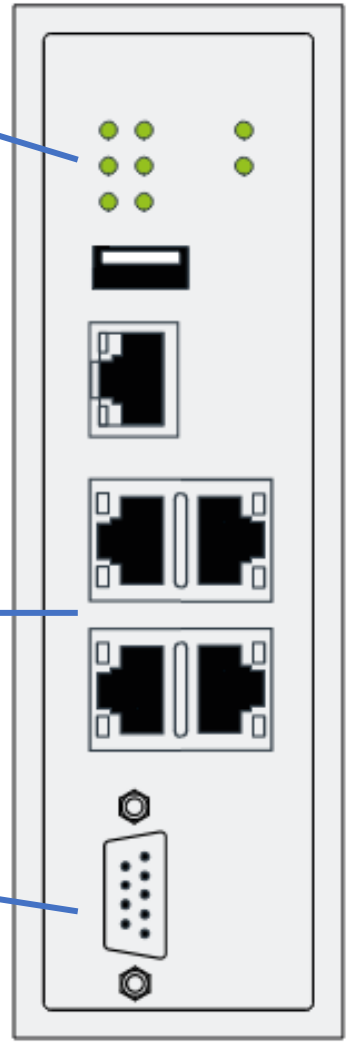
| Features | RK20 | RK21 | RK22 |
|---|---|---|---|
| USB 2.0 | 1 | 1 | 1 |
| WAN Gigabit | 1 | 1 | 1 |
| LAN Gigabit | 1 | 1 | 4 |
| Serial port (multi-standard isolated) | ✓ | ✓ | ✓ |
| WiFi | X | ✓ | ✓ |
| 4G Modem | X | ✓ | ✓ |

# UBIQUITY ROUTERS: DETAILED VIEW OF RK22

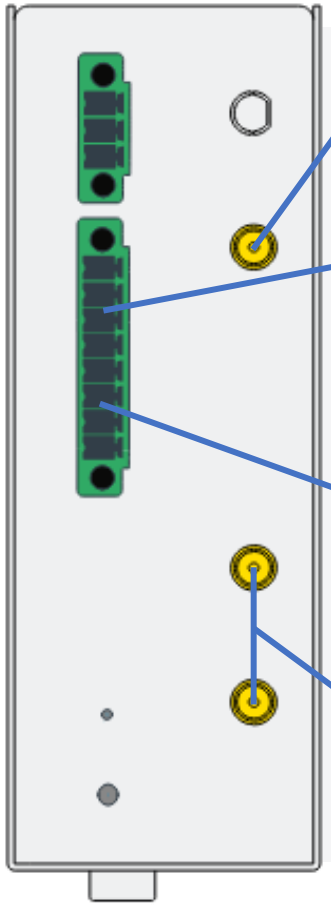
Status LEDs

integrated Ethernet switch

Serial Port



*Frontal View*



*Upper View*

4G Modem

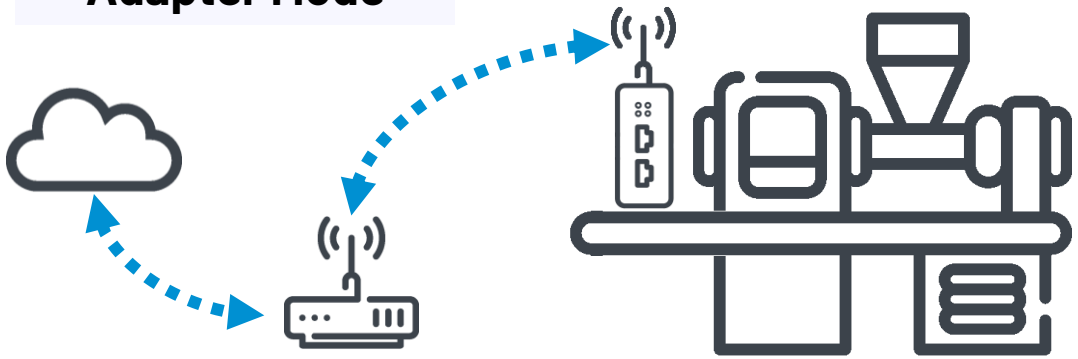
2x Digital Inputs
- Activate Connection to Ubiquity Network
- Reset Command

