



## **FIBERME Communications LLC.**

---

FCM630A Series IP PBX - High Availability User Guide

# Table of Contents

<b>INTRODUCTION.....</b>	<b>6</b>
<b>TYPICAL NETWORK TOPOLOGY .....</b>	<b>7</b>
<b>HA PREREQUISITES .....</b>	<b>8</b>
Prerequisites.....	8
Connecting FCM for HA Setup.....	8
Network Configuration.....	8
<b>HA CONFIGURATIONS .....</b>	<b>10</b>
<b>HA CONFIGURATION PARAMETERS.....</b>	<b>15</b>
<b>VERIFY HA SETTINGS .....</b>	<b>21</b>
<b>ACTIVE/STANDBY ROLE IN HA .....</b>	<b>22</b>
Automatic Failure Detection.....	22
Active FCM: Self-Failure Detection .....	22
Standby FCM: Periodic Heartbeat.....	23
Force Switch.....	23
<b>FIRMWARE UPGRADE.....</b>	<b>24</b>
<b>REPLACING FCM IN HA.....</b>	<b>25</b>
<b>DISABLING HA SETUP .....</b>	<b>27</b>
<b>SERVICE STATUS .....</b>	<b>30</b>
Active/Standby Status.....	30
Web UI Access for FCM.....	30
<b>FAILOVER DURING CALL .....</b>	<b>31</b>
<b>DATA SYNC .....</b>	<b>32</b>
<b>BACKUP AND RESTORE.....</b>	<b>33</b>
<b>MAINTENANCE.....</b>	<b>34</b>



## Table of Figures

Figure 1: Typical Network Topology .....	4
Figure 2: Network Settings .....	6
Figure 3: HA Settings on Primary FCM.....	7
Figure 4: HA Settings on Secondary FCM .....	8
Figure 5: HA Configured on Secondary FCM .....	9
Figure 6: HA Status on Secondary FCM .....	9
Figure 7: HA Status for Active FCM.....	13
Figure 8: HA Status for Standby FCM.....	13
Figure 9: Active and Standby FCM Failover.....	14
Figure 10: Force Switch .....	15
Figure 11: System Alert Events.....	20
Figure 12: HA Logs .....	20

## Table of Tables

Table 1: HA Related Parameters.....	10
-------------------------------------	----



## INTRODUCTION

High Availability feature on FIBERME FCM630A provides enterprises a reliable solution for PBX redundancy and failover support. In HA setup, there are two FCM with one FCM in “active” role and the other in “standby” role. The two FCM must be the same model and use the same firmware version. The data on the active FCM will be synchronized to the standby FCM in real-time manner and the standby FCM monitors active FCM’s running status regularly. When the active FCM runs into hardware or critical software issues, the standby FCM will take over immediately and become the active server. HA feature supports automatic call recovery for UDP point-to-point calls and conference calls, allowing enterprises to communicate and collaborate without the hassle of service interruption.



