Spectralink IP-DECT Server 200/400/6500
Spectralink Virtual IP-DECT Server One

Microsoft Teams

Integration Guide

722-0214-000 Rev: G
September 2025

Copyright Notice

Notice

Warranty

The Product Warranty and Software License and Warranty and other support documents are available at http://support.spectralink.com/.

Contact Information

US Location
+1 303-441-7500

Spectralink Corporation
305 S. Arthur Ave.
Louisville, CO 80027
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 1344 206591

Spectralink Europe UK
The Lightbox, Willoughby
Rd, Bracknell, RG12 8FB
United Kingdom

infoemea@spectralink.com

Contents

Chapter 1: About This Guide

This guide describes how to configure a Spectralink IP-DECT Server 200/400/6500 or a Virtual IP-DECT Server One for integrating the Microsoft Teams Gateway.

In the following, the servers will be referred to as “Spectralink IP-DECT Server”.

This guide is intended for qualified technicians and the reader is assumed to have a basic knowledge about the Spectralink IP-DECT Server and Microsoft Teams. It is also assumed, that you have an installed and functioning Spectralink IP-DECT Server and an active Microsoft Teams account.

The guide is divided into two parts:

- Spectralink IP-DECT Server
- Handset onboarding and sign-in

Each part describes the general configuration and the user administration.

Environment Information

- Microsoft Teams - Navigate to the Microsoft documentation site for the latest Microsoft documentation.
- Spectralink IP-DECT Server 200/400/6500 (must have firmware version PCS22Aa or newer)
- Spectralink Virtual IP-DECT Server One (must have firmware version PCS22Aa or newer)
- Spectralink DECT Handsets 72x2, 75x2, 76x2 and 77x2 (must have firmware PCS22Ab or newer)
- Spectralink S-Series Handsets S33, S35 and S37
- Spectralink network and security requirements - see description of communication ports for the relevant server in the Server Installation and Configuration Guide.

Spectralink prerequisites

Microsoft Teams integration is supported exclusively on S-Series handset models (S33, S35 and S37), PP7 handset models (72x2, 75x2, 76x2, 77x2), Funktel ATEX handsets, and the following serves: Spectralink IP-DECT Server 200/400/6500 and Spectralink Virtual IP-DECT Server One.

End of life KIRK base stations, 7xx0 and Butterfly DECT Handset models are not supported.

Microsoft prerequisites

There is no additional cost for organizations to use SIP Gateway, and any users meeting the following requirements can use SIP Gateway:

- Users must be licensed for Teams Phone (via any Office 365 E5, Microsoft 365 license that includes Teams Phone, or as a standalone license)
- SIP devices for calls must be enabled in the calling policy the user has assigned
- PSTN numbers must be assigned in the Teams Admin Center (TAC)
- No proxies are allowed

For information on ports, whitelisting of IP addresses and more, refer to the Microsoft documentation available online at: https://docs.microsoft.com/en-us/microsoftteams/sip-gateway-configure

Related Documentation

All Spectralink documents are available at http://support.spectralink.com/.

Spectralink Documentation

Subject	Documentation
Spectralink DECT Handsets	For more information about the handset, refer to the user guide available online at http://support.spectralink.com/products.
Synchronization and Deployment Guide	For more information about synchronization and deployment, refer to the guide available online at http://support.spectralink.com/products.
Spectralink IP-DECT Server	For more information about the server, refer to the guide available online at http://support.spectralink.com/products.
Provisioning	For more information about provisioning, refer to the guide available online at http://support.spectralink.com/products.
Spectralink Technical Bulletins	Available online at http://support.spectralink.com/products.
Release Notes	Document that describes software changes, bug fixes, outstanding issues, and hardware compatibility considerations for new software releases. Available online at http://support.spectralink.com/products.
Spectralink DECT Training material	To gain access to the Spectralink training material, you must attend training and become a Spectralink Certified Specialist. Please visit http://partneraccess.spectralink.com/training/classroom-training for more information and registration.

Chapter 2: Feature List

The following features are supported:

	Supported features
Telephony	• Make and receive basic calls • Message Waiting Indication (MWI) and voice mail access • Caller ID • Call Hold and Resume • Call Transfer (blind, semi-attended, attended) • Call Forwarding • Call Waiting • Global Do Not Disturb (DND) • DTMF tones • Music on Hold (MOH) • Shared Line (up to 3 handsets)
User experience	• Centralized Phonebook via LDAP • Local Phonebook generated from user data • Call Completed Elsewhere • Teams status indication on DECT handset (onboarded /signed in) / In-call presence indication
Management/Administration	• Remote sign-out and re-onboarding through the IP-DECT server web interface • SIP credentials auto-sync (time configurable) • End user sign-in / sign-out with user managed credentials • Bulk provisioning and sign-in using the IP-DECT server GUI (10 users at a time) • Admin controlled show/hide Teams menu in handset • End-user remote (TAC side) sign-out warning • Choice of stand-by text provisioned OTA automatically (display name, DDI, Extension, last 3, 4, 5 or 6 digits of DDI number) • DECT server auto configuration when Teams is enabled (all parameters needed to work with Teams are set automatically)
Security	• Secure Voice - TLS 1.2 • Domain allow list (security feature to only allow company domain users to sign in)
Value added Spectralink features	• AMIE integration • Centralized management and provisioning via DECT server management capability • Multi-language (on handsets)

	Supported features
	• Microsoft Teams color logo in the DECT handset display when Teams integration is enabled

Chapter 3: Configuration and Feature Details

Supported features	*Description/Setting*
Make and receive basic calls	Allows user to make and answer calls.
Message Waiting Indication (MWI) and voice mail access	Notifies the user when a new voice message has been received. Access voice messages by dialing your own number or through the supported voicemail feature code *99*. Alternatively, you can access your voice messages by navigating to the Teams menu on your handset. Available only on Spectralink Handsets.
Caller ID	Display Caller ID information for incoming and outgoing calls.
Call Hold and Retrieve	Allows user to place active calls on hold.
Call Transfer (blind, semi-attended, attended)	Allows user to transfer the active call to some other number.
Call Forwarding	Allows the user to: • Reset/disable call forwarding Disable call forwarding by dialing code ***32***. • Enable call forwarding Enable call forwarding by dialing code ***33***, followed by the desired extension. E.g.: ***33*123456*** will forward all calls 123456 • Custom timeout forwarding Enable call forwarding after a set number of seconds by dialing code ***34***, followed by the desired number of seconds, and lastly the extension). E.g.: ***34*10*123456*** will forward all calls to **123456** after 10 seconds Default timeout is 20 seconds. • Simultaneous ring Enable the calling of a secondary extension after 20 seconds by dialing code ***35***, followed by the desired extension. E.g.: ***35*123456*** will ensure that both your extension and **123456** will ring simultaneously after 20 seconds.
Call Waiting	Allows user to answer another incoming call when already in an active call. The user can then choose to: • Ignore the call waiting • Decline the call waiting • Accept the call waiting If the user accepts the call, then they can toggle between the two calls or disconnect one of the two or both.

Supported features	*Description/Setting*
Centralized Phonebook	Supports integration with LDAP and pulls contact names, numbers, titles and other information to form a phonebook. There is also an option to generate a local phonebook from the IP-DECT server, using only DECT handset numbers, if no LDAP server is configured.
Do Not Disturb (DND)	Allows user to silence incoming calls. Note: The DND status is applied on the handset and also to other devices logged in with Teams.
DTMF	Supports touch-tone feature codes.
Spectralink IP-DECT Gateway support	Gateway function extends MS Teams to users/devices operating in legacy cable environments using Digital DECT Base Stations connected to the IP-DECT Gateway.
Jitter buffer	Helps with mitigating one-way audio delay if the arrival of RTP packets is out of sync.
Music on Hold (MOH)	Play music to callers on hold.
Presence	Displays a locally handled presence status, such as: • A DND logo, signaling the DND state • An available state, which is shown on the handset's front screen, indicating a successful connection and registration to Microsoft Teams. • A yellow dot, signaling that the handset is currently in the on-boarding state
Secure Voice - TLS 1.2	Encrypted call security.
Shared line	Supports SIP forking together with additional Microsoft Teams devices and/or soft clients

Note:

It is possible to make and receive calls, to and from: Microsoft Teams PC clients, Web clients, Phones or any other devices connected to the Microsoft SIP Gateway, and lastly PSTN (mobile phones or fixed lines).

The capability to make and receive calls will be dependent on how Microsoft Teams is set up.

Chapter 4: Spectralink IP-DECT Server

Below is a description of how to configure the Spectralink IP-DECT Server and an overview of all the automatically configured fields changed in the Microsoft Teams provisioning process.

Note:

It is assumed that you have installed and configured the Spectralink IP-DECT Server solution including deployment and administration of base stations before continuing the configuration described below.

You can access the web-based Administration Page of the Spectralink IP-DECT Server through a standard web browser by entering the IP address discovered by UPnP, along with the username and password.

- Default username of the system is: **admin**
- Default password of the system is: **admin**

The IP address can also be obtained by dialing ***999*00 + Off-hook on handsets

Configuring the Spectralink IP-DECT Server

Infrastructure version requirements

To support the configuration described in this guide:

- Spectralink IP-DECT Server 200/400/6500 must have firmware version PCS22Aa or newer
- Spectralink Virtual IP-DECT Server One must have firmware version PCS22Aa or newer
- Spectralink DECT Handsets 72x2, 75x2, 76x2, 77x2 must have firmware PCS22Ab or newer
- Spectralink S-Series Handsets S33, S35 or S37

License installation

In order to set up Microsoft Teams, you must first install a Microsoft Teams Integration or DECT Complete Software and Services Bundle (exclusive to IP-DECT Server 400) license on your Spectralink IP-DECT Server.

When using a Spectralink IP-DECT Gateway, the Microsoft Teams Integration license can be extended to users on Digital Base Stations connected via 2/4-pair cables to the Gateway.

Each Spectralink IP-DECT server must be individually fitted with a feature license:

Licenses	*Description*
1 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 400 12 Users (14232882)	Allows: Up to 12 users. Access to MS Teams Integration Software, Technical Support 8-5
3 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 400 12 Users (14233700)	Allows: Up to 12 users. Access to MS Teams Integration Software, Technical Support 8-5
5 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 400 12 Users (14233705)	Allows: Up to 12 users. Access to MS Teams Integration Software, Technical Support 8-5
1 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 400 +48 Users (14232883)	Allows: An additional 48 users. Access to MS Teams Integration Software, Technical Support 8-5
3 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 400 +48 Users (14233701)	Allows: An additional 48 users. Access to MS Teams Integration Software, Technical Support 8-5
5 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 400 +48 Users (14233706)	Allows: An additional 48 users. Access to MS Teams Integration Software, Technical Support 8-5
1 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 30 Users (14232884)	Allows: Up to 30 users. Access to MS Teams Integration Software, Technical Support 8-5
3 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 30 Users (14233702)	Allows: Up to 30 users. Access to MS Teams Integration Software, Technical Support 8-5
5 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 30 Users (14233707)	Allows: Up to 30 users. Access to MS Teams Integration Software, Technical Support 8-5
1 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 +150 Users (14232885)	Allows: An additional 150 users. Access to MS Teams Integration Software, Technical Support 8-5
3 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 +150 Users (14233703)	Allows: An additional 150 users. Access to MS Teams Integration Software, Technical Support 8-5

Licenses	*Description*
5 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 +150 Users (14233708)	Allows: An additional 150 users. Access to MS Teams Integration Software, Technical Support 8-5
1 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 +500 Users (14232886)	Allows: An additional 500 users. Access to MS Teams Integration Software, Technical Support 8-5
3 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 +500 Users (14233704)	Allows: An additional 500 users. Access to MS Teams Integration Software, Technical Support 8-5
5 Year MS Teams Direct integration (includes Software Assurance) | IP-DECT Server 6500 +500 Users (14233709)	Allows: An additional 500 users. Access to MS Teams Integration Software, Technical Support 8-5
1 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE 30 Users (14233237)	Allows: Up to 30 users. Access to MS Teams Integration Software, Technical Support 8-5
3 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE 30 Users (14233272)	Allows: Up to 30 users. Access to MS Teams Integration Software, Technical Support 8-5
5 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE 30 Users (14233275)	Allows: Up to 30 users. Access to MS Teams Integration Software, Technical Support 8-5
1 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE +150 Users (14233238)	Allows: An additional 150 users. Access to MS Teams Integration Software, Technical Support 8-5
3 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE +150 Users (14233273)	Allows: An additional 150 users. Access to MS Teams Integration Software, Technical Support 8-5
5 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE +150 Users (14233276)	Allows: An additional 150 users. Access to MS Teams Integration Software, Technical Support 8-5
1 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE +500 Users (14233239)	Allows: An additional 500 users. Access to MS Teams Integration Software, Technical Support 8-5

Licenses	*Description*
3 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE +500 Users (14233274)	Allows: An additional 500 users. Access to MS Teams Integration Software, Technical Support 8-5
5 Year MS Teams Direct integration (includes Software Assurance) | Virtual IP-DECT Server ONE +500 Users (14233277)	Allows: An additional 500 users. Access to MS Teams Integration Software, Technical Support 8-5
MS Teams perpetual Firmware Update License | IP-DECT Server 200 (14232887)	Allows: Access to MS Teams Integration Software, Technical Support 8-5
User License | Spectralink DECT Server 8000 30 Users (14232867)	Allows: Up to 30 users. Access to MS Teams Integration Software, Technical Support 8-5

Microsoft Teams can also be acquired for the Spectralink IP-DECT Server 400 through the DECT Complete Plan license (All-inclusive Software and Services Pack), as an alternative option to the integration licenses.

