Microsoft Teams Integration Guide

Integration Guide

QMS 9.4

This document contains information about the configuration of Quality Management Suite for recording Teams calls via Compliance Recording.

Enghouse Interactive

Table of Contents

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

About This Document

Audience

This document is for the contact center system administrator who installs, configures, and integrates Microsoft Teams with Enghouse Interactive Quality Management Suite (QMS).

Reference materials

The content contained in this document works in combination with the information and procedures in the following documents or Help.

- Quality Management Suite System Design Guide
- Quality Management Suite Installation Guide
- Quality Management Suite High Availability Guide

Document conventions

This document uses the following text formats and notation conventions.

Text format

Bold text indicates a button, field, link, option name, or similar function requiring an action.

Italicized text indicates new terms, directory paths, or references to external documents.

Notes and cautions

Icons used throughout this document identify additional details or special conditions.

Note

Provides additional information or describes special circumstances.

Caution

Warns of user actions that may cause system failure or irreversible conditions.

Stop

Describes actions that you should only perform under the supervision of Enghouse Customer Support.

Contact information

For more information regarding Enghouse products, services, and support, please visit **www.enghouse.com**.

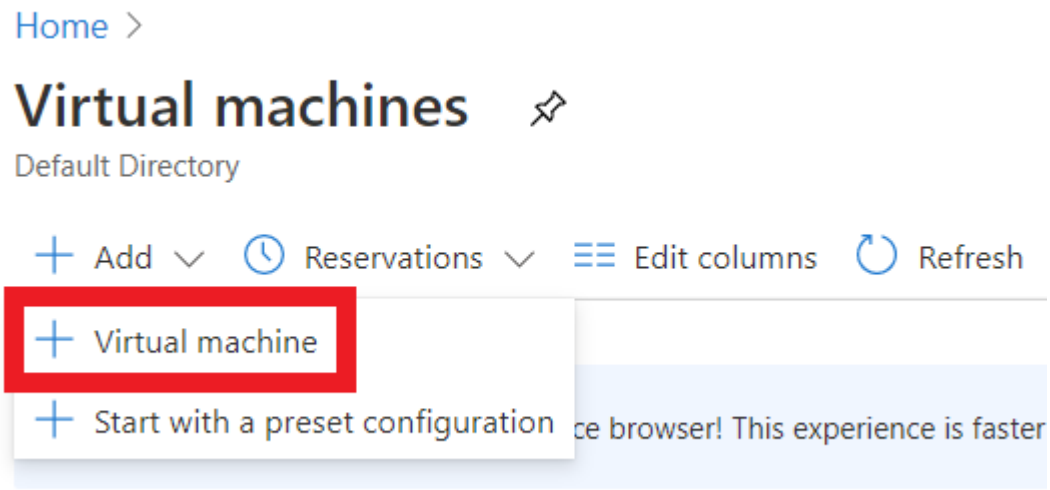
Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Create Azure VM

You will need to create a VM in Azure to host QMS, which contain the Teams Native Recording bot. The QMS Teams bot is part of the QMS Call Recording Service and is used when the PBX Type for the Call Recording Service is set to “Microsoft Teams Native Recording”.

First, browse to the Azure portal at https://portal.azure.com and login as a user that has permissions to create virtual machines. On the home screen click on Virtual Machines:

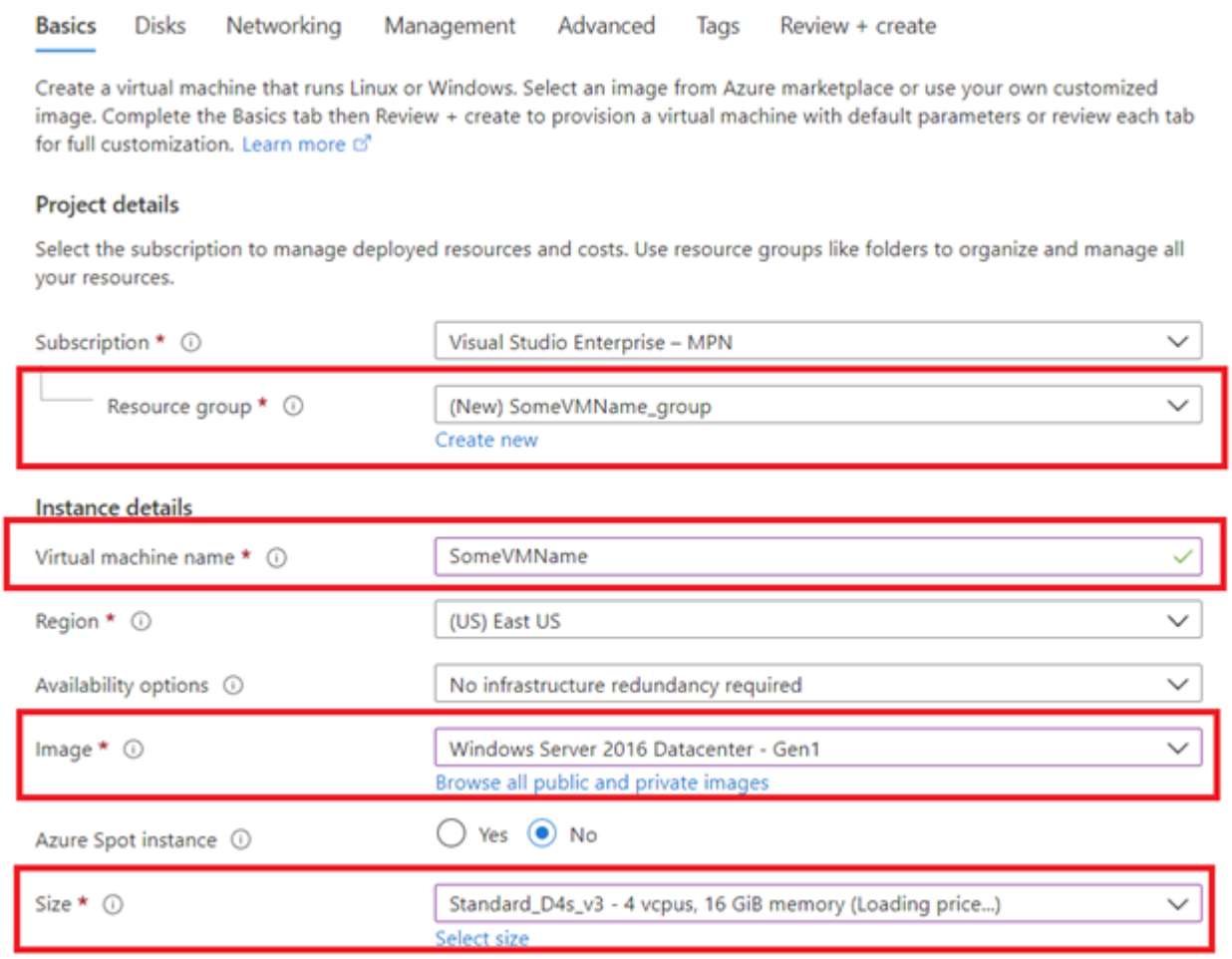
Next, click on “Add -> Virtual Machine”:



After clicking on Virtual Machine, the “Create a virtual machine” Basics page will open. On this page you will need to configure a few details:

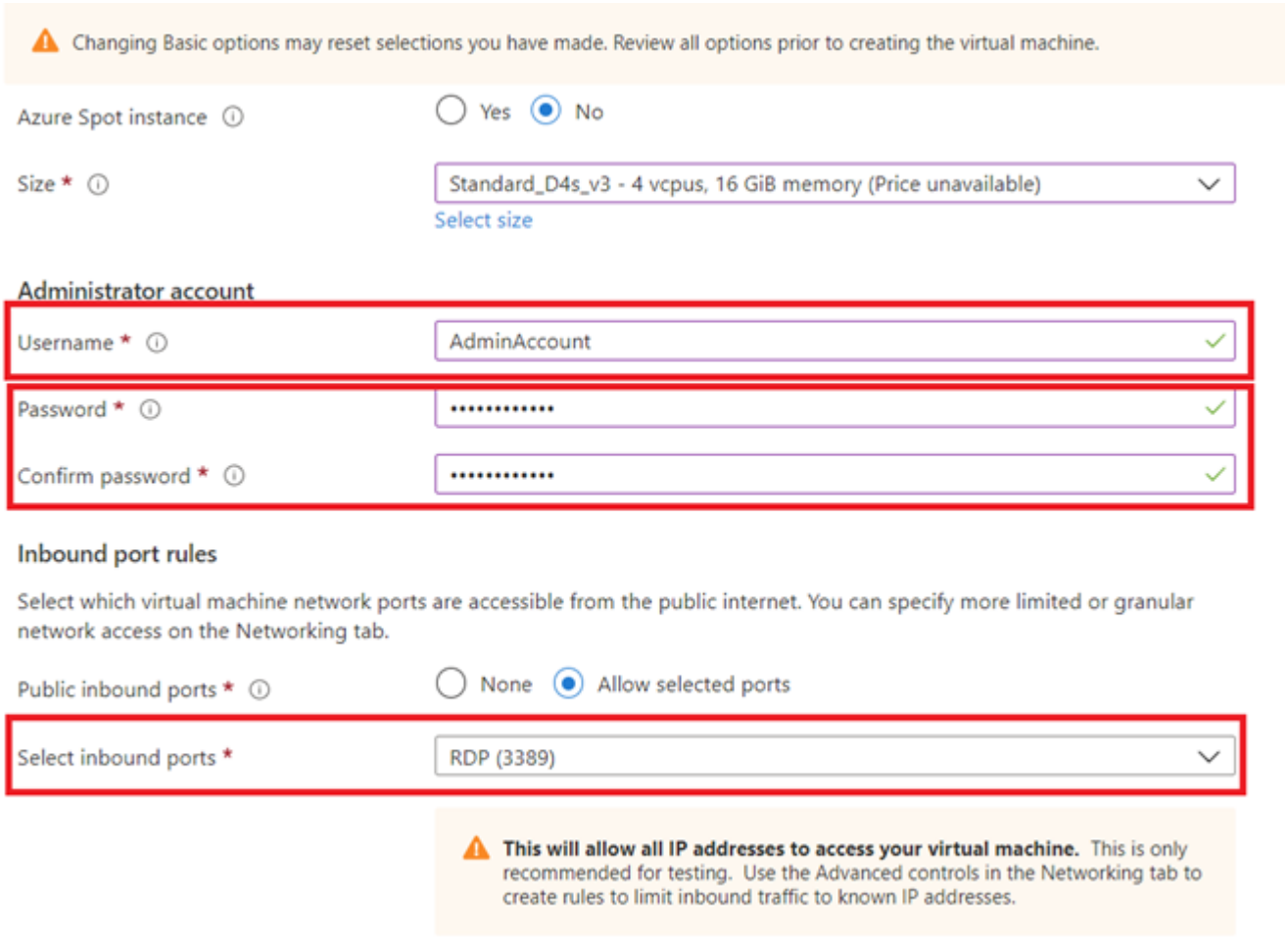
- Select an existing Resource Group or create a new one.
- Give the VM a Name.
- Select a Windows Server VM Image.
- Select a VM Size based on the expected workload. More information on server sizes can be found in the Quality Management Suite System Design Guide.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



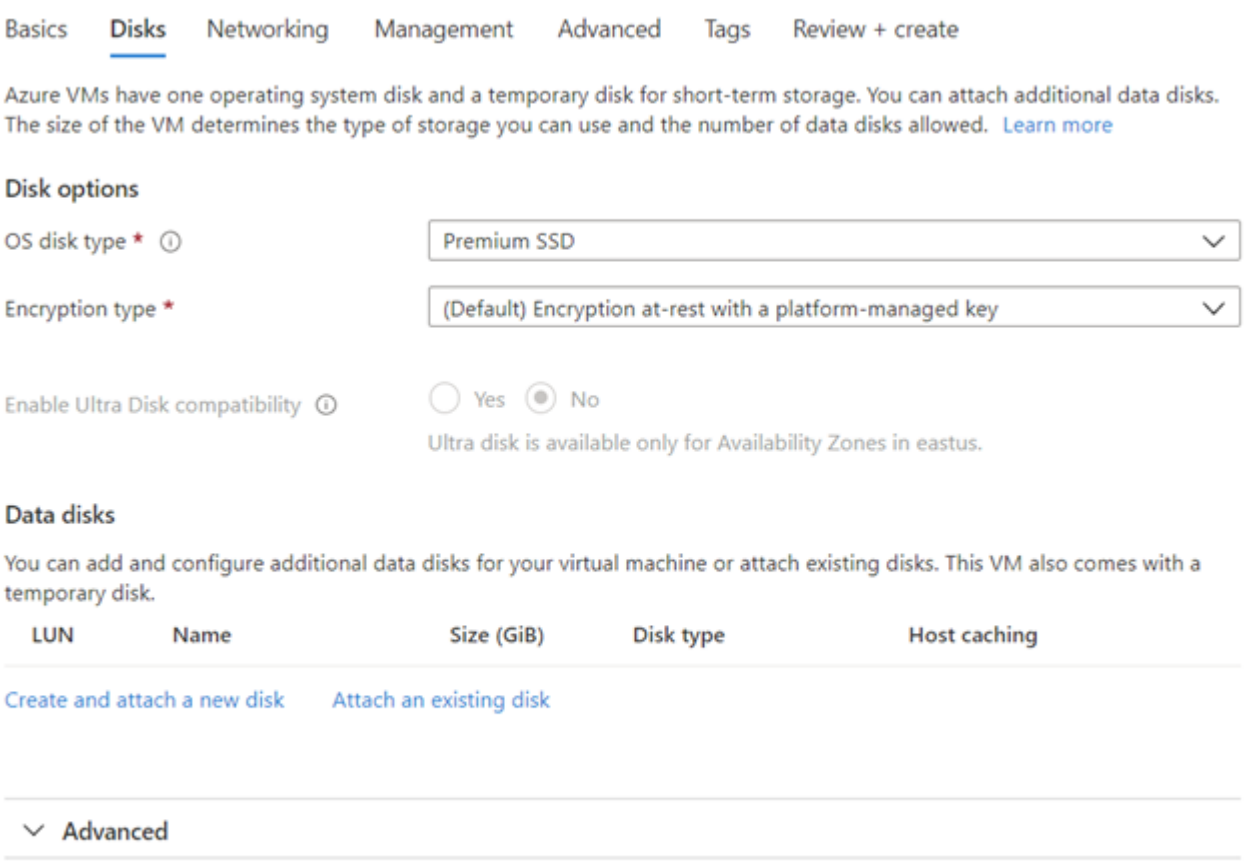
Next, create an administrator account and give it a password. Also, allow the inbound RDP port so that remote RDP sessions can be created:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