2x Digital Outputs
- Connected to Ubiquity Network
- Remote Access ongoing

WiFi

# UBIQUITY ROUTERS: WIFI MODE

WiFi as
**Adapter Mode**



Modem/Router
for Internet Access

WiFi as
**Access Point**

Modem/Router
for Internet Access

Laptop, Tablet, Smartphone
can connect to the
automation subnet
and if needed
access internet
via Internet Sharing

# CONNECTIVITY SERVICES

# CONNECTIVITY SERVICES

NEW
with 13.5

## BEST ROUTE FOR REMOTE ACCESS

Automatic selection of the best route
through one of the Relay Servers

## LOCAL CONNECTION

Interactive Access
to devices on the local network [1]

## CONNECTION AUTHORIZATION

Operator/Technician
can authorize
the remote connection

## OVER-THE-AIR UPDATES

Runtime/Firmware updates
for remote devices

Updates can be scheduled

[1] works without Internet Access and without domain concurrent connection license
it's supported by the Windows Runtimes, OptixPanel HMIs and RK2x Routers (devices may require firmware update)

# CONNECTIVITY SERVICES

NEW with 14

## DOMAIN MANAGEMENT

User profiling and
Permissions control

Subfolders act as sub-domains

## DEVICE MANAGEMENT

Sub-devices definition
with actions/services

Invite user to a device

## AUDIT

Audit of connections
and administration activities

## GEOLOCATION

View of remote devices
on geographical map
based on public IP address

# CONNECTIVITY SERVICES

## APPS

Augmented Reality App
for video streaming with VoIP

VPN App

## SINGLE SIGN-ON

Single Sign-On
interfacing with 3rd party
OpenID identity providers (1)

## ASSISTANCE REQUEST

Operator/Technician
can send assistance request

Notifications are visible in UBIQUITY
Manager and/or via e-mail

## 3rd PARTY INTEGRATION

Integration
on 3rd party application
through Web API (2)

(1) requires an Unlimited Concurrent Connections license and a feasibility assessment by ASEM Engineering
(2) the web API is used for domain management, SDK allow to open VPN tunnel and File Transfer

