VOSS Insights
MS Teams Cloud Collector Build

Release 22.1

May 09, 2022

Legal Information

Please take careful note of the following legal notices:

-
- VOSS, VisionOSS and VOSS Automate 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. Introduction

The VOSS Insights MS Teams collector in conjunction with the VOSS Insights Dashboard provides an insight into service and quality of MS Teams users' experience. For example, enriched data can be displayed in an easily customizable dashboard format based on the range of your business use cases. This includes advanced and scheduled multi-vendor reporting using calculated data and allows users to populate and analyse their measurement values based on complex multi-dimensional comparison of attributes over time.

The VOSS Insights MS Teams collector is configured in your MS Azure Tenant environment and can then integrated with VOSS Insights Dashboard.

Document Purpose

The primary objective of this document is to define the process for building and integrating the VOSS Insights MS Teams collector in Microsoft Azure to a VOSS Insights dashboard.

Specifically, the aim is to focus on VOSS Insights and its role as Service Assurance for the solution.

Audience

This document is intended for use by Customer Azure admin and engineers and VOSS staff involved in the implementation and support of the VOSS Insights Solution.

Scope

The scope of this document is to cover Service Assurance design for the solution.

2. Frequently asked questions

Does the global reader account need any licenses?

No the user does not need any licences to be purchased

Does the global reader account need to be built in the same region?

The region in which the global reader user is created has to be the same region that the container has to be built to allow the right permissions for the global reader to access the API.

Can the global reader user account be stored on an Active directory server?

No the global reader needs to be an Azure user. This is because the system can not do the two factor authentication to the login screen of the Active Directory server.

Containers and default public IP address, what happens if the container restarts?

If the container is restarted a new IP address is allocated. This could affect and network policies and rules between the MS Teams collector in Azure and the location of the Dashboard server. Consider making the IP address for the container static.

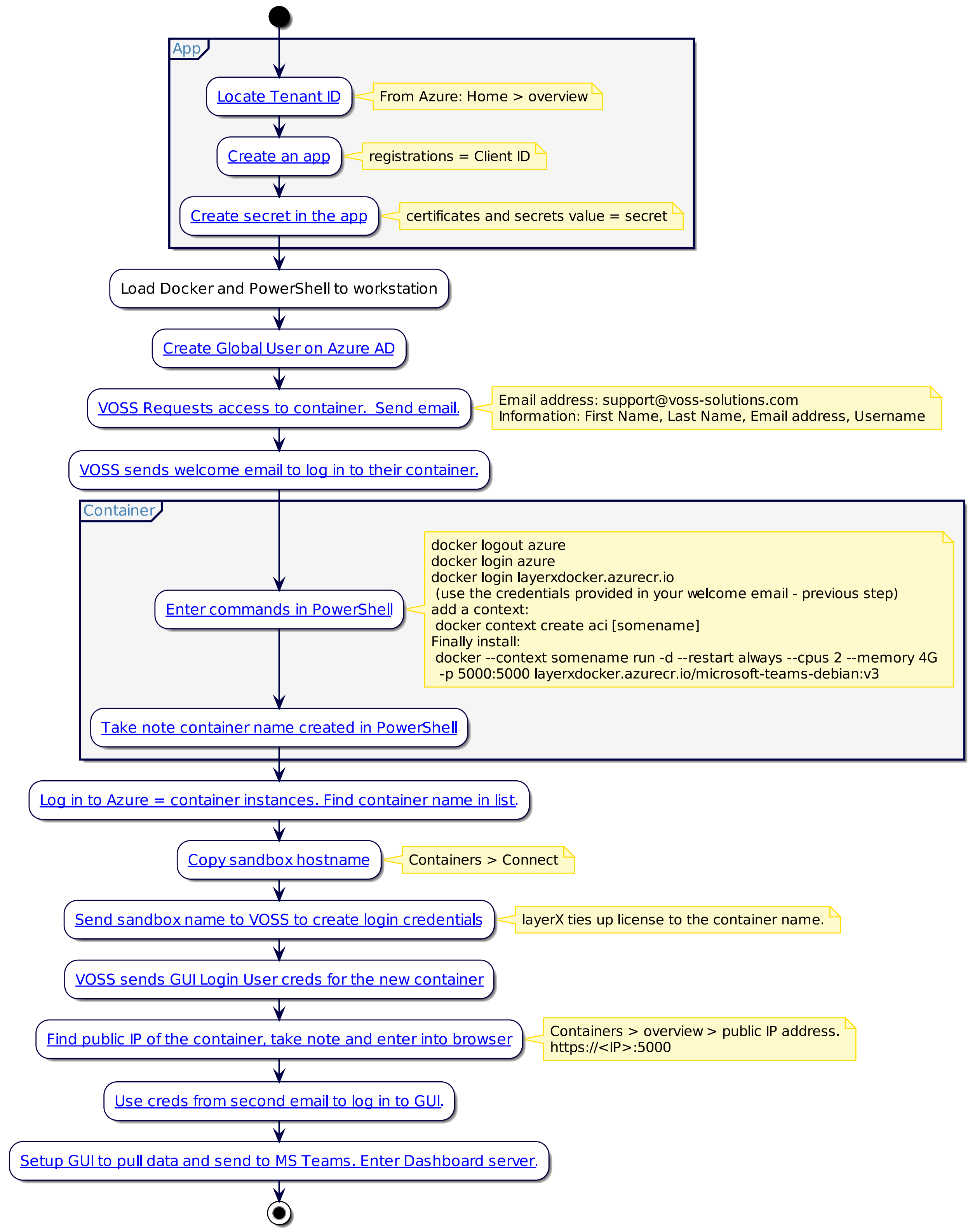
Can the username and password for the container image registry be used on different customer?

No the username and password is specific to the customer and is valid for 6 months.

Can VOSS help explain the network setup in the Azure platform?

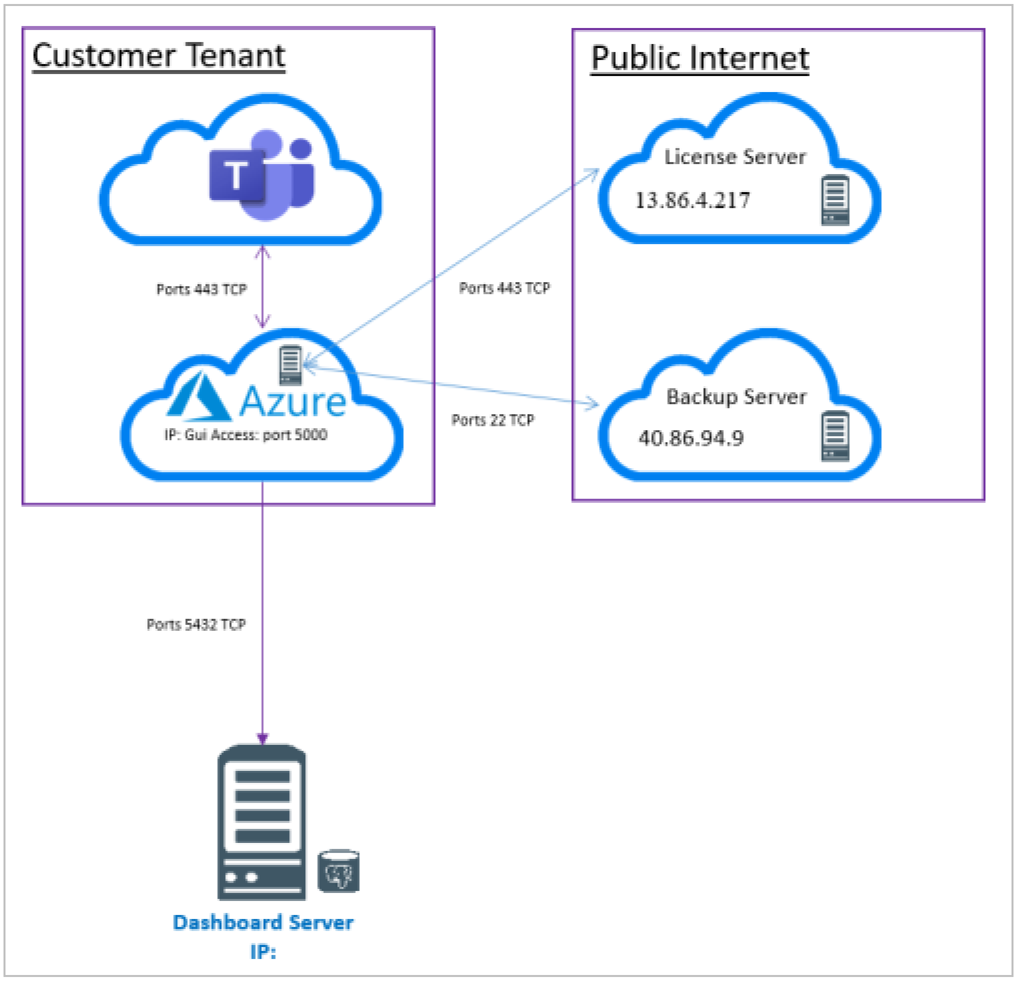
The customer will need to provide a design and expert who ensures the business security rules and policies are adhered to in the build process. This guide acts as a generic guide to get the collector working but the customer may wish to alter network to change security settings.

3. High Level Build process


App
Locate Tenant ID
From Azure: Home > overview
Create an app
registrations = Client ID
Create secret in the app
certificates and secrets value = secret
Load Docker and PowerShell to workstation
Create Global User on Azure AD
VOSS Requests access to container. Send email.
Email address: support@voss-solutions.com
Information: First Name, Last Name, Email address, Username
VOSS sends welcome email to log in to their container.
Container
Enter commands in PowerShell
Take note container name created in PowerShell
Log in to Azure = container instances. Find container name in list.
Copy sandbox hostname
Containers > Connect
Send sandbox name to VOSS to create login credentials
layerX ties up license to the container name.
VOSS sends GUI Login User creds for the new container
Find public IP of the container, take note and enter into browser
Containers > overview > public IP address.
https://<IP>:5000
Use creds from second email to log in to GUI.
Setup GUI to pull data and send to MS Teams. Enter Dashboard server.

```
docker logout azure
docker login azure
docker login layerxdocker.azurecr.io
 (use the credentials provided in your welcome email - previous step)
add a context:
 docker context create aci [somename]
Finally install:
 docker --context somename run -d --restart always --cpus 2 --memory 4G
  -p 5000:5000 layerxdocker.azurecr.io/microsoft-teams-debian:v3
```

4. Architecture Diagram



5. 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)	Unidirectional	TCP	443 (Encrypted)
2	Cloud collector agent (IP: Any) *	VOSS Dashboard Server (IP: Defined by the client)	Unidirectional	TCP	5432 (Encrypted)
3	Cloud collector agent (IP: Any) * / **	VOSS License Server (IP: 13.86.4.217)	Unidirectional	TCP	443 (Encrypted)
4	Cloud collector agent (IP: Any) * / **	VOSS Cloud Backup Server (IP: 40.86.94.9)	Unidirectional	TCP	22 (Encrypted)
5	Administrative portal users of the cloud collector (IP: Any)	Cloud collector agent (IP: Defined by the client) *	Unidirectional	TCP	443 (Encrypted)
6	Administrative portal users of the cloud collector (IP: Any)	Cloud collector agent (IP: Defined by the client) *	Unidirectional	TCP	5000 (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.

6. Container Sizing

Sizing requirement	Size of container
CPU	2 CPU
Memory	4 Gb Ram

7. Send Email to Get Container Login Details

The repository where the container is located is a private registry and to get access and load the container from the image, a user needs to be created to access the image.

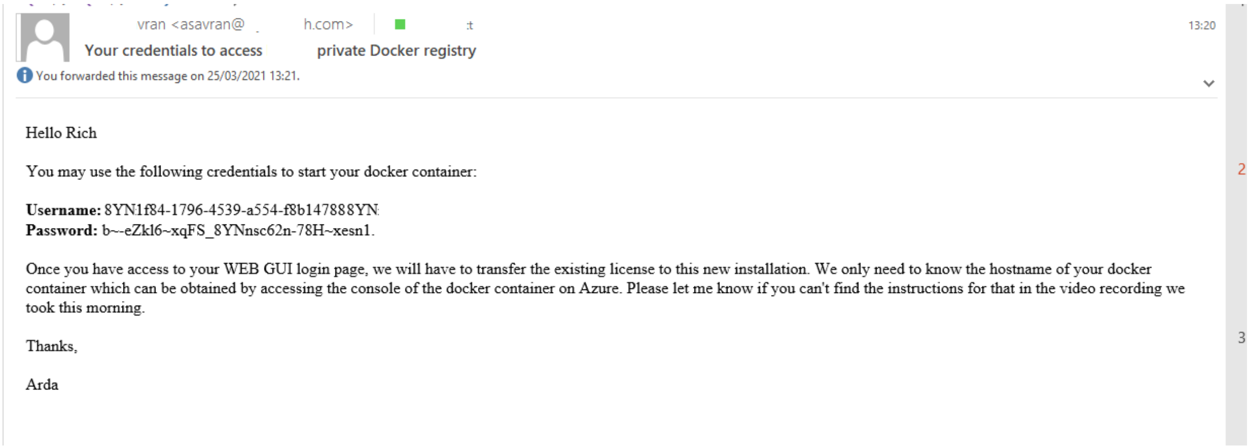
A VOSS engineer will need to send an email to VOSS to have a user created. A user can only be created if the customer has a valid license.

The email information to supply:

- Email address: support:voss-solutions.com
- Subject: User to be created for private docker registry
- Message body:
  - Customer name:
  - First name of customer:
  - Last Name of Customer:
  - Email address of customer:

This request will be processed after 14:00 GMT time. Once the request has been processed, the customer will get a copy of the username and password to log in and to get the docker container image.

The following is a example of the email.



vran <asavran@ h.com> :t 13:20

Your credentials to access private Docker registry

You forwarded this message on 25/03/2021 13:21.

Hello Rich

You may use the following credentials to start your docker container:

Username: 8YN1f84-1796-4539-a554-f8b147888YN

Password: b~-eZkl6~xqFS_8YNnsc62n-78H~xesn1.

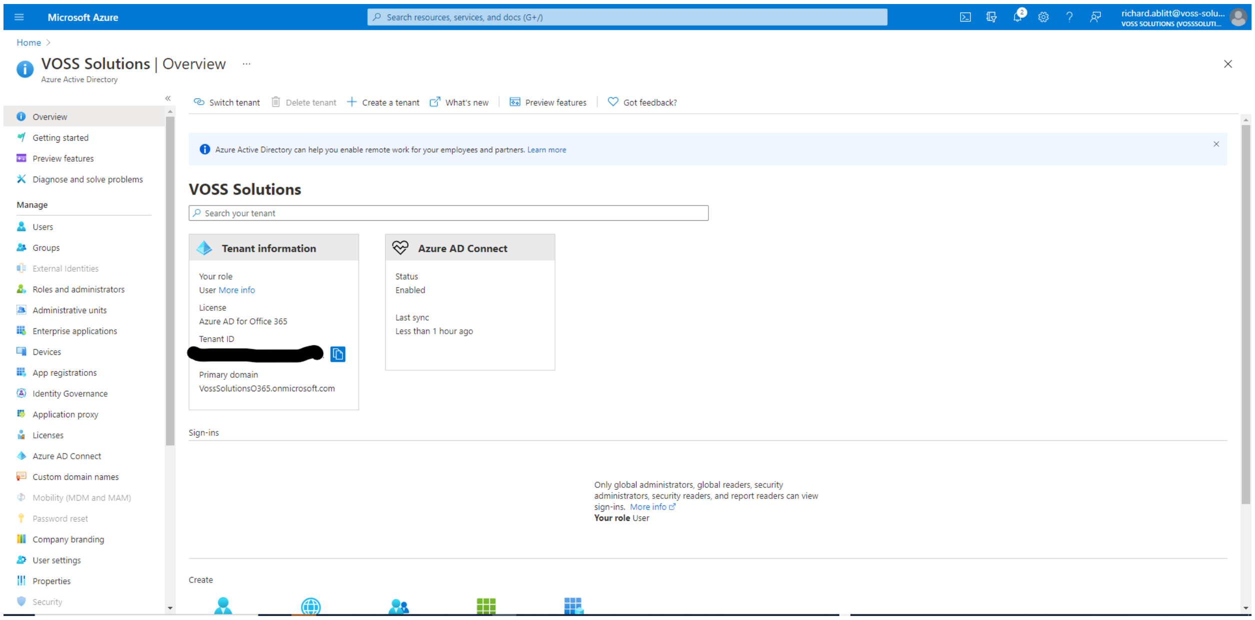
Once you have access to your WEB GUI login page, we will have to transfer the existing license to this new installation. We only need to know the hostname of your docker container which can be obtained by accessing the console of the docker container on Azure. Please let me know if you can't find the instructions for that in the video recording we took this morning.

Thanks,

Arda

8. Take a Note of the Tenant ID

Log in to portal.azure.com and on the **Overview** page, take a note of the **tenant ID** which will be added in to the GUI later.