## TYPICAL NETWORK TOPOLOGY

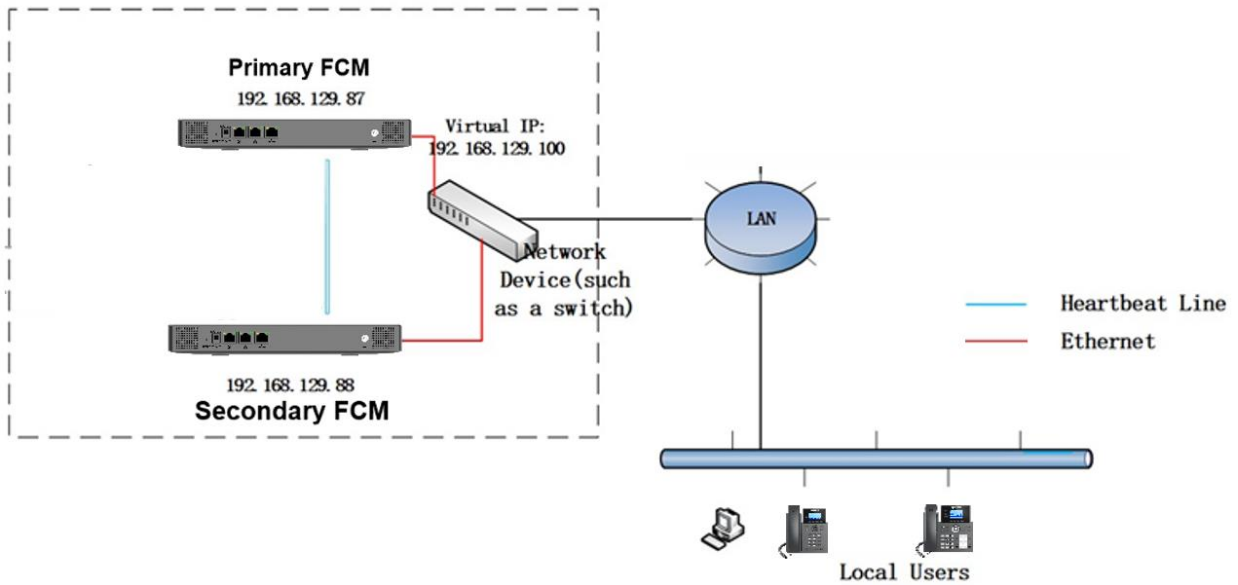


Figure 1: Typical Network Topology

The two FCM in High Availability setup must be deployed in the same location and connected directly to each other via heartbeat port on each FCM. The primary FCM and secondary FCM can be connected to each other via a straight-through Ethernet cable on the heartbeat port. For each FCM, connect its WAN or LAN port to the uplink network device.



# HA PREREQUISITES

## Prerequisites

The two FCM used for High Availability deployment must be the same model and use the same firmware version to ensure proper sync-up on the configuration and data.

## Connecting FCM for HA Setup

The two FCM in High Availability setup must be deployed in the same location and connected directly to each other via heartbeat port on each FCM.

- Connect a straight-through Ethernet cable between the heartbeat port on the primary FCM and secondary FCM.
- For each FCM, connect its WAN or LAN port to the uplink network device (such as a switch or router).

## Network Configuration

Before enabling High Availability feature on the two FCM, the system admin must configure each FCM with proper network settings.

### Notes:

- The network "Method" on the FCM must be set to "Switch" or "Router".
- The IPv4 address configured on the FCM must be static IP. It can be configured under FCM web UI→Network Settings→Basic Settings.



Network Settings

**Basic Settings**    802.1X Settings    Static Routes    Port Forwarding    ARP Settings

Method:

MTU:

**IPv4 Address**    IPv6 Address

Preferred DNS Server:

**LAN**

IP Method:

\* IP Address:

\* Subnet Mask:

\* Gateway IP:

\* DNS Server 1:

DNS Server 2:

Layer 2 QoS 802.1Q/VLAN Tag:

Layer 2 QoS 802.1p Priority Value:

Figure 2: Network Settings



## HA CONFIGURATIONS

For two new FCM on factory default setting, system admin can choose to configure any of them for HA first. However, if one of the FCM is already configured, up and running for PBX service, system admin should configure this FCM as HA Primary server and complete all HA settings on it first so it can act as active role. Please refer to the steps below to configure HA on FCM:

1. Ensure both FCM have the same model and same firmware version. They have been connected properly at the same location and configured with static IP.
2. Select one FCM to be the active device (FCM A). If both FCM are new on factory default settings, select any of them as the active FCM. If one of the FCM is already configured and running, then select this FCM as the active device.
3. Log in the active FCM (FCM A) web UI and go to System Settings→HA page. Enable HA and configure FCM A as Primary station type. Please refer to HA related parameters in table 2 below and complete other HA related settings. Save the HA settings on FCM A and reboot FCM A. Ensure FCM A boots up normally.

The screenshot displays the 'HA Settings' page in a web interface. At the top, there are two tabs: 'HA Settings' (selected) and 'HA Log'. The settings are as follows:

High Available Enable:	<input checked="" type="checkbox"/>
Force Switch:	Switch
* HA Station Type:	Primary
* HA Cluster IP:	192.168.129.64
* HA Peer IP:	192.168.129.43
* HA Peer MAC Address:	
* Heartbeat Port:	9527
* Heartbeat Timeout Period (s):	7
Software Fault Switch:	<input checked="" type="checkbox"/>
Hardware Fault Switch:	

Figure 3: HA Settings on Primary FCM





4. Verify HA status on FCM A. Log in FCM A using its static IP and admin login information. On web UI→System Settings→HA page, ensure HA function is enabled. HA status should display “Active”.
5. After ensuring FCM A’s HA status as active, configure FCM B as secondary FCM and complete FCM B’s HA settings. Log in FCM B’s web UI and go to System Settings→HA page, enable HA and set the station type as “Secondary”. Please refer to HA related parameters in table 2 below to complete other HA related settings. Save the settings and reboot FCM B.

The screenshot shows the 'HA Settings' page for a Secondary FCM. The page has two tabs: 'HA Settings' (active) and 'HA Log'. The settings are as follows:

Parameter	Value
High Available Enable:	<input checked="" type="checkbox"/>
Force Switch:	Switch
* HA Station Type:	Secondary
* HA Cluster IP:	192.168.129.64
* HA Peer IP:	192.168.129.57
* HA Peer MAC Address:	
* Heartbeat Port:	9527
* Heartbeat Timeout Period (s):	7
Software Fault Switch:	<input checked="" type="checkbox"/>
Hardware Fault Switch:	

**Figure 4: HA Settings on Secondary FCM**

6. After FCM B boots up normally, log in FCM B’s web UI via its static IP address and admin login information. Go to System Settings→HA page, ensure the HA function is enabled, “Switch” button is grey and only HA peer IP / peer MAC address options are available for configuration. The HA status should display as “Standby”.