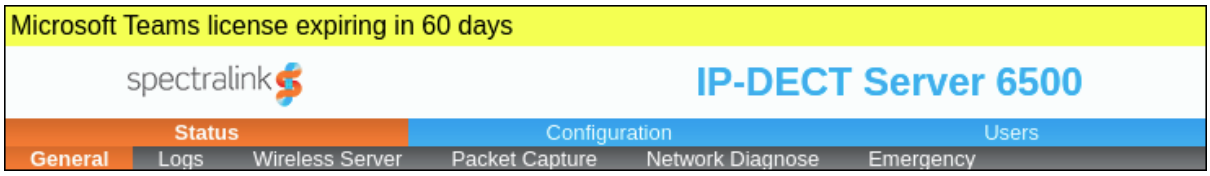
Licenses	*Description*
1 Year DECT Complete Software and Services Bundle | IP-DECT Server 400 - per user license (72712901)	Allows: SpectraCare for IP-DS 400, IP-DECT Base Stations and S-Series handsets AMIE for IP-DECT Cisco Unified CM Integration MS Teams Integration LAN sync Handset Sharing Configuration-over-the-air (COTA) and Enhanced Provisioning license
3 Year DECT Complete Software and Services Bundle | IP-DECT Server 400 - per user license (72712903)	Allows: SpectraCare for IP-DS 400, IP-DECT Base Stations and S-Series handsets AMIE for IP-DECT Cisco Unified CM Integration MS Teams Integration LAN sync Handset Sharing Configuration-over-the-air (COTA) and Enhanced Provisioning license

Licenses	*Description*
5 Year DECT Complete Software and Services Bundle | IP-DECT Server 400 - per user license (72712905)	Allows: SpectraCare for IP-DS 400, IP-DECT Base Stations and S-Series handsets AMIE for IP-DECT Cisco Unified CM Integration MS Teams Integration LAN sync Handset Sharing Configuration-over-the-air (COTA) and Enhanced Provisioning license

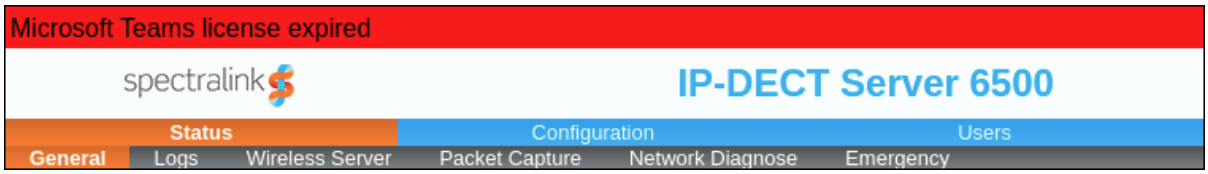
To order and install a Teams Integration license on your Spectralink IP-DECT Server, please consult the License Ordering and Loading section of the Install and Configuration Guide.

Note:
When a Microsoft Teams integration license expires, subscriptions will be disabled, preventing the addition of new handsets on the server. Subscription can only be enabled again by loading a new Microsoft Teams license.

When 60 days or fewer are left until the license expires, a yellow warning banner will be displayed in the GUI.



Once the license has expired, a red banner will be displayed in the GUI.



Microsoft Teams Settings

To setup Microsoft Teams from the web-based Administration Page

Go to **Configuration** -> **Microsoft Teams** and input the following settings:

Field	*Setting*
Provisioning	
Method	DHCP (default value): automatically get the Microsoft Teams provisioning server URL using DHCP option 160. This option needs to be configured on your DHCP server first. Static: manually enter the Microsoft Teams provisioning server URL according to your region • EMEA: http://emea.ipp.sdg.teams.microsoft.com/ • Americas: http://noam.ipp.sdg.teams.microsoft.com/ • APAC: http://apac.ipp.sdg.teams.microsoft.com/ For more information on how to configure your SIP gateway, please consult the Gateway Configuration Guide from Microsoft. Disabled: disable provisioning
URL	The URL used for Microsoft Teams provisioning.
General	
Configuration sync time (hh:mm)	Synchronize new configurations from the provisioning server at a specific time. Synchronizations are performed daily. If left empty, no synchronizations will be performed.
Handset limit per account	Allowed number of handsets to sign-in to the same Teams account. Set to 2 by default.
Domain whitelist	Allowed domains in a comma separated list. If left empty all domains are allowed.
Show handset standby text as	Changes the handset standby text to one of the following options: • Assigned phone number • Phone number extension • Last 3, 4, 5, 6 digits of the phone number • Display name In order for the standby text to update on the handset, the user must sign in again after the setting is applied.
Set secondary username as	Change your secondary username based on your Microsoft Teams Admin Center configurations: • None • Extension • Last 3, 4, 5, 6 digits of the phone number If a handset is logged out of Teams, it can still receive messages (from the server or other handsets) on the secondary username, as long as no other handsets are logged into the same account. This is because the secondary username is tied to the account, not the handset and it will transfer to the most recently logged-in handset on the account.

Field	*Setting*
	In order for the secondary username to update, the user must sign in again after the setting is applied.
Enable remote sign out warning	Enables the option to send out a warning from the server to the handset, indicating that the handset is signed out.
Remote sign out warning tone	Changes the remote sign out warning tone
Dispatchable location from SIP header X-switch-info	
Enable	If enabled and supported, a custom header X-switch-info is included in SIP REGISTER and INVITE messages, containing the handset MAC address/IPEI, IP-DECT server subnet length, and base station BSSID/MAC address. The remote server uses this information to determine the user's emergency call location.
X-switch-info mac field	Changes the X-switch info mac field to one of the following options: • Handset IPEI • RFP MAC address
Handset Sign in menu	
Hide Sign in	Hides the sign-in option from the sign-in handset menu
Hide Re-onboard	Hides the re-onboard option from the sign-in menu
Handset Sign out menu	
Hide Voicemail	Hides the voicemail option from the sign-out handset menu
Hide CFW	Hides the CFW option from the sign-out handset menu
Hide DND	Hides the DND option from the sign-out handset menu
Hide Sign out	Hides the sign-out option from the sign-out handset menu
Hide Re-onboard	Hides the re-onboard option from the sign-out handset menu

Note:

If the Microsoft Teams services become unavailable, calls and MSF messages will be internally routed through your secondary username.

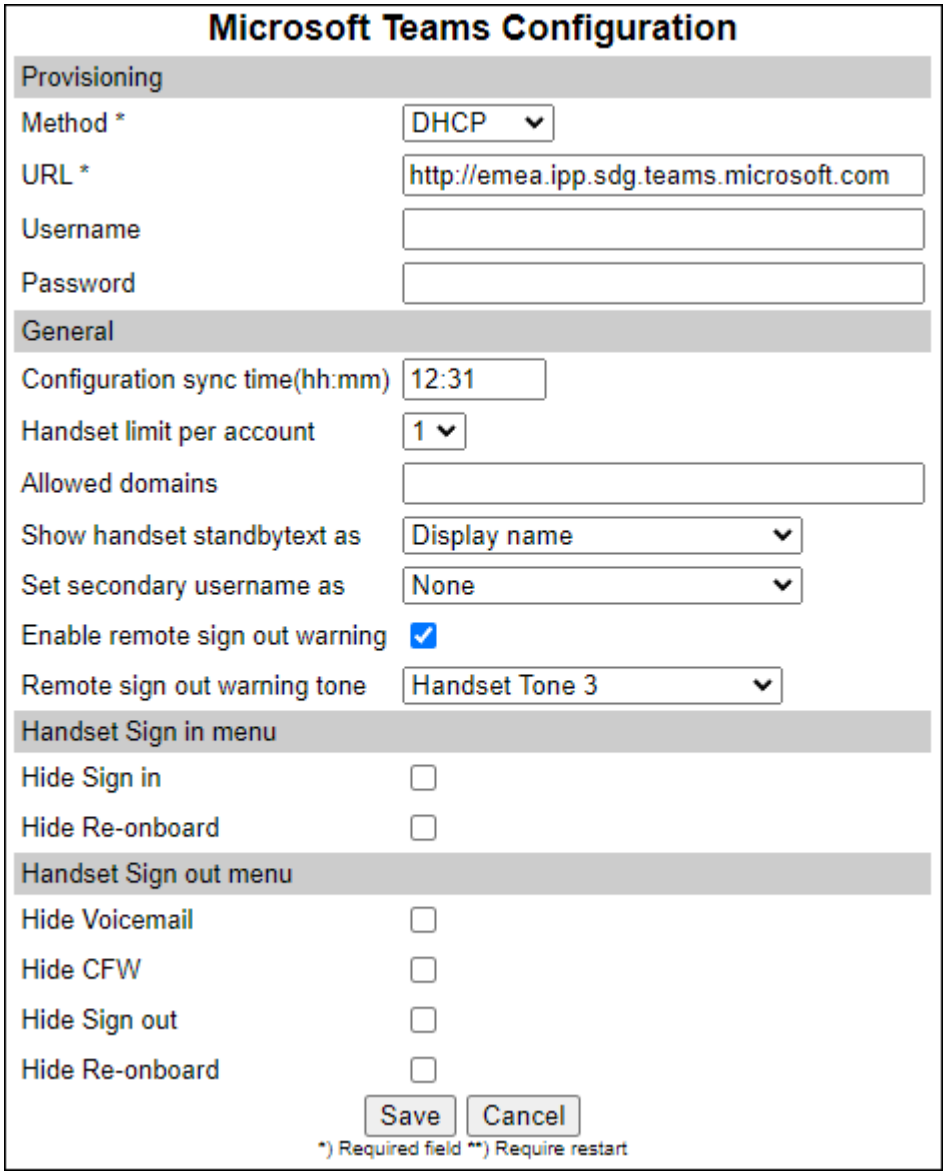
To set an extension as a secondary username on the IP-DECT Server, you must first configure it in the Microsoft Teams Admin Center. Likewise, using the last 3/4/5/6 digits of the phone number as a secondary username assumes that Microsoft Teams has been configured in accordance to your company's dial plan.

For further information, please consult the Microsoft Teams admin documentation.

Note:

At least one handset has to be subscribed to the server in order for the provisioning process to initiate.

A connection status to the provisioning server can be seen under **Status** -> **General** -> **Quick status**



Remote sign-out and re-onboarding

For handsets that have previously completed the on-boarding process, remote sign-out and re-onboarding are available by accessing **Users** -> **List Users** from the Web interface.

Remote sign-out enables an admin to quickly sign out multiple users, by selecting them from the User List and pressing Sign Out.

Re-onboarding enables the admin to remotely initiate the onboarding process for multiple users, by selecting them from the User List and pressing Re-onboard. Starting this process will sign out the handset, and contact the Microsoft Teams provisioning server to get the latest onboarding configurations.

When a handset/user is signed out remotely from the Teams Admin Center (TAC), or from any other Microsoft application not related to a user/IP-DECT server function, an alarm can be setup for the DECT handsets by enabling the remote sign out warning option on the IP-DECT server.

