

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

COPYRIGHT NOTICE:

© 2020, CyberData Corporation, ALL RIGHTS RESERVED.

This configuration guide and related materials are the copyrighted property of CyberData Corporation. No part of this configuration guide or related materials may be reproduced or transmitted, in any form or by any means (except for internal use by licensed customers), without prior express written permission of CyberData Corporation. This configuration guide, and the products, software, firmware, and/or hardware described in this configuration guide are the property of CyberData Corporation, provided under the terms of an agreement between CyberData Corporation and recipient of this configuration guide, and their use is subject to that agreement and its terms.

DISCLAIMER: Except as expressly and specifically stated in a written agreement executed by CyberData Corporation, CyberData Corporation makes no representation or warranty, express or implied, including any warranty or merchantability or fitness for any purpose, with respect to this configuration guide or the products, software, firmware, and/or hardware described herein, and CyberData Corporation assumes no liability for damages or claims resulting from any use of this configuration guide or such products, software, firmware, and/or hardware. CyberData Corporation reserves the right to make changes, without notice, to this configuration guide and to any such product, software, firmware, and/or hardware.

OPEN SOURCE STATEMENT: Certain software components included in CyberData products are subject to the GNU General Public License (GPL) and Lesser GNU General Public License (LGPL) “open source” or “free software” licenses. Some of this Open Source Software may be owned by third parties. Open Source Software is not subject to the terms and conditions of the CyberData COPYRIGHT NOTICE or software licenses. Your right to copy, modify, and distribute any Open Source Software is determined by the terms of the GPL, LGPL, or third party, according to who licenses that software. Software or firmware developed by CyberData that is unrelated to Open Source Software is copyrighted by CyberData, subject to the terms of CyberData licenses, and may not be copied, modified, reverse-engineered, or otherwise altered without explicit written permission from CyberData Corporation.

TRADEMARK NOTICE: CyberData Corporation and the CyberData Corporation logos are trademarks of CyberData Corporation. Other product names, trademarks, and service marks may be the trademarks or registered trademarks of their respective owners.

Revision Information

12/2/20 – Initial Release

Table of Contents

1.0 Why use Ribbon?	4
1.1 Implementation Diagram	5
1.2 Connecting Ribbon to Microsoft Teams	6
1.3 Pre-Requisites for Integrating Ribbon SBC and Microsoft Teams.....	7
1.3.1 Overview of Steps Required	7
1.4 Picking the right Ribbon SBC.....	8
2.0 Ribbon SBC Setup Steps	9
2.1 Updating Firmware.....	9
2.2 Uploading Certificates	9
2.3 VoIP Settings	9
2.4 TLS Settings.....	11
2.5 B2BUA and Trunk Settings	13
3.0 Registering a CyberData Device to the Local IP-PBX	17
4.0 Contact CyberData Corporation.....	19

