

TEAMS DYNAMIC 911 GUIDE

[Category]

Prepared By – John Miller
Cloud Solutions Architect



jmiller@enablingtechcorp.com



+14436255192

Contents

CHAPTER 1 TEAMS DYNAMIC 911 AND 911 WORK FROM HOME.....	12
Introduction.....	12
What is Dynamic 911 and why it so Important	12
Microsoft Teams Support for Dynamic 911.....	12
Which Teams Clients support Dynamic 911?	13
Which Teams Clients and devices do not support Dynamic 911?	13
Which Teams Clients support Dynamic 911 for Work from Home?.....	13
Which Teams Clients and devices do not support Dynamic 911 for Work from Home?	13
Legal Requirements	13
Kari’s Law	14
RAY BAUM’s Act	14
State and Local Municipality Dynamic 911 Regulation	14
What do Companies using Microsoft Teams Voice need to consider when setting up Dynamic 911?	15
How does Microsoft Teams meet the Legal Requirements for Dynamic 911?	17
Kari’s Law	17
RAY BAUM’s Act	17
Summary	17
CHAPTER 2 PLANNING AND IMPLEMENTING EMERGENCY ADDRESSES AND LOCATIONS IN MICROSOFT TEAMS	19
Introduction.....	19
Overview and Terms.....	19
Teams Emergency Addresses.....	20
Teams Emergency Addresses “Description and Organization Name” Columns	20
Recommendation	21
Teams Locations\Places.....	21
Key Points	22
Adding Teams Emergency Addresses	22
Adding Teams Places	23
Summary	23
CHAPTER 3 CONFIGURING MICROSOFT TEAMS FOR KARI’S LAW COMPLIANCE	24
Introduction.....	24
Notification Requirement.....	24
Teams Emergency Calling Policy	24

Why should Emergency Calling Policies be dynamically assigned?.....	25
How are Emergency Calling Policies applied to Work from Home and other externally connected users? ...	26
Teams Objects for Dynamically Assigning Emergency Policies	28
Teams Tenant Trusted IP Addresses	28
Tenant Network Regions	29
Tenant Network Sites.....	29
Tenant Network Subnets.....	30
Direct Emergency Dialing Requirement	31
Teams Emergency Call Routing Policies	31
Notes for the Attributes.....	32
Typical Teams Emergency Call Routing Policy	34
Configuration Notes for Teams Emergency Policies.....	34
Summary.....	34
CHAPTER 4 CONFIGURING TEAMS TO COMPLY WITH RAY BAUM’S ACT	36
Introduction.....	36
Automatic Provisioning of Dispatchable Locations to Emergency Services	36
Determining the Microsoft Teams User’s current Dispatchable Location.....	36
Validated and Unvalidated Addresses.....	38
Microsoft Teams Calling Plan and Operator Connect Users	38
Microsoft Teams Direct Routing Users.....	38
Configuring Microsoft Teams to comply with the RAY BAUM Act for Dynamic 911.....	41
Teams Emergency Addresses and Locations\Places.....	42
Teams Tenant Trusted IP Addresses	42
Teams Location Information System (LIS) Database and Network Elements	42
Teams Admin Center	43
Using the Network Switch and Ports Network Elements to provide Dynamic 911 Locations.....	44
Defining Teams Locations for Network Switch Ports	44
A Tip from Experience	47
Suggestions.....	48
Summary.....	49
CHAPTER 5 TEAMS DYNAMIC 911 – WORK FROM HOME	50
Introduction.....	50
Is this feature turned on by default?	50
Teams Admin Center	50
Teams PowerShell.....	52

Who will this effect?52

Will there be any impact on Training, Corporate Health and Safety or Compliance Policies?53

How does this work?53

Can WFH be used if an On-Premises user cannot get a Dynamic 911 Location?60

Work from Home Call Flows61

Calling Plan and Operator Connect Users.61

Direct Routing Users62

Summary63

CHAPTER 6 MAKING TEAMS DYNAMIC 911 TEST CALLS64

 Introduction.....64

 Making test calls using the “933” Test Number65

 Making 911 Test Calls.....67

 Schedule a Test Call with the Local PSAP67

 Recording the Test Call.....70

 General Recommendations.....70

 Preparation.....71

 Performing the Test.....71

 Results Analysis72

 For Direct Routing users:72

 Summary73

CHAPTER 7 TEAMS TROUBLESHOOTING74

 Introduction.....74

 Prevention75

 Teams Client Troubleshooting.....76

Teams Desktop Client76

 933 Test Number82

 calling-debug.txt Debug Log File.....86

 Troubleshooting Teams with the calling-debug.txt.....87

Locating the Teams Dynamic 911 Information87

 File Structure89

 Information Contained in the “calling-debug.txt”90

 “calling-debug.txt” Section Definitions90

Location Policy Section90

 Current Emergency Address Section.....91

 Current MT Location Response92

Using the calling-debug.txt to troubleshoot the Current Location and other Issues 101

ERSP Troubleshooting 104

 Troubleshooting for Calling Plan and Operator Connect Users 105

 Troubleshooting for Direct Routing Users 107

Teams Dynamic 911 Test Plans 110

 Teams Dynamic 911 Client Test Plan 110

Sample Test Plans 112

Summary 114

CHAPTER 8 TEAMS DYNAMIC 911 LEGAL REQUIREMENTS, MAINTENANCE, DOCUMENTATION, TRAINING, AND OTHER SUBJECTS..... 115

 Training your users to not use Teams to make calls to Emergency Services 115

 Teams Installation Date and “Grandfathering” of Kari’s Law and the RAY BAUM Act 115

 Maintenance 115

 Documentation 116

 Training 116

CHAPTER 9 CONFIGURING TEAMS DYNAMIC 911 OBJECTS AND ELEMENTS 117

 Teams Emergency Addresses 117

Teams Admin Center 117

 Teams PowerShell 121

 Teams Locations\Places 122

Teams Admin Center 122

 Teams PowerShell 123

 Teams Emergency Calling Policies 125

Teams Admin Center 125

 Teams PowerShell 126

 Teams Emergency Call Routing Policies 127

Teams Admin Center 127

 Teams PowerShell 127

 Teams Tenant Trusted IP Addresses 128

Teams Admin Center 128

 Teams PowerShell 129

 Teams Tenant Network Regions 130

Teams Admin Center 130

 Teams PowerShell 131

 Teams Tenant Network Site 132

<i>Teams Admin Center</i>	132
Teams PowerShell.....	132
Teams Tenant Network Subnets.....	133
<i>Teams Admin Center</i>	133
Teams PowerShell.....	134
Teams LIS Network Element General Notes.....	135
Teams LIS Subnets.....	136
<i>Teams Admin Center</i>	136
Teams PowerShell.....	137
Teams LIS Wireless Access Points.....	139
<i>Teams Admin Center</i>	139
Teams PowerShell.....	140
Teams LIS Network Switches.....	141
<i>Teams Admin Center</i>	141
Teams PowerShell.....	142
Teams LIS Network Switch Ports.....	143
<i>Teams Admin Center</i>	143
Teams PowerShell.....	144
CHAPTER 10 PUTTING IT ALL TOGETHER: EXAMPLE TEAMS DYNAMIC 911 CONFIGURATION 145	
Fictional Company General Information and Locations.....	145
Risk Management Team.....	145
Building Configuration.....	146
Telephony Information.....	147
Wide Area Network Configuration.....	148
Local Area Network Configuration.....	148
Wired.....	148
Wireless.....	152
Internet Connectivity.....	154
Teams Telephony Configuration.....	154
Corporate Security.....	155
PCI Dynamic 911 Calling Requirements.....	155
Dispatchable Locations.....	155
Analog Devices.....	156
Work from Home and Externally Signed on Users.....	156
Emergency Call Notifications.....	157

Emergency Call Routing for the Direct Routing Users.....	157
Teams Dynamic 911 Configuration.....	157
High Level Process.....	157
Emergency Response Service Provider (ERSP).....	159
Emergency Addresses.....	159
Places\Locations.....	161
Emergency Call Routing Policies	162
Emergency Calling Policy	164
Tenant Trusted IP Addresses	166
Tenant Network Regions	167
Teams Tenant Network Sites.....	168
Teams Tenant Network Subnets.....	169
Dynamic 911 – Location Information System (LIS) – Network Elements.....	172
Dynamic 911 Location Derivation Analysis and Conclusions.....	173
Subnet Network Elements	175
Wireless Access Points Network Elements.....	177
Network Switch Network Elements.....	179
Network Switch Port Network Elements.....	180
REFERENCES.....	182
Federal Communications Commission	182
Microsoft Dynamic 911 and Work from Home.....	182
Microsoft – Other Relevant Teams Voice Articles	182
ACRONYMS.....	183
INDEX	184

Table of Figures

Figure 1 NASA VAB - Kennedy Space Center	16
Figure 2 Teams Emergency Addresses	20
Figure 3 Boeing Everett Production Facility	26
Figure 4 Teams Emergency Calling Policy Attributes	27
Figure 5 Adding a Teams Emergency Calling Policy	28
Figure 6 Complex Tenant Network Site Configuration	30
Figure 7 Emergency Call Routing Policy Attributes	32
Figure 8 Sample Teams Emergency Call Routing Policy	34
Figure 9 Sample PIDF-LO Information from an SBC Syslog	39
Figure 10 Adding Teams LIS Network Elements	43
Figure 11 WireShark Trace with LLDP-MED Information	45
Figure 12 LLDP-MED Information from the PSDiscoveryProtocol PowerShell Module	46
Figure 13 Example Input for LIS Port Information	46
Figure 14 Emergency Location Information for A Teams user on an internal on-premises Network	47
Figure 15 Bad Wiring Closet	48
Figure 16 Enabling the Work from Homes External Location Lookup Mode	51
Figure 17 Enabling the Work from Home External Location Lookup Mode-cont'd	52
Figure 18 Teams WFH - Suggested and Unverified Address	55
Figure 19 WFH – Editing or Confirming the Suggested Address	55
Figure 20 Editing the Suggested Address	56
Figure 21 Teams Suggested Addresses based on User Input	56
Figure 22 Teams Cannot Provide a Suggestion for the typed Address.	57
Figure 23 Manual Address Entry	57
Figure 24 Manual Input of Correct Current Location	58
Figure 25 WFH - Location Not Detected.	59
Figure 26 WFH - Manually entering an Address.	59
Figure 27 Teams Dynamic 911 WFH - Call handling Logic - Calling Plan and Operator Connect Users	61
Figure 28 Teams Dynamic 911 WFH - Call handling Logic - Direct Routing Users	62
Figure 29 Current Emergency Location in the Teams Client	64
Figure 30 Current Location from the Calls Tab in the Teams Client	65
Figure 31 Emergency Location	68
Figure 32 Emergency Services information for Albany County, NY	68
Figure 33 State Level 911 Administrator Contact Information Lookup	69
Figure 34 NY State 911 Administrator Contact Information	70
Figure 35 Current Dynamic 911 Location in the Teams Client	76
Figure 36 Hovering over the Current Location	77
Figure 37 Troubleshooting the Current Location and Drop-Down Options of an on-premises user	78
Figure 38 Troubleshooting the Current Location and Drop-Down Options of a Work from Home User	79
Figure 39 Current Dynamic 911 Location Missing	79
Figure 40 Accessing the Emergency location under Settings in the Teams Client	82
Figure 41 Teams Call Window when dialing 933	83
Figure 42 Creating the Teams Debug Logs	86
Figure 43 Locating the "calling-debug.txt" file on a Windows Desktop	87

Figure 44 Locating the Teams Dynamic 911 Information in the "calling-debug.txt" file	89
Figure 45 "calling-debug.txt" - Location Policy Section	91
Figure 46 "calling-debug.txt" "type" field values	92
Figure 47 "calling-debug.txt" - Current Emergency Address Section	92
Figure 48 "calling-debug.txt" - Current MT Location Response - emergencyCallingPolicy Sub-Section	93
Figure 49 "calling-debug.txt" - Current MT Location Response - emergencyCallRoutingPolicy Sub-Section	93
Figure 50 "calling-debug.txt" - Current MT Location Response - networkRoamingPolicy Sub-Section	94
Figure 51 "calling-debug.txt" - Current MT Location Response - endpointNetwork and networkSiteId	94
Figure 52 calling-debug.txt - Current MT Location Response - locationinfo Sub-Section	94
Figure 53 calling-debug.txt - Current MT Location Response - address Sub-Section	95
Figure 54 calling-debug.txt - Current MT Location Response - enableLocationBasedRouting,siteAddress,subnetId	95
Figure 55 calling-debug.txt - Current MT Location Response - debugInfo\ncsDebugInfo Sub-Section	95
Figure 56 Locating Tenant Trusted IP Addresses in the TAC	96
Figure 57 calling-debug.txt - Current MT Location Response - debugInfo\siteMatchInfo Sub-Section	97
Figure 58 Locating Tenant Network Sites in the TAC	98
Figure 59 calling-debug.txt - Current MT Location Response - debugInfo\networkLocationMatchInfo Sub-Section	98
Figure 60 Locating an LIS Network Element and verifying its associated location in the TAC	99
Figure 61 Reverse method of locating an LIS Network Element and its associated location in the TAC	101
Figure 62 calling-debug.txt - Current MT Location Response - debugInfo\mtdebuginfo Sub-Section	101
Figure 63 Using the calling-debug.txt to Troubleshoot the Current Location of an On-Premises User	103
Figure 64 Using the calling-debug.txt to Troubleshoot a Work from Home User	104
Figure 65 Sample Teams Dynamic 911 Client on-premises Test Plan	112
Figure 66 Sample Teams Dynamic 911 - 933 bot Test Plan	112
Figure 67 Sample Teams Dynamic 911 - 911 Call Test Plan	113
Figure 68 Adding an Emergency Address	117
Figure 69 Adding an Emergency Address - Country	117
Figure 70 Adding an Emergency Address-Automatic	118
Figure 71 Adding an Emergency Address - Manual Entry	118
Figure 72 Adding an Emergency Address - Validated Address	119
Figure 73 Adding an Emergency Address - Completed	119
Figure 74 Teams Emergency Address in PowerShell	120
Figure 75 Teams Default Location Record for an Emergency Address	120
Figure 76 Teams Emergency Address - LocationID for Default Location	121
Figure 77 Adding a Teams Location\Place	122
Figure 78 Adding a Teams Location\Place - New Place	122
Figure 79 Adding a Teams Location\Place – Location Name	123
Figure 80 Adding a Teams Location\Place - Completed	123

Figure 81 Teams Location\Place record in PowerShell	124
Figure 82 Teams Emergency Calling Policies	125
Figure 83 Teams Emergency Calling Policy Attributes	125
Figure 84 Teams Emergency Calling Policy - Configuration	126
Figure 85 Teams Emergency Call Routing Policies	127
Figure 86 Teams Tenant Trusted IP Addresses	128
Figure 87 Teams Tenant Trusted IP Addresses - Configuring	129
Figure 88 Teams Tenant Network Regions	130
Figure 89 Teams Tenant Network Regions - Configuring	131
Figure 90 Teams Tenant Network Sites	132
Figure 91 Teams Tenant Network Subnets	133
Figure 92 Teams Tenant Network Subnets - Configuring	134
Figure 93 Teams Location Information System (LIS) Network Elements	135
Figure 94 Teams Location Information System (LIS) Subnets	136
Figure 95 Teams Location Information System (LIS) Subnets - Configuration	137
Figure 96 Teams Location Information System (LIS) Wireless Access Points	139
Figure 97 Teams Location Information System (LIS) Wireless Access Points - Configuration	139
Figure 98 Teams Location Information System (LIS) Network Switches	141
Figure 99 Teams Location Information System (LIS) Network Switches - Configuration	141
Figure 100 Teams Location Information System (LIS) Network Switch Ports	143
Figure 101 Teams Location Information System (LIS) Network Switch Ports - Configuration	143
Figure 102 PCI Logo	145
Figure 103 Building Location Map	147
Figure 104 General Building Information	147
Figure 105 Warehouse – Subnets	150
Figure 106 Warehouse - Quadrants and Network Switches	151
Figure 107 Wired Subnet Inventory	152
Figure 108 Wireless Subnets	153
Figure 109 Wireless Access Points	154
Figure 110 Direct Internet Access Information	154
Figure 111 Warehouse Building with Dispatchable Location Quadrants	156
Figure 112 Teams Emergency Addresses – Summary Table	160
Figure 113 Teams Emergency Addresses - CSV Input File	160
Figure 114 Teams Emergency Addresses	160
Figure 115 Teams Place Records – Summary Table	161
Figure 116 Teams Locations/Places - CSV Input File	161
Figure 117 Teams Place Records - Vickers-Headquarters Building	162
Figure 118 Teams Emergency Call Routing Policies - Summary Table	162
Figure 119 Teams Emergency Call Routing Policies	163
Figure 120 Voice Routes for Direct Routing Emergency Calling	164
Figure 121 PSTN Usages for Direct Routing Emergency Calling	164
Figure 122 Teams Emergency Calling Policies - Summary Table	165
Figure 123 Teams Emergency Calling Policies	166
Figure 124 Teams Tenant Trusted IP Addresses - Summary Table	167
Figure 125 Teams Tenant Trusted IP Address - CSV Input File	167
Figure 126 Teams Tenant Trusted IP Addresses	167
Figure 127 Teams Tenant Network Regions	168

Figure 128 Teams Tenant Network Sites - Summary Table	168
Figure 129 Teams Tenant Network Sites - CSV Input File	168
Figure 130 Teams Tenant Network Sites	169
Figure 131 Teams Tenant Network Subnets - Summary Table	170
Figure 132 Teams Tenant Network Subnets - CSV Input File	171
Figure 133 Teams Tenant Network Subnets - Example Tenant Network Site Shown	172
Figure 134 Subnet Network Elements - Summary Table	175
Figure 135 Subnet Network Elements - CSV Input File	176
Figure 136 Wireless Access Point Network Elements - Summary Table	177
Figure 137 Wireless Access Point Network Elements - CSV Input File	178
Figure 138 Network Switch Network Elements - Summary Table	179
Figure 139 Network Switch Network Elements - CSV Input File	179
Figure 140 Network Switch Port Network Elements - Summary Table	180
Figure 141 Network Switch Port Network Elements - Input CSV File	181

Chapter 1 Teams Dynamic 911 and 911 Work from Home

Introduction

Correctly routing emergency calls to the appropriate Public Safety Answering Point (PSAP) is a legal requirement in the United States. There can be some nuances when using any phone service, but this White Paper addresses the options and configurations in Microsoft Teams. All options (Calling Plans, Operator Connect and Direct Routing) are addressed here. See [Deciding Between Direct Routing and Calling Plans \(enablingtechcorp.com\)](https://enablingtechcorp.com) for a primer if needed.

What is Dynamic 911 and why it so Important

The purpose of Dynamic 911 is to ensure that when a user in the United States makes an emergency call, that the call be routed to the appropriate Public Safety Answering Point based on the user's current location. By getting the caller to the right PSAP, the closest emergency responders to the caller can be determined and dispatched. Dynamic 911 is an element in the US telephony infrastructure that is applicable to all its participants. This White Paper is focused on implementing Dynamic 911 for organizations using Microsoft Teams Voice.

There are several reasons why an organization should implement Dynamic 911 on their telephony system:

1. The health, safety, and wellbeing of their employees.
2. Compliance with Federal, State, and local laws related to emergency services calling and avoidance of fines for non-compliance.
3. Protection for the organization from litigation related to the amount of time it took for the emergency responders to arrive at the exact location of the emergency caller as it relates to the dispatchable location provided by the organization's phone system.

Microsoft Teams Support for Dynamic 911

For Calling Plan and Operator Connect users, the Dynamic Emergency Calling feature is included and enabled by default. It is an end-to-end solution. Teams can determine an Emergency Caller's current location and automatically pass the call and the current location information to the appropriate PSAP.

For Teams Direct Routing users, Teams can determine an Emergency Caller's current location and pass that information to the client's Session Border Controller (SBC). The call and the information must then be passed to an Emergency Routing Service Provider (ERSP) before it can be presented to a PSAP. It is the responsibility of the customer to engage with an ERSP of their choice. The customer has the option of disabling Dynamic Emergency Calling for Teams Direct Routing users.

Microsoft Teams Dynamic 911 supports emergency services calling from the organization's external and Work from Home (WFH) Teams users. This feature is available for Calling Plan, Operator Connect and Direct Routing users. It is not enabled by default.

Which Teams Clients support Dynamic 911?

- Teams desktop client for Microsoft Windows and the Apple macOS.
- Teams mobile client for Apple iOS client version 1.0.92.2019121004 and App Store version 1.0.92 and greater.
- Teams mobile client for Android client and Google Play store version 1416/1.0.0.2019121201 and greater
- Teams Phone version 1449/1.0.94.2019110802 and greater.
- Teams Rooms on Windows and Android.

Which Teams Clients and devices do not support Dynamic 911?

- Teams Web Client.
- Legacy Lync\Skype for Business 3rd Party IP Phone (3PIP).

Which Teams Clients support Dynamic 911 for Work from Home?

- Teams Windows Client.
- Teams Mac Client.
- Teams Mobile Client with some limitations.
 - The client does not support entering addresses.
 - It does not “remember” the association between addresses and network locations. See the information below for details on these limitations.

Which Teams Clients and devices do not support Dynamic 911 for Work from Home?

- Teams Phones.
- Teams Rooms.
- Teams Web Client.
- Legacy Lync\Skype for Business 3rd Party IP Phone (3PIP).

Legal Requirements

Congress and the Federal Communications Commission (FCC) enacted laws in 2018 and 2019 that address aspects of [Dynamic 911 Calling in the United States for Multi-Line Telephone Systems \(MLTS\)](#):

- Kari’s Law – Signed into law on February 16, 2018, and went into effect on February 16, 2020.
- RAY BAUM’s (Repack Airwaves Yielding Better Access for Users of Modern Services) Act – Enacted on August 1, 2019. It went into effect as of January 6, 2021, with additional requirements effective as of January 6, 2022.

Kari's Law

- The law applies to on-premises fixed and non-fixed devices and off-premises devices. It basically applies to all devices attached to a Multi-Line Telephone System (MLTS).
- Kari's Law is "forward-looking" and applies only to MLTS's manufactured, imported, offered for first sale or lease, first sold, or leased, or installed after February 16, 2020.
- It requires that the system support direct dialing of 911 without having to dial a prefix or access code. You cannot require a user to dial 9911 to make a call to Emergency Services.
- The law also has a Notification Requirement:
 - Used to facilitate building entry by first responders.
 - When a call to Emergency Services is made a notification must be sent to an on-site or off-site central location where someone is likely to see or hear the notification.
 - The notifications must be a conspicuous on-screen notification with an audible alarm through a client application, smartphone text message or email.
 - The notification shall at a minimum include:
 - The fact that a 911 call has been made.
 - A valid callback number and,
 - The information about the caller's location that the MLTS provides to the Emergency Services provider with the 911 call; provided, however that the notification does not have to include a callback number or location information if it is technically infeasible to provide the information.



RAY BAUM's Act

- This law applies to all on-premises fixed devices associated with an MLTS as of January 6, 2021. For these devices, a dispatchable location must be automatically provided to Emergency Services when a 911 call is placed.
- The law's coverage was extended to on-premises non-fixed devices and off-premises devices on January 6, 2022.
- The RAY BAUM Act is also forward-looking and applies to MLTS's using the two (2) deadlines above.
- The location must be provided automatically where technically feasible otherwise the information can be based on end user manual update or enhanced location information. Enhanced location information refers to the use of coordinates or Geocodes (latitude and longitude).
- Dispatchable locations must consist of the validated street address of the emergency services caller plus additional information to adequately identify the caller's location such as floor, suite, apartment, etc.



State and Local Municipality Dynamic 911 Regulation

- At least twenty-four (24) States have existing laws regarding emergency services Calling. These rules can complement the Federal laws if they are not inconsistent with them.
- The specific elements of emergency calling that they cover vary greatly.

- Some municipalities have requirements that supersede those of the State.
- A current list of these requirements can be found in the [911 Legislation Database](#) on the [National Conference of State Legislatures website](#).
 - Intrado is an ERSP that has for many years offered products and services designed for Microsoft Lync, Skype for Business and Teams Direct Routing and other products.
- Following are some sample State regulations:
 - Florida
 - Provided addresses must be precise to the station level. This seems to apply to any business entity with a [Private Branch Exchange](#) (PBX).
 - "Each PBX system installed after January 1, 2004, must be capable of providing automatic location identification to the station level."
 - "Automatic location identification" or "ALI" means the automatic display at the Public Safety Answering Point (PSAP) of the caller's telephone number, the address or location of the telephone, and supplementary emergency services information."
 - Note: ALI is not dynamic. It is a static mapping of locations to phone numbers.
 - New York
 - The regulations apply to "public buildings" which they define as "any building belonging to the state, county, town, village, school district or any other political or civil subdivision of state or local government".
 - The regulation appears to require compliance with Kari's Law but does not mandate the providing of any address information when making an emergency services call.
 - North Carolina
 - Has no regulations.

What do Companies using Microsoft Teams Voice need to consider when setting up Dynamic 911?

- Organizations need to determine their required compliance with laws and regulations governing emergency services calling by their employees. The legal department, compliance officer and human resources personnel are the usual parties that will make this determination for the firm.
- These personnel should consider exceeding the regulatory requirements to reduce risk and liability to the firm related to issues with their users being able to complete calls to emergency services while providing an appropriate dispatchable location.
- Following is a scenario to illustrate this point based on a famous building:



Figure 1 NASA VAB - Kennedy Space Center

The NASA [Vehicle Assembly Building](#) (VAB) at the Kennedy Space Center is the largest single floor building in the world.

*Its single floor covers over 8 acres measuring 716 feet x 518 ft with a height of 526 feet.

*Since its construction to support the Apollo missions, the interior layout of the building has changed. There are at times discrete levels and rooms that could be used as dispatchable locations for emergency calls.

*The State of Florida currently does not have any laws that complement the RAY BAUM act providing a more specific definition of what should constitute a dispatchable location.

*Legally, the Kennedy Space Center would need to only provide the floor the emergency caller is on when a call is placed.

*The required notification to the VAB's security team would provide the caller's location as "1st Floor".

*Providing this level of information to emergency responders could result in a delaying their arrival to the exact location of the emergency caller.

*In a civil suit, a jury could determine that while the Space Center complied with all applicable Federal and State laws, they were negligent in providing a more precise location to the emergency responders resulting in delaying their arrival on scene resulting in an unnecessary worsening of the situation for the caller.

- Once the requirements for emergency services calling have been established by the organization's legal and compliance personnel, it becomes the responsibility of the technical personnel to implement these policies.
- The technical personnel must determine whether their existing telephony and network infrastructure can support the implementation of these policies. They will have to determine the level of remediation that will be needed if they do not. For example:
 - How can the caller's floor be determined?
 - The subnet they are on?
 - The Wireless Access Point they are connect to?
 - The network switch they are connected to?
 - The port on the switch?

How does Microsoft Teams meet the Legal Requirements for Dynamic 911?

- Microsoft Teams includes policies and mechanisms to help an organization comply with Kari’s Law, the RAY BAUM Act and most superseding State and Local regulations.

Kari’s Law

- For Microsoft Teams Calling Plan, Operator Connect and Direct Routing users, Teams Emergency Calling Policies will send notifications to building specific corporate resources when a user makes an emergency services call.
- These policies can be provisioned dynamically to Teams users. As an organization’s users move from building to building, they will automatically be assigned a policy that can notify the building’s personnel based on their current location.
- The Emergency Calling Policies are also used to ensure that emergency callers do not need to dial anything other than “911” to reach emergency services.



RAY BAUM’s Act

- Microsoft Teams can provide an emergency location from anywhere a user is signed onto a device attached to the on-premises local area network.
 - For this to work, the organization must configure Microsoft Teams to provide a dispatchable location for every location in every organizational building that a Teams user might be signed in from.
- For external and Work from Home users, Teams can derive automatically or help the users define their current dispatchable location.
 - The organization must train the external and Work from Home users on how to properly use this feature.

Summary

- Microsoft Teams can help organizations comply with the legal requirements for emergency services calling.
- It is the client’s responsibility to comply with all laws and regulations regarding emergency calling from a company provided Multi-Line Telephone System (MLTS) telephone system.
- The client should confer with their in-house counsel, Compliance Officer and Human Resources department on the requirements for organizational level Emergency Calling policies, definition of dispatchable locations and related business practices. These personnel may create corporate policies that exceed the Federal, State or Local definitions of appropriate dispatchable locations to provide additional legal and liability protection for the organization.
- Clear instructions on how to make calls to emergency services using the organization’s telephony equipment must be provided to all the organization’s users. The users must be trained in how to verify their location when working externally or from home.
- The organization’s Corporate Counsel, Compliance Office or Human Resources department should decide on whether the organization’s users must acknowledge receipt of the instructions for making calls to Emergency Services using the organization’s telephony system.

- The information configured by the client to provide Emergency Calling services to its users must be accurate. At all times, the client's correct current location information must be provided to the PSAP and ERSP.
- The client should test the emergency services Call Flow on a regular basis.

Chapter 2 Planning and Implementing Emergency Addresses and Locations in Microsoft Teams

Introduction

To properly route emergency calls to the correct Public Safety Access Point (PSAP) when using Microsoft Teams, you will need to create Microsoft Teams Emergency Addresses for each one of your buildings. This section explains the details to ensure you're meeting RAY BAUM's Act, Kari's Law, and state regulations.

Overview and Terms

Teams Dynamic Emergency Calling is enabled by default for Microsoft Teams Calling Plan and Operator Connect users. Though it is enabled, it will not work without additional configuration. Before you can assign telephone numbers to your Microsoft Teams Calling Plan and Operator Connect users you must configure Emergency Addresses and Emergency Location\Places that represent the primary dispatchable locations of your on-premises users.

A Location\Place must be assigned to Teams Phone System numbers as they are being assigned to your Calling Plan and Operator Connect users. This Location\Place is referred to as the "address of record" (AOR) for a Calling Plan or Operator Connect user. This can be thought of as a "default" address for the number that can be provided to emergency providers if the caller's current location cannot be determined dynamically by Microsoft Teams. This is the first component of Teams Dynamic Calling encountered when setting up Teams for Calling Plan, Operator Connect and Teams Direct Routing users.

The address of record is assigned to Calling Plan users by the organization's Teams Administrators. There are three (3) assignment options for Operator Connect users:

1. The Operator Connect Operator (OCO) assigns the AORs to the phone numbers. The organization's Teams Administrators can change them later in the Teams Admin Center.
2. The OCO doesn't assign the AORs but allows the Teams Administrators to assign them in the Teams Admin Center.
3. The OCO assigns the AORs to the phone numbers. The Teams Administrators are not allowed to change them. The Administrators must contact the OCO to make changes to phone numbers and their assigned AORs.

The availability of these options varies among the Operator Connect vendors.

Locations\Places must be assigned to the network elements added to the Teams Location Information System (LIS) database. This association of a dispatchable location to a network subnet, wireless access point, switch or switch port is what puts the "Dynamic" in "Teams Dynamic 911".

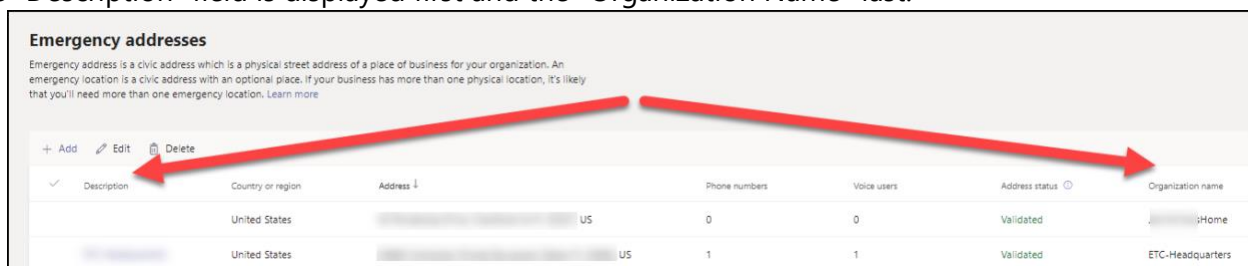
The Emergency Location\Place in Dynamic 911 parlance is also referred to as a "dispatchable location". These are the addresses that are provided to emergency responders to direct them to an emergency services caller. The RAY BAUM Act requires that Multi-Line Telephone Systems (MLTS) installed after January 6, 2021, must automatically provide a dispatchable location to Emergency Services when a 911 call is placed. The definition of what constitutes a dispatchable location is very much up for debate and discussed previously.

Teams Emergency Addresses

- In Microsoft Teams, Emergency Addresses commonly represent the Street or Front Door address of the organization's buildings.
- Location\Places associated with Emergency Addresses are required for customers using Teams Calling Plan and Operator Connects.
- When you add an Emergency Address (also referred to as a Civic Address) to Teams, a Teams Location\Place record is automatically created.
- This Location\Place record represents the Street Address or "Front Door" location of the building.
- Each Emergency Address record includes:
 - The Organization Name.
 - A Description of the building.
 - A unique identifier for the record is called a CivicAddressID.
 - The full Street Address of the building:
 - "House" Number.
 - Street Name.
 - Pre and Post Directional Street Name Information.
 - Street Suffix.
 - City.
 - State or Province.
 - Postal Code.
 - Country or Region.
 - Geocodes:
 - Latitude.
 - Longitude.
 - The optional Emergency Location Identification Number (ELIN) associated with the Emergency Address.
- The DefaultLocationID is the LocationID of the Location\Place record that was created when the Emergency Address record was added. The LocationID is a unique identifier for Teams location records.

Teams Emergency Addresses "Description and Organization Name" Columns

- Microsoft has recently changed how the fields for the "Emergency Addresses" in the Teams Admin Center are displayed.
- The "Description" field is displayed first and the "Organization Name" last.



Emergency addresses

Emergency address is a civic address which is a physical street address of a place of business for your organization. An emergency location is a civic address with an optional place. If your business has more than one physical location, it's likely that you'll need more than one emergency location. [Learn more](#)

+ Add Edit Delete

Description	Country or region	Address	Phone numbers	Voice users	Address status	Organization name
	United States	US	0	0	Validated	Home
	United States	US	1	1	Validated	ETC-Headquarters

Figure 2 Teams Emergency Addresses

- The “Organization Name” is passed on to the Public Safety Answering Point (PSAP) and the first responders.
- The information in the “Description” field is not passed on to the PSAP or emergency responders.
- The default value for the “Organization Name” field is pulled from the name provided when a Microsoft 365 tenant is created. It may not be the organization’s Name used at the Emergency Address’s actual location.
In other words, it may not be the name on the “Front of the Building”, nor the name used in the Building Directory, or the name known to the security desk personnel in a multi-tenant building.

Recommendation

- **Think about the information that would be provided to the PSAP and first responders should someone call emergency services from each of your company’s buildings.**
- The “Description” and “Organization Name” fields do not require unique values. Every one of your “Emergency Addresses” can have the same value for “Organization Name”.
- The combination of the “Organization Name” and “Description” should clearly identify each building.
- **Place the name that is used for each building “at the building” in the Organization Name field. It should begin with the organization’s name that the Emergency Responders will look for and need to be able to find when they arrive on the scene.**
- If the Organization Name is “eGroup Enabling Technologies” but is referred to as “eGroup ETC” at the location on “10 Main Street, Anywhere, US 11111”, then use “eGroup ETC” as the Organization name for that “Emergency Address” record.
- Some examples of “Organization Names” for eGroup Enabling’s buildings might be:
 - eGroup Enabling Technologies – HQ
 - eGroup ETC – Support Center
 - eGroup ETC - Sales
- Use the “Description” field to help you clearly, uniquely, and unambiguously identify the building for your users and system administrators.
- When assigning Calling Plan numbers to users, you can search for a location based on the Description of the Emergency Address.
- Use the names used for the buildings as they are known to your personnel in the Description field. Your users might refer to the Headquarters building as “Esteros” or “The Murphy Building” or the “Tower”. Use the vernacular your users are used to in the “Description” field.
- Use the same naming logic when setting up records for Automatic Line Identification (ALI) with the Emergency Response Service Providers (ERSP) and similar services when using Teams Direct Routing.

Teams Locations\Places

- Location\Place records are assigned to Microsoft Teams Calling Plan and Operator Connect users and network elements in the Location Information System (LIS) database. Emergency Address records are not assigned to either of these entities.
- It is these records that are used to provide dispatchable locations to emergency providers when an emergency services call is placed by Calling Plan, Operator Connect or Direct Routing users
- All Emergency Addresses have a default Location\Place record. This record represents the Street or “Front Door” address of the building.

- The value of the “Location Name” of the default record is blank or null in the PowerShell location object.
- This location does not “explicitly” appear in the list of Locations\Places of an Emergency Address record.
- A building can have additional Location\Place records.
 - These records are added to the Emergency Address records and represent more specific locations in a building such as a floor, suite, room, or apartment. For a building with sixty (60) floors providing a dispatchable location that includes the floor number will allow the emergency responders to get to the caller much faster than if they did not have that information.
 - The Location\Place records have a Location Name that must be unique for the Emergency Address record. You cannot have two (2) Locations\Places for an Emergency Address named “First Floor”.
 - Multiple Emergency Address records can have identical Location\Place names such as “First Floor”.
- The Location\Place records created for an Emergency Address include the street address, Geocodes and ELIN (if used) information of the parent Emergency Address record.
- Each record includes the CivicAddressID of the Emergency Address record.
- All child Location\Place records of an Emergency Address record will have the same CivicAddressID.
- Each Location\Place record has a unique internal identifier named the LocationID.
- Location\Place records can have an optional ELIN number that overrides the ELIN number of the parent Emergency Address record. If an ELIN number is not provided in the Location\Place record, the record will use the ELIN of the parent Emergency Address record if there is one.

Key Points

1. There should be an Emergency Address record for all company buildings regardless of whether there are or will be Teams users homed in the location.
2. Teams will allow you to add Emergency Addresses with the same Organization Name and Address. Do not do this! Have one record for each building to keep the Organization Names and Street Addresses unique and unambiguous.
3. Before creating your Emergency Addresses and Location\Place records, document them thoroughly. You will be able to use this documentation to later create these records through PowerShell.
4. If you are creating these manually or through PowerShell, determine the latitude and longitude of the Emergency Addresses. You will not be able to assign a Teams Location\Place to a Calling Plan or Operator Connect number or Location Information System (LIS) database network element that does not have Geocodes.

Adding Teams Emergency Addresses

- Emergency Addresses must be validated against the Master Street Address Guide (MSAG) database.
- Teams will perform this validation automatically when adding emergency addresses through the Teams Admin Center.
- Validation is a separate step and command when adding the addresses through PowerShell
- Once validated, the information in an Emergency Address cannot be changed. If you need to make changes to a record, you will have to:

1. Unassign the Emergency Address's "child" Places from all Calling Plan and Operator Connect users and LIS database entries.
2. Delete all the Emergency Address's Places.
3. Delete the Emergency Address.
4. Create a replacement Emergency Address.
5. Re-add all the Places.
6. Reassign the Places to the Calling Plan and Operator Connect users and LIS database records.

Adding Teams Places

- You must first decide which Locations\Places you will need to add to Teams.
- This is discussed in the previous section, "Planning Emergency Calling for Microsoft Teams" under the "Who" section.

Summary

- In most cases, create an Emergency Address for all buildings.
- Keep your Organization (building) Names clear and unique. Do not add Emergency Addresses with the same Organization Name.
- Emergency Addresses can be added using PowerShell but you will have to determine their Geocodes first
- The Locations\Places you add will be mostly determined by what your business determines to be suitable dispatchable locations that meet regulatory, legal, and business liability protection and needs.

Chapter 3 Configuring Microsoft Teams for Kari's Law Compliance

Introduction

Kari's Law was signed into law on February 16, 2018, and went into effect on February 16, 2020. The law provides requirements for direct emergency call dialing and notification of on-premises personnel when someone makes an emergency services call. The notification is to help facilitate access to the building and the emergency caller by first responders. While not clearly stated, the law infers that when a user places a call to emergency services that the call will be routed by the customer's telephone services to a Public Safety Answering Point (PSAP). State and municipal laws and regulations can supersede Federal laws if they are not inconsistent with them.

Notification Requirement

- The notification requirement of Kari's law is used to facilitate building entry by first responders.
- When a call to emergency services is made a notification must be sent to an on-site or off-site central location where someone is likely to see or hear the notification.
- The notifications must be conspicuous on-screen notifications with an audible alarm through a client application, smartphone text message or email.
- The notification shall at a minimum include:
 - The fact that a 911 call has been made.
 - A valid callback number and,
 - The information about the caller's location that the MLTS provides to the Emergency Services provider with the 911 call; provided, however that the notification does not have to include a callback number or location information if it is technically infeasible to provide the information
 - Teams Emergency Calling Policies are used to meet the Notification requirement of Kari's Law.
- They are applicable to both Teams Calling Plan, Operator Connect and Teams Direct Routing users.

Teams Emergency Calling Policy

- **The Emergency Calling policy should be assigned to the user based on the building in which they are currently located.** In other words, the assignment of the Emergency Calling policy should be **dynamic and not static**. There are some cases where a static assignment of an Emergency Calling policy is appropriate.
- There are four (4) ways an Emergency Calling policy or Emergency Call Routing policy can be applied to Teams users:
 1. Global (Org-Wide default) – This assignment has the lowest priority. The Global (Org-Wide default) policy will be assigned to users who do not get a policy through site level or direct assignment. This policy is static in nature. It does not change for the user even if the user is working from different buildings on the Corporate Campus.
 2. Tenant Network Site Level – These policies are assigned dynamically based on the building in which the Teams endpoint is currently signed in. If you are signed into the Headquarters building, you will get the policy specific to the Headquarters building. If you are in the Warehouse, you will get the Warehouse's policy. Site level assigned policies take priority over the Global (Org-Wide default) policy but would be

superseded by a directly assigned user level policy. These policies are associated with a defined Tenant Network Site. Please see the section below on scoping Teams Emergency Policies.

3. **User Level** – These policies are assigned directly to the user. They are static in nature. The user will use the same policy in all company buildings. If assigned to a user, it has the highest priority and will be the effective policy for the user. The policies can also be assigned to users via batch policy assignment and policy packages¹.
 4. **Group Policy Assignment** – Policies can be associated with Active Directory or Entra Active Directory groups. The associated policy will be assigned to the members of the group. If a user is a member of more than one group with a policy assignment, the policies can be prioritized in the Teams Admin Center or through the equivalent PowerShell command.
- There is an order of preference that determines a user’s effective policy:
 - User or batch assigned policies.
 - Policies associated to groups.
 - Global (Org-wide default) policies.

Why should Emergency Calling Policies be dynamically assigned?

1. This boils down to two (2) simple questions:
 1. Does the company have Teams users working in more than one company building?
 2. If the answer to the first question is yes, will the same parties be notified if someone places a call to emergency services from any of these buildings?
2. If you answered “Yes” to the first and “No” to the second, you would need to dynamically assign the Emergency Calling policy to your users.
3. Even if you only have one (1) building, you should still create an Emergency Calling policy for the building.
4. Emergency Calling Policies are applied to all Teams users, including those working from home.
5. In the past, the recommendation has been to use the Global (Org-Wide Default) policy for Companies with a single building. Whenever a user made a 911 call, the users and group listed in the policy would receive a notification that the call had been made.
6. Even before the addition of the Work from Home feature, these users and group were probably getting notifications for calls made by Teams users who were not signed onto the company’s networks. There typically isn’t any point or benefit to sending a notification when a Work from Home user makes an emergency call.
7. The new recommendation is to create Emergency Calling Policies for all company buildings.
8. The Work from Home users will be dynamically assigned the Global (Org-Wide Default) policy. This policy would usually be configured without any notifications when an emergency call is made. This is discussed later in this document.
9. To dynamically assign these policies, each building’s policy should be associated with a Teams Tenant Network Site.

¹ [Assign policies to users and groups - Microsoft Teams | Microsoft Learn](#)

10. **It is a best practice to have a Tenant Network Site for each of a company's buildings.** Yes, you could consolidate several buildings into a single Tenant Network Site, but at some point, in the future, there is a good chance that it will come back to haunt you!
 11. Tenant Network Sites for each building will allow you to associate building specific Emergency Calling and Emergency Call Routing policies with each building.
 12. Presuming that each building has a specific set of parties to be notified when an emergency services call is made in the building, having an Emergency Calling policy for each building becomes an obvious design decision.
 13. Separate emergency numbers can be defined in an Emergency Calling Policy. You can define "911" and "933" separately assigning different notification modes to each. The use case would be to not send a notification when "933" is dialed or to send the notification to the IT team for testing purposes.
- **There will be some cases where there could be separate notification parties for the same building:**



Figure 3 Boeing Everett Production Facility

The [Boeing Everett Production facility](#) is where the 747, 767, 777 and 787 airliners are built. The manufacturing building covers 98.3 acres and is over 1 km long x ½ km wide. It is very likely that for a building this size, there are multiple notification parties for different sections of the building. Using Multiple Tenant Network Sites and Emergency Calling Policies for this single building would be appropriate.

How are Emergency Calling Policies applied to Work from Home and other externally connected users?

1. The notification tenet of Kari's Law does not directly address these users.
2. Common sense suggests that the notification requirement does not apply to these users. It is highly unlikely that there would be any corporate personnel who could "facilitate building entry" to a location not owned by the company such as a user's home.
3. If you have configured your environment to use dynamically assigned policies, your users working from home or other outside locations would use the Global (Org-Wide default) Emergency Calling policy.
4. In some cases, the Corporate Human Resources personnel and others may want to be notified when an employee dials emergency services. If this is a requirement, add these personnel to the notification targets for all your policies, even the Global (Org-wide default). These personnel will likely want to know about these calls whether an employee is on or off site.

Configuring a Teams Emergency Calling Policy

- These policies have eight (8) attributes and support multiple emergency numbers.:

Attribute	Description
Name	The name of the policy
Description	A Description of the policy. This should include the purpose of the policy
External location lookup mode	Enabled or Disables the Work from Home feature
Emergency service disclaimer	A text string of up to 350 characters shown at the top of the Calls app. Users must acknowledge the disclaimer by clicking the "OK" button.
Emergency Numbers	
Emergency dial string	-Specifies the emergency phone number -You can have separate emergency number treatments when 911 or 933 are dialed. -Each number can have different notification modes.
Numbers to dial for emergency calls notifications	-The PSTN phone cannot be unmuted even when the mode is set to "Conferenced in muted but are able to unmute" -Phone numbers should be in e.164 format
Notification mode	A drop down box with four (4) Choices: None Send notification only Conferenced in but muted Conferenced in and are unmuted If you select one of the "Conferenced" modes, you must enter a Phone Number or Users and Groups in the notification options
Users and groups for emergency calls notifications	-You can put in up to ten (10) entries of users and/or groups that will be notified when an emergency call is placed. -You can enter email addresses of users and the names of distribution or security groups separated by semi-colons ";". -Total number of users cannot exceed fifty (50).

Figure 4 Teams Emergency Calling Policy Attributes

- A user with Teams administrator permissions will be required to add and remove notification users from the policies. If you send the notifications to a distribution or security group, you will be able to delegate the management of the group membership to an owner who does not have Teams administration permissions such as the manager of the Corporate Security Department.
- You can add a new policy by clicking the "Add" button or edit a policy by clicking on it then the "Edit" button:

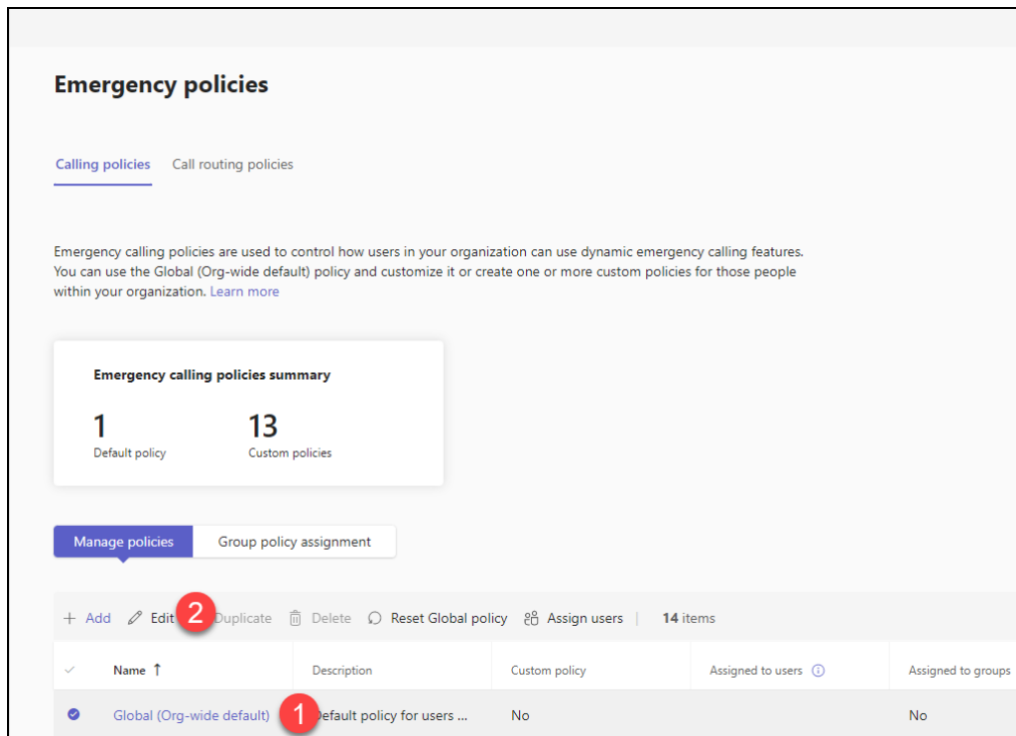


Figure 5 Adding a Teams Emergency Calling Policy

Teams Objects for Dynamically Assigning Emergency Policies

- Teams Emergency Calling policies should be dynamically assigned based on the Teams user's current location. There should be an Emergency Calling policy for each of a company's buildings. When a user signs on to the company network in a building, the policy for the building should be dynamically assigned to the user. The Global (Org-Wide Default) Emergency Calling policy gets automatically assigned to Work from Home users.
- Teams Emergency Call Routing policies generally won't need to be dynamically assigned based on the user's location. If you only have a single SBC, you'd literally never have to dynamically assign one of these policies. The use cases for dynamically assigning these policies are discussed below. The Global (Org-Wide Default) Emergency Call Routing policy will usually be appropriate for users when they are working from home.
- These policies are made "dynamic" by assigning them to the appropriate Teams Tenant Network Site. A Teams Tenant Network Site should be created for each of the company's buildings. There are some use cases where a building might have more than one (1) Tenant Network Site. These situations were previously described.
- A Tenant Network Site is associated with one (1) Teams Emergency Calling policy and one (1) Teams Emergency Call Routing policy. By default, Tenant Network Sites are associated with the Global (Org-Wide default) Emergency Calling and Emergency Call Routing policies.
- It is perfectly acceptable for a Tenant Network Site to be assigned an Emergency Calling policy appropriate to the site and to have the Global (Org-Wide default) Emergency Call Routing policy assigned. The reverse is also true.
- In addition to the building specific Emergency Calling policies, several other Teams objects must be configured to support current location based dynamic policy assignment:
 - Teams Tenant Trusted IP Addresses.
 - Teams Tenant Network Regions.
 - Teams Tenant Network Sites.
 - Teams Tenant Network Subnets.

Teams Tenant Trusted IP Addresses

- Required for implementing location scoped Teams Emergency policies.
- If you have configured Microsoft Teams to comply with the RAY BAUM Act to provide dynamic dispatchable locations to a PSAP or ERSP, you will have already added these addresses to Teams.
- An IPv4 Tenant Trusted IP record should be added for all devices providing Direct Internet Access (DIA) to users on the company's networks including routers, firewalls, or other perimeter devices.
- Entries can be made for single IP addresses, or a range based on the address and a subnet mask.
- Microsoft recommends that both an IPv4 and IPv6 address for these devices be added to the Tenant Trusted IP table.
 - If not already configured, the client should ask their Internet Service Provider (ISP) to provision an IPv6 address for their devices providing DIA to their users.

- These can be single IPv6 addresses or ranges with subnet masks like the IPv4 addresses. All addresses should be statically provided by the ISPs.
- The router/firewall will have to be configured to listen for and send traffic using IPv6.
- **The client's internal networks do not need to be configured to support IPv6 addressing or routing.**

Tenant Network Regions

- Tenant Network Sites must be assigned to a Tenant Network Region.
- Tenant Network Regions are not directly used for dynamic emergency policy assignment. They come more into play when configuring Teams Location Based Routing (LBR) or Teams Local Media Optimization (LMO).
- If you are not using Teams LBR or LMO, then create a Region for each Country in which you have a building.

Tenant Network Sites

- Tenant Network Sites generally represent each of a company's buildings. In some cases, a building may have more than one (1) Tenant Network Site.
- Each building should have at least one (1) Tenant Network Site.
- Tenant Network Sites must be assigned to a Tenant Network Region and will contain at least one (1) Tenant Network Subnet.
- Tenant Network Sites can be used to assign Teams Emergency Calling Policies and Teams Emergency Call Routing policies dynamically to Teams users based on their current location.
- The number of configured Tenant Network Sites and the numbers of Teams Emergency Locations\Places will probably not be the same. It is the nature of the beast.
- The layout of your Tenant Network Sites will depend on combining the requirements for Teams Emergency Calling and Teams Emergency Call Routing Policies. The location scoping requirements of both policies need to be considered when determining the setup of your Tenant Network Sites and Tenant Network Subnets.
- For example:
 - A customer has five (5) buildings.
 - They also have two (2) Direct Routing SBCs.
 - They created Emergency Calling policies for each of the five (5) buildings.
 - They created two (2) Emergency Call Routing policies, one (1) for each SBC.
 - In each building, the customer wanted to route calls for even numbered subnets to the East Coast SBC and the rest to the West Coast SBC.
 - To meet this requirement, the customer created ten (10) Tenant Network Sites.

Building Name	Tenant Network Site Name	Region	Subnets	Emergency Calling Policy	Emergency Call Routing Policy
Headquarters	Headquarters-East	US	10.10.2.0/24 10.10.4.0/24 10.10.6.0/24 10.10.8.0/24	Headquarters	SBC-East
	Headquarters-West	US	10.10.3.0/24 10.10.5.0/24 10.10.7.0/24 10.10.9.0/24	Headquarters	SBC-West
Manufacturing	Manufacturing-East	US	10.10.12.0/24 10.10.14.0/24 10.10.16.0/24 10.10.18.0/24 10.10.20.0/24 10.10.22.0/24 10.10.24.0/24	Manufacturing	SBC-East
	Manufacturing-West	US	10.10.13.0/24 10.10.15.0/24 10.10.17.0/24 10.10.19.0/24 10.10.21.0/24 10.10.23.0/24 10.10.25.0/24	Manufacturing	SBC-West
R&D	R&D-East	US	10.10.32.0/24 10.10.34.0/24	R&D	SBC-East
	R&D-West	US	10.10.33.0/24 10.10.35.0/24	R&D	SBC-West
Warehouse	Warehouse-East	US	10.10.42.0/24 10.10.44.0/24 10.10.46.0/24 10.10.48.0/24 10.10.50.0/24 10.10.52.0/24 10.10.54.0/24	Warehouse	SBC-East
	Warehouse-West	US	10.10.43.0/24 10.10.45.0/24 10.10.47.0/24 10.10.49.0/24 10.10.51.0/24 10.10.53.0/24 10.10.55.0/24	Warehouse	SBC-West
Meeting Center	Meeting Center-East	US	10.10.64.0/24	Meeting Center	SBC-East
	Meeting Center-West	US	10.10.65.0/24	Meeting Center	SBC-West

Figure 6 Complex Tenant Network Site Configuration

Tenant Network Subnets

- A Tenant Network Subnet can only be assigned to one (1) Tenant Network Site.
- You can add both IPv4 and IPv6 subnets.
- All subnets, except for Virtual Private Networking (VPN) subnets, in a building that a Teams user might connect to should be added as Tenant Network Subnets. This includes subnets homed on wireless networks
- A subnet mask is required when adding the subnets.
- You cannot use super netting or route summarization when adding subnets.
- Tenant Network Subnets should not be confused with the LIS subnet network elements. They are used for different purposes. In some cases, you will have to all your subnets as Tenant Network subnets and LIS subnet network elements.

Direct Emergency Dialing Requirement

Under Kari's Law, a Multi-Line Telephone System (MLTS) must be configured to not require a United States based emergency services caller to dial any number other than 911. In the past, there have been MLTS systems that have required that emergency services be dialed with number strings such as 9911. Compliance with this requirement is simple for Microsoft Teams Calling Plan, Operator Connect and Direct Routing users.

