

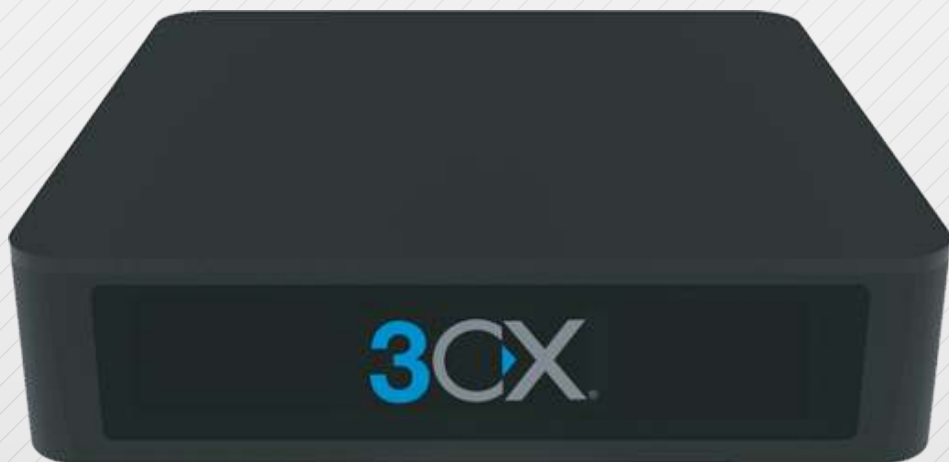


**Model:** HA 3CX

**3CX**

**APPLIANCE**

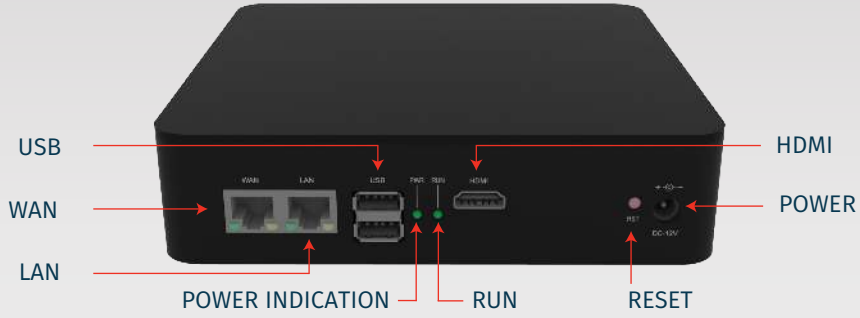
**QUICK START**



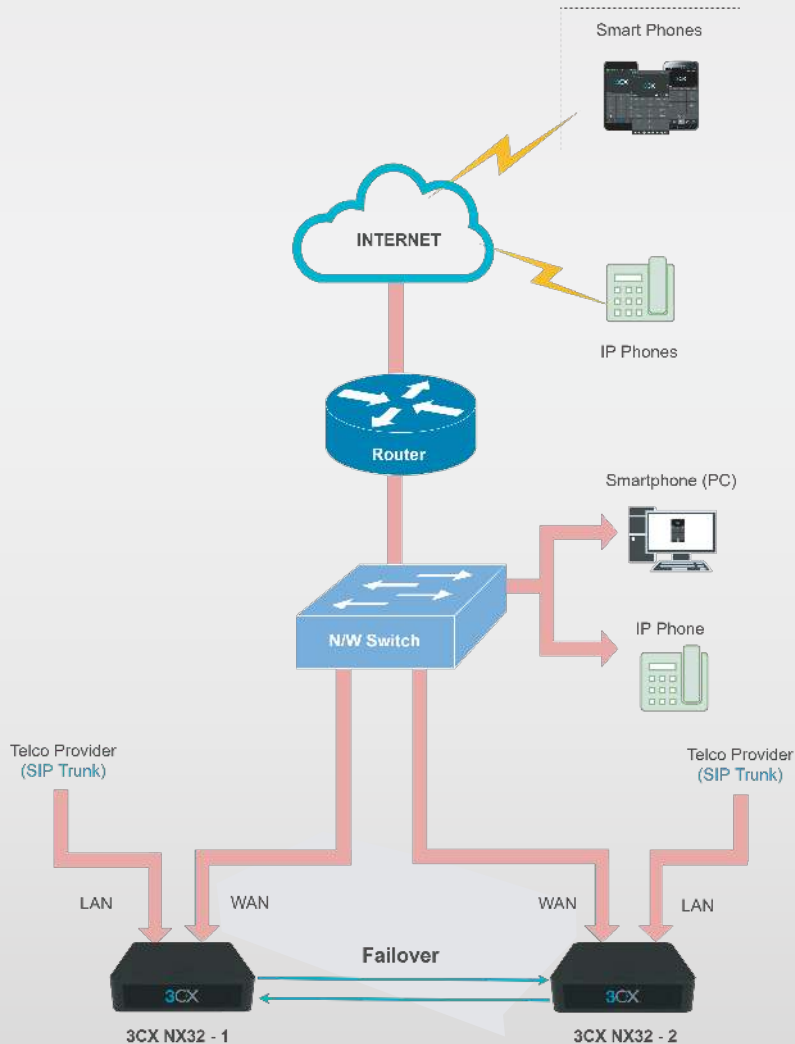
**BREAK FREE**

A SOFTWARE BASED ON PBX

# Steps to be followed:



## HA 3CX - Network Connection Map



# Configuring Failover with 3CX and NX32:

- Step 1:** Introduction
- Step 2:** Licensing
- Step 3:** Failover Form
- Step 4:** Topologies
- Step 5:** Pre-requisites
- Step 6:** Configuring the Active and Passive Servers
  - A) Configuring the Active Server (#1)
  - B) Configuring the Passive Server (#2)
- Step 7:** Failover Server Configuration
- Step 8:** Custom Failover Usage

## 01 Introduction

The Failover feature in 3CX allows you to create a standby replica of your PBX. In the event that your PBX fails, your replica PBX becomes active minimizing downtime and data loss. Follow the required steps below to activate this functionality.

## 02 Licensing

An Enterprise (ENT) or Professional (PRO) license key is required in order to enable the failover functionality. With an ENT license key, the DNS TTL resolution for a 3CX provided FQDN is set to 5 minutes, whereas a Pro license key uses a 6 hour TTL causing a much longer reconnect time for IP phones, 3CX Apps, 3CX SBCs or the 3CX Web Client.

## 03 Failover Form

3CX uses an active - passive approach using built-in configuration replication with a maximum offset of 24h. The active host processes calls and presence information, while the passive host monitors the active host. In case of a