Fuze Digital Solutions

# Security Policy

## Hosting Environment Security Policy


***Document Information:***
***Revision*** 2.04
***Rev. Date*** 6/27/2024

***Author Information:***
***Author*** Eric Cairns
***Email*** ecairns@fuzedigital.com
***Phone*** (425) 246-2834

# 1 Introduction

## 1.1 Overview

Fuze Digital Solutions regards security and availability as two of their highest corporate priorities. To ensure the highest level of security and availability, policies have been created to regulate the maintenance and interaction with the application environment, including disaster recovery and business continuity. All interaction with the application environment is governed by these policies, and in turn these policies are strictly enforced. This document details these policies, collectively known as the "security policy".

## 1.2 Infrastructure Overview

### 1.2.1 Data Center

The hosted application environment is currently Microsoft's Azure cloud. Given that the Fuze Suite application is primarily written using Microsoft technologies, Azure is the best fit cloud provider. Using Azure allows Fuze to scale up and down as needed to support customer usage. Additionally Azure allows Fuze to keep current in both operating systems and developer platforms with minimal effort. Lastly, it allows failover techniques that were just not practical with on-premise, bare-metal servers.

Fuze uses Amazon's S3 service for off-site backup of customer data as well as failover option in the very unlikely event of a complete Azure failure.

### 1.2.2 Network Architecture

All application server virtual machines are connected on a single virtual network in the Azure US West region. Azure application security groups are used to control port access to each server based on its role, web server, database server, and mail server. An Azure Point-to-Site VPN is setup to allow on-demand access from anywhere for pre-approved personnel.

The only server and ports that are available to the public Internet are the web server's port 80 (http) and 443 (ssl), email ports 25,465,587,993,995 (smtp, secure pop, secure imap). Any other access requires the establishment of a vpn. Development and database servers have no available ports on the public Internet.

Fuze uses Microsoft Azure Active Directory (AD) for all internal user accounts. Each user must have their own password and must not share accounts or passwords. Additionally, each Azure AD account must have Multi-Factor Authentication turned on.

DNS services are provided by Amazon's cloud services, Route 53. Fuze uses an outside DNS provider so that in the event of a total failure of Azure, traffic can be re-routed to the Amazon cloud services failover instances. See section 6 for more information on backups and failovers.

### 1.2.3 VPN Architecture

Fuze uses Azure's Point-to-Site VPN to allow administrative access to all virtual machines. In addition to having an Azure AD account, each user that needs to access the

VPN must be placed in a special Azure AD group as well as have a client SSL certificate issued to them individually.

Once a VPN session has been established, the VPN client is issued a private address on a virtual network gateway and can communicate with the servers as though it was on an internal virtual network.

### 1.2.4 Database Architecture

All production customers are hosted using Azure SQL Databases in an elastic pool. Using Azure SQL rather than an installed copy of Microsoft SQL Server, removes the need for Fuze to administer, patch and maintain its own database environment and allows for scaling up or down on-demand to match customer needs. Alerts are setup to proactively notify Fuze in the event of a spike in usage. Additionally, usage is evaluated manually on a regular basis to ensure the allocated CPU and disk space is correct for current usage.

Non-production databases may be hosted on an installed copy of SQL Server Express on a virtual machine dedicated to a database role. This prevents these test or staging databases from negatively affecting the performance of production databases hosted in a shared elastic pool.

### 1.2.5 Server Architecture

Servers in the hosting environment fall into one of three categories: Web/Application Servers, Database Servers, and Development/Staging Servers. Web/Application servers host the core Fuze Suite application and provide the public http and https interface for interacting with the application. The Database Servers provide caching and batch processing for production instances, as well as database services for non-production databases. Development/Staging Servers provide source control as well as test environments for testing during the development cycle.

There are currently two web/application servers that have incoming traffic load-balanced between them using an Azure Load Balancer. If needed, some virtual machines may be dedicated to specific high-volume customers only. Because the core application is completely stateless, additional web/application servers can be added to the load balancer up to the limits of the load balancing software being used, which is currently one thousand back-end servers. All web/application servers currently use Windows Server 2016 Data Center or later as their operating systems.

The web/application servers host four portions of the application: the asp.net front-end, the business/data access layer, a batch job to process alerts, and a batch job to convert emails to incidents. Since version 7.0 the business and data access layers have been written using C#/.NET. The current version of .NET being used is 4.8. The web servers are periodically imaged so that copies can be brought online based on need.

