

**Planning & Design Document**

**SVB PROD Environment**

|  |
| --- |
|  |

Document Change Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Requester** | **Author** | **Change/Review** |
| 13/06/2020 | 1.0 | Krishna Prasad | Karthick Kumar | Initial Issue |
|  |  |  |  |  |
|  |  |  |  |  |

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| DR Proceddure | Access Control | | |
| Modified By | Karthick Kumar | Modified Date | 15/06/2020 |
| Reviewed By |  | Review Date |  |
| Approved By |  | Approval Date |  |
| Modified By |  | Modified Date |  |
| Reviewed By |  | Review Date |  |
| Approved By |  | Approval Date |  |

**List of Acronyms**

|  |  |
| --- | --- |
| **Name** | **Definition** |
| SVB | Silicon Valley Bank |
| VNET | Virtual Network |
| VM | Azure Virtual Machine |
| SA | Azure Storage Account |
| IAM | Identity and Access Management |
| MFA | Multi Factor Authentication |
| NSG | Network Security Group |
| DNS | Domain Name System |
| AZ | Availability Zone |
| RSV | Recovery Service Vault |
| KV | Keyvault |
| HA | High Availability |
| DR | Disaster Recovery |
| VPN | Virtual Private Network |

**Table of Contents**

[1 Introduction 4](#_Toc43816255)

[1.1 Purpose: 4](#_Toc43816256)

[1.2 Scope: 4](#_Toc43816257)

[2 Azure Subscription 4](#_Toc43816258)

[3 Network design topology 4](#_Toc43816259)

[3.1 SVB Prod VM details: 5](#_Toc43816260)

[3.2 SVB Prod SQL Failover group and DB details: 5](#_Toc43816261)

[3.3 PAAS Common- Prod SFTP VM and LB details: 5](#_Toc43816262)

[3.4 PAAS Common- Prod SFTP MFT SQL: 5](#_Toc43816263)

[4 High Availability 5](#_Toc43816264)

[4.1 High Availability on Azure with Availability Zones 6](#_Toc43816265)

[4.2 Virtual Machine: 6](#_Toc43816266)

[4.3 VPN Gateway / VPN Connection: 6](#_Toc43816267)

[4.4 Azure Firewall: 7](#_Toc43816268)

[4.5 Application Gateway 8](#_Toc43816269)

[4.6 Azure SQL DB 9](#_Toc43816270)

[4.7 Azure File Share 9](#_Toc43816271)

[4.8 Azure Key Vault 10](#_Toc43816272)

[5 Backup 10](#_Toc43816273)

[6 Disaster Recovery 11](#_Toc43816274)

[7 Monitoring 11](#_Toc43816275)

[8 Miscellaneous 12](#_Toc43816276)

[9 Onboarding/Off boarding 12](#_Toc43816277)

# Introduction

Payment as a service (Pass) - VolPay application for SVB has been hosted on Azure cloud.

## Purpose:

This document provides details around as to how the planning and design implemented for SVB customer.

## Scope:

Scope of this document include information on SVB Azure infrastructure, which includes deployment of VolPay application and Other Infra related resources.

# Azure Subscription

To setup this SVB environment we used below subscription.

