Using CyberData Devices on Microsoft Teams with Ribbon

Document Part # 931816A
Relevant for all CyberData products

CyberData Corporation
3 Justin Court
Monterey, CA 93940
(831) 373-2601

Using CyberData Devices on Microsoft Teams with Ribbon
Document # 931816A

Revision Information

12/2/20 – Initial Release

Table of Contents

1.0 Why use Ribbon?

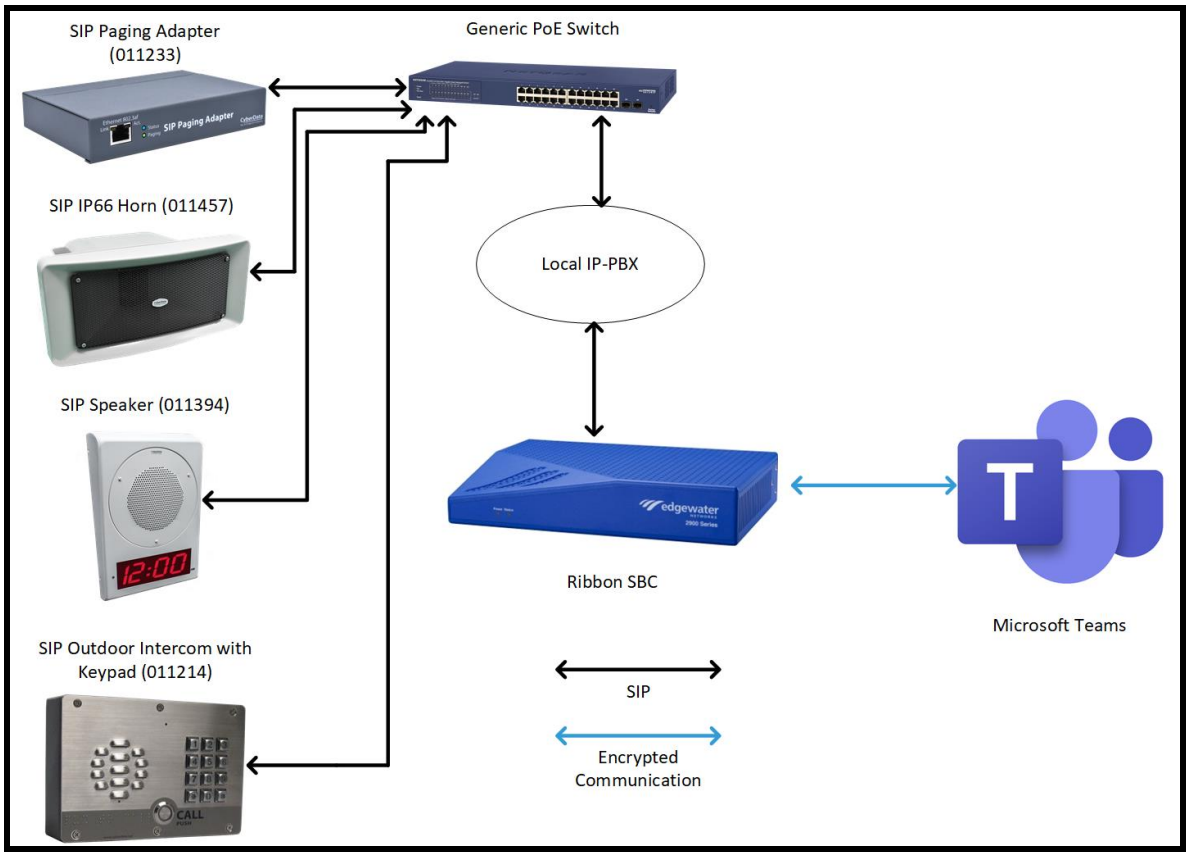
Using CyberData devices on the Microsoft Teams platform requires an intermediary device to communicate between Microsoft Teams and the CyberData hardware. This is due to limitations on what hardware can operate in the Microsoft Teams environment. As such, manufacturers like Ribbon are required to facilitate that operation. There are a variety of options to connect endpoints to Microsoft Teams. Ribbon makes a fantastic set of session border controllers (SBCs) that can facilitate using CyberData devices with Microsoft Teams.

Ribbon is a manufacturer of SBCs that can integrate with Microsoft Teams utilizing the Direct Routing feature. This allows for extension numbers to be dialed directly from Microsoft Teams that correlate with CyberData endpoints like intercoms, paging adapters, or speakers. This functionality works in both directions, allowing not only calls to be made from Microsoft Teams to CyberData Devices but CyberData hardware to Microsoft Teams. This facilitates the simple integration of any CyberData product into a Microsoft Teams environment.

With a one-time fee, Ribbon is a great choice for integrating any hardware with Microsoft Teams. Ribbon has a large line of hardware to connect VoIP accessory devices to Microsoft Teams. These units range from virtual machine-based options to large rack-mountable devices and are great hardware-based alternatives to use with Teams.