The handset will display a message, and will play the Handset Tone set on the server, to signal that user action is required. Causes for sign-out can be also related to conditional access, or other Azure-related limitations in how long a Teams SIP gateway user can be signed in.

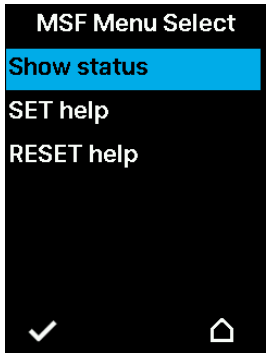
DND Mode

The handset can be set to DND Mode in order to automatically reject all calls. The status of the MS-Teams desktop or web application will also be updated to “do not disturb”, provided the user is logged in.

The status can be set to DND by calling *30* on your handset and it can be reset by calling *31*.

The current DND status can also be verified on the handset from the **Microsoft Teams** submenu -> **DND** -> **Show Status**.

In the same DND submenu the codes for setting and resetting the DND are also displayed in the **SET help** and **RESET help** options.



Automatically configured fields

The following IP-DECT Server fields will be automatically changed when the server is configured for Microsoft Teams

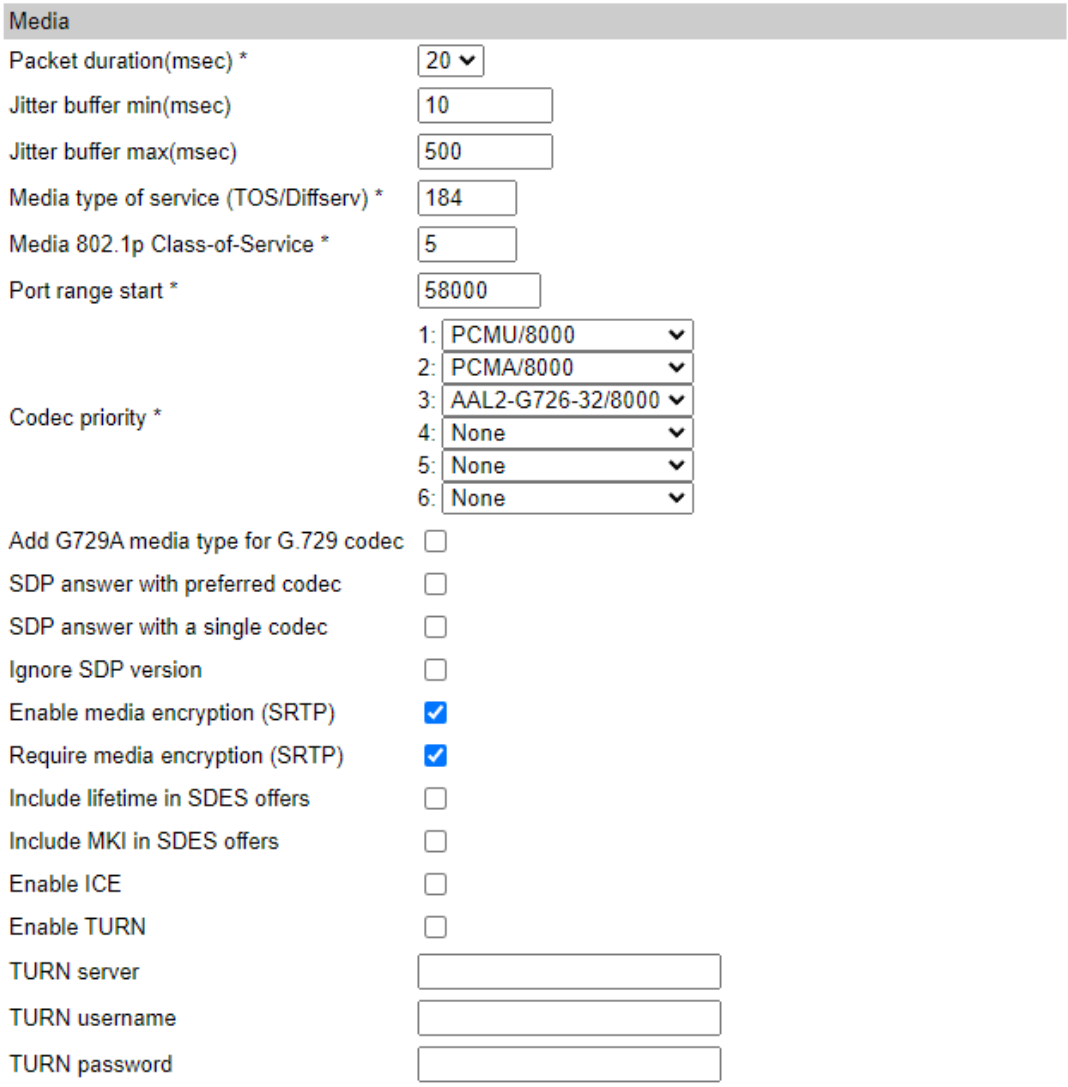
Field	*Setting*
SIP Configuration – General	
Local port	5060

Field	*Setting*
Transport	TLS
DNS method	DNS SRV
Register each endpoint on separate port	Disabled
Send all messages to current registrar	Disabled
Allow internal routing fallback	Enabled
Registration expire (sec)	IP-DECT 200/400 – 600 sec IP-DECT 6500 – 1200 sec Virtual IP-DECT Server One – 2400 sec
Handset power off action	De-register
Blacklist timeout (sec)	300
GRUU	Enabled
NAT keepalive	SIP OPTIONS (rfc3261)
NAT keepalive interval (sec)	30
Send BYE with REFER	Disabled
Lync	Disabled
SIP Configuration – Media	
Jitter buffer min (msec)	10
Jitter buffer max (msec)	500
Enable media encryption (SRTP)	Enabled
Require media encryption (SRTP)	Enabled
Include lifetime in SDES offers	Disabled
Include MKI in SDES offers	Disabled
SIP Configuration – Call status	
Call waiting	Enabled
Wireless Server Configuration – DECT	
Subscription allowed	Enabled
Automatically disable subscription allowed	Disabled
Access code (IP-DECT Server 200/400)	Default value: last 4 digits of the ARI code
Handset login (SfB)	Disabled
Handset sharing	Disabled
Provisioning Configuration – Default server	
NOTIFY check_sync	Disabled

Field	*Setting*
Provisioning Configuration – Firmware server	
NOTIFY check_sync	Disabled
Provisioning Configuration – License server	
NOTIFY check_sync	Disabled
Provisioning Configuration – Configuration and users server	
NOTIFY check_sync	Disabled
Phonebook Configuration – System user data	
Sync time(hh:mm)	00:00
Security Configuration – Data protection	
Remove user passwords from exported data	Enabled

SIP Configuration

General	
Local port *	5060
Transport *	TLS
DNS method *	DNS SRV
Default domain *	example.com
Register each endpoint on separate port	☐
Send all messages to current registrar	☐
Allow internal routing fallback	☐
Registration expire(sec) *	2400
Max pending registrations *	1
Handset power off action	De-register
Max forwards *	70
Client transaction timeout(msec) *	16000
Blacklist timeout(sec) *	3600
SIP type of service (TOS/Diffserv) *	96
SIP 802.1p Class-of-Service *	3
GRUU	☑
Use SIPS URI	☐
TLS allow insecure	☐
TCP ephemeral port in contact address	☐
NAT keepalive	SIP OPTIONS (rfc3261)
NAT keepalive interval(sec)	30
Send Hold before REFER	☑
Send BYE with REFER	☐
Convert SIP URI to phone number	☑



Jitter buffer

The jitter buffer is a feature that helps with mitigating RTP packet jitter by temporarily storing incoming packets and releasing them at a constant rate. It has the following default values:

- Jitter Buffer min (msec): 10 (with a range of 10-1000)
- Jitter Bugger max (msec): 500 (with a range of 10-1000)

If persistent audio delays are experienced, the buffer max values can be further adjusted to a lower value (eg. 300 or even 100). Once set, these settings are sent to all connected media resources, including new media resources connecting to the IP-DECT Server.

Note:

The feature codes used for call forwarding are also automatically configured by Microsoft and cannot be changed from the IP-DECT Server Web interface.

Note:

The IP-DECT Server backup function will be unable to backup user data when the server is configured for Microsoft Teams.

Chapter 5: Handset onboarding and Sign-in

Below is a description on how to setup a handset to connect to a Spectralink IP-DECT Server configured with Microsoft Teams. This section assumes that the DECT handsets have been upgraded to firmware version PCS22Ab or newer, prior to performing the following steps. This process consists of two parts:

The onboarding phase, in which the handset subscribes to the Spectralink IP-DECT Server and is provisioned securely by the Microsoft Teams provisioning server. Once the handset has received the onboarding configuration, it will register on the onboarding server, and it will be ready for the next phase.

The sign-in phase, in which the user signs into Microsoft Teams, by pairing the handset with their Microsoft Teams account. This can be done in three ways:

- As a **local sign-in** on the handset, by getting the pairing code directly on the DECT handsets Teams menu after selecting sign-in.
- As a **remote sign-in**, initiated from the Spectralink IP-DECT Server GUI. You can generate up to 10 pairing codes at the same time. Each pairing code will also have a link directly to the Microsoft Sign-in page, where the code will be automatically copied.
- As a **sign-in using the Teams admin center**, where the admin adds the handset's IPEI as the MAC address on a provisioned user and activates the handset by sending a *55*+verification code to the onboarding server. The handset is then found under the *Waiting for sign-in* tab, where you can get the paring code for the handset for the normal device login and sign-in procedure.

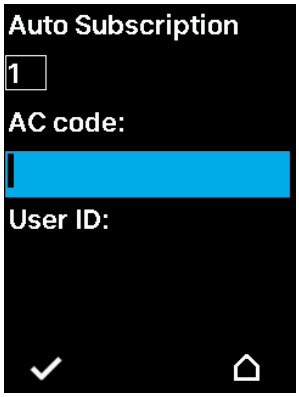
Note:

Local sign-in is only available on Spectralink Handsets.

Handset onboarding

To connect the handset to the Microsoft on-boarding server

1 Turn on the DECT handset. The following screen should be displayed:



Note:

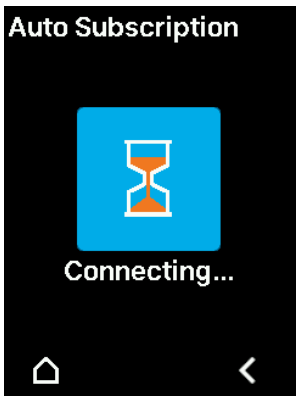
If the above screen is not displayed, the handset needs to be restored to the default factory settings. In order to perform a factory reset, type *99940* HOOK key and OK. The factory reset PIN code is 0000.

The Auto subscription screen will be displayed after the handset reboots.

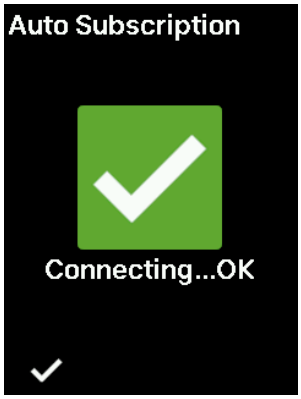
2 Subscribe the handset:

- IP-DECT Server 200 or 400: Input the **AC code** into the field. The **AC code** consists of the last 4 digits of the ARI, and can be viewed either from the IP-DECT server Web interface (Status -> General), or from the label on the rear side of the server.
- IP-DECT Server One or IP-DECT Server 6500: enable subscription on the DECT server and you will be able to subscribe the handset without an AC code or you can set a code in the web UI.

