Rahul Nair

Sify Digital Services  Tidel Park, Taramani, Chennai - 113

Sify Managed Wi-Fi Service Descriptor

Table of Contents

[Review & Approval 2](#_Toc154679745)

[Product Overview 3](#_Toc154679746)

[Service Overview 3](#_Toc154679747)

[Objectives 4](#_Toc154679748)

[Scope of Work 5](#_Toc154679749)

[Capabilities 6](#_Toc154679750)

[Service Components 6](#_Toc154679751)

[Service Tiers 7](#_Toc154679752)

[Service Deliverables 7](#_Toc154679753)

[Service Implementation 8](#_Toc154679754)

[Service Assurance 8](#_Toc154679755)

[SLA 10](#_Toc154679756)

[Network SLA 10](#_Toc154679757)

[Delivery SLA 10](#_Toc154679758)

[Operation SLA 10](#_Toc154679759)

[CPQ Related Information 11](#_Toc154679760)

[Order Login Data for GUI 11](#_Toc154679761)

[Terms & Conditions 11](#_Toc154679762)

[General T&Cs 11](#_Toc154679763)

[Payment Terms 12](#_Toc154679764)

# Review & Approval

|  |  |  |
| --- | --- | --- |
| **Document Name** | Sify Managed Wi-Fi Service Descriptor | |
| **Version** | 1.0 | |
| **Document Owners** | Rahul Nair | Senior Product Executive |
| Suresh Gummaraju | General Manager |

# Product Overview

This Service Descriptor Document outlines the specifications of Sify’s Managed WiFi service on the Aruba & Meraki platforms. The aim behind this document is to describe the features & specifications of the Sify Managed WiFi product which will cater to customers who need a highly scalable, cloud-managed wi-fi service which is tightly integrated with the Aruba/ Cisco ecosystems.

The managed WiFi market has been experiencing significant growth due to the proliferation of wireless devices, the rise of IoT (Internet of Things), and the increasing dependence on WiFi in various industries. Several technology and telecommunication companies offer managed WiFi based products, including Cisco Systems, Networks (a Hewlett Packard Enterprise company and others.

Some of the most important trends deciding the success of these players are Security features, including encryption, threat detection, and user authentication, are critical components of managed WiFi services, addressing the growing concern of cyber threats. Many managed WiFi services are offered through cloud-based platforms, providing scalability, ease of management, and remote accessibility. Solutions with advanced analytics and reporting capabilities are gaining popularity as businesses seek to understand and optimize their WiFi networks.

The managed WiFi market is expected to continue growing as technological advancements, 5G adoption, and the integration of WiFi 6 (802.11ax) standards shape the industry's future.

# Service Overview

Sify’s Wi-Fi 6 ready platform promises high performance, low latency, and advanced security even in crowded areas.

Key elements of our Managed WiFi solution are –

• Cloud-based Centralized Authentication Infrastructure

• Cloud-based Centralized WLAN Monitoring Console

• Captive Portal for Guest Management

• Access Points at Customer sites

**Authentication Infrastructure**

Sify’s Managed WiFi services provides robust network access control with granular role-based policies for authentication, authorization, continuous monitoring, and enforcement. Its highly interoperable features enable robust network access control. This is achieved through the Clear Pass Policy Manager (CPPM) on the Aruba platform & via the Identity Service Engine (ISE) on the Meraki platform.

The advanced endpoint posture assessments on both platforms can automatically remediate or quarantine endpoints that violate corporate security and compliance policies.

