Grandstream Networks, Inc.

SoftwareUCM –
High Availability User Guide: Local HA

SoftwareUCM – High Availability User Guide: Local HA

The High Availability feature on the Grandstream SoftwareUCM provides enterprises with a reliable solution for PBX redundancy and failover support. In HA setup, there are two SoftwareUCM instances with one instance in the "active" role and the other in the "standby" role. The two instances must use the same firmware version. The data on the active SoftwareUCM instance will be synchronized to the standby SoftwareUCM instance in a real-time manner, and the standby SoftwareUCM instance monitors the active SoftwareUCM's running status regularly. When the active instance runs into hardware or critical software issues, such as a power outage or network disconnection, the standby instance of the SoftwareUCM 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.

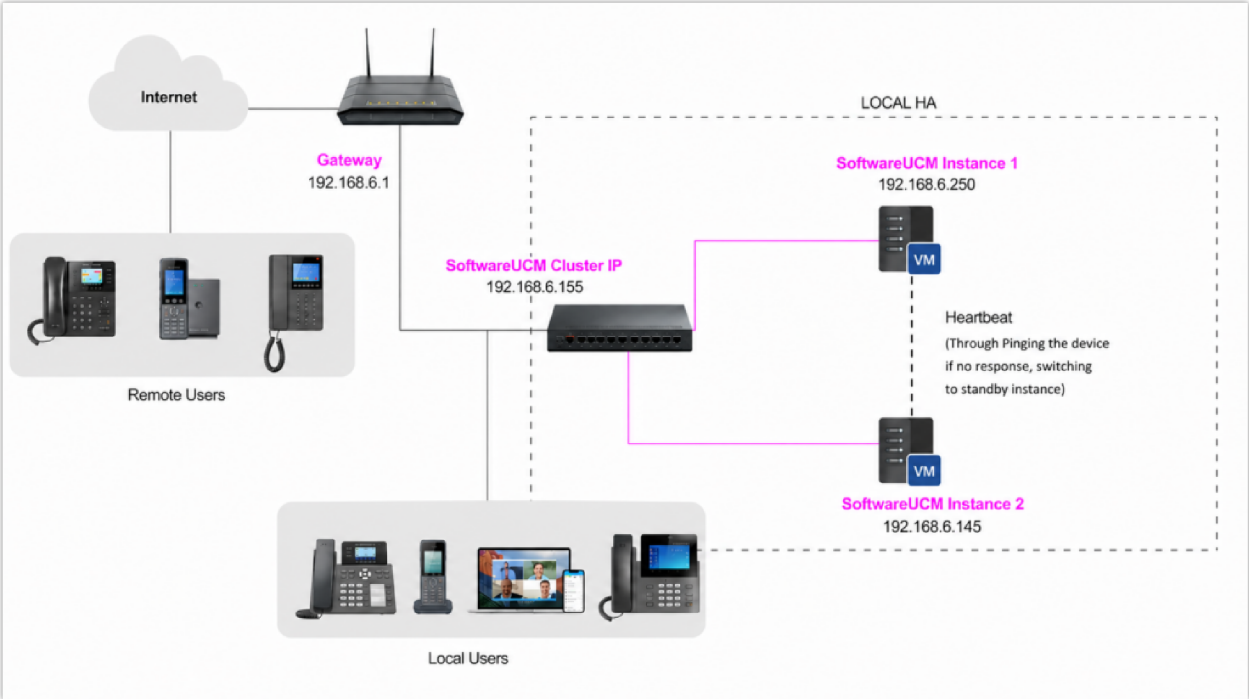
This guide outlines the key points and precautions of the HA function for SoftwareUCM. It provides detailed step-by-step procedures for the equipment failure replacement process when operating in a High Availability (HA) environment.

NETWORK TOPOLOGY

Single LAN Deployment

Below is a configuration scenario where we set two softwareUCM instances in HA mode, with a cluster IP that can be used by the administrators for extensions registrations and further VoiP configurations.

Here is how the network configuration maps to the two SoftwareUCM instances (using the scenario where the Primary instance is Active and the Secondary instance is Standby):



NETWORK TOPOLOGY

Initial Network State:

- **SoftwareUCM instance 1 (Primary Site / Active):** 192.168.6.250
- **SoftwareUCM instance 2 (Secondary Site / Standby):** 192.168.6.145
- **HA Cluster (Virtual IP):** 192.168.6.155

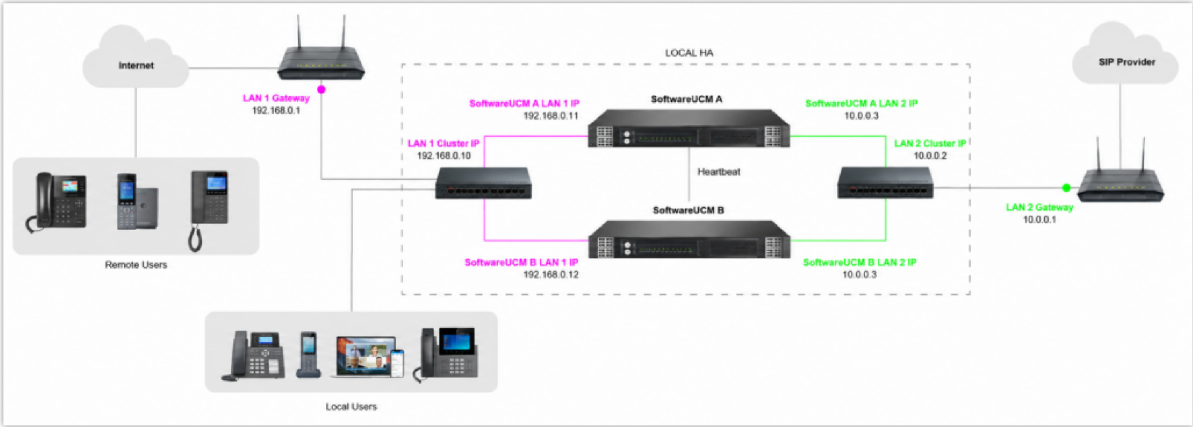
The two instances in the High Availability setup must be deployed in the same LAN. For each instance, connect its RJ45 port to the uplink network device to connect it to the LAN.

Please refer to this section of the guide to carry on the configuration: [**HA Configurations**]

Dual LAN Deployment

Below is a configuration scenario where two SoftwareUCM instances are deployed in High Availability (HA) Dual LAN mode. In this setup, both LAN interfaces participate in the HA configuration, with dedicated Cluster IPs assigned for LAN 1 and LAN 2. These Cluster IPs can be used by administrators for extension registrations, SIP trunk connectivity, and further VoIP service configurations.

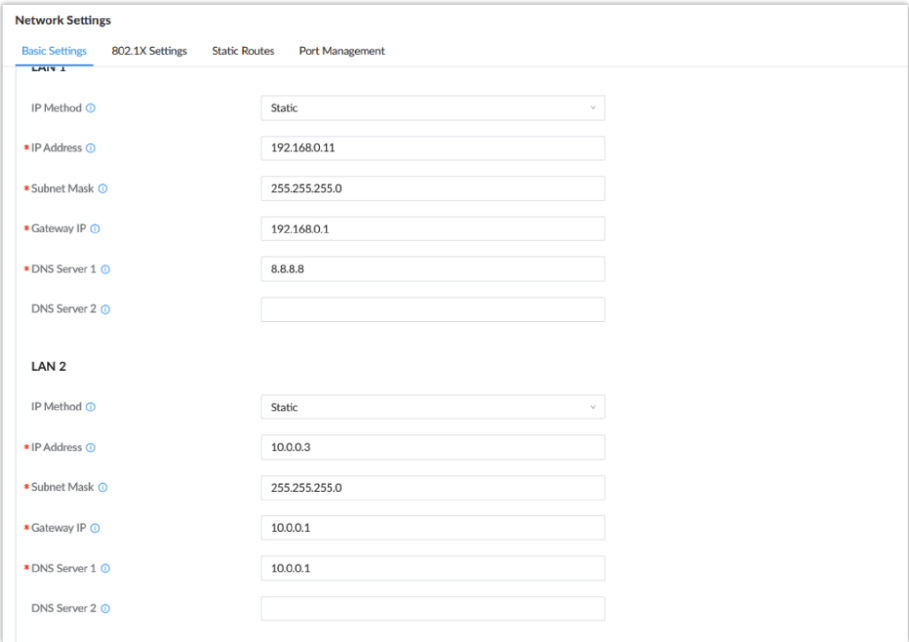
The following section explains how the network configuration maps to the two SoftwareUCM instances when the Primary instance is operating in Active mode and the Secondary instance is operating in Standby mode.



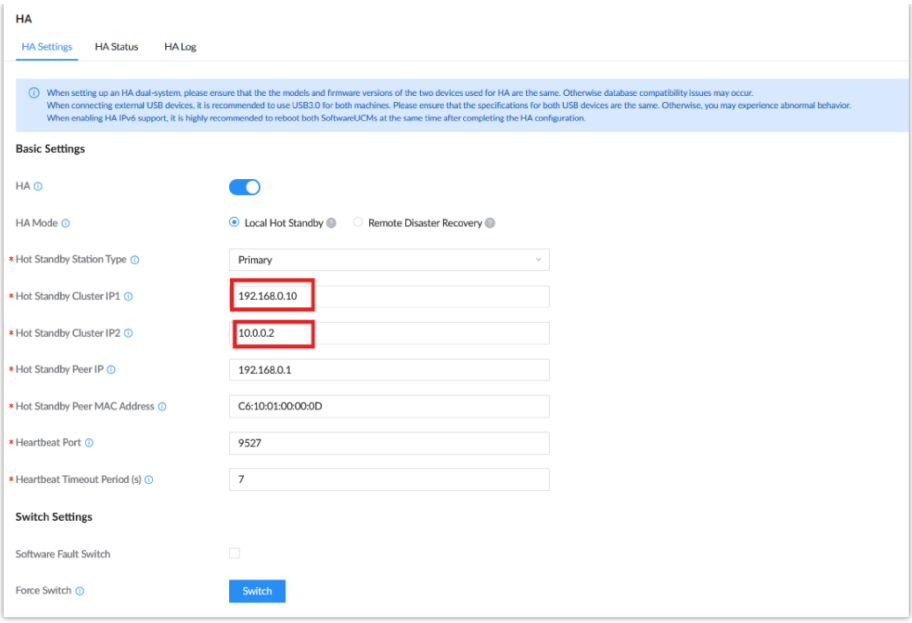
Initial Network State Example:

LAN 1 Network

- **SoftwareUCM A LAN 1 IP (Primary Site / Active):** 192.168.0.11
- **SoftwareUCM B LAN 1 IP (Secondary Site / Standby):** 192.168.0.12
- **LAN 1 Cluster IP (Virtual IP):** 192.168.0.10
- **LAN 1 Gateway:** 192.168.0.1



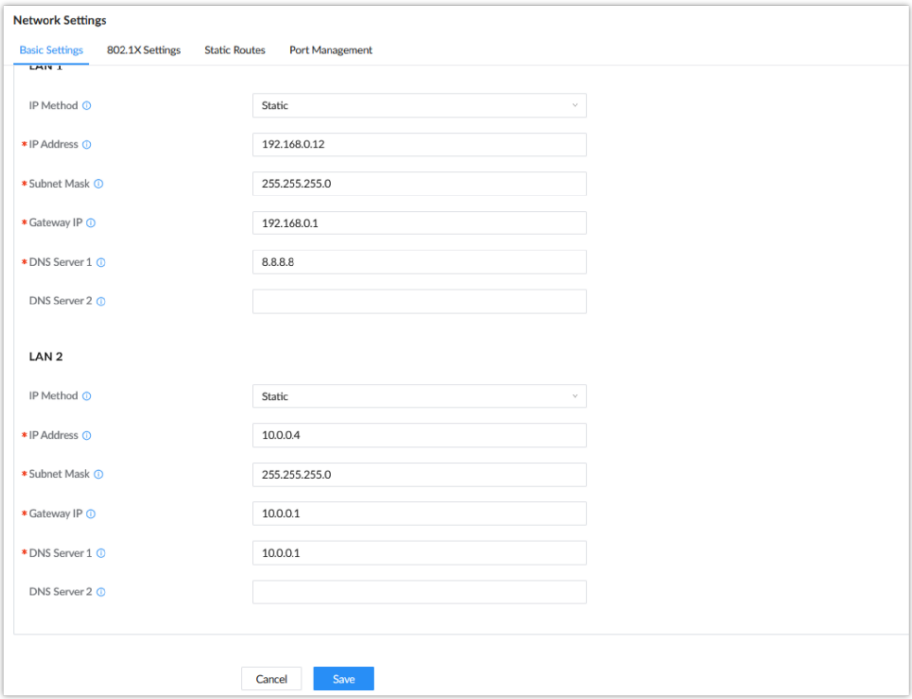
Network Settings



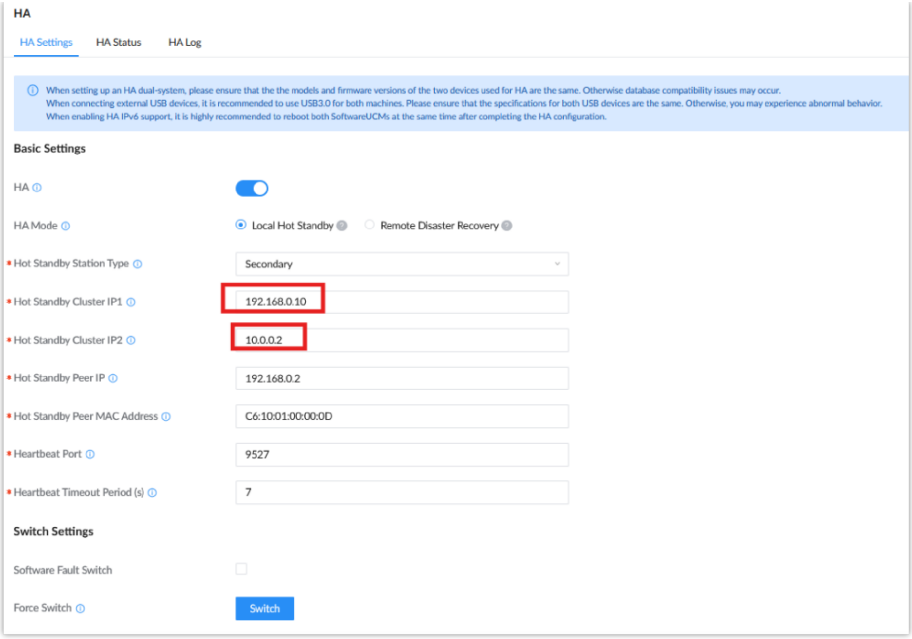
Local Hot Standby Primary

LAN 2 Network

- **SoftwareUCM A LAN 2 IP (Primary Site / Active):** 10.0.0.3
- **SoftwareUCM B LAN 2 IP (Secondary Site / Standby):** 10.0.0.4
- **LAN 2 Cluster IP (Virtual IP):** 10.0.0.2
- **LAN 2 Gateway:** 10.0.0.1



Network Settings



Local Hot Standby Secondary

In the Dual LAN High Availability deployment, both SoftwareUCM instances must be deployed within the same LAN environment for each corresponding interface. LAN 1 interfaces from both instances should be connected to the same LAN 1 network segment, while LAN 2 interfaces should be connected to the same LAN 2 network segment.

For proper HA communication and failover synchronization, both SoftwareUCM instances must maintain network connectivity through both LAN interfaces. The heartbeat communication between the two instances is used to monitor the operational status of each node and ensure seamless failover in the event of a system or network failure.

> **Notes**
>
> Throughout the remainder of this guide, the configuration examples and procedures will focus on the Single LAN deployment mode for simplicity and clarity. The Dual LAN deployment mode follows the same overall High Availability logic and configuration workflow.
>
> However, instead of configuring a single network interface, administrators must configure:
>
> - Two separate LAN interfaces (LAN 1 and LAN 2) on each SoftwareUCM
> - Two static IP addresses per SoftwareUCM instance
> - Two Cluster IPs (one Virtual IP for each LAN)
> - Two separate gateway/network paths if required by the deployment
>
> In a Dual LAN deployment, it is mandatory that both servers participating in the Local HA setup support Dual NIC functionality.
>
> For bare-metal deployments, this means that each server must have two physical network interfaces/cards installed.
>
> For virtualized deployments (VMware, Hyper-V, VirtualBox, KVM, etc.), each SoftwareUCM virtual machine must be configured with two separate virtual network adapters/interfaces attached to the appropriate LAN segments.
>
> This ensures that both LAN 1 and LAN 2 can operate independently, providing redundant communication paths and improved network resiliency for the HA environment.

Key Precautions and Prerequisites

Prerequisites

The two SoftwareUCM instances 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.

> **Note**

The minimum firmware version required to be installed on the SoftwareUCM for HA support is 1.0.33.7+

Connecting SoftwareUCM for HA Setup

The two SoftwareUCM instances in the High Availability setup must be deployed in the same LAN.

- For each SoftwareUCM instance, connect the LAN port of the computer on which the instance is hosted to the uplink network device (such as a switch or router).

Network Configuration

Before enabling the High Availability feature, each SoftwareUCM must be configured with the appropriate network settings.

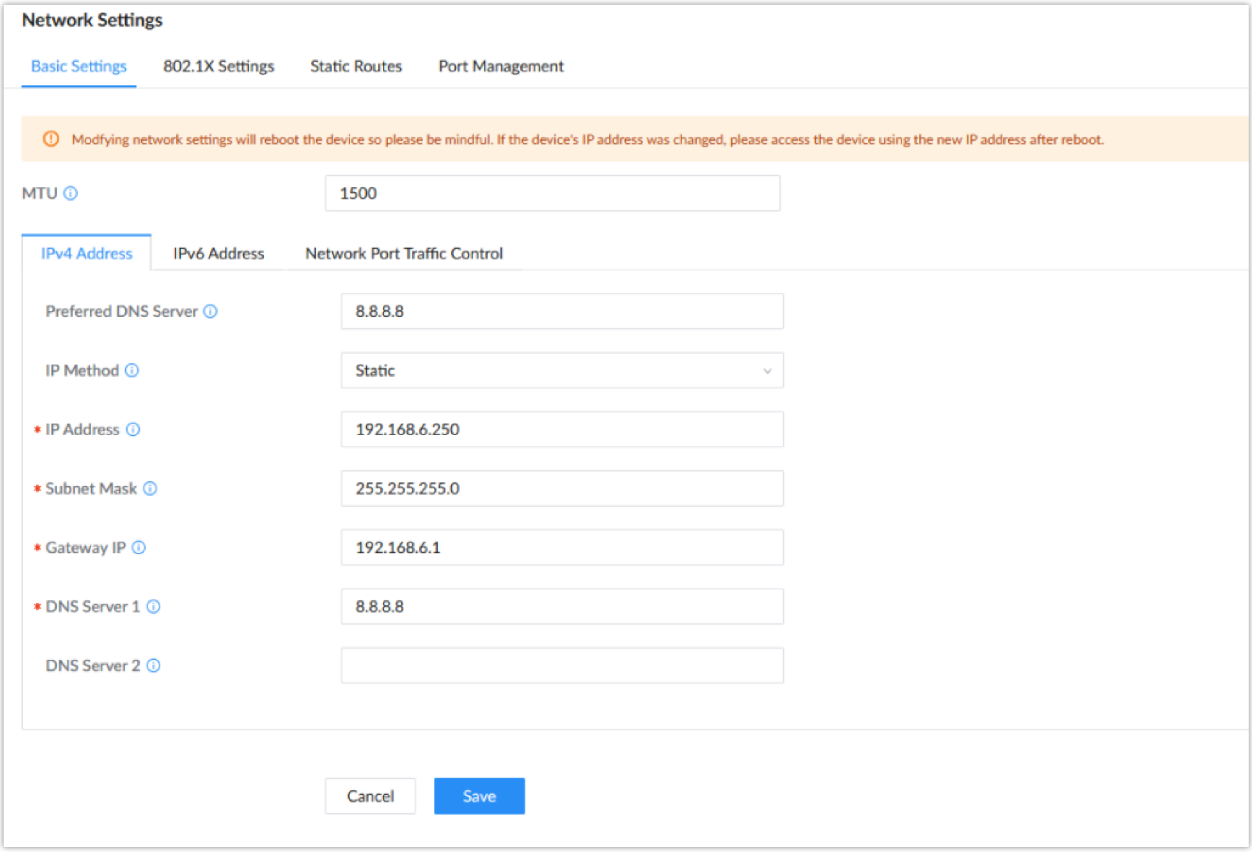
- The network setup methods available on the SoftwareUCM are **Single Network Interface Card** and **Dual Network Interface Card**, depending on the deployment scenario. This includes configurations such as local HA deployment, remote disaster recovery deployment, and other networking setups. In this test, we will proceed with the **Single Network Interface Card** method.

