

Splunk Universal Forwarder to Cribl Edge Migration

Accelerate your journey to Edge with expert-guided migration services

OVERVIEW

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 and applying best practices throughout. 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.

KEY SERVICE BENEFITS			
Optimal Architecture	Risk-Managed Migration	Empowerment and Transparency	Faster Time-to-Value
Lay the groundwork for long-term success with a deployment strategy that supports scalable and agile data collection.	Structured phases ensure stability, minimal downtime, and clear rollback paths.	Clear communication and thorough documentation at every step.	Accelerated migration process guided by experts to free your team for higher-priority initiatives.

Migration Scope

A FOCUSED PLAN FOR:

- Supported Operating Systems:



Linux



Windows

- 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 Subleet 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.

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.

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 and Edge functionality
 - Decommission validated UFs post-confirmation

PHASE 4:

Iterative Rollout

- **Controlled Migrations Phases:** Continued until all UFs have transitioned to Cribl Edge.
- **Decommissioning Validation and Documentation:** Conducted for each migration phase before UF retirement.



Achieve modern, flexible data collection with Cribl Edge.

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.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including [Cribl Stream](#), the industry's leading observability pipeline, [Cribl Edge](#), an intelligent vendor-neutral agent, [Cribl Search](#), the industry's first search-in-place solution, and [Cribl Lake](#), a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: [Cribl sandboxes](#) | Join us: [Slack community](#) | Follow us: [LinkedIn](#) and [Twitter](#)

©2025 Cribl, Inc. All Rights Reserved. 'Cribl' and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries. All third-party trademarks are the property of their respective owners. OPG-0016-EN-1-0425