



Security Architecture

Abstract

This document provides a description of the network architecture and security design of Rockwell Automation's FactoryTalk® Remote Access™ solution.

Audience

This document is aimed to network administrators, security auditors and decision makers to provide a complete description of the security management and design to evaluate if FactoryTalk® Remote Access™ is compliant to their security standards and their use case scenarios.

Design Consideration

The core task of FactoryTalk Remote Access is to connect securely to a client to remote devices through the Internet (considered an insecure network). Thus, security is paramount on all design and implementation decisions, more than any other usability aspects.

Component Architecture

| | |
|--|---|
| FactoryTalk Remote Access Runtime | <p>The software service that runs on remote devices to allow remote access to the device itself from Frontend clients.</p> <p>The Runtime is available for open systems such as Windows computers and for closed systems, such as Rockwell Automation's industrial routers. The same security considerations apply in each case.</p> |
| Access Servers | <p>Access Servers are a distributed, redundant set of servers that enables device connection and provides a location for clients to connect to devices.</p> |
| FactoryTalk Remote Access Domain | <p>The domain is a logical container that stores all the resources of a customer account: users, groups, and devices, and their configurations, folders, authorization rules and logs.</p> |
| Web Frontend | <p>The interactive web client allows users to log in into their FactoryTalk Remote Access organization and connects to remote devices that run the FactoryTalk Remote Access Runtime. Administrative users can also use the Web Frontend to manage the security rules and the configuration of devices.</p> <p>Advanced functions like VPN are achieved by using applets (Tools) that can be started directly from the web browser.</p> <p>In this document, the web frontend is generically referenced as a Frontend client.</p> |
| Relay Servers | <p>These servers in are in multiple regions and act as a public relay endpoint between Control Center and Runtime. They are not directly exposed and reachable through the Internet.</p> |
| FactoryTalk Remote Access Web API | <p>This API exposes the API needed by the Web Frontend and the Tools Applets to work and provides for other auxiliary facilities such as software updates.</p> |

Network and Protocol Design

It is important to have a brief understanding of the described components and how they work together to understand the security architecture better.

The architecture can be divided in two parts, one supporting client connection and authentication, and one supporting the Frontend to Runtime connection.

Access Server and Web API

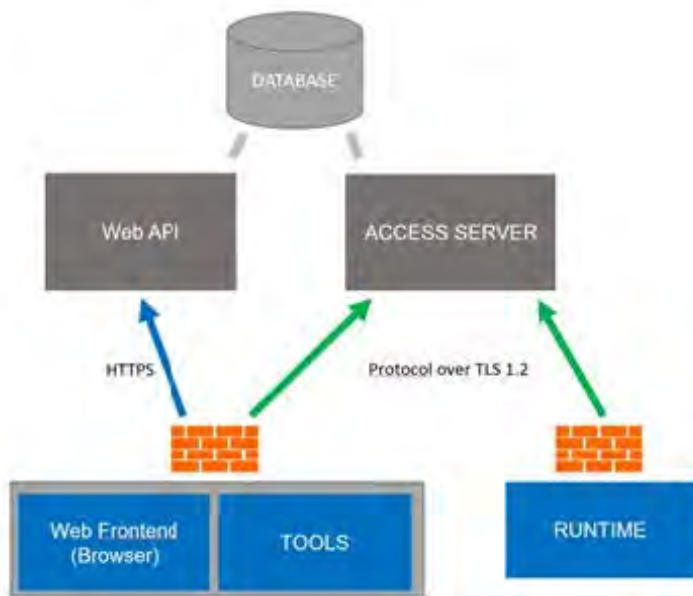


Figure 1: Simplified Network Schema

The authentication to the FactoryTalk Remote Access Domain is done by the Web API for the Web Frontend and Tools and by the Access Server for the Runtime. The FactoryTalk Remote Access Domain information is stored in a database that is behind the Web API and Access Server.