# LICENSE MODEL

# LICENSING MODEL

## Connectivity services

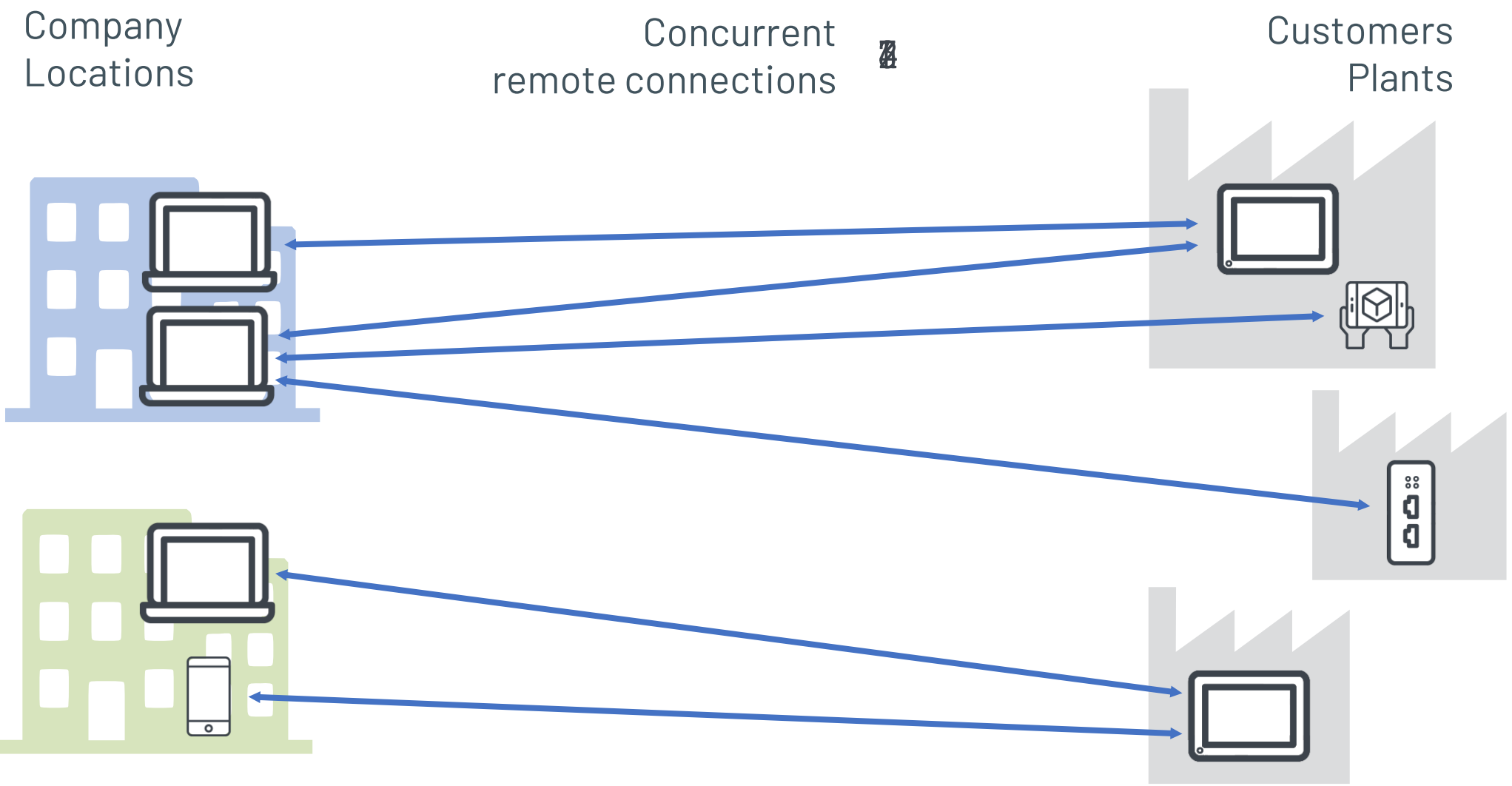
Based on the
**Number of concurrent remote connections**
with devices

## Runtimes

Available for
iPCs, HMIs and Routers

Perpetual License
**Basic** and **Pro**

# CONNECTIVITY SERVICES: CONCURRENT CONNECTIONS



# CONNECTIVITY SERVICES: DETAILS

## UBIQUITY Connectivity Services

- Annual fee
- License based on an Activation Key to use on the Domain through UBIQUITY Manager
- Available sizes of concurrent remote connections
  - 1 remote connection
  - 2 concurrent remote connections
  - 5 concurrent remote connections
  - 10 concurrent remote connections
  - Unlimited concurrent remote connections [1]

[1] includes also the *"Basic concurrent access"* feature: any Runtime without a license will be recognized as with the Basic license

# RUNTIMES LICENSES FOR IPC AND HMI

| UBIQUITY Runtime for iPC [1] and HMI [2] | BASIC | PRO |
|---|---|---|
| ▪ Interactive tools: Remote Desktop, Chat [3], File transfer, Task manager<br>▪ VPN to the device with integrated Firewall and Routing Rules<br>▪ Support for multiple connections from different UBIQUITY Manager Tools with separate VPNs for each client<br>▪ Local Connection to use Interactive tools and VPN without internet access | ✓ | ✓ |
| ▪ VPN to the automation subnet with integrated Firewall and Routing Rules<br>▪ Serial and USB passthrough<br>▪ Internet connection sharing (ICS) with devices on the automation subnet | - | ✓ |

[1] any ASEM iPC, includes Ubiquity Runtime Basic license
[2] any ASEM HMI, includes Ubiquity Runtime Basic or Pro license depending on the model
[3] available on Runtime for Windows and on ASEM HMI25/30/40