There is a single database server that provides caching services using Redis as well as batch processing using scheduled tasks. Caching is done solely for performance and can be removed via a single configuration setting in the application configuration files. The database server is periodically imaged so that copies can be brought online based on need.

# 2 Employee Access Policy

## 2.1 Employee Remote Access Policy

Fuze only grants employees the minimum amount of access needed to perform their job functions. Access to customer data is only given to employees that require access for support or administrative purposes. Additionally, Fuze performs background checks on employees before granting them access to customer data. Background checks will include, at a minimum, criminal records and academic or professional references.

Remote access requires the combination of an Azure AD user, multi-factor authentication and an SSL client certificate for VPN access.

## 2.2 Termination of Access Policy

In the event an employee is terminated, or no longer requires higher level of access to perform job functions, the employee's access will be updated immediately upon change of status. This includes locking out the employee's Active Directory ID, removing their permissions and revoking the certificate used for VPN access.

## 2.3 Physical Access Policy

Now that the application is hosted entirely in Azure, physical access by Fuze employees or customers is no longer possible.

# 3 Remote Access Policy

## 3.1 Overview

All non-public remote access to the hosting environment is strictly controlled. Remote access to the hosting environment requires a Point-to-Site VPN connection to Azure. VPN access is only given to personnel who are necessary for the ongoing maintenance of the system. Each user who is given access to the VPN has an individual username and password that can be revoked individually as well as an SSL certificate that can also be revoked.

The only public access points to the application are through the web servers on ports 80 (http) and 443 (https). Security on traffic through these ports is controlled through the custom security module of the application. The security module uses a username/password authentication scheme and/or a single sign-on (SSO) module to verify a user's identity. The application uses cookies and authentication tokens to maintain state after login.

# 4 Server Security Policy

## 4.1 Overview

Even though an Azure Network Security Group strictly regulates the type of traffic allowed into the system, all servers in the hosting environment are hardened and monitored on a regular basis. Administrative personnel are required to deal with any

incidents immediately and take any additional action required to ensure the integrity of the entire system.

## 4.2 Patches

Because all servers located in the hosting environment are standardized on Microsoft software, tools can be used to automate the detection of necessary patches. Fuze currently uses Nexpose to scan all servers once a month to identify missing patches and any other security configuration issues. If new patches are identified as necessary, the patches will be scheduled for installation. At no time are patches to be applied in an automated fashion without the explicit sign-off of each patch by administrative staff. Patches will only be applied immediately if the threat level of the security risk warrants immediate application. Otherwise patches will be applied 2-3 days after the patch has been released, and the Internet community has time to evaluate the quality of the patch. If other users of the patch identify any issues, the patch will not be applied until all issues have been resolved. If the patch allows it, uninstallation information will be kept for 60 days past the application date of the patch.

Personnel responsible for applying patches are required to subscribe to vendor patch notification lists. If a new patch is released between checks of the system, it is to be evaluated for criticality and applied immediately, if warranted.

Application of Service Packs from Microsoft will follow the same procedure as patches, except that they will only be applied unless a severe threat to the hosting environment is covered only by the service pack, or at least 2 weeks have passed since the release of the Service Pack.

## 4.3 System Monitoring

### 4.3.1 Log Monitoring

All of the servers and the firewall will be monitored on a regular basis for intrusion attempts or other critical system notifications. The firewall and all servers must be configured to log failed connection attempts, failed logins, and attempts to access privileged files by unauthorized accounts, at a minimum. Fuze uses Nagios as its primary log monitoring tool.

In addition to the normal logging provided by the operating system, all servers have the EventSentry tool installed on them that emails administrative personnel in the event of an unexpected application, security or system event. This provides an immediate off-site record of the event and allows staff to deal with events as they occur, rather than waiting for the regular log review process.

Any log entries that indicate an intrusion attempt, must be dealt with immediately. Administrative staff is required to identify, first if the intrusion was successful, and if so to immediately take corrective action. If the intrusion was unsuccessful, the source is identified, to the extent possible, and follow-up action taken with any and all parties associated or complicit with the attempt. Law enforcement authorities will be notified as necessary and appropriate.

Any log entries that indicate a system condition that requires action, must be prioritized immediately. If the condition is non-critical and does not require downtime, corrective

action should be taken after business hours Pacific Time, or as soon as is appropriate. If the condition is critical, it should be dealt with immediately, invoking any system fail-over contingencies necessary to ensure uninterrupted access to the system.

