

Using CyberData Devices on Microsoft Teams with Vodia



Document Part #931805A
Relevant for all CyberData products.

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

Using CyberData Devices on Microsoft Teams with Vodia Document #931805A

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

9/10/2020 – Initial Release

Table of Contents

1.0 Why use Vodia?	4
1.1 Implementation Diagram	5
2.0 Connecting Vodia to Microsoft Teams	6
2.1 Pre-Requisites for Integrating Vodia and Microsoft Teams	7
2.1.1 Overview of steps required	7
2.2 Vodia Setup Steps	8
2.2.1 Create Fully Qualified Domain	8
2.2.2 Create Extensions	8
2.2.3 Create a Trunk on Vodia PBX	12
2.3 Microsoft Teams Office 365 Setup	13
2.3.1 Create a domain in Office 365	13
2.3.2 Create users in the domain	13
2.3.2 Use PowerShell to connect to Office 365	14
2.3.3 Create a PSTN Gateway to connect to the Vodia PBX	14
2.3.4 Enabling Direct Routing	15
2.3.5 Configure Voice Routing for Outgoing calls to the Vodia System	16
3.0 Registering a CyberData Device to the Vodia PBX.....	18
4.0 Contact CyberData Corporation.....	20

1.0 Why use Vodia?

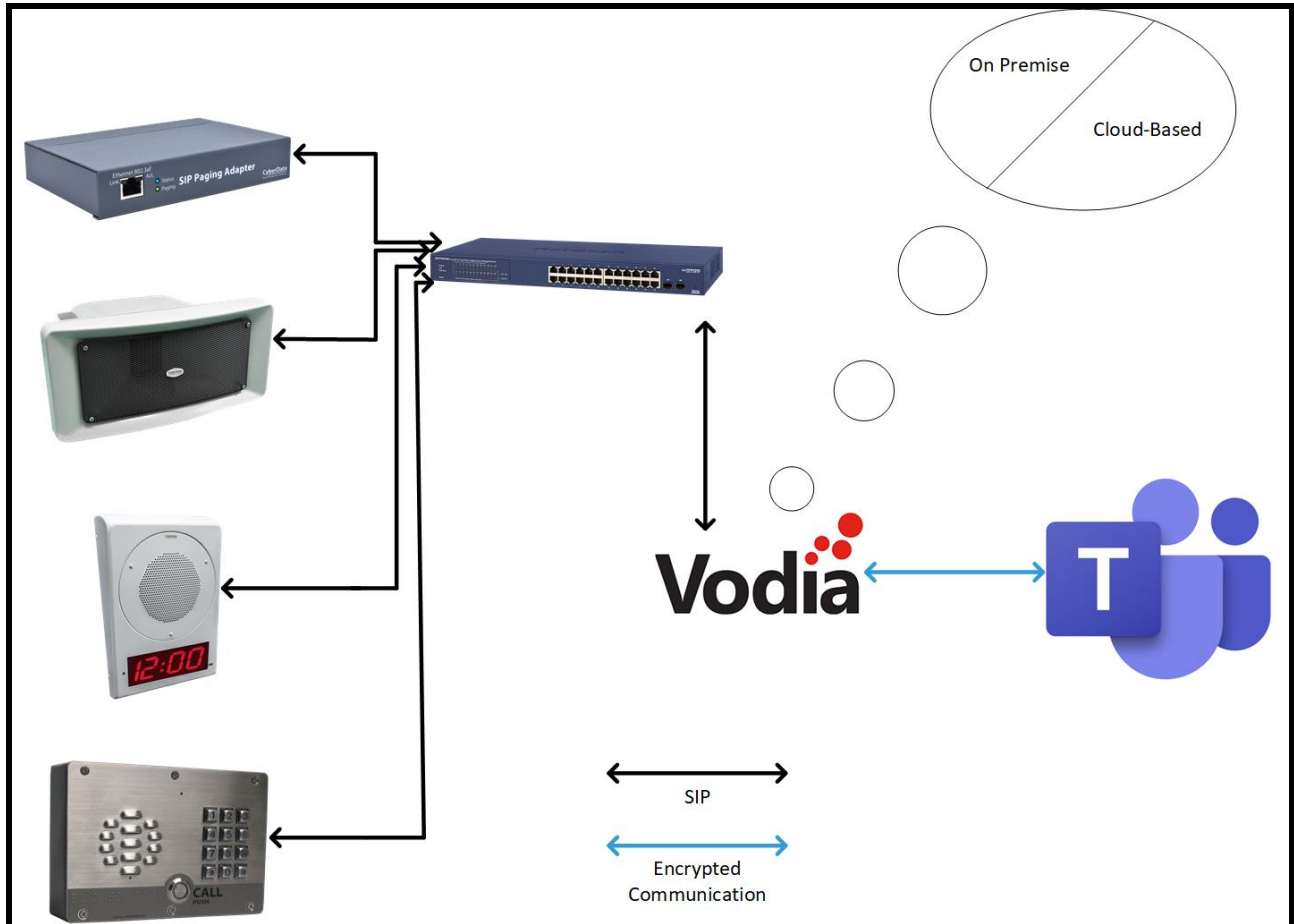
Using CyberData devices on the Microsoft Teams platform requires an intermediary device to communicate between Microsoft Teams and the CyberData hardware. This is due to limitations on what hardware can operate in the Microsoft Teams environment. As such, services like Vodia are required to facilitate that operation. There are a variety of options to connect endpoints to Microsoft Teams, however they can be costly. Vodia is a great economical choice for using any CyberData equipment with Microsoft Teams.