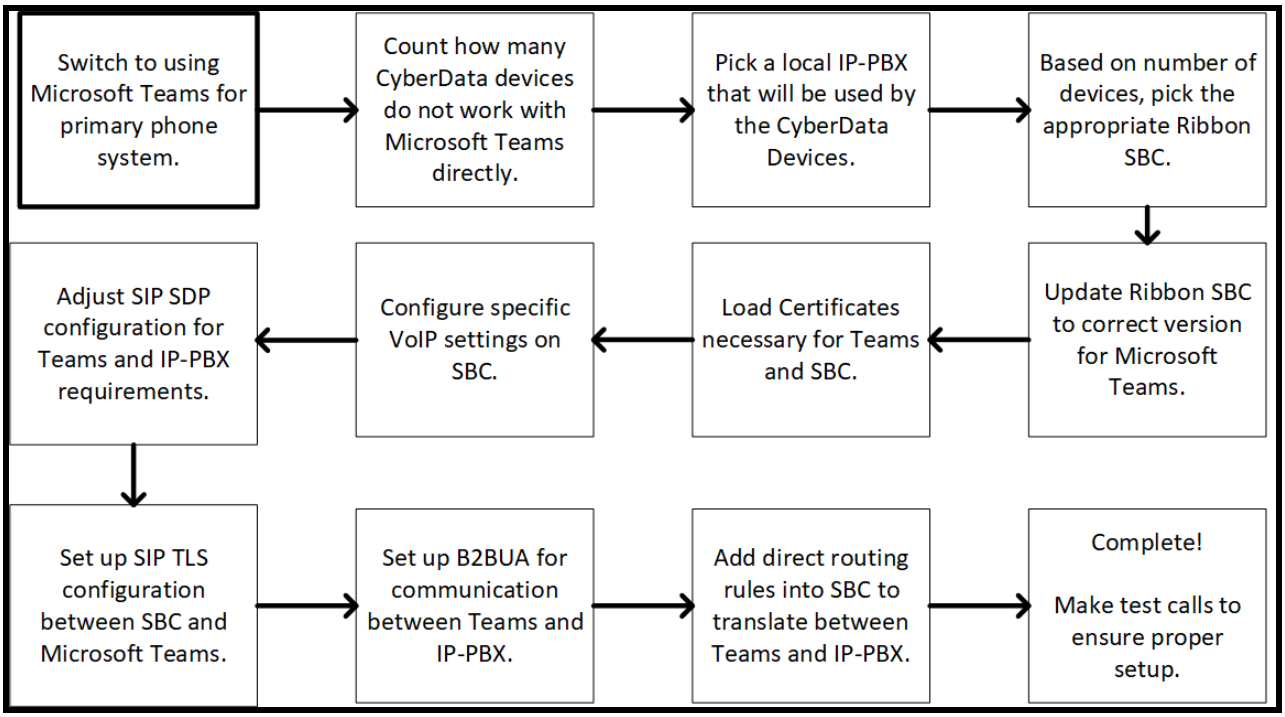
1.1 Implementation Diagram

Figure 1-1. Implementation Example



1.2 Connecting Ribbon to Microsoft Teams

Figure 1-2. Process map of Ribbon Integration with Microsoft Teams



1.3 Pre-Requisites for Integrating Ribbon SBC and Microsoft Teams

There are several items that are required to successfully integrate the Ribbon hardware and Microsoft Teams. Make sure all of these are supported before progressing.

- Microsoft Teams, Office 365 account.
- A domain in Office 365 with FQDN that is owned by the site.
- User(s) in Office 365 with at least E3 or E5 license(s) that supports direct routing.
- IP-PBX on-premise or hosted for use with Microsoft Teams.
- A domain (which is FQDN) with a valid certificate.
- EdgeMarc device with firmware version 15.6.0 or later.
- Capability to create a SIP Trunk.

Assuming that all the pre-requisites are met, please follow these steps to set up the Session Border Controller for use with Microsoft Teams.

1.3.1 Overview of Steps Required

These steps are a '1000-foot view' of the steps required to complete the process. These steps will be defined in more depth in subsequent sections.

EdgeMarc Setup steps

1. Ensure firmware version 15.6.0 or above.
2. Load certificates necessary for Trunks, Microsoft Teams, and SBC.
3. Change VoIP Settings on SBC.
4. Change SIP SDP settings for requirements of IP-PBX.
5. Set up SIP TLS rules for communication between SBC and Microsoft Teams.
6. Set up Back to Back User Agent (B2BUA) for communication between Microsoft Teams and IP-PBX.
7. Add direct routing rules into SBC to translate calls from IP-PBX to Microsoft Teams and from Teams to IP-PBX.

1.4 Picking the Right Ribbon SBC

Ribbon produces many different SBCs and it can be tough to pick the right one for each deployment. For this document, we will outline "Microsoft Certified Edge SBCs" which are designed for Small Business to Enterprise level customers. These SBCs are designed to sit on the edge of the network and interface with Microsoft Teams and a local IP-PBX.

There are three main factors when choosing an SBC for a deployment, number of total sessions, Hardware/Virtualized server, and Connection options. Here is a chart from Ribbon to help with that determination.

