sectona

Solution Brief

Find Out ISO/IEC 27002 Requirements Specific to Privileged Access

ISO 27002 standard has been made consistent on privacy, information security and cryptography with the Organization for Economic Co-operation and Development guidelines. ISO 27002 Code of Practice is a framework providing international best practices in information security controls and systems interoperability implemented in a variety of legal and cultural environments. ISO 27002 standard has been designed as a guidance manual for organizations implementing international best practices in information security controls. Among the listed practices, clauses around privileged access as highlighted below.

Requirements

Requirement 9.2.3

The allocation and use of privileged access rights should be restricted and controlled

Requirement 9.2.5

Asset owners should review users' access rights at regular intervals

Requirement 9.4.1

Access to information and application system functions should be restricted in accordance with the access control policy

Requirement 9.4.2

Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.

Requirement 9.4.3

Password management systems should be interactive and should ensure quality passwords

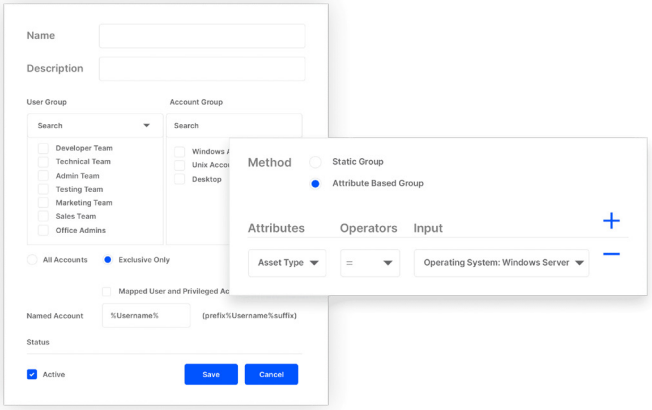
Explore How Sectona Helps You Achieve Compliance with ISO 27002

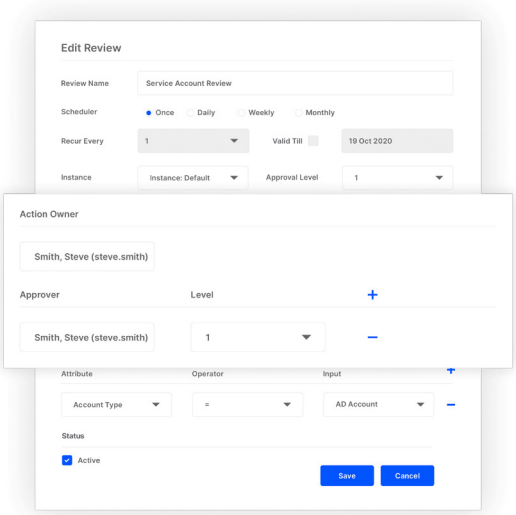
Sectona privileged access management, an integrated solution with several components like privileged access, remote session collaboration, threat analytics, and session recording follows best practices in information security controls w.r.t. privileged access as intended by the ISO 27002 framework. Here are few use-cases in line with the ISO 27002:

Addressing Requirement 9.2.3

Implement Access Control Policy

Implement access control policy easily for system administrators accessing multiple assets and accounts. Define policies based on assets or accounts. Segregate access for default and shared accounts while demonstrating compliance.





Addressing Requirement 9.2.5

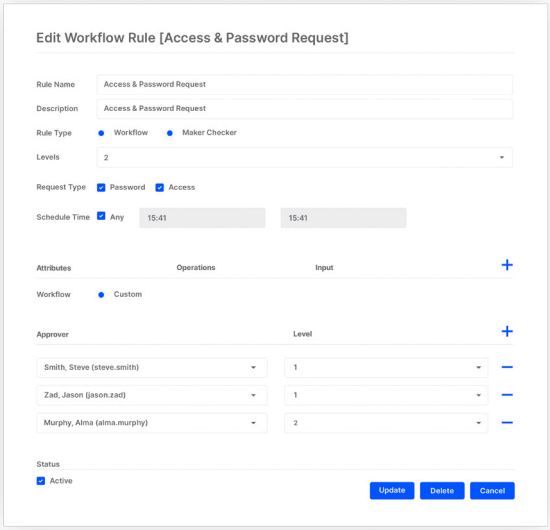
Automate Access Reviews

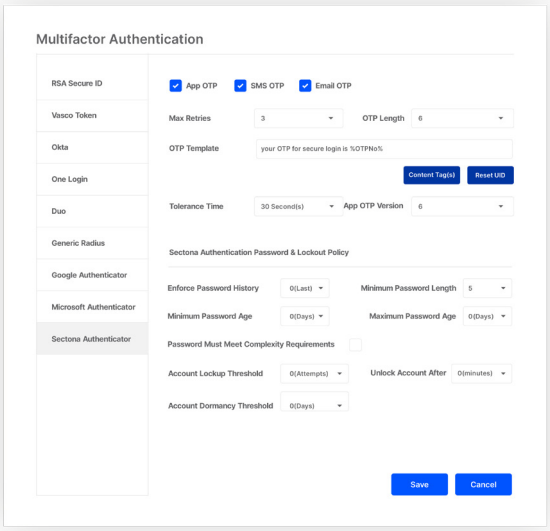
Go beyond manual excel-sheet based reviews and review & certify access to default accounts, service accounts and other accounts with automated workflow based system.

Addressing Requirement 9.4.1

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.

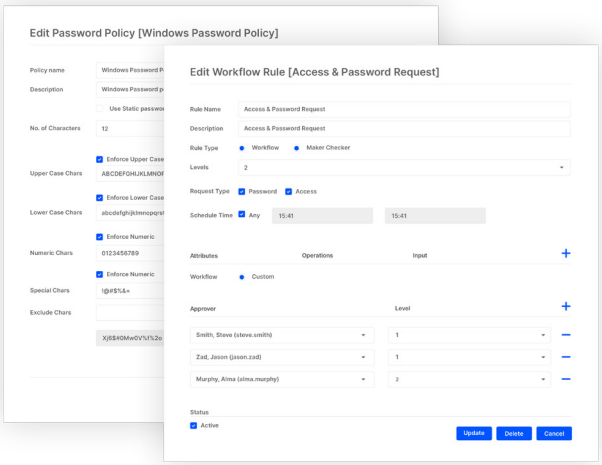




Addressing Requirement 9.4.2

Enforce MFA Authentication for Admins

Enforce second level of authentication & verification of all users by configuring customizable MFA mechanisms or free to use Sectona MFA.



Addressing Requirement 9.4.3

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.

sectona

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 on X (Twitter) or @Sectona on linkedin