1.0 Why use Ribbon?

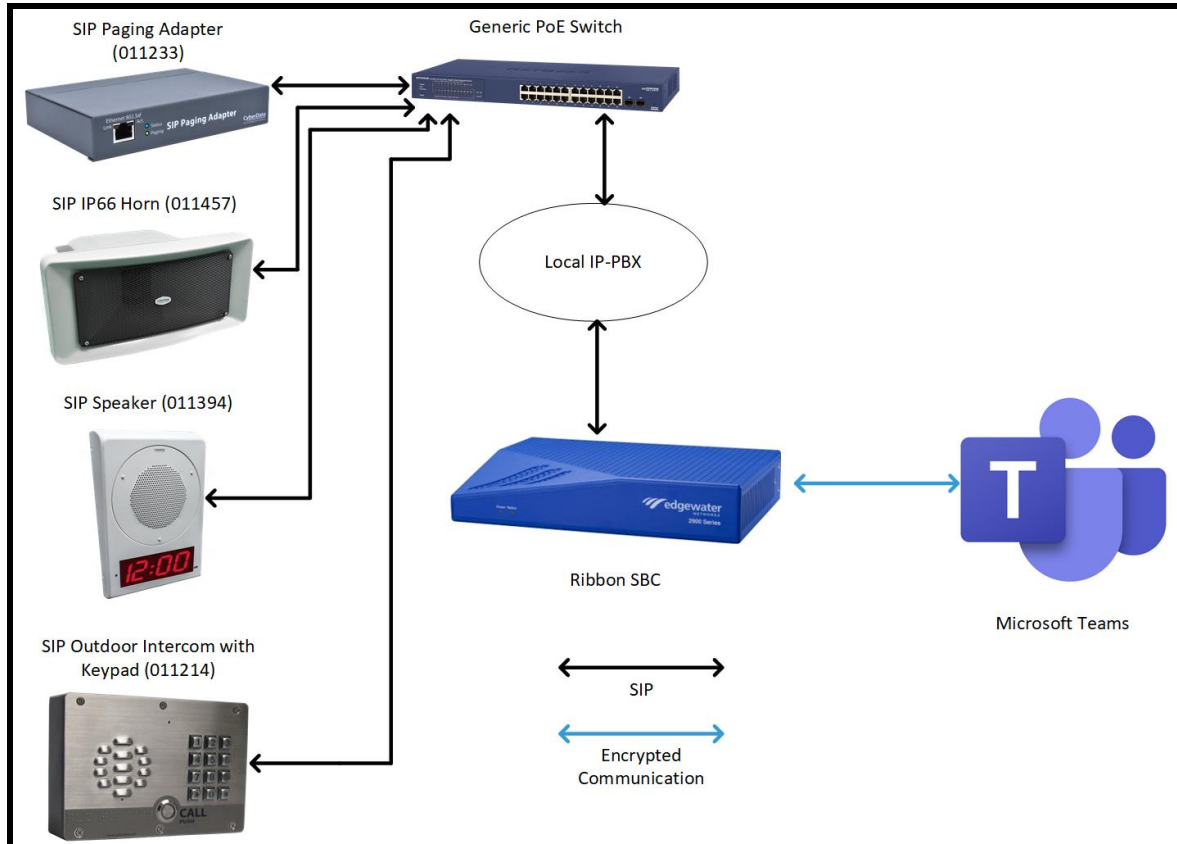
Using CyberData devices on the Microsoft Teams platform requires an intermediary device to communicate between Microsoft Teams and the CyberData hardware. This is due to limitations on what hardware can operate in the Microsoft Teams environment. As such, manufacturers like Ribbon are required to facilitate 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.