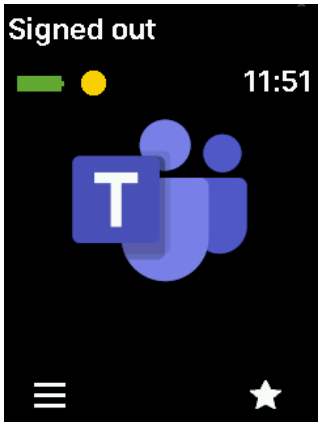
3 The handset will now attempt to subscribe to the server (this process may take several minutes)



After a successful OTA connection is established, the following icon will be displayed:



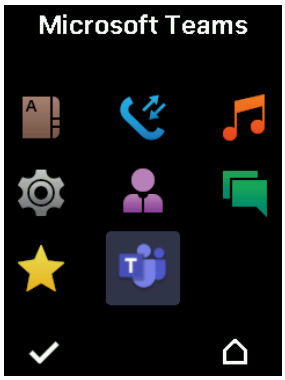
4 The handset will automatically begin the on-boarding process. After a few seconds the handset screen should indicate a successful connection:



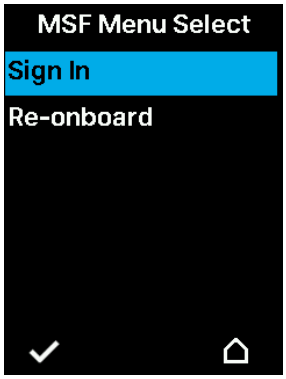
Local and Remote Sign-in

To locally sign-in to Microsoft Teams

1 Press the Menu softkey on the handset, and select the “Microsoft Teams” option



2 Select Sign in



3 The handset will request a pairing code from Microsoft

If successful, the handset will display a pairing URL and code, similar to the ones below:

4 Note down the URL and the pair code.

Note:

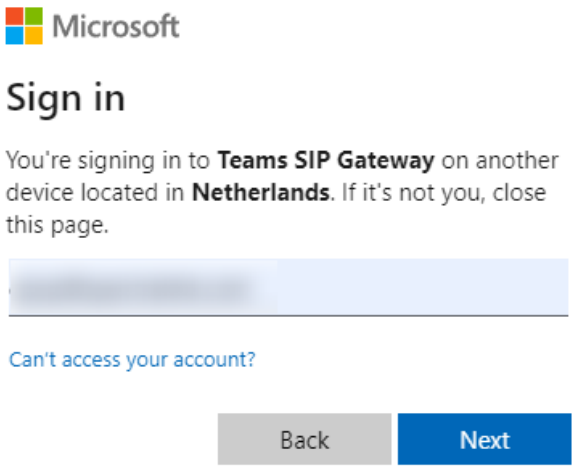
If the pairing URL and code are not displayed, make sure that your DHCP server provides NTP and DNS services to the DECT system, and that it has access to the internet.

Your firewall might need to be configured according to Microsoft specifications.

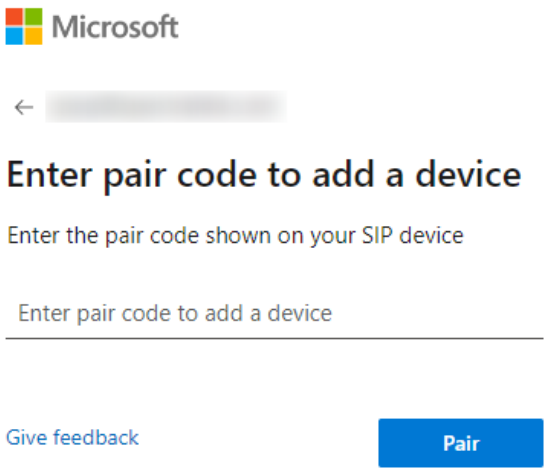
5 The rest of the sign-in process is done on a PC or smartphone with an internet browser:

a. Go to the pairing URL: https://aka.ms/siplogin

b. If you're not already logged in, you will be prompted to log into your Microsoft Teams account in order to pair the device

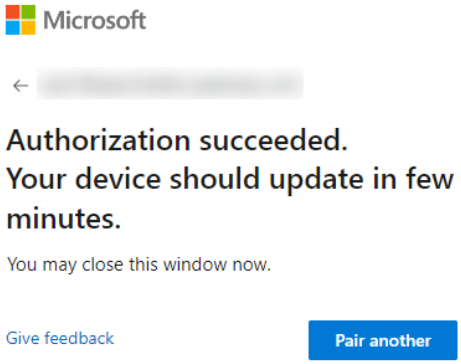


c. Enter the pair code:

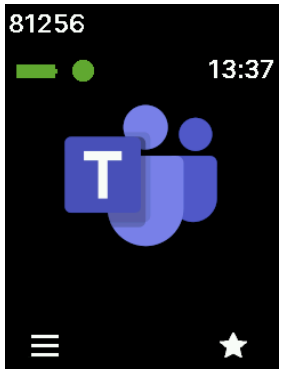


Note:
The pairing code is **not** case sensitive.

d. After the following screen is displayed, the sign-in process will be complete and you can safely close the page or pair another device.

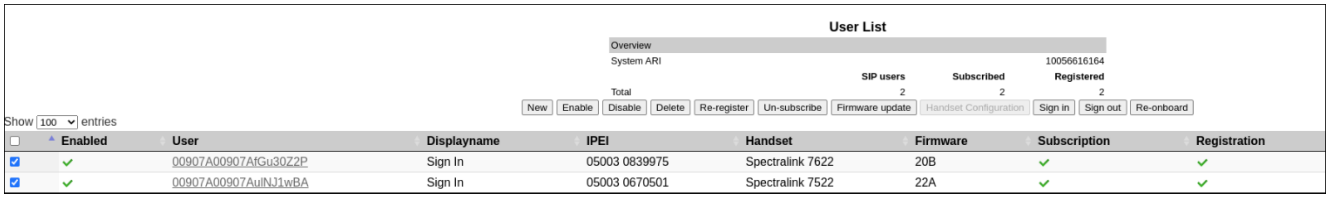


It might take a few minutes for the DECT Server to pair the handset with your Teams account. After the pairing process is complete, your DDI number and the green status icon will be displayed on the screen, indicating that the handset is registered and ready to use:

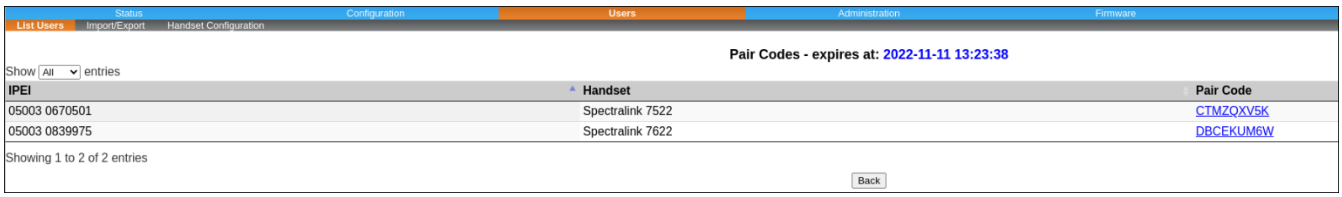


To remotely sign-in to Microsoft Teams

1. Access the IP-DECT server GUI and navigate to **Users** -> **List Users**.
2. Select up to 10 users, using the checkbox in the leftmost column.



3. Press the **Sign in** button, and a new Pair code will be generated.



4 Each pair code will have a link pointing to the Microsoft Teams Sign-in page. Clicking on any of the pair codes will open the Microsoft Teams Sign-in page.

5 Once on the Microsoft Teams Sign-in page, the pairing code will be automatically copied. You can either paste it, or manually input it into the Code field, and then follow the Sign-in steps presented at Step 5 here.

Teams Admin Center Sign-in

In addition to the **local and remote sign-in** methods, administrators can also opt to use the **TAC sign-in** method to sign-in one or multiple devices from the Teams Admin Center. To sign-in using the Teams Admin Center:

Add a device MAC address

Before adding a device MAC address, you must first complete the following steps to provision a new device:

1 Sign into the Teams admin center.

2 Expand **Teams Devices** and chose **SIP devices**.

3 Select **Provision devices** from the **Actions** tab found the upper right corner.

In the **Provision devices** window, you can either add the MAC address manually, or upload a file. The MAC address for a DECT handset is the handset IPEI number.

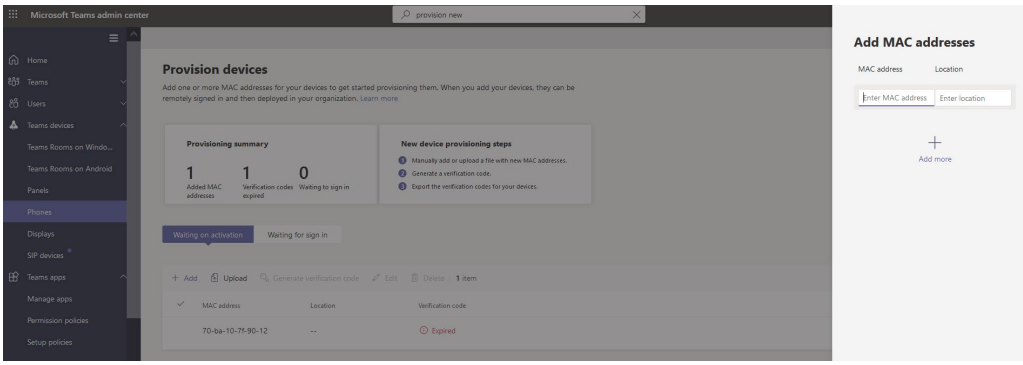
Note:

You can identify the unique IPEI number on a handset in two ways:

- From the handset: **Menu**> **Status**> **General**
- From label by removing the battery cover and battery

To manually add a device MAC address:

1 From the **Waiting on activation** tab, select **Add.**



2 In the pop-out found in the right corner, enter the MAC ID (IPEI of the nadset).

3 Enter a location (optional), which can help administrators identify the server/location of the newly provisioned handsets.

4 Select **+ Add** to add more devices, or press **Apply** when finished.

To add MAC addresses via a file:

1 From the **Waiting on activation** tab, select **Upload MAC IDs**.

2 Download the file template from the pop-out window.

3 Enter the MAC ID (Handset IPEI) and location (optional), and then save the file.

4 **Select a file**, and then select **Upload**.

Generate a verification code

In order to continue the **TAC sign-in** process, a verification code must be generated. The verification code is generated on the device level, or in bulk, and is valid for 24 hours.

1 From the **Waiting on activation** tab, select an existing MAC ID and select **Generate verification code**. A code is created for the MAC address and is shown in the **Verification Code** column.

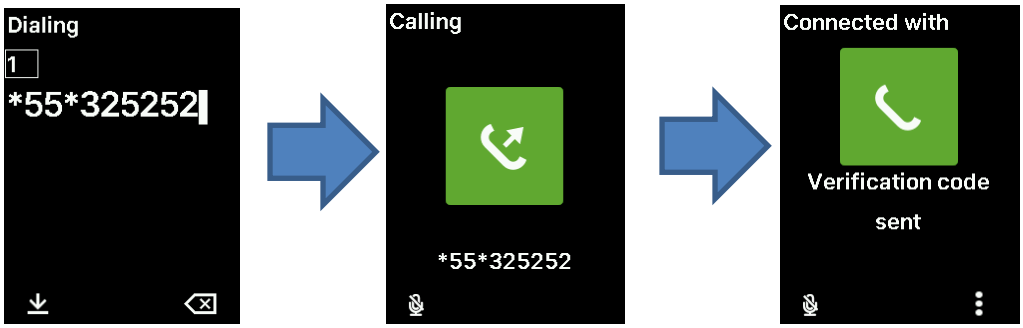
2 Provide the list of MAC IDs (IPEI) and verification codes to the field technicians. You can export the details directly into a file, by pressing the Excel icon on the right side. Once exported, you can share the file with the administrators who are doing the actual installation of the DECT system and handsets.

Provision the DECT handset

After the device is powered on and connected to the IP-DECT server (as per the onboarding process above), the administrator must provision the device.

This step must be completed on the DECT handset itself, using the verification code created in the previous step.