All clients are assumed to be configured behind a firewall that only allows outgoing connections. The connection from clients to the Access Server uses TLS 1.2 with certificate authentication.

Clients can use the default TCP 443 outgoing port or they can be configured to use either port 80 or port 5935 (TLS is still used), depending on which is best to comply with local IT policies. Clients automatically test available outgoing ports, but they can be configured for a fixed port.

Access Servers are redundant and fault tolerant. They are reachable by a couple of exposed endpoints and clients should be able to reach both for best service availability.

The Web API is a REST (Representational State Transfer) API that offers authentication/authorization and administration functions to frontends, such as administering folders, devices, users, and groups, or getting software update download URLs. HTTPS is used for connecting to such services.

FactoryTalk Remote Access Web API

It exposes the API needed by the Web Frontend and the Tools Applets to work as well as other auxiliary facilities such as software updates.

Relay Servers

When there is a remote access session between a Web Frontend, a Tools Applet and a Runtime, a Relay Server is used for data forwarding. Relay Servers allow both Frontends and Runtime to stay safe behind their firewalls as no incoming ports on their side must be open.

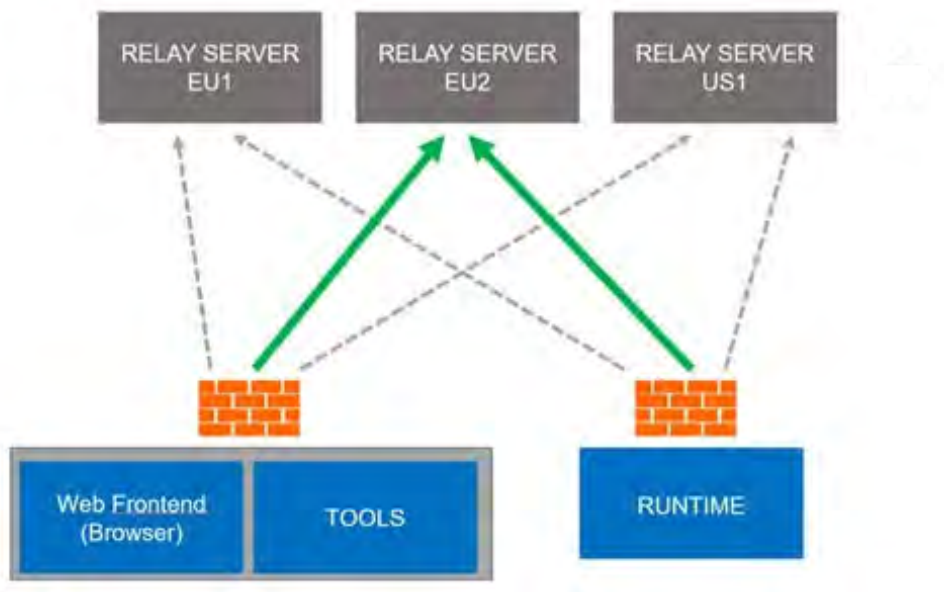


Figure 2: Relay Servers

Frontend and Runtime automatically choose the relay server to use from a pool of available list of servers list, provided dynamically by the Access Server.

In order to select a best Relay Server for a certain remote access session, both Frontend and Runtime perform a connection test to all relay servers and measure their respective network performances. Both Frontend and Runtime results are then combined in order to select the best relay. This automatic behavior can be disabled, and clients can be configured to use a fixed relay server.

Transport Security

Access Server Connection

TLS 1.2 connections are used for the connection between clients and the Access Server. The following minimum cipher suites are used by the clients:

| | |
|-----------------------------------|--------------------------------------|
| Cipher version | TLS v.1.2 |
| Key Exchange | ECDH (Elliptic-curve Diffie-Hellman) |
| Authentication | RSA |
| Encoding | AES-256 |
| Mac (Message Authentication Code) | SHA-384 |

These connections can be easily verified by looking at the application logs or by using Wireshark.