Edgeview Management *– A centralized interface to monitor and troubleshoot issues with SBC and Trunks.*

Sessions *– Number of concurrent calls.*

SBC Product Line	Edgeview Management	Number of Sessions	Hardware or Virtualized	Notes/Connection options
SBC SWe Lite	Yes	1,000	Virtualized or Public Cloud	-
SBC 1000	No	192	Hardware	FXO/FXS Ports
SBC 2000	No	600	Hardware	T1/E1 & FXS Ports
Edgemarc 2900	Yes	300	Hardware	FXS & PoE Ports
Edgemarc 4000	Yes	500	Hardware	T1/E1 & FXS Ports
Edgemarc 6000	Yes	500	Hardware	LTE WAN option, T1/E1 & FXS Ports
Edgemarc 7000	Yes	2,000	Hardware	7400: Hot Swappable Power Supplies

2.0 Ribbon SBC Setup Steps

These steps go into detail on how to prepare the Ribbon SBC to integrate with Microsoft Teams Office 365.

2.1 Updating Firmware

1. Log into the Ribbon SBC and check the firmware version and upgrade if necessary. Admin → Upgrade Firmware

Note: *The firmware version used in testing was firmware 15.6.0, the version may have been updated after the release of this guide.*

2.2 Uploading Certificates

1. Certificates must be uploaded to the Ribbon Device. Security → Certificates

Note: *The number and type of certificates required will vary with each deployment.*

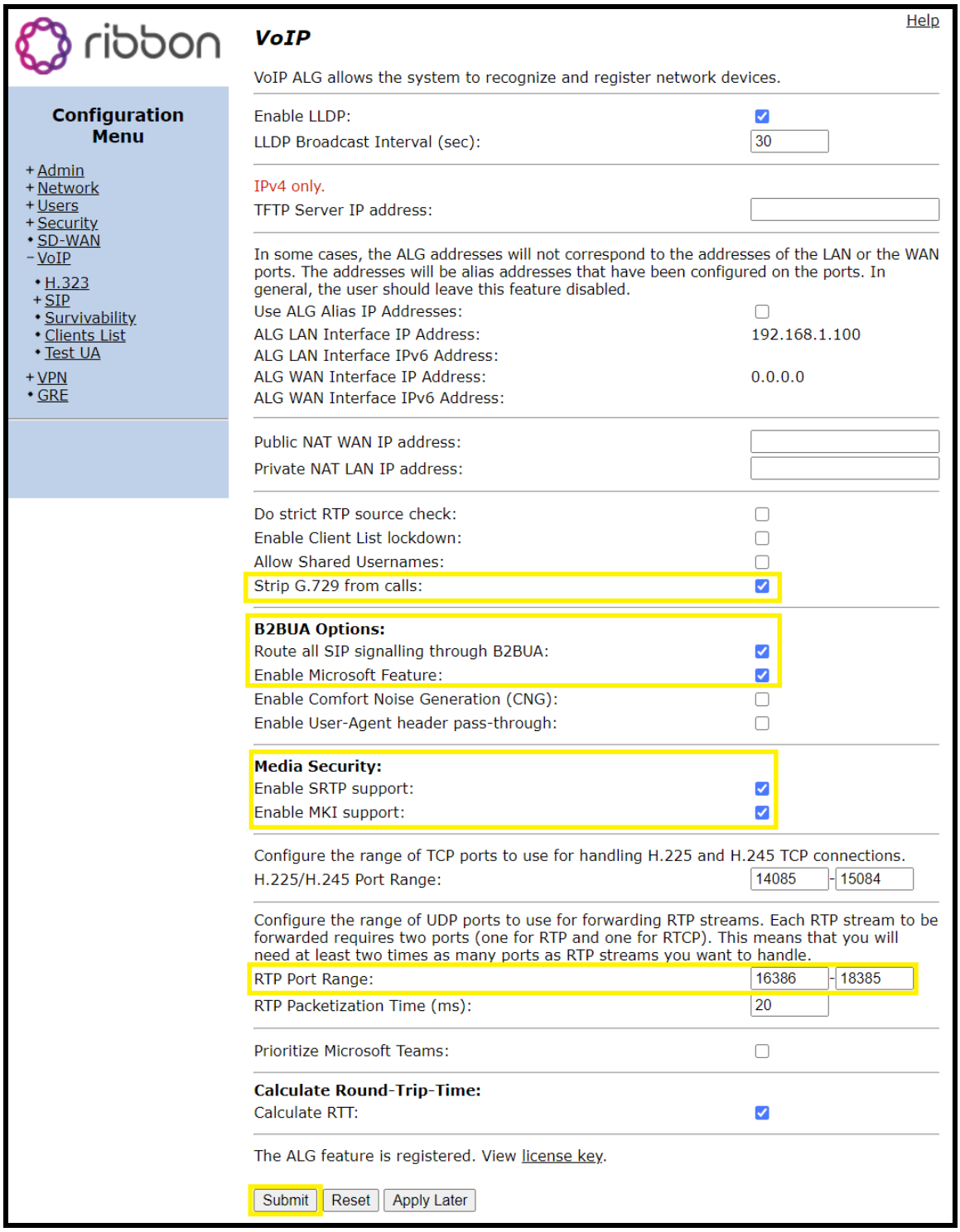
Note: *Certificates can also be created by the SBC that are either self-signed OR the SBC can facilitate a signing request from a certificate authority.*

2.3 VoIP Settings

1. VoIP Settings must be changed to work with Microsoft Teams. To reach VoIP Settings, click on **VoIP.**
2. Make the following changes:
    a. Check the box for "**Strip G.729 from Calls**".
    b. Check the box for "**Route all SIP signaling through B2BUA**".
    c. Check the box for "**Enable Microsoft Feature**".
    d. Check the box for "**Enable SRTP Support**".
    e. Check the box for "**Enable MKI Support**".
    f. Adjust the RTP Port Range in accordance with how many ports are required.