HA

HA Settings    HA Status    HA Log

High Available Enable:

Force Switch:

\* HA Station Type: Secondary

\* HA Cluster IP: 192.168.129.64

\* HA Peer IP: 192.168.129.57

\* HA Peer MAC Address:

\* Heartbeat Port: 9527

\* Heartbeat Timeout Period (s): 7

Software Fault Switch:

Hardware Fault Switch:

Figure 5: HA Configured on Secondary FCM

HA

HA Settings    **HA Status**    HA Log

HA Status: Dual

HA Full Backup Status: Idle

MAC Address of Current UCM:

Role of Current UCM: Standby

Figure 6: HA Status on Secondary FCM



## HA CONFIGURATION PARAMETERS

Table 1: HA Related Parameters

Settings	Description	Value Range	Default Value	Notes
<b>High Available Enable</b>	Enable or disable HA.	Yes/No	No	
<b>Force Switch</b>	Force to switch the roles of active FCM and standby FCM.	NA	NA	Caution: Please do not use this function unless necessary (e.g., it can be used during firmware upgrading).
<b>HA Station Type</b>	Configure the HA station type for the FCM.	Primary Secondary	NA	In HA setup, one FCM must be primary and the other one must be secondary.
<b>HA Cluster IP</b>	This is the IP address for the active FCM in service.	NA	NA	This IP address is shared by the primary and secondary FCM. The FCM in active status providing PBX service will always be using this IP address regardless it's the primary or secondary FCM. This IP address can only be used for the active FCM.
<b>HA Peer IP</b>	This is the IP address of the peer FCM in HA setup.	NA	NA	This is the static IP address of the peer FCM in HA setup connected via heartbeat port.
<b>HA Peer MAC Address</b>	This is the MAC address of the peer FCM in HA setup.	NA	NA	This is the MAC address of the peer FCM in HA setup connected via heartbeat port.
<b>Heartbeat Port</b>	This is the port used for communication between the two FCM via heartbeat port.	0 - 65535	9527	It is recommended to use default port.



<b>Heartbeat Timeout Period (s)</b>	This is the heartbeat timeout period that active and standby FCM will check with each other for the status (in seconds).	3 - 10	7	If the standby FCM detects the active FCM disconnected, when it reaches the timeout, failover will be triggered and the standby FCM will start taking over as active FCM.
<b>Software Fault Switch</b>	Enable failover upon software failure	On/Off	Off	If enabled, when there is critical software failure such as deadlock or system crash detected, it will trigger failover from active FCM to standby FCM. Otherwise, failover will not happen.
<b>Hardware Fault Switch</b>	Enable failover upon hardware failure	On/Off	Off	If enabled, when there is hardware failure, it will trigger failover from active FCM to standby FCM. Otherwise, failover will not happen.

After enabling High Available feature, please configured the following parameters:

- **Station Type (mandatory):**

In HA setup, one FCM must be set as primary and the other one must be set as secondary. The two FCM cannot be configured as the same type. Otherwise, HA function will not work properly. This configuration is to ensure that there is always a FCM on active status and the other one on standby status during negotiation which will automatically determine the active/standby server. When failure condition happens, it is crucial that the failover mechanism does not end up with two active servers negotiated.

The active FCM is the PBX providing service and it's not always the primary server configured in HA. The primary secondary station type is configured but any FCM in HA setup can be the active or standby role when needed. For example, if FCM A is configured as primary station type and FCM B is configured as secondary station type, at the beginning FCM A is in active role and FCM B is in standby role. After failover happens, FCM A's station type configuration is still primary but it's now in standby role and FCM B is in active role.



- **HA Cluster IP (mandatory):**

This is the IP address for the FCM that provides PBX service in HA setup. This IP is always associated with the FCM in active status. For example, when configuring IP phone to register to FCM, this is the SIP server IP address to be configured on the IP phone. When configuring SIP peer trunk, this is the SIP server IP address to be configured as peer trunk server IP. In HA setup, the static IP configured for each FCM will not be used for PBX service directly. Normally the cluster IP address is in the same subnet as the static IP address configured on the FCM.

- **HA Peer IP (mandatory):**

This is the static IP configured on the peer FCM in HA setup.

- **Peer MAC Address (optional):**

This is the MAC address of the peer FCM in HA setup.

- **Heartbeat Port (mandatory):**

This is the port used for communication between active and standby FCM for heartbeat negotiation. It is recommended to use the default port number 9527.

- **Heartbeat Timeout Period (mandatory):**

This is the timeout period for heartbeat (in seconds). The standby FCM will check regularly whether the active FCM is working normally. If the standby FCM detects that the active FCM has been disconnected for this period, the standby FCM will consider the active FCM in faulty state and will then automatically take over as active FCM.

