

# PowerApps Security Features

## TABLE OF CONTENTS

- 1 Introduction
- 2 Security features

---

*PowerApps offers the ability to deploy a secure HR system globally and remain worry-free about losing control of your critical HR data.*

---

## INTRODUCTION

Security is usually something every organisation looks at as an afterthought to implementing IT systems. However in the current business environment and especially with more and more IT systems being used over heterogeneous networks and from the road, security becomes ever more important.

This is more so in the case of HR systems for all types of organisations. Whilst traditional enterprise applications like SFA have been the cornerstone of success for a modern mobile workforce, it does not get delivered to all employees across the organisation. On the other hand an HR application is likely to be used by every employee and manager using self service.

Apart from the ease of access to the latest employee information, self service brings its own pitfalls for sensitive data because it potentially opens up the sensitive HR system to whoever has access over the web.

PowerApps is designed using a robust security framework which addresses these concerns and goes beyond traditional security systems in managing the security of employee data.

The key features of PowerApps that enable an unparalleled level of security are as follows:

1. Ability to have n-tier deployment with different Application servers for web access and local access.
2. Robust login security.
3. Encryption of communication.

The detailed specifications for each of the above capabilities are described in this document.

Continued... Section 1: N-tier deployment

## SECURITY FEATURES

### 1. N-Tier deployment

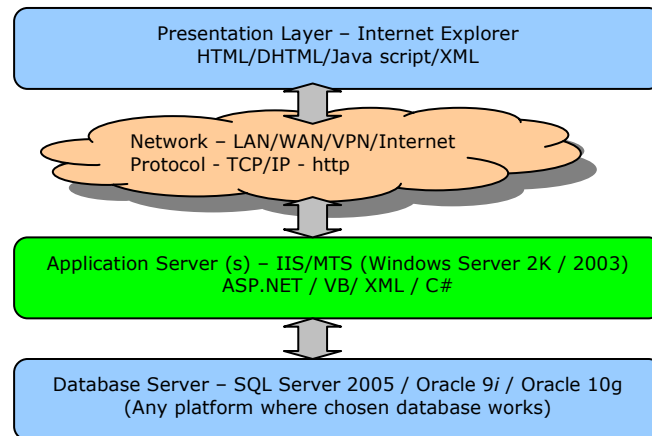
The inherent design of PowerApps is a web-architected platform which can be deployed over an Intranet or even the Internet. By separating the Application server (see diagram below) from the Database server, it is possible to deploy the Application outside the firewall in a DMZ and have a secure access to the Database through the firewall.

In addition to Application server de-militarisation, it is possible to deploy multiple Application servers which could be hosted behind the firewall for internal users and also outside the firewall for external users. In this manner, the external application server could be deployed to provide access only to the self-service modules. This strategy ensures that even in the event the external Application server is compromised, it would never be able to provide access to sensitive modules which are not published on self-service (e.g., Compensation data, Employee Master etc).

---

*PowerApps can be effectively deployed in a secure data center within a Firewall or in the DMZ. It also supports multiple application servers to handle load-balancing.*

---



Just as the n-tier architecture supports layered access, it can also be used to provide a load balanced Application farm by having multiple application servers to handle high volume of self service users. This is especially useful during peak periods e.g., the month-end when everyone wants to log in at the same time to view their Payslips.

Continued... Section 2: Login Security

## 2. Robust Login security

**a) Password changing:** Ability to allow / disallow employee to change Password.

PowerApps puts the control with the IS department to decide whether employees can change their own password.

**b) Single sign on:** PowerApps login can work on a single-sign-on platform and integrate the PowerApps login with Active Directory / ldap and any other directory authentication systems.

**c) Password strength:** Multiple parameters can be set to strengthen the passwords chosen by users. This ensures the passwords maintained by PowerApps are compliant to the organisations' IT policy. Password strength can be controlled using minimum password length, maximum password length, having a minimum number of special characters in the password, forcing users to have some numeric or text values in the password, and controlling how many times the same character can appear in the password.

**d) Password history:** Password hacking is controlled further by controlling how many days the same password can be retained before the employee has to change it, as also keeping a password history for a specific number of days (configurable), within which the user cannot use the same password used earlier.

**e) Account lockout:** PowerApps also allows you to specify the maximum number of invalid login attempts after which the password gets locked as also the lockout duration.

---

*Various measures for control over password strength, account management and secure directory integration put PowerApps in the best of class for secure applications*

---

Continued... Section 3: Secure Architecture

### 3. Secure Architecture

The architecture of PowerApps is designed to be secure from the ground up. A brief description of the measures taken in the Application design that help protect your system is given here:

- a) **Secure HTTP:** Being a web-designed application the entire suite of modules can be deployed over ssl. There is no limitation to any part of the application being used over standard https protocol. This enables businesses to deploy the signed certificate on the web server thus ensuring that all data between the Internet-connected employees and the DMZ webserver is encrypted.
- b) **Secure privileges:** Privileges are always assigned to Application roles and roles are attached to users. This ensures the group of users with privileges is controlled and there is no runaway assignment of privileges to individual users.
- c) **Encrypted password storage:** Passwords are stored in the PowerApps database in an encrypted manner, thus server administrators do not get access to the user login passwords.
- d) **Encrypted password exchange:** Even in the situation that the application is being used over the Intranet without https, PowerApps ensures that the passwords cannot be retrieved using network sniffers. The password is sent out in an MD5 hash format. This ensures packet sniffers present in the network do not pose any threat to your HR system.
- e) **Clear client memory:** The client browser memory is cleared and hence does not have any password stored in it. This ensures that a memory dump of the client PC will not reveal the password.
- f) **SQL injection blocked:** The architecture of PowerApps ensures that SQL injections cannot take place. At no point is the user input used in a manner that SQL injections can be attempted. Standard measures are taken across all application modules which block SQL injection possibilities.
- g) **Blockage of privilege escalation:** Any user can only access those pages / modules which are made available to them through the PowerApps security rights assignment. Users can never access any module directly which is not available to them through the PowerApps framework. The product architecture is designed to block out all the techniques of privilege escalation.

---

*A secure architecture ensures the application does not leak sensitive data over the network or expose the possibility of getting data from users's PCs*

---

Continued... next page

- h) **Application pages expiry:** Once a user logs out of the system, all the application pages would expire. This ensures that no user can access the pages by scavenging the browser cache.
- i) **User activity tracking:** All activities of the user starting from log-in to log-out are tracked and maintained in the activity log for further analysis. The system reports unsuccessful logins, login attempts and also account lockout.

**Note:** Some of the above advanced security features are available only with the PowerApps advanced security add-on module.