# RUNTIMES LICENSES FOR ROUTERS

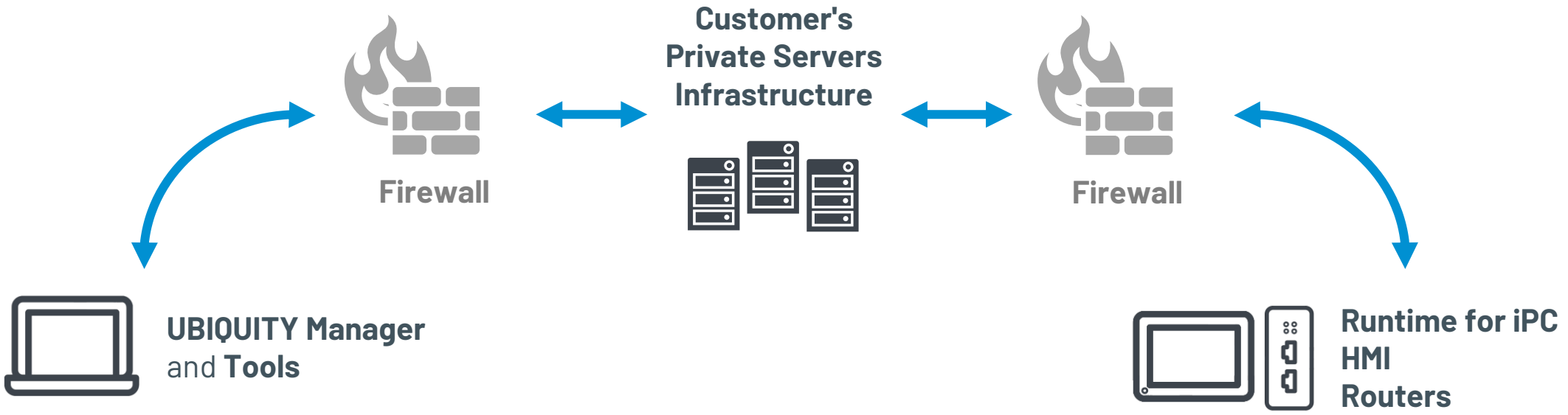
| UBIQUITY Runtime for Router [1] | PRO ROUTER |
|---|---|
| ▪ Interactive tools: File transfer, Task manager<br>▪ VPN to the device with integrated Firewall and Routing Rules<br>▪ Support for multiple connections from different UBIQUITY Manager Tools with separate VPNs for each client<br>▪ Local Connection to use Interactive tools and VPN without internet access | ✓ |
| ▪ VPN to the automation subnet with integrated Firewall and Routing Rules<br>▪ Serial and USB passthrough<br>▪ Internet connection sharing (ICS) with devices on the automation subnet | ✓ |
| ▪ Programming NAT rules between Ethernet interfaces<br>▪ Programming static Routing rules between Ethernet interfaces | ✓ |

[1] any UBIQUITY Router includes the Ubiquity Pro Router license

# PRIVATE SERVER

# PRIVATE SERVER: OVERVIEW

- UBIQUITY Manager and UBIQUITY Manager Tools
- Ubiquity Private Server Infrastructure
- Runtime, HMI and Routers



# PRIVATE SERVER: WHY?

## FULL CONTROL

The IT department
can have full control
over the whole
servers infrastructure

Ubiquity servers can be installed
on physical or virtual machine
hosted on premises or on a private cloud

## EXTRA SECURITY

Gather an extra degree of security
thanks to the separation
from the Public Infrastructure

Any possible data breach,
server maintenance,
connectivity downtime
on the  public infrastructure
does not effect the private

# PRIVATE SERVER: LICENSE MODEL


## PRIMARY SERVER

Acts as Access Server
and Relay Server
with
Unlimited concurrent connections

Includes the first year
of Maintenance and Technical Support
Following years require annual payment.


## SECONDARY SERVER

Acts only as a Relay Server

Can be used for redundancy,
decrease latency,
traffic balancing.