Access Servers use an SSL server certificate signed using SHA-256 with RSA by a well-known certificate authority.

Relay Server Connection

The End-to-end encryption securing remote access connections between Control Center and Runtime uses an AES-256 CBC with a session key securely exchanged through a separate Access Server connection during the handshake phase. Since the Relay Server never participates to this handshake and is used after the session key has been exchanged, it cannot decode the incoming traffic and the connection is truly end-to-end secure.

The underlying transport can be TCP (used for performance reasons) or TLS1.2 (as fallback for compatibility with firewalls requiring a TLS connection). Confidentiality is not guaranteed by TLS in this case, but by the upper-level AES-256 encapsulation.

For security reasons, the TCP transport can be disabled in favor of the TLS1.2 connection.

Web API Connection

All Frontends use HTTPS for web APIs. Web servers use an SSL server certificate signed using SHA-256 with RSA by a well-known certificate authority.

Remote Access Tools Security

FactoryTalk Remote Access uses secure connections to communicate across networks.

VPN

Once a Tools Applet client is connected to a Runtime client, a VPN connection can be established depending on how the “VPN access” permission is given to a user on a given device.

The FactoryTalk Remote Access VPN works at level 2 of the ISO/OSI protocol stack, that is, it encapsulates Ethernet frames instead of IP packets. This is done for best compatibility with common industrial scenarios, where non-IP protocols or broadcast messages are used.

The VPN is implemented by installing a virtual Ethernet adapter on the Frontend PC.

FactoryTalk Remote Access Runtime can intercept low-level network traffic of selected physical interfaces and channel it to the Frontend’s virtual Ethernet adapter. For both the Frontend machine and the FactoryTalk Remote Access Runtime device, it appears as if the Frontend machine is physically connected to the selected Runtime LAN.

Even if level 2 is below IP, by default the Runtime service automatically assigns a free IP to the Frontend virtual VPN adapter. This is done for convenience, since most useful protocols are IP based and thus ready to work. Moreover, IPs from the actual physical subnets are used. No virtual IP subnets and consequent routing rules are created.

The Runtime periodically polls for existing devices on the network by sending ARP messages. It discovers “free” IPs that can be later assigned to VPN connections. This policy is handy but can be changed if a stricter and more controlled configuration is needed. An IP pool can be configured on the device so the Runtime will only assign IPs coming from this pool. In this case, no ARP discovery is performed.

Having the Frontend PC virtually connected to the physical device network is powerful and useful, but it can be configured and limited in several ways to comply with ICT policies.

VPN firewall rules can be configured in the FactoryTalk Remote Access organization to control what kind of traffic of a certain combination of device/sub-device/user/protocol can be remotely used. These rules can be obtained by configuring firewall rules across the organization hierarchy. Rules are hierarchical, per-user, per-resource, or per-resource group, and can be limited to a certain remote MAC address, remote IPs, subnets, and Ethernet or IP protocols, in an ALLOW – DENY fashion. The resulting set of rules is calculated by the server before a VPN connection starts and are enforced on both Frontend and Runtime.

The best practice regarding security is to enable only the protocols and reachable destination needed by a specific remote user or user group. This makes the VPN connection even more secure than an actual physical local connection, because in a physical connection, the local PC firewall is the only mechanism to limit traffic. In our case, the FactoryTalk Remote Access infrastructure takes care of enforcing the security rules decided by the administrator.

File Transfer

Remote file operations (download, upload, rename, delete) are served through the FactoryTalk Remote Access Service process. This process is running with local system privileges by default. In any case, the FactoryTalk Remote Access organization admin can enable or disable this operation for remote users depending on how the File Transfer permission is propagated to a particular device for a specific user.

Device registration to Domain / Configuration Via Local Network

The registration to a domain or the configuration can be carried out using specific applets that work on the local network. These applets use an AES-256 GCM algorithm to encrypt the network traffic.