Teams Emergency Call Routing Policies

Microsoft Teams Calling Plan and Operator Connect Users

- You do not need to do anything to comply with this requirement. Teams Emergency Call Routing Policies do not need to be configured to support Calling Plan and Operator Connect users nor are they applicable.
- If an Emergency Call Routing policy is assigned to a Calling Plan or Operator Connect user, it is ignored.
- Teams recognizes calls dialed as "911" as Emergency Calls and will treat them as such.
- Microsoft also supports the test number, "933". Dialing this will connect the caller with a bot that will read back the Calling Number and the current location of the user if it can be determined. If not, it will read back the caller's address of record.

Microsoft Teams Direct Routing Users

- Teams Emergency Call Routing Policies **must be configured** if you are implementing Teams Direct Routing.
- The policies can be found in the Teams Admin Center by clicking on "Voice" then "Emergency policies" and "Call routing policies" at the top of the page.
- Most US based tenants will only need the Global (Org-wide default) Emergency Call Routing policy. If there is more than one (1) Direct Routing Session Border Controller (SBC) a client may add a second policy. Adding a second policy can be easily accomplished in the Teams Admin Center.
- Teams provides two (2) policies by default that cannot be deleted:
 - Global (Org-Wide default).
 - TestECRP.
- The Global (Org-Wide default) policy is automatically applied to all Teams Direct Routing users. The TestECRP is an example of a user level policy. This type of policy can be directly assigned to individual users or to Teams Tenant Network Sites.
- Some customers will install more than one (1) Teams Direct Routing SBC. The most common reasons for this include:
 - Resiliency.
 - Capacity.
 - Regionality.
- Resiliency can be addressed with the PSTN Usage attribute of the policy. This is discussed below.
- Dynamic Tenant Network Site level assignment of the Emergency Call Routing policy can be used to route emergency services calls to the SBCs based on capacity and regionality requirements.
- If you have both an East and West coast SBC, you can use Dynamic Tenant Network Site level assignment of the Emergency Call Routing policy to dynamically route emergency services calls from users east of the Mississippi River through the East coast SBC and the rest through the West coast SBC.
- The scoping of these policies to Tenant Network Sites is covered previously.

- Emergency Call Routing Policies have two (2) purposes:
 - Enable dynamic 911 calling for Direct Routing users.
 - Properly route emergency calls from Direct Routing users to the SBC(s).
- The emergency numbers that Teams Direct Routing Users can dial are controlled by the Teams Emergency Call Routing policy.
- The Emergency Call Routing policy is also used to route the call to the customer’s SBC(s). The SBCs will then route the calls to an Emergency Routing Service Provider (ERSP) before they are routed to the appropriate PSAP. This satisfies the implied requirement of Kari’s law and explicit requirement of the RAY BAUM act that emergency calls be routed to an appropriate PSAP.
- If no Emergency Call Routing Policies have the “Dynamic Emergency Calling” option enabled, Teams will not retrieve policy and location information and include it as part of an emergency services call. Turning this off essentially disables dynamic 911.
 - Teams will not send notifications to internal monitoring personnel. This would leave the company in violation of Kari’s Law.
 - The user’s current location will not be sent to the SBC, ERSP or PSAP violating the RAY BAUM Act
 - Routing of emergency services calls would have to be handled exclusively by Teams Online Voice Routing Policies.
- There are six (6) attributes in an Emergency Call Routing policy that control direct emergency dialing:

Attribute	Description
Name	The name of the policy
Description	A Description of the policy. This should include the purpose of the policy
Dynamic Emergency Calling	<ul style="list-style-type: none"> • This switch turns on Dynamic Emergency Calling for Teams Direct Routing users • If the switch is turned off, you will have to address emergency services calling and routing in Teams Dial Plans and Teams Online Voice Routing Policies for your Teams Direct Routing users to comply with the Direct Emergency Dialing requirement of Kari’s Law • Dynamic Emergency Calling must be enabled to be able to configure Teams to comply with the automatic location requirement of the RAY BAUM Act using the built-in capabilities of Teams
Emergency Dial String	<ul style="list-style-type: none"> • The Emergency Dial String is the phone number that will be sent to the SBCs when a Direct Routing user makes an emergency services call • Emergency Call Routing Policies can include more than one Dial String. Each must be unique
Emergency Dial Mask	<ul style="list-style-type: none"> • Each Emergency Dial String can have one or more Emergency Dial Masks separated by a semi-colon, “911;9911;112” • The masks are used to identify emergency calls based on the various ways a user might dial an emergency call.
PSTN Usage	<ul style="list-style-type: none"> • Teams Voice Routes are what are used to route emergency calls to the Company’s Direct Routing SBC(s) • In most cases, there will be one PSTN Usage and one Voice Route for each Direct Routing SBC

Figure 7 Emergency Call Routing Policy Attributes

Notes for the Attributes

Emergency Dial String

- The Emergency Dial String is the phone number that will be sent to the SBCs when a Direct Routing user makes an emergency services call.

- Emergency Call Routing Policies can include more than one Dial String. Each must be unique
- In the United States, “911” will be the most common Dial String added to Emergency Call Routing Policies. In some cases, the number passed will be different.
- If your ERSP supports it, “933” will almost always be added as a Dial String in an Emergency Call Routing policy.

Emergency Dial Mask

- Each Emergency Dial String can have one or more Emergency Dial Masks separated by a semi-colon, “911;9911;112”.
- The masks are used to identify emergency calls based on the various ways a user might dial an emergency call.
- In the United States “911” should always be added as a mask to comply with Kari’s Law. Even if it is remotely possible that a user might inadvertently dial “9911”, you should add this mask.
- Most European and Asian users are used to dialing “112” to reach emergency services. It may be prudent to add this mask in case a visiting European or Asian colleague dialed “112” instead of “911” from a user’s signed in Teams device or Common Area Phone.
- There is a myriad of other emergency numbers foreign visitors to a company’s offices might dial. They should be added as needed.
- If your ERSP supports the “933” test number, a common dial mask would be “933;9933”.

PSTN Usage

- PSTN Usages are Teams telephony objects that contain Teams Voice Routes. An in-depth discussion of Teams Voice Routing is beyond the scope of this document. To get more information on the subject please review [Configure voice routing for Direct Routing](#).
- Teams Voice Routes are what are used to route emergency calls to the company’s Direct Routing SBC(s).
- In most cases, there will be one PSTN Usage and one Voice Route for each Direct Routing SBC.
- Companies may have more than one Direct Routing SBC for geographic reasons, redundancy, etc. In these instances, you will almost always need more than one Voice Route, PSTN Usage and Emergency Call Routing policy for emergency calling.
- At times, a company will have two (2), or more, SBCs to provide resiliency for Direct Routing:
 - Resiliency can be achieved by adding a usage with a route for each SBC to an online voice routing policy.
 - Setting up route resiliency in an Emergency Call Routing policy is more challenging due to its only supporting a single PSTN usage.
 - The trick is to add two (2) routes to the usage and leverage the priority attribute of the routes.
 - When more than one (1) route with the same “Dialed Number Pattern” is added to a usage, the “Priority” attribute of the route can be used to ensure that the route with the lower “Priority” has precedence over the route with a higher “Priority”.
 - The result will be that Teams will try the route with the lower Priority first.
 - If you want to do round robin routing between two (2), or more, SBCs, you can add both SBCs to a single route.

Typical Teams Emergency Call Routing Policy

- Following is a sample Teams Emergency Call Routing policy for:
 - A United States based tenant.
 - One Direct Routing SBC resulting in a single PSTN Usage named “Emergency” and a single Voice Route also named “Emergency”.
 - The Voice Route will match if the called number is 911 or 933 and will route these calls to the SBC.
 - If your ERSP does not support a test number, delete the Dial String for 933:

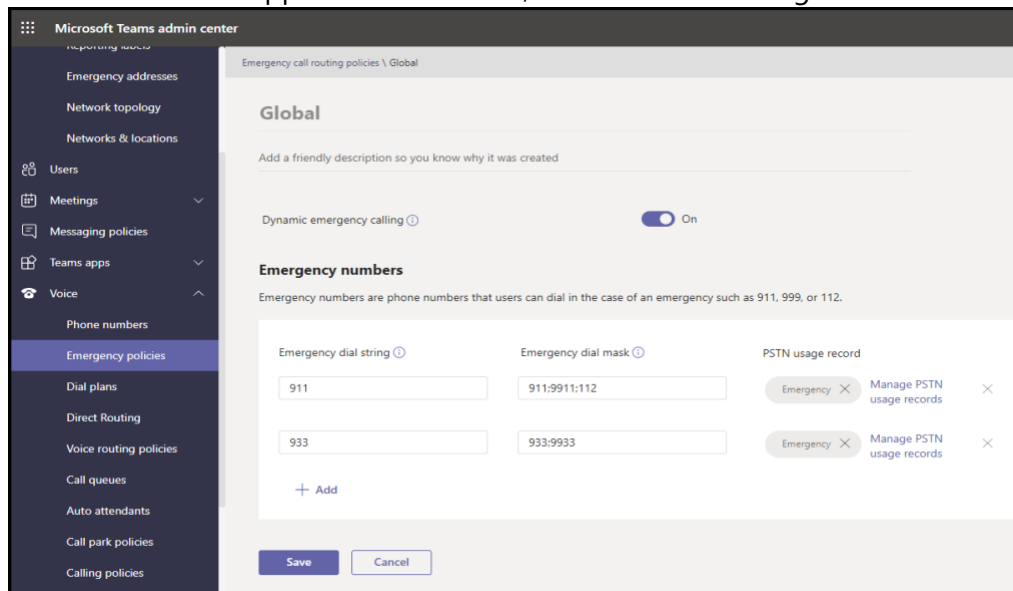


Figure 8 Sample Teams Emergency Call Routing Policy

Configuration Notes for Teams Emergency Policies

- The number of Teams Emergency Calling and Emergency Routing Policies you need to configure will probably be different. Teams Emergency Calling Policies are applicable to Teams Calling Plan, Operator Connect and Teams Direct Routing customers. Teams Emergency Routing Policies are only applicable to Teams Direct Routing installations.
- You will end up with a Teams Emergency Calling policy for each one of your company’s buildings.
- The number of Teams Direct Routing SBCs will likely affect the number of Emergency Call Routing Policies that need to be created.

Summary

- Kari’s Law went into effect on February 16, 2020, and applies to all MLTS installed on or after that date.
- The law includes a prohibition for requiring users to dial anything other than 911 on an MLTS to reach emergency services.
- This is built into Microsoft Teams for Calling Plan and Operator Connect users.
- Emergency Call Routing policies are required for Teams Direct Routing users to comply with both Kari’s Law and the RAY BAUM Act.

- There is also a requirement to notify an internal resource when a user places an emergency services call. **Emergency Calling Policies must be configured for Calling Plan, Operator Connect and Direct Routing installations to ensure compliance.**

Chapter 4 Configuring Teams to Comply with RAY BAUM's Act

Introduction

The RAY BAUM (Repack Airwaves Yielding Better Access for Users of Modern Services) Act was enacted on August 1, 2019. It applies to all on-premises fixed devices associated with a multiline telephone system (MLTS) as of January 6, 2021. The coverage will be extended on January 6, 2022 to include all on-premises non-fixed devices and all off-premises devices.

- For on-premises non-fixed devices, dispatchable locations must consist of the validated street address of the Emergency Services caller plus additional information to adequately identify the caller's location such as floor, suite, apartment, etc.
- State and municipal laws and regulations can supersede Federal laws if they are not inconsistent with them.

Automatic Provisioning of Dispatchable Locations to Emergency Services

- The act requires that "dispatchable locations" must be automatically provided to Emergency Services when a 911 call is placed.
- For all devices, the location must be provided automatically where technically feasible otherwise the information can be based on end user manual update or enhanced location information.
- Enhanced location information refers to the use of coordinates or Geocodes (latitude and longitude) to determine a location. Most of the Teams clients will attempt to get the Geocodes from the Operating Systems location services.
- The discussion of what constitutes a "dispatchable location" is covered above. There are several factors used to determine what the appropriate definition of dispatchable locations are for a company .
- Microsoft Teams clients can be signed on to one of three (3) general locations:
 - Corporate on-premises networks.
 - External or home networks.
 - Virtual Device Infrastructure (VDI) device networks.
- Microsoft Teams Dynamic 911 provides the dispatchable location for users logged into Microsoft Teams from corporate on-premises networks from both fixed and non-fixed devices. Teams has had this capability for several years.
- Microsoft Teams Dynamic 911 for Work from Home (WFH) provides the dispatchable location for users logged into Microsoft Teams from external or home networks. This feature became available in December 2021. A detailed discussion of this feature and how to enable it can be found in the Work from Home section below.
- Dynamic 911 for Azure Virtual Desktop, VMware and Citrix VDI clients is expected to be available in February 2022.

Determining the Microsoft Teams User's current Dispatchable Location

- The following process is the same for Teams Calling Plan, Operator Connect and Direct Routing users.
- Shortly after signing in, the Teams client will ask the device's Operating System for some information:
 - The Public IP of the Internet router that the device's Internet traffic flows through.

- Network Elements.
 - Subnet.
 - Attached Wireless Access Point.
 - Chassis ID of the Network Switch the device is attached to.
 - The Port on the Network Switch the device is attached to.
 - The device's Geocodes attained from the Operating System's location services.
- The client will send all this information to the Teams service.
- The Teams Service will use this information to simultaneously derive a Dynamic 911 location and a WFH location.
 - Dynamic 911 Location:
 - If the Public IP matches a defined Teams Trusted IP Address, the Teams service will try to match the values of the Network Elements to the Network Elements in Teams.
 - If it gets a match, Teams will send the location information associated with the matched element as the current Dynamic 911 dispatchable location of the Teams device.
 - This Dynamic 911 location will be returned to the Teams client.
 - Dynamic 911 for WFH:
 - At the same time, the Teams service will attempt to lookup an address based on the Geocodes provided by the Operating System's location service.
 - If it gets a match, it will provide this location back to the Teams device.
- **If the Teams device gets a location back from both queries, the device will use the location provided by Dynamic 911.**
 - **This location is defined as a validated location.**
 - **The user cannot change this location in their Teams client.**
- If the device does not get a Dynamic 911 location:
 - But gets a WFH location, the Teams client will ask the user to verify the offered location. If the user verifies the location, it is considered a validated location.
 - The user can change the suggested WFH location. The user will be able to type in a correct location. The Teams client will do a live map search as the user types in the address. If the map search returns an address and the user approves it, it is a validated address.
 - If Teams does not return a suggested address based on the Geocodes, the user can manually enter the address with the map search suggesting an address as the user types it in.
 - If the map search does not return a correct result, the user can continue to type in the address and approve it. This is considered an unvalidated address.
 - If the user does not approve a suggested address and does not correct it, the address is an unvalidated address.
 - If Teams does not return a suggested address based on the Geocodes and the user does not add and approve the address, Teams will use the Address of Record for the user for Calling Plan and Operator Connect users. For Direct Routing users, there will be no value for the device's dispatchable location. In both cases, the dispatchable location would be classified as an unvalidated address.
- WFH users should be trained to always approve an address in the Teams client.

Validated and Unvalidated Addresses

- Dynamic 911 dispatchable locations should always be treated as validated addresses by Microsoft Teams.
- **Verification of an address by a WFH user determines if their call to emergency services will be routed directly to the PSAP or will first be routed to the Emergency Call Response Center (ECRC).**
- Calls with validated addresses will be routed directly to the PSAP for Teams Calling Plan users.
- Calls from Teams Direct Routing users with validated and unvalidated addresses will be routed by the SBC to the ERSP then automatically to the PSAP by the live agent.
- Calls from Teams Calling Plan and Operator Connect users with unvalidated addresses will first be routed to the ECRC. A live agent will ask the caller to confirm their current address. The agent will then route the call to the PSAP based on this address.
- Most ERSPs provide the option to create an Automatic Line Identification (ALI) table. This is a static mapping of a telephone number to a location. This is essentially the Teams Direct Routing version of a Teams Calling Plan or Operator Connect address of record. While not a perfect solution, it may someday reduce the amount of time in getting the emergency services caller to the PSAP when Teams cannot provide a dispatchable location to the ERSP.

Microsoft Teams Calling Plan and Operator Connect Users

On-Premises Devices

- All on-premises devices should receive a dispatchable location from Teams Dynamic 911.
- Microsoft Teams will deliver the dispatchable location information for Microsoft Teams Calling Plan and Operator Connect users directly to the PSAP.
- This is a default configuration for Calling Plan and Operator Connect users requiring no additional administration by the customer.

External and WFH Devices

- Emergency Services calls from Teams devices with validated address for their dispatchable location will be routed directly by Microsoft to the appropriate PSAP.
- Calls with unvalidated or blank dispatchable locations will be routed to the ECRC. The ECRC agent will be able to see the unvalidated address of record during the call. The ECRC agent will route the call to the PSAP once the caller's current location has been determined.

Microsoft Teams Direct Routing Users

- Microsoft Teams will add the dispatchable location information for validated and unvalidated addresses to the Session Description Protocol (SDP) section of the SIP INVITE routed the customer's Teams Direct Routing Session Border Controller (SBC). **The addresses forwarded to the ERSP do not indicate if they are validated or unvalidated.**
- This information is referred to as the Presence Information Data Format – Location Object (PIDF-LO). It is presented in the Extensible Markup Language (XML) format.
- An Emergency Location Identification Number (ELIN) can also be sent with the PIDF-LO information.

- If you enable logging on the SBC you will be able to see the PIDF-LO information in the trace. Following is an example of some PIDF-LO information. The “method” field is used by the ERSPs to determine if the provided address information has been validated and verified. This is discussed in the sections below. The formatting has been modified for easier readability:

```

Content-Type: application/pidf+xml
Content-Disposition: render;handling=required
Content-ID: <sip:jdoe@panhandleci.com>

<?xml version="1.0" encoding="utf-8"?>
<presence xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" entity="sip:jdoe@panhandleci.com" xmlns="urn:ietf:params:xml:ns:pidf">
  <tuple id="tuple0">
    <status>
      <geopriv xmlns="urn:ietf:params:xml:ns:pidf:geopriv10">
        <location-info>
          <Point srsName="urn:ogc:def:crs:EPSG::4326" xmlns="http://www.opengis.net/gml">
            <pos>30.4761 -86.1468</pos>
          </Point>
          <civicAddress xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
            <country>US</country>
            <A1>FL</A1>
            <A2></A2>
            <A3>Freeport</A3>
            <PRD></PRD>
            <RD>Power Line Road</RD>
            <STS></STS>
            <POD></POD>
            <HNO>166</HNO>
            <HNS></HNS>
            <LOC>Office 306</LOC>
            <NAM>Panhandle Consumer Industries</NAM>
            <PC>32439</PC>
            <ELIN></ELIN>
          </civicAddress>
        </location-info>
        <usage-rules>
          <retransmission-allowed xmlns="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy">true</retransmission-allowed>
        </usage-rules>
        <method>
          LIS
        </method>
      </geopriv>
    </status>
  </tuple>
</presence>

```

Figure 9 Sample PIDF-LO Information from an SBC Syslog

- ERSPs support routing emergency services calls by using PIDF-LO information or the ELIN. Some offer both.
- Some ERSP’s and SIP Trunk vendors offer emergency call routing by using an ALI database. This type of routing is not dynamic, and its use may violate the RAY BAUM Act. It is commonly used as a “last resort” for determining the address of a 911 caller.
- Some SIP Trunk vendors resell ERSP services, or have built their own and can provide ERSP functionality supporting PIDF-LO and/or ELIN based routing.
- The ELIN is a Phone Number associated with a dispatchable location. The association of the number and the location are maintained in a database hosted at the ERSP. It is an alternative method for delivering an emergency caller’s current dispatchable location to the PSAP.

Dynamic 911 and Teams Direct Routing Session Border Controllers

- The web page, [Session Border Controllers certified for Direct Routing](#) provides a list of SBCs certified by Microsoft for Teams Direct Routing
- Most of the SBCs on the list are certified to be integrated with any of the ERSPs listed at the bottom of the page.
- Approximately half of the SBCs support using ELINs to route emergency calls.
- Customers need to consider this when purchasing SBCs to be used for Teams Direct Routing.

Adding the ERSP

- The customer should solicit service proposals from several ERSP vendors. A list of vendors certified can be found on the [Session Border Controllers certified for Direct Routing](#) web page previously referenced.
- The customer would establish an interface from the SBC to the ERSP. This will usually be over a dedicated SIP Trunk connection.
- Using the connection to the ERSP, the customer will configure the router to send the emergency call including the PIDF-LO information to the ERSP. The ERSP will “read” the dispatchable location information in the PIDF-LO and will automatically route the emergency caller to the appropriate PSAP. The SIP INVITE sent to the ERSP by the SBC will have the emergency caller’s Source\Calling Number in the SIP “From” field and the emergency number, “911” in the United States, in the “To” field.
- If the call does not have a dispatchable location, the call will usually be redirected to a live agent at the ERSP. The agent will ask the caller for their current location and will route the call and the location to the appropriate Public Safety Answering Point (PSAP). Each ERSP may handle these calls differently. The customer should consider this when evaluating ERSPs.

Using ELINs with the ERSP

- There are a few additional required configuration steps to use ELINs instead of the PIDF-LO information to refer to the current dispatchable location of a Teams Direct Routing emergency caller:
 1. The same ELIN number can be assigned to more than one Emergency Address or Location\Place record.
 2. The customer will have to acquire and assign unique telephone numbers to each of their Teams Emergency Address and Location\Place records referring to a dispatchable location. These will have to be Direct Inward Dial (DID) numbers. These numbers must be DIDs in case the PSAP needs to call the emergency caller back should the original call get disconnected. DIDs assigned to Teams users cannot be used as ELINs. The DIDs assigned to statically placed devices such as Common Area Phones and Teams Meeting Room devices generally can be used as ELINs.
 3. The ELIN numbers must be added to the appropriate Teams Emergency Address and Location\Place records. As a reminder, Teams Emergency Address records cannot be modified once created. This includes adding, changing, or deleting the ELIN number. For this reason, it is recommended when using ELINs to put the ELIN numbers on the Location\Place records instead of the Emergency Address records. An ELIN number can be added to the default location record of the Emergency Address.
 - a. The information with the validated address of the dispatchable location and the assigned phone number will have to be provided to the telephony provider or ELIN in a format defined by them.
 - b. The SBCs will have to be configured to “handle” ELIN numbers in emergency calls. For some SBC vendors this requires the purchase of an “ELIN” license. On most SBCs there will be a switch(es) or setting(s) that will need to be modified to support the use of ELINs.
 - c. Some SBCs have a mechanism that can handle callbacks from the PSAP for ELIN callers.
 - i. This is a very important feature for the case where ELINs can be assigned to multiple Teams Emergency Addresses and Locations\Places.
 - ii. These SBCs will keep track of the original phone number of the emergency services caller and the ELIN that was sent to the ERSP.

- iii. If the PSAP calls the ELIN number back, the SBC will route the call to the source number of the most recent instance of the ELIN call.
4. The customer will configure the SBC to send the emergency call to the telephony provider or ERSP.
5. To send the ELIN, the SBC (this is true for AudioCodes SBCs and is likely true for other vendor's products) will place the emergency caller's Calling Name and Source\Calling number in the "P-Asserted Identity" field of the SIP INVITE.
6. The ELIN number will be placed in the "From" field of the SIP INVITE and the emergency number, "911" in the United States, in the "To" field.
7. The provider on receipt of the call will look up the ELIN number in the customer's database to get the dispatchable location of the Teams Direct Routing emergency services caller.
8. The provider will use the location information to direct the call to the appropriate PSAP.
9. The user's calling number must not be overridden or replaced when the user makes an emergency call.
10. The customer should check with their ELIN provider to see how they will handle calls that do not have an ELIN.

Emergency Calling and the Teams Caller ID Policy

- PSAPs will sometimes call the emergency services caller back. They will call the user using the Calling Number presented when the user placed the call.
- In Teams, Caller ID Override Policies can be configured. Information on these can be found on the [Manage Caller ID Policies in Microsoft Teams](#) web page. Customer's will frequently use these to replace the user's phone number with the company's Main Number.
- If the PSAP tries to call the emergency services caller back, they would dial the Main Number. They would not be able to reach the original caller directly.
- To prevent this problem:
 - In the Teams Admin Center (TAC) turn on the "Forward P-Asserted Identity (PAI) header" switch for the SBCs. This switch will usually already be turned on.
 - On the SBC you will need to create a rule (on AudioCodes SBCs this would be a Message Manipulation rule) that matches these criteria:
 - Dialed number is 911 or 933.
 - The value of the SIP FROM and P-ASSERTED IDENTITY header do not match.
 - If there is a match:
 - Replace the value in the SIP FROM header with the value in the P-ASSERTED IDENTITY header.
 - In some cases, you will not be able to turn the setting on in Teams. If you can't:
 - Don't use the Teams Calling Line Identity policy to override your user's Caller ID.
 - Setup your Caller ID overrides on the SBC.
 - Set these up to do the override if the dialed number is not 911 or 933.

Configuring Microsoft Teams to comply with the RAY BAUM Act for Dynamic 911

- Required objects\elements for Teams Calling Plan and Operator Connect users:
 - Teams Emergency Addresses.

- Teams Emergency Locations\Places.
- Teams Tenant Trusted IP Addresses.
- One or more of the Network Elements in the Teams Location Information System (LIS) Database.
- Additional requirements for Direct Routing users:
 - Configuration of at least one (1) Teams Emergency Call Routing policy with “Dynamic Emergency Calling” enabled.
 - Connecting the SBC(s) to an ERSP or SIP Trunk vendor who can leverage the PIDF-LO information or ELINs provided by Teams.
- Tenant Network Regions, Tenant Network Sites and Tenant Network Subnets.
 - These are only required if you need to scope either of the Teams Emergency Policies by building or location.

Teams Emergency Addresses and Locations\Places

- This is discussed in Chapter 2.

Teams Tenant Trusted IP Addresses

- Required for determining an emergency services caller’s location to be provided to a PSAP for Microsoft Teams Calling Plan and Operator Connect users or ERSP for Microsoft Teams Direct Routing users.
- Teams Tenant Trusted IPs are used to determine if the caller is making an emergency services call from an on-premises internal network.
- An IPv4 Tenant Trusted IP record should be added for all routers, firewalls, or other perimeter devices that provide user access to the Internet.
- Entries can be made for single IP addresses, or a range based on the address and a subnet mask.
- Microsoft recommends that both an IPv4 and IPv6 address for these devices be added to the Tenant Trusted IP table.
 - If not already configured, the client should ask their Internet Service Provider (ISP) to provision an IPv6 address for their devices providing Direct Internet Access (DIA) to their users.
 - These can be single IPv6 addresses or ranges with subnet masks like the IPv4 addresses. All addresses should be statically provided by the ISPs.
 - The router/firewall will have to be configured to listen for and send traffic using IPv6.
 - **The client’s internal networks do not need to be configured to support IPv6 addressing or routing.**

Teams Location Information System (LIS) Database and Network Elements

- The Teams Local Information System Database (LIS) is used to determine an emergency caller’s current location and provide that information to the PSAP or ERSP when making an emergency services call! It is truly what makes 911 calling dynamic!
- At its heart, the LIS allows us to associate a defined Teams Location\Place to a network element in the LIS database:
 - Network Subnets.
 - The Basic Service Set IDs of Wireless Access Points.

- Chassis IDs of network switches.
- Specific ports on network switches.
- The ultimate question when configuring the LIS Database is whether to use Subnets, Wireless Access Point, Switches or Switch Ports, or a combination of these, to identify the current location of a user when they make an Emergency Services call.
- There are three (3) required steps to answer this question:
 - Review any applicable State or Municipal laws and regulations that define what a dispatchable location is beyond the definition in the RAY BAUM Act (additional information to adequately identify the caller's location such as floor, suite, apartment, etc.).
 - Discuss with your corporate counsel, risk and compliance managers and human resources department their requirement for the precision of the dispatchable location requirement. This level could exceed the regulatory requirement.
 - Work with the corporate IT team to determine how to provide the required level of dispatchable location based on the configuration of the elements of the network infrastructure.
- The process to determine this required level of dispatchable location is discussed in more detail above.

Teams Admin Center

1. To add network elements to the LIS database in the Teams Admin Center, click on "Locations" then "Networks and Locations". Select the type of element you want to add then click the "Add" button.

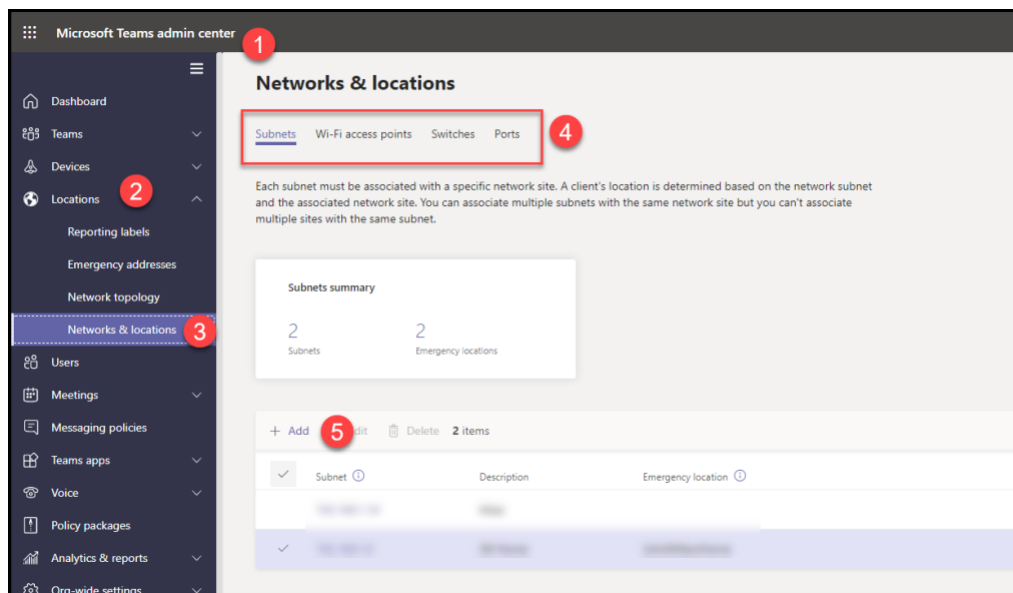


Figure 10 Adding Teams LIS Network Elements

2. For each element you will need to add:
 - The identifier such as the subnet or the chassis ID of a switch. The subnet element also requires the type of subnet (IPv4 or IPv6) while the Port element requires the switch Chassis ID and Port ID.
 - The Location\Place to associate with the element.

- An optional, but recommended, description of the element.
3. Click the “Apply” button.

Using the Network Switch and Ports Network Elements to provide Dynamic 911 Locations

- Configuring the Teams Location Information System (LIS) Subnet and Wireless Access Point (WAP) Network Elements is straightforward.
- Some Companies will have to use the LIS Network Switches or Ports network elements to derive locations for user’s placing calls to emergency services.
- These Companies are compelled to use these, instead of the Subnets or WAPs because the company’s business dynamic 911 rules dictate that locations must be specific down to the office or cube number.
- In some cases, the dynamic 911 rules may require precision to the floor but due to how the networks and subnets are setup, the Switches or Ports still would need be used to satisfy this requirement.
 - An organization occupies three (3) non-contiguous floors in a multi-tenant building.
 - They have a single IP subnet in use on all three (3) floors. They also have a second subnet for their Conference Room equipment.
 - Devices are connected to network switches dedicated to each floor. The Conference Room equipment, which is on each floor, is cross connected to a common network switch.
 - They wanted to use floor level precision for their devices.
 - To meet the requirement, the floor level locations were assigned to the switches on each floor.
 - The floor level locations were assigned to the ports on the common Conference Room switch individually.
- For some Companies, implementing dynamic 911 and having to use the network Ports to determine a location can be a major undertaking.
- It is common for Companies to not have accurate (or any) documentation detailing the switch port that a specific network jack is connected to.
- If you are in this situation, you are going to have to map this out. This will be, almost without exception, a manual process with a significant requirement for manpower.

Defining Teams Locations for Network Switch Ports

1. Verify that your network switches can provide [Link Layer Discovery Protocol – Media Endpoint Discovery](#) (LLDP) information to your Teams endpoints and to turn it on.
 - LLDP-MED is a vendor neutral protocol that is like the well-known [Cisco Discovery Protocol](#) (CDP.)
 - It appears that the [Institute of Electronics and Electrical Engineers](#) (IEEE) first wrote about it in 2009.
 - Microsoft Teams clients “listen” for LLDP-MED information and can use it to derive a dynamic 911 location.
 - Most business class network switches manufactured in the last ten (10) years should support this protocol. A Netgear ProSAFE non-business class switch doesn’t while a Cisco 2960 does.
 - In most cases, it will be turned off by default.

- Check with the vendor to see if your switch supports it and how to turn it on.
- 2. Discover the format of the LLDP-MED Chassis ID and Port information from the switches being presented to the Teams endpoints.
 - You should get a sample of this information from an example of every switch in your network. It is worthwhile to do this even if you have different models of switch from the same vendor.
 - Different versions of firmware on the same model of switch could produce differently formatted LLDP-MED information. It would be a good idea to spot check identical switches with different levels of firmware.
 - You may find this information in the manuals for the switch.
 - Take a [WireShark](#) (or similar tool) network trace from your endpoints.
 - Start a trace and let it run for a few minutes.
 - Stop the trace and apply the filter "lldp" to the captured packets.
 - In the example below, the switch was sending the LLDP information to the endpoint every thirty (30) seconds.
 - The Chassis ID of the switch is "30:37:a6:33:f7:2a".
 - The Port ID is "Gi0/42".

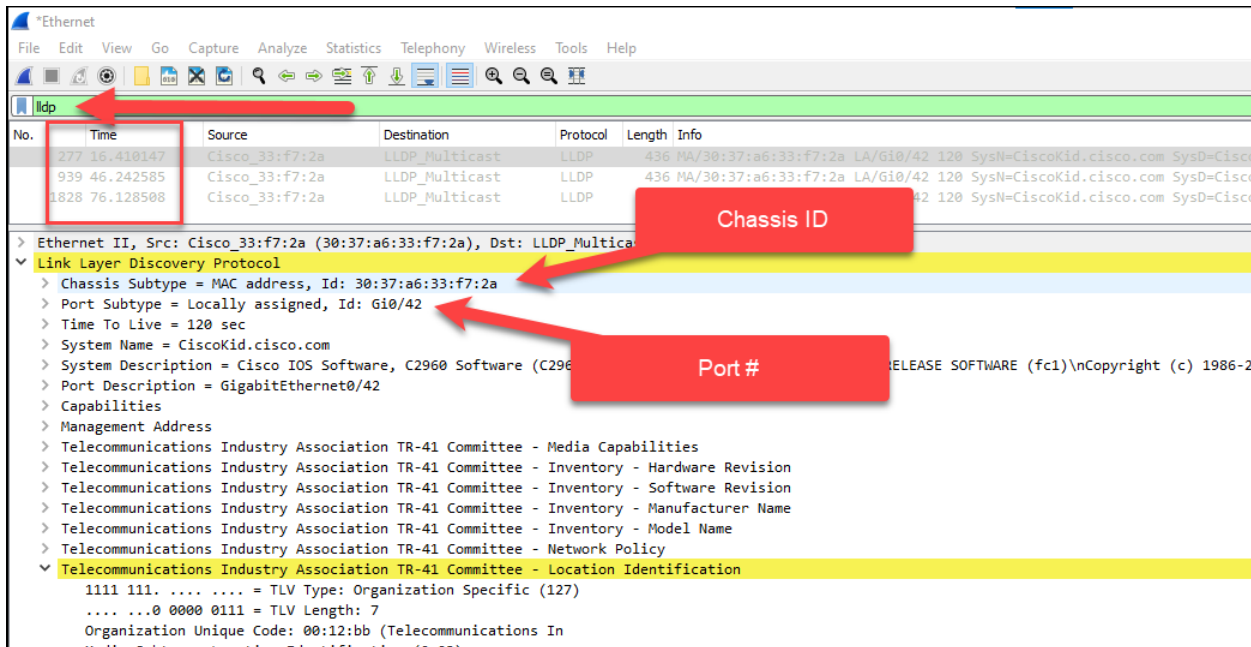


Figure 11 WireShark Trace with LLDP-MED Information

- Use the [PSDiscoveryProtocol Windows PowerShell Module](#).
 - Download and install the module on a Teams endpoint.
 - Open an Administrator level PowerShell Session.
 - Run the command:
 - Invoke-DiscoveryProtocolCapture -Type LLDP | Get-DiscoveryData.
 - The Chassis ID of the switch is "3037a633f72a".
 - The Port ID is "Gi0/42".

```
PS C:\WINDOWS\system32> Invoke-DiscoveryProtocolCapture -Type LLDP | Get-DiscoveryProtocolData

TimeToLive      : 120
Model          : WS-C2960G-48TC-L
VLAN           : 1
SystemDescription : Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 12.2(44)SE6, RELEASE SOFTWARE (fc1)
                Copyright (c) 1986-2009 by Cisco Systems, Inc.
                Compiled Mon 09-Mar-09 18:10 by gereddy
Port           : Gi0/42
Device         :
PortDescription : GigabitEthernet0/42
IPAddress      : {192.168.1.11}
ChassisId      : 3037A633F72A
Computer       :
Type           : LLDP
```

Figure 12 LLDP-MED Information from the PSDiscoveryProtocol PowerShell Module

3. Create an Excel table, database table, etc. to capture the required information.

Building	Office Number	Network Jack ID	Floor	Chassis ID	Port Number
				30:37:a6:33:f7:2a	Gi0/01
				30:37:a6:33:f7:2a	Gi0/02
				30:37:a6:33:f7:2a	Gi0/03
				30:37:a6:33:f7:2a	Gi0/04
				30:37:a6:33:f7:2a	Gi0/05
				30:37:a6:33:f7:2a	Gi0/06
				30:37:a6:33:f7:2a	Gi0/07
				30:37:a6:33:f7:2a	Gi0/08
				30:37:a6:33:f7:2a	Gi0/09
				30:37:a6:33:f7:2a	Gi0/10
				30:37:a6:33:f7:2a	Gi0/11
				30:37:a6:33:f7:2a	Gi0/12
				30:37:a6:33:f7:2a	Gi0/13
				30:37:a6:33:f7:2a	Gi0/14
				30:37:a6:33:f7:2a	Gi0/15
				30:37:a6:33:f7:2a	Gi0/16
				30:37:a6:33:f7:2a	Gi0/17
				30:37:a6:33:f7:2a	Gi0/18
				30:37:a6:33:f7:2a	Gi0/19
				30:37:a6:33:f7:2a	Gi0/20
				30:37:a6:33:f7:2a	Gi0/21
				30:37:a6:33:f7:2a	Gi0/22
				30:37:a6:33:f7:2a	Gi0/23
				30:37:a6:33:f7:2a	Gi0/24

Figure 13 Example Input for LIS Port Information

4. Capture the required information for all locations. There may be some network testing tools that could aid in the process. This will require a lot of time and manpower to get an accurate map.

5. **Once you have the map, make a rule for your network administrators that they should never move a cable to another switch port without accurately documenting it. It might be a good idea to require a Change Control for these types of moves.**
6. Add all required Emergency Addresses and Places to Teams. You will need a Place\Location record for each individual office. Use PowerShell to load the Places into Teams.
7. Add several test Port records to Teams.
 - The Ports can be added through the Teams Admin Center.
 - In Teams PowerShell, use the [Set-CsOnlineLISPort](#) command to add new records.
 - You will need the Location ID corresponding to the office that is connected to the Port.
 - The ChassisID can be added in any of these formats.
 - "3037a633f72a".
 - "30:37:a6:33:f7:2a".
 - "30-37-a6-33-f7-2a".
8. Keep in mind that changes to most of the Dynamic 911 objects and elements can take several hours to converge down to the Teams clients.
9. In the Teams client, go to Settings->Calls and scroll down to verify that the Teams client can derive an accurate dynamic 911 location based on its Port. If it doesn't, you will have to perform some "trial and error" methodology to determine a format that will work.

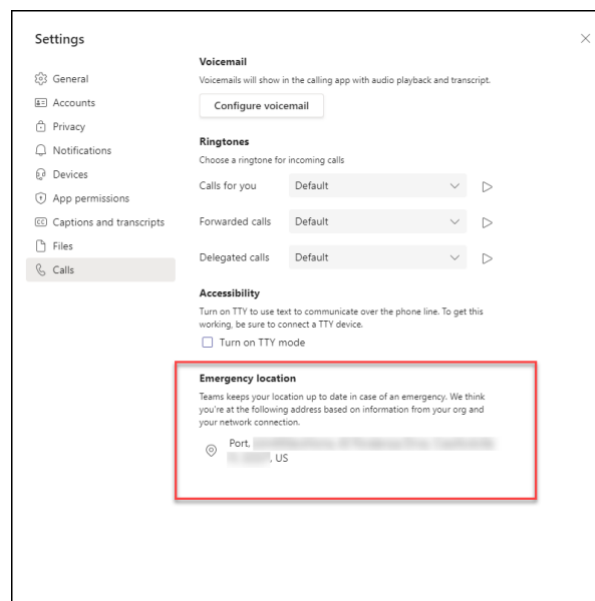


Figure 14 Emergency Location Information for A Teams user on an internal on-premises Network

10. Add the rest of the Port records to Teams through PowerShell.

A Tip from Experience

- Several years ago, I managed a relocation of the company I was working for.

- After the architect designed the space, we reviewed the blueprints and verified\specified the locations of voice and data jacks for each office.
- Every room on the blueprint had a room number defined by the architect.
- With the blueprints in hand, we put the cabling job out to bid.
- Some of the requirements we had for the cabling included:
 - All runs should be labeled with an identifier for the jack on the wall and an identifier for the patch panel in the wiring closet.
 - The jack identifier included the room number from the blueprint. We were able to look at the blueprint and see every jack that we needed to be installed.
 - Full CAT 5 testing was to be performed on every run and the vendor was required to provide the results to us.
- The vendor put multiple identical labels on every cable run spacing them every ten (10) to twenty (20) feet.
- In addition to knowing that all the runs tested good, we ended up with a list that mapped each of the network jacks in the offices to a port on one of the patch panels in the wiring closet.
- Using this information, we added the switch and port that each of the patch panel connections was connected to. We ended up with a list that we could have used for Teams dynamic 911.

Suggestions

- See if your network administrators or facilities personnel have similar documentation from when the office space was built out.
- If you have this information, you can follow the patch cord from the patch panel to the network switches and create a table showing the port on the patch panel and the switch port it was connected to and merge it with the wiring inventory. The combination of the lists would result in your having a mapping of network switch ports to office locations.
- This will save you from creating the inventory by physically visiting every network jack in your space.
- If your wiring closet looks like this, now would be a good time to pull all the patch cords out, rewire and document as you go:



Figure 15 Bad Wiring Closet

- Bottom line:
 - Try to track down accurate blueprints for your office space.
 - See if you have an inventory from the network wiring contractor of the runs that they installed.
 - Look at the back of your wireframe and the patch panels. See if there are labels on them and if the information corresponds to your office numbering scheme. If you don't have the wiring inventory, the labels may still be helpful.

Summary

- If you need to use the "Ports" network element to derive a user's dynamic 911 location, it will be a painful but not impossible task to gather the needed documentation. The good news is once you have it, it's easy to load tens of thousands of Port records into Teams through PowerShell.

Chapter 5 Teams Dynamic 911 – Work from Home

Introduction

Configuring Microsoft Teams to comply with the part of the RAY BAUM (Repack Airwaves Yielding Better Access for Users of Modern Services) Act that went into force on January 6, 2021, is detailed above.

In this section, we will provide information on the “Work from Home” (WFH) functionality added to the Microsoft Teams Dynamic 911 solution in December 2021. WFH is intended to bring Microsoft Teams into compliance with the part of the RAY BAUM act that will come into effect on January 6, 2022.

The first part of the RAY BAUM Act went into effect on January 6, 2021 and requires that a dispatchable location be automatically provided to the Public Safety Access Point (PSAP) when an emergency services call is placed from fixed on-premises devices connected to a Multi-Line Telephone System (MLTS). Dispatchable locations must consist of the validated street address of the emergency services caller plus additional information to adequately identify the caller’s location such as floor, suite, apartment, etc.

The second part of the Act addresses calls made from non-fixed on-premises and all off-premises devices connected to a MLTS. Microsoft Teams has had the ability to provide dispatchable locations for non-fixed on-premises devices for a few years. It did not have the ability to do so for all off-premises devices until the introduction of WFH.

Is this feature turned on by default?

- No, the Teams administrator must turn this on in the Team Emergency Calling policy.
- The feature can be turned on in both the Teams Admin Center and in Teams PowerShell.

Teams Admin Center

1. To enable the Work from Home feature in the Teams Admin Center, click on “Voice”.
2. Click “Emergency policies”.
3. Then “Calling Policies”.
4. Click the “Add” button to add a new policy or click on the policy name to Edit an existing policy.

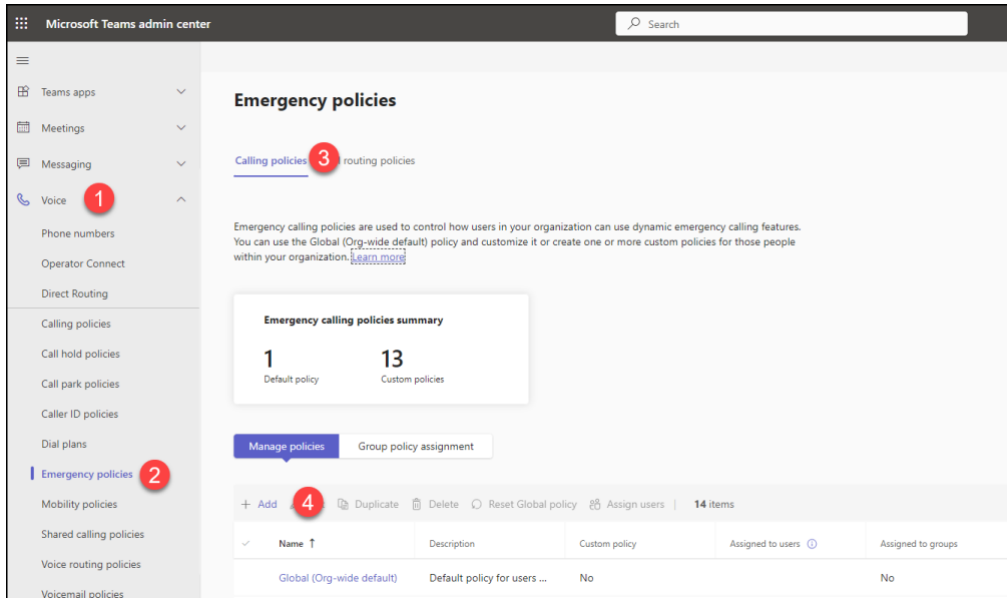


Figure 16 Enabling the Work from Homes External Location Lookup Mode

- Click the “External location lookup mode” switch to the “On” position. Finish adding or editing the policy and click the apply button.

Emergency calling policies \ Add

Add emergency calling policy

Add a description so you know why it was created

External location lookup mode On **5**

Emergency service disclaimer

Enter emergency services disclaimer, if needed.

Emergency numbers

Emergency numbers are phone numbers that users can dial in the case of an emergency such as 911, 999, or 112.

Emergency dial string	Notification Groups	Number to dial for emergency nc	Notification mode
933			None

Save Cancel

Figure 17 Enabling the Work from Home External Location Lookup Mode-cont'd

Teams PowerShell

- To enable this for a single Emergency Calling policy named “Headquarters”, run this command in a Microsoft Teams PowerShell Session:


```
Set-CsTeamsEmergencyCallingPolicy -Identity "Headquarters" -ExternalLocationLookupMode Enabled
```
- To enable this for all Emergency Calling Policies, run this command:


```
Get-CsTeamsEmergencyCallingPolicy | Set-CsTeamsEmergencyCallingPolicy -ExternalLocationLookupMode Enabled
```

Who will this effect?

- This will change the user experience for:
 - Microsoft Teams users who are signed on to an endpoint that is not connected to their Corporate Network.
 - Users working from home full or part time.

- Users signed into networks at airports, customer or vendor locations, libraries, coffee shops, their mom’s house, etc.
- Users using a cellular network or signed on to cellular hotspots.
- WFH is initially supported for these clients:
 - Teams Windows Client.
 - Teams Mac Client.
 - Teams Mobile Client with some limitations.
 - The client does not support entering addresses.
 - It does not “remember” the association between addresses and network locations.

Will there be any impact on Training, Corporate Health and Safety or Compliance Policies?

- Yes, you will need to educate your users on how to use this new feature. The Teams users must know how to use this feature correctly.
- There are some “touchy” considerations when implementing this capability. It is ultimately the user’s responsibility to verify the address being provided to the PSAP by the Teams client is complete and accurate at all times.
- Corporations should consider the legal and liability ramifications of the WFH feature. If a user were to call emergency services through the Teams client with an incorrect address associated with their current location, what litigious exposure is there for the Corporation?
 - Is there exposure if the Corporation did not provide proper training on the use of WFH?
 - If the responsibility of the user to ensure the accuracy of an address was not made clear in the Employee handbook?
- Enabling has asked Microsoft if there are any safeguards available such as a report that could show proper use or compliance with address verification within Teams. Microsoft’s response will be added here.
- Please remember that when Teams sends a location to a Teams Direct Routing SBC, no distinction can be made on the location as to its verification by the user. All locations are treated the same by the SBC and the ERSP. If the ERSP gets a location (right or wrong for the user), it will use it to determine the PSAP to route the call to.

How does this work?

- After signing in, the Teams client will send a location request to the Teams tenant backend service (also known as Teams Dynamic 911 setup for your Corporate Network) and will simultaneously ask the endpoint’s Operating System to provide a location.
- A location returned by Teams Dynamic 911 has precedence over one returned by the Operating System.
- The Operating System will return a location for the machine if:
 - It has been able to determine the location of your machine. The Operating System will use a combination of several sources to determine your location:
 - Global Positioning System (GPS).
 - Nearby Wireless Access Points.
 - Cell Towers.
 - Your IP address.

- The Location Privacy Settings on a Windows endpoint are configured to allow Teams to access your location from the Operating System.
 - If you do not want to grant these permissions or your IT Administrators have configured policies that don't permit it, you will still be able to manually provide your current location to Microsoft Teams.
 - If you see a message like the following, your IT Administrators are managing these policies for you:

*Some of these settings are hidden or managed by your organization.
 - The Location Privacy Settings on your endpoint must be properly configured to pass the requested information from your Operating System to Microsoft Teams.
 - There are several good articles available on how to configure these settings including [Windows location service and privacy](#) for the Windows 10 and Windows 11 Operating Systems.
- The first time Teams asks the Operating System to provide a location; the user will be asked if they want to allow Teams to do so. Microsoft recommends that the user provides this permission. If they do not, they will still be able to provide their location manually.
- The Operating System will return a location in the form of Geocodes. These are the latitude and longitude of the location.
- Teams will send the Geocodes to the Teams backend service and Azure Maps². The backend service will return the best match for the Geocodes.

² <https://learn.microsoft.com/en-us/azure/azure-maps/about-azure-maps>

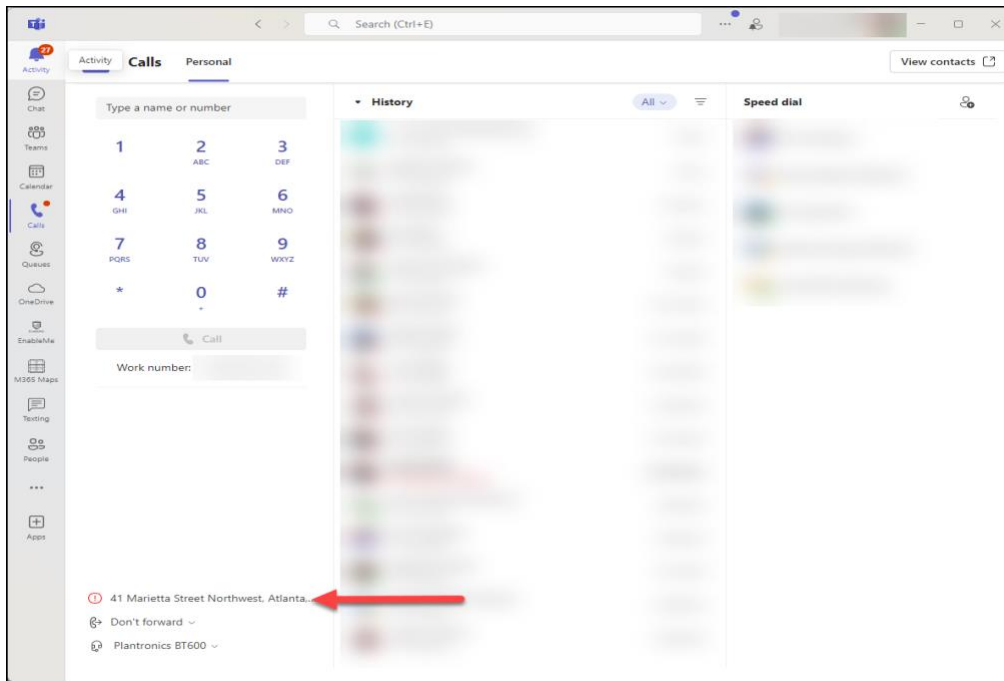


Figure 18 Teams WFH - Suggested and Unverified Address

- The user will have the option to confirm or edit the provided address.

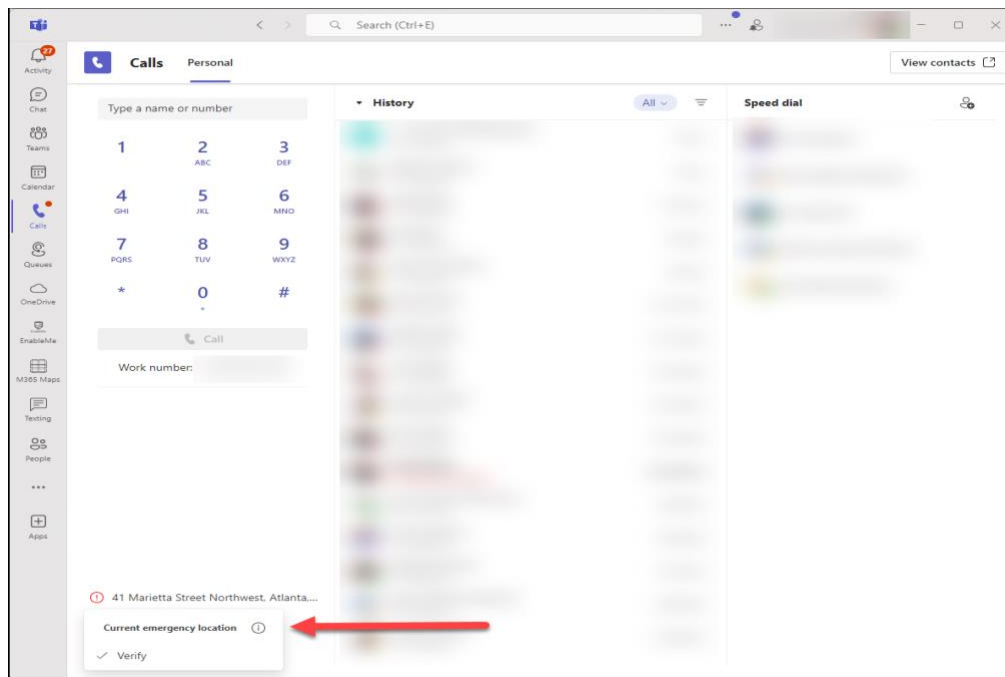


Figure 19 WFH – Editing or Confirming the Suggested Address

- Microsoft and many others working on these solutions have observed that the Geocodes retrieved from the Operating System do not always accurately reflect the current location.
- Even if the Geocodes are correct, there are problems with Azure Maps and the public databases that match addresses to the Geocodes.

- For these reasons, addresses derived from Operating System Geocodes must be confirmed or corrected by the user. It is hoped that in the future, these confirmations will not be required.
- After clicking on the “Edit” button, the user is presented with the address acquired by the Teams client.
- The user can start to type the correct address in the “Address” field. As the user is typing, the Teams client will try to find an address that matches what has been typed. Teams will sometimes come up with several options.
- If Teams comes up with the correct address, the user can click on it then on the “Confirm” button.