Key features of the MWiFi authentication infrastructure are –

• AI-Powered Visibility

• Robust Authentication

• Secure Authorization

• Reliable Policy Enforcement

• Powerful Integrations

• SSO Support

# Objectives

Chief service objectives of the MWiFi product are –

|  |  |
| --- | --- |
| **Objectives** | **Description** |
| Reliability and Performance | Ensure a stable and high-performing WiFi network to support uninterrupted operations and enhance user experience. |
| Scalability | Accommodate the growing number of devices and users on the network, providing flexibility for business expansion. |
| Security | Implement robust security measures, including encryption and intrusion detection, to protect against cyber threats. |
| Centralized Management | Facilitate easy monitoring and control of the network through a centralized management system for efficient operations. |
| Cost Efficiency | Provide a cost-effective solution by reducing the need for on-site IT staff and optimizing resource utilization. |
| Quality of Service (QoS) | Prioritize critical applications and services to ensure consistent and reliable performance, especially for real-time applications. |
| Guest Access Management | Offer secure and controlled guest WiFi access with features such as authentication, time limits, and bandwidth restrictions. |
| Analytics and Reporting | Provide tools for gathering insights into user behavior, network performance, and other metrics to inform decision-making. |
| Compliance Requirements | Address industry-specific regulatory compliance requirements related to data protection and privacy on the WiFi network. |
| Remote Management | Enable remote management and troubleshooting to efficiently address issues and implement changes across multiple locations. |

# Scope of Work

The purpose of the Sify managed WiFi service is that it meets the diverse needs of businesses, ensuring a reliable, secure, and scalable wireless network infrastructure.

Sify’s proposed solutions in general include the below components. These are provided by Sify & are procured, deployed & managed end-to-end by Sify as part of its fully rounded managed Wi-Fi service. The solution components are subject to change as further discovery is made of Customer’s network landscape –

|  |  |  |
| --- | --- | --- |
| **Solution Components** | **Line Items** | **Description** |
| Active Components | Wireless AP | The AP is the gateway for the users to wirelessly access internet / intranet from their end devices (Laptops/Tablets/Smartphones/Handhelds). |
| Port PoE Switches | PoE switch powers up the APs and allows data flow between the APs. |
| Licenses | NMS & NAC licenses |
| Aggregation Switches | Aggregation Switch aggregates traffic from multiple PoE switches deployed in an area and provides a single uplink to the LAN access switch. |
| Connectivity Options | Fully managed router/ firewall with MPLS/ ILL based management link |
| Passive Components | Console Cables | Console Cables for Access Points |
| Passive Cabling | UTP cabling for connecting the APs with the PoE switches. |
| Sify Services | Managed Services | 24x7x365 monitoring & management services from Sify NOC |
| Web Development | Web Development for captive portal |
| True BusinessID | SSL Certificate for the captive portal |
| Installation | Installation & Setup |
| VM | VM Instance for CPPM |

Support is required from the Customer for below activities:

* Suggestions required from Customer for user authentication mechanism.
* Integration with existing infrastructure devices.
* Access permission to sites for deployment of network elements.
* UPS-power, earthing, collocation space & cooling for network elements.
* Provisioning of WAN links for end use access.
* Provide details for captive portal to be configured in Wi-Fi setup.
* Provide details of internet access policy for Wi-Fi setup.
* Application testing & security.
* Providing internet access for the WiFi network.
* Managing the performance of internet connectivity if not provided by Sify.
* Providing permission for inter-floor & Inter-building Passive Cabling,
* AD – integration support.
* VLAN for each SSID & Management VLAN should be allowed in Customer LAN.
* Customer to provide power point and access switch within 80m from Sify Access Points.

# Capabilities

Sify’s Managed WiFi brings the following capabilities to the table –

• Role-based network access enforcement for multi-vendor wireless, wired and VPN networks.

• Posture checks for endpoint compliance.

• User profiling and Device Profiling

• Health-check capabilities to ensure compliance and network safeguards before devices connect.

• Supports multiple authentication/authorization sources (AD, LDAP, SQL dB).

• Self-service device onboarding with built-in certificate authority (CA) for BYOD.

• Supports NAC and MDM integration for mobile device assessments.

• Comprehensive integration with the OEM Security Exchange Program.

• End user device monitoring with NOC services.

• User Access can be tracked for monitoring and troubleshooting.

• Availability of intuitive policy configuration templates and visibility troubleshooting tools.

# Service Components

WLAN as a service consist of following below components:

* Access Point – deployed in every customer site with capabilities supporting WIFI6 & WIFI6E.
* Switches – deployed in every customer site with capabilities supporting PoE+.
* Security Appliance – deployed in customer place with firewall and tunnel capability.
* NMS Dashboard – Applications hosted in public cloud for network device management and monitoring.
* Transport networks – Provides last mile network connectivity to CE’s that establishes connection towards Control & Management plane communication and data plane Communication.
* Service management portal – a single pane of glass for complete service lifecycle management.