Authentication

Use different types of authentication to help make sure that only authorized users have access to systems.

Authentication of Users to Servers

The users of FactoryTalk Remote Access can sign in to the service by using their FactoryTalk® Hub™ supported credentials.

Authentication of Runtimes to Servers

When the FactoryTalk Remote Access Runtime connects to the Access Server for the first time, it obtains a signed identity file that contains the device UID in the FactoryTalk Remote Access Domain. The certificate is used for authenticating devices to the server and relies on the operating system file system security. The certificate file is only accessible by elevated processes.

FactoryTalk Remote Access Routers use an additional hardware feature that delivers device binding to a certain organization. In FactoryTalk Remote Access Routers, the UID is written in the hardware during the production stage in the factory and cannot be changed. Once the Router is registered to a FactoryTalk Remote Access Domain, it cannot be registered to another organization until the legitimate organization admin deregisters it from their organization. This is made possible by correlating the actual device identity to the hardware UID. This way, even if a threat actor obtains physical access to the Router and performs a factory reset to reconfigure it, they won't be able to register it to their organization and thus use the Router for malicious remote access to the network.

Authentication of Access Servers to Frontends and Runtime

As mentioned, clients use TLS 1.2 for connecting to Access Servers. Access Servers use an SSL server certificate signed by a well-known certificate authority. Clients can verify the signature against the certificate authority certificates installed in the system.

Operation Audit

The FactoryTalk Remote Access clients automatically record the operations, for example - device removal or renaming - performed on their organization resources by users. This information is sent to the FactoryTalk Remote Access organization. Admins can query the audit log at any time by using frontends. This feature cannot be disabled or deleted, even by admins.

Each log contains the following information:

- The user that performed the operation.
- The operation code (such as rename of a device).
- The resource that was the object of the operation (for example, a device).
- The time stamp.
- A description of the operation performed.

In more detail, the audit trail contains:

- Login/logout of users.
- All CRUD (create, rename, update, delete) operations performed on all organization resources:
 - Users
 - Groups
 - Permissions
 - Device
 - Configurations
- All remote access operations, with starting time and ending time.

In addition, the organization admin can enable a full log of all operations performed during every remote access session including:

- Start/end times of remote-control sessions (view-only or interactive).
- Files transferred.
- Processes started and stopped.
- Protocols, IPS, and MACs contacted in a VPN session.

Authorization

FactoryTalk Remote Access authorization model is similar to the Active Directory's model.

The customer's FactoryTalk Remote Access organization contains all the organization resources: users, groups and devices. The organization administrator can design the organization and its rules to map any

kind of organizational structure. Specifically, new users and groups can be created to map the organization properly and make configuration easier and more scalable.

Policies and permission rules can be applied to single resources or folders to apply them in a hierarchical way.

Finally, the Web API and the Access Server will enforce types of operations (such as remote desktop or file transfer) that will be allowed for a certain user of a certain resource (such as a remote device).

The FactoryTalk Remote Access online help describes all the ways authorization rules can be configured.

Cyberattacks Countermeasures

This section briefly describes FactoryTalk Remote Access countermeasures to help protect against some common cyberattacks.

Brute force detection

After a few unsuccessful sign in attempts, Access Server blocks all the incoming public IP addresses for a few minutes.

This measure makes brute force JSON Web Token (JWT) attack attempts ineffective.

Code Signing

FactoryTalk Remote Access application binaries are signed with a private key. This confirms that users can validate the authenticity and integrity of FactoryTalk Remote Access applications.

Man-in-the-middle

Access Server, Web APIs, and Frontend-Runtime connections all use end-to-end encryption (explained earlier) that make man-in-the-middle attacks not possible.