Vodia is a cloud hosted or on-premise VoIP service 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 simple integration of any CyberData product into a Microsoft Teams environment.

With a low monthly fee, Vodia is the ideal choice for integrating any hardware with Microsoft Teams. Vodia has a scaling price model based on the number of extensions used that allows larger users to get a more economical price. However, Vodia starts as low as \$6.30 a month for five lines which makes it the best choice as compared to other hardware-based SBC options.

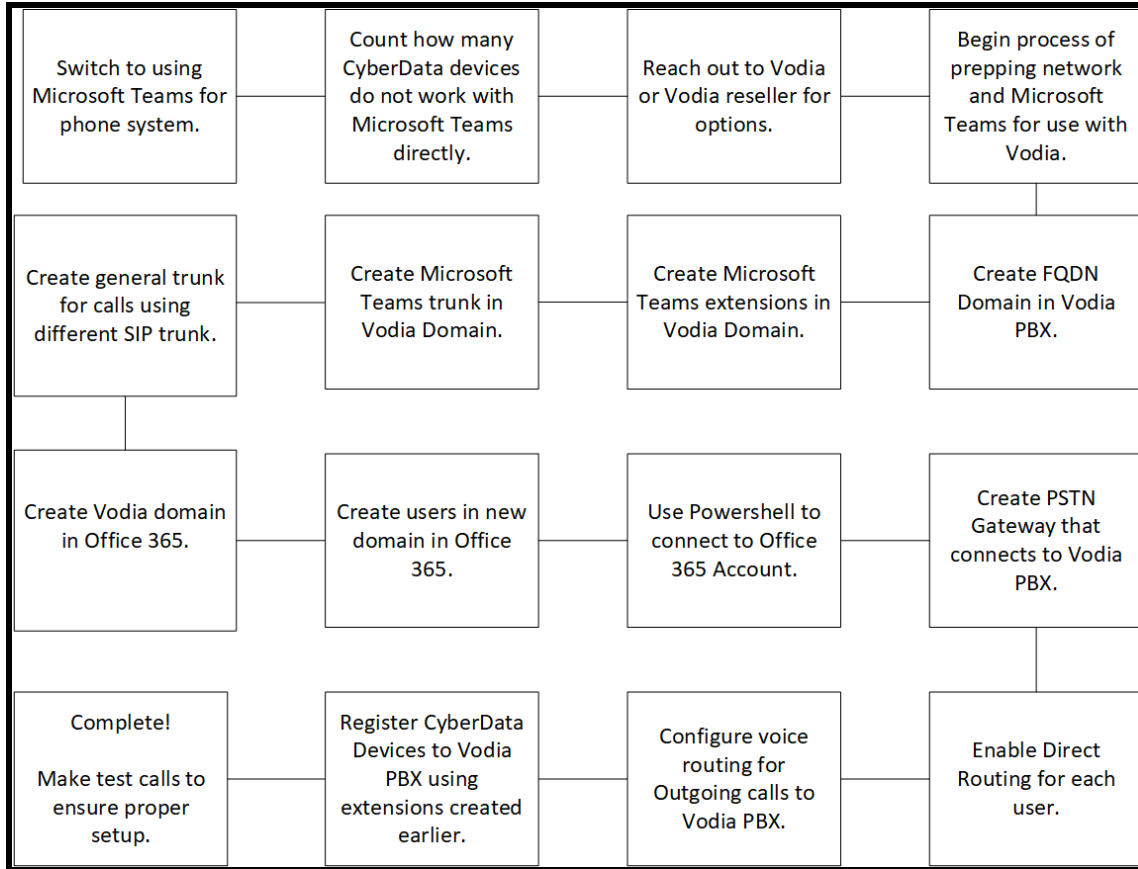
1.1 Implementation Diagram

Figure 1-1. Implementation Example



2.0 Connecting Vodia to Microsoft Teams

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



2.1 Pre-Requisites for Integrating Vodia and Microsoft Teams

There are several pre-requisites that are required to integrate Vodia 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.
- Vodia PBX on premise or hosted with Microsoft Teams integration.
- A domain (which is FQDN) in Vodia PBX with a valid certificate.
- Capability to create a SIP Trunk.

Assuming all the pre-requisites are met, please follow these steps to setup the connection between Vodia and Microsoft Teams. This information is taken from the [Vodia and Microsoft Teams Integration Manual](#). Vodia also has a YouTube video that walks through this whole process [here](#).

2.1.1 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.

Vodia Setup steps

1. Create a domain in the Vodia PBX with an FQDN.
2. Create the Microsoft Teams extensions in the domain created in the prior step.
3. Make a Microsoft Teams trunk in the domain.
4. Create a general use trunk in the domain.

Microsoft Teams Setup Steps

