Gimmal

Cloud Technical Specifications

Gimmal Physical

Contents

Version History

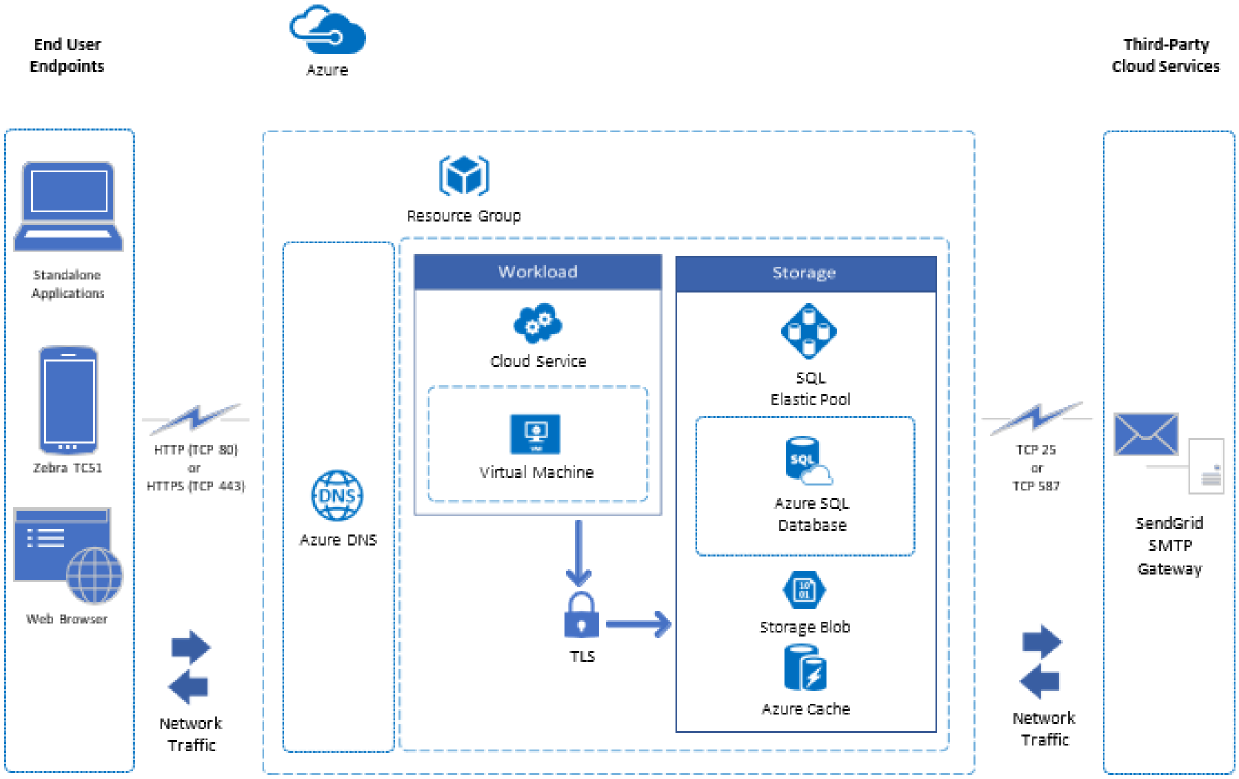
Version	Approved By	Effective Date	Product Version	Description of Change
1	Will Irwin	10/11/2021	3.11	Created for Gimmal Physical v3.11
2	Terry Butler	03/03/2022	3.11	Updated screen shots and format
3	Terry Butler	08/23/2022	3.11	Added data center details, removed duplicative information
4	Marta Farensbach	12/5/2022	3.12	Minor updates for Gimmal Physical 3.12
5	Marta Farensbach	3/30/2023	3.12	Clarification for supported devices

Introduction

Gimmal Physical is a web-based application that is offered as either a cloud-based or on-premises solution. The technical specifications in this document for the following sections are specific to cloud installations. The Gimmal Physical web application and data will be stored on the Microsoft cloud computing platform known as Azure. Azure is a top-rated cloud provider and is responsible for cloud security, data backup and cloud uptime and availability. This arrangement gives you all the features provided in Gimmal combined with the security resources provided by Microsoft Azure.

Application Architecture

By architecture design, the Gimmal Physical web application and database run fully on Azure where each solution is isolated by customer, no multitenancy, no shared resources other than the Azure platform.



Application Architecture Components

Gimmal Physical application architecture includes the following components.

