



Mida Deployment Guide

Mida C³ - Cloud Contact Center For Microsoft Teams

Document Version: 1.1



Document Information

Revision	Date	Description	Updates	Product Version
1.0	01/09/2021	First approved version of this manual	-	3.1.0
1.2	22/04/2022	Minor review	Add Multi-Tenants section	3.1.5

Table of Contents

1.	Introduction.....	3
1.1	Legal Statements	3
1.2	Preface.....	3
1.3	Audience.....	4
1.4	Notations	4
1.5	Operations Flow	4
2.	Deploying Mida C ³ – Cloud Contact Center via Azure Marketplace.....	6
2.1	Azure Marketplace	6
2.2	Basic.....	7
2.3	Disks.....	9
2.4	Networking	11
2.5	Management	13
3.	License application & install updates	17
3.1	License Request and Setup.....	17
3.2	Preference settings.....	19
3.3	Update a new release	20
4.	Configure SBC	24
4.1	Configurations – Ribbon SBC SWe Lite	25
4.2	Connect Mida C ³ - Cloud Contact Center and PSTN to Ribbon SBC SWe Lite	26
5.	Multi-tenant systems: add tenants.....	38

1. Introduction

1.1 Legal Statements

THE SPECIFICATION AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

ACCESS TO THE SOFTWARE REQUIRES THE PURCHASE OF A VALID LICENSE. Mida Solutions OFFERS SUPPORT AND SOFTWARE BUG FIXES IF THE CUSTOMER IS UNDER A VALID SUPPORT AND MAINTENANCE CONTRACT. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR VENDOR REPRESENTATIVE FOR FURTHER INFORMATION.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. Mida Solutions DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

IN NO EVENT SHALL Mida Solutions OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF Mida Solutions OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

All trademarks mentioned in this document are the property of their respective owners.

Any Internet Protocol (IP) address and phone/fax number used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Mida Platform

© 2022/2025 Mida Solutions, All rights reserved.

Mida C³ - Cloud Contact Center for Microsoft Teams

© 2022/2025 Mida Solutions, All rights reserved.

1.2 Preface

This document is part of the official documentation of Mida Solutions products and details functionalities, user interface, options, and working modes in detail. The system allows the user to configure all system functions using a simple and intuitive WEB interface. Please refer to the reference table for a complete list of documents relevant to system configuration.

1.3 Audience

The present document addresses both end-users and system administrators of the products.

1.4 Notations



This document highlights, where possible, the main parameters and operations through **bold** or *italics* text and all parts that might be critical during system configuration or use. Critical parts are also marked with the Warning symbol reported here on the left.

1.5 Operations Flow

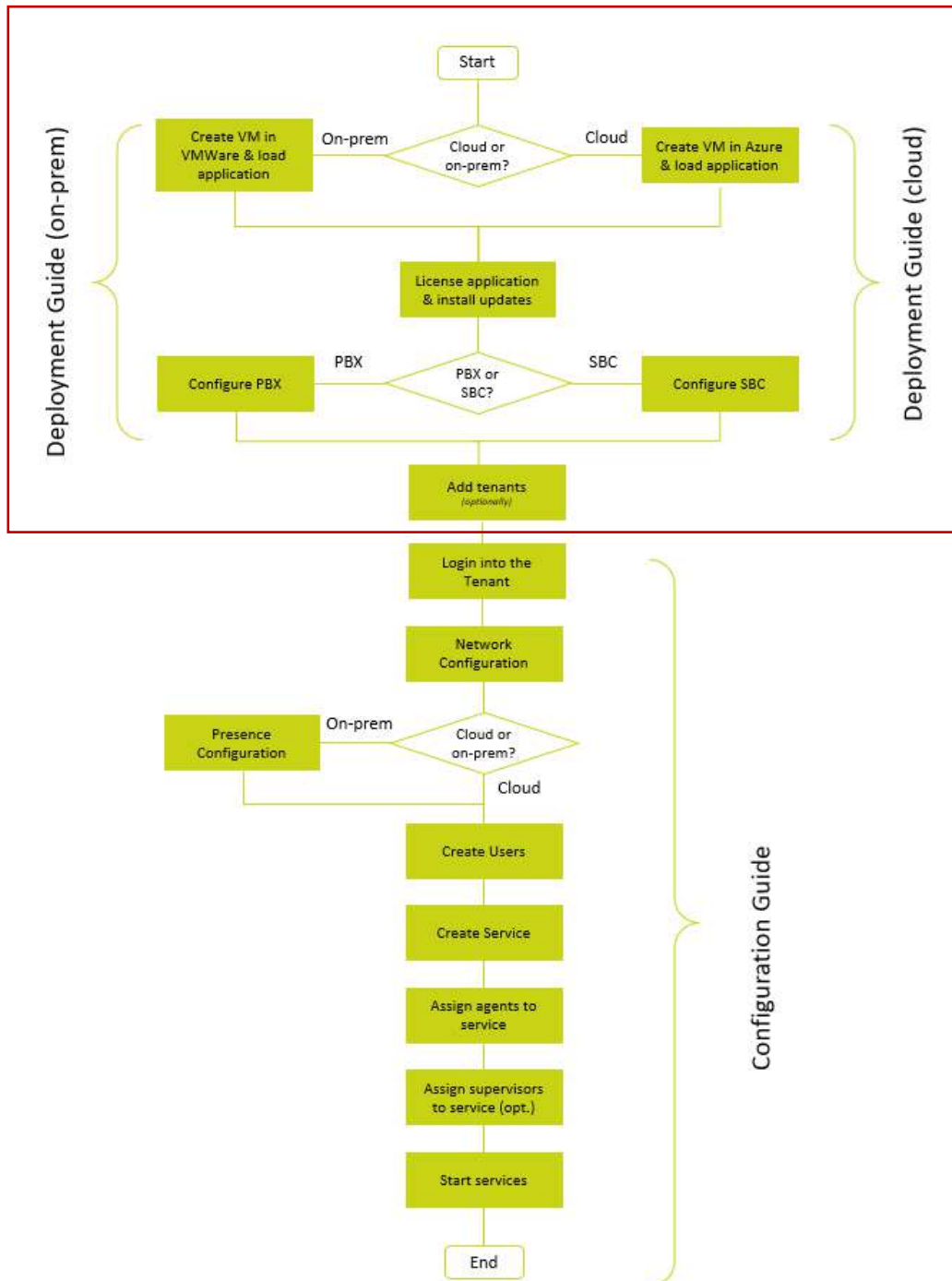
The flow chart represented below gives a step-by-step view of the actions required to complete set up Mida C³ – Cloud Contact Center. This guide covers the initial part of the deployment, including the following logical steps:

- Creation of the VM in MS Azure
- Deployment of the C³ – Cloud Contact Center image onto the VM
- Licensing of C³ – Cloud Contact Center
- Installation of any required application update (may not be required)
- Configuration of the SBC

The second part, which covers the full configuration of the application, is detailed in another manual (see [Mida C³ – Configuration Guide - Azure](#))

The flow chart will be visible at various points along with this manual, to inform which step is being described.

This Guide is intended to help you deploy Mida Solutions' applications. Please be aware that in order to use Mida's products you should also complete the instructions included in the [Configuration Guide](#) of the product you purchased.



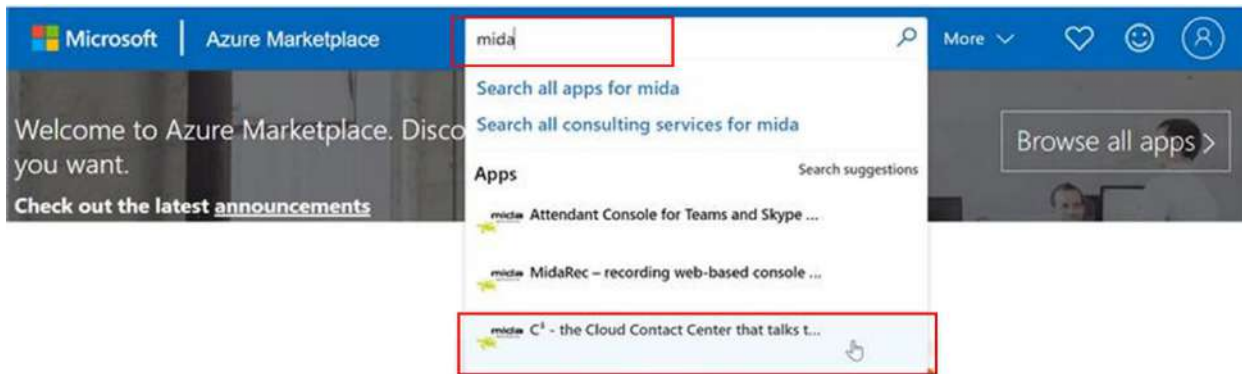
2. Deploying Mida C³ – Cloud Contact Center via Azure Marketplace

Deploying Mida C³ – Cloud Contact Center via Azure Marketplace is very simple as it comes almost entirely pre-configured.

Follow the next steps to complete the deployment successfully.

2.1 Azure Marketplace

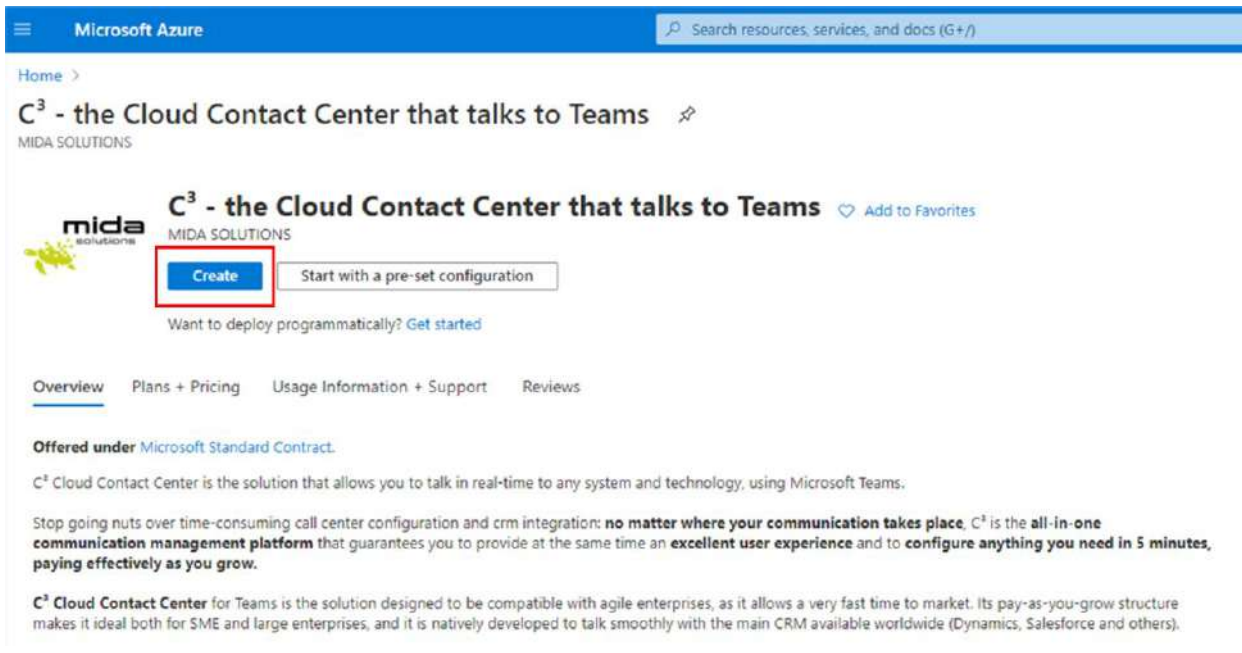
1. Access the [Azure Marketplace](#);
2. In the menu on the top, search for **Mida C³ – Cloud Contact Center**



3. Click on **Mida C³ – the Cloud Contact Center that talks to Teams**,
4. Click on **Get it now** and then on continue



5. Click on **Create**;



The procedure will guide you through the steps required to create your virtual machine in Microsoft Azure and install Mida C³ - Cloud Contact Center. The display will show a window with several tabs: each tab is a step forward in the deployment process, as detailed in the next Sections.



Note: the whole procedure assumes you can create a Virtual Machine in Microsoft Azure: this usually requires some form of contract to be signed with Microsoft.

2.2 Basic

In the **Basic** tab, configure the fields as:

- a. **Resource group**: select the desired resource group or create a new group (as in the figure below);

Home > C³ - the Cloud Contact Center that talks to Teams >

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Image *

[See all images](#)

Azure Spot instance ☐

Size * [See all sizes](#)

Resource group creation dialog:

A resource group is a container that holds related resources for an Azure solution.

Name *

- b. **Virtual machine name:** insert your preferred name (in the figure below “C³-Deployment”);
- c. **Region:** select your Country area
- d. **Size:** this field should be automatically set to the minimum required size for the C³ – Cloud Contact Center to work. The table below gives further information about the VM specifications based on the requirements of the contact center in terms of agents and channels. In case of doubts, please contact support@midasolutions.com to verify the best size for your needs.

VM configuration	Max number of simultaneously logged agents + supervisors	Max number of channels
F2S (2vCPU, 4GB RAM, 160GB vHDD)	200	150
F4S (4vCPU, 8GB RAM, 320GB vHDD)	400	300
F8S (8vCPU, 16GB RAM, 640GB vHDD)	800	600

- e. **Authentication type:** select **Password** and insert the desired credentials.

Leave the other field by default.

Home > C3 - the Cloud Contact Center that talks to Teams >

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region *

Availability options

Image * [See all images](#)

Azure Spot instance ☐

Size * [See all sizes](#)

Administrator account

Authentication type ☐ SSH public key ☒ Password

Username *

Password *

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ☐ None ☒ Allow selected ports

Select inbound ports *

Warning: This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[See all images](#)

Azure Spot instance ☐

Size * [See all sizes](#)

Administrator account

Authentication type ☐ SSH public key ☒ Password

Username *

Password *

Confirm password *

2.3 Disks

1. Proceed by clicking on **Next: Disks** and select the desired **OS disk type**. No other settings are required.

Home > C² - the Cloud Contact Center that talks to Teams >

Create a virtual machine

Basics **Disks** Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more C²](#)

Disk options

OS disk type *

Standard SSD

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Encryption type *

(Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility

☐

Ultra disk is available only for Availability Zones in north europe.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk	Attach an existing disk			

Advanced



Note: this step creates a minimal disk that is good enough for PoC or trial purposes, but would not be sufficient for a fully operational system. The table below provides the guidelines for sizing the disk based on the number of channels and users. Please refer to your Mida Solutions reference person if you have any doubt about its interpretation or if your requirements are not included.

VM configuration	Max number of simultaneously logged agents + supervisors	Max number of channels
2vCPU, 4GB RAM, 160GB vHDD	200	150
4vCPU, 8GB RAM, 320GB vHDD	400	300
8vCPU, 16GB RAM, 640GB vHDD	800	600

If you would also deploy Mida Recorder, the disk size should be selected based on the traffic volume and retention period. As a rule of thumb, 1 Erlang of traffic under an average usage (8 busy hours/day) requires about 8 Gbyte of storage every month (30 days). You may try to use this rule to size the additional disk required by the recorder, but it's strongly suggested that you consult your Mida Solutions reference person to get advice.