- **Software Fault Switch:**

If enabled, when the active FCM experiences software failure such as system crash with core dump generated, it will trigger failover automatically and the standby FCM will take over. If disabled, HA alert events will be reported without failover.

- **Hardware Fault Switch:**

If enabled, when the active FCM has hardware, it will trigger failover automatically and the standby FCM will take over. If disabled, HA alert events will be reported without failover.

- **Force Switch:**

This will force active and standby FCM to switch roles. It will trigger the standby FCM to take over and switch the active FCM to standby role. This should be used only when necessary, such as firmware upgrading or if active FCM cannot automatically trigger switchover.

After the above configurations, click on Save and follow the reboot prompt to reboot the device.

**Note:** HA configuration requires the FCM to reboot. Please reboot the FCM during non-service hour to avoid service interruption.



## VERIFY HA SETTINGS

1. After configuring HA settings on both FCM, log in the FCM web UI from each FCM's static IP using the active FCM's login information and check HA status. Under HA status page, both FCM should show HA Status as "Dual". One of the FCM should show its role as "Active" and the other one should show "Standby". For "HA Full Backup Status", it will show backup in progress during backup and show as idle during the rest of the time.

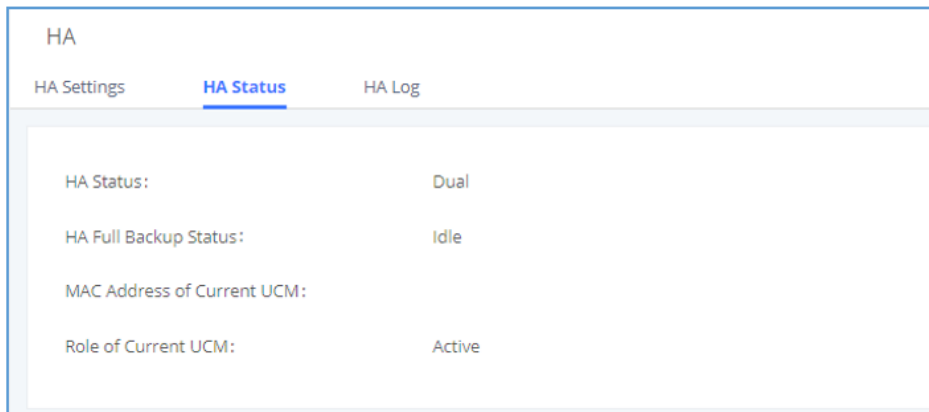


Figure 7: HA Status for Active FCM

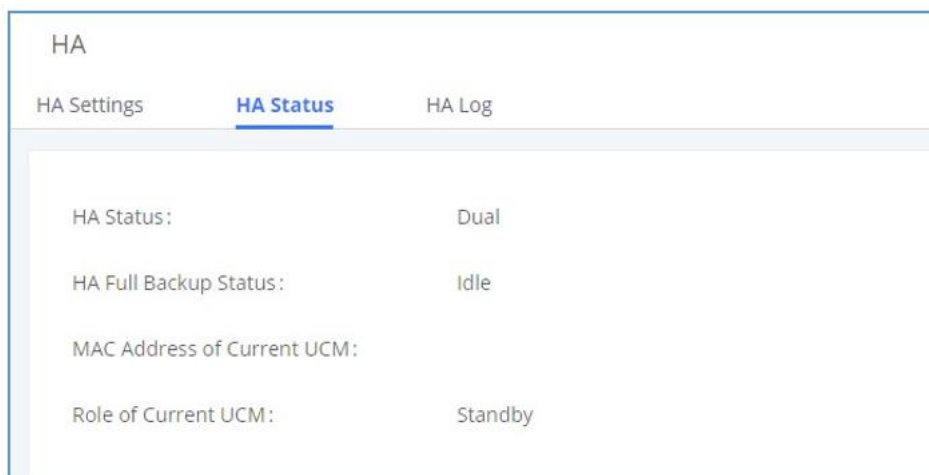


Figure 8: HA Status for Standby FCM

2. Log in the active FCM's web UI and create new SIP extensions. Then log in the standby FCM's web UI to check whether the same extensions created on active FCM are synchronized here. If there are already endpoints registered to FCM, both FCM should show the same extensions and registration status. This indicates that the active FCM's data has been synchronized to the standby FCM.