failure of the active host (independent of application, OS or hardware failure), the passive host stops its monitoring role and takes over as the active host. The passive host's configuration determines in which state the active host is declared failed in order to initiate the failover switch.

## Steps to be followed:

# 04 Topologies

The following network scenarios are covered by the failover process:

- On-premise (NAT):
- Scenario A: with only remote extensions
- Scenario B: with local and/or remote extensions
- Cloud (Public Host):
- Scenario C: with only remote extensions as STUN / SBC

A failover from an on-premise host to a cloud host and vice versa is not supported. Documentation and processing are solely tested and supported while using 3CX provided public FQDNs. Theoretically it is possible to use custom public FQDN for the process, however, it is the administrator's obligation to control, update and manage all relevant DNS entries as required.

# 05 Pre-requisites

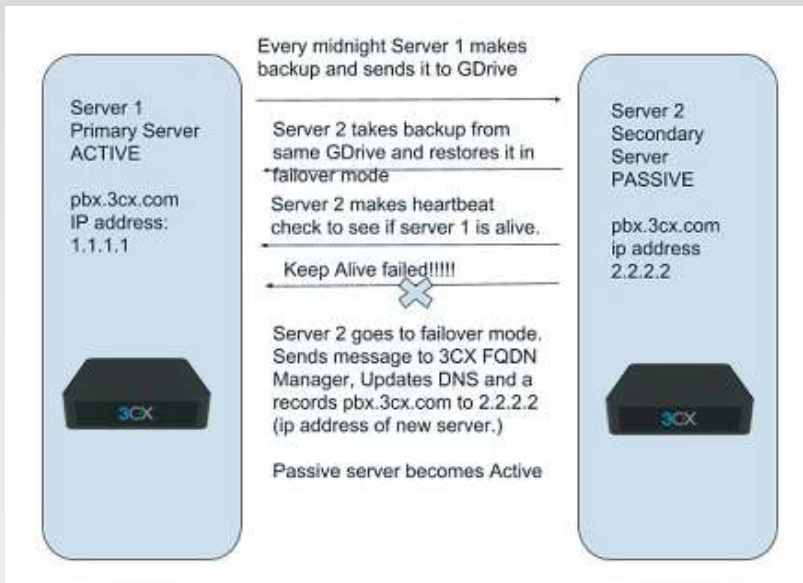
Before configuring or enabling 3CX failover on your 2 servers, the 3CX installations need to conform to these requirements.

1. Two (2) 3CX cloud PBXs each with its own public IP, both installed with identical settings, including FQDN, SSL Certificate, SIP, Tunnel, web server ports and web server type.
2. When configuring 3CX after the installation, you need to select 3CX FQDN.
3. The "Select interface" field needs to be set to the FQDN (not the IP) in the "Extension" > "Phone Provisioning" tab > "IP Phone" section.



