



MS Teams Cloud Collector Build

Jul 01, 2021

Legal Information

Please take careful note of the following legal notices:

- Copyright © 2021 VisionOSS Limited.
All rights reserved.
- VOSS, VisionOSS and VOSS-4-UC are trademarks of VisionOSS Limited.
- No part of this document may be reproduced or transmitted in any form without the prior written permission of VOSS.
- VOSS does not guarantee that this document is technically correct, complete, or that the product is free from minor flaws. VOSS endeavors to ensure that the information contained in this document is correct, whilst every effort is made to ensure the accuracy of such information, VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.
- This document is used entirely at the users own risk. VOSS cannot be held responsible or liable for any damage to property, loss of income, and or business disruption arising from the use of this document.
- The product capabilities described in this document and the actual capabilities of the product provided by VOSS are subject to change without notice.
- VOSS reserves the right to publish corrections to this document whenever VOSS deems it necessary.
- All vendor/product names mentioned in this document are registered trademarks and belong to their respective owners. VOSS does not own, nor is related to, these products and vendors. These terms have been included to showcase the potential of the VOSS solution and to simplify the deployment of these products with VOSS should you select to utilize them.

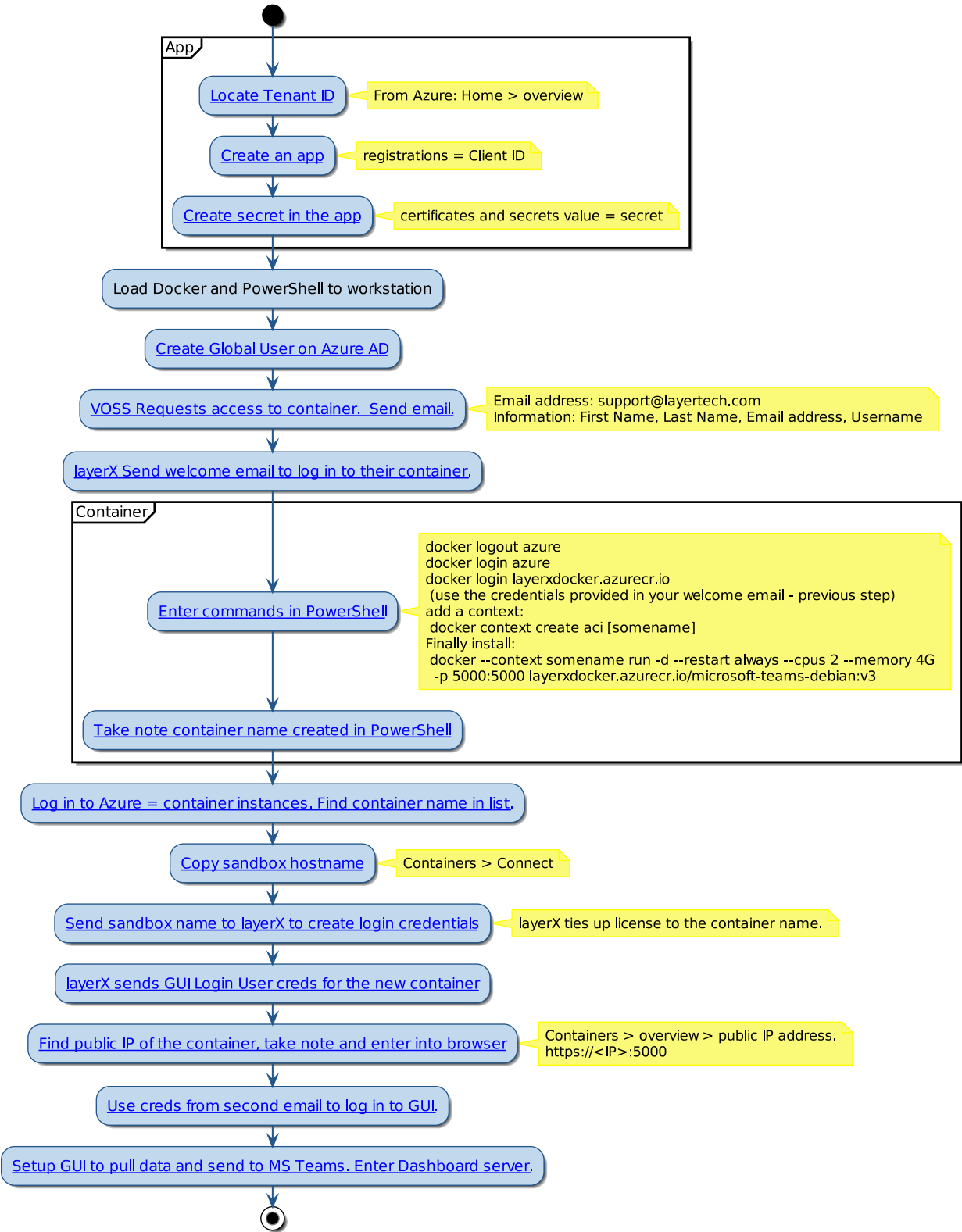
Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

Contents

- 1 High Level Build process** **1**
- 2 Port Information** **3**
- 3 Send email to get Lx Container log in details** **5**
- 4 Create an app in Azure** **6**
- 5 Create a User** **9**
 - 5.1 General steps 15
 - 5.2 Build Container 15
- 6 GUI login user email request** **18**
- 7 Azure Container Instance Specification** **19**
- 8 Configuration Steps** **20**
 - 8.1 Import the module file 24
- 9 Solutions to Basic Installation Challenges** **26**
 - 9.1 Issue #1: You cannot log in to your cloud collector’s WEB GUI with your credentials. 26
 - 9.2 Issue #2: You cannot connect a data source profile to the Dashboard Server. 26
 - 9.3 Issue #3: You cannot connect to your cloud collector’s login page at all. 26
 - 9.4 Issue #4: You created your “Microsoft Health” successfully but you are not able to see any data on your “Service Health Status” dashboards. 27

1. High Level Build process



2. Port Information

Please make sure that the following ports are open on the corresponding firewalls:

Rule	From Device	To Device	Direction	Protocol	Port Number
1	Cloud collector agent (IP: Any) *	Cloud Microsoft APIs (IP: Any)	Uni-directional	TCP	443 (Encrypted)
2	Cloud collector agent (IP: Any) *	VOSS Dashboard Server (IP: Defined by the client)	Uni-directional	TCP	5432 (Encrypted)
3	Cloud collector agent (IP: Any) * / **	VOSS License Server (IP: 13.86.4.217)	Uni-directional	TCP	443 (Encrypted)
4	Cloud collector agent (IP: Any) * / **	VOSS Cloud Backup Server (IP: 40.86.94.9)	Uni-directional	TCP	22 (Encrypted)
5	Administrative portal users of the cloud collector (IP: Any)	Cloud collector agent (IP: Defined by the client) *	Uni-directional	TCP	443 (Encrypted)

Prerequisites:

- Build dashboard server and have the IP address to hand
- Open up ports between the dashboard server and the Azure cloud collector
- Build Azure AD global reader account
- Build App

Please create a dedicated user account on your Microsoft Admin Portal with “Global Reader” privileges.

[See details in the Microsoft 365 documentation](#)

VOSS agent will be using this account to collect the information it needs to display the historical Microsoft Teams call details. For further support, please contact the VOSS Team.

- Please register your VOSS agent as an app on your Azure portal using details provided by Microsoft.

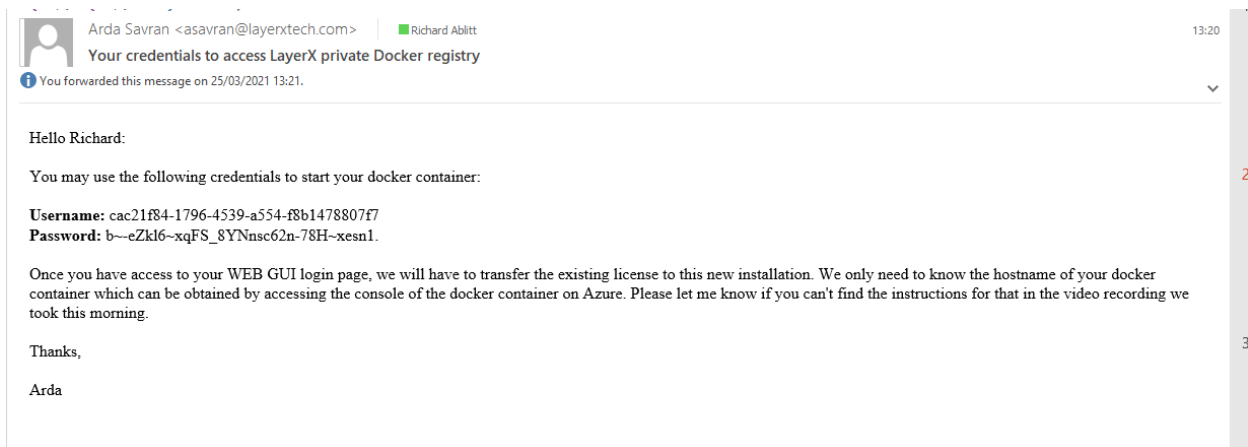
[See details in the Microsoft Quickstart](#)

VOSS agent will be using this account to collect the information it needs to display Microsoft 365 service health status and incidents. For further support, please contact the VOSS Team.

-
- You will need your Azure admin portal login details and VOSS provided credentials to install the Azure Container Instance in the relevant ACI context.
 - Please contact VOSS support to get your cloud agent access package before any configuration. This package should include:
 - * Access link to your VOSS Cloud Agent Webapp via a WEB portal.
 - * A set of credentials to access your VOSS Cloud Agent Webapp via a WEB portal.
 - An encrypted import module file to enable some of the internal features of the agent.

3. Send email to get Lx Container log in details

Send an email to LX to get the Username and password to be able to log in to get the docker container image.