  Note

  If only one network interface card is detected by the SoftwareUCM, the option to choose between single or dual network modes will not be displayed. In this case, the system will automatically use the **Single Network Interface Card** mode by default. The selection option will only appear when the SoftwareUCM detects two valid network interface cards.

- All LAN interfaces used by HA must be assigned static IPv4 addresses. These addresses can be configured from **SoftwareUCM Web UI→Network Settings→Basic Settings**.

Static addressing is required so that the HA cluster IP addresses can be bound consistently to the active node during operation.



SoftwareUCM Network Settings

Storage Device

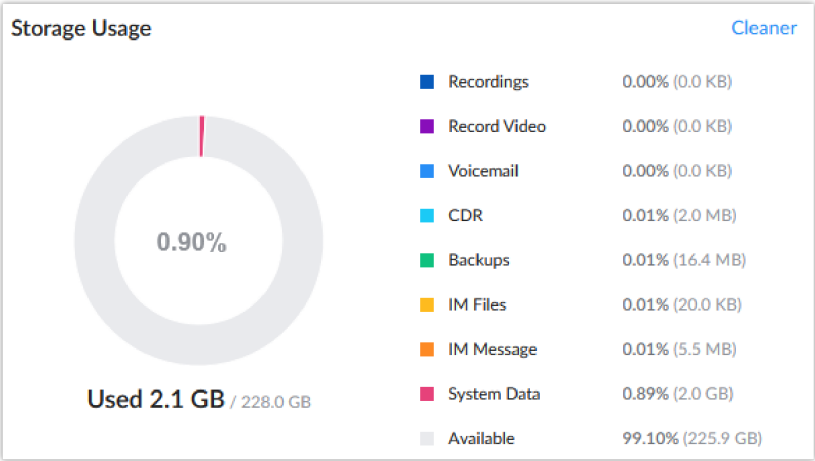
Before enabling the High Availability feature on the two SoftwareUCM instances, the system administrator must ensure that both systems are deployed with sufficient and comparable storage capacity. SoftwareUCM supports both local storage and external storage devices, such as USB storage devices. SD cards may also be used when connected through a supported USB adapter on the host machine. All data is stored on the storage resources available to the host system, whether the deployment is on a virtual machine or a bare metal system.

For example, if SoftwareUCM A is deployed on a system with 500 GB of available storage space, SoftwareUCM B should also be provisioned with a similar amount of storage capacity. This ensures that the standby instance can handle the same data load and avoids potential issues during synchronization or failover.

> **Note**
>
> On some computers, only specific USB ports may properly detect the inserted USB drive. Please verify and test the available USB ports on your desktop device.

If cloud-based services such as GDMS storage are used, both SoftwareUCM instances must support and have access to the same cloud services. However, it is not necessary to manually configure identical storage paths before enabling High Availability, as the active SoftwareUCM configuration will be automatically synchronized to the standby instance once HA is enabled.

The SoftwareUCM storage configuration and status can be found under SoftwareUCM webUI → Storage Status → Dashboard:



Storage Status Under Dashboard

HA Configurations

For SoftwareUCM without SoftwareUCM RemoteConnect Plan

HA Configuration

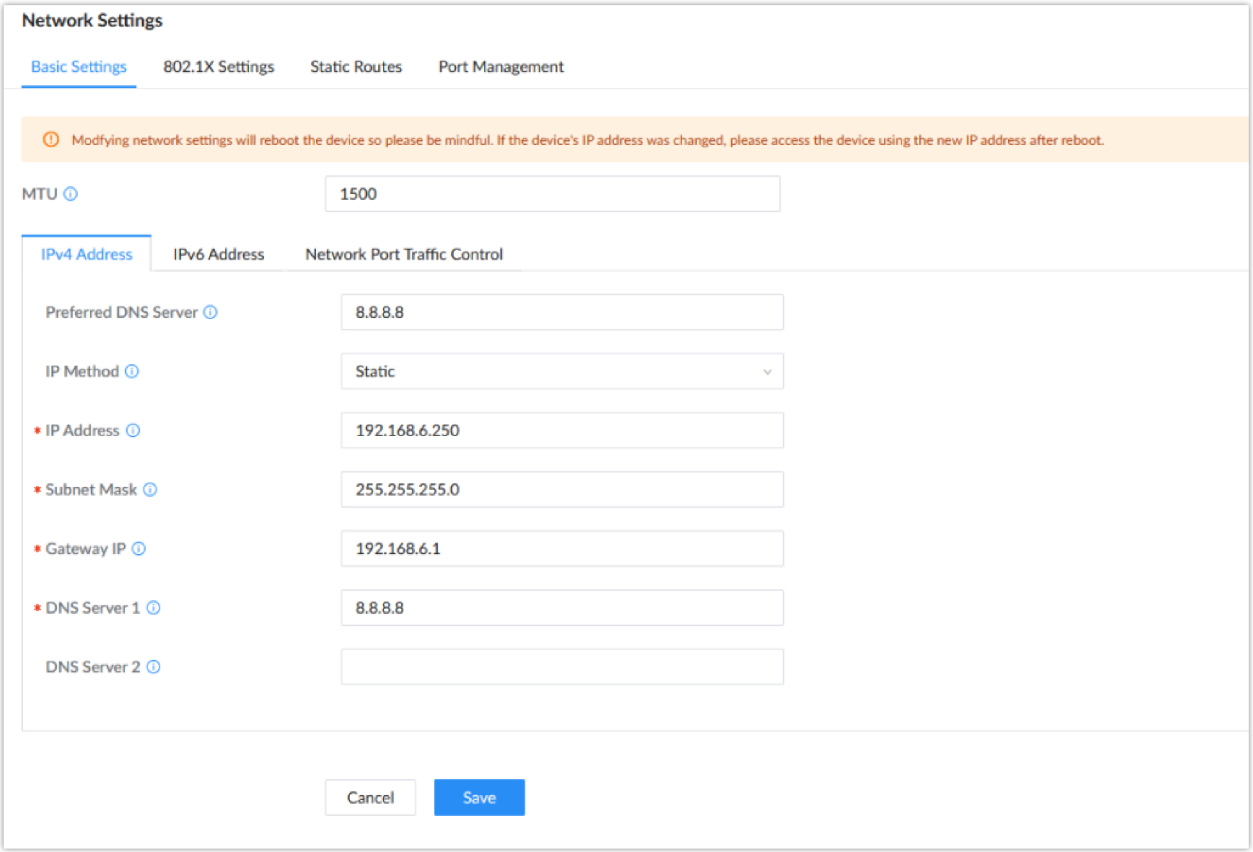
For two new SoftwareUCM instances on the factory default setting, the system admin can choose to configure any of them for HA first. However, if one of the SoftwareUCM instances is already configured, up and running for PBX service, the system admin should configure this SoftwareUCM as an HA Primary server and complete all HA settings on it first so it can act as an active role. Assuming no UCMRC (RemoteConnect) service is used on any SoftwareUCM, please refer to the steps below to configure HA on SoftwareUCM:

1. Ensure both SoftwareUCM instances have the same model and the same firmware version. They have been connected properly at the same location and configured with a static IP. The SoftwareUCM admin also needs to ensure that the same type and amount of storage is connected to each SoftwareUCM.
2. Select one SoftwareUCM to be the active device (SoftwareUCM A). If both SoftwareUCM instances are new on factory default settings, select any of them as the active SoftwareUCM. If one of the SoftwareUCM instances is already configured and running, then select this SoftwareUCM as the active device.

3. If Cloud IM service is needed, please enable Cloud IM on SoftwareUCM A (active SoftwareUCM) and ensure Cloud IM is disabled on the other SoftwareUCM (SoftwareUCM B).

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

The IPv4 address configured on the SoftwareUCM must be a static IP. It can be configured under **Network Settings > Basic Settings**.



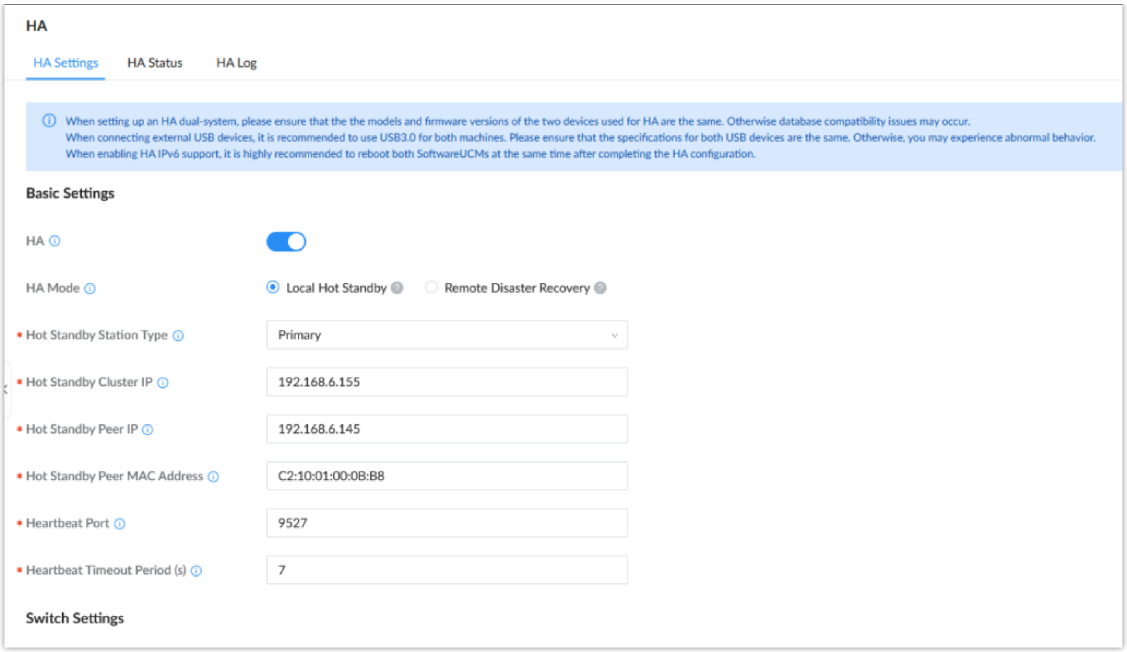
SoftwareUCM Network Settings Single LAN

- Log in to the active SoftwareUCM (SoftwareUCM A) web UI and go to the System Settings→HA page. Enable HA and configure SoftwareUCM A as the primary station type.