To compute the required disk size, follow these steps:

- Determine the peak Erlang rate **E** of your network. This value is used to license the recorder, so it should be available from the license itself or by contacting your Mida Solutions representative
- Determine the number of busy hours **BH** for your network. This is the number of hours where you expect to have traffic to be recorded
- Determine the retention period **RP** for the recorded calls, i.e. how long such calls must be kept in the Recorder's storage

- Compute the required storage (in GB) using the following formula:

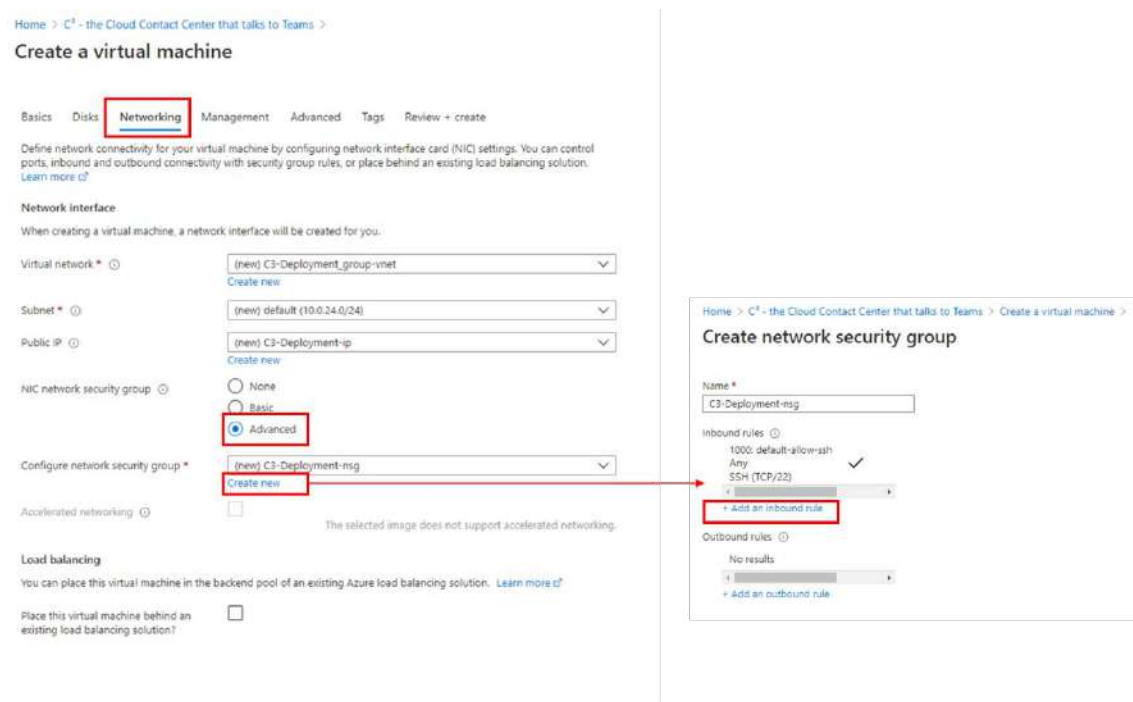
$$S = \frac{E \times BH \times RP \times 34560}{1024 \times 1024}$$

2. Proceed by clicking on **Next: Networking**;

2.4 Networking

In the **Networking** tab:

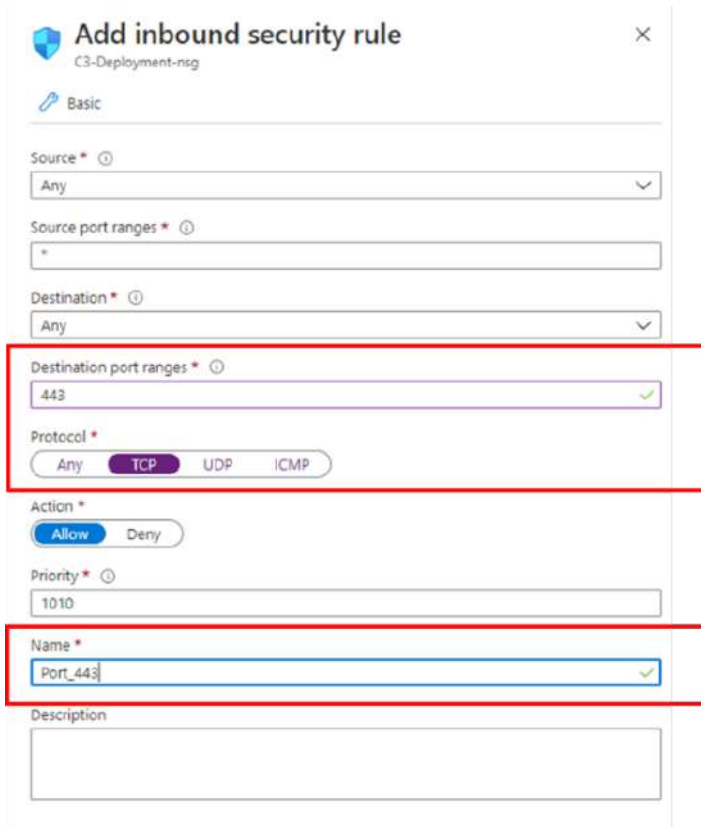
- Virtual network:** select the desired virtual network from the dropdown menu;
- NIC network security group:** select advanced and create a new security group.
The network security group allows defining which network ports should be opened. You will have to configure them as detailed below.
To start, click **Create new** in the **Configure network security group** option.



To add the inbound security rules, click on **Add an inbound rule** and, in the **Add inbound security rule** section insert the **Destination port ranges**, select the **Protocol** and give the new port the desired **Name**. Do this for all the ports listed in the table below.

Ports to be opened are:

- 443/tcp,
- 80/tcp,
- 4573/tcp,
- 5060/tcp,
- 10000-20000/udp,
- 161/udp, 5060/udp,
- 5038/tcp,
- 3535/tcp,
- 3536/tcp.



Add inbound security rule
C3-Deployment-nsg

Basic

Source * ⓘ
Any

Source port ranges * ⓘ
*

Destination * ⓘ
Any

Destination port ranges * ⓘ
443

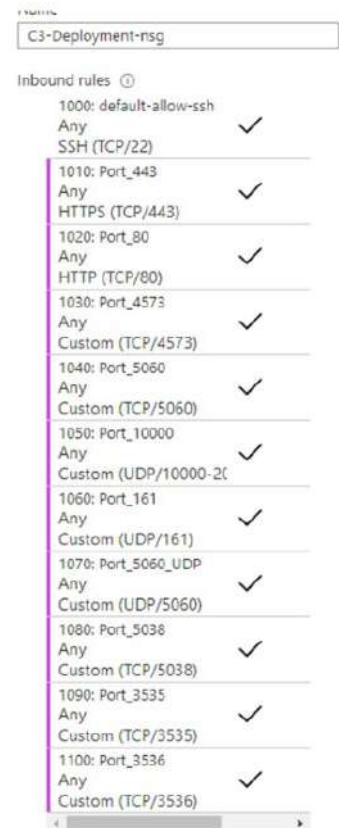
Protocol *
Any TCP UDP ICMP

Action *
Allow Deny

Priority * ⓘ
1010

Name *
Port_443

Description



C3-Deployment-nsg	
Inbound rules ⓘ	
1000: default-allow-ssh	✓
Any SSH (TCP/22)	
1010: Port_443	✓
Any HTTPS (TCP/443)	
1020: Port_80	✓
Any HTTP (TCP/80)	
1030: Port_4573	✓
Any Custom (TCP/4573)	
1040: Port_5060	✓
Any Custom (TCP/5060)	
1050: Port_10000	✓
Any Custom (UDP/10000-20000)	
1060: Port_161	✓
Any Custom (UDP/161)	
1070: Port_5060_UDP	✓
Any Custom (UDP/5060)	
1080: Port_5038	✓
Any Custom (TCP/5038)	
1090: Port_3535	✓
Any Custom (TCP/3535)	
1100: Port_3536	✓
Any Custom (TCP/3536)	

Once completed, the opened port list should look as shown in the picture on the right.

If the configuration is completed, click **OK** and then **Next: Management**.

2.5 Management

1. In the **Management** tab, just select the desired **Boot diagnostic**

Home > C³ - the Cloud Contact Center that talks to Teams >

Create a virtual machine


Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.


Azure Security Center
Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
[Learn more](#)

✔ Your subscription is protected by Azure Security Center basic plan.


Monitoring

Boot diagnostics 


☒ Enable with managed storage account (recommended)
☐ Enable with custom storage account
☐ Disable


Enable OS guest diagnostics  ☐

Identity


System assigned managed identity  ☐

Azure Active Directory

Login with AAD credentials (Preview)  ☐

 This image does not support Login with AAD.

Auto-shutdown

Enable auto-shutdown  ☐

[Review + create](#) [< Previous](#) [Next: Advanced >](#)

2. Click on **Review + create** once complete.
3. In the **Review + create** page, review all Virtual Machine details and click on **Create** to proceed with the Virtual Machine deployment.

Home > C³ - the Cloud Contact Center that talks to Teams >

Create a virtual machine

Validation passed

Basics Disks Networking Management Advanced Tags **Review + create**

PRODUCT DETAILS

C³ - the Cloud Contact Center that talks to Teams
by MIDA SOLUTIONS
[Microsoft Enterprise Contract](#) | [Privacy policy](#)

Standard F2s
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Not covered by credits ⓘ
0.0000 EUR/hr

Subscription credits apply ⓘ
0.0953 EUR/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (2) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Preferred e-mail address *

Preferred phone number *

Create < Previous Next > [Download a template for automation](#)

Home >

CreateVm-midasolutions.midalcc01-midalcc01-20210122121912 | Overview

Deployment

Search (Ctrl+F)

Overview Inputs Outputs Template

We'd love your feedback →

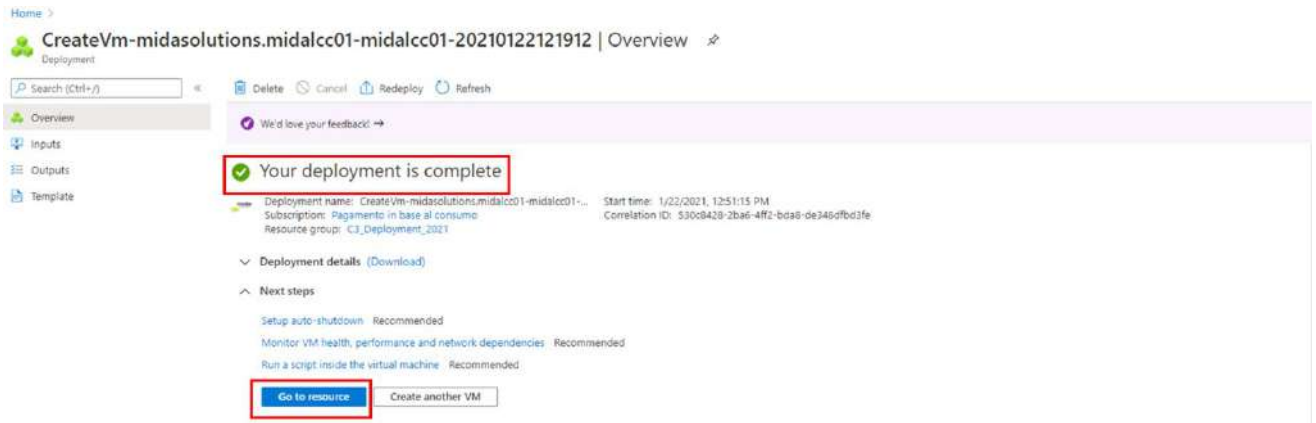
Deployment is in progress

Deployment name: CreateVm-midasolutions.midalcc01-midalcc01-... Start time: 1/22/2021, 12:51:15 PM
Subscription: Pagamento in base al consumo Correlation ID: 530c6428-2ba6-4ff2-bda8-de348dfbd3fe
Resource group: C3_Deployment_2021

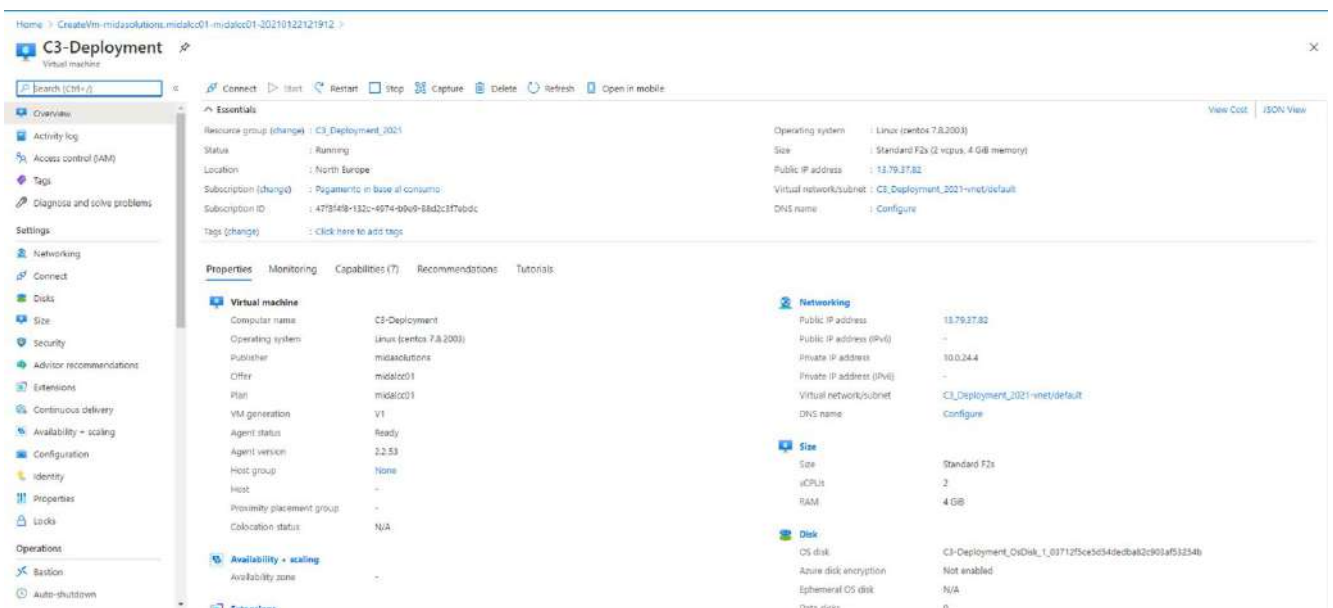
Deployment details (Download)

Resource	Type	Status	Operation details
C3-Deployment-ip	Microsoft.Network/publicAddresses	OK	Operation details
C3_Deployment_2021-vnet	Microsoft.Network/virtualNetworks	Created	Operation details
C3-Deployment-nsg	Microsoft.Network/networkSecurityGroups	OK	Operation details

This may take a while and the system will notify you once the procedure is complete.