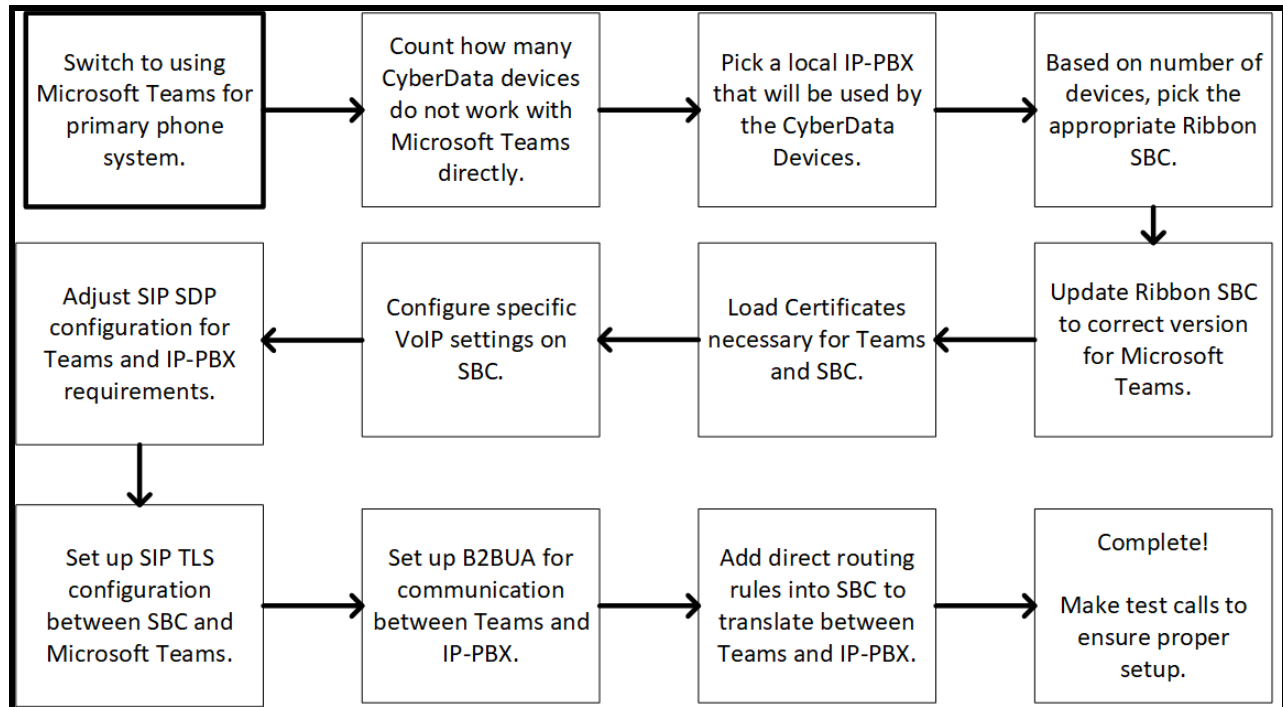
1.1 Implementation Diagram

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.

<u>SBC Product Line</u>	<u>Edgeview Management</u>	<u>Number of Sessions</u>	<u>Hardware or Virtualized</u>	<u>Notes/Connection options</u>
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

ribbon **VoIP** [Help](#)

VoIP ALG allows the system to recognize and register network devices.

Enable LLDP: ☒

LLDP Broadcast Interval (sec):

IPv4 only.

TFTP Server IP address:

In some cases, the ALG addresses will not correspond to the addresses of the LAN or the WAN ports. The addresses will be alias addresses that have been configured on the ports. In general, the user should leave this feature disabled.

Use ALG Alias IP Addresses: ☐

ALG LAN Interface IP Address:

ALG LAN Interface IPv6 Address:

ALG WAN Interface IP Address:

ALG WAN Interface IPv6 Address:

Public NAT WAN IP address:

Private NAT LAN IP address:

Do strict RTP source check: ☐

Enable Client List lockdown: ☐

Allow Shared Usernames: ☐

Strip G.729 from calls: ☒

B2BUA Options:

Route all SIP signalling through B2BUA: ☒

Enable Microsoft Feature: ☒

Enable Comfort Noise Generation (CNG): ☐

Enable User-Agent header pass-through: ☐

Media Security:

Enable SRTP support: ☒

Enable MKI support: ☒

Configure the range of TCP ports to use for handling H.225 and H.245 TCP connections.

H.225/H.245 Port Range: -

Configure the range of UDP ports to use for forwarding RTP streams. Each RTP stream to be forwarded requires two ports (one for RTP and one for RTCP). This means that you will need at least two times as many ports as RTP streams you want to handle.

RTP Port Range: -

RTP Packetization Time (ms):

Prioritize Microsoft Teams: ☐

Calculate Round-Trip-Time:

Calculate RTT: ☒

The ALG feature is registered. View [license key](#).

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

TLS

Port:

TLS Protocol:

TLSv1.2 ▾

Ciphers String:

LAN:

Certificate: Default ▾

Policy: No check ▾

WAN:

Certificate: SBC_Cert ▾

Policy: Verify if provided ▾

Exclude sips headers for TLS Transport ☐

NAT Traversal **Warning: This feature is beta and may not function correctly with certain NAT devices**
Select the NAT Traversal method to use when the system is behind a NAT device:
☒ Disabled
☐ RFC-3581
☐ STUN

SDP Modifications

SDP Codec Operation:

SDP Section that will be modified:

Codecs (comma separated list):

Reject when No Match Codec: ☒

Strip Matched Expressions:

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

SIP Use New Port On Hold Resume: ☒
Priority Numbers

Priority Number 1:

Priority Number 2:

Priority Number 3:

Priority Number 4:

Enable SIP Statistics: ☒

Registration Rate-Pacing parameters are available on the [Survivability page](#).