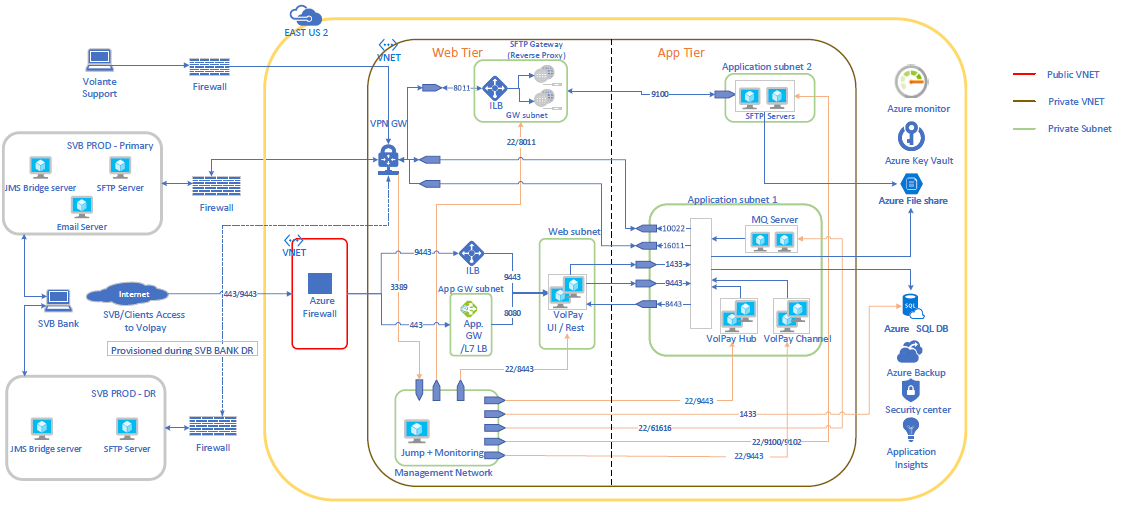
For UAT: Pay as you go

For PRD & DR: PAAS-Production

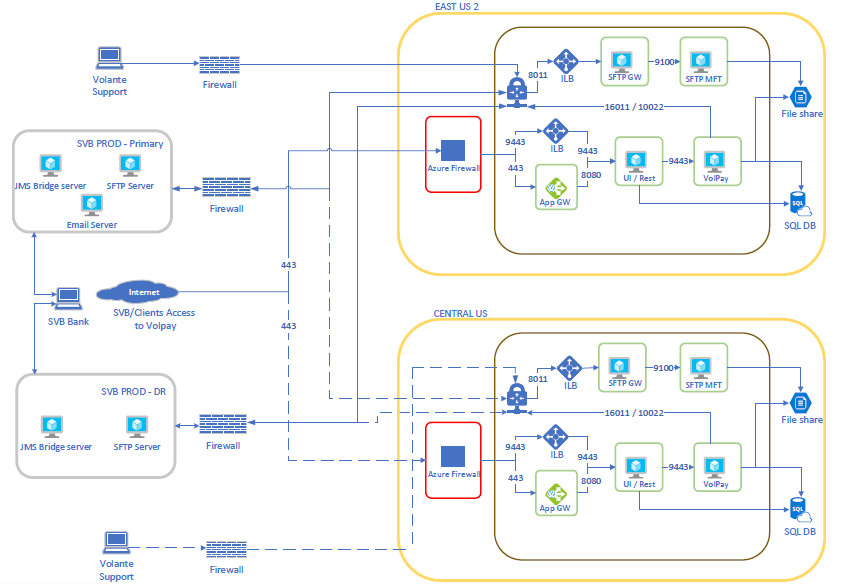
# Network design topology

Below is the network design topology for SVB customer. Each component will be discussed in detail in following sections.

1. SVB – Volpay production network topology



1. SVB – Volpay disaster recovery network topology



## SVB Prod VM details:

|  |  |  |
| --- | --- | --- |
| Name | Private IP address | Role |
| svbprdmgmtjmpvm | 172.16.36.4 | Jump Server |
| svbprdinfrajpvm | 172.16.36.5 | Jump Server |
| svbprduirestvm1 | 172.16.33.4 | VolPay UI / Rest |
| svbprduirestvm2 | 172.16.33.5 | VolPay UI / Rest |
| svbprdvolchnvm1 | 172.16.34.6 | VolPay Channel |
| svbprdvolchnvm2 | 172.16.34.7 | VolPay Channel |
| svbprdvolhubvm1 | 172.16.34.8 | VolPay Hub |
| svbprdvolhubvm2 | 172.16.34.9 | VolPay Hub |
| svbprdamqsvm1 | 172.16.34.4 | Active MQ Server |
| svbprdamqsvm2 | 172.16.34.5 | Active MQ Server |

## SVB Prod SQL Failover group and DB details:

Primary SQL Server: svbprdsqlserver.database.windows.net

Secondary SQL Server: svbdrsqlserver.database.windows.net

Failover group name: svbprdsqldbfg.database.windows.net

Database name: svbprdsqldb

## PAAS Common- Prod SFTP VM and LB details:

|  |  |  |
| --- | --- | --- |
| hmsprdsftpsvm1 | 192.168.16.4 | HMS PRD SFTP Server |
| hmsprdsftpsvm2 | 192.168.16.5 | HMS PRD SFTP Server |
| hmsprdsftpgwvm1 | 192.168.17.4 | HMS PRD SFTP Gateway |
| hmsprdsftpgwvm2 | 192.168.17.5 | HMS PRD SFTP Gateway |
|  | 192.168.17.6 | HMS PRD SFTP Gateway LB |

