

Compliance Mapping

SOC 2

How Admin By Request Helps

Document Information

Code: MD-HAH-SOC2

Version: 1.0

Date: 17 April 2025

SOC 2 - How Admin By Request Helps

The following table outlines how Admin By Request helps your organization comply with the SOC 2 framework.

Trust Service	Requirement	How ABR helps to ensure compliance
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	By using Admin By Request, you will ease the burden on your internal access reviews as privileged accounts do not exist.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Admin By Request ensures preventive, detective and automated privileged access controls throughout the entire organization, which is a mandatory control to meet the SOC 2 requirements.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objective.	Admin By Request ensures that privileged access to sensitive resources is restricted to authorized personnel on a per application basis or for a limited period of time. This eases the burden on IT resources and meets the requirements on implementation of logical access security software.
CC6.3	The entity authorized, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Features such as Remote Access in Admin By Request Server Edition also help you to connect securely to servers and establish and maintain inventory of assets in your network.

Trust Service	Requirement	How ABR helps to ensure compliance
CC6.6	The entity implements logical access security measures to protect against threats from outside its systems' boundaries.	Access to sensitive resources within your environment is made easy and secure is made very easy with the Remote Access functionality in Admin By Request Server Edition, which leverages familiar Admin By Request approval flows and features to enable secure, browser-based connections to servers and network endpoints.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	This solution revolutionizes the way IT administrators manage and access critical systems by eliminating reliance on traditional VPNs and jump servers, while maintaining a secure and segregated setup, with all features and configurations accessible from the intuitive and familiar Admin By Request Portal. Furthermore, by using Admin By Request, you can demonstrate compliance with the protection of each endpoint in your organization.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objective.	The integration between Admin By Request and <i>OPSWAT MetaDefender</i> enables your organization to prevent malicious software from entering your environment through its endpoints. When a user requests to run a file with administrative privileges, the file can be scanned in real-time to block malware using several anti-virus engines. This happens without any performance or waiting penalty and it doesn't conflict with any security software you may have on your endpoints, because it happens in the cloud. If the file is flagged as malicious, it is blocked before it can do any damage

Document History

Version	Author	Changes
1.0 17 April 2025	Steve Dodson	Initial document release.