4. Create an app in Azure

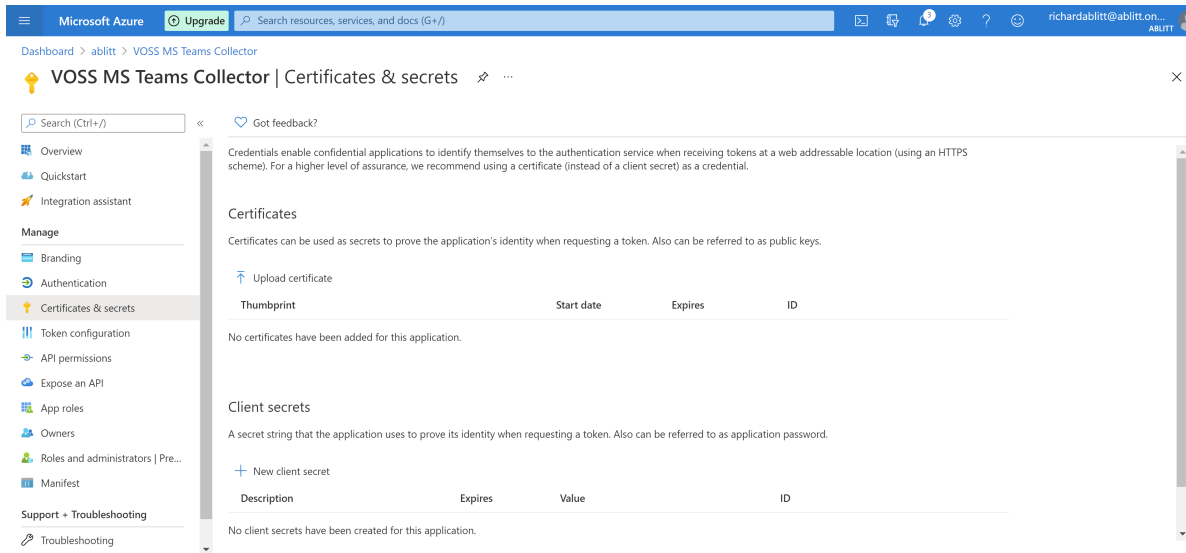
1. **Microsoft Azure > App registrations**
2. +New Registration
3. Give it a name
4. Select the access type (Used Single Tenant)
5. Click register

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page title is 'Register an application'. The 'Name' field is set to 'VOSS MS Teams Collector'. The 'Supported account types' section is expanded, showing four radio button options: 'Accounts in this organizational directory only (ablit only - Single tenant)' (selected), 'Accounts in any organizational directory (Any Azure AD directory - Multitenant)', 'Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)', and 'Personal Microsoft accounts only'. There is a 'Help me choose...' link below the radio buttons. The 'Redirect URI (optional)' section is also visible, with a note that it's optional but required for most authentication scenarios. At the bottom, there is a 'Register' button and a link to 'Microsoft Platform Policies'.

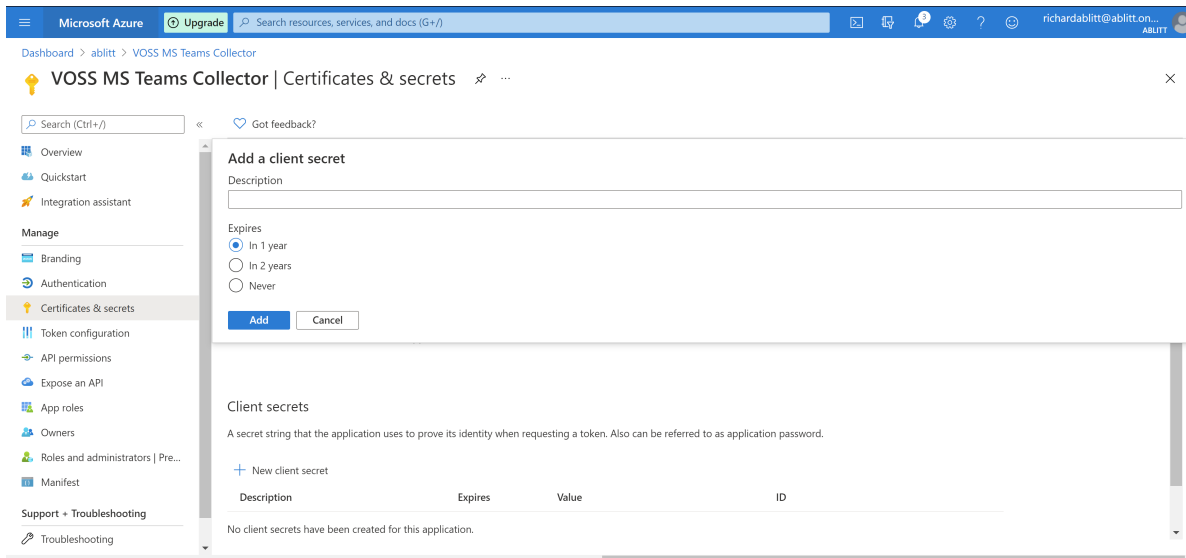
Take note of the following details

Application (client) ID	46828bda-ca72-4dbf-b20e-f0ba72bdfef7f
Directory (tenant) ID	c85200ba-cf50-48e8-91f1-0c0805f1c9dc