1. Create a domain in the Office 365 account that is linked to Microsoft Teams.

Note: This domain would be the same domain from the Vodia portion of steps.

2. Create users in the domain and assign these users E3, E5 or other licenses that support “Direct Routing”.
3. Use PowerShell to connect the trunks to the Microsoft Teams Office 365 Account.

2.2 Vodia Setup Steps

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

2.2.1 Create Fully Qualified Domain

1. Log into the Vodia system. This system can be cloud hosted OR can be on-premise using the Vodia IOP.
2. Navigate to the Domain List.
3. Press Create to make a new domain.
4. Create a new FQDN that meets the following requirements.
 - a. Resolves to the Vodia PBX.
 - b. Is part of the domain created on the Office 365 account.
 - c. Has a valid certificate.

Example: “pbx.company.com” where the Office 365 domain is “company.com”

Note: The Vodia system supports Let’s Encrypt that can create a certificate for free automatically.

2.2.2 Create Extensions

5. Navigate to the domain created in the prior steps by clicking the domain.

Figure 2-1. Current Domains

Current Domains ?

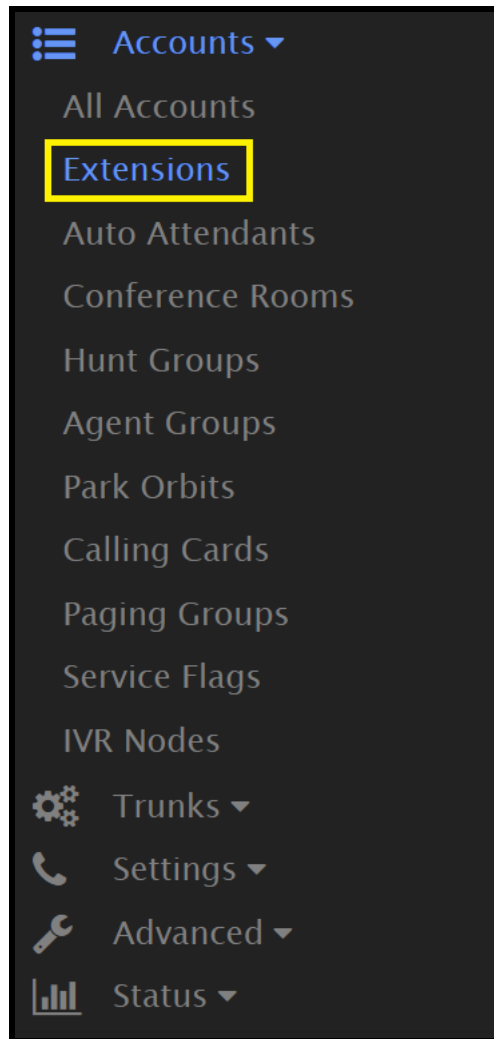
This list shows the domains that are currently available on this system. To visit the domain, click on the domain link. You can edit the domain parameters that are only available to the system administrator by clicking on the edit button. To download a backup of the domain, click on the download button. You can use that backup when you create a new domain. The name "localhost" has a special meaning: it matches all names that are not assigned to other domains. In order to make a domain available in the network, you will have to set up DNS records for this domain unless you are just using IP addresses as the domain name.

