A MITEL
PRODUCT
GUIDE

MiCollab

MiCollab Client Resiliency Guide

Release 9.7

March 2023

Mitel
Powering connections

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®).**The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website:http://www.mitel.com/trademarks.

Contents

Purpose of this Guide 1

In MiCollab Release 7.1 onwards, MiCollab Client softphones support Domain Name System (DNS)-based Session Initiation Protocol (SIP) resiliency with clustered MiVoice Border Gateways (MBGs) or clustered Communication Platforms (PBXs). This guide provides the DNS configuration required to support SIP resiliency for MiCollab Client softphones in an Enterprise or Cloud environment.

Overview 2

This chapter contains the following sections:

The MiCollab Client softphone supports SIP for audio and video communication. It uses SIP for all call-related signaling, Transport Layer Security (TLS), Secure Real-time Transport Protocol (SRTP), and resiliency support.

In an Enterprise or Cloud environment, a SIP softphone can connect to the network either through an MBG or a PBX in a cluster. SIP softphone resiliency ensures that users experience minimal disruption in service when the MBG or the PBX to which the softphone is connected goes out of service. The Registrar/Proxy file in the MiCollab Client softphone lists the hostnames of multiple MBGs and PBXs. The softphone re-registers with any of the MBGs in the list subject to the priority and weighting settings to re-establish the service. The softphones register on client start-up or after the registration interval time expires.

2.1 Supported MiCollab Clients

The following MiCollab Clients support DNS-based SIP resiliency:

- MiCollab for PC Client
- MiCollab MAC Desktop Client
- MiCollab for Mobile Client
  - Android
  - iPhone (supports only MBG resiliency)

Note:

MiCollab users can start the Client even when the MiCollab Server is not reachable but with limited functionality. See ***MiCollab Client End-User Online Help*** > ***Troubleshooting*** > ***MiCollab Client Server Connection Issues*** section for information on the functionality.

2.2 How SIP resiliency works

In an Enterprise or Cloud environment, the softphones are connected to the network through an MBG cluster or a PBX cluster. One element of the cluster must be defined as the primary and one or more among the remaining elements as the secondary.

For MiVoice Border Gateway

To enable resiliency when a softphone is connected through an MBG, you use DNS to map the Fully Qualified Domain Name (FQDN) of the cluster to the hostnames of the member MBGs. This mapping is contained in the configuration file on the DNS server. If the MBG that supports the softphones goes out of service, the softphones use the configuration data that they received from the DNS server to register with an alternate MBG (secondary) in the cluster. This allows the softphone to re-establish the service.

For MiVoice Business

To enable resiliency when a softphone is connected directly to an MiVB, the secondary element for the softphone must be defined in the MiVB server. You must also select the same secondary element from the **User and Services** page in the MiCollab server. You must then use DNS to map the FQDN of the cluster to the hostnames of the member MiVBs. This mapping is contained in the configuration file on the DNS server. If the MiVB that supports the softphone goes out of service, the softphones use the configuration data that they received from the DNS server to register with an alternate MiVB (secondary) in the cluster. This allows the softphone to re-establish the service.

Note:

For MiVB resiliency to work, Teleworker must be set to OFF.

For networks with MBG and MiVB

When a softphone is connected to a network that has both MBG and MiVB, the user must enable resiliency for both MBG and MiVB. See the sections “For Mivoice Border Gateway” and “For MiVoice Business”.

2.3 DNS Service Records

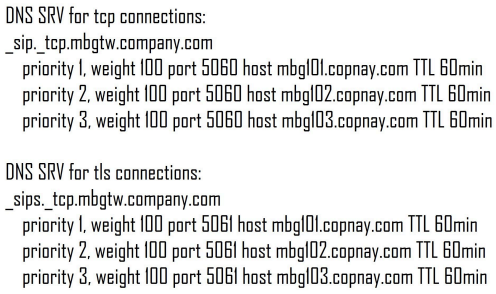
DNS Service (SRV) records are used to provide FQDN-to-hostname mapping and to specify priorities, weightings, port configuration and Time to Live (TTL). If the MBG or MiVB that connects the softphone to the network fails, the softphone registers with a secondary MBG or MiVB in the cluster depending on the data configuration in the SRV record. An SRV record name is made up of the service and the protocol in use.

For SIP, there are only three valid DNS SRV transport protocols. These are:

- _sip._tcp
- _sips._tcp
- _sip._udp (not supported by MiCollab)

The following figure shows two sample DNS SRV records for an MBG resilient network. This will be similar for an MiVB resilient network.

Figure 1: Sample DNS SRV Records



Note:
For TCP connection the SIP DNS SRV prefix is _sip, while for TLS this changes to _sips.

Note:
The MiCollab Softphone does not support load balancing. Each MBG configured in the SRV record should have its own priority.

In the above sample records:

- FQDN of the MBG cluster is "mbgfw.company.com’

- Primary registrar/proxy = mbgfw.company.com
- "mbgfw.company.com" maps to the following MBG nodes:
  - mbg101.company.com
  - mbg102.company.com
  - mbg103.company.com
- priority: determines the order in which the MBGs or MiVBs are used. Thus, mbg101 and mbg102 (priority 1) would be utilized before mbg103 (priority 2).
- weightings: determines the workload handled by the MBGs or MiVBs. The higher the weighting, the greater the workload. The workload for an MBG or MiVB is equal to its weighting divided by the total weighting for the assigned priority. mbg102 would therefore handle 3/4 of the workload for priority 1 MBGs.
- port: identifies the SIP port used (5060 is default for TCP; 5061 is default for TLS).
- TTL: identifies the duration for which the data remains in the network. In this example, after 60 minutes, the timer expires and the softphone updates its Registrar/Proxy file with the latest version from the DNS server.

Typical Deployment 3

This chapter contains the following sections:

3.1 For MBG

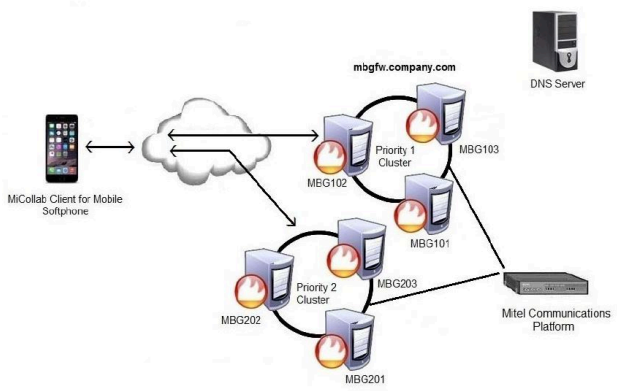
In a typical Cloud deployment, the softphones use DNS SRV records to receive service through a preferred cluster of two or more MBGs with access to a backup MBG. The MBGs in the cluster provide access to a communication platform (MiVoice Business, MiVoice 5000 or MiVoice MX-ONE). The communication platforms can also provide varying degrees of resiliency.