All logs that contain entries relating to an intrusion event will be kept indefinitely. Other log entries may be cleared after 60 days if necessary.

### 4.3.2 Availability Monitoring

Fuze uses Nagios to monitor system and application services and statistics across all of the servers in our network. Individual servers are constantly monitored for memory usage, CPU usage, free disk space and unexpected events in the event log. Nagios also continuously checks specific installed instances of the application to ensure that the web services and customer-facing portions of the application are all working properly. These checks are done against individual servers, and the Azure Load Balancer. In the event that Nagios detects a failure in any one of these checks, Fuze administrative staff are emailed and/or paged with detailed information about the failure within minutes of it occurring.

In addition to the local Nagios monitoring, Fuze uses Solarwinds Pingdom (www.pingdom.com) to monitor the entire system from an external source. The Pingdom checks are configured to check basic services in the system every 5 minutes to ensure the Azure services are available. If any of the services are unavailable Fuze on-call personnel are sent an SMS message with details of the failure.

## 4.4 Server Passwords

Only proper support personnel are given passwords to servers in Azure. Each user has an account and password that can be revoked individually. Server passwords must be changed quarterly, and adhere to the Password Policy outlined in section 10 of this document.

## 4.5 Connections with External Systems

Permanent connections should only be established with external systems when all other options are exhausted. If at all possible, a stateless, encrypted https connection should be used to connect to and from external systems. If a permanent connection must be established on the public Internet, a VPN must be utilized to establish the connection to the external system.

## 4.6 On-call Personnel

An on-call technician is available 24 hours a day, 7 days a week to handle any system failures or incidents. Technicians must be available by email, pager, or cell phone at all times and must be able to receive automated system notifications via one of these mediums. The on-call technician must be within a reasonable distance of an access point to the data center.

All on-call personnel must be properly trained in the design and maintenance of the application environment. They must also be trained in the policies laid out in this document.

# 5 Database Security Policy

## 5.1 Overview

The application uses Azure SQL Databases as its relational database management system. To ensure the integrity of the database system, the following rules are enforced on the database servers:

1. Access to database system is permitted to only machines on the Azure virtual network. Under no circumstances can a client from the public Internet make a direct connection to the database servers.
2. The built-in administrative account is never used in any application or script that connects with the database server.

Patching and maintenance of the Azure SQL Database is done by Azure itself and ensures timely updates of any security patches.

## 5.2 Database Credentials

The administrative account is never used in the application itself or any utility scripts that access the database servers. The administrative account is only to be used for troubleshooting or maintenance purposes and then only when another account will not suffice.

## 5.3 Remote Access

Access to the database system is restricted to computers on the Azure virtual network. Valid database credentials are still required to connect to individual databases, even if the connecting computer is on the virtual network.

# 6 Backup/Fault Tolerance Policy

## 6.1 Overview

The hosting environment is designed to be as fault tolerant and recoverable as possible. Single points of failures are minimized and a pervasive backup system is in place to recover the system in case of failure.

## 6.2 Data Center

The bulk of Azure services are housed in the Azure US West Data Center. Microsoft has a 99.995% average uptime and guarantees a 99.9% uptime in their Service Level Agreement.

## 6.3 Web Servers

### 6.3.1 Fault Tolerance

There are currently two web servers using an Azure Load Balancer to balance incoming traffic between the servers. In the event of failure of one of the web servers all incoming traffic will be routed automatically to the remaining web servers. Because the application is stateless, as many servers as necessary can be added to the load balancer to handle the traffic load. Because individual customer's installations are completely separate from each other, if necessary new, separate clusters can be created at the existing environment or at another site to balance traffic.

The web servers are currently running Windows 2016 Datacenter using IIS 10.

### 6.3.2 Azure Storage Sync Service

Almost all customer data is stored in a SQL Server database that has its own fault tolerance policy, see section 6.4.1. However, there are a few custom files as well as any uploaded customer files, such as images used in knowledge items, that need to be stored on a file system. Azure Storage Sync Service is used to automatically replicate these files between web servers. Each server is part of a storage sync account, which replicates files on all participating servers as well as an Azure Storage account. Any new file, change to existing file, or deletion of a file is automatically and seamlessly replicated to all other web servers.

### 6.3.3 Backup

Backup for the web servers is done in two ways. The VM itself is backed up once a day and maintained for 30 days. If needed, the VM can be restored to any of the currently available back-ups.