## Steps to be followed:

### Overview of how it works:



## 06 Configuring the Active and Passive Servers

### A) Configuring the Active Server (#1)

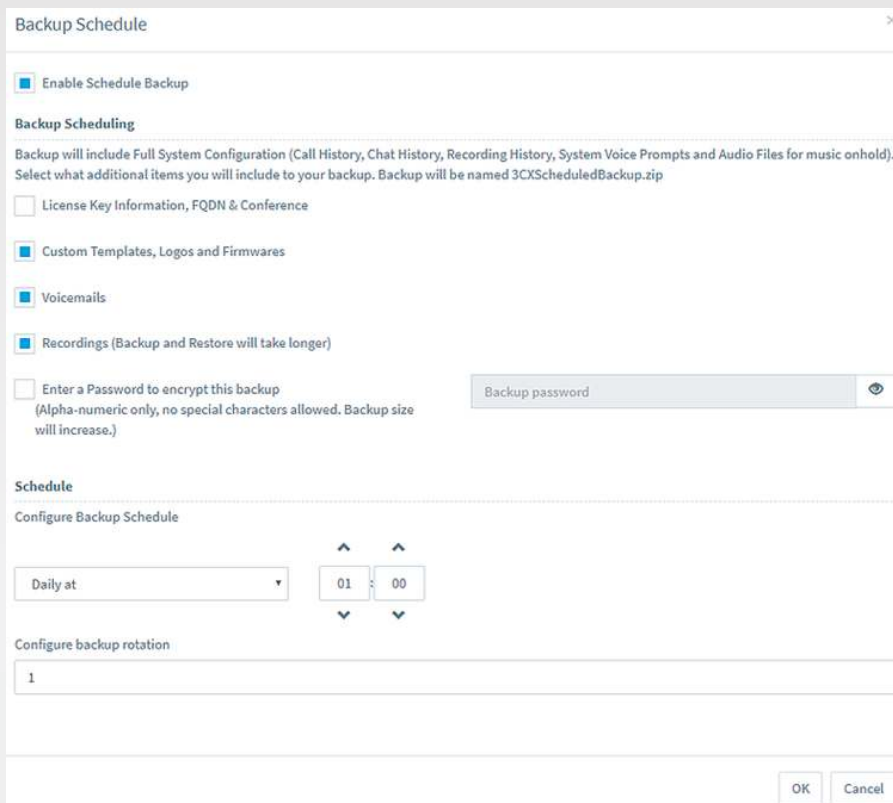
1. We assume that server #1 is your production server with 3CX already pre-installed and configured.

<b>IP Phone</b>
Provisioning Method
Local LAN (in the office)
Provisioning Link: <a href="http://192.168.3.160:5000/provisioning/pc56bscs195k/">http://192.168.3.160:5000/provisioning/pc56bscs195k/</a>
Mac Address
7C2F80BE80EB
Select Interface
192.168.3.160
192.168.3.160
10.65.0.160
<b>companys.3cx.eu</b>

## Steps to be followed:

2. All extensions need to be provisioned using the FQDN, via the **“Select Interface”** field in **“Extension”** > **“Phone Provisioning”** tab > **“IP Phone”** section.

3. Go to **“Backup and Restore”** > **“Location”** and select **Google Storage** as the location type, or specify other backup options, e.g. SMB or SFTP. For this example, backups are stored in the **“3CX\_PBX\_Backups”** folder in a Google Storage bucket.

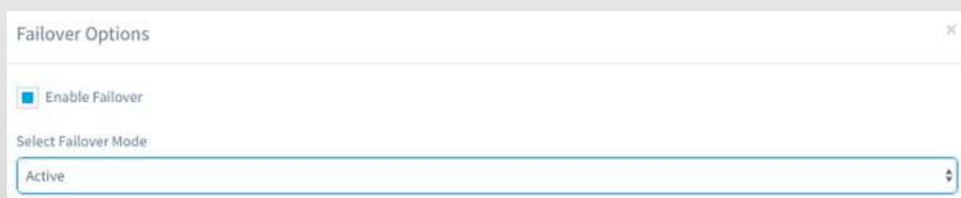


The screenshot shows the 'Backup Schedule' configuration window. It has a title bar with a close button. The main content area is divided into sections:

- Enable Schedule Backup:** A checkbox that is checked.
- Backup Scheduling:** A section with a descriptive paragraph: 'Backup will include Full System Configuration (Call History, Chat History, Recording History, System Voice Prompts and Audio Files for music onhold). Select what additional items you will include to your backup. Backup will be named 3CXScheduledBackup.zip'. Below this are several checkboxes:
  - License Key Information, FQDN & Conference
  - Custom Templates, Logos and Firmwares
  - Voicemails
  - Recordings (Backup and Restore will take longer)
  - Enter a Password to encrypt this backup (Alpha-numeric only, no special characters allowed. Backup size will increase.)
- Schedule:** A section with the heading 'Configure Backup Schedule'. It contains a dropdown menu set to 'Daily at', followed by two spinners for time, set to '01' and '00'. Below this is another section 'Configure backup rotation' with a text input field containing the number '1'.

