

Find Out SWIFT Requirements Specific to Privileged Access

The increasing payment frauds in customer's environments have led to the launch of the Customer Security Program (CSP) aimed at improving information sharing among the community, enhancing customer experiences, and providing audit frameworks. Revolving around the objectives of securing an organization's environment, restricting privileged access, and responding to anomalous activities, a set of 16 mandatory and 11 advisory security controls have been described to which customer must attest to and have proof of compliance. Among the clauses that customers must adhere to CSP framework around privileged access are highlighted below:

Requirements

Requirement 1

Ensure protection of SWIFT user's local infrastructure, virtual platforms and control the access of operating system privileged accounts

Requirement 4.2

Prevent compromise of a single authenticator factor that authorized access to SWIFT systems by implementing multi-factor authentication

Requirement 5.4

Protect Physically and logically recorded passwords

Requirement 4.1

Ensure passwords are sufficiently resistant against common passwords through an effective password policy

Requirement 5.1

Enforce security principles of need-to-know access, least privileged access and segregation of duties for operator accounts

Requirement 6.4

Record security events and detect anomalous activities and operations within the SWIFT environment

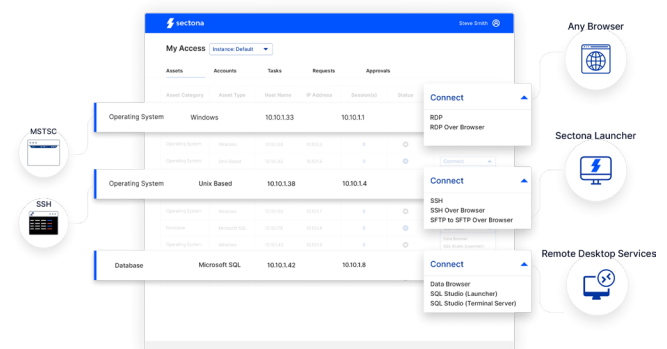
Explore How Sectona Helps You Achieve Compliance with SWIFT

Sectona Privileged Access Management Solution is an integrated solution of several capabilities like password management, session management and threat analytics adhered to and governed by customers in the SWIFT environment. Listed below are few of the use cases compliant with each of the clauses of the SWIFT Framework w.r.t privileged access.

Addressing Requirement 1

Monitor Every SWIFT Privileged Session

Capture comprehensive logs of all critical sessions in video format. Logs are stored in an encrypted format and provide auditable details accessible only to authorized personnel for improved governance.



Add New Account(s) Local Accounts

Asset Type	Account Name	Authentication Type	Host Name
Windows Active Directory	steve.smith	Password	Local / 10.10.1101
Windows Active Directory	Jason.J	Password	Local / 10.10.1101
Windows Active Directory	tejas.sontawane	Password	Local / 10.10.1101
Windows Server	Administrator	Password	DMFALOVER01 / 10.10.1158
Windows Server	Administrator	Password	SECTONMAULTSTO / 10.10.1.232
Windows Server	Administrator	Password	DMG04WIN2K16 / 172.16.100.12
Windows Server	Administrator	Password	DMG14WIN2K19 / 172.16.100.12
Windows Server	Administrator	Password	PR003WIN2K16 / 10.10.1113
Windows Server	Administrator	Password	PR003WIN2K16 / 10.10.1111
Windows Server	Administrator	Password	PR004WIN2K16 / 10.10.1118

- Manage Account
- Manage Linked Groups
- Session Activity
- Account Trial
- Password Change History
- Password Checkout Trail
- View Trail

Addressing Requirement 4.1

Automate Password Management

Manage and Inventorize privileged accounts across infrastructure. Leverage strong password change capabilities from discovery, onboarding to rotation for all vendor supplied default accounts.

Addressing Requirement 4.2

Enforce MFA Authentication for Admins

Add a second layer of authentication to SWIFT environment by configuring customizable MFA mechanisms including token-based or built-in app-based OTP.