DataCenter

Security Standards

Access Servers, Database Servers and the Web API servers are hosted on Microsoft Azure. Azure is certified for ISO/IEC 27001:2013 and other security standards and certifications. Refer to the following pages:

<https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001>

<https://azure.microsoft.com/en-us/overview/trusted-cloud/>

FactoryTalk Remote Access Relay Servers are hosted in heterogeneous and geographically spread locations to be statistically nearer to either Frontend or Runtime in order to lower latency. However,

because of the special FactoryTalk Remote Access network architecture explained earlier, they cannot cause any availability or security issues. Specifically:

- Relay Servers are dynamically discovered. Even if a node is not available, clients will automatically switch to the others.
- Relay Servers are an intermediate hop of an end-to-end encrypted channel, explained earlier. A man-in-the-middle attack scenario is not possible.
- No data is stored on Relay Servers.

Backup

SQL backups are automatically managed by Azure and geographically spread in order to minimize the possibility of data loss.

Software Updates

Updates of the Tools Applet, Runtime and device firmware containing the FactoryTalk Remote Access software, are published on a regular basis.

The updates can be either downloaded from the website and installed manually, or they can be installed by the Access Server semi-automatically. In the latter case, an organization admin is still responsible for manually deciding what device to update and when (immediately or within a scheduled time frame). After giving instructions to the servers via Frontend, the updates will be delivered from the cloud as planned.

A fully automatic update function without user intervention is not available for security reasons, because FactoryTalk Remote Access is meant to be installed and used in mission-critical installations.

Data Breach Policy

A data breach generally refers to the unauthorized access and retrieval of information that may include corporate and / or personal data.

In this context, a data breach refers to access to FactoryTalk Remote Access Servers and its data.

The regulations across the various jurisdictions in which Rockwell Automation operates require Rockwell Automation to make reasonable security arrangements to help protect the personal data that we possess or control, to help prevent unauthorized access, collection, use, disclosure, or similar risks.

Employees, parties external to the organization, or computer system errors, can cause data breaches.

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary.
- Maintain a register of compliance failures.
- Notify the Supervisory Authority of any compliance failures that are material either on their own or as part of a pattern of failures.

Rockwell Automation will notify any affected clients after becoming aware of a data breach. However, Rockwell Automation does not have to notify the data subjects if anonymized data is breached. Specifically, notifying data breach subjects is not required if the data controller has implemented techniques like encryption along with adequate technical and organizational protection measures to the personal data affected by the data breach.


Best Practices

- In the case of software installations on Windows machines, a firewall in the network (it is best if the firewall is a hardware firewall) should be configured so that all connections from the Internet to the machine are blocked. Only one outgoing port should be used by FactoryTalk Remote Access (TCP port 443, 80 or 5935) and kept open from the machine to the Internet
- Windows machines should only run controlled and safe software.
- The FactoryTalk Remote Access software should be updated in case security improvements are released.
- Given the suggestions made earlier, and given a proper, static and controlled industrial environment, an antivirus software can be avoided.
- A strong administrator password change per IEC 62443-3-3 is enforced to register a Router to an organization. Keep the administrator password safe and do not share it with unauthorized personnel.
- FactoryTalk Remote Access Routers can be connected to the Internet through its WAN port. FactoryTalk Remote Access Routers don't enable any service through that port and will only need an outgoing connection through to the configured outgoing port (TCP port 443, 80 or 5935). They basically don't expose any surface to known attacks from the outside. We periodically test the latest version of the firmware stack against new kinds of attacks. However, for the best security, an additional specialized firewall hardware would achieve the best protection from the outside.

Resources

For further reading:

[Rockwell Automation Security Governance Overview](#)
[A Comprehensive Guide for Securing Critical Infrastructure Whitepaper](#)

Connect with us.    

rockwellautomation.com ————— expanding **human possibility**[®]

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Rockwell Automation is a trademark of Rockwell Automation, Inc. Trademarks not belonging to Rockwell Automation are the property of their respective companies.

September 2023
Copyright © 2023 Rockwell Automation, Inc. All rights reserved. Printed in USA.