The following figure shows a deployment in which DNS resiliency for the MiCollab Client softphones is supported by two MBG clusters.

On startup, or after the TTL expires, the softphone queries the DNS server and the DNS server returns the list of configured MBGs. The softphone starts with the highest priority entries and selects an MBG based on the weightings. If the MBG is unavailable, the softphone attempts to connect to other members at the same priority level; otherwise, it moves a member at the next priority level down. This distributes the load according to weights across the available MBGs.

You can also create a lower priority list on the DNS server that directs the softphone service to another MBG cluster to provide reasonable (possibly more expensive) service in the event that the MBG cluster associated with higher priority list goes out of service.

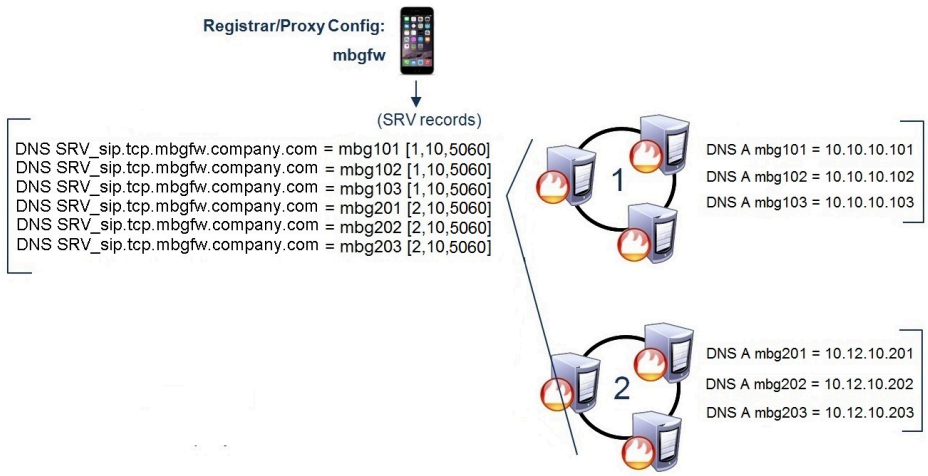
Figure 2: Softphone Resiliency in Cloud Deployment



The softphones periodically poll the MBGs in the higher priority list so that once service is restored, the user's softphone returns to the preferred MBG cluster.

MiCollab Client softphones use SRV records. Other SIP phones can use other DNS queries, such as A-records or NAPTR. The following figure shows an example of DNS SRV entries for resilient softphones in cloud deployment (assuming equal weighting):

Figure 3: DNS SRV Entries for Resilient Softphones in Cloud Deployment



3.2 For MiVB

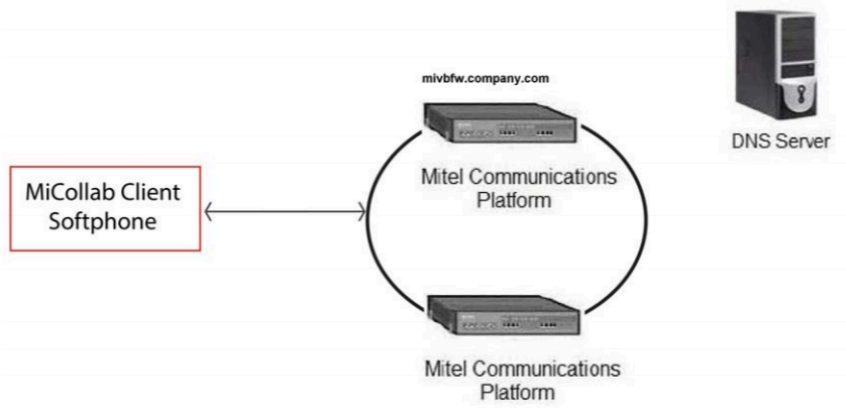
In an Enterprise deployment, the softphones use DNS SRV records to receive service through a preferred cluster of two or more MiVBs with access to a backup MiVB.

The following figure shows a deployment in which DNS resiliency for the MiCollab Client softphones is supported by a MiVB cluster.

On startup, or after the TTL expires, the softphone queries the DNS server and the DNS server returns the list of configured MiVBs. The softphone starts with the highest priority entries and selects an MiVB based on the weightings. If the MiVB is unavailable, the softphone attempts to connect to other members at the same priority level; otherwise, it moves a member at the next priority level down. This distributes the load according to weights across the available MiVBs.

You can also create a lower priority list on the DNS server that directs the softphone service to another MiVB cluster to provide reasonable (possibly more expensive) service in the event that the MiVB cluster associated with higher priority list goes out of service.

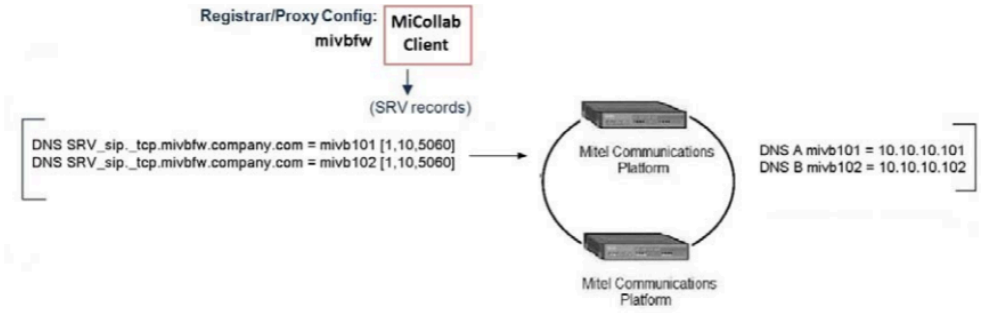
Figure 4: Softphone Resiliency in Enterprise Deployment



The softphones periodically poll the MiVBs in the higher priority list so that once service is restored, the user's softphone returns to the preferred MiVB cluster.

