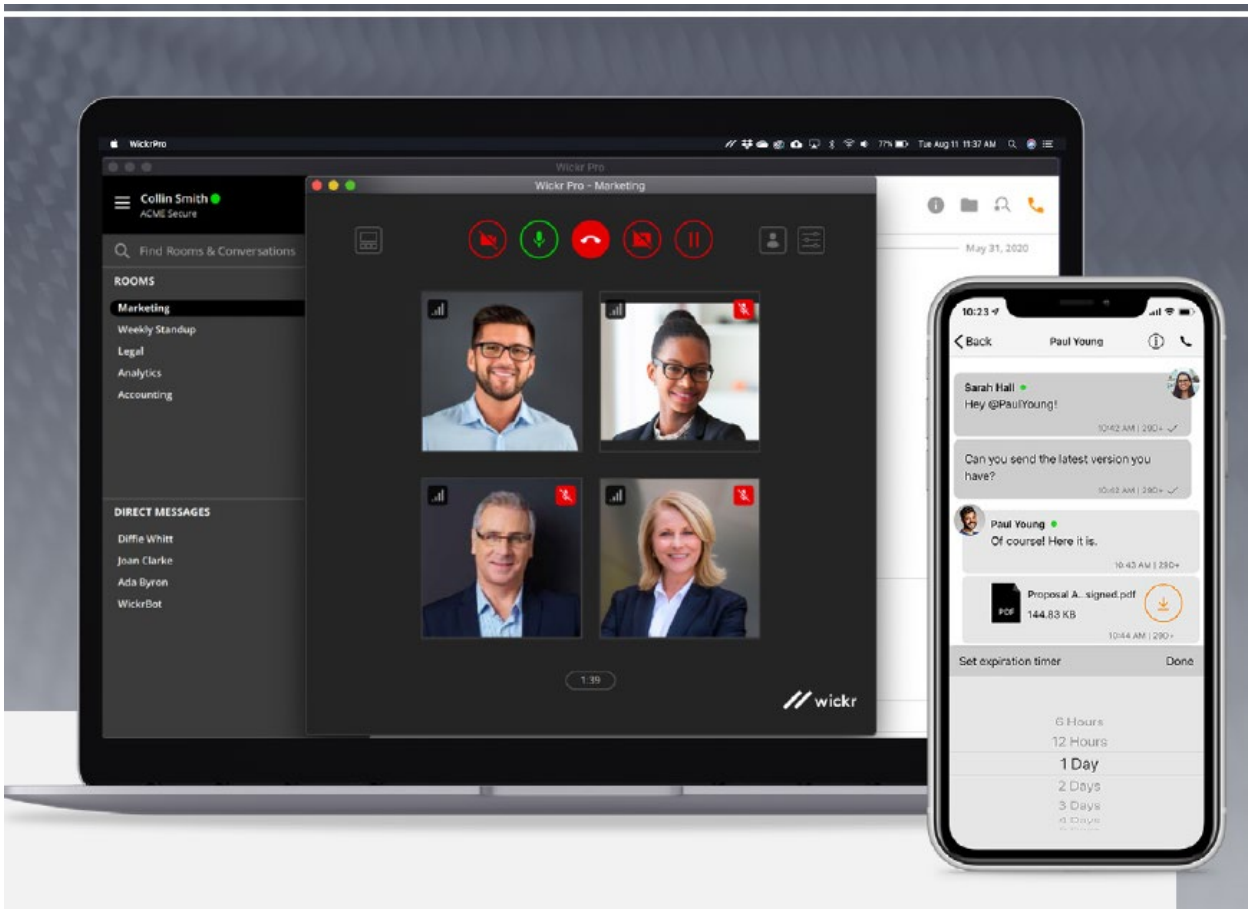
Global Federation Tech Brief

Deploy unique technological services for unique organizational needs.



carahsoft

For more information, contact Carahsoft or our reseller partners:
wickr@carahsoft.com | (866)-421-4683

Introduction

Deploying technology services can be tricky business. Organizational needs differ with regard to:

- Hosting: cloud or bare metal, on-premise or colo, managed or self-hosted, multi-tenant or single-tenant
- Availability: uptime, redundancy, RTO, RPO, SLA
- Compliance: privacy, security, data residency, data retention
- Integration: APIs and connections with external systems

Organizations need flexible product and deployment options that don't paint them into a corner of non-interoperability. For communication and collaboration services, the difficulty lies in interacting with users who are external to the organization. We are pleased to introduce Global Federation, a feature designed to minimize the impact of deployment decisions on our customers' ability to collaborate externally.