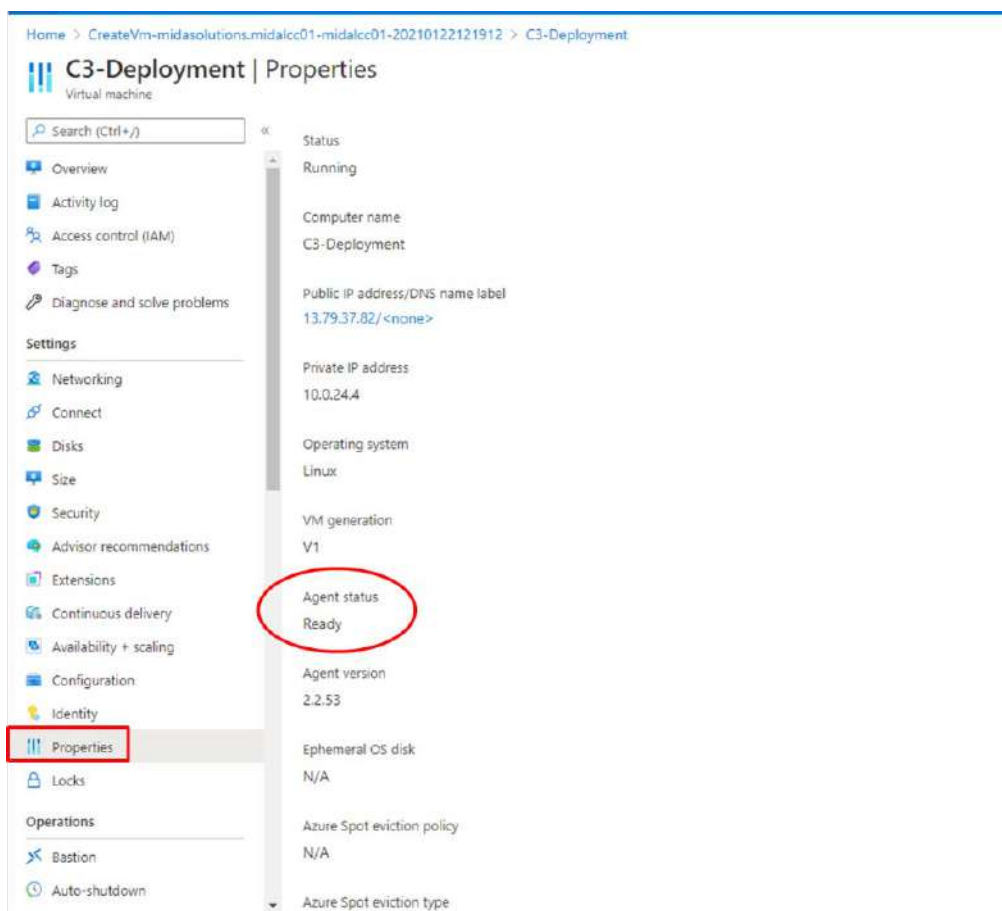


When the deployment is completed, click **Go to resource**.
 The page below will appear.



Please note that to use the VM, Microsoft Azure needs to activate an agent. If the agent activation is not automatically configured, open the created virtual machine from the virtual machine list, and go to **Setting > Properties**.

In Properties, you can see if the agent status is ready, as in the figure below. If not, you need to activate it.



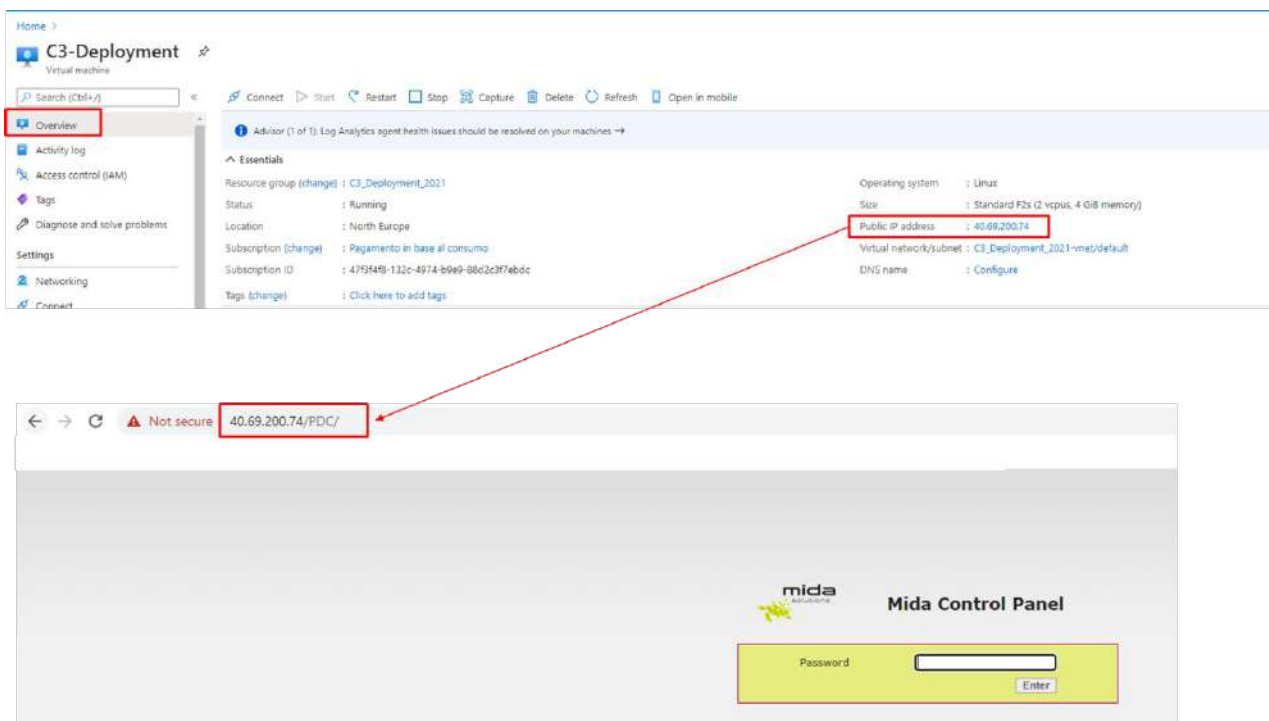
3. License application & install updates

3.1 License Request and Setup

To use the Mida products you have chosen, you need to install a valid system license.

Please note that the Virtual Machine you download from Azure Marketplace comes already with 30 days trial license with some limitations. It is for evaluation purposes only. If you plan to have a final deployment you should follow the procedures below to obtain a valid perpetual license.

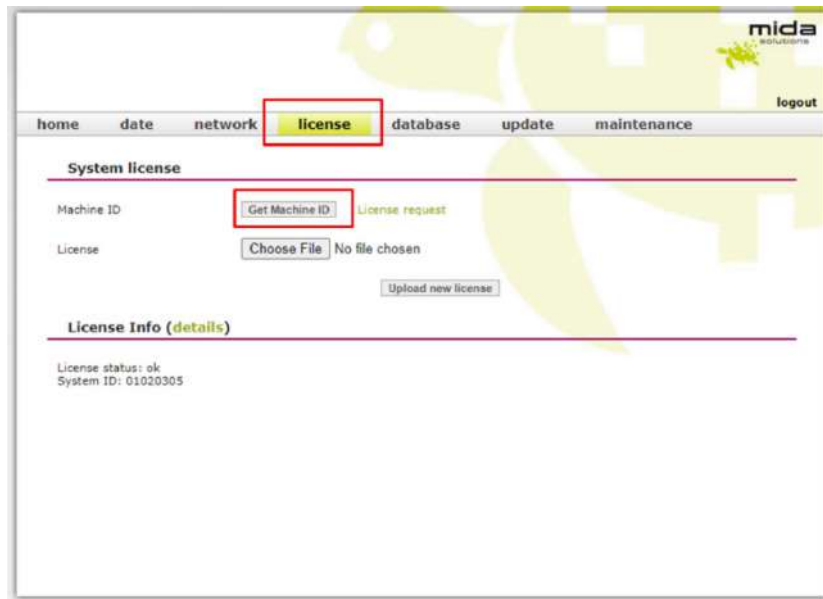
The Virtual Machine has a Public IP address. You can find it in the overview panel. Copy and paste it into a web browser, adding “/PDC/”, as in the figure below.



The first-access password is admin, do not forget to change it for future login.

Open the “license” tab (see picture below).

Press **Get Machine ID**.



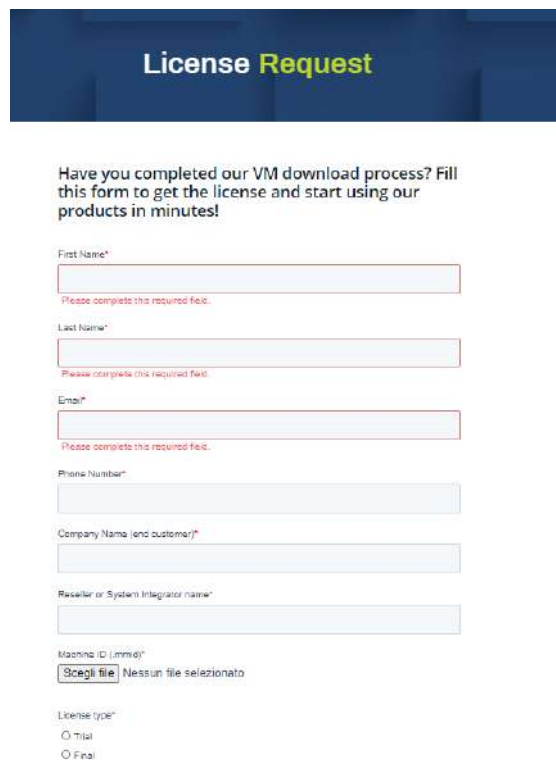
Download the MidaGetLicense.mmidi file from the system: this is required to submit a license request. Now you should get in contact with Mida Solutions to get your license. To do so, use the online **license request** form: <http://www.midasolutions.com/support/license-request/>

The form (see the following picture) shall be filled in reporting all relevant information such as your name and surname, email address, phone number, end customer company name, and reseller or System integrator you prefer to involve.

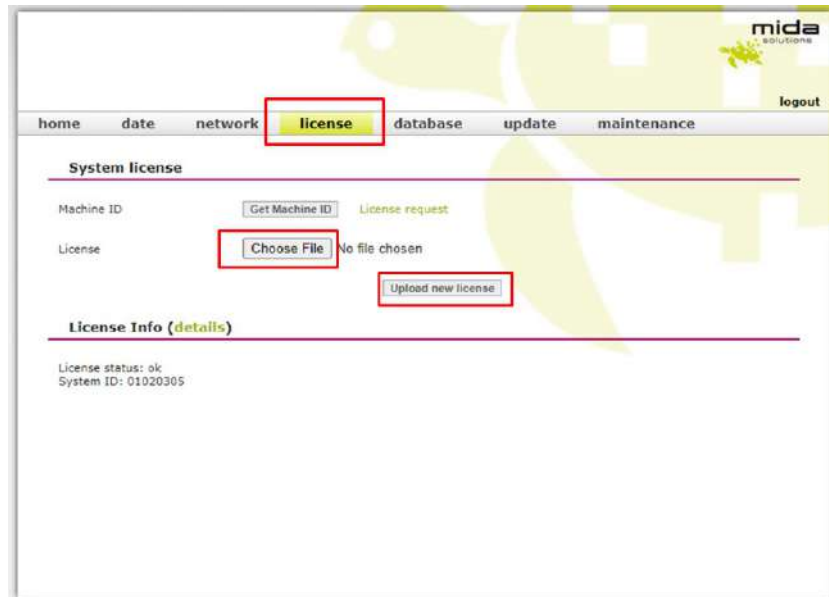
Upload the Machine ID file you just downloaded (.mmidi) and specify the license type you are requesting: trial or final license. Click on the authorization flag, insert optional notes and press submit.

You will receive immediately a confirmation email and Mida will process your request as soon as possible.

Once you have received the **license file** from Mida Solutions, go back to the “/PDC/” web page you used to generate the .mmidi file and upload it.

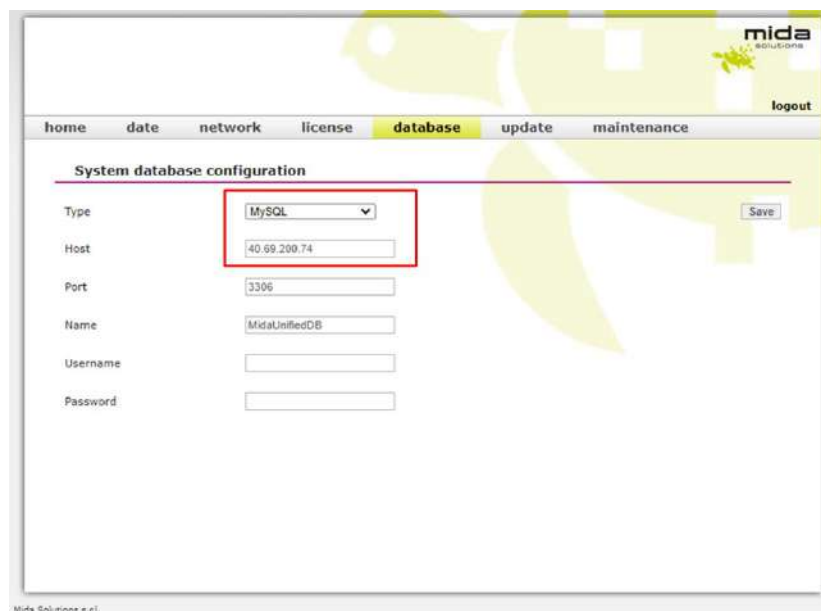


To do so, press **Upload new license** (as in the picture below).



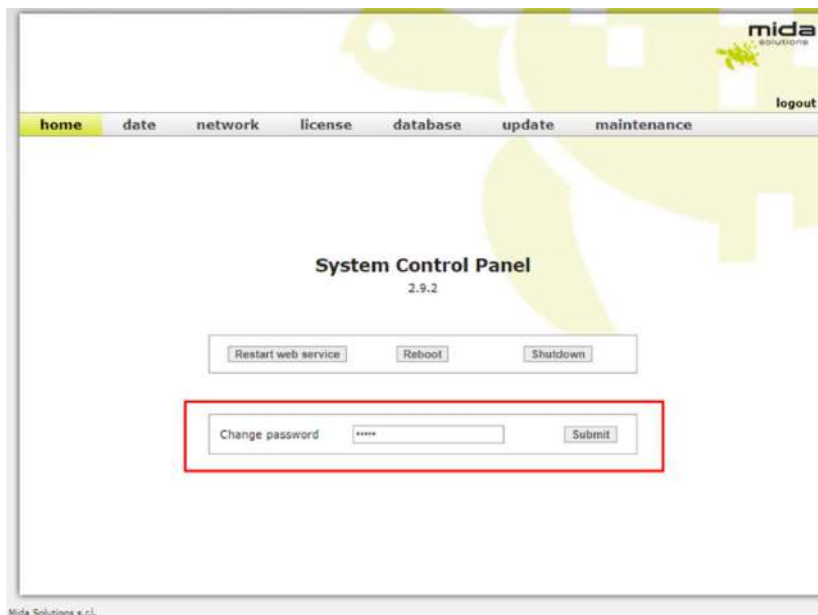
3.2 Preference settings

In the database area, you can configure the application's database. **Mida products normally make use of an internal database** (as in the picture below), **but can also use an external one.**



If you decide to use the internal database, don't change the default settings that appear on the page. Otherwise, select the database type (it could be MySQL or MS SQLServer) and provide values for all the required parameters.

To change the default password for the /PDC/, you should now go to the home section and set the new one.



Now you have correctly set the license and you can start using Mida Solutions' products. If you like, you can customize other sections (like "date", "maintenance") or you can leave them by default.

For further details on the Control Panel please refer to "Mida Appliance-Administration Manual".

For further details on the main platform portal and administration options please refer to "Mida Unified Portal-Administration & User Manual".