VOSS Solutions | Overview

Azure Active Directory

Azure Active Directory can help you enable remote work for your employees and partners. Learn more

VOSS Solutions

Tenant information

Your role
User More info

License
Azure AD for Office 365

Tenant ID
[redacted]

Primary domain
VossSolutionsO365.onmicrosoft.com

Azure AD Connect

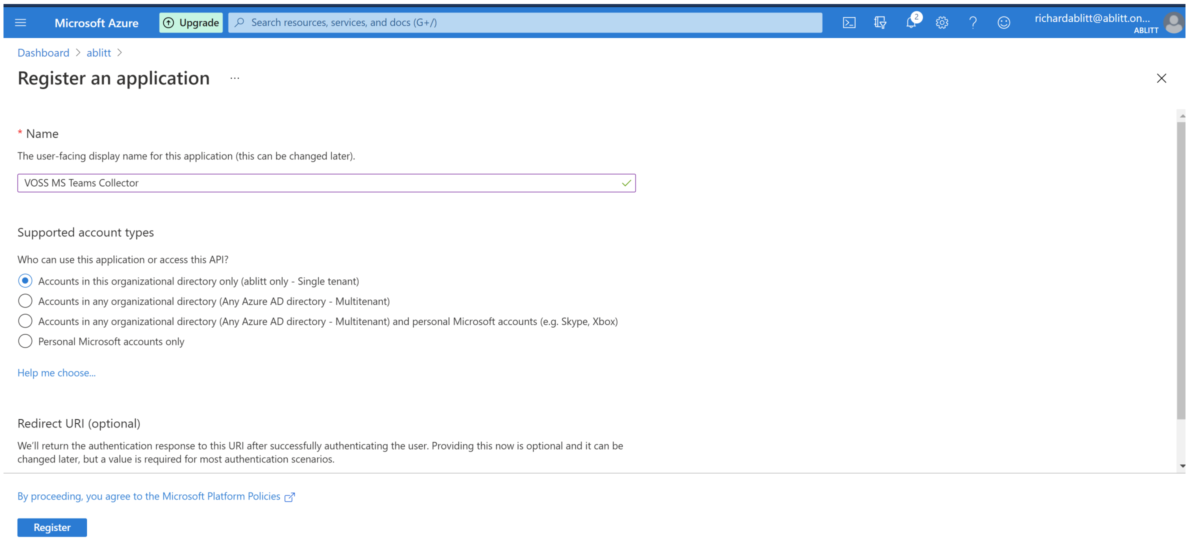
Status
Enabled

Last sync
Less than 1 hour ago

Only global administrators, global readers, security administrators, security readers, and report readers can view sign-ins. More info
Your role User

9. 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


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
richardablitt@ablitt.on...
ABLITT
Dashboard > ablitt >

Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

VOSS MS Teams Collector

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (ablitt only - Single tenant)

○ 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)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

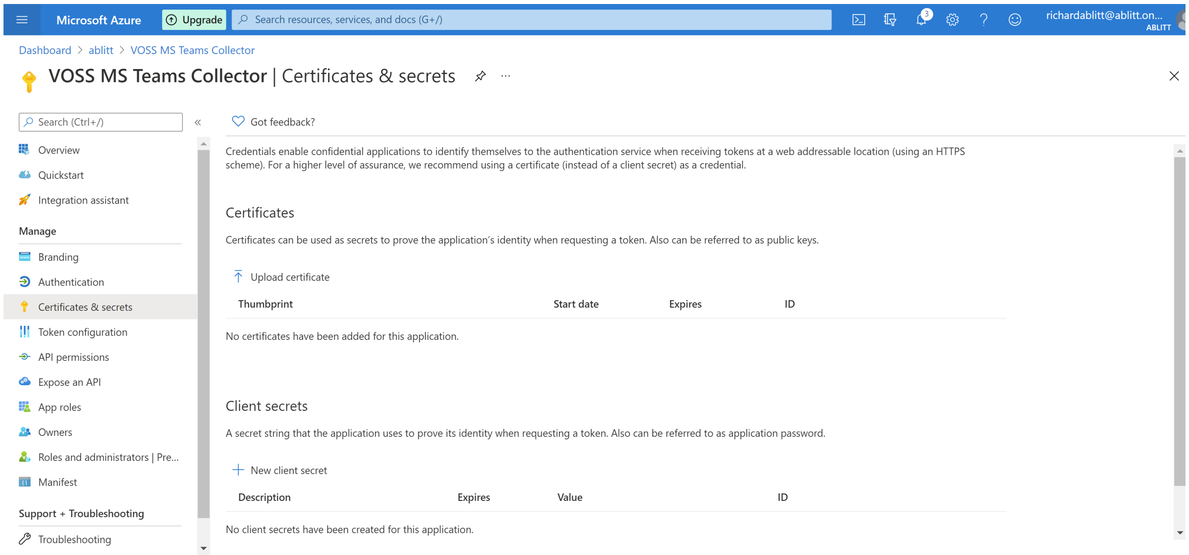
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the Microsoft Platform Policies

Take note of the following details

Application (client) ID	a7228bda-ca72-4dbf-b20e-f0ba72ba727f
Directory (tenant) ID	c85a72ba-cf50-48e8-91f1-0c08a721c9dc

6. In the app just created Go to **Certificates and secrets**



VOSS MS Teams Collector | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

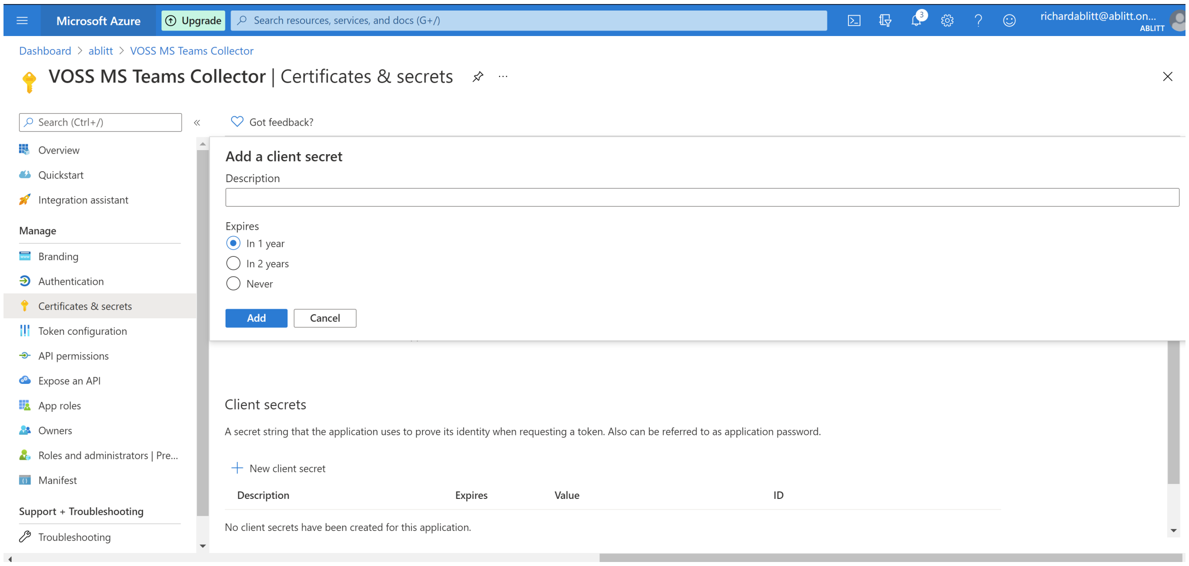
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID

No client secrets have been created for this application.

7. In the **Clients secrets** section **+New client secret**



VOSS MS Teams Collector | Certificates & secrets

Add a client secret

Description

Expires

● In 1 year

○ In 2 years

○ Never

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

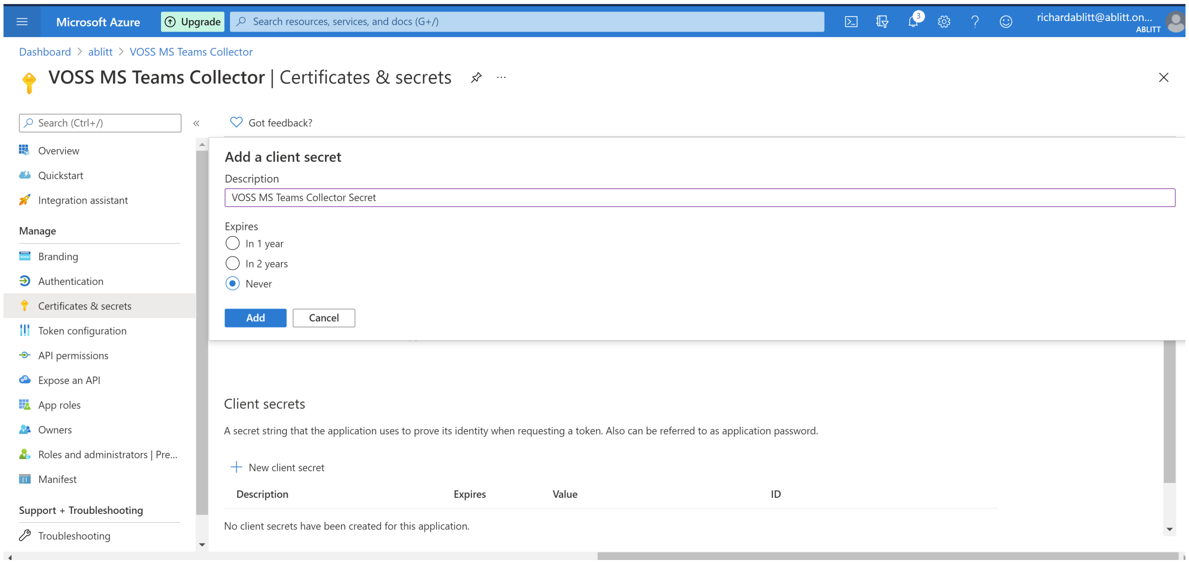
Description	Expires	Value	ID

No client secrets have been created for this application.

Give the secret a **Description**.

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

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com



VOSS MS Teams Collector | Certificates & secrets

Add a client secret

Description: VOSS MS Teams Collector Secret

Expires

○ In 1 year

○ In 2 years

● Never

Add | Cancel

Client secrets

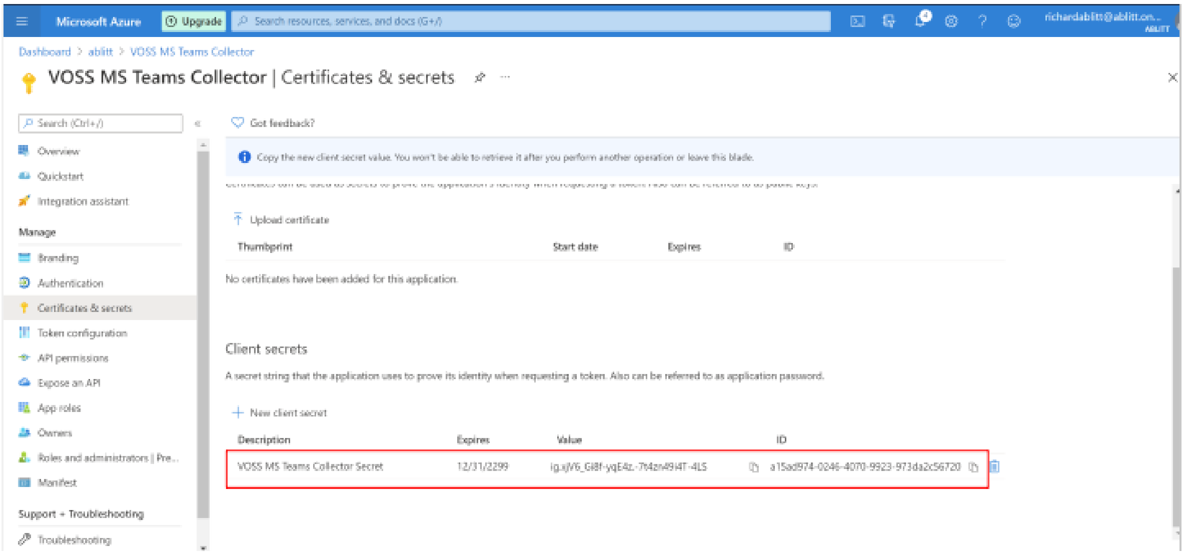
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID

No client secrets have been created for this application.

9. Copy the value against the new secret created as this will be added to the cloud collector GUI later.



VOSS MS Teams Collector | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Thumbprint	Start date	Expires	ID

No certificates have been added for this application.

Client secrets

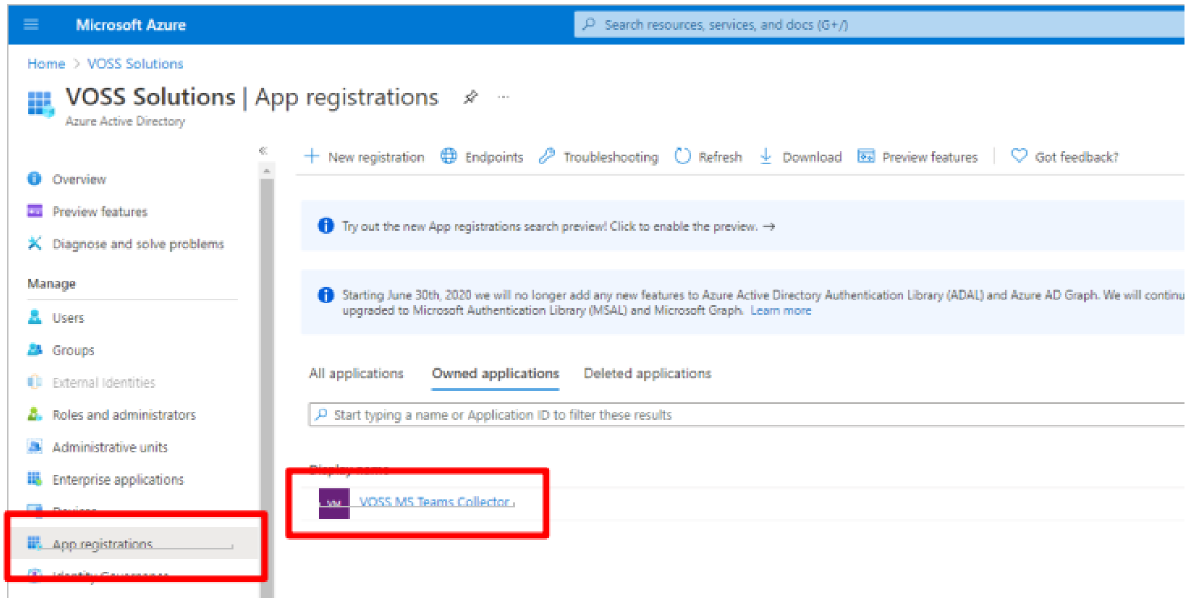
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
VOSS MS Teams Collector Secret	12/31/2299	ig.xjV6_Gi8f-yqE4z.-7t4zn49i4T-4LS	a15ad974-0246-4070-9923-973da2c56720

10. Assign Role to App

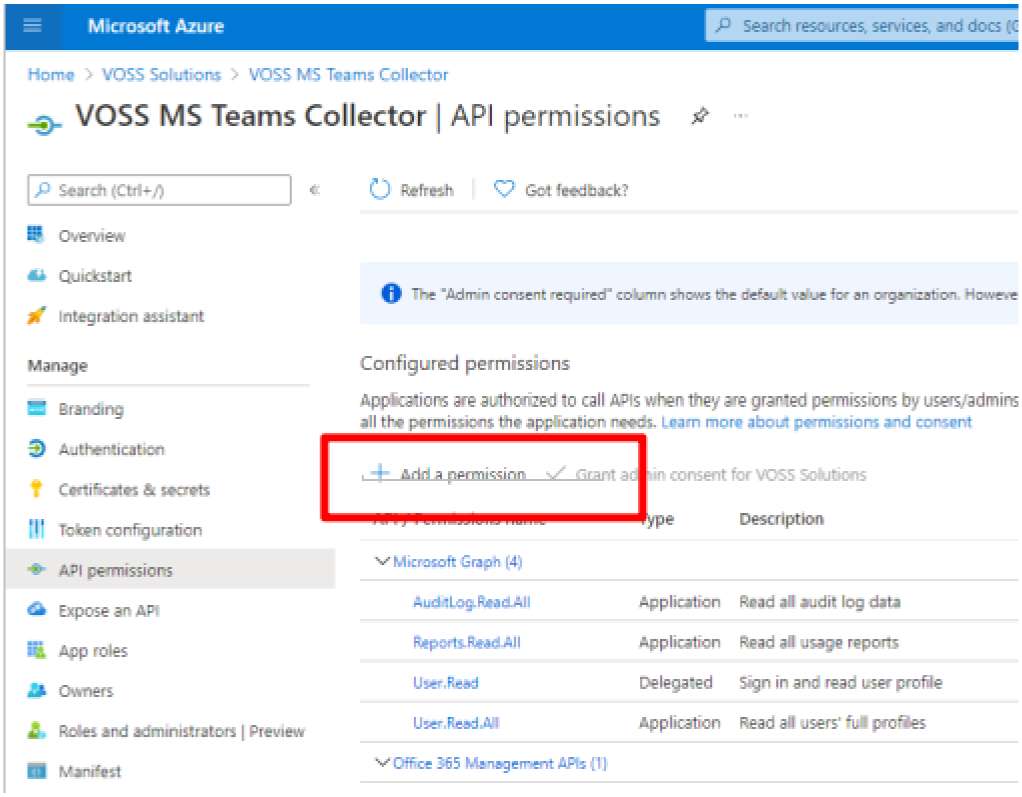
1. Go to portal.azure.com > **Azure AD** > **App registrations** > select the app.



Try out the new App registrations search preview! Click to enable the preview. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continu upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

2. Go to portal.azure.com > **Azure AD** > **App registrations** > select the app > **API permissions**.



VOSS MS Teams Collector | API permissions

The "Admin consent required" column shows the default value for an organization. Howeve

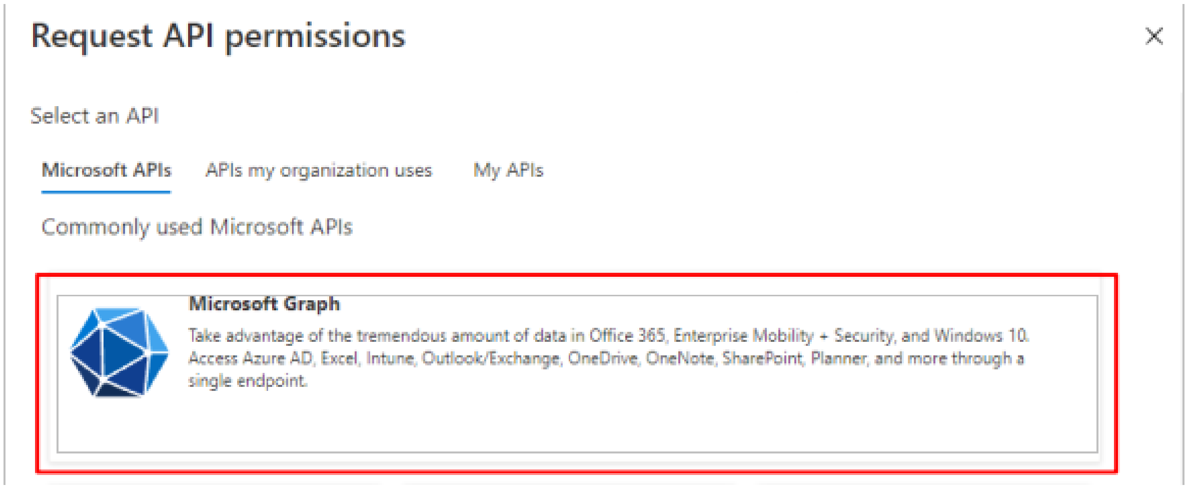
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description
Microsoft Graph (4)		
AuditLog.Read.All	Application	Read all audit log data
Reports.Read.All	Application	Read all usage reports
User.Read	Delegated	Sign in and read user profile
User.Read.All	Application	Read all users' full profiles
Office 365 Management APIs (1)		

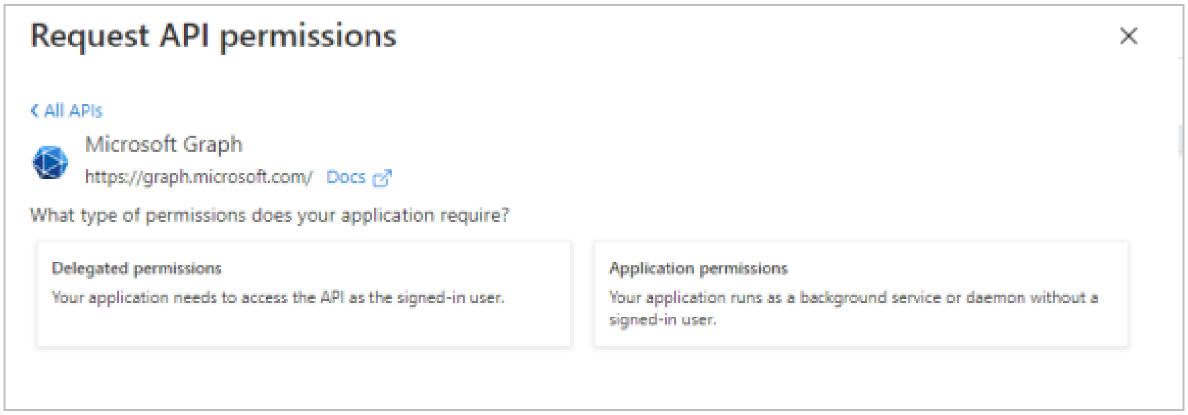
Click **Add a permission**.