# ACTIVE/STANDBY ROLE IN HA

## Automatic Failure Detection

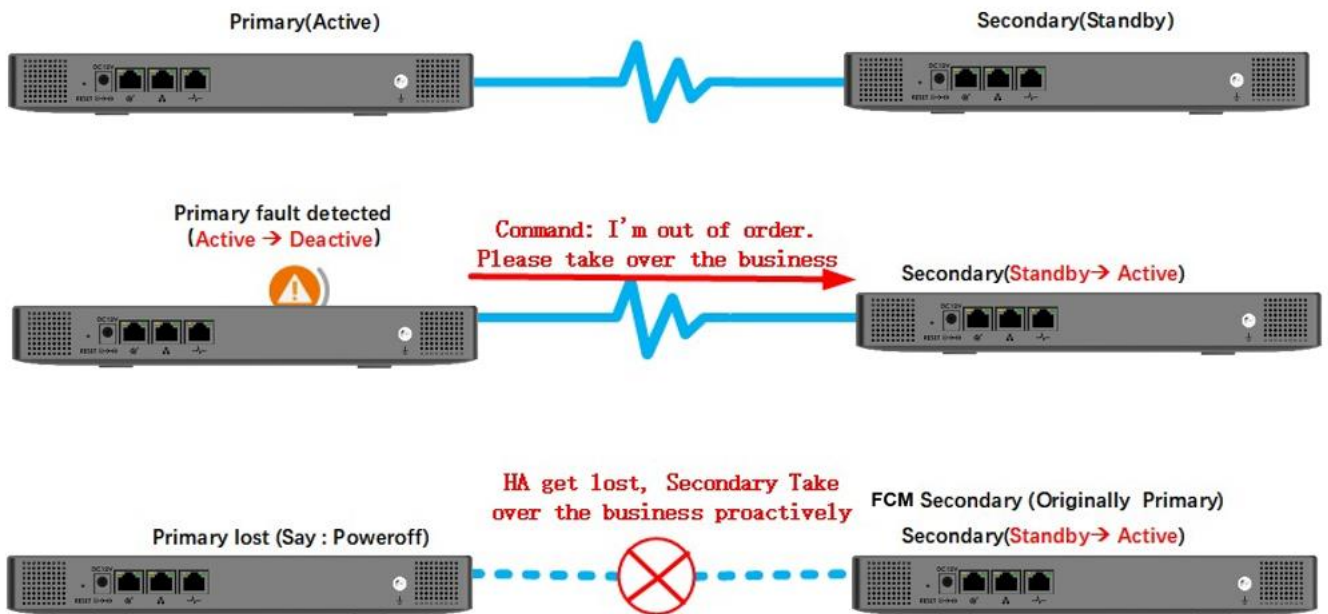


Figure 9: Active and Standby FCM Failover

## Active FCM: Self-Failure Detection

The active FCM monitors and regularly checks whether there is any failure on itself. When there is failure detected on itself, it will notify the standby FCM to take over as active server. Then the original active FCM will reboot automatically and become the standby server. This scenario applies to active FCM which has part of the function or specific service in faulty status, and it can still work partially without shutting down the service completely.

For example, if the active server has a core dump generated for a core service, WAN/LAN port disconnection, with this detection and notification mechanism, the standby FCM can take over immediately without noticeable delay or service interruption.



