SteelConnect Manager

SteelConnect Manager is a cloud-based centralized management platform that monitors and manages networking appliances, such as wireless access points, switches and gateways, that the customer deploys at its sites. Administrators can use SteelConnect Manager to view network health, deploy appliances and make policy changes.

SteelConnect Manager collects data regarding the use of the customer's network by the customer edge devices connecting to the internet via the customer's network, which includes information about those devices, such as MAC address, IP address, device type, etc. (collectively, "**Customer Data**"). The information below addresses SaaS versions of the SteelConnect Manager software; for on-premise deployments, Riverbed does not have access to Customer Data collected by SteelConnect Manager.

Processing of Customer Data

Using Riverbed networking appliances along with SteelConnect Manager, the customer can design and deploy a network from which their enterprise and guests can access the internet. Customer Data is transmitted to SteelConnect Manager servers via the networking appliances for purposes of displaying network configuration and health information, analytics and insights back to the customer.

SteelConnect Manager is designed to manage and monitor networks, not individuals. Certain customers may choose to configure their networks to process certain types of data for their use that may include personal data. Configuration settings are completely within the customer's control and customers may change their settings to address data privacy and security concerns. More information about such settings is available on Riverbed's support website.

Storage and Transfer

Customers may select the data center region in which their SteelConnect Manager will be hosted. Available SteelConnect Manager data center regions include the United States, Germany and Australia. To provide customers with the best possible service, Riverbed operates a follow-the-sun 24/7 global support delivery model. Riverbed transfers any personal data in compliance with applicable legislation, including ensuring that transfers of personal data outside of the EEA are subject to appropriate safeguards.

Security Measures

SteelConnect Manager provides industry standard data security mechanisms and controls that incorporate 'privacy by design and privacy by default' principles. Such measures include but are not limited to:

Encryption

- ***SteelConnect appliances***: Customer Data is transmitted from a customer's edge device to SteelConnect hardware access points with which the edge device connects, and the access points transmit Customer Data by means of an encrypted connection to SteelConnect Manager servers for display via SteelConnect Manager. Each SteelConnect gateway ships with a Riverbed-signed certificate which is used for authenticating the gateway with SteelConnect Manager and establishing a secure communications channel via TLS connection.
- ***Cloud management platform***: SteelConnect Manager is SSL-secured and password-protected; communications between a user's browser and the management portal is encrypted leveraging a HTTPS-enabled connection.

- ***Databases***: SteelConnect Manager servers reside in state-of-the-art data centers that comply with a variety of IT security standards, including SOC 1, SOC 2 and ISO 27001. Customer Data stored on SteelConnect Manager servers is encrypted at rest using industry standard AES-256 algorithm.

Access Controls

SteelConnect Manager provides customers with the ability to implement and configure detailed access controls in order to help regulate access to Customer Data and any personal data included therein. Customers can define specific user roles and groups to which pre-defined permissions are assigned.

Data Segregation and Infrastructure

SteelConnect Manager is built on a multitenant architecture with utmost care to ensure separation of data between multiple tenants on the cloud-hosted infrastructure.

Security Standards and Certifications

Riverbed's corporate security policies are aligned with the NIST 800-171 standard, which includes the following key control requirements: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity. At this time, SteelConnect Manager has been issued a SOC 2 Type 1 audit report and will be undergoing annual SOC 2 Type II audits of its security practices and policies going forward.

Customer Data Backup, Retention and Deletion

Customer Data is backed-up daily. Upon closure of a customer SteelConnect Manager account, Riverbed will delete all Customer Data at the customer's request. Requests for return of Customer Data or other deletion requests are handled on a case-by-case basis.