1 On a provisioned DECT handset, enter *55* followed by the activation code, and press the Off-hook key.

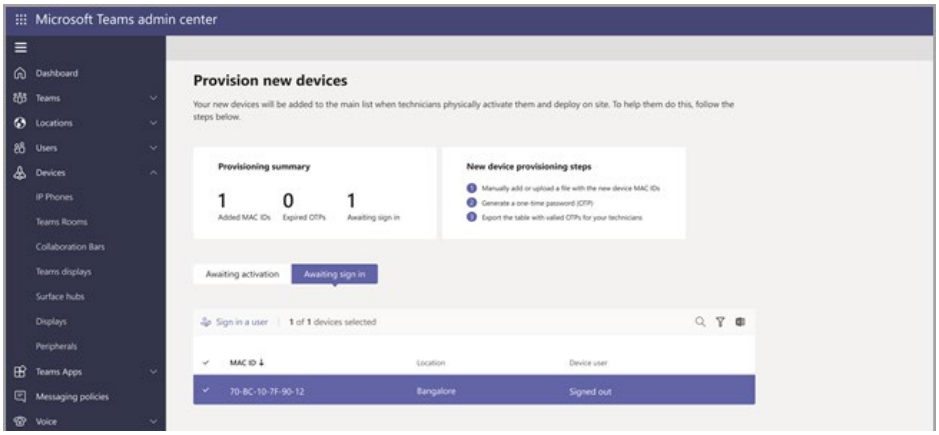


2 The handset will return “Verification code sent” in the handset’s display, and will hang-up after 10 seconds.

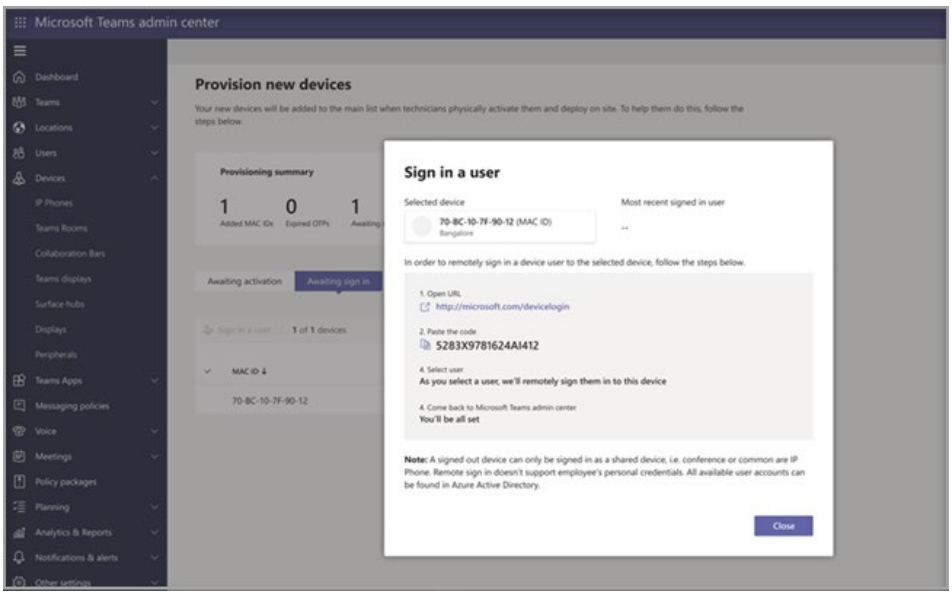
First-time remote sign-in

The provisioned device appears in the **Waiting for sign-in** tab. Start the remote sign-in process by selecting each device individually.

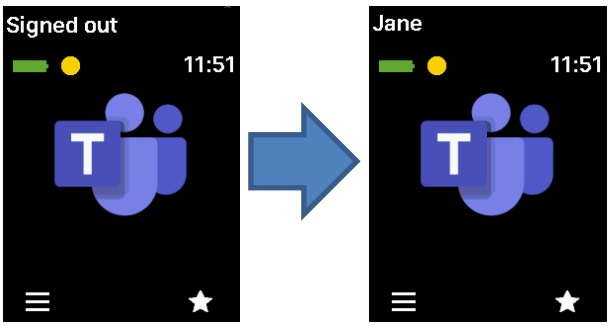
1 Select a device from the **Waiting for sign-in** tab.



2 Follow the instructions displayed in the **Sign in a user** box, and then select **Close** when done.



3 The DECT handset's display will show the display text chosen in the IP-DECT server Teams menu, with the default option set to Display name.

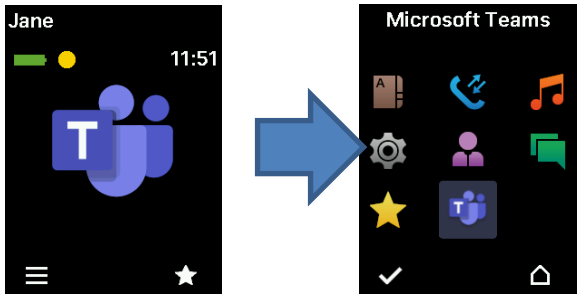


Chapter 6: Handset Sign-out

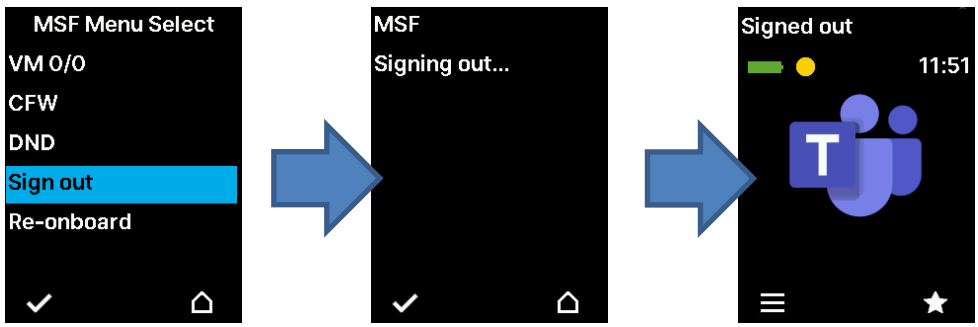
You can sign-out from Teams in different ways, either on the DECT handsets itself using the Teams menu, from the IP-DECT server GUI or directly from the Teams admin center (TAC).

To sign out from a DECT handset

1 Enter the handset Menu, and select Microsoft Teams



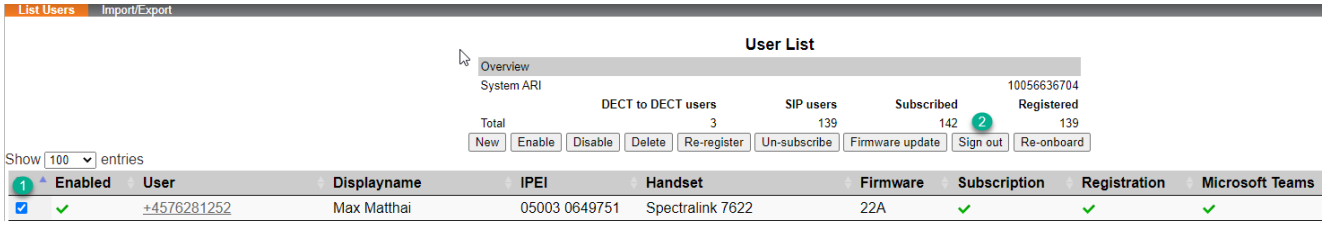
2 Select **Sign out**. The handset will display “Signing out…”, and will return to the idle screen, ready for a new sign-in.



To sign out a DECT handset from the IP-DECT server GUI

1 Access the IP-DECT server GUI and navigate to **Users** -> **List Users**.

2 Select the user(s) you want to sign out, and click the **Sign out** button.

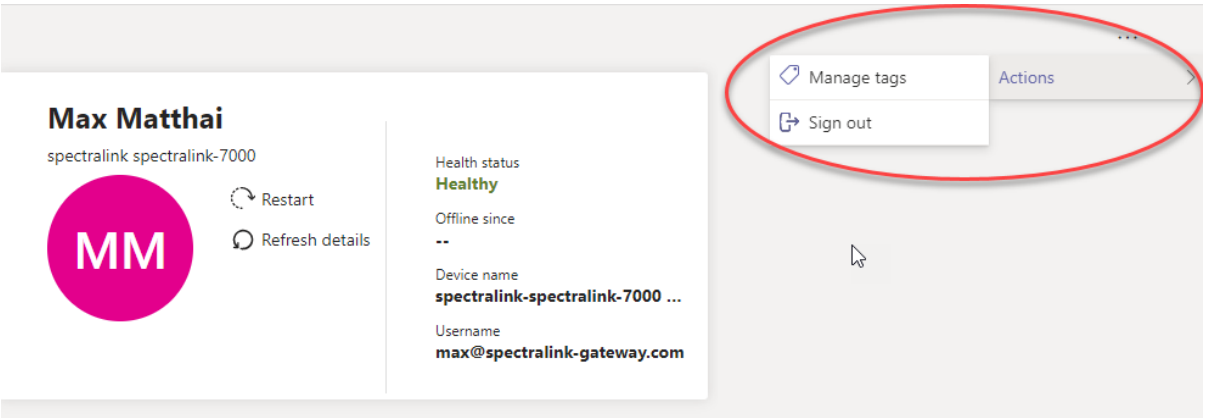


To remotely sign out a user from the Teams Admin Control Panel (TAC)

3 Log in to the Teams admin center and select **Teams devices** -> **SIP devices**

4 On the right side, in the SIP devices pane, select the device you want to sign out.

5 On the device's **Details** pane, select the **Details** tab. In the upper right corner on the **Actions** menu, select **Sign out.**



Chapter 7: Microsoft Teams Dynamic Location

This chapter provides an overview of the MS Teams SIP Gateway dynamic location feature, which enables precise tracking of a user's location during emergency calls.

Quick configuration

Step	Action	Details / Fields
1. Sign in	Go to Teams Admin Center	Sign in with Teams admin account
2. Create Emergency Location	Locations → Emergency addresses → Add	Enter name, country/region, street, city, postal code, verify & save
3. Add a Place	Locations → Places → Add	Choose emergency location → Add floor, wing, or room identifiers → Save
4. Add BSSID Location Matching **OR**	Select any Place -> Wi-Fi access points → Add	Enter BSSID (Available in Administration -> Dispatchable Locations on the IP-DECT Server) → Assign to emergency location → Apply
5. Add Switch Location Matching	Select any Place -> Ports -> Add (Also enable LLDP from Configuration -> General on the IP-DECT Server)	Enter Port and Chassis ID (Available in Administration -> Dispatchable Locations on the IP-DECT Server) -> Assign to emergency location -> Apply

✔ **Result: Users' emergency calls will include correct validated address & location info (auto-detected via BSSID if configured).**

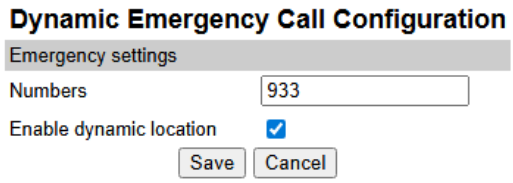
Detailed instructions on how to configure the IP-DECT Server and the Teams Admin Center are provided in the section below.

Configuring the IP-DECT Server

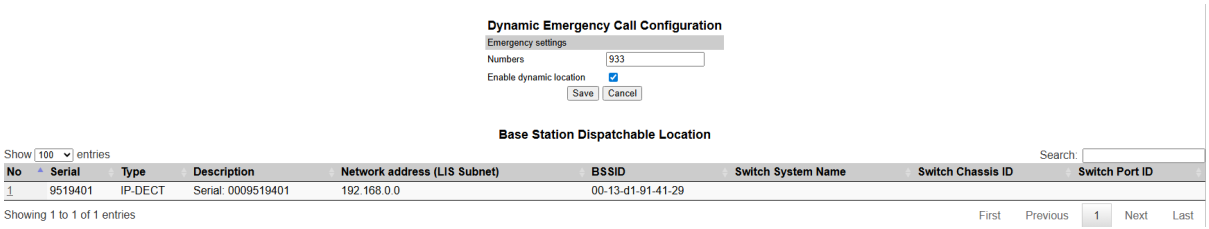
To enable the use of Dynamic Location, the feature must first be activated on the IP-DECT server. This functionality can operate with or without LLDP.

Dynamic Location is only available on the Spectralink IP-DECT Server once the server has been provisioned for MS Teams and the MS Teams feature has been enabled via **Administration** -> **Features**. To Enable Dynamic Location:

1. Log in to the IP-DECT Server.
2. Navigate to **Administration** -> **Dispatchable Locations**
3. Input an emergency number
4. Check the **Enable Dynamic Location** box and click **Save**.