MiCollab Client softphones use SRV records. Other SIP phones can use other DNS queries, such as A-records or NAPTR. The following figure shows an example of DNS SRV entries for resilient softphones in enterprise deployment (assuming equal weighting):

Figure 5: DNS SRV Entries for Resilient Softphones in Enterprise Deployment



MiCollab Client Softphone Resiliency 4

This chapter contains the following sections:

The following sections describe the behavior of the softphone in a resilient network:

- when the softphone is connected to MiVB through MBG
- when the softphone is directly connected to MiVB

4.1 When the softphone is connected to MiVB through MBG

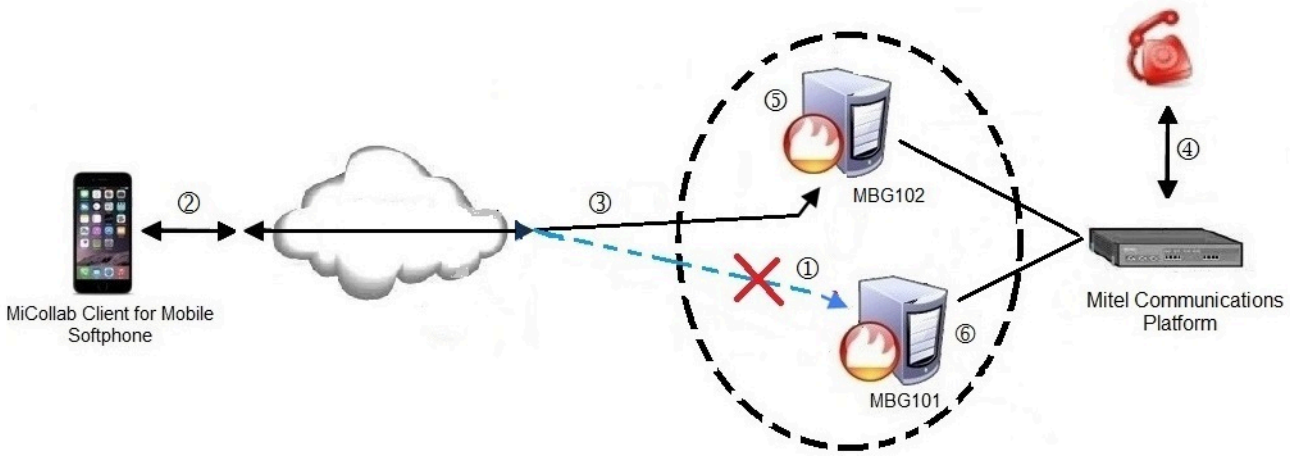
This section describes the behavior when the softphone is connected to MiVB through MBG, and the MBG goes out of service.

1. If the MiVB to which a softphone is registered is taken out of service, or if the connection to that MiVB is lost, an ongoing call is not affected (unless that call is going to a PSTN Trunk through that MiVB). However, mid call features do not work. The call can be ended using the End Call button. The ongoing call is maintained until the SIP session timer times out. The MBG redirects the next SIP softphone registration to the secondary MiVB. When the call ends, the softphone automatically re-registers with the secondary MiVB. This is supported by the MBG.
2. If the MBG to which a softphone is registered is taken out of service, or if the connection to that MBG is lost, the ongoing call is dropped. The softphone re-registers automatically with another MBG in the cluster.
3. When the primary MiVB/MBG recovers, the softphone re-registers automatically with the primary MiVB/MBG.
4. If there is no ongoing call at the time of an MBG outage, the softphone detects the loss of registration (either on its own or when the user tries to make a call) and re-registers automatically with the secondary MBG.
5. Incoming calls cannot connect with the softphone until the softphone registers with the secondary MBG. During this registration period, incoming calls are routed to voicemail if the user has a mailbox on a Mitel communications platform.
6. Calls that are in setup state when the MBG outage occurs are also dropped. The user is notified of the failure.

7. When the service outage occurs, the softphone initiates registration with another MBG in the list. After the softphone registers, it receives service from the secondary MBG. Note that MiCollab Client features such as Status and Presence provide limited service when the softphone is connected to a secondary MBG.
8. For an iOS softphone with Push Notification, if an MBG outage occurs:

   a. When there is an incoming call to the phone, the PBX sends the push INVITE to the MBG's address to wake up the device to receive the call. The device cannot reach the MBG (that is down) and the call is dropped.
   b. The device will then try to connect the second MBG in the list. If the PBX registration is successful, the next push INVITE from the PBX will be sent to the second MBG and the push notification will be received by the device.
9. If the MiCollab server fails at any time during the failures described here, the calls are not affected and re-registration on the MBG continues automatically as described; that is, the softphone is not dependent on the MiCollab server in order to register.

Figure 6: Client Softphone Resiliency with MBG Cluster



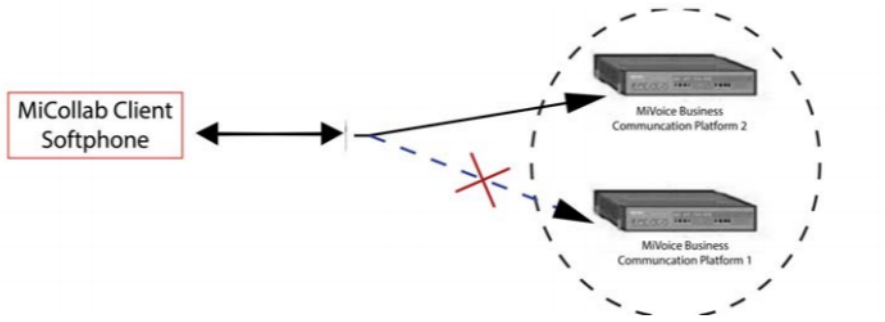
4.2 When the softphone is directly connected to MiVB

This section describes the behavior when the softphone is directly connected to MiVB, and the MiVB goes out of service.

1. If the MiVoice Business (MiVB) to which a softphone is registered is taken out of service, or if the connection to that MiVB is lost, an ongoing call is not affected (unless that call is going to a PSTN Trunk through that MiVB). However, mid call features do not work. The call can be ended using the End Call button. The ongoing call is maintained until the SIP session timer times out. When the call ends, the softphone automatically re-registers with the secondary MiVB. After the primary MiVB returns to service, the softphone automatically re-registers with the primary MiVB.

2. If there is no ongoing call at the time of MiVB outage, the softphone detects the loss of registration (either on its own or when the user tries to make a call) and automatically re-registers on the secondary MiVB.
3. Incoming calls cannot connect to the softphone until it automatically registers with the secondary MiVB. During this registration period, incoming calls are routed to voicemail if the user has a mailbox on a Mitel communications platform.
4. If the MiCollab server fails at any time during the failures described here, the calls are not affected and re-registration on the MiVB continues automatically as described; that is, the softphone is not dependent on the MiCollab server in order to register.