3.3 Update a new release

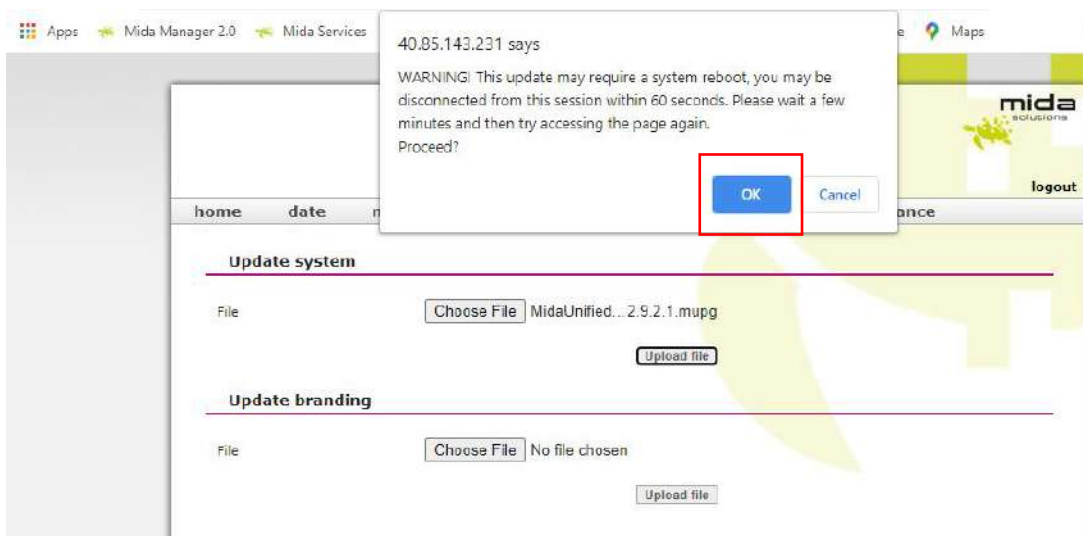
To make sure the installed version is the last one, **contact Mida Solutions at licensing@midasolutions.com**. In the event there is a more recent release available, we will send you a link from which you can download the image file (.mupg) to update it. You should then go to the "update" section of the PDC to upload and install it (as in the picture below).

The update process normally requires some minutes, please wait and follow the instruction.



The image displays two screenshots of the Mida Solutions web application interface, specifically the 'update' tab. The top screenshot shows the 'Update system' section with a 'Choose File' button and 'No file chosen' text. The bottom screenshot shows the same section with a file named 'MidaUnified...2.9.2.1.mupg' selected. Both screenshots show the 'Update branding' section below it, which also has a 'Choose File' button and 'No file chosen' text. The 'update' tab is highlighted in the navigation bar.

After clicking on “upload file” a pop-up will appear to warn you the upload may require a system reboot to be completed. Click ok and then wait for the update to be completed, the process might take some minutes.



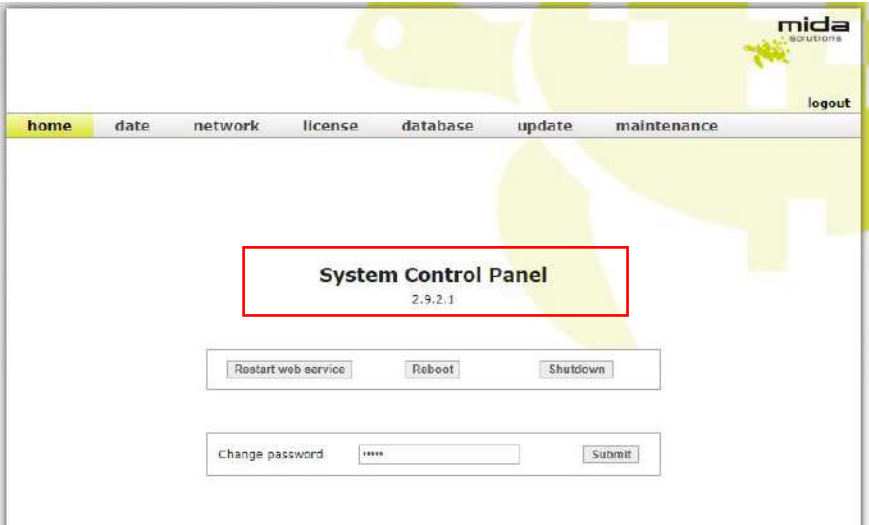
When the file is correctly uploaded, you will see a written notice. Now the update process will start.



Update in progress...

The system is currently updating, please wait...

Once the update has finished, in the "home" section you will see the new system release (as in the picture below). It is always a good practice to reboot the VM after updating it with a new release.



4. Configure SBC

For Microsoft Teams Direct Routing, Mida C³ - Cloud Contact Center could be integrated into the following certificated SBCs:

- Ribbon
- AudioCodes
- Oracle
- Cisco
- Avaya
- Italtel
- Nokia
- Patton

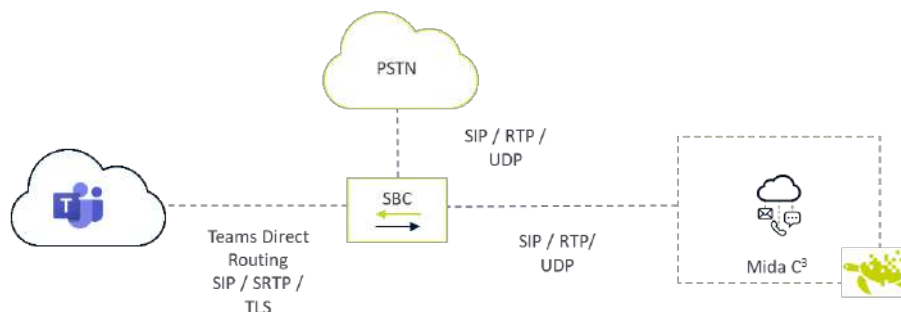
In this guide, Mida helps you to perform a **basic configuration of the Ribbon SWe Lite SBC and connect it to Mida C³ - Cloud Contact Center for Teams.**



Of course, both Teams and the SBC can have a much more complex configuration to address specific needs in the customer's architecture. Fields not mentioned, in this guide, can maintain default values.

There are three main steps you should do:

- Connect the SBC to Teams
- Connect Mida C³ - Cloud Contact Center to the SBC
- Connect the PSTN to the SBC



Team users must have a phone number in E.164 format, with the "+" character at the beginning. The same applies to all numbers that a Teams user calls through the PSTN network. So, the simplest solution is to configure the agents in C³ directly with their telephone number in Teams, which will be in the format +<country code><area code><telephone number>.

Note that Teams agents must necessarily have the Phone System license and they must be configured as agents in C³ (for details on this, please refer to the [Mida C³ - Configuration Guide](#)).

1. **Configuration of transformation rules (Transformation).** These are rules to handle the called numbers and CLIDs. The following rules must be created:
 - Rules for calls routed to Teams
 - Rules for calls routed to C³
2. **Configuring the Call Routing Table.** Indicates how to handle the calls coming in from the different connections. The following tables must be created:
 - Tables for calls coming from Teams
 - Tables for calls coming from C³
 - Tables for calls coming from the PSTN
3. **SIP Profiles (SIP Profiles).** They define how to handle SIP dialogues in the different interfaces. SIP profiles must be created for the following interfaces:
 - Teams
 - C³
 - PSTN
4. **Server Tables (SIP Server Tables).** They contain the information required to reach the different servers the SBC is connected to. Server tables must be created to reach:
 - Teams
 - C³
 - PSTN
5. **Media List.** It defines the configuration of the media that can be used in the different interfaces, also according to the different licenses available in the SBC. In our example, we consider the minimal hypothesis of using G.711 only, with its two variants A-Law and u-Law. Lists must be defined for the following interfaces:
 - Teams
 - C³
 - PSTN
6. **Signaling Groups.** They define how the various connection interfaces are to be managed by appropriately combining all the configurations set out in the previous points. Signaling groups must be created for the following interfaces:
 - Teams
 - C³
 - PSTN

4.1 Configurations – Ribbon SBC SWe Lite



This guide assumes that:

- The SBC network interfaces are configured with the appropriate IP addresses

- The configuration of the SBC required to connect Ribbon SBC to Microsoft Teams has been completed following the instructions in the [Ribbon configuration guide](#).
- the SBC is regularly equipped with the necessary licenses
- the SBC has the necessary certificates on board (see the [Ribbon configuration guide](#))

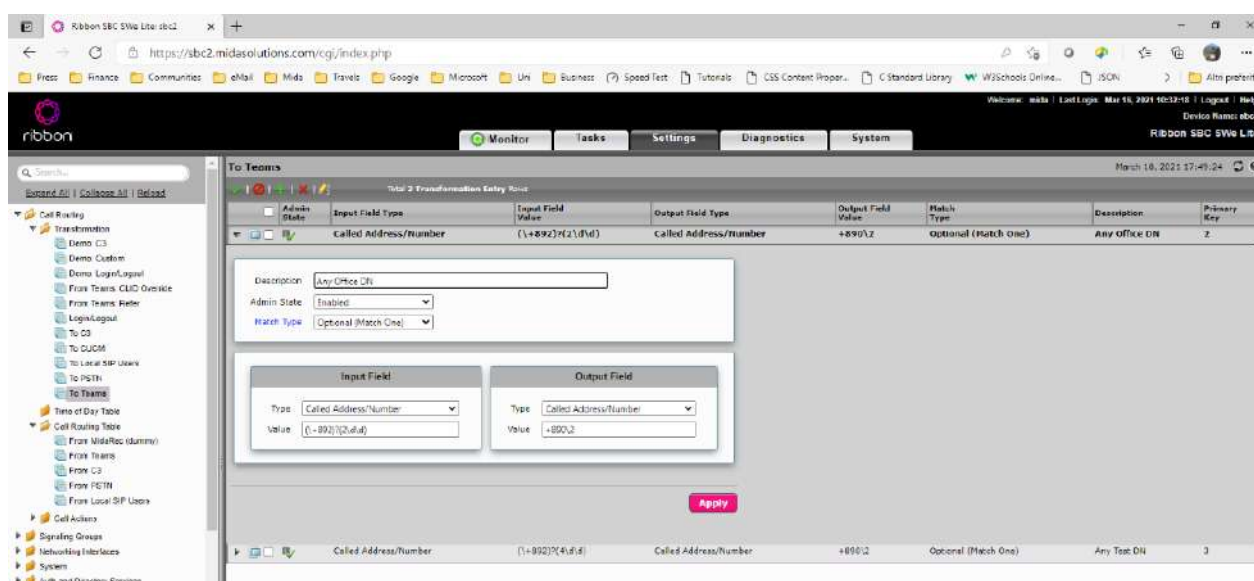
If the SBC is in Azure all this requires only one network interface with a static IP.

4.2 Connect Mida C³ - Cloud Contact Center and PSTN to Ribbon SBC SWe Lite

To set up the connection between Mida C³ - Cloud Contact Center and the Ribbon SBC, follow the steps below and insert values as stated in the screenshots if no other values are specified.

1. Go to **Call Routing > Transformation** and create a new **Transformation table**. This transformation will change the call destination with the proper Teams number.

Transformation table - To Teams



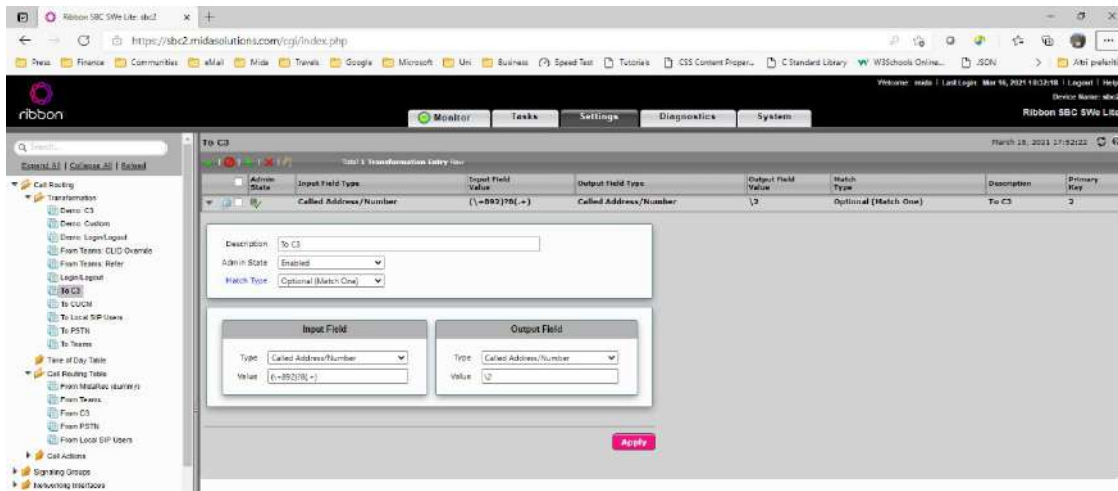
The screenshot shows the 'To Teams' transformation table configuration in the Ribbon SBC SWe Lite web interface. The interface includes a sidebar with navigation options like 'Call Routing', 'Transformation', 'Demo C3', 'Demo Custom', 'From Teams: CUCM', 'From Teams: HMI', 'From Teams: HMI', 'To CUCM', 'To Local SIP Users', 'To PSTN', 'To Teams', 'From MidaRoc (dummy)', 'From Teams', 'From C3', 'From PSTN', 'From Local SIP Users', 'Call Actions', 'Signaling Groups', 'Networking Interfaces', 'System', and 'Auth and Directory Services'.

The main configuration area for the 'To Teams' transformation table is shown. It includes a table with columns: Admin State, Input Field Type, Input Field Value, Output Field Type, Output Field Value, Match Type, Description, and Primary Key. The table contains two entries:

Admin State	Input Field Type	Input Field Value	Output Field Type	Output Field Value	Match Type	Description	Primary Key
Enabled	Called Address/Number	(1+892)(2,d,d)	Called Address/Number	+89012	Optional (Match One)	Any Office DN	1
Enabled	Called Address/Number	(1+892)(4,d,d)	Called Address/Number	+89012	Optional (Match One)	Any Test DN	2

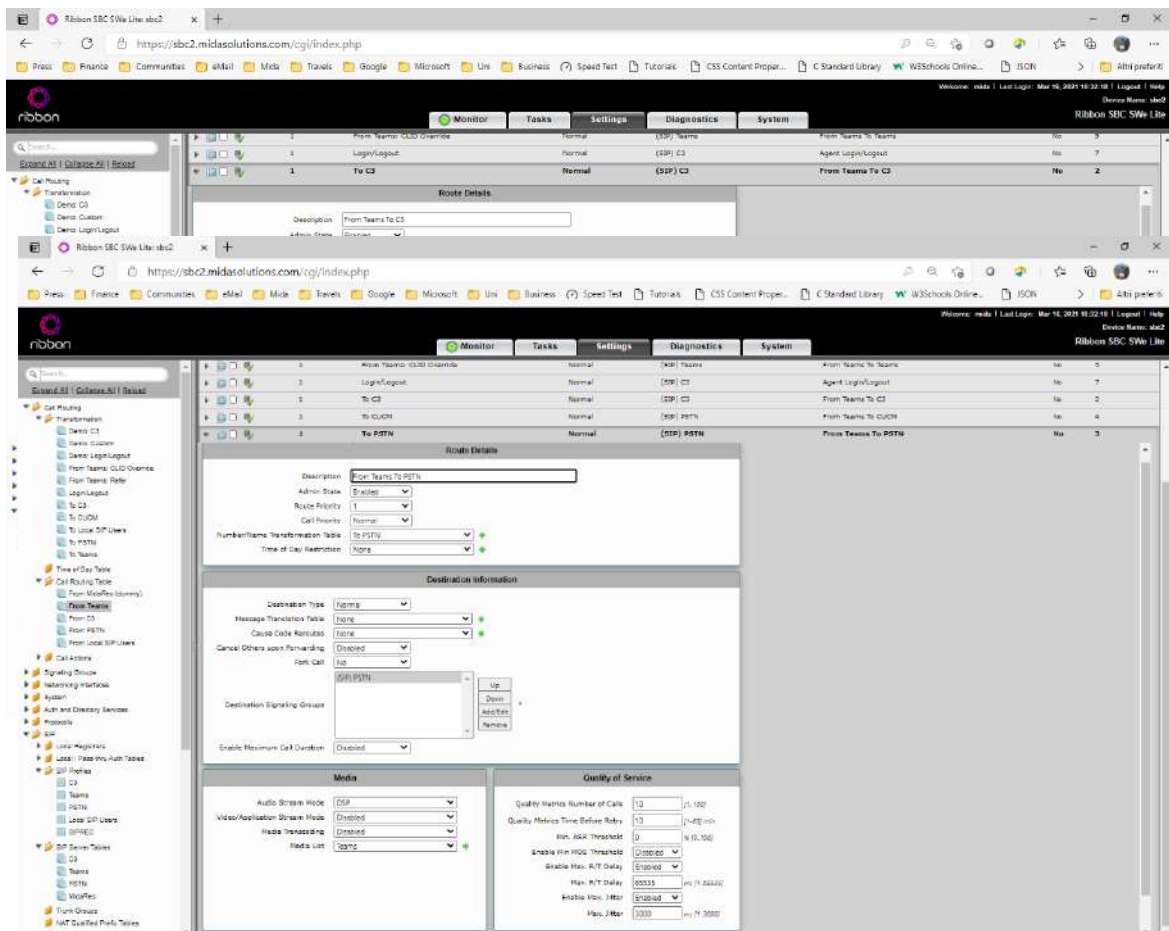
Below the table, there are input and output field configuration sections. The 'Input Field' section shows a 'Type' of 'Called Address/Number' and a 'Value' of '(1+892)(2,d,d)'. The 'Output Field' section shows a 'Type' of 'Called Address/Number' and a 'Value' of '+89012'. An 'Apply' button is located at the bottom right of the configuration area.