Submit

Reset

Apply Later

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

Trunking Devices

Name	Address	Port	Group	Username	Registration Status	Transport	SRTP
<input checked="" type="checkbox"/> Local-PBX	192.168.1.200	5060				UDP	Disabled
<input checked="" type="checkbox"/> Teams01	sip.pstnhub.microsoft.com	5061				TLS	Mandatory

New Entry

Name: Model:

☒ Address(IP/FQDN): Use DNS SRV: ☐

Port: Transport:

SRTP:

Source FQDN:

☐ Username: Password:

Authenticate Registration: ☐

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

Create New Routing Group

Name:

Select group members:

	Name	Address
<input checked="" type="checkbox"/>	Teams01	sip.pstnhub.microsoft.com
<input checked="" type="checkbox"/>	Teams02	sip2.pstnhub.microsoft.com
<input type="checkbox"/>	Local-PBX	192.168.1.200

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

Figure 2-5. Routing Group Settings

Existing Routing Groups						
Group Name	State	Keep Alive	Load Balance	Invite Failover	Trust Enabled	Trusted List
TEAMS_GROUP	available	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	sip-all.pstnhub.microsoft.com
Members for Group: TEAMS_GROUP Refresh						
Name	FQDN	Address	Trusted	Last Event	State	
TEAMS01	sip.pstnhub.microsoft.com	52.114.7.24:5061	<input checked="" type="checkbox"/>	OPTIONS	available	
TEAMS02	sip2.pstnhub.microsoft.com	52.114.132.46:5061	<input checked="" type="checkbox"/>	OPTIONS	available	
TEAMS03	sip3.pstnhub.microsoft.com	52.114.76.76:5061	<input checked="" type="checkbox"/>	OPTIONS	available	
Keep Alive Settings						

- Click Submit to confirm all changes.
- Next, rules need to be created to convert calls from local PBX to Teams and from Teams to local PBX
- Navigate to B2BUA and scroll to Actions.
- Create rules for 'To_Teams' to send messages from local PBX to teams.
- 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

- First, create a group for ToTeams.

Figure 2-6. ToTeams

Actions

Name	Send	Prio	Hunt	Header	Refer-To-ReINV
ToTEAMS	✓			✓	✓
TOIPBX	✓			✓	

New Entry

Name:

Send To:

- ☒ Trunking Device:
- ☐ Client:
- ☐ URI:
- ☐ Response:

Prioritize: ☐

Serial Hunting:

E.164 Conversion rule: Conversion mode:

Header Manipulations:

Header	Value
Request-URI	'sip:+91' + \$to.uri.user + '@sip.pstnhub.microsoft.com' + \$env.target_port + ';user=phone'
To	\$to.displayName + ' <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

Header:

Value:

12. Next, create a ToSIPTrunk set of rules.

Figure 2-7. To SIP Server

Actions

Name	Send	Prio	Hunt	Header	Refer-To-ReINV
ToTEAMS	✓			✓	✓
ToSIPTrunk	✓			✓	

New Entry

Name:

Send To:

- ☒ Trunking Device:
- ☐ Client:
- ☐ URI:
- ☐ Response:

Prioritize: ☐

Serial Hunting:

E.164 Conversion rule: Conversion mode:

Header Manipulations:

Header	Value
From	\$from.displayName + ' <sip:' + substr(\$from.uri.user, 2, 0) + '@' + \$env.out_intf_host + '>'
Contact	\$from.displayName + ' <sip:' + substr(\$from.uri.user, 2, 0) + '@' + \$env.out_intf_host + ':' + \$env.out_intf_port + '>' + \$contact.parameter
To	\$to.displayName + ' <sip:' + substr(\$to.uri.user, -4, 4) + '@' + \$env.out_intf_host + '>'
Request-URI	'sip:' + substr(\$request.uri.user, -4, 4) + '@' + \$env.target_host + ':' + \$env.target_port