  Note:

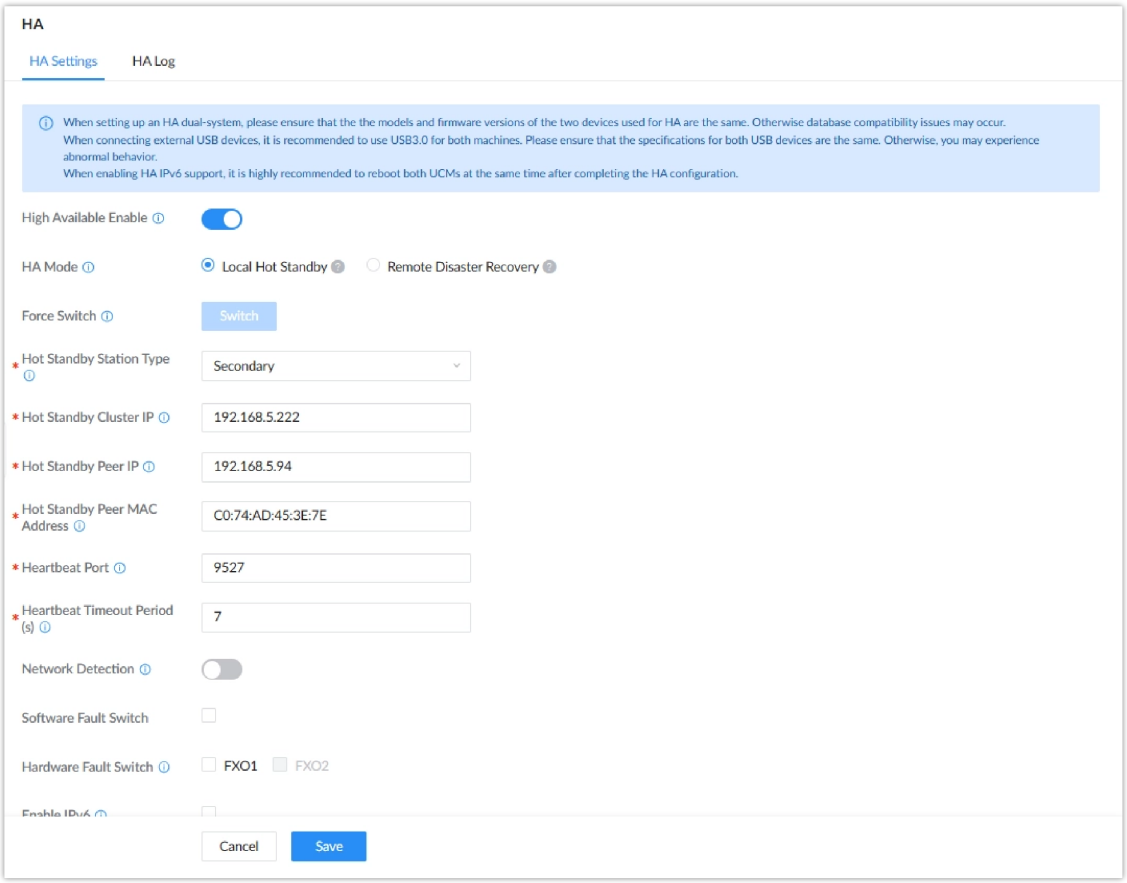
  Please refer to HA-related parameters in the [HA CONFIGURATION PARAMETERS] section below to complete other HA-related settings.

- Save the HA settings on SoftwareUCM A and reboot SoftwareUCM A. Ensure SoftwareUCM A boots up normally.



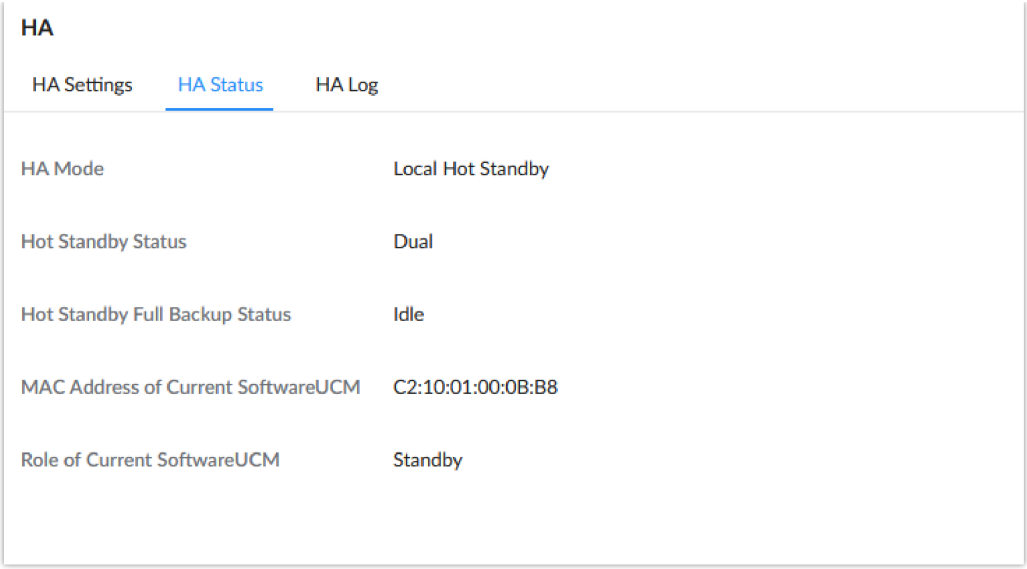
HA Settings on Primary UCM

5. After SoftwareUCM A restarts with HA parameters configured, verify the HA dual-node status. Log in to SoftwareUCM A's web UI using its static IP and administrator credentials. Navigate to **System Settings** → **HA**, confirm that the HA function is enabled, then click **HA Status**. SoftwareUCM A should display as "Active" and operate as a single node.
6. Once SoftwareUCM A is confirmed active, configure SoftwareUCM B as the secondary node. Log in to SoftwareUCM B's web UI, go to **System Settings** → **HA** → **HA Settings**, enable the HA function, and set the station type to "Secondary". Complete the other HA-related parameter configurations as per the HA parameter descriptions below. Save the settings and restart SoftwareUCM B.



HA Settings on Secondary UCM

7. After SoftwareUCM B restarts with HA parameters configured, log in to SoftwareUCM B's web UI using **its static IP address and SoftwareUCM A's administrator credentials**. Navigate to **System Settings** → **HA** and confirm that the HA function is enabled, the "Switch" toggle button is grayed out, and only the HA Peer IP Address option is available for configuration. Click **HA Status** to verify that SoftwareUCM B's role is displayed as "Standby".



HA Status on Secondary UCM

HA Configuration Parameters

Settings	Description	Value Range	Default Value	Notes
HA	Enable or disable HA.	Toggle On/Off	No	–
HA Mode	Configure HA mode. "Local Hot Standby": Deploy HA in the same location which provides redundancy and recovery in case the primary SoftwareUCM has hardware issues. "Remote Disaster Recovery": Deploy two SoftwareUCM instances in different locations to prevent service interruption in case of large-scale disaster at the primary SoftwareUCM site.	Local Hot Standby Or Remote Disaster Recovery	Local Hot Standby	For "Local Hot Standby", SoftwareUCM must use network mode "Switch" or "Router" and use static IP address. For "Remote Disaster Recovery", SoftwareUCM must be configured with static IP. Grandstream end devices are fully supported with SoftwareUCM HA remote disaster recovery feature for failover.
Hot Standby Station Type	Configure the HA station type for the SoftwareUCM.	Primary Secondary	NA	In HA setup, one SoftwareUCM must be primary and the other one must be secondary.
Hot Standby Cluster IP 1	This is the IP address for the active SoftwareUCM in service. for LAN1	NA	NA	This IP address is shared by the primary and secondary SoftwareUCM. The SoftwareUCM in active status providing PBX service will always be using this IP address regardless it's the primary or secondary SoftwareUCM. This IP address can only be used for the active SoftwareUCM.
Hot Standby Cluster IP 2	This is the IP address for the active SoftwareUCM in service. for LAN2	NA	NA	To use this service, the active and standby SoftwareUCM systems must use the same static IP address

				corresponding to network segment of LAN2.
Hot Standby Peer IP	This is the IP address of the peer SoftwareUCM in HA setup.	NA	NA	This is the static IP address of the peer SoftwareUCM in HA setup connected via heartbeat port.
Hot Standby Peer MAC Address	This is the MAC address of the peer SoftwareUCM in HA setup.	NA	NA	This is the MAC address of the peer SoftwareUCM in HA setup connected via heartbeat port.
Heartbeat Port	This is the port used for communication between the two SoftwareUCM via the heartbeat port.	0 – 65535	9527	It is recommended to use default port.
Heartbeat Timeout Period (s)	This is the heartbeat timeout period that active and standby SoftwareUCM will check with each other for the status (in seconds).	3 – 10	7	If the standby SoftwareUCM detects the active SoftwareUCM disconnected when it reaches the timeout, failover will be triggered and the standby SoftwareUCM will start taking over as active SoftwareUCM .
Software Fault Switch	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 SoftwareUCM to standby SoftwareUCM. Otherwise, failover will not happen.
Force Switch	Force to switch the roles of active SoftwareUCM and standby SoftwareUCM.	NA	NA	**Caution: Please do not use this function unless necessary (e.g., it can be used during firmware upgrading).**
Network Detection	Monitor the network connection status of the devices. If an Active device detects a network disconnection from the network detection node, it will notify the Standby device to take over operations, ensuring reliable business continuity. HA settings on both ends must match. If mismatched, the Active device's settings will take priority.	Toggle On/Off	Off	–
Network Detection Node 1/2	It is recommended to use a reliable address, such as a gateway address, as the detection node, this configuration should correspond to the IP address of the device's network interface. ● The standby device does not initiate switchover on	IPv4 IP Address	N/A	When configuring the Dual Network Interface Card mode for two separate LANs in a Local HA deployment, you will have the option to configure two network detection nodes, with one node assigned to each LAN.