Note: *Each device will need two RTP ports, one for RTP and one for RTCP, so at least double the number of devices that will be used with the SBC.*

Figure 2-1. VoIP Settings



3. Click Submit to save changes.
4. From **VoIP** click on **SIP**.

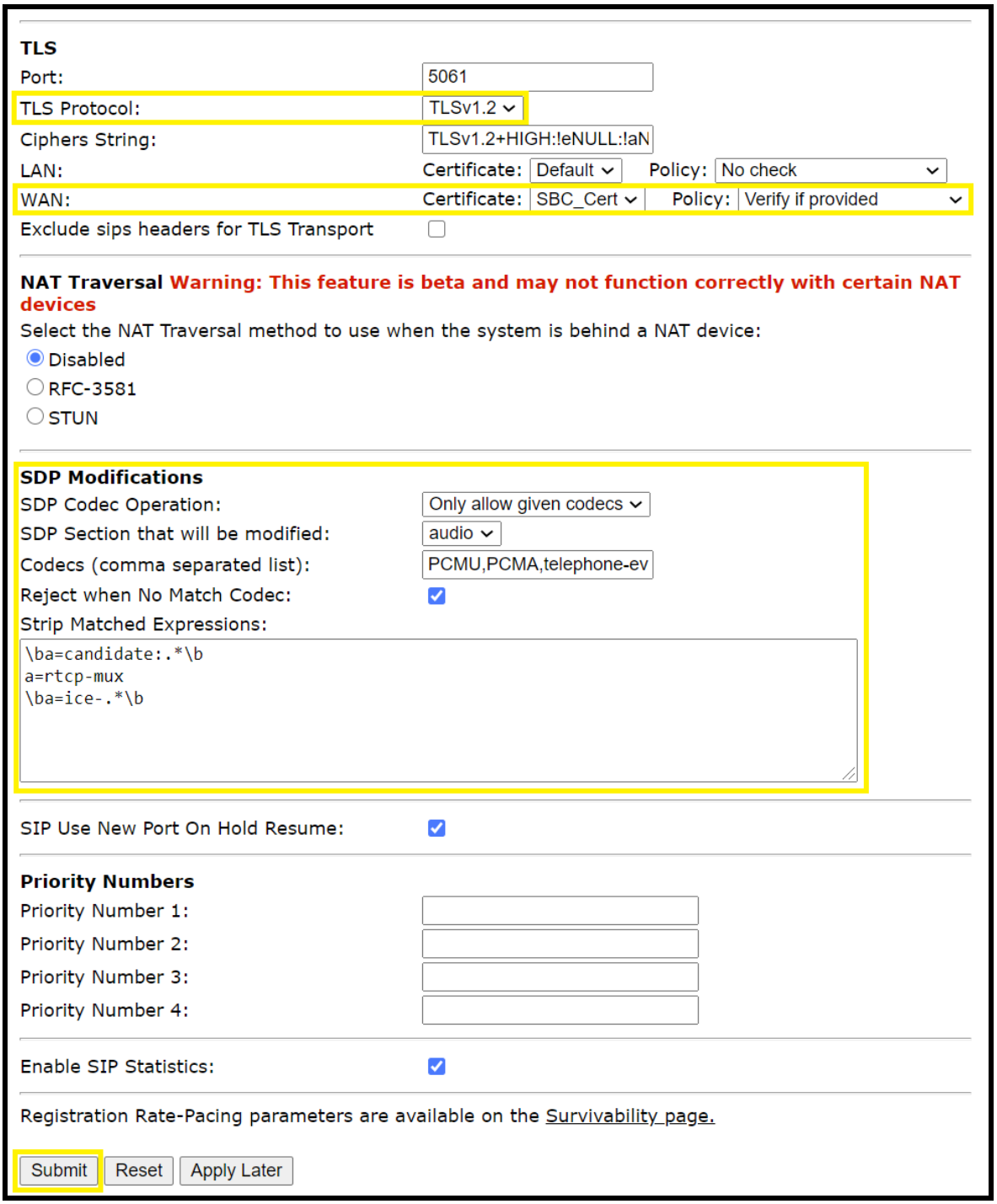
2.4 TLS Settings

1. In the TLS Section set TLS Protocol to TLSv1.2.
2. Set the LAN and WAN certificates to the required certificates from the earlier step.
3. Set the WAN certificate policy to "**Verify if provided**".
4. Check the box for "**Exclude sips headers for TLS Transport**".
5. In the **SDP Modifications** section make the following adjustments:
    a. Set SDP Codec Operation to "Only allow given codecs".
    b. Set SDP Section that will be modified to "Audio".
    c. In the Codecs section, enter "PCMU, PCMA, telephone-event".
    d. Add these expressions to "Strip Matched Expressions":

\ba=candidate:.*\b
a=rtcp-mux
\ba=ice-.*\b

Note: *Enabling SIP Statistics is not required but can be helpful for analytics.*