## PAAS Common- Prod SFTP MFT SQL:

SQL Server name: hmsprdsftpclrserver.database.windows.net

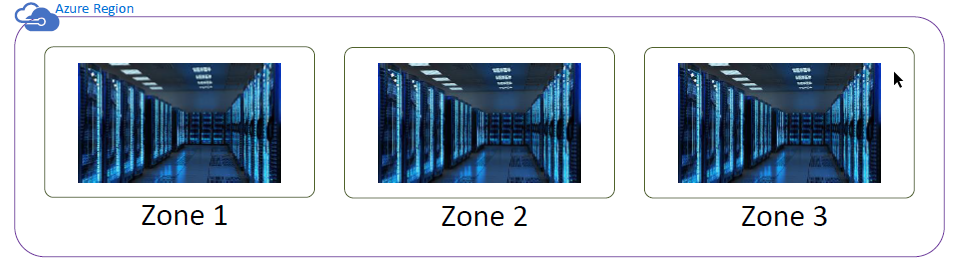
Database name: hmsprdsftpclsterdb

# High Availability

VolPay Production Environment designed to have High Availability enabled on all infrastructure components involved in the deployment. We’ll briefly see how HA is achieved for key components in sections below

## High Availability on Azure with Availability Zones

Availability Zones are unique physical locations with independent power, network, and cooling. Each Availability Zone is comprised of one or more datacentres and houses infrastructure to support highly available, mission critical applications. Availability Zones are tolerant to datacentre failures through redundancy and logical isolation of services.

****

Benefits of Availability Zone that protect application outages from below scenarios

1. Unexpected underlying hardware failure

2. Planned underlying hardware maintenance activity

3. Entire datacentre level failure

## Virtual Machine:

VolPay application has installed and configured on VM. To achieve HA for VolPay application, we have used two VM for each application component (VolPay UI/Rest, Hub, Channel, ActiveMQ) and placed them on two different zones. If there is any issue with one application VM during underlying hardware or during software upgrade, we still have another VM to provide HA.

## VPN Gateway / VPN Connection:

To use VolPay application, SVB has established the VPN connection with Volante Azure environment. To achieve HA for VPN, we have used zone redundant option which will ensure the availability of VPN even if entire zone goes down.

From SVB side, they have provided two gateway device details as primary and backup to attain HA.

We have used the custom policy parameters for VPN connection.

IKE Phase 1

|  |  |
| --- | --- |
| Key Encryption | AES256 |
| Integrity | SHA1 |
| Diffie-Hellman Group | Group 2 1024 bit |
| IKE Timeout | (28800 seconds) |
| IKE Mode | Main |

IPSec Phase 2

|  |  |
| --- | --- |
| Data Encryption | AES256 |
| Integrity | SHA1 |
| Diffie-Hellman Group | Group 2 1024 bit |
| IPSEC Timeout | 600 |
| Perfect Forward Secrecy (PFS) | None |

|  |  |  |
| --- | --- | --- |
| VPN Connection Name | VPN Gateway Name | Local Gateway Name |
| svb-prd-chandler-azure-s2s-connection-new | svb-prd-vpn-gw | svb-prd-chandler-local-gw |
| svb-prd-dallas-azure-s2s-connection-new | svb-prd-vpn-gw | svb-prd-chandler-local-gw |

## Azure Firewall:

Azure Firewall is a managed, cloud-based network security service that protects our Azure Virtual Network resources. It's a fully stateful firewall-as-a-service with built-in high availability and unrestricted cloud scalability. Azure Firewall is configured during deployment to span multiple Availability Zones for increased availability.