Domain	Users	Extensions	Registrations	Country Code
<input type="checkbox"/> pbx.company.com	1	1	0 (0%)	49

[+ | Create](#) [Delete](#)

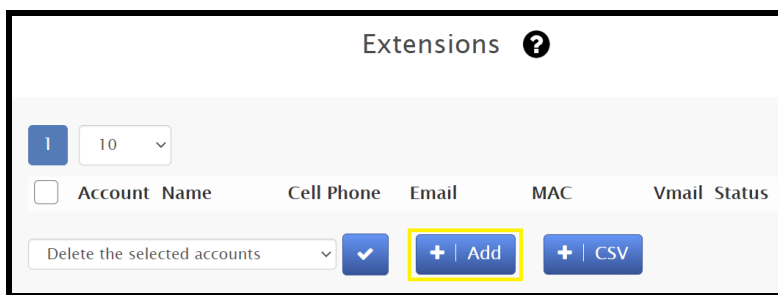
6. Go to the **Extensions** section under Accounts.

Figure 2-2. Extensions



7. Press Add.

Figure 2-3. Add Extension



8. Enter the extension number.

Figure 2-4. Extension Creation

Create Extension	
Account Names	123 ✓
First name	Outdoor ✓
Last name	Intercom ✓
Email addresses for extension	Example.Email@Fake.com ✓
PIN	●●●●
PIN (repeat)	●●●●
Cell phone number	617-446-1399
Automatically generate web password	Yes <input type="checkbox"/>
Automatically generate SIP password	Yes <input type="checkbox"/>
Upload picture	Choose File No...n
○ Cancel + Create	

Note: This number must be the same number used later in the Microsoft Teams Office 365 section.


9. Press create to finish the extension.
10. Click on the extension to adjust its settings.
11. Under the General tab change the Administrative Usage Restriction to **Teams**.

Figure 2-5. Usage Restriction

Extension

General Redirection Mailbox Email Registration Permission
Buttons Provisioning Action URL Customize Graphs

[Click here](#) to switch into user-mode.

Administrator only 

Account number(s):

Extension feature set:

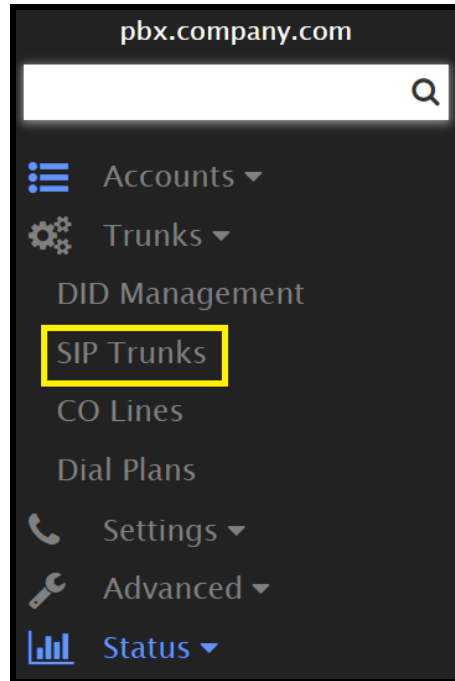
12. Save.

13. Repeat these steps as necessary for all extensions.

2.2.3 Create a Trunk on Vodia PBX

- 14. Navigate to the domain “pbx.company.com” that was created earlier.
- 15. Go to Trunks and then SIP Trunks.

Figure 2-6. SIP Trunks



- 16. Press **Add**.
- 17. Set the provider to “Teams”.

Figure 2-7. Microsoft Teams SIP Trunk

A screenshot of a web form titled 'Create service provider trunk (SIP trunks)'. The form has a blue header with a close button. It contains five input fields: 'Provider' (a dropdown menu with 'Teams' selected), 'Name' (text input with 'Teams'), 'User name (for registration)' (text input with 'Teams Trunk'), 'Password' (password input with dots and a visibility toggle), and 'DID' (text input with '123456789'). At the bottom, there are two buttons: 'Cancel' and 'Create'.