Multifactor Authentication

RSA Secure ID App OTP SMS OTP Email OTP

Visco Token Max Retries: 3 OTP Length: 6

Okta OTP Template: your OTP for secure login is %OTPNo%

One Login [Content Tags](#) [Reset UID](#)

Duo Tolerance Time: 30 Seconds App OTP Version: 6

Generic Radius Sectona Authentication Password & Lockout Policy

Google Authenticator

Microsoft Authenticator

Sectona Authenticator

Enforce Password History: 0(Last) Minimum Password Length: 5

Minimum Password Age: 0(Days) Maximum Password Age: 0(Days)

Password Must Meet Complexity Requirements

Account Lockup Threshold: 0(Attempts) Unlock Account After: 0(minutes)

Account Dormancy Threshold: 0(Days)

[Save](#) [Cancel](#)

Edit Workflow Rule [Access & Password Request]

Rule Name: Access & Password Request

Description: Access & Password Request

Rule Type: Workflow Maker Checker

Levels: 2

Request Type: Password Access

Schedule Time: Any 15:41 15:41

Attributes: Operations Input

Workflow: Custom

Approver Level

Smith, Steve (steve.smith)	1
Zad, Jason (jason.zad)	1
Murphy, Alma (alma.murphy)	2

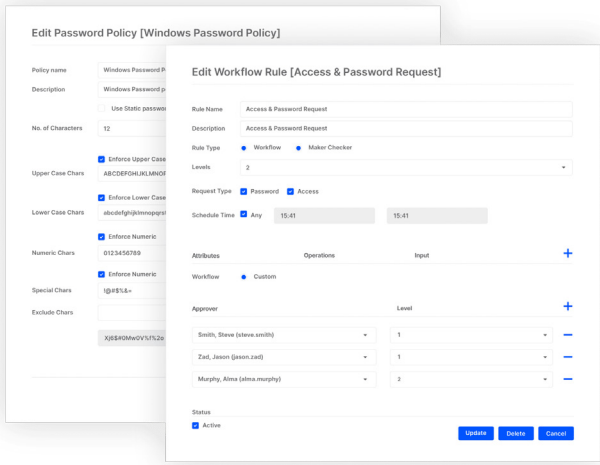
Status: Active

[Update](#) [Delete](#) [Cancel](#)

Addressing Requirement 5.1

Enable Need-Based Access to Resources

Configure access policy definitions based on user roles & functions. Define access to critical data and enforce restrictions on a need-to-know, need-to-access basis with strong workflow based access.



Addressing Requirement 5.4

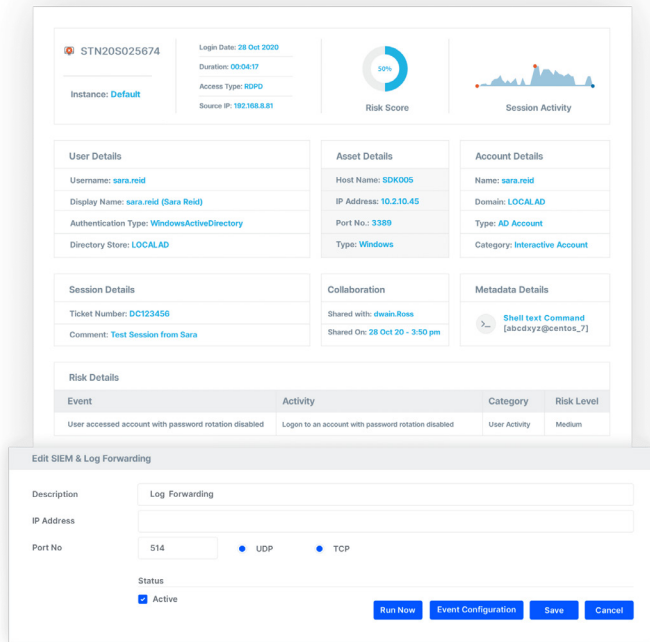
Implement Password Management System

Leverage strong password change capabilities from discovery, onboarding to rotation for all privileged accounts in a secure, encrypted, tamper – proof storage.

Addressing Requirement 6.4

Leverage Risk-Based Scoring & SIEM Integration

Detect risky events events for administrator activities with risk based scoring & SIEM integration.



Sectona is the leading Privileged Access Management company focused on protecting access to enterprise privileged accounts spread across data centers and the cloud. We have a global footprint, with a diverse client base from industries including Banking, Insurance, Government Institutions, Telecom Services, and Information Technology.

For more information, visit www.sectona.com and follow [@SectonaTech](https://twitter.com/SectonaTech) on X (Twitter) or [@Sectona](https://www.linkedin.com/company/sectona) on linkedin