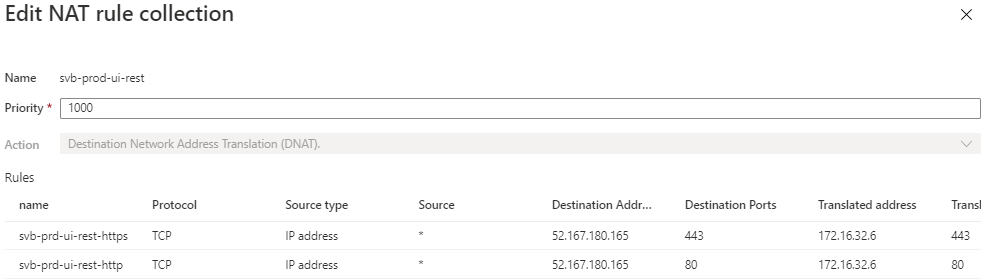
**Key Features**

Threat intelligence-based filtering can be enabled for firewall to alert and deny traffic from/to known malicious IP addresses and domains. The IP addresses and domains are sourced from the Microsoft Threat Intelligence feed.

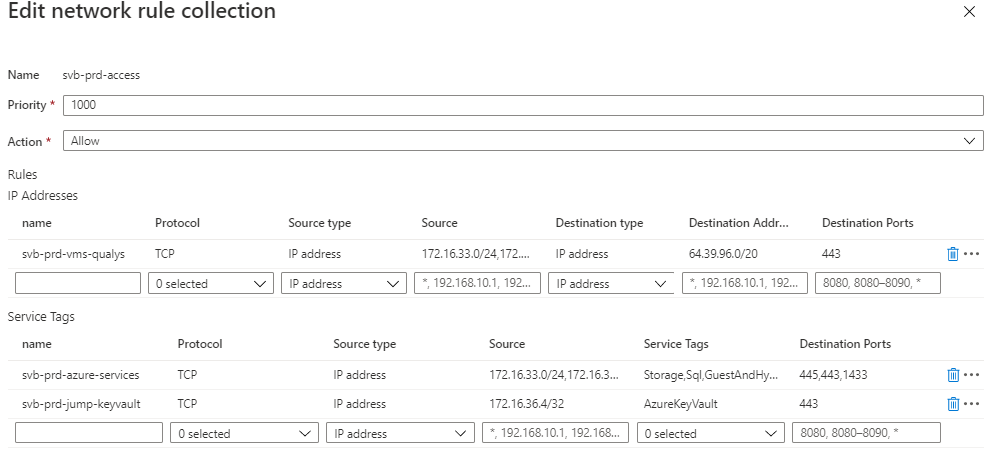
Outbound SNAT support

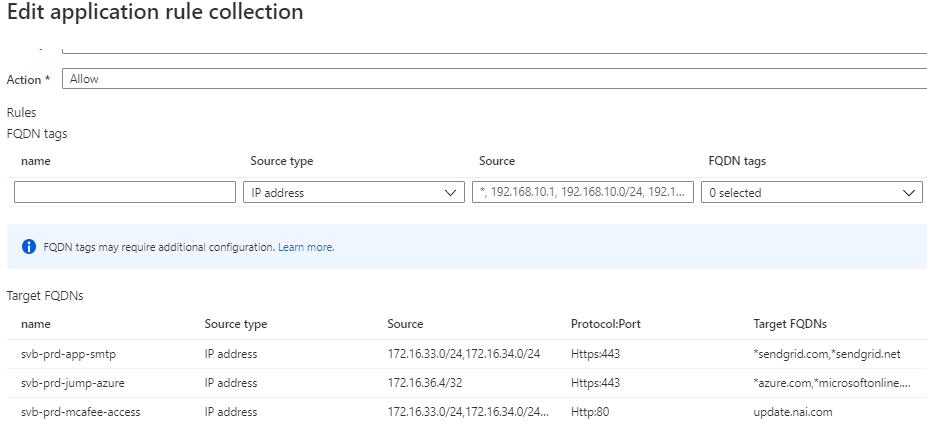
Inbound DNAT support

We have created DNAT rule for UI/Rest application to secure and filter the network traffic. In DNAT rule, any traffic is coming from internet for port 80 and 443 on firewall IP has redirected to Application Gateway private IP on port 80 and 443. Please see the rule details below



We have blocked internet access from application VM and created the route table to route the internet traffic to azure firewall and opened the firewall rules to specific Ips and service tag enabled for azure services.





