Silverfort

SWIFT Customer Security Controls Framework (CSCF) v2025

Silverfort Identity Protection Platform Compliance

RAP Technology for SWIFT Compliance: Runtime Access Protection enables coverage of key SWIFT CSCF controls including 1.2 (OS Privileged Account Control), 4.2 (Multi-Factor Authentication), 5.1 (Logical Access Control), 6.5A (Intrusion Detection), and 7.1 (Cyber Incident Response) without deploying agents on individual systems.

The SWIFT Customer Security Controls Framework (CSCF) v2025 represents the latest evolution in securing the global financial messaging infrastructure that facilitates trillions of dollars in daily transactions. As cyber threats targeting financial institutions become increasingly sophisticated, SWIFT has enhanced its mandatory security controls to ensure member institutions maintain robust defenses against advanced persistent threats, insider attacks, and credential-based compromises.

Financial institutions within the SWIFT messaging network are increasingly targeted by sophisticated cyber threats focused on their critical infrastructure. The SWIFT Customer Security Controls Framework (CSCF) v2025 establishes stringent identity management and access control requirements that organizations must implement to maintain network connectivity and protect global financial systems, introducing enhanced requirements across multiple domains with particular emphasis on identity and access management controls.

The CSCF v2025 introduces enhanced requirements across multiple domains, with particular emphasis on identity and access management controls that form the foundation of secure SWIFT operations. These requirements mandate comprehensive multi-factor authentication, advanced logging and monitoring capabilities, privileged access controls, and robust incident response procedures. Organizations must demonstrate not only technical compliance but also operational maturity in managing identity-related risks across their SWIFT infrastructure.

Silverfort addresses these challenges through its innovative agentless identity protection platform, which uniquely extends modern security controls topreviously unprotected systems. Silverfort's patented Runtime Access Protection (RAP) technology integrates directly with existing identity infrastructure and provides full protection across all authentication protocols and systems without requiring software agents or infrastructure modifications.

Silverfort for SWIFT CSCF v2025

Silverfort integrates with all Identity and Access Management (IAM) productsand infrastructures to achieve full visibility into all authentications and accessattempts of user and service accounts across SWIFT environments. Silverfortprovides ongoing risk analysis, advanced MFA enforcement, andcomprehensive Identity Threat Detection and Response (ITDR) capabilitiesspecifically designed for critical financial infrastructure.

Silverfort for SWIFT CSCF v2025 ProtectionHighlights

Secure Networks and Systems: All network traffic is controlled bycustom access policies that enforce SWIFT security zone requirementsand prevent unauthorized lateral movement.

Securing Privileged Users: Enforce MFA or access blocking policies onall privileged users, both human administrators and service accounts,across legacy SWIFT applications and modern infrastructure.

Detect and Respond to Identity Threats: Detect common credential access, privilege escalation, and lateral movement attacks targeting SWIFT infrastructure, and respond automatically with real-time blocking.

Continuous Monitoring: All access requests are monitored to detectanomalies and prevent malicious access in real time, withcomprehensive audit trails for regulatory compliance.

Detailed Control Mapping

1.2 OS Privileged Account Control

Security Control: Priveledged access monitoring and control

Coverage level: **Full**

Silverfort provides automated discovery and continuous classification of all privileged accounts across SWIFT infrastructure, including undocumented service accounts and shadow administrators. Real-time enforcement of least privilege policies by limiting account usage top redefined sources, destinations,and protocols. Full monitoring of administrative activities across the Windows, Linux, and Unix platforms without requiring software agents or system modifications. Virtual fencing capabilities prevent lateral movement and privilege escalation by restricting privileged accounts toauthorized SWIFT resources only.

2.6 Operator Session Confidentiality

Security Control: Session protection via multi-factor authentication

Coverage level: **Full**

Silverfort provides automated discovery and continuous classification of all privileged accounts across SWIFT infrastructure, including undocumented service accounts and shadow administrators. Real-time enforcement of least privilege policies by limiting account usage top redefined sources, destinations,and protocols. Full monitoring of administrative activities across the Windows, Linux, and Unix platforms without requiring software agents or system modifications. Virtual fencing capabilities prevent lateral movement and privilege escalation by restricting privileged accounts toauthorized SWIFT resources only.