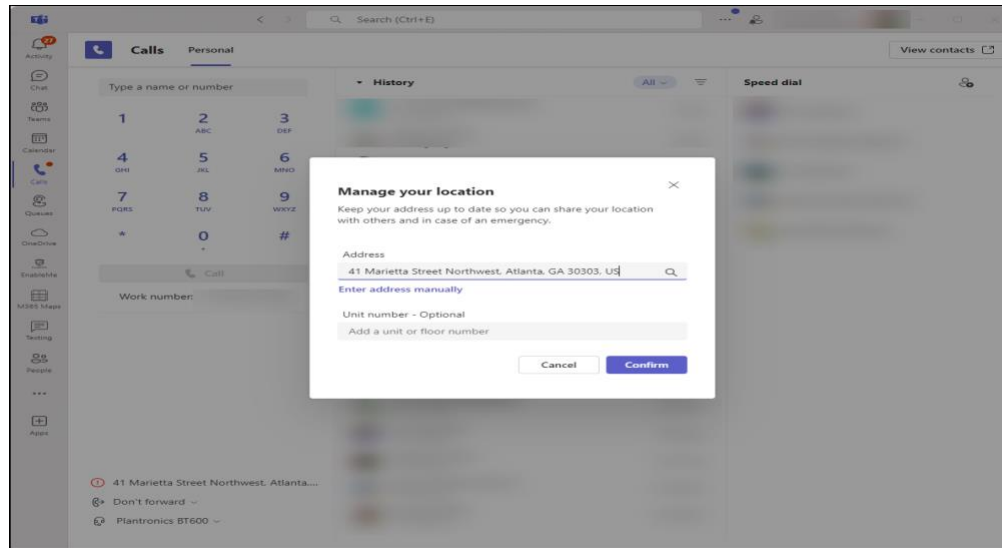


Figure 20 Editing the Suggested Address

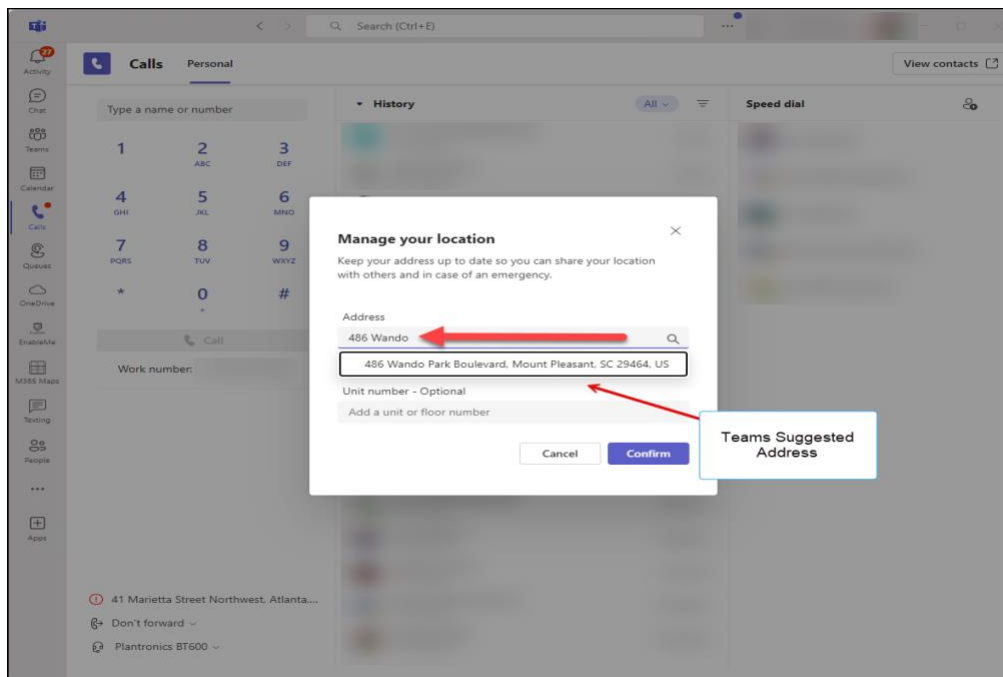


Figure 21 Teams Suggested Addresses based on User Input

- Sometimes Teams will not be able to determine any suggested addresses based on the user’s input.
- The user can clear what they typed from the “Address” box then click the “Enter address manually” button. This will open the address entry form which will allow the user to manually enter their complete address.

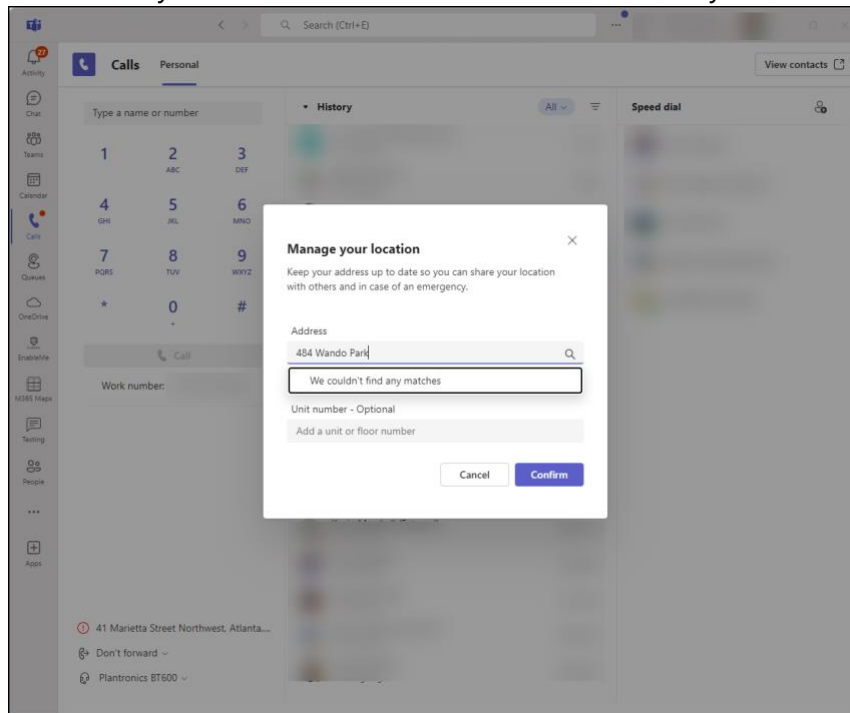


Figure 22 Teams Cannot Provide a Suggestion for the typed Address.

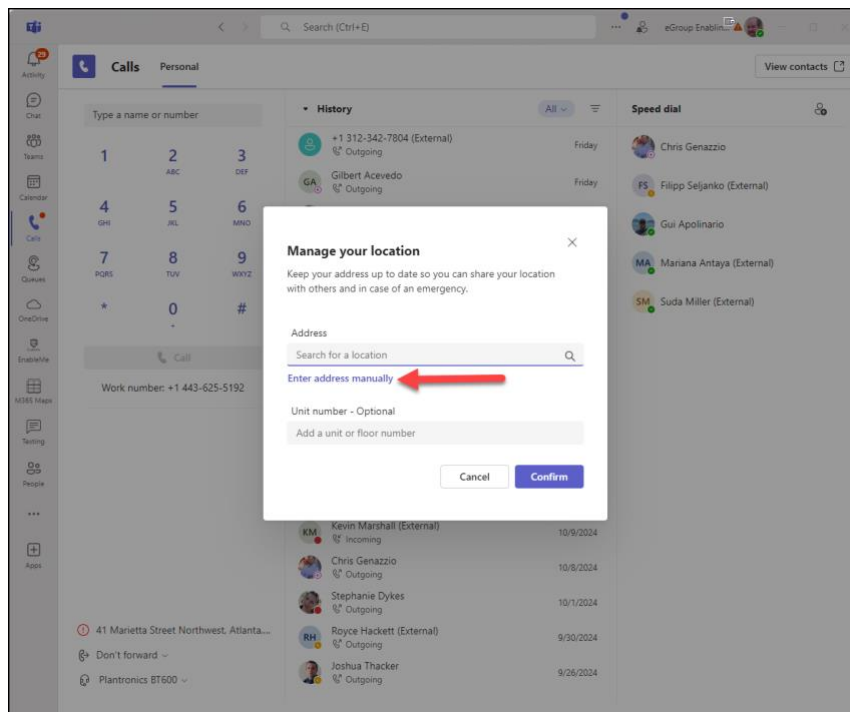


Figure 23 Manual Address Entry

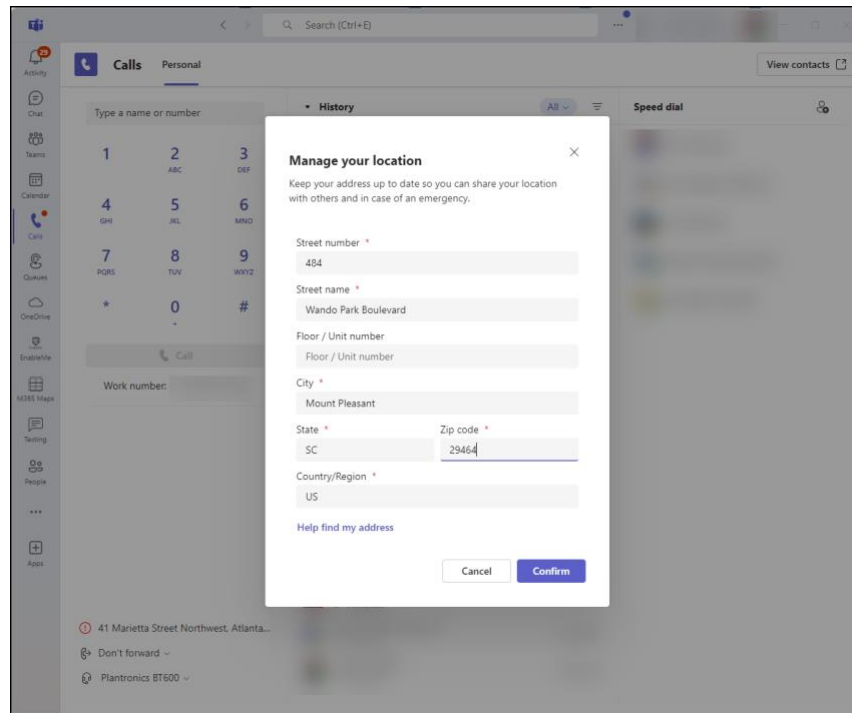


Figure 24 Manual Input of Correct Current Location

- Once confirmed or edited, the address will be saved for the user with a reference to the current network. If the user signs on to Teams while connected to the same network, the saved address will be used as the suggested address.
 - If the user confirms the suggested address, it is “classified” as a “validated address”. When a user with a “validated address” places an emergency services call, Teams will route the call to the PSAP for Calling Plan and Operator Connect Users.
 - For Direct Routing users, Teams will send the PIDF-LO (Presence Information Data Format - Location Object) information and the ELIN (Emergency Line Identification Number) for the location to the Session Border Controller (SBC). The ERSP will route these calls directly to the PSAP.
 - If the suggested address is incorrect, the user should correct it. To correct it they can start typing the address into the “Address” field of the “Manage your location” form. The Teams client will try to suggest one or more addresses based on the user’s input. If Teams can find the correct address, the user can click on it then the “Confirm” button. This process will result in the current location being “classified” as a “validated address” and emergency service calls made by this user will be routed directly to the PSAP.
 - If Teams cannot suggest the correct address, the user will have to enter it manually. These addresses are “classified” as “unvalidated addresses”. When a Calling Plan or Operator Connect user makes an emergency services call, Teams will route the call to the ECC for screening. Once the ECC agent has acquired the caller’s address, the call will be routed to the PSAP by the agent. The Direct Routing ERSP will route the call to their ECRC for screening before routing to the PSAP.
- If the user does not confirm or correct the suggested address, it will be treated as an “unvalidated address.”

- The Teams backend service will not be able to provide an address for the user for any of these reasons:
 - The user did not provide permission for Microsoft Teams to get a location from the Operating System.
 - The Location Privacy Settings are not configured to provide the Operating System's location to Teams.
 - The Teams backend service could not suggest any addresses for the Geocodes presented by the Operating System.

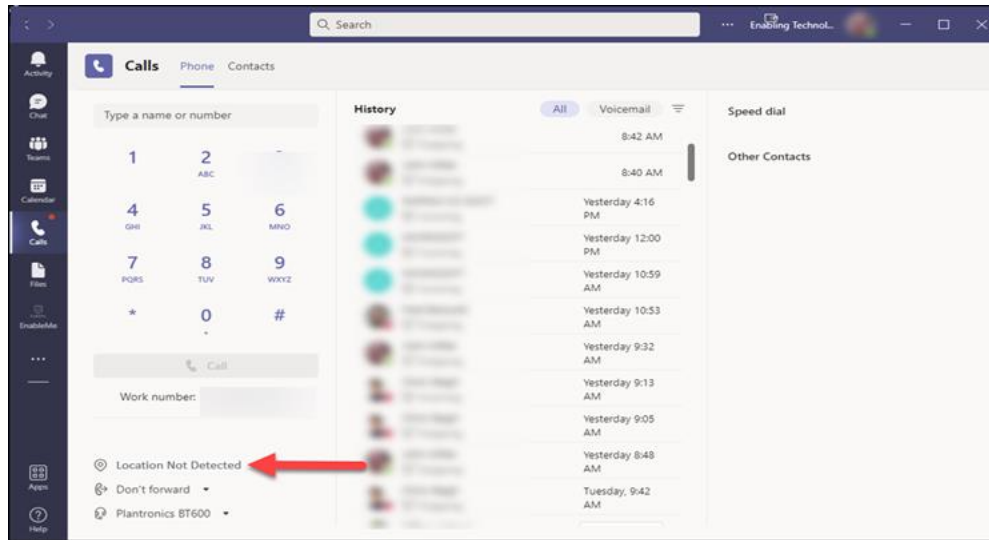


Figure 25 WFH - Location Not Detected.

- In this case, the user will be able to manually enter their current address.

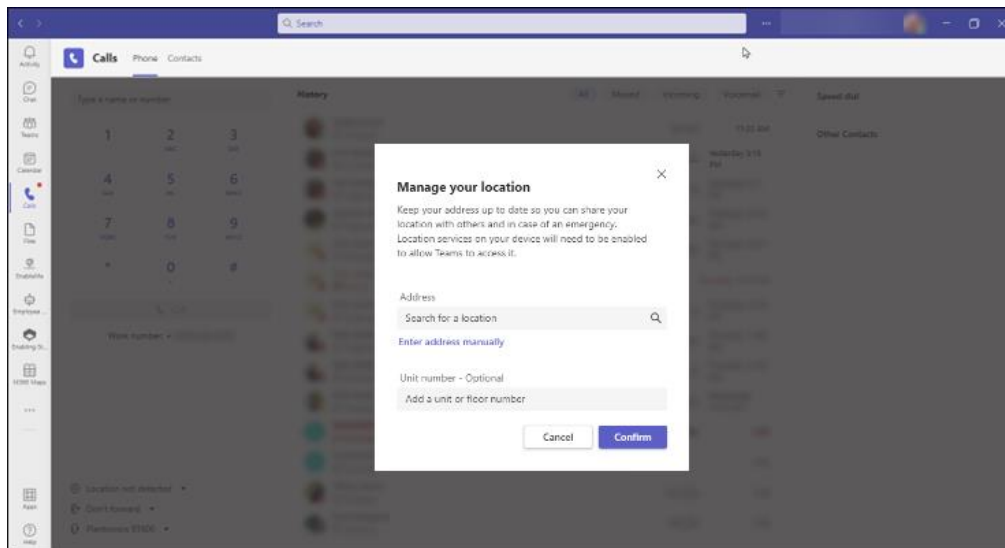


Figure 26 WFH - Manually entering an Address.

Can WFH be used if an On-Premises user cannot get a Dynamic 911 Location?

- The technical answer is “Yes” but the legal answer may be “No” or “it depends.”
- Keep in mind that the RAY BAUM Act as of January 6, 2022, specifies that a Dynamic Location should automatically be provided for all calls made from any device connected to a MLTS.
- In terms of compliance with the Act, this use case should never happen. Fixed and non-fixed devices connected to an organization’s on-premises networks should always get a location from Dynamic 911.
- If a user is not on a network with a network identifier that matches a Wireless Access Point, Switch Port, Switch or Subnet defined by the administrators as a network location, the user will be treated as an off-premises WFH user.
- The Corporation should ensure that all networks that could host Teams users and devices are properly configured for Teams Dynamic 911.
- Microsoft may be adding the ability to track this type of error and provide reporting.
- The Corporation should educate their users to report when this happens.
- Put another way, a user on an organizational network should never see the dialogs and flows associated with the WFH functionality.

Work from Home Call Flows

Calling Plan and Operator Connect Users.

Teams Endpoint location	A Dynamic location is determined from a client network identifier	Teams Gets GeoCodes from the Operating System	The Teams Backend Service suggests an address from the GeoCodes	The user confirms that the suggested address is correct	The user edits the address and confirms an address suggested by the map search	The user manually edits their address.	The user adds the address and confirms an address suggested by the map search	The user adds the address manually	Address Status	What happens when the user makes an Emergency Services Call?
On-Premises	Yes								Validated	The call is routed to the PSAP
Off-Premises	No	Yes	Yes	Yes					Validated	The call is routed to the PSAP
Off-Premises	No	Yes	Yes		Yes				Validated	The call is routed to the PSAP
Off-Premises	No	Yes	Yes			Yes			Not validated	The call is screened by the ECRC then routed to the PSAP
Off-Premises	No	Yes	Yes	No					Not provided	The user's address of record is provided to the ECRC for screening and the call is routed to the PSAP
Off-Premises	No	Yes	No				Yes		Validated	The call is routed to the PSAP
Off-Premises	No	Yes	No					Yes	Not validated	The call is screened by the ECRC then routed to the PSAP
Off-Premises	No	Yes	No					No	Not provided	The user's address of record is provided to the ECRC for screening and the call is routed to the PSAP
Off-Premises	No	No	No				Yes		Validated	The call is routed to the PSAP
Off-Premises	No	No	No					Yes	Not validated	The call is screened by the ECRC then routed to the PSAP
Off-Premises	No	No	No					No	Not provided	The user's address of record is provided to the ECRC for screening and the call is routed to the PSAP

Figure 27 Teams Dynamic 911 WFH - Call handling Logic - Calling Plan and Operator Connect Users

Direct Routing Users

Teams Endpoint location	A Dynamic location is determined from a client network identifier	Teams Gets GeoCodes from the Operating System	The Teams Backend Service suggests an address from the GeoCodes	The user confirms that the suggested address is correct	The user edits the address and confirms an address suggested by the map search	The user manually edits their address.	The user adds the address and confirms an address suggested by the map search	The user adds the address manually	Address Status	What happens when the user makes an Emergency Services Call?
On-Premises	Yes								Validated	<p>*Teams routes the call to the SBC</p> <p>*The SBC sends the call to the ERSR</p> <p>*The ERSR determines the appropriate PSAP for the location and routes the call to the PSAP</p> <p>*If a PSAP cannot be determined, the call is routed to the ERSR's ECRC and live agent, then to the PSAP</p>
Off-Premises	No	Yes	Yes			Yes			Validated	
Off-Premises	No	Yes	Yes				Yes		Non-Validated	
Off-Premises	No	Yes	Yes			No			Not provided	
Off-Premises	No	Yes	No					Yes	Non-Validated	
Off-Premises	No	Yes	No					No	Not provided	
Off-Premises	No	No						Yes	Non-Validated	
Off-Premises	No	No						No	Not provided	
Off-Premises	No	No	No				Yes		Validated	
Off-Premises	No	No	No					Yes	Not validated	
Off-Premises	No	No	No					No	Not provided	

Figure 28 Teams Dynamic 911 WFH - Call handling Logic - Direct Routing Users

Summary

- The second part of the RAY BAUM Act went into effect on January 6, 2022, and applies to all MLTS sold or installed after this date.
- It requires that a dispatchable location be provided to the PSAP when a user places an emergency call from an MLTS.
- Non-fixed on-premises and all off-premises devices are required to comply by January 6, 2022.
- With the rollout of the Dynamic 911 WFH capability, Teams can provide dispatchable locations for all fixed and non-fixed on-premises and off-premises devices .
- The process to configure Teams to provide these locations for WFH users is the same for Teams Calling Plan, Operator Connect, and Direct Routing users.
- This feature will not work unless the Work from Home users are diligent about verifying their current address when using Microsoft Teams.

Chapter 6 Making Teams Dynamic 911 Test Calls

Introduction

There is one aspect of Microsoft Teams Dynamic 911 testing that is usually overlooked, making a successful 911 call. What constitutes a successful call?

- The call reached the Public Safety Answering Point (PSAP)
- The call reached the correct PSAP
- The PSAP agent sees the caller's correct phone number
- The PSAP agent receives the caller's correct location
- Verifying the Emergency Location in Teams

Once Microsoft Teams Dynamic 911 has been setup, including the Work from Home (WFH) feature, we can verify the user's current location in the Teams client. The location that Teams has derived for the user's current location can be seen by clicking on Settings in the Teams client then on "Calls":

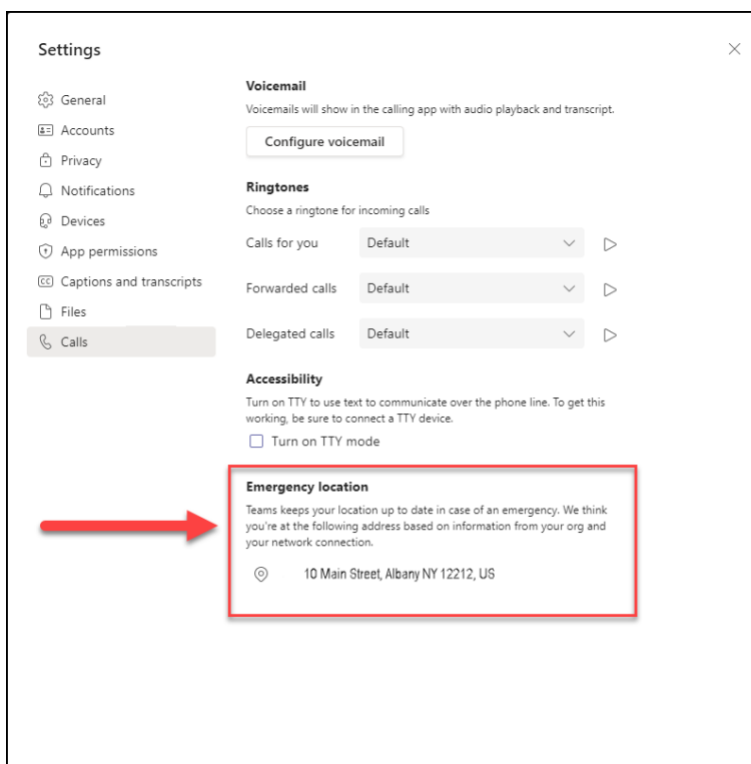


Figure 29 Current Emergency Location in the Teams Client

- The location can also be found on the "Calls" tab in the Teams client:

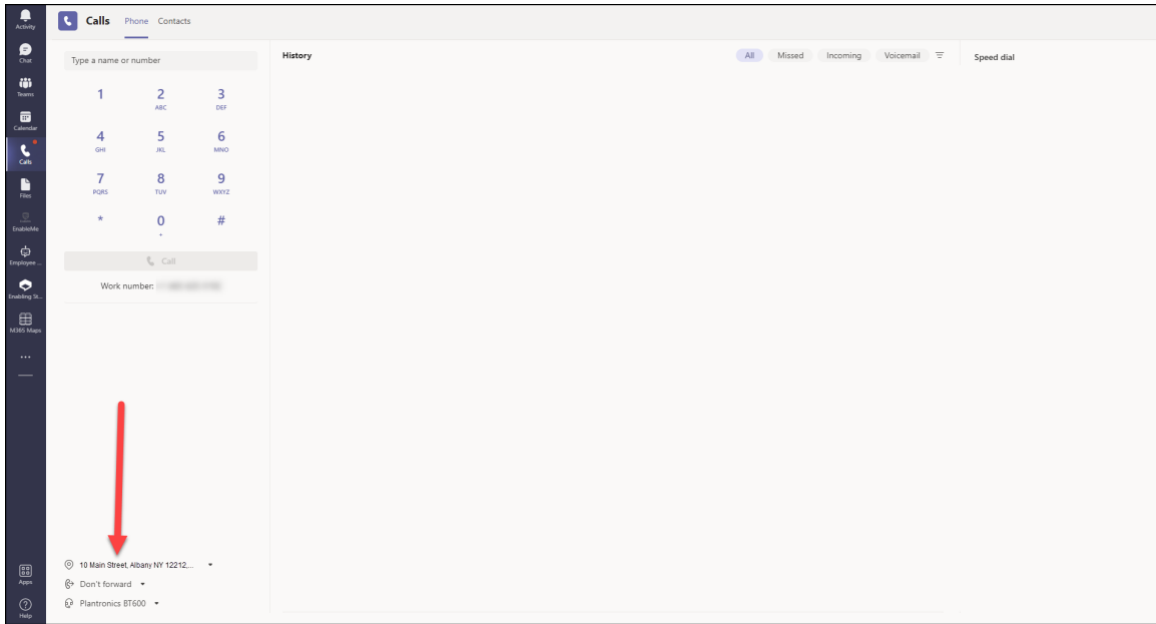


Figure 30 Current Location from the Calls Tab in the Teams Client

Checking this information will provide some of the answers needed to verify whether Teams Dynamic 911 and WFH are working correctly:

1. Is the Teams client able to determine a user's current location?
2. Is the correct location provided for a corporate network connected Teams client? Are the Emergency Address and specific location correct based on the user's current subnet, connected wireless access point, connected switch or switch port?
3. Does a WFH user see the address that they have validated for their current location?

The client's technical teams should investigate and resolve incorrect or unexpected results.

Making test calls using the "933" Test Number

For Calling Plan and Operator Connect users, the Emergency Response Service Provider (ERSP) function is included and built into the Teams service. Direct Routing customers will have engaged with a 3rd Party ERSP or will acquire the ERSP functionality through their SIP Trunk vendor.

Teams Calling Plan and Operator Connect users can leverage the built in "933" test number as part of their Emergency Services Calling testing. Most of the ERSPs and SIP Trunks support dialing "9933", or some other test number, in their systems.

Calls to "933" test numbers are used to verify what should happen when a user makes a real emergency call 911. They do not conclusively indicate what will happened when a Teams user calls 911.

When a Calling Plan or Operator Connect user dials 933 from a Teams client that supports Dynamic 911, they will be connected to a bot hosted in the Teams Service. The caller will hear a message describing how an actual Emergency Call would be handled by the service:

- Your subscriber identifier. This is your phone number.

- The bot will tell you whether your Teams client has determined that your current address includes a latitude and longitude.
- The bot will tell you whether your call will be routed to the PSAP or to the Emergency Call Center(ECC). If the call were routed to the ECC, you would be connected to an agent through the Teams service who would verbally verify your current location before forwarding your call to the appropriate PSAP. In our previous blog article, [Work from Home on Teams & Comply with RAY BAUM](#), we discuss how the decision is made to route emergency calls to the PSAP or the ECC.
- The bot also provides you the option of recording a test message and having it played back.

The experience when a Teams Direct Routing user calls “933” varies based on which ERSP handles the call. Generally, similar information should be provided by these systems.

Calling the “933” test number will provide the following Dynamic 911 testing results:

1. For Calling Plan and Operator Connect users signed in from a Corporate Network:
 - a. Does the call make it to the Teams Service bot?
 - b. Is the user in “live” mode?
 - c. Is the user’s phone number read back correctly?
 - d. Is the user’s current address read back correctly? The bot did not read back the specific location.
 - e. Will the call be routed to the PSAP? It should be for network connected users
2. For Calling Plan and Operator Connect Work from home users:
 - a. Does the call make it to the Teams Service bot?
 - b. Is the user in “live” mode?
 - c. Is the user’s phone number read back correctly?
 - d. Is the user’s current address read back correctly? The bot did not read back the specific location
 - e. Based on the information in the previously mentioned Work from Home article, if the user should be routed to the PSAP, does the bot say that the location coverage will be the Public Safety Answering Point? If they should be routed to the ECC is the location coverage “Emergency Call Center”?
3. For Direct Routing users signed in from a Corporate Network:
 - a. Does the ERSP or SIP Trunk provider answer the call to the test number?
 - b. These providers may or may not provide an indicator like “live” mode. Check with your vendor. Ask them what the user experience should be when they call the test number
 - c. The information the vendors provide through their test numbers varies. Verify that the information they do provide is correct.
 - d. The test number should indicate that these calls will be routed to the PSAP if they are valid street addresses. In most cases, they should be
4. For Direct Routing Work from Home users:
 - a. Does the ERSP or SIP Trunk provider answer the call to the test number?

- b. These providers may or may not provide an indicator like “live” mode. Check with your vendor. Ask them what the user experience should be when they call the test number
- c. The information the vendors provide through their test numbers varies. Verify that the information they do provide is correct
- d. If the Teams caller shows “Location Not Detected” in their Teams client, a blank address will be sent to the ERSP or the SIP Trunk Vendor. These calls should be routed to the vendor’s Emergency Call Resource Center (ECRC) and a live agent. The vendors will look at all other calls with addresses and determine the appropriate PSAP. If a PSAP cannot be determined, the call should be routed to the vendor’s ECRC. The test bot may or may not provide this information. Verify whatever is provided

Making 911 Test Calls

How do you know that when one of your users makes a real 911 call that it will work without testing it? The information above can only be used to verify the calling number and address that will be sent by Teams when a user makes a 911 call. It can also indicate if a call will be routed to a Public Safety Answering Point, EMC\ECRC. It cannot guarantee:

- That a call to 911 will complete
- That the call will go to a PSAP when it should
- That the call will go to the correct PSAP based on the address
- That the PSAP agent will see the caller’s correct phone number and address
- That the call will go to the EMC\ECRC when it should
- That the EMC\ECRC agent will route the call to the correct PSAP based on the address verified by the caller
- That the PSAP agent will see the caller’s correct phone number and address that they verified with the EMC\ECRC agent

The only way to verify this is to make 911 test calls. The 911 system does not like to be bogged down with test calls. 911 calls should only be used for real emergencies. However, for the health and safety of their employees and to avert potential litigation, Companies should periodically place 911 test calls.

Schedule a Test Call with the Local PSAP

Many jurisdictions require the scheduling of 911 test calls to not overburden the dispatchers. Unscheduled calls can sometimes result in a fine.

According to the [911.gov](https://www.911.gov) website, you should contact the local PSAP before making a test call. You will need to determine the appropriate PSAP for the location information that you expect to be used during the call. PSAPs are usually run by local Counties or City Governments. You will need to find the non-emergency number for the PSAP to schedule the test call.

For example, under Settings->Calls in the Teams client you see this information for the test user's Emergency location:

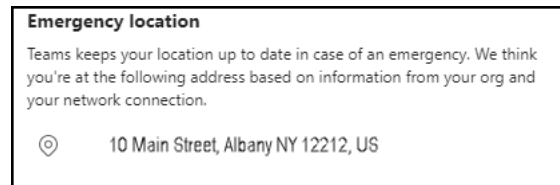


Figure 31 Emergency Location

1. Determine in what County Albany, NY is in. Albany, NY is in Albany County.
2. Search on the Internet for "Albany County, NY Emergency Services".
3. Locate the "Non-Emergency" phone number:

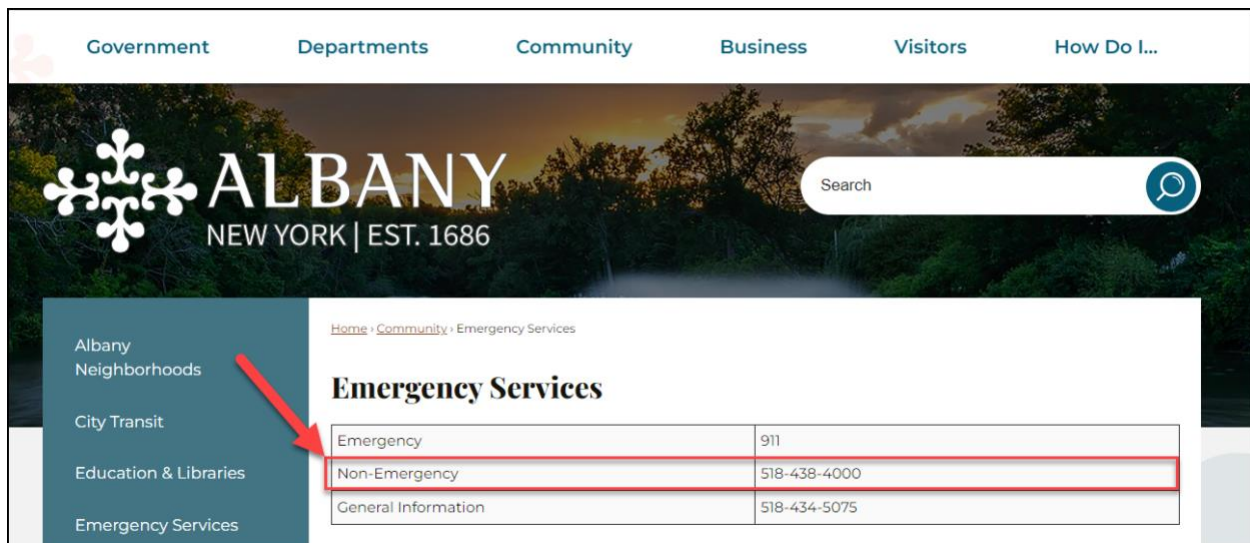


Figure 32 Emergency Services information for Albany County, NY

4. Dial the number and ask to schedule a 911 test call. If the person you are speaking to can't schedule the call, they should be able to refer you to the correct party.

The 911.gov site optionally suggests contacting the State directly to get the state’s procedures for making test calls as well as a contact directory for the PSAPs in the state. Through the “[State 911 Contacts](#)” page on the National Association of State 911 Administrators (NASNA) you can use the form to get the contact information for your State’s 911 administrator:

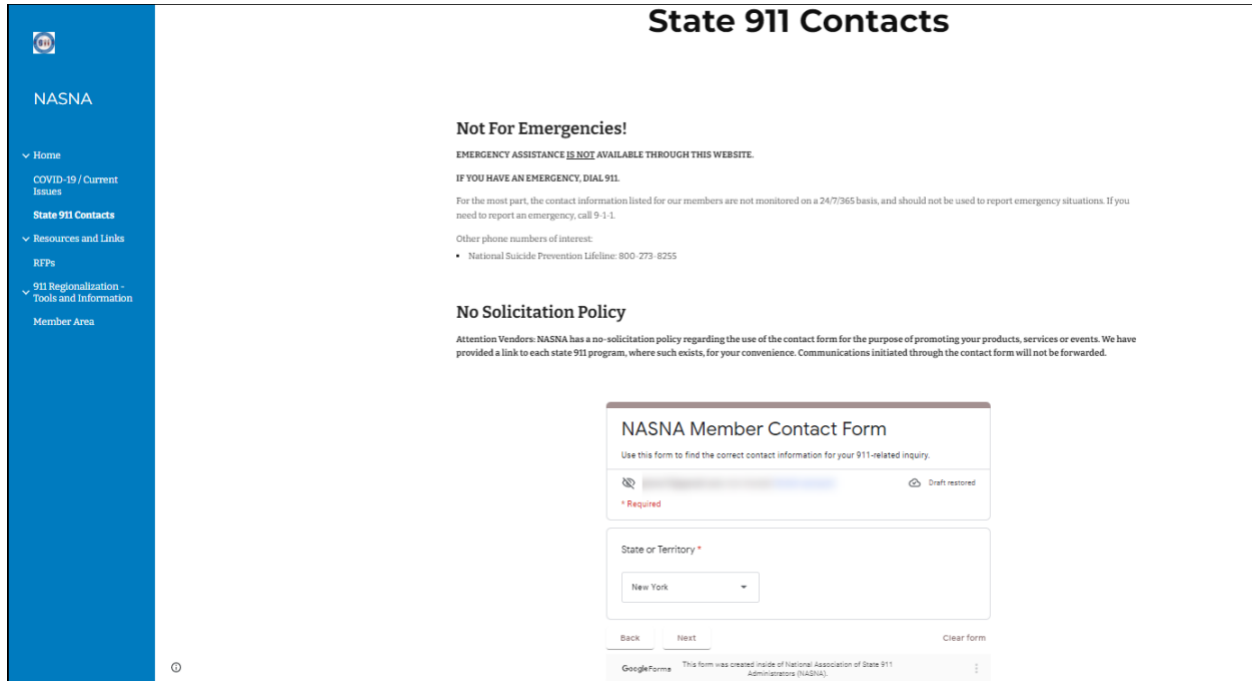


Figure 33 State Level 911 Administrator Contact Information Lookup

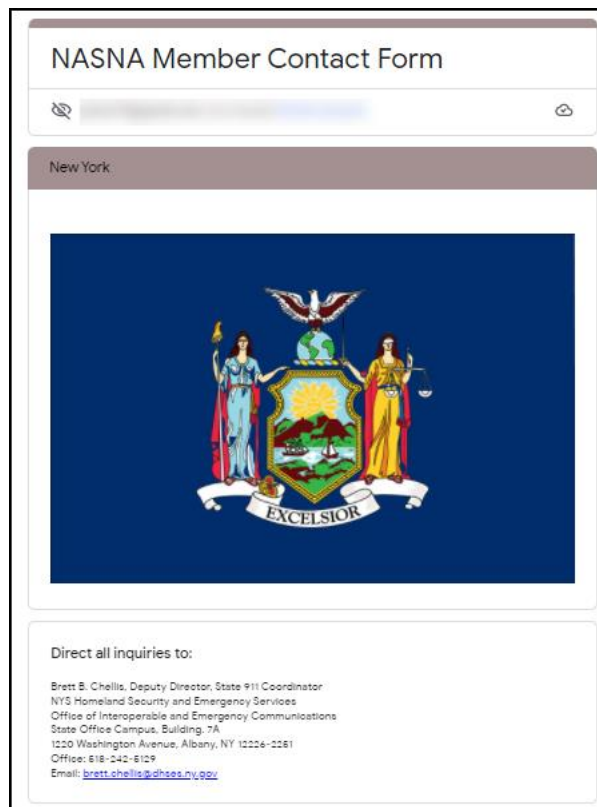


Figure 34 NY State 911 Administrator Contact Information

Several States including [Oregon](#), [Pennsylvania](#) and [Tennessee](#) have published their PSAP directories to the Internet. You can also do an Internet search to see if your state's directory is available.

Recording the Test Call

Recording your test call serves a few purposes:

- You will have a record of the conversation including the PSAP agent's readback of the calling number and the provided address. Don't waste the agent's time by trying to write down this information while on the call.
- The County or City may fine you for making the test call. The recording may help if you end up contesting the fine with the jurisdiction.

One of the simplest ways to record the call is to use a speakerphone and a voice recorder. If you don't have a voice recorder, most cellular phones have a voice recorder application.

General Recommendations

- Do not waste the PSAP's agent's time!
 - Don't chitchat.
 - Good manners (please and thank you) waste time.
 - Don't even say "Hi, how are you today".
- Do not hang up when making the call!

- Find a quiet place to make the call from. Close the office door! Focus on the call.
- Avoid making these calls during the 911 system's busy hours:
 - 6:00 – 9:00 AM.
 - Lunch Time.
 - 4:00 – 7:00 PM.
- Tuesdays through Thursdays are usually the best time.
- You should try to make at least two (2) test calls, one that should go to the PSAP and one that should go to the EMC or ECRC.

Preparation

- Schedule the test call(s) with the appropriate PSAP.
 - Gather:
 - The Calling Number.
 - The location that the Teams client will send to the Teams Service or Direct Routing Session Border Controller (SBC).
 - Determine whether the call should be routed directly to the PSAP or to the EMC\ECRC.
 - The name of the County where the expected location is located.
 - For Direct Routing users:
 - Determine the Teams Emergency Call Routing policy applied to the user making the test call. Determine from the policy which SBC the call should go through.
 - Prepare to capture the call on the SBC's logging system.
 - Create a table to document the test calls and their results
 - Get ready to record the call. You want to spend as little time as possible on the call with the PSAP agent.
 - Prepare your "script".
 - Here is the "script" I've used for several years. It is short and gets to the point:
"This is not an emergency call. <<pause>>

I am a telephony engineer, and I am testing our ability to make 911 calls. Can you please read back my calling number and the address that you see for this call?"
 - Find a quiet place to make the call from. Close the office door! Focus on the call.

Performing the Test

1. If you use Direct Routing, start the SBC logging.
2. Start your call recording.
3. Dial 911.
4. Use your script during the call.
5. Once completed, stop the recording and the logging.
6. Document the results.

Results Analysis

Document and retain the results of the test calls. You may need this information later!

For the test call, verify that:

- The call reached the Public Safety Answering Point (PSAP).
- The call reached the correct PSAP.
- The PSAP agent read back the caller's correct phone number.
- The PSAP agent read back the caller's correct location.

If any of these criteria failed for a Calling Plan or Operator Connect user, open a ticket with Microsoft support.

For Direct Routing users:

- If the call did not complete:
 - Check the log on the SBC for the call.
 - If the call does not appear in the SBC log, in Microsoft Teams check:
 - The applicable Teams Emergency Call Routing policy.
 - The PSTN usage defined in the policy.
 - The route(s) assigned to the PSTN usage.
 - If Teams shows any problems or errors with the SBC.
 - If the call does appear, verify that it was correctly routed to the ERSP or SIP Trunk vendor.
 - If it was routed correctly, open a support ticket with the ERSP or SIP Trunk vendor.
 - If the call did not reach the correct PSAP.
 - Find the call in the SBC log.
 - Check the location information in the Session Description Protocol (SDP) section of the SIP INVITE for the call. Verify that it matches what Teams said it would send to the SBC
 - If it matches, open a support ticket with the ERSP or SIP Trunk vendor.
 - If it doesn't match, open a Microsoft support ticket.
 - If the PSAP agent does not read back the correct number of the caller.
 - Find the call in the SBC log.
 - Check the value in the "From" field in the header section of the SIP INVITE for the call coming from Teams. Also verify the value in the SIP INVITE going to the ERSP or SIP Trunk Vendor.
 - If the value is wrong in the INVITE coming from Teams, open a support ticket with Microsoft Support. This issue would have likely surfaced when making a "933" test call.
 - If the value is wrong in the INVITE going to the ERSP or SIP Trunk vendor and the value in the Teams INVITE is correct, the problem is on the SBC itself.
 - If the value in both INVITES is correct, open a ticket with the ERSP or SIP Trunk vendor.
 - If the PSAP agent does not read back the correct address information for a call that went directly to the PSAP.
 - Find the call in the SBC log.

- Check the location information in the SIP INVITE for the call. Verify that it matches what Teams says it would send to the SBC .
- If it matches, open a support ticket with the ERSP or SIP Trunk vendor.
- If the PSAP agent does not read back the correct address information for a call that went to the ECRC before going to the PSAP.
 - Review the call recording and verify that the ECRC agent read back the address provided by the caller correctly.
 - If the read back is correct, open a support ticket with the ERSP or SIP Trunk vendor.

Summary

- The installation of Teams Dynamic 911 and the Work from Home feature cannot be fully validated without making actual 911 test calls.
- The “933” or other emergency test numbers are no guarantee that when a real Teams Dynamic 911 call is made it will:
 - Reach a Public Safety Answering Point (PSAP).
 - Be routed to the correct PSAP based on the caller’s location.
 - Be delivered to the PSAP with the caller’s correct phone number.
 - Be sent to the PSAP with the caller’s correct location.
- Any of these issues will result in delays in getting the first responders to a 911 caller. The ramifications of this could be severe for the caller and the company.
- All things equal, failed 911 test calls are more likely for Direct Routing users than Calling Plan or Operator Connect users. Direct Routing has a few more moving parts when handling Dynamic 911 calls. Once the call is routed from Microsoft Teams to the SBC, the success of the call is dependent on the correct configuration of the SBC and the deployment and integration of the ERSP or the SIP Trunk vendor. Even if the SBC provides the correct calling number and user location, there could still be issues with the ERSP or SIP Trunk vendor routing the call to the correct PSAP.
- Most PSAPs allow 911 test calls but require that they be scheduled ahead of time. Contact the appropriate PSAP on their non-emergency number to find out how to schedule these calls.
- Keep the calls brief, to the point and clear that they are not actual emergency calls.
- Record the test calls.
- Make test calls that should go directly to the PSAP and calls that should first be routed to the EMC\ECRC. Make sure that calls that go through the EMC\ECRC are routed to the appropriate PSAP.
- Enabling Technologies is available and ready to answer any Microsoft Teams and Teams Dynamic 911 questions that you might have. Please contact us at contact@enablingtechcorp.com

Chapter 7 Teams Troubleshooting

Introduction

Let's review why we need to set up Teams Dynamic 911 and Work from Home, it is not to comply with Kari's Law and the RAY BAUM Act. The reason we are going through all this effort is to provide for the health and safety of the organization's most important asset, its personnel. The Federal, State and Local laws provide the requirements for:

- How 911 calls should be dialed.
- Notification of the appropriate organizational personnel who can provide access and escort for the first responders.
- Automatically providing a caller's accurate current location. By providing an accurate current location the components of Teams Dynamic 911 and the other dependent players can automatically route an emergency call to the correct PSAP based on the caller's current location in most cases.

The Teams Dynamic 911 solution requires the proper configuration and functioning of:

- Teams Calling Plan Users.
 - Microsoft Teams Dynamic 911 and Work from Home.
 - Microsoft acting as the ERSP and provider of the ECC.
- Team Operator Connect Users.
 - Microsoft Teams Dynamic 911 and Work from Home.
 - The Operator Connect vendor acting as the ERSP and provider the ECC.
- Teams Direct Routing Users.
 - Microsoft Teams Dynamic 911 and Work from Home.
 - The organization's Direct Routing SBCs.
 - The ERSP and their ECRC. This could be a 3rd party provider, or it could be a SIP Trunk provider.

The organization's users are the front-line of Teams Dynamic 911 troubleshooting. They must be trained in the proper use of Teams Dynamic 911. This boils down to the requirement that they verify the accuracy of their current location in the Microsoft Teams client. On-premises users must advise the support desk when they see a missing or inaccurate location in their Teams client. Work from Home users must let the service desk know if they don't see any location information at all! The users need to do this when they start up the Teams client or when they change the network the running device is on. On-premises users cannot correct an incorrect or missing location. The support desk and Teams administrators need to be able to diagnose the cause of a bad location for on-premises users quickly and to provide remediation as soon as possible. The onus of having a correct current location for Work from Home users is squarely with the user.

Except for the Emergency Call Routing Policy, the Teams side configuration and troubleshooting for Calling Plan, Operator Connect and Direct Routing users is identical. There is no explicit additional Dynamic 911 configuration required for Calling Plan and Operator Connect users. Teams Dynamic 911 is automatically enabled for all these users. Direct Routing users require the configuration of Teams Emergency Call Routing Policies, their Direct Routing SBCs and an interface to a 3rd Party ERSP or SIP Trunk vendor who can provide the functionality. Some ERSPs or SIP Trunk vendors require that the client enable the user's phone numbers for

Dynamic 911. In most cases the client needs to provide a “default” location for the phone number while it is being enabled.

Microsoft, the Operator Connect vendors and the Direct Routing ERSPs will route emergency services calls based on the information passed to them by Teams. They route emergency calls based on the presumption that what is being passed to them accurately reflects the caller’s current location.

Prevention

The best way to prevent problems with the accurate delivery of emergency services calls is to be proactive. Technology failures can range from being an inconvenience to taking a tangible financial toll on an organization. A failure in correctly and efficiently routing an emergency services call can be a life and death problem. We should always try to prevent technology problems. In the case of Dynamic 911 we must try harder! As Gene Krantz of NASA famously said during the Apollo 13 accident, “Failure is not an option!”³

For on-premises users we need to ensure that:

1. Teams Dynamic 911 is enabled for all Teams voice enabled users.
2. Teams users always get an accurate current location when they start up their Teams client.
3. Based on their on-premises location, the correct Emergency Calling Policy is being dynamically applied to the user’s Teams session.
4. The list of notifyees is up to date.
5. The notifyees know what to do on receipt of a notification.
6. Emergency calls get ultimately routed by Teams and the ERSPs to the appropriate PSAP.
7. For Direct Routing users:
 - a. Verify that all Teams numbers have been enabled for Dynamic 911 with the ERSP vendor.
 - b. Ensure that SBC based Caller ID overrides are not applied for emergency services calls. Teams automatically takes care of this for overrides applied through the Teams Calling Line identity policy.

For Work from Home users, we need to ensure that:

1. Teams Dynamic 911 is enabled for all Teams voice enabled users.
2. If their location is “Location is not Detected”, they can add their current address.
3. They can confirm or edit a suggested location.
4. The Global (org-wide default) Emergency Calling Policy is applied to their current session.
5. Emergency calls get ultimately routed by Teams and the ERSPs to the appropriate PSAP.
6. For Direct Routing users,
 - a. Verify that all Teams numbers have been enabled for Dynamic 911 with the ERSP vendor.

³ https://en.wikipedia.org/wiki/Failure_Is_Not_an_Option

- b. Ensure that SBC based Caller ID overrides are not applied for emergency services calls. Teams automatically takes care of this for overrides applied through the Teams Calling Line Identity policy.

Teams Client Troubleshooting

There are three (3) primary tools available for troubleshooting the current location in the Teams client:

1. The Teams Desktop Client
2. 933 Test Number.
3. CALLING-DEBUG.TXT debug log file.

Teams Desktop Client

The Teams Desktop client has information that can help troubleshoot the display of an accurate current location. The current Dynamic 911 location can be found in the Teams Desktop client by clicking on the “Calls” tab:

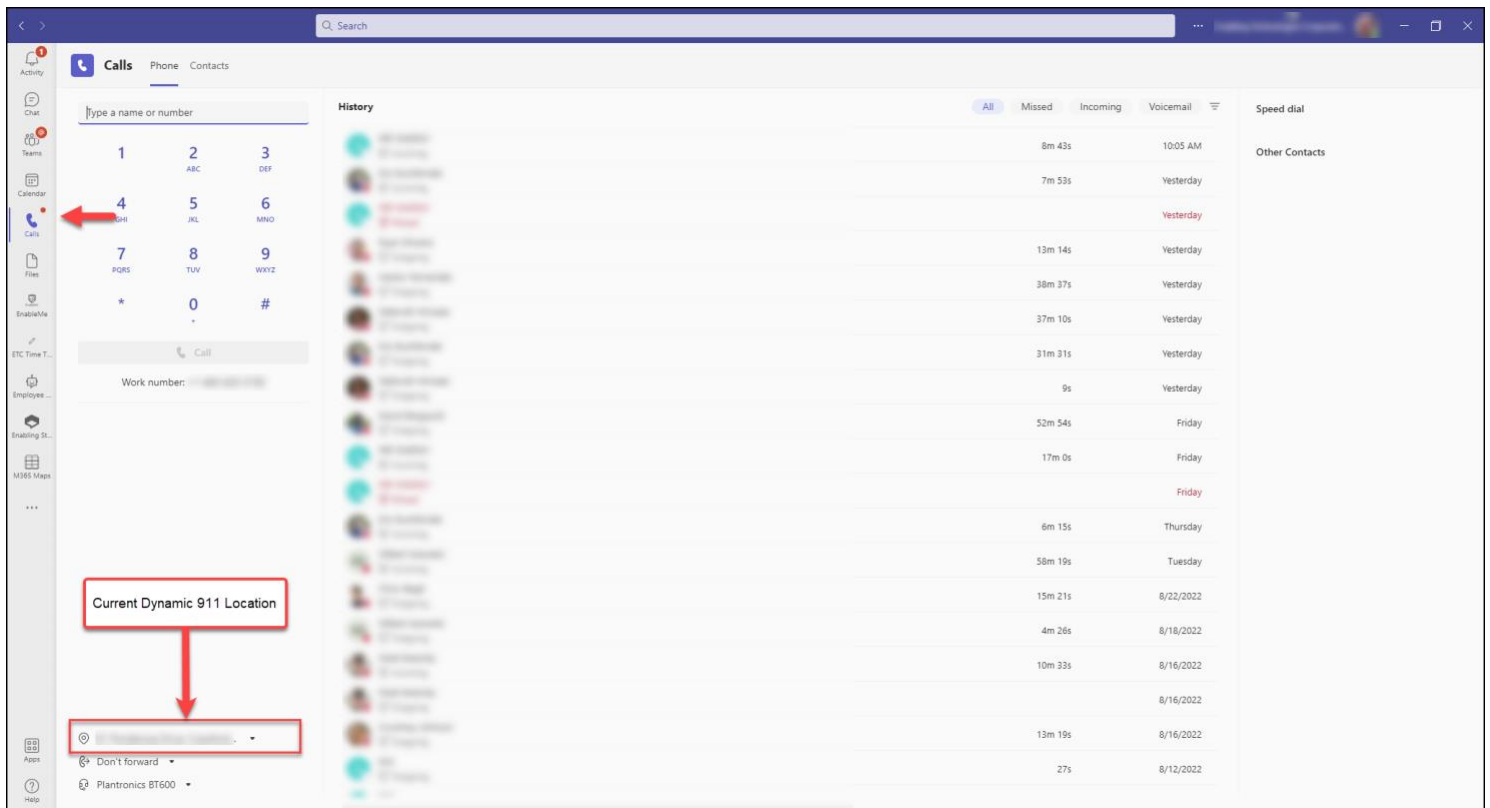


Figure 35 Current Dynamic 911 Location in the Teams Client

You should be able to see all the information when you hover over the location including the precise location in the building. There should be a precise location, such as “Floor 1”, “Office 306”, etc. for on-premises users. A specific location may not be there for Work from Home users, they can add one at their discretion:

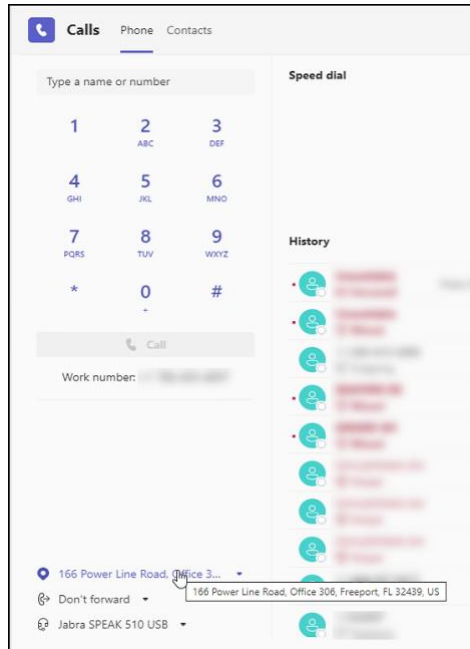


Figure 36 Hovering over the Current Location

There is a drop-down arrow next to the current location in the Teams Desktop client. The available options on the drop-down menu can be used to verify that the location being presented accurate and is that of an on-premises user. The options can also indicate if a Work from Home user has confirmed or edited a suggested current location.

For an on-premises user:

1. The displayed address should be correct.
2. There should be a correct specific location within the address.
3. The drop-down options should display "Work Location" greyed out.

For a Work from Home user who has confirmed or edited the suggested location:

1. The displayed address should be correct.
2. There may be a specific location with the address.
3. The drop-down options should display "Edit" or "Reset".

For both types of users, any other combination of location accuracy and drop-down options would be incorrect.

The following table provides a list of the combinations of the current location and drop-down options for an on-premises user that you might see. There is only one combination where the Teams current location would be accurate. The rest of the scenarios represent the cases where the Teams client would be presenting incorrect information.

The Teams client will present the ERSP with the derived information whether it is correct or not. Incorrect information will ultimately result in a failed emergency services call. Yes, calls with incorrect information should ultimately be routed to the correct PSAP. However, they will first have to be handled by the ERSP's ECC or

ECRC. Again, calls from on-premises users should always have a correct address and location and will always be routed directly to the correct PSAP. Later, we will look at this table again mapping the observations to information we can glean from the calling-debug.txt debug log file to provide a root cause for the results.