	its own. ● Only IP addresses are supported. ● For correct operation, this setting must be configured identically on both devices.			
Enable IPv6	If enabled, HA will support IPv6 while compatible with IPv4.	On/Off	Off	Please enable this option if IPv6 is required for HA deployment. Otherwise, please keep it off. Before enabling this option, please configure both UCMs with static IPv6 address.
Sync External Storage Files	Syncs externally stored files (USB, NAS, etc.) on the Active SoftwareUCM to the Standby SoftwareUCM's external storage. External storage must be of the same type and capacity. It is recommended to manually sync existing external storage files after setting up HA for the first time. Files created after HA has been set up will be automatically synced.	N/A	N/A	–

HA Related Parameters

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

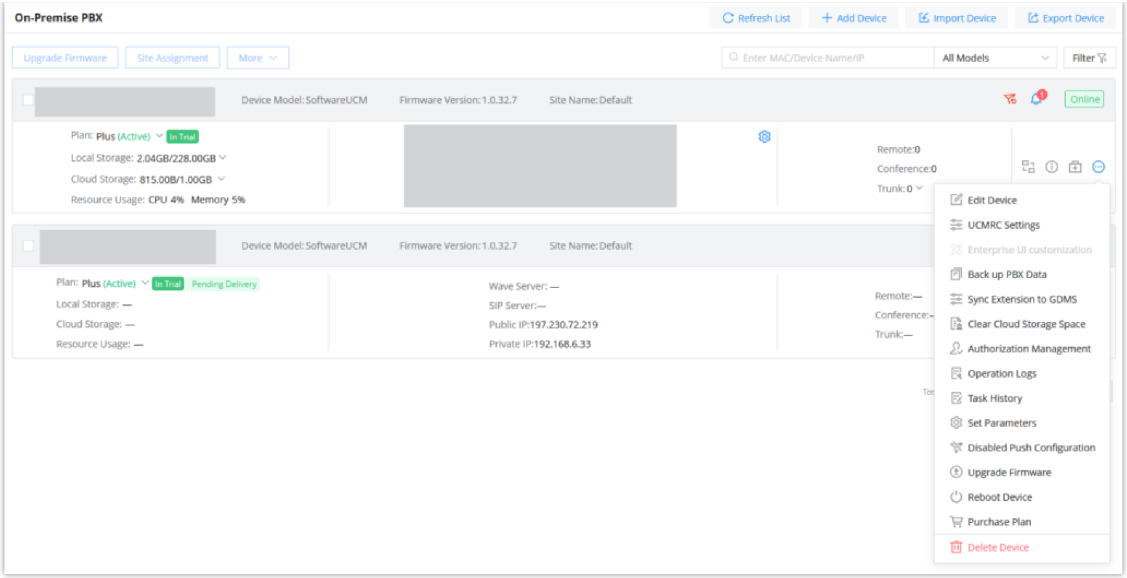
> **Critical Note**
>
> HA configuration requires the SoftwareUCM to reboot. Please reboot the SoftwareUCM instance during non-service hours to avoid service interruption.

SoftwareUCM RemoteConnect Configurations

UCM RemoteConnect Plan

To ensure that the SoftwareUCM RemoteConnect plan can be used normally on HA setup, the SoftwareUCM RemoteConnect plan must be purchased and assigned to both SoftwareUCM on GDMS. If only one SoftwareUCM has a SoftwareUCM RemoteConnect plan, the GDMS operation may fail due to HA backup. If only one SoftwareUCM has the SoftwareUCM RemoteConnect plan with HA support, HA-related functions will not work in HA deployment.

Log into GDMS web UI and go to UCMRC→SoftwareUCM Devices. Click to add a new device and enter the SoftwareUCM information.



Add SoftwareUCM to GDMS

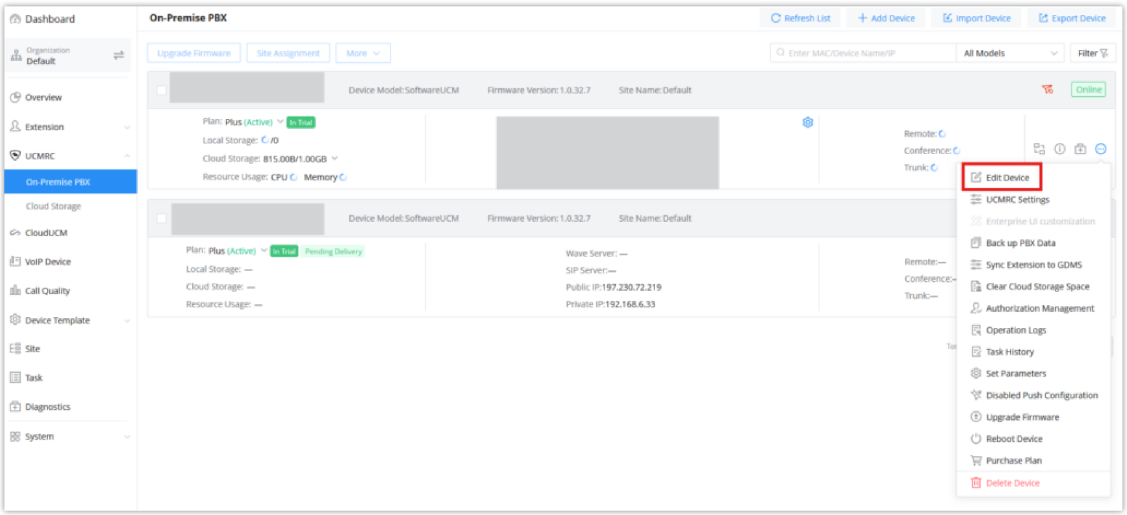
Custom Domain Configuration

Info

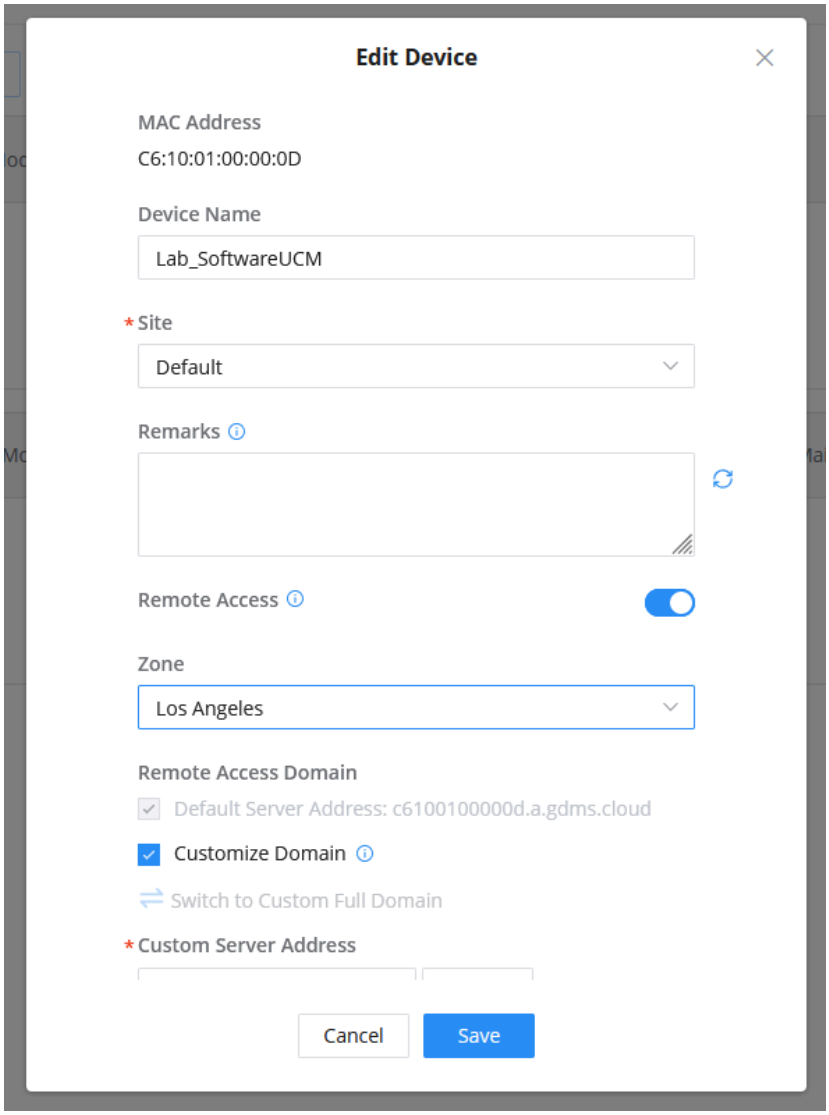
If you need to purchase the SoftwareUCM RemoteConnect plan with a custom domain, please use the following link to refer to more details and to purchase the corresponding plan. https://ucmrc.gdms.cloud/plans

For two SoftwareUCM devices that have purchased the UCMRC package with HA service, you must configure a custom server address or domain name for the **SoftwareUCM set as Primary**.

Custom Domain Name must be set via GDMS. Log in to GDMS and go to UCMRC System→SoftwareUCM Devices, select the SoftwareUCM, and click on "Edit Device" to configure it.