3. Select the **Microsoft Graph** API.



Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

4. Select **Application permissions**.



Request API permissions

< All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

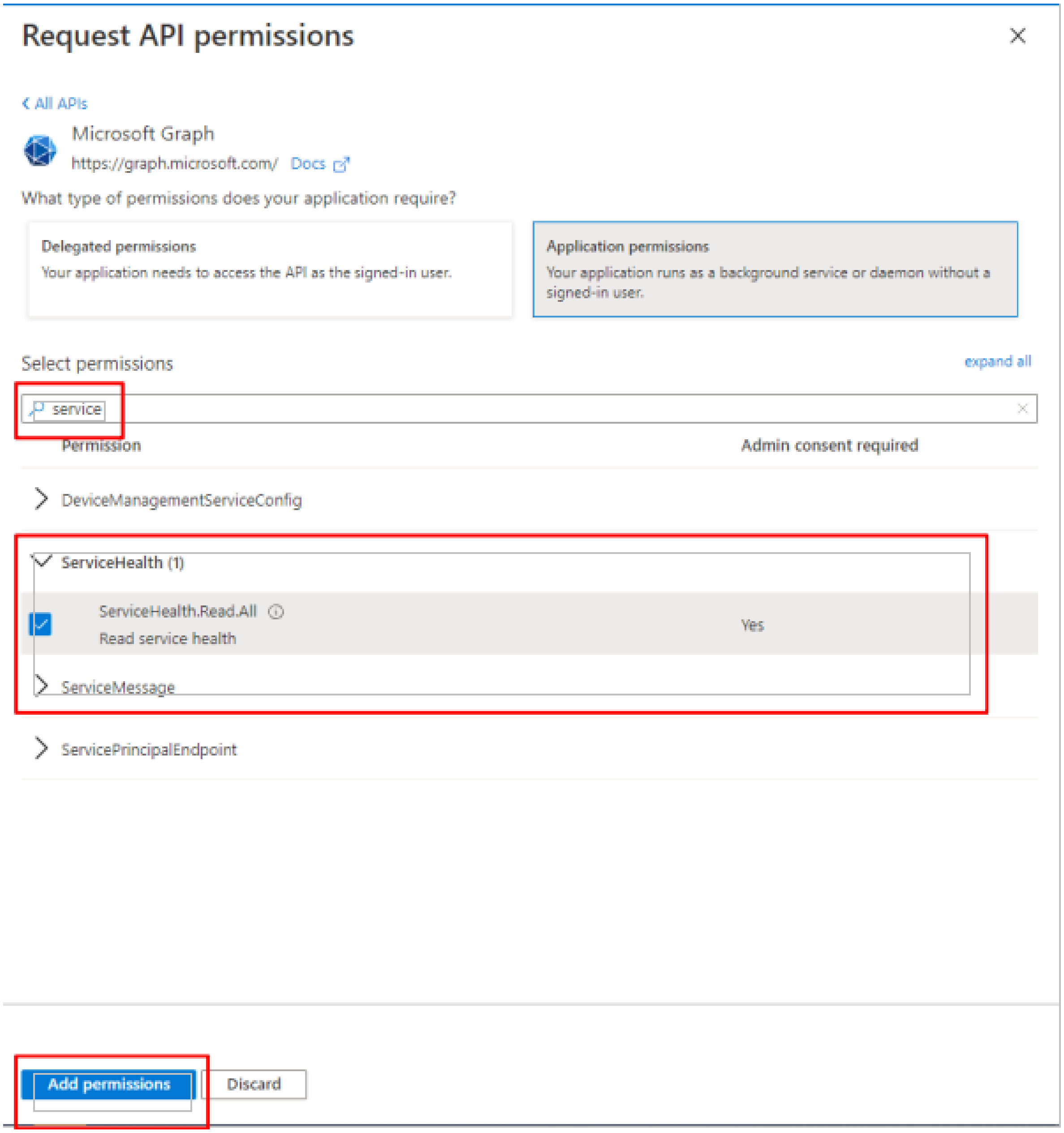
Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

5. Use the search to find the Service health read. Select the role and select **Add permissions**.



Request API permissions

< All APIs

Microsoft Graph

https://graph.microsoft.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

service

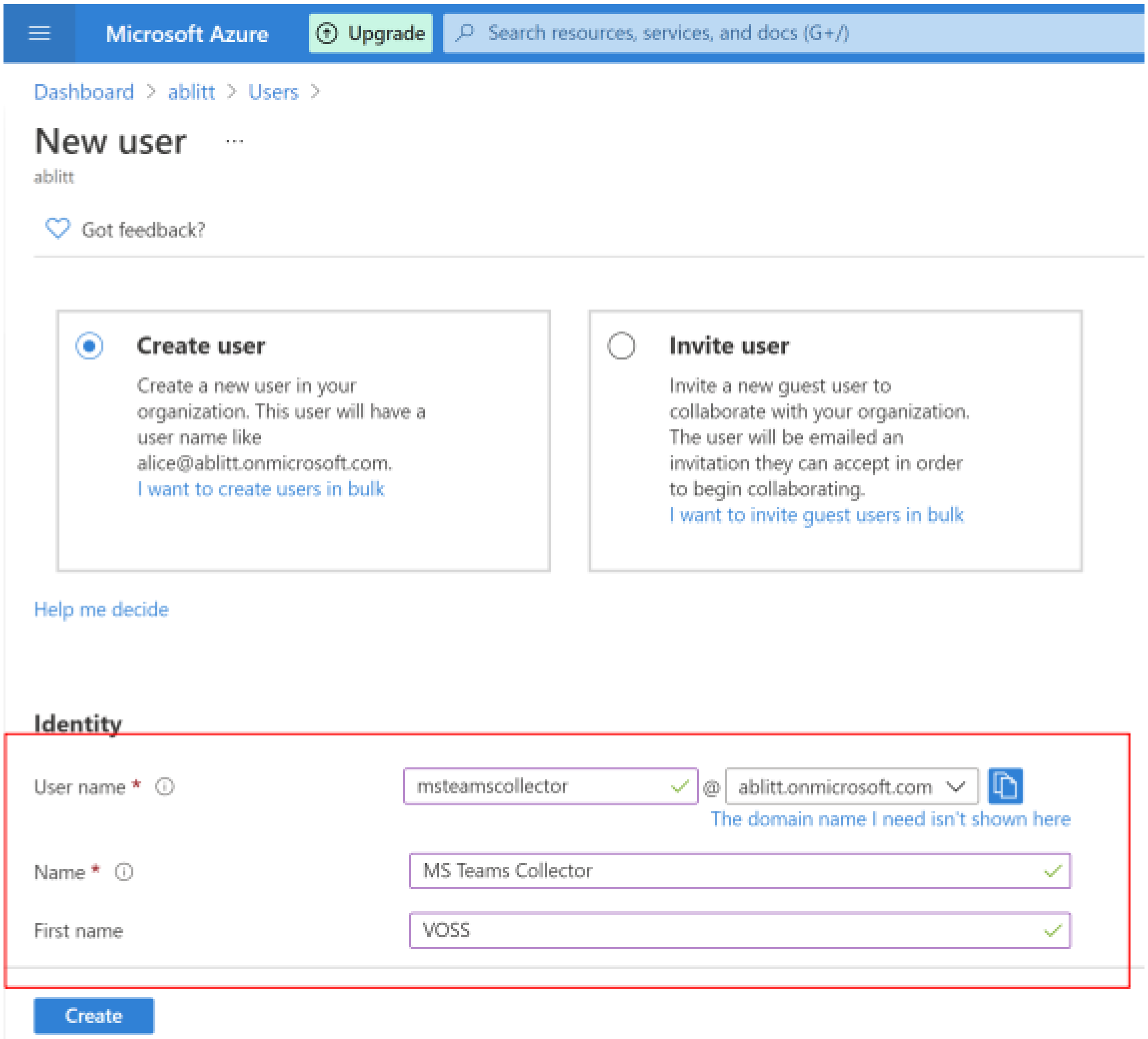
Permission	Admin consent required
> DeviceManagementServiceConfig	
∨ ServiceHealth (1)	
☑ ServiceHealth.Read.All Read service health	Yes
> ServiceMessage	
> ServicePrincipalEndpoint	

An administrator will need to grant consent by logging in and granting admin consent for the customer to make the option active.

11. Create an Azure Service Account User

The following section explains how to create a global reader user that allows the MS Teams collector in Azure to access the MS Teams admin API and gather the data that will be sent to the dashboard server.

1. Log in to portal.azure.com and select the Azure active directory icon
2. Azure Active directory > **Users**
3. **+ New user**
4. Fill out the following:



● Create user

Create a new user in your organization. This user will have a user name like alice@ablitt.onmicrosoft.com.
I want to create users in bulk

○ Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
I want to invite guest users in bulk

User name *: msteamscollector @ ablitt.onmicrosoft.com
The domain name I need isn't shown here

Name *: MS Teams Collector

First name: VOSS

- 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**

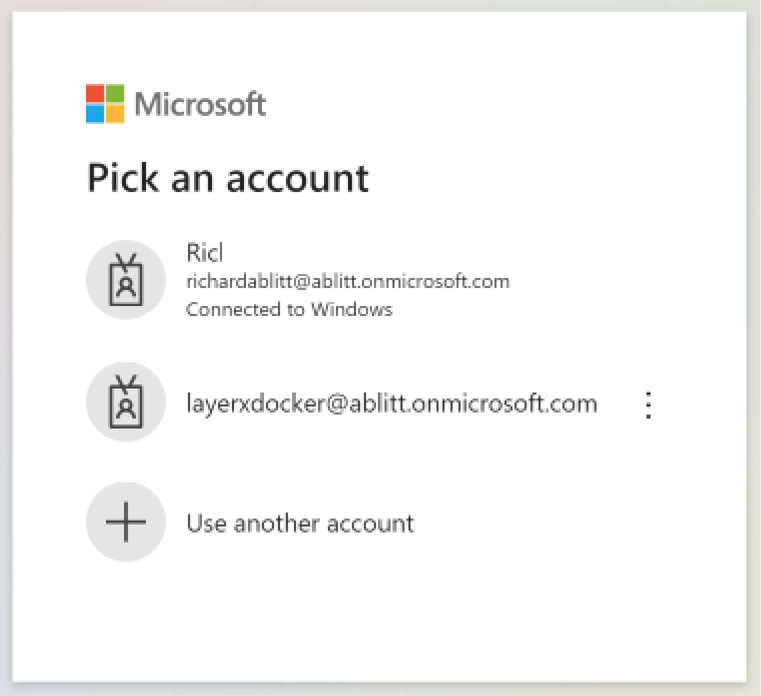
The user needs to log in once to ensure and make sure there are no password issues or authentication issues. This will ensure the following do not stop a successful connection:

- Password is correct
- Password has not expired
- Not forcing user to change password on first login
- No need to verify user password via email
- No need to verify user password via text
- No two factor authentication with passcode generator
- User is not being directed to a on premise active directory
- User can login successfully

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

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

   Choose **Use another account**.



Microsoft

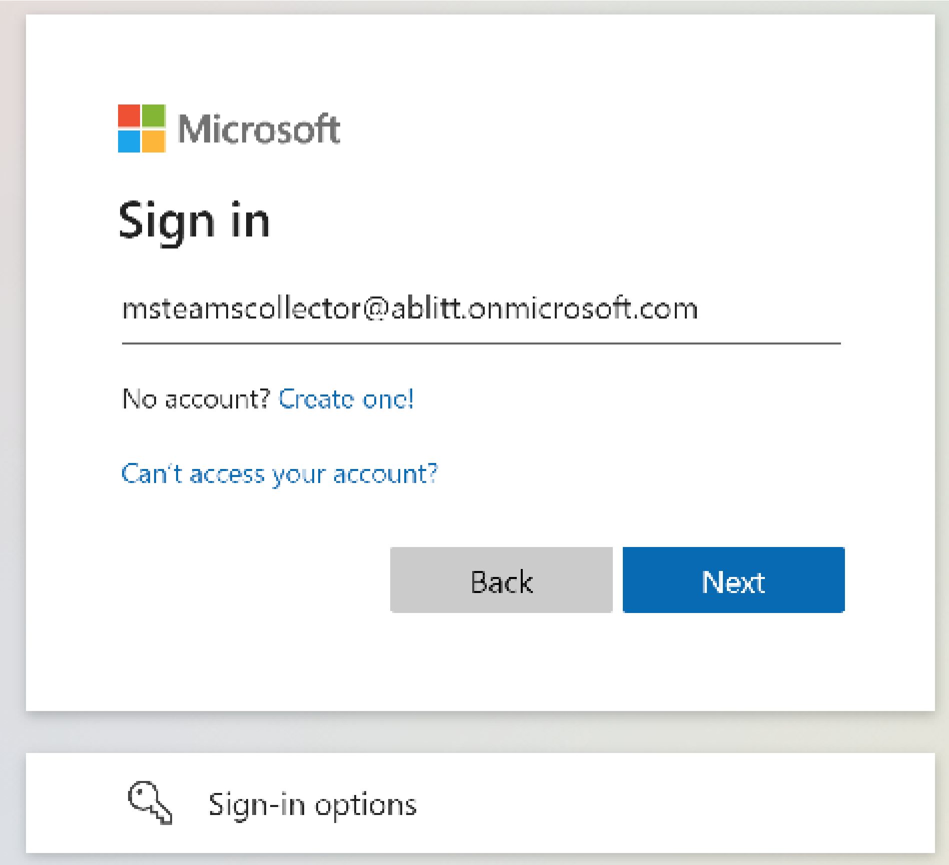
Pick an account

Ricl
richardablitt@ablitt.onmicrosoft.com
Connected to Windows

layerxdocker@ablitt.onmicrosoft.com

Use another account

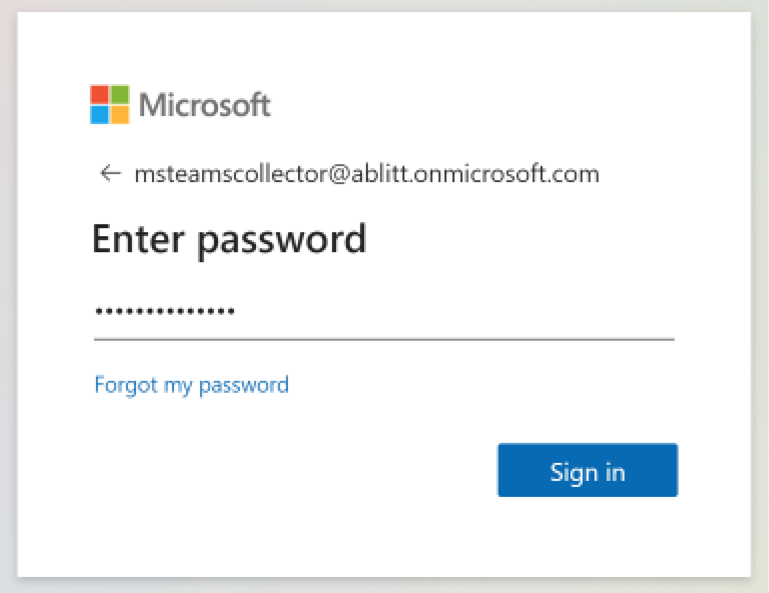
6. Enter global reader account created.