Figure 7: Client Softphone Resiliency with MiVB Cluster



4.3 TLS and SRTP support

The softphones support TLS and SRTP for audio when they are connected to the following communication platforms:

- MiVoice Border Gateway
- MiVoice Business
- MiVoice 5000 and
- MiVoice MX-ONE

TLS versions 1.1 and 1.2 support SIP traffic encryption as well as SRTP encryption (using SDES) of audio media streams. TLS 1.0 does not support this functionality.

Video stream is not encrypted or decrypted in MiCollab Release 7.1 or later.

All SIP-related security measures and SDES parameter negotiation in the Session Description Protocol (SDP) in the softphone are handled by the M5t SIP stack while all low-level certificate and key management is handled by OpenSSL 1.0.1 or later versions.

4.4 Supported RFCs

The MiCollab Client softphone supports the following Request for Comments (RFCs):

- RFC 1321 The MD5 Message-Digest Algorithm For authentication
- RFC 2782 A DNS RR for specifying the location of services (DNS SRV)
- RFC 2976 The SIP INFO Method
- RFC 3261 SIP v2.0: Session Initiation Protocol
- RFC 3263 Session Initiation Protocol (SIP): Locating SIP Servers (NAPTR)
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3265 SIP-Specific Event Notification (Subscribe/Notify)
- RFC 3311 The Session Initiation Protocol UPDATE Method
- RFC 3323 Privacy Mechanism
- RFC 3325 Private Extensions to the SIP for Asserted Identity within Trusted Networks
- RFC 3326 The Reason Header Field for the Session Initiation Protocol (SIP)
- RFC 3515 The Session Initiation Protocol (SIP) Refer Method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3725 Best Current Practices for Third Party Call Control
- RFC 3842 A Message Summary and Message Waiting Indication Event Package
- RFC 3891 The Session Initiation Protocol (SIP) 'Replaces' Header
- RFC 3892 The SIP Referred-By Mechanism
- RFC 3960 Early Media and Ringing Tone Generation
- RFC 4028 Session Timers
- RFC 4566 SDP: Session Description Protocol
- RFC 5923 Connection Reuse in the Session Initiation Protocol (SIP)

4.5 Limitations of MiCollab Client SIP Softphones

If a user manually disables the Softphone in the MiCollab Client and then later starts the MiCollab in an offline mode, where the MiCollab server cannot be reached, the Softphone toggle will be disabled until the server is reachable again. This behavior is intended to prevent two Clients from logging-in to the same DN at the same time.

Configuration 5

This chapter contains the following sections:

This sections describes the configuration that needs to be carried on the MiVoice Border Gateway and the MiVoice Business server for the resiliency feature to work.

5.1 Configuration for MiVoice Border Gateway

Prerequisites

- MiCollab Client installed with Release 7.0 or later
- MBGs installed, configured, and clustered
- DNS server and an available domain nam

Configure MiCollab Client Softphones and Specify FQDN

Specify the Fully Qualified Domain Name of the MBG cluster in the MiCollab Client Deployment Profiles.

1. Log in to the MiCollab Server Manager.
2. Under **Applications**, click **MiCollab Client Deployment**.

Note:

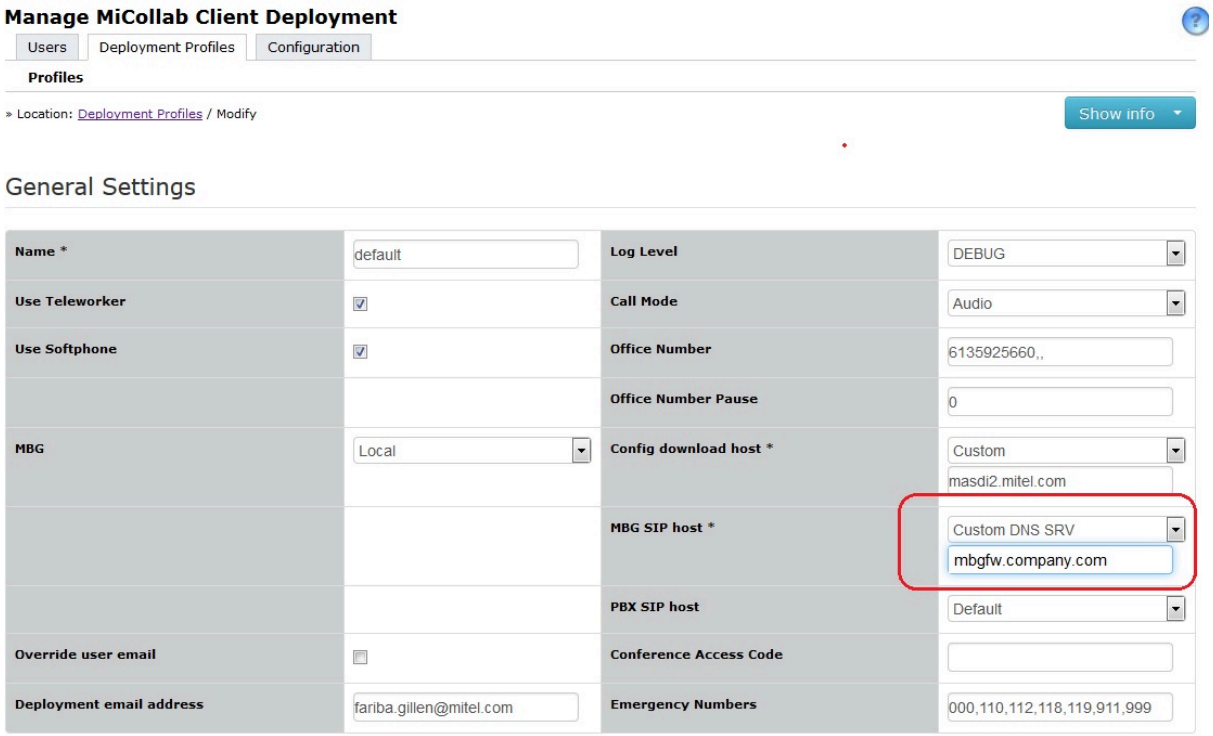
Configure the MiCollab Client softphones using the MiCollab Client Deployment blade. See ***MiCollab Client Deployment Online Help > Configuration Tab*** for instructions on configuring MiCollab Client Softphones.

3. On the **Deployment Profiles** tab, create client profiles with the FQDN of the MBG cluster.

   - Under **General Settings**, ensure that the **Use Teleworker** option is selected.
   - Set the MBG SIP host field to "Custom DNS SRV"
   - Enter the FQDN of the MGB cluster (for example: mbgfw.company.com).

> **Note**:
> For MiCloud deployments with MiCloud Management Portal (MMP), you will need to modify the Default Profile as described in Additional Configuration in MiCollab Client Deployment Service for MiCloud Deployment with MMP.