Observations in the Teams Client	Current Location Correct?	Drop-Down Location Options	Is the Teams current location information correct?	Call Routing	Successful 911 call?
The current location, including the specific place is correct. The drop-down option is "Work Location".	Yes	Work Location (Greyed Out)	Yes	Directly to the PSAP.	Yes
The current location or the place are incorrect and the drop-down option is "Work Location".	No	Work Location (Greyed Out)	No	Directly to the PSAP.	No
The current address is correct but the place is missing and the drop-down option is "Location not Editable".	Yes	Location not Editable (Greyed Out)	No	To the ECC/ECRC before routing to the PSAP.	No
The current address is incorrect, the place is missing and the drop-down option is "Location not Editable".	No	Location not Editable (Greyed Out)	No	To the ECC/ECRC before routing to the PSAP.	No
The current address is correct but the place is missing and the drop-down option is "Verify".	Yes	Verify	No	To the ECC/ECRC before routing to the PSAP.	No
The current address is incorrect and the place is missing. The drop-down option is "Verify".	No	Verify	No	To the ECC/ECRC before routing to the PSAP.	No
There is no current location displayed at all.			No	To the ECC/ECRC before routing to the PSAP.	No

Figure 37 Troubleshooting the Current Location and Drop-Down Options of an on-premises user

The accuracy of the current location of a Work from Home user depends on the user confirming or correcting the address suggested by the Teams client. Calls from confirmed addresses will always be routed directly to the PSAP. Failure to take any action will always result in the routing of 911 calls to the ECC or ECRC.

Observations in the Teams Client and user action	Current Location Correct?	Drop-Down Location Options	User Action Taken	Call Routing	Successful 911 call?
The Teams client suggested a correct location. The user verified the location.	Yes	Verify	User verified the location.	Directly to the PSAP.	Yes
The Teams client suggested a correct location. The user did nothing.	Yes	Verify	Did Nothing	To the ECC/ECRC before routing to the PSAP.	No
The Teams client suggested an incorrect address. The user corrected the address.	No	Verify	User verified the location.	To the ECC/ECRC before routing to the PSAP.	Yes
The Teams client suggested an incorrect address. The user did not correct the address.	No	Verify	Did Nothing	To the ECC/ECRC before routing to the PSAP.	No
The Teams client could not suggest an address. The user added the correct address.	Location not Detected	Verify	User added the location.	To the ECC/ECRC before routing to the PSAP.	Yes
The Teams client could not suggest an address. The user did not add a correct address.	Location not Detected	Verify	Did Nothing	To the ECC/ECRC before routing to the PSAP.	No
There is no current location displayed at all.				To the ECC/ECRC before routing to the PSAP.	No

Figure 38 Troubleshooting the Current Location and Drop-Down Options of a Work from Home User

Troubleshooting

1. The current location line is missing. The user is not enabled for Teams Dynamic 911.

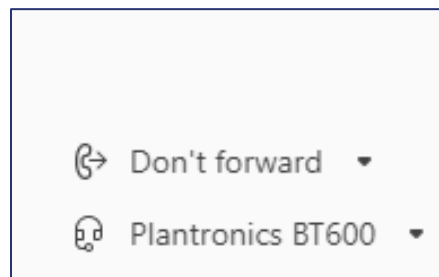


Figure 39 Current Dynamic 911 Location Missing

Resolution:

- Contact Microsoft Technical Support for Calling Plan users.
- Contact the vendor for Operator Connect Users.
- Check that the “Dynamic emergency calling switch” in the “Emergency Call Routing Policy” assigned to the user is turned on. This can be determined from the calling-debug.txt log file.

2. The Location is wrong for an on-premises user. Teams Dynamic 911 is not configured correctly.

Resolution:

- Retrieve and review the information in the calling-debug.txt file described below.
3. The Location is wrong for a Work from Home user, or the drop-down option is, "Location not Detected".

Resolution:

- The user should add or correct the location.
4. An on-premises user sees any drop-down options other than "Work Location".

Resolution:

- Retrieve and review the information in the calling-debug.txt file described below.
5. A Work from Home user sees "Location not Detected"

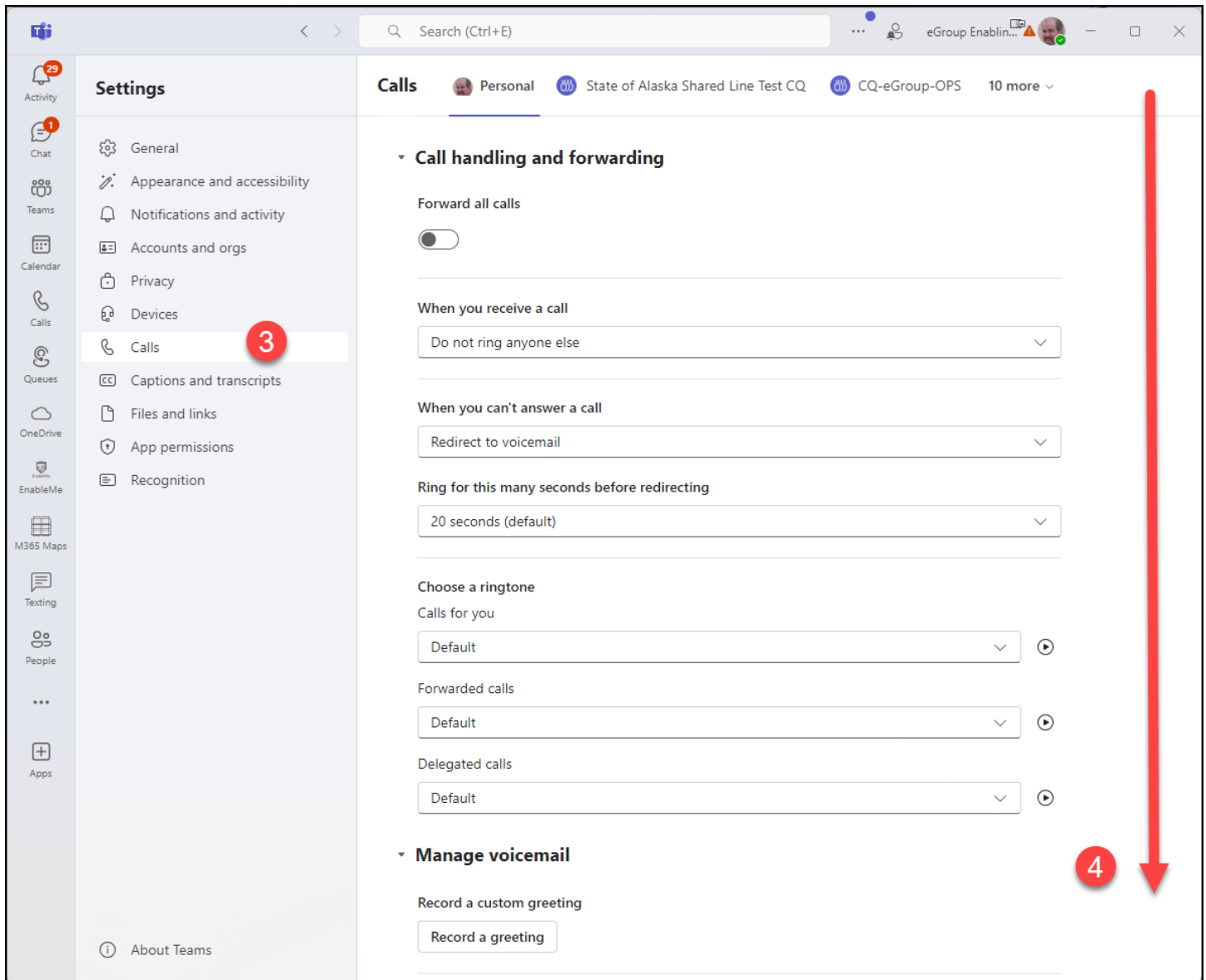
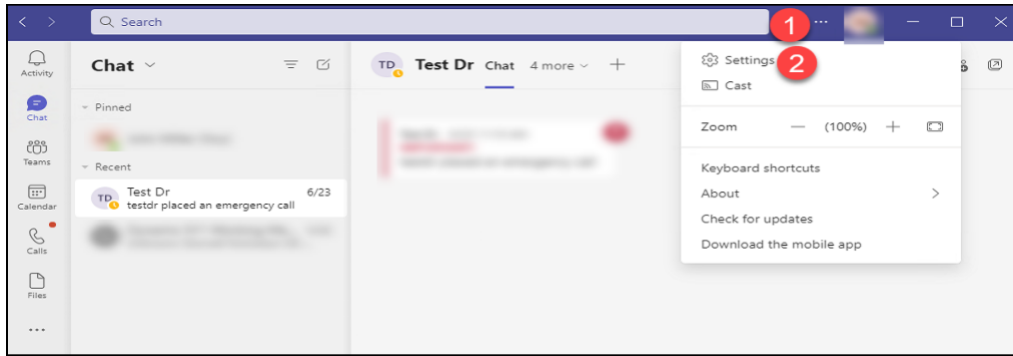
Resolution:

- This is not a problem if the organization has created Group, Intune or similar policies that block the enablement of Location Services on the organization's Windows and Mac devices. This is the expected result for this configuration.
- This is a problem if the organization has created Group, Microsoft Intune or similar policies to enable Location Services for the organization's Windows and Mac devices. Troubleshoot why the policy is not being applied or effective on the user's device.
- It may also be a problem if the organization has provided instructions to the user's on how to enable Location Services. Review the local settings on the user's device. If they are correct the issue may be that the device cannot ascertain its current latitude and longitude, or the Teams service cannot derive an address for the provided coordinates.

Emergency Location Information in the Settings->Calls Menu

The current Emergency Location can also be found by:

1. Clicking the three (3) dots next to the user's icon in the Teams client.
2. Clicking on "Settings".
3. Clicking on "Calls".
4. Scrolling to the bottom of the "Calls" information and looking for the "Emergency Location" section.



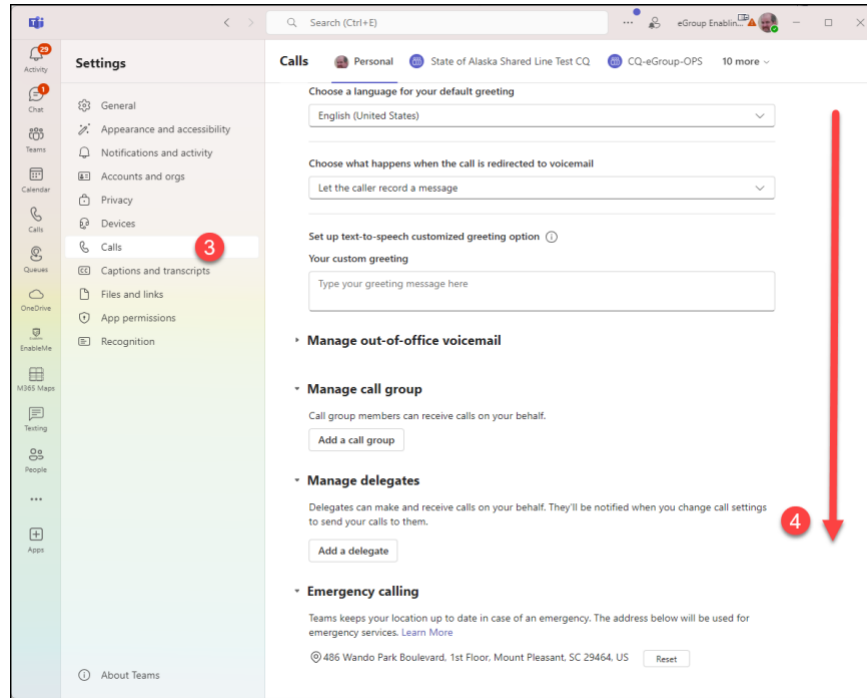


Figure 40 Accessing the Emergency location under Settings in the Teams Client

There should be an “Emergency location” section. The location should match that seen on the “Calls” tab of the Teams client.

933 Test Number

933 is the 911 test number provided by Microsoft. The Operator Connect vendors should support 933. Most of the Direct Routing ERSPs and SIP Trunks with ERSP support also support 933 but to varying degrees. When a Calling Plan, Operator Connect or Direct Routing user dials 933 from the Teams Desktop client, they should see a screen that looks like the one below:

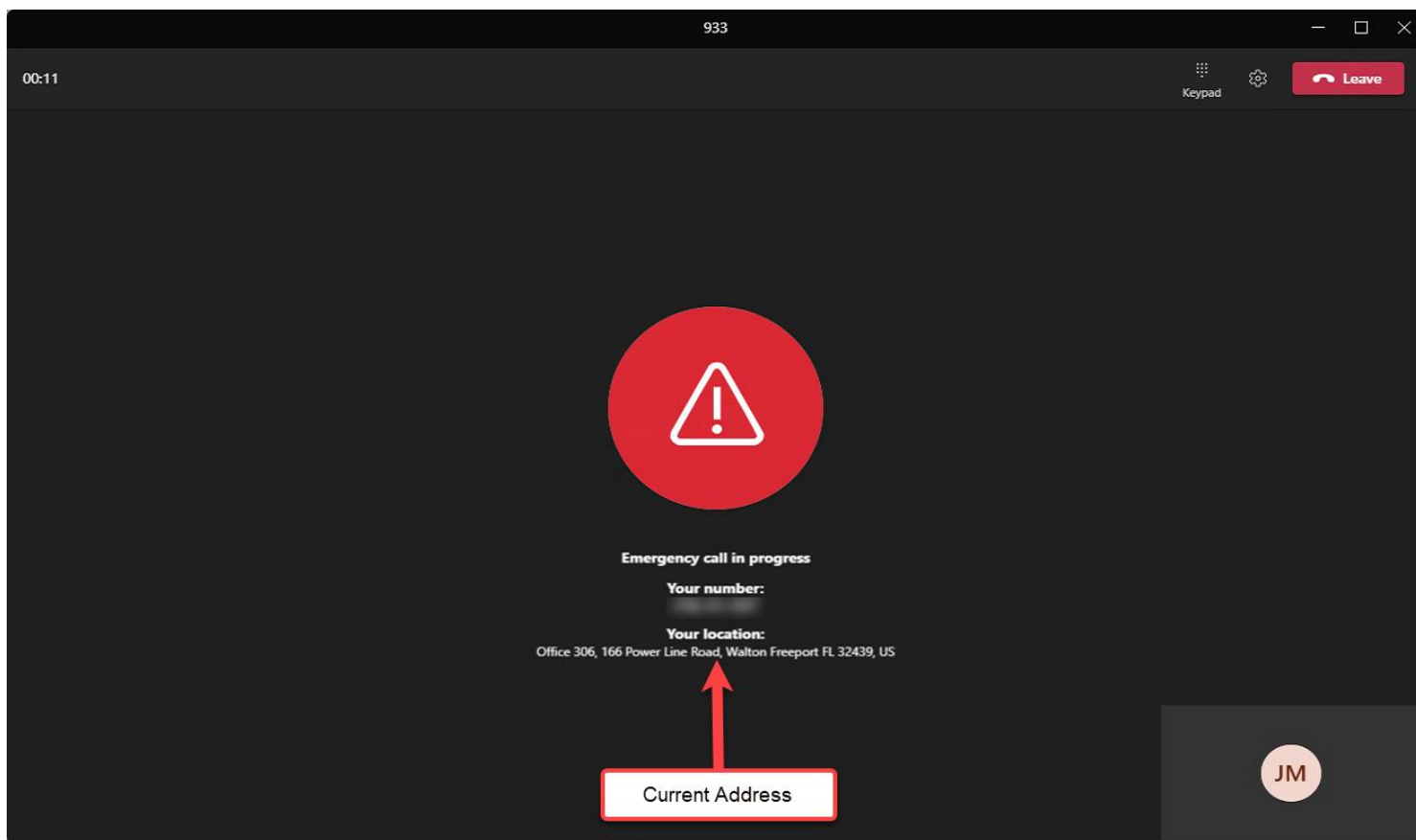


Figure 41 Teams Call Window when dialing 933

Once connected, the caller should hear a “bot” playing back information about the call. The information provided to Calling Plan users includes:

- A statement that you have reached the “911 Test System”.
- That your account is in “Live Mode”
- Your “Subscription Identifier”. The bot should correctly read back your ten (10) digit phone number as displayed in the Teams client.
- The fact that an address had been provided.
- That the latitude and longitude have been provided.
- That your location coverage will be “Public Safety Answering Point” or “Emergency Call Center”. This is dependent on whether the location is validated and verified. This is covered elsewhere
- The address, including the County will be read back to you.
- You will be given the option to record a short message and have it played back to you.

The bot’s for Operator Connect and Direct Routing users should provide similar information.

The 933 number, other than dialing 911, is the only way to verify that the notifications setup in the Teams Emergency Calling policies are working correctly. Dialing 933 in the Teams client will trigger the [notification of organizational personnel](#) that an emergency services call has been made. The notified personnel are determined by the Teams Emergency Calling policy applied to the user’s current Teams session. For on-

premises users, the notified personnel should be personnel assigned to the building from where the caller dialed 933. No notification will usually be sent when a Work from Home user dials 933 or 911.

Troubleshooting

1. The 933 bot does not answer.

Resolution:

- Contact Microsoft Technical Support for Calling Plan users.
- Contact the vendor for Operator Connect Users.
- For Direct Routing users:
 - Check the Emergency Call Routing Policy applied to the user.
 - The effective policy can be found in the “calling-debug.txt” or Teams Admin Center.
 - Make sure there is a Dial Mask\Dial String entry for 933.
 - Check the applied PSTN Usage and underlying routes.
 - Check the status of the Direct Routing SBC referenced in the route(s).
 - Check the SBC (These notes are applicable to AudioCodes SBCs. Adapt them as necessary to other manufacturers products).
 - Check the SBC Call Detail Record (CDR) History for the call: Monitor menu->Monitor tab->VoIP Status folder->SBC CDR History.
 - Repeat the call while capturing a Syslog. Check the Syslog.
 - Verify that the call was delivered to the SBC by Teams.
 - Check that the destination number is “933”.
 - Verify that the call was routed to the ERSP or the appropriate SIP Trunk.
 - Open a support ticket with the ERSP or SIP Trunk vendor.

2. The read back for a Calling Plan user indicates that they are not in “Live Mode”.

Resolution:

- Contact Microsoft Technical Support

3. The information in the display and/or read back is incorrect.

Resolution:

- Contact Microsoft Technical Support for Calling Plan users.
- Contact the vendor for Operator Connect Users.
- For Direct Routing users:
 - Check the SBC (These notes are applicable to AudioCodes SBCs. Adapt them as necessary to other manufacturers products).
 - Repeat the call while capturing a Syslog. Check the Syslog.
 - The phone number in the “FROM” field in the SIP header should be the caller’s number.

- The 'PRIORITY' field in the SIP header should say "emergency".
 - [Review the information in the PIDF-LO section](#) of the SDP for the call leg coming from Teams to the SBC. Verify that it is correct.
 - The address information should match the Teams current location.
 - The "method" field should be:
 - "LIS" for an on-premises location.
 - "ASSIST" for a Work from Home confirmed location.
 - "MANUAL" for an edited Work from Home location.
 - "CLS" for a Work from Home location that was neither confirmed nor edited.
 - Review the information in the PIDF-LO section of the SDP for the call leg leaving the SBC and going to the ERSP or SIP Trunk vendor. It should match the information from the inbound leg of the call. Verify that it is correct.
 - Open a support ticket with the ERSP or SIP Trunk vendor.
4. The readback of the "Location Coverage" is incorrect. It is read back as "Emergency Call Center" when it should be "Public Safety Answering Point" or vice-versa.

Resolution:

- Contact Microsoft Technical Support for Calling Plan users.
- Contact the vendor for Operator Connect Users.
- For Direct Routing users:
 - Check the SBC.
 - Repeat the call while capturing a Syslog. Check the Syslog.
 - Review the information in the PIDF-LO section of the SDP for the call leg coming from Teams to the SBC. Verify that it is correct.
 - The "method" field should be:
 - "LIS" for an on-premises location.
 - "ASSIST" for a Work from Home confirmed location.
 - "MANUAL" for an edited Work from Home location.
 - "CLS" for a Work from Home location that was neither confirmed nor edited
 - If the "method" is wrong, contact Microsoft or the Operator Connect vendor's support as appropriate.
 - If it is correct, contact the ERSP or SIP Trunk vendor's support.

calling-debug.txt Debug Log File

The “calling-debug.txt” file is one of the Teams debug log files. This file contains the information the Teams client uses about the current device to determine the current location of the device and the appropriate Emergency Calling and Emergency Call Routing policies to be applied to the current session. The file also includes a value for the “type” and “method” elements. These are used to indicate to Microsoft, the Operator Connect vendor or the ERSP whether the call should be routed directly to the PSAP or the ECC\ECRC. The “calling-debug.txt” is the primary troubleshooting tool to resolve these issues:

- The user does not see any location information on the “Calls” tab of the Teams client.
- The current location for an on-premises user is incorrect.
- An on-premises user has a Work from Home location.
- Emergency Calls from on-premises users are routed to the ECC\ECRC and not directly to the correct PSAP.
- The incorrect Emergency Calling Policy is used when an on-premises user makes an emergency call.
- It can also be used to troubleshoot location problems for Work from Home users.

These log files can be generated when needed from Teams Windows and Mac desktop clients

- Windows Clients
 1. Open the System Tray on the Windows Desktop.
 2. Right Click on the Teams icon.
 3. Click on “Collect Support Files”.
 4. When finished, a “File Explorer” window will open pointing at a directory named “MSTeams Support Logs”. The date and time the logs were collected is appended to the directory name. There will also be a ZIP file named “PROD-WebLogs” with the date and time appended. Double click on the ZIP file to open it.

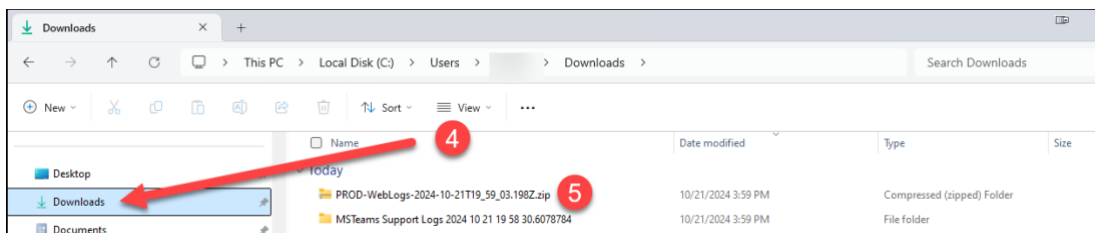
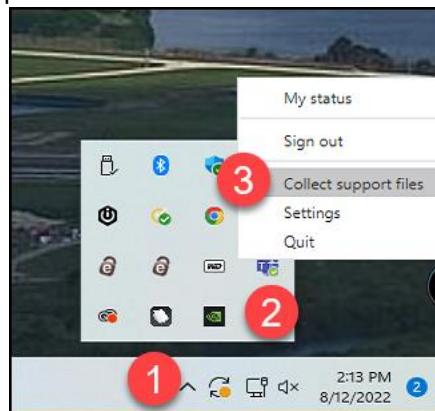


Figure 42 Creating the Teams Debug Logs

5. Double click on the folder whose name begins with "User (Primary;".
6. Locate the file named "calling-debug.txt". Open the file in "notepad.exe" or your favorite text editor.

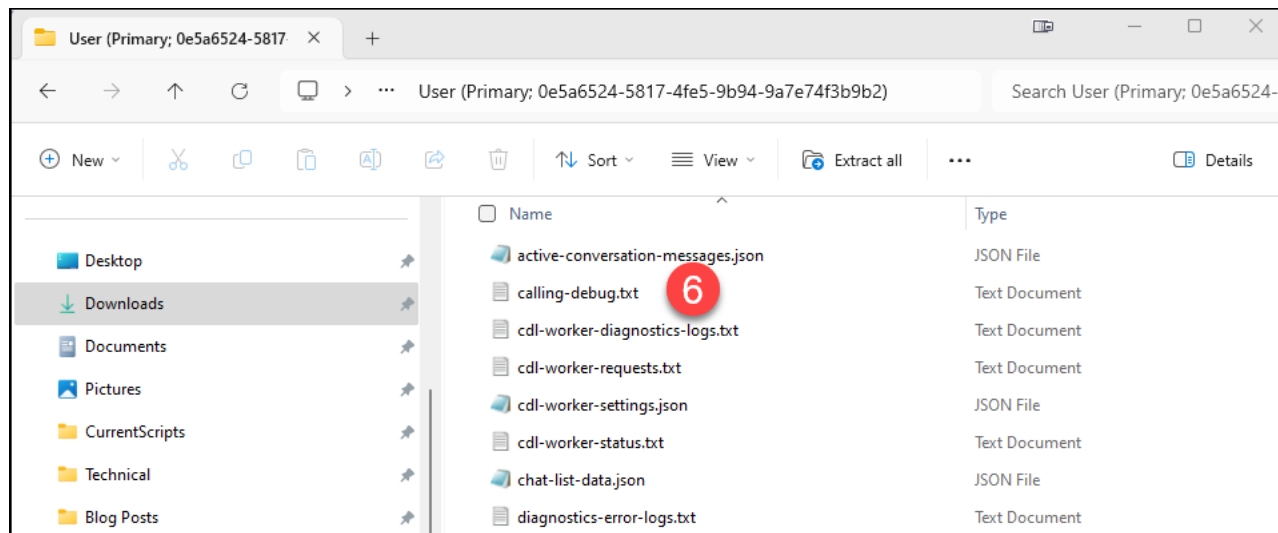


Figure 43 Locating the "calling-debug.txt" file on a Windows Desktop

- Mac Clients
 1. Press "Option" + "Command" + "Shift" + "1".
 2. The files can be found in "~/Downloads".

Troubleshooting Teams with the calling-debug.txt

Locating the Teams Dynamic 911 Information

The "calling-debug.txt" debug log can be used to troubleshoot Teams calling and Teams Dynamic 911. The Dynamic 911 debugging information is found at the end of the file.

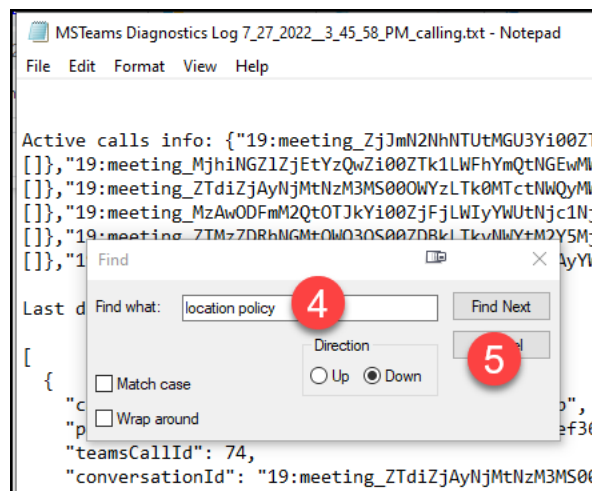
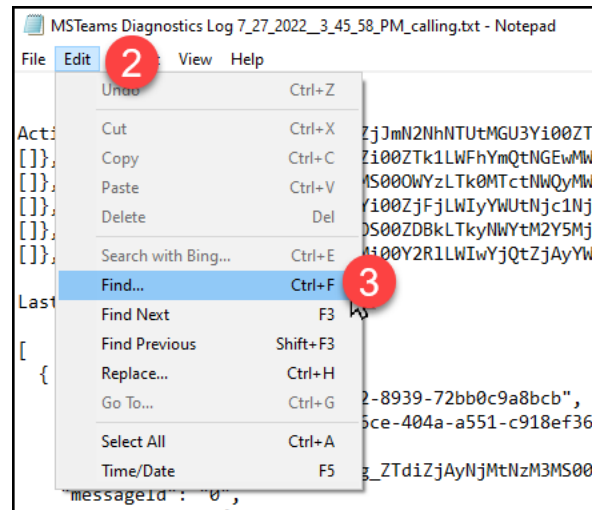
1. Open the "calling-debug.txt" in Windows Notepad. You can also use your editor of choice.
2. Click "Edit".
3. Click "Find".
4. In the "Find what:" box type "location policy".
5. Click the "Find Next" Button. Some "calling-debug.txt" files, do not have the "Location Policy" header. If it can't be found, try searching for "isCallingPlanUser" which may precede the "Location Policy" header.
6. Resize the window and use the scroll bar as needed to view the data.

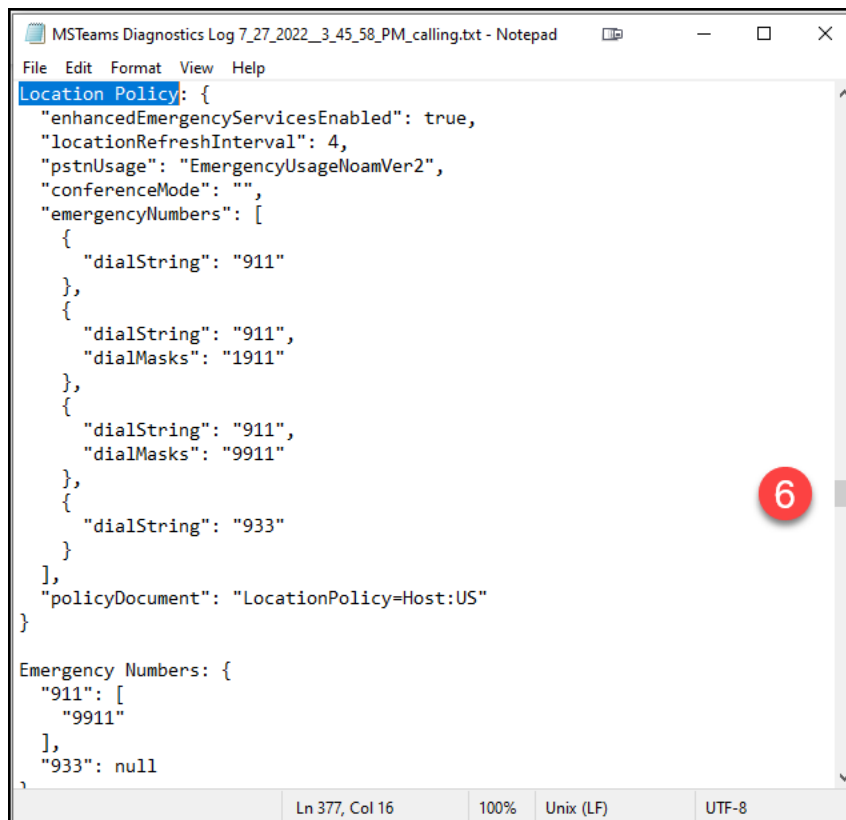


```
MSTeams Diagnostics Log 7_27_2022_3_45_58_PM_calling.txt - Notepad
File Edit Format View Help

Active calls info: {"19:meeting_ZjJmN2NhNTUtMGU3Yi00ZTAyLWJmYjctMTQzMDBiZTBjYzRi@thread.v2":{"callsMap":{},"calls":
[]},"19:meeting_MjhiNGZlZjEtYzQwZi00ZTk1LWFhYmQtNGEwMmIzOWYyY2Vm@thread.v2":{"callsMap":{},"calls":
[]},"19:meeting_ZTdiZjAyNjMtNzM3MS00WYzLTk0MTctNWQyMWQ3YT1iNDQ5@thread.v2":{"callsMap":{},"calls":
[]},"19:meeting_MzAwODFmM2Q0OTJkYi00ZjFjLWIyYWUtNjc1NjM3ZmU0NjJi@thread.v2":{"callsMap":{},"calls":
[]},"19:meeting_ZTMzZDRhNGMtOWQ3OS00ZDBkLTkyNWYtM2Y5Mjc0OTcwMmNm@thread.v2":{"callsMap":{},"calls":
[]},"19:meeting_YWE1NWFljOGYtYmU0Mi00Y2RlLWIwYjQtZjAyYWJiNWY1OTFm@thread.v2":{"callsMap":{},"calls":[]}}

Last disposed calls:
[
{
  "callId": "c5225566-78a6-4832-8939-72bb0c9a8bcb",
  "participantId": "8bcd7f91-d6ce-404a-a551-c918ef36ff8c",
  "teamsCallId": 74,
  "conversationId": "19:meeting_ZTdiZjAyNjMtNzM3MS00WYzLTk0MTctNWQyMWQ3YT1iNDQ5@thread.v2",
  "messageId": "0",
  "coordinates": {
    "type": 1,
    "joinType": 0,
    "conversationId": "19:meeting_ZTdiZjAyNjMtNzM3MS00WYzLTk0MTctNWQyMWQ3YT1iNDQ5@thread.v2"
  }
}
```





```

MSTeams Diagnostics Log 7_27_2022_3_45_58_PM_calling.txt - Notepad
File Edit Format View Help
Location Policy: {
  "enhancedEmergencyServicesEnabled": true,
  "locationRefreshInterval": 4,
  "pstnUsage": "EmergencyUsageNoamVer2",
  "conferenceMode": "",
  "emergencyNumbers": [
    {
      "dialString": "911"
    },
    {
      "dialString": "911",
      "dialMasks": "1911"
    },
    {
      "dialString": "911",
      "dialMasks": "9911"
    },
    {
      "dialString": "933"
    }
  ],
  "policyDocument": "LocationPolicy=Host:US"
}

Emergency Numbers: {
  "911": [
    "9911"
  ],
  "933": null
}
Ln 377, Col 16    100%    Unix (LF)    UTF-8

```

Figure 44 Locating the Teams Dynamic 911 Information in the "calling-debug.txt" file

File Structure

- A "calling-debug.txt" has at least three (3) separate sections:
 - Location Policy
 - Current Emergency Address
 - Current MT Location Response
- The Teams Desktop client will cache previously discovered information for network locations. These will be contained in a section named "Networks and Locations known". Each location has a "Network" and "Location" tagged sub-section. The first cached location is designated "Network 1:" and "Location 1:".
- A network location is defined as a unique combination of a Public IP and network subnet for a remote Teams user.
- The Public IP is the address provisioned, usually by the Internet Service Provider, on the internet facing side of the router or firewall that the Teams client\device is routing traffic through to reach the Microsoft Teams cloud.
- As the Teams client starts up for a Work from Home user, it checks to see if there is a cached network location with the same Public IP and subnet ID of the current session. If there is one, Teams will use that information. If not, Teams will try to derive the current location for the session based using the Work from Home feature requiring the user to confirm or edit the suggested location.
- There could be several previous cached network locations in a "calling-debug.txt" file. Teams will cache the different network locations that the device has connected to.

- When the Teams client starts up, it will look at the current Public IP and current subnet of the device. It will try to match this information to a cached location. If it gets a match, Teams will use the cached location.
- The cached locations do not really have any relevance for on-premises users. For Work from Home users, the user would not have to “Add”, “Edit” or “Confirm” a location that they have previously done so for.

Information Contained in the “calling-debug.txt”

- The example below includes sample data for an on-premises Calling Plan user configured in the fictitious commercial organization, Panhandle Consumer Industries, described later in this document.
- The layout and content of a “calling-debug.txt” is the same for a Calling Plan and Operator Connect user. Differences for Direct Routing users are noted.
- We can assume that Teams Dynamic 911 with the Work from Home feature for the fictitious organization has been correctly and completely configured in the organization’s Office 365 tenant:
 - Emergency Address records for all organizational buildings have been created.
 - All required Location\Place records have been added.
 - All Tenant Trusted IP addresses have been added.
 - Each building in the organization has been defined as a Tenant Network Site. The subnets in each building have been added to the appropriate Tenant Network Site.
 - An Emergency Calling Policy has been created for each building and associated with the corresponding Tenant Network Site. The “External location lookup mode” parameter is set to “False” for the Tenant Network Site oriented Emergency Calling Policies.
 - The “External location lookup mode” is enabled in the Global (org-wide default) Emergency Calling Policy.
 - All Location Information System (LIS) network elements have been defined and associated with “non-Front Door” Teams locations\places.
 - On premises Teams clients always get a network defined location. The current location of remote user is determined by the Work from Home feature of Teams Dynamic 911.
 - Location Services has been enabled on all client machines and configured to provide access to the Teams client.

“calling-debug.txt” Section Definitions

Location Policy Section

- This is the Calling Plan user version of the Teams “Emergency Call Routing” Policy.
 - This policy supports dialing “911” to make an emergency services call as is required by Kari’s Law.
 - The policy also supports dialing “1911” and “9911”. These are included because these were two (2) frequently used dial strings for making emergency calls on legacy telephony systems. Their presence does not violate Kari’s Law.

- This section will include the dial strings and dial masks in the applied “Teams Emergency Call Routing Policy” applied to a Direct Routing user.
- The information in this section should be identical for all US based Calling Plan users in commercial and education tenants. The value of “pstnUsage” will vary from tenant to tenant.
- “isCallingPlanUser” is always “true” for a Calling Plan and Operator Connect user, “false” for a Direct Routing user.
- Teams Dynamic 911 is enabled for all Calling Plan and Operator Connect users. This is reflected in the “true” value for “enhancedEmergencyServicesEnabled”.

```

isCallingPlanUser: true
Location Policy: {
  "enhancedEmergencyServicesEnabled": true,
  "locationRefreshInterval": 4,
  "pstnUsage": "EmergencyUsageNoamVer2",
  "conferenceMode": "",
  "emergencyNumbers": [
    {
      "dialString": "911"
    },
    {
      "dialString": "911",
      "dialMasks": "1911"
    },
    {
      "dialString": "911",
      "dialMasks": "9911"
    },
    {
      "dialString": "933"
    }
  ],
  "policyDocument": "LocationPolicy=Host:US"
}
Emergency Numbers: {
  "911": [
    "9911"
  ],
  "933": null
}

```

Figure 45 “calling-debug.txt” - Location Policy Section

Current Emergency Address Section

- The Teams Emergency Address of the current location is provided in this section.
 - The specific Teams Location\Place is provided in the “additionalInfo” field.
- The “type” field should be “LIS” for an on-premises location. This field is used to indicate if the provided address and location represents a validated and verified address. The “LIS” value indicates that this is an on-premises location automatically derived and based on a validated Teams Civic Address. On-premises locations are always validated and verified. There are other possible values for the “type” field:

Value	Current Location Type
LIS	On-premises location
ASSIST	Work from Home verified location
MANUAL	Work from Home manually entered verified location
CLS	Work from Home location that was neither verified or corrected

Figure 46 "calling-debug.txt" "type" field values

- The "editable" value indicates if the Teams user can edit or correct the provided location. This will be "false" if the type is "LIS".
- The Geo codes are those of the Teams Civic Address record for the location.

```

Current Emergency Address: {
  "address": {
    "companyName": "Panhandle Consumer Industries",
    "streetName": "Coastal Highway",
    "houseNumber": "1321",
    "cityOrTown": "Panacea",
    "stateOrProvince": "FL",
    "additionalInfo": "Floor 1 - Data Center",
    "country": "US",
    "postalOrZipCode": "32346"
  },
  "type": "LIS",
  "editable": false,
  "geocoordinates": {
    "latitude": 30.4761,
    "longitude": -86.1468
  }
}

```

Figure 47 "calling-debug.txt" - Current Emergency Address Section

Current MT Location Response

- This is the information that the Teams client is currently using for Dynamic 911 on the device.
- It is comprised of four (4) sections with a few standalone lines of information:
 1. emergencyCallingPolicy section
 2. networkRoamingPolicy section
 3. Standalone lines
 - endpointNetwork
 - networkSiteID
 4. locationInfo section
 - Geo Codes
 - address
 - Standalone line
 - Method
 5. Standalone Lines
 - enableLocationBasedRouting
 - siteAddress
 - subnetID

6. debugInfo section

- ncsDebugInfo sub-section
- siteMatchInfo sub-section
- networkLocationMatchInfo sub-section
- mtDebugInfo sub-section

emergencyCallingPolicy

- Provides the currently effective “Emergency Calling Policy” and its settings. This should be the policy associated with the current derived Tenant Network Site.
- This reflects the settings related to the notification requirement of Kari’s Law as they apply to a specific organizational building.
- The “externalLocationLookupMode” indicates if the Work from Home feature is enabled.

```
Current MT location response:
{
  "emergencyCallingPolicy": {
    "notificationDialOutNumber": [REDACTED],
    "externalLocationLookupMode": "Enabled",
    "notificationMode": "ConferenceUnMuted",
    "policyDocument": "TeamsEmergencyCallingPolicy=Tenant:Headquarters"
  },
}
```

Figure 48 “calling-debug.txt” - Current MT Location Response - emergencyCallingPolicy Sub-Section

emergencyCallRoutingPolicy

- This section will only appear for Direct Routing users.
- Teams Dynamic 911 can be enabled or disabled for Direct Routing users through the “allowEnhancedEmergencyServices” setting. In most cases, this should be set to “true”.
- The defined emergency numbers are displayed with their associated “onlinePSNTUsage”.
- The name of the policy applied to this session is also provided

```
"emergencyCallRoutingPolicy": {
  "allowEnhancedEmergencyServices": true,
  "emergencyNumbers": [
    {
      "dialString": "911",
      "dialMasks": "911;9911;112;999",
      "onlinePSNTUsage": "Emergency"
    },
    {
      "dialString": "933",
      "dialMasks": "933;9933",
      "onlinePSNTUsage": "Emergency"
    }
  ],
  "policyDocument": "TeamsEmergencyCallRoutingPolicy=Global"
}
```

Figure 49 “calling-debug.txt” - Current MT Location Response - emergencyCallRoutingPolicy Sub-Section

networkRoamingPolicy

- Not relevant for Teams Dynamic 911.

```

"networkRoamingPolicy": {
  "allowIPVideo": true,
  "mediaBitRateKb": 50000,
  "policyDocument": "TeamsMeetingPolicy=Host:RestrictedAnonymousAccess"
},

```

Figure 50 "calling-debug.txt" - Current MT Location Response - networkRoamingPolicy Sub-Section

endpointNetwork

- This indicates if the Teams client is behind a Tenant Trusted IP Address.
- This should always be "Trusted" for on premises Calling Plan, Operator Connect and Direct Routing users.

networkSiteId

- Shows the Teams Tenant Network Site based on the current network information acquired by the Teams client.
- Based on the previous assumptions, there should always be a Tenant Network Site value for this field.

```

"endpointNetwork": "Trusted",
"networkSiteId": "Headquarters",

```

Figure 51 "calling-debug.txt" - Current MT Location Response - endpointNetwork and networkSiteId

locationInfo

- If the device's Operating System's Location Services are enabled, the latitude and longitude provided by them are displayed. The enabled Location Services may sometimes be unable to provides this information.

```

"locationInfo": {
  "confidence": "Low",
  "coordinates": {
    "latitude": "30.02743",
    "longitude": "-84.38999"
  },

```

Figure 52 calling-debug.txt - Current MT Location Response - locationinfo Sub-Section

address

- The Teams Civic Address and Location\Place information derived from the applied LIS Network Element is displayed. The Location\Place is provided in the "additonalInfo" field. This information should match the information in the "Current Emergency Address" section.
- The "method" field should be "LIS". This field is used to indicate to Microsoft (or the Emergency Service Response Center for Direct Routing users) if the provided address and location represent a valid address and a verified address. The "LIS" value indicates that this is an on-premises location automatically derived and based on a validated Teams Civic Address.

```
"address": {  
  "companyName": "Panhandle Consumer Industries",  
  "streetName": "Coastal Highway",  
  "houseNumber": "1321",  
  "cityOrTown": "Panacea",  
  "stateOrProvince": "FL",  
  "additionalInfo": "Floor 1 - Data Center",  
  "country": "US",  
  "postalOrZipCode": "32346"  
},  
"method": "LIS"  
},
```

Figure 53 calling-debug.txt - Current MT Location Response - address Sub-Section

enableLocationBasedRouting

- The setting for enabling of location-based routing is provided. This is not applicable to Teams Dynamic 911.

siteAddress

- The name of the effective Tenant Network Site is again provided in the "siteaddress" field.

subnetId

- The device's current subnet is listed in the "subnetId" field.

```
"enableLocationBasedRouting": false,  
"siteAddress": "Headquarters",  
"subnetId": "192.168.1.0",
```

Figure 54 calling-debug.txt - Current MT Location Response - enableLocationBasedRouting,siteAddress,subnetId

debugInfo

ncsDebugInfo

- The "ncsDebugInfo" section provides an indication of whether the device is currently located "behind" a "Tenant Trusted IP address". The value for "reason" for on premises devices should always be "Matched".

```
"debugInfo": {  
  "ncsDebugInfo": {  
    "trustedIpMatchInfo": {  
      "publicIp": "169.45.21.8",  
      "trustedIPAddress": "169.45.21.8",  
      "maskbits": 29,  
      "reason": "Matched",  
      "_comment": "Match Client Public IP to Tenant Trusted IP"  
    },  
  },  
}
```

Figure 55 calling-debug.txt - Current MT Location Response - debugInfo\ncsDebugInfo Sub-Section

- The defined “Tenant Trusted IP addresses” can be found in the Teams Admin Center (TAC):
 1. Open the TAC.
 2. Click on “Locations”.
 3. Click on “Network Topology”.
 4. Click on “Trusted IPs”.
 5. Look for the “publicIp” in the list of “Trusted IPs”.

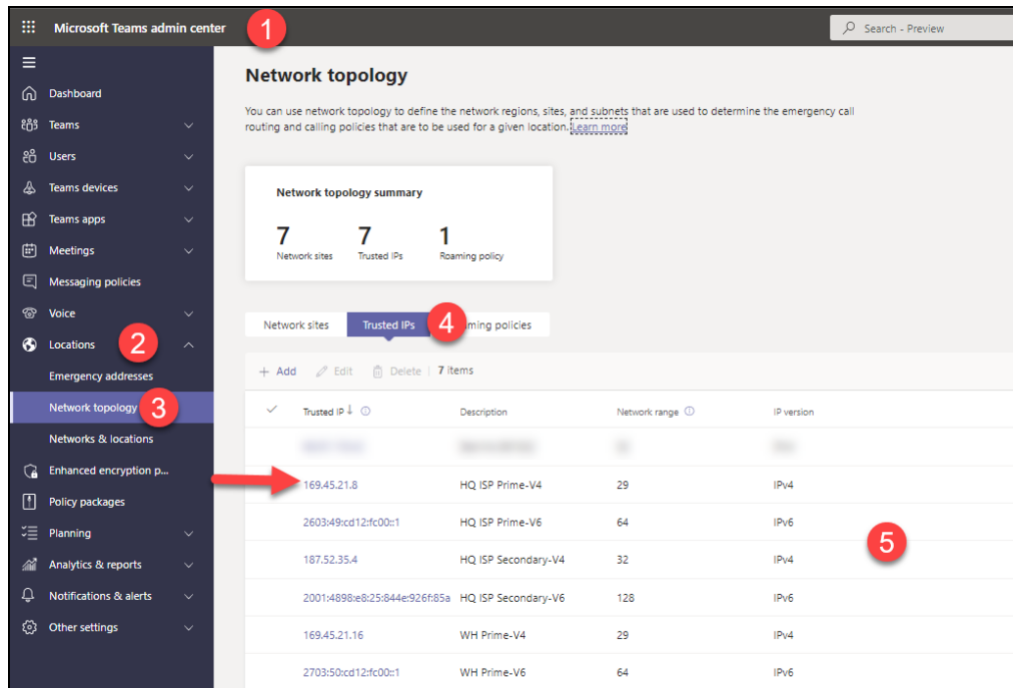


Figure 56 Locating Tenant Trusted IP Addresses in the TAC

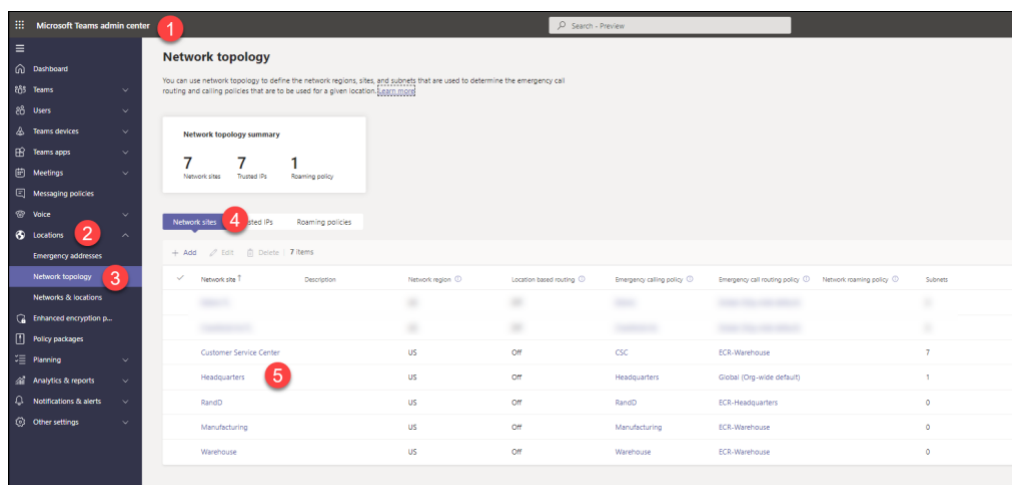
siteMatchInfo

- The “siteMatchInfo” subsection provides detailed information for how the current “Tenant Network Site” was derived.
- It also provides details about the “Tenant Network Site” including the name of its associated “Teams Emergency Calling Policy”. The “Teams Emergency Call Routing Policy” would be shown if the “calling-debug.txt” came from a Direct Routing user.
- The “reason” field should always be “Matched” for a “calling-debug.txt” from an on-premises user.

```
"siteMatchInfo": {  
  "ipv4": "192.168.1.15",  
  "subnetLengthIPv4": "24",  
  "subnetId": "192.168.1.0",  
  "maskBits": 24,  
  "teamsEmergencyCallingPolicyTag": "TeamsEmergencyCallingPolicy=Tenant:Headquarters",  
  "networkSiteId": "Headquarters",  
  "enableLocationBasedRouting": false,  
  "reason": "Matched",  
  "_comment": "Used to match endpoint subnet to Tenant site if trustedIpMatchInfo matches"  
}
```


Figure 57 calling-debug.txt - Current MT Location Response - debugInfo\siteMatchInfo Sub-Section

- This can be verified:
 1. Open the TAC.
 2. Click on "Locations".
 3. Click on "Network Topology".
 4. Click on "Network Sites".
 5. Click on the "Network Site" that matches the "networkSiteID" value in the "siteMatchInfo" section.
 6. Verify that the "subnetID" is in the list of Subnets.
 7. Check the "Emergency Calling Policy", it should match the value of "teamsEmergencyCallingPolicyTag". For a Direct Routing user, additionally verify the "teamsEmergencyCallRoutingPolicyTag".



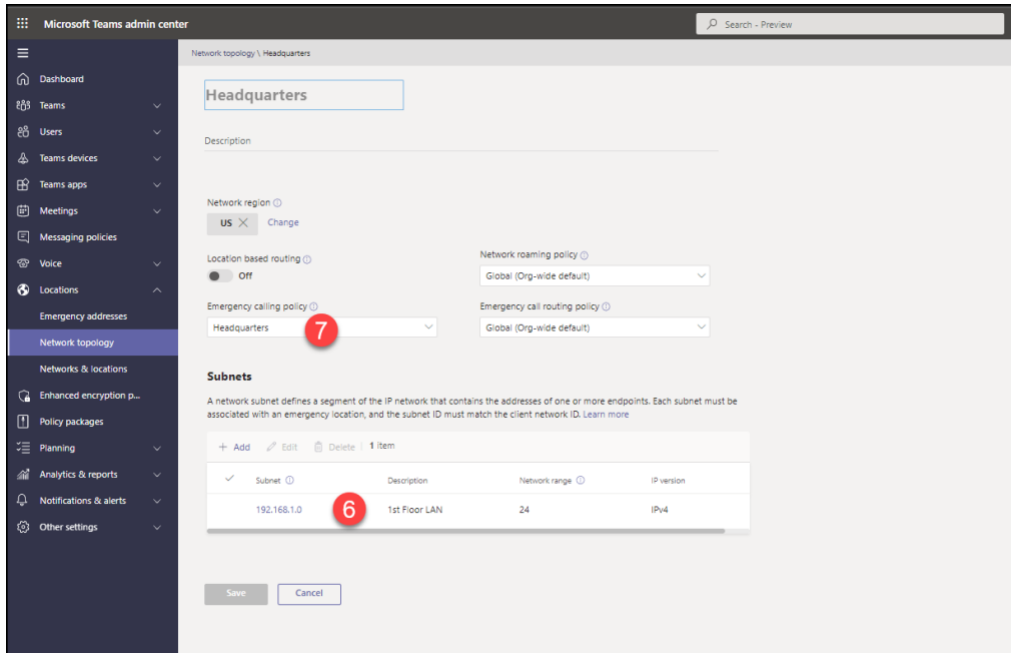


Figure 58 Locating Tenant Network Sites in the TAC

networkLocationMatchInfo

- The “networkLocationMatchInfo” subsection displays information about which LIS network element was matched to provide a location ID.
- The “matchedNetworkType” field displays which of the LIS Network Elements it matched on. If its value is “CLS” none of the LIS Network Elements could be matched. The client will use the available latitude and longitude to determine a current address.
- The “matchingIdentity” will display the specific network information it used to make the match. If the value of “matchedNetworkType” is CLS, the latitude and longitude will populate this field.
- In the example, a match was made to an LIS Port. It’s associated “locationID” is provided. The Chassis ID and Port it matched on is also provided.
- If you look up the “locationId” in the Teams Places\locations table, you should see the address information listed previously in the log.

```

"networkLocationMatchInfo": {
  "locationId": "b26735f0-e104-11ec-9b35-e9ea03b87a6b",
  "matchedNetworkType": "Port",
  "matchingIdentity": "30-37-a6-33-f7-1f_Gi0/31",
  "ipv4": "192.168.1.15",
  "chassisId": "30-37-a6-33-f7-1f",
  "portId": "Gi0/31",
  "reason": "Matched",
  "_comment": "Used to find emergency address,against Tenant Location Network Information (LIS), otherwise against Client Geo Location Information (CLS) if available"
}
    
```

Figure 59 calling-debug.txt - Current MT Location Response - debugInfo\networkLocationMatchInfo Sub-Section

- To verify this information:
 1. Open the TAC.
 2. Click on “Locations”.

3. Click on “Networks & locations”.
4. Click on the heading that matches the “matchedNetworkType”, in this case “Port”.
5. Look for the “portID” in the list of “Ports”
6. Click on the matched port.
7. Click the “Edit” button.
8. The location should match the information in the previous “address” sub-section of the “Current MT Location Response” section of the “calling-debug.txt”.