6. In the app just created Go to **Navigate > Certificates and Secrets**

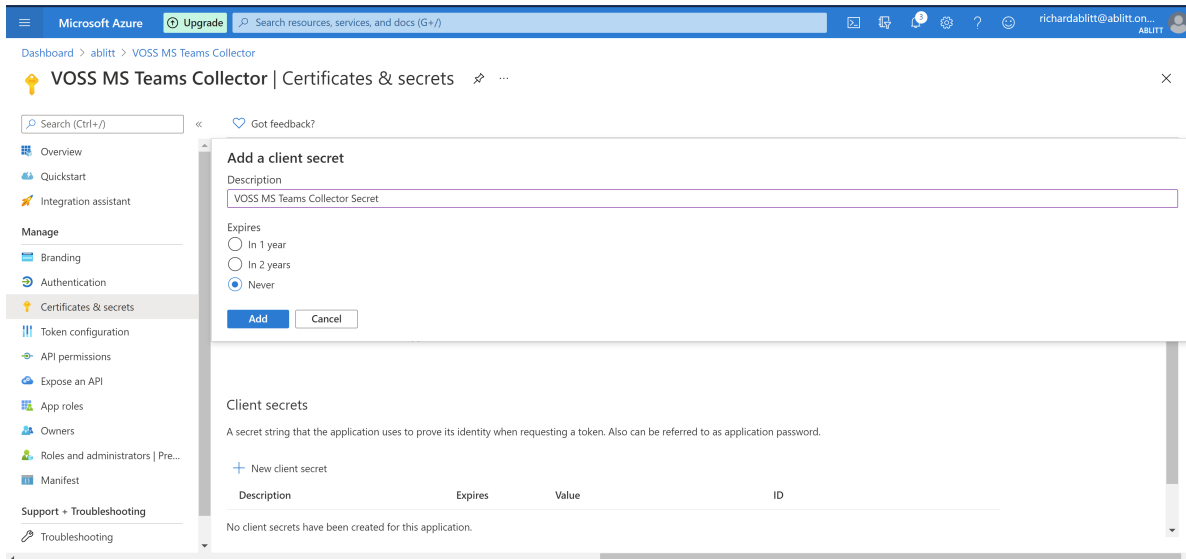


7. In the **Clients Secrets** section **+New Client Secrets**

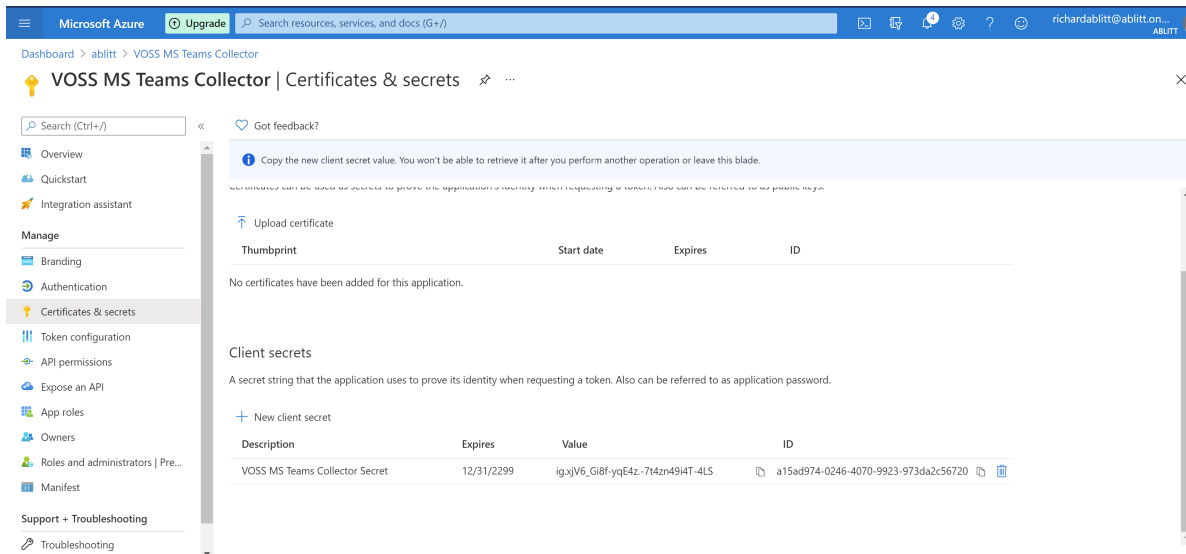


Give the secret a description

8. Choose expire (if 1 or 2 years this will need to be added and renewed)



9. Copy the value against the new secret created

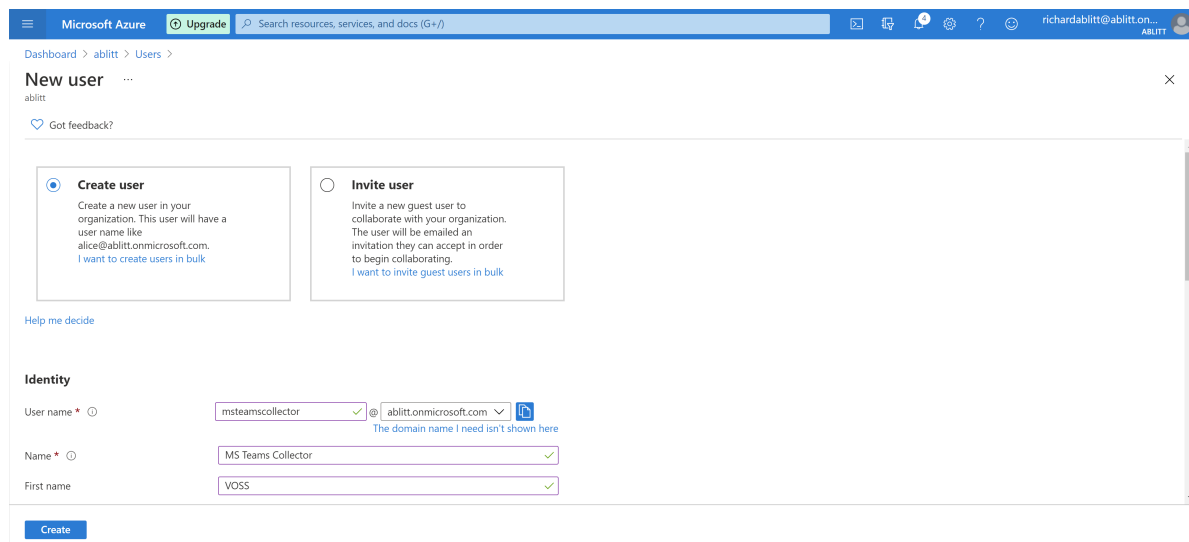


5. Create a User

1. Azure Active directory > Users

2. + New user

Fill out the following:



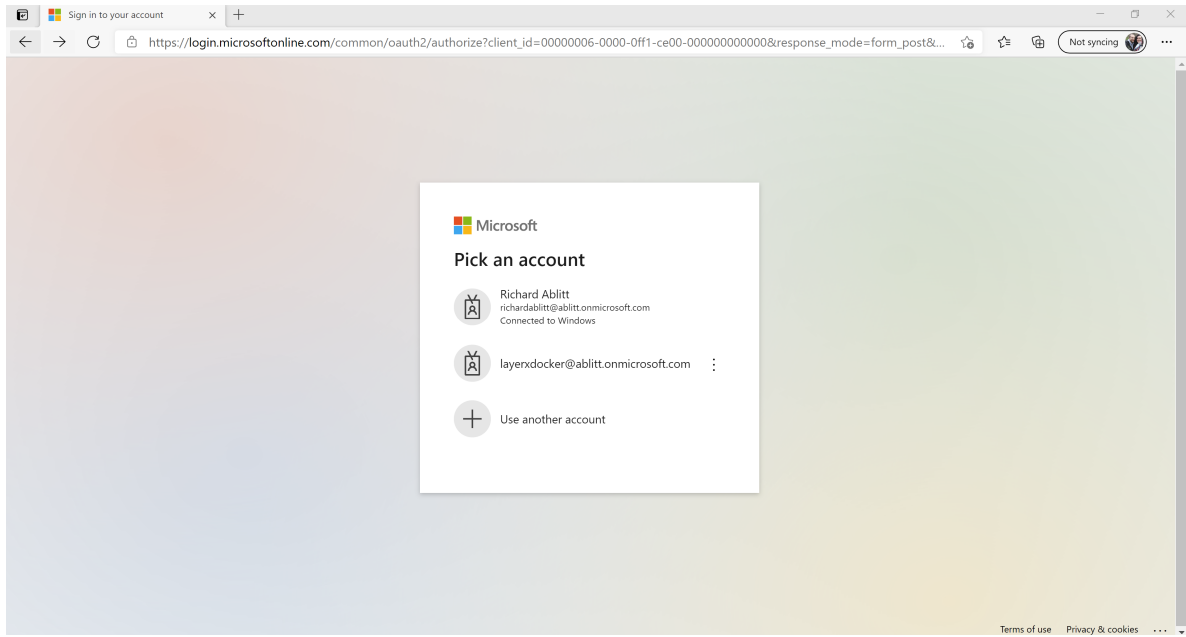
The screenshot shows the 'New user' form in the Microsoft Azure portal. The form is titled 'New user' and has a close button (X) in the top right corner. Below the title, there is a 'Got feedback?' link. The form is divided into two main sections: 'Create user' and 'Invite user'. The 'Create user' section is selected with a radio button. Below these sections, there is a 'Help me decide' link. The 'Identity' section contains several input fields: 'User name' (with a dropdown menu showing 'msteamscollector' and a checkmark), 'Name' (with a dropdown menu showing 'MS Teams Collector' and a checkmark), and 'First name' (with a dropdown menu showing 'VOSS' and a checkmark). The domain name is set to 'ablitt.onmicrosoft.com'. A 'Create' button is located at the bottom left of the form.

- Username
- Name
- First Name
- Last Name
- Let Me create the password > Enter a password
- Group = Company specific (left blank in lab)
- Roles = Global Reader

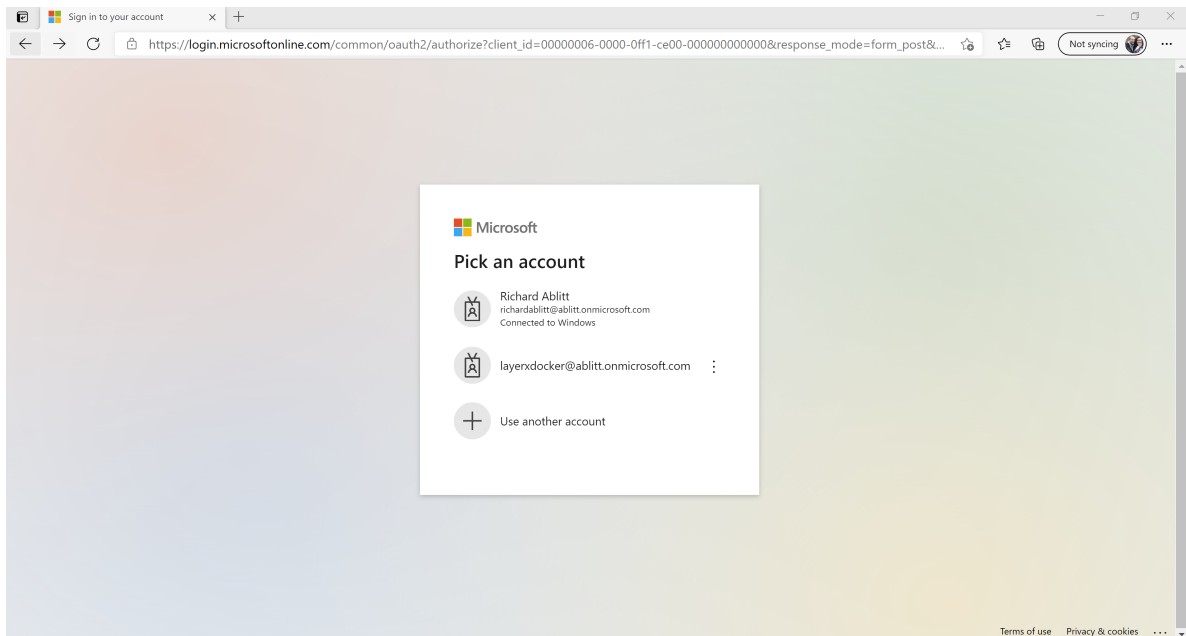
Select **Create**

3. The user needs to log in once to change the password for the first time and verify Admin

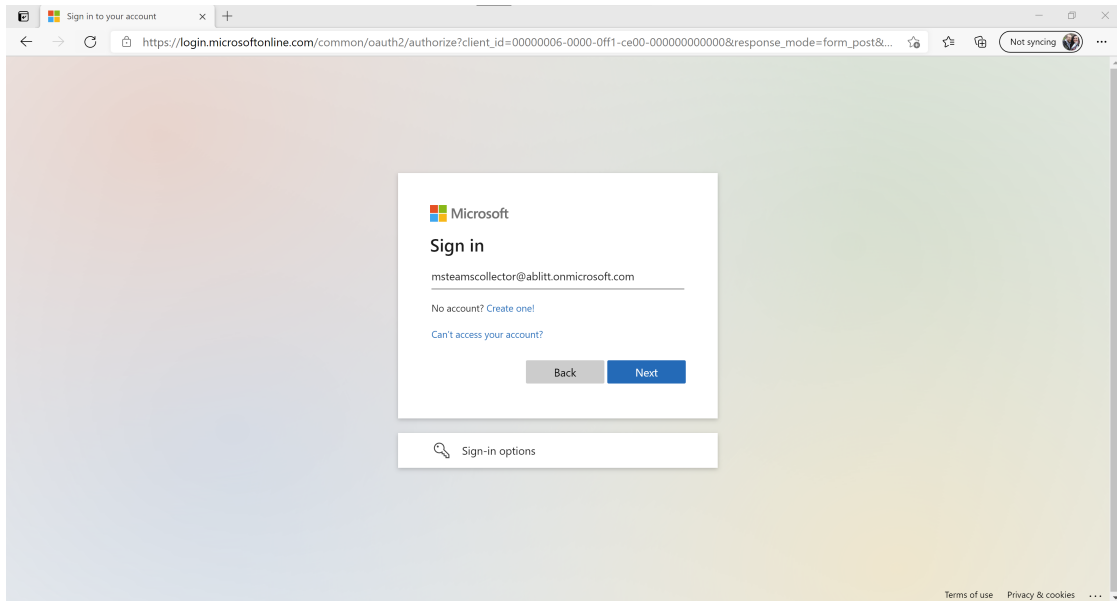
Navigate to <http://admin.microsoft.com/>