Edit Device



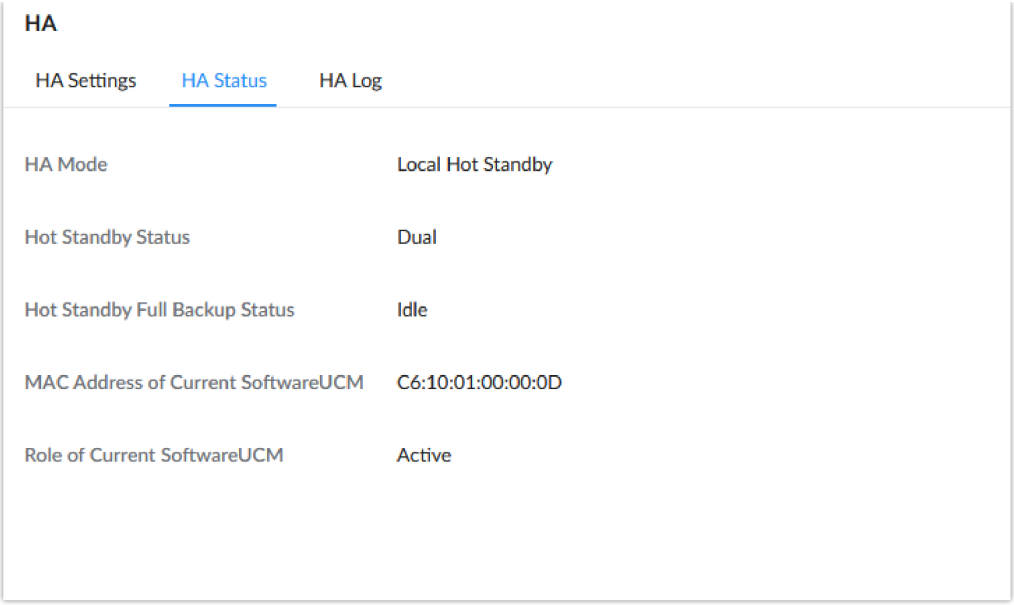
Configure Custom Domain

Click on "Switch to Custom Domain" to edit device custom server access, private secret key, etc. Save the configuration. After changing the custom domain name, please notify SoftwareUCM users of the new public address for SoftwareUCM. For more information about configuring a custom domain name on GDMS, please refer to the GDMS user manual.

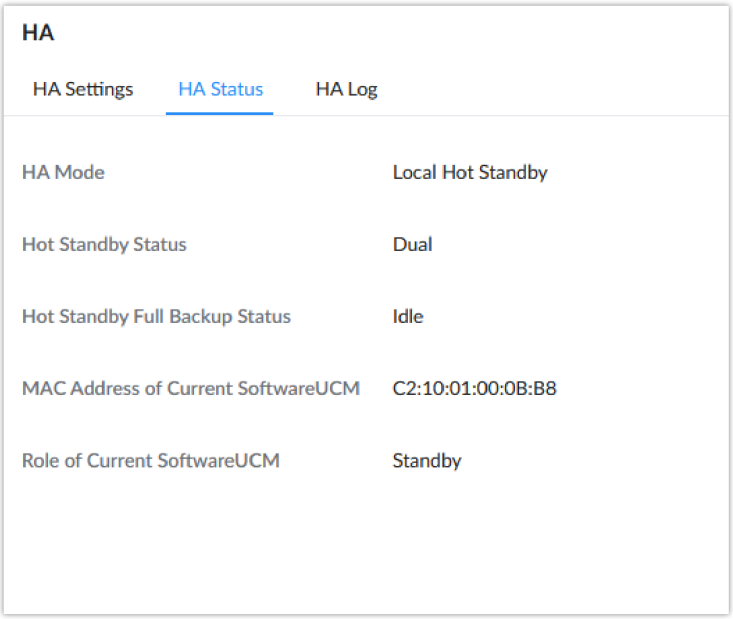
> **Note:**
>
> If you need to purchase a UCMRC plan with HA service rights, please contact the corresponding equipment agent for more details.

Verify HA Settings

1. After configuring HA settings on both SoftwareUCM instances, log in to the SoftwareUCM web UI from each SoftwareUCM's static IP using the active SoftwareUCM's login information and check HA status. Under the HA status page, both SoftwareUCM instances should show HA Status as "Dual". One of the SoftwareUCM instances 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.



HA Status for Active SoftwareUCM

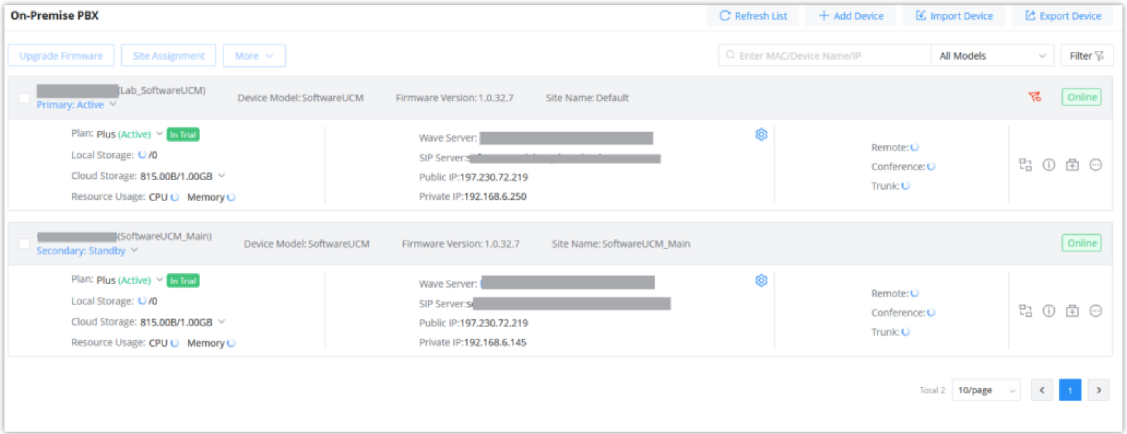


HA Status for Standby SoftwareUCM

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

Verify HA Status via GDMS

GMDS allows the user to verify which SoftwareUCM is primary and which one is secondary. On the GDMS interface, go to the **SoftwareUCM Device** tab.

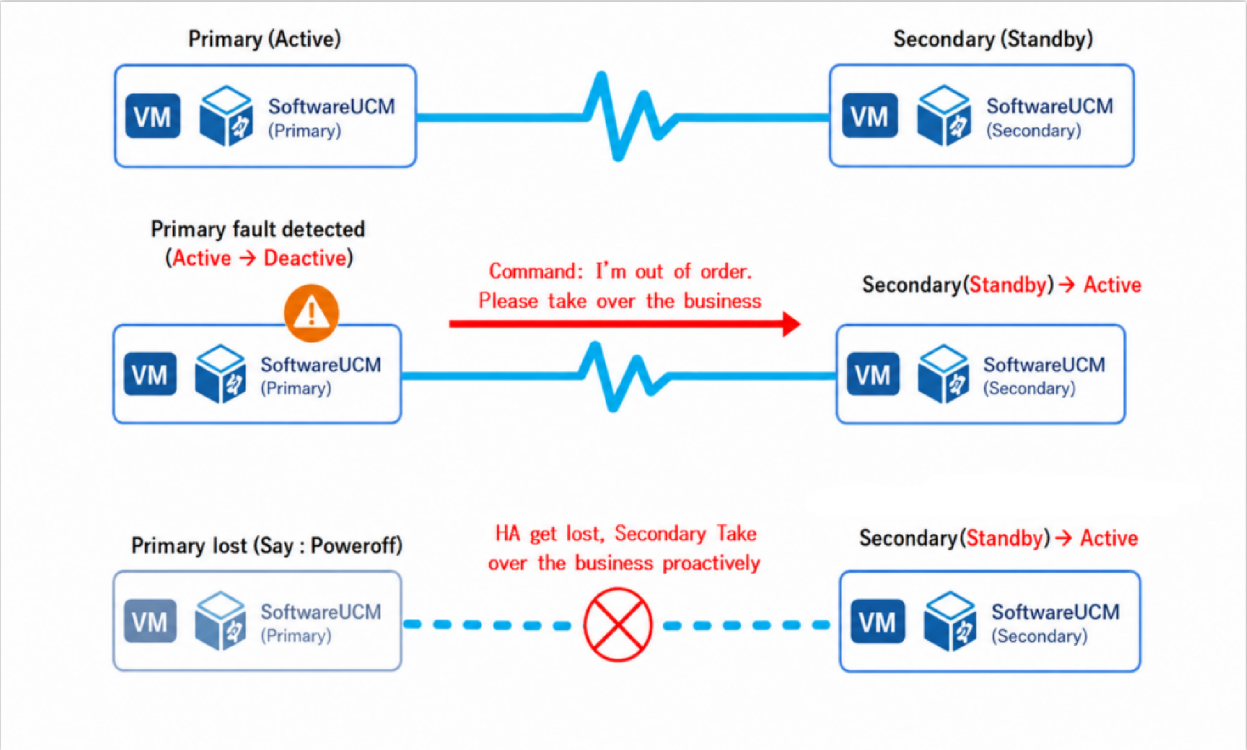


- **Primary**: indicates the primary SoftwareUCM.
- **Secondary:** indicates the secondary SoftwareUCM.

If you want to check which SoftwareUCM is performing high availability with which SoftwareUCM, click on “spare” or “host” to verify,

Active/Standby Role in HA

Automatic Failure Detection



Active and Standby SoftwareUCM Failover

Active SoftwareUCM: Self-Failure Detection

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

Standby SoftwareUCM: Periodic Heartbeat

On HA mode, the standby SoftwareUCM will check the active SoftwareUCM’s status periodically by sending a heartbeat message to the active SoftwareUCM. The heartbeat message is sent via a ping to the primary SoftwareUCM instance IP address. If the active SoftwareUCM is under normal working conditions, it will respond to the standby SoftwareUCM after it receives a heartbeat request from the standby SoftwareUCM. If the active SoftwareUCM runs into a faulty situation, such as the network chip becoming abnormal or the power adapter no longer functioning, it will stop responding to heartbeat requests. After the heartbeat timeout period expires, the standby SoftwareUCM will consider the active SoftwareUCM as faulty and begin taking over as the active server.