At the bottom right, there are 'OK' and 'Cancel' buttons.

4. Click on **“Backup Schedule”**, select backup options to include, set the backup schedule and click **“OK”** to save your configuration. A daily off-hours backup is recommended, e.g. start backup at 1:00 AM and upload **“3CXScheduledBackup.zip”** (latest backup filename) to Google storage.



The screenshot shows the 'Failover Options' configuration window. It has a title bar with a close button. The main content area is divided into sections:

- Enable Failover:** A checkbox that is checked.
- Select Failover Mode:** A dropdown menu with 'Active' selected.

## Steps to be followed:

5. Now, click the **“Failover”** button, set the **“Enable Failover”** checkbox and select **“Active”**. Press OK to save.

The active server (#1) is successfully configured, with scheduled automatic backups stored in the Google Storage folder. Proceed to the next step to configure the passive server (#2).

### B) Configuring the Passive Server (#2)

**! Important:** For scenarios where the Active/Primary and Passive/Failover servers are behind different public IP addresses, when you first complete the installation of the Passive server and you run through the installation options, your public FQDN will be rewritten to the public IP of the Failover server. To re-write your external FQDN to resolve back to the public IP of the Active server, you need to edit the license for your primary server in **“Settings” > “License”** and click on **“OK”**, to switch back the FQDN to the 3CX primary server and restart its services.

## 07 Failover Server Configuration

Switch to the passive server (#2) and install the 3CX Phone System using the same configuration settings as your active server.

Restore Schedule

Enable Schedule Restore

Schedule an automatic restore then the scheduled restore will take the most recent backup with name "3CXScheduledBackup.zip".  
Note: If you are scheduling backups automatically, then the scheduled restore will take the most recent backup.

**Restore Schedule**

Configure Restore Schedule

Daily at  :

Do not start services after restore

Enter Password to decrypt this backup  
(Alpha-numeric only, no special characters allowed.)

OK Cancel

1. Whilst on server #2 click on **“Backup and Restore” > “Restore Schedule”**, enable Schedule Restore and set a time for the restore to be applied. Check the option **“Do not start services after restore”**. Press OK to save.

## Steps to be followed:

The screenshot shows a 'Failover Options' dialog box with the following settings:

- Enable Failover
- Select Failover Mode: Passive
- IP address of ACTIVE server: 1.1.1.1
- Failover Tests:  SIP Server,  Webservice,  Tunnel
- Failover Behavior: Time interval between tests in seconds: 30
- Failover when all selected tests fail
- Failover when at least one of the selected tests fail
- Failover Script Operations: Choose a script to launch BEFORE 3CX Services are started: pre\_3cx\_start.sh; Choose a script to launch AFTER 3CX Services are started: post\_3cx\_start.sh

2. Click on the **“Failover”** button, check **“Enable Failover”** and select **“Passive”** in the **“Select Failover Mode”** dropdown.

- Enter the IP address of the active server (#1), e.g. **1.1.1.1**
- Select which services you want to monitor: SIP Server, Web Server or Tunnel Server.
- Select the interval for the heartbeat checks to be made, (default 30 seconds) and configure whether failover occurs if one or all tests fail.
- Press OK to save the configuration and start monitoring.

When the active server (#1) fails, the passive detects this and takes over. With the backup already restored, the failover action triggers the 3CX DNS Servers to update the FQDN to the IP address of the new active server (#2).

It is important that the previously active server (#1) is shutdown to avoid conflict with the server that just took over.

**Note :** Gateways (FXS/FXO) in a failover scenario are only supported when local to your PBX system, i.e. reachable via LAN. Even in cases where there is a site-to-site VPN between NATed Servers, we cannot Support Gateway Registration and failover to the Failover server as it depends on manufacturer/model/gateway capabilities.



Steps to be followed:

## 08 Custom Failover Usage

For Failover use with custom FQDN and LAN-to-LAN or LAN-to-Cloud scenarios, to update your DNS and FQDNs when failover occurs, you need to use advanced scripting and services like Active Directory to run shell scripts with administrative privileges.