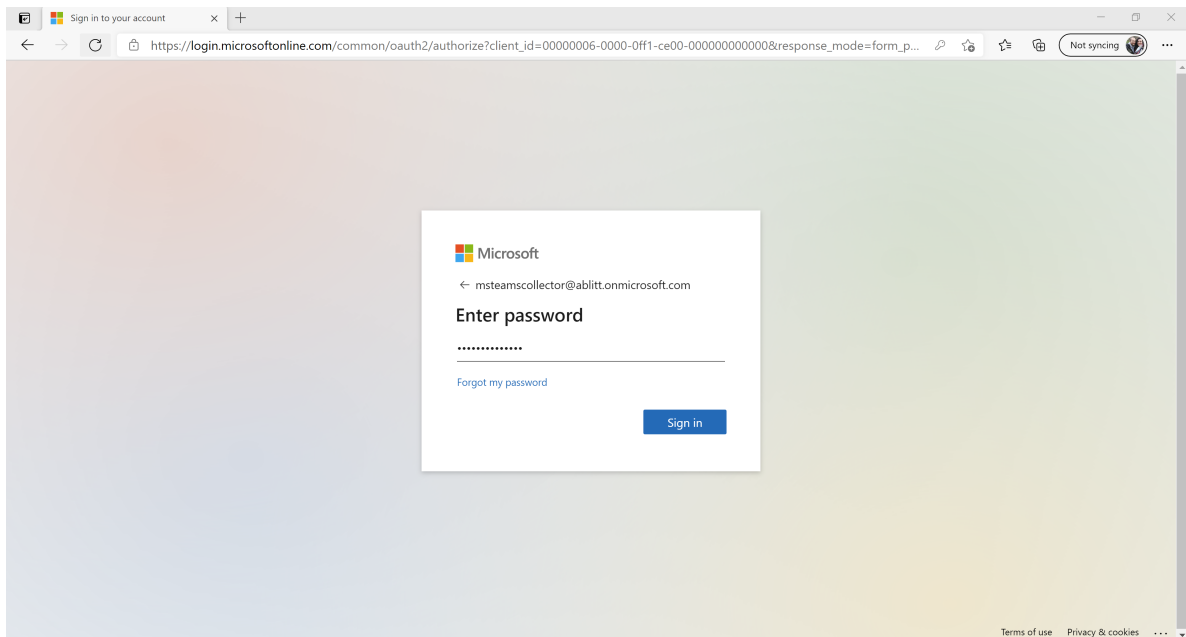
4. Use another account



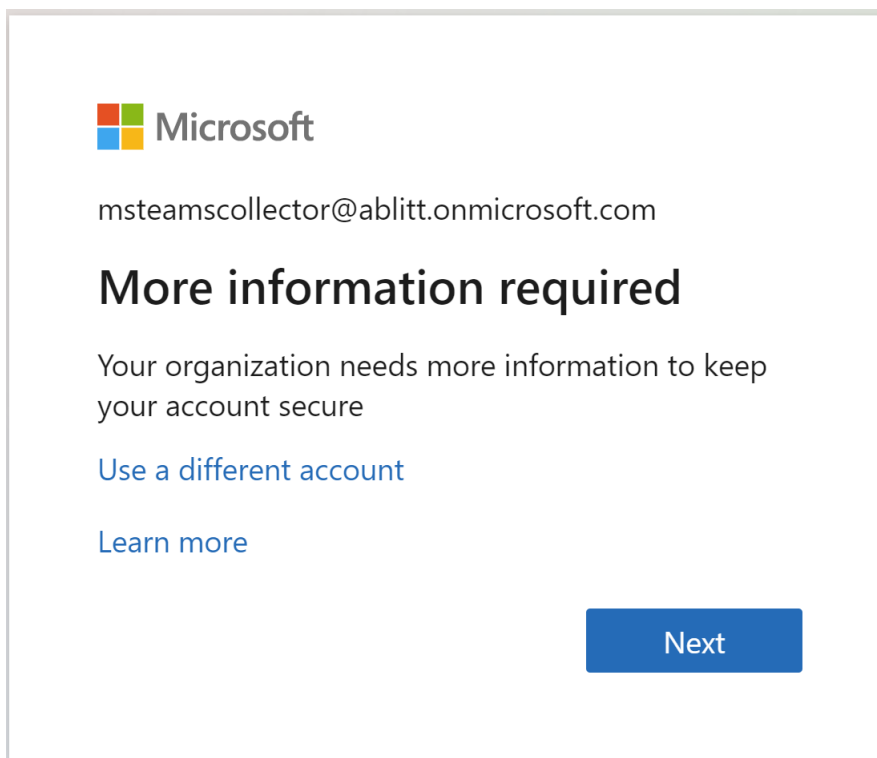
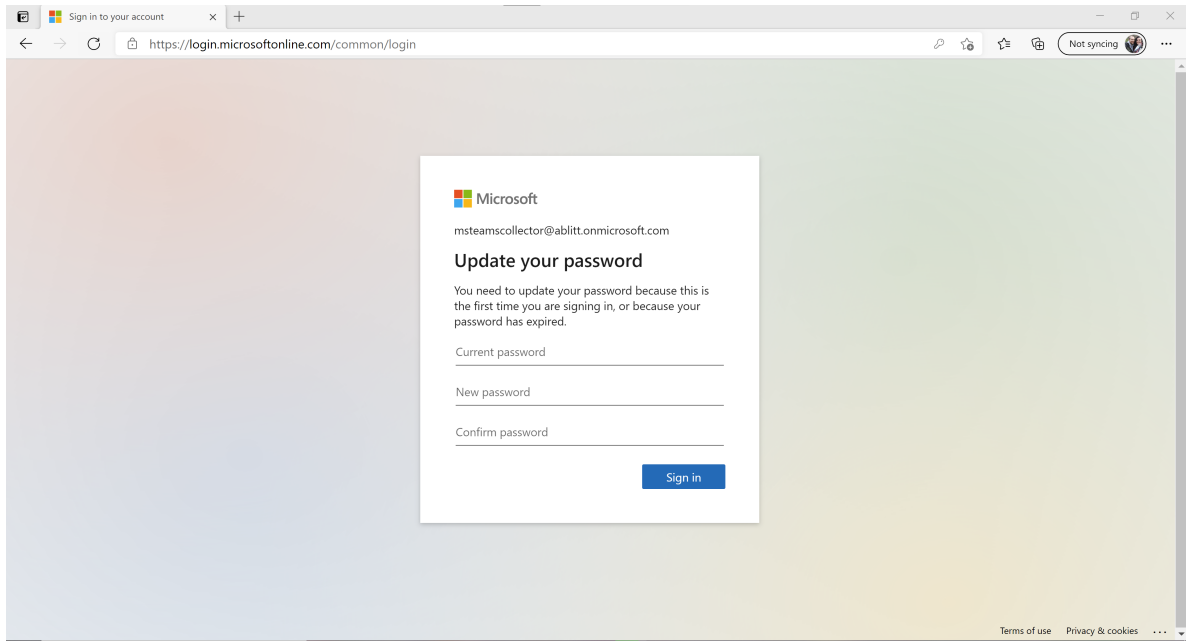
5. Enter global reader account created



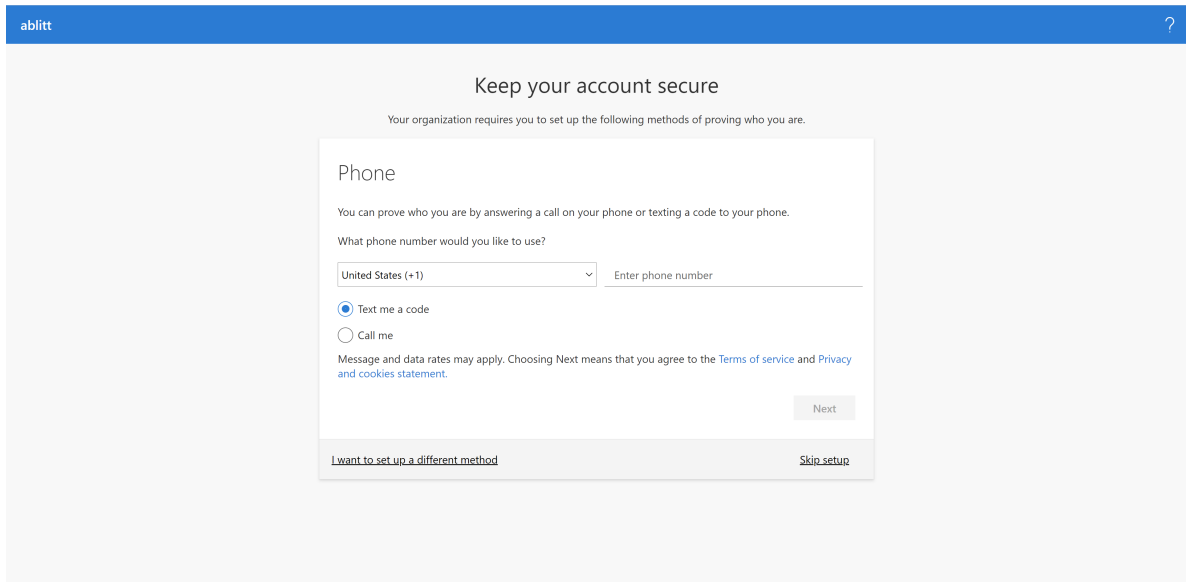
6. Select **Next** and enter password



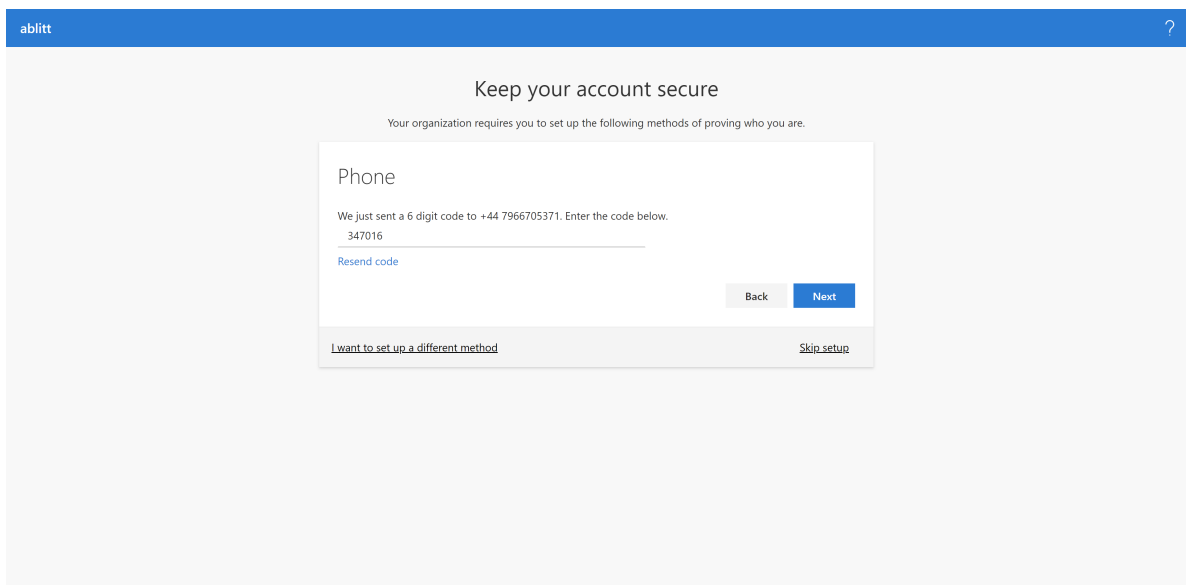
7. Enter password and create a new password