Figure 2-2. TLS Settings



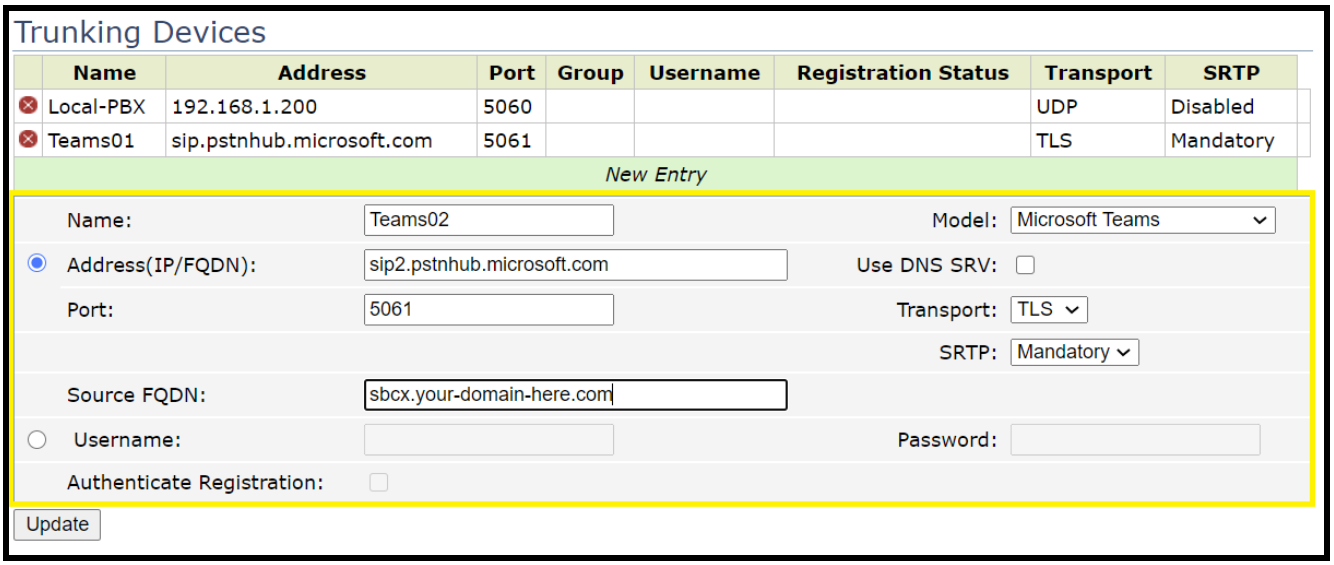
6. Click Submit to save changes.

2.5 B2BUA and Trunk Settings

1. From **SIP** navigate to **B2BUA** to set the trunking devices.
2. Add the Name, Address, Model, Port, Transport, SRTP, and Source FQDN for all necessary trunks.

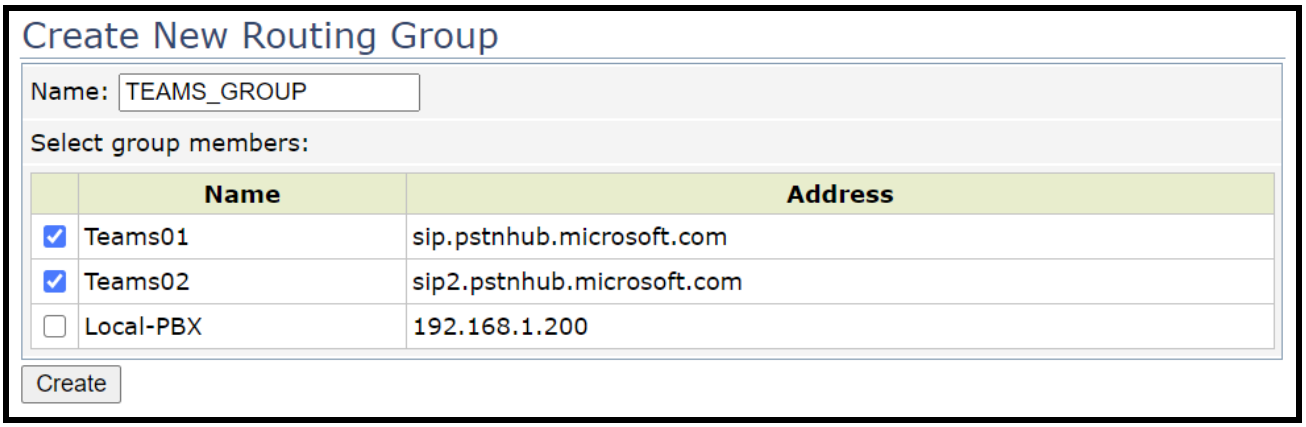
Note: *Each Microsoft Teams implementation is different, some may have more trunks than others.*