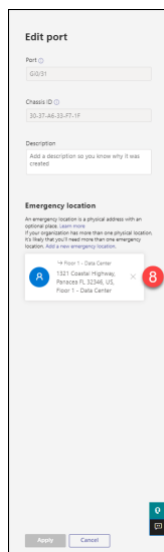
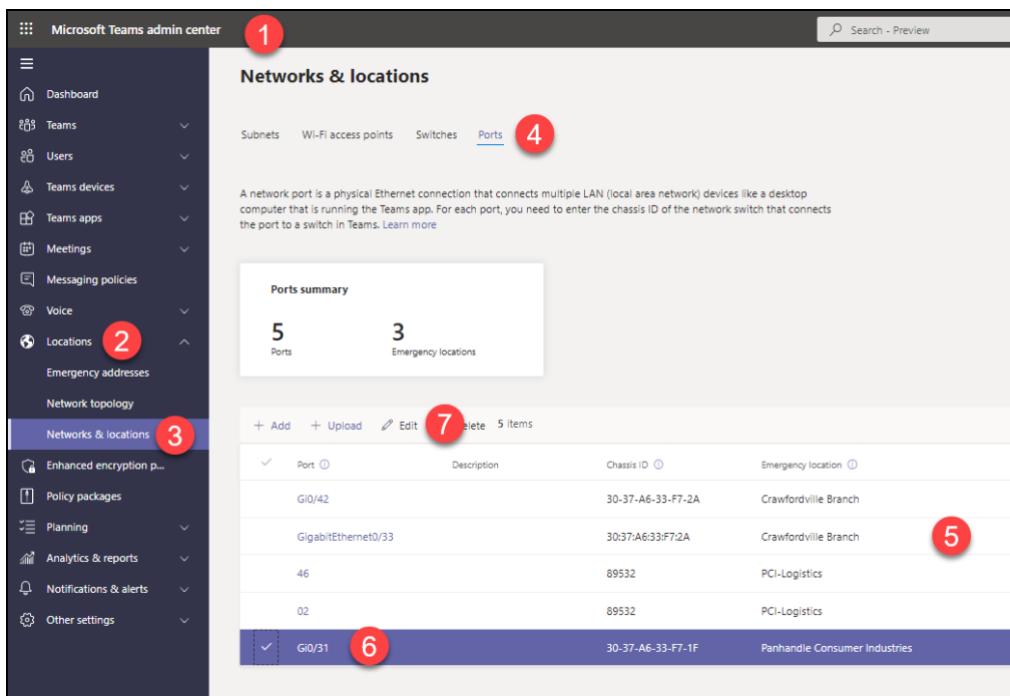
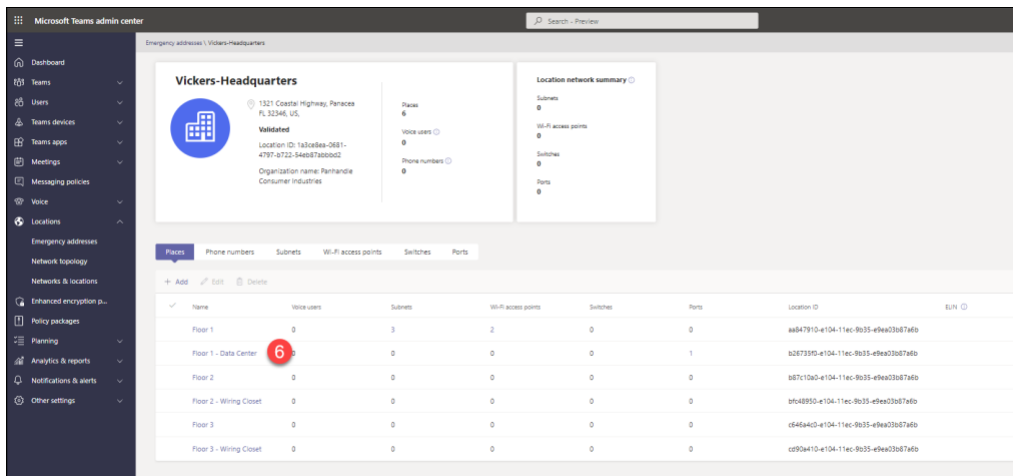
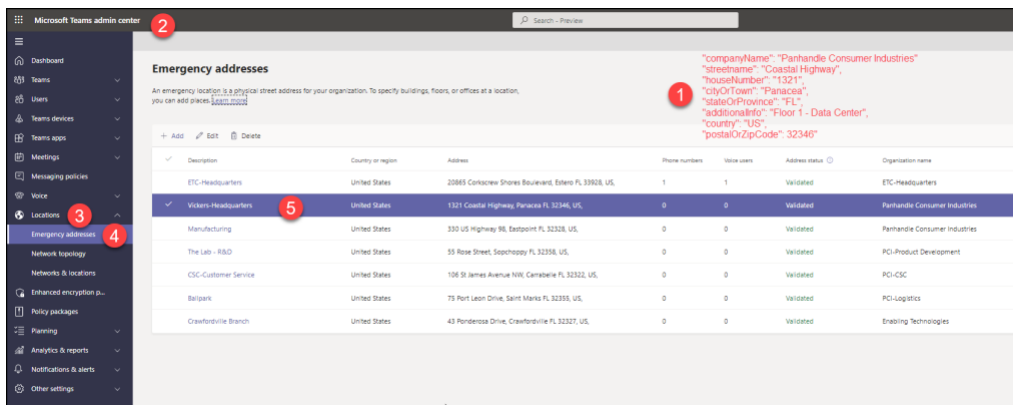


Figure 60 Locating an LIS Network Element and verifying its associated location in the TAC

- There is also a “reverse” way to verify the information:
 1. Note the information in the “address” sub-section of the “Current MT Location Response” section.
 2. Open the TAC.
 3. Click on “Locations”.
 4. Click on “Emergency Addresses”.
 5. Click on the matching “Emergency Address”.
 6. Click on the location from the “additionalInfo” field.
 7. Click on the tab corresponding to the value of “matchedNetworkType”, in this case “Ports”.
 8. The matching record should be listed.



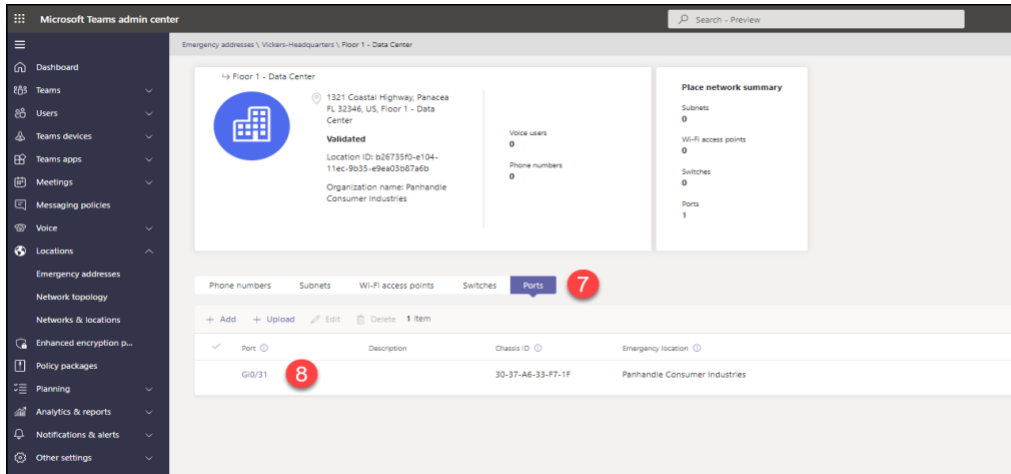


Figure 61 Reverse method of locating an LIS Network Element and its associated location in the TAC

mtDebugInfo

- In this section the "isDirectRoutingOnlyUser" is an indication if the signed in user is a Direct Routing user. For a Calling Plan or Operator Connect user, the previous "isCallingPlanUser" setting will be "true", while the value for this setting will be "false". For a Direct Routing user, "isCallingPlanUser" will be "true" while the value for this second setting will be "false".
- The effective "Emergency Calling" and "Network Roaming" Policies are provided. The "Emergency Call Routing" Policy is also provided for Direct Routing users.
- The method used for assigning these policies is also provided.

```
"mtDebugInfo": {  
  "isDirectRoutingOnlyUser": true,  
  "emergencyCallingPolicyTag": "TeamsEmergencyCallingPolicy=Tenant:Headquarters",  
  "emergencyCallRoutingPolicyTag": "TeamsEmergencyCallRoutingPolicy=Tenant or Host Global",  
  "networkRoamingPolicyTag": "Default",  
  "emergencyCallingPolicyAssignedTo": "Tenant:Headquarters",  
  "emergencyCallRoutingPolicyAssignedTo": "Tenant or Host Global",  
  "networkRoamingPolicyAssignedTo": "Tenant or Host Global",  
  "ncsResponseReceived": true,  
  "correlationId": "622EFACE3A054BC2AAE69ED00ED6ACDC"  
}
```

Figure 62 calling-debug.txt - Current MT Location Response - debugInfo\mtdebuginfo Sub-Section

Using the calling-debug.txt to troubleshoot the Current Location and other Issues

Teams on-premises users have little to no involvement in whether the Teams client will provide them an accurate current location. The accuracy of the current location is wholly dependent on the accuracy of the setup of the data for the:

- Emergency Addresses.
- Locations\Places.
- Tenant Trusted IP Addresses.
- LIS Network Elements.

The dynamic assignment of the Emergency Calling Policy for all on-premises users and the Emergency Call Routing Policy for Direct Routing users is dependent on the accuracy of the:

- Tenant Network Regions.
- Tenant Network Sites.
- Tenant Network Subnets.
- Correct assignment of the Emergency Calling and Emergency Call Routing policies to the correct Tenant Network Sites.

For on-premises users, they need only to check that the current location in the Teams client is correct. On-premises users cannot correct a current location, but they must advise the organization's support desk of the issue. Off-premises users must always check the current location and take some action. They must confirm the location, edit an incorrect location, or add a missing location. They should also add more specific location information when confirming a location such as an apartment number, floor number, etc. as appropriate.

The information in the calling-debug.txt can be used to troubleshoot:

- Incorrect address or specific location information for an on-premises user.
- An on-premises user with a Work from Home current location.
- 911 or 933 emergency call notification problems for on-premises users.
 - Notifications not being sent.
 - Notifications being sent to incorrect personnel.
- No current location at all for both on-premises and Work from Home users.

The calling-debug.txt can be used to verify:

- An on-premises user is located behind a Public IP listed in the Teams Tenant Trusted IP addresses.
- An on-premises user is connected to an IP subnet defined as a Teams Tenant Network Subnet that has been associated with a Teams Tenant Network site.
- The Teams Tenant Network site derived for the user matches the building the user is located in.
- The correct Teams Emergency Calling and Teams Emergency Call Routing policies have been assigned to the user's derived Teams Tenant Network site.
- The "type" and "method" values are both "LIS" for an on-premises user.
- The notifyees, to a degree, listed in the Teams Emergency Calling policy are the correct ones for the associated Teams Tenant Network Site. If one or more groups are associated with the policy, further research would have to be done to check their membership. The accuracy of phone number notifyees would also have to be checked.

Earlier tables in this chapter, showed how the current location and the drop-down options could be used to identify problems with the current location. Information from the calling-debug.txt will tell us why the user is not getting a correct current location in their Teams desktop client:

Observations in the Teams Client	Teams Client Values		calling-debug.txt Values					Is the Teams current location information correct?	Call Routing	Successful 911 call?
	Current Location Correct?	Drop-Down Location Options	Tenant Trusted IP Match?	Tenant Network Subnet/Site Match?	LIS Network Element Match	Type	Method			
The current location, including the specific place is correct. The drop-down option is "Work Location".	Yes	Work Location (Greyed Out)	Yes	Yes	Yes	LIS	LIS	Yes	Directly to the PSAP.	Yes
The current location or the place are incorrect and the drop-down option is "Work Location".	No	Work Location (Greyed Out)	Yes	Yes	Yes	LIS	LIS	No	Directly to the PSAP.	No
The current address is correct but the place is missing and the drop-down option is "Location not Editable".	Yes	Location not Editable (Greyed Out)	Yes	Yes	No	CLS	CLS	No	To the ECC/ECRC before routing to the PSAP.	No
The current address is incorrect, the place is missing and the drop-down option is "Location not Editable".	No	Location not Editable (Greyed Out)	Yes	Yes	No	CLS	CLS	No	To the ECC/ECRC before routing to the PSAP.	No
The current address is correct but the place is missing and the drop-down option is "Verify".	Yes	Verify	No	No	No	CLS	CLS	No	To the ECC/ECRC before routing to the PSAP.	No
The current address is incorrect and the place is missing. The drop-down option is "Verify".	No	Verify	No	No	No	CLS	CLS	No	To the ECC/ECRC before routing to the PSAP.	No
There is no current location displayed at all.								No	To the ECC/ECRC before routing to the PSAP.	No

Figure 63 Using the calling-debug.txt to Troubleshoot the Current Location of an On-Premises User

Information in the calling-debug.txt can also be useful when troubleshooting issues for Working from Home users. It can tell you if the user confirmed or edited the suggested address. It can also tell you what they entered as an address. In the calling-debug.txt of a Work from Home user:

- The Teams Tenant IP Address should never match.
- There should not be a match on the Tenant Network Subnet or a Tenant Network Site.
- A Work from Home user should always have the "Global (org-wide default)" Teams Emergency Calling Policy assigned to them.
- There will never be a match of an LIS Network element.
- The value of "method" will always be "CLS". The values for "type" will be "Assist", "CLS" or "Manual".

Observations in the Teams Client and user action	Teams Client Values		calling-debug.txt values			User Action Taken	Call Routing	Successful 911 call?
	Current Location Correct?	Drop-Down Location Options	Type	Method	Emergency Calling Policy			
The Teams client suggested a correct location. The user verified the location.	Yes	Verify	ASSIST	CLS	Global (org-wide default)	User Verified the location.	Directly to the PSAP.	Yes
The Teams client suggested a correct location. The user did nothing.	Yes	Verify	CLS	CLS	Global (org-wide default)	Did Nothing.	To the ECC/ECRC before routing to the PSAP.	No
The Teams client suggested an incorrect address. The user corrected the address.	No	Verify	MANUAL	CLS	Global (org-wide default)	User corrected and verified the location.	Directly to the PSAP.	Yes
The Teams client suggested an incorrect address. The user did not correct the address.	No	Verify	CLS	CLS	Global (org-wide default)	Did Nothing.	To the ECC/ECRC before routing to the PSAP.	No
The Teams client could not suggest an address. The user added the correct address.	Location Not Detected	Verify	MANUAL	CLS	Global (org-wide default)	Location added and verified by the user.	Directly to the PSAP.	Yes
The Teams client could not suggest an address. The user did not add a correct address.	Location Not Detected	Verify	CLS	CLS	Global (org-wide default)	Did Nothing.	To the ECC/ECRC before routing to the PSAP.	No
There is no location displayed at all							To the ECC/ECRC before routing to the PSAP.	No

Figure 64 Using the calling-debug.txt to Troubleshoot a Work from Home User

ERSP Troubleshooting

Microsoft, the Operator Connect vendors and the Direct Routing ERSPs will route calls based on the information they receive from Teams. We can refer to these parties as the "routing vendors". Calls will not be routed correctly if the location information passed to them from Teams is incorrect.

If a user placed a 933-test call and the information displayed on the screen in their Teams client and the readback of their location did not match their physical location, opening a ticket with the routing vendor would not be the correct first troubleshooting step. If the presented current location and readback of the current location is correct, we can then move on to verifying that the routing vendor routed the call correctly.

There are a few cardinal rules regarding how Teams emergency service calls should be routed by the vendors:

1. All calls from on-premises users should be routed directly to the correct PSAP based on the user's current location.
2. All calls from Work from Home users who have confirmed a suggested address should go directly to the PSAP based on the confirmed address.
3. All other emergency service calls from Work from Home users should go to the ECC\ECRC and then be routed to the appropriate PSAP.
4. Direct calls to the PSAP and calls routed by an ECC\ECRC agent should always be routed to the appropriate PSAP based on the caller's current location.

As mentioned previously, the best way to troubleshoot Teams Dynamic 911 calling is through prevention and regular testing. Develop a plan to make both 933 and 911 test calls on a regular basis. You can assume that if a 933 test call fails, a subsequent 911 test call using the same parameters will also fail. Before placing a test 911 call, you should have performed a test 933 call. The frequency of these calls will need to be determined by each organization's assessment of risk and consequences involved in failed live 911 calls. The testing and results must be documented.

The guidance below should be used for troubleshooting failed 933 and 911 test calls. It can also be used to troubleshoot failed live 911 calls. If a test call fails, it is extremely important to document the failed call and steps taken to resolve the issue. A failed and resolved 933 test call should almost always be followed up with a 911 test call using the same parameters of the 933 call.

Troubleshooting for Calling Plan and Operator Connect Users

There are two (2) primary tools we can use to verify emergency services calls are being routed correctly by the vendors:

1. Calling the 933 Test Number.
2. Placing live test 911 calls.

Calling the 933 Test Number

1. Dial 933 from a signed-on Teams client.
2. Take a screenshot or copy the information Teams presents in the call box.
3. Listen to the 933 bot and verify that it correctly reads back:
 1. That the user is in "Live" mode.
 2. The phone number.
 3. Address.
 4. Specific location (1st Floor, Room 305, etc.)
4. The bot should correctly indicate if the call would be routed to the PSAP or the ECC\ECRC.
5. If you chose to make a recording, it should have been played back to you correctly.

Once the call has been completed, verify that all the information provided in the Teams call box and the readback is correct. At this point, the next steps if something is wrong are simple:

- Check to see if there are any service advisories in the Office 365 Admin Center related to the problem.
- If not, contact Microsoft technical support.

You can call 933 as often as you need to. It is a good practice to make 933 calls from various on-premises locations on a regular basis and evaluate the results.

911 Test Calls

1. Do not perform a 911 test call without first successfully completing a 933 test call.
2. Following the guidance in the [Placing 911 test calls](#) section of this document, schedule and make a 911 test call from an on-premises location.
3. Take a screenshot or copy the information Teams presents in the call box.
4. Verify that the call was routed to the correct PSAP in a timely manner and that the PSAP received the correct location information.
5. Repeat the process from a Work from Home location with a confirmed location.
6. Verify that the call was routed to the correct PSAP in a timely manner and that the PSAP received the correct location information.
7. Make live 911 call from an edited Work from Home location.
8. Document whether the ECRC agent answered the call in a timely manner. Note any issues in the interaction with the agent.
9. Note the amount of time it took for the agent to transfer the call to the PSAP. Note any issues in the handoff from the agent to the PSAP.
10. Verify that the ECRC handed off the call and location information to the appropriate PSAP.

There are several types of live 911 call failures:

- The call doesn't complete.
- It does not get routed to the appropriate PSAP.
- There is either no audio or one-way audio.
- The PSAP receives incorrect location information.

If a 911 call fails:

- Document the failed 911 call.
 - Gather as much information as possible.
 - Do not let the documentation effort significantly slow down the troubleshooting process!
 - Document the date and time of the onset of the problem and when it was resolved.
 - In this case, there is no such thing as too much documentation.
- A second 911 call should be attempted as soon as possible from any location. This is to determine if there is a systemic problem with Teams 911 calling. You can forego the recommendation to schedule a test 911 call in this instance. [Placing 911 test calls](#) has been described in an earlier section of this document.
- **If the second call fails, open a "Sev A" ticket with Microsoft or your Operator Connect vendor immediately!**
- If the test call works, try to make a test call from the location of the first call.

- Regardless of the result, a support ticket should be opened with Microsoft or the Operator Connect vendor immediately to determine why the user's 911 call failed. Press them for the root cause and an explanation of what they have done or will do to prevent the issue in the future.
- The organization should advise their Microsoft Account team of the issue in writing if this was a failed call from a Calling Plan or Operator Connect user. The organization's Operator Connect vendor's account team should also be advised in writing.
- The organizations risk management, compliance and human resources personnel should be advised in writing of the failed live 911 call. Provide as much detail about the call, the testing, root cause, resolution and steps being taken by the organization and vendors to prevent a reoccurrence.

Troubleshooting for Direct Routing Users

The use of 933 test calls and placing 911 test calls are equally valuable tools for emergency services calling for Direct Routing users. There are some differences in how to troubleshoot any issues.

Calling the 933 Test Number

For Direct Routing users, there are two (2) elements to observe when placing 933 test calls:

- The Teams client will display the caller's phone number and Teams current location which should be accurate.
- The ERSP's bot will answer the call and readback the information to the caller. If the call is not answered by the ERSP's bot, the Teams client will not display the emergency call information.

As mentioned earlier, support for the test number and the content of the readback will vary amongst the ERSP and SIP Trunk vendors. Whatever the bot reads back should be accurate. If any element of the readback is incorrect, the routing of the call between Teams, the SBC and the ERSP needs to be reviewed.

- If the call to the bot goes through but the display of the caller's phone number or current location in the Teams client is incorrect, contact Microsoft support.
- For all other problems:
 - Make a test outbound call from a Teams user. This is a simple test to verify that the SBC is working properly with Teams voice for outbound calls in general.
 - Check to see if there are reports of PSTN calling problems among your other Teams users.
 - Check the health of Teams in the Microsoft 365 portal.
 - Check the status of the SBC in the TAC.
 - Check the SBC from its management interface.:
 - Verify that the SBC is operating correctly.
 - Check the status of the Teams Proxy Set on the SBC. It should be "ONLINE" for at least one of the members in the Proxy Set.
 - The Proxy Set associated with the ERSP's and SIP Trunk vendors will almost always show "ONLINE" even if the connection has failed.
 - Start an SBC Syslog.
 - Place a second 933 test call and verify that the call is being routed to the SBC from Teams.
 - The phone number in the "FROM" field in the SIP header should be the caller's number.

- The 'PRIORITY' field in the SIP header should say "emergency".
- Review the information in the PIDF-LO section of the SDP for the call leg coming from Teams to the SBC. Verify that it is correct.
 - The address information should match the Teams current location.
 - The "method" field should be:
 - "LIS" for an on-premises location.
 - "ASSIST" for a Work from Home confirmed location.
 - "MANUAL" for an edited Work from Home location.
 - "CLS" for a Work from Home location that was neither confirmed nor edited.
 - Review the information in the PIDF-LO section of the SDP for the call leg leaving the SBC and going to the ERSP or SIP Trunk vendor. It should match the information from the inbound leg of the call. Verify that it is correct.
- Review the Syslog and look for anything else that might be causal.
- If the call is not being properly routed through the SBC, open a support ticket with your provider of support for the SBC.
- If the call is being properly routed through the SBC, open a support ticket with the ERSP or SIP Trunk vendor.

Making 911 Test Calls

There are several types of Direct Routing live 911 call failures:

- The call doesn't complete.
- It does not get routed to the appropriate PSAP.
- There is either no audio or one-way audio.
- A problem with the ERSP or SIP Trunk vendor.
- The PSAP receives incorrect location information.
- A problem at the PSAP.

If a 911 test call fails:

- If the call fails, the root cause of the problem could be with one or more of:
 - The Microsoft 365 and Teams infrastructure.
 - The routing of the call by Teams to the SBC.
 - The SBC.
 - The routing of the call from the SBC to the ERSP or SIP Trunk vendor.
 - The ERSP or SIP Trunk vendor.
 - The PSAP.
- Document the failed 911 call.
 - Gather as much information as possible.
 - Do not let the documentation effort significantly slow down the troubleshooting process!
 - Document the date and time of the onset of the problem and when it was resolved.
 - In this case, there is no such thing as too much documentation.

- Start a Syslog on the SBC.
- A second 911 call should be attempted as soon as possible from any location. This is to determine if there is a systemic problem in the Teams 911 call flow. You can forego the recommendation to schedule a test call in this instance. [Placing 911 test calls](#) has been described in an earlier section of this document.
- **If the second call fails, open a “Sev A” ticket with Microsoft immediately!.** The root cause of the problem may not be with Microsoft but opening a case at this point will save some time if they end up owning the root cause.
- If the test call works, try to make a test call from the location of the first failed 911 call.
- Make a test outbound call from a Teams user. This is a simple test to verify that the SBC is working properly with Teams voice for outbound calls in general.
- Check to see if there are reports of PSTN calling problems among other Teams users.
- Check the health of Teams in the Microsoft 365 portal.
- Check the status of the SBC in the TAC.
 - Check the SBC from its management interface.:
 - Verify that the SBC is operating correctly.
 - Check the status of the Teams Proxy Set on the SBC. It should be “ONLINE” for at least one of the members in the Proxy Set.
 - The Proxy Set associated with the ERSP’s and SIP Trunk vendors will almost always show “ONLINE” even if the connection has failed.
 - Review the second 911 test call in the SBC’s Syslog and verify that the call is being routed to the SBC from Teams.
 - The phone number in the “FROM” field in the SIP header should be the caller’s number.
 - The ‘PRIORITY’ field in the SIP header should say “emergency”.
 - Review the information in the PIDF-LO section of the SDP for the call leg coming from Teams to the SBC. Verify that it is correct.
 - The address information should match the Teams current location.
 - The “method” field should be:
 - “LIS” for an on-premises location.
 - “ASSIST” for a Work from Home confirmed location.
 - “MANUAL” for an edited Work from Home location.
 - “CLS” for a Work from Home location that was neither confirmed nor edited.
 - Review the information in the PIDF-LO section of the SDP for the call leg leaving the SBC and going to the ERSP or SIP Trunk vendor. It should match the information from the inbound leg of the call. Verify that it is correct.
 - Look for anything causal in the Syslog.
 - If the call is not being properly routed through the SBC, open a “Sev A” support ticket with your provider of support for the SBC.
 - If the call is being properly routed through the SBC, open a “Sev A” support ticket with the ERSP or SIP Trunk vendor.

- Regardless of the result, open a support ticket with the party that you have determined owns the root cause of the original (or both) test 911 calls. Press them for the root cause and an explanation of what they have done or will do to prevent the issue in the future.
- The organization should advise the root cause vendor's account team of the issue in writing.
- The organizations risk management and human resources personnel should be advised in writing of the failed live 911 call. Provide as much detail about the call, the testing, root cause, resolution and steps being taken by the organization and vendors to prevent a reoccurrence.

Teams Dynamic 911 Test Plans

Organizations should have and use test plans when implementing Microsoft Teams Dynamic 911. They should be part of the installation process. Test plans should be used regularly to verify that Teams Dynamic 911 is working correctly and that calls are being delivered accurately to the PSAP. The purpose of the test plan is to ensure that you have tested the Teams clients used by your organization and the ERSP for both on premises and Work from Home users. It may be easier to use two (2) separate test plans:

1. Teams Dynamic 911 client test plan
2. Teams Dynamic 911 ERSP test plan

Teams Dynamic 911 Client Test Plan

This plan can be used to verify that the various Teams clients in use within the organization are providing the expected information before a user places a 933 or 911 test call. These tests should be completed with all tests passing before placing 933 or 911 test calls in the production environment.

This sample test plan includes all the available Teams clients and how they support Dynamic 911 and the Work from Home feature for reference. You can add additional tables for devices connected to a Virtual Private Network (VPN) or Virtual Device Infrastructure (VDI) devices. Adjust this plan to meet your needs. To use the test plan for on-premises users (a sample test plan for Work from Home users is included) enter:

1. A Description for the test.
2. The location that you expect to see in the Teams client. This should match the current location of the signed in user.
3. The actual location in the Teams client.
4. If the locations match, the test would be scored as a "Pass", if not it will be labeled as a "Fail".
5. The rest of the columns would be used to document the information in the calling-debug.txt at the time of the test.
6. Add additional notes as needed including the cause of the failure.
7. If you are not using a particular client, delete it from the table or mark the test as "Waived – N/A".

Teams Dynamic 911 ERSP Test Plan (933 Calls)

We can use this test plan to verify that the ERSPs bot is working correctly and "reading back" the expected information for the call. Before making a 933 test call, you should have first verified that the Teams client is deriving the expected location correctly. To use this test plan for on-premises callers, enter:

1. The test caller's name.
2. The caller's phone number.
3. The name of the PSAP that you expect to answer the call. This will usually be the county in which the caller's address is located.
4. The building name in Teams.
5. The specific location of the caller in the building.
6. The City, State and County of the address.
7. Date and time of the call.
8. If you answer "Yes" to all four (4) questions in the "Results" and the amount of time to answer the call was "reasonable", score the call as a "PASS". Otherwise, it is a "FAIL".
9. Include the reason and other relevant information in the "Notes" column.

Sample Test Plans

Teams Dynamic 911 Testing On-Premises Tests Basic Wired or WIFI Connection																				
Test	Client/Endpoint	Client Supports Teams Dynamic 911?	Client Supports Teams WFH?	Test Description	Expected Result - Include Expected Location	Actual Result - Include Actual Location	Pass/Fail	calling-debug.txt Information											Notes	
								IP Address	Mask	LIS Subnet	LIS BSSID	LIS Chassis ID	LIS Poert	Client Public IP	Trusted IP Match?	Tenant Network Subnet?	Tenant Network Site?	Emergency Calling Policy?		Emergency Call Routing Policy?
1	Teams Windows Desktop	Yes	Yes	Connect to a Wired network	Headquarters - Floor 1	Headquarters - Floor 1	PASS	10.11.21.153	22	10.11.20.0		10-b3-d5-9b-8d-80	Gi1/0/24	198.7.212.40	Yes	10.11.20.0	Headquarters	Headquarters	N/A	
2	Teams Mac Desktop	Yes	Yes	Connect to a Wired network	Headquarters - Floor 2	Headquarters - Floor 1	FAIL	10.12.13.140	22	10.12.12.0		10-b3-d5-af-6e-68	Gi1/0/12	198.7.212.40	Yes	10.12.12.0	Headquarters	Headquarters	N/A	LIS Subnet mapped to wrong location ID
3	Teams Web Client	No	No																	
4	Teams Mobile - IOS - WIFI	Yes	Yes - No Verify																	
5	Teams Mobile - Android - WIFI	Yes	Yes - No Verify																	
6	Teams Mobile - IOS - Cellular	Yes	Yes - No Verify																	
7	Teams Mobile - Android - Cellular	Yes	Yes - No Verify																	
8	Native Teams Phone - Wired	Yes	Yes																	
9	Native Teams Phone - Wireless	Yes	Yes																	
10	SIP Phone - Teams SIP Gateway	Yes	Yes																	
11	Analog Device	No	No																	

Figure 65 Sample Teams Dynamic 911 Client on-premises Test Plan

Teams Dynamic 911 Testing On-Premises Tests Calls to 933 - Microsoft Test Bot																	
Test	Caller Name	Caller's Phone Number	Who do you expect to answer the call? (Which County or City's PSAP)	Building Name	Location	City	State	County	Call Date	Call Time	Results						Notes
											Pass or Fail? (Pass=Yes to all questions-Automatically Derived)	How long did it take before the call was answered? (seconds)	Was the call answered by the bot? (Yes/No)	Calling Number Correct (Yes/No)?	Provided location correct including the specific location in the building? (Yes/No)	Did the bot indicate that the call would be routed to the PSAP?(Yes/No)	
1	John Doe	+14435551234	Wakulla	Headquarters	Floor 1	Panacea	FL	Wakulla	8/29/2022	2:20 PM	PASS	15	Yes	Yes	Yes	Yes	
2																	
3																	
4																	
5																	
6																	
7																	
8																	
9																	
10																	

Figure 66 Sample Teams Dynamic 911 - 933 bot Test Plan

**Teams Dynamic 911 Testing
On-Premises Tests
Calls to 911**

Test	Caller Name	Caller's Phone Number	Who do you expect to answer the call? (Which County or City's PSAP)	Test Call Setup				Wired or WIFI	Building Name	Location	City	State	County	Results						Notes
				Has a test call been scheduled? (Y/N/Not Required)	Test Call Date	Test Call Time	Notes							Pass or Fail? (Pass=Yes to all questions-Automatically Derived)	How long did it take before the call was answered? (seconds)	Was the call answered by the PSAP? (Yes/No)	Was the call answered by the expected PSAP? (Yes/No- Correct for the caller's location)	Calling Number Correct (Yes/No)?	Provided location correct including the specific location in the building? (Yes/No)	
1	John Doe	+14435551234	Wakulla	Yes	8/29/2022	3:05 PM		Wired	Headquarters	Floor 1	Panacea	FL	Wakulla	PASS	15	Yes	Yes	Yes	Yes	
2																				
3																				
4																				
5																				
6																				
7																				
8																				
9																				
10																				

Figure 67 Sample Teams Dynamic 911 - 911 Call Test Plan

Summary

- “Failure is not an option” when making Teams Dynamic 911 calls. The call must get through to the correct PSAP with the correct and complete location information of the caller.
- Troubleshooting should be avoided at all costs. This is a solution that must always work correctly.
- Prevent dynamic 911 calling problems by regularly testing the installation. Testing should include placing test 911 calls.
- User submitted location, and other, problems must be resolved as quickly as possible.
- If there is a failed 933 test or failed 911 call, address these as soon as possible and thoroughly document the issue and the resolution.
- If the root cause of the problem is with Microsoft, an Operator Connect vendor or Direct Routing SBC, make the organization’s account team aware of the issue and its resolution.
- The display of the current location and the options in its drop-down menu in the Teams client can be used as a first level troubleshooting tool for problems with incorrect current locations.
- The calling-debug.txt debug log file is the key tool for troubleshooting the specific root cause of an incorrect location in the Teams client.
 - The log file can also be used to verify that the correct Emergency Calling and Emergency Call Routing policies are being assigned to the user.
 - The file can be used to verify that Work from Home users are confirming or correcting suggested locations.
- Before making test 933 and 911 calls, you must ensure that the Teams client is deriving the correct current location for the caller.
- The ERSPs will route 911 calls based on the information passed from Teams. If the information is wrong, the call will not route correctly.

Chapter 8 Teams Dynamic 911 Legal requirements, Maintenance, documentation, training, and other Subjects

Training your users to not use Teams to make calls to Emergency Services

- This is a common question in the Teams community:
 - *“Can we tell our Teams Users to not use Teams to make emergency services calls? Would we then not have to setup Teams Dynamic 911?”*
- Companies can train their users to not use Teams to call emergency services. Keep in mind that not all employees will always have another means available to them to make emergency services calls during the business day. Not all employees have cell phones, or they may be restricted from using them during business hours.
- Keeping in mind that this is not a qualified legal opinion, you would still need to configure your Teams voice environment to comply with all federal, state, and local regulations regarding emergency services calls.
- There are several anecdotes on the web about Federal Communications Commission (FCC) fines for non-compliance with Kari’s Law. Initial fines of \$10,000 and daily fines have been discussed.

Teams Installation Date and “Grandfathering” of Kari’s Law and the RAY BAUM Act

- Both pieces of legislation indicate that they are “forward-looking”. This means that they are only applicable to MLTS systems manufactured, imported, offered for first sale or lease, first sold, or leased, or installed prior to the various enactment dates.
- Again, a non-professional legal opinion, if you completed the move of all your telephony to Teams voice prior to February 16, 2020, you are probably exempt from both Kari’s Law and the RAY BAUM Act.
- If you completed the move to Teams voice between February 16, 2020, and January 6, 2021, you would likely need to comply with Kari’s Law but be exempt from the RAY BAUM Act’s January 6, 2021, requirement.
- Any Teams voice implementations completed after January 6, 2022, would need to comply with all aspects of both regulations
- Exemptions from State and local regulations would have to be reviewed. In some cases, these regulations could compel a company to comply with the Federal laws to satisfy the State or local requirements
- The bottom line, is review this with your in-house counsel and remember that

Maintenance

- Real estate, legal and network architecture changes will impact the installation of Teams Dynamic 911
- These changes can make a company non-compliant with the rules exposing them to penalties and can pose a health and safety risk to its employees
- A company’s Teams Administrators must know when anything changes in the company that would require updating the Teams Dynamic 911 configuration. Here are some examples of changes that would be relevant:

- Real-estate changes.
 - New buildings.
 - New office space in new States.
 - Buildings added through merger or acquisition.
 - Occupying additional space in a shared office space building.
- Adding a new wired or wireless subnet.
- Adding more Wi-Fi access points.
- Adding additional network switches.
- Replacing network switches, wireless access points, etc.
- The laws and regulations covering Dynamic 911 are not static. The Administrators must be aware of these changes and how they will impact the deployment.
- For many reasons in addition to these presented, Companies that do not have a well-documented and efficient Change Control Process-----need to get one!

Documentation

- Experience shows that the more documentation you have for the implementation of Dynamic 911, the easier the process will go. This effort will result in a less costly, quicker, safer, and more accurate installation of Teams Dynamic 911.
- The documentation of the deployment does not end with the installation. It must always be kept accurate reflecting the running state of Dynamic 911.
- Companies could be compelled to provide this documentation to regulators, insurers, auditors, etc. This documentation could help the company when dealing with litigation.

Training

- A company's users are taught how to make phone calls using the Corporate phone system.
- User's must be trained on how to call emergency services through Microsoft Teams.
- It is extremely important that external and WFH users be trained on the importance of their always validating their locations when out of the office.
- Training is important for the health and safety of a company's employees. It can also protect the company from some adverse litigation.

Chapter 9 Configuring Teams Dynamic 911 objects and Elements

Teams Emergency Addresses

Teams Admin Center

1. To add an Emergency Address through the Teams Admin Center, click on “Locations” then “Emergency addresses”.

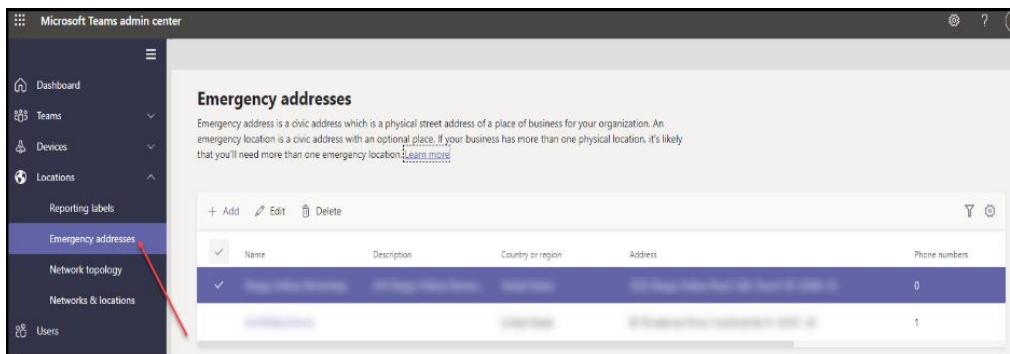


Figure 68 Adding an Emergency Address

2. Click the “Add” button to add an Emergency Address.
3. Click the “Country or Region” drop down and select the address’s Country.

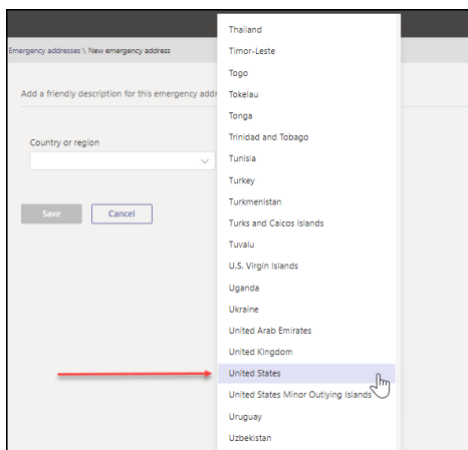


Figure 69 Adding an Emergency Address - Country

4. Enter any additional descriptive information in the “Description” field at the top of the Emergency Address input screen.

- Put the Building Name in the "Organization Name" field towards the bottom of the screen. Teams will let you create multiple records with the same "Organization Name". From experience, this will cause you a lot of problems in keeping your Emergency Addresses in order. Use a unique name in the "Organization Name" field for every Emergency Address you create.
- Start typing in the building's full address including the City, State and Zip Code. Teams will try to match your typing against a record in the MSAG. Once it "offers" you the correct record, click it to select it. The record may not exactly match what you typed in. In the example, "Hwy" was typed in, but the MSAG address has it as "Highway".

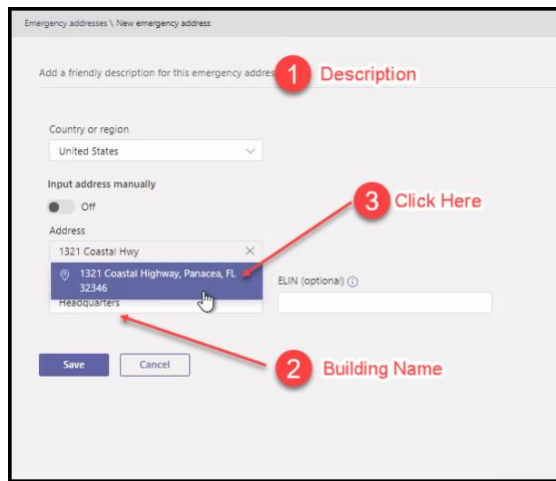


Figure 70 Adding an Emergency Address-Automatic

- If you turn on the "Input address manually" button, you will be presented with individual fields for the address, including the latitude and longitude that you will have to provide.

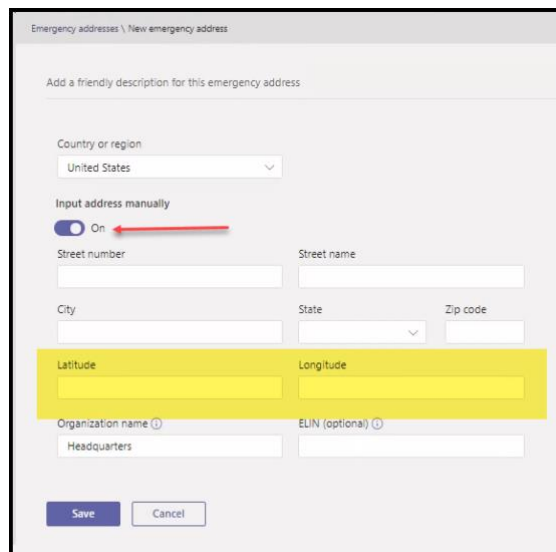


Figure 71 Adding an Emergency Address - Manual Entry

- Teams should show you a map with the location indicated.

9. Add an ELIN Number if required and Click the “Save” button.

Figure 72 Adding an Emergency Address - Validated Address

10. Once you click “Save”, you will be returned to the list of Emergency Addresses and advised that the record was created.

Name	Description	Phone numbers	Voice users	Address status
Headquarters		0	0	Validated

Figure 73 Adding an Emergency Address - Completed

- “Behind the Scenes”, Teams will have created a CsOnlineLISCivicAddress record for the Emergency Address.
 - A unique CivicAddressID would be assigned to it and the latitude and longitude from the MSAG information would have been added.
 - The “Building Name” which you put in the “Organization Name” field ends up in the “companyName” field while the information that you put in the “Description” field is in the “Description” field in the CsOnlineLISCivicAddress record.
 - You can view these records in PowerShell using the Get-CsOnlineLISCivicAddress command.

```
RunspaceId      : 18f05376-0c18-4d2a-a264-e665abe63511
TenantId        : 4e27fad0-016a-4428-b743-bd3a711b16ca
CivicAddressId  : 7060f979-4d4b-4b17-938e-a734a8dd2663
HouseNumber     : 1321
HouseNumberSuffix :
PreDirectional  :
StreetName      : Coastal Highway
StreetSuffix    :
PostDirectional :
City            : Panacea
CityAlias       :
PostalCode      : 32346
StateOrProvince : FL
CountryOrRegion : US
Description     :
CompanyName     : Headquarters
CompanyTaxId    :
DefaultLocationId : d63dde2c-4a9c-4c9a-8e1a-830cdf339ce
ValidationStatus : Validated
NumberOfVoiceUsers : 0
NumberOfTelephoneNumbers : 0
ResultSize      : 0
NumberOfResultsToSkip : 0
Latitude        : 30.02743
Longitude       : -84.38999
Confidence      :
Elin            :
Force           : False
```

Figure 74 Teams Emergency Address in PowerShell

- Teams will have also automatically created a Location\Place record, CsOnlineLISLocation.
 - This record is the “default” place for the Emergency Address, the Street level or “front door” address of the building. Assigning a default place to a user/phone number or location may violate the requirements of the RAY BAUM act.
 - You can view the Locations\Places in PowerShell by running the command Get-CsOnlineLISLocation.

```
RunspaceId      : 18f05376-0c18-4d2a-a264-e665abe63511
TenantId        : 4e27fad0-016a-4428-b743-bd3a711b16ca
LocationId      : d63dde2c-4a9c-4c9a-8e1a-830cdf339ce
CivicAddressId  : 7060f979-4d4b-4b17-938e-a734a8dd2663
Location        :
CompanyName     : Headquarters
CompanyTaxId    :
HouseNumber     : 1321
HouseNumberSuffix :
PreDirectional  :
StreetName      : Coastal Highway
StreetSuffix    :
PostDirectional :
City            : Panacea
CityAlias       :
PostalCode      : 32346
StateOrProvince : FL
CountryOrRegion : US
Description     :
ValidationStatus : Validated
NumberOfVoiceUsers : 0
NumberOfTelephoneNumbers : 0
ResultSize      : 0
Latitude        : 30.02743
Longitude       : -84.38999
Confidence      :
Elin            :
Force           : False
```



Figure 75 Teams Default Location Record for an Emergency Address

- When you click on the Name of the Emergency Address in the Admin Center, you will see:
 - All Places associated with the Emergency Address except for the default.
 - Associated Calling Plan and Operator Connect User’s Phone Numbers.
 - LIS Subnets associated with this Place.
 - LIS Wireless Access Points associated with this Place.
 - LIS Switches associated with this Place.

- LIS Switch Ports associated with this Place.
- At the top of the screen, you will also see the LocationID of the “front door” default record for the Emergency Address. This location will not appear in the “Places” table below.

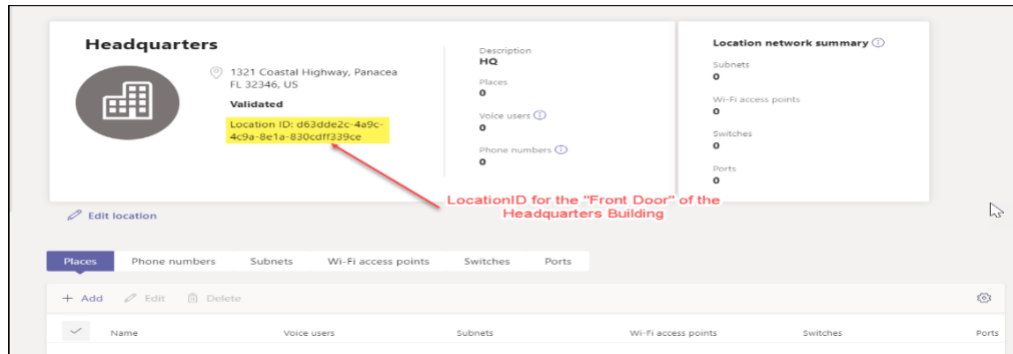


Figure 76 Teams Emergency Address - LocationID for Default Location

Teams PowerShell

- The Teams PowerShell commands to manage Emergency Addresses are:
 - [New-CsOnlineLISCivicAddress](#)
 - [Get-CsOnlineLISCivicAddress](#)
 - [Remove-CsOnlineLISCivicAddress](#)
 - [Set-CsOnlineLISCivicAddress](#)
- If you have a small number of Emergency Addresses to add, use the Teams Admin Center. Otherwise, consider using a PowerShell script that references a Comma Separated Value file for the information.
- If you are going to add these with a PowerShell Script, you will need a Comma Separated Value file with the required information properly formatted.
- Before adding an Emergency Address through PowerShell or a PowerShell script you will need to gather the latitude and longitude for each of the addresses that you would like to add. Teams refers to these as the Geocodes. You will also need these to manually add an Emergency Address in the Teams Admin Center as described previously.

Teams Locations\Places

Teams Admin Center

1. Click on the Emergency Address that you would like to add a Teams Place to:

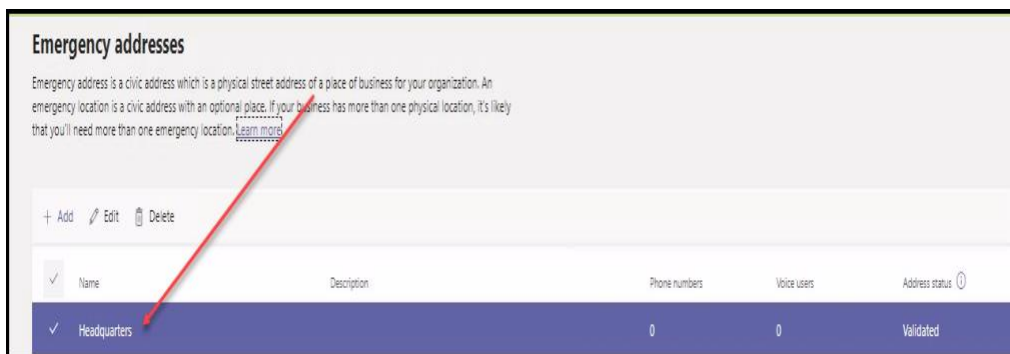


Figure 77 Adding a Teams Location\Place

2. Select the "Places" tab and click the "Add" button.

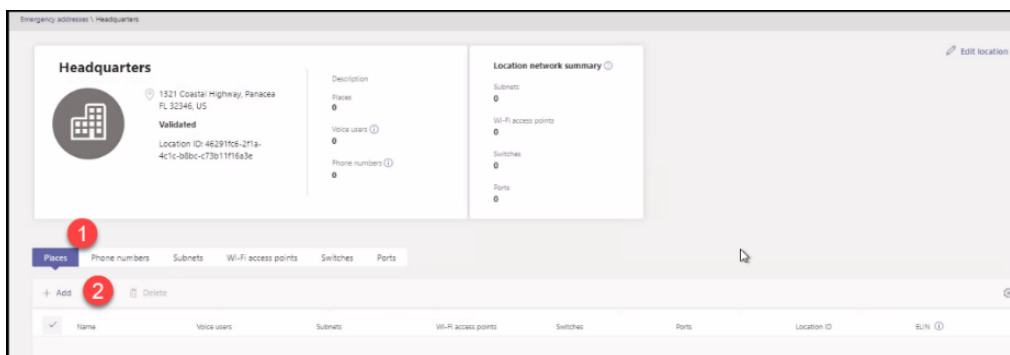


Figure 78 Adding a Teams Location\Place - New Place

3. In the "Name" field, type in the name of the Place such as Floor 1, First Floor, Suite 200, Floor 3 Office 309, etc.

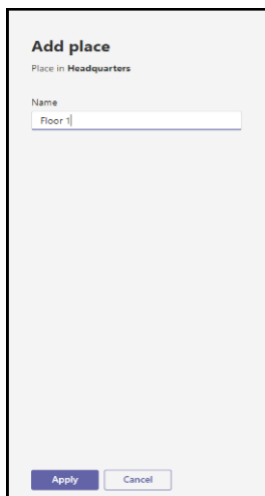
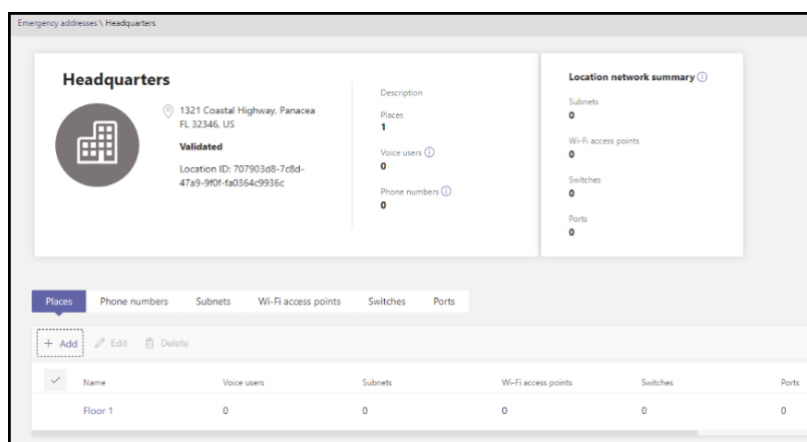


Figure 79 Adding a Teams Location\Place – Location Name

4. Click the “Apply” button.



Name	Voice users	Subnets	Wi-Fi access points	Switches	Ports
Floor 1	0	0	0	0	0

Figure 80 Adding a Teams Location\Place - Completed

Teams PowerShell

- The Teams PowerShell commands to manage Locations\Places are:
 - [New-CsOnlineLISLocation](#)
 - [Get-CsOnlineLISLocation](#)
 - [Set-CsOnlineLISLocation](#)
 - [Remove-CsOnlineLISLocation](#)
- You can use the `New-CsOnlineLISLocation` command to add Teams Places. You will need the CivicAddressID of the Teams Emergency Address before you can add a Place.
- If you are going to add these with a PowerShell Script, you will need a Comma Separated Value (CSV) file with the appropriate CivicAddressID and the name of the Location\Place. You may optionally add an ELIN to override the parent’s ELIN.

- The command can also be used to add a new Teams Place and Teams Emergency Address at the same time. This is not a recommended way to use this command. It is best to add and validate a Teams Emergency Address before adding any Teams Places.
- The output of Get-CsOnlineLISLocation for the first added Teams Place shows a new unique LocationID, the CivicAddressID of the Teams Emergency Address and "Floor 1" in the "Location" field.

```

RunspaceId      : 6f15b731-09e1-4458-b112-b971d0834fd7
TenantId        : 4e27fad0-016a-4428-b743-bd3a711b16ca
LocationId      : 5bb1bc68-2fd1-4b9d-b1a6-b01c13d102a3
CivicAddressId  : 131dfaa4-f0be-4301-ae4-5dd75217d4df
Location        : Floor 1
CompanyName     : Headquarters
CompanyTaxId    :
HouseNumber     : 1321
HouseNumberSuffix :
PreDirectional  :
StreetName      : Coastal Highway
StreetSuffix    :
PostDirectional :
City            : Panacea
CityAlias       :
PostalCode      : 32346
StateOrProvince : FL
CountryOrRegion : US
Description     :
ValidationStatus : Validated
NumberOfVoiceUsers : 0
NumberOfTelephoneNumbers : 0
Latitude        : 30.02743
Longitude       : -84.38999
Confidence      :
Elin            :
ResultSize      : 0
NumberOfResultsToSkip : 0
Verb            :
CorrelationId   :
Force           : False
  
```

Figure 81 Teams Location\Place record in PowerShell

Teams Emergency Calling Policies

Teams Admin Center

- The policies can be found in the Teams Admin Center by clicking on “Voice” then “Emergency policies” and “Calling policies” at the top of the page.

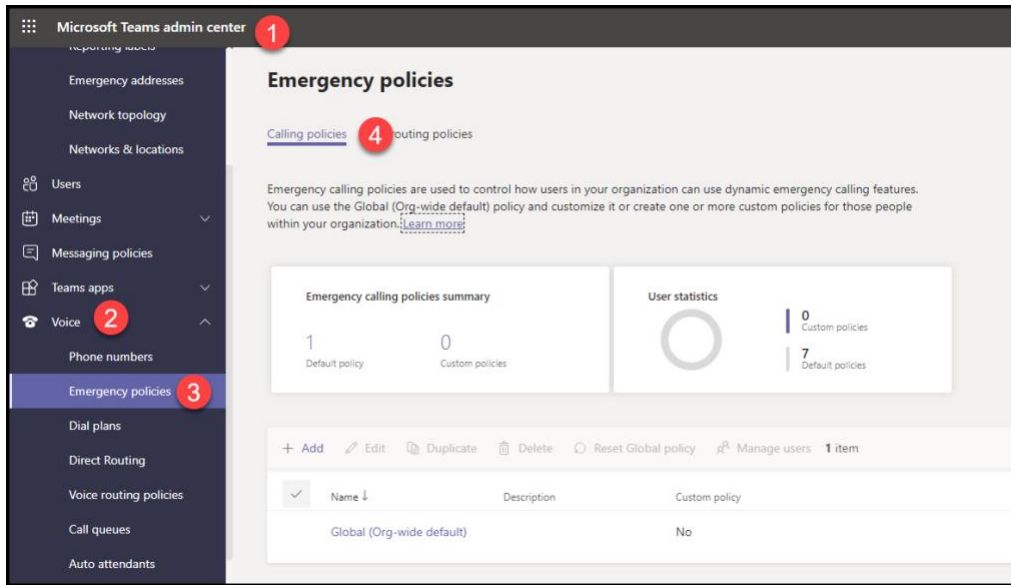


Figure 82 Teams Emergency Calling Policies

- The policies have eight (8) attributes and support multiple emergency numbers.:

Attribute	Description
Name	The name of the policy
Description	A Description of the policy. This should include the purpose of the policy
External location lookup mode	Enabled or Disables the Work from Home feature
Emergency service disclaimer	A text string of up to 350 characters shown at the top of the Calls app. Users must acknowledge the disclaimer by clicking the "OK" button.
Emergency Numbers	
Emergency dial string	-Specifies the emergency phone number -You can have separate emergency number treatments when 911 or 933 are dialed. -Each number can have different notification modes.
Numbers to dial for emergency calls notifications	-The PSTN phone cannot be unmuted even when the mode is set to "Conferenced in muted but are able to unmute" -Phone numbers should be in e.164 format
Notification mode	A drop down box with four (4) Choices: None Send notification only Conferenced in but muted Conferenced in and are unmuted If you select one of the "Conferenced" modes, you must enter a Phone Number or Users and Groups in the notification options
Users and groups for emergency calls notifications	-You can put in up to ten (10) entries of users and/or groups that will be notified when an emergency call is placed. -You can enter email addresses of users and the names of distribution or security groups separated by semi-colons ";". -Total number of users cannot exceed fifty (50).

Figure 83 Teams Emergency Calling Policy Attributes

- A user with Teams administrator permissions will be required to add and remove notification users from the policies. If you send the notifications to a distribution or security group, you will be able to delegate the

management of the group membership to an owner who does not have Teams administration permissions such as the manager of the Corporate Security Department.