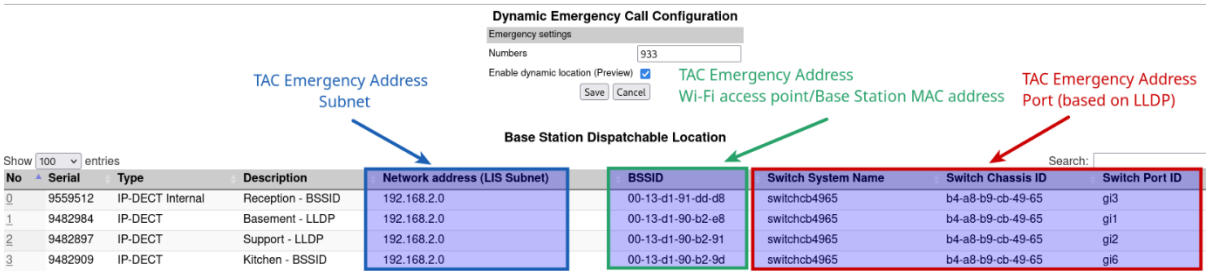
Once the settings are saved, the server will create a **Base Station Dispatchable Location** table, displaying all connected Base Stations installed at various locations throughout the site.



If using LLDP to detect the location of the base station

1. Navigate to **Configuration** -> **General** -> **LLDP.**
2. Select the "**Enabled**" checkbox to enable LLDP-based detection of Switch Chassis and Port ID.

When enabling LLDP, the **Base Station Dispatchable Location** table will display additional information regarding the Switch System Name, Switch Chassis ID and Switch Port ID. All the dispatchable location information in the table can also be used to configure the Teams Admin Center (TAC) directly.



Teams Admin Center Emergency Location Configuration

Determining the Emergency Location Match Order

In Microsoft Teams, determining a user's emergency location (also known as the emergency address) is essential for accurate Emergency Calling (E911) support. Teams uses a prioritized matching order of network identifiers to automatically assign the appropriate emergency location. This ensures the most precise and reliable location is selected based on the available network data.

Emergency Address Match Order (Highest to Lowest Priority):

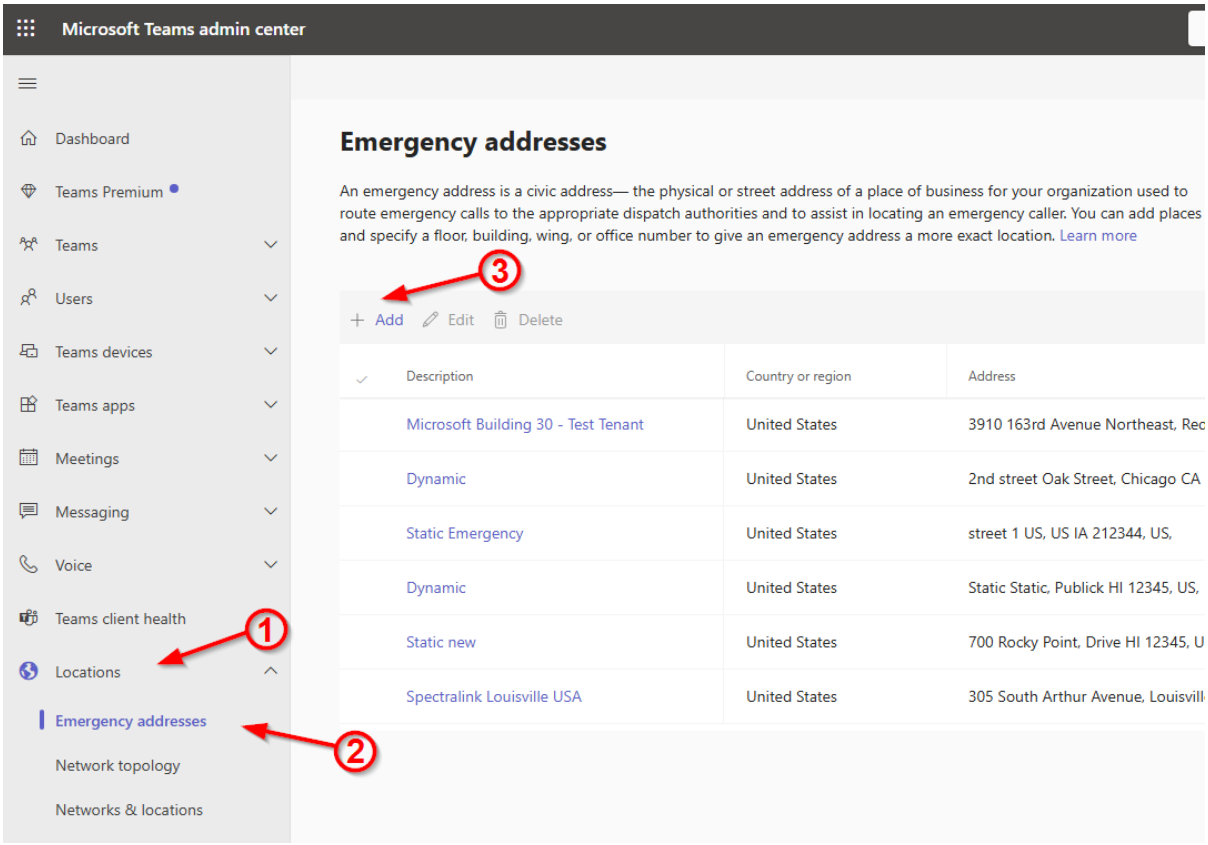
1. **BSSID** – Basic Service Set Identifier: Unique identifier for Wi-Fi or DECT base station access points. Provides the highest level of location accuracy.
2. **Subnet** - IP Subnet (Network Address): Matches users based on their Base Station's IP subnet.
3. **Port** - Switch Port: Identifies the specific port on a network switch where the Base Station is connected.
4. **Chassis ID** - Switch Identifier: Usually a MAC address; identifies the switch itself if port-level information isn't available.

Teams attempts to match a user's location using this order. Once a match is found, the corresponding emergency location is assigned, and the process stops - ensuring the most granular match is always used.

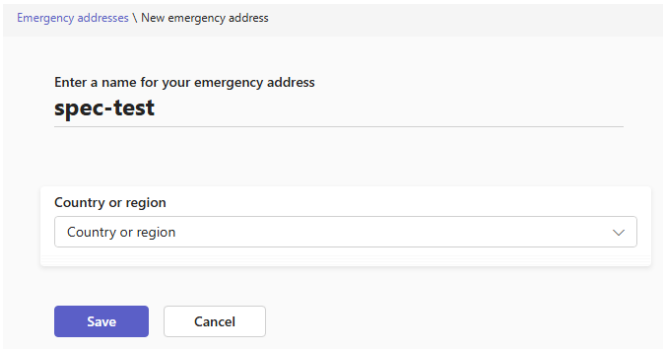
Configuring Emergency Addresses in Teams Admin Center

To set up emergency locations:

1. Log in to the Microsoft Teams Admin Center.
2. Navigate to **Locations** -> **Emergency Addresses** and click **Add** to create a new emergency address.

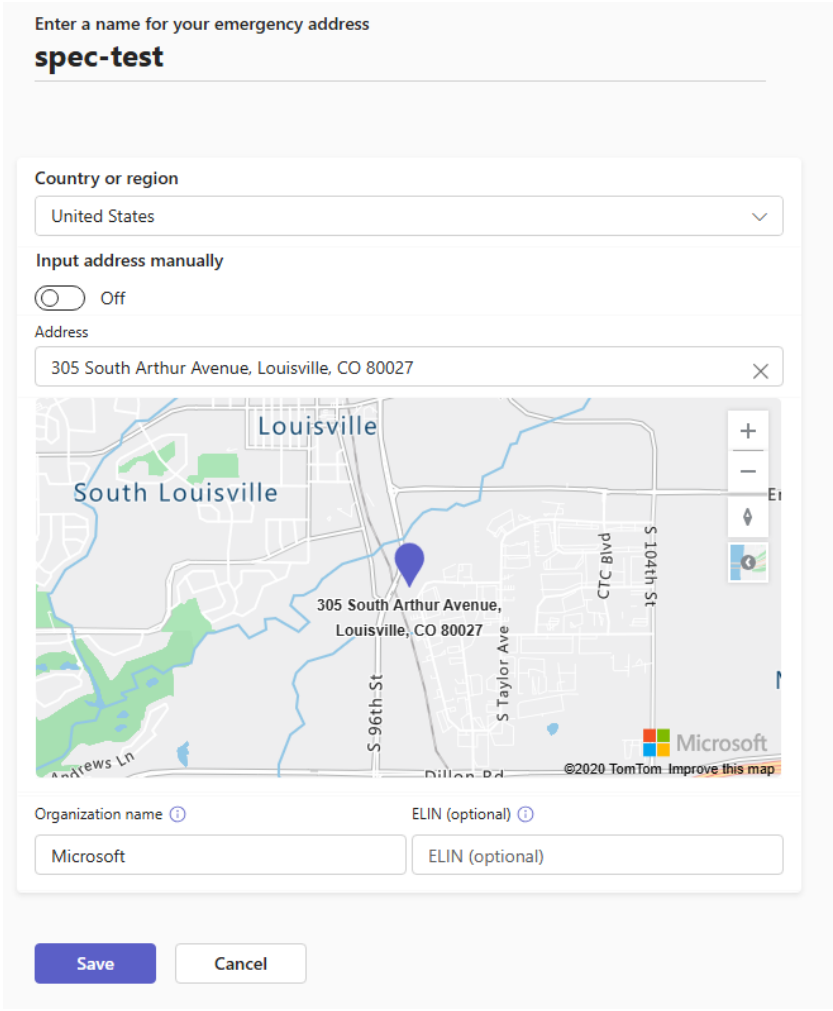


3. On the next scree, enter an emergency address name and select your country



4. Selecting your country will display a few additional fields where you can input:
    - Address: Input your address here.
    - Organization name: The organization name of your tenant is pre-populated in this field, but it can be edited.
    - ELIN (Optional): When dividing your emergency addresses into locations or places, each emergency location can have one or more ELINs (Emergency Location Identifier Numbers) with different numbers for dialing emergency services. See the Microsoft Teams documentation for more details.

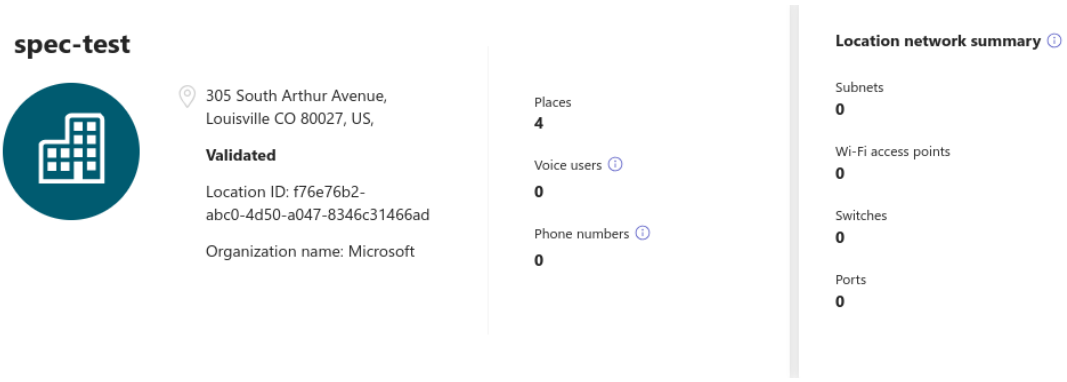
    If the address isn't found, turn on **Input address manually** for a more detailed address input form.



5. Select **Save**.
6. After the address has been created, make sure it has been Validated. This can be viewed in the Emergency Address list, or by selecting the newly created address.

Note:

Once an emergency address has been validated it cannot be edited.