18. Set a name for the trunk, for example “Teams Trunk”.
19. Press Create.
20. Press Add again to make another trunk. This trunk will use a Trunk any other trunk provider.

Note: This will require a Trunk from a trunk provider of the reader’s choice.

21. Configure the second trunk as recommended by the Trunk provider. This trunk is used for incoming and outgoing calls.

2.3 Microsoft Teams Office 365 Setup

These steps will walk through the setup process required on Office 365 and Microsoft Teams.

2.3.1 Create a domain in Office 365

1. Open a browser and log into the Office 365 Admin account.
2. From the Microsoft 365 Admin Center press **Setup** then **View**.
3. Click “**Get your custom domain set up**” and then **Manage**.
4. Choose the company domain name. Example “company.com”

Note: This domain must be owned by the site.

5. Use one of the steps to verify that the domain is owned by the site.

2.3.2 Create users in the domain

6. From the Microsoft 365 Admin Center go to Users and then Active Users.
7. Click Add a User.
8. Set the names of the users and give a unique username that is used for the email.

Note: Make sure to sure the domain created in section 3.3.1.

2.3.2 Use PowerShell to connect to Office 365

This section outlines how to connect to Office 365 using PowerShell which is essential for the final steps of the process. These steps are taken from the [“Manage Skype for Business Online with PowerShell”](#) knowledgebase article.

9. Open Windows PowerShell.
10. Run the following commands

```
Import-Module SkypeOnlineConnector
$userCredential = Get-Credential
$fbSession = New-CsOnlineSession -Credential $userCredential
Import-PSSession $fbSession
```

11. In the Windows PowerShell Credential Request box type the Skype for Business Online administrator account name and password.
12. Click OK.

2.3.3 Create a PSTN Gateway to connect to the Vodia PBX

Using the PowerShell connection to Skype for Business a gateway will need to be created. To confirm the right account is being used run the following command in PowerShell.

*Get-Command *onlinePSTNGateway**

The command will return four functions that allow management of the SBC.

Command Type	Name	Version	Source
Function	Get-CsOnlinePSTNGateway	1.0	tmp_v5fiu1no.wxt
Function	New-CsOnlinePSTNGateway	1.0	tmp_v5fiu1no.wxt
Function	Remove-CsOnlinePSTNGateway	1.0	tmp_v5fiu1no.wxt
Function	Set-CsOnlinePSTNGateway	1.0	tmp_v5fiu1no.wxt

After confirming the correct account is selected, the gateway will need to be created. To create the gateway run the following command replacing “pbx.company.com” with the FQDN created on the Vodia PBX with a valid certificate.

New-CsOnlinePSTNGateway -Identity pbx.company.com -Enabled \$true -SipSignallingPort 5061 -MaxConcurrentSessions 100

The command once entered will return this information.

Identity	pbx.company.com
FQDN	pbx.company.com
SipSignallingPort	5061
FailoverTimeSeconds	10
ForwardCallHistory	False
ForwardPai	False
SendSipOptions	True
MaxConcurrentSessions	100
Enabled	True

The parameters of the gateway can be verified with the command:

Get-CsOnlinePSTNGateway -Identity pbx.company.com

Which provides the following information:

Identity	pbx.company.com
FQDN	pbx.company.com
SipSignallingPort	5061
CodecPriority	SILKWB,SILKNB,PCMU,PCMA
ExcludedCodecs	
FailoverTimeSeconds	10
ForwardCallHistory	False
ForwardPai	False

2.3.4 Enabling Direct Routing

The next step after creating the PSTN Gateway is to enable direct routing. Direct Routing is required on Microsoft Teams to allow calls from teams to the Vodia system and vice versa.

Use this command to enable direct routing on the individual user.

Note: This must be done on ALL users that require direct routing.

Set-CsUser -Identity "John Smith" -OnPremLineURI tel:4002 -EnterpriseVoiceEnabled \$true -HostedVoiceMail \$true

In this example command "John Smith" is the name of the targeted user. "-OnPremLine URI tel:4002 is an example of an extension number that will be used. This number should match the one used on the Vodia system. For this example, a four-digit number was used but it can be less digits or even a full E.164 number if necessary.

At this point it should be possible to call from Vodia to Microsoft Teams but not Teams to Vodia.