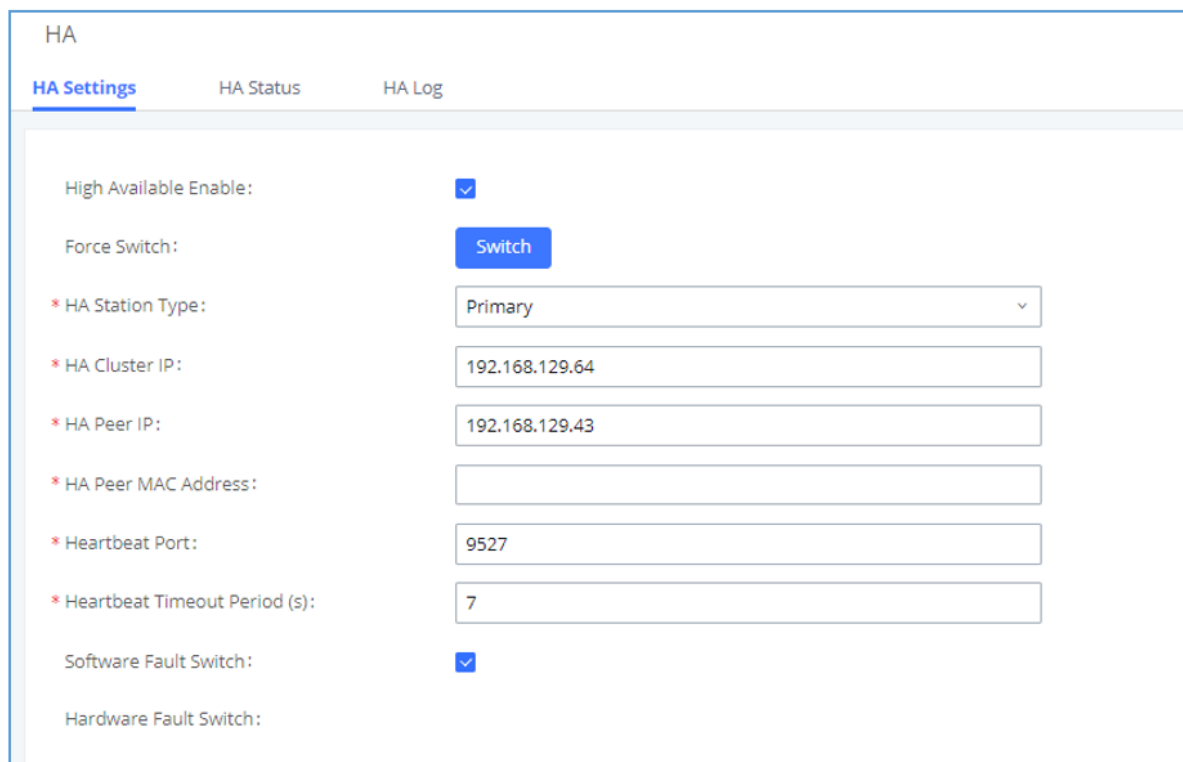
## Standby FCM: Periodic Heartbeat

On HA mode, the standby FCM will check the active FCM's status periodically by sending heartbeat message to the active FCM. The heartbeat message is sent via the heartbeat port. If the active FCM is under normal working condition, it will respond to the standby FCM after it receives heartbeat request from the standby FCM. If the active FCM runs into faulty situation such as network chip becomes abnormal or power adapter no longer works, it will stop responding heartbeat request. After the heartbeat period times out, the standby FCM will consider the active FCM as faulty and start taking over as the active server.

The heartbeat timeout period determines how soon the standby FCM can detect active server's failure and switch over. By default, the heartbeat timeout period is 7 seconds. Users could modify the heartbeat timeout period as preferred, and this will affect the detection/switchover sensitivity.

## Force Switch

For the current active FCM, system admin can click on Force Switch "Switch" button on its web UI HA settings page to force triggering the active/standby role change manually. This operation should be only used during firmware upgrade or the active FCM encounters issue that requires force switchover to be triggered manually.



HA	
<u>HA Settings</u> HA Status    HA Log	
High Available Enable:	<input checked="" type="checkbox"/>
Force Switch:	<button>Switch</button>
* HA Station Type:	Primary
* HA Cluster IP:	192.168.129.64
* HA Peer IP:	192.168.129.43
* HA Peer MAC Address:	
* Heartbeat Port:	9527
* Heartbeat Timeout Period (s):	7
Software Fault Switch:	<input checked="" type="checkbox"/>
Hardware Fault Switch:	<input type="checkbox"/>

Figure 10: Force Switch





## FIRMWARE UPGRADE

To ensure that there is no service interruption in HA setup, upgrading FCM requires user to follow below steps strictly:

Step 1: Log in the web UI of the standby FCM (A), upload firmware via web UI and the standby FCM will reboot. Wait for it to boot up.

Step 2: After the standby FCM (A) boots up, log in the web UI of the active FCM (B) and check the HA web page. "Force Switch" button on the FCM B's HA web page will be available. Press it to manually trigger switchover. After switchover, FCM A will become active and FCM B becomes standby.

Step 3: After switchover, log in FCM B and upload firmware to its web UI. FCM B will reboot and request data from FCM A for full backup.

In short, when upgrading FCM in HA setup, the standby FCM needs to be upgraded first and becomes active FCM. Then we can upgrade the standby FCM. This will ensure the active FCM is always working and providing PBX functions, so there is no service interruption during upgrading or switchover.



## REPLACING FCM IN HA

Assuming 2 FCM (A and B) in HA setup, FCM A is in active status and FCM B is in standby status. FCM B becomes defective and requires replacement. Please follow the steps below to replace the defective FCM B with FCM C:

1. Turn off the power for FCM B.
2. Modify FCM A's HA settings by changing HA Peer MAC address from FCM B to FCM C's MAC address. Save and reboot FCM A.
3. After FCM A boots up, log in FCM A web UI and confirm the HA status to be Active. Connect FCM C to the HA setup using appropriate cables for WAN port, heartbeat port, and etc.
4. After FCM C boots up, log in FCM C web UI and configure network settings to be the same as FCM B. After configuration, FCM C has the same static IP as FCM B.
5. Log in FCM C's web UI, enable HA, configure HA station type and other HA settings to be the same as FCM B. Save and reboot FCM C.
6. After FCM C boots up, check and verify the HA status. FCM A should be active and FCM C should be standby.

**Note:** HA configuration requires the FCM to reboot. Please reboot the FCM during non-service hour to avoid service interruption.

## DISABLING HA SETUP

If HA setup is no longer required for the FCM, log in the web UI using the active FCM's IP or the cluster's IP and go to system settings → HA page to disable HA. Save and reboot the FCM. After both FCM boot up, check the HA status and it should show HA as off.