Figure 2-3. B2BUA Trunking Configuration



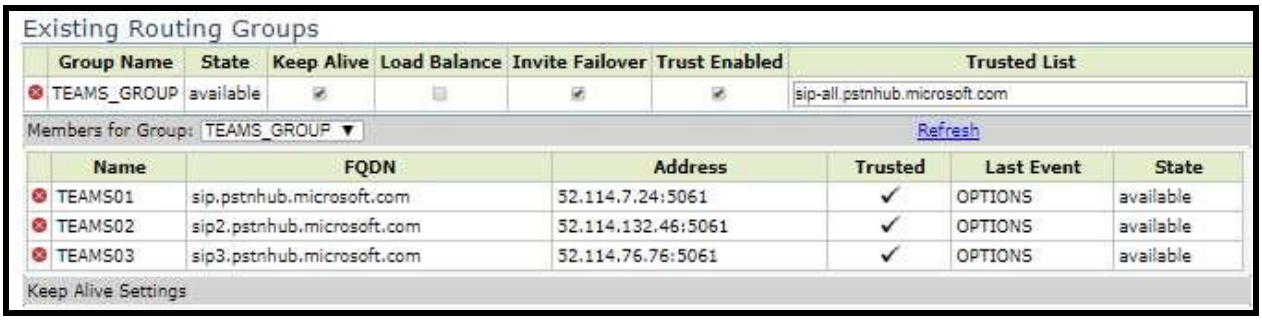
3. Next create routing groups to handle priorities between the different trunks. From **SIP** select **Trunking Group Availability**.
4. Create the routing group by setting the name and checking the boxes for all the Teams servers.

Figure 2-4. Create a New Routing Group



5. Next. Check the boxes to set the "Keep Alive", "Invite Failover" and "Trust Enabled" for the routing group.

Figure 2-5. Routing Group Settings



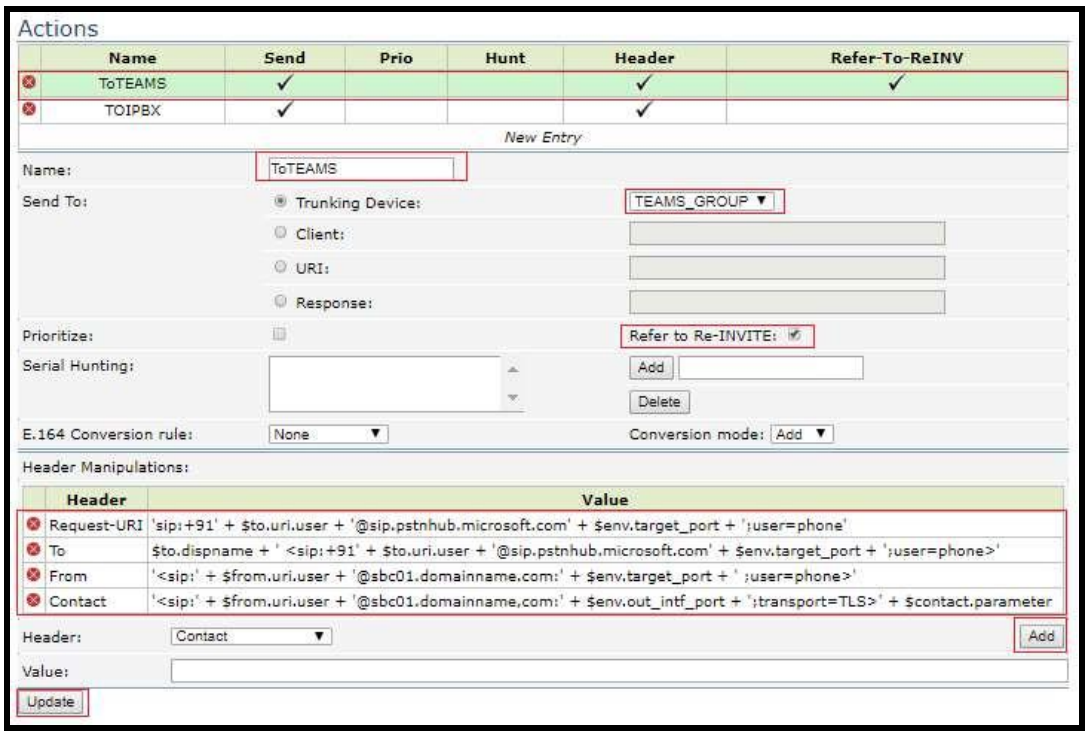
6. Click Submit to confirm all changes.
7. Next, rules need to be created to convert calls from local PBX to Teams and from Teams to local PBX
8. Navigate to B2BUA and scroll to Actions.
9. Create rules for 'To_Teams' to send messages from local PBX to teams.
10. Rules need to be created for the "Request-URI", "To", "From", and "Contact" Headers.

Note: This is the syntax necessary for the rules. Set the country code as required for the location.