Additionally, the individual components are backed up to an Azure Storage account and off-site to an Amazon S3 bucket. Because the web servers host the stateless application itself and not customer data, the backup requirements for the servers are minimal. Each night the application roots, COM/.NET modules, and batch executables are backed up to a separate utility server. Files are copied off-site to an Amazon S3 bucket each night.

An image of the web servers is maintained so that a new server can be brought online by creating a new VM from that image and running a script that copies the latest version of all components to the server.

## 6.4 Database Servers

### 6.4.1 Fault Tolerance

Fuze relies on the Azure SQL Databases high availability architecture provided by Microsoft. The high availability model built-in to Azure SQL Databases is extensive and far beyond what any small to medium-sized business can provide.

### 6.4.2 Backup

Within the Azure SQL Database service each database maintains the ability to do point-in-time recovery back to any point in the last seven days, and a full backup once a day maintained for 30 days.

Additionally, each customer database is exported up in its entirety as a bacpac file every day from Azure and copied to an Azure Storage Account and an Amazon S3 Bucket. The off-site S3 bucket maintains a four-week window of backup files.

# 7 Network Security

## 7.1 Network Security Group

All services are hosted on a virtual network that has a default network security group to control access to the servers. Each server is in one or more application security group

which defines its role. The network security group then uses the application security group to allow access to certain ports based on membership. Web servers allow ports 80 and 443 for web traffic. The mail server allows ports 25 and 587 for SMTP and secure SMTP, ports 143 and 993 for IMAP and secure IMAP, and ports 110 and 995 for POP and secure POP.

Ports 22 (ssh) and 3389 (remote desktop) are only accessible through the VPN.

### 7.2 Web Application Firewall

All publicly addressable web servers must have a web application firewall installed on them to inspect traffic and block requests that are flagged as a threat.

Currently the web servers use Modsecurity IIS as the web application firewall with OWASP rules as the basis of the security ruleset. The core rules have been modified to fit the application, reducing false positives.

Internal tools are used to parse the modsecurity log files and look for traffic that may need additional actions. IP addresses that make large numbers of requests may be blocked entirely. Rules are updated as needed based on real traffic.

### 7.3 DDOS Protection

Fuze utilizes IP specific DDOS protection provided by Azure as needed in the unlikely event of a DDOS attack. Each IP address is protected and configured separately and can be tuned as needed.

## 8 Backup Environment

Fuze maintains a pre-configured Amazon EC2 instance that can take over the hosting of the application in the event of a complete failure of the Azure services.

The instances are configured in the stopped state. The instance is brought online once per month to update it to the latest application code, which is also backed up to Amazon S3 nightly. The instance also has a script that automates the process of copying the latest code base and one or all customer databases and files to the instance.

A single instance was chosen for simplicity and the ease of activation during a disaster. It is intended to be a stop-gap measure that will run all customer instances until the Azure infrastructure can be brought back online or a permanent cloud based solution can be launched. The size of the instance can be updated on the fly to accommodate customer traffic needs.

Once the application web servers have been updated and properly configured and the customer databases have been restored, the DNS records for the application can be updated to point to the AWS environment and traffic will be shifted to the backup environment.

# 9 DNS

Fuze uses Amazon's Route 53 for DNS services. Route 53 gives redundancy for DNS services and allows for an off-site location to alter DNS mappings in the event of a total failure of Azure services. See the Route 53 information page for more information on Route 53: https://aws.amazon.com/route53/

# 10 Audit Policy

## 10.1 Auditing by Fuze

Fuze operations personnel review this policy and its implementation on a quarterly basis. If the sections of this policy are not being properly followed, corrective action is taken immediately. The document is also revised as necessary to document any new policies and conditions.

Any employees found to be violating the policies laid out in this document will be subject to disciplinary action, up to and including termination. Employees are required to read and be trained on the policies in this document before being given access to the hosting environment.

## 10.2 Auditing by Customers

Customers may audit Fuze for compliance with this document with the following conditions:

1. Port Scanning and Penetration Testing may be done without prior notice, but notice must be given immediately after the tests are concluded, with a summary of the results.
2. Any Port Scanning/Penetration Testing must be done with the utmost care to not damage any system or data. The party engaging in the testing is responsible for any damage that may result from their testing.
3. Tests of Denial of Service (DOS) attacks may not be done at any time.
4. Customers will be given access to generic security logs and data that is specific to that customer. Customers will never be given access to other customer's data and logs.