2.3.5 Configure Voice Routing for Outgoing calls to the Vodia System

These next steps will create rules for when calls should use the PSTN Gateway used before to send calls to the Vodia PBX. The rules can be either a called number pattern or a called number pattern and a specific user that makes the call.

Call Routing involves four factors:

- Online PSTN Gateway: Microsoft Teams and the SBC/PBX are connected via the gateway.
- Voice Route: Utilizes Online PSTN Gateways where the calling number matches a pattern
- PSTN Usage: Combines Voice route and other PSTN usages. Allows for different voice routing policies.
- Voice Routing Policies: Uses PSTN Usages. Can be assigned to multiple users.

To summarize the flow:

User → Voice Routing Policy → PSTN Usage → Voice Route → PSTN Gateway

For this example, the user is a PBX extension of Vodia, so the calls should first go there and Vodia can route the calls accordingly. There are other ways to handle this flow, but for this guide everything will be routed through Vodia.

Example Flow:

User: John Smith → Policy1 (Voice Policy) → Usage1 (PSTN Usage) → pbx.company.com (PSTN Gateway)

1. Create the usage with the following PowerShell Command

```
Set-CsOnlinePstnUsage -Identity Global -Usage @{Add="Usage1"}
```

2. Check for available usages with this command.

```
Get-CsOnlinePSTNUsage
```

3. Create the route with the Vodia PSTN Gateway and the usage created in step 1 of this section.

```
New-CsOnlineVoiceRoute -Identity "Route1" -NumberPattern "\+(\d{4})|^\d{4}" -  
OnlinePstnGatewayList pbx.company.com -Priority
```

4. Create the voice policy with the usage from step 1.

```
New-CsOnlineVoiceRoutingPolicy "Policy1" -OnlinePstnUsages "Usage1"
```

5. Allow usage of the Policies to all necessary users with the following command.

Grant-CsOnlineVoiceRoutingPolicy -Identity "John Smith" -PolicyName "Policy1"

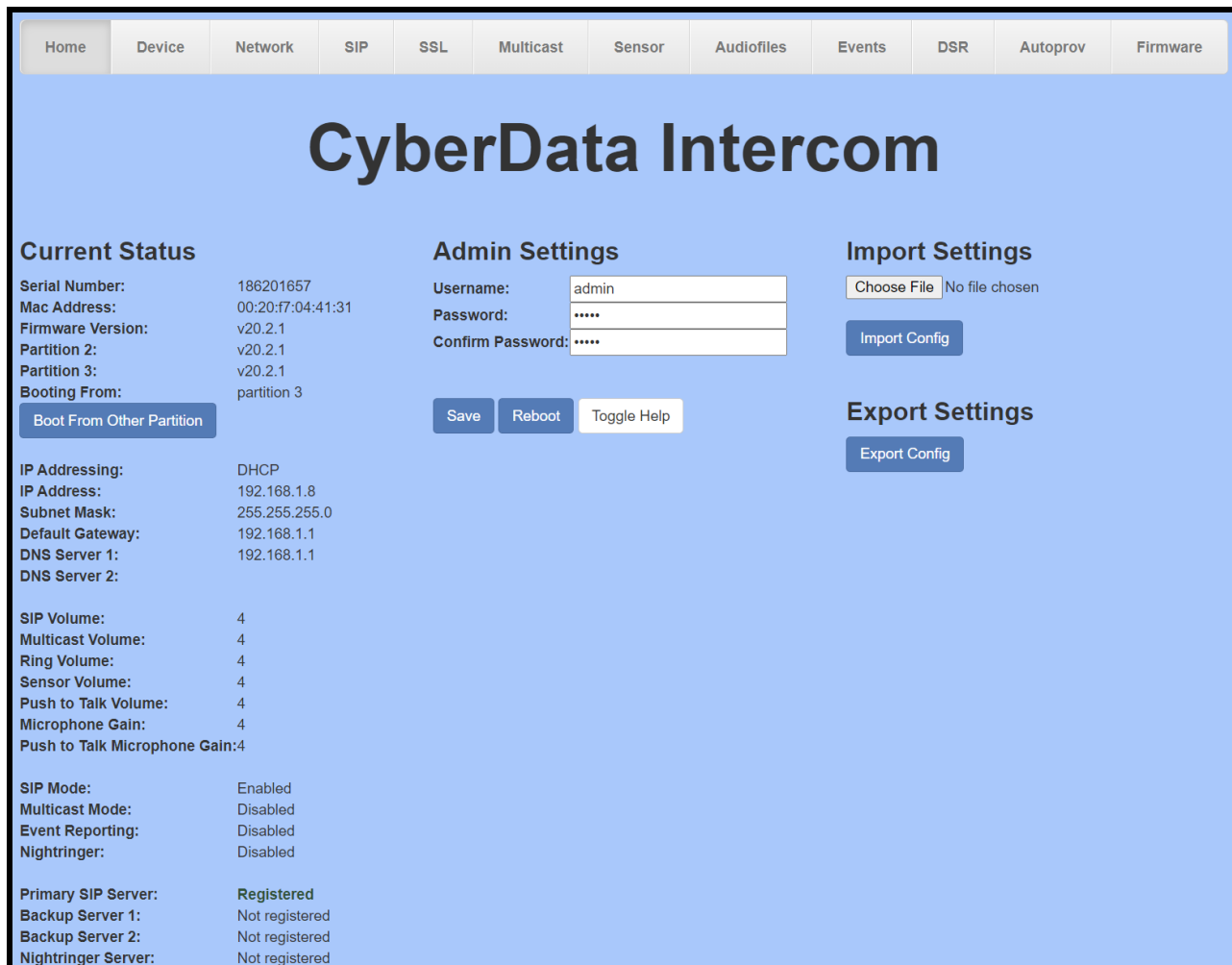
The Microsoft Teams and Vodia integration should now be complete. Our example John Smith can send and receive calls made using the Vodia PBX.