Request-URI 'sip:+91' + $to.uri.user + '@sip.pstnhub.microsoft.com' + $env.target_port + ';user=phone'
To $to.dispname + ' <sip:+91' + $to.uri.user + '@sip.pstnhub.microsoft.com' + $env.target_port + ';user=phone>'
From '<sip:' + $from.uri.user + '@sbc01.domainname.com:' + $env.target_port + ' ;user=phone>'
Contact '<sip:' + $from.uri.user + '@sbc01.domainname.com:' + $env.out_intf_port + ';transport=TLS>' + $contact.parameter

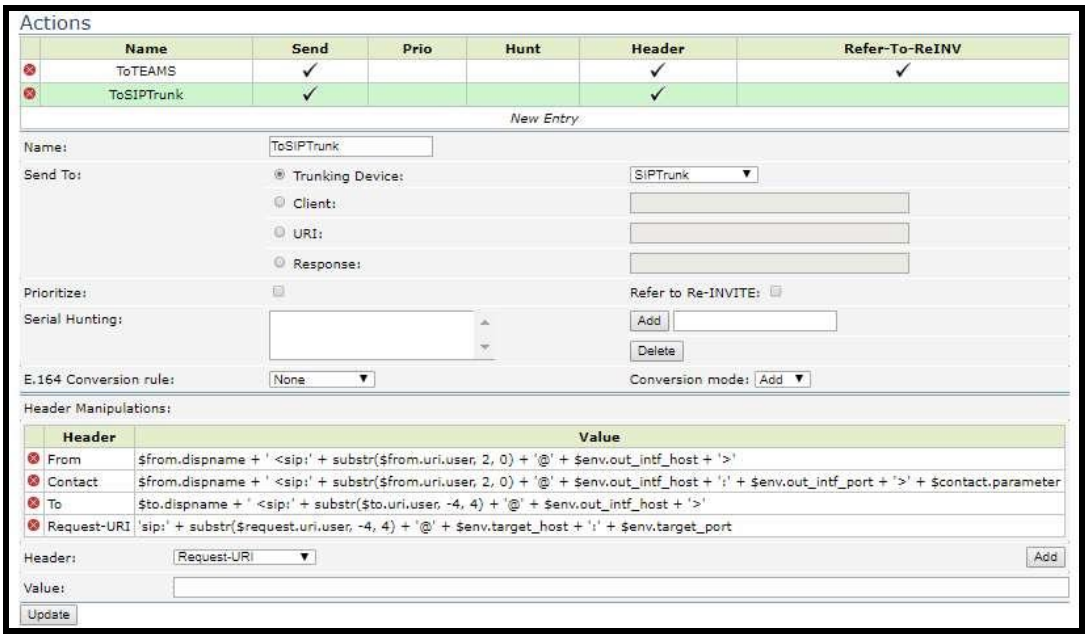
11. First, create a group for ToTeams.

Figure 2-6. ToTeams



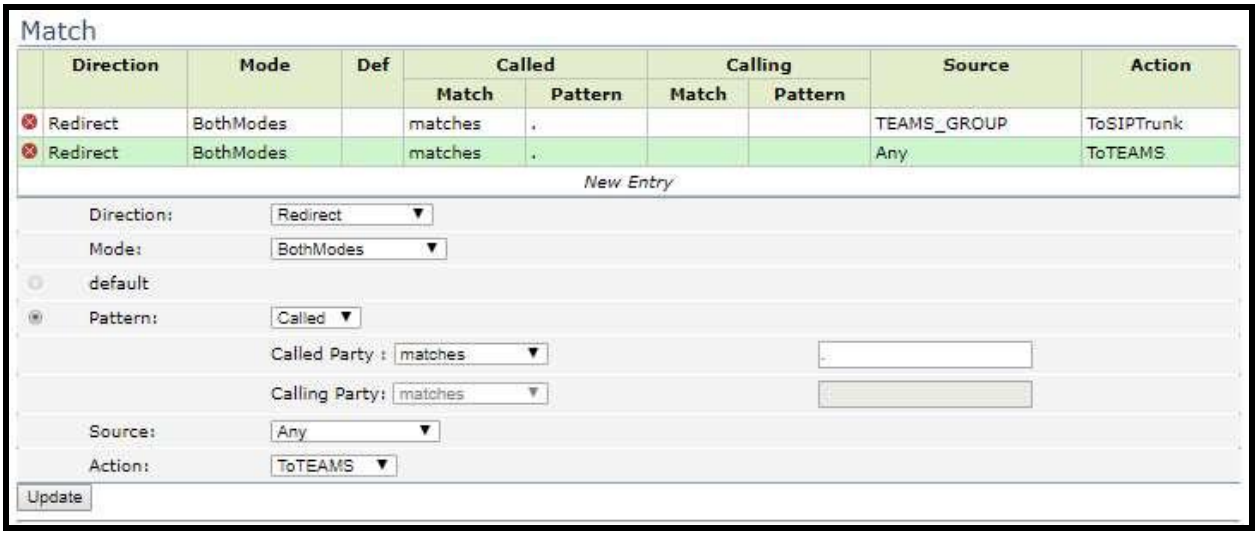
12. Next, create a ToSIPTrunk set of rules.