Header:

Value:

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

Figure 2-8. Match to Teams

Match									
	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
<input checked="" type="checkbox"/>	Redirect	BothModes		matches	.			TEAMS_GROUP	ToSIPTrunk
<input checked="" type="checkbox"/>	Redirect	BothModes		matches	.			Any	ToTEAMS
New Entry									
Direction:		Redirect ▼							
Mode:		BothModes ▼							
<input type="radio"/> default									
<input checked="" type="radio"/> Pattern:		Called ▼							
		Called Party :		matches ▼					
		Calling Party :		matches ▼					
Source:		Any ▼							
Action:		ToTEAMS ▼							
Update									

14. Create a match to the local PBX.

Figure 2-9. Match to Local PBX

Match									
	Direction	Mode	Def	Called		Calling		Source	Action
				Match	Pattern	Match	Pattern		
<input checked="" type="checkbox"/>	Redirect	BothModes		matches	.			TEAMS_GROUP	ToSIPTrunk
<input checked="" type="checkbox"/>	Redirect	BothModes		matches	.			Any	ToTEAMS
New Entry									
Direction:		Redirect ▼							
Mode:		BothModes ▼							
<input type="radio"/> default									
<input checked="" type="radio"/> Pattern:		Called ▼							
		Called Party :		matches ▼					
		Calling Party :		matches ▼					
Source:		TEAMS_GROUP ▼							
Action:		ToSIPTrunk ▼							
Update									

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

The screenshot displays the 'Home' tab of the CyberData Intercom web interface. At the top, there is a navigation bar with tabs: Home, Device, Network, SIP, SSL, Multicast, Sensor, Audiofiles, Events, DSR, Autoprovisioning, and Firmware. The main content area is titled 'CyberData Intercom' and is divided into four primary sections:

- Current Status:** Displays device information such as Serial Number (186201657), Mac Address (00:20:f7:04:41:31), Firmware Version (v20.2.1), and Partition information. It includes a 'Boot From Other Partition' button.
- Admin Settings:** Contains fields for Username (admin), Password (masked with dots), and Confirm Password (masked with dots). It features 'Save', 'Reboot', and 'Toggle Help' buttons.
- Import Settings:** Includes a 'Choose File' button and a status 'No file chosen'. An 'Import Config' button is present.
- Export Settings:** Features an 'Export Config' button.

Below these sections, there are additional configuration options for IP Addressing (DHCP, 192.168.1.8), SIP Volume, Multicast Volume, Ring Volume, Sensor Volume, Push to Talk Volume, Microphone Gain, and various modes (SIP Mode, Multicast Mode, Event Reporting, Nightringer). It also shows server registration status for Primary SIP Server (Registered), Backup Server 1, Backup Server 2, and Nightringer Server.

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

The image shows a screenshot of the 'SIP Settings' tab in a software interface. The background is light blue. The title 'SIP Settings' is in bold black text at the top left. Below the title, there are several configuration options, each with a label and a corresponding input field or checkbox. The options are: 'Enable SIP operation:' with a checked checkbox; 'Register with a SIP Server:' with a checked checkbox; 'Primary SIP Server:' with a text field containing '10.0.0.253'; 'Primary SIP User ID:' with a text field containing '199'; 'Primary SIP Auth ID:' with a text field containing '199'; 'Primary SIP Auth Password:' with a text field containing six dots; and 'Re-registration Interval (in seconds):' with a text field containing '360'.

Setting	Value
Enable SIP operation:	<input checked="" type="checkbox"/>
Register with a SIP Server:	<input checked="" type="checkbox"/>
Primary SIP Server:	10.0.0.253
Primary SIP User ID:	199
Primary SIP Auth ID:	199
Primary SIP Auth Password:
Re-registration Interval (in seconds):	360

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.