- You can add a new policy by clicking the “Add” button or edit a policy by clicking on it then the “Edit” button:

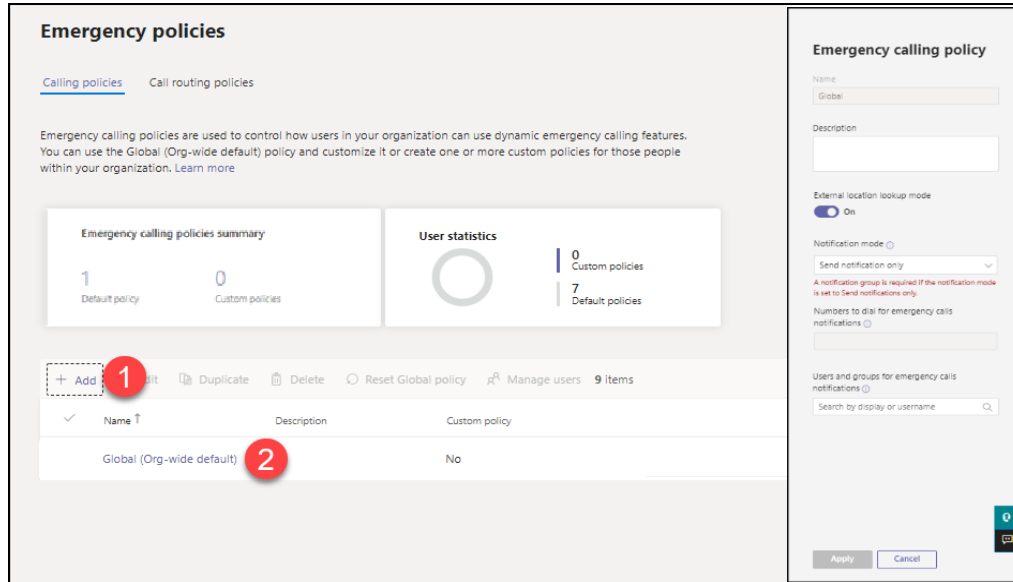


Figure 84 Teams Emergency Calling Policy - Configuration

Teams PowerShell

- The Teams PowerShell commands to manage Emergency Calling Policies are:
 - [New-CsTeamsEmergencyCallingPolicy](#)
 - [Get-CsTeamsEmergencyCallingPolicy](#)
 - [Remove-CsTeamsEmergencyCallingPolicy](#)
 - [Set-CsTeamsEmergencyCallingPolicy](#)
 - [Grant-CsTeamsEmergencyCallingPolicy](#)
- It may be easier to add these policies through PowerShell if you have a lot of them. Otherwise, add them through the Teams Admin Center.

Teams Emergency Call Routing Policies

Teams Admin Center

- The policies can be found in the Teams Admin Center by clicking on “Voice” then “Emergency policies” and “Call routing policies” at the top of the page.

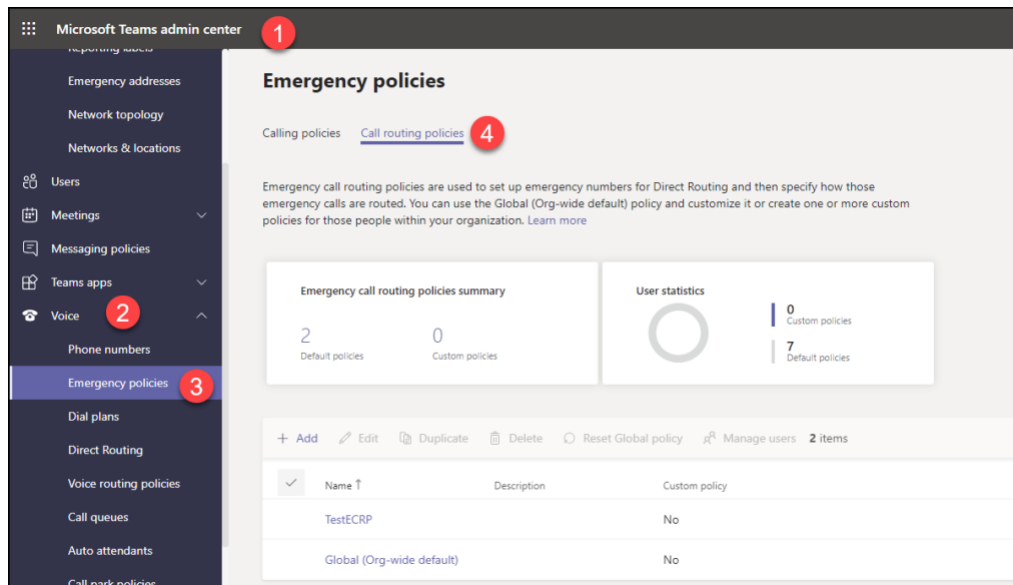


Figure 85 Teams Emergency Call Routing Policies

Teams PowerShell

- The Teams PowerShell commands to manage Emergency Call Routing Policies are:
 - [New-CsTeamsEmergencyCallRoutingPolicy](#)
 - [Get-CsTeamsEmergencyCallRoutingPolicy](#)
 - [Remove-CsTeamsEmergencyCallRoutingPolicy](#)
 - [Set-CsTeamsEmergencyCallRoutingPolicy](#)
 - [Grant-CsTeamsEmergencyCallRoutingPolicy](#)

Teams Tenant Trusted IP Addresses

Teams Admin Center

1. In the Teams Admin Center click on “Locations” then “Network topology” then the “Trusted IPs” tab. Click the “Add” button.

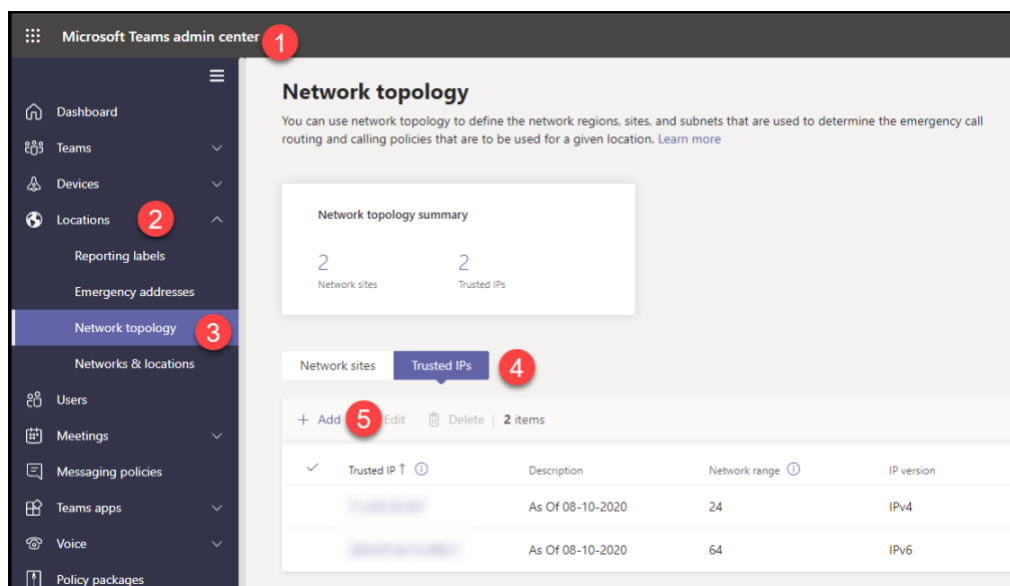


Figure 86 Teams Tenant Trusted IP Addresses

2. Click the “IP Version” drop down and select “IPv4” or “IPv6”.
3. Enter the IP Address in the “IP address” field.
4. Put the subnet mask in the “Network Range” field.
5. Add a description as required.
6. Click the “Apply” button.

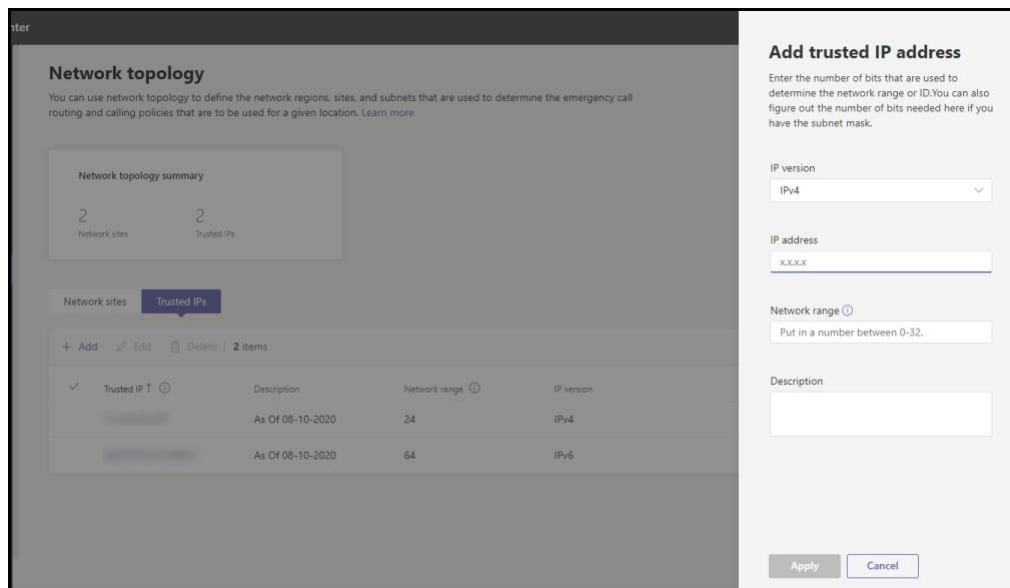


Figure 87 Teams Tenant Trusted IP Addresses - Configuring

Teams PowerShell

- The Teams PowerShell commands to manage the Trusted IP addresses are:
 - [New-CsTenantTrustedIPAddress](#)
 - [Get-CsTenantTrustedIPAddress](#)
 - [Set-CsTenantTrustedIPAddress](#)
 - [Remove-CsTenantTrustedIPAddress](#)
- Most organizations will not have many Tenant Trusted IP addresses to add to Teams. Manage them in the Admin Center instead of through PowerShell.
 - Teams Tenant Trusted IP addresses can be added through the Teams Online PowerShell Module
 - To create a new Tenant Trusted IP address, you will need to use the [New-CsTenantTrustedIPAddress](#) command.
 - If you are going to add these with a PowerShell script, you will need a Comma Separated Value file with the required information properly formatted.

Teams Tenant Network Regions

Teams Admin Center

1. To add a Tenant Network Region through the Teams Admin Center, click on “Locations” then “Network Topology” and “Manage Network Regions” in the upper right-hand corner of the screen.

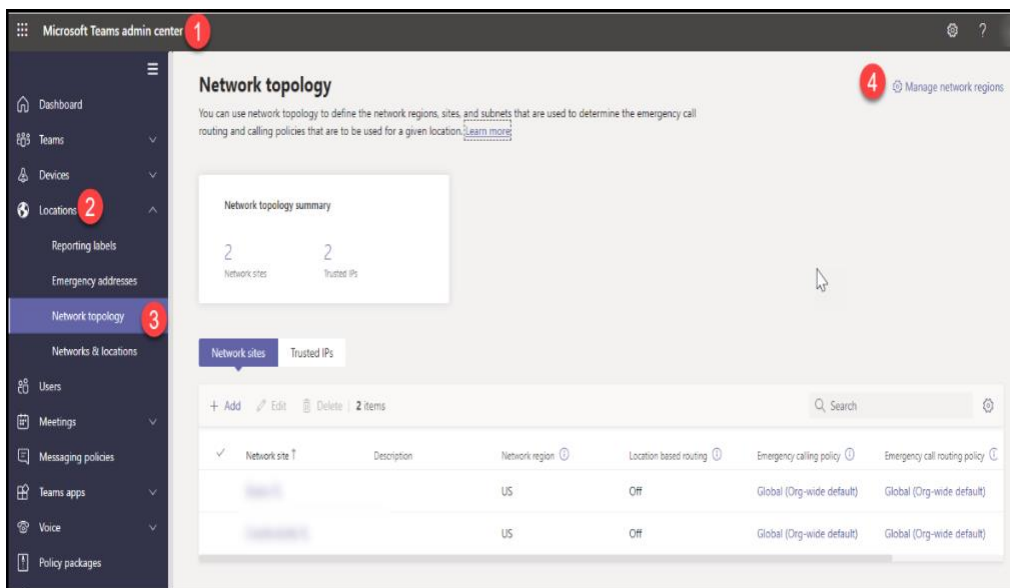


Figure 88 Teams Tenant Network Regions

2. Click in the entry box and enter the name of the region then click the “Add” button then the “Close” button on receipt of the notification that the region has been added.

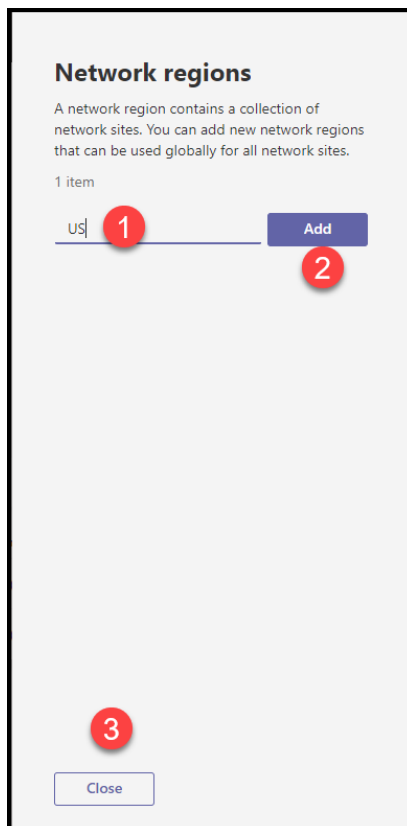


Figure 89 Teams Tenant Network Regions - Configuring

Teams PowerShell

- The Teams PowerShell commands to manage the Tenant Network Regions are:
 - [New-CsTenantNetworkRegion](#)
 - [Get-CsTenantNetworkRegion](#)
 - [Remove-CsTenantNetworkRegion](#)
 - [Set-CsTenantNetworkRegion](#)
- Most customers who are not also implementing Teams LBR or LMO will not have very many Tenant Network Regions to Teams. Manage these regions in the Admin Center instead of through PowerShell
- Tenant Network Regions can be added through the Teams Online PowerShell Module.
- To create a new Tenant Network Region, you will need to use the [New-CsTenantNetworkRegion](#) command.
- If you are going to add these with a PowerShell Script, you will need a Comma Separated Value file with the required information properly formatted.

Teams Tenant Network Site

Teams Admin Center

1. To add a Tenant Network Site through the Teams Admin Center, click on “Locations” then “Network Topology” and click the “Network Sites” tab then the “Add” button.

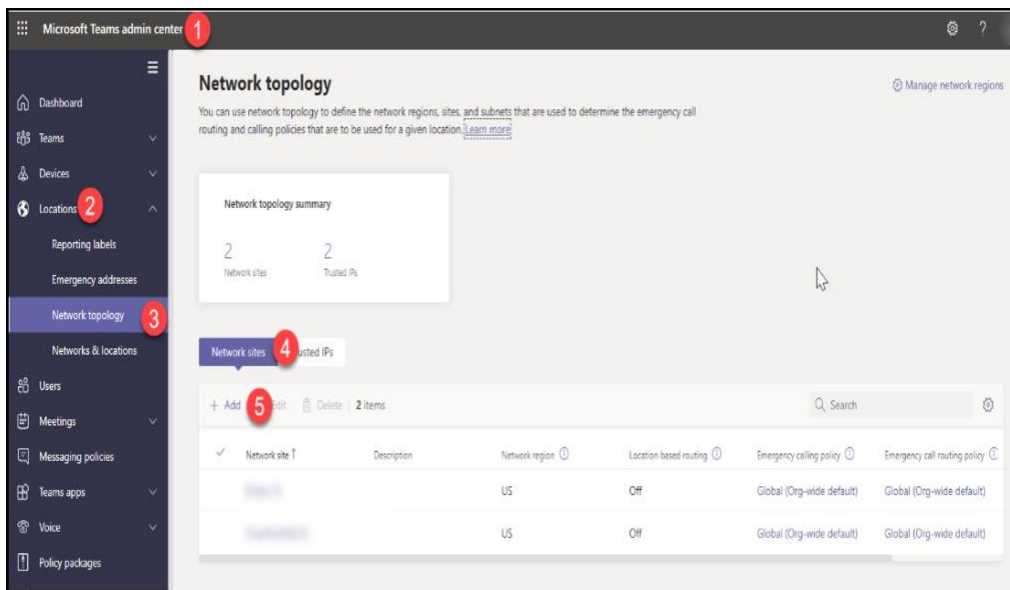


Figure 90 Teams Tenant Network Sites

2. Fill in the form:
 - o Add Network Site – This is the name of the Site.
 - o Description – An optional description.
 - o Add network region – Click the “+” sign and select an existing region or add one.
 - o Emergency calling policy – Select the previously created policy appropriate to the site.
 - o Emergency call routing policy - Select the previously created policy appropriate to the site.
3. Click the “Save” button. The subnets will be added in the next step.

Teams PowerShell

- The Teams PowerShell commands to manage Teams Tenant Network Sites are:
 - [New-CsTenantNetworkSite](#)
 - [Get-CsTenantNetworkSite](#)
 - [Remove-CsTenantNetworkSite](#)
 - [Set-CsTenantNetworkSite](#)
- If you have a lot of Tenant Network Sites to add, consider using the Teams Online PowerShell Module instead of the Teams Admin Center.
- Tenant Network Sites can be added through the Teams Online PowerShell Module.

- If you are going to add these with a PowerShell Script, you will need a Comma Separated Value file with the required information properly formatted.

Teams Tenant Network Subnets

Teams Admin Center

1. To add a Tenant Network Subnet to an existing Tenant Network Site, click on the Site then click the "Add" button.

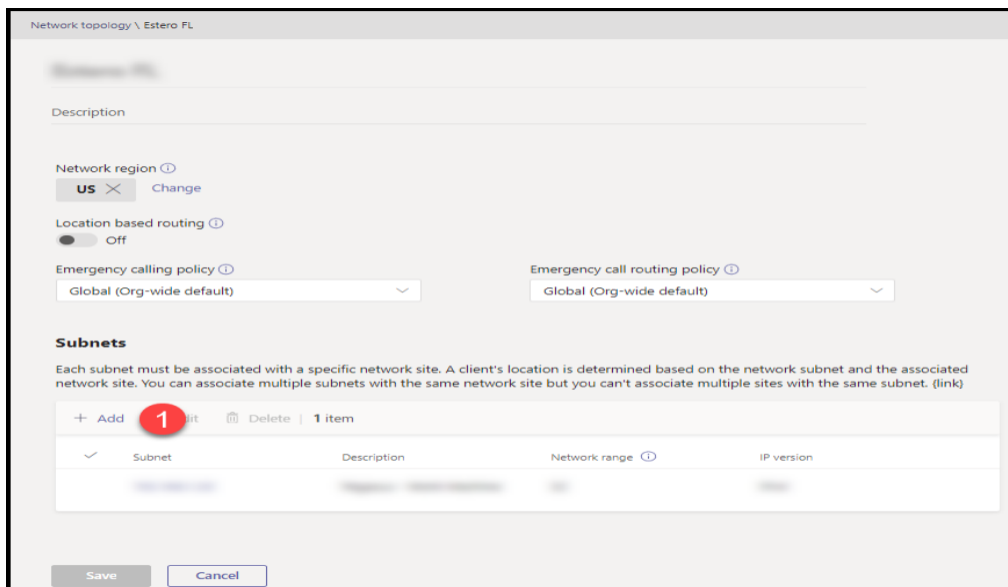


Figure 91 Teams Tenant Network Subnets

2. Fill in the form:
 - IP Version – Select IPv4 or IPv6.
 - IP address – Enter the IP Address of the subnet.
 - Network Range – Enter the subnet mask.
 - Description – Enter a Description providing the location of the subnet.
3. Click the "Apply" button.

Add

Each subnet must be associated with a specific network site. A client's location is determined based on the network subnet and the associated network site. You can associate multiple subnets with the same network site but you can't associate multiple sites with the same subnet.

IP version
IPv4 1

IP address
|xxx 2

Network range ⓘ
Put in a number between 0-32. 3

Description
4

5
Apply Cancel

Figure 92 Teams Tenant Network Subnets - Configuring

Teams PowerShell

- The Teams PowerShell commands to manage Teams Tenant Network Sites are:
 - [New-CsTenantNetworkSubnet](#)
 - [Get-CsTenantNetworkSubnet](#)
 - [Remove-CsTenantNetworkSubnet](#)
 - [Set-CsTenantNetworkSubnet](#)
- If you have a lot of Tenant Network Subnets to add, consider using the Teams Online PowerShell Module instead of the Teams Admin Center.

Teams LIS Network Element General Notes

- There are no “New-Cs” PowerShell commands for any of these elements in the LIS database. If you use the “Set-Cs” command and there is no record for the element and a Location, it will be created. If the record exists, it will be overwritten.
 - There is one very important note about configuring subnets in the LIS Database. When you add a subnet to the LIS Database there is no field for the subnet’s mask. The reason for this is due to how a user’s subnet is identified when placing an emergency services call.
 - When a user makes an emergency services call, the Teams client will gather the IP address and subnet mask configured for the endpoint. The Teams client will use this information to determine the user’s subnet and attempt to match it to an LIS subnet record.
 - For example:
 - A user’s machine has an IP address of 10.1.21.34 with a 23-bit mask (255.255.254.0)
 - Applying the mask to the IP address will result in the IP address falling within the range of 10.1.20.1 through 10.1.21.254 with a subnet ID of 10.1.20.0
 - If you added a subnet record to the LIS database for 10.1.21.0, the endpoint’s IP address and subnet mask would never make a match in the LIS Database
 - For this endpoint, an LIS subnet record for 10.1.20.0 would result in a match
1. To add network elements in the Teams Admin Center, click on “Locations” then “Networks and Locations”. Select the type of element you want to add then click the “Add” button.

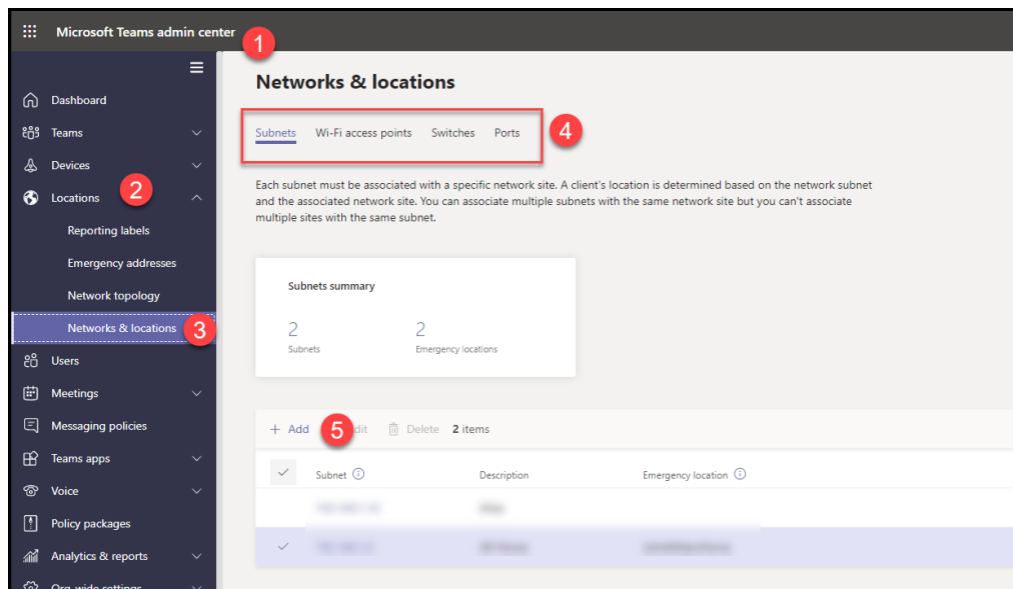


Figure 93 Teams Location Information System (LIS) Network Elements

2. For each element you will need to add:
 - The identifier such as the subnet or the chassis ID of a switch. The subnet element also requires the type of subnet (IPv4 or IPv6) while the Port element requires the switch Chassis ID and Port ID.

- The Location\Place to associate with the element.
 - An optional, but recommended, description of the element.
3. Click the “Apply” button.

Teams LIS Subnets

Teams Admin Center

1. To add subnet network elements, click on “Locations” then “Networks and Locations” then “Subnets” and the “Add” button.

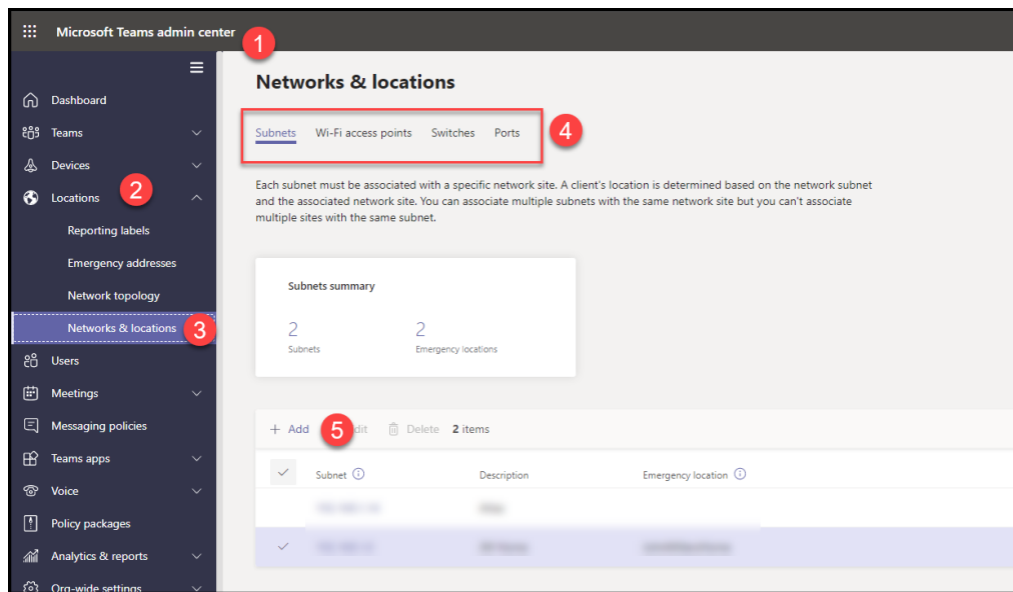


Figure 94 Teams Location Information System (LIS) Subnets

Add subnet

IP version
IPv4

Subnet ⓘ
xxxx

Description
Add a friendly description so you know why it was created

Emergency location
An emergency location is a civic address with an optional place. If your organization has more than one physical location, it's likely that you'll need more than one emergency location. Learn more
Add an emergency location if you want to create a one.

Search by city

Apply Cancel

Figure 95 Teams Location Information System (LIS) Subnets - Configuration

2. Add the values to the appropriate field.
3. Click the "Apply" button.

Teams PowerShell

- The Teams PowerShell commands to manage the Subnet network elements are:
 - [Set-CsOnlineLISSubnet](#)
 - [Get-CsOnlineLISSubnet](#)
 - [Remove-CsOnlineLISSubnet](#)
- There is one very important note about configuring subnets in the LIS Database. When you add a subnet to the LIS Database there is no field for the subnet's mask. The reason for this is due to how a user's subnet is identified when placing an emergency services call.
 - When a user makes an emergency services call, the Teams client will gather the IP address and subnet mask configured for the endpoint. The Teams client will use this information to determine the user's subnet and attempt to match it to an LIS subnet record.
 - For example:
 - A user's machine has an IP address of 10.1.21.34 with a 23-bit mask (255.255.254.0).
 - Applying the mask to the IP address will result in the IP address falling within the range of 10.1.20.1 through 10.1.21.254 with a subnet ID of 10.1.20.0.

- If you added a subnet record to the LIS database for 10.1.21.0, the endpoint's IP address and subnet mask would never make a match in the LIS Database.
- For this endpoint, an LIS subnet record for 10.1.20.0 would result in a match.

Teams LIS Wireless Access Points

Teams Admin Center

1. To add Wireless Access Point network elements, click on “Locations” then “Networks and Locations” then “Wi-Fi Access Points” and the “Add” button.

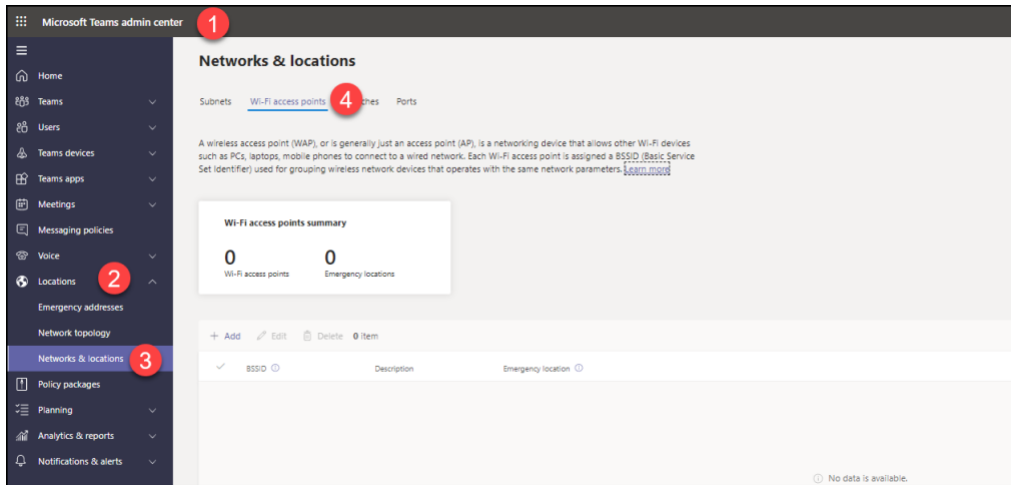


Figure 96 Teams Location Information System (LIS) Wireless Access Points

Figure 97 Teams Location Information System (LIS) Wireless Access Points - Configuration

2. Add the values to the appropriate fields.

- The pairs of characters in the [Basic Service Set Identifiers](#) (BSSID) must be separated by hyphens (“-”).
 - You can use an asterisk (“*”) as a wildcard on the last one or two characters of the BSSID.
3. Click the “Apply” button.

Teams PowerShell

- The Teams PowerShell commands to manage the Wireless Access Point network elements are:
 - [Set-CsOnlineLISWirelessAccessPoint](#)
 - [Get-CsOnlineLISWirelessAccessPoint](#)
 - [Remove-CsOnlineLISWirelessAccessPoint](#)

Teams LIS Network Switches

Teams Admin Center

1. To add switch network elements, click on “Locations” then “Networks and Locations” then “Switches” and the “Add” button.

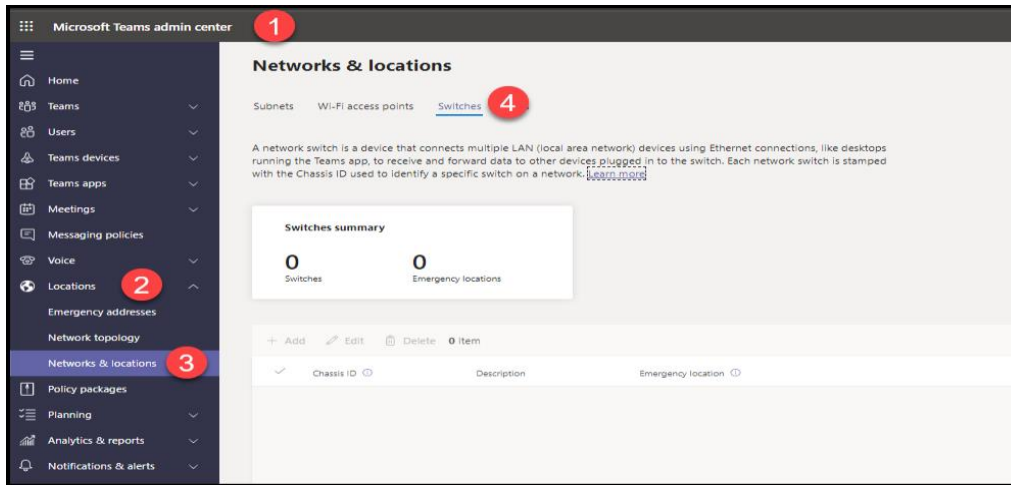


Figure 98 Teams Location Information System (LIS) Network Switches

A screenshot of the 'Add network switch' configuration form. The form has three main sections: 'Chassis ID' with a text input field; 'Description' with a text area and a prompt 'Add a friendly description so you know why it was created'; and 'Emergency location' with a text area, a 'Search by city' dropdown menu, and a search icon. At the bottom of the form, there are 'Apply' and 'Cancel' buttons.

Figure 99 Teams Location Information System (LIS) Network Switches - Configuration

2. Add the values to the appropriate fields.
 - o The pairs of characters in the Chassis ID must be separated by hyphens (" - ").
3. Click the “Apply” button.

Teams PowerShell

- The Teams PowerShell commands to manage the Network Switch network elements are:

[Set-CsOnlineLISSwitch](#)

[Get-CsOnlineLISSwitch](#)

[Remove-CsOnlineLISSwitch](#)

Teams LIS Network Switch Ports

Teams Admin Center

1. To add Switch Port network elements, click on “Locations” then “Networks and Locations” then “Ports” and the “Add” button.

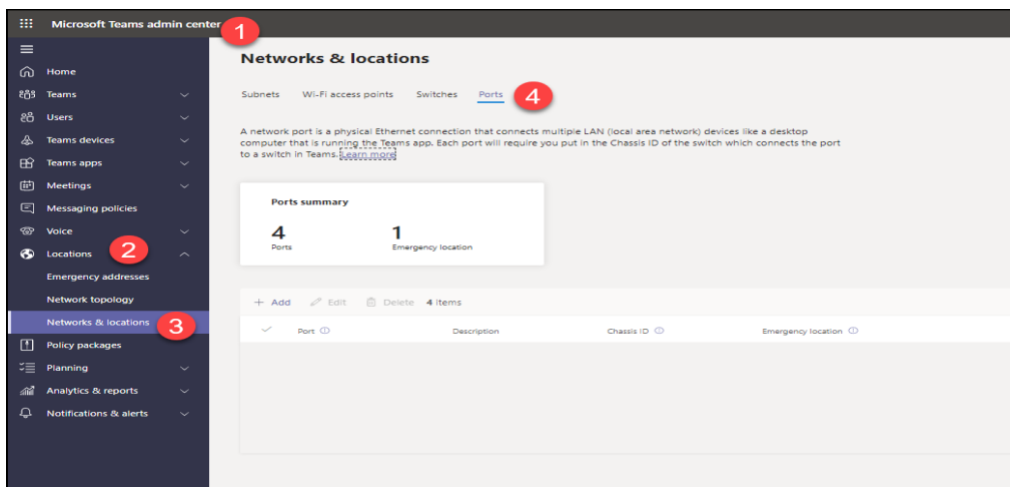


Figure 100 Teams Location Information System (LIS) Network Switch Ports

The 'Add port' form contains the following fields and sections:

- Port**: A text input field.
- Chassis ID**: A text input field.
- Description**: A text area with a placeholder: "Add a friendly description so you know why it was created".
- Emergency location**: A section with a heading and a sub-heading: "An emergency location is a civic address with an optional place. If your organization has more than one physical location, it's likely that you'll need more than one emergency location. Learn more. Add an emergency location if you want to create one." Below this is a "Search by city" dropdown menu and a search input field.
- Buttons**: "Apply" and "Cancel" buttons at the bottom.

Figure 101 Teams Location Information System (LIS) Network Switch Ports - Configuration

2. Add the values to the appropriate fields.

- You cannot add a Port that includes a forward or backward slash through the Teams Admin Center. If your ports have either of these, you will have to add them through Teams PowerShell.
- The pairs of characters in the Chassis ID must be separated by hyphens (“-”).

3. Click the “Apply” button.

Teams PowerShell

- The Teams PowerShell commands to manage the Network Switch Port network elements are:

[Set-CsOnlineLISPort](#)

[Get-CsOnlineLISPort](#)

[Remove-CsOnlineLISPort](#)

Chapter 10 Putting it all together: Example Teams Dynamic 911 Configuration

Fictional Company General Information and Locations

- “Panhandle Consumer Industries” is the name of our fictional company. It is in the “Forgotten Coast” area of the Florida Panhandle.
- It was founded and privately owned by a retired oysterman, Bob Vickers.
- The company has about 1,000 employees. They design, manufacture, sell and ship a variety of products used for cooking and serving the famous Apalachicola oysters for the home market.



Figure 102 PCI Logo

- At any given time, they have about 100 full time remote workers or outside salespeople calling on clients. The salespeople are spread all over the country.
- There are no physical sales or marketing offices outside of the Forgotten Coast.
- The customer has begun documenting their environment in Microsoft Excel workbooks.
- Their primary tenant domain is “panhandleci.onmicrosoft.com” and their primary user domain is “panhandleci.com”.

Risk Management Team

- The company setup a Risk Management Team (RMT). The team is comprised of corporate and external counsel, human resources, and internal security managers. The co-Directors of the team are the Vice-President of Operations, Charles Steadman and the Director of Human Resources, Felicia Gannon.
- The RMT has been tasked with developing a plan to implement and comply with Kari’s Law, the RAY BAUM act and state regulations regarding dynamic 911 for both on and off premises users.

Building Configuration

- The addresses listed are real addresses of other businesses. They have been used as examples because they are actual addresses that could be validated against the Master Street Address Guide (MSAG) and Azure Maps.
- The company has five (5) buildings spread across several towns and about sixty (60) miles east to west:
 1. Headquarters.
 - Located at 1321 Coastal Hwy, Panacea, FL 32346.
 - This building has five (5) floors.
 - The sign at the entrance of the building says:
“Panhandle Consumer Industries”
 - The building is also referred to as “Vickers” or the “Vickers building”.
 2. Manufacturing.
 - Located at 330 US Highway 98, Eastpoint, FL 32328.
 - This building has three (3) floors.
 - “Panhandle Consumer Products” is the name on the building.
 3. Warehouse.
 - Located at 75 Port Leon Drive, Saint Marks, FL 32355.
 - One very large open floor split into three (3) functional areas.
 - A control room referred to as the “bullpen” housing a variable number of seasonal users and endpoints.
 - The building’s sign says “PCI-Logistics”. The employees commonly refer to it as the “Ballpark”.
 4. Research and Development.
 - Located at 55 Rose Street, Sopchoppy, FL 32358.
 - This building has one (1) floor.
 - The building is known as “PCI-Product Development” and known to the employees as “The Lab”.
 5. Customer Service Center.
 - Located at 106 St James Ave NW, Carrabelle, FL 32322.
 - The company occupies the sixth and ninth floors in a multi-tenant corporate building.
 - The building’s directory on the ground floor lists the company’s floors as “PCI-CSC”. The employees refer to it as the “CSC”.



Figure 103 Building Location Map

Building Name	Address	City	State	Zip Code	Floors
Headquarters	1321 Coastal Hwy	Panacea	FL	32346	1 2 3 4 5
Manufacturing	330 US Highway 98	Eastpoint	FL	32328	1 2 3
Research and Development	55 Rose Street	Sopchoppy	FL	32358	1
Customer Service Center	106 St James Ave NW	Carabelle	FL	32322	6 9
WareHouse	75 Port Leon Drive	Saint Marks	FL	32355	1 Bullpen

Figure 104 General Building Information

Telephony Information

- Half of the company’s users are Calling Plan users while the rest are Direct Routing users. When asked, the Chief Information Office (CIO) stated that they had some commitments for the PSTN SIP trunks connected to their Session Border Controllers (SBCs) and had to maintain and pay for these until the end of 2026.
- The client’s users are licensed for:
 - Microsoft Teams.
 - Microsoft Phone System.
 - Microsoft Audio Conferencing.
 - Calling Plan users also have these licenses:
 - Domestic or Domestic and International Calling Plan.
 - Communication Credits

- Contractually, they were able to move half the users, their phone numbers and PSTN traffic off the SIP trunks and port them to Teams Phone System and Calling Plans.
- The Calling Plan users have all been provisioned with the Microsoft Domestic Calling Plan license.
- The Calling Plan and Direct Routing users are randomly distributed amongst the five (5) buildings and the remote users.
- When a user joins the company, they are provided with an available Direct Inward Dial (DID) phone number from the Teams Calling Plan inventory or one of the DID ranges homed on the SIP trunks.
- The users will “keep” their phone numbers throughout their tenure with the company. If a user moves their office from the Headquarters building to the Manufacturing building, they will keep their DID.
- There are two (2) Teams Direct Routing SBCs. One is in the Headquarters building and the other is in the Warehouse.
 - hqdrsbc.panhandleci.com.
 - whdrsbc.panhandleci.com.
- The Teams Voice Routing Policies have been configured to provide resiliency should one of the SBCs fail.
- There is one (1) twenty-four (24) port SIP to Analog gateway, also known as an Analog Telephone Adapters (ATAs), in each of the company’s buildings. The ATAs in the Headquarters, Manufacturing, R&D or Customer Service Center buildings route their calls to and from the Headquarters Direct Routing SBC. The Warehouse ATA routes it’s calls through the Warehouse SBC.

Wide Area Network Configuration

- There are separate subnets for user data and user voice.
- The peer-to-peer and Public Switched Telephony Network (PSTN) audio traffic for the on-premises Teams Desktop and Web client users run on data subnets.
- Teams physical phones, Common Area Phones and Conference Room devices are connected to voice subnets.
- The five (5) buildings are well connected over a mature fully redundant wide area network (WAN).
- Except for the WAN links, DMZ and server subnets, the user data and voice subnets in the buildings never span buildings.
- Based on this, there will always be at least two (2) user subnets in each of the five (5) buildings; one for data and one for voice traffic.

Local Area Network Configuration

Wired

Offices

- When designing the network plan for the buildings, the decision was made that user data and voice subnets would never physically span more than one (1) floor. The Headquarters building started out with five (5) data and five (5) voice subnets.
- Some of the buildings have required more than one (1) data or voice subnet per floor.
 - These additional subnets were added based on the demand for IP addresses.

- In other words, when all the available IP addresses in the original data subnet have been used up, a second data subnet for the floor was added.
- Two (2) users sitting next to each other could have IP addresses on different data and/or voice subnets.
- The second and fourth floors of the Headquarters building have each required additional data and voice subnets.
- Network switches in the buildings are found in wiring closets on each of the floors. Devices on each floor are only connected to switches in their floor's wiring closet.

Warehouse

- The Warehouse is a huge single floor building. The building has three (3) clearly defined physical areas:
 - Shipping
 - Receiving
 - On Hand Inventory
- It has a control room referred to as the "Bullpen". This space houses the Warehouse's Security Desk and a seasonally changing number of devices and users.
- The Warehouse was initially setup with a single data and a single voice subnet available to devices in all three (3) areas.
- The Bullpen was added later and has been setup with its own data and voice subnets.
- The network design for the Warehouse floor specifies that network switches are dedicated to specific quadrants. Devices located in the North quadrant will only be connected to North Quadrant switches.
- Devices in the Bullpen can be connected to any switch, regardless of quadrant, that has an available port.
- There is a single wiring closet\data center through which all network connections are terminated.
- Users and devices on the Warehouse floor all use addresses in the same subnet(s).
- Bullpen devices use different subnets than those provisioned for the Warehouse floor devices.

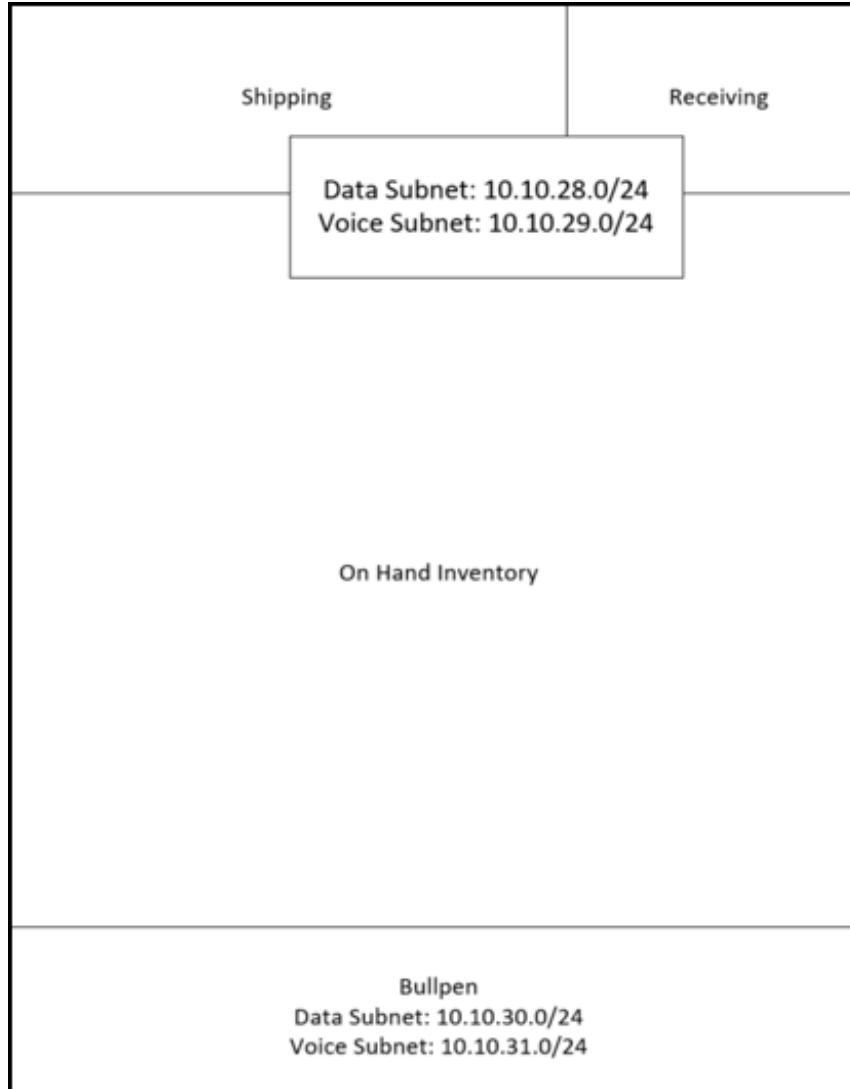


Figure 105 Warehouse – Subnets

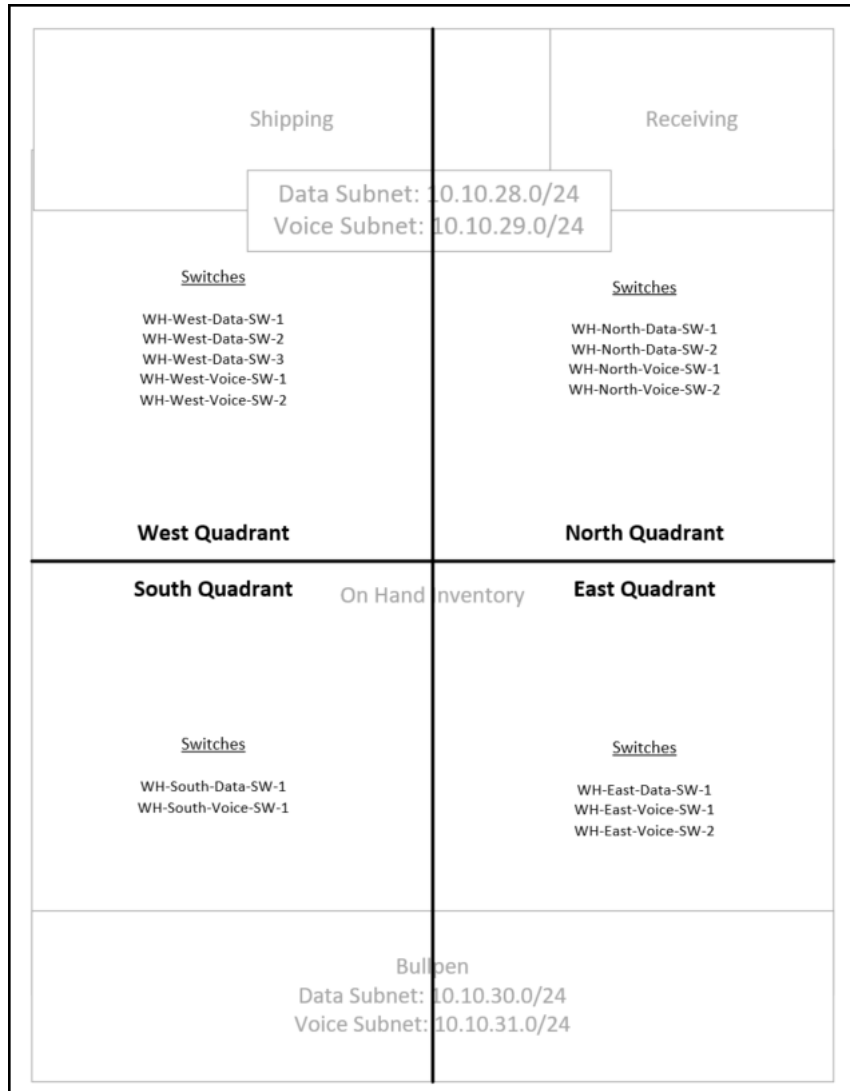


Figure 106 Warehouse - Quadrants and Network Switches

Building	Floor	Type	Subnet Name	Subnet	Mask
Headquarters	1	Data	HQ-1-Data-Alpha	10.10.2.0	24
	1	Voice	HQ-1-Voice-Alpha	10.10.3.0	24
	2	Data	HQ-2-Data-Alpha	10.10.4.0	24
	2	Voice	HQ-2-Voice-Alpha	10.10.5.0	24
	2	Data	HQ-2-Data-Bravo	10.10.6.0	24
	2	Voice	HQ-2-Voice-Bravo	10.10.7.0	24
	3	Data	HQ-3-Data-Alpha	10.10.8.0	24
	3	Voice	HQ-3-Voice-Alpha	10.10.9.0	24
	4	Data	HQ-4-Data-Alpha	10.10.10.0	24
	4	Voice	HQ-4-Voice-Alpha	10.10.11.0	24
	4	Data	HQ-4-Data-Bravo	10.10.12.0	24
	4	Voice	HQ-4-Voice-Bravo	10.10.13.0	24
Manufacturing	5	Data	HQ-5-Data-Alpha	10.10.14.0	24
	5	Voice	HQ-5-Voice-Alpha	10.10.15.0	24
	1	Data	MA-1-Data-Alpha	10.10.16.0	24
	1	Voice	MA-1-Voice-Alpha	10.10.17.0	24
	2	Data	MA-2-Data-Alpha	10.10.18.0	24
	2	Voice	MA-2-Voice-Alpha	10.10.19.0	24
R & D	3	Data	MA-3-Data-Alpha	10.10.20.0	24
	3	Voice	MA-3-Voice-Alpha	10.10.21.0	24
	1	Data	RD-1-Data-Alpha	10.10.22.0	24
Customer Service Center	1	Voice	RD-1-Voice-Alpha	10.10.23.0	24
	6	Data	CS-6-Data-Alpha	10.10.24.0	24
	6	Voice	CS-6-Voice-Alpha	10.10.25.0	24
	9	Data	CS-9-Data-Alpha	10.10.26.0	24
Warehouse	9	Voice	CS-9-Voice-Alpha	10.10.27.0	24
	1	Data	WH-1-Data-Alpha	10.10.28.0	24
	1	Voice	WH-1-Voice-Alpha	10.10.29.0	24
	Bullpen	Data	WH-Bullpen-Data-Alpha	10.10.30.0	24
	Bullpen	Voice	WH-Bullpen-Voice-Alpha	10.10.31.0	24

Figure 107 Wired Subnet Inventory

Wireless

- The company owns Wireless Access Points (WAP) and their supporting hardware and software. All equipment and software were purchased from a single manufacturer.
- The coverage pattern for most WAPs is spherical in shape. In a multi-floor building this coverage could extend to the floor the WAP is on and the floors above and below.
- The WAPs that were purchased allow for the coverage shape to be modified.
- The vendor was able to help the company shape the coverage pattern of the WAPs to not extend to other floors.
- The company has provided instructions to their users to only connect to the Wi-Fi network for the floor that they are currently located on. The users are also instructed to not setup these networks to be automatically connected to their computers.
- Due to the difficulty in a Wi-Fi user determining which Warehouse quadrant they are in, Wi-Fi users on the Warehouse floor are permitted to automatically connect to any of the available quadrant wireless networks. The network team has verified that as users move from quadrant to quadrant, their devices automatically connect to one of the quadrant’s WAPs. They should not connect to either of the Bullpen’s WAPs while on the Warehouse floor.
- Each floor has at least two (2) WAPs. The Warehouse has two (2) WAPs in each quadrant and two (2) in the Bullpen.

- Each floor has its own wireless data subnet. The Headquarters building, for example, with five (5) floors started out with five (5) wireless subnets and ten (10) WAPs.
- The WAPS on a floor were initially configured to provide IP addresses through the Dynamic Host Configuration Protocol (DHCP) for a single subnet.
- Based on the demand for addresses, additional subnets were provisioned and assigned to the DHCP servers for a given floor's WAPs.
- The 3rd floor of the Headquarters building, and the 9th floor of the Customer Services location have both required the provisioning of additional Wi-Fi subnets.
- In the Warehouse, each quadrant has been assigned two (2) WAPs.
 - The coverage of the WAPs has been tailored to the shape of the quadrant.
 - The Warehouse started out with a single Wi-Fi subnet for all the quadrants.
 - They have since added two (2) additional subnets.
- The Warehouse Bullpen also has two (2) WAPs with shaped coverage providing addresses for a single subnet.

Building	Floor	Type	Subnet Name	Subnet	Mask
Headquarters	1	WLAN	HQ-1-Data-WLAN-Alpha	10.10.50.0	24
	2	WLAN	HQ-2-Data-WLAN-Alpha	10.10.51.0	24
	3	WLAN	HQ-3-Data-WLAN-Alpha	10.10.52.0	24
	3	WLAN	HQ-3-Data-WLAN-Bravo	10.10.53.0	24
	4	WLAN	HQ-4-Data-WLAN-Alpha	10.10.54.0	24
Manufacturing	5	WLAN	HQ-5-Data-WLAN-Alpha	10.10.55.0	24
	1	WLAN	MA-1-Data-WLAN-Alpha	10.10.56.0	24
	2	WLAN	MA-2-Data-WLAN-Alpha	10.10.57.0	24
R & D	3	WLAN	MA-3-Data-WLAN-Alpha	10.10.58.0	24
	1	WLAN	RD-1-Data-WLAN-Alpha	10.10.59.0	24
Customer Service Center	6	WLAN	CS-6-Data-WLAN-Alpha	10.10.60.0	24
	9	WLAN	CS-9-Data-WLAN-Alpha	10.10.61.0	24
	9	WLAN	CS-9-Data-WLAN-Bravo	10.10.62.0	24
Warehouse	1	WLAN	WH-1-Data-WLAN-Alpha	10.10.63.0	24
	1	WLAN	WH-1-Data-WLAN-Bravo	10.10.64.0	24
	1	WLAN	WH-1-Data-WLAN-Charlie	10.10.65.0	24
	Bullpen	WLAN	WH-Bullpen-Data-WLAN-Alpha	10.10.66.0	24

Figure 108 Wireless Subnets

Building	Floor	WAP Name	BSSID	Subnets	
Headquarters	1	HQ-1-WAP-Alpha	D6-41-B8-19-79-FF	10.10.50.0/24	
	1	HQ-1-WAP-Bravo	8A-BF-11-84-69-C7		
	2	HQ-2-WAP-Alpha	ED-87-FC-47-C2-D5	10.10.51.0/24	
	2	HQ-2-WAP-Bravo	65-3C-E7-A1-64-37		
	3	HQ-3-WAP-Alpha	DF-4B-8D-8A-C5-49	10.10.52.0/24 10.10.53.0/24	
	3	HQ-3-WAP-Bravo	C5-D8-79-16-34-53		
	4	HQ-4-WAP-Alpha	8D-A1-35-6B-D5-FC	10.10.54.0/24	
	4	HQ-4-WAP-Bravo	CD-84-67-4B-33-87		
5	HQ-5-WAP-Alpha	E5-EE-E2-C8-46-34	10.10.55.0/24		
5	HQ-5-WAP-Bravo	88-27-A9-B7-C1-F3			
Manufacturing	1	MA-1-WAP-Alpha	F3-CF-40-4F-7C-8E	10.10.56.0/24	
	1	MA-1-WAP-Bravo	53-FC-48-EE-E5-EA		
	2	MA-2-WAP-Alpha	C6-C6-97-15-41-AF	10.10.57.0/24	
	2	MA-2-WAP-Bravo	1F-9B-A8-E3-D4-3A		
	3	MA-3-WAP-Alpha	88-36-B5-8E-18-AB	10.10.58.0/24	
	3	MA-3-WAP-Bravo	ED-F0-E9-C8-E2-21		
R & D	3	RD-3-WAP-Alpha	E4-2C-CB-15-A6-41	10.10.59.0/24	
	3	RD-6-WAP-Bravo	95-42-C7-D7-D9-AA		
Customer Service Center	6	CS-6-WAP-Alpha	BE-D4-F0-5D-23-F6	10.10.60.0/24	
	6	CS-6-WAP-Bravo	8E-99-D3-31-58-86		
	9	CS-9-WAP-Alpha	58-58-12-E8-CD-99	10.10.61.0/24 10.10.62.0/24	
	9	CS-9-WAP-Bravo	F3-64-D1-AB-11-27		
Warehouse	1N	WH-1N-WAP-Alpha	57-27-C5-EB-72-B4	10.10.63.0/24 10.10.64.0/24 10.10.65.0/24	
	1N	WH-1N-WAP-Bravo	B0-73-18-7A-DB-EC		
	1S	WH-1S-WAP-Alpha	17-B9-47-54-33-30		
	1S	WH-1S-WAP-Bravo	60-DF-4C-F4-3C-9A		
	1E	WH-1E-WAP-Alpha	53-D5-DB-39-84-B8		
	1E	WH-1E-WAP-Bravo	88-41-54-2C-FA-5E		
	1W	WH-1W-WAP-Alpha	44-A2-80-D0-15-9B		
	1W	WH-1W-WAP-Bravo	11-BD-37-D8-CE-91		
	Bullpen	WH-Bullpen-WAP-Alpha	C2-8E-35-D7-2A-B9		10.10.66.0/24
	Bullpen	WH-Bullpen-WAP-Bravo	48-FC-6D-A1-17-35		

Figure 109 Wireless Access Points

Internet Connectivity

- There are three (3) perimeter devices on their wide area network (WAN) that provide users and servers with Internet and Microsoft Teams access.
- The company uses two (2) different Internet Service Providers (ISPs). The routers in the Headquarters building are connected to different ISPs while the router in the Warehouse is connected to the “Primary” ISP.
- The ISPs have enabled static IPv6 addresses on all three (3) circuits:

Building	Router Name	Internet Facing Addresses			
		IPv4 Address	IPv4 Subnet Mask	IPv6 Address	IPv6 Subnet Mask
Headquarters	HQ ISP Prime	169.45.21.8	29	2603:49:cd12:fc00::1	64
	HQ ISP Secondary	187.52.35.4	32	2001:4898:e8:25:844e:926f:85ad:dd8e	128
Warehouse	WH Prime	169.45.21.16	29	2703:50:cd12:fc00::1	64

Figure 110 Direct Internet Access Information

Teams Telephony Configuration

- The company has both Microsoft Teams Calling Plan and Teams Direct Routing users.