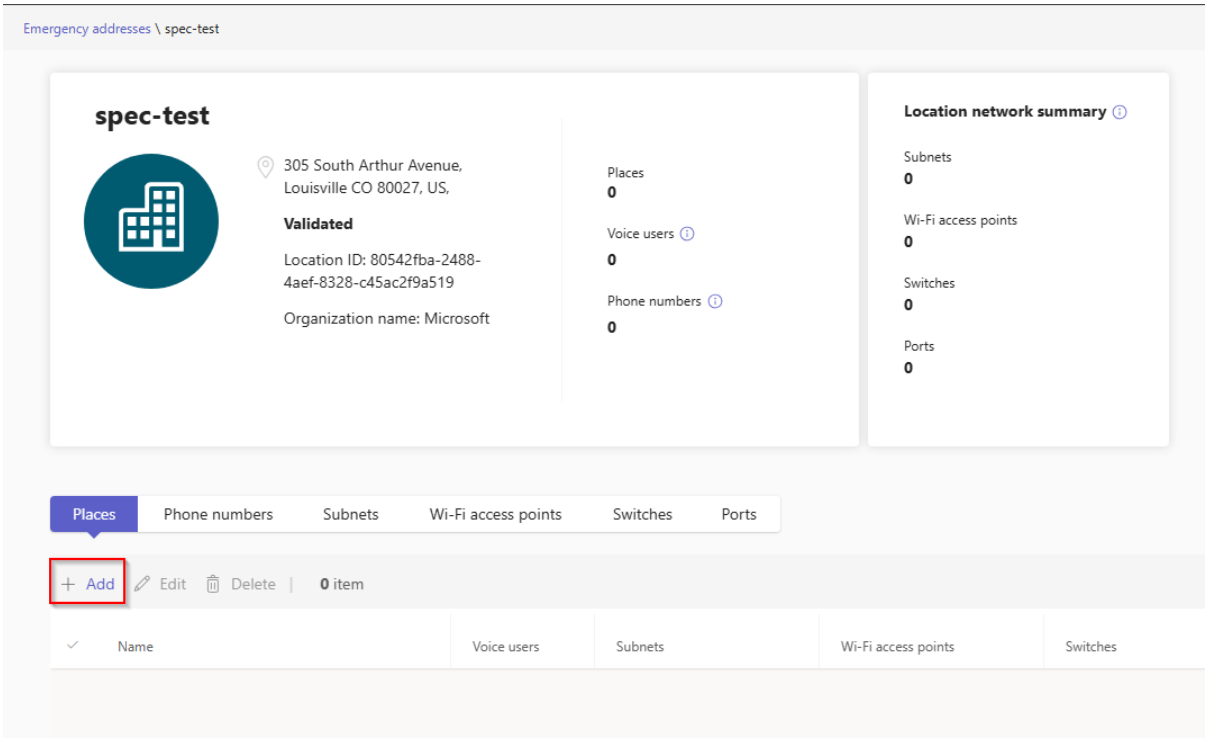
Location matching methods

In this section, we will go through the different location matching methods available in the Teams Admin Center and explain how to configure each one individually.

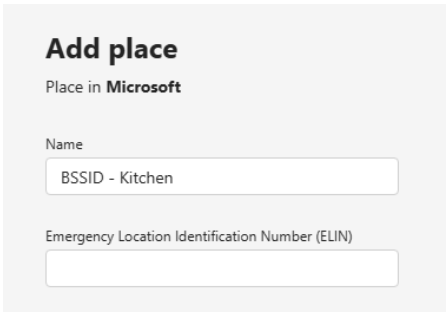
BSSID (Wi-Fi Access Point)

To enable BSSID location matching:

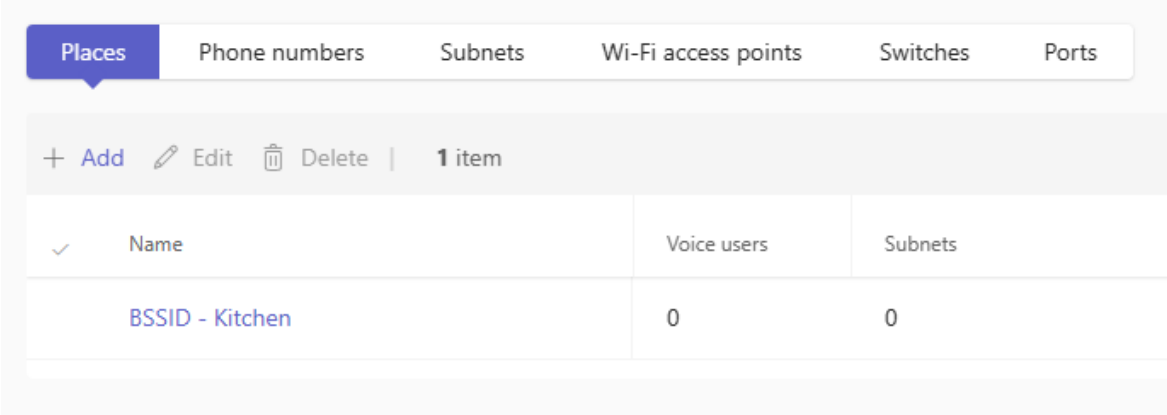
1. Navigate to **Locations** -> **Emergency Addresses** in the Teams Admin Center.
2. Select the desired emergency address (the previously created spec-test address in our example)
3. In the **Places** tab, select the **Add** button.



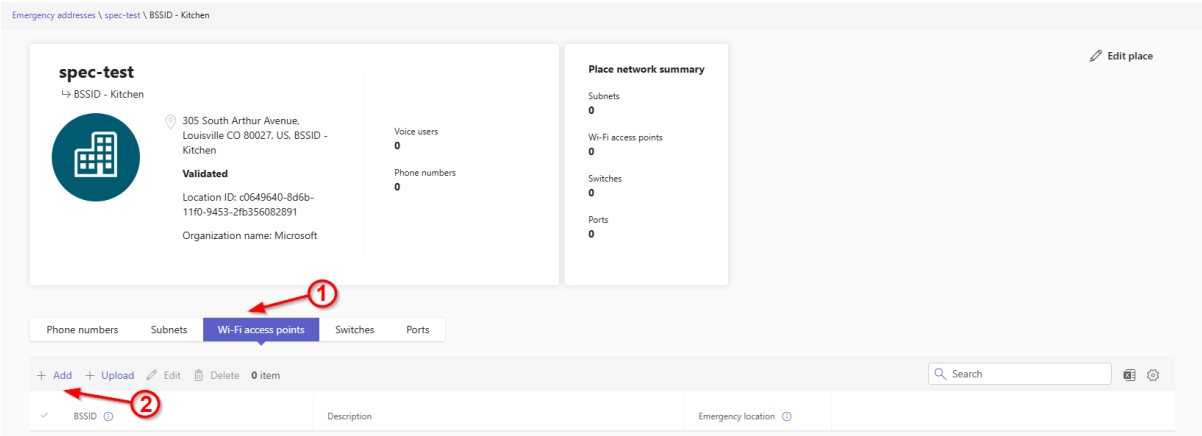
4. Add a name, optionally an ELIN and select **Apply**.



5. From the **Places** tab, select the newly created place (**BSSID – Kitchen** in this case)

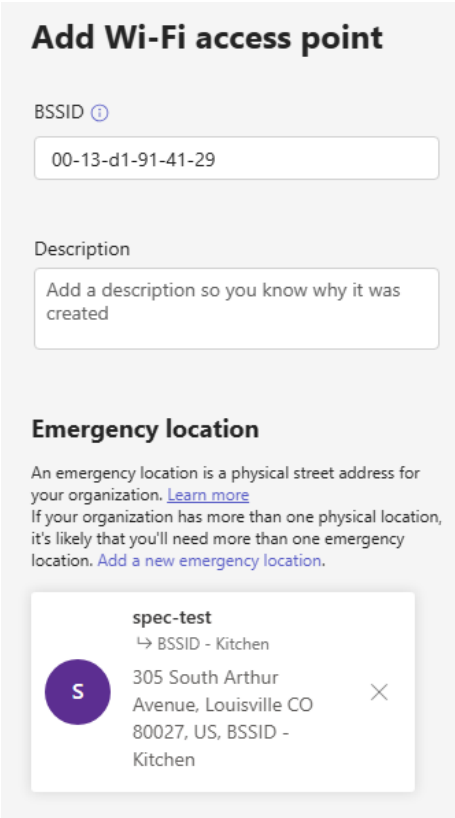


6. Navigate to the **Wi-Fi access points** tab and select **Add**.



7. On the next screen, input the Base Station BSSID and optionally a description.

   The BSSID can be acquired from the IP-DECT Server GUI from: **Administration** -> **Dispatchable Locations**.



Note:

Refresh the page if the **Emergency location** is not automatically updated at this step.

8. Select **Apply**.
9. Repeat steps 6 through 8 for each additional Base Station located at the same place.

Note:

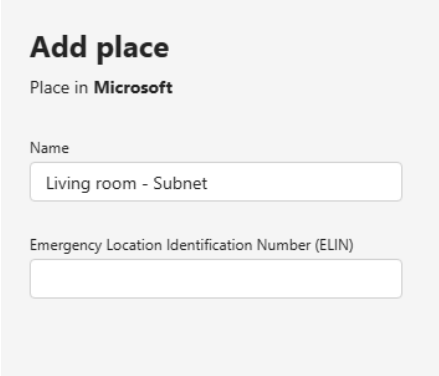
The Teams Admin Center location configuration must be updated whenever an IP-DECT base station is replaced.

Subnet

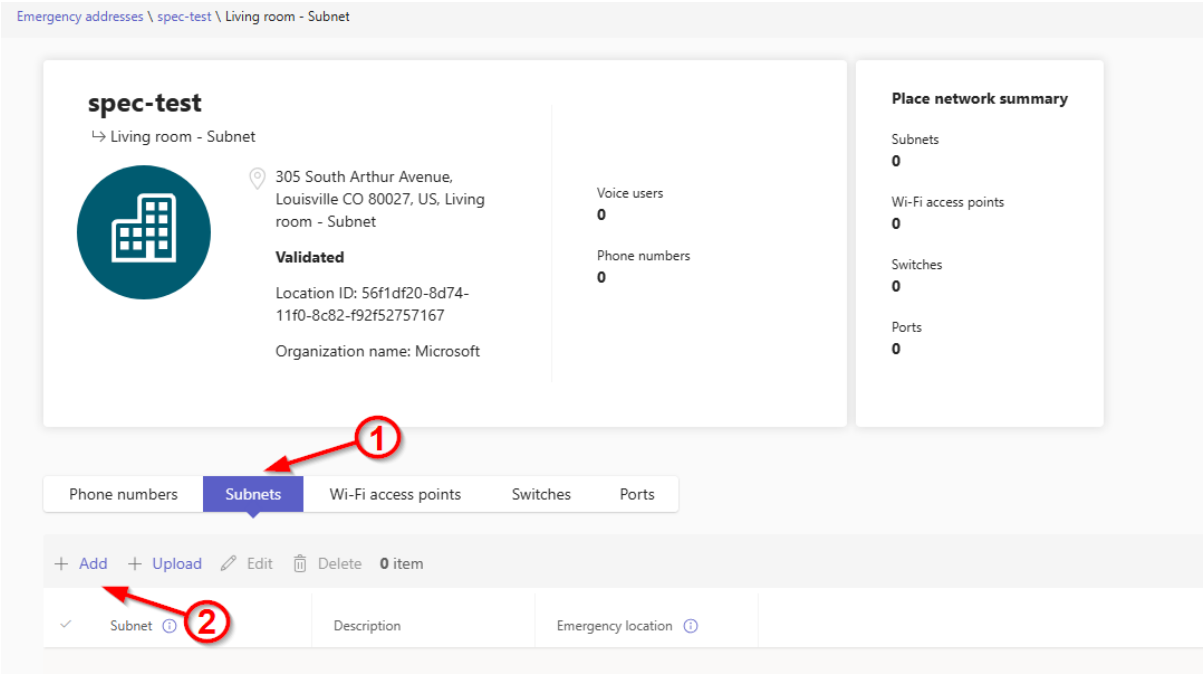
To enable Subnet location matching:

1. Navigate to **Locations** -> **Emergency Addresses** in the Teams Admin Center.
2. Select the desired emergency address (the previously created spec-test address in our example)
3. In the **Places** tab, select the **Add** button.