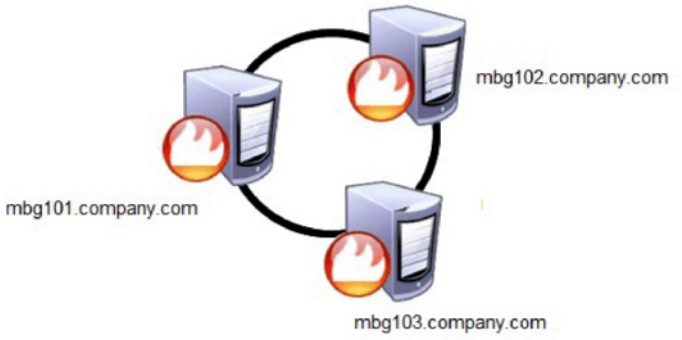
Figure 8: MBG Cluster FQDN



Configure the MiVoice Border Gateway cluster

Configure each MBG in the cluster with the hostnames of the other MBGs in the cluster. The following shows an example of a cluster in which each MBG is configured with the hostnames of the other MBGs in the cluster.

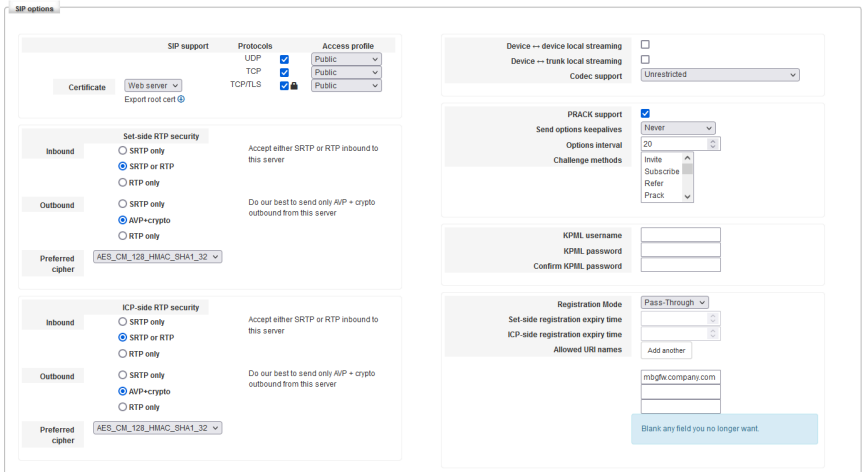
Figure 9: MBG Cluster with Hostnames (example)



Complete the following steps on *each MBG in the cluster*:

1. Log in to the MBG Server Manager (for example: mbg201.company.com).
2. Click **System Configuration > Settings**.
3. Under **SIP Options**, ensure that the TCP/TLS box is selected.
4. Under **Allowed URI names** (see Figure 10):
   - Click **Add another** to add the DNS SRV FQDN.
   - Enter the DNS SRV FQDN that you defined earlier.
5. Click **Save**.

Figure 10: MBG SIP Options



6. Add the following configuration override to each MBG:

Filename	Section	Parameter	Content
Filename	Section	Parameter	Content
tug.ini	proxy::sip_tcp	idle_timeout	1200
tug.ini	proxy::sip_tls	idle_timeout	1200

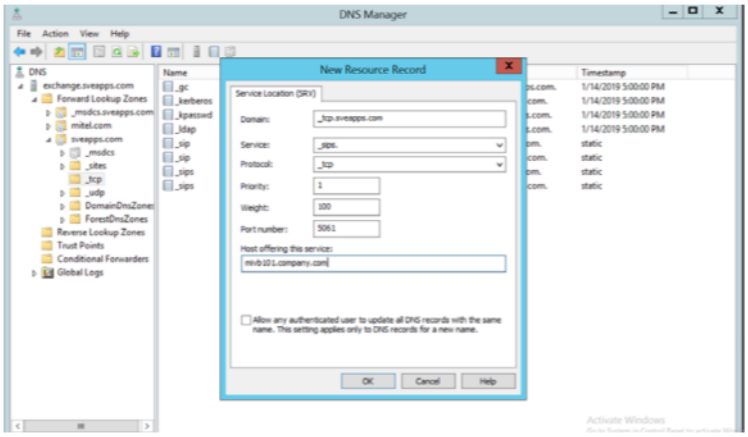
This configuration override will prolong the life of the mobile phone batteries.

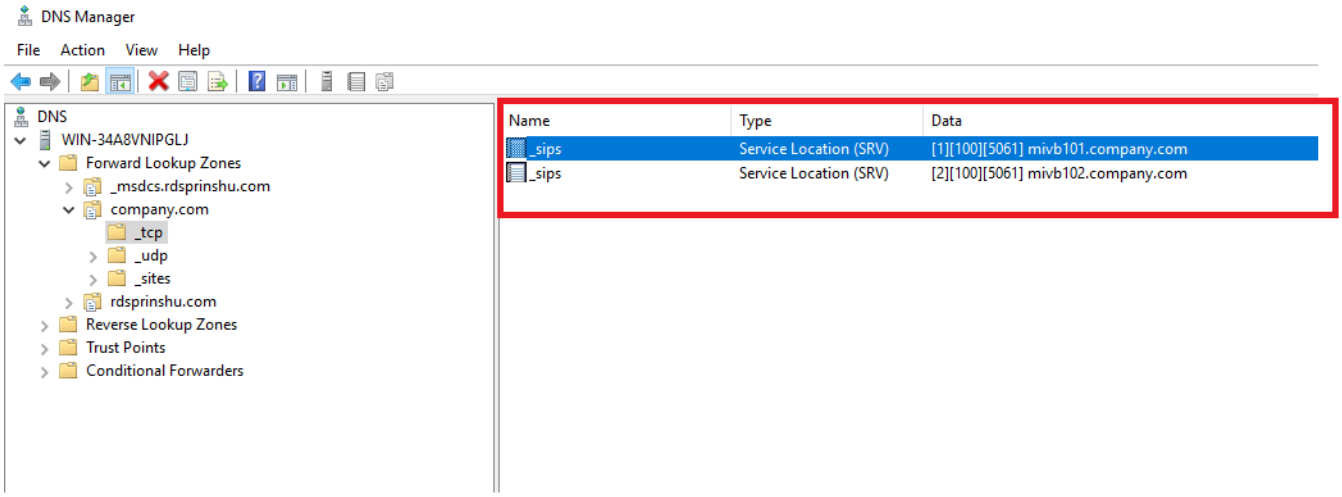
Configure DNS Server

Configure the DNS SRV records on the DNS server to provide the mapping between the MBG FQDN and the MBG cluster member hostname, and to specify priorities, weightings, port configuration, and Time to Live (TTL). "DNS SRV Entries for Resilient Softphones in Cloud Deployment" provides a mapping example

The following figure shows an example of the DNS server configuration settings.