- There are two (2) Teams Direct Routing SBCs. One is in the Headquarters building and the other is in the Warehouse.
- 75% of the company's users are setup with Teams Calling Plans while the rest are Direct Routing users.

Corporate Security

- Each of the buildings has its own Security Desk and personnel.
- The Customer Service location has a Security Desk on both the sixth and ninth floors.
- The Security personnel at the Customer Service location work closely with the building's own personnel.

PCI Dynamic 911 Calling Requirements

Dispatchable Locations

- The State of Florida statute 365.175 "Emergency telephone number 911 private branch exchange-private switch automatic location identification" became effective for Public Branch Exchange" systems installed after January 1, 2004. It states that:
 - "Each PBX system installed after January 1, 2004, must be capable of providing automatic location identification to the station level"
- The RMT have assessed that this statute does not address dynamic 911. It appears to be limited to requiring static automatic line identification (ALI).
- There are no additional local ordinances related to emergency services calling in any of the towns in which PCI has offices.
- Looking beyond the requirement of the RAY BAUM act to:
 - "Provide the validated street address of the calling party, plus additional information such as suite, apartment or similar information necessary to adequately identify the location of the calling party"
- The RMT have determined that when a user makes an emergency call from the Headquarters, Manufacturing, R&D or Customer Service Center buildings, the dispatchable location should provide the floor in the building that they are placing the call from.
- Calls made from data centers, machine\equipment rooms and wiring closets should clearly provide the floor and name of the room in the dispatchable location.
- Calls from Teams users in the very large single-story Warehouse should provide a dispatchable location in the Warehouse based on a quadrant.
- The floor of the Warehouse is divided into North, South, East, and West quadrants.
- There is no correlation between the subnets and the quadrants.
- Calls from devices in the "Bullpen" will be identified as coming from the "Bullpen".

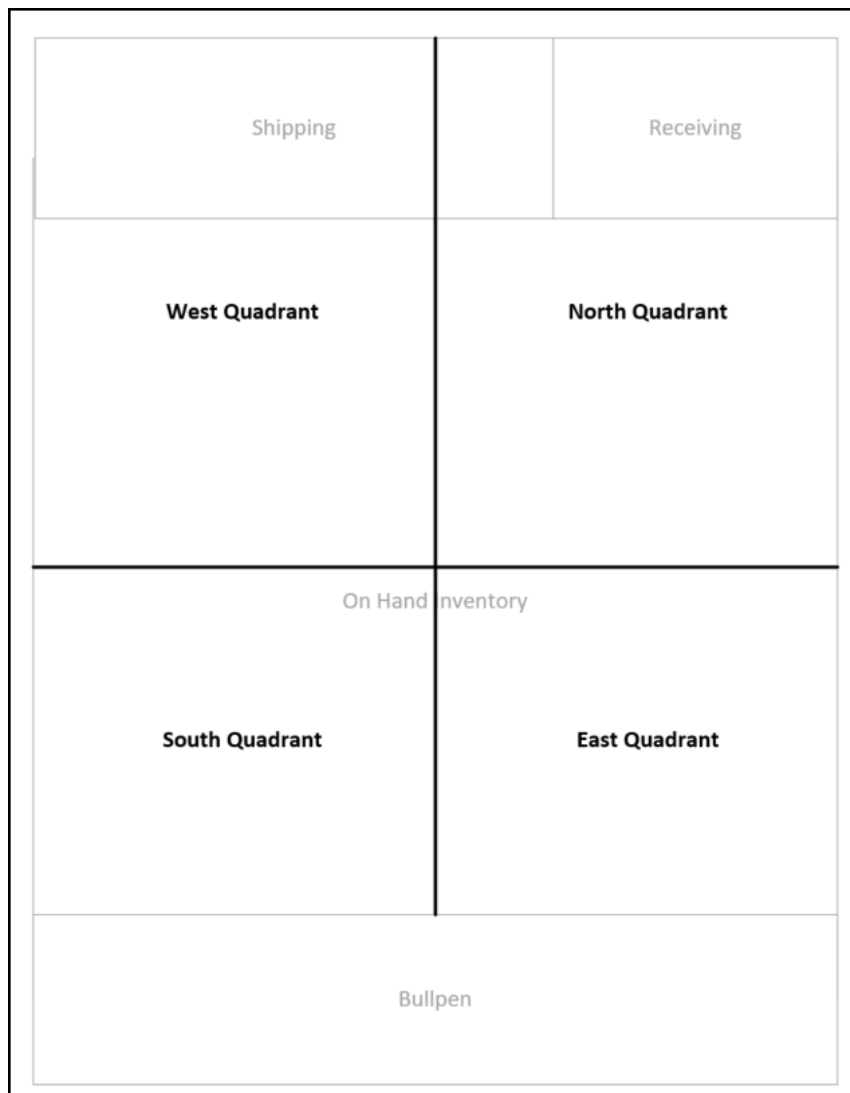


Figure 111 Warehouse Building with Dispatchable Location Quadrants

Analog Devices

- The Analog devices connected to the ATAs never move.
- The RMT requires that dispatchable locations be provided when calls are made to emergency services from all analog devices.
- The devices should use the previously provided level of precision based on their locations. The alarm systems and environmental monitoring equipment using analog circuits will never place calls to a Public Safety Answering Point (PSAP).

Work from Home and Externally Signed on Users

- The RMT have directed that Dynamic 911 for Work from Home must be configured and supported.

Emergency Call Notifications

- The RMT wants emergency call notifications to be routed to the security desks in each of the buildings for calls placed by users connected to subnets in the building.
- The RMT also wants the building's Security Desk at the Customer Service location to be advised when a Customer Service user makes an emergency services call.
- The parties receiving the notification should be conferenced into the call being made to emergency services. They should be initially muted, but able to unmute as needed.
- The RMT understands that notification participants contacted through a phone number will not be able to unmute while joined to an emergency services call.
- Emergency Call notification policies should not be statically assigned to the users. Users should be dynamically provisioned with a policy based on the corporate location where they have signed on to Microsoft Teams.
- The Vice President, Charles Steadman, the Director of Human Resources, Felicia Gannon and the Director of Security, Samuel Bard, are to receive all emergency call notifications as well.

Emergency Call Routing for the Direct Routing Users

- The RMT wants there to be SBC resiliency when a Direct Routing user places a call to emergency services.
- The Emergency Call Routing policies should not be statically assigned to the users. Users should be dynamically provisioned with a policy based on the corporate location from where they have signed on to Microsoft Teams.

Teams Dynamic 911 Configuration

- The RMT presented their findings and recommendations at the end of 2019. They were approved by the Board of Directors.
- The RMT passed the findings to the Chief Information Officer (CIO), Jonathan Sperling, and asked him to present a detailed implementation plan to the RMT by the end of the second quarter of 2020.
- While developing the plan with his team, the CIO instructed his Information Technology (IT) team to:
 - Determine how to implement the design.
 - Gather and create the detailed information necessary to execute the design.
 - Provide a timeline starting on August 1, 2020, for deploying the solution and completing it before the end of the year.
 - Comply with Kari's Law, all parts of the RAY BAUM Act and all applicable State and local relevant requirements.
 - "Work smarter, not harder" and take advantage of tools such as PowerShell scripting to help speed up the installation.

High Level Process

1. Meet with the internal training resources to discuss user documentation and training for Teams Dynamic 911 and Dynamic 911 for Work from Home.

2. Solicit proposals from Emergency Response Service Providers (ERSPs) to provide Dynamic 911 routing for the Teams Direct Routing users.
3. Setup and test the interface between the SBCs and ERSP.
4. Gather the locations and phone numbers of the on-premises analog devices.
5. Add this information to the ERSP's Automatic Line Identification (ALI) system.
6. Add any missing Teams Emergency Addresses. Some, if not all, may already be there. They may have been created when the Calling Plan users were setup.
 - Confirm all building addresses.
 - Acquire accurate Geocodes (latitude and longitude) for each building.
7. Add any missing Teams Emergency Places to the Emergency Addresses.
 - Some, if not all, may already be there. They may have been created when the Calling Plan users were setup.
8. Update as needed, the address of record (Teams Place\Location) assigned to the Calling Plan users.
 - They should have a location reflecting the floor or quadrant of their "permanent" office location.
9. Determine the quantity of composition of Emergency Calling Policies. Add them to Teams.
 - Organize the notification entities\targets.
 1. Get the phone numbers of the external parties who will be notified through their phone numbers, i.e., the building's Security Desk in the building occupied by the Customer Service Center.
 2. Create Office 365, or other types of groups, to cover the in-house notification entities
 - Security Desks in each building.
 - RMT Oversight Group.
 - VP of Operations.
 - Director of Human Resources.
 - Director of Security.
 - Add the policies to Teams.
 - Using the Teams PowerShell module, enable Dynamic Work from Home on each policy.
10. Determine the number of Emergency Call Routing Policies needed.
 - Add usages and routes as needed to Teams.
 - Create the Emergency Call Routing Policies.
 - Verify that the Teams Voice Policies include emergency services routing rules. These would be used by Teams clients, such as the web client, that do not support Teams Dynamic 911.
11. Add the Teams Trusted IP addresses to Teams.
12. Create the Teams Network Region(s).
13. Create Teams Tenant Network Sites.
 - Assign the appropriate Teams Emergency Calling policy to each site.
 - Assign the appropriate Teams Emergency Call Routing policy to each site.
 - Create the Teams Tenant Network Subnets and add them to the Teams Tenant Network Sites.
14. Add the Location Information System (LIS) network element records to Teams assigning the correct locations.
 - Subnets.

- Wireless Access Points.
 - Switches.
 - Ports.
15. Test Dynamic 911.
- Verify that a dynamic 911 location can be determined from every on-premises network location throughout the company.
16. Test Dynamic 911 for Work from Home.
- Verify that it is working properly.
 - Ensure that anyone using Teams remotely is verifying their current locations when starting up the Teams client.
17. Modify the address of record for the Teams Calling Plan full time Work from Home users.
- Determine or define a “permanent” on-premises building to assign to each user.
 - Assign the default or front door location of the building to each user and their Calling Plan phone number.
 - Remove any locations\places and emergency addresses representing the home addresses of the Work from Home users. These addresses are not necessary when Dynamic 911 for Work from Home is working properly.

Emergency Response Service Provider (ERSP)

- The company decided to take advantage of the SIP Trunk provider’s option to add ERSP functionality to the configuration of the existing SIP Trunks.
- The company will be able to create static Automatic Line Identification (ALI) records for the analog devices attached to the ATAs.
- This addon service will enable the SIP Trunks to route calls from the Teams Direct Routing users to the PSAP or an Emergency Call Response Center (ECRC).
 - The SIP Trunk Provider will route calls to the appropriate PSAP based on the PIDF-LO information transmitted by Teams to the SBC.
 - Absent PIDF-LO information, such as for calls coming from the analog devices, the ERSP will attempt to determine the caller’s location using the ALI information.
- The company decided against using Emergency Line Identification Numbers (ELIN) for this purpose.

Emergency Addresses

- The addresses of the five (5) Corporate buildings were verified. The Geocodes for each of the buildings was retrieved from Azure Maps.
- Emergency Address records for each of the five (5) buildings were created or updated in the Teams Admin Center. The Geocodes for any existing records were verified.

Organization Name	Description	House Number	House Number Suffix	Pre-Directional	Street Name	Street Suffix	Post Directional	City	State	Country	Zip Code	Latitude	Longitude
Panhandle Consumer Industries	Vickers-Headquarters	1321			Coastal Hwy			Panacea	FL	US	32346	30.0270645	-84.3899317
Panhandle Consumer Industries	Manufacturing	330			US Highway 98			Eastpoint	FL	US	32328	29.7361794	-84.881201
PCI-Product Development	The Lab - R&D	55			Rose Street			Sopchoppy	FL	US	32358	30.0611246	-84.491716
PCI-CSC	CSC-Customer Service	106			St James Ave		NW	Carabelle	FL	US	32322	29.8510135	-84.6650561
PCI-Logistics	Ballpark	75			Port Leon Drive			Saint Marks	FL	US	32355	30.190515	-84.2156192

Figure 112 Teams Emergency Addresses – Summary Table

```

CompanyName,Description,HouseNumber,HouseNumberSuffix,PreDirectional,Streetname,StreetSuffix,PostDirectional,City,StateOrProvince,CountryOrRegion,PostalCode,Latitude,Longitude
Panhandle Consumer Industries,Vickers-Headquarters,1321,,,Coastal Hwy,,,Panacea,FL,US,32346,30.0270645,-84.3899317
Panhandle Consumer Industries,Manufacturing,330,,,US Highway 98,,,Eastpoint,FL,US,32328,29.7361794,-84.881201
PCI-Product Development,The Lab - R&D,55,,,Rose Street,,,Sopchoppy,FL,US,32358,30.0611246,-84.491716
PCI-CSC,CSC-Customer Service,106,,,St James Ave,,NW,Carabelle,FL,US,32322,29.8510135,-84.6650561
PCI-Logistics,Ballpark,75,,,Port Leon Drive,,,Saint Marks,FL,US,32355,30.190515,-84.2156192

```

Figure 113 Teams Emergency Addresses - CSV Input File

Emergency addresses

Emergency address is a civic address which is a physical street address of a place of business for your organization. An emergency location is a civic address with an optional place. If your business has more than one physical location, it's likely that you'll need more than one emergency location. [Learn more](#)

+ Add Edit Delete

✓	Description	Country or region	Address	Phone numbers	Voice users	Address status ⓘ	Organization name ↓
	The Lab - R&D	United States	55 Rose Street, Sopchoppy FL 32358, US	0	0	Validated	PCI-Product Development
	Ballpark	United States	75 Port Leon Drive, Saint Marks FL 32355, US	0	0	Validated	PCI-Logistics
	CSC-Customer Service	United States	106 St James Avenue NW, Carrabelle FL 32322, US	0	0	Validated	PCI-CSC
	Vickers-Headquarters	United States	1321 Coastal Highway, Panacea FL 32346, US	0	0	Validated	Panhandle Consumer Industries
	Manufacturing	United States	330 US Highway 98, Eastpoint FL 32328, US	0	0	Validated	Panhandle Consumer Industries

Figure 114 Teams Emergency Addresses

Places\Locations

- Based on the requirements, twenty-eight (28) Teams Places were added. PowerShell was used to add the records:

Description	Organization Name	Place	ELIN	Teams Values
				CivicAddress ID
Vickers-Headquarters	Panhandle Consumer Industries	Floor 1		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 1 - Data Center		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 2		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 2 - Wiring Closet		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 3		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 3 - Wiring Closet		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 4		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 4 - Wiring Closet		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 5		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Vickers-Headquarters	Panhandle Consumer Industries	Floor 5 - Wiring Closet		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772
Manufacturing	Panhandle Consumer Industries	Floor 1		d9e1fa53-33a7-44a4-abaf-37714a6b367b
Manufacturing	Panhandle Consumer Industries	Floor 1 - Data Center		d9e1fa53-33a7-44a4-abaf-37714a6b367b
Manufacturing	Panhandle Consumer Industries	Floor 2		d9e1fa53-33a7-44a4-abaf-37714a6b367b
Manufacturing	Panhandle Consumer Industries	Floor 2 - Wiring Closet		d9e1fa53-33a7-44a4-abaf-37714a6b367b
Manufacturing	Panhandle Consumer Industries	Floor 3		d9e1fa53-33a7-44a4-abaf-37714a6b367b
Manufacturing	Panhandle Consumer Industries	Floor 3 - Wiring Closet		d9e1fa53-33a7-44a4-abaf-37714a6b367b
The Lab - R&D	PCI-Product Development	Floor 1		0d99f93b-747a-455e-b2bc-d224aeb9ce90
The Lab - R&D	PCI-Product Development	Floor 1 - Data Center		0d99f93b-747a-455e-b2bc-d224aeb9ce90
CSC-Customer Service	PCI-CSC	Floor 6		00d751d1-e39a-464b-867c-8f73828b139b
CSC-Customer Service	PCI-CSC	Floor 6 - Data Center		00d751d1-e39a-464b-867c-8f73828b139b
CSC-Customer Service	PCI-CSC	Floor 9		00d751d1-e39a-464b-867c-8f73828b139b
CSC-Customer Service	PCI-CSC	Floor 9 - Wiring Closet		00d751d1-e39a-464b-867c-8f73828b139b
Ballpark	PCI-Logistics	Floor 1N		cb3faa9b-1aed-46c8-9995-64f5e681ef56
Ballpark	PCI-Logistics	Floor 1S		cb3faa9b-1aed-46c8-9995-64f5e681ef56
Ballpark	PCI-Logistics	Floor 1E		cb3faa9b-1aed-46c8-9995-64f5e681ef56
Ballpark	PCI-Logistics	Floor 1W		cb3faa9b-1aed-46c8-9995-64f5e681ef56
Ballpark	PCI-Logistics	Bullpen		cb3faa9b-1aed-46c8-9995-64f5e681ef56
Ballpark	PCI-Logistics	Ballpark - Data Center		cb3faa9b-1aed-46c8-9995-64f5e681ef56

Figure 115 Teams Place Records – Summary Table

CivicAddressID,Location,ELIN
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 1
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 1 - Data Center
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 2
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 2 - Wiring Closet
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 3
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 3 - Wiring Closet
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 4
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 4 - Wiring Closet
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 5
7c81ade3-6e35-4cc2-8feb-98e1ca4ec772,Floor 5 - Wiring Closet
d9e1fa53-33a7-44a4-abaf-37714a6b367b,Floor 1
d9e1fa53-33a7-44a4-abaf-37714a6b367b,Floor 1 - Data Center
d9e1fa53-33a7-44a4-abaf-37714a6b367b,Floor 2
d9e1fa53-33a7-44a4-abaf-37714a6b367b,Floor 2 - Wiring Closet
d9e1fa53-33a7-44a4-abaf-37714a6b367b,Floor 3
d9e1fa53-33a7-44a4-abaf-37714a6b367b,Floor 3 - Wiring Closet
0d99f93b-747a-455e-b2bc-d224aeb9ce90,Floor 1
0d99f93b-747a-455e-b2bc-d224aeb9ce90,Floor 1 - Data Center
00d751d1-e39a-464b-867c-8f73828b139b,Floor 6
00d751d1-e39a-464b-867c-8f73828b139b,Floor 6 - Data Center
00d751d1-e39a-464b-867c-8f73828b139b,Floor 9
00d751d1-e39a-464b-867c-8f73828b139b,Floor 9 - Wiring Closet
cb3faa9b-1aed-46c8-9995-64f5e681ef56,Floor 1N
cb3faa9b-1aed-46c8-9995-64f5e681ef56,Floor 1S
cb3faa9b-1aed-46c8-9995-64f5e681ef56,Floor 1E
cb3faa9b-1aed-46c8-9995-64f5e681ef56,Floor 1W
cb3faa9b-1aed-46c8-9995-64f5e681ef56,Bullpen
cb3faa9b-1aed-46c8-9995-64f5e681ef56,Ballpark - Data Center

Figure 116 Teams Locations/Places - CSV Input File

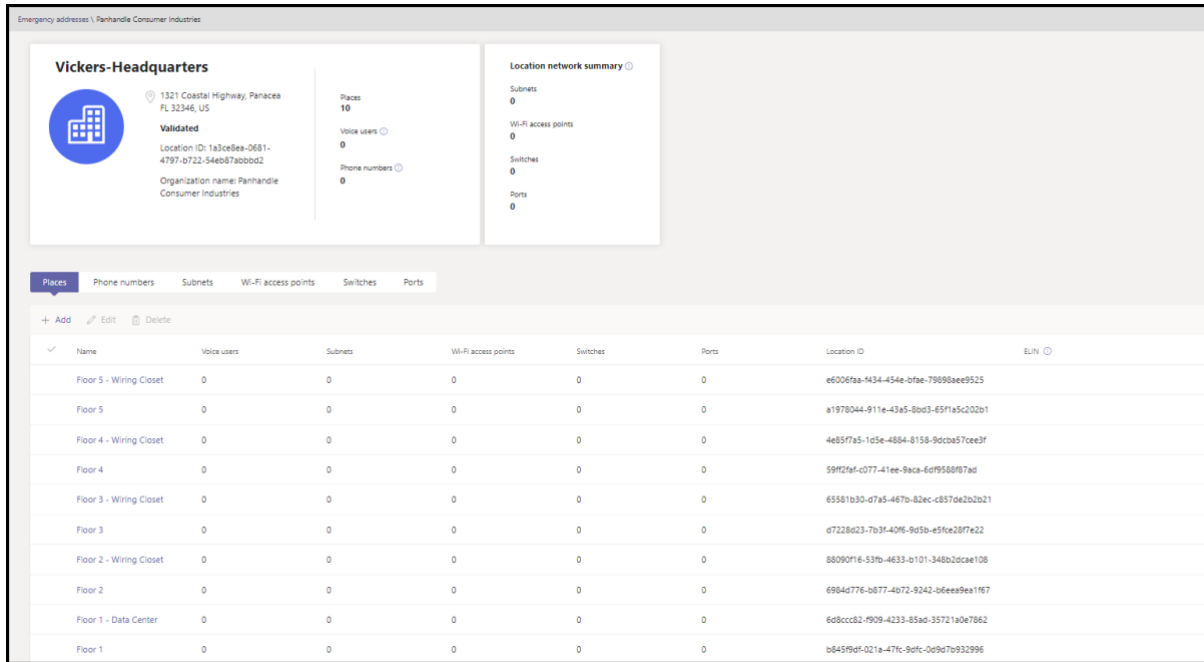


Figure 117 Teams Place Records - Vickers-Headquarters Building

Emergency Call Routing Policies

- The Emergency Call Routing Policies are only applicable to the Teams Direct Routing users.
- PCI wants to route all Emergency Service calls from the Headquarters, R & D and Customer Service Center buildings to the Headquarters SBC and if it fails, route the calls through the Warehouse SBC.
- Emergency Services calls from users in the Warehouse and Manufacturing buildings are to be routed to the Warehouse SBC and failing that, to the Headquarters-SBC.
- Calls from external and Work from Home users are to be routed through the Headquarters SBC and if it fails, through the Warehouse SBC.
- Two (2) Emergency Call Routing Policies were added:
 - ECR-Headquarters.
 - ECR-Warehouse.

Identity	Associated Tenant Network Sites	Dynamic Emergency Calling	Emergency Numbers		
			Emergency Dial String	Emergency Dial Mask	OnlinePSTNUsage
Global (Org-Wide Default)	None	On	911	911	ECR-Headquarters
			933	933	ECR-Headquarters
ECR-Headquarters	Headquarters RandD Customer Service Center	On	911	911	ECR-Headquarters
			933	933	ECR-Headquarters
ECR-Warehouse	Manufacturing Warehouse	On	911	911	ECR-Warehouse
			933	933	ECR-Warehouse

Figure 118 Teams Emergency Call Routing Policies - Summary Table

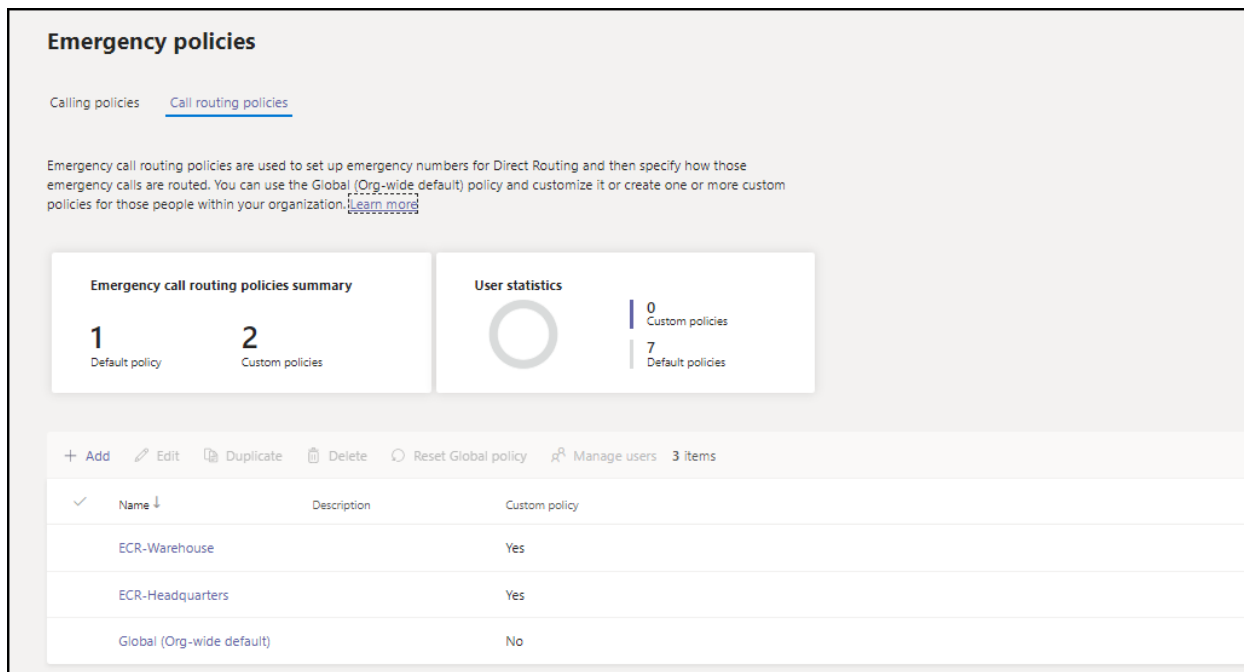


Figure 119 Teams Emergency Call Routing Policies

- PCI wants the Emergency Call Routing policies to be applied dynamically to Teams users calling emergency services from an internal network. There should be no Teams users with an Emergency Call Routing policy directly assigned to them.
- The “ECR-Headquarters” policy will be associated with the Tenant Network Sites, as they are created, for the Headquarters, R & D and Customer Service Center buildings.
- The “ECR-Warehouse” policy will be associated with the Tenant Network Sites for the Manufacturing building and the Warehouse.
- The Global (Org-Wide default) Emergency Call Routing policy will be applicable to external and Work from Home users.
- Two (2) “online PSTN usages” and four (4) “voice routes” were added:
 - The first usage, ECR-Headquarters has two (2) routes:
 - ECR-Headquarters-Primary:
 - Routes the calls through the Headquarters SBC.
 - Route priority is set to one (1).⁴
 - ECR-Warehouse-Secondary:
 - Routes the calls through the Warehouse SBC.
 - This route is only used if the first route fails.
 - Route priority is set to four (4).
 - The second usage, ECR-Warehouse also has two (2) routes:
 - ECR-Warehouse-Primary:

⁴ When more than one (1) route with the same “Dialed Number Pattern” is added to a usage, the “Priority” attribute of the route can be used to ensure that the route with the lower “Priority” has precedence over the route with a higher “Priority”.

- Routes the calls through the Warehouse SBC.
- Route priority is set to two (2).
- ECR-Headquarters-Secondary:
 - Routes the calls through the Headquarters SBC.
 - This route is only used if the first route fails.
 - Route priority is set to three (3).

Direct Routing
Direct Routing lets you connect a supported Session Border Controller (SBC) to Microsoft Phone System to enable voice calling features. You can add, edit, and view information about your SBCs, voice routes, and PSTN usage records.

Direct routing summary

2	10	2
Total SBCs	Voice routes	SBCs with issues

SBCs | **Voice routes**

+ Add | Edit | Move up | Move down | Delete | Items

✓	Priority	Voice route	Description	Dialed number pattern	PSTN usage	SBCs enrolled
	1	ECR-Headquarters-Primary		^\+1(911 933)\$	ECR-Headquarters	hadr1sbc.panhandieci.com
	2	ECR-Warehouse-Primary		^\+1(911 933)\$	ECR-WareHouse	whdr1sbc.panhandieci.com
	3	ECR-Headquarters-Secondary		^\+1(911 933)\$	ECR-Headquarters	hadr1sbc.panhandieci.com
	4	ECR-Warehouse-Secondary		^\+1(911 933)\$	ECR-WareHouse	whdr1sbc.panhandieci.com

Figure 120 Voice Routes for Direct Routing Emergency Calling

PSTN usage records
You can add a new PSTN usage record or select one from below.
0 items selected

+ Add

- Emergency
- Service
- Domestic
- International
- Emergency2
- ECR-Headquarters
- ECR-WareHouse

Figure 121 PSTN Usages for Direct Routing Emergency Calling

Emergency Calling Policy

- The Emergency Calling policies apply to both the Teams Calling Plan and Teams Direct Routing users.

- Based on the requirements provided by the RMT, Emergency Calling Policies for each of the buildings were created.
 - Office 365 Distribution Groups were created for the security desks in each of the buildings
 - SecDesk-Headquarters.
 - SecDesk-CSC.
 - SecDesk-RandD.
 - SecDesk-Warehouse.
 - SecDesk-Manufacturing.
 - An additional Distribution Group, "RMT-Notification" was created for the:
 - Vice-President of Operations.
 - Director of Human Resources.
 - Director of Security.
- The phone number of the security desk of the building that Customer Services is located is "+18505559999".
- The "ExternalLocationLookupMode" parameter was set to "Enabled" for all the policies.
- Each policy was associated with its respective Tenant Network Site as they were created.

Identity	Associated Tenant Network Sites	External Location Lookup Mode	Notification Mode	Numbers to Dial for emergency calls Notification	Users and Groups for emergency call notifications
Global (Org-Wide Default)	None	Enabled	Conferenced in and unmuted		RMT-Notification
Headquarters	Headquarters	Disabled	Conferenced in and unmuted		RMT-Notification SecDesk-Headquarters
CustomerService	Customer Service Center	Disabled	Conferenced in and unmuted	+18508241234	RMT-Notification SecDesk-CSC
RandD	RandD	Disabled	Conferenced in and unmuted		RMT-Notification SecDesk-RandD
Manufacturing	Manufacturing	Disabled	Conferenced in and unmuted		RMT-Notification SecDesk-Manufacturing
Warehouse	Warehouse	Disabled	Conferenced in and unmuted		RMT-Notification SecDesk-Warehouse

Figure 122 Teams Emergency Calling Policies - Summary Table

Emergency policies

Calling policies | Call routing policies

Emergency calling policies are used to control how users in your organization can use dynamic emergency calling features. You can use the Global (Org-wide default) policy and customize it or create one or more custom policies for those people within your organization. [Learn more](#)

Emergency calling policies summary

1 Default policy | 8 Custom policies

User statistics

0 Custom policies | 7 Default policies

+ Add | Edit | Duplicate | Delete | Reset Global policy | Manage users | 9 items

Name	Description	Custom policy
Warehouse		Yes
RandD		Yes
Manufacturing		Yes
CSC		Yes
Headquarters		Yes
Global (Org-wide default)		No

Figure 123 Teams Emergency Calling Policies

Tenant Trusted IP Addresses

- Six (6) Tenant Trusted IP Address records were added to Teams.

IP Version	IP Address	Network Range	Description
IPv4	169.45.21.8	29	HQ ISP Prime - v4
IPv6	2603::49:cd12:fc00::1	64	HQ ISP Prime - v6
IPv4	187.52.35.4	32	HQ ISP Secondary - v4
IPv6	2001:4898:e8:25:844e:926f:85ad:dd8e	128	HQ ISP Secondary - v6
IPv4	169.45.21.16	29	WH Prime - v4
IPv6	2703::50:cd12:fc00::1	64	WH Prime - v6

Figure 124 Teams Tenant Trusted IP Addresses - Summary Table

```

ipaddress,Description,Maskbits
169.45.21.8,HQ ISP Prime - v4,29
2603::49:cd12:fc00::1,HQ ISP Prime - v6,64
187.52.35.4,HQ ISP Secondary - v4,32
2001:4898:e8:25:844e:926f:85ad:dd8e,HQ ISP Secondary - v6,128
169.45.21.16,WH Prime - v4,29
2703::50:cd12:fc00::1,WH Prime - v6,64
    
```

Figure 125 Teams Tenant Trusted IP Address - CSV Input File

Network topology

You can use network topology to define the network regions, sites, and subnets that are used to determine the emergency call routing and calling policies that are to be used for a given location. [Learn more](#)

Network topology summary

3 Network sites **7** Trusted IPs

Network sites **Trusted IPs**

+ Add Edit Delete | 7 items

Trusted IP	Description	Network range	IP version
2703:50:cd12:fc00::1	WH Prime-V6	64	IPv6
169.45.21.16	WH Prime-V4	29	IPv4
2001:4898:e8:25:844e:926f:85a	HQ ISP Secondary-V6	128	IPv6
187.52.35.4	HQ ISP Secondary-V4	32	IPv4
2603:49:cd12:fc00::1	HQ ISP Prime-V6	64	IPv6
169.45.21.8	HQ ISP Prime-V4	29	IPv4

Figure 126 Teams Tenant Trusted IP Addresses

Tenant Network Regions

- A single region, "US", was added to Microsoft Teams.

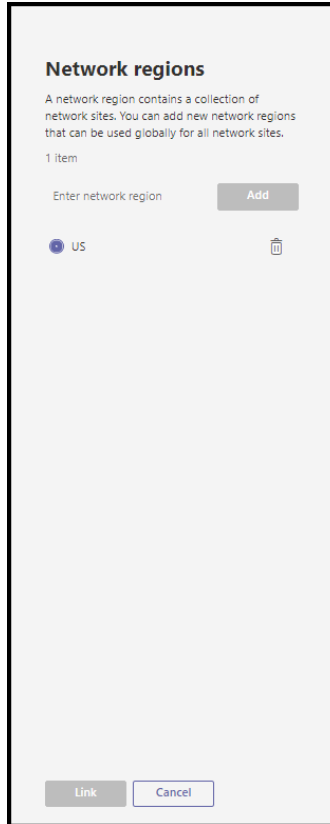


Figure 127 Teams Tenant Network Regions

Teams Tenant Network Sites

- The names of the Tenant Network Sites matched, as closely as possible, the building’s name.
- The Sites were created with their associations with the Emergency Calling and Emergency Call Routing policies.

Tenant Network Site Name	Tenant Network Region	Tenant Network Site Description	Teams Emergency Calling Policy	Teams Emergency Call Routing Policy
Headquarters	US		Headquarters	Headquarters
Manufacturing	US		Manufacturing	Warehouse
RandD	US		RandD	Headquarters
Customer Service Center	US		CustomerService	Headquarters
Warehouse	US		Warehouse	Warehouse

Figure 128 Teams Tenant Network Sites - Summary Table

```

NetworkSiteID,Description,NetworkRegionID,EmergencyCallingPolicy,EmergencyCallRoutingPolicy
Headquarters,,US,Headquarters,Headquarters
Manufacturing,,US,Manufacturing,Warehouse
RandD,,US,RandD,Headquarters
Customer Service Center,,US,CustomerService,Headquarters
Warehouse,,US,Warehouse,Warehouse
    
```

Figure 129 Teams Tenant Network Sites - CSV Input File

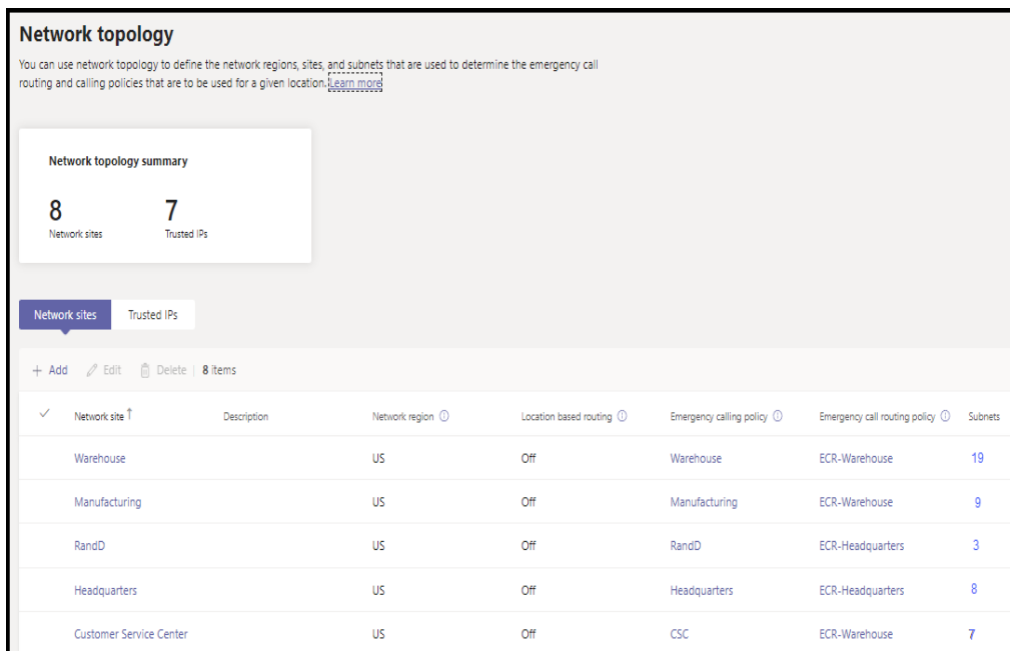


Figure 130 Teams Tenant Network Sites

Teams Tenant Network Subnets

- The network team documented all the subnets in the company's five (5) buildings. This information was used to add the Tenant Network Subnets to the Tenant Network Sites.

Building	Tenant Network Site Name	Floor	Type	Subnet Name	Subnet	Network Range
Headquarters	Headquarters	1	Data	HQ-1-Data-Alpha	10.10.2.0	24
		1	Voice	HQ-1-Voice-Alpha	10.10.3.0	24
		1	Data-WLAN	HQ-1-Data-WLAN-Alpha	10.10.50.0	24
		2	Data	HQ-2-Data-Alpha	10.10.4.0	24
		2	Voice	HQ-2-Voice-Alpha	10.10.5.0	24
		2	Data	HQ-2-Data-Bravo	10.10.6.0	24
		2	Voice	HQ-2-Voice-Bravo	10.10.7.0	24
		2	Data-WLAN	HQ-2-Data-WLAN-Alpha	10.10.51.0	24
		3	Data	HQ-3-Data-Alpha	10.10.8.0	24
		3	Voice	HQ-3-Voice-Alpha	10.10.9.0	24
		3	Data-WLAN	HQ-3-Data-WLAN-Alpha	10.10.52.0	24
		3	Data-WLAN	HQ-3-Data-WLAN-Bravo	10.10.53.0	24
		4	Data	HQ-4-Data-Alpha	10.10.10.0	24
		4	Voice	HQ-4-Voice-Alpha	10.10.11.0	24
		4	Data	HQ-4-Data-Bravo	10.10.12.0	24
		4	Voice	HQ-4-Voice-Bravo	10.10.13.0	24
		4	Data-WLAN	HQ-4-Data-WLAN-Alpha	10.10.54.0	24
		5	Data	HQ-5-Data-Alpha	10.10.14.0	24
		5	Voice	HQ-5-Voice-Alpha	10.10.15.0	24
		5	Data-WLAN	HQ-5-Data-WLAN-Alpha	10.10.55.0	24
Manufacturing	Manufacturing	1	Data	MA-1-Data-Alpha	10.10.16.0	24
		1	Voice	MA-1-Voice-Alpha	10.10.17.0	24
		1	Data-WLAN	MA-1-Data-WLAN-Alpha	10.10.56.0	24
		2	Data	MA-2-Data-Alpha	10.10.18.0	24
		2	Voice	MA-2-Voice-Alpha	10.10.19.0	24
		2	Data-WLAN	MA-2-Data-WLAN-Alpha	10.10.57.0	24
		3	Data	MA-3-Data-Alpha	10.10.20.0	24
3	Voice	MA-3-Voice-Alpha	10.10.21.0	24		
3	Data-WLAN	MA-3-Data-WLAN-Alpha	10.10.58.0	24		
R & D	RandD	1	Data	RD-1-Data-Alpha	10.10.22.0	24
		1	Voice	RD-1-Voice-Alpha	10.10.23.0	24
Customer Service Center	Customer Service Center	6	Data	CS-6-Data-Alpha	10.10.24.0	24
		6	Voice	CS-6-Voice-Alpha	10.10.25.0	24
		6	Data-WLAN	CS-6-Data-WLAN-Alpha	10.10.60.0	24
		9	Data	CS-9-Data-Alpha	10.10.26.0	24
		9	Voice	CS-9-Voice-Alpha	10.10.27.0	24
		9	Data-WLAN	CS-9-Data-WLAN-Alpha	10.10.61.0	24
		9	Data-WLAN	CS-9-Data-WLAN-Bravo	10.10.62.0	24
Warehouse	Warehouse	1	Data	WH-1-Data-Alpha	10.10.28.0	24
		1	Voice	WH-1-Voice-Alpha	10.10.29.0	24
		1	Data-WLAN	WH-1-Data-WLAN-Alpha	10.10.63.0	24
		1	Data-WLAN	WH-1-Data-WLAN-Bravo	10.10.64.0	24
		1	Data-WLAN	WH-1-Data-WLAN-Charlie	10.10.65.0	24
		Bullpen	Data	WH-Bullpen-Data-Alpha	10.10.30.0	24
		Bullpen	Voice	WH-Bullpen-Voice-Alpha	10.10.31.0	24
Bullpen	Data-WLAN	WH-Bullpen-Data-WLAN-Alpha	10.10.66.0	24		

Figure 131 Teams Tenant Network Subnets - Summary Table

SubnetID	Description	MaskBits	NetworkSiteID
10.10.2.0	HQ-1-Data-Alpha	24	Headquarters
10.10.3.0	HQ-1-Voice-Alpha	24	Headquarters
10.10.50.0	HQ-1-Data-WLAN-Alpha	24	Headquarters
10.10.4.0	HQ-2-Data-Alpha	24	Headquarters
10.10.5.0	HQ-2-Voice-Alpha	24	Headquarters
10.10.6.0	HQ-2-Data-Bravo	24	Headquarters
10.10.7.0	HQ-2-Voice-Bravo	24	Headquarters
10.10.51.0	HQ-2-Data-WLAN-Alpha	24	Headquarters
10.10.8.0	HQ-3-Data-Alpha	24	Headquarters
10.10.9.0	HQ-3-Voice-Alpha	24	Headquarters
10.10.52.0	HQ-3-Data-WLAN-Alpha	24	Headquarters
10.10.53.0	HQ-3-Data-WLAN-Bravo	24	Headquarters
10.10.10.0	HQ-4-Data-Alpha	24	Headquarters
10.10.11.0	HQ-4-Voice-Alpha	24	Headquarters
10.10.12.0	HQ-4-Data-Bravo	24	Headquarters
10.10.13.0	HQ-4-Voice-Bravo	24	Headquarters
10.10.54.0	HQ-4-Data-WLAN-Alpha	24	Headquarters
10.10.14.0	HQ-5-Data-Alpha	24	Headquarters
10.10.15.0	HQ-5-Voice-Alpha	24	Headquarters
10.10.55.0	HQ-5-Data-WLAN-Alpha	24	Headquarters
10.10.16.0	MA-1-Data-Alpha	24	Manufacturing
10.10.17.0	MA-1-Voice-Alpha	24	Manufacturing
10.10.56.0	MA-1-Data-WLAN-Alpha	24	Manufacturing
10.10.18.0	MA-2-Data-Alpha	24	Manufacturing
10.10.19.0	MA-2-Voice-Alpha	24	Manufacturing
10.10.57.0	MA-2-Data-WLAN-Alpha	24	Manufacturing
10.10.20.0	MA-3-Data-Alpha	24	Manufacturing
10.10.21.0	MA-3-Voice-Alpha	24	Manufacturing
10.10.58.0	MA-3-Data-WLAN-Alpha	24	Manufacturing
10.10.22.0	RD-1-Data-Alpha	24	RandD
10.10.23.0	RD-1-Voice-Alpha	24	RandD
10.10.59.0	RD-1-Data-WLAN-Alpha	24	RandD
10.10.24.0	CS-6-Data-Alpha	24	Customer Service Center
10.10.25.0	CS-6-Voice-Alpha	24	Customer Service Center
10.10.60.0	CS-6-Data-WLAN-Alpha	24	Customer Service Center
10.10.26.0	CS-9-Data-Alpha	24	Customer Service Center
10.10.27.0	CS-9-Voice-Alpha	24	Customer Service Center
10.10.61.0	CS-9-Data-WLAN-Alpha	24	Customer Service Center
10.10.62.0	CS-9-Data-WLAN-Bravo	24	Customer Service Center
10.10.28.0	WH-1-Data-Alpha	24	Warehouse
10.10.29.0	WH-1-Voice-Alpha	24	Warehouse
10.10.63.0	WH-1-Data-WLAN-Alpha	24	Warehouse
10.10.64.0	WH-1-Data-WLAN-Bravo	24	Warehouse
10.10.65.0	WH-1-Data-WLAN-Charlie	24	Warehouse
10.10.30.0	WH-Bullpen-Data-Alpha	24	Warehouse
10.10.31.0	WH-Bullpen-Voice-Alpha	24	Warehouse
10.10.66.0	WH-Bullpen-Data-WLAN-Alpha	24	Warehouse

Figure 132 Teams Tenant Network Subnets - CSV Input File

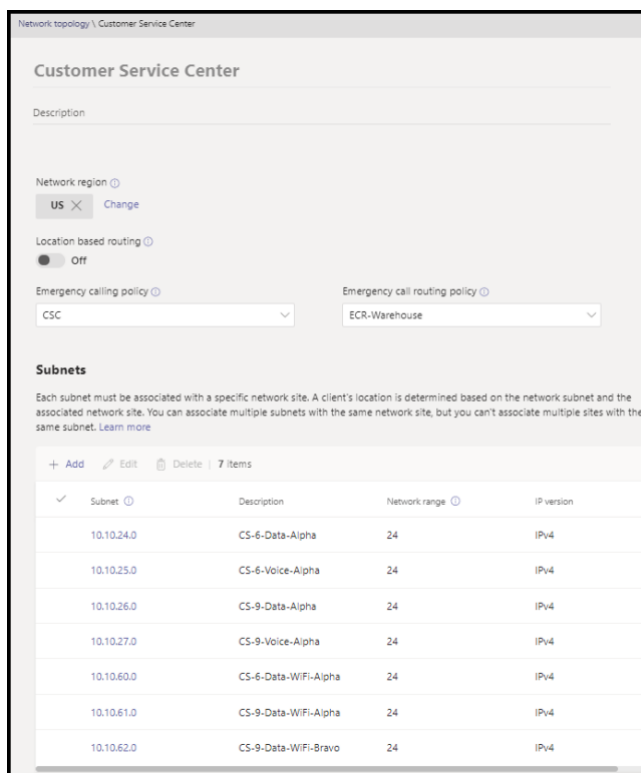


Figure 133 Teams Tenant Network Subnets - Example Tenant Network Site Shown

Dynamic 911 – Location Information System (LIS) – Network Elements

- Based on the requirements set forth by the RMT, the company will be using all four (4) network element types to set their environment up to support the requirement of the RAY BAUM act to automatically provide a dynamically derived dispatchable location when a user calls emergency services from an on-premises network location.
 - Subnets
 - Wireless Access Points
 - Switches
 - Ports
- The CIO and network team reviewed the requirements and were able to define the correct mixture of the network elements to meet them.

Requirements

- **A dynamic location must be derived whenever a user is connected to a corporate physical or Wi-Fi network. A user should never fail to receive a dynamic location when connected to the corporate infrastructure.**
- **External and Work from Home users should never receive a dynamic 911 location.** They should always be required to verify their current location.
- Calls from the Headquarters, Manufacturing, R&D or Customer Service Center buildings:

- The dispatchable location should provide the floor in the building in addition to the “front door” address.
- Calls made from a Wi-Fi network:
 - Should reflect the floor in the building on which the Wireless Access Point is installed.
 - The floor number is to be provided in addition to the building’s “front door” address.
 - This is predicated on the users connecting to the correct Wireless Access Point. They must connect to a Wi-Fi network associated with the floor that they are on .
- Calls made from data centers, machine\equipment rooms and wiring closets in the buildings:
 - Provide the floor and name of the room in the dispatchable location in addition to the “front door” address.
- Calls from the floor of the Warehouse:
 - Provide a dispatchable location in the Warehouse based on the quadrant where the Teams user is signed on.
 - The floor of the Warehouse is divided into North, South, East, and West quadrants
- Calls from devices in the Warehouse’s “Bullpen”:
 - These calls should be identified as coming from the “Bullpen” in addition to the “front door” address of the Warehouse.

Dynamic 911 Location Derivation Analysis and Conclusions

- The network team confirmed that location\place records had been added to Teams for every floor in all the company’s buildings.
- Records for each of the four (4) quadrants in the Warehouse and the Bullpen had been created.
- Records for the data centers and wiring closets in each building were in place.
- The team documented the location of the subnets and the Basic Service Set Identifiers (BSSIDs) of the wireless access points by floor.
 - The Subnet network element will be used to derive a location for the non-Wi-Fi users on the office floors and in the Warehouse’s Bullpen.
 - The Wireless Access Point network element will be used for Wi-Fi connected users in these locations. This network element takes precedence over the Subnet network element if a location could be determined from both elements.
 - The Wireless Access Points are strongly correlated to subnets that are not designed to traverse floors. Presuming that the range of the WAPs have been shaped correctly, they should inhibit connections from devices on different floors
 - Based on this configuration, the network team could have used the Subnet network element for the Wi-Fi “owned” subnets. The team decided to use the Wireless Access Point element to permit them in the future to provide a more granular location on the floors as needed. They currently do not have a need for this but felt that this may become a requirement in the future.
 - The network team decided to create Subnet network element records for the Wi-Fi subnets. These will serve as a “backup” if the Teams endpoint cannot derive a location based on the BSSID of the connected Wireless Access Point.

- The subnets on the floor of the Warehouse are shared by users and devices in each of the four (4) quadrants.
 - The team determined that the subnets on the Warehouse floor could not be used to provide a quadrant specific location for the users.
 - The network switches and WAPs on the floor are quadrant specific.
 - The team determined that the “Switch” and “Wireless Access Point” LIS network elements will be needed to provide quadrant specific locations for the users on the Warehouse floor.
 - The team gathered the Chassis IDs of the switches and the BSSIDs of the Wireless Access Points in each of the four (4) quadrants.
 - The network team decided to create Subnet network element records for the physical and Wi-Fi subnets on the Warehouse floor. These will serve as a “backup” if the Teams endpoint cannot derive a device’s location based on the Chassis ID or BSSID of the connected Wireless Access Point.
- The data centers and wiring closets require very specific location resolution.
 - For this level of precision of the dispatchable location, the network team determined that they would need to use the Port network element.
 - The team gathered the Chassis ID and Port numbers of all available user or device network connections in each of these rooms. There are typically between three (3) and six (6) of these connections available in each location.
- The network team produced individual summary tables and Comma Separated Value (CSV) files for each of the four (4) network elements. The CSV files were used as inputs to PowerShell scripts to add the network elements to Teams.