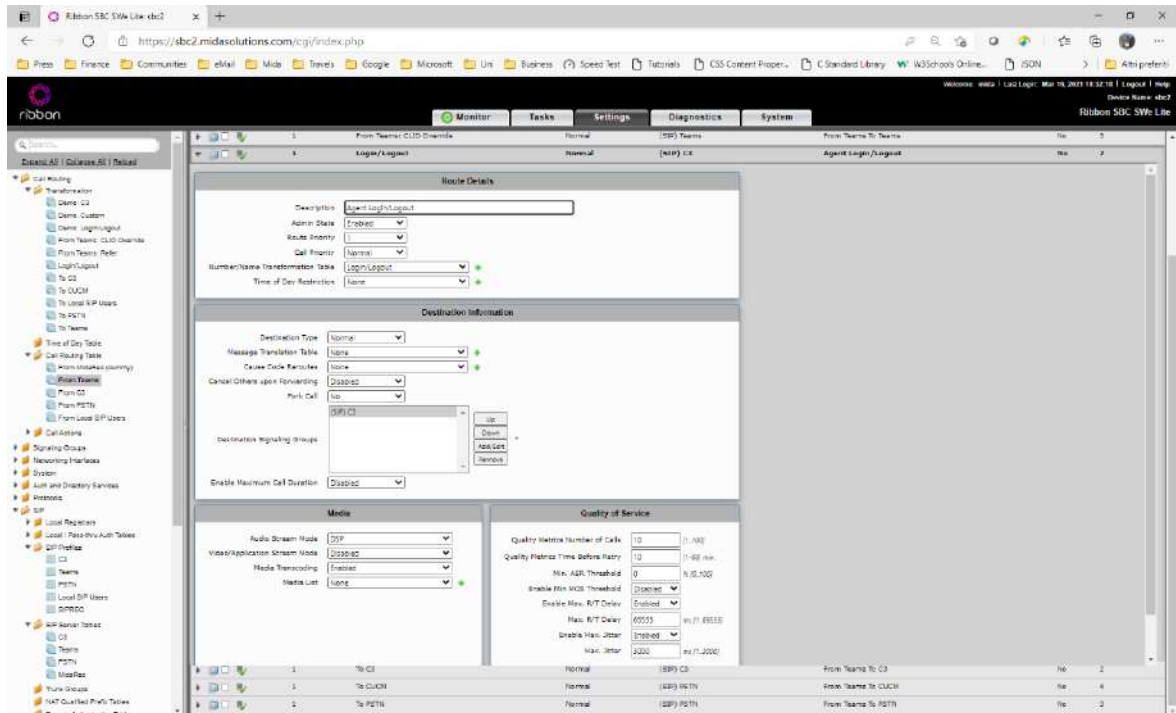
Transformation table - To C³



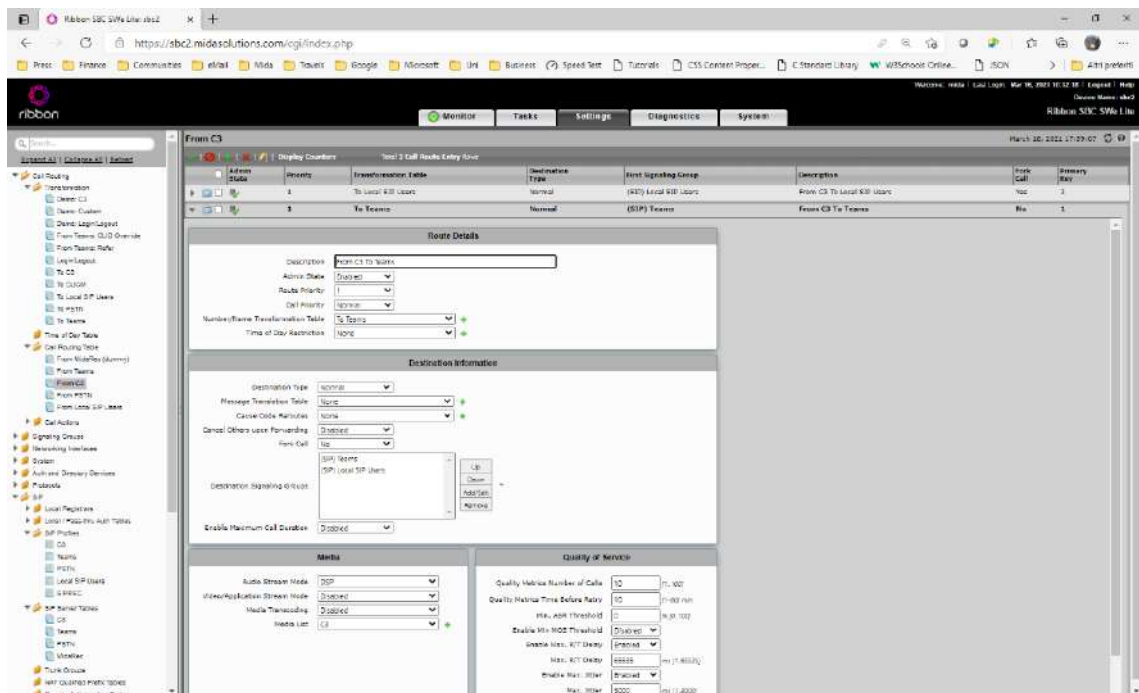
2. Go to **Call Routing > Call Routing Table** and create the new call routes.

Call Routing Table - From Teams

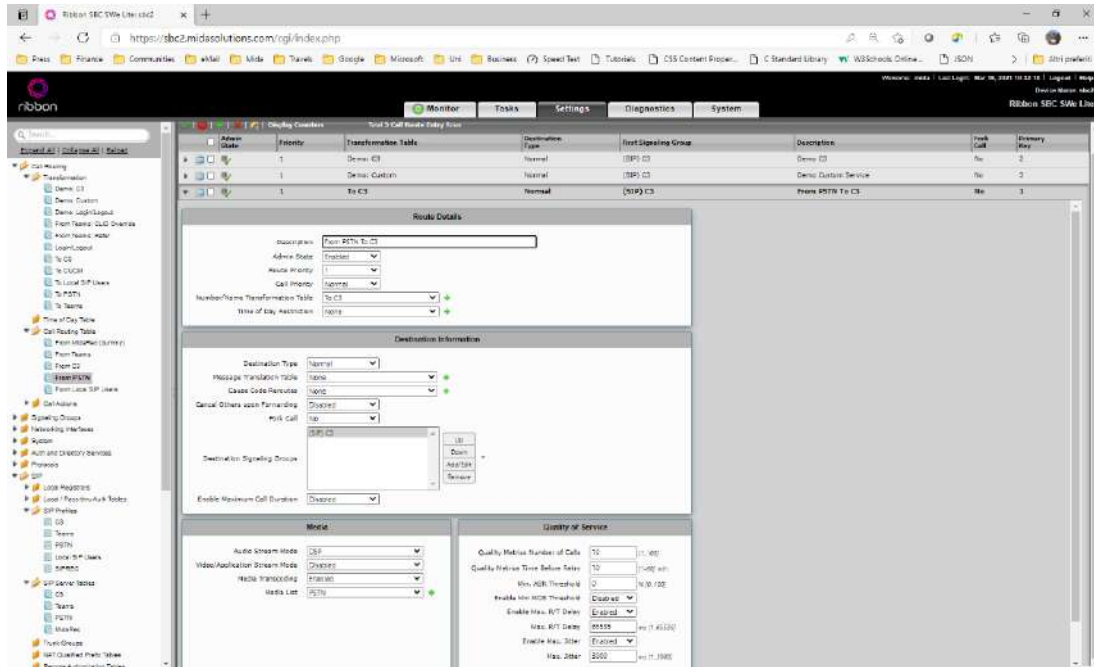




Call Routing Table - From C³



Call Routing Table - From PSTN



The screenshot shows the 'Call Routing Table' configuration in the Ribbon SBC Web UI. The table lists three entries:

Admin	Priority	Transformation Table	Destination Type	Port/Signaling Group	Description	Trunk	Priority
1	1	Service CS	Normal	CSIP CS	Service CS	No	1
1	1	Service Custom	Normal	CSIP CS	Service Custom Service	No	2
1	1	To CS	Normal	CSIP CS	Phone 9070 To CS	No	3

The 'Route Details' section for the selected entry shows:

- Source:** From PSTN To CS
- Destination:** CSIP CS
- Transformation Table:** Service Custom
- Port/Signaling Group:** CSIP CS
- Description:** Phone 9070 To CS

The 'Destination Information' section shows:

- Destination Type:** Normal
- Message Translation Table:** None
- Case Code Renumber:** None
- General Others user Forwarding:** Disabled
- Enable Call:** Yes
- Enable Maximum Call Duration:** Disabled

The 'Media' section shows:

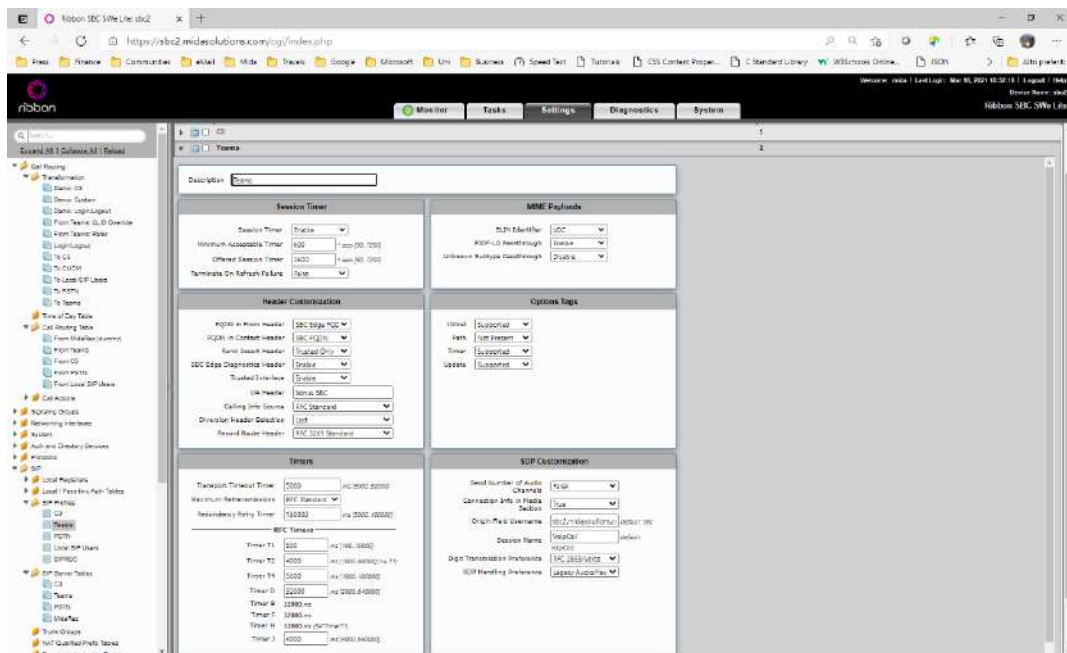
- Audio Stream Mode:** G.711
- Video/Animation Stream Mode:** Disabled
- Media Transcoding:** Disabled
- Media Loss:** Disabled

The 'Quality of Service' section shows:

- Quality Metrics:**
 - Quality Metrics Number of Calls: 10
 - Quality Metrics Time Before Delay: 10
 - Min. ASR Threshold: 0
 - Enable Max. RTT Delay: Disabled
 - Max. RTT Delay: 0
 - Enable Max. Delay: Disabled
 - Max. Delay: 0

3. Go to **SIP > SIP Profiles** and create these new entries.

SIP Profiles - Teams



The screenshot shows the 'SIP Profiles' configuration in the Ribbon SBC Web UI. The profile is named 'Teams'.

Session Timer:

- Session Timer:** Disabled
- Minimum Acceptable Timer:** 600
- Offered Session Timer:** 600
- Terminate On Refresh Failure:** Disabled

Header Customization:

- Request in Header:** SIP-Dialog
- Request in Content Header:** SIP-Dialog
- Request in Content Header:** SIP-Dialog
- SIP-Dialog Description Header:** Disabled
- Trunk/Session Header:** Disabled
- Call Info Header:** SIP-Dialog
- Director Header:** Disabled
- Request Header:** SIP-Dialog

Options:

- Options:** Supported
- Options:** Supported
- Options:** Supported
- Options:** Supported

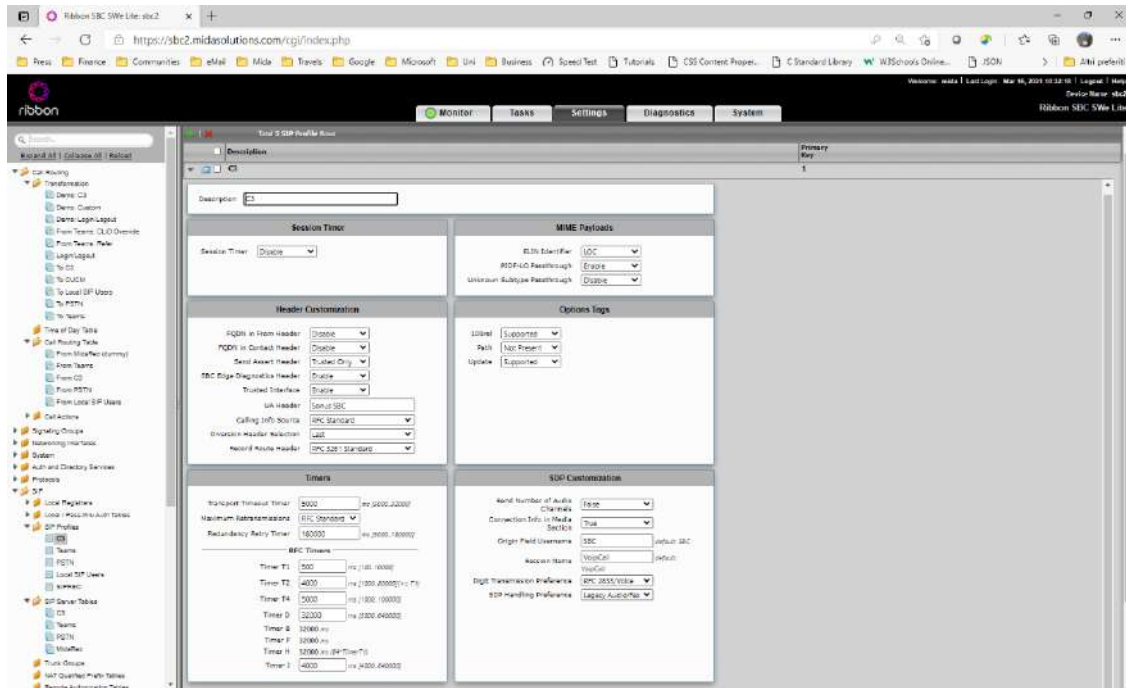
Timers:

- Transport Timeout:** 6000
- Maximum Retransmissions:** 10
- Retransmission Interval:** 1000
- RTT Timeout:** 6000
- RTT Timeout:** 6000
- RTT Timeout:** 6000
- RTT Timeout:** 6000
- RTT Timeout:** 6000
- RTT Timeout:** 6000
- RTT Timeout:** 6000

SIP Customization:

- Send Number of Audio Channels:** 1
- Correlation Info in Header:** Disabled
- Origin Peer Username:** SIP-Dialog
- Origin Peer Password:** SIP-Dialog
- Origin Peer Username:** SIP-Dialog
- Origin Peer Password:** SIP-Dialog

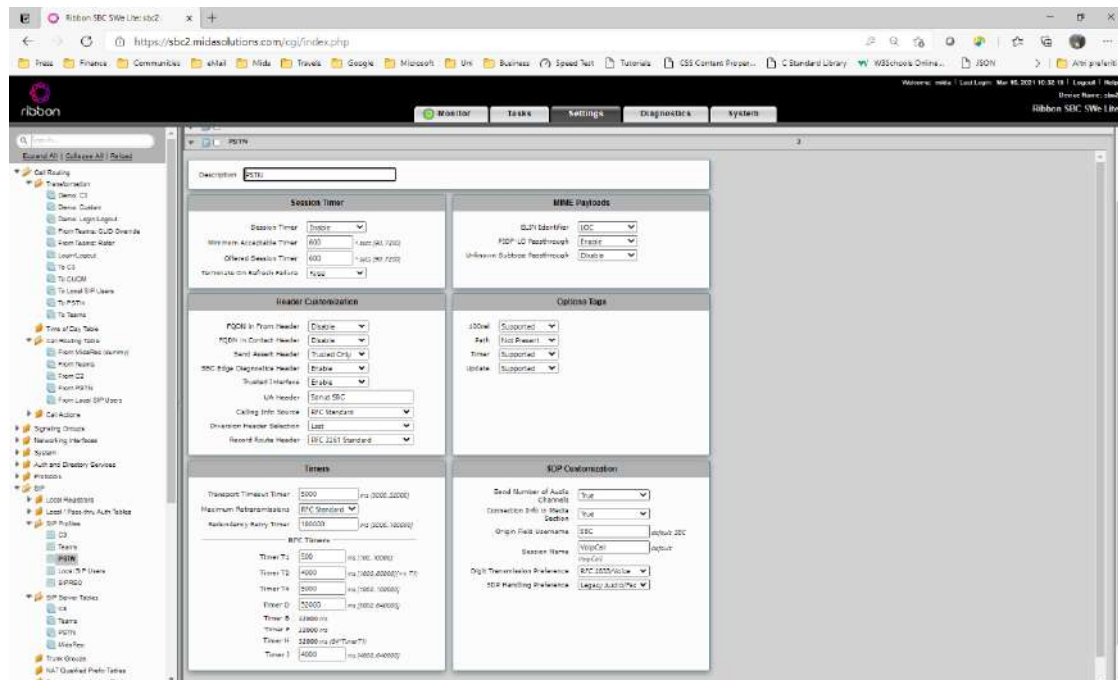
SIP Profiles - C³



The screenshot shows the 'SIP Profile' configuration page for 'C3' in the Mida Solutions web interface. The interface includes a sidebar with navigation options like 'Call Routing', 'Transformation', and 'SIP Profiles'. The main content area is divided into several sections:

- Session Timer:** Includes a 'Session Timer' dropdown set to 'Disable'.
- MIME Payloads:** Includes 'SDP Identifier' (set to 'LOC'), 'RTP-Jitter Passthrough' (set to 'Enable'), and 'Unknown Subtype Passthrough' (set to 'Disable').
- Header Customization:** Includes 'PQDN in From Header' (set to 'Disable'), 'PQDN in Contact Header' (set to 'Disable'), 'Send Asset Header' (set to 'Trusted Only'), 'SBC Edge Diagnostic Header' (set to 'Disable'), 'Trusted Interface' (set to 'E164'), 'UA Header' (set to 'SIP-SEC'), 'Calling Info Source' (set to 'RFC Standard'), 'Diversion Header Selection' (set to 'Last'), and 'Record Route Header' (set to 'RFC 3261 Standard').
- Options Tags:** Includes 'Allow' (set to 'Supported'), 'Path' (set to 'Not Present'), and 'Update' (set to 'Supported').
- Timers:** Includes 'Transport Timeout Timer' (set to 2000), 'Maximum Pathlength' (set to 'RFC Standard'), 'Redundancy Retry Timer' (set to 180000), and a list of BFC Timers (Timer T1 to T7) with their respective values and units.
- SIP Customization:** Includes 'Send Number of Audio Channels' (set to 'True'), 'Connection Info in Media Section' (set to 'True'), 'Origin Field Username' (set to 'SBC'), 'Session Name' (set to 'VoIPCall'), 'RTP Transmission Preference' (set to 'RFC 3261/1890'), and 'SIP Handling Preference' (set to 'Legacy Audio/Video').

SIP Profiles – PSTN

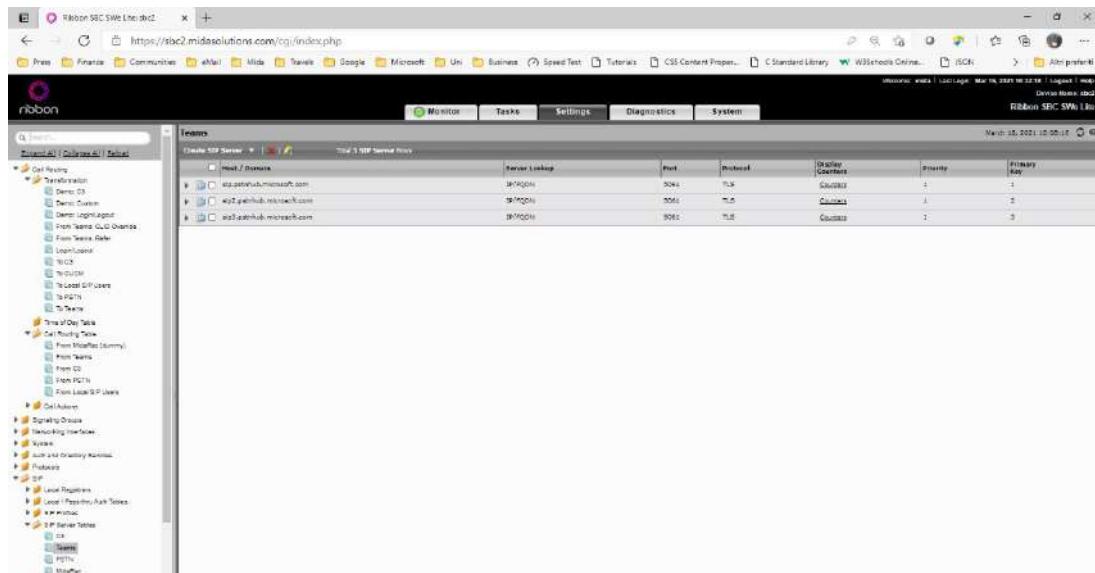


The screenshot shows the 'SIP Profile' configuration page for 'PSTN' in the Mida Solutions web interface. The interface is similar to the C3 profile but with specific settings for PSTN:

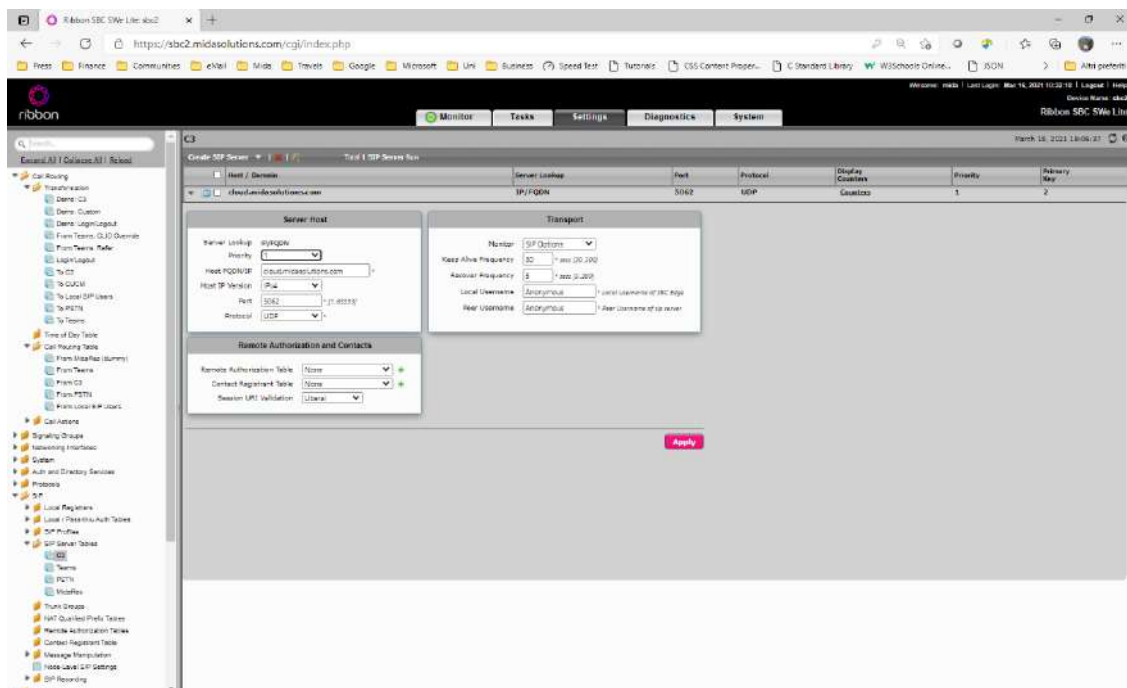
- Session Timer:** Includes a 'Session Timer' dropdown set to 'Disable', 'Minimum Acceptable Timer' (set to 600), 'Offered Session Timer' (set to 600), and 'Termination on Multiple Failure' (set to 'Noop').
- MIME Payloads:** Includes 'SDP Identifier' (set to 'LOC'), 'RTP-Jitter Passthrough' (set to 'Enable'), and 'Unknown Subtype Passthrough' (set to 'Disable').
- Header Customization:** Includes 'PQDN in From Header' (set to 'Disable'), 'PQDN in Contact Header' (set to 'Disable'), 'Send Asset Header' (set to 'Trusted Only'), 'SBC Edge Diagnostic Header' (set to 'Disable'), 'Trusted Interface' (set to 'E164'), 'UA Header' (set to 'SIP-SEC'), 'Calling Info Source' (set to 'RFC Standard'), 'Diversion Header Selection' (set to 'Last'), and 'Record Route Header' (set to 'RFC 3261 Standard').
- Options Tags:** Includes 'Allow' (set to 'Supported'), 'Path' (set to 'Not Present'), and 'Update' (set to 'Supported').
- Timers:** Includes 'Transport Timeout Timer' (set to 2000), 'Maximum Pathlength' (set to 'RFC Standard'), 'Redundancy Retry Timer' (set to 180000), and a list of BFC Timers (Timer T1 to T7) with their respective values and units.
- SIP Customization:** Includes 'Send Number of Audio Channels' (set to 'True'), 'Connection Info in Media Section' (set to 'True'), 'Origin Field Username' (set to 'SBC'), 'Session Name' (set to 'VoIPCall'), 'RTP Transmission Preference' (set to 'RFC 3261/1890'), and 'SIP Handling Preference' (set to 'Legacy Audio/Video').

4. Go to **SIP > SIP Server Tables** and create a new SIP Server.

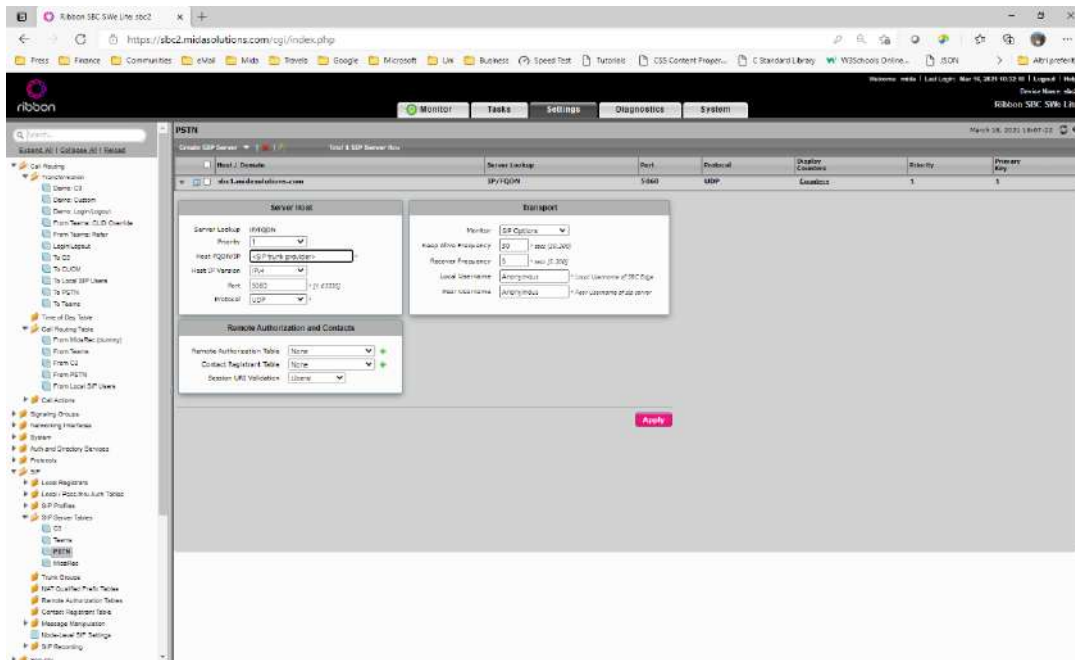
SIP Server - Teams (follow the [Ribbon configuration guide](#))