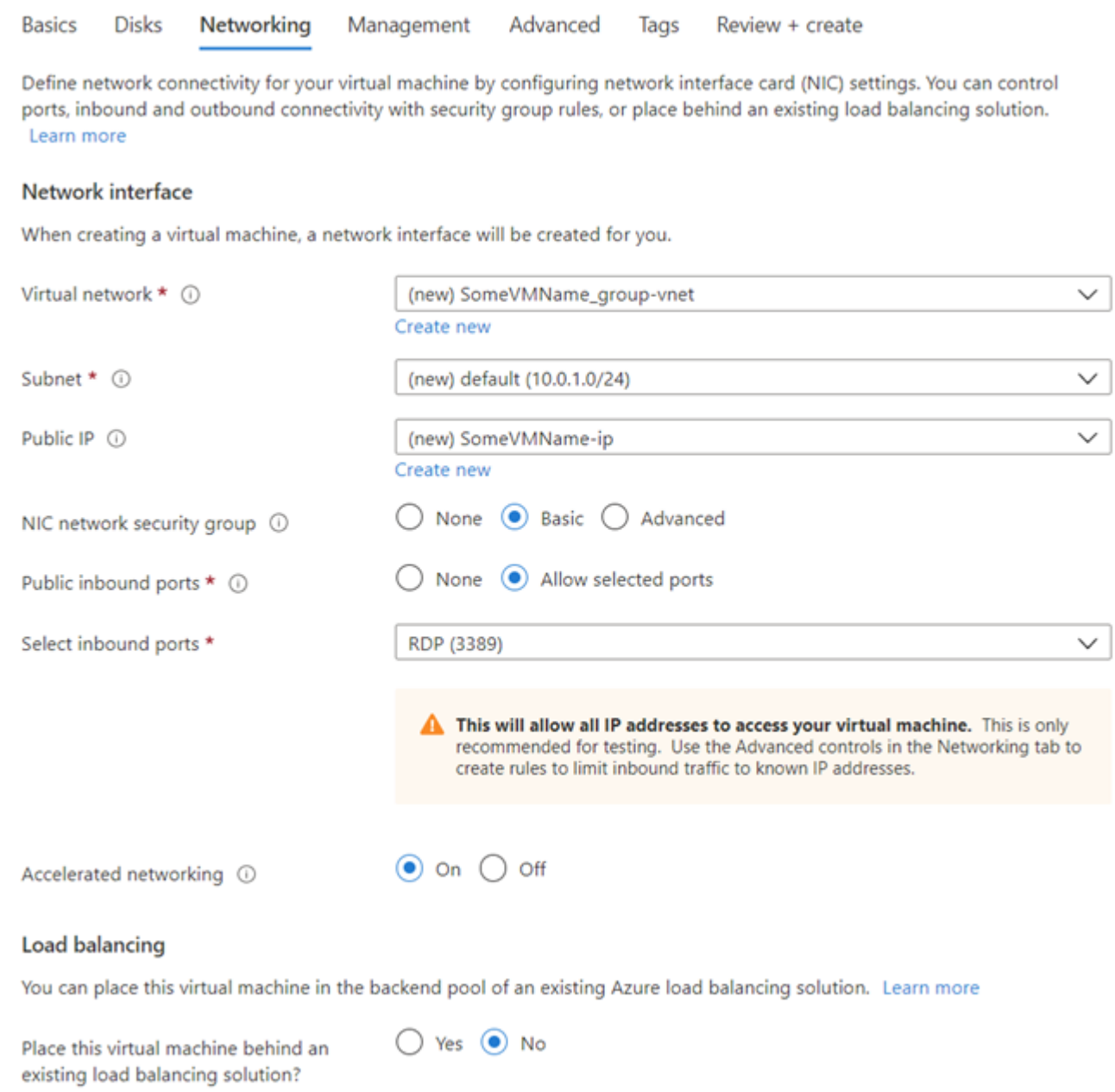
Next, click “Next: Disks >”, which will take you to the “Create a virtual machine” Disks page. On this page you can optionally add additional disks to the VM if you are going to store recordings long term on the Azure VM:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



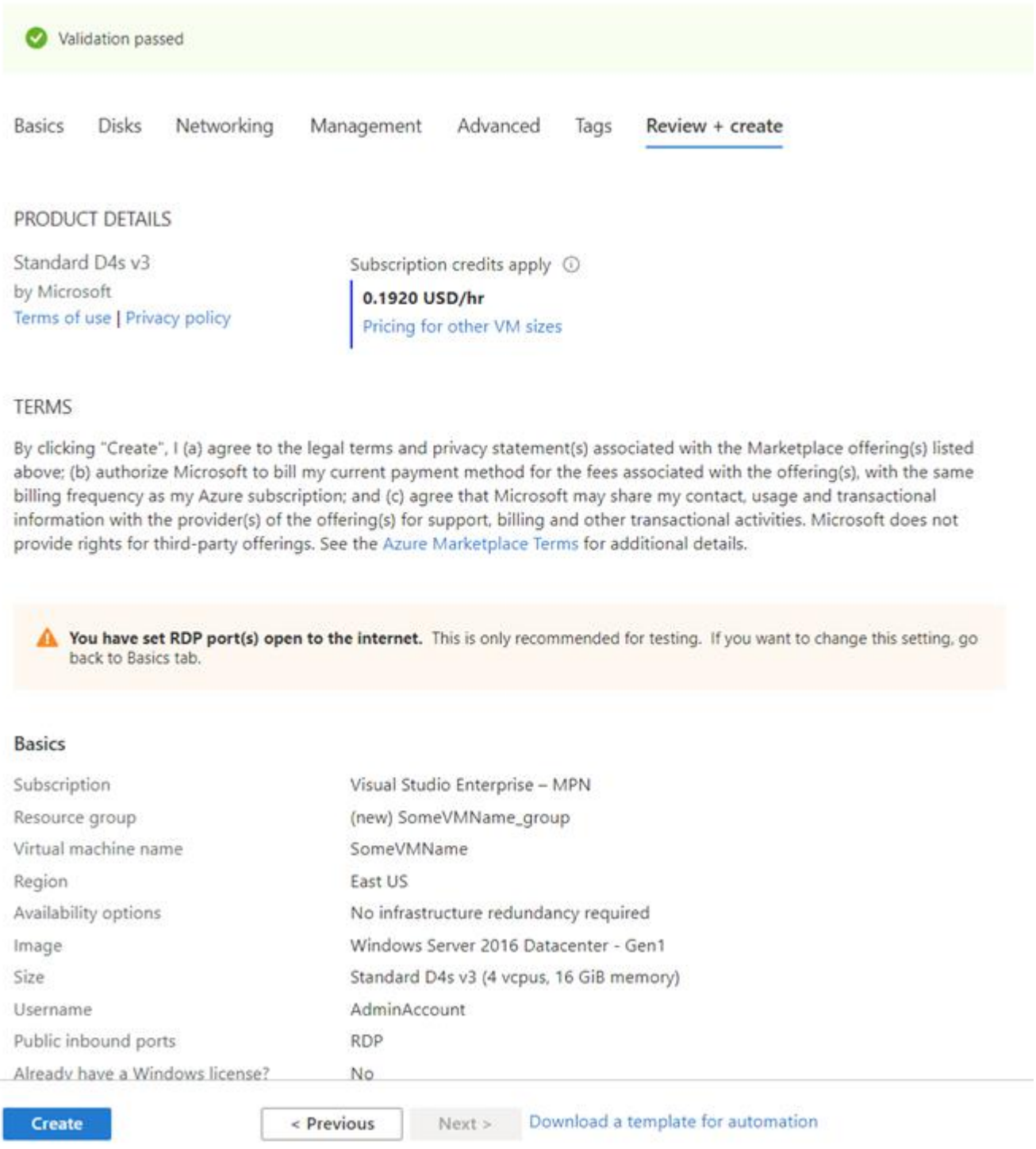
Once you have added any additional disks that may be required, click “Next: Networking >”, which will take you to the “Create a virtual machine” Networking page. On this page you can configure any network settings you wish to set, or leave the defaults and allow Azure to configure them for you:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



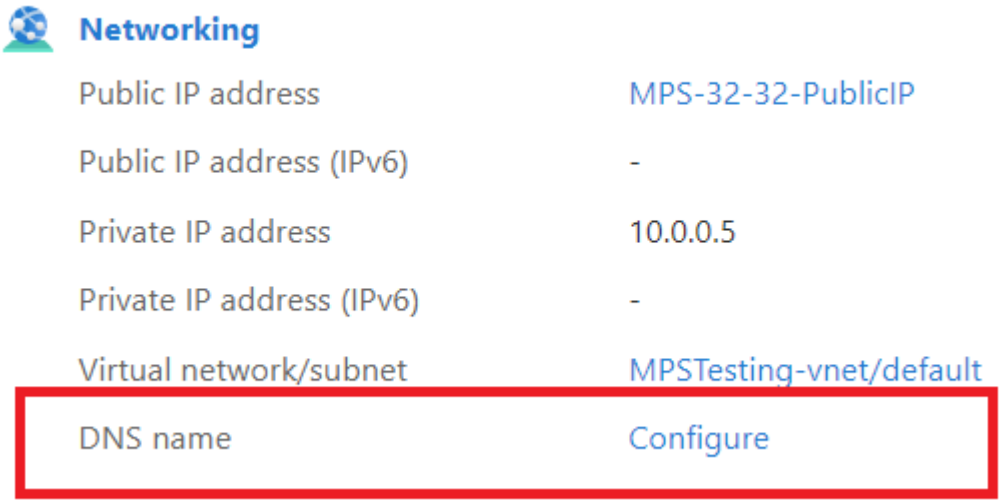
Once you have finished with the Networking page, click “Review + Create”, which will take you to the “Create a virtual machine” Review + Create page where you can review the settings for the VM. Once you are ready to move forward, click on Create.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988


Validation passed
Basics
Disks
Networking
Management
Advanced
Tags
Review + create
PRODUCT DETAILS
Standard D4s v3
by Microsoft
Terms of use | Privacy policy
Subscription credits apply
0.1920 USD/hr
Pricing for other VM sizes
TERMS
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.
You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.
Basics
Subscription
Visual Studio Enterprise – MPN
Resource group
(new) SomeVMName_group
Virtual machine name
SomeVMName
Region
East US
Availability options
No infrastructure redundancy required
Image
Windows Server 2016 Datacenter - Gen1
Size
Standard D4s v3 (4 vcpus, 16 GiB memory)
Username
AdminAccount
Public inbound ports
RDP
Already have a Windows license?
No
Create
< Previous
Next >
Download a template for automation

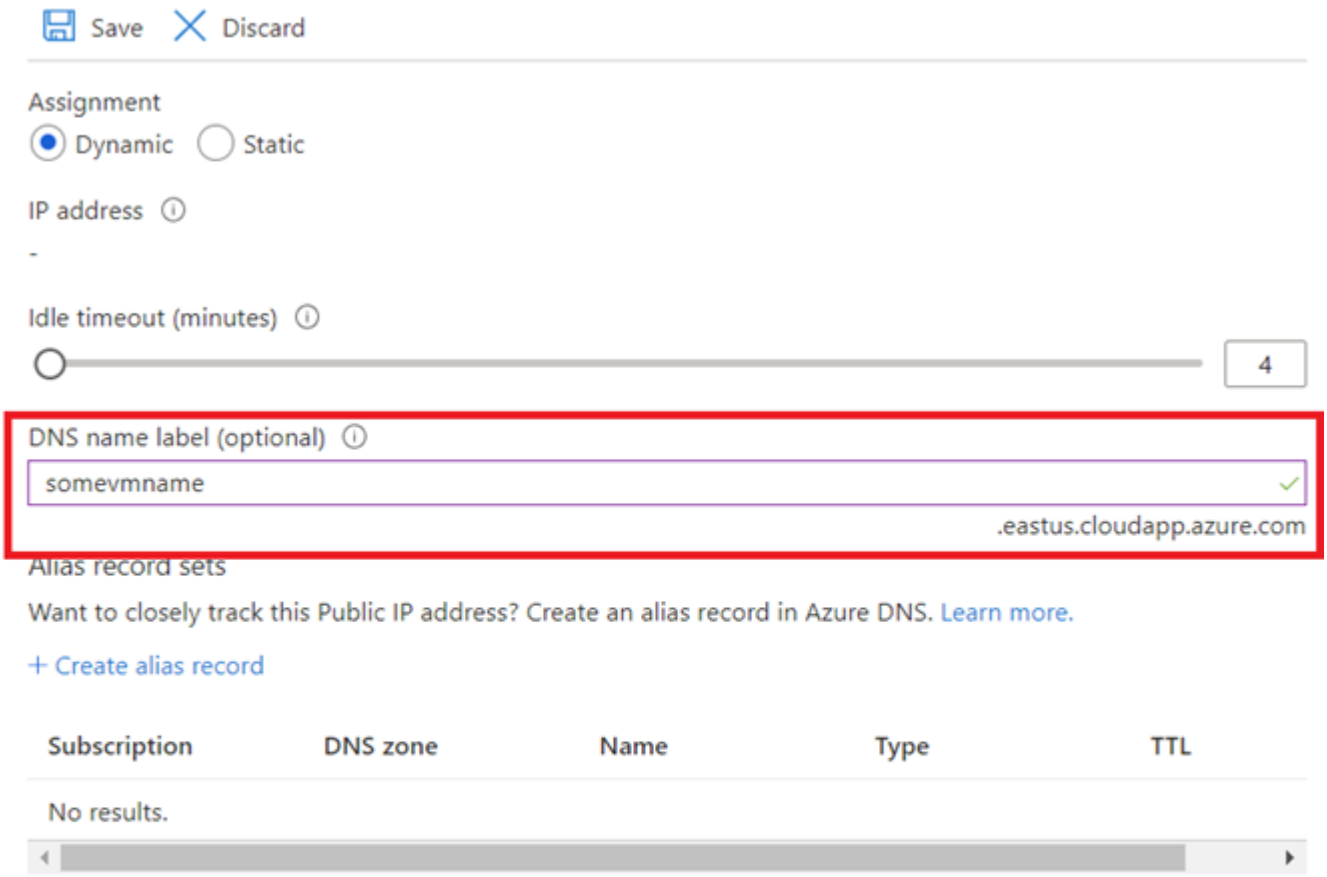
Configure Azure VM

Once the VM has been created, it should be accessible from the “Home -> Virtual Machines” page in Azure. On the Virtual Machines page click on the newly created VM, which will allow you to further configure the VM. On the configuration page click on the “DNS name” field to configure it:

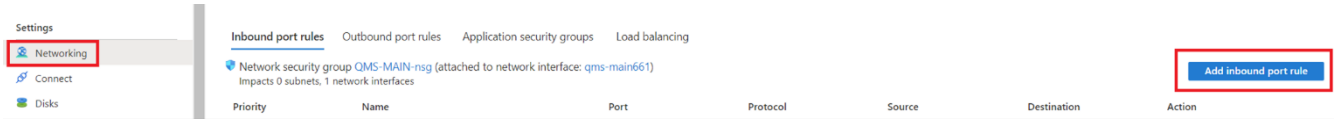


This will take you to the Public IP address Configuration page which will allow you to configure the DNS name for the VM. Enter a DNS value, typically the machine name in lower case, and click Save:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