Sign in

msteamscollector@ablitt.onmicrosoft.com

6. Select **Next** and enter password

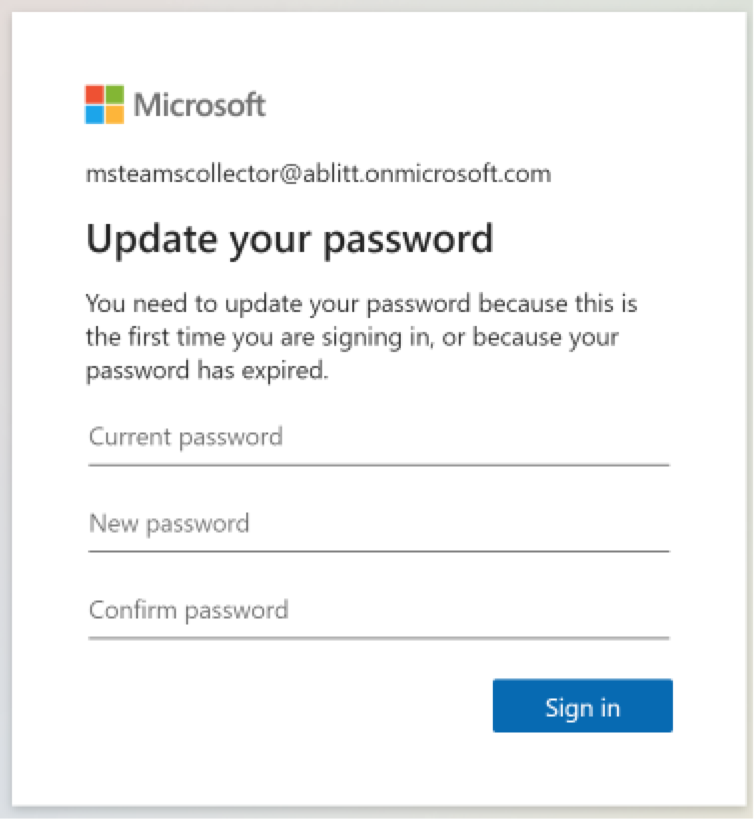


msteamscollector@ablitt.onmicrosoft.com

Enter password

••••••••••••••

7. Enter password and create a new password



Microsoft

msteamscollector@ablitt.onmicrosoft.com

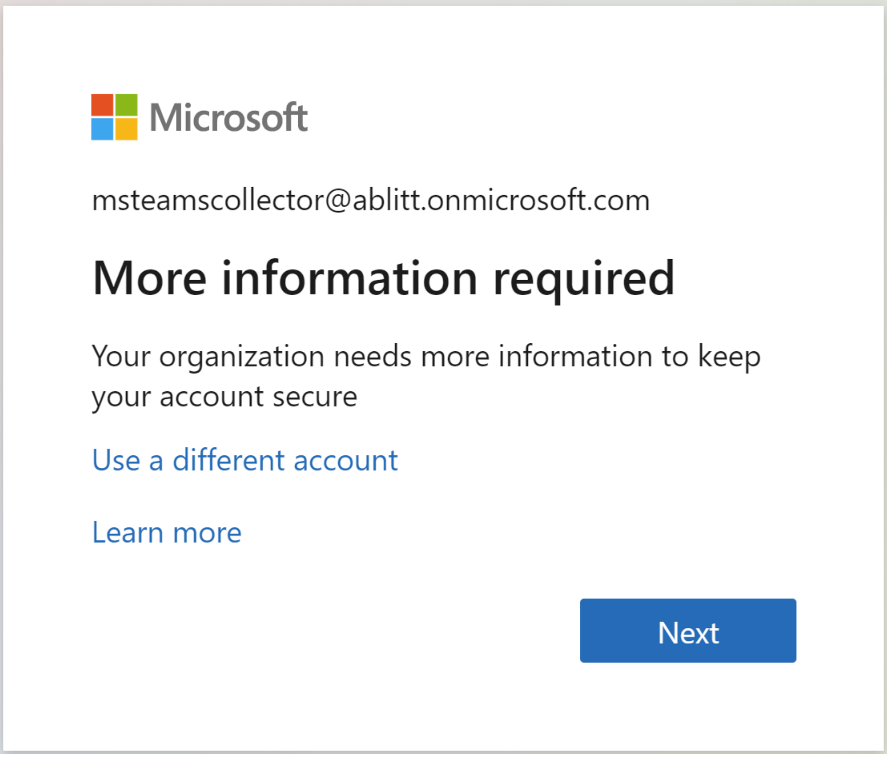
Update your password

You need to update your password because this is the first time you are signing in, or because your password has expired.

Current password

New password

Confirm password



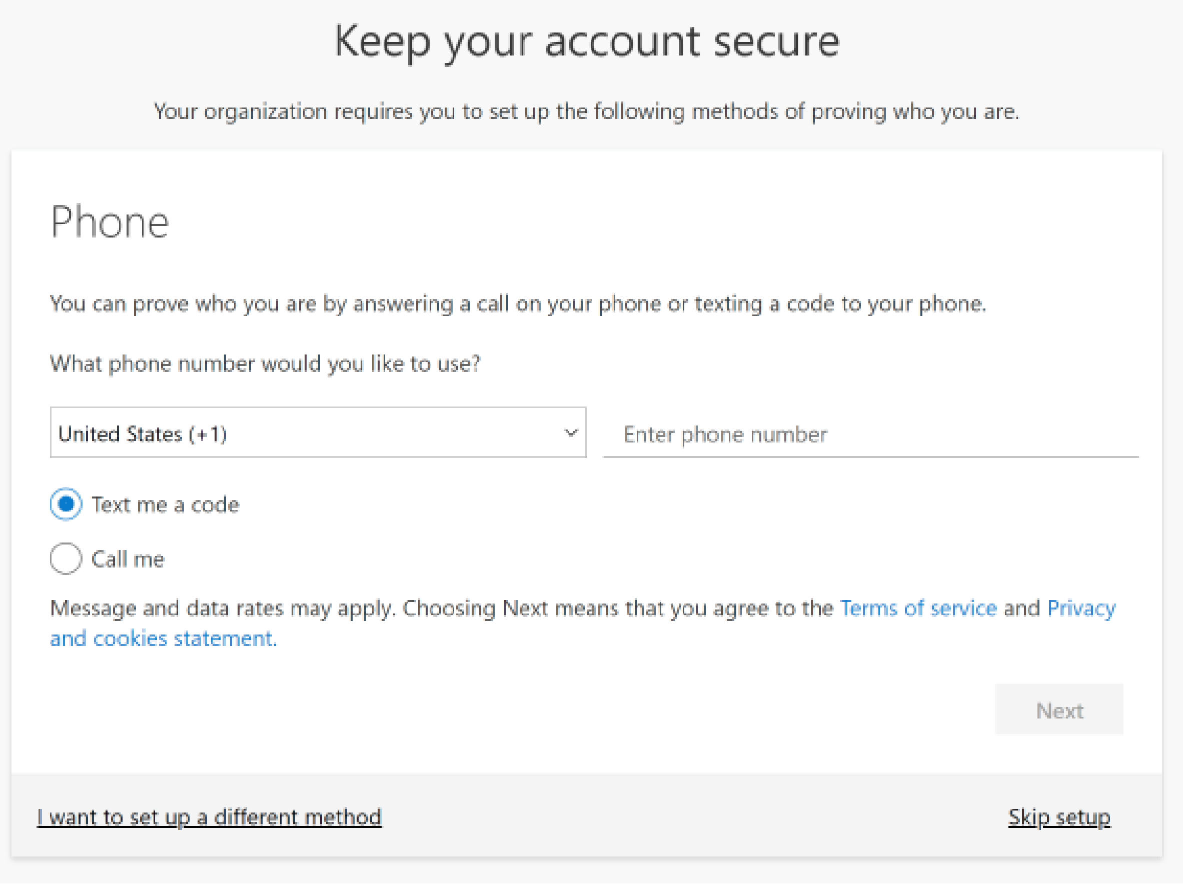
Microsoft

msteamscollector@ablitt.onmicrosoft.com

More information required

Your organization needs more information to keep your account secure

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



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

You can prove who you are by answering a call on your phone or texting a code to your phone.

What phone number would you like to use?

United States (+1)

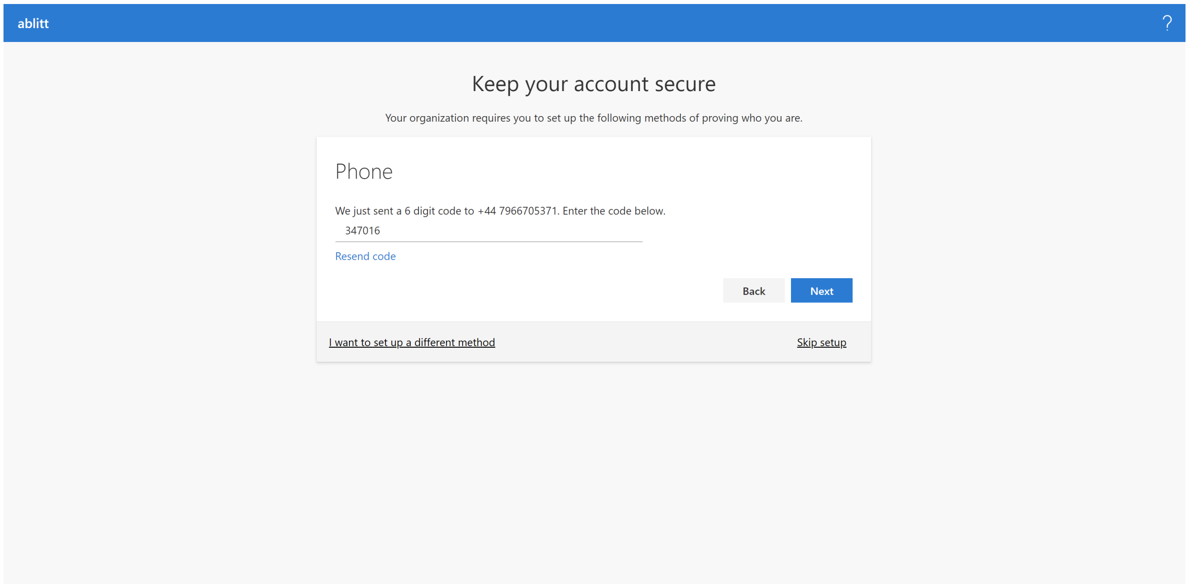
Enter phone number

● Text me a code

○ Call me

Message and data rates may apply. Choosing Next means that you agree to the Terms of service and Privacy and cookies statement.

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



Keep your account secure

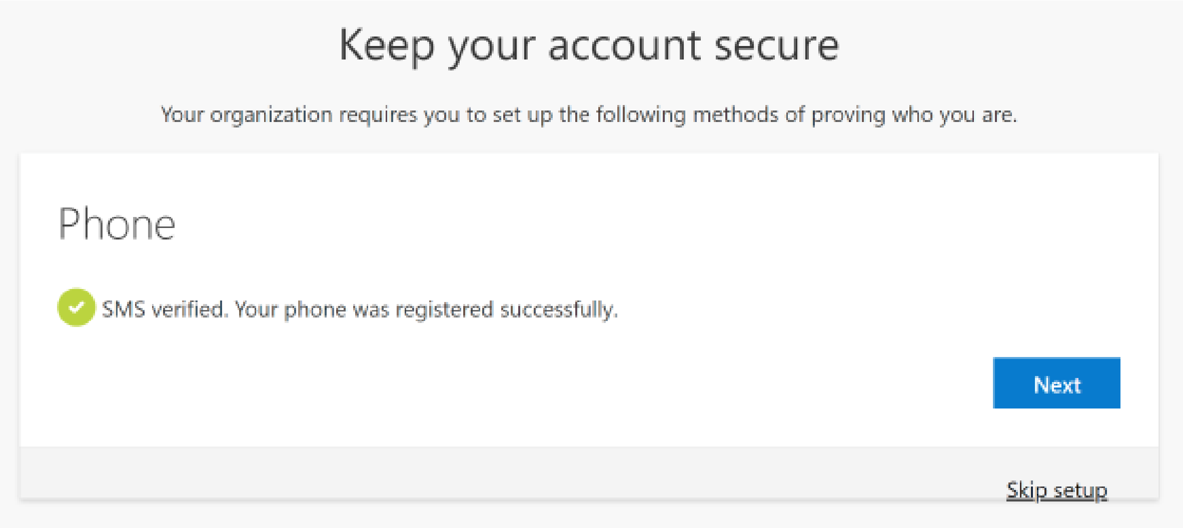
Your organization requires you to set up the following methods of proving who you are.

Phone

We just sent a 6 digit code to +44 7966705371. Enter the code below.

347016

Next



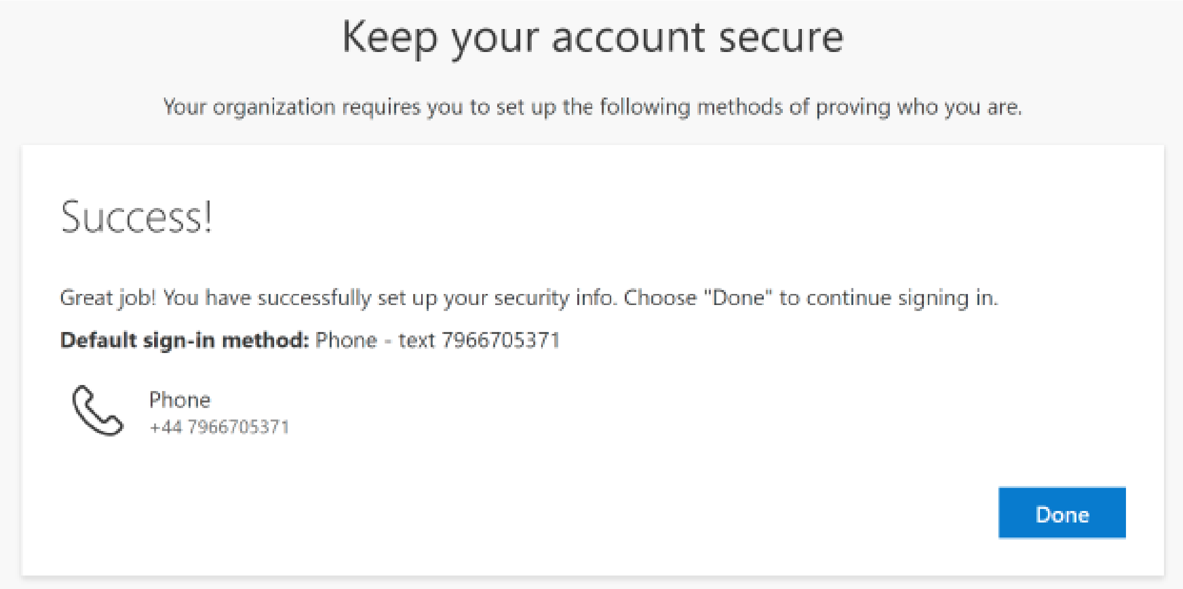
Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Phone

✓ SMS verified. Your phone was registered successfully.

Next



Keep your account secure

Your organization requires you to set up the following methods of proving who you are.

Success!

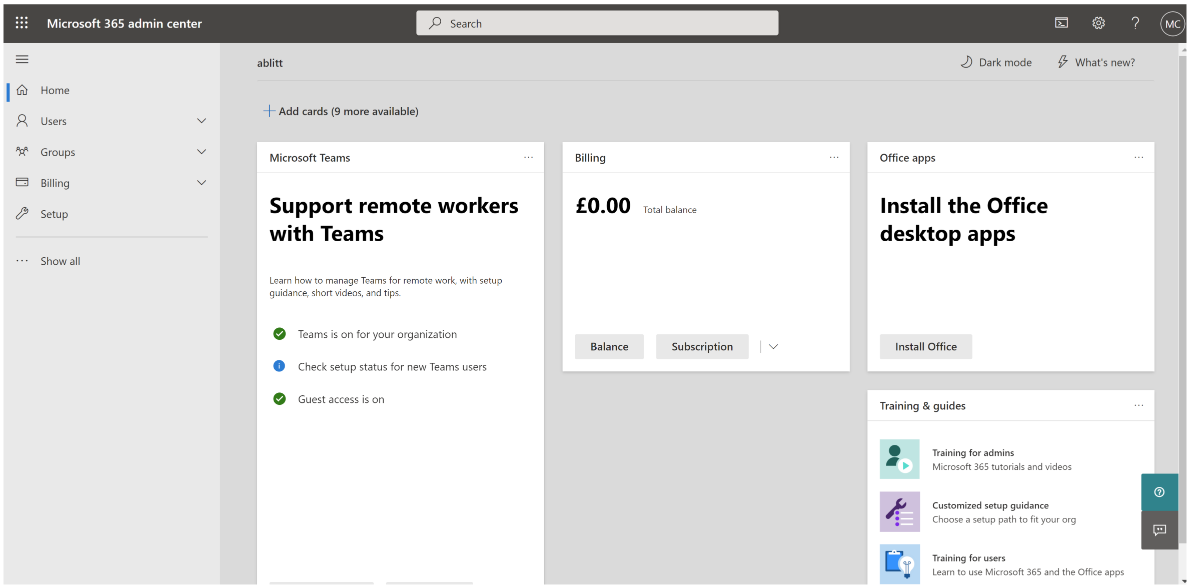
Great job! You have successfully set up your security info. Choose "Done" to continue signing in.

Default sign-in method: Phone - text 7966705371

Phone
+44 7966705371

Done

9. Successfully logged in



Support remote workers with Teams

Learn how to manage Teams for remote work, with setup guidance, short videos, and tips.