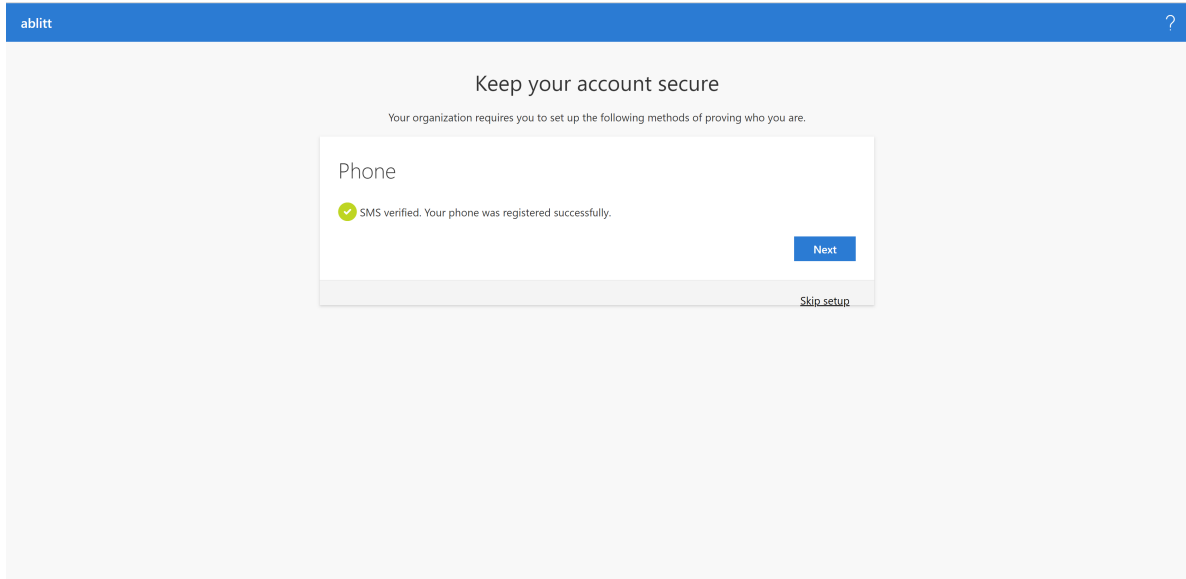
Don't skip this otherwise you cant use it in the collector



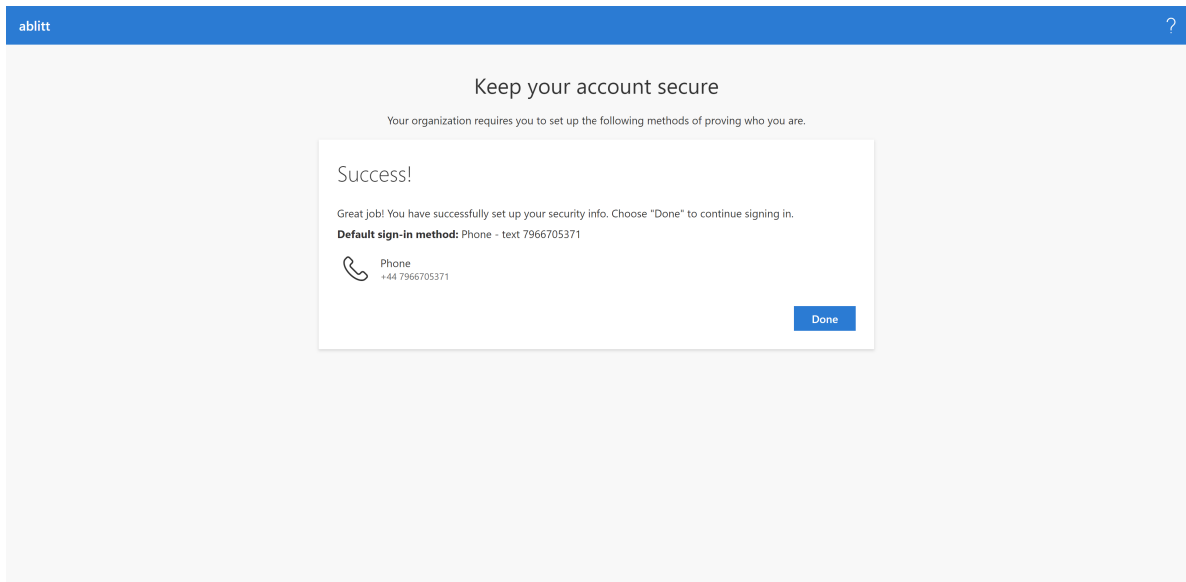
8. Once you have received a text with the code enter it into the box