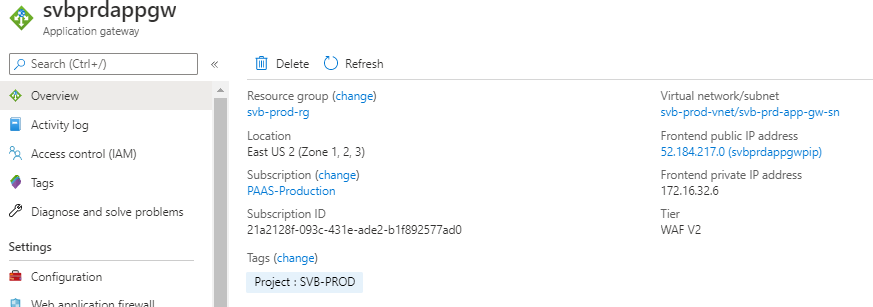
## Application Gateway

WAF is deployed spanning multiple Availability Zones to offer zonal failure resiliency, removing the need to provision separate Application Gateway instances in each zone. The backend pool for VolPay applications are similarly distributed across availability zones.

**Key Features**

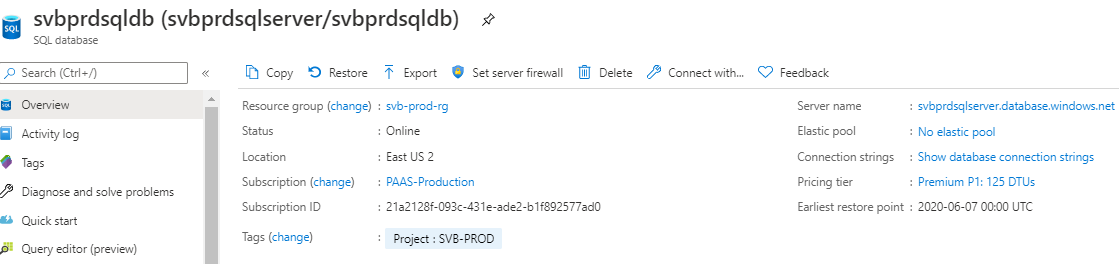
Secure Sockets Layer (SSL/TLS) termination – We have installed tagglobal.svb.com / tag.svb.com and volantetech.com SSL on application gateway.

We have enabled Web application firewall (WAF) to provide centralized protection of web applications from common exploits and vulnerabilities. WAF is based on rules from the OWASP (Open Web Application Security Project) core rule sets 3.1



## Azure SQL DB

VolPay application is using Azure SQL DB for storing the data. We have chosen single database with Premium tier for zone redundant availability. Database can be access only from jump server, web tier and app tier using service endpoint connectivity. Transparent Data Encryption (TDE) has enabled with customer managed key. We configured geo replication with failover enabled on central us (DR) region for disaster recovery.



## Azure File Share

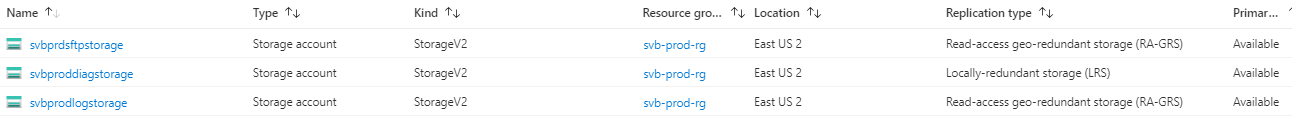
We have created three file shares for SVB deployment.

VolPay using azure file share for SFTP file consumption from SVB. This file share has been mounted on SFTP servers, VolPay Hub and Channel servers. So that once the file has dropped by SVB customer on file share, VolPay will pick the file and process it and after processed it will drop them on their SFTP servers.

One storage account for VM boot diagnostics and another storage account for storing the diagnostics logs.

Storage accounts have encrypted with customer managed key and replicated the data to across region for DR purpose.

Except boot diagnostics storage, rest of both storage account can be accessed only from jump servers or from application subnets using service endpoint.