- Teams is on for your organization
- Check setup status for new Teams users
- Guest access is on

£0.00 Total balance

Install the Office desktop apps

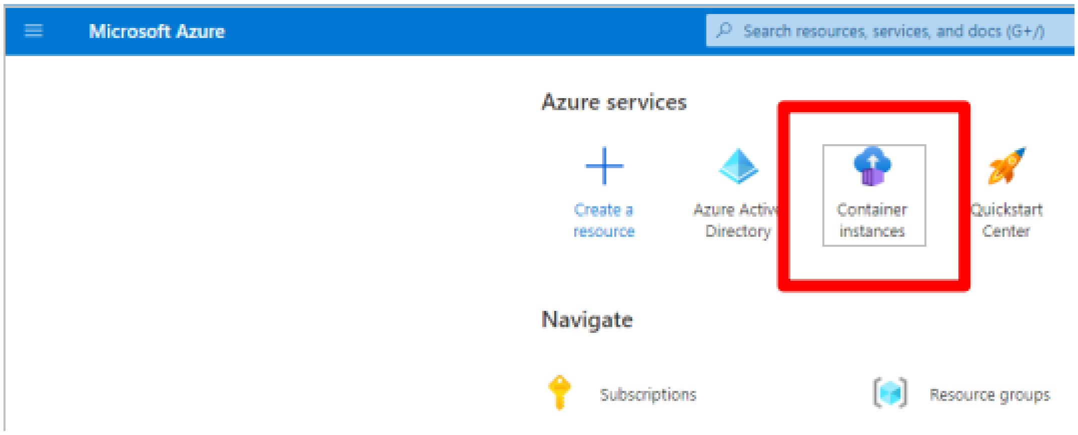
Training for admins
Microsoft 365 tutorials and videos

Customized setup guidance
Choose a setup path to fit your org

Training for users
Learn to use Microsoft 365 and the Office apps

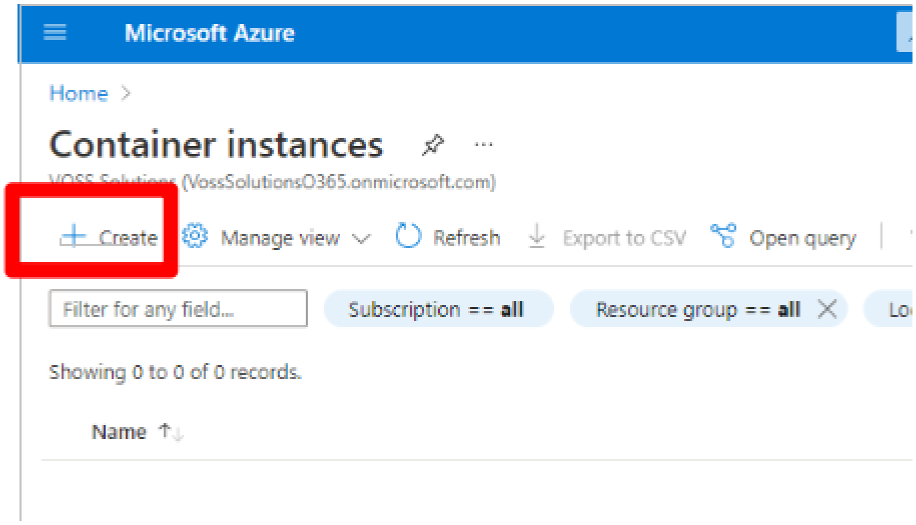
12. Build the Azure Collector using the Azure GUI

1. Log in to portal.azure.com.
2. Click on the icon **Container Instances**.



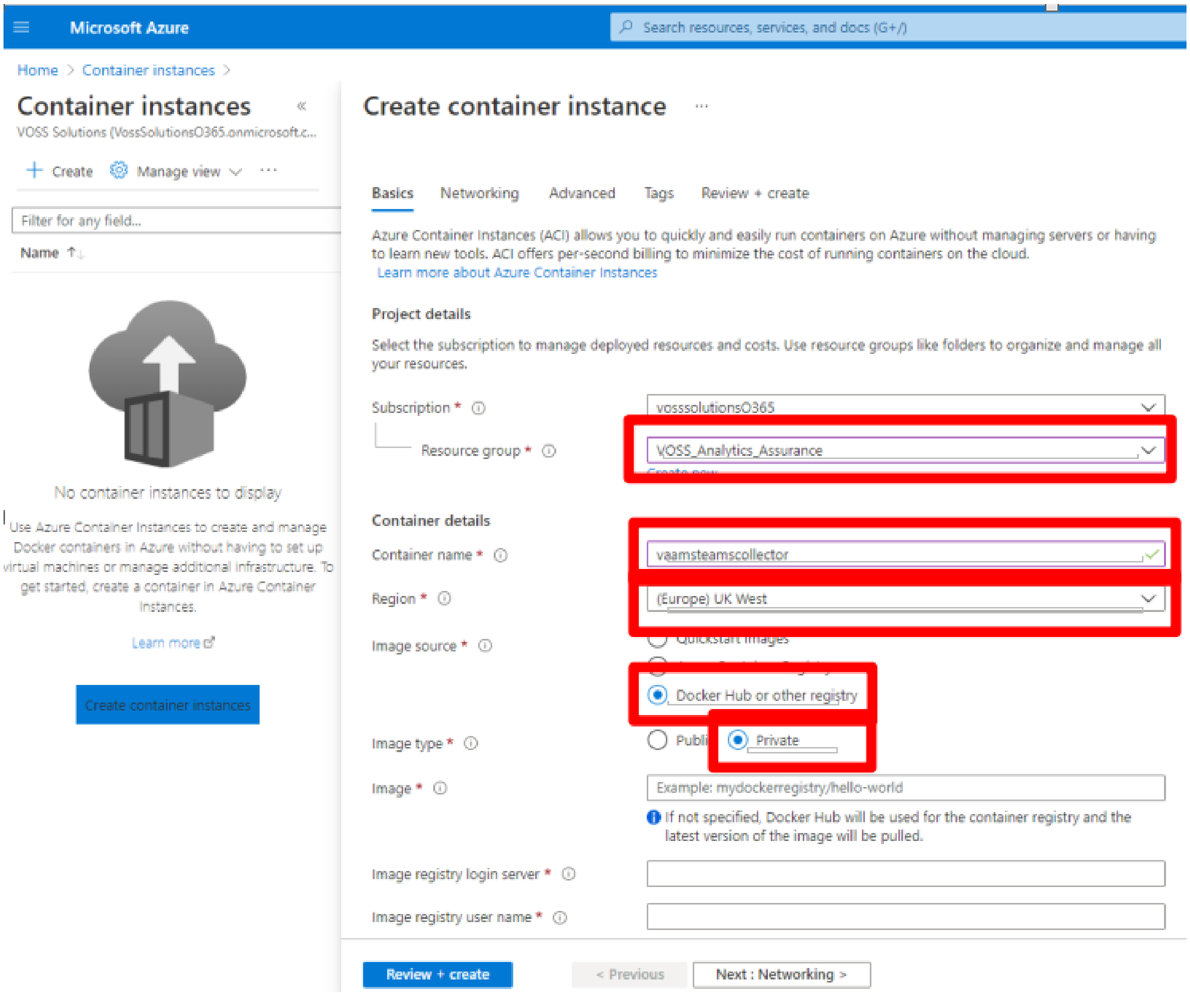
Note: First time users may have to enter payment details to cover the Azure running costs.

3. Click the **Create** button.



4. Fill out the following details:
   - **Resource group**: customer specific

- **Container name**: example msteams collector
- **Region**: needs to match global reader user
- **Image source**: docker hub or other registry



No container instances to display

Use Azure Container Instances to create and manage Docker containers in Azure without having to set up virtual machines or manage additional infrastructure. To get started, create a container in Azure Container Instances.

Create container instance

Azure Container Instances (ACI) allows you to quickly and easily run containers on Azure without managing servers or having to learn new tools. ACI offers per-second billing to minimize the cost of running containers on the cloud.
Learn more about Azure Container Instances

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *: vosssolutionsO365

Resource group *: VOSS_Analytics_Assurance

Create new

Container details

Container name *: vaamsteamscollector

Region *: (Europe) UK West

Image source *: ○ Quickstart images ○ Azure Container Registry ● Docker Hub or other registry

Image type *: ○ Public ● Private

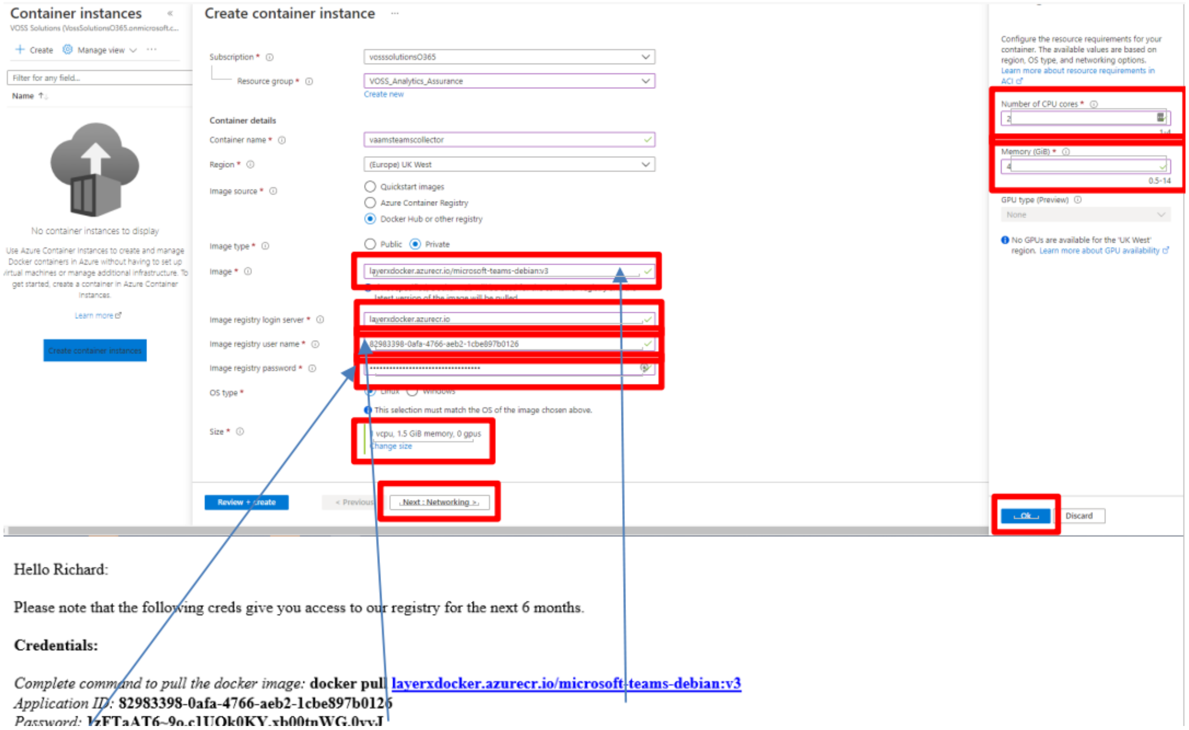
Image *: Example: mydockerregistry/hello-world

If not specified, Docker Hub will be used for the container registry and the latest version of the image will be pulled.

Image registry login server *

Image registry user name *

5. The following information comes from the first email that is sent



Container instances
VOSS Solutions (VossSolutionsO365.onmicrosoft.c...
+ Create
Manage view
Filter for any field...
Name
No container instances to display
Learn more
Create container instances
Create container instance
Review + create
< Previous
Next : Networking >
Ok
Discard

Use Azure Container Instances to create and manage Docker containers in Azure without having to set up virtual machines or manage additional infrastructure. To get started, create a container in Azure Container Instances.

Subscription *: vosssolutionsO365

Resource group *: VOSS_Analytics_Assurance

Container details

Container name *: vaamsteamscollector

Region *: (Europe) UK West

Image source *: ○ Quickstart images ○ Azure Container Registry ● Docker Hub or other registry

Image type *: ○ Public ● Private

Image *: layerxdocker.azurecr.io/microsoft-teams-debian:v3

Image registry login server *: layerxdocker.azurecr.io

Image registry user name *: 82983398-0afa-4766-aeb2-1cbe897b0126

Image registry password *: ••••••••••••••••••••••••••••••••••

OS type *: ● Linux ○ Windows

This selection must match the OS of the image chosen above.

Size *: 1 vcpu, 1.5 GiB memory, 0 gpus

Configure the resource requirements for your container. The available values are based on region, OS type, and networking options. Learn more about resource requirements in ACI

Number of CPU cores *: 2 (1-4)

Memory (GiB) *: 4 (0.5-14)

GPU type (Preview): None

No GPUs are available for the 'UK West' region. Learn more about GPU availability

Hello Richard:

Please note that the following creds give you access to our registry for the next 6 months.

Credentials:

Complete command to pull the docker image: **docker pull layerxdocker.azurecr.io/microsoft-teams-debian:v3**
Application ID: **82983398-0afa-4766-aeb2-1cbe897b0126**
Password: **lzFTaAT6~9o.c1UQk0KY.xb00tnWG.0vyJ**

- **Image**: layerxdocker.azurecr.io/microsoft-teams-debian:v3
- **Image registry login server**: layerxdocker.azurecr.io
- **Image registry user name**: application ID from email
- **Image registry password**: password from email

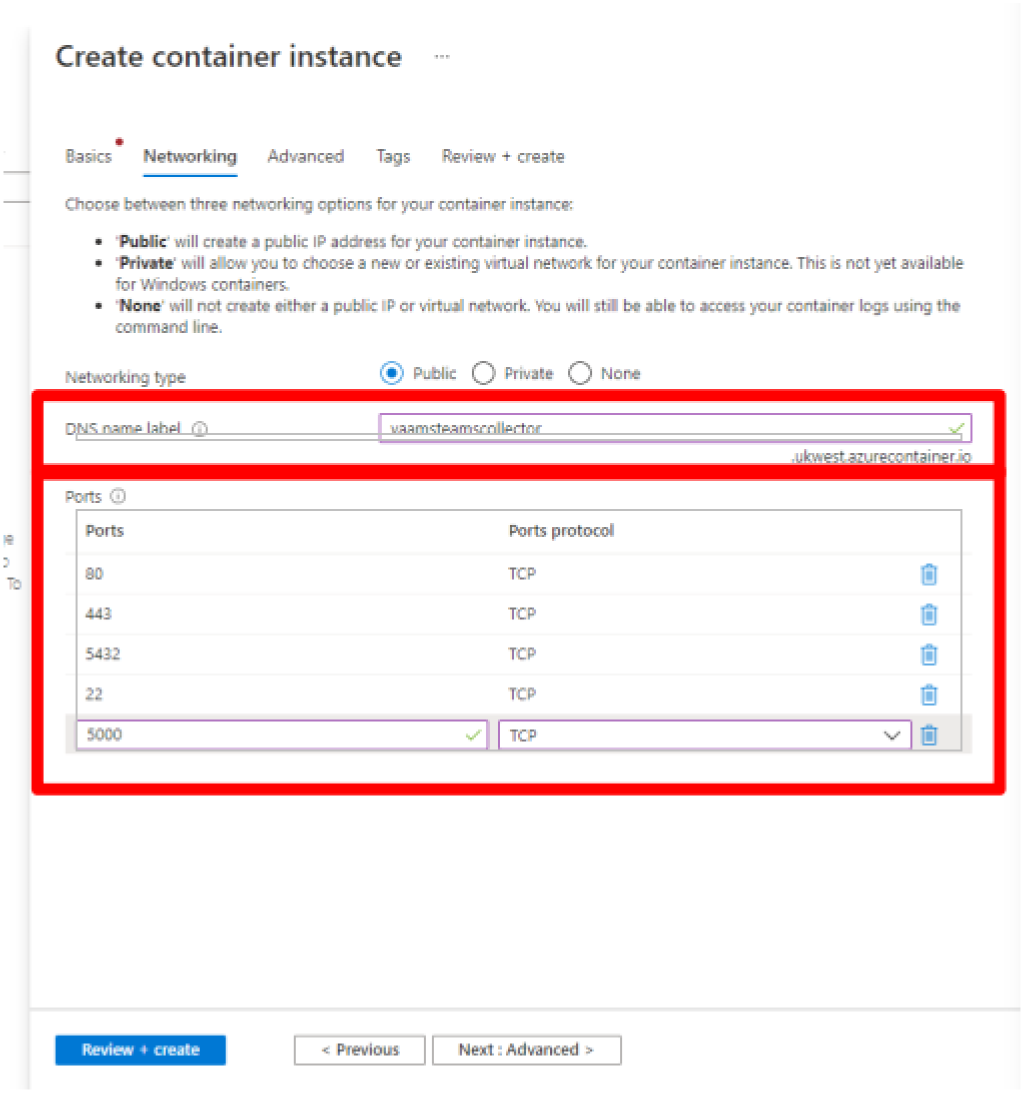
Change size of container:

- **Number of CPU cores**: 2
- **Memory (GiB)**: 4

Click **OK** to change the container size

5. Click **Review + create** to build standard
6. Click **Next : Networking**

Note: It is the customer's responsibility to define their network, business policies and implementation. The following section acts as knowledge sharing.



Create container instance ...

Choose between three networking options for your container instance:

- '**Public**' will create a public IP address for your container instance.
- '**Private**' will allow you to choose a new or existing virtual network for your container instance. This is not yet available for Windows containers.
- '**None**' will not create either a public IP or virtual network. You will still be able to access your container logs using the command line.

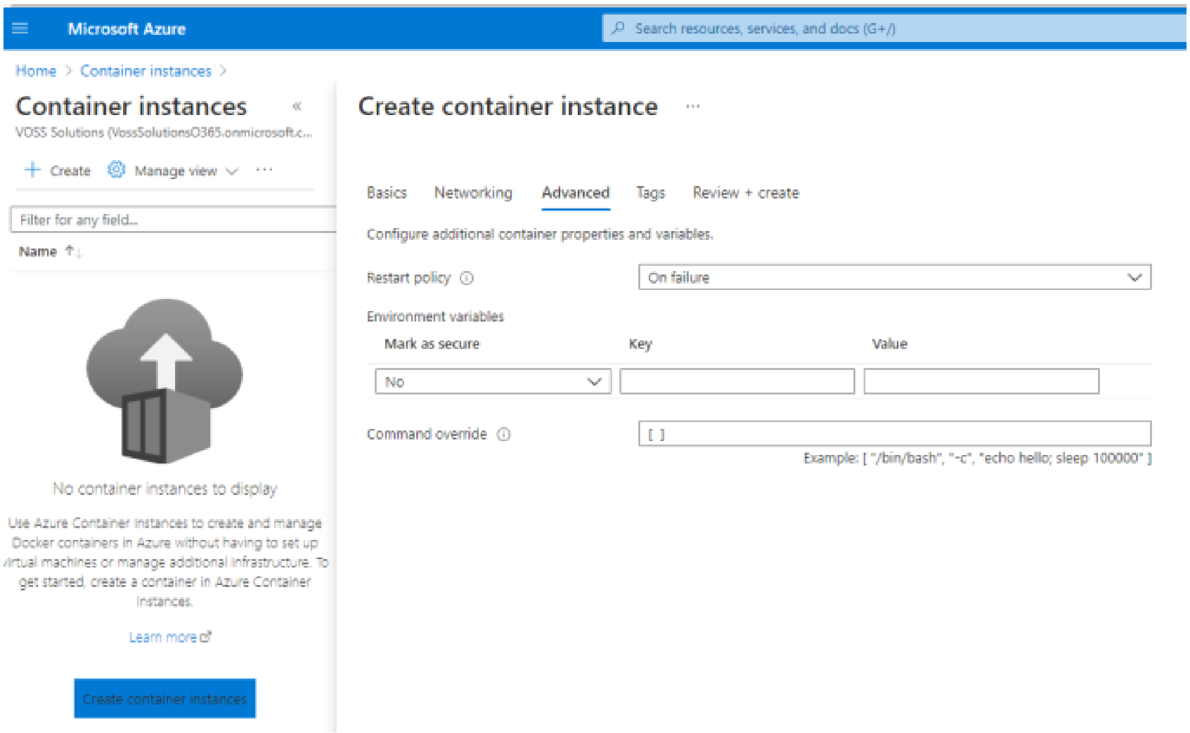
Networking type ● Public ○ Private ○ None

DNS name label ⓘ vaamsteamscollector ✓ .ukwest.azurecontainer.io

Ports ⓘ

Ports	Ports protocol
80	TCP
443	TCP
5432	TCP
22	TCP
5000	TCP

7. **Advanced**: Customer specific requirement


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Container instances >
Container instances
VOSS Solutions (VossSolutionsO365.onmicrosoft.c...
Create
Manage view
Filter for any field...
Name
No container instances to display
Use Azure Container Instances to create and manage Docker containers in Azure without having to set up virtual machines or manage additional infrastructure. To get started, create a container in Azure Container Instances.
Learn more
Create container instances
Create container instance
Basics
Networking
Advanced
Tags
Review + create

Configure additional container properties and variables.

