

Splunk Universal Forwarder to Cribl Edge migration services

Accelerate your journey from Splunk Universal Forwarders to Cribl Edge with expert-guided migration services.



The **AI Platform**
for Telemetry

Seamlessly migrate from **Splunk Universal Forwarders (UFs) to Cribl Edge** with confidence. Cribl's Professional Services team ensures minimal disruption by leveraging the full capabilities of Cribl Edge, including centralized fleet management, support across Windows, Linux, macOS, and Kubernetes environments, and modern node visibility for migration validation. Our structured approach empowers your team to focus on strategic goals—whether you're modernizing your SIEM, decoupling data collection to control vendor costs, or maximizing operational efficiency in the AI era.

Migration scope

A focused plan for:

- **Supported environments:**



- **Custom scripts & collectors:**

Evaluated individually, REST collectors will be recommended where applicable, and migration of scripts requiring extensive customization will be clearly identified and potentially scoped separately.

Deliverables

Gain confidence and clarity with:

- Documented Fleet and Subfleet configurations
- Compatibility report of migrated and non-migrated apps
- Validation documentation for each phase
- Decommissioning confirmation for all UFs

Customer requirements

To ensure a successful engagement, customers are expected to:

- Provide necessary documentation (infrastructure diagram, serverclass.conf, deployment-apps)
- Participate in planning interviews and validation sessions
- Review and approve data validation results post-migration

Out-of-scope activities

Migration of unsupported OS or complex script-based collectors unless specifically contracted, and troubleshooting or modification of third-party applications identified as incompatible without prior agreement.



Optimal architecture

Lay the groundwork for long-term success with a deployment strategy that supports scalable and agile data collection, centralized fleet management, and clean Fleet/Subfleet design.



Risk-managed migration

Structured phases ensure stability, minimal downtime, and clear rollback paths, with better visibility into node connectivity during rollout.



Empowerment and transparency

Clear communication and thorough documentation at every step.



Faster time-to-value

Accelerated migration guided by experts to free your team for higher-priority initiatives, while setting you up for easier configuration management and ongoing upgrades.

Engagement phases

Our experienced consultants collaborate closely with your team to ensure a high-quality migration experience that strengthens your flexibility and operational efficiency. The process includes:

PHASE 1: Discovery and assessment

- **Infrastructure mapping:** Obtain current deployment infrastructure diagrams, including layouts of all forwarders.
- **Configuration collection:** Gather `serverclass.conf` files and `deployment-apps` from customer's Deployment Server.

PHASE 2: Planning & design

- **Interviews & analysis:** Conduct in-depth discussions with the customer's team to understand configuration variability across the deployment and determine optimal Fleet and Subfleet layouts.
- **Fleet architecture design:** Utilize insights from previous deployments and current customer requirements, including RBAC considerations and potential need for additional Leaders.
- **App compatibility pre-check:** Use migration tooling to analyze and categorize deployment-apps for easy migration or identify them as out of scope, while accounting for routing complexity, destination readiness, and persistent queue considerations where applicable.

PHASE 3: Edge deployment & configuration

- **Leader configuration:** Set up additional Leaders as necessary based on the design phase.
- **Initial migration wave:** Deploy and configure Cribl Edge nodes parallel to existing UFs for the initial subset.
 - Run both UF and Edge in parallel, ensuring data continuity
 - Validate data integrity, Edge functionality, and node connectivity during rollout
 - Decommission validated UFs after confirmation

PHASE 4: Iterative rollout

- **Controlled migration phases:** Continue controlled migration phases until all UFs have transitioned to Cribl Edge.
- **Decommissioning validation and documentation:** Conducted for each migration phase before UF retirement.



Key takeaways

- Migrate from Splunk Universal Forwarders to Cribl Edge with a structured, low-risk engagement designed to preserve data continuity and reduce operational disruption.
- Plan for modern Edge deployments with centralized fleet management across Windows, Linux, macOS, and Kubernetes environments.
- Use phased validation, rollout controls, and documented checkpoints to move from legacy forwarders to a more flexible telemetry collection strategy.
- Give your team more choice, control, and flexibility in the AI era while modernizing telemetry collection.



Achieve modern, flexible data collection

Our team is here to ensure your success throughout your transition—all with minimal risk and maximum value. Let's tackle your data management journey together and give you more choice, control, and flexibility in the AI era.

FAQ: Splunk Universal forwarder to Cribl Edge migration

WHAT IS THIS MIGRATION SERVICE?

This professional services engagement helps customers move from Splunk Universal Forwarders to Cribl Edge through a structured process that covers discovery, planning, deployment, validation, and decommissioning.

WHY MOVE FROM SPLUNK UNIVERSAL FORWARDERS TO CRIBL EDGE?

Customers typically migrate to modernize telemetry collection, reduce vendor dependency, improve architectural flexibility, and make data collection easier to manage at scale.

WHAT PLATFORMS CAN CRIBL EDGE SUPPORT IN THIS ENGAGEMENT?

This engagement can support Cribl Edge deployments across Windows, Linux, macOS, and Kubernetes environments, with custom scripts and collectors evaluated individually.

HOW IS MIGRATION RISK REDUCED?

Risk is reduced through phased rollout waves, parallel operation of UF and Edge during validation, documented checkpoints, and explicit decommissioning only after successful confirmation.

WHAT DOES THE CUSTOMER NEED TO PROVIDE?

Customers need to provide current-environment documentation, participate in planning and validation sessions, and review and approve migration results.

WHAT IS NOT INCLUDED BY DEFAULT?

Unsupported operating systems, highly customized script migrations, and third-party application remediation are out of scope unless specifically contracted.



The **AI Platform** for Telemetry

Learn more at cribl.io
Try [Cribl Sandboxes](#)

Join our [Slack community](#)
Follow us on [LinkedIn](#) and [X](#)