Next, you need to configure the inbound ports for the Teams Native Recording integration. To do this we need to go to the Networking in the VM settings and click on “Add Inbound port rule”:

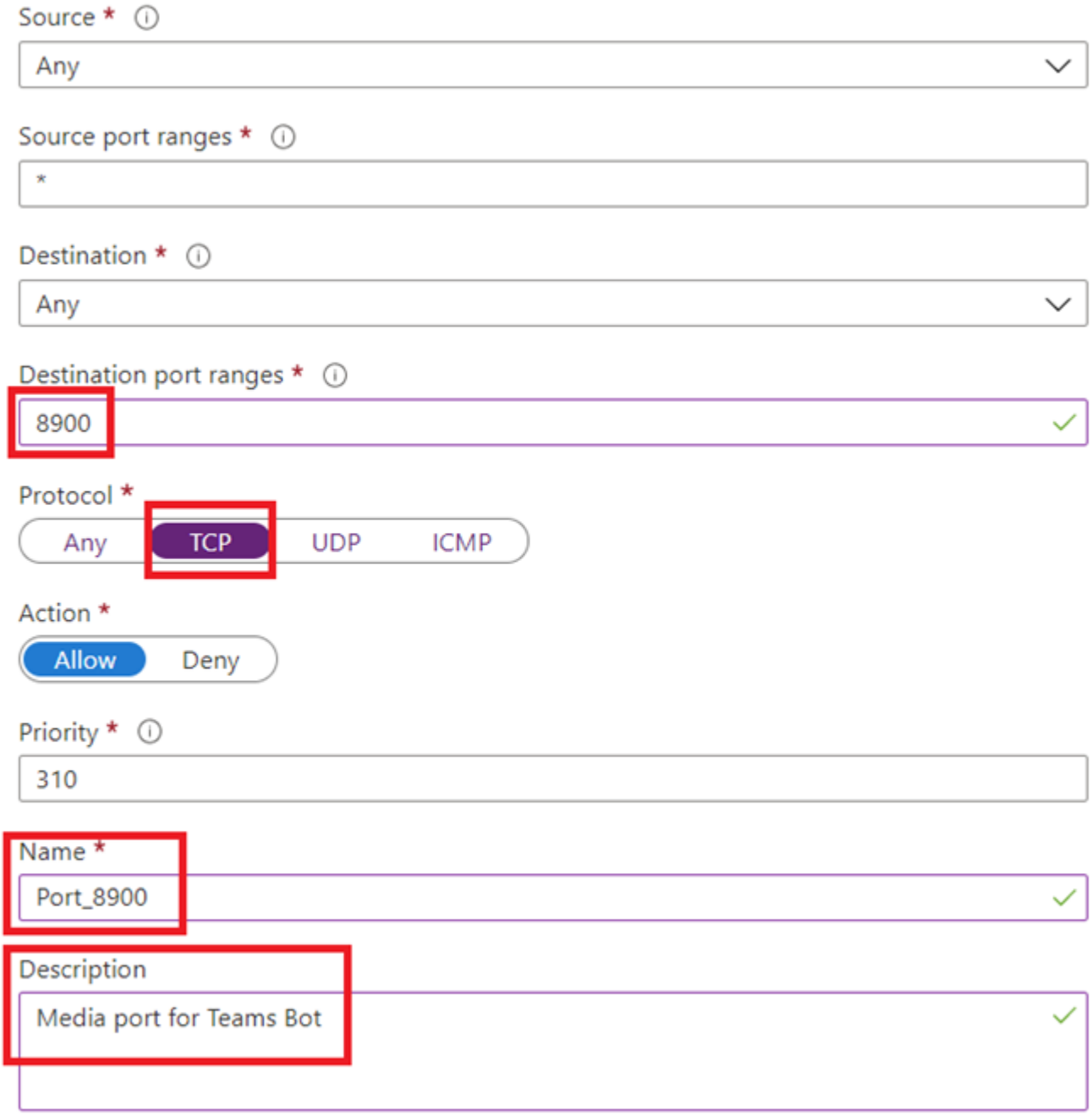


You will need to add 2 ports you will also enter these ports into the QMS Call Recording Service configuration later:

- 8900 TCP – Teams Media Port
- 8901 TCP – Teams Call Control Port

Teams Media Port:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



Teams Call Control Port:

Source * ⓘ

Any

Source port ranges * ⓘ

*

Destination * ⓘ

Any

Destination port ranges * ⓘ

8901

Protocol *

Any | TCP | UDP | ICMP

Action *

Allow | Deny

Priority * ⓘ

310

Name *

Port_8901

Description

Call Control port for Teams Bot

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Configure Azure VM Windows OS

Once the VM Settings have been configured, you need to configure some Windows settings. First, add firewall rules to the server to open the Teams ports that we configured in the VM Settings. To do that you will need to connect to the VM using RDP and open an elevated (Administrator) PowerShell instance to run the following commands (change the port information if you are not using the default ports used above):

New-NetFirewallRule -displayname 'QMS Teams Bot Media' -direction inbound -action allow -protocol tcp -LocalPort 8900

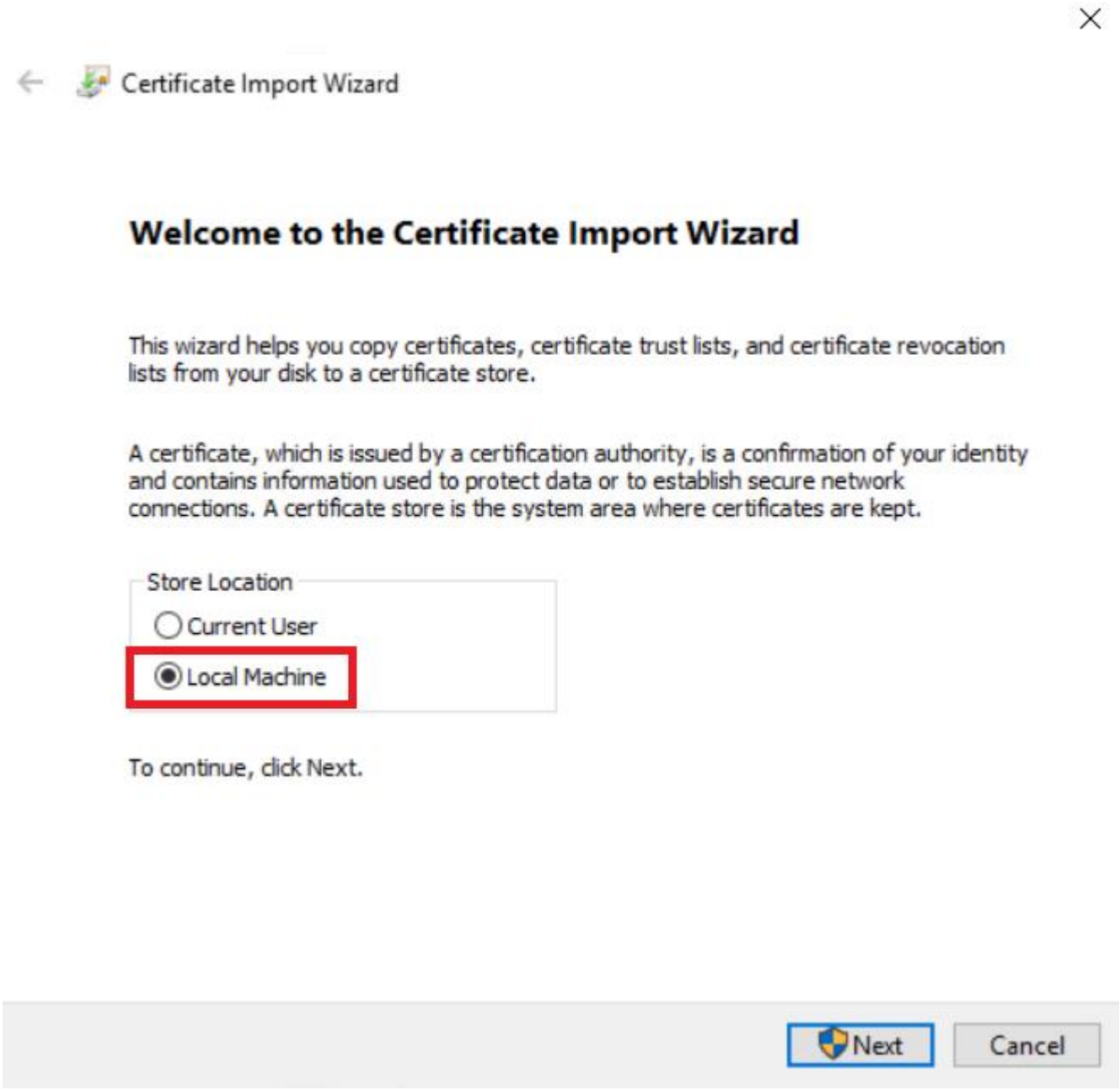
New-NetFirewallRule -displayname 'QMS Teams Bot Call Control' -direction inbound -action allow -protocol tcp -LocalPort 8901

Next, you need to obtain an SSL certificate for the VM to use to secure the Teams ports as Teams requires both the Call Control and Media ports to be secured, and will only communicate with a trusted endpoint. The SSL certificate must meet the following criteria:

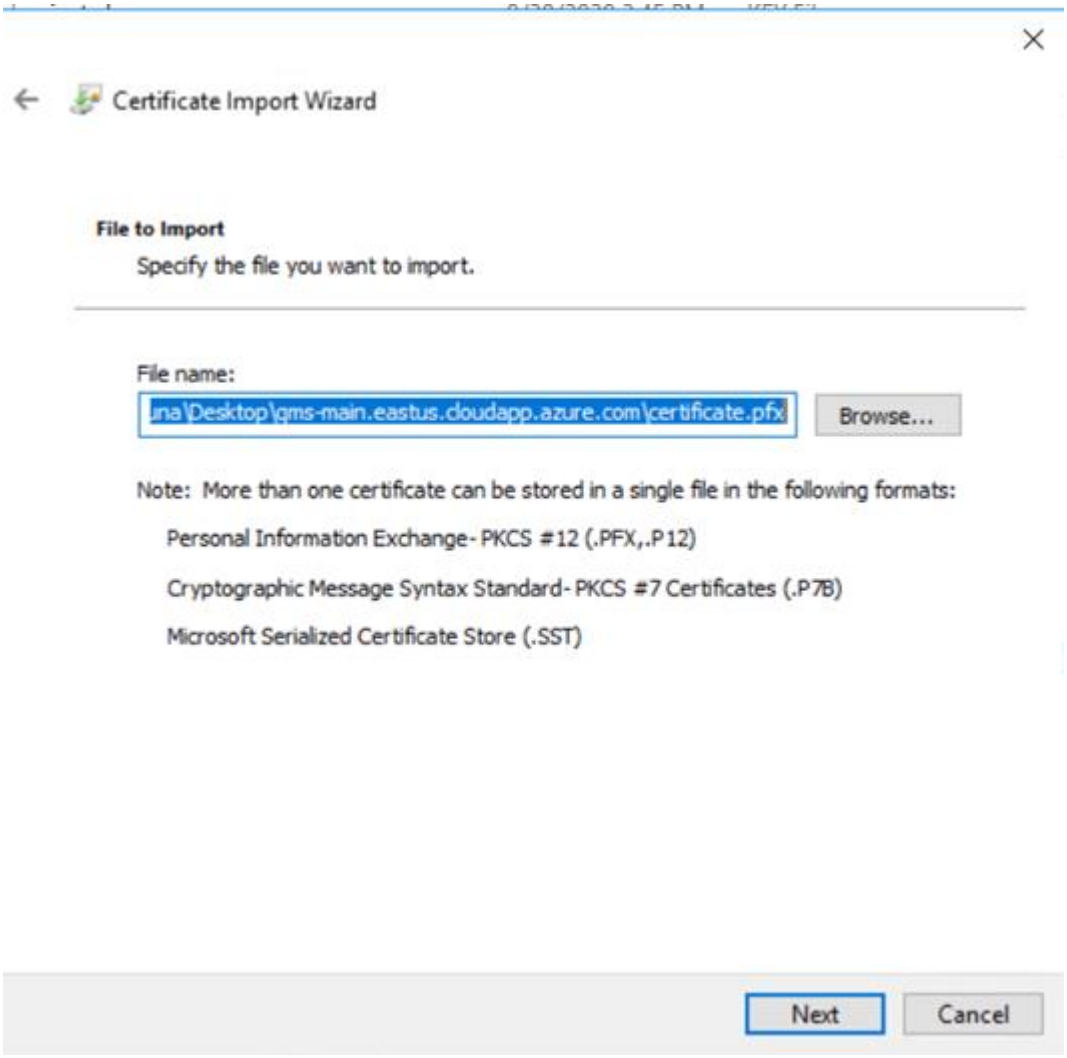
- The SSL certificate must be in .PFX format (not .CER) and include the private key information. Only CSP-stored certificates are supported by the Microsoft media platform, CNG/KSP certificates are not supported.
- The SSL certificate must be issued by a public trusted Certificate Authority that is listed as a Participant in the Microsoft Trusted Root Program (https://ccadb-public.secure.force.com/microsoft/IncludedCACertificateReportForMSFT)

After the certificate has been generated, you will need to import the .PFX certificate into the Personal store for the local machine on the QMS Azure VM. To do this, right click on the .PFX file and select “Install PFX”. This will take you to the opening Certificate Import page, where you will select Local Machine and click Next:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