SIP Server - C³

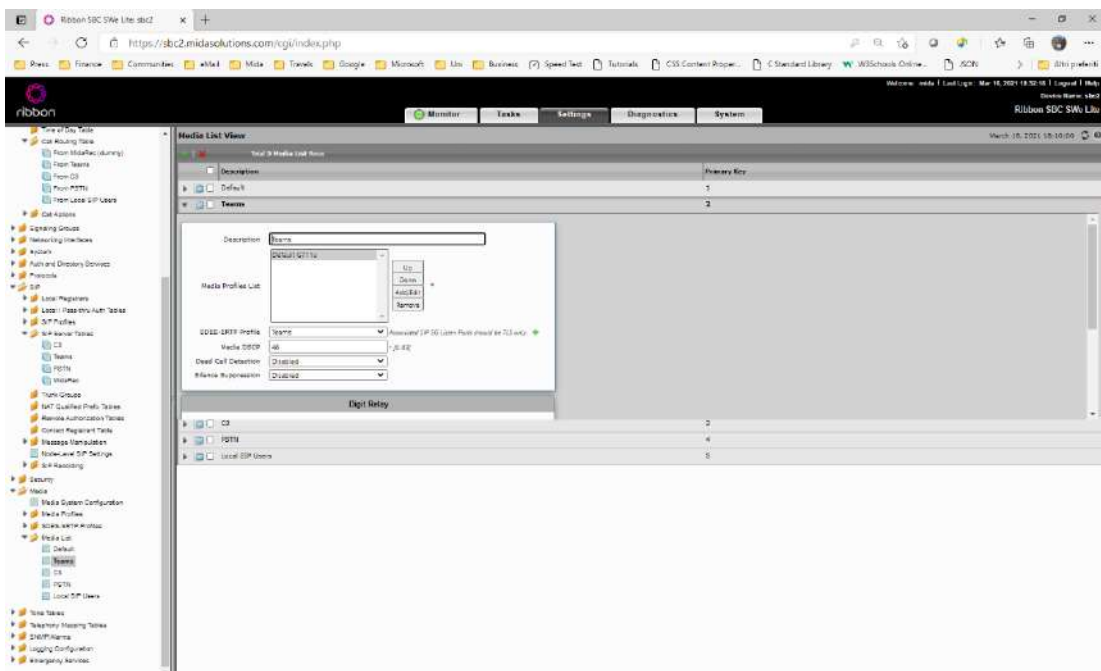


SIP Server - PSTN

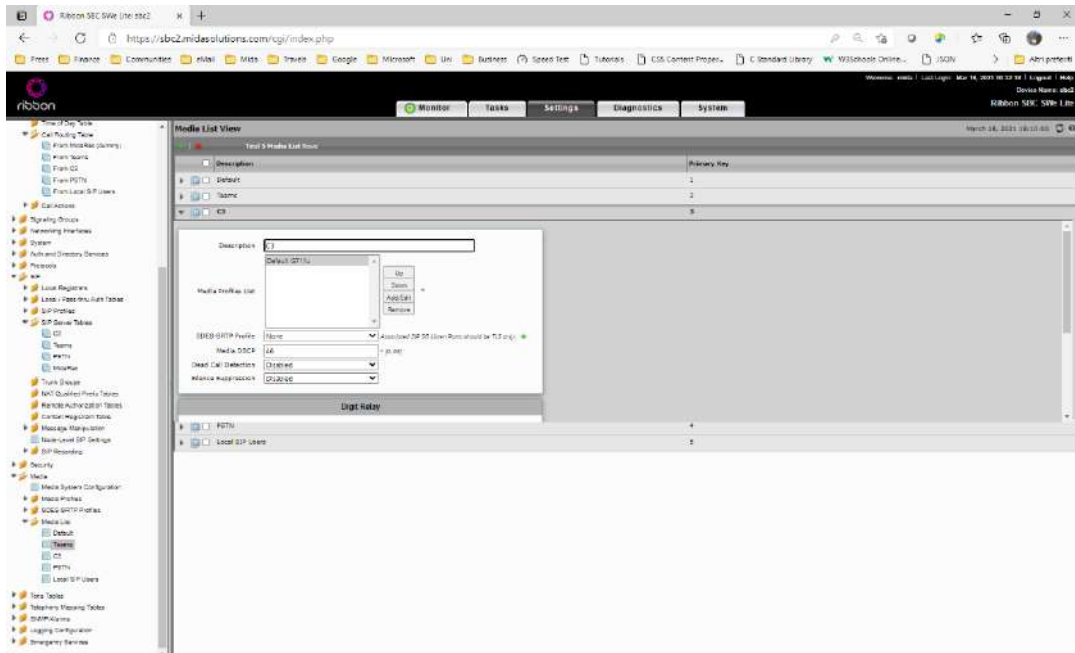


5. Go to **Media List** and create these new entries

Media List – Teams

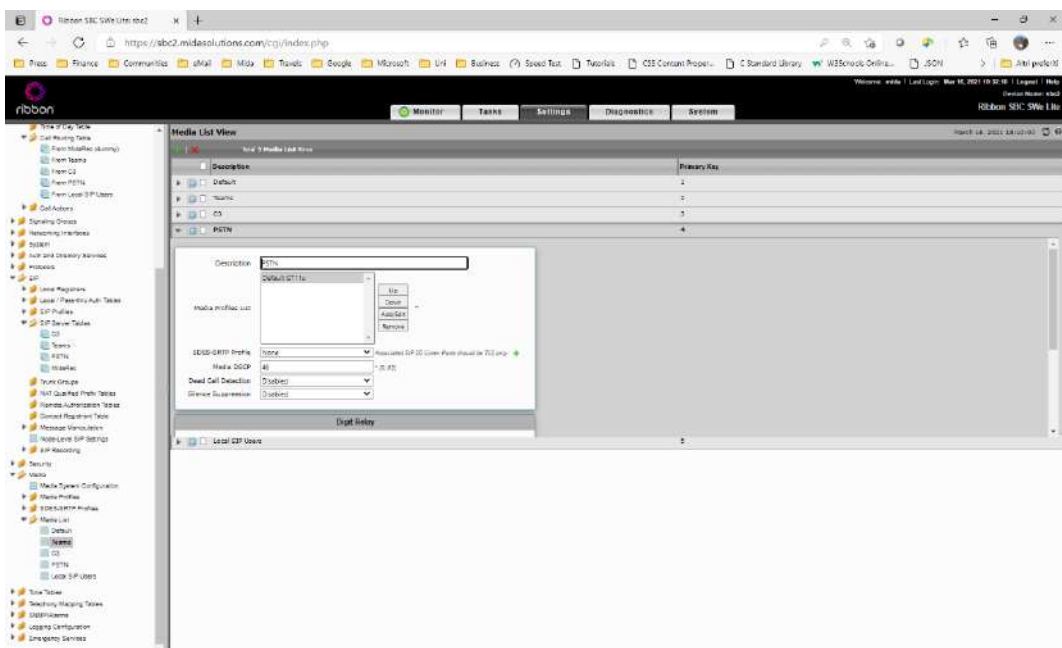


Media List - C³



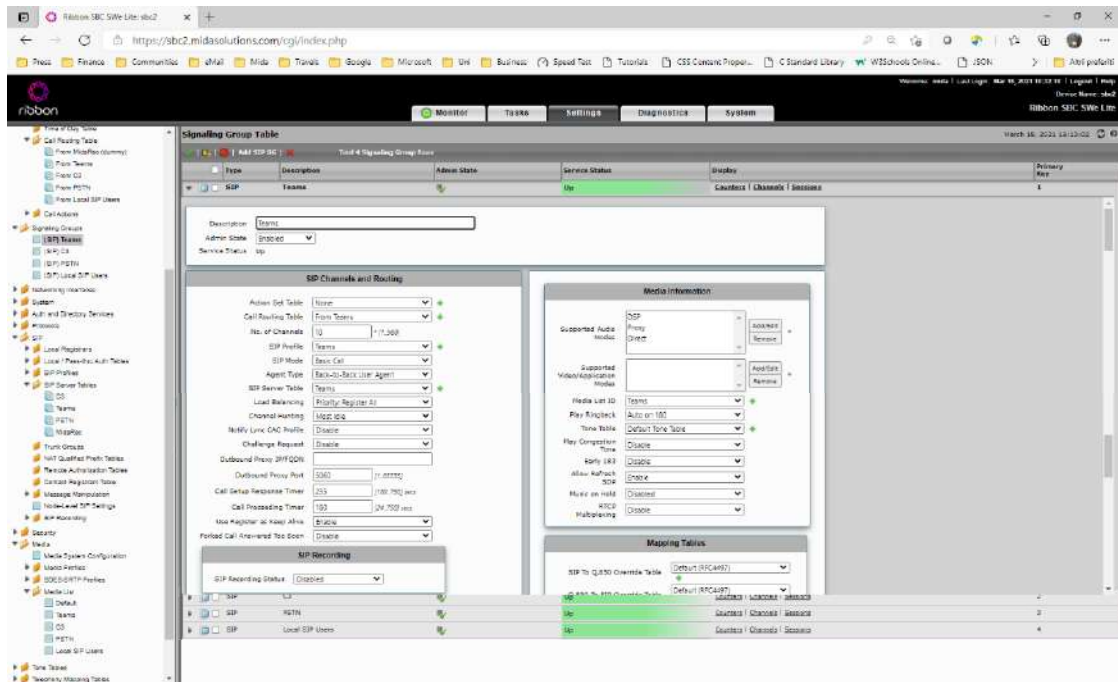
Select a single codec, or A-Law or u-Law.

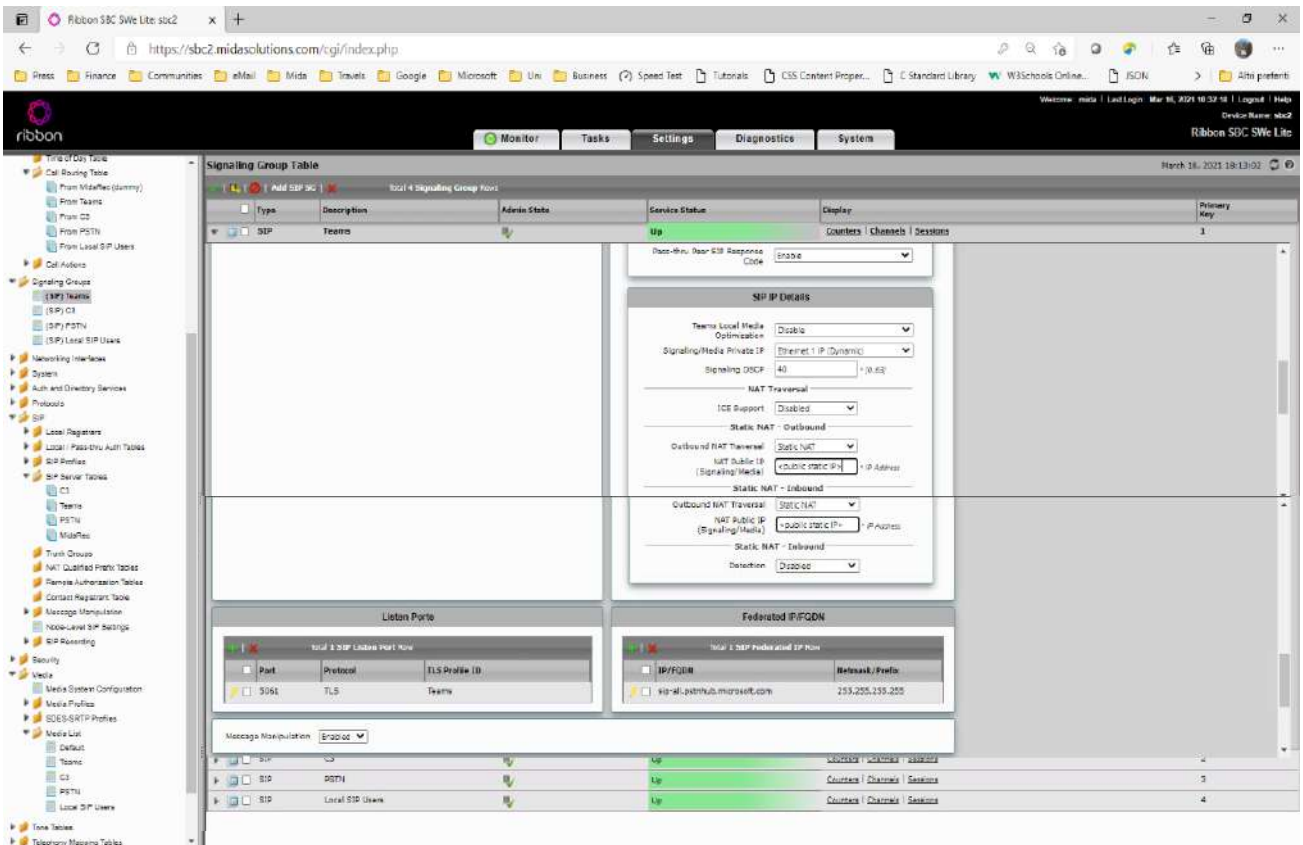
Media List - PSTN



6. **Signaling Groups** and create a new entry (“Signaling Group”)

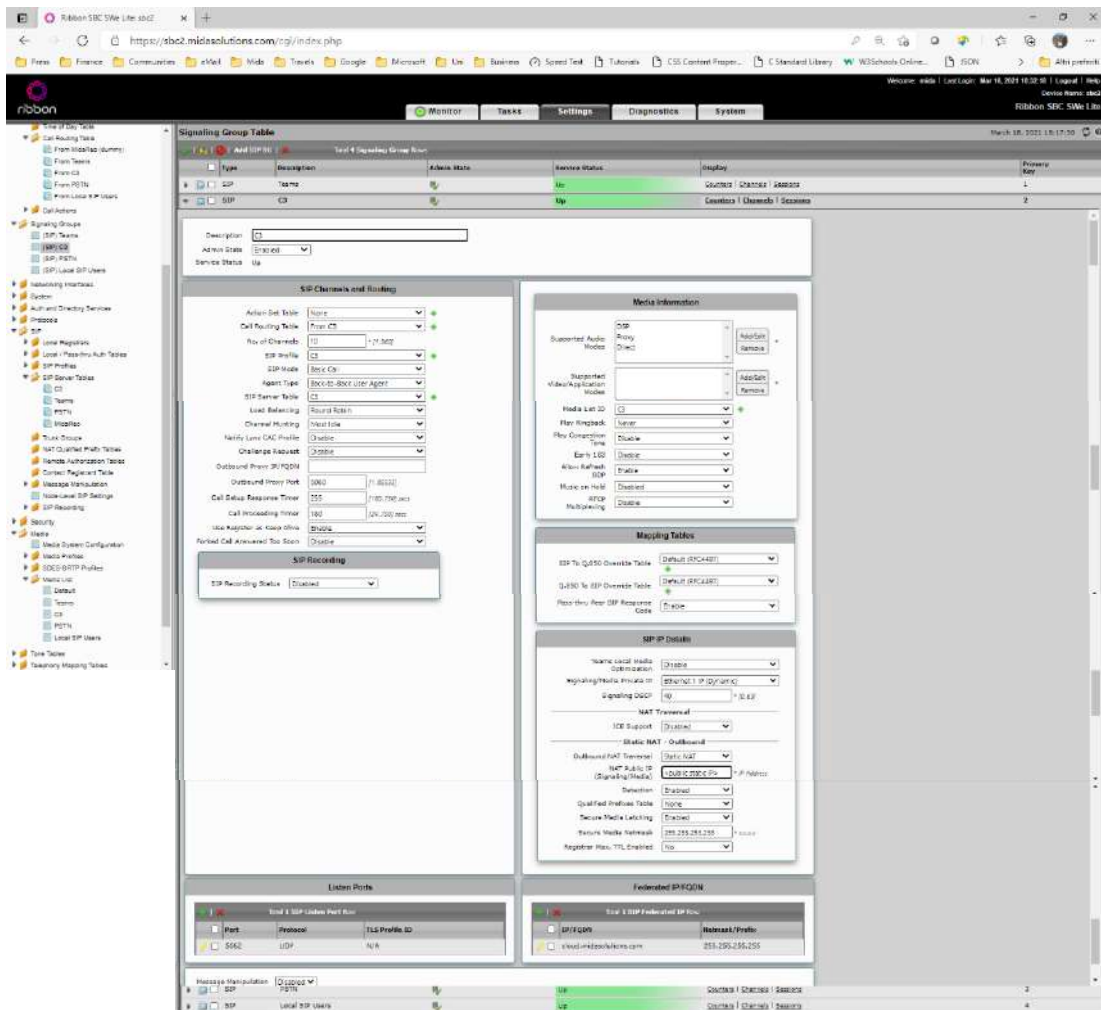
Signaling Groups - Teams (follow the [Ribbon configuration guide](#))





The screenshot displays the Ribbon SBC SWE Lite sbc2 web interface. The browser address bar shows <https://sbc2.midasolutions.com/cgi/index.php>. The interface includes a navigation menu on the left with categories like Trunk, Call Routing, Signaling, and Security. The main content area is titled "Signaling Group Table" and shows a table with columns: Type, Description, Admin State, Service Status, Display, and Primary Key. The table lists three rows: SIP, SIP, and SIP. The SIP row is selected, and its configuration is shown in a sidebar on the right. The configuration includes sections for SIP IP Details, Listen Ports, and Federated IP/FQDN. The SIP IP Details section shows various settings like Trunk Local Media, Signaling/Media Private IP, and NAT Traversal. The Listen Ports section shows a table with columns: Port, Protocol, and TLS Profile ID. The Federated IP/FQDN section shows a table with columns: IP/FQDN and Network/Prefix. The bottom of the interface shows a table with columns: Type, Description, Admin State, Service Status, Display, and Primary Key, listing three rows: SIP, SIP, and SIP.

