REDSEAL FULLY MANAGED SERVICES
Technical Requirements

RedSeal's Fully Managed Services (FMS) is a subscription service offer to enhance a client's security posture using RedSeal's network modeling, risk-based prioritization capabilities and the proven methodology of Discover, Investigate, and Act.

For the purposes of RedSeal's Fully Managed Services offering, the following technical requirements must be met by the client to ensure smooth delivery of business outcomes.

Identification of Stakeholders

Please confirm stakeholders from the different teams RedSeal FMS team will be working with—such as Networking, Security, Compliance, Cloud Security, etc.—this will help in investigating the RedSeal findings and drive remediation actions with proper owners.

Additionally, at least one Technical Contact is required, who will be the primary customer engineer working with RedSeal FMS team on next steps, as well as at least one Executive Sponsor or Manager—for planning in our weekly review sessions and assistance connecting us with other customer teams when needed. A customer project manager is ideal, but not required.

Technical Working Session

Your team will meet with the RedSeal ProServ Engineer (PSE) in ongoing deep-dive sessions to work together on operationalizing the RS platform, investigating the discovered findings from RedSeal and thereby gaining business value with RedSeal's use cases.

Weekly Management Review Session

Your team will meet with our PSE and Project Manager for a ~30-minute call each week, where we will review key performance metrics, critical security findings, action register, and future project plans.

Collection of Network and Cloud Devices

RedSeal requires confirmation that your network configurations will be provided either via CMDB data import or service accounts established for direct configuration collection. Refer to RedSeal's latest plugin guide for required permission levels as they vary from vendor to vendor.

Note: TACACS and admin access are strongly encouraged to expedite ingestion.

Network Context

If available, please share naming conventions for your devices, as well as any network diagrams or VISIOs—this gives the RedSeal team a better understanding of your network.

Critical Assets

Identify critical assets (such as cardholder data, source code database, etc.) so that RedSeal PSE can customize the RedSeal Default "(Business) Value" metric, emphasizing their importance to critical business activities when calculating risk.

Segmentation Policy

Provide documentation of data access control policies to create zone and policy configuration changes that accurately reflect organizational policy.

VPN Access for RedSeal Platform

Remote VPN access to the RedSeal server will be required for the RedSeal PSE to do their ongoing work. The following information is taken from the RedSeal Installation and Administration Guide (version 9.4)

Client Network Access Requirements

The client host must have network access to the RedSeal server as follows:

- If the server is running on a physical appliance, the workstation must have https access through **port 443** to install the client application. **Port 80** http connections redirect to **port 443**
- To set up two factor authentication, the RedSeal server must have TCP access through **port 10443**
- To run the client application after it is installed, the workstation must have TCP access to the RedSeal server. The server can be either a physical or virtual appliance with client host connections through **ports 3825, 3826,** and **3835**

Required Ports for Encrypted Data Exchanges

Several ports are required for access to the RedSeal server when operating in a secure environment requiring encrypted data exchanges.

Port	Use
22	SSH access to the CLI
3825 & 3826	RedSeal Java client-server communications using TLS
3835	Administrative tasks such as client and server logging using TLS
443	Installing the Java client, web-based reports, web-based API, and online help
10443	Certificate authentication
389	LDAP for data collection
636	LDAP over SSL (optional)
1812	RADIUS for user authentication

Requirements for Cluster Datahub and Spoke Ports

For the specified ports, ensure that they are open in the hub and spokes and that environmental network access controls (firewalls and routers) permit communication between the hub and spokes over the ports (all TCP).

Port	Use
5432	JDBC/TLS Encrypted data channel used by a spoke to read and write to the central database at the datahub
3826	JMS/TLS Encrypted channel used to distribute work items. A spoke connects to the datahub over that port for work orchestration
3835	RMI/TLS Encrypted channel used by the datahub and spokes for cluster administration, such as health and status monitoring, and upgrades

RedSeal Toolbox

The below is a list of software tools and utilities that a RedSeal PSE needs access to deliver the RedSeal FMS. These utilities need to be present on or accessible from the remote desktop or VDI instance provided to the RedSeal PSE.

Windows

Tool Name	Location	Purpose
Putty	www.putty.org	SSH Client
NotePad++	https://notepad-plus-plus.org/download/	Text/Source Editor
ExamDiff	http://www.prestosoft.com/edp_examdiff.asp	Diff/Merge Tool
curl.exe	https://curl.haxx.se/	cURL command line
Java 8	https://java.com/en/download/	Java Runtime
Google Chrome	https://www.google.com/chrome/	Web Browser
Mozilla Firefox	www.mozilla.org	Web Browser
7zip	http://www.7-zip.org	Compression/Encryption
MS Word & Excel		Productivity if available
LibreOffice	http://www.libreoffice.org/	Productivity, only if MS Office unavailable
ExamDiff	https://www.prestosoft.com/edp_examdiff.asp	Freeware Diff tool

Mac/Linux

Tool Name	Location	Purpose
Kdiff	http://kdiff3.sourceforge.net/	Diff Tool
Java 8	https://java.com/en/download/	Java Runtime
Google Chrome	https://www.google.com/chrome/	Web Browser
Mozilla Firefox	www.mozilla.org	Web Browser
MS Word & Excel		Productivity if available, LibreOffice alternative ok
iWork Numbers & Pages		Productivity, if MS Office unavailable.
Keka	http://www.kekaosx.com/en/	Compression/Encryption (Mac 7zip port)
7zip	http://www.7-zip.org	Compression/Encryption for Linux