# Service Tiers

|  |  |  |  |
| --- | --- | --- | --- |
| **Tier** | **Basic** | **Enterprise** | **Industrial** |
| **Feature** | Guest Access | Guest Access | Guest Access |
| AD Integration | AD Integration / BYOD |
| BYOD | Policy Enforcement / Advance Security |
| Policy Enforcement | Custom Web Pages |
| Custom Web Pages | Outdoor APs |
| Advance Security | Location Based Services |

# Service Deliverables

|  |  |
| --- | --- |
| **Deliverable** | **Description** |
| Monitoring & Reporting | 24x7 pro-active monitoring of network and Devices related metrics and reporting on Aruba dashboard and metric specific dashboard.  Ability to view real-time and historic reporting in Aruba Dashboard and Sify Aakaash. |
| Configuration management | Management data is replicated across independent same-region data centers in real time. The same data is also replicated in automatic nightly archival backups hosted by in-region third-party cloud storage services.  Configuration audit for compliance |
| Incident management | Ticketing – customers can use Sify Aakaash as single portal for managing incidents.  MWIFI prepares RCA for incidents raised by customers and on-request.  Fault and performance management – this would be based on logs, events and data retrieved from Aruba Dashboard and central components |
| Change management | MWIFI manages all changes to be executed in customer WLAN networks – MACD based on requests from customer and proactively.  Changes are carried out on Aruba dashboard and Central components.  Customer would be providing approval for every change based on detailed POA prepared by MWIFI |
| Inventory management | Managing inventory of customer devices within the scope of managed Wireless services – network wide and site wide  Managing logical resource of customer network – WLAN networks, IP address (WLAN, LAN, WAN), VLAN, customer site contact information details etc. |
| Vendor management | MWIFI co-ordinates with Aruba vendors to work on issues related to managed Wireless services |
| Provider governance | MWIFI owns the complete transport provider lifecycle management. This includes identifying transport providers in each customer site, engaging with provider for ordering till circuit turn up, connecting transport links to Security appliance, Router or Firewall, coordinating with transport providers for any issues |
| Implementation and transition services | Implementation & transition services will be the responsibility of Sify’s delivery teams unless this scope is outsourced to a 3rd party in exceptional cases. |
| SLA reporting | Sify MWIFI is the single owner for all enterprise network connectivity of managed Wireless services. Sify Aakaash is the common portal for managing end to end SLA between Aruba Components which includes Access Point, Switches, and Security Appliance. |

# Service Implementation

Sify will follow a transition plan to ensure a systematic and effective deployment of the managed WiFi service, minimizing disruptions, optimizing performance for end-users & ensuring a smooth migration of services. The plan will be adjusted based on the specific needs and scale of the project.