Restart policy: On failure

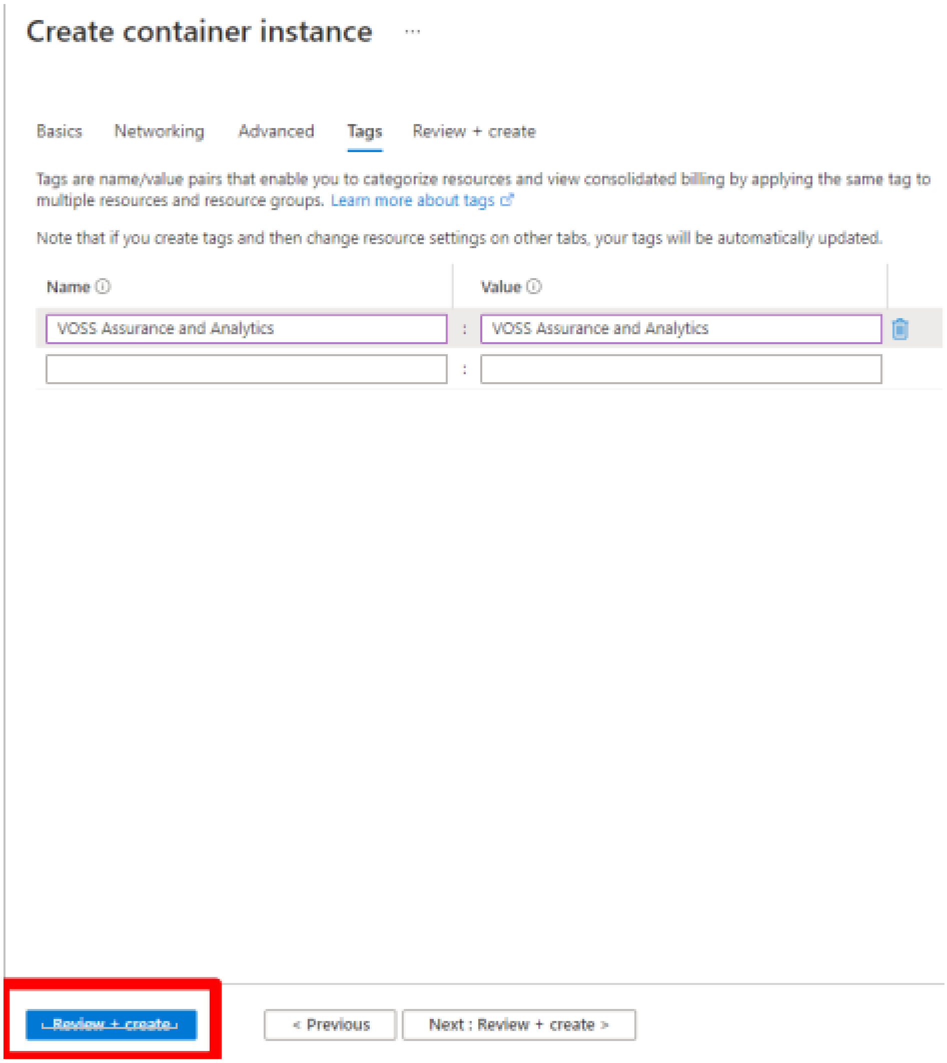
Environment variables

Mark as secure	Key	Value
No		

Command override: [ ]

Example: ["/bin/bash", "-c", "echo hello; sleep 100000"]

8. **Tags**: Add a tag if you require



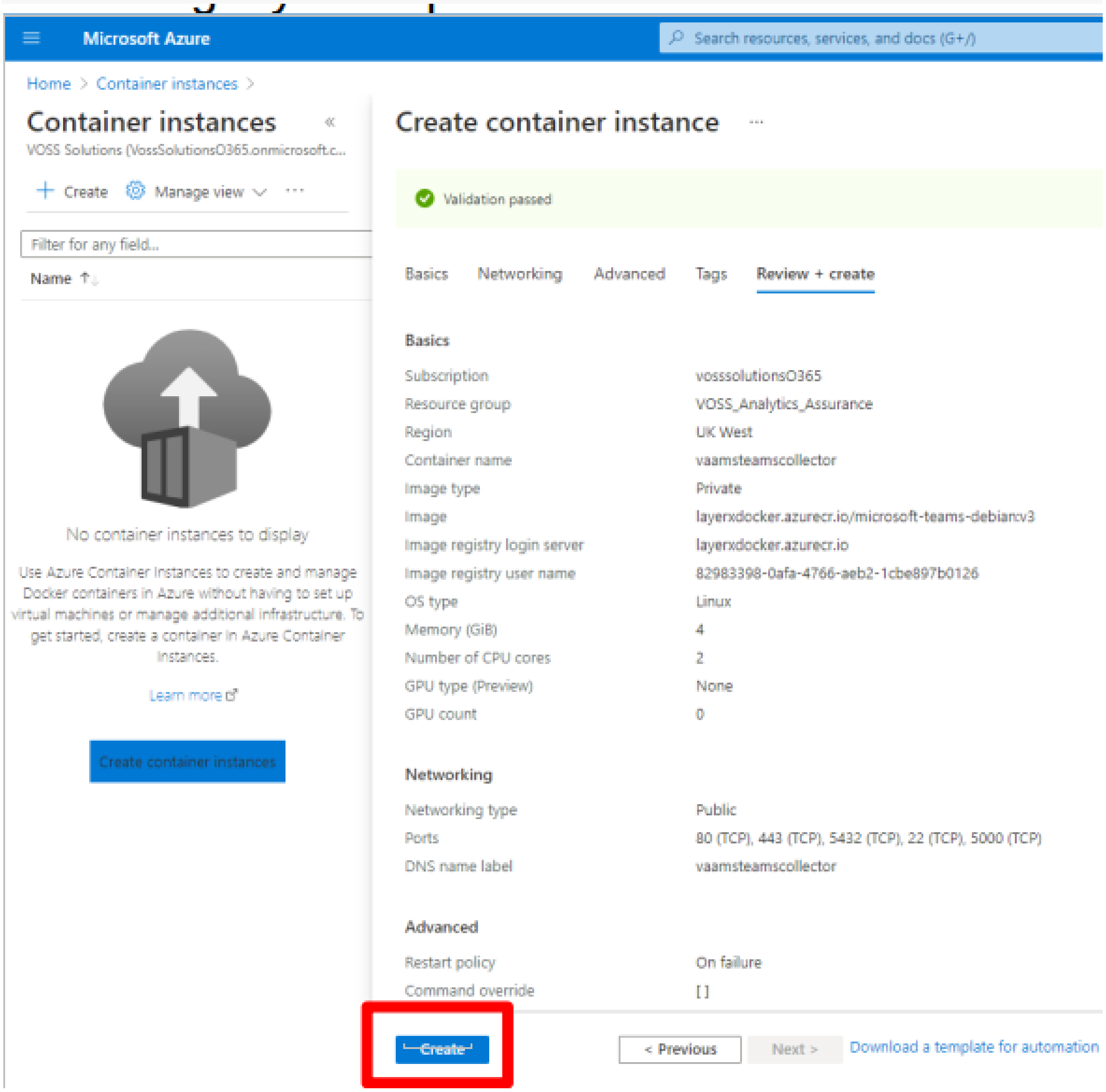
Create container instance ···

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ		Value ⓘ
VOSS Assurance and Analytics	:	VOSS Assurance and Analytics
	:	

9. **Review + create**



Microsoft Azure
Search resources, services, and docs (G+/)
Home > Container instances >
Container instances
VOSS Solutions (VossSolutionsO365.onmicrosoft.c...
+ Create
Manage view
Filter for any field...
Name ↑↓
No container instances to display
Use Azure Container Instances to create and manage Docker containers in Azure without having to set up virtual machines or manage additional infrastructure. To get started, create a container in Azure Container Instances.
Learn more
Create container instances
Create container instance
Validation passed
Basics
Networking
Advanced
Tags
Review + create
Create
< Previous
Next >
Download a template for automation

Basics

Subscription	vosssolutionsO365
Resource group	VOSS_Analytics_Assurance
Region	UK West
Container name	vaamsteamscollector
Image type	Private
Image	layerxdocker.azurecr.io/microsoft-teams-debian:v3
Image registry login server	layerxdocker.azurecr.io
Image registry user name	82983398-0afa-4766-aeb2-1cbe897b0126
OS type	Linux
Memory (GiB)	4
Number of CPU cores	2
GPU type (Preview)	None
GPU count	0

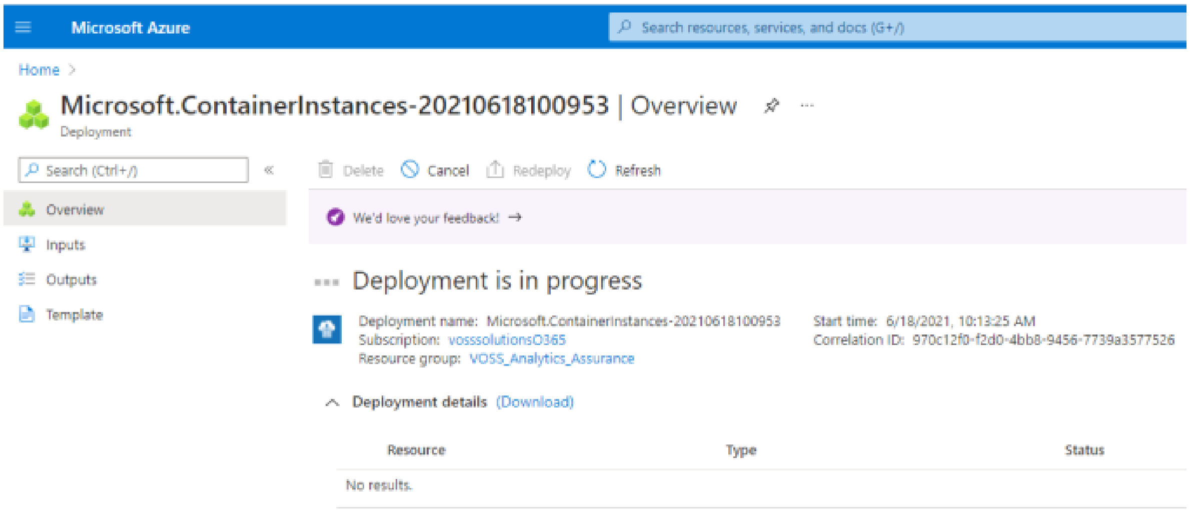
Networking

Networking type	Public
Ports	80 (TCP), 443 (TCP), 5432 (TCP), 22 (TCP), 5000 (TCP)
DNS name label	vaamsteamscollector

Advanced

Restart policy	On failure
Command override	[ ]

Click **Create**. Make sure the container deploys and causes no errors. It should take 2-3 minutes to deploy.


Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Microsoft.ContainerInstances-20210618100953 | Overview
Deployment
Search (Ctrl+/)
Delete
Cancel
Redeploy
Refresh
Overview
Inputs
Outputs
Template
We'd love your feedback! →

Deployment is in progress

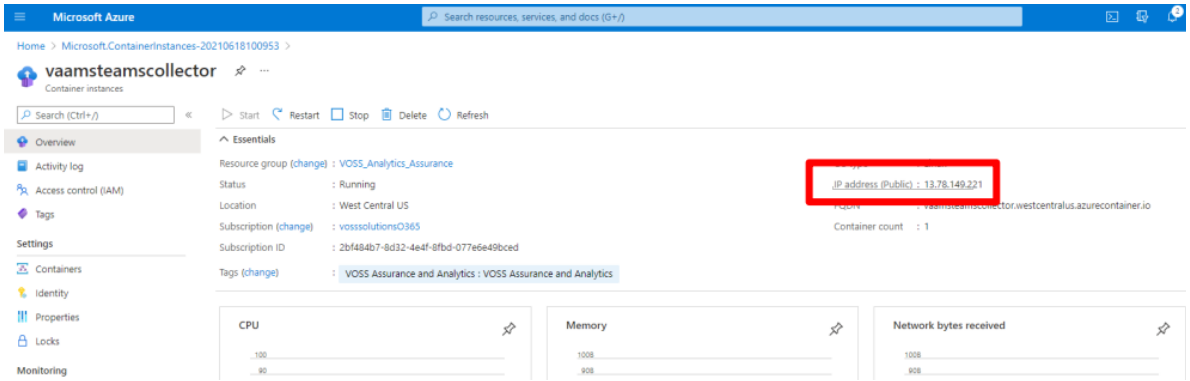
Deployment name: Microsoft.ContainerInstances-20210618100953
Subscription: vosssolutionsO365
Resource group: VOSS_Analytics_Assurance

Start time: 6/18/2021, 10:13:25 AM
Correlation ID: 970c12f0-f2d0-4bb8-9456-7739a3577526

Deployment details (Download)

Resource	Type	Status
No results.		

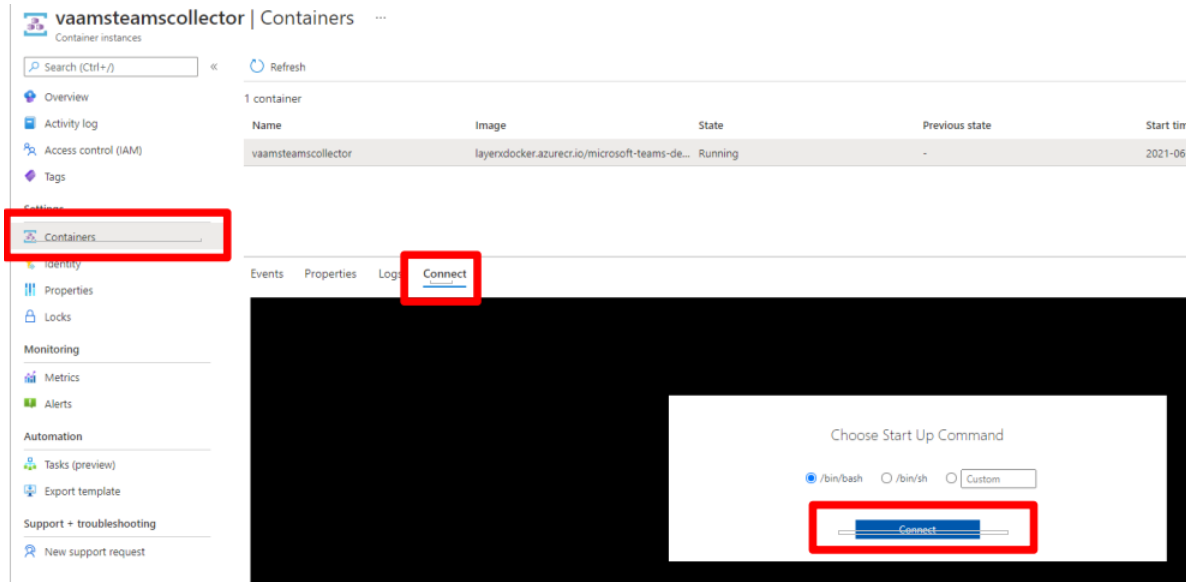
10. Take a note of the public IP (private if you done this as part of the customer security network setup).



Resource group (change) : VOSS_Analytics_Assurance
Status : Running
Location : West Central US
Subscription (change) : vosssolutionsO365
Subscription ID : 2bf484b7-8d32-4e4f-8fbd-077e6e49bced
Tags (change) : VOSS Assurance and Analytics : VOSS Assurance and Analytics

IP address (Public) : 13.78.149.221
FQDN : vaamsteamscollector.westcentralus.azurecontainer.io
Container count : 1

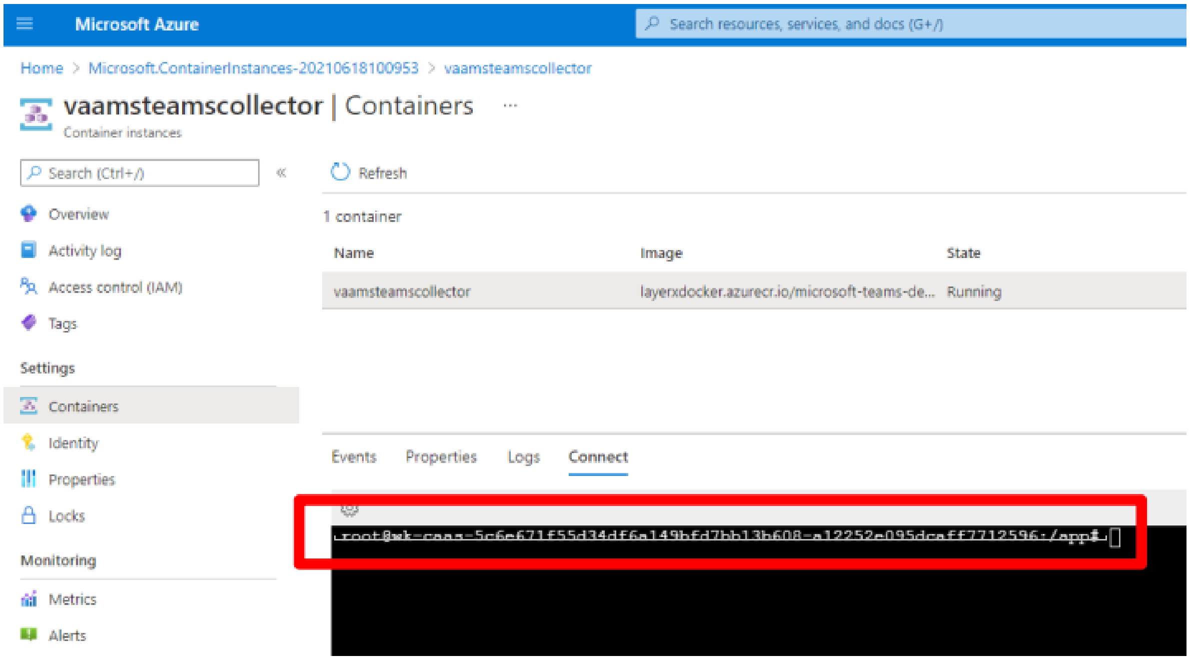
11. In the container instance that has been created, click **Containers** > **Connect** tab > **Connect** button.