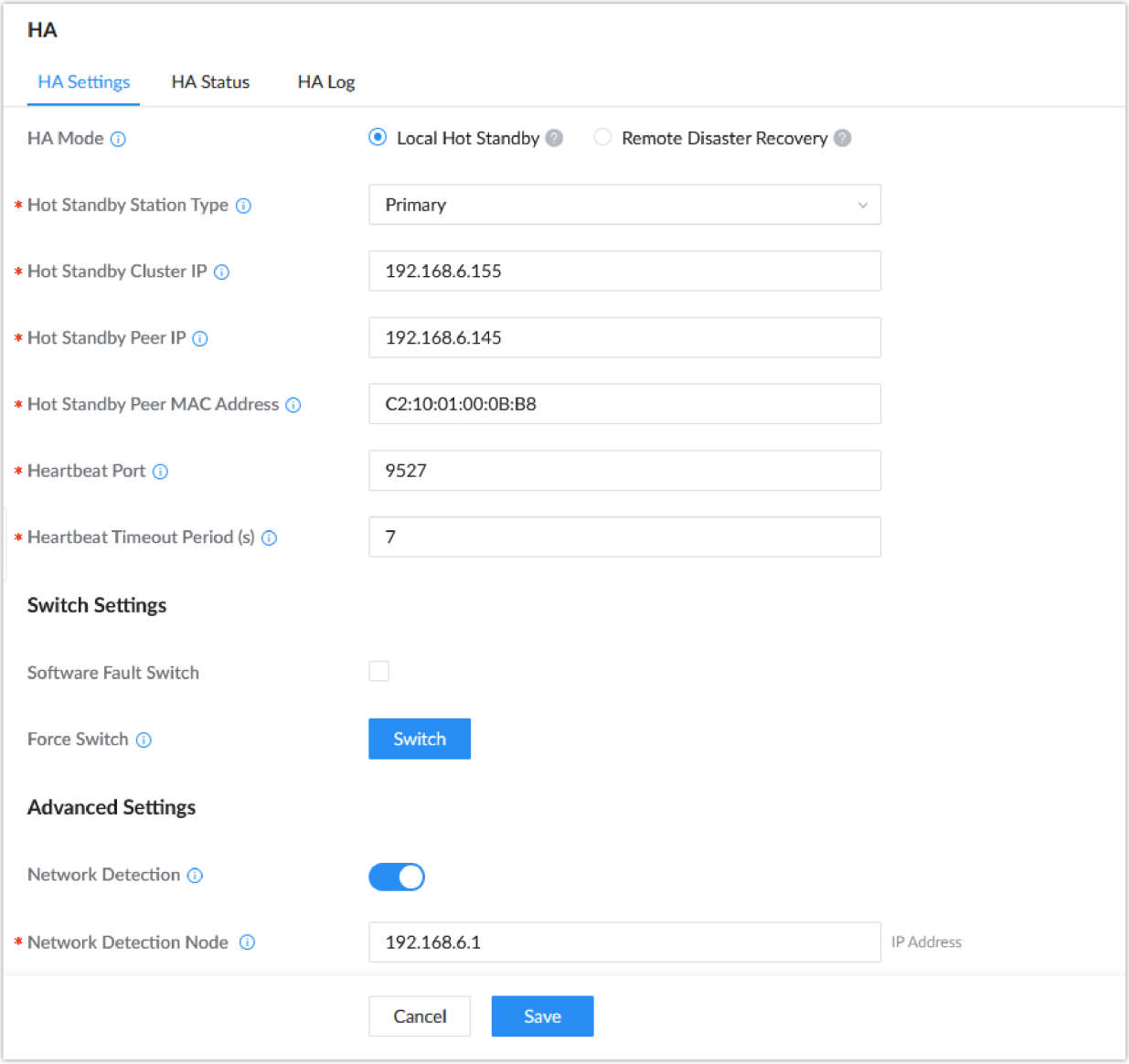
The heartbeat timeout period determines how quickly the standby SoftwareUCM can detect an active server failure and perform a switchover. By default, the heartbeat timeout period is 7 seconds. Users can modify the heartbeat timeout period as needed, which will affect the detection and switchover sensitivity.

Note

In environments with unstable or high-latency network connections, it is recommended to increase the heartbeat timeout period appropriately to help prevent frequent or unnecessary switchovers caused by temporary network interruptions.

Force Switch

For a SoftwareUCM currently in the Active role, you can click the Switch button to change between Active and Standby roles. This operation is generally avoided unless performing a firmware upgrade or if the current Active SoftwareUCM encounters a problem that requires manual switching.



Firmware Upgrade

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

- **Step 1:** Log in to the web UI of the standby SoftwareUCM (B), upload firmware via web UI, and the standby SoftwareUCM will reboot. Wait for it to boot up.
- **Step 2:** After the standby SoftwareUCM (B) boots up, log in to the web UI of the active SoftwareUCM (A) and check the HA web page. The "Force Switch" button on the SoftwareUCM B's HA web page will be available. Press it to manually trigger a switchover. After switchover, SoftwareUCM B will become active, and SoftwareUCM A will become standby.
- **Step 3:** After switchover, log in to SoftwareUCM A and upload firmware to its web UI. SoftwareUCM A will reboot and request data from SoftwareUCM B for a full backup.

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

Replacing SoftwareUCM in HA

HA Equipment Failure Replacement Process (With UCMRC Package)

When two SoftwareUCM devices have purchased a UCMRC package with HA service from GDMS, they form an HA dual-machine configuration. The following steps apply when Device A and Device B have already formed an HA environment, and Device B fails and needs to be replaced by a new Device C. Assuming 2 SoftwareUCM (A and B) with UCMRC plan on GDMS have been set up for HA, and SoftwareUCM B becomes defective, which requires replacement, please follow the steps below to replace the defective SoftwareUCM B with SoftwareUCM C.

Scenario 1: Site A is Primary (Active), Site B is Secondary (Standby)

1. Contact technical support to assist in replacing the device and follow the RMA process to apply for a license for the new Device C for HA.
2. Clearly define the requirements: specify a device replacement in an HA scenario, clarify the role information of the old Device B, and provide Device B's device information. For physical machines, provide the device information file and MAC address; for virtual machines, provide the existing MAC address.
3. After activating Device C's license, add Device C to GDMS and purchase a UCMRC package with HA permissions identical to those for A and B.
4. The administrator deletes Device B from the host console.
5. Modify the HA parameters of Device A by changing the peer MAC address from B to the MAC address and IP address of Device C, save, and restart.
6. After Device A restarts, confirm that it is in an Active state.
7. After Device C starts up, perform basic network settings. These parameters must be the same as those for B, ensuring Device C is configured with the identical site type and static IP address.
8. Ensure storage device consistency and disable Cloud IM on Device C if necessary.
9. Configure the HA parameters on Device C to mirror all configuration parameters from B, save, and restart.
10. Once Device C restarts, check the HA status to confirm all devices are in HA status, with A being the Active role and C being the Standby role.

Scenario 2: Site A is Secondary (Active), Site B is Primary (Standby)

1. Using GDMS, delete the custom server address or domain name of Device B.
2. Contact technical support to follow the RMA process and apply for an HA license for Device C. Provide the same detailed role and device/MAC information for the old Device B as outlined previously.
3. After activating Device C's license, add it to GDMS, purchase the UCMRC HA package, and configure Device C's custom server address or domain name through GDMS to ensure it matches B's previous domain.
4. The administrator deletes Device B from the host console.
5. Modify Device A's HA parameters, changing the peer MAC address to Device C, save, and restart. Confirm A is in an Active state.
6. Boot Device C and perform identical network settings to B (including site type and static IP). Check storage consistency and disable Cloud IM.
7. Enable and configure Device C's HA parameters (the same as B), explicitly setting the site type to Primary. Save and restart.
8. Verify the HA status shows A as Active and C as Standby.
9. Once this dual-machine status is correctly established and the full backup process has been completed , the administrator must perform a manual switchover operation. This transfers the Active role to the Primary site, while the Secondary site is downgraded to the disaster recovery standby state.

HA Equipment Failure Replacement Process (Without UCMRC Package)

When two SoftwareUCM instances form an HA dual-machine system without using a UCMRC package, follow these steps if Device B fails and is replaced by Device C. This applies when Device A is in an Active state and Device B is in a Standby state, regardless of their site type:

1. The administrator deletes Device B from the host console.
2. Modify Device A's HA parameters by changing the peer MAC address from B to Device C, save, and restart. Confirm that A remains in an Active state.
3. Contact support to follow the RMA process and apply for a license for Device C in the HA scenario. Clearly define the requirements and provide Device B's exact role and MAC/device information.
4. After activating Device C's license, configure its basic network settings to match B identically (same site type and static IP address).
5. Check storage consistency between devices and disable Cloud IM on Device C.
6. Enable and configure the HA parameters in Device C to match Device B, save, and restart.
7. After Device C restarts, check the status to ensure all devices are in HA status, with A acting as Active and C as Standby

> **Critical Note:**
>
> HA configuration requires the SoftwareUCM to reboot. Please reboot the SoftwareUCM instances during non-service hours to avoid service interruption.

Disabling HA Setup

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

Cloud IM in HA Setup

Please ensure only one SoftwareUCM in the HA setup has Cloud IM enabled. If using a domain name assigned from GDMS, please ensure both SoftwareUCM devices have the SoftwareUCM RemoteConnect plan, which supports Cloud IM.

After the active SoftwareUCM A in HA setup enables Cloud IM, the standby SoftwareUCM B will synchronize from SoftwareUCM A and obtain Cloud IM service as well. Cloud IM service is always available on the active SoftwareUCM, and the associated MAC address will change if the active/standby SoftwareUCM changes. Therefore, failover in the HA setup does not affect the Cloud IM service.

If SoftwareUCM B fails and a replacement SoftwareUCM C with Cloud IM disabled takes its place to form a dual-node HA system with SoftwareUCM A, Cloud IM will continue to provide HA services for both nodes without any additional configuration. However, if Cloud IM was previously enabled on SoftwareUCM C, it must be disabled before swapping to ensure Cloud IM is not active when SoftwareUCM C replaces SoftwareUCM B.

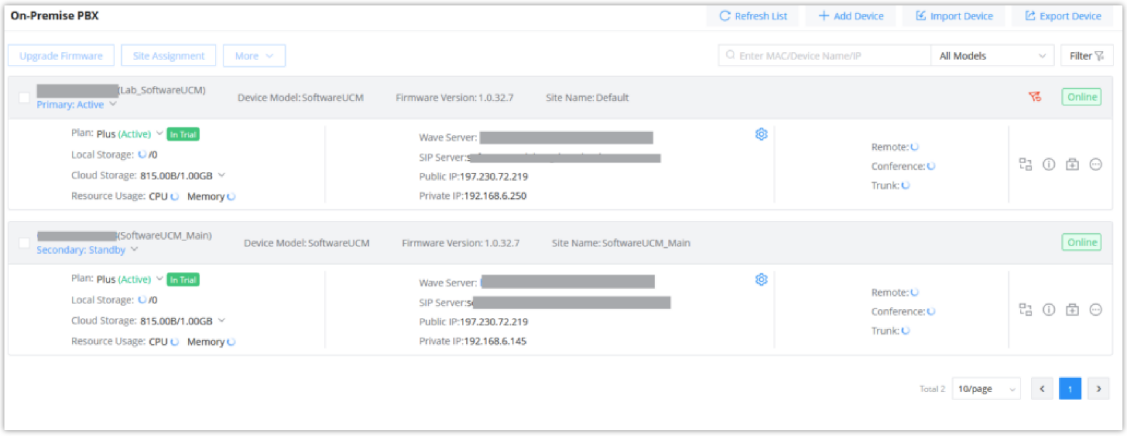
> **Note**
>
> Check if Cloud IM is enabled on the secondary device. If it is enabled, disable Cloud IM to ensure the new device replaces the old one without the Cloud IM service.