What is Global Federation?

Global Federation is our current generation product capability that lets users communicate securely across all Wickr products. Users who are part of their company network on Wickr Pro SaaS, for example, can now collaborate with users not only on Wickr Pro, but on Wickr's consumer messaging platform or even privately hosted Wickr Enterprise deployments.

It means that your organization can deploy on any Wickr product you wish, in any way you wish, and know that it will not impact your ability to communicate with external parties.

Perhaps most importantly, it de-links account ownership (licensing, provisioning, management, de-provisioning) and collaboration potential. You maintain complete control with regard to user management, security policy and feature settings for users in your organization - you can even control the system infrastructure - while external parties with whom you collaborate can approach and use Wickr their own way.

How Does It Work?

Wickr SaaS platforms federate automatically, but in private Wickr Enterprise deployments, a federation service manages the boundary between the system and the outside world, forwarding inter-system user info requests and messages to our SaaS platforms and other private deployments.

Message routing is based on user domain, with federated usernames following the convention: <user>@<domain>. Each federation service administrator manages a whitelist of domains and external service addresses with which they wish to communicate.

Security Aspects

Message security

No changes were made to our crypto protocol or security to support federated messaging. The only difference is some user information and crypto material is pulled from a remote federation service.

Service exposure

Participation in Global Federation adds three Internet-facing services to a typical Wickr Enterprise deployment:

1. a main federation service, which is an HTTPS service on port 443 configured with a valid 3rd party X.509 certificate, to manage global routing
2. a file proxy sub-service, which is an HTTPS service on port 443 configured with a valid 3rd party X.509 certificate, to manage federated file sharing
3. an audio/video conferencing sub-service, which is a media relay service on a configurable TCP/UDP port range, to host federated calls

Inter-service transport encryption

Communication between federation services is secured with Wickr transport encryption at the application layer, authenticated via a public key pinned in the Global Federation domain whitelist. The encrypted application layer traffic is then tunneled inside of TLS for further obfuscation. It is important to note here that any message traffic traversing this link is already encrypted (via Wickr E2EE) and unreadable to the service itself.

Client connectivity

Wickr clients communicate exclusively with their native service for federated messaging and file sharing functions. Wickr conferencing requires users to connect to a common conferencing server, so for federated calls, all clients communicate directly with the caller's (initiator's) conferencing service.

Compliance

Wickr maintains a SOC 2 Type II audit report covering our Wickr Pro and Wickr Me SaaS platforms. Private-hosted Wickr Enterprise deployments can support virtually any infrastructure compliance regime (E.g, DOD IL4/5), including other legal or regulatory requirements such as message monitoring or archival.

Information Risk Mitigation

Wickr client interfaces provide indicators to increase user awareness when messaging external users. Messages sent in error can also be recalled and removed automatically from all receiving Wickr clients.

For more information visit www.wickr.com

Thank you for downloading this Wickr whitepaper resource! Carahsoft is the distributor for Wickr Federal solutions available via GSA, SEWP, ITES, and other contract vehicles.

To learn how to take the next step toward acquiring Wickr's solutions, please check out the following resources and information:

For additional resources:
carah.io/carahsoftresources

For additional Wickr solutions:
carah.io/wickrresources

To set up a meeting:
wickr@carahsoft.com
703-871-8548

For upcoming events:
carah.io/wickrevents

For additional AI and Machine Learning solutions:
carah.io/AIMachineLearning

To purchase, check out the contract vehicles available for procurement:
carah.io/procurement