1 container

Name	Image	State	Previous state	Start tim
vaamsteamscollector	layerxdocker.azurecr.io/microsoft-teams-de...	Running	-	2021-06

This displays the sandbox name which needs to be copied. This name is what the licensing server uses to associate the customer container with the user so they can log in to the GUI.



vaamsteamscollector | Containers

Container instances

1 container

Name	Image	State
vaamsteamscollector	layerxdocker.azurecr.io/microsoft-teams-de...	Running

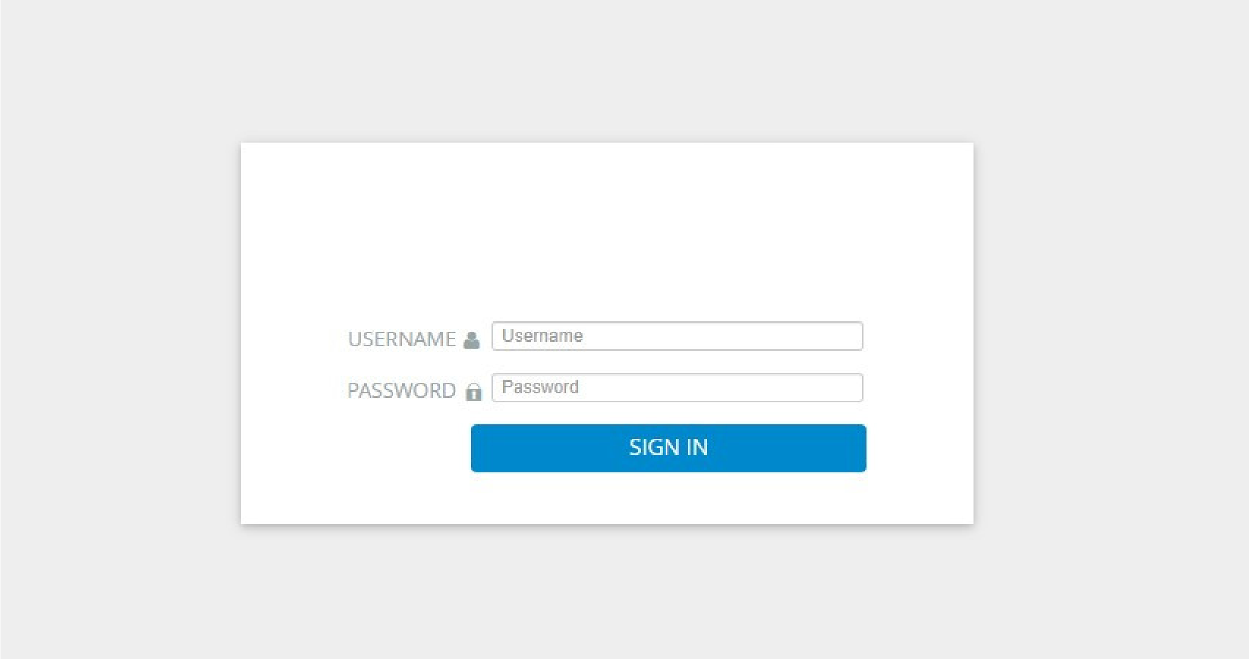
```
root@wk-caas-5c6e671f55d34df6a149bfd7bb13b608-a12252e095dcaff7712596:/app#
```

13. Check GUI Access

Before sending the email to get the container sandbox name associated with the user, it is best practice to log on to the GUI of the system to make sure there are no networking issues as these will need to be resolved before the setup can be completed.

Open up an internet browser and navigate to `https://<public or private ip>:5000`

Note: If it is a private network you may need to be on the corporate network to access the collector GUI.

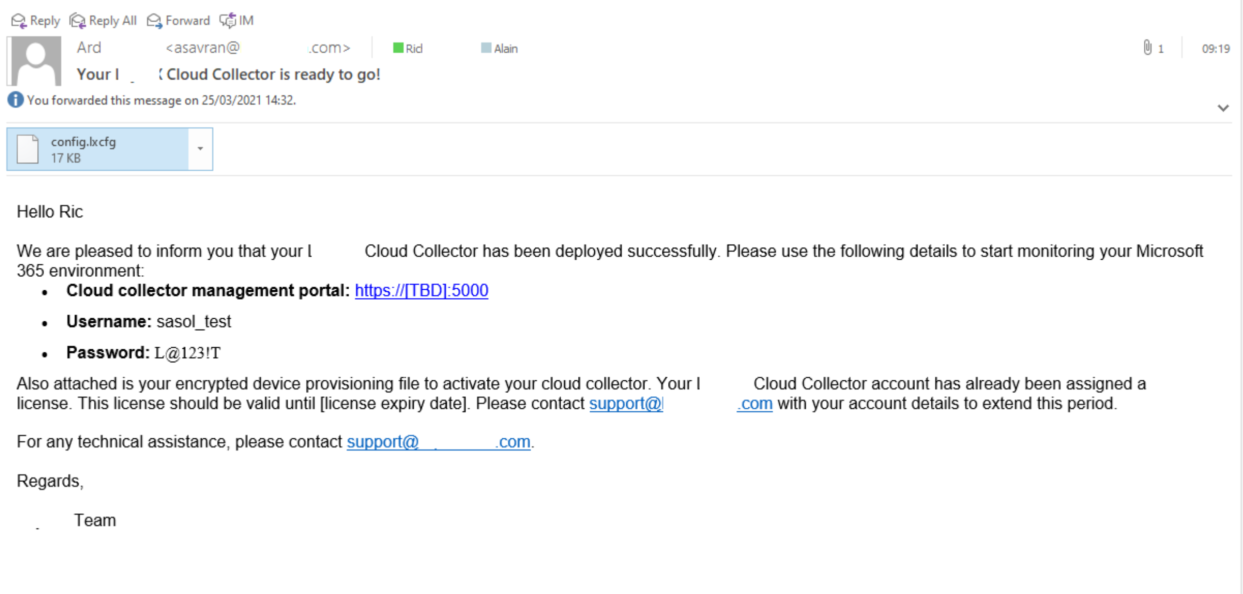


14. GUI login user email request

A VOSS engineer will need to send a email to support@voss-solutions.com with the following information

- Email address: support:voss-solutions.com
- Subject: User to be created for private docker registry
- Message body:
  - Customer name:
  - First name of customer:
  - Last Name of Customer:
  - Email address of customer:
  - Sandbox name:
  - Container name:

The following image is an example of information that will be sent back:



Ard <asavran@ .com>

Your I (Cloud Collector is ready to go!

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

config.lxcfg
17 KB

Hello Ric

We are pleased to inform you that your I 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
- **Username:** sasol_test
- **Password:** L@123!T

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

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

Regards,

Team

15. MS Teams Collector Configuration Steps

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

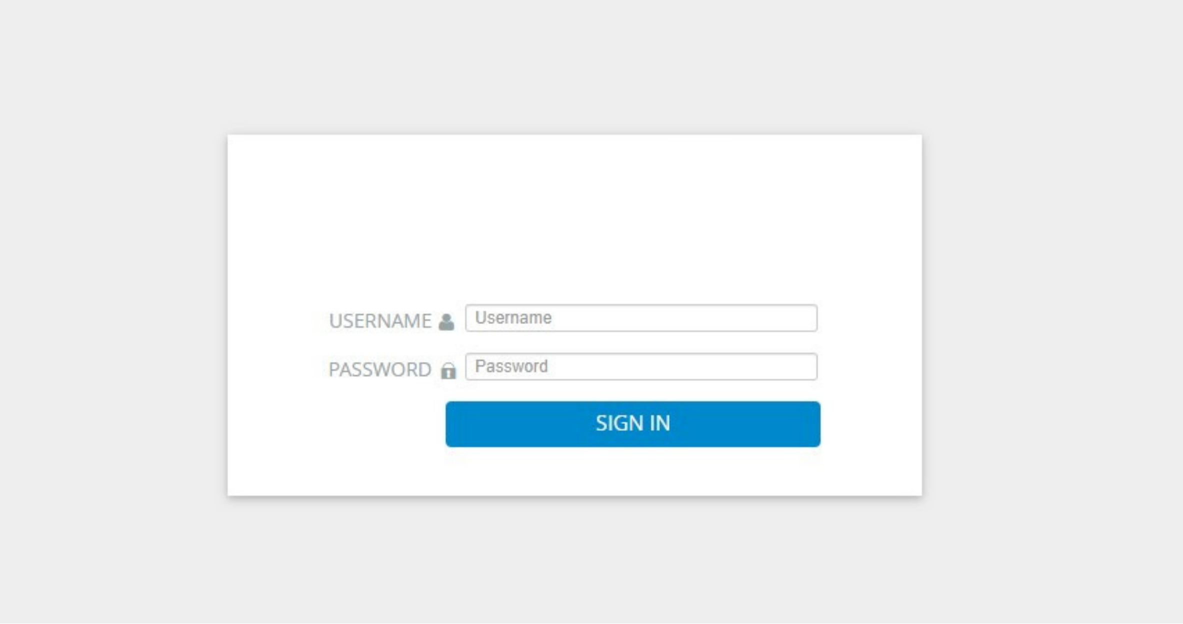


Figure 1 - VOSS Insights Agent login screen

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

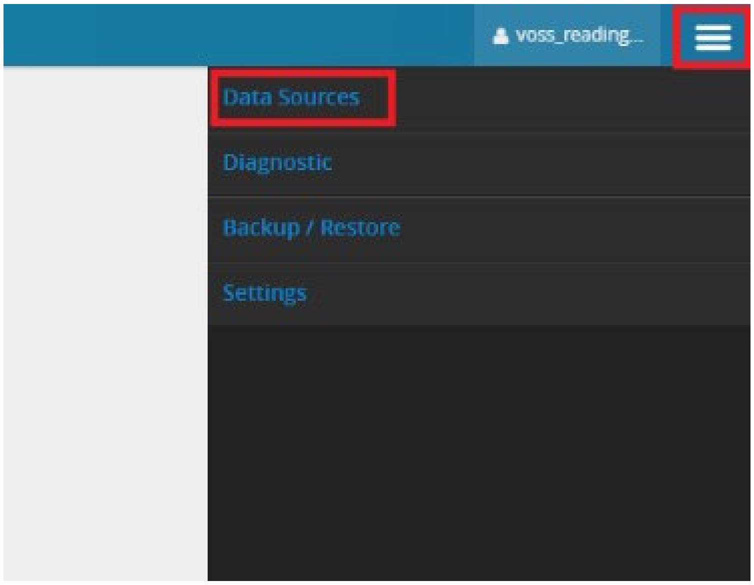
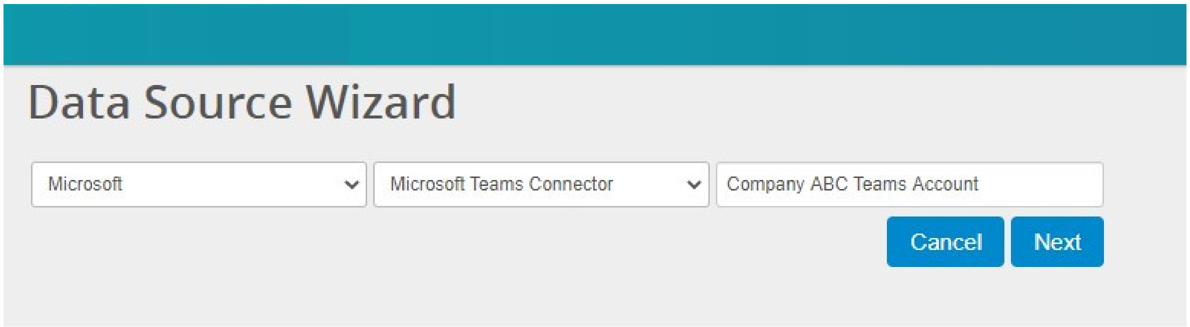


Figure 2 - VOSS Insights Agent data source configuration

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:



Microsoft

Microsoft Teams Connector

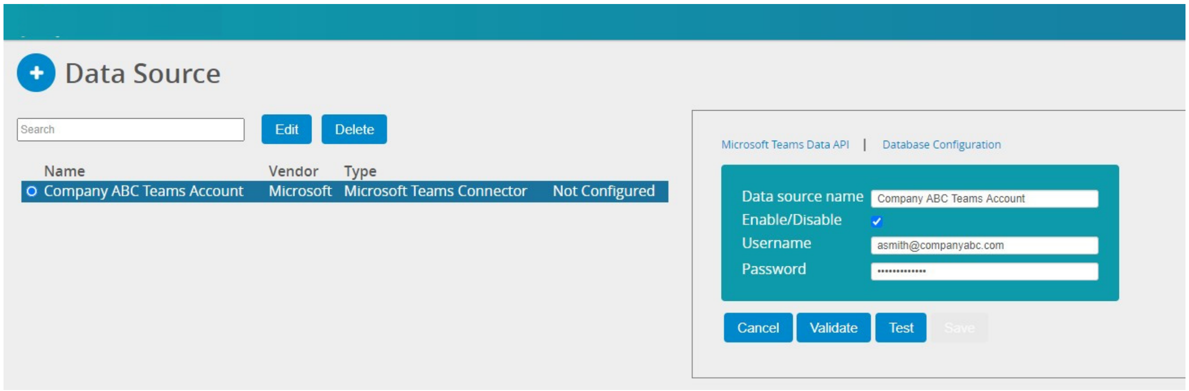
Company ABC Teams Account

Figure 3 - VOSS Insights 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.

   This information comes from the second email explained in *GUI login user email request*.



Name	Vendor	Type	
○ Company ABC Teams Account	Microsoft	Microsoft Teams Connector	Not Configured

Data source name	Company ABC Teams Account
Enable/Disable	☑
Username	asmith@companyabc.com
Password	•••••••••••••

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.

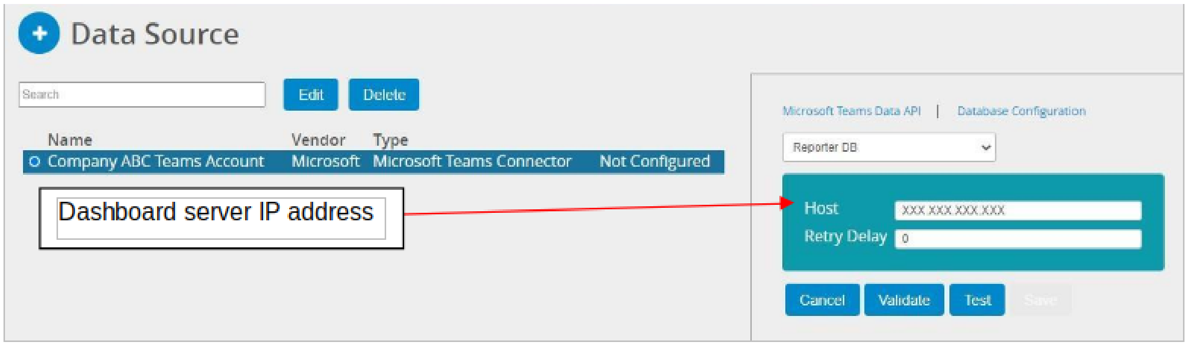
Note:

- 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 Insights Dashboard Server which will host your collected data.
11. From the drop-down menu, select "Reporter DB".
12. **Host**: enter the IP address for the VOSS Insights 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 Insights 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 through 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 Insights Dashboard Server.
16. Click on the **Save** button to finalize the database configuration.


Data Source
Search
Edit
Delete
Dashboard server IP address
Microsoft Teams Data API | Database Configuration
Cancel
Validate
Test
Save

Name	Vendor	Type	
○ Company ABC Teams Account	Microsoft	Microsoft Teams Connector	Not Configured

Reporter DB

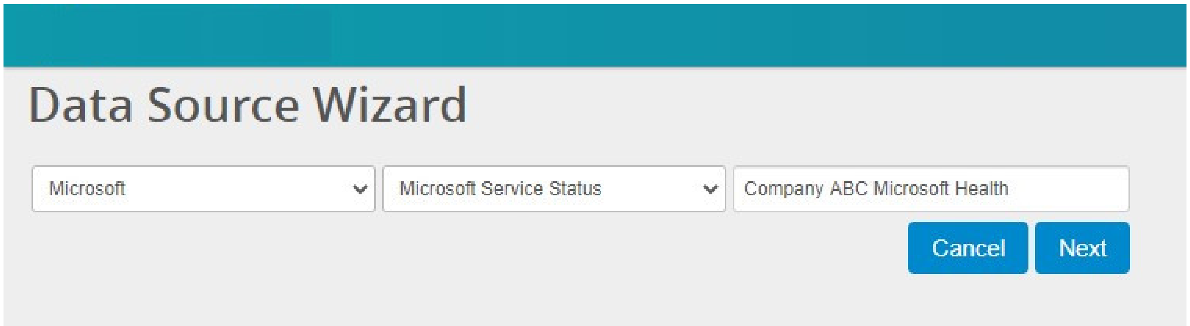
Host: xxx.xxx.xxx.xxx

Retry Delay: 0

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.

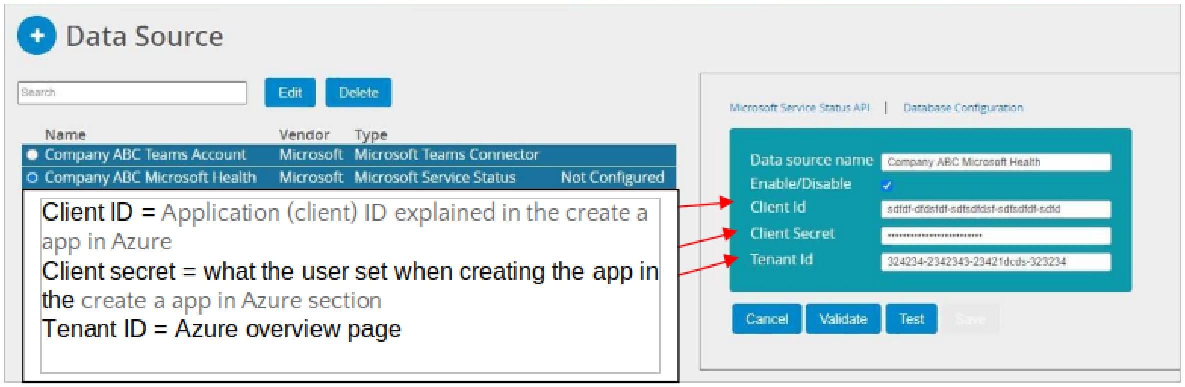
17. Click on the **+** sign next to **Data Source** on the top left corner again to create a new data source.
18. On the next screen, please choose the **vendor** and **type** as “Microsoft” and “Microsoft Teams Connector” respectively; give your data source a name, and click on the **Next** button:



Microsoft | Microsoft Service Status | Company ABC Microsoft Health

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.