Using SoftwareUCM RemoteConnect with HA

If the user has purchased a SoftwareUCM RemoteConnect plan with HA, the GDMS web page can show the SoftwareUCM with HA status "Host" or "Spare".

> **Note**

For more information about UCMRC plans, please refer to the following link: https://ucmrc.gdms.cloud/plans



GDMS Display for SoftwareUCM HA Status

Switching SoftwareUCM RemoteConnect Role in HA

Prerequisites:

- Both SoftwareUCM instances must have the SoftwareUCM RemoteConnect plan with the HA feature purchased on GDMS.
- UCMRC service has been successfully delivered to both SoftwareUCM.

Implementations:

- The call service is provided by GDMS and the active SoftwareUCM.
- When the active SoftwareUCM A is in a faulty condition and has triggered a switchover, the standby SoftwareUCM B will take over and become active. SoftwareUCM B will send the switchover command to GDMS and notify GDMS that call service will be provided by SoftwareUCM B and GDMS afterwards.

Note

1. With UCMRC, after the SoftwareUCM is configured with HA, SoftwareUCM will notify its HA role to GDMS. System admin does not need to designate the HA role for SoftwareUCM on GDMS.
2. On GDMS, the system admin can still remotely access and operate each SoftwareUCM in HA. However, the configuration on the standby SoftwareUCM is limited because it synchronizes data from the active SoftwareUCM regularly in the HA backup process.
3. The PBX providing service is the active SoftwareUCM. However, GDMS will always assign the domain name for the Remote Connect service based on the primary SoftwareUCM as configured initially.

SoftwareUCM HA Device Licenses

Proper licensing is strictly required for SoftwareUCM HA equipment.

- **License File Details:** The SoftwareUCM HA standby license uses a separate license file (the license file will be marked HA Slave and will include the MAC address of the host machine). The SoftwareUCM License package will add an add-on: HA Slave. When you place an order, select this add-on and the price of the entire license will be reduced (for example, by 30%).
- **Pricing:** The SoftwareUCM License package features an “HA Slave” add-on. When you place an order, select this add-on to reduce the price of the entire license (for example, by **10%** to **30%**).
- **Configuration Limits:** SoftwareUCM instances using an HA standby license can only be configured with HA on the corresponding Primary machine within the license.
- **Important Warning:** If HA mode is not configured, any extensions created on the local machine will not work or be used.

Service Status

Active/Standby Status

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

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

Web UI Access for UCM

After the HA setup is completed, the cluster IP becomes a floating IP for providing external services. To log in to the SoftwareUCM web UI, the system admin only needs to enter the cluster IP address. Regardless of any role switch, the floating IP remains unchanged and is always bound to the SoftwareUCM currently in the Active role, providing services. For example, assuming the HTTP/HTTPS port is 8089, the system admin can access the active SoftwareUCM using the URL https://cluster_IP:8089.

- System admin can log into the current active SoftwareUCM using https://cluster_IP:8089 or https://activeUCM_IP:8089.
- If the system admin logs into the standby SoftwareUCM's web UI by using the standby SoftwareUCM IP https://standbyUCM_IP:8089 and attempts to modify configurations, it will not be allowed. The system will prompt that configuration is restricted on the standby SoftwareUCM.

> **Important Note**
>
> After HA setup, the administrator identity and account information from the active SoftwareUCM are synchronized to and overwrite those on the standby SoftwareUCM. Therefore, when logging in through the floating cluster IP or either SoftwareUCM device's IP address, the system admin must always use the administrator credentials of the current active SoftwareUCM.

Log in Wave

After HA configuration, the login URL for Wave may be changed. Users can log in to Wave using the following addresses:

1. **Log in via IP.**

Since the SoftwareUCM providing the RemoteConnect service can be the primary or secondary SoftwareUCM, the user should always use the cluster IP to log in to Wave. For example, https://cluster_IP:8089/gswave#.

2. **Log in via domain name.**

No matter whether a failover happens, users can always use the domain name assigned from the GDMS Remote Connect service, which is determined by the initially configured primary SoftwareUCM.

Failover during Call

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

> **Notes**
>
> - Currently, if the call is using UDP as a transport method, the call can be recovered after switchover. However, if the call is using TCP as a transport method, the call cannot be recovered after switchover.

- Point-to-point calls, such as audio calls 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 a data sync mechanism:

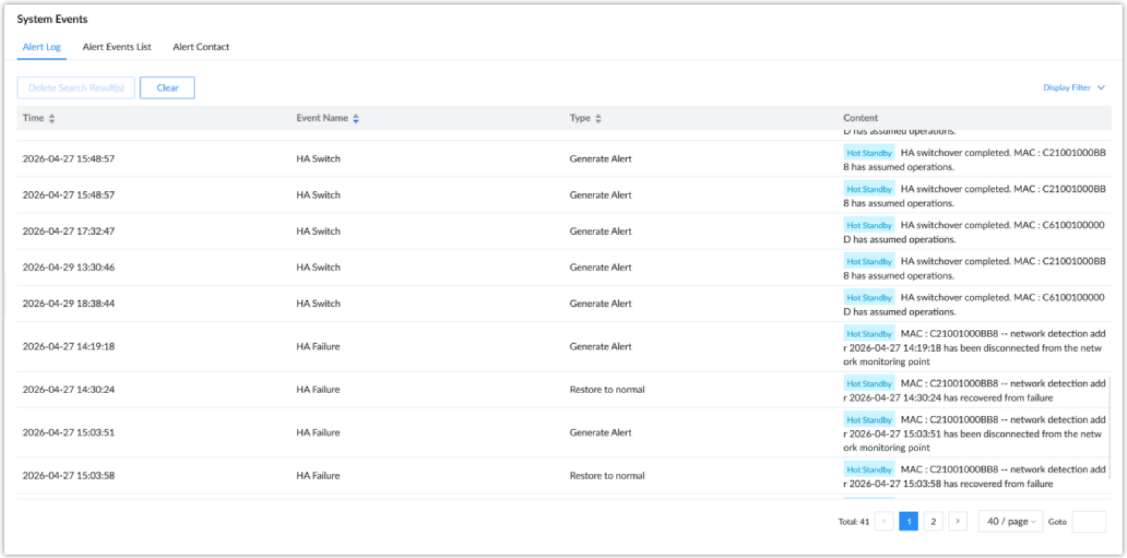
1. After SoftwareUCM boots up, the standby SoftwareUCM will send requests for all the data on the active SoftwareUCM and perform data sync. Every time the active SoftwareUCM has a configuration change, it will also synchronize the data to the standby SoftwareUCM automatically and immediately.
2. Data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

Backup and Restore

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

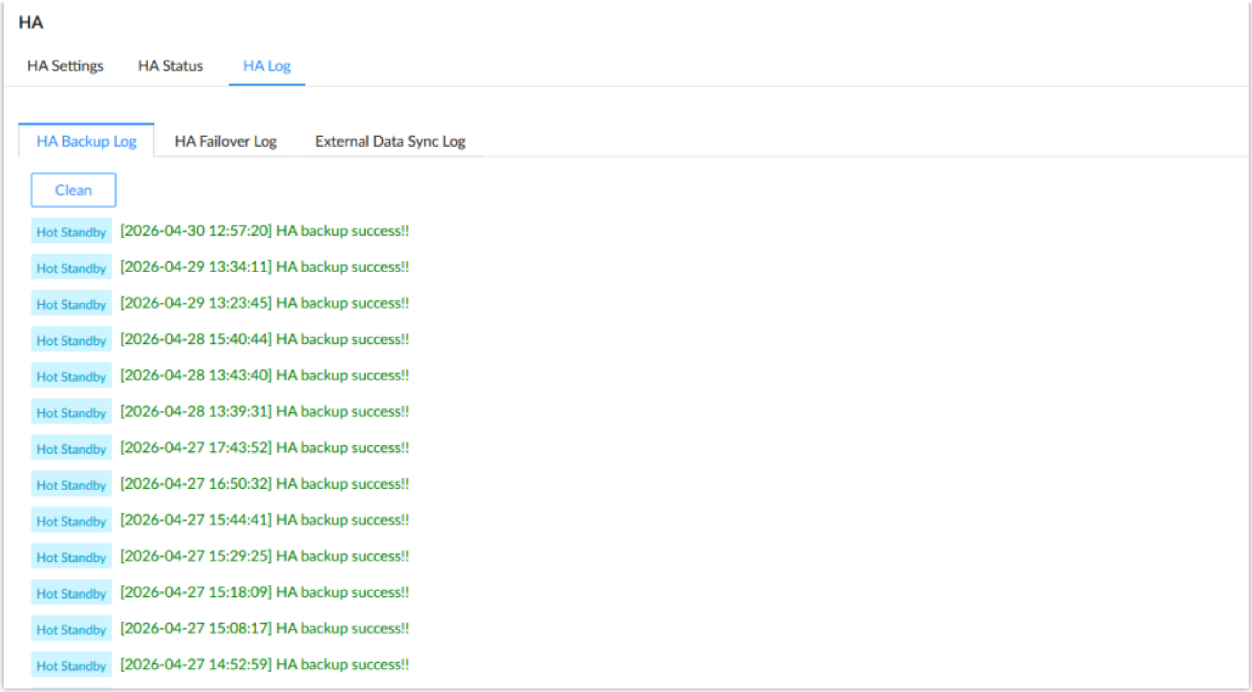
Maintenance

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



System Alert Events

The HA log also shows all HA backup and failover logs.



HA Logs

Need Support?

Can't find the answer you're looking for? Don't worry we're here to help!

CONTACT SUPPORT