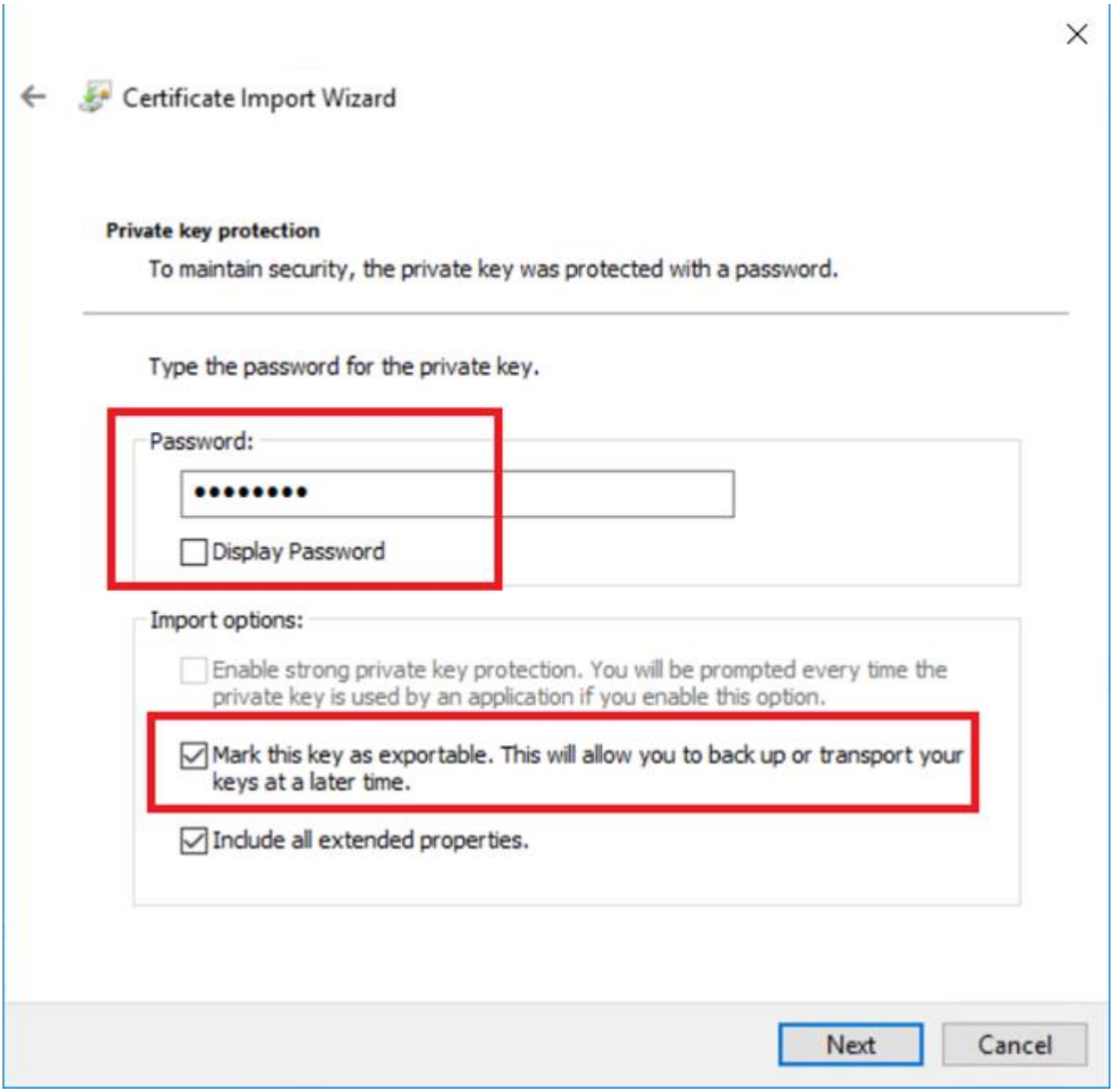


Next, verify that the correct file is displayed for import and click Next:



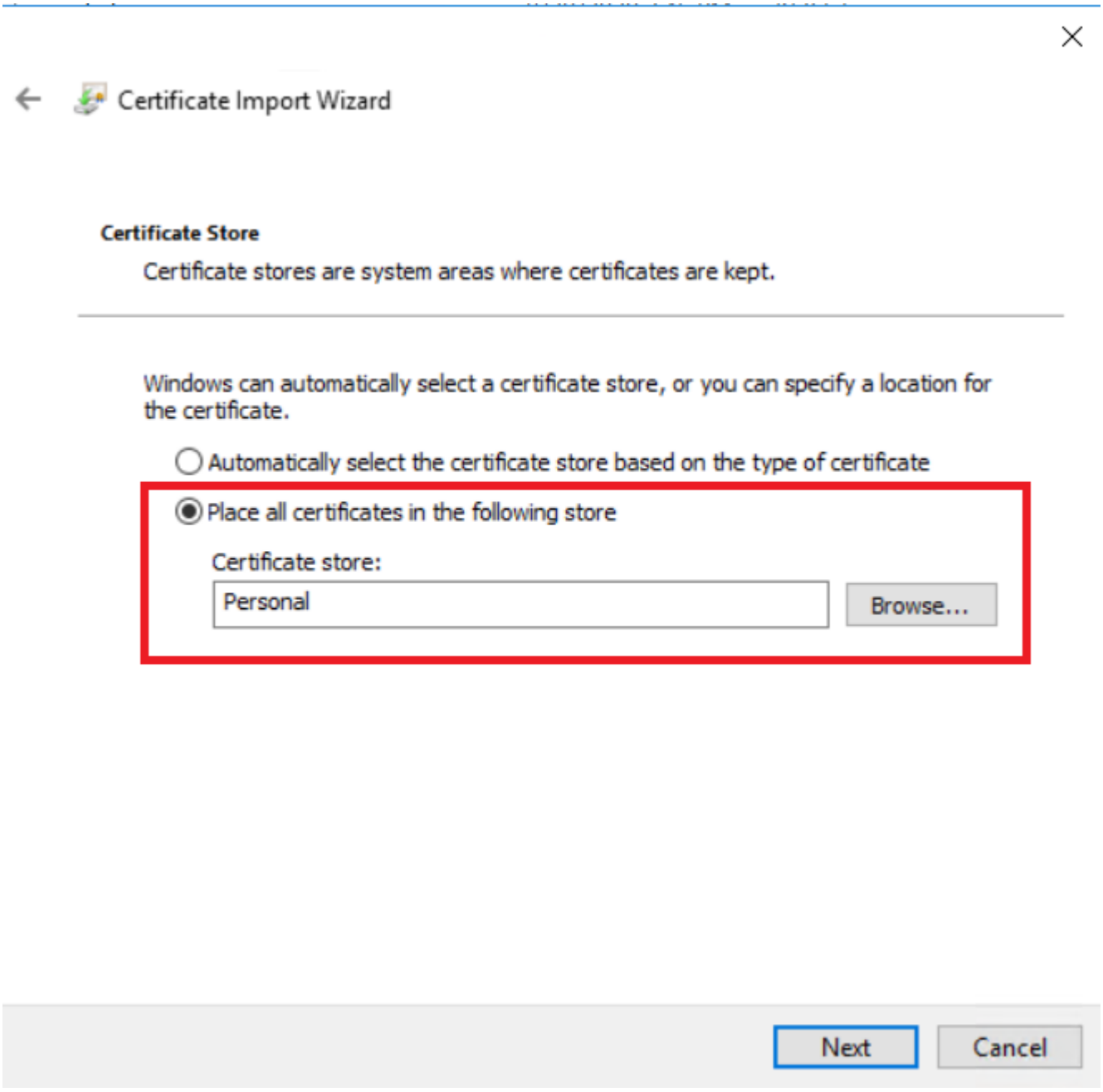
Next, enter the password for the private key and make sure the “Mark this key as exportable” option is selected and click Next:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

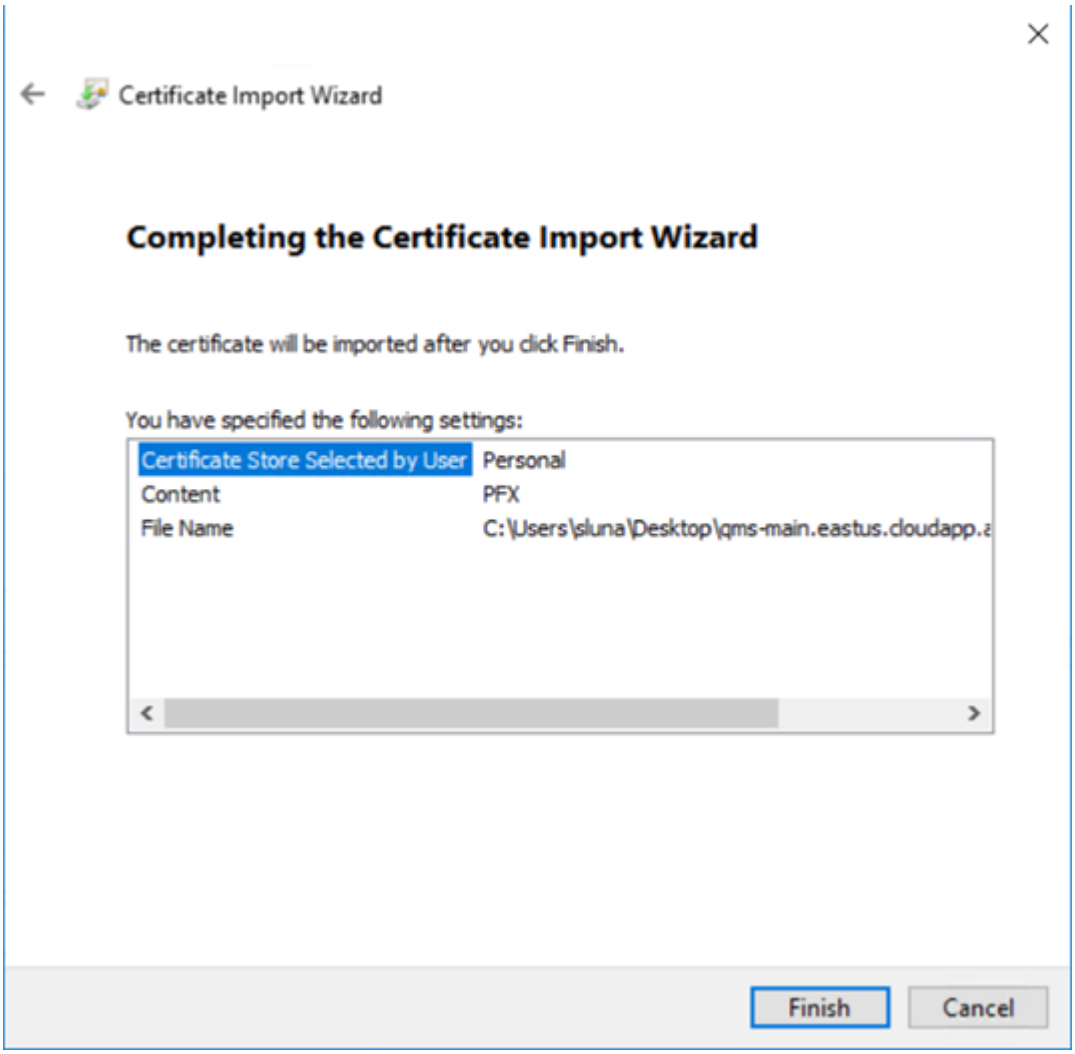


Next, select the “Personal” store as the location to place the certificate and click Next:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



Finally, verify the information on the Completing the Certificate Import Wizard page and click Finish:



Once the certificate has been imported it will need to be bound to the Teams ports that we configured in the VM settings. To do this you will need to open an elevated (Adminstrator) command prompt and run the following two commands (change the port information if you are not using the default ports used above):

netsh http add sslcert ipport=0.0.0.0:8900 certhash=<Thumbprint of the Certificate> appid={00000000-0000-0000-0000-000000000000}

netsh http add sslcert ipport=0.0.0.0:8901 certhash=<Thumbprint of the Certificate> appid={00000000-0000-0000-0000-000000000000}

In the future, when the certificate has expired and a new one is issued. You will need to remove the existing certificate bound to the ports and bind the new certificate with the same two commands above. You can remove the existing certificate from the ports using the two commands below:

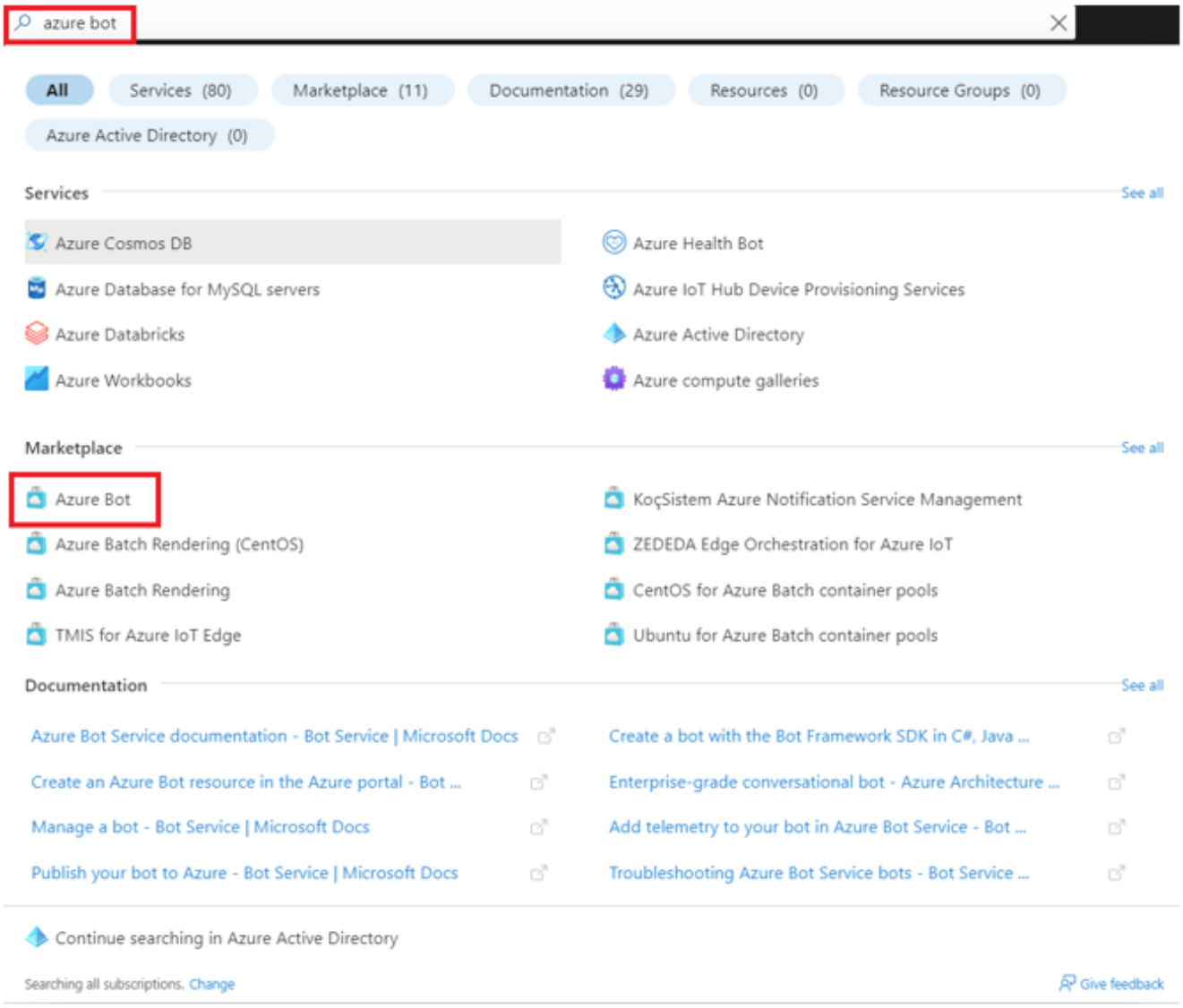
netsh http delete sslcert ipport=0.0.0.0:8900

netsh http delete sslcert ipport=0.0.0.0:8901

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Register the Azure Bot

In order for the QMS Recording Service to be able to receive call control and audio from Teams, we need to configure the compliance recording bot in Azure. To do this, first search for “Azure Bot” in the Azure search bar and click on “Azure Bot”:



Next, on the bot configuration page, provide the following details and click create:

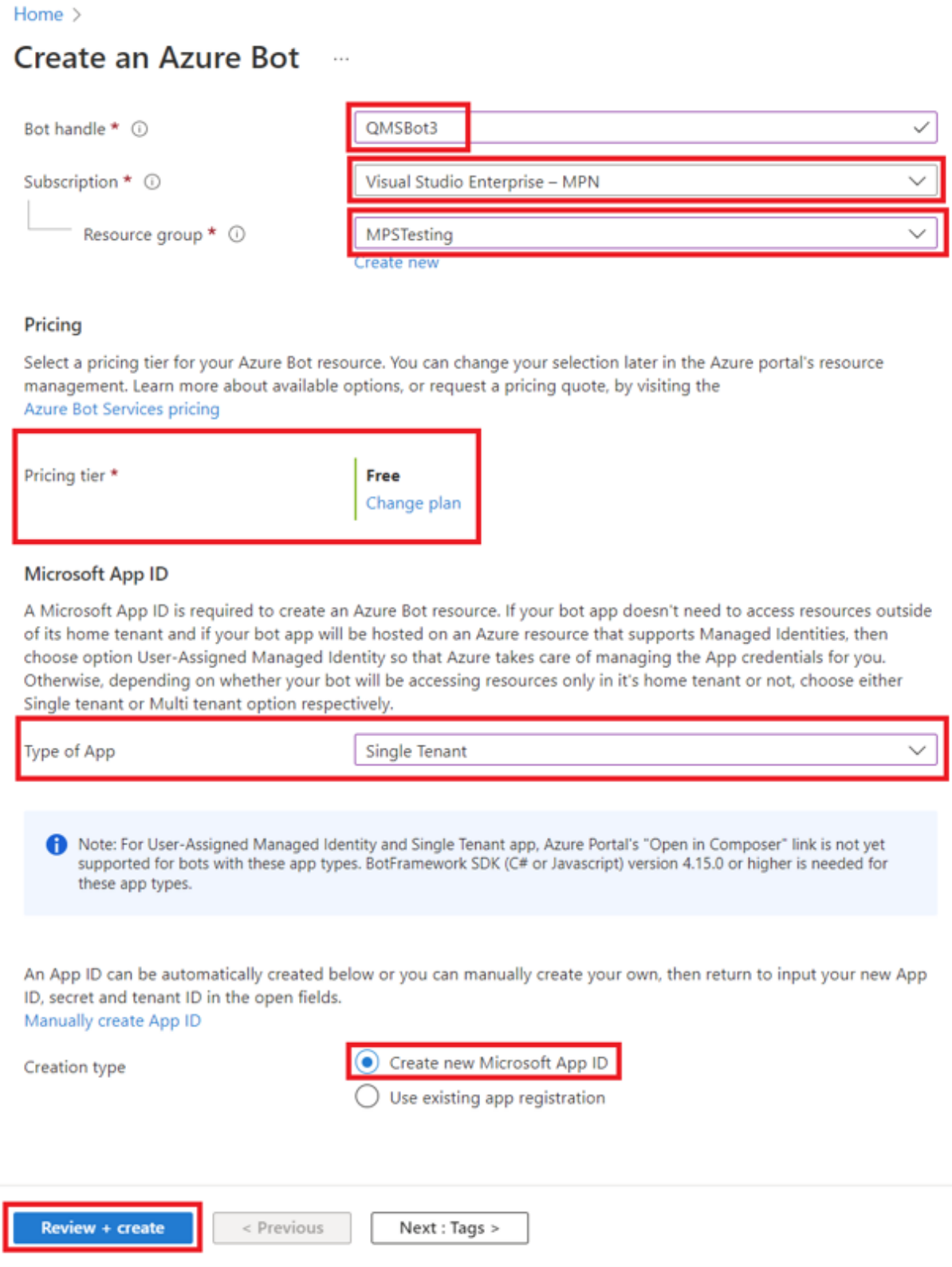
- Choose a handle for the bot.
- Select a subscription.
- Select the resource group to be used for the Bot.
- Select the F0 pricing tier.
- Select the Type of App

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

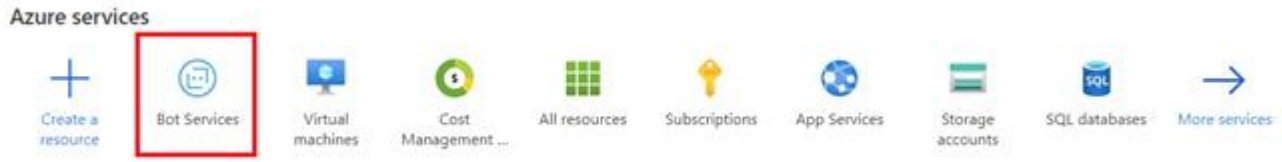
- Single Tenant – Select this option if the Azure tenant the Bot is hosted in is the same as the Azure tenant that Teams is hosted in. This is the most common case.
- Multi Tenant – Select this option if the Azure tenant the Bot is hosted in is different than the Azure tenant that Teams is hosted in.

- Select “Create New Microsoft App ID”

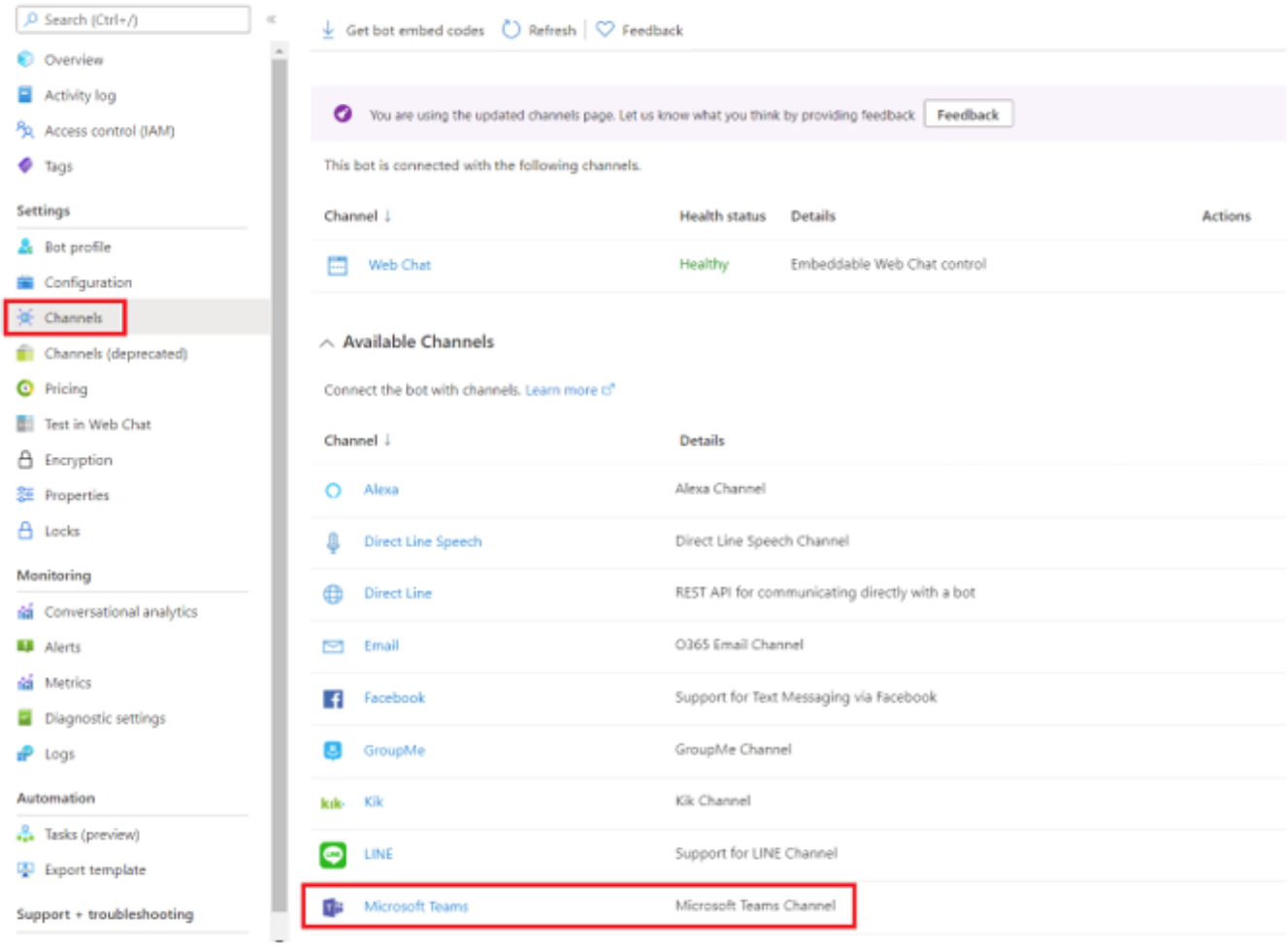
Publish Date: Tuesday, January 23, 2024
UID: E20190902550988


Home >
Create an Azure Bot
Bot handle *
QMSBot3
Subscription *
Visual Studio Enterprise – MPN
Resource group *
MPSTesting
Create new
Pricing
Select a pricing tier for your Azure Bot resource. You can change your selection later in the Azure portal's resource management. Learn more about available options, or request a pricing quote, by visiting the
Azure Bot Services pricing
Pricing tier *
Free
Change plan
Microsoft App ID
A Microsoft App ID is required to create an Azure Bot resource. If your bot app doesn't need to access resources outside of its home tenant and if your bot app will be hosted on an Azure resource that supports Managed Identities, then choose option User-Assigned Managed Identity so that Azure takes care of managing the App credentials for you. Otherwise, depending on whether your bot will be accessing resources only in it's home tenant or not, choose either Single tenant or Multi tenant option respectively.
Type of App
Single Tenant
Note: For User-Assigned Managed Identity and Single Tenant app, Azure Portal's "Open in Composer" link is not yet supported for bots with these app types. BotFramework SDK (C# or Javascript) version 4.15.0 or higher is needed for these app types.
An App ID can be automatically created below or you can manually create your own, then return to input your new App ID, secret and tenant ID in the open fields.
Manually create App ID
Creation type
Create new Microsoft App ID
Use existing app registration
Review + create
< Previous
Next : Tags >

After selecting the options in the Create an Azure Bot page, click “Review + Create” which will take you to the confirmation page. If the options are all correct, click “Create” to create the Azure Bot. Once the Azure Bot has been created, go to Bot Services in the Azure Services list or search for Bot Services in the Azure search bar.

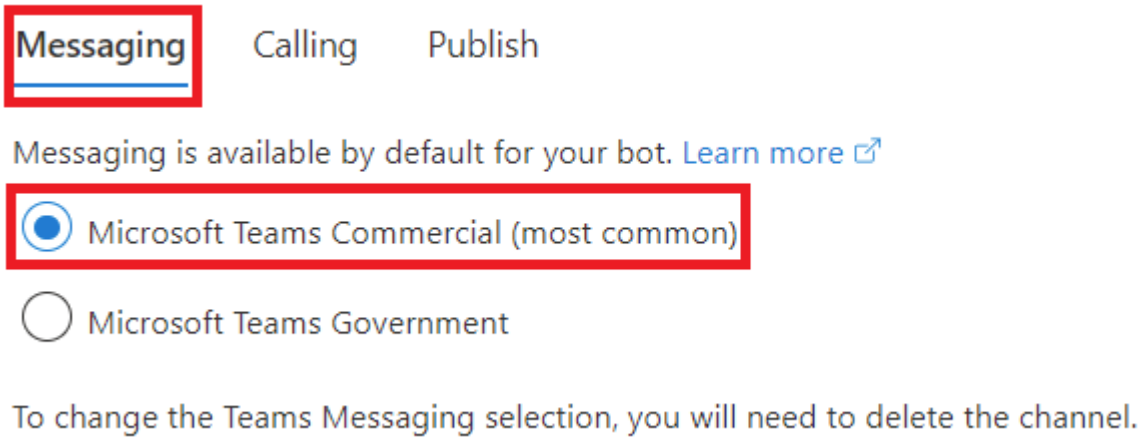


Next, select the bot and go to Channels and select the Microsoft Teams channel:



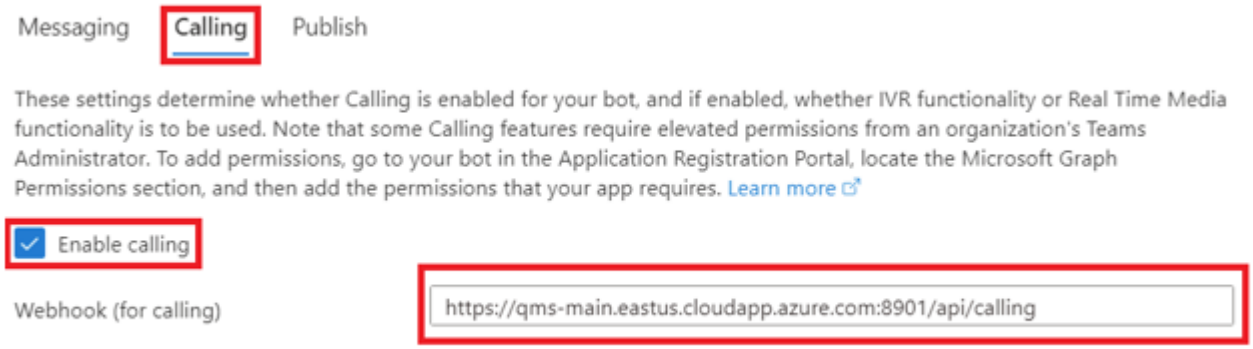
Next, agree to the terms of service and leave the Microsoft Teams Commercial option selected under Messaging:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