Signaling Groups - C³



The screenshot displays the Ribbon SBC S/W Lite web interface, specifically the 'Signaling Group Table' and configuration details for a SIP group.

Signaling Group Table:

Type	Description	Admin Status	Service Status	Display	Priority
SIP	Test SIP	Up	Up	Group 1 123456 123456	1
SIP	Test SIP	Up	Up	Group 2 123456 123456	2

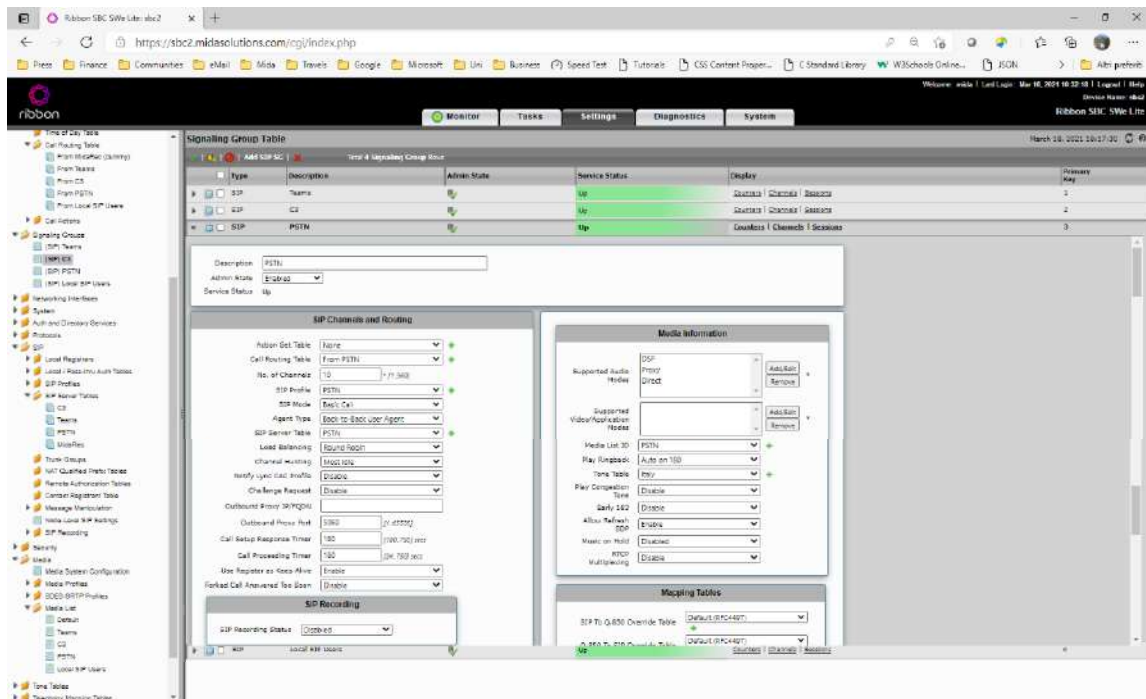
Configuration Details for SIP Group 1:

- Description:** Test SIP
- Admin Status:** Up
- Service Status:** Up
- SIP Channels and Routing:**
 - Active Set Table: None
 - Call Routing Table: None
 - Row of Channels: 10
 - SIP Profile: 10
 - SIP Mode: Basic SIP
 - Agent Type: Basic SIP User Agent
 - SIP Server Table: 10
 - Load Balancing: Round Robin
 - Channel Mapping: None
 - Media Line QoS Profile: None
 - Challenge Request: None
 - Outbound Proxy: 10.10.10.10
 - Outbound Proxy Port: 5060
 - Call Setup Timeout: 100
 - Call Teardown Timeout: 100
 - Call Forwarding Timeout: 100
 - Use Registrar as Proxy: No
 - Periodic Call Abandonment: No
- SIP Recording:**
 - SIP Recording Status: Disabled
- Media Information:**
 - Supported Audio Modes: G.711, G.722, G.729
 - Supported Video/Audio Modes: H.264, H.265, VP8, VP9
 - Media Line QoS: G.711
 - Header Compression: None
 - Play Compression: None
 - Early SIP: Disabled
 - Early SIP: Disabled
 - Media Line QoS: G.711
 - Media Line QoS: G.711
- Mapping Tables:**
 - SIP To QoS Mapping Table: Default (SIP2QoS)
 - QoS To SIP Mapping Table: Default (QoS2SIP)
 - Play to SIP Mapping Table: None
- SIP IP Details:**
 - Trunk Local Media: 10.10.10.10
 - Trunking/Trunking Profile: SIP2SIP
 - Signaling QoS: 10
 - NAT Traversal: No
 - ICE Traversal: No
 - Static NAT - Outbound: No
 - Outbound NAT Traversal: No
 - NAT Public IP (Signaling/Media): 10.10.10.10
 - Trunking: No
 - Secure Media Linking: No
 - Secure Media Linking: No
 - Applicable SIP TLS Enabled: No
- Listen Ports:**

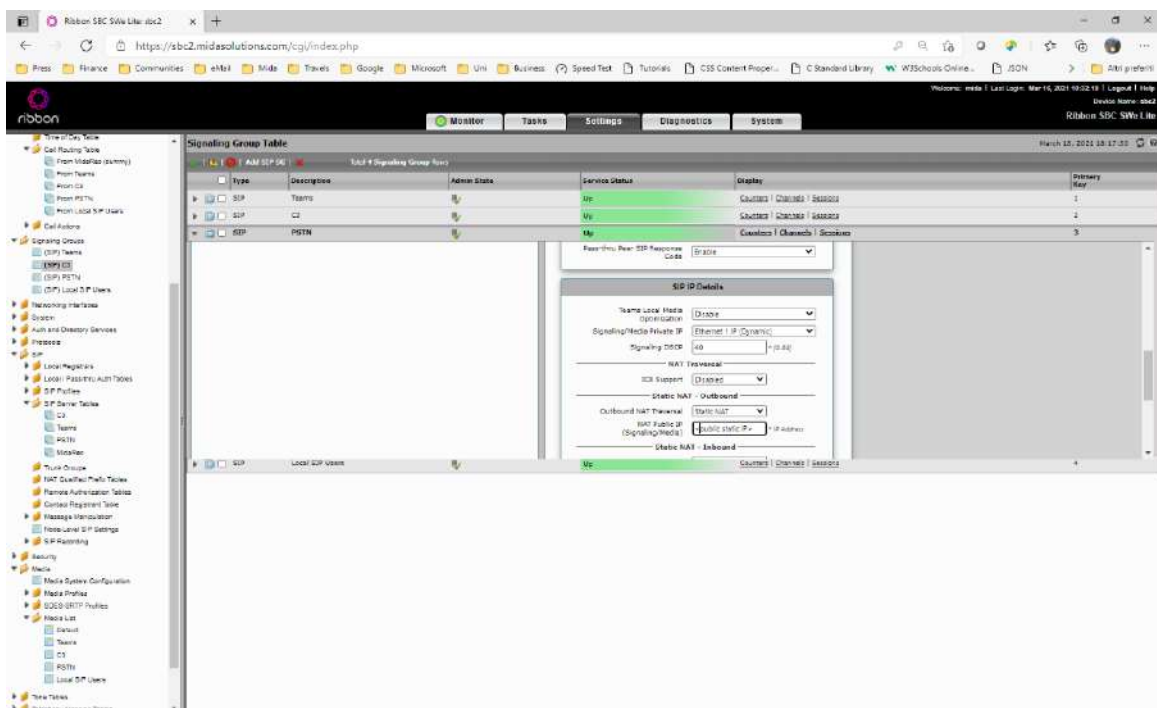
Port	Protocol	TLS Profile ID
5060	UDP	Any
- Federated SIPQoS:**

SIPQoS	Network/Profile
10	10.10.10.10

Signaling Groups - PSTN



The screenshot shows the Ribbon SBC S/W User Interface. The left sidebar contains a tree view with categories like Call Routing, Signaling Groups, and Media. The main area displays the 'Signaling Group Table' for 'Local Signaling Group Rows'. The table lists three rows: SIP Trunks, SIP CS, and SIP PSTN. The 'SIP PSTN' row is selected, and its configuration is shown in the right pane. The configuration includes 'SIP Channels and Routing' (Name: PSTN, From: PSTN, No. of Channels: 10, SIP Profile: PSTN, SIP Mode: Best Call, Agent Type: Back to Back user Agents, SIP Server Table: PSTN, Load Balancing: Round Robin, Max. 90%, Notify Local SIP Profile: Disabled, Outbound Proxy SIP Profile: Disabled, Outbound Proxy Port: 5060, Call Setup Response Time: 100, Call Processing Time: 100, Use Register as Host Agent: Enabled, Forked Call Answered Too Soon: Disabled) and 'Media Information' (Supported Audio: G.711, G.722, G.729, Supported Video/Application: None, Media List ID: PSTN, Play/Response: Auto on 100, Tone: 1000, Play Completion Time: 100, Early 242: Disabled, Allow Refresh SIP: Enabled, Music on Hold: Disabled, Multiplexing: Disabled). The 'Mapping Tables' section shows 'SIP To Q.850 Override Table' and 'Q.850 To SIP Override Table'.



The screenshot shows the Ribbon SBC S/W User Interface. The left sidebar contains a tree view with categories like Call Routing, Signaling Groups, and Media. The main area displays the 'Signaling Group Table' for 'Local Signaling Group Rows'. The table lists three rows: SIP Trunks, SIP CS, and SIP PSTN. The 'SIP CS' row is selected, and its configuration is shown in the right pane. The configuration includes 'SIP IP Details' (Name Local Media: Disabled, Signaling/Media Private IP: Ethernet 1 (Dynamic), Signaling DSCP: 46, NAT Traversal: Disabled, Static NAT: Outbound, Outbound NAT Traversal: Static NAT, NAT Public IP (Signaling/Media): Public Static IP, Static NAT: Inbound). The 'Mapping Tables' section shows 'SIP To Q.850 Override Table' and 'Q.850 To SIP Override Table'.

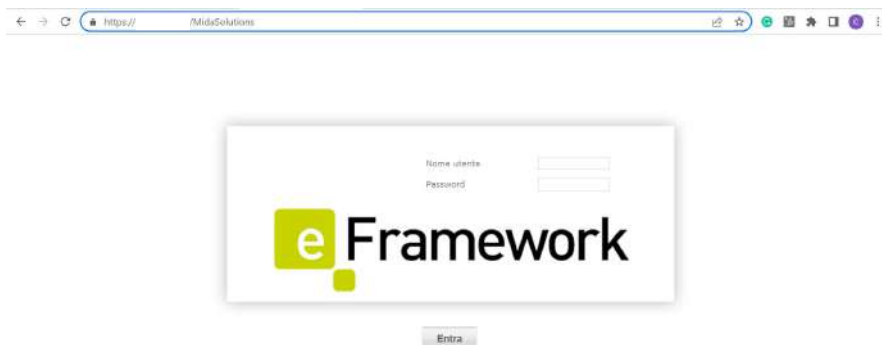
5. Multi-tenant systems: add tenants

Multi-Tenant systems are useful when multiple organizations are sharing the same application server. When the multi-tenant option is enabled, administrator profiles are slightly different compared to standard systems.

If you are our partner with more than one customer, you can handle them on our multi-tenant platform using one single Virtual Machine. Please refers to this paragraph only if it is your case, otherwise, you can leave out this paragraph.

In the No Tenant section of the Mida Unified Portal – MUP (which is the Mida Solutions products' main interface), it is possible to add tenants and handle them. Here it is also possible to set some parameters that concern all the tenants because these settings are related to the unique Virtual Machine.

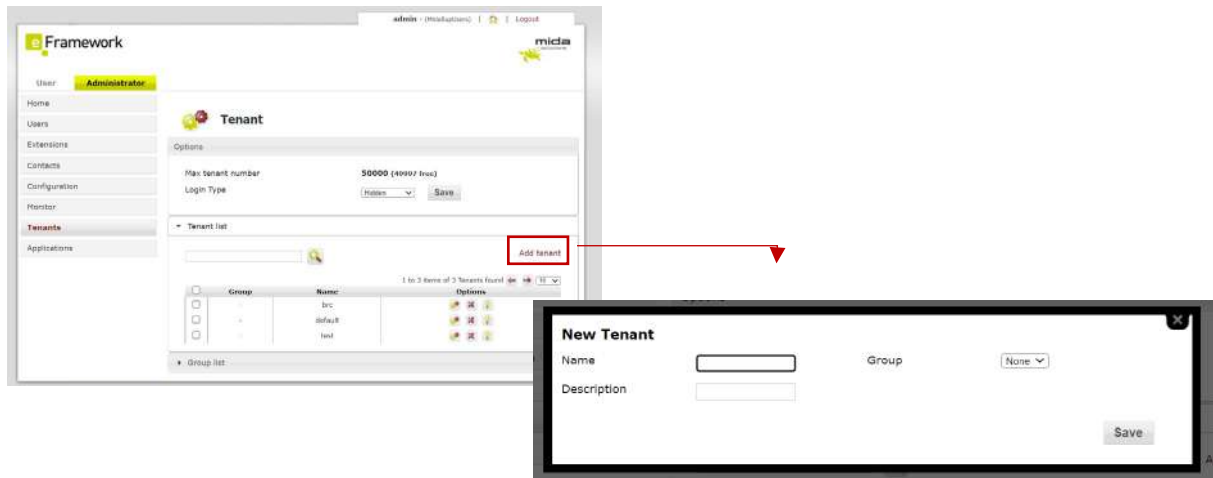
1. Access to the super-tenant administration page at <http://<IP ADDRESS>/MidaSolutions> with these credentials:
 - Username: admin
 - Password: admin



2. Check to be logged as **Super-Tenant**.



- From the navigation menu on the left, go to Administrator > **Tenants**. The page will show the already existing tenants and will enable to create new ones simply clicking on the **Add new** option.



- Insert here the name and the description of the new tenant and click on Save.
- The new tenant is now ready to be use.



Please note that:

- the tenant's name will be the one the tenant uses to log in to his MUP.
- the procedure of adding a tenant takes a few minutes. Wait a moment before the tenant log in into the Mida Unified Portal (as explained below).
- by default, each new tenant has an admin user
- it is possible to organize tenants in group.

For each tenant, the page allows to:

- Edit** – open the edit tenant page to change the name, the description, and the group;
- Delete** – a warning dialog box will open to ask for confirmation;
- Disable** – a warning dialog box will open to ask for confirmation.

- To access the new tenant's Mida Unified Portal just go to `http:// <IP ADDRESS>/NEW_TENANT_NAME` and use the following credentials.

- Username: admin
- Password: tenant name with the first letter of the chosen name capitalized and the current year written with numbers. This is a password given by default. At any time, it is possible to change it.

For example, if the tenant's name is brc, to log in use:

- the URL `http:// <IP ADDRESS>/brc`
- the user's name admin
- the password: Brc2022

As shown in the picture below, the tenant can check to be logged in his Mida Unified Portal.

