FUNCTIONAL REQUIREMENT DOCUMENT

Microsoft Local Administrator Password Solution (LAPS)

Document Information

|  |  |
| --- | --- |
| Document Attributes | Description |
| Document ID | Doc001 |
| Author | Sandeep Taksande |
| Contributor | - |

Revision History

|  |  |  |
| --- | --- | --- |
| Version | Date | Changes |
| Draft | 01-October-2024 | New Document |
| V0.1 |  |  |
|  |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer/ Approver | Role | Comments | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1. Introduction 4](#_Toc178685326)

[1.1 Purpose 4](#_Toc178685327)

[1.2 Scope 4](#_Toc178685328)

[2. Functional Requirements 4](#_Toc178685329)

[2.1 Password Management 4](#_Toc178685330)

[2.2 Policy Enforcement 4](#_Toc178685331)

[2.3 Integration 4](#_Toc178685332)

[2.4 Auditing and Reporting 4](#_Toc178685333)

[2.5 Security 5](#_Toc178685334)

[3. Non-Functional Requirements 5](#_Toc178685335)

[4. Acceptance Criteria 5](#_Toc178685336)

# 1. Introduction

## 1.1 Purpose

This document outlines the functional requirements for implementing Microsoft Local Administrator Password Solution (LAPS) within [Organization Name]. LAPS is a tool designed to manage and rotate local administrator passwords on domain-joined computers.

## 1.2 Scope

The scope of this FRD includes:

* Identification of functional requirements for LAPS implementation.
* Definition of key functionalities and features.
* Establishment of integration points with existing systems.
* Identification of non-functional requirements.

# 2. Functional Requirements

## 2.1 Password Management

* **Centralized Password Management:** LAPS should provide a centralized platform to manage local administrator passwords across the organization.
* **Password Rotation:** LAPS should enforce regular password rotation for local administrator accounts, preventing the use of weak or outdated passwords.
* **Password Complexity:** LAPS should enforce password complexity policies to ensure that local administrator passwords meet minimum security standards.
* **Password Expiration:** LAPS should automatically expire local administrator passwords after a predefined time period.

## 2.2 Policy Enforcement

* **Policy Configuration:** LAPS should allow administrators to configure and enforce password policies, such as password length, complexity, and expiration.
* **Policy Compliance:** LAPS should monitor compliance with password policies and report any violations.

## 2.3 Integration

* **Active Directory Integration:** LAPS should seamlessly integrate with Active Directory to manage local administrator accounts and enforce password policies.
* **Group Policy Integration:** LAPS should leverage Group Policy to deploy and manage password policies across the organization.

## 2.4 Auditing and Reporting

* **Audit Logging:** LAPS should log password changes, policy violations, and other relevant events for auditing purposes.
* **Reporting Capabilities:** LAPS should provide reports on password usage, policy compliance, and security incidents.

## 2.5 Security

* **Password Encryption:** LAPS should encrypt stored passwords to protect them from unauthorized access.
* **Role-Based Access Control:** LAPS should implement role-based access control to restrict access to sensitive password information.

# 3. Non-Functional Requirements

* **Performance:** LAPS should perform efficiently without impacting the overall performance of the network or domain-joined computers.
* **Scalability:** LAPS should be scalable to handle a large number of managed computers and passwords.
* **Reliability:** LAPS should be highly reliable and avoid disruptions to password management services.
* **Usability:** LAPS should provide a user-friendly interface for administrators to manage password policies and monitor compliance.

# 4. Acceptance Criteria

* LAPS successfully manages and rotates local administrator passwords for all domain-joined computers.
* Password policies are enforced consistently across the organization.
* LAPS integrates seamlessly with Active Directory and Group Policy.
* Audit logs and reports are generated as required.
* LAPS meets the performance, scalability, reliability, and usability requirements.