2.9 Transaction Business Controls

Security Control: Access enforcement layer for transaction systems

Coverage level: **Supporting**

Controls access to transaction processing systems and validatesuser permissions before allowing access to SWIFT messaging interfaces. Enforces authenticationand authorization policies that complement business logic validation systems. Monitors transaction system access patterns and detects unusual activity that may indicate unauthorized transaction attempts. Does not replace business logic validation but provides essential identity verification layer.

4.1 Password Policy

Security Control: Login policy enforcement via identity provider integration

Coverage level: **Supporting**

Integrates with existing identityproviders to enforce comprehensiveauthentication policies across SWIFTinfrastructure. Detects weakauthentication attempts includingpassword-only access and appliesadditional security measuresautomatically. Monitorsauthentication events acrossLDAP/S, NTLM, and Kerberosprotocols to ensure policycompliance. Works within existingpassword management frameworksto enhance rather than replacecurrent policy enforcementmechanisms.

4.2 Multi-Factor Authentication

Security Control: Context-aware MFA across all access methods

Coverage level: Full

Silverfort can enforce MFA on any access request, whether on-premises, remote, or third-party, and for every level of credentials,from regular users to administrators. In Active Directory environments, Silverfort enforces MFA and access policies on any LDAP/S, NTLM, andKerberos authentications. Thisexpands MFA protection to command-line tools, legacy SWIFTapplications, IT infrastructure and network devices without requiring software agents or system modifications. Context-aware policies adapt MFA requirements based on risk levels, user behavior,source networks, and access patterns while maintaining operational continuity.

5.1 Logical Access Control

Security Control: Unified policy engine with risk-based access control

Coverage level: Full

Real-time enforcement of least privilege principles across all authentication attempts without requiring individual system configurations. Provides full visibility into user access patterns, with automatic account classification based on behavior, privilege levels,and risk scores. Implements dynamic access control that adapts to changing risk conditions and access patterns. Broad role-based access control integration with existing directory services and identity management systems. Automated policy enforcement prevents unauthorized access while maintaining flexibility for legitimate business requirements.

5.2 Token Management

Security Control: Integration and enforcement of token-based authentication

Coverage level: Full

Monitors all token-basedauthentication attempts acrossSWIFT infrastructure including smartcards, hardware security modules,and software tokens. Detectsanomalous token usage patternsand potential token compromisescenarios through behavioralanalysis. Integrates seamlessly withexisting token management systemswhile providing enhancedmonitoring and control capabilities.Comprehensive logging providesdetailed audit trails for all token-based authentications includingtoken lifecycle events and usagepatterns. When anomalies are detected, enforces additionals ecurity measures includingsecondary authentication ortemporary access restrictions.

6.4 Logging and Monitoring

Security Control: Real-time access logs with SIEM integration

Coverage level: Full

Captures every authentication attempt at the protocol level providing detailed audit trails thatinclude user identity, source and destination systems, authentication methods, and risk assessments. Monitoring capabilities extend beyond basic logging to include real-time detection of suspicious authentication patterns, failed login attempts, and policy violations. Integration with existing SIEM solutions provides centralized security event correlation while automated alerting ensures high-risk activities receive immediate attention. Advanced filtering capabilities enable security teams to quickly identify misconfigurations, suspicious activities, and policy violations across entire SWIFT infrastructure.

6.5A Intrusion Detection

Security Control: Anomaly detection with behavior-based policies

Coverage level: Supporting

Uses artificial intelligence and machine learning to establish behavioral baselines for all users and service accounts across SWIFT infrastructure. Detects access patterns that deviate from normal behavior including unusual access times, unexpected source locations, and privilege escalation attempts. When threats are detected,responds automatically with access blocking, MFA enforcement, oraccount isolation providing immediate threat containment. Complements traditional network-based intrusion detection by focusing on identity-level threat indicators that may bypass perimeter security controls.

7.1 Cyber Incident Response Planning

Security Control: Real-time enforcement and response automation

Coverage level: Full

Enables immediate blocking of compromised accounts or suspicious access patterns across allSWIFT systems without requiring individual system configurations. During security incidents, providescrucial forensic information including complete trails of useractivity and access patterns leadingup to and during security events.This information proves invaluablefor understanding attackprogression, identifying compromised systems, anddetermining scope of potential dataexposure. Integration with existing incident response tools and SIEMplatforms ensures identity-related security events are properly incorporated into organizational incident response procedures.