Next

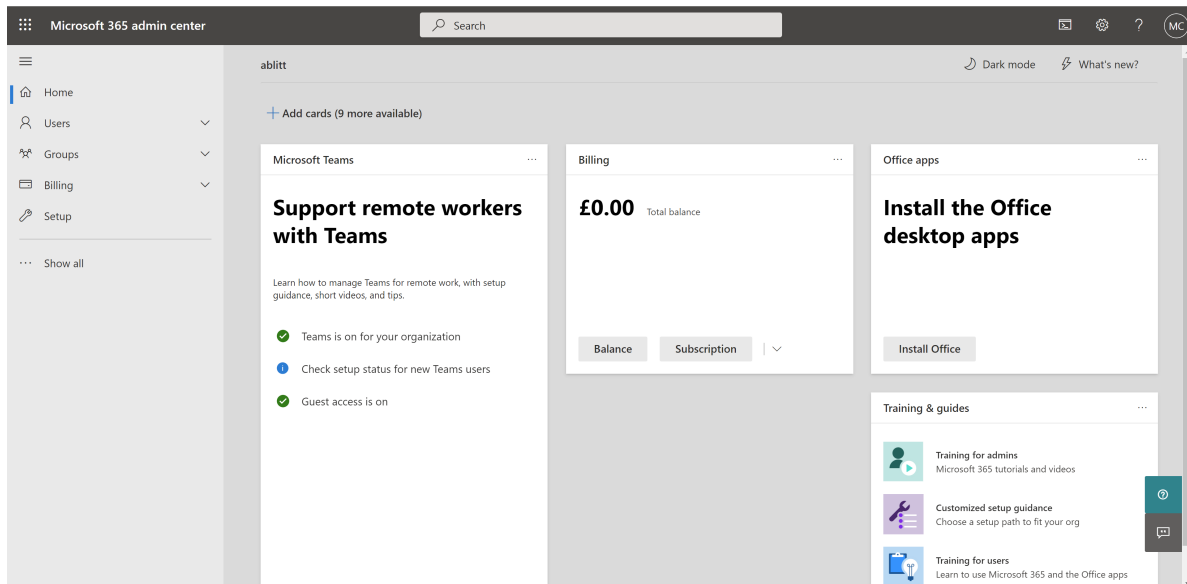


Next



Done

9. Successfully logged in

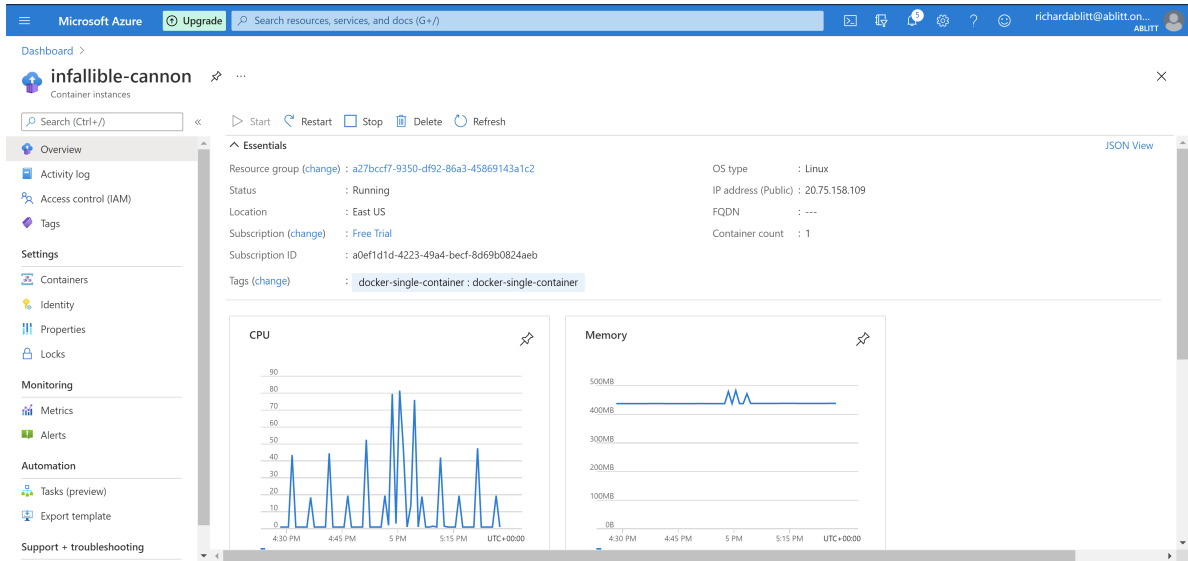


5.1. General steps

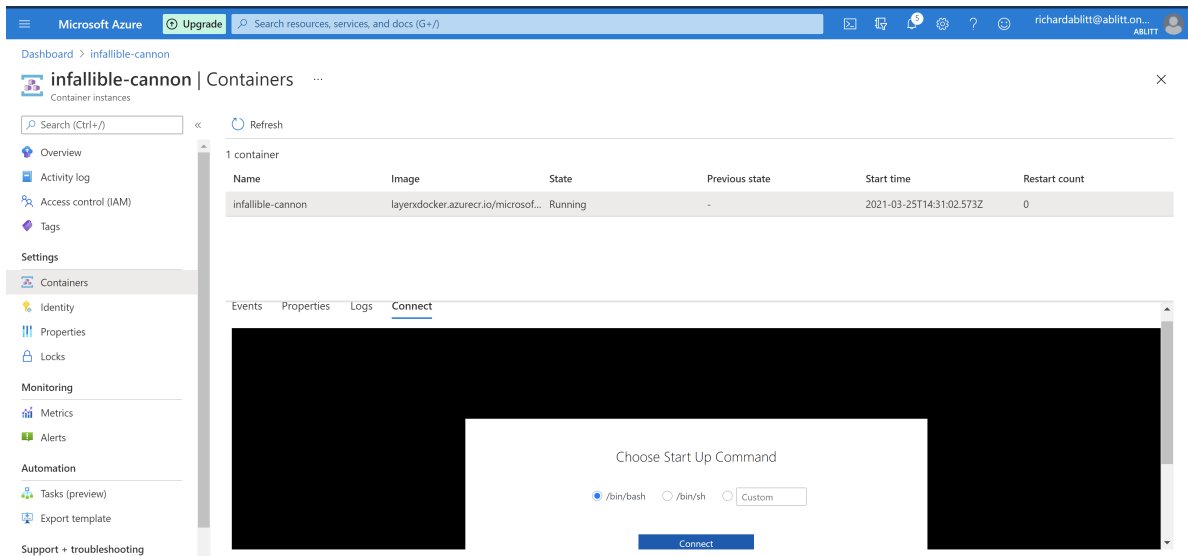
- Email to get welcome email with log in details
- Load Docker and load Powershell on the user workstation.
These have to be loaded and connected before commands can be run.

5.2. Build Container

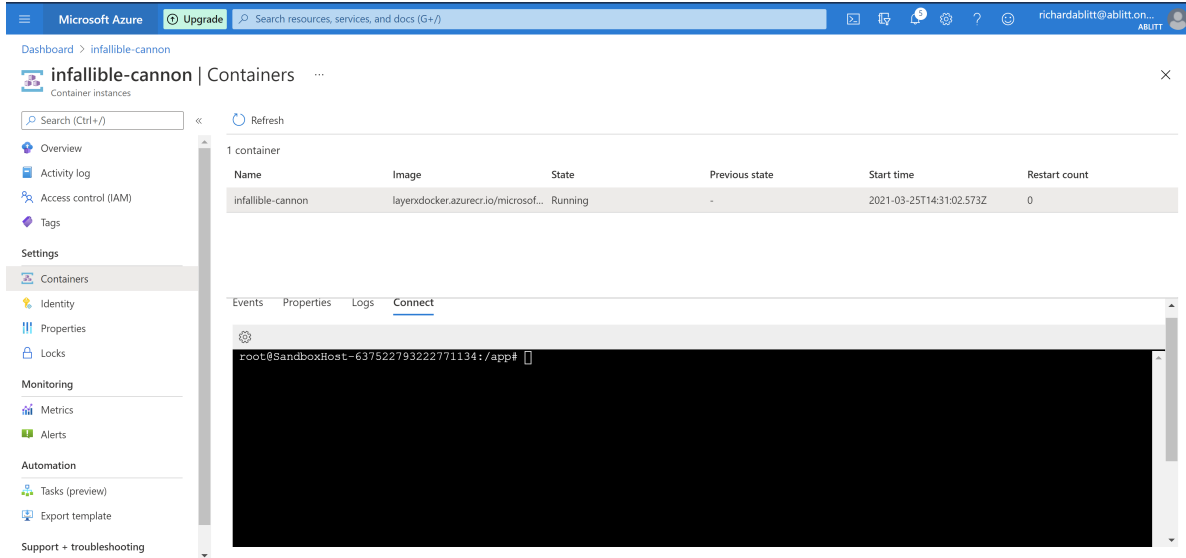
1. Navigate to **Azure > Container Instances**
2. Find container name created in power shell and select it
3. Take note of the public IP



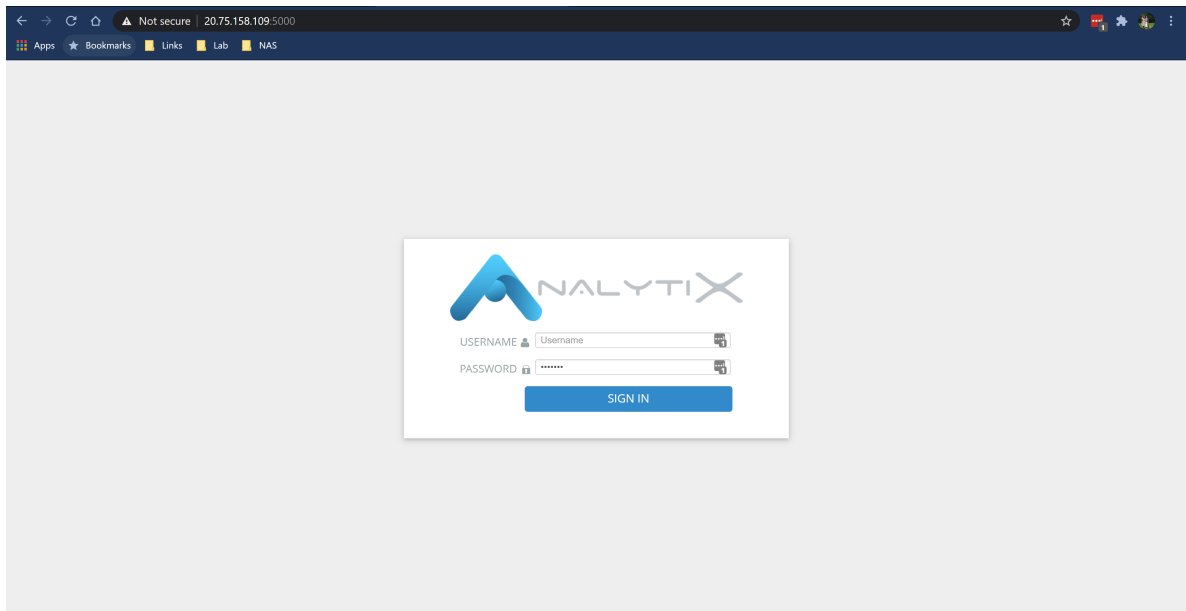
Container name > containers



4. Click connect



5. Take the sandbox name and email to Lx to get a user create and associated for logging in to the GUI
6. Open a New tab: `https://<container public IP:5000>`
7. Await the email for user details
8. Log in to the GUI



6. GUI login user email request

Reply Reply All Forward IM

Arda Savran <asavran@layerxtech.com> Richard Abilt; Alain Jansen 09:19

Your LayerX Cloud Collector is ready to go!

You forwarded this message on 25/03/2021 14:32.

config.lxcfg
17 KB

Hello Richard:

We are pleased to inform you that your LayerX Cloud Collector has been deployed successfully. Please use the following details to start monitoring your Microsoft 365 environment:

- **Cloud collector management portal:** [https://\[TBD\]:5000](https://[TBD]:5000)
- **Username:** sasol_test
- **Password:** L@123!T

Also attached is your encrypted device provisioning file to activate your cloud collector. Your LayerX Cloud Collector account has already been assigned a license. This license should be valid until [license expiry date]. Please contact support@layerxtech.com with your account details to extend this period.

For any technical assistance, please contact support@layerxtech.com.

Regards,

LayerX Team

7. Azure Container Instance Specification

Following are the minimum technical specifications for a VOSS Cloud Collector in Azure ACI:

2xCPU and 4Gig RAM with NO persistent storage.

To build the Azure ACI using docker:

- Reference the Docker Docs for further information.
- If you have docker installed on your Mac or PC or just installed docker, follow the steps below:
 1. **docker logout azure**
 2. **docker login azure** (Follow the on screen instructions and use your admin creds)
 3. **docker login layerxdocker.azurecr.io** (use the creds provided in your welcome email)
 4. Optional step if your don't have a Azure context built or as instructed by your Azure Sysadmin.
 - To add a context. **docker context create aci [somename]**
 - Follow on screen instructions
 - Finally install and run your CI by typing the syntax below – no quotes

```
docker --context somename run -d --restart always --cpus 2 --memory 4G -p 5000:5000 layerxdocker.azurecr.io/microsoft-teams-debian:v3
```

Log in into your admin portal using the web browser and confirm ACI is present and running.