Figure 11: DNS Server Configuration Settings





5.2 Configuration for MiVoice Business (without MiVoice Border Gateway)

Prerequisites

- MiCollab Client Release 7.0 or later installed.
- MiVBs installed, configured, and clustered
- DNS server and an available domain name.
- Teleworker set to OFF.

Configure MiVoice business

For information about configuring a resilient MiVoice Business system network, see the *Implementing Resiliency* section in the *Resiliency Guidelines*.

Configure MiCollab Client Softphones and specify FQDN

The following are the steps for setting up a MiCollab Client softphone to support SIP resiliency:

1. Log in to the MiCollab Server Manager.
2. Under **Applications**, click **User and Services**.
3. Click the **User** tab.
4. Click **Show all**. Users are listed alphabetically by their last names. Services appear as column headings along the top of the directory.

5. Click on the **Phones**tab. Choose the same **Secondary Element**that you specified in the MiVoice Business server.
6. Click **Save**.
7. Under **Applications**, click **MiCollab Client Deployment**.

> **Note**:
> Configure the MiCollab Client softphones using the MiCollab Client Deployment blade. See MiCollab Client Deployment Online Help > Configuration Tab for instructions on configuring MiCollab Client Softphones.

8. On the **Deployment Profiles** tab, create client profiles with the FQDN of the MiVB cluster.
   - Under **General Settings**, ensure that the **Use Teleworker** option is disabled.
   - Set the PBX SIP host field to "Custom DNS SRV"
   - Enter the FQDN of the MiVB cluster (for example mivbfw.company.com).

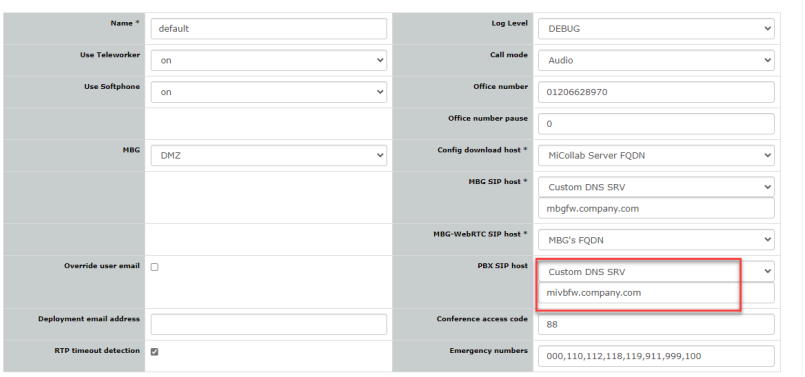


Figure 12: MiVB Cluster FQDN

Configure DNS Server

Configure the DNS SRV records on the DNS server to provide the mapping between the MiVB FQDN and the MiVB cluster member hostname, and to specify priorities, weightings, port configuration, and Time to Live (TTL). Figure 5 provides a mapping example.

Figure 14 shows an example of the DNS server configuration settings and Figure 14 shows an example of the SRV records.

Figure 13: DNS Server Configuration Settings

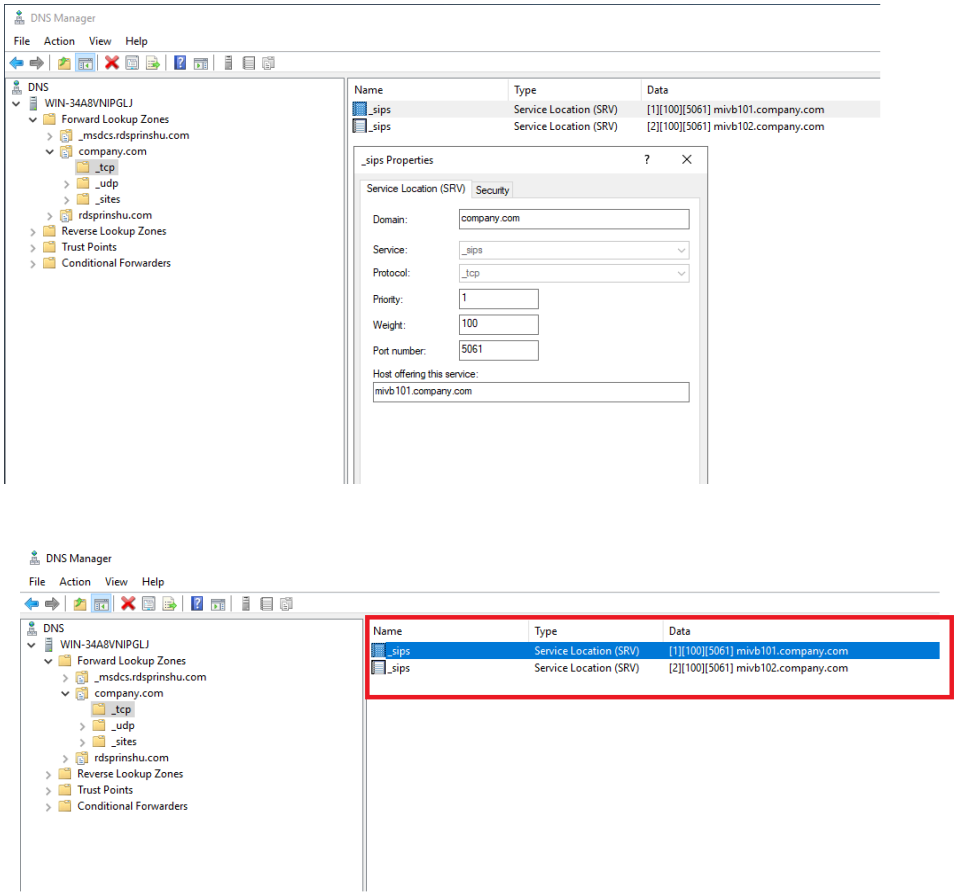


Figure 14: SRV Records List

5.3 Configuration for a network with softphone connections to both MBG and MiVB

In a network where some softphones connect directly to MiVB, while others connect through MBG, DNS SRV resiliency must be configured for both methods of access.

Prerequisites

- MiCollab Client Release 7.0 or later installed.
- MBGs and MiVBs installed, configured, and clustered
- DNS server and an available domain name.

Configure MiVoice border gateway

For information about configuring a resilient MiVoice Border Gateway system network, see Configuration for MiVoice Border Gateway.