# SERVICE STATUS

## Active/Standby Status

After HA setup is completed, the PBX will provide service using the HA cluster IP. During initial stage, standby FCM will request and synchronize up all data from the active FCM.

The standby FCM monitors and prepares to become active at any time when needed. Manual configuration on standby FCM is restricted because it always synchronizes up data from active FCM. When the active FCM has any hardware or critical software failure, the standby FCM will immediately take over and becomes the active FCM. The previous active FCM will reboot and become the standby FCM. Calls during the role switchover will be recovered after failover process completes.

## Web UI Access for FCM

After HA setup is completed, the system admin can use the cluster IP address to log in the current active FCM for configurations. The cluster IP address is always bind to the active FCM. For example, assuming HTTP/HTTPS port is 8089, system admin can access FCM using URL [https://cluster\\_IP:8089](https://cluster_IP:8089).

If the system admin logs in the standby FCM's web UI by using the standby FCM IP and attempts to modify configurations, it will not be allowed. The system will prompt that configuration is restricted on the standby FCM.

**Note:** HA setup will synchronize up admin login information from the active FCM to the standby FCM. Therefore, when system admin logs in the FCM web UI using the active FCM IP, standby FCM IP or the cluster IP, the active FCM's login information always needs to be used.



## FAILOVER DURING CALL

When the active server encounters failure, if there is ongoing call on the active server, the switchover process will only cause a few seconds of audio cutoff and then it will be recovered automatically.

### *Notes:*

- Currently, if the call is using UDP as transport method, the call can be recovered after switchover. However, if the call is using TCP as transport method, the call cannot be recovered after switchover.
- Point-to-point calls such as audio call or audio meeting can be recovered after switchover. However, for calls using ring group, call queue and other call features and services, the call will not be automatically recovered.

## DATA SYNC

HA setup provides data sync mechanism:

1. After FCM boots up, the standby FCM will send requests for all the data on active FCM and perform data sync. Every time when the active FCM has configuration change, it will also synchronize up the data to the standby FCM automatically and immediately.
2. Data sync is triggered in real-time manner. It not only synchronizes up configuration data, but also extensions, voicemail, CDR, etc.
3. Every day at midnight, a full backup will be performed to ensure active and standby FCM always have the same data on daily basis.

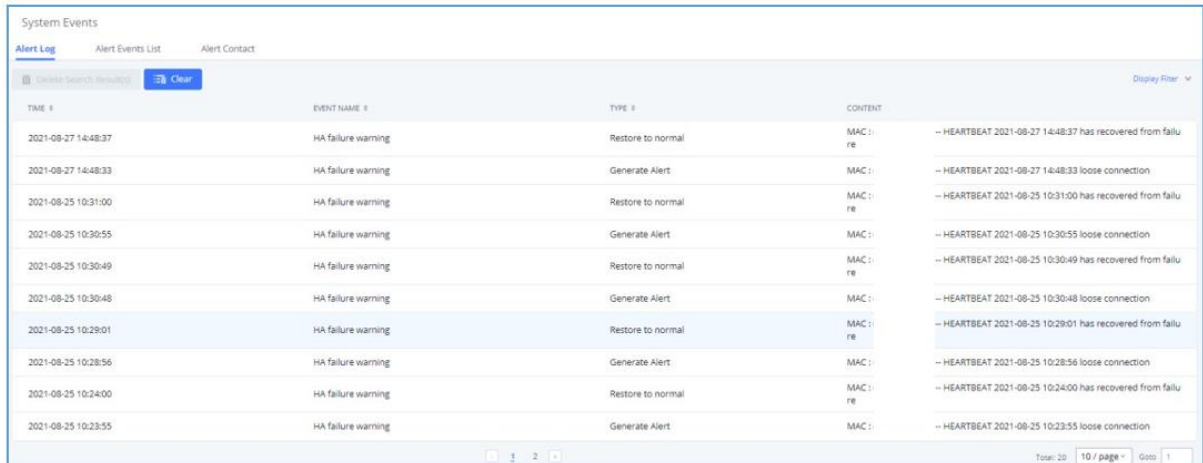
## BACKUP AND RESTORE

For backup restore, the admin needs to log in the active FCM and restore the FCM first. FCM devices will reboot automatically. Once the FCM finishes booting up, the standby FCM will start synchronizing up data from the active FCM to restore the backup as well.