1. Azure DNS to resolve CNAME mapping to dedicated Azure Cloud Service URL.
2. Azure Resource Group groups the following components per client.
   a. Azure Cloud Service which runs a dedicated virtual machine hosting the Gimmal Physical web application.Cloud Service connections to all other components within Azure leverage TLS for secure encrypted connection.
   b. Azure SQL Elastic Pool or Azure SQL Database, depending on client data load, client

database willbe hosted either on a dedicated SQL Elastic Pool or SQL Database.

c. Azure Storage Blob stores all electronic files created by the Gimmal Physical web application.Digital Content module relies on Storage Blob to store electronic records.

d. Azure Cache (Redis Cache) is used for session management and cache scenarios to improveperformance within the Gimmal Physical web application.

3. SendGrid SMTP Gateway is used to send transactional email from the Gimmal Physical web application. Connection to SMTP gateway can be either thru port TCP 25 (unencrypted) or port TCP 587 (encrypted viaTLS).

Data Centers

Gimmal Physical utilizes the following Azure data centers: East US, Canada Central, US Gov Virginia and Northern Europe.

Security

Service Organization Controls Standards

Microsoft covered cloud services are audited at least annually against the SOC reporting framework by independent third-party auditors. The audit for Microsoft cloud services covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service. Microsoft has achieved SOC 1 Type 2, SOC 2 Type 2, and SOC 3 reports.

Certificates

Secure Sockets Layer (SSL) and Code Signing certificates are provided and managed by the client with assistanceprovided by the Gimmal System Engineer Team.

Information Protection and Encryption

Transport Layer Security TLS (Encryption-in-transit)

SQL Database secures customer data by encrypting data in motion with Transport Layer Security. SQL Server enforces encryption (SSL/TLS) at all times for all connections. This ensures all data is encrypted"in transit" between the client and the server.

Transparent Data Encryption (Encryption-at-rest)

Transparent Data Encryption (TDE) for Azure SQL Database adds a layer of security to help protect data atrest from unauthorized or offline access to raw files or backups. Common scenarios include datacenter theft or unsecured disposal of hardware or media such as disk drives and backup tapes. TDE encrypts the entire database using an AES encryption algorithm, which doesn’t require application developers to makeany changes to existing applications.

In Azure, all newly created SQL databases are encrypted by default and the database encryption key is protected by a built-in server certificate. Certificate maintenance and rotation are managed by the serviceand requires no input from the user.

Identity Management Integration and Single Sign On (SSO)

Gimmal Physical can integrate with the following Identity Management/Single Sign On (SSO) technologies:

- Okta
- Azure Active Directory (AD)
- Microsoft Active Directory Federation Services (ADFS)
- SAML2-based Identity Providers (IdP)

Installation Components

Component	Description	Deployment Unit
Gimmal Physical Web Access	Software to access Gimmal Physical application.	Modern Web Browser
ScannerConnect(optional)	A standalone application that provides an interface for the ZebraDS4608/4278 barcode scanners.	Client Workstation
Email Notifications	Software to send email messages from Gimmal Physical application.	SendGrid
PortableConnect(optional)	A standalone application that provides an interface for the Zebra TC52 barcode scanner.	Client Workstation

Additional Supporting Applications

Optional Software

- **FileConnect**: a Windows service that interfaces with Gimmal Physical web services to push data from network file shares or local folders to Gimmal Physical for storage. A UI is provided to configure the service.
- **ScannerConnect**: a standalone application that allows users to transfer items in Gimmal Physical. Used fortethered scanner devices to avoid issues with ActiveX which is specific to the Internet Explorer web browser and nearing end-of-life.
- **PortableConnect**: An Android application that allows the Zebra TC51 mobile computer device tocollect scans and perform transfers in Gimmal Physical.

Gimmal Physical REST API

An extensive library of REST-based web services is available for consumption.

Device Hardware

Supported Devices

Device	Description	Specifications
Zebra DS4608 (Tethered Scanner)	A quick way to check in and out items within the ScannerConnect application, normally used at a file room check-point.	• USB port • Direct-to-Serial cable for the scanner, with a COM-to-USB adapter • Driver for the adapter; PC recognize the scanner as a COM port connection • 6ft range tethered scanner • ScannerConnect application
Zebra LI4278 (Wireless Scanner)	A quick way to check in and out items within the ScannerConnect application, normally used at a file room check-point. The base is connected to the computer and the scanner has a limited range.	• USB port • Direct-to-Serial cable for the scanner, with a COM-to-USB adapter • Driver for the adapter; PC to recognize the scanner as a COM port connection • 80-foot range • ScannerConnect application
Zebra TC52 (Mobile Scanner)	This scanner is often used in a warehouse, office building, or campus environment to both check in and out items, as well as reconcile the Gimmal Physical database with where items actually are located.	• USB port for the dock • PortableConnect application • Android 11