Toll Gate Reviews

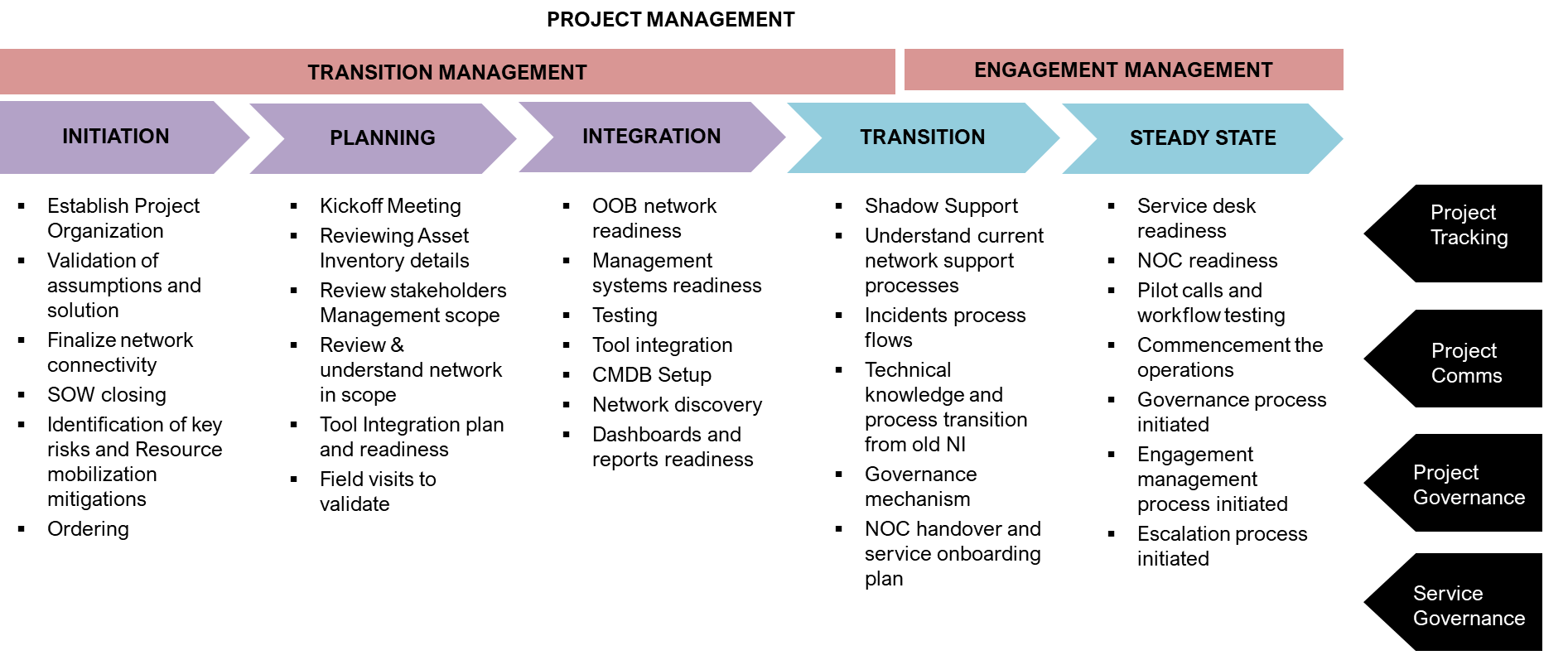
Transition Metrics

Transition Reporting

Transition Governance will ensure below aspects of service migration are correctly followed –

* Project Management
* Relationship Management
* Partner Management
* Risk Management
* Human Resource
* Contract Management
* Knowledge Management
* Tools / Best Practices
* Quality Management

**Transition Workflow:**



# Service Assurance

The managed Wi-Fi product must deliver reliable, efficient, and secure internet connectivity for users across various scenarios and locations. The below given performance metrics will be monitored in order to

|  |
| --- |
| **Performance Metrics** |
| Network Availability/Uptime |
| Throughput |
| Latency |
| Packet Loss |
| Jitter |
| Coverage Area |
| Signal Strength |
| Capacity |
| Load Balancing Efficiency |
| Client Roaming Performance |
| Client Connection Time |
| Guest Access Performance |
| Device Onboarding Time |
| Security Effectiveness |
| Bandwidth Utilization |
| Incident Response Time |
| Firmware Update Success Rate |
| User Satisfaction Scores |

**Sify’s On-Call Support Teams:**

|  |  |
| --- | --- |
| **Position** | **Role** |
| Sify Project Manager | Responsible for reaching the goals and fulfilling the objectives of the project, within the time limits, costs defined by the customer and Sify management.  During the project, the Project Manager is the first line interface between customer and Sify Management. The Project Manager will therefore act diligently and honestly in all such dealings and will encourage and motivate project team members to act likewise. Project Manager will also do a timely escalation to the sponsors of the project |
| Central Helpdesk | First level of contact for day-to-day operations of the network for onsite engineers.  Escalates to appropriate level within the stipulated time frame on non-compliance of agreed service levels. |
| Onsite Engineer (L1) | First level local contact for customers.  Provide remote hands & feet support to NOC.  Initial troubleshooting of the network issues.  Report generation based on customer requirement / reporting frequency. |
| Field Support Engineers | Remote hands support for Onsite Transition Engineers.  Responsible for on-field support for SLA adherence.  Service Provider coordination for troubleshooting & fixing up errors & failures. |
| Sify Sales Account Manager | Overall relationship is maintained between customer and Sify during the project. The Account Manager will also be responsible for ensuring any commercial change arises due to a change in scope to be taken up with customer. Actively participates in review process. |

# SLA

Sify’s service offerings are SLA-driven and offer a good value proposition to corporations seeking to improve the return on their IT investments.