It's optional and require the presence
of the Primary Server but can be installed
in a distinct geographic location

# PUBLIC VS PRIVATE SERVER

| CONNECTIVITY SERVICES | PUBLIC | PRIVATE |
|---|---|---|
| ▪ **USER, GROUPS and SUB DOMAINS:** User profiling and Permissions control | ✓ | |
| ▪ **AUDIT**: Audit of connections and administration activities | ✓ | |
| ▪ **ASSISTANCE REQUEST and CONNECTION AUTHORIZATION**: User can request assistance from the remote device and User can authorize the remote connection | ✓ | |
| ▪ **LOCAL CONNECTION**: Interactive Access to devices on the local network | ✓ | |
| ▪ **SUB-DEVICES**: Define devices in the automation subnetwork with easy access to their services | ✓ | |
| ▪ **INVITE USER TO DEVICE**: Invite a user to access to a device with temporary permissions | ✓ | |
| ▪ **APPS**: Augmented Reality App and VPN App (Android and iOS) | ✓ | |
| ▪ **BEST ROUTE :** Automatic selection of the best route through one of the Relay Servers | ✓ | ✓ (1) |
| ▪ **OVER-THE-AIR UPDATES**: Runtime/Firmware updates for remote devices | ✓ | - |
| ▪ **MAP/GEOLOCATION**: View of remote devices on geographical map based on public IP address | ✓ | ✓ (2) |
| ▪ **SINGLE SIGN-ON**: Single Sign-On interfacing with 3rd party OpenID identity providers | ✓ (3) | ✓ |
| ▪ **3rd PARTY INTEGRATION**: Integration on 3rd party application through Web API and Tools SDK | ✓ | |
| ▪ **BASIC CONCURRENT ACCESS:** any Runtime will be recognized as with the Basic license | ✓ (3) | ✓ |

(1) require at least one Secondary Server license
(2) require to purchase a Geolocation service from a 3rd party provider
(3) available only with "Unlimited concurrent connections"

# UBIQUITY
# vs
# FT REMOTE ACCESS


FT Remote Access

UBIQUITY

Part of FT HUB

Integration with FT Optix

Integration with FT Design Studio

Web Client

Runtime
for Windows10
and Linux Ubuntu22

Trial Period

License based on
Concurrent Connection

Unlimited License

Wired/Wireless Routers

Local Connection

Geolocation

Remote Device Update

Device/Router Setup via USB (1)

Single Sign-On (with external OpenID Connect provider)

Runtime for WCE, WinXP, Win7

Augmented Reality App (includes VoIP)

VPN App

Private Server

Web API + SDK

(1) In the near future will be available also in FT Remote Access



ASEM A ROCKWELL AUTOMATION COMPANY | Rockwell Automation

FT Remote Access

UBIQUITY

- FT Remote Access Runtime (Win, Linux)
- Stratix 4300 Remote Access Router
- 1756 Embedded Edge Compute

- OptixPanel
- OptixEdge

- UBIQUITY Runtime (Win, Linux)
- RK2 UBQIUITY Router



ASEM A ROCKWELL AUTOMATION COMPANY | Rockwell Automation

# UBIQUITY
# VS
# UBIQUITY X

# UBIQUITY VS UBIQUITY X

| UBIQUITY - Domain features [1] | UBIQUITY X - Domain features |
|---|---|
| ✓ Best route selection, | ✓ Best route selection, |
| ✓ Geolocation, | ✓ Geolocation, |
| ✓ Remote Connection authorization, | ✓ Remote Connection authorization, |
| ✓ Remote Runtime/Firmware updates with scheduling, | ✓ Remote Runtime/Firmware updates with scheduling, |
| ✓ Users, Groups and permission management, | ✓ Users, Groups and permission management, |
| ✓ Audit of Connections and Operations, | ✓ Audit of Connections and Operations, |
| ✓ WebAPI and SDK for 3rd party integration [2] | ✓ WebAPI and SDK for 3rd party integration |
| | ✓ Access to new Relay Servers for low latency, |
| | ✓ Sub-devices, |
| | ✓ Invite user to a device, |
| | ✓ Assistance request, |
| | ✓ Single Sign-On with 3rd party OpenID identity providers [3] |
| | ✓ Augmented Reality App and VPN App for Android and iOS |

[1] Features related to Runtimes and/or Embedded Devices remain available on both Ubiquity and Ubiquity X domains
[2] Available only for domains created before 1 November 2019
[3] Require license "Unlimited concurrent remote connections"

# SECURITY ARCHITECTURE

# SECURITY BY DESIGN: OUR FOUNDATIONAL PRINCIPLE

## SECURITY FIRST APPROACH

We built Ubiquity with security as our cornerstone. This isn't an afterthought—it's embedded in our DNA.