Subnet Network Elements

Building	Floor	Type	Subnet Name	Subnet	Network Range	Description	Organization Name	Teams Values		
								CivicAddressID	Location	Location ID
Headquarters	1	Data	HQ-1-Data-Alpha	10.10.2.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 1	b845f9df-021a-47fc-9dfc-0d9d7b932996
	1	Voice	HQ-1-Voice-Alpha	10.10.3.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 1	b845f9df-021a-47fc-9dfc-0d9d7b932996
	1	Data-WLAN	HQ-1-Data-WLAN-Alpha	10.10.50.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 1	b845f9df-021a-47fc-9dfc-0d9d7b932996
	2	Data	HQ-2-Data-Alpha	10.10.4.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	2	Voice	HQ-2-Voice-Alpha	10.10.5.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	2	Data	HQ-2-Data-Bravo	10.10.6.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	2	Voice	HQ-2-Voice-Bravo	10.10.7.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	2	Data-WLAN	HQ-2-Data-WLAN-Alpha	10.10.51.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	3	Data	HQ-3-Data-Alpha	10.10.8.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	3	Voice	HQ-3-Voice-Alpha	10.10.9.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	3	Data-WLAN	HQ-3-Data-WLAN-Alpha	10.10.52.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	3	Data-WLAN	HQ-3-Data-WLAN-Bravo	10.10.53.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	4	Data	HQ-4-Data-Alpha	10.10.10.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4	59ff2faf-c077-41ee-9aca-6df9588f87ad
	4	Voice	HQ-4-Voice-Alpha	10.10.11.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4	59ff2faf-c077-41ee-9aca-6df9588f87ad
	4	Data	HQ-4-Data-Bravo	10.10.12.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4	59ff2faf-c077-41ee-9aca-6df9588f87ad
	4	Voice	HQ-4-Voice-Bravo	10.10.13.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4	59ff2faf-c077-41ee-9aca-6df9588f87ad
	4	Data-WLAN	HQ-4-Data-WLAN-Alpha	10.10.54.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4	59ff2faf-c077-41ee-9aca-6df9588f87ad
	5	Data	HQ-5-Data-Alpha	10.10.14.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 5	a1978044-911e-43a5-8bd3-65f1a5c202b1
	5	Voice	HQ-5-Voice-Alpha	10.10.15.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 5	a1978044-911e-43a5-8bd3-65f1a5c202b1
	5	Data-WLAN	HQ-5-Data-WLAN-Alpha	10.10.55.0	24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 5	a1978044-911e-43a5-8bd3-65f1a5c202b1
Manufacturing	1	Data	MA-1-Data-Alpha	10.10.16.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1	8123e39515d9d-9b23860f-15921a5ca2496
	1	Voice	MA-1-Voice-Alpha	10.10.17.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1	8123e39515d9d-9b23860f-15921a5ca2496
	1	Data-WLAN	MA-1-Data-WLAN-Alpha	10.10.56.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1	8123e39515d9d-9b23860f-15921a5ca2496
	2	Data	MA-2-Data-Alpha	10.10.18.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2	6273c39997e0e-2c85125c-80770d6ee1995
	2	Voice	MA-2-Voice-Alpha	10.10.19.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2	6273c39997e0e-2c85125c-80770d6ee1995
	2	Data-WLAN	MA-2-Data-WLAN-Alpha	10.10.57.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2	6273c39997e0e-2c85125c-80770d6ee1995
	3	Data	MA-3-Data-Alpha	10.10.20.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3	0684b48409a9b-1e34846b-48116a0bf7845
	3	Voice	MA-3-Voice-Alpha	10.10.21.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3	0684b48409a9b-1e34846b-48116a0bf7845
	3	Data-WLAN	MA-3-Data-WLAN-Alpha	10.10.58.0	24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3	0684b48409a9b-1e34846b-48116a0bf7845
R & D	1	Data	RD-1-Data-Alpha	10.10.22.0	24	The Lab - R&D	PCI-Product Development	0d99f93b-747a-455e-b2bc-d224aeb9ce90	Floor 1	4562e70524e2a-8f85542f-02687a3fe1681
	1	Voice	RD-1-Voice-Alpha	10.10.23.0	24	The Lab - R&D	PCI-Product Development	0d99f93b-747a-455e-b2bc-d224aeb9ce90	Floor 1	4562e70524e2a-8f85542f-02687a3fe1681
	1	Data-WLAN	RD-1-Data-WLAN-Alpha	10.10.59.0	24	The Lab - R&D	PCI-Product Development	0d99f93b-747a-455e-b2bc-d224aeb9ce90	Floor 1	4562e70524e2a-8f85542f-02687a3fe1681
Customer Service Center	6	Data	CS-6-Data-Alpha	10.10.24.0	24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 6	7079b37062b0e-2f73317c-83271b1da1725
	6	Voice	CS-6-Voice-Alpha	10.10.25.0	24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 6	7079b37062b0e-2f73317c-83271b1da1725
	6	Data-WLAN	CS-6-Data-WLAN-Alpha	10.10.60.0	24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 6	7079b37062b0e-2f73317c-83271b1da1725
	9	Data	CS-9-Data-Alpha	10.10.26.0	24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 9	5909b78084e1d-8e96821e-56764f8bf6004
	9	Voice	CS-9-Voice-Alpha	10.10.27.0	24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 9	5909b78084e1d-8e96821e-56764f8bf6004
	9	Data-WLAN	CS-9-Data-WLAN-Alpha	10.10.61.0	24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 9	5909b78084e1d-8e96821e-56764f8bf6004
Warehouse	1	Data	WH-1-Data-Alpha	10.10.28.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1	9174d55009e5f-1f29694b-75644b2fc0968
	1	Voice	WH-1-Voice-Alpha	10.10.29.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1	9174d55009e5f-1f29694b-75644b2fc0968
	1	Data-WLAN	WH-1-Data-WLAN-Alpha	10.10.63.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1	9174d55009e5f-1f29694b-75644b2fc0968
	1	Data-WLAN	WH-1-Data-WLAN-Bravo	10.10.64.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1	9174d55009e5f-1f29694b-75644b2fc0968
	1	Data-WLAN	WH-1-Data-WLAN-Charlie	10.10.65.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1	9174d55009e5f-1f29694b-75644b2fc0968
	Bullpen	Data	WH-Bullpen-Data-Alpha	10.10.30.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor Bullpen	9043a07798e1c-1d84142e-06203c4ed0806
	Bullpen	Voice	WH-Bullpen-Voice-Alpha	10.10.31.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor Bullpen	9043a07798e1c-1d84142e-06203c4ed0806
	Bullpen	Data-WLAN	WH-Bullpen-Data-WLAN-Alpha	10.10.66.0	24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor Bullpen	9043a07798e1c-1d84142e-06203c4ed0806

Figure 134 Subnet Network Elements - Summary Table

Subnet,Description,LocationID
10.10.2.0,HQ-1-Data-Alpha,b845f9df-021a-47fc-9dfc-0d9d7b932996
10.10.3.0,HQ-1-Voice-Alpha,b845f9df-021a-47fc-9dfc-0d9d7b932996
10.10.50.0,HQ-1-Data-WLAN-Alpha,b845f9df-021a-47fc-9dfc-0d9d7b932996
10.10.4.0,HQ-2-Data-Alpha,6984d776-b877-4b72-9242-b6eea9ea1f67
10.10.5.0,HQ-2-Voice-Alpha,6984d776-b877-4b72-9242-b6eea9ea1f67
10.10.6.0,HQ-2-Data-Bravo,6984d776-b877-4b72-9242-b6eea9ea1f67
10.10.7.0,HQ-2-Voice-Bravo,6984d776-b877-4b72-9242-b6eea9ea1f67
10.10.51.0,HQ-2-Data-WLAN-Alpha,6984d776-b877-4b72-9242-b6eea9ea1f67
10.10.8.0,HQ-3-Data-Alpha,d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
10.10.9.0,HQ-3-Voice-Alpha,d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
10.10.52.0,HQ-3-Data-WLAN-Alpha,d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
10.10.53.0,HQ-3-Data-WLAN-Bravo,d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
10.10.10.0,HQ-4-Data-Alpha,59ff2faf-c077-41ee-9aca-6df9588f87ad
10.10.11.0,HQ-4-Voice-Alpha,59ff2faf-c077-41ee-9aca-6df9588f87ad
10.10.12.0,HQ-4-Data-Bravo,59ff2faf-c077-41ee-9aca-6df9588f87ad
10.10.13.0,HQ-4-Voice-Bravo,59ff2faf-c077-41ee-9aca-6df9588f87ad
10.10.54.0,HQ-4-Data-WLAN-Alpha,59ff2faf-c077-41ee-9aca-6df9588f87ad
10.10.14.0,HQ-5-Data-Alpha,a1978044-911e-43a5-8bd3-65f1a5c202b1
10.10.15.0,HQ-5-Voice-Alpha,a1978044-911e-43a5-8bd3-65f1a5c202b1
10.10.55.0,HQ-5-Data-WLAN-Alpha,a1978044-911e-43a5-8bd3-65f1a5c202b1
10.10.16.0,MA-1-Data-Alpha,8123e39515d9d-9b23860f-15921a5ca2496
10.10.17.0,MA-1-Voice-Alpha,8123e39515d9d-9b23860f-15921a5ca2496
10.10.56.0,MA-1-Data-WLAN-Alpha,8123e39515d9d-9b23860f-15921a5ca2496
10.10.18.0,MA-2-Data-Alpha,6273c39997e0e-2c85125c-80770d6ee1995
10.10.19.0,MA-2-Voice-Alpha,6273c39997e0e-2c85125c-80770d6ee1995
10.10.57.0,MA-2-Data-WLAN-Alpha,6273c39997e0e-2c85125c-80770d6ee1995
10.10.20.0,MA-3-Data-Alpha,0684b48409a9b-1e34846b-48116a0bf7845
10.10.21.0,MA-3-Voice-Alpha,0684b48409a9b-1e34846b-48116a0bf7845
10.10.58.0,MA-3-Data-WLAN-Alpha,0684b48409a9b-1e34846b-48116a0bf7845
10.10.22.0,RD-1-Data-Alpha,4562e70524e2a-8f85542f-02687a3fe1681
10.10.23.0,RD-1-Voice-Alpha,4562e70524e2a-8f85542f-02687a3fe1681
10.10.59.0,RD-1-Data-WLAN-Alpha,4562e70524e2a-8f85542f-02687a3fe1681
10.10.24.0,CS-6-Data-Alpha,7079b37062b0e-2f73317c-83271b1da1725
10.10.25.0,CS-6-Voice-Alpha,7079b37062b0e-2f73317c-83271b1da1725
10.10.60.0,CS-6-Data-WLAN-Alpha,7079b37062b0e-2f73317c-83271b1da1725
10.10.26.0,CS-9-Data-Alpha,5909b78084e1d-8e96821e-56764f8bf6004
10.10.27.0,CS-9-Voice-Alpha,5909b78084e1d-8e96821e-56764f8bf6004
10.10.61.0,CS-9-Data-WLAN-Alpha,5909b78084e1d-8e96821e-56764f8bf6004
10.10.62.0,CS-9-Data-WLAN-Bravo,5909b78084e1d-8e96821e-56764f8bf6004
10.10.28.0,WH-1-Data-Alpha,9174d55009e5f-1f29694b-75644b2fc0968
10.10.29.0,WH-1-Voice-Alpha,9174d55009e5f-1f29694b-75644b2fc0968
10.10.63.0,WH-1-Data-WLAN-Alpha,9174d55009e5f-1f29694b-75644b2fc0968
10.10.64.0,WH-1-Data-WLAN-Bravo,9174d55009e5f-1f29694b-75644b2fc0968
10.10.65.0,WH-1-Data-WLAN-Charlie,9174d55009e5f-1f29694b-75644b2fc0968
10.10.30.0,WH-Bullpen-Data-Alpha,9043a07798e1c-1d84142e-06203c4ed0806
10.10.31.0,WH-Bullpen-Voice-Alpha,9043a07798e1c-1d84142e-06203c4ed0806
10.10.66.0,WH-Bullpen-Data-WLAN-Alpha,9043a07798e1c-1d84142e-06203c4ed0806

Figure 135 Subnet Network Elements - CSV Input File

Wireless Access Points Network Elements

Building	Floor	WAP Name	BSSID	Subnets	Description	Organization Name	Teams Values		
							CivicAddressID	Location	Location ID
Headquarters	1	HQ-1-WAP-Alpha	D6-41-B8-19-79-FF	10.10.50.0/24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 1	b845f9df-021a-47fc-9dfc-0d9d7b932996
	1	HQ-1-WAP-Bravo	8A-BF-11-84-69-C7		Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 1	b845f9df-021a-47fc-9dfc-0d9d7b932996
	2	HQ-2-WAP-Alpha	ED-87-FC-47-C2-D5	10.10.51.0/24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	2	HQ-2-WAP-Bravo	65-3C-E7-A1-64-37		Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	3	HQ-3-WAP-Alpha	DF-48-8D-8A-C5-49	10.10.52.0/24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	3	HQ-3-WAP-Bravo	C5-D8-79-16-34-53	10.10.53.0/24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	4	HQ-4-WAP-Alpha	8D-A1-35-68-D5-FC	10.10.54.0/24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4	59ff2faf-c077-41ee-9aca-6df9588f87ad
	4	HQ-4-WAP-Bravo	CD-84-67-4B-33-87		Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4	59ff2faf-c077-41ee-9aca-6df9588f87ad
	5	HQ-5-WAP-Alpha	E5-EE-E2-C8-46-34	10.10.55.0/24	Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 5	a1978044-911e-43a5-8bd3-65f1a5c202b1
	5	HQ-5-WAP-Bravo	88-27-A9-B7-C1-F3		Vickers-Headquarters	Panhandle Consumer Industries	7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 5	a1978044-911e-43a5-8bd3-65f1a5c202b1
Manufacturing	1	MA-1-WAP-Alpha	F3-CF-40-4F-7C-8E	10.10.56.0/24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1	b845f9df-021a-47fc-9dfc-0d9d7b932996
	1	MA-1-WAP-Bravo	53-FC-48-EE-E5-EA		Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1	b845f9df-021a-47fc-9dfc-0d9d7b932996
	2	MA-2-WAP-Alpha	C6-C6-97-15-41-AF	10.10.57.0/24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	2	MA-2-WAP-Bravo	1F-9B-A8-E3-D4-3A		Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2	6984d776-b877-4b72-9242-b6eea9ea1f67
	3	MA-3-WAP-Alpha	88-36-B5-8E-18-AB	10.10.58.0/24	Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	3	MA-3-WAP-Bravo	ED-F0-E9-C8-E2-21		Manufacturing	Panhandle Consumer Industries	d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
R & D	3	RD-3-WAP-Alpha	E4-2C-CB-15-A6-41	10.10.59.0/24	The Lab - R&D	PCI-Product Development	0d99f93b-747a-455e-b2bc-d224aeb9ce90	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
	3	RD-6-WAP-Bravo	95-42-C7-D7-D9-AA		The Lab - R&D	PCI-Product Development	0d99f93b-747a-455e-b2bc-d224aeb9ce90	Floor 3	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
Customer Service Center	6	CS-6-WAP-Alpha	BE-D4-F0-5D-23-F6	10.10.60.0/24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 6	7079b37062b0e-2f73317c-83271b1da1725
	6	CS-6-WAP-Bravo	8E-99-D3-31-58-86		CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 6	7079b37062b0e-2f73317c-83271b1da1725
	9	CS-9-WAP-Alpha	58-58-12-E8-CD-99	10.10.61.0/24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 9	5909b78084e1d-8e96821e-56764f8bf6004
	9	CS-9-WAP-Bravo	F3-64-D1-AB-11-27	10.10.62.0/24	CSC-Customer Service	PCI-CSC	00d751d1-e39a-464b-867c-8f73828b139b	Floor 9	5909b78084e1d-8e96821e-56764f8bf6004
Warehouse	1N	WH-1N-WAP-Alpha	57-27-C5-EB-72-B4	10.10.63.0/24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1N	1924d70509a0f-0c15945d-72364b9fe3673
	1N	WH-1N-WAP-Bravo	B0-73-18-7A-DB-EC		Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1N	2751b13748b2e-3d72055a-07917d3ee5199
	1S	WH-1S-WAP-Alpha	17-B9-47-54-33-30	10.10.64.0/24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1S	2071b51538e7b-1d56931e-25476d2cc9763
	1S	WH-1S-WAP-Bravo	60-DF-4C-F4-3C-9A		Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1S	8602e05907f0d-3c31569b-72846a7eb2667
	1E	WH-1E-WAP-Alpha	53-D5-DB-39-84-B8	10.10.65.0/24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1E	8183d12905a1a-4b85106f-12321c5af2453
	1E	WH-1E-WAP-Bravo	88-41-54-2C-FA-5E		Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1E	2501e53225b8b-8f54662f-72329a6bb8627
	1W	WH-1W-WAP-Alpha	44-A2-80-D0-15-9B	10.10.66.0/24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1W	7364d71052f1d-0e95109c-32983c3fa3888
	1W	WH-1W-WAP-Bravo	11-BD-37-D8-CE-91		Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1W	0834d78417e6b-3b37262c-42100e0aa1554
	Bullpen	WH-Bullpen-WAP-Alpha	C2-8E-35-D7-2A-B9	10.10.66.0/24	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor Bullpen	9043a077981ec-1d84142e-06203c4ed0806
	Bullpen	WH-Bullpen-WAP-Bravo	48-FC-6D-A1-17-35		Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor Bullpen	9043a077981ec-1d84142e-06203c4ed0806

Figure 136 Wireless Access Point Network Elements - Summary Table

BSSID	Description	LocationID
D6-41-B8-19-79-FF	HQ-1-WAP-Alpha	b845f9df-021a-47fc-9dfc-0d9d7b932996
8A-BF-11-84-69-C7	HQ-1-WAP-Bravo	b845f9df-021a-47fc-9dfc-0d9d7b932996
ED-87-FC-47-C2-D5	HQ-2-WAP-Alpha	6984d776-b877-4b72-9242-b6eea9ea1f67
65-3C-E7-A1-64-37	HQ-2-WAP-Bravo	6984d776-b877-4b72-9242-b6eea9ea1f67
DF-4B-8D-8A-C5-49	HQ-3-WAP-Alpha	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
C5-D8-79-16-34-53	HQ-3-WAP-Bravo	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
8D-A1-35-6B-D5-FC	HQ-4-WAP-Alpha	59ff2faf-c077-41ee-9aca-6df9588f87ad
CD-84-67-4B-33-87	HQ-4-WAP-Bravo	59ff2faf-c077-41ee-9aca-6df9588f87ad
E5-EE-E2-C8-46-34	HQ-5-WAP-Alpha	a1978044-911e-43a5-8bd3-65f1a5c202b1
88-27-A9-B7-C1-F3	HQ-5-WAP-Bravo	a1978044-911e-43a5-8bd3-65f1a5c202b1
F3-CF-40-4F-7C-8E	MA-1-WAP-Alpha	b845f9df-021a-47fc-9dfc-0d9d7b932996
53-FC-48-EE-E5-EA	MA-1-WAP-Bravo	b845f9df-021a-47fc-9dfc-0d9d7b932996
C6-C6-97-15-41-AF	MA-2-WAP-Alpha	6984d776-b877-4b72-9242-b6eea9ea1f67
1F-9B-A8-E3-D4-3A	MA-2-WAP-Bravo	6984d776-b877-4b72-9242-b6eea9ea1f67
88-36-B5-8E-18-AB	MA-3-WAP-Alpha	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
ED-F0-E9-C8-E2-21	MA-3-WAP-Bravo	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
E4-2C-CB-15-A6-41	RD-3-WAP-Alpha	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
95-42-C7-D7-D9-AA	RD-6-WAP-Bravo	d7228d23-7b3f-40f6-9d5b-e5fce28f7e22
BE-D4-F0-5D-23-F6	CS-6-WAP-Alpha	7079b37062b0e-2f73317c-83271b1da1725
8E-99-D3-31-58-86	CS-6-WAP-Bravo	7079b37062b0e-2f73317c-83271b1da1725
58-58-12-E8-CD-99	CS-9-WAP-Alpha	5909b78084e1d-8e96821e-56764f8bf6004
F3-64-D1-AB-11-27	CS-9-WAP-Bravo	5909b78084e1d-8e96821e-56764f8bf6004
57-27-C5-EB-72-B4	WH-1N-WAP-Alpha	1924d70509a0f-0c15945d-72364b9fe3673
B0-73-18-7A-DB-EC	WH-1N-WAP-Bravo	2751b13748b2e-3d72055a-07917d3ee5199
17-B9-47-54-33-30	WH-1S-WAP-Alpha	2071b51538e7b-1d56931e-25476d2cc9763
60-DF-4C-F4-3C-9A	WH-1S-WAP-Bravo	8602e05907f0d-3c31569b-72846a7eb2667
53-D5-DB-39-84-B8	WH-1E-WAP-Alpha	8183d12905a1a-4b85106f-12321c5af2453
88-41-54-2C-FA-5E	WH-1E-WAP-Bravo	2501e53225b8b-8f54662f-72329a6bb8627
44-A2-80-D0-15-9B	WH-1W-WAP-Alpha	7364d71052f1d-0e95109c-32983c3fa3888
11-BD-37-D8-CE-91	WH-1W-WAP-Bravo	0834d78417e6b-3b37262c-42100e0aa1554
C2-8E-35-D7-2A-B9	WH-Bullpen-WAP-Alpha	9043a07798e1c-1d84142e-06203c4ed0806
48-FC-6D-A1-17-35	WH-Bullpen-WAP-Bravo	9043a07798e1c-1d84142e-06203c4ed0806

Figure 137 Wireless Access Point Network Elements - CSV Input File

Network Switch Network Elements

Building	Floor	Switch Name	Chassis ID	Teams Values				
				Description	Organization Name	CivicAddressID	Location	Location ID
Warehouse	1N	WH-North-Data-SW-1	89532	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1N	1924d70509a0f-0c15945d-72364b9fe3673
	1N	WH-North-Data-SW-2	50294	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1N	1924d70509a0f-0c15945d-72364b9fe3673
	1N	WH-North-Voice-SW-1	57923	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1N	1924d70509a0f-0c15945d-72364b9fe3673
	1N	WH-North-Voice-SW-2	18406	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1N	1924d70509a0f-0c15945d-72364b9fe3673
	1S	WH-South-Data-SW-1	65877	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1S	2071b51538e7b-1d56931e-25476d2cc9763
	1S	WH-South-Voice-SW-1	50279	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1S	2071b51538e7b-1d56931e-25476d2cc9763
	1W	WH-West-Data-SW-1	46117	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1W	7364d71052f1d-0e95109c-32983c3fa3888
	1W	WH-West-Data-SW-2	28395	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1W	7364d71052f1d-0e95109c-32983c3fa3888
	1W	WH-West-Data-SW-3	36416	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1W	7364d71052f1d-0e95109c-32983c3fa3888
	1W	WH-West-Voice-SW-1	49453	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1W	7364d71052f1d-0e95109c-32983c3fa3888
	1W	WH-West-Voice-SW-2	92676	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1W	7364d71052f1d-0e95109c-32983c3fa3888
	1E	WH-East-Data-SW-1	70920	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1E	2501e53225b8b-8f54662f-72329a6bb8627
	1E	WH-East-Voice-SW-1	48592	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1E	2501e53225b8b-8f54662f-72329a6bb8627
1E	WH-East-Voice-SW-2	58281	Ballpark	PCI-Logistics	cb3faa9b-1aed-46c8-9995-64f5e681ef56	Floor 1E	2501e53225b8b-8f54662f-72329a6bb8627	

Figure 138 Network Switch Network Elements - Summary Table

```

ChassisID,Description,LocationID
89532,WH-North-Data-SW-1,1924d70509a0f-0c15945d-72364b9fe3673
50294,WH-North-Data-SW-2,1924d70509a0f-0c15945d-72364b9fe3673
57923,WH-North-Voice-SW-1,1924d70509a0f-0c15945d-72364b9fe3673
18406,WH-North-Voice-SW-2,1924d70509a0f-0c15945d-72364b9fe3673
65877,WH-South-Data-SW-1,2071b51538e7b-1d56931e-25476d2cc9763
50279,WH-South-Voice-SW-1,2071b51538e7b-1d56931e-25476d2cc9763
46117,WH-West-Data-SW-1,7364d71052f1d-0e95109c-32983c3fa3888
28395,WH-West-Data-SW-2,7364d71052f1d-0e95109c-32983c3fa3888
36416,WH-West-Data-SW-3,7364d71052f1d-0e95109c-32983c3fa3888
49453,WH-West-Voice-SW-1,7364d71052f1d-0e95109c-32983c3fa3888
92676,WH-West-Voice-SW-2,7364d71052f1d-0e95109c-32983c3fa3888
70920,WH-East-Data-SW-1,2501e53225b8b-8f54662f-72329a6bb8627
48592,WH-East-Voice-SW-1,2501e53225b8b-8f54662f-72329a6bb8627
58281,WH-East-Voice-SW-2,2501e53225b8b-8f54662f-72329a6bb8627
    
```

Figure 139 Network Switch Network Elements - CSV Input File

Network Switch Port Network Elements

Building	Floor	Office Name	Office Number	Switch Name	Chassis ID	Port Name	Port Number	Description	Organization Name	Teams Values	CivicAddressID	Location	Location ID
Headquarters	1	Data Center		HQ-Floor 1-Data-SW-1	30050	HQ-Floor 1-Data-SW-1:01	01	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 1- Data Center	6d8cc82-1909-4233-85ad-35721a0e7862
	1	Data Center		HQ-Floor 1-Data-SW-1	30050	HQ-Floor 1-Data-SW-1:19	19	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec773	Floor 1- Data Center	6d8cc82-1909-4233-85ad-35721a0e7862
	1	Data Center		HQ-Floor 1-Data-SW-1	30050	HQ-Floor 1-Data-SW-1:10	10	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec774	Floor 1- Data Center	6d8cc82-1909-4233-85ad-35721a0e7862
	1	Data Center		HQ-Floor 1-Data-SW-1	30050	HQ-Floor 1-Data-SW-1:40	40	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec775	Floor 1- Data Center	6d8cc82-1909-4233-85ad-35721a0e7862
	1	Data Center		HQ-Floor 1-Data-SW-1	30050	HQ-Floor 1-Data-SW-1:37	37	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec776	Floor 1- Data Center	6d8cc82-1909-4233-85ad-35721a0e7862
	1	Data Center		HQ-Floor 1-Data-SW-1	30050	HQ-Floor 1-Data-SW-1:11	11	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec777	Floor 1- Data Center	6d8cc82-1909-4233-85ad-35721a0e7862
	2	Wiring Closet		HQ-Floor 2-Data-SW-1	63059	HQ-Floor 2-Data-SW-1:14	14	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 2- Wiring Closet	88090f16-53fb-4633-b101-348b2dcae108
	2	Wiring Closet		HQ-Floor 2-Data-SW-1	63059	HQ-Floor 2-Data-SW-1:32	32	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec773	Floor 2- Wiring Closet	88090f16-53fb-4633-b101-348b2dcae108
	2	Wiring Closet		HQ-Floor 2-Data-SW-1	63059	HQ-Floor 2-Data-SW-1:07	07	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec774	Floor 2- Wiring Closet	88090f16-53fb-4633-b101-348b2dcae108
	3	Wiring Closet		HQ-Floor 3-Data-SW-1	44048	HQ-Floor 3-Data-SW-1:43	43	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 3- Wiring Closet	65581b30-d7a5-467b-82ec-c857de2b2b21
	3	Wiring Closet		HQ-Floor 3-Data-SW-1	44048	HQ-Floor 3-Data-SW-1:40	40	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec773	Floor 3- Wiring Closet	65581b30-d7a5-467b-82ec-c857de2b2b21
	3	Wiring Closet		HQ-Floor 3-Data-SW-1	44048	HQ-Floor 3-Data-SW-1:22	22	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec774	Floor 3- Wiring Closet	65581b30-d7a5-467b-82ec-c857de2b2b21
	3	Wiring Closet		HQ-Floor 3-Data-SW-1	44048	HQ-Floor 3-Data-SW-1:06	06	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec775	Floor 3- Wiring Closet	65581b30-d7a5-467b-82ec-c857de2b2b21
	4	Wiring Closet		HQ-Floor 4-Data-SW-1	23247	HQ-Floor 4-Data-SW-1:17	17	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 4- Wiring Closet	4e85f7a5-1d5e-4884-8158-9dcb57cee3f
	4	Wiring Closet		HQ-Floor 4-Data-SW-1	23247	HQ-Floor 4-Data-SW-1:21	21	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec773	Floor 4- Wiring Closet	4e85f7a5-1d5e-4884-8158-9dcb57cee3f
	4	Wiring Closet		HQ-Floor 4-Data-SW-1	23247	HQ-Floor 4-Data-SW-1:31	31	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec774	Floor 4- Wiring Closet	4e85f7a5-1d5e-4884-8158-9dcb57cee3f
	5	Wiring Closet		HQ-Floor 5-Data-SW-1	30787	HQ-Floor 5-Data-SW-1:30	30	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec772	Floor 5- Wiring Closet	e6006faa-1434-454e-bfae-79898ae9525
	5	Wiring Closet		HQ-Floor 5-Data-SW-1	30787	HQ-Floor 5-Data-SW-1:06	06	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec773	Floor 5- Wiring Closet	e6006faa-1434-454e-bfae-79898ae9525
	5	Wiring Closet		HQ-Floor 5-Data-SW-1	30787	HQ-Floor 5-Data-SW-1:43	43	Vickers-Headquarters	Panhandle Consumer Industries		7c81ade3-6e35-4cc2-8feb-98e1ca4ec774	Floor 5- Wiring Closet	e6006faa-1434-454e-bfae-79898ae9525
	Manufacturing	1	Data Center		MA-Floor 1-Data-SW-1	67500	MA-Floor 1-Data-SW-1:01	01	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1- Data Center
1		Data Center		MA-Floor 1-Data-SW-1	67500	MA-Floor 1-Data-SW-1:24	24	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1- Data Center	8538a95268d3c-8b08991a-48133f6cc9375
1		Data Center		MA-Floor 1-Data-SW-1	67500	MA-Floor 1-Data-SW-1:07	07	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1- Data Center	8538a95268d3c-8b08991a-48133f6cc9375
1		Data Center		MA-Floor 1-Data-SW-1	67500	MA-Floor 1-Data-SW-1:18	18	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1- Data Center	8538a95268d3c-8b08991a-48133f6cc9375
1		Data Center		MA-Floor 1-Data-SW-1	67500	MA-Floor 1-Data-SW-1:30	30	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 1- Data Center	8538a95268d3c-8b08991a-48133f6cc9375
2		Wiring Closet		MA-Floor 2-Data-SW-1	43695	MA-Floor 2-Data-SW-1:31	31	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2- Wiring Closet	0758f8040e5a-6e65443b-752239fc0323
2		Wiring Closet		MA-Floor 2-Data-SW-1	43695	MA-Floor 2-Data-SW-1:39	39	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2- Wiring Closet	0758f8040e5a-6e65443b-752239fc0323
2		Wiring Closet		MA-Floor 2-Data-SW-1	43695	MA-Floor 2-Data-SW-1:42	42	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 2- Wiring Closet	0758f8040e5a-6e65443b-752239fc0323
3		Wiring Closet		MA-Floor 3-Data-SW-1	11343	MA-Floor 3-Data-SW-1:11	11	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3- Wiring Closet	0332c65484f3f-8f14876f-44532c6cf5189
3		Wiring Closet		MA-Floor 3-Data-SW-1	11343	MA-Floor 3-Data-SW-1:35	35	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3- Wiring Closet	0332c65484f3f-8f14876f-44532c6cf5189
3		Wiring Closet		MA-Floor 3-Data-SW-1	11343	MA-Floor 3-Data-SW-1:23	23	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3- Wiring Closet	0332c65484f3f-8f14876f-44532c6cf5189
3		Wiring Closet		MA-Floor 3-Data-SW-1	11343	MA-Floor 3-Data-SW-1:21	21	Manufacturing	Panhandle Consumer Industries		d9e1fa53-33a7-44a4-abaf-37714a6b367b	Floor 3- Wiring Closet	0332c65484f3f-8f14876f-44532c6cf5189
R & D	1	Data Center		RD-Floor 1-Data-SW-1	28681	RD-Floor 1-Data-SW-1:05	05	The Lab - R&D	PCI-Product Development		0d99f93b-747a-455e-b2bc-d224eab9ce90	Floor 1- Data Center	2775f13280d3e-1b91565d-59129d1ba3925
	1	Data Center		RD-Floor 1-Data-SW-1	28681	RD-Floor 1-Data-SW-1:19	19	The Lab - R&D	PCI-Product Development		0d99f93b-747a-455e-b2bc-d224eab9ce90	Floor 1- Data Center	2775f13280d3e-1b91565d-59129d1ba3925
	1	Data Center		RD-Floor 1-Data-SW-1	28681	RD-Floor 1-Data-SW-1:04	04	The Lab - R&D	PCI-Product Development		0d99f93b-747a-455e-b2bc-d224eab9ce90	Floor 1- Data Center	2775f13280d3e-1b91565d-59129d1ba3925
Customer Service Center	6	Data Center		CS-Floor 6-Data-SW-1	66409	CS-Floor 6-Data-SW-1:24	24	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 6- Data Center	9228c82841c3d-0e44091d-64589b4ef6510
	6	Data Center		CS-Floor 6-Data-SW-1	66409	CS-Floor 6-Data-SW-1:42	42	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 6- Data Center	9228c82841c3d-0e44091d-64589b4ef6510
	6	Data Center		CS-Floor 6-Data-SW-1	66409	CS-Floor 6-Data-SW-1:43	43	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 6- Data Center	9228c82841c3d-0e44091d-64589b4ef6510
	6	Data Center		CS-Floor 6-Data-SW-1	66409	CS-Floor 6-Data-SW-1:34	34	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 6- Data Center	9228c82841c3d-0e44091d-64589b4ef6510
	6	Data Center		CS-Floor 6-Data-SW-1	66409	CS-Floor 6-Data-SW-1:26	26	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 6- Data Center	9228c82841c3d-0e44091d-64589b4ef6510
	9	Wiring Closet		CS-Floor 9-Data-SW-1	59652	CS-Floor 9-Data-SW-1:11	11	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 9- Wiring Closet	1212f82791c1d-4c82856d-54667a3bf6300
	9	Wiring Closet		CS-Floor 9-Data-SW-1	59652	CS-Floor 9-Data-SW-1:13	13	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 9- Wiring Closet	1212f82791c1d-4c82856d-54667a3bf6300
	9	Wiring Closet		CS-Floor 9-Data-SW-1	59652	CS-Floor 9-Data-SW-1:16	16	CSC-Customer Service	PCI-CSC		00d751d1-e39a-464b-867c-8f73828b139b	Floor 9- Wiring Closet	1212f82791c1d-4c82856d-54667a3bf6300
	Warehouse	Bulpen	Bulpen Jack 19		WH-North-Data-SW-1	89532	WH-North-Data-SW-1:46	46	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen
Bulpen		Bulpen Jack 10		WH-North-Data-SW-1	89532	WH-North-Data-SW-1:02	02	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	1924d70509a0f-0c15945d-72364b9fe3673
Bulpen		Bulpen Jack 04		WH-North-Data-SW-1	89532	WH-North-Data-SW-1:32	32	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	1924d70509a0f-0c15945d-72364b9fe3673
Bulpen		Bulpen Jack 13		WH-North-Data-SW-1	89532	WH-North-Data-SW-1:01	01	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	1924d70509a0f-0c15945d-72364b9fe3673
Bulpen		Bulpen Jack 14		WH-North-Data-SW-1	89532	WH-North-Data-SW-1:29	29	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	2071b151538e7b-1d56931e-25476d2cc9763
Bulpen		Bulpen Jack 01		WH-North-Data-SW-2	50294	WH-North-Data-SW-2:22	22	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	2071b151538e7b-1d56931e-25476d2cc9763
Bulpen		Bulpen Jack 05		WH-West-Data-SW-2	28395	WH-West-Data-SW-2:43	43	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	7364d71052f1d-0e95109c-32983c3fa3888
Bulpen		Bulpen Jack 25		WH-West-Data-SW-2	28395	WH-West-Data-SW-2:25	25	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	7364d71052f1d-0e95109c-32983c3fa3888
Bulpen		Bulpen Jack 07		WH-West-Data-SW-2	28395	WH-West-Data-SW-2:44	44	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	7364d71052f1d-0e95109c-32983c3fa3888
Bulpen		Bulpen Jack 20		WH-West-Data-SW-2	28395	WH-West-Data-SW-2:14	14	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	7364d71052f1d-0e95109c-32983c3fa3888
Bulpen		Bulpen Jack 12		WH-West-Data-SW-2	28395	WH-West-Data-SW-2:26	26	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	7364d71052f1d-0e95109c-32983c3fa3888
Bulpen		Bulpen Jack 32		WH-West-Data-SW-2	28395	WH-West-Data-SW-2:32	32	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	2501e53225b8b-8f54662f-732329a6bb8627
Bulpen		Bulpen Jack 22		WH-West-Data-SW-2	28395	WH-West-Data-SW-2:41	41	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Bulpen	2501e53225b8b-8f54662f-732329a6bb8627
Bulpen		Data Center		WH-South-Data-SW-1	35641	WH-South-Data-SW-1:25	25	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Ballpark - Data Center	5890b11995e9f-0f86936c-19175f0fc2305
Bulpen		Data Center		WH-South-Data-SW-1	35641	WH-South-Data-SW-1:24	24	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Ballpark - Data Center	5890b11995e9f-0f86936c-19175f0fc2305
Bulpen		Data Center		WH-South-Data-SW-1	35641	WH-South-Data-SW-1:31	31	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Ballpark - Data Center	5890b11995e9f-0f86936c-19175f0fc2305
Bulpen		Data Center		WH-South-Data-SW-1	35641	WH-South-Data-SW-1:46	46	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Ballpark - Data Center	5890b11995e9f-0f86936c-19175f0fc2305
Bulpen		Data Center		WH-South-Data-SW-1	35641	WH-South-Data-SW-1:45	45	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Ballpark - Data Center	5890b11995e9f-0f86936c-19175f0fc2305
Bulpen		Data Center		WH-South-Data-SW-1	35641	WH-South-Data-SW-1:21	21	Ballpark	PCI-Logistics		cb3faa9b-1aed-46c8-9995-64f5e681ef56	Ballpark - Data Center	5890b11995e9f-0f86936c-19175f0fc2305

Figure 140 Network Switch Port Network Elements - Summary Table

ChassisID	PortID	Description	LocationID
30050,01	HQ-Floor 1-Data-SW-1:01	6d8ccc82-f909-4233-85ad-35721a0e7862	
30050,19	HQ-Floor 1-Data-SW-1:19	6d8ccc82-f909-4233-85ad-35721a0e7862	
30050,10	HQ-Floor 1-Data-SW-1:10	6d8ccc82-f909-4233-85ad-35721a0e7862	
30050,40	HQ-Floor 1-Data-SW-1:40	6d8ccc82-f909-4233-85ad-35721a0e7862	
30050,37	HQ-Floor 1-Data-SW-1:37	6d8ccc82-f909-4233-85ad-35721a0e7862	
30050,11	HQ-Floor 1-Data-SW-1:11	6d8ccc82-f909-4233-85ad-35721a0e7862	
63059,14	HQ-Floor 2-Data-SW-1:14	88090f16-53fb-4633-b101-348b2dcae108	
63059,32	HQ-Floor 2-Data-SW-1:32	88090f16-53fb-4633-b101-348b2dcae108	
63059,07	HQ-Floor 2-Data-SW-1:07	88090f16-53fb-4633-b101-348b2dcae108	
44048,43	HQ-Floor 3-Data-SW-1:43	65581b30-d7a5-467b-82ec-c857de2b2b21	
44048,40	HQ-Floor 3-Data-SW-1:40	65581b30-d7a5-467b-82ec-c857de2b2b21	
44048,22	HQ-Floor 3-Data-SW-1:22	65581b30-d7a5-467b-82ec-c857de2b2b21	
44048,06	HQ-Floor 3-Data-SW-1:06	65581b30-d7a5-467b-82ec-c857de2b2b21	
23247,17	HQ-Floor 4-Data-SW-1:17	4e85f7a5-1d5e-4884-8158-9dcba57cee3f	
23247,21	HQ-Floor 4-Data-SW-1:21	4e85f7a5-1d5e-4884-8158-9dcba57cee3f	
23247,31	HQ-Floor 4-Data-SW-1:31	4e85f7a5-1d5e-4884-8158-9dcba57cee3f	
30787,30	HQ-Floor 5-Data-SW-1:30	e6006faa-f434-454e-bfae-79898aee9525	
30787,06	HQ-Floor 5-Data-SW-1:06	e6006faa-f434-454e-bfae-79898aee9525	
30787,43	HQ-Floor 5-Data-SW-1:43	e6006faa-f434-454e-bfae-79898aee9525	
67500,01	MA-Floor 1-Data-SW-1:01	8538a95268d3c-8b08991a-48133f6cc9375	
67500,24	MA-Floor 1-Data-SW-1:24	8538a95268d3c-8b08991a-48133f6cc9375	
67500,07	MA-Floor 1-Data-SW-1:07	8538a95268d3c-8b08991a-48133f6cc9375	
67500,18	MA-Floor 1-Data-SW-1:18	8538a95268d3c-8b08991a-48133f6cc9375	
67500,30	MA-Floor 1-Data-SW-1:30	8538a95268d3c-8b08991a-48133f6cc9375	
43695,31	MA-Floor 2-Data-SW-1:31	0758f80430e5a-6e65443b-75223f9fc0323	
43695,39	MA-Floor 2-Data-SW-1:39	0758f80430e5a-6e65443b-75223f9fc0323	
43695,42	MA-Floor 2-Data-SW-1:42	0758f80430e5a-6e65443b-75223f9fc0323	
11343,11	MA-Floor 3-Data-SW-1:11	0332c65484f3f-8f14876f-44532c6cf5189	
11343,35	MA-Floor 3-Data-SW-1:35	0332c65484f3f-8f14876f-44532c6cf5189	
11343,23	MA-Floor 3-Data-SW-1:23	0332c65484f3f-8f14876f-44532c6cf5189	
11343,21	MA-Floor 3-Data-SW-1:21	0332c65484f3f-8f14876f-44532c6cf5189	
28681,05	RD-Floor 1-Data-SW-1:05	2775f13280d3e-1b91565d-59129d1ba3925	
28681,19	RD-Floor 1-Data-SW-1:19	2775f13280d3e-1b91565d-59129d1ba3925	
28681,04	RD-Floor 1-Data-SW-1:04	2775f13280d3e-1b91565d-59129d1ba3925	
66409,24	CS-Floor 6-Data-SW-1:24	9228c82841c3d-0e44091d-64589b4ef6510	
66409,42	CS-Floor 6-Data-SW-1:42	9228c82841c3d-0e44091d-64589b4ef6510	
66409,43	CS-Floor 6-Data-SW-1:43	9228c82841c3d-0e44091d-64589b4ef6510	
66409,34	CS-Floor 6-Data-SW-1:34	9228c82841c3d-0e44091d-64589b4ef6510	
66409,26	CS-Floor 6-Data-SW-1:26	9228c82841c3d-0e44091d-64589b4ef6510	
59652,11	CS-Floor 9-Data-SW-1:11	1212f82791c1d-4c82856d-54667a3bf6300	
59652,34	CS-Floor 9-Data-SW-1:34	1212f82791c1d-4c82856d-54667a3bf6300	
59652,16	CS-Floor 9-Data-SW-1:16	1212f82791c1d-4c82856d-54667a3bf6300	
89532,46	WH-North-Data-SW-1:46	1924d70509a0f-0c15945d-72364b9fe3673	
89532,02	WH-North-Data-SW-1:02	1924d70509a0f-0c15945d-72364b9fe3673	
89532,32	WH-North-Data-SW-1:32	1924d70509a0f-0c15945d-72364b9fe3673	
89532,01	WH-North-Data-SW-1:01	1924d70509a0f-0c15945d-72364b9fe3673	
89532,29	WH-North-Data-SW-1:29	2071b51538e7b-1d56931e-25476d2cc9763	
50294,22	WH-North-Data-SW-2:22	2071b51538e7b-1d56931e-25476d2cc9763	
28395,43	WH-West-Data-SW-2:43	7364d71052f1d-0e95109c-32983c3fa3888	
28395,25	WH-West-Data-SW-2:25	7364d71052f1d-0e95109c-32983c3fa3888	
28395,44	WH-West-Data-SW-2:44	7364d71052f1d-0e95109c-32983c3fa3888	
28395,14	WH-West-Data-SW-2:14	7364d71052f1d-0e95109c-32983c3fa3888	
28395,26	WH-West-Data-SW-2:26	7364d71052f1d-0e95109c-32983c3fa3888	
28395,32	WH-West-Data-SW-2:32	2501e53225b8b-8f54662f-72329a6bb8627	
28395,41	WH-West-Data-SW-2:41	2501e53225b8b-8f54662f-72329a6bb8627	
35641,25	WH-South-Data-SW-1:25	5890b11995e9f-0f86936c-19175f0fc2305	
35641,24	WH-South-Data-SW-1:24	5890b11995e9f-0f86936c-19175f0fc2305	
35641,31	WH-South-Data-SW-1:31	5890b11995e9f-0f86936c-19175f0fc2305	
35641,46	WH-South-Data-SW-1:46	5890b11995e9f-0f86936c-19175f0fc2305	
35641,45	WH-South-Data-SW-1:45	5890b11995e9f-0f86936c-19175f0fc2305	
35641,21	WH-South-Data-SW-1:21	5890b11995e9f-0f86936c-19175f0fc2305	

Figure 141 Network Switch Port Network Elements - Input CSV File

References

Federal Communications Commission

[Multi-line Telephone Systems – Kari’s Law and RAY BAUM’S Act 911 Direct Dialing, Notification, and Dispatchable Location Requirements](#)

Microsoft Dynamic 911 and Work from Home

[Emergency calling terms and conditions](#)

[Manage Emergency Calling](#)

[Plan and configure dynamic emergency calling](#)

[Emergency addresses for remote locations](#)

[Add, change, or remove an emergency location for your organization](#)

[Add, change, or remove a place for an emergency location in your organization](#)

[Assign or change the place for an emergency location for a user](#)

[Emergency Calling Labels](#)

[Manage emergency calling policies in Microsoft Teams](#)

[Manage emergency call routing policies for Direct Routing](#)

[Network settings for cloud voice features in Microsoft Teams](#)

[Manage your network topology for cloud voice features in Microsoft Teams](#)

Microsoft – Other Relevant Teams Voice Articles

[Session Border Controllers certified for Direct Routing](#)

Acronyms

ALI	Automatic Line Identification
AOR	Address of Record
BSSID	Basic Service Set ID
CP	Teams Calling Plans
DIA	Direct Internet Access
DR	Teams Direct Routing
ECC	Emergency Call Center
ECRC	Emergency Call Routing Center
ELIN	Emergency Location Identification Number
ERSP	Emergency Response Service Provider
FCC	Federal Communications Commission
LBR	Teams Location Based Routing
LIS	Location Information System
LLDP-MED	Link layer discovery protocol-Media Endpoint Discovery
LMO	Teams Local Media Optimization
MSAG	Master Street Address Guide
MLTS	Multi-Line Telephone System
OC	Teams Operator Connect
OCO	Operator Connect Operator
PBX	Public Branch Exchange
PSAP	Public Safety Answering Point
RAY BAUM	Repack Airwaves Yielding Better Access for Users of Modern Services
VDI	Virtual Device Infrastructure
VPN	Virtual Private Network
WAP	Wireless Access Point
WFH	Work from Home

Index

- 9
- 933 Test Number _____ 76, 82, 105, 107
- A**
- ALI (Automatic Line Identification) 15, 21, 38, 39, 155, 158, 159, 183
- AOR(Address of Record) _____ 19, 37, 183
- Apple macOS _____ 13
- AudioCodes _____ 41, 84
- Azure Maps _____ 54, 55, 146, 159
- B**
- Boeing Everett Production facility _____ 26
- BSSID (Basic Service Set Identifier) 140, 173, 174, 183
- C**
- Caller ID _____ 41, 75, 76
- Calling Policies __ 17, 24, 25, 26, 28, 29, 34, 35, 50, 52, 83, 90, 125, 126, 158, 164, 165, 166
- calling-debug.txt 76, 78, 79, 80, 84, 86, 87, 89, 90, 91, 92, 93, 94, 101, 102, 103, 104, 110, 114
- CDP (Cisco Discovery Protocol) _____ 44
- CDR (Call Detail Record) _____ 84
- Comma Separated Value _121, 123, 129, 131, 133
- CsOnlineLISCivicAddress _____ 119, 121
- Get-CsOnlineLISCivicAddress _____ 119
- New-CsOnlineLISCivicAddress _____ 121
- CsOnlineLISLocation _____ 120, 123, 124
- Get-CsOnlineLISLocation _____ 120, 123, 124
- New-CsOnlineLISLocation _____ 123
- Remove-CsOnlineLISLocation _____ 123
- Set-CsOnlineLISLocation _____ 123
- CsOnlineLISPort _____ 47, 144
- Get-CsOnlineLISPort _____ 144
- Remove-CsOnlineLISPort _____ 144
- Set-CsOnlineLISPort _____ 47, 144
- CsOnlineLISSubnet _____ 137
- Get-CsOnlineLISSubnet _____ 137
- Remove-CsOnlineLISSubnet _____ 137
- Set-CsOnlineLISSubnet _____ 137
- CsOnlineLISSwitch _____ 142
- Get-CsOnlineLISSwitch _____ 142
- Remove-CsOnlineLISSwitch _____ 142
- Set-CsOnlineLISSwitch _____ 142
- CsOnlineLISWirelessAccessPoint _____ 140
- Get-CsOnlineLISWirelessAccessPoint _____ 140
- Remove-CsOnlineLISWirelessAccessPoint _ 140
- Set-CsOnlineLISWirelessAccessPoint _____ 140
- CsTeamsEmergencyCallingPolicy _____ 52, 126
- Get-CsTeamsEmergencyCallingPolicy__ 52, 126
- Grant-CsTeamsEmergencyCallingPolicy__ 126
- New-CsTeamsEmergencyCallingPolicy_____ 126
- Remove-CsTeamsEmergencyCallingPolicy_ 126
- Set-CsTeamsEmergencyCallingPolicy _ 52, 126
- CsTeamsEmergencyCallRoutingPolicy _____ 127
- Get-CsTeamsEmergencyCallRoutingPolicy_ 127
- Grant-CsTeamsEmergencyCallRoutingPolicy _____ 127
- New-CsTeamsEmergencyCallRoutingPolicy 127
- Remove-CsTeamsEmergencyCallRoutingPolicy _____ 127
- Set-CsTeamsEmergencyCallRoutingPolicy _ 127
- CsTenantNetworkRegion _____ 131
- Get-CsTenantNetworkRegion _____ 131
- New-CsTenantNetworkRegion _____ 131
- Remove-CsTenantNetworkRegion _____ 131
- Set-CsTenantNetworkRegion _____ 131
- CsTenantNetworkSite _____ 132
- Get-CsTenantNetworkSite _____ 132
- New-CsTenantNetworkSite _____ 132
- Remove-CsTenantNetworkSite _____ 132
- Set-CsTenantNetworkSite _____ 132
- CsTenantNetworkSubnet _____ 134
- Get-CsTenantNetworkSubnet _____ 134
- New-CsTenantNetworkSubnet _____ 134
- Remove-CsTenantNetworkSubnet _____ 134
- Set-CsTenantNetworkSubnet _____ 134
- CsTenantTrustedIPAddress _____ 129
- Get-CsTenantTrustedIPAddress _____ 129
- New-CsTenantTrustedIPAddress _____ 129
- Remove-CsTenantTrustedIPAddress _____ 129
- Set-CsTenantTrustedIPAddress _____ 129

D

DefaultLocationID _____ 20
 DIA (Direct Internet Access) _____ 28, 42, 154, 183
 Dispatchable Location__ 12, 14, 15, 16, 17, 19, 21,
 22, 23, 28, 36, 37, 38, 39, 40, 41, 43, 50, 63,
 155, 156, 172, 173, 174, 182
 Dynamic 911 12, 13, 14, 15, 17, 19, 36, 37, 38, 39,
 41, 44, 47, 50, 53, 60, 61, 62, 63, 64, 65, 66, 73,
 74, 75, 76, 79, 87, 89, 90, 91, 92, 93, 95, 105,
 110, 112, 113, 114, 115, 116, 117, 145, 155,
 156, 157, 158, 159, 172, 173, 182

E

ECC (Emergency Call Center) __ 58, 66, 74, 77, 78,
 83, 85, 86, 105, 183
 ECRC(Emergency Call Response Center)__ 38, 58,
 67, 71, 73, 74, 78, 86, 105, 106, 159, 183
 ELIN(Emergency Location Identification Number)
 ____ 20, 22, 38, 39, 40, 41, 58, 119, 123, 159, 183
 Emergency Addresses __ 19, 20, 21, 22, 23, 40, 41,
 42, 47, 100, 101, 117, 118, 119, 121, 158, 159,
 160
 Emergency Location\Places 19, 20, 29, 38, 42, 47,
 64, 68, 80, 82, 158, 183
 Emergency Policies _____ 28, 31, 50, 125, 127
 ERSP(Emergency Routing Service Provider) __ 12,
 15, 18, 21, 28, 32, 33, 34, 38, 39, 40, 41, 42, 53,
 58, 65, 66, 67, 72, 73, 74, 75, 77, 82, 84, 85, 86,
 104, 107, 108, 109, 110, 158, 159, 183

F

FCC(Federal Communications Commission) __ 13,
 115, 182, 183
 First Responders _____ 21

G

Geocodes __ 14, 20, 22, 23, 36, 37, 54, 55, 56, 59,
 121, 158, 159

I

Institute of Electronics and Electrical Engineers44
 Intrado _____ 15
 IPv4 _____ 28, 29, 30, 42, 43, 128, 133, 135
 IPv6 _____ 28, 29, 30, 42, 43, 128, 133, 135, 154
 ISP(Internet Service Provider)_____ 28, 42, 89, 154

K

Kennedy Space Center _____ 16

L

Latitude 14, 20, 22, 36, 54, 66, 80, 83, 94, 98, 118,
 119, 121, 158
 LIS Network Elements 37, 42, 43, 44, 98, 101, 135,
 172, 175, 176, 177, 178, 179, 180, 181
 Subnets28, 29, 30, 42, 43, 44, 97, 102, 120, 133,
 134, 136, 137, 150, 153, 158, 169, 170, 171,
 172
 Switch Ports _____ 43, 44, 121, 143
 Switches _____ 43, 44, 120, 141, 151, 159, 172
 Wireless Access Points__ 42, 53, 120, 139, 152,
 154, 159, 172, 173, 174, 177
 LIS(Location Information System) _ 19, 21, 22, 23,
 30, 42, 43, 44, 46, 85, 90, 91, 92, 94, 98, 99,
 101, 102, 103, 108, 109, 120, 121, 135, 136,
 137, 138, 139, 141, 143, 158, 172, 174, 183
 LLDP-Med (Link Layer Discovery Protocol –
 Media Endpoint Discovery) _____ 44, 45, 46, 183
 LMO(Teams Local Media Optimization) _ 29, 131,
 183

Location Not Detected _____ 59, 67
 Location Privacy Settings _____ 54, 59
 Location Services _____ 80, 90, 94
 LocationID _____ 20, 22, 121, 124
 Longitude _____ 20

M

Microsoft Intune _____ 80
 Microsoft Lync _____ 15
 Microsoft Technical Support _____ 79, 84, 85
 Microsoft Windows _____ 13
 MLTS(Multi-Line Telephone System) __ 13, 14, 17,
 19, 24, 31, 34, 36, 50, 60, 63, 115, 183
 MSAG(Master Street Address Guide)22, 118, 119,
 146, 183

N

NASA Vehicle Assembly Building _____ 16
 Notification Requirement _____ 14, 24
 O

Operator Connect__12, 17, 19, 20, 21, 22, 23, 24,
 31, 34, 35, 36, 37, 38, 41, 42, 58, 61, 63, 65, 66,

72, 73, 74, 75, 79, 82, 83, 84, 85, 86, 90, 91, 94, 101, 104, 105, 106, 107, 114, 120, 183	114, 147, 148, 154, 155, 157, 158, 159, 162, 164, 182, 183
Operator Connect Operator _____ 19, 183	Teams Emergency Call Routing Policies ___ 24, 26, 28, 29, 31, 32, 33, 34, 42, 71, 72, 86, 102, 114, 157, 158, 163, 168
Organization Name ____ 20, 21, 22, 23, 118, 119	Dynamic emergency calling switch ____ 12, 79
P	Teams Emergency Calling Policies 17, 24, 25, 26, 27, 28, 29, 34, 35, 52, 75, 86, 90, 93, 96, 97, 101, 103, 125, 126, 158, 164, 165, 166
PBX(Private Branch Exchange) _____ 15, 155, 183	External Location Lookup Mode 52, 90, 93, 165
PIDF-LO (Presence Information Data Format – Location Object) 38, 39, 40, 42, 58, 85, 108, 109, 159	Teams Local Media Optimization _____ 29, 183
PSAP (Public Safety Answering Point) _ 12, 15, 18, 19, 21, 24, 28, 32, 38, 39, 40, 41, 42, 50, 53, 58, 63, 64, 66, 67, 68, 70, 71, 72, 73, 74, 75, 77, 78, 83, 85, 86, 105, 106, 108, 110, 111, 114, 156, 159, 183	Teams Mobile client for Android _____ 13
PSTN (Public Switched Telephone System) 31, 33, 34, 72, 84, 107, 109, 147, 148, 163, 164	Teams Online Voice Routing Policies _____ 32
R	Teams Operator Connect _____ 183
RAY BAUM Act _ 14, 17, 19, 28, 32, 34, 39, 41, 43, 50, 60, 63, 74, 115, 157	Teams Phone _____ 13, 19, 148
S	Teams Phone System _____ 19, 148
SBC(Session Border Controller) 12, 28, 29, 31, 32, 33, 34, 38, 39, 40, 41, 42, 53, 58, 71, 72, 73, 75, 76, 84, 85, 107, 108, 109, 114, 147, 148, 157, 159, 162, 163, 164, 182	Teams Rooms _____ 13
SDP (Session Description Protocol) _____ 38, 72, 85, 108, 109	Teams Voice Routing _____ 33, 148
SIP Trunk Vendors __ 39, 42, 65, 72, 73, 74, 84, 85, 107, 108, 109	Dialed Number Pattern _____ 33, 163
Skype for Business _____ 13, 15	PSTN Usage _____ 31, 33, 34, 84, 164
Suggested Address _____ 55, 56	Voice Routes _____ 33, 164
T	Teams Web Client _____ 13
TAC(Teams Admin Center) _ 19, 20, 22, 25, 31, 41, 43, 47, 50, 84, 96, 97, 98, 99, 100, 101, 107, 109, 117, 121, 122, 125, 126, 127, 128, 130, 132, 133, 134, 135, 136, 139, 141, 143, 144, 159	Tenant Network Regions ___ 28, 29, 42, 102, 130, 131, 167, 168
Teams Administrator Permissions _____ 27, 125	Tenant Network Sites _ 26, 28, 29, 31, 42, 98, 102, 132, 134, 158, 163, 168, 169
Teams Calling Line Identity Policy _____ 41, 76	Tenant Network Subnets 28, 29, 30, 42, 102, 133, 134, 158, 169, 170, 171, 172
Teams Calling Plans _____ 12, 148, 155, 183	Tenant Trusted IP Addresses 28, 42, 96, 101, 128, 129, 166, 167
Teams Desktop Client _____ 13, 102	Test Number _____ 65, 76, 82, 105, 107
Teams Direct Routing __ 12, 15, 17, 19, 21, 24, 29, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 53, 58, 62, 63, 65, 66, 71, 72, 73, 74, 75, 82, 83, 84, 85, 90, 91, 93, 94, 96, 97, 101, 104, 107, 108,	V
	VAB(NASA Vehicle Assembly Building) _____ 16
	VDI(Virtual Desktop Infrastructure) __ 36, 110, 183
	VPN(Virtual Private Networking) ____ 30, 110, 183
	W
	WFH(Work from Home) 12, 13, 17, 25, 26, 28, 36, 37, 38, 50, 52, 53, 55, 59, 60, 61, 62, 63, 64, 65, 66, 73, 74, 75, 76, 77, 78, 79, 80, 84, 85, 86, 89, 90, 93, 102, 103, 104, 105, 106, 108, 109, 110, 114, 116, 156, 157, 158, 159, 162, 163, 172, 182, 183
	Manual Address Entry _____ 57
	Unvalidated Address _____ 38

Validated Address _____ 119

Work Location _____ 77, 80