Network SLA

Uptime: > 99.50%

Delivery SLA

The project delivery timelines will be 12 - 14 weeks from the date of Sify’s acceptance of a customer PO. Any delays caused due to Customer premises or infrastructure not being ready will result in extension of delivery timelines.

Operation SLA

**Incident Management**

|  |  |
| --- | --- |
| **SLA Attributes** | **SLA Indicators** |
| Incident Notification | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 – Online |
| Incident Response | Severity 1 - 15 mins  Severity 2 - 30 mins  Severity 3 – 120 mins |
| Incident / Problem Resolution | Severity 1 – 4 Hours  Severity 2 – 8 hours  Severity 3 – 24 hours |
| Sify GNOC Availability | >99.90% |
| Sify Service Portal Availability | >99.50% |

**Note:** \* From the time of call / trouble ticket logged on to Sify’s portal

**Change Management**

|  |  |
| --- | --- |
| **SLA Attributes** | **SLA Indicators** |
| Any changes to the network / Wi-Fi setup | Customer will be informed 24 hours in advance or Customer must make a request 24 hours in advance of the changes to be executed (does not include hardware replacements) |
| Change Resolution | Severity 1 – 4 hours  Severity 2 – 8 hours  Severity 3 – 48 hours |

# CPQ Related Information

Order Login Data for GUI



# Terms & Conditions

## General T&Cs

* All pricing provided is exclusive of applicable taxes.
* The contract period will be applicable as per the PO.
* The project delivery timelines will be 12 - 14 weeks from the date of Sify’s acceptance of a customer PO. Any delays caused due to Customer premises or infrastructure not being ready will result in extension of delivery timelines.
* Additional Charges are applicable for any additional cabling requirements.
* Any physical hardware damage caused by the customer will incur hardware charges for replacement of faulty hardware (OTC). Customer must provide UPS Power and earthing for the WiFi devices.
* Early Termination charges are applicable for any services terminated within the contract period.
  + In the event of performance degradation in Sify’s scope of work, which is brought to the notice of Sify in writing, Sify shall use all means available to rectify the same immediately and communicate to the customer on the action taken.
  + If the performance degradation is not rectified within one month (1 month) from the time Sify acknowledges the customer complaint in writing/mail and if this performance degradation is repeated for the same site / network element for 3 consecutive times within a calendar quarter after Sify has taken necessary corrective measures, Customer has the option of terminating the contract with 1 month notice period for the affected site / network element.
  + If the Customer chooses to terminate the entire contract for convenience or any other reason other than performance degradation of the service, the customer is liable to pay the annual recurring charges for the remaining period of the contract on a pro-rata basis. These charges will pertain to any Hardware and/or Software Licenses that have been specifically deployed for the use of the customer.
* Any requirement of changing the WiFi feature tier will result in associated change of commercials.
* Any changes to the Solution design and configuration will result in a design change along with the revised commercials.
* The provisioning/commissioning of any unmanaged or managed network security services (apart from anything included within WiFi Solution) is considered out of scope.
* All payments will be as per Sify's payment terms and conditions.
* 24\*7 proactive monitoring and management of the network as defined in the solution document is included.
* The customer will sign a scope of work document along with the PO and that will be considered as the reference for sign off on delivery of the project. Any scope not explicitly mentioned in the SOW will be considered out of scope of the project.

## Payment Terms

|  |  |  |
| --- | --- | --- |
| **Billing T&C** | **Notice Period** | **Billing Dispute** |
| Direct Sale: 100% on delivery | 30 days in advance | Billing Disputes to be raised within 15 days of invoice submission. No claims raised later would not be accepted |
| Recurring Charge: Quarterly in Advance | 30 days in advance | Billing Disputes to be raised within 15 days of invoice submission. No claims raised later would not be accepted |

**<<<<<<<<<<<<<<<<<<<<<<< END OF DOCUMENT >>>>>>>>>>>>>>>>>>>>**