# 11 Media Disposal Policy

Physical media is no longer used in any capacity as part of normal operations. In the event physical media is created and needs to be disposed of, any physical media storing any code or data will be overwritten using a secure drive wiping tool such as Active@ KillDisk and destroyed. No physical media will be resold for use by another party.

# 12 Password Policy

## 12.1 General Policy

Unless otherwise noted all passwords used in the hosting environment must conform to the following password policy.

1. Passwords must be at least 8 characters in length.

2. Passwords must include at least one alpha character, one numeric character and one non-alphanumeric character.
3. Passwords must be changed on at least a quarterly basis.
4. Passwords must not be words found in a dictionary.
5. Passwords must never be given out over the phone or through email.
6. Passwords must never be used in a clear-text network communication.
7. Passwords must never appear in an unencrypted document.
8. This policy applies to any external system that impact the hosting environment, such as Internet Registrars, off-site monitoring, and off-site backup storage.

# 13 Intrusion Notification Policy

## 13.1 Intrusion Detection and Containment

In the event of an intrusion, Fuze's first priority will be to block and/or contain the intrusion. Priority will also be given to preserving forensic evidence as much as possible during containment. If at all reasonably possible, disk images and network logs will be copied off site.

## 13.2 Intrusion Notification Policy

Once the intrusion is contained Fuze will perform an initial analysis to determine which customers need to be notified and gather the data to include in the notification. If Fuze cannot reasonably determine which specific customers are affected, then all customers will be notified. An initial notification must be sent within 48 hours of containment. The following data will be gathered, if at all possible, and sent to affected customers to notify them of the incident.

1. Date/time of the intrusion and date/time of containment.
2. The method of access.
3. The method of containment.
4. A description of what data intruders had read or write access to.
5. Any evidence data was copied or destroyed.
6. Any known information about the attacker.

Fuze will also provide extracts to customers who wish to notify individual end users of the breach. If any of the above information cannot be reliably determined Fuze will state so in the initial notification but also outline the worst-case scenario.

In the interest of timeliness the initial notification will be made via email, but a written copy of the notification can be provided upon request via U.S. mail.

After the initial notification, Fuze will continue analysis of the intrusion, working with customers and law enforcement as appropriate. Fuze will make every reasonable effort to answer customer questions regarding the specifics of the breach. Once analysis of the intrusion is complete, Fuze will create a final report containing the final versions of each item outlined in the initial notification. The final report will also include a detailed report on updates to infrastructure and the security policy needed to prevent a breach from happening in the future.

### 13.3 Data Retention

1. Fuze will keep the final report of the intrusion indefinitely.
2. Fuze will keep raw forensic data in an off-site location for at least 12 months.
3. Fuze will keep any notes or analysis documents for at least 12 months.
4. All incidents created by customers in relation to the breach will be kept indefinitely.

## 14 Application Change Management

### 14.1 Licensed Customers

Licensed customers receive application updates once per year, along with a document that outlines the new features and options in the update.

Fuze will work with licensed customers to schedule the upgrade weeks in advance. Typically, licensed upgrades take 1-2 hours with 15-30 minutes of downtime, depending on the specifics of the licensed installation.

### 14.2 Hosted Customers

To ensure that hosted customers have access to the latest features and bug fixes, Fuze practices continuous integration, with deployments typically happening once per week. Optional new features are always installed in the disabled state so that customers may enable them when and if they choose. All new features are accompanied by updated documentation.

### 14.3 Deployment Process

All application code is stored in source control, currently Git. Fuze maintains a build server to build the latest version of the application from source control and deploy it to a testing server.

For normal deployments Fuze does a full build of the application from source control to the test server. The deployment is done through a script and requires administrator level permissions to execute, which is only given to personnel approved to update the application. Updates are tested on the testing server and updates are validated there before deployment.

Once all updates have been approved, a production server is removed from the production load balancer, and once all connections have been cleared that server is updated with the exact build used on the testing server. This is also done through a script requiring administrator permissions on the build server. Once the update is complete the updated server is added back into the load balancer and the server(s) containing the old application are removed. If a roll-back is needed, the updated server is removed from the cluster and the server containing the old version of the application is added back in, automatically putting the application back in its last known good state.

The application is never updated directly from developer workstations, only through scripting. In rare cases when a high-priority bug fix is needed the production servers may be updated with a patch containing only the bug fix, rather than a full build. The patch is still created from a full build created from Git that was deployed to the testing server.