4. Add a **Name**, optionally an **ELIN** and select the **Apply** button.

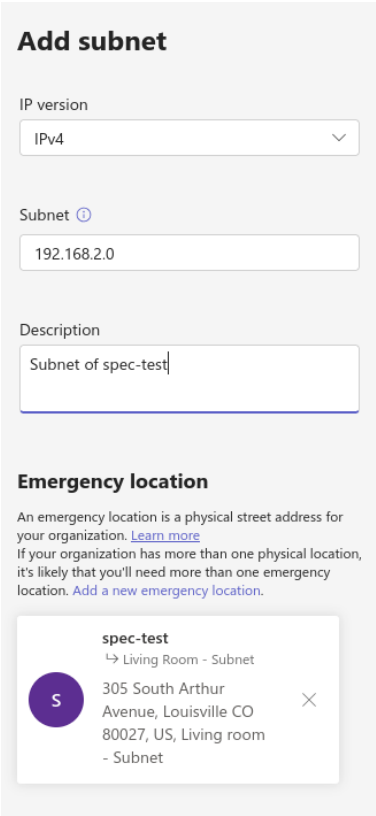


5. From the **Places** tab, select the newly created place (**Living room – Subnet** in this case).
6. Navigate to the **Subnets** tab and select **Add**.



7. On the next screen select IPv4 and add the **Base Station Network Address** in the **Subnet** field.

   The **Base Station Network Address** can be acquired from the IP-DECT Server GUI from: **Administration -> Dispatchable Locations**.



Note:

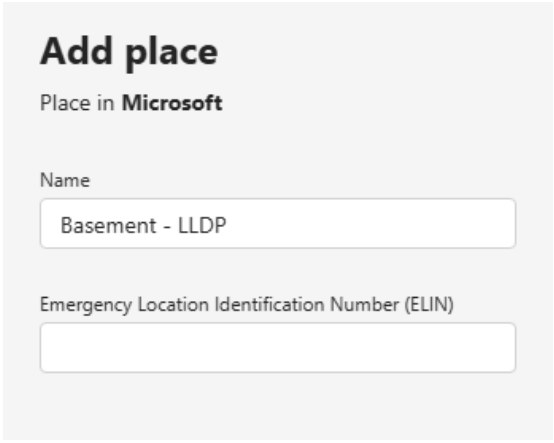
Refresh the page if the **Emergency location** is not automatically updated at this step.

8. Select **Apply**.
9. Repeat steps 6 through 8 for each additional Base Station located at the same place.

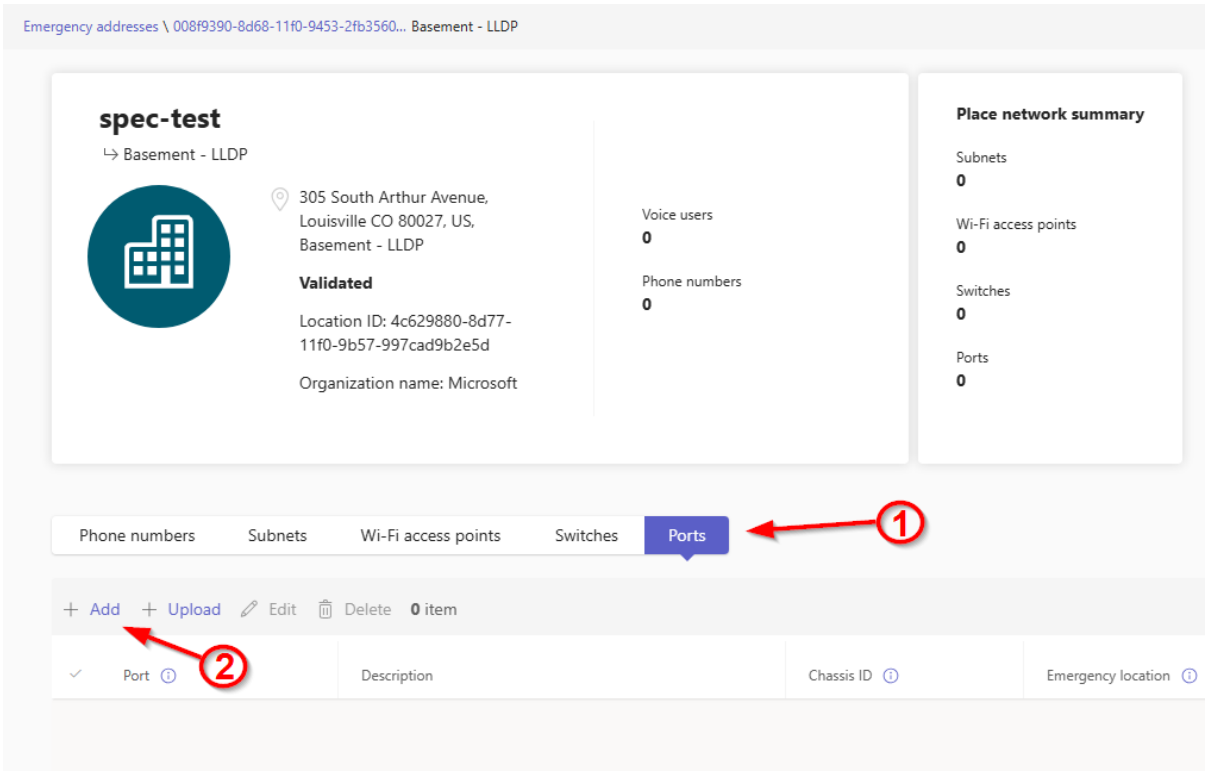
Switch Chassis ID and Port ID

To enable Switch Chassis ID and Port ID location matching

1. Navigate to **Locations** -> **Emergency Addresses** in the Teams Admin Center.
2. Select the desired emergency address (the previously created spec-test address in our example)
3. In the **Places** tab, select the **Add** button.
4. Add a **Name**, optionally an **ELIN** and select the **Apply** button.



5. From the **Places** tab, select the newly created place (**Basement – LLDP** in this case)
6. Navigate to **Ports** and select **Add**.

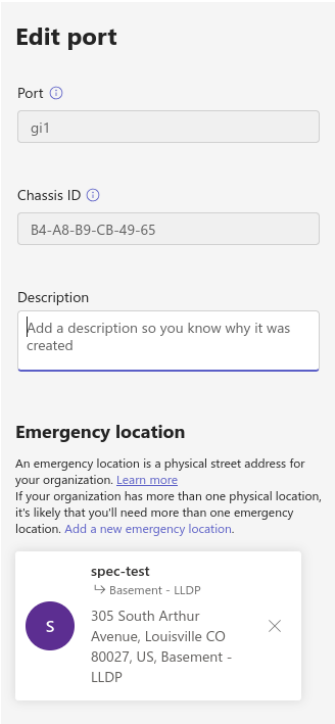


Note:

The process for enabling location matching strictly through Switch Chassis ID is identical to the one described in the following steps, but is handled through the **Switches** tab instead of the **Ports** tab, and does not use a port.

7. On the newly displayed page, input the **Port** and **Chassis ID**.

Both the **Switch Port ID** and the **Switch Chassis ID** can be acquired from the IP-DECT Server GUI from: **Administration** -> **Dispatchable Locations**.



Note:

Refresh the page if the **Emergency location** is not automatically updated at this step.

8. Select **Apply**.
9. Repeat steps 6 through 8 for each additional Base Station located at the same place.

Evaluation of Location Matching Strategies

Using LLDP

Advantages:

- No need to update the Teams Admin Center location configuration when replacing IP-DECT base stations.

Disadvantages:

- The network switch must support LLDP and have it enabled.
- Switch access is required for configuration and troubleshooting.

Using BSSID

Advantages:

- Only the MAC address of the IP-DECT base station is needed.
- Works independently of switch configuration (no need for LLDP support).

Disadvantages:

- The Teams Admin Center location configuration must be updated whenever an IP-DECT base station is replaced.

Test emergency number 933 (US Only)

The 933 number is a test emergency service available exclusively in the United States. It enables users and administrators to validate emergency call routing and location detection without contacting an actual emergency number such as 911.

This service is particularly valuable when configuring Microsoft Teams emergency calling, as it helps ensure that dynamic location information and routing policies are accurately implemented.

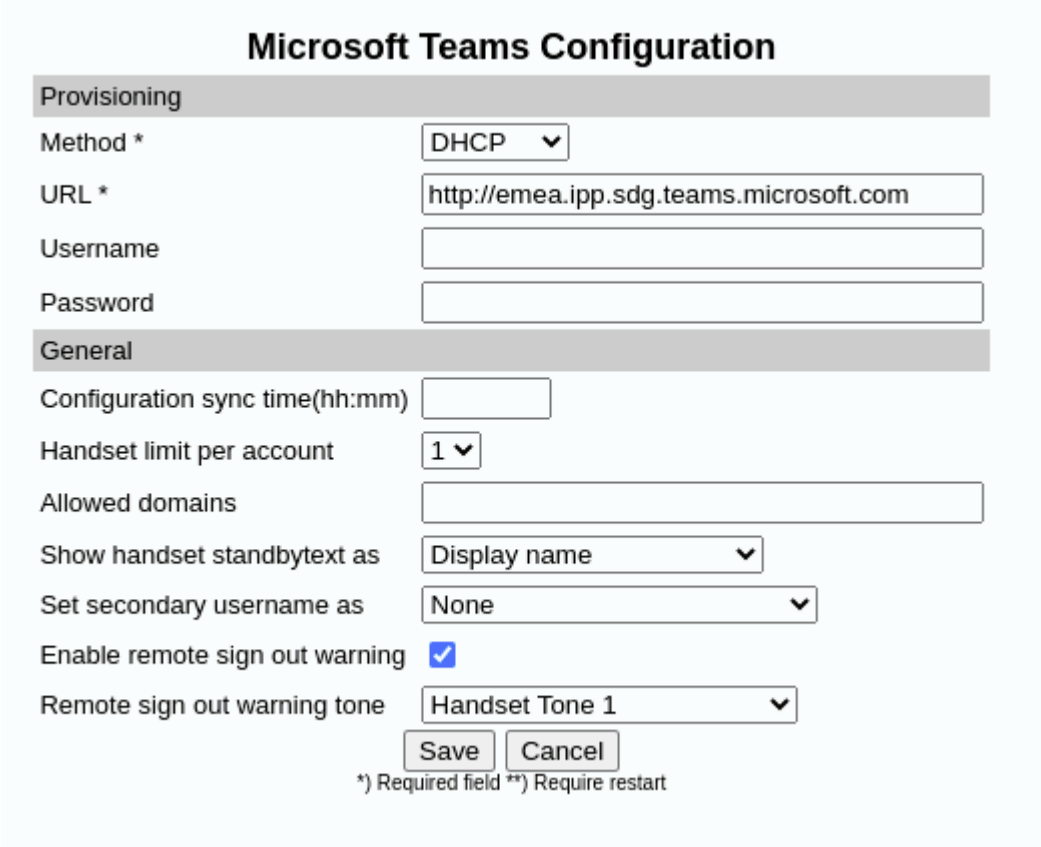
When dialed, 933 connects to an automated system that announces through the following information:

- The subscriber identifier (calling line ID)
- A confirmation whether you address, longitude and latitude are provided
- Your configured emergency address for that user
- In building location of the user identified by the base station, or by the base station’s switch chassis ID/port ID (if using LLDP)

Chapter 8: Migrating from other systems to Microsoft Teams

If your server is configured with other interfaces (Skype for Business, anynode SBC, Ring Central, etc.), there is a seamless migration process available that enables you to quickly reconfigure your server with Microsoft Teams, without requiring a factory reset.

To migrate from other systems to Microsoft Teams



1. Make a full system backup:
   a. Go to **Administration** -> **Backup**
   b. Press **Save** on the **Full system backup** option
2. Upgrade the IP-DECT Server firmware to version PCS22Aa or newer, and the Handset firmware to version PCS22Ab or newer.
3. Remove any licenses related to the previously installed interface:
   a. Go to **Administration** -> **License**
   b. Under **Loaded licenses**, find the relevant license (e.g., Skype for Business license) and click **Delete**

4 Add a valid Teams license. Please consult the License Installation section of this guide on how to add a license.

5 After applying the Teams license, the provisioning URL will be automatically set for the EMEA region. If the IP-DECT Server is located in a different region, the provisioning URL must be changed for your appropriate region in order for the provisioning process to commence. Alternatively, DHCP option 160 can be used to automatically get the provisioning URL. (See the provisioning settings in the Microsoft Teams Settings section)

Any handset already connected to the server will immediately begin the onboarding process as described in the Handset onboarding chapter, provided that it has the appropriate firmware version installed.

Note:

When a Microsoft Teams license is loaded on the IP-DECT server, all 3rd party handsets will be removed, with the exception of handsets configured as DECT to DECT.