8. Configuration Steps

1. Use your web browser to go to your VOSS Agent's management portal.
2. Log in with the credentials provided by the VOSS support Team:

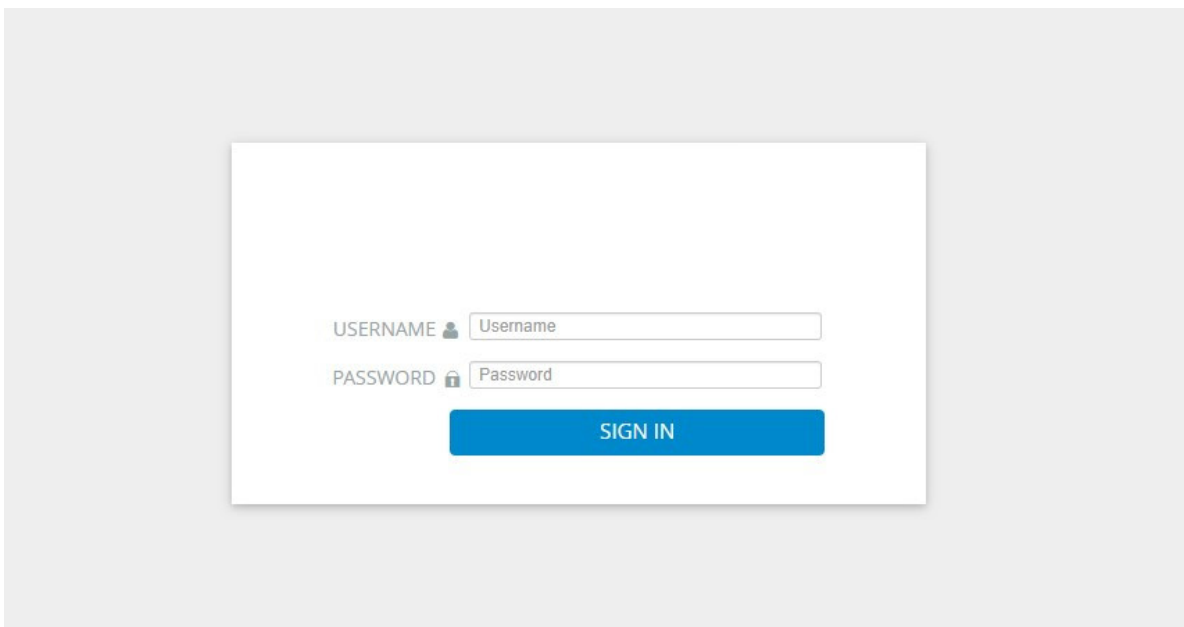


Figure 1 - VOSS Agent login screen

3. Click on the menu button on the top right corner and select **Data Sources**:

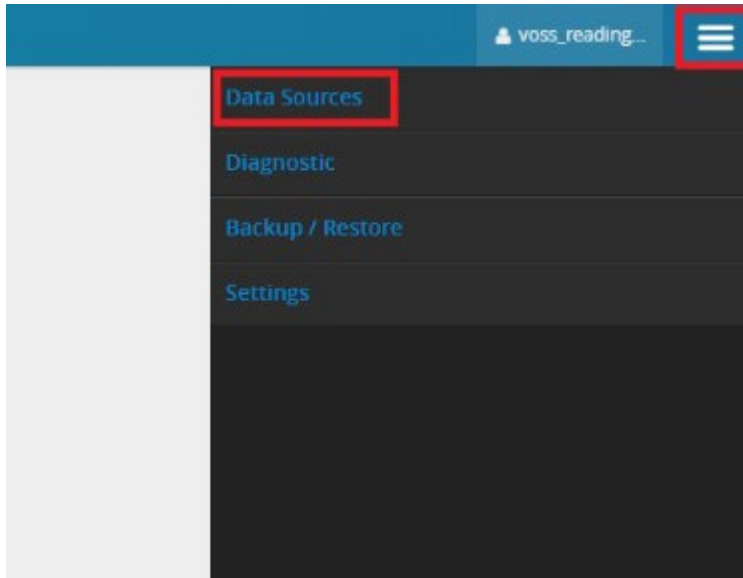


Figure 2 - VOSS Agent data source configuration

This will direct you to the data source configuration page.

4. Click on the blue + sign on the top left corner to create a new data source.
5. On the next screen, please choose the **vendor** and **type** as “Microsoft” and “Microsoft Teams Connector” respectively; give your data source a name, and click on the **Next** button:

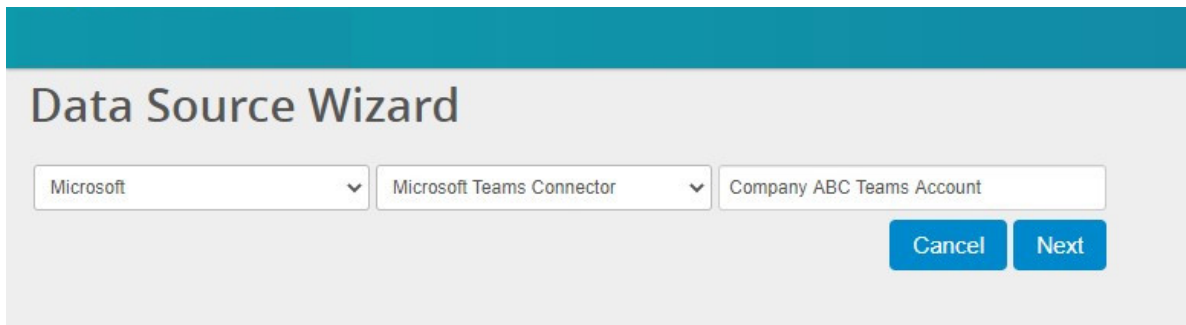


Figure 3 - VOSS Agent data source configuration for Microsoft Teams

6. On the next screen, choose the newly defined data source, and click on **Edit**. This will enable the corresponding database and API configuration menus. Start with the Data API configuration. Enter the following:
 - Data Source Name: This is a description of your data source.
 - Enable/Disable checkbox: Make sure that this checkbox is checked for successful data collection.
 - Username: Enter the username for the “Global Reader” account that was generated on the Microsoft Admin Portal as part of the prerequisites for this guide.
 - Password: Enter the password for the “Global Reader” account that was generated on the Microsoft Admin Portal as part of the prerequisites for this guide.

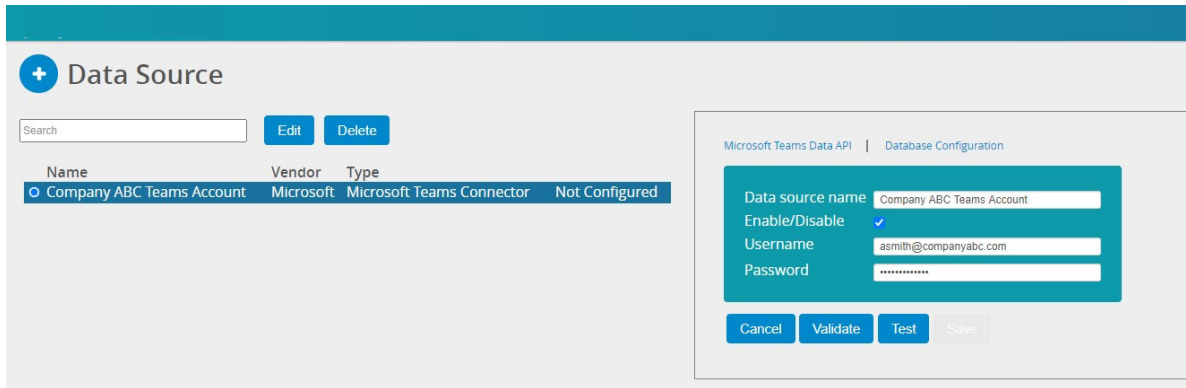


Figure 4 - VOSS Agent Microsoft API configuration for Teams

7. Click on the **Validate** button which validates that all the required values are entered.
8. Click on the **Test** button which checks your Microsoft “Global Reader” account access.
9. Click on the **Save** button to finalize the API configuration.

Note:

- The **Save** button will not be available until you validate your configuration and test it against the Microsoft API.
- Depending on the network connection speed that is available to VOSS Cloud Collector, the “Test” phase may take up to a minute.

10. Click on the **Database Configuration** tab for the same data source profile. This is where you enter the connection details for a VOSS Dashboard Server which will host your collected data.
11. From the drop-down menu, select “Reporter DB”.
12. Enter the IP address for the VOSS Dashboard Server.
13. “Retry Delay” is used to determine how long to wait before attempting to connect to the Dashboard Server Database after a failed connection. You may leave this attribute as is.

Note: VOSS Collector uses an encrypted channel to upload the processed data to VOSS Dashboard Server. This is a unidirectional connection that is initiated by the VOSS Collector using port TCP/5432. In case, you have a firewall/NAT device between the VOSS Collector and your Dashboard Server, please ensure that you make the necessary changes on your network to allow this incoming traffic thru the firewall/NAT device. If the collector is hosted by VOSS, our support team can provide the specific public IP address that the incoming connection attempts will be coming from.

14. Click on the **Validate** button which validates the values entered.
15. Click on the **Test** button which checks the connectivity to VOSS Dashboard Server.
16. Click on the “Save” button to finalize the database configuration.

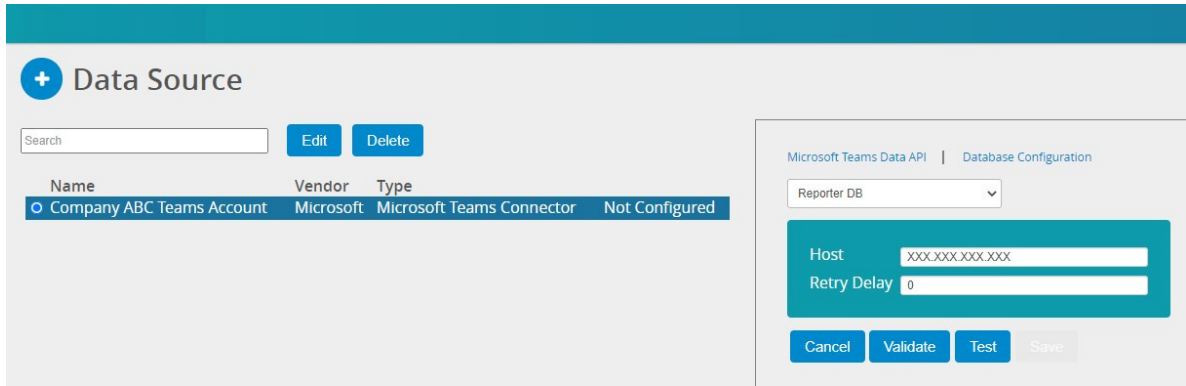


Figure 5 - VOSS Agent database configuration

At this point, we completed the configuration that is needed to collect and process Microsoft Teams data. The next step is to create a data source to collect the service health details.