3.0 Registering a CyberData Device to the Vodia PBX

This section will outline how to register a CyberData device with the Vodia system. This section will assume that Vodia and Microsoft Teams integration is complete.

1. Log into the web interface of the CyberData Device.
2. Navigate to the SIP Tab.

Figure 3-1. Home Tab



3. Set the Primary SIP Server field to the FQDN of the domain configured on the Vodia PBX.
4. Set the Primary SIP User ID to the account number of the user.
5. Set the Primary SIP Auth Id to the account number of the user.
6. Set the Primary SIP Auth Password to the value listed in the extension profile on Vodia.
7. Set the RTP port to 49152.

Figure 3-2. CyberData SIP Tab

The screenshot shows the 'SIP' configuration tab in the CyberData Intercom web interface. The page is titled 'CyberData Intercom' and features a navigation menu at the top with tabs for Home, Device, Network, SIP (active), SSL, Multicast, Sensor, Audiofiles, Events, DSR, Autoprovisioning, and Firmware. The main content area is divided into several sections:

- SIP Settings:** Includes checkboxes for 'Enable SIP operation' and 'Register with a SIP Server', both checked. Fields for 'Primary SIP Server' (pbx.company.com), 'Primary SIP User ID' (123), 'Primary SIP Auth ID' (123), 'Primary SIP Auth Password' (masked), and 'Re-registration Interval (in seconds)' (360). It also includes sections for Backup SIP Server 1 and 2, Remote SIP Port (5060), Local SIP Port (5060), SIP Transport Protocol (UDP), TLS Version (1.2 only), and Outbound Proxy settings.
- Nighthringer Settings:** Fields for 'SIP Server', 'SIP User ID', 'SIP Auth ID', 'SIP Auth Password', and 'Re-registration Interval (in seconds)' (360).
- Dial Out Settings:** Fields for 'Dial out Extension' (204), 'Extension ID' (id204), 'Send Multicast Audio' (checkbox), 'Multicast Address' (224.5.5.5), 'Multicast Port' (5050), and 'Repeat Message' (1).
- Call Disconnection:** Field for 'Terminate Call after delay' (0).
- Audio Codec Selection:** Dropdown menu for 'Codec' set to 'Auto Select'.
- RTP Settings:** Fields for 'RTP Port (even)' (49152), 'Jitter Buffer' (50), and 'RTP Encryption (sRTP)' (Disabled).

At the bottom of the configuration area, there are three buttons: 'Save', 'Reboot', and 'Toggle Help'.

Note: The Vodia system supports all SIP Transport protocols so choose a protocol based on the requirements of your network. Any transport will work.

When using UDP or TCP keep the remote SIP port set to 5060.

If using TLS set the Remote SIP Port to 5061.

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.