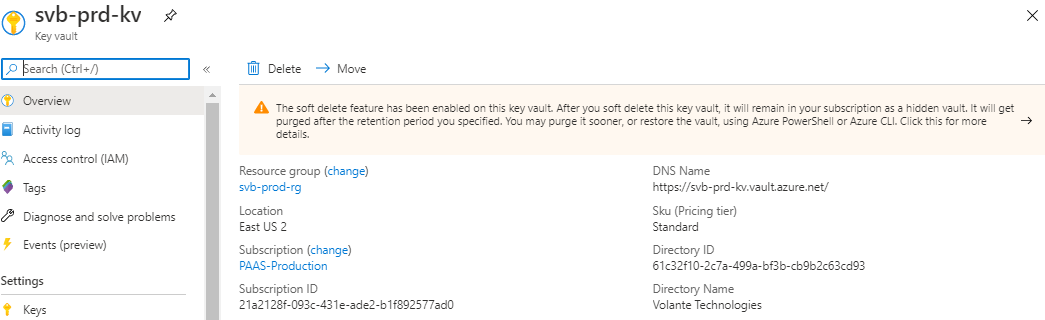
## Azure Key Vault

To secure the environment, we have used customer managed key rather azure service managed key. For SQL and Storage, we have created two different keys.

Keys can be accessed only from allowed network range like from jump servers for managing the keys.

In access key policies, only cloud infra team and application service principal have access to encrypt and decrypt keys.

We have enabled soft delete option for 90 days. In case if there is any keys got deleted accidently, we will be able to restore using PowerShell commands.



# Backup

**For VM:** We have automated the VM snapshot backups using automation account. Runbook will be executed every week and take snapshots for all the VM’s in prod resource group. For VM snapshot, we have kept 4 weeks as retention period.

**For SQL DB**: SQL Database uses SQL Server technology to create full backups every week, differential backups every 12 hours, and transaction log backups every 5 to 10 minutes. The backups are stored in RA-GRS storage blobs that are replicated to a paired datacentre for protection against a datacentre outage. When you restore a database, the service determines which full, differential, and transaction log backups need to be restored.

Point in Time Restore: 35 days retention

Long Term Retention policy: Monthly backup retention to 6 months.



# Disaster Recovery

For SVB deployment, DR has considered with RTO of 4 hours and RPO of 1 hour as agreed with customer. Complete environment has planned to deploy on DR region. For VM, Azure site recovery has used, For SQL, geo replication with failover group used, for file share, read only geo replicated storage has used. For rest of the networking components like virtual network, subnets, route table, network security group have preconfigured already. During the time of DR, we will deploy azure firewall, application gateway and VPN connection.

We have separate document for DR invoke procedure with all details.

# Monitoring

We have used azure native monitoring for SVB infrastructure.

Log Analytics Workspace

Network Watcher

Azure Monitor

Below are the parameters has configured to monitor.

**VM availability** – We have configured heartbeat alert between VM and Log analytics. If the server is not available, it will stop sending data to log analytics hence we will receive alert. Additionally, azure health alert has configured for VM.

**Port monitoring** – All the application services are listening on specific ports are monitoring using network watcher. If any port goes down, we will get alert.

**CPU, Memory, Disk usage monitoring** – For all the VM, we have installed log analytics agent to send the data and configured monitor. If the threshold has reached above 70%, we will get alert.

**Azure Firewall** – health alert for FW availability and if there is any create, update or delete activity happened then we will get notification.

**Application Gateway** – Unhealthy host alert and failed request alert has configured.

**Azure Load Balancer**- SFTP GW LB health probe alert configured

**SQL Database inaccessible alert**- If SQL DB lost connectivity with keyvault, DB will go to inaccessible state and we will get alert.

**SQL database-** CPU, Storage, DTU, Failed Connections alerts configured.

**SQL Server**- Any firewall changes we will alert

**Storage Account**: Azure storage account availability and if any changes on storage accounts, we will get alert notification.

**Key Vault**- If any changes in the keyvault, we will get notification.

**NSG Rule** – If any new NSG or NSG rule create / update / delete, we will get notification

# Miscellaneous

VolPay application will be triggering an email to end users if their password expired for UI login or if their payment got rejected. Volante uses SendGrid for domain authentication method for SVB.COM as we send email using svb.com email address.

# Onboarding/Off boarding

If any new user request for access they must be given with the below access after appropriate approval in place.

**To Onboard:**

Azure portal access

SVB UAT/Prod VPN for the new user to connect jump VM.

Jump server – user must be created and share the credential with user.

Teleport user creation with “SVB-support” role to access SVB VM’s

**To Offboard:**

All the above access must be removed

**\*\*\*\*\*\*\*\*\*End\*\*\*\*\*\*\*\*\***