Figure 2-7. To SIP Server



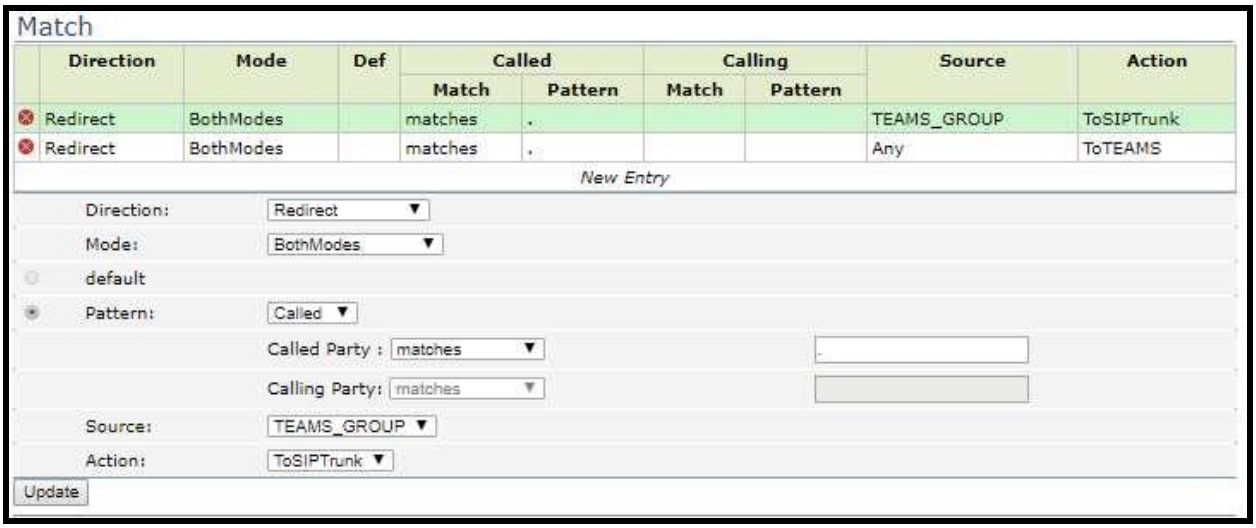
13. Next, Matches need to be created for both Teams and for the local PBX

Figure 2-8. Match to Teams



14. Create a match to the local PBX.

Figure 2-9. Match to Local PBX



At this point, the SBC is set up to work with Microsoft Teams. Take the necessary steps to set up the local IP-PBX to communicate with the Ribbon SBC. The process of setup will vary from manufacturer to manufacturer so that section will not be covered in this document.

3.0 Registering a CyberData Device to the Local IP-PBX

This section will outline how to register a CyberData device with the generic Local IP-PBX. This section will assume that the local IP-PBX is communicating with the Ribbon SBC as well as the SBC communicating with Microsoft Teams.

Note: *Since this section is written to give a general understanding of how to register a CyberData device with a local IP-PBX, please consult specific guides for the phone system being used. The process can vary from company to company, but the general process is the same.*

1. Log into the web interface of the CyberData Device.

Figure 3-1. Home Tab

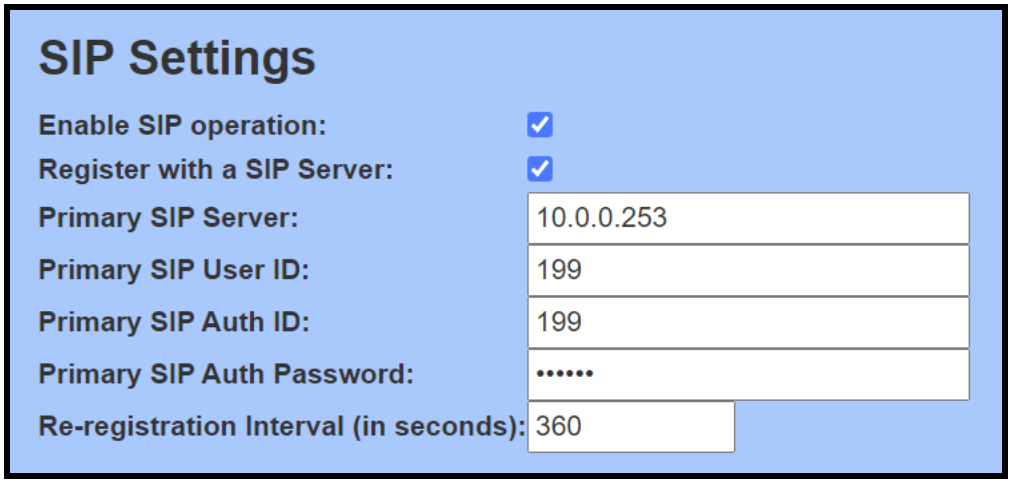
2. Navigate to the SIP Tab.

3. Set the **"Primary SIP Server"** field to the IP Address or FQDN of the local PBX.
4. Set the **"Primary SIP User ID"** to the extension number of the device.
5. Set the **"Primary SIP Auth Id"** to the extension number or Authentication ID.

Note: *The Auth ID will vary from platform to platform, so please consult documentation for the phone system being used.*

6. Set the **"Primary SIP Auth Password"** to the password for the extension.

Figure 3-2. CyberData SIP Tab



4.0 Contact CyberData Corporation

Sales

For sales-related questions, please visit our Contact CyberData Sales web page for more information.

Technical Support

For CyberData Technical Support, please submit a Contact CyberData VoIP Technical Support form on our website.

The CyberData VoIP Technical Support Contact form initiates a troubleshooting ticket which CyberData uses for quality assurance purposes.

Additionally, the Contact VoIP Tech Support form tells us which phone system you are using, the make and model of the network switch, and other essential troubleshooting information we need to efficiently assist with a resolution. Please also include as much detail as possible in the Describe Problem section of the form. Your installation is extremely important to us.

Documentation Feedback

We realize changes to the software or hardware of the solution may render this document obsolete. We welcome and encourage documentation feedback to ensure continued applicability.