Configure MiVoice business

For information about configuring a resilient MiVoice Business system network, see Configuration for MiVoice Business (without MiVoice Border Gateway).

Configure MiCollab Client Softphones and specify fqdn

The following are the steps for setting up a MiCollab Client softphone to support SIP resiliency:

1. Log in to the MiCollab Server Manager.
2. Under **Applications**, click **MiCollab Client Deployment**.

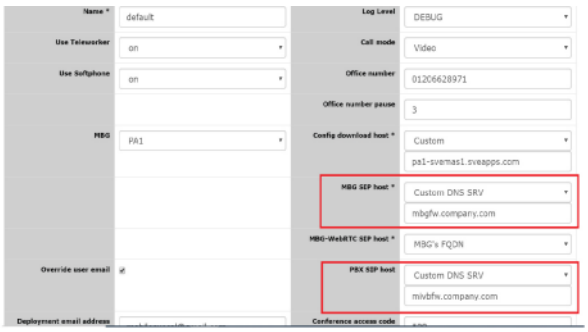
> **Note**:
> Configure the MiCollab Client softphones using the MiCollab Client Deployment blade. See*MiCollab Client Deployment Online Help* > *Configuration Tab* for instructions on configuring MiCollab Client Softphones.

3. On the **Deployment Profiles** tab, create client profiles with the FQDN of the MBG, and MiVB cluster.
   - Set the MBG SIP host field to "Custom DNS SRV"
   - Enter the FQDN of the MGB cluster (for example: mbgfw.company.com).
   - Set the PBX SIP host field to "Custom DNS SRV"
   - Enter the FQDN of the MiVB cluster (for example: mivbfw.company.com).

To connect a softphone to the network through MBG, Teleworker must be set to **ON**. From the MiCollab Client, go to **Settings** > **General** > **Use Teleworker**.

To connect a softphone to the network through MiVB, Teleworker must be set to **OFF**. From the MiCollab Client, go to **Settings** > **General** > **Use Teleworker**.

Figure 15: MBG and MiVB Cluster FQDN


Name *
default
Log Level
DEBUG
Use Teleworker
on
Call mode
Video
Use Softphone
on
Office number
01206628971
Office number pause
3
MBG
PA1
Config download host *
Custom
pa1-svemas1.sveapps.com
MBG SIP host *
Custom DNS SRV
mbgfw.company.com
MBG-WebRTC SIP host *
MBG's FQDN
Override user email
PBX SIP host
Custom DNS SRV
mivbfw.company.com
Deployment email address
Conference access code

MiCloud Deployments with Non-Resilient and Resilient Devices

6

This chapter contains the following sections:

Overview

For MiCloud deployments with MMP, use the same external MBG cluster FQDN for both the following:

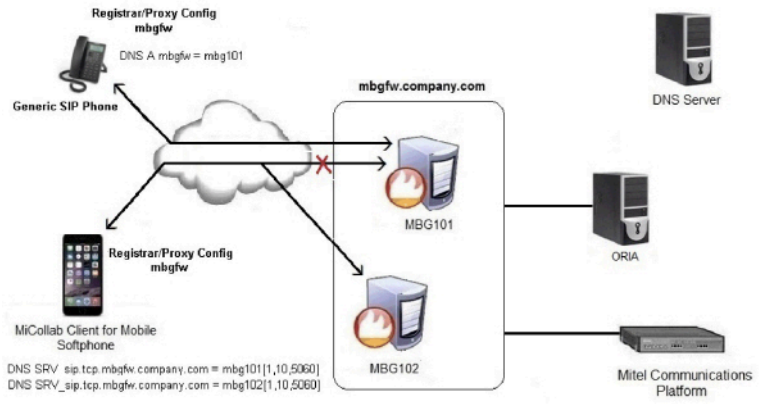
- non-resilient devices such as generic SIP phones (with DNS A records)
- resilient MiCollab softphones (with DNS SRV records).

This section illustrates how to configure a MiCloud deployment using a single MBG external hostname field. This solution is purely a DNS programming exercise.

6.1 Deployment Example

The following figure shows a resilient MiCollab softphone and a non-resilient generic SIP phone.

Figure 16: MiCloud Deployment with Non-Resilient and Resilient Devices



6.2 Configure MMP with FQDN/IP Address of MBG

1. Log in to the MMP administration interfaces.
2. Access the **Home** > **MiVoice Border Gateways** > **Register MiVoice Border Gateway Cluster** page.
3. Configure the Public Facing FQDN/IP address of the external MBG cluster (to which the external devices connect):

   - "FQDN of External MBG Cluster — MiVoice Business Platform" shows a MiVoice Business platform deployment
   - "FQDN of External MBG — MiCollab Platform" shows a MiCollab platform deployment

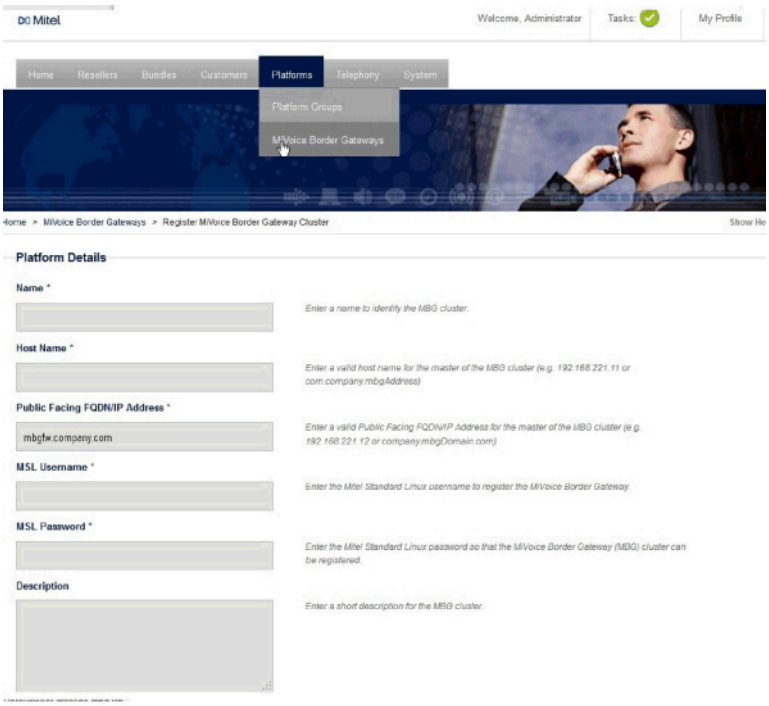
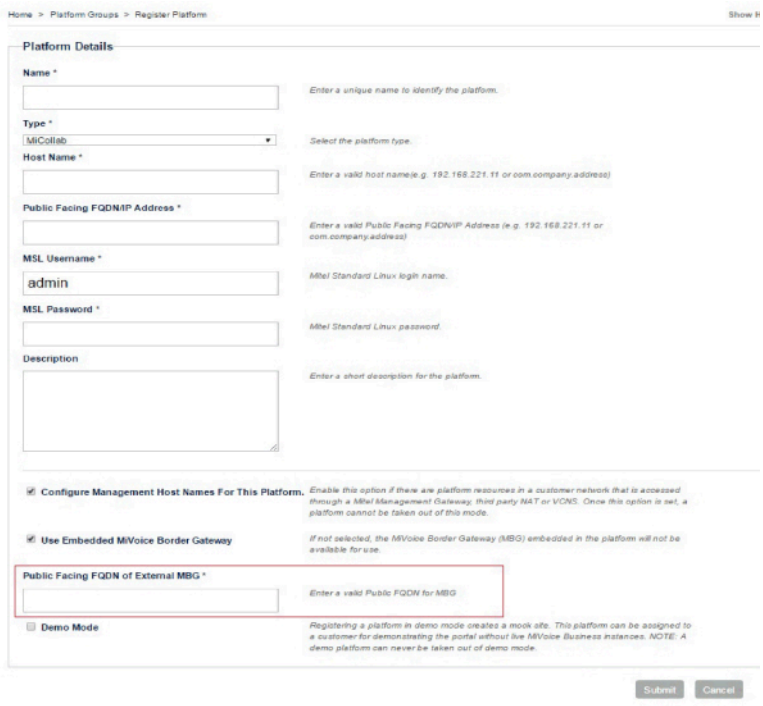