17. Click on the blue + sign on the top left corner again to create a new data source.
18. On the next screen, please choose the **vendor** and **type** as “Microsoft” and “Microsoft Teams Connector” respectively; give your data source a name, and click on the **Next** button:

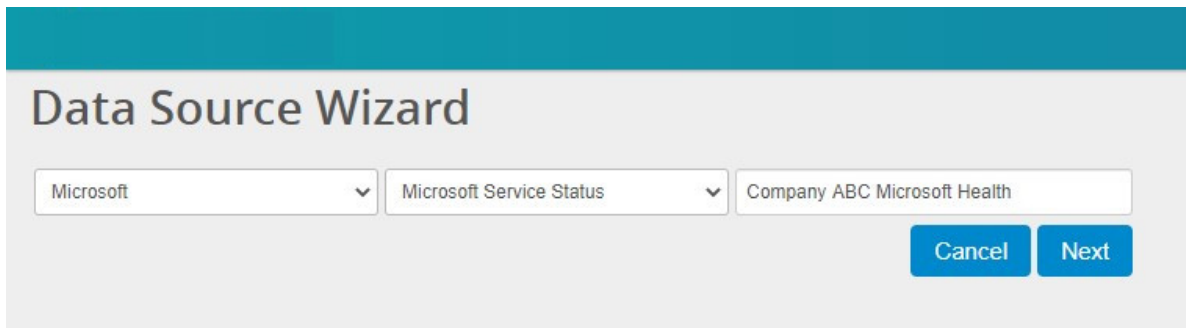


Figure 6 - VOSS Agent data source configuration for Microsoft Health Status

19. On the next screen, choose the newly defined data source, and click on **Edit**. This will enable the corresponding database and API configuration menus. Start with the Status API configuration. Enter the following:
 - Data Source Name: This is a description of your data source.
 - Enable/Disable checkbox: Make sure that this checkbox is checked for successful data collection.
 - Client ID: The client ID that you created during application registration.
 - Client Secret: The client secret that you created during application registration.
 - Tenant ID: The tenant ID that is assigned to your Microsoft Azure account.

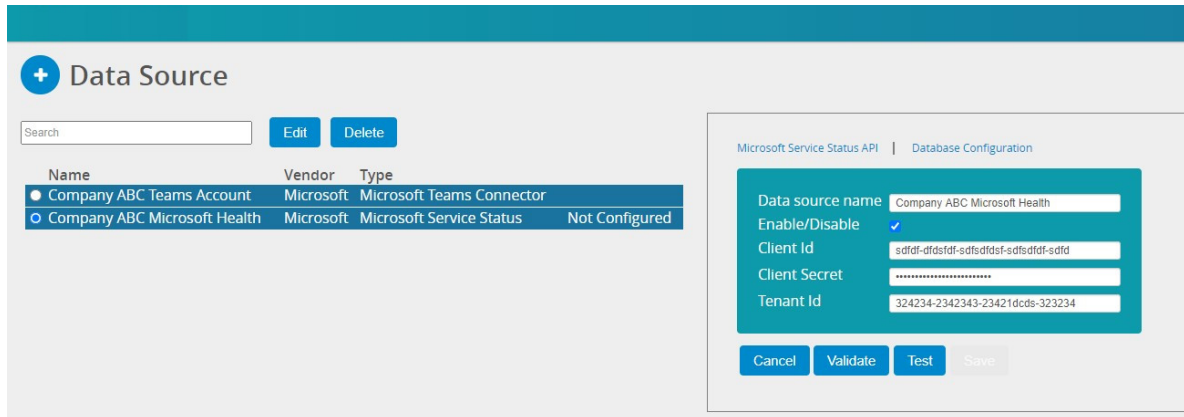


Figure 7 - VOSS Agent Microsoft API configuration for Teams

20. Click on the **Validate** button which validates that all the required values are entered.
21. Click on the **Test** button which checks for successful authentication with the Microsoft API.
22. Click on the **Save** button to finalize the API configuration.

Note:

- The **Save** button will not be available until you validate your configuration and test it against the Microsoft API.
- Depending on the network connection speed that is available to VOSS Cloud Collector, the “Test” phase may take up to a minute.

23. Click on the **Database Configuration** tab for the same data source profile. This is where you enter the connection details for a VOSS Dashboard Server which will host your collected data.
24. From the drop-down menu, select **Reporter DB**.
25. Enter the IP address for the VOSS Dashboard Server.
26. “Retry Delay” is used to determine how long to wait before attempting to connect to the Dashboard Server Database after a failed connection. You may leave this attribute as is.

At this point, we completed the configuration that is needed to collect and process Microsoft 365 Health and Incident data. Your VOSS Cloud collector is already collecting data.

There is only one more step remaining before you can start seeing some data on your dashboards. The module file that configures all the services and features internally for your needs to be imported to your cloud collector.

8.1. Import the module file

The final step is to import the module file that enables the internal features needed to start the collection.

1. Click on your username on the top right corner and choose the **Configuration** menu:

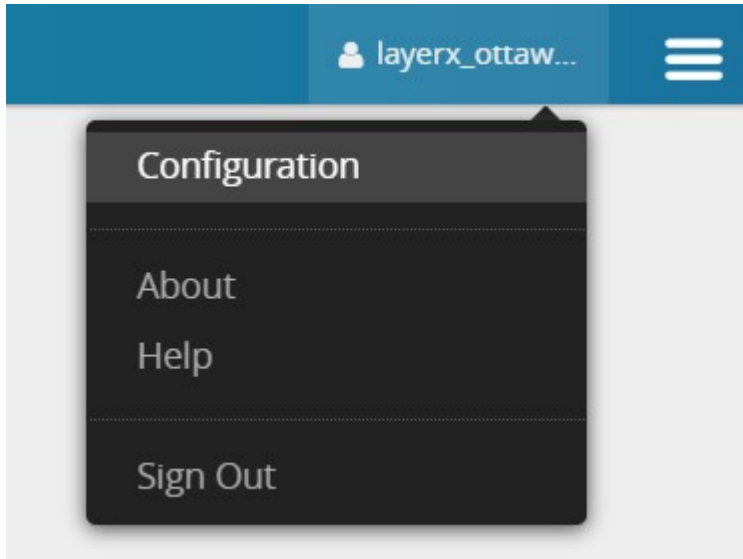


Figure 6 - VOSS Agent import module

2. Click on the **Choose File** button and locate the import file that you received from VOSS.
3. Click on the **Upload and Check** button.

Note: The import process will not work unless the API and database configurations are complete.

4. Click on the **Deploy** button to complete the import:

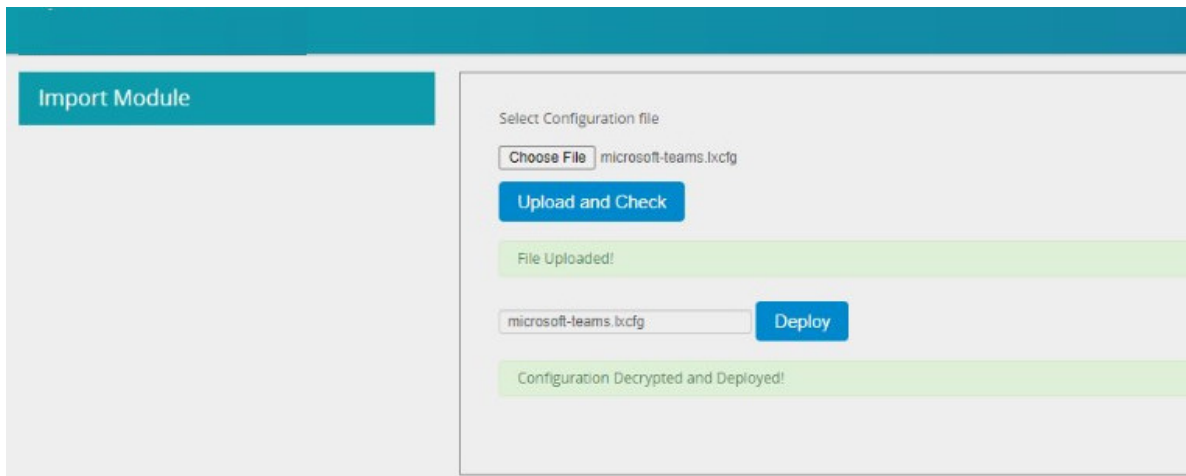


Figure 7 - VOSS Agent module deployment

5. The configuration of the agent is now complete. Please proceed to your Dashboard server and locate your corresponding Microsoft Teams dashboards.

9. Solutions to Basic Installation Challenges

In this section, a few basic issues and solutions for them will be covered. If the offered solutions do not work, please contact VOSS Support Team.

Note: When you contact VOSS Support, always include the following details in your request:

- Your username to login to your cloud collector.
 - Screenshots of the issue.
 - Diagnostic log files available on WEB GUI.
-

9.1. Issue #1: You cannot log in to your cloud collector's WEB GUI with your credentials.

Solutions:

- Please check your credentials. Try to enter them manually instead of copying and pasting them from somewhere.
- Contact VOSS support and have your credentials validated for a potential typo or license expiry.

9.2. Issue #2: You cannot connect a data source profile to the Dashboard Server.

Solutions:

- Please confirm that TCP port 5432 is open between your cloud collector and Dashboard Server.
- Please confirm that your Dashboard server is on SP63 or later. If that is not the case, it should be patched by the VOSS Support Team to support Microsoft 365 dashboards.

9.3. Issue #3: You cannot connect to your cloud collector's login page at all.

Solutions:

9.4. Issue #4: You created your “Microsoft Health” successfully but you are not able to see any data on your “Service Health Status” dashboards.

- Contact VOSS support to verify any unexpected service issues.

9.4. Issue #4: You created your “Microsoft Health” successfully but you are not able to see any data on your “Service Health Status” dashboards.

Solutions:

- Please confirm that you have the correct permissions assigned to the application you created on the Azure portal for the cloud collector. To collect service health status, the “ServiceHealth.Read.All” permission has to be assigned to the application.