

ALGOSEC FOR SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a global provider of secure financial messaging services. SWIFT is the industry standard for global financial transactions. The SWIFT Customer Security Controls Framework provides security controls for SWIFT users. AlgoSec can help you prepare for the SWIFT regulatory audit and ensure your network is always aligned with the standards requirements.

Financial institutions are a frequent target of cyber-attacks. While customers are responsible for protecting their own environments and access to SWIFT, the Customer Security Programme (CSP) supports customers in the fight against cyber fraud. The CSP establishes a common set of security controls designed to help customers to secure their local environments and to foster a more secure financial ecosystem.

The SWIFT Customer Security Controls Framework describes a set of security controls for SWIFT users and supports customers in reinforcing the security of their SWIFT-related infrastructure. The security controls establish a security baseline for the entire community and must be implemented by all users on their local SWIFT infrastructure.

Align Network Security with SWIFT Requirements Using AlgoSec

AlgoSec enables you to automate your network security policy management at zero-touch. It provides end-to-end visibility and analysis of the network security infrastructure, including firewalls, routers and cloud security groups, as well as business applications and their connectivity flows — across cloud, SDN and on-premise enterprise networks.

Ensure Continuous Compliance with AlgoSec

Using the AlgoSec network security policy management solution enables you to automatically identify gaps in compliance, remediate them and instantly generate audit-ready compliance reports to ensure continuous compliance.



Generate a **SWIFT COMPLIANCE REPORT** for all applicable network security devices, at the click of a button.



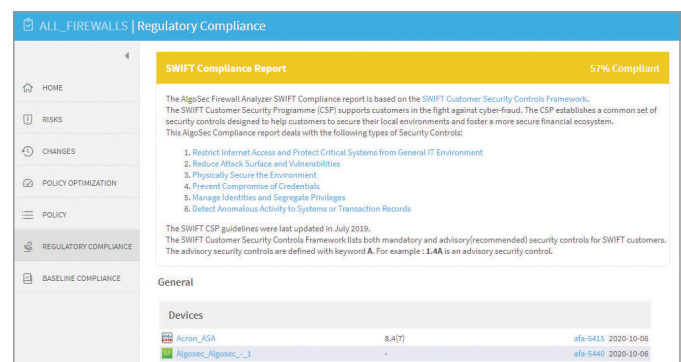
Get an up-to-date accurate **SNAPSHOT** of the organization's compliance status.



Immediately **PINPOINT GAPS IN COMPLIANCE** and get actionable recommendations for remediation.



Proactively assess **SWIFT RISK AND COMPLIANCE** for every firewall rule change.



SWIFT Compliance Report 57% Compliant

The AlgoSec Firewall Analyzer SWIFT Compliance report is based on the SWIFT Customer Security Controls Framework. The SWIFT Customer Security Programme (CSP) supports customers in the fight against cyber-fraud. The CSP establishes a common set of security controls designed to help customers to secure their local environments and foster a more secure financial ecosystem. This AlgoSec Compliance report deals with the following types of Security Controls:

1. Restrict Internet Access and Protect Critical Systems from General IT Environment
2. Reduce Attack Surface and Vulnerabilities
3. Physically Secure the Environment
4. Prevent Compromise of Credentials
5. Manage Identities and Segregate Privileges
6. Detect Anomalous Activity to Systems or Transaction Records

The SWIFT CSP guidelines were last updated in July 2019. The SWIFT Customer Security Controls Framework lists both mandatory and advisory (recommended) security controls for SWIFT customers. The advisory security controls are defined with keyword A. For example: 1.4A is an advisory security control.

Device	Compliance	Last Audit
Acron_ASA	84(7)	afa-9415 2020-10-06
AlgoSec_AlgoSec_1	-	afa-5440 2020-10-06

AlgoSec provides audit-ready compliance reports that pinpoint compliance status and provide actionable recommendations for remediation.