Riverbed Xirrus EasyPass

Riverbed Xirrus EasyPass is a cloud-based management platform for managing Wi-Fi network access. It simplifies the administration and management of secure access for User SSO, BYOD, Guest and IoT devices.

Xirrus EasyPass collects network access management data that is user-related (i.e. MAC address, IP address, social media public profile login) and performance-related (i.e. applications, application usage, connection speeds, throughput) from the devices connecting to a customer's Wi-Fi network (collectively, "**Customer Data**"). A high-level overview of relevant topics is provided below.

Processing of Customer Data

Using Xirrus EasyPass, customers' network administrators can provision network access for individuals and their devices. Customer Data is transmitted to Xirrus EasyPass servers from the end user's device via the Riverbed Xirrus access points for the purpose of connecting to the network. EasyPass architecture is designed to separate Customer Data from end user traffic data (i.e. web browsing, internal applications, etc.) such that only Customer Data flows to Xirrus EasyPass servers, while end-user traffic data remains on the customer's LAN and flows directly to its destination.

Ultimately, EasyPass is designed to provide secure and simple network access, not monitor individuals. Certain customers may choose to configure EasyPass 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.

Storage and Transfer

Riverbed Xirrus EasyPass servers are located in the United States. 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

Riverbed Xirrus EasyPass 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

- ***Xirrus access points***: Customer Data is transmitted from a customer's edge device to Xirrus access points with which the edge device connects, and the access points transmit Customer Data by means of an encrypted connection to Xirrus EasyPass servers.
- ***Cloud management platform***: The Xirrus EasyPass management platform is SSL-secured and password-protected; communications between a user's browser and the management portal can be encrypted leveraging a TLS-enabled connection.
- ***Databases***: Xirrus EasyPass 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 Xirrus EasyPass servers is encrypted at rest.

Access Controls

Xirrus EasyPass provides customers with the ability to implement and configure detailed management platform 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.

Customers may restrict, control or block end user access to the Wi-Fi network based on specific policies with granular controls (i.e. access to network, certain hosts, certain applications, certain devices, time of day/week).

Data Segregation and Infrastructure

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

Security Standards

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.

Customer Data Backup, Retention and Deletion

Customer Data is backed-up daily and statistical data is backed-up five (5) times per week. Data is retained in raw form for thirty (30) days after which only aggregated data is stored along with associated device information for a period of up to twelve (12) months.

Customers have the option to delete certain types of data associated with provisioning EasyPass guest access within the XMS-Cloud management platform.

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