# MAINTENANCE

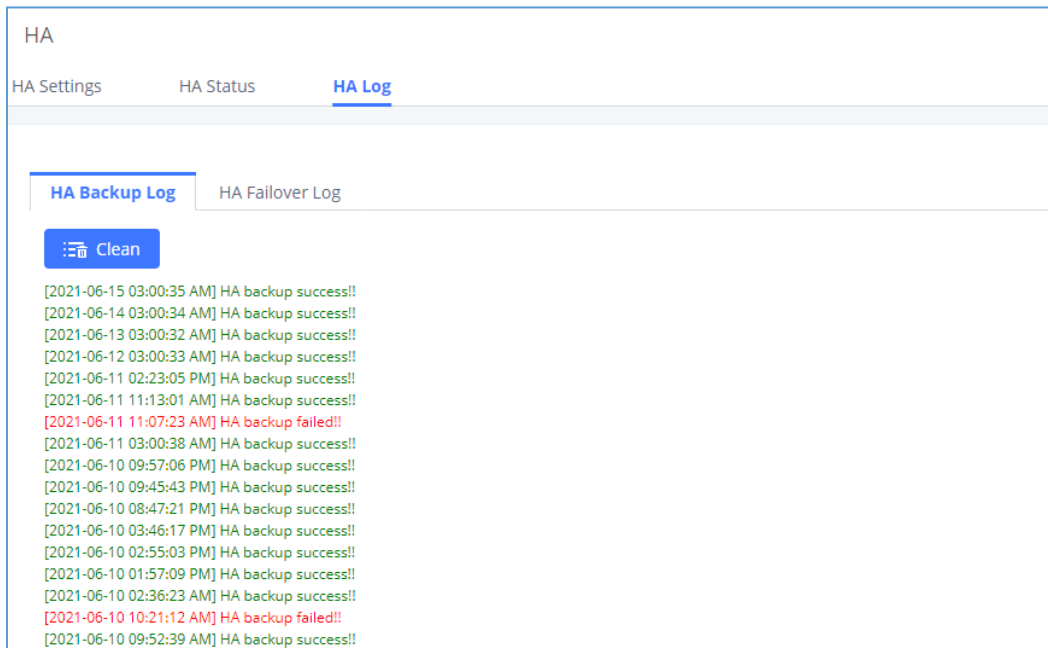
In HA setup, system admin can check HA related alerts under FCM web UI's system events page to learn if there is any abnormal event related to HA. According to the alerts, admin can further diagnose by checking the event time and logs with more details.



TIME	EVENT NAME	TYPE	CONTENT
2021-08-27 14:48:37	HA failure warning	Restore to normal	MAC: re -- HEARTBEAT 2021-08-27 14:48:37 has recovered from failu
2021-08-27 14:48:33	HA failure warning	Generate Alert	MAC: re -- HEARTBEAT 2021-08-27 14:48:33 loose connection
2021-08-25 10:31:00	HA failure warning	Restore to normal	MAC: re -- HEARTBEAT 2021-08-25 10:31:00 has recovered from failu
2021-08-25 10:30:55	HA failure warning	Generate Alert	MAC: re -- HEARTBEAT 2021-08-25 10:30:55 loose connection
2021-08-25 10:30:49	HA failure warning	Restore to normal	MAC: re -- HEARTBEAT 2021-08-25 10:30:49 has recovered from failu
2021-08-25 10:30:48	HA failure warning	Generate Alert	MAC: re -- HEARTBEAT 2021-08-25 10:30:48 loose connection
2021-08-25 10:29:01	HA failure warning	Restore to normal	MAC: re -- HEARTBEAT 2021-08-25 10:29:01 has recovered from failu
2021-08-25 10:28:56	HA failure warning	Generate Alert	MAC: re -- HEARTBEAT 2021-08-25 10:28:56 loose connection
2021-08-25 10:24:00	HA failure warning	Restore to normal	MAC: re -- HEARTBEAT 2021-08-25 10:24:00 has recovered from failu
2021-08-25 10:23:55	HA failure warning	Generate Alert	MAC: re -- HEARTBEAT 2021-08-25 10:23:55 loose connection

Figure 11: System Alert Events

HA log also shows all HA backup and failover logs.



HA Backup Log	HA Failover Log	
<p>[2021-06-15 03:00:35 AM] HA backup success!! [2021-06-14 03:00:34 AM] HA backup success!! [2021-06-13 03:00:32 AM] HA backup success!! [2021-06-12 03:00:33 AM] HA backup success!! [2021-06-11 02:23:05 PM] HA backup success!! [2021-06-11 11:13:01 AM] HA backup success!! <b>[2021-06-11 11:07:23 AM] HA backup failed!!</b> [2021-06-11 03:00:38 AM] HA backup success!! [2021-06-10 09:57:06 PM] HA backup success!! [2021-06-10 09:45:43 PM] HA backup success!! [2021-06-10 08:47:21 PM] HA backup success!! [2021-06-10 03:46:17 PM] HA backup success!! [2021-06-10 02:55:03 PM] HA backup success!! [2021-06-10 01:57:09 PM] HA backup success!! [2021-06-10 02:36:23 AM] HA backup success!! <b>[2021-06-10 10:21:12 AM] HA backup failed!!</b> [2021-06-10 09:52:39 AM] HA backup success!!</p>		

Figure 12: HA Logs