## STRATEGIC PRIORITIZATION

When making implementation decisions, security takes precedence. We never compromise protection for convenience.

## SECURE CONNECTIONS ACROSS UNTRUSTED NETWORKS

Ubiquity's primary mission: establishing secure client connections to remote devices across the insecure Internet.

# SECURE COMMUNICATIONS & ENCRYPTION

1

## HTTPS COMMUNICATIONS

All communications with Access Servers and Web API utilize HTTPS on TCP port 443, ensuring encrypted data transmission. SSL certificates from trusted Certification Authorities authenticate server identities.

2

## RELAY SERVER PROTECTION

Securely forward traffic between Clients and Runtime without requiring inbound ports, utilizing end-to-end AES-256 encryption with securely exchanged session keys.

3

## SECURE PROTOCOLS

UBIQUITY Manager employs Secure Web Socket (WSS) protocol, providing an additional layer of protection for real time communication and control operations.

# STRONG AUTHENTICATION & ACCESS MANAGEMENT

## COMPLEX PASSWORDS

User authentication requires domain name, username and password, and domain admin can enforce complex passwords.

## TWO-FACTOR AUTHENTICATION

Support for TOTP-based two-factor authentication (RFC 6238) compatible with applications like Google Authenticator provides an additional security layer beyond passwords.

## AUTHORIZATION SYSTEM

The embedded authorization system allows administrators to define granular permissions for users, groups, and devices, ensuring principle of least privilege.

# COMPREHENSIVE AUDIT & TRACEABILITY

## COMPLETE AUDIT LOGGING

The system maintains a comprehensive audit log recording all operations including logins/logouts, configuration changes, and remote access activities.

## TAMPER-PROOF RECORDS

Audit logs cannot be disabled or deleted, even by administrators, ensuring the integrity of security records.

## REMOTE SESSION LOGGING

Administrators can enable detailed logging of all operations during remote access sessions, including transferred files and processes started or terminated, providing complete visibility into system interactions.

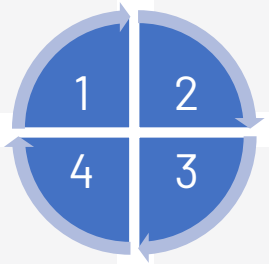
# THREAT PROTECTION

## BRUTE FORCE PROTECTION

Countermeasures against brute force attacks include temporary IP address blocking after failed attempts.

## SECURE PASSWORD STORAGE

Passwords are stored as salted hashes, protecting against rainbow table attacks and database breaches.




## CERTIFIED CLOUD INFRASTRUCTURE

Hosted on a certified ISO 27001 cloud infrastructure, providing enterprise-grade infrastructure protection.

## DIGITAL SIGNATURES

Binaries are digitally signed to guarantee authenticity and integrity, preventing tampering or malicious replacement.

# VULNERABILITY MANAGEMENT & COMPLIANCE

## VULNERABILITY MANAGEMENT

In Rockwell Automation, a dedicated Product Security Incident Response Team (PSIRT) handles product security incidents, while a 24x7 Security Operations Center monitors for threats.

## SECURITY BY DESIGN IEC 62443

Our secure-development practices align with international standards IEC 62443 to help protect industrial systems and critical infrastructures.

## SECURITY FRAMEWORKS

Rockwell Automation follows NIST Cybersecurity Framework, ensuring comprehensive security practices across identification, protection, detection, response, and recovery functions.

# THANK YOU

ASEM

A ROCKWELL AUTOMATION COMPANY