Detailed Control Mapping

Universal Coverage Across All SWIFT Architectures

Silverfort's agentless deployment model provides consistent identity protection capabilities regardless of underlying SWIFT architecture. Organizations implementing Architecture A1 (full local SWIFT infrastructure) benefit from comprehensive coverage across messaging and communication interfaces, while those using Architecture B (service provider access) gain enhanced visibility and control over operator access scenarios.

Customer Connector Environments (Architecture A4)

Organizations utilizing customer connectors face unique challenges insecuring the boundary between SWIFT infrastructure and back-office systems. Silverfort addresses these challenges through network-aware access policiesthat enforce different security requirements based on source and destination networks. Provides comprehensive monitoring and control of authentication to middle ware and file transfer servers that bridge SWIFT and back-office environments.

Service Provider Access Scenarios

Financial institutions accessing SWIFT services through third-party providersoften struggle to maintain visibility and control over authentication events. Silverfort's multi-tenant monitoring capabilities enable organizations to maintain isolated yet comprehensive monitoring across different client environments, while federated authentication support accommodates complex authentication scenarios involving multiple identity providers.

Implementation Benefits

Agentless Deployment Model

The most significant advantage lies in providing full security coverage without requiring software agents, inline proxies, or system modifications. This is especially important in SWIFT environments where modifying critical financial infrastructure can be challenging due to change control requirements, vendor support constraints, and operational risk considerations. Organizations can implement Silverfort without disrupting existing SWIFT operations. This eliminates extended testing and validation cycles.

Universal Protocol Support

SWIFT environments typically involve authentication across multiple protocols and systems including modern web applications, legacy mainframe connections, and network infrastructure devices. Silverfort's support forLDAP/S, NTLM, Kerberos, and modern authentication protocols ensures full coverage regardless of underlying technology stack. This universal protocolsupport enables consistent security policies across entire SWIFT ecosystems.

Advanced Threat Detection Capabilities

Traditional security approaches often focus on perimeter protection or signature-based detection, which can miss sophisticated attacks that leverage legitimate credentials and standard authentication mechanisms. Silverfort's behavioral analytics approach provides complementary detection layer that identifies subtle changes in access patterns that may indicate compromise.The platform's AI-powered risk assessment analyzes user behavior, accesstiming, source locations, and authentication patterns compared to traditionalsystems that typically only validate credentials.

Operational Excellence

Beyond security benefits, Silverfort provides significant operational advantages for organizations managing SWIFT compliance requirements. Centralized policy management eliminates the need to configure security controls across individual systems. Detailed monitoring provides the visibility required for ongoing compliance validation. Automated reporting capabilities streamline SWIFT CSCF attestation processes.

Key Silverfort Advantages for SWIFT Compliance

Rapid Deployment Timeline

Implementation and activation within days rather than months typical of traditional security solutions. This speed comes from the platform's ability to work within existing identity infrastructure rather than requiring extensive integration projects across individual systems and applications.

Legacy System Protection

Extends modern security controls to legacy SWIFT applications, homegrown systems, and critical infrastructure that resist modern security implementations. Command-line administrative tools, legacy applications,and network devices receive the same level of protection as modern web-based interfaces.

Comprehensive Privileged Access Management

Automated discovery capabilities prove particularly valuable in SWIFT environments, where service accounts and automated processes often remain undocumented or hidden within complex system architectures. Silverfort identifies these accounts automatically, maps their dependencies, and provides visibility into usage patterns without requiring manual discovery processes that can take months to complete.

Compliance Automation

Continuous monitoring and automated reporting for privileged access compliance requirements streamlines SWIFT CSCF attestation processes and ongoing compliance maintenance. Organizations can demonstrate comprehensive compliance with SWIFT requirements while building foundation for more secure and resilient future.

About Silverfort

Silverfort secures all facets of identity. We deliver end-to-end identity security across the entire IAM infrastructure, eliminating gaps and blind spots, giving businesses visibility into their identity fabric and extending protection to resources previously inaccessible to identity security tools. This is all done via a patented technology that natively integrates with your entire IAM infrastructure, Runtime Access Protection™ (RAP). It is lightweight, easy to use and deploy, and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity across every environment, analyze exposures to reduce your attack surface, and enforce security controls inline to stop lateral movement, ransomware propagation, and other identity threats.

To learn more about Silverfort's SWIFT CSCF v2025 compliance capabilitiesand explore how the platform can address your specific requirements

Learn more at silverfort.com