Name	Vendor	Type	
● Company ABC Teams Account	Microsoft	Microsoft Teams Connector	
○ Company ABC Microsoft Health	Microsoft	Microsoft Service Status	Not Configured

Client ID = Application (client) ID explained in the create a app in Azure
Client secret = what the user set when creating the app in the create a app in Azure section
Tenant ID = Azure overview page

Data source name: Company ABC Microsoft Health
Enable/Disable: ☑
Client Id: sdfdf-dfdsfdf-sdfsdfdsf-sdfsdfdf-sdfd
Client Secret: ************************
Tenant Id: 324234-2342343-23421dcds-323234

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. **Host**: 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.

15.1. 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:

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

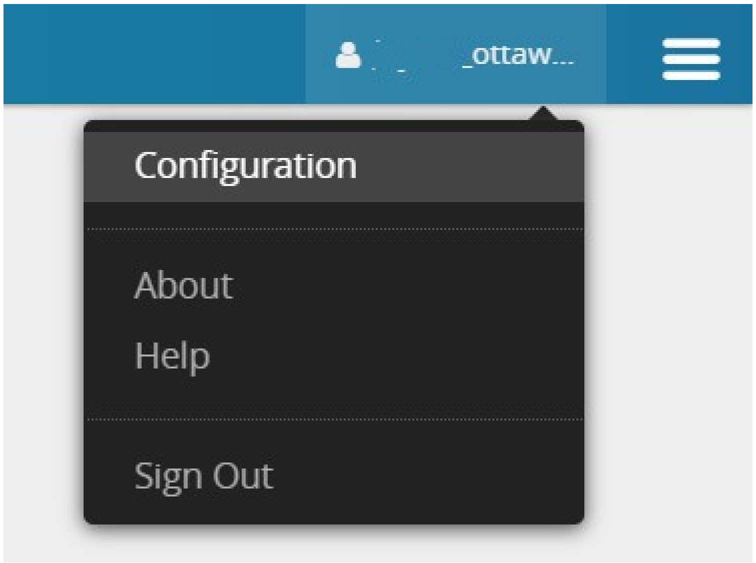


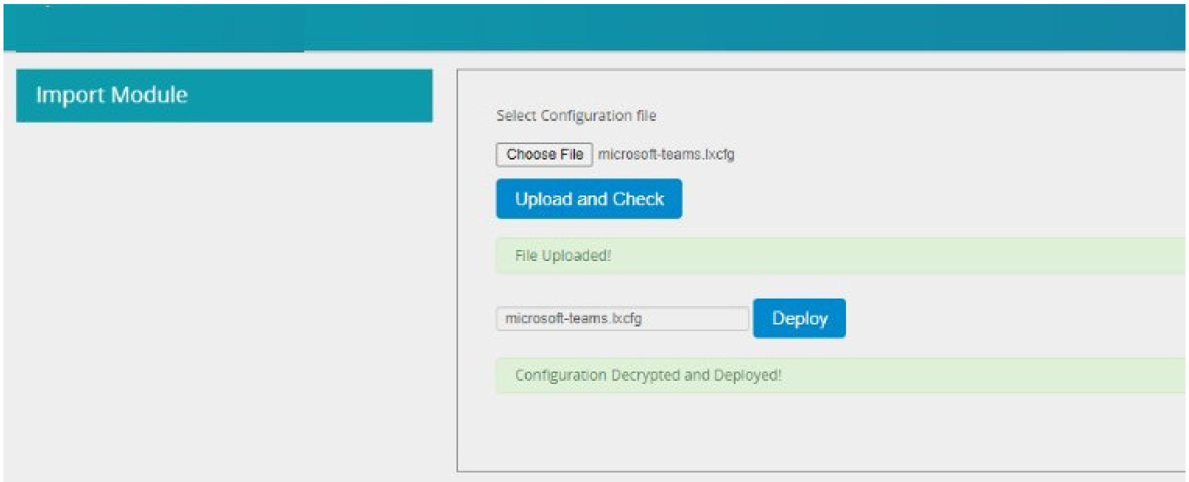
Figure 6 - VOSS Insights Agent import module

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:



Select Configuration file

microsoft-teams.lxcfg

File Uploaded!

microsoft-teams.lxcfg

Configuration Decrypted and Deployed!

Figure 7 - VOSS Insights 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.

We appreciate and value your comments. Email: doc-feedback@voss-solutions.com

16. 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.

16.1. 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.

16.2. 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.

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

Solutions:

- Contact VOSS support to verify any unexpected service issues.

16.4. 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.

17. Appendix

17.1. Issues

If the container is restarted, a new IP address is allocated. This could affect and network policies and rules between the MS Teams collector in Azure and the location of the Dashboard server. Consider making the IP address for the container static.

When creating the global reader account, it sets the expiry of the password to 2 years, so this will need to be updated on the MS Teams collector, otherwise the data collection will cease.

17.2. Prerequisites

- Build dashboard server and have the IP address available
- 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 Microsoft Admin.

  - VOSS Insights 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 Insights 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.

17.3. 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.

The email that was sent earlier in the process and the welcome email with log in details will be used to log in to the docker container registry to download the docker image.

On the users PC:

- Load Docker
- Load PowerShell

17.4. 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

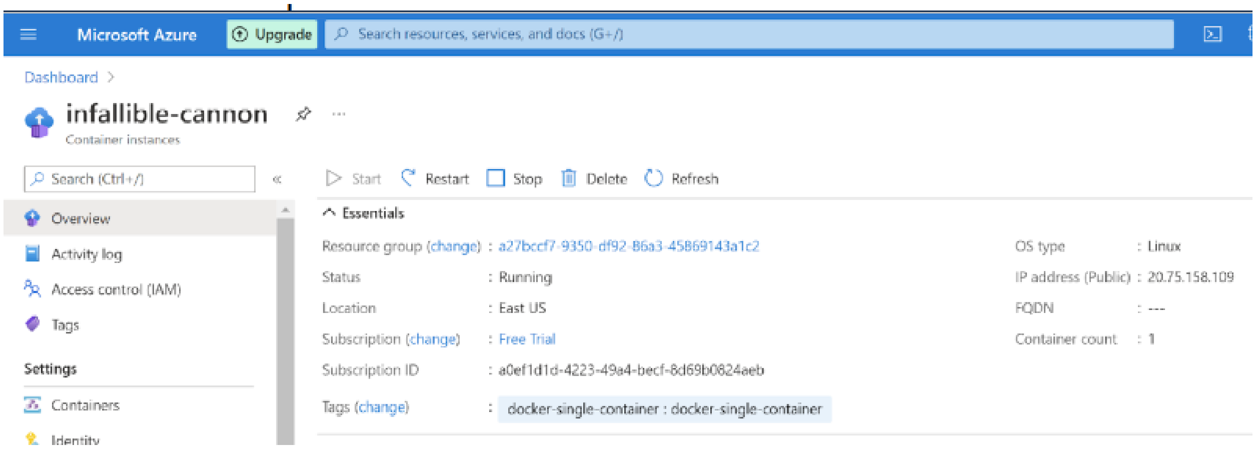
```
docker --context somename run -d --restart always --cpus 2 --memory 4G -p␣
↪5000:5000 layerxdocker.azurecr.io/microsoft-teams-debian:v3
```

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

Navigate to Azure: **Container Instances**.

Find container name created in PowerShell and select it.

Take note of the public IP:



infallible-cannon

Container instances

Resource group (change) : a27bccf7-9350-df92-86a3-45869143a1c2

Status : Running

Location : East US

Subscription (change) : Free Trial

Subscription ID : a0ef1d1d-4223-49a4-becf-8d69b0824aeb

Tags (change) : docker-single-container : docker-single-container

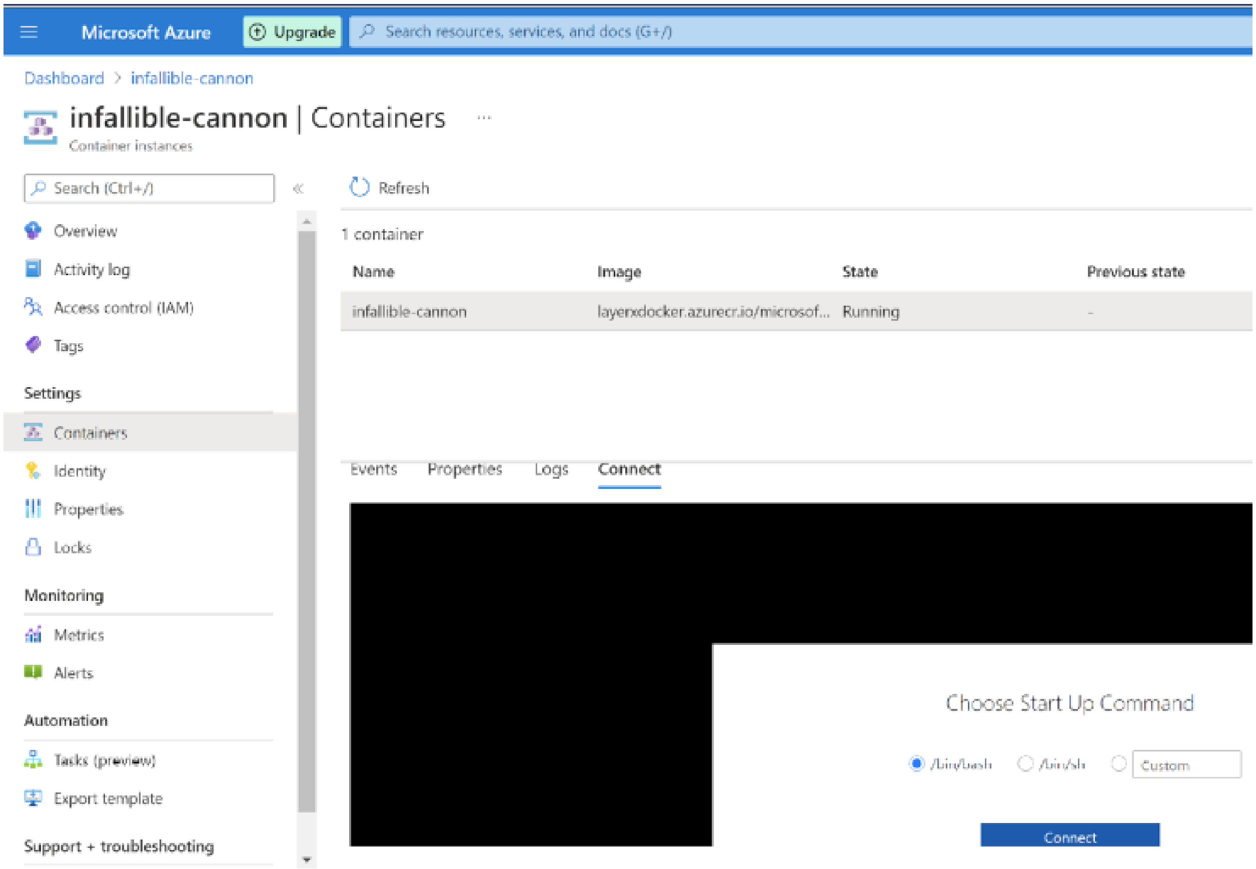
OS type : Linux

IP address (Public) : 20.75.158.109

FQDN : ---

Container count : 1

Container name > **Containers**.



infallible-cannon | Containers

Container instances

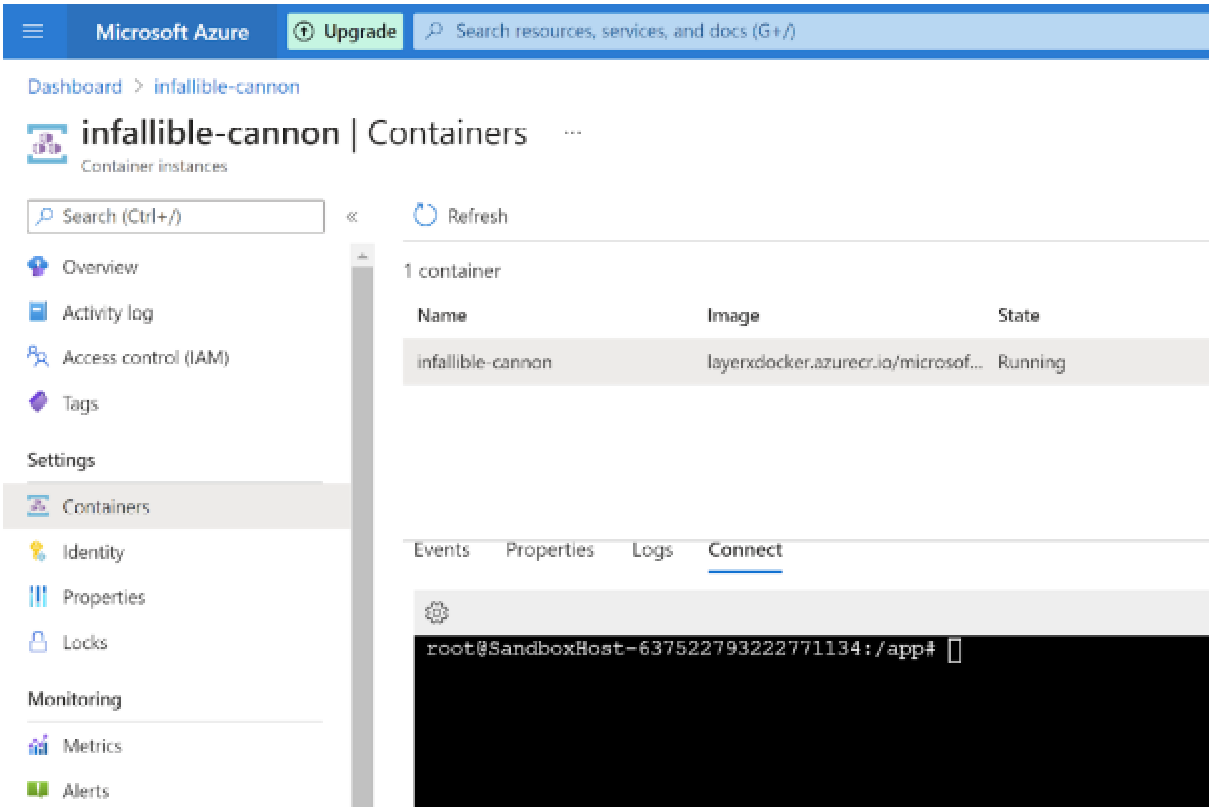
1 container

Name	Image	State	Previous state
infallible-cannon	layerxdocker.azurecr.io/microsof...	Running	-

Choose Start Up Command

● /bin/bash ○ /bin/sh ○ Custom

Click **Connect**.



1 container

Name	Image	State
infallible-cannon	layerxdocker.azurecr.io/microsof...	Running

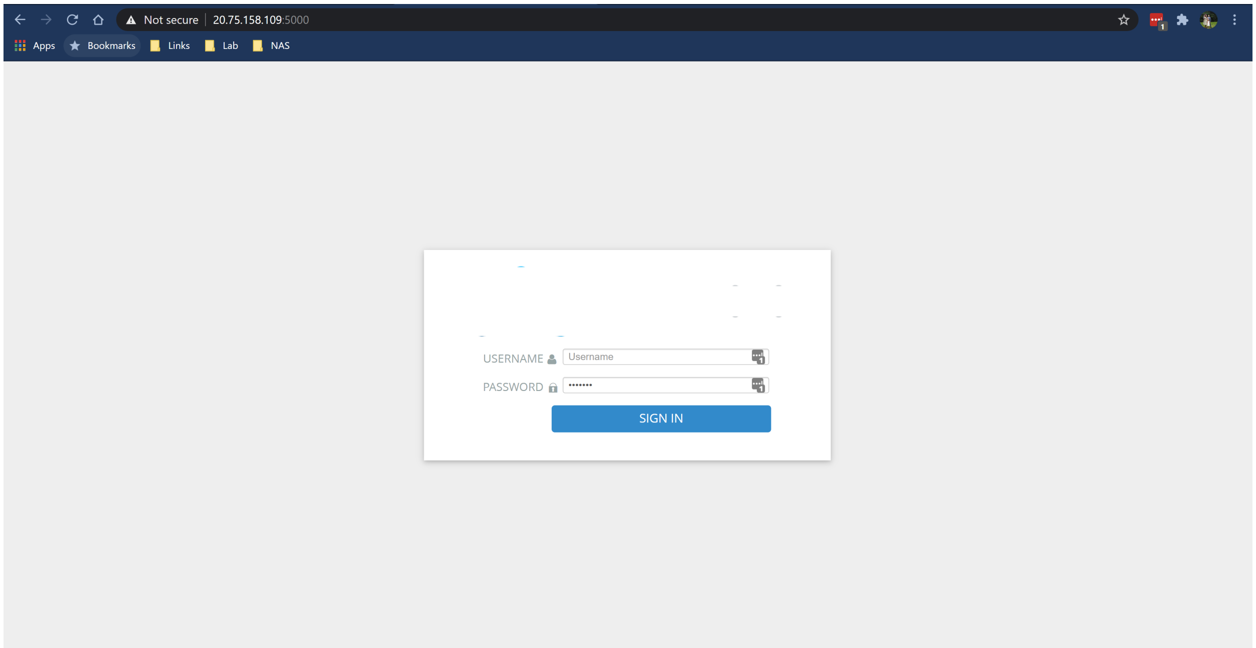
```
root@SandboxHost-637522793222771134:/app#
```

Take the sandbox name and email to VOSS to get a user created and associated for logging into the cloud collector GUI.

Open a New tab: `https://<container public IP>:5000`

Await the email for user details.

Log in to the GUI.



17.5. Notes

- PowerShell requires a Windows PC. MAC users can load docker and use the MAC command line
- PowerShell seems to store credentials for first docker build - need to clear for multi customers, or could be the list context names to see what could be used. Default is the default one but customers might have their own = docker context list

** DOCUMENT ID: 20220509193528