Figure 17: FQDN of External MBG Cluster — MiVoice Business Platform

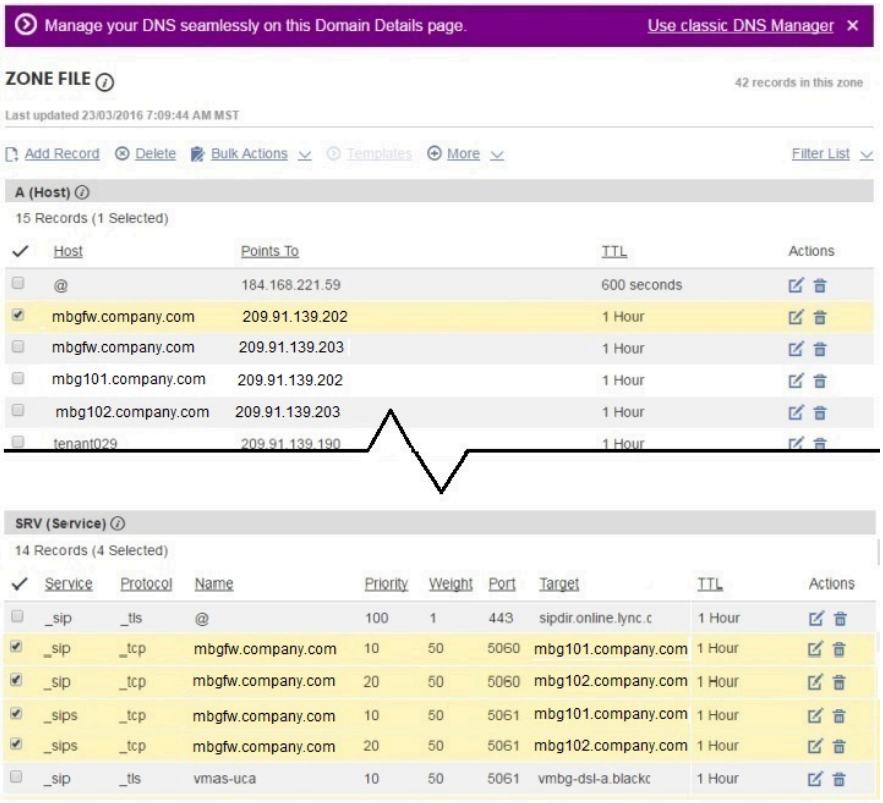
Figure 18: FQDN of External MBG — MiCollab Platform



6.3 Configure DNS Server

The foolowing figure shows an example of the DNS A and resilient DNS SRV entries on a GoDaddy server:

Figure 19: Configuration Example on GoDaddy


Manage your DNS seamlessly on this Domain Details page.
Use classic DNS Manager
ZONE FILE
42 records in this zone
Last updated 23/03/2016 7:09:44 AM MST
Add Record
Delete
Bulk Actions
Templates
More
Filter List
A (Host)
15 Records (1 Selected)
Host
Points To
TTL
Actions
@ 184.168.221.59 600 seconds
mbgfw.company.com 209.91.139.202 1 Hour
mbgfw.company.com 209.91.139.203 1 Hour
mbg101.company.com 209.91.139.202 1 Hour
mbg102.company.com 209.91.139.203 1 Hour
tenant029 209.91.139.190 1 Hour
SRV (Service)
14 Records (4 Selected)
Service
Protocol
Name
Priority
Weight
Port
Target
TTL
Actions
_sip _tls @ 100 1 443 sipdir.online.lync.c 1 Hour
_sip _tcp mbgfw.company.com 10 50 5060 mbg101.company.com 1 Hour
_sip _tcp mbgfw.company.com 20 50 5060 mbg102.company.com 1 Hour
_sips _tcp mbgfw.company.com 10 50 5061 mbg101.company.com 1 Hour
_sips _tcp mbgfw.company.com 20 50 5061 mbg102.company.com 1 Hour
_sip _tls vmas-uca 10 50 5061 vmbg-dsl-a.blackc 1 Hour

Additional Configuration in MiCollab Client Deployment Service for MiCloud Deployment with MMP 7

The built-in SIP softphone of the MiCollab Client application supports SIP resiliency with an MBG, such that if the call signaling path is disrupted or the MBG is taken out of service, the softphone registers with an alternate MBG to regain service.

By default, MMP pushes the host addresses FQDNs of the configured platforms (example: MiCollab, MBG, MiVoice Business) to the MiCollab Deployment service and the MiCloud \MMP System administrator does not need to provision the deployment profile on the MiCollab Deployment service in advance.

In situations where mobile softphone resiliency is required, then you must log in to the MiCollab Client Deployment service and change the “SIP Port” field of the Softphone Settings to a value of zero (0) in the default configuration profile. This must be completed before the MMP bundle that contains the MiCollab (Next Gen) SIP Softphone is assigned to a customer in MMP (see the following figure).

Figure 20: MiCollab Client Deployment Service — SIP Port Configuration