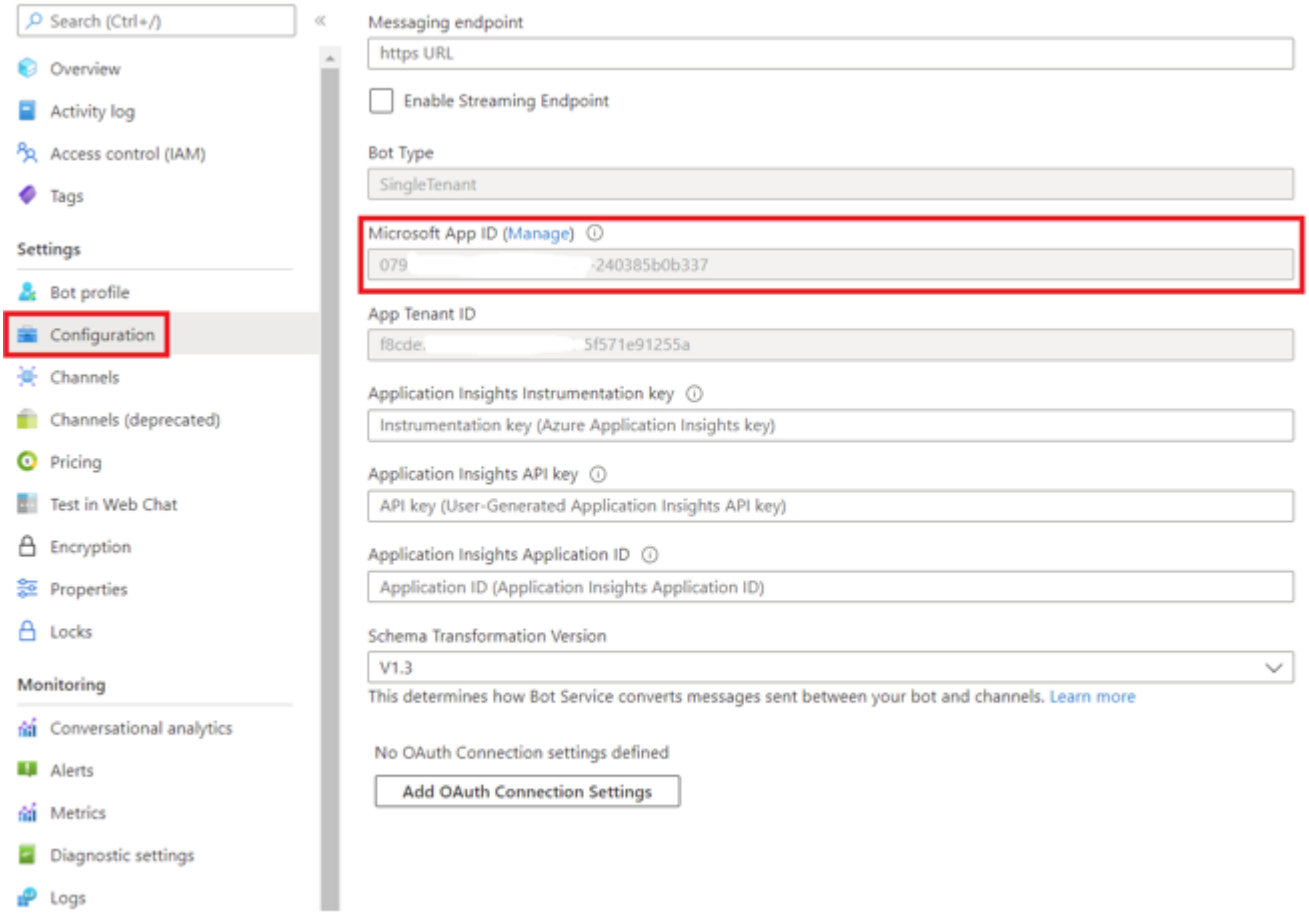


Next, in the Teams channel configuration set the following and click Apply:

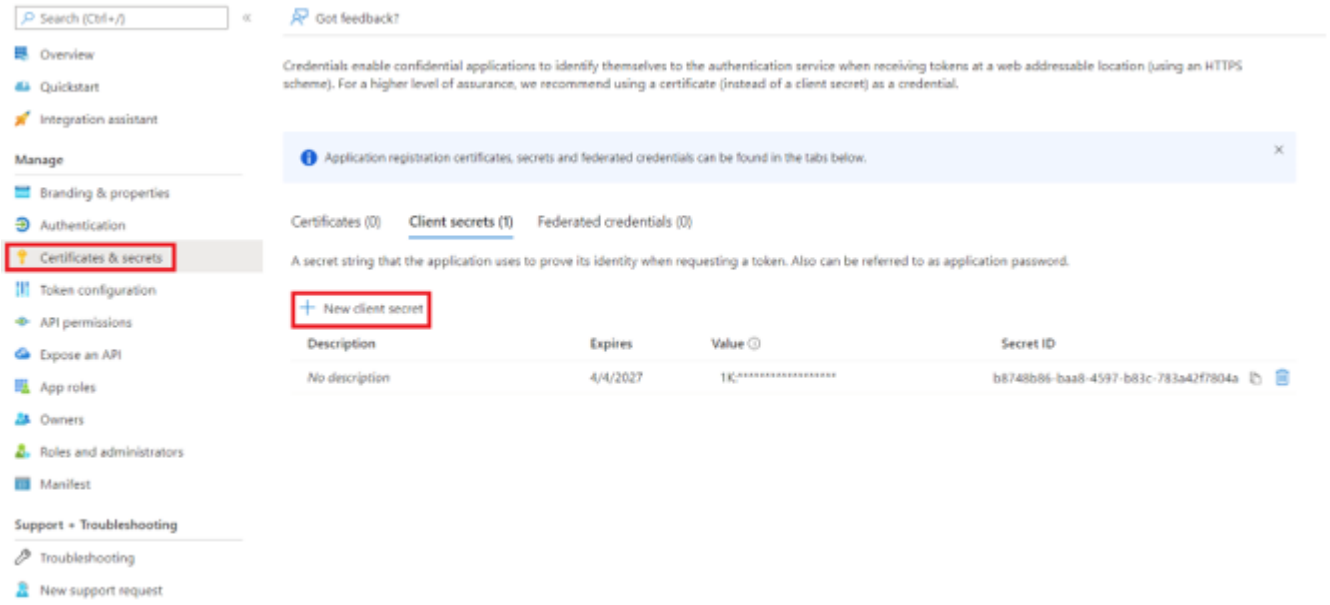
- Select “Calling”.
- Make sure “Enable calling” is selected.
- Enter the webbook URL. This should take the form of https://<FQDN>:8901/api/calling where FQDN is that of the QMS VM hosting the Call Recording Service (change the port if you are using a different Call Control port than the default port above). The FQDN value must also match the subject of the certificate.



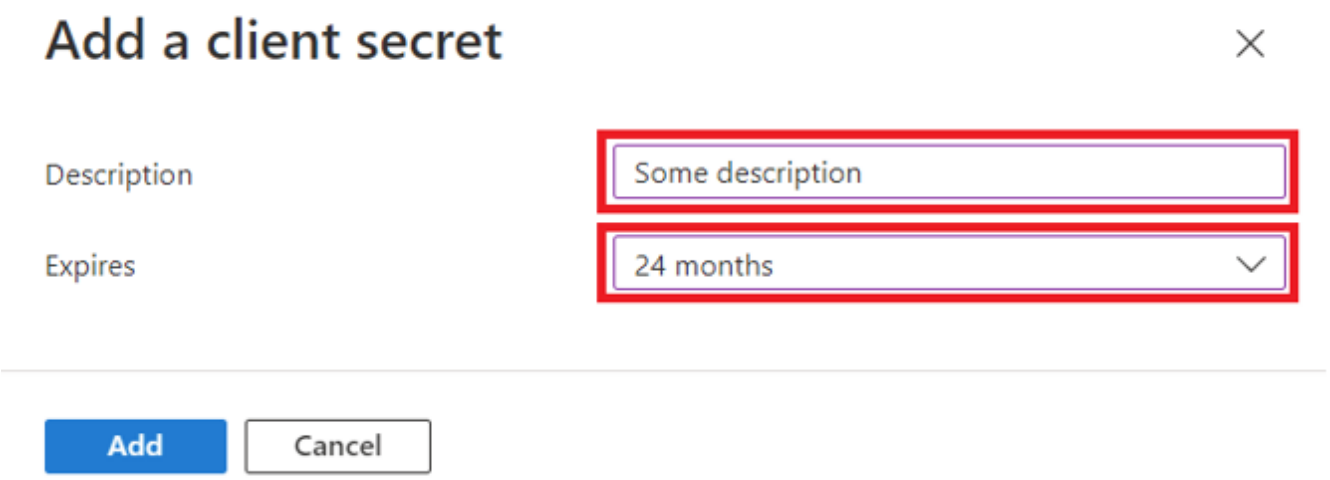
Next, select Configuration and find the Microsoft App ID. Copy this ID for later use in the QMS config, and click on Manage:



Next, go to “Certificates & Secrets” and click on “New client secret”:



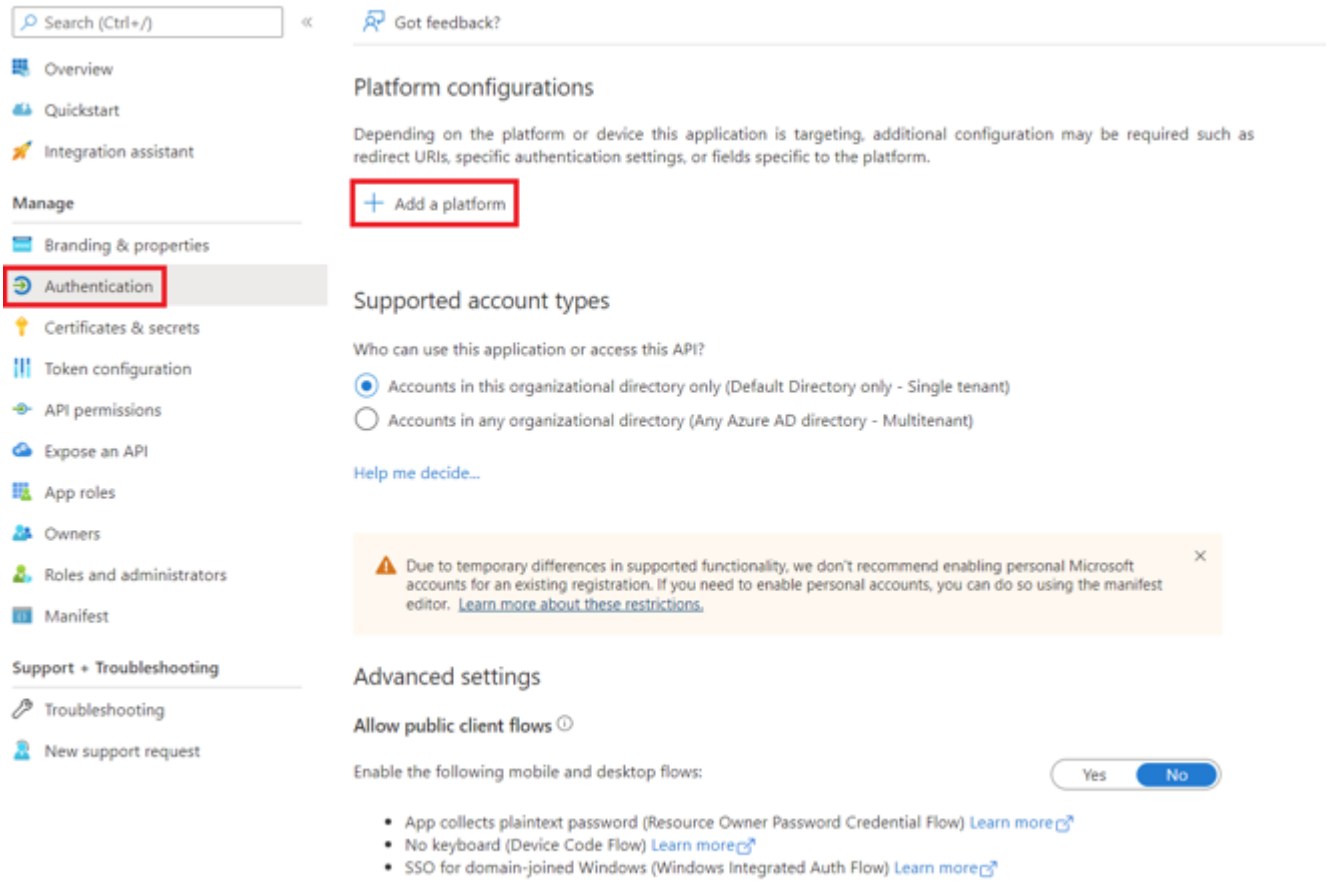
Once you have clicked on new client secret, the Add a client secret dialog will open and you will need to provide a description and an expiration and click Add:



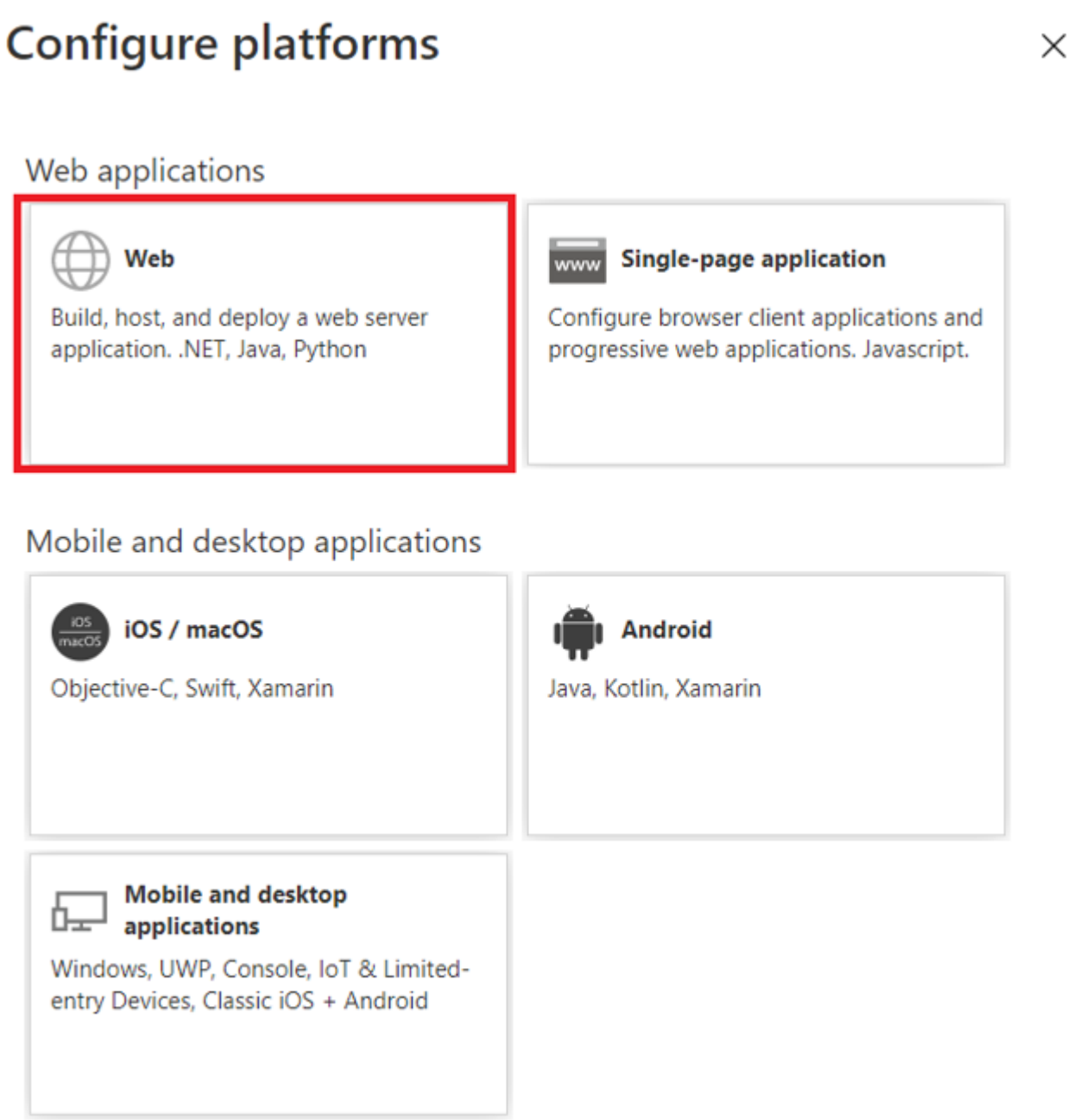
Once the secret has been generated, make sure that you copy the secret for use later when configuring the Call Recording Service in QMS:

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

While still in the Manage App area, click on “Authentication” and then click on “Add a platform”:

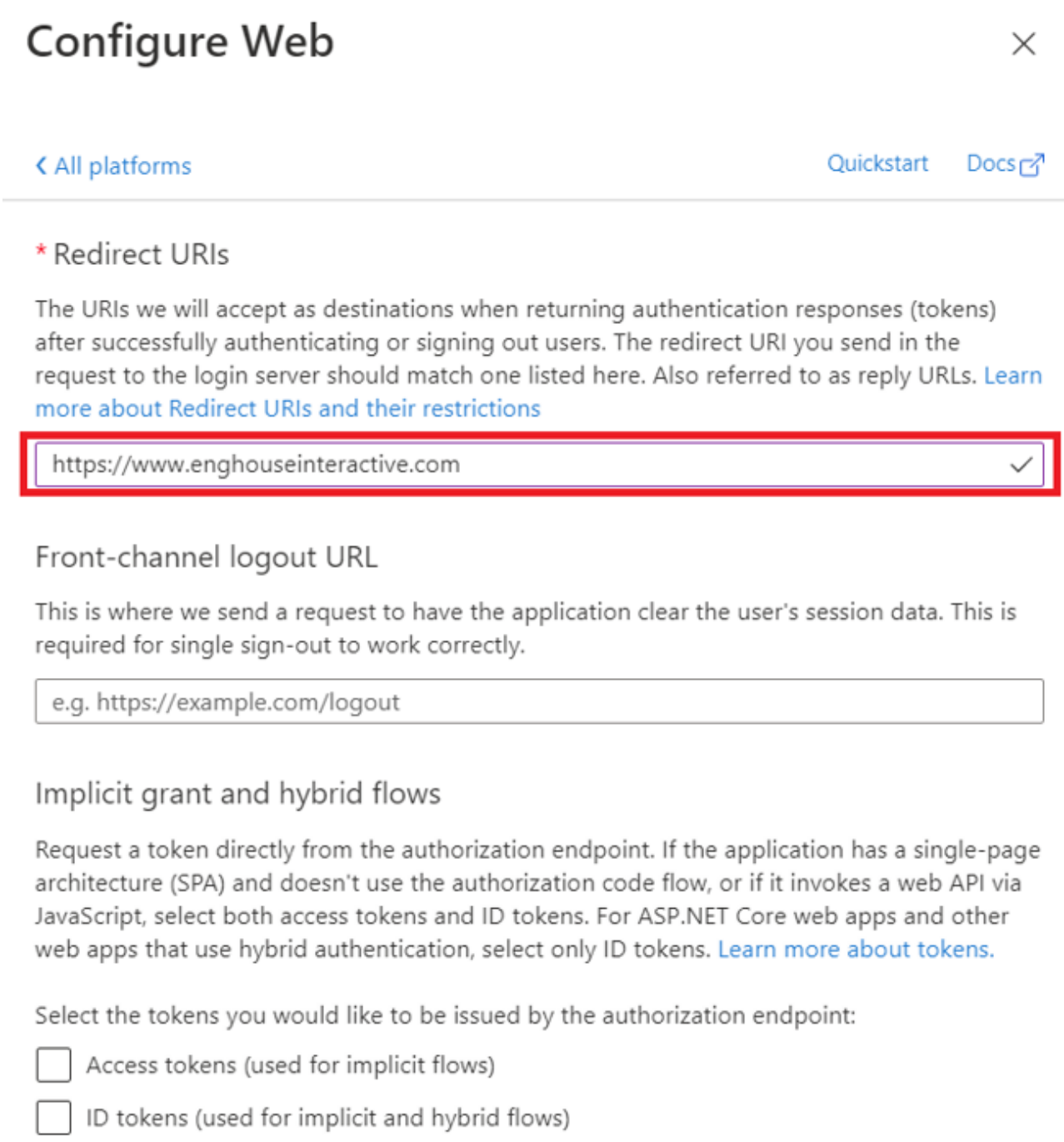


In the Configure platforms dialog select “Web”:

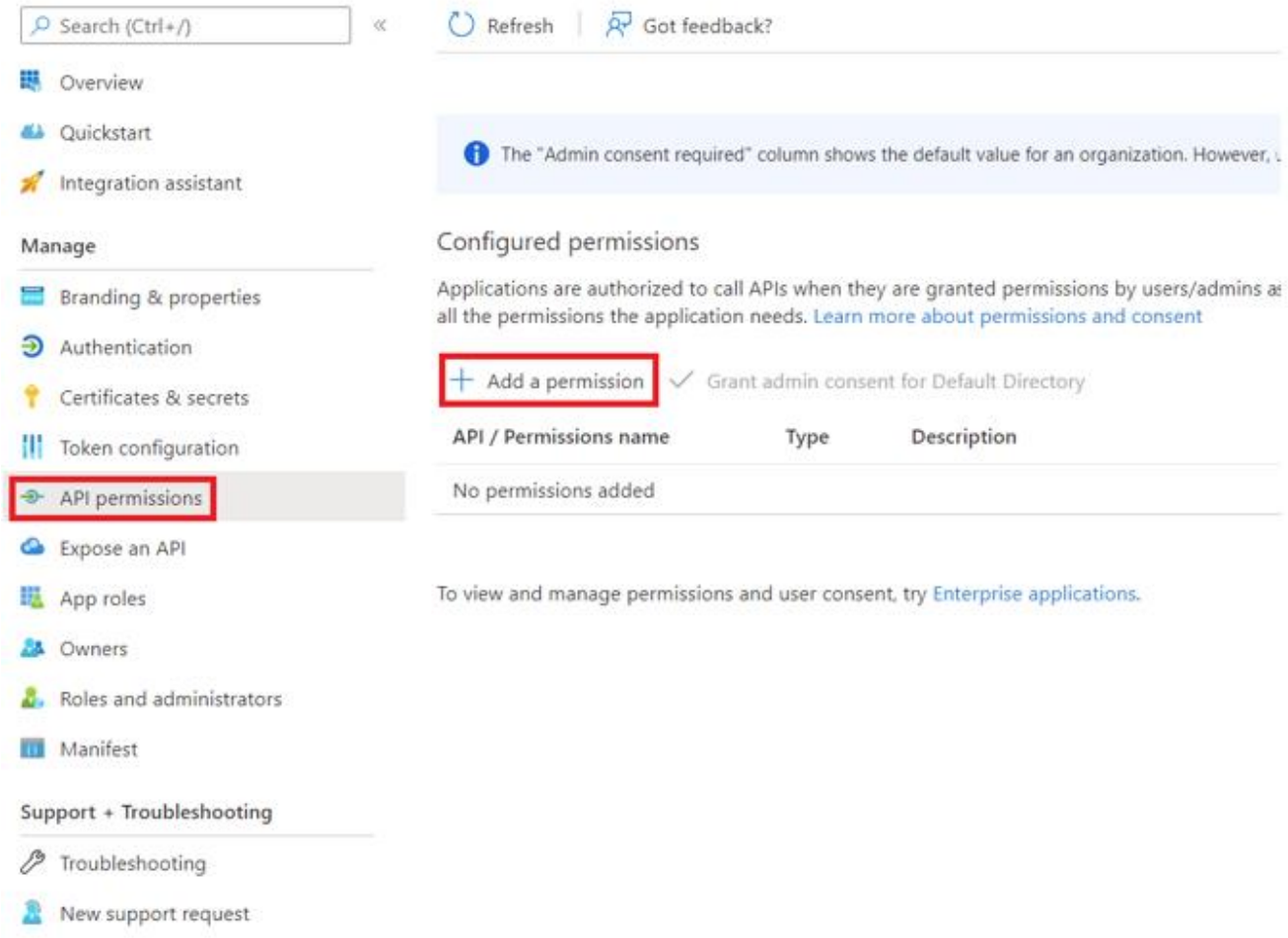


In the Configure Web dialog set the Redirect URIs to https://www.enghouseinteractive.com/ which will be used later in the consent URL and must match the value used in the consent URL. Then click configure:

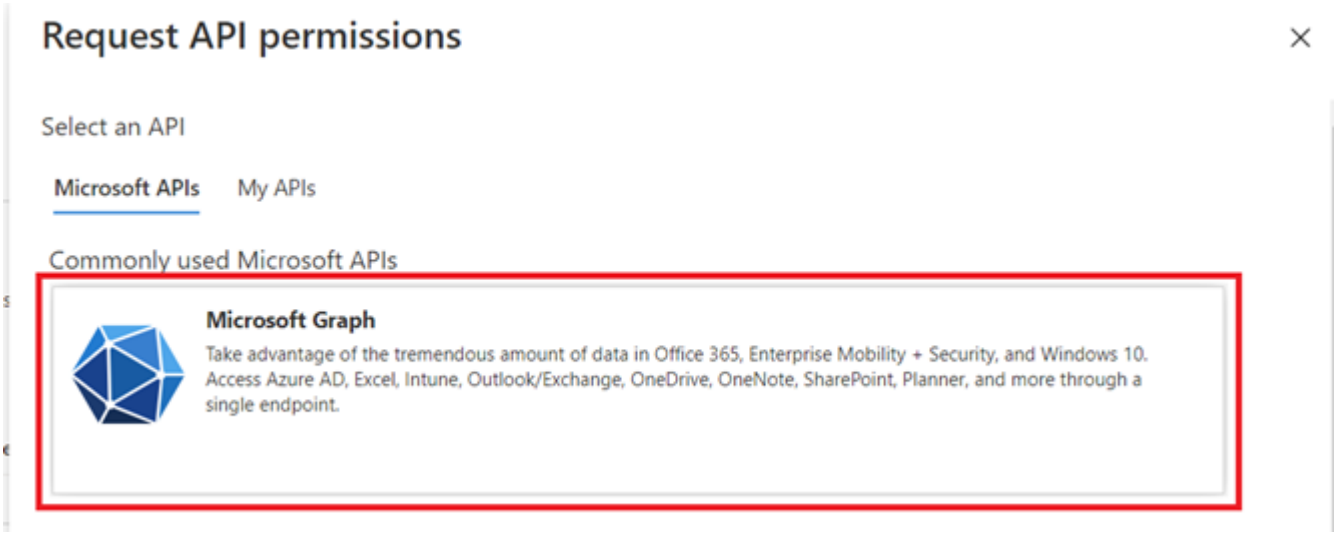
Publish Date: Tuesday, January 23, 2024
UID: E20190902550988



While still in the Manage App area, click on “API Permissions” and then click on “Add a permission”:



In the API Permissions dialog select “Microsoft Graph”:

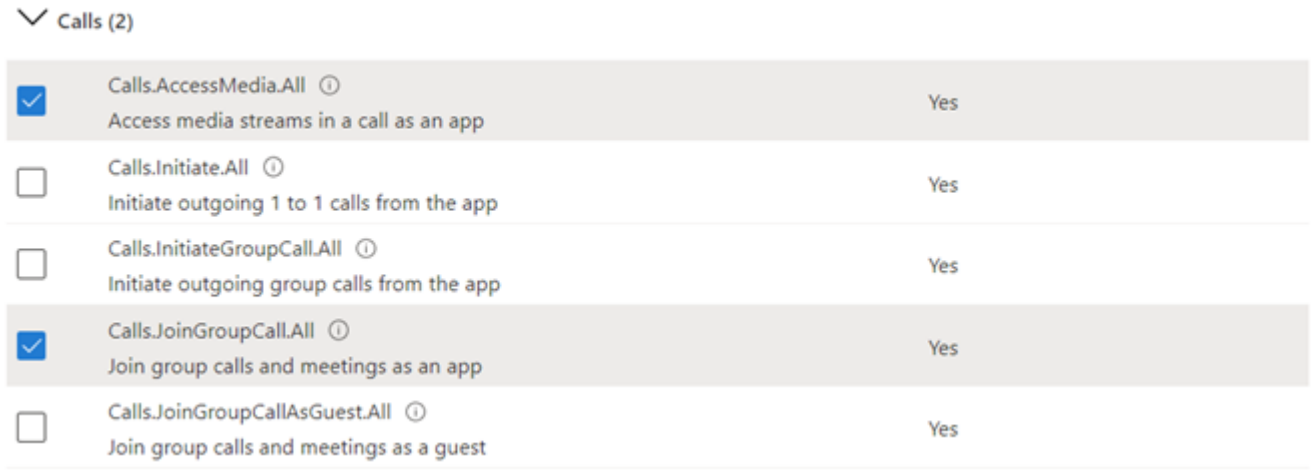


Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Select “Application permissions” and select the following permissions:

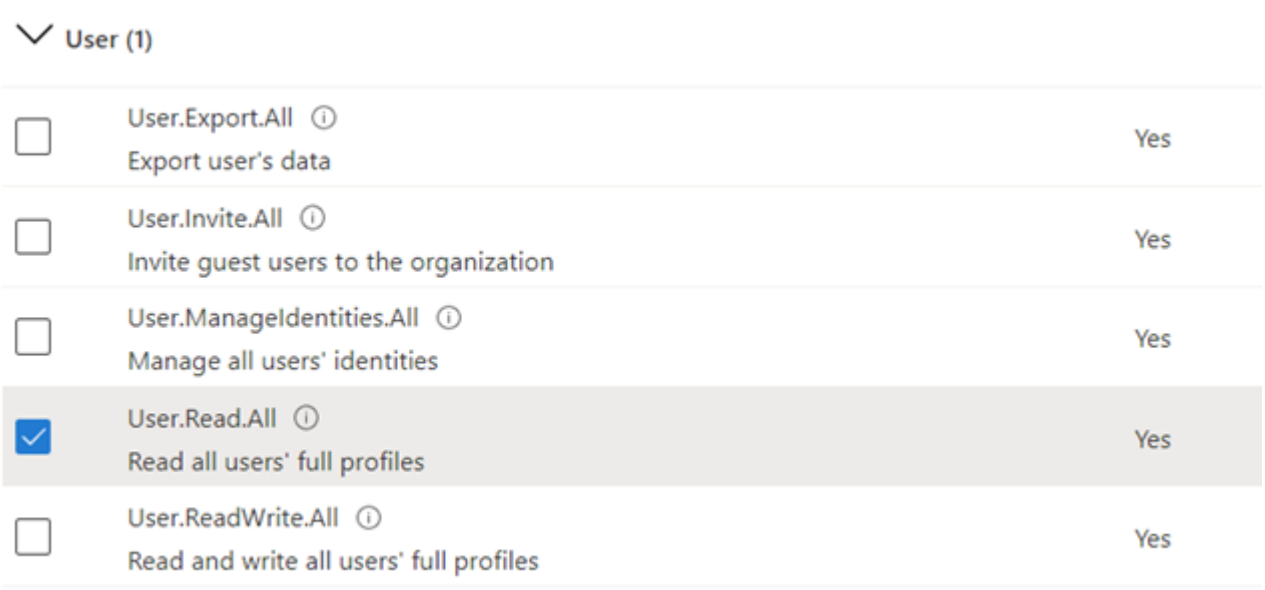
Calls

- Calls.AccessMedia.All
- Calls.JoinGroupCall.All



User

- User.Read.All



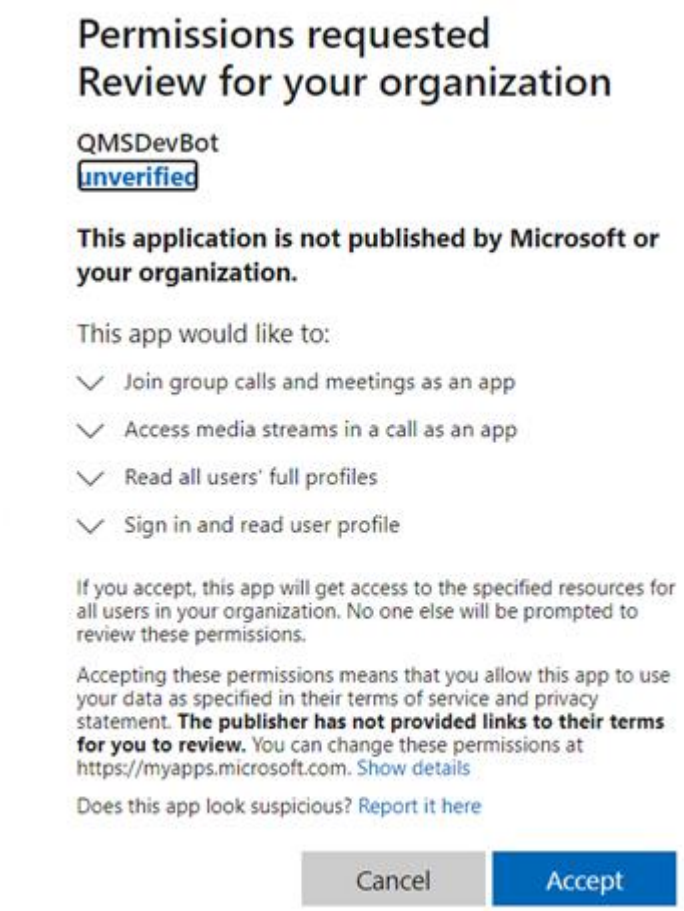
Once the permissions have been added to the bot (and any time in the future when changes may be made to the permissions granted), you will need to have a Teams Tenant admin accept the permissions. To do this you must go to a consent URL that is built using your Teams Tenant ID and the Application ID for the Teams Bot created above. The URL will take the form of:

https://login.microsoftonline.com/<TenantID>/adminconsent?client_id=<BotAppID>&state=12345&redirect_uri=https://www.enghouseinteractive.com/

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

- The TenantID should be your Microsoft Teams Tenant ID.
- The BotAppID should be the App Id from the Bot channel registration performed earlier.

Once you have the consent URL built, enter it into a Web browser, which will prompt you to login using your Teams Tenant admin user information, accept the permissions.



Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Configure Compliance Policy and Users

In order to configure Teams to automatically invite the QMS Recording Service bot into a Teams user's calls, we need to register the bot as an Application Instance with Teams. We also will need to create a compliance recording policy and assign the application instance to the policy. Finally we will need to assign the compliance recording policy to each Teams user that will be recorded by QMS. To do this we will need to execute some powershell commands using the credentials of a Teams tenant administrator.

Login to Powershell

Before you can execute any of the following commands you will need to import the MicorosoftTeams module into your powershell session.

- MicrosoftTeams module (https://docs.microsoft.com/en-us/microsoft-365/enterprise/manage-skype-for-business-online-with-microsoft-365-powershell?view=o365-worldwide)

From a server with the MicrosoftTeams module installed run the following in PowerShell and provide the credentials for the Teams tenant admin account:

Import-Module MicrosoftTeams
$credential = Get-Credential
Connect-MicrosoftTeams -Credential $credential

Create Application Instance

Once the Teams tenant admin account has been logged into the powershell session you can now run commands to manage the Teams environment. To create a new application instance you will run the following powershell command:

New-CsOnlineApplicationInstance -UserPrincipalname <UPN> -DisplayName "<DisplayName>" -ApplicationId <BotAppID>

- The UPN should be a unique name for the bot. For example if your recording server machine name is QMS-MAIN you could use, qms-main_RecordingBot@myteamsdomain.com
- The DisplayName should be something informative to describe the recording bot. For example if the recording server name is QMS-MAIN then DisplayName could be "QMS-MAIN Recording Bot"
- The BotAppID should be the App Id from the Azure Bot creation performed earlier.

Once the Application Instance has been registered the ObjectID for the application instance will be displayed in the powershell window. Save this ObjectID as you will need it later. If you need to retrieve the object ID later you can do so with the following powershell command:

Get-CsOnlineApplicationInstance | Where-Object {$_.DisplayName -eq "<DisplayName>"}

- The DisplayName should be the same as what was entered for the New-CsOnlineApplicationInstance above.

Next, we need to sync the application instance with the following powershell command:

Sync-CsOnlineApplicationInstance -ObjectId <ObjectID>

- The ObjectID should be the object ID that was returned after executing the New-CsOnlineApplicationInstance described above.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Create and Configure Compliance Recording Policy

Once the application is registered and synced we need to create a Compliance Recording Policy in Teams by executing the following powershell command:

New-CsTeamsComplianceRecordingPolicy -Tenant <TenantID> -Enabled $true -Description "<PolicyDesc>" -Identity "<PolicyName>"

- The TenantID should be your Microsoft Teams Tenant ID. (Note: this parameter has been removed in newer versions of the Microsoft Teams Powershell Module)
- The PolicyDesc should be something informative to describe the policy. For example, "QMS Native Recording for Teams".
- The PolicyName should be something informative to identify the policy. For example, "QMSTeamsComplianceRecording"

Once the compliance recording policy has been created, if we are setting up a non-HA QMS recording instance, we need to add the application instance to the policy by executing the following powershell command:

Set-CsTeamsComplianceRecordingPolicy -Tenant <TenantID> -Identity "<PolicyName>" -ComplianceRecordingApplications @(New-CsTeamsComplianceRecordingApplication -Tenant <TenantID> -Parent "<PolicyName>" -Id <ObjectID>)

- The TenantID should be your Microsoft Teams Tenant ID. (Note: this parameter has been removed in newer versions of the Microsoft Teams Powershell Module)
- The PolicyName should be the same value entered for the New-CsTeamsComplianceRecordingPolicy command described above.
- The ObjectID should be the object ID that was returned after executing the New-CsOnlineApplicationInstance described above.

If you are setting up a QMS HA pair of recorders you will first need to create a second bot and a second application instance for the second HA recorder. Once that is complete you will need to add both application instances to the policy by executing the following powershell command:

Set-CsTeamsComplianceRecordingPolicy -Tenant <TenantID> -Identity "<PolicyName>" -ComplianceRecordingApplications @(New-CsTeamsComplianceRecordingApplication -Tenant <TenantID> -Parent "<PolicyName>" -Id <ObjectID_1>), @(New-CsTeamsComplianceRecordingApplication -Tenant <TenantID> -Parent "<PolicyName>" -Id <ObjectID_2>)

- The TenantID should be your Microsoft Teams Tenant ID. (Note: this parameter has been removed in newer versions of the Microsoft Teams Powershell Module)
- The PolicyName should be the same value entered for the New-CsTeamsComplianceRecordingPolicy command described above.
- The ObjectID_1 should be the object ID that was returned after executing the New-CsOnlineApplicationInstance described above for the first recorder.
- The ObjectID_2 should be the object ID that was returned after executing the New-CsOnlineApplicationInstance described above for the second recorder.

You can verify that the compliance recording policy has been added and the current settings by executing the following powershell command:

Get-CsTeamsComplianceRecordingPolicy | Where-Object {$_.Identity –eq "Tag:<PolicyName>"}

- The PolicyName should be the same value entered for the New-CsTeamsComplianceRecordingPolicy command described above.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Once the application has been added to the compliance recording policy, we need to configure the compliance recording application. By default, a compliance recording policy requires the bot to answer and if for any reason the bot is unable to answer calls will fail. We change this behavior to not require the bot to answer before letting a call itself to connect by executing the following powershell command (Note: if you setting up a QMS HA pair of recorders you will run this command for each recorder using the corresponding ObjectID):

Set-CsTeamsComplianceRecordingApplication -Identity "<ApplicationIdentity>" -RequiredBeforeCallEstablishment $false -RequiredDuringCall $false -RequiredBeforeMeetingJoin $false -RequiredDuringMeeting $false

- The ApplicationIdentity is built based on the PolicyName and ObjectID from the previous commands and takes the form "Tag:<PolicyName>/<ObjectID>". For example, if your PolicyName is "QMSTeamsComplianceRecording" and your ObjectID is "dd833e27-c980-49eb-a4e8-9f72ca5bd954" then your ApplicationIdentity would be "Tag:QMSTeamsComplianceRecording/dd833e27-c980-49eb-a4e8-9f72ca5bd954"

Grant Compliance Recording Policy to Teams Users

After setting up the compliance recording policy, we now need to grant the policy to the Teams users that QMS will be monitoring. You can grant the recording policy to a single user by executing the following powershell command (can take several minutes to be applied):

Grant-CsTeamsComplianceRecordingPolicy -Identity <TeamsUserIdentity> -PolicyName "<PolicyName>"

- The TeamsUserIdentity should be the Teams user's Universal Principal Name, which by convention is typically the Office 365 username/email address. For example user@domain.com.
- The PolicyName should be the same value entered for the New-CsTeamsComplianceRecordingPolicy command described above.

You can also grant the policy to an entire department by executing the following powershell command (can take several minutes to be applied):

Get-CsOnlineUser -Filter {Department -eq "<DepartmentName>"} | Grant-CsTeamsComplianceRecordingPolicy -PolicyName <PolicyName>

- The DepartmentName

You can verify what users have been granted the compliance recording policy by executing the following powershell command:

Get-CsOnlineUser | Where-Object {$_.TeamsComplianceRecordingPolicy -like "<PolicyName>"} | Select UserPrincipalName

- The PolicyName should be the same value entered for the New-CsTeamsComplianceRecordingPolicy command described above.

You can revoke the policy from a single user by executing the following powershell command:

Grant-CsTeamsComplianceRecordingPolicy -Identity <TeamsUserIdentity> -PolicyName $null

- The TeamsUserIdentity should be the Teams user's Universal Principal Name, which by convention is typically the Office 365 username/email address. For example user@domain.com.

Disable And Enable Compliance Recording Policy

There is a known limitation with Teams where long delays in call setup for compliance recording Teams users can occur if all of the QMS Call Recording Services for the compliance policy have been shut down. The most common case for this would be during maintenance windows that occur during periods of time where live calls

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

are taken by compliance recording users. These delays can be avoided by temporarily disabling the compliance recording policy during outages.

You can disable the compliance recording policy as a whole by executing the following powershell command:

Set-CsTeamsComplianceRecordingPolicy -Identity <PolicyName> -Enabled $false

- The PolicyName should be the same value entered for the New-CsTeamsComplianceRecordingPolicy command described previously.

You can then re-enable the compliance recording policy by executing the following powershell command:

Set-CsTeamsComplianceRecordingPolicy -Identity <PolicyName> -Enabled $true

- The PolicyName should be the same value entered for the New-CsTeamsComplianceRecordingPolicy command described previously.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

QMS Configuration

QMS version 8.1 or greater is required.

To configure Quality Management Suite for recording Teams calls via Native Recording, complete the following steps.

1. From the computer running the Enghouse Interactive Data Service, open a web browser and access the URL http://localhost/qms. The Quality Management Login page displays.
2. Enter administrative credentials into the Username and Password fields and then click Login. The Quality Management interface displays.
3. Select Services under the Administration category on the right-side of the window. The Services tab displays.
4. Click Call Recording and click the Edit button. The CallRecording [host] tab displays.
5. Click the PBX Type drop-down under Service Details and select Microsoft Teams Native Recording.
6. Enter the fully qualified domain name of the server running the Call Recording Service into the FQDN of the Call Recording Service field.
7. Enter the public IP Address of the server running the Call Recording Service into the Public IP Address of the Call Recording Service field.
8. Enter the application ID for the Teams bot into the Teams Bot App ID field.
9. Enter the client secret for the Teams bot into the Teams Bot Client Secret field.
10. Enter your teams Tenant ID into the Microsoft Teams Tenant ID field.
11. Enter the thumbprint for the certificate used to secure the Teams communication into the Certificate Thumbprint field.
12. Enter the port to be used for Call Control into the Call Control Port field.
13. Enter the port to be used for Media into the Audio Port field.
14. Click the Save button in the Actions bar.
15. Click Users under the Administration category on the right-side of the window. The Users tab displays.
16. Configure all users that Quality Management Suite will be able to access and configure recorded calls.
17. The Microsoft Teams Username field in the Call Recording Settings section must match the Universal Principal Name for the user in Microsoft Teams, by convention this is typically the same as the Office 365 users user/e-mail name. For example, user@domain.com.
18. Click the Save button in the Actions bar.
19. Repeat steps 13-15 for each user to extension entry listed.

Firewall Configuration

The QMS Recording Service requires the following ports to be open to accommodate the Teams Native integration:

Port	Protocol	Description
8900	(TCP)	Inbound connections from Microsoft Teams for Teams Bot Media Control

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Port	Protocol	Description
8901	(TCP)	Inbound connections from Microsoft Teams for Teams Bot Call Control
3478-3481	(UDP)	Inbound and Outbound from/to Microsoft Teams for Teams Bot Media

Configuration File Settings

The following are Teams Native PBX-specific settings that can be added if necessary to the CallRecordingService.exe.config file, located in the QMS installation folder. All key names are case-sensitive.

EnableTeamsNativeRecordingStatusUpdate: Set to True to enable recording status updates. When enabled calls that are being recorded will indicate in the teams client that they are recording or an audio announcement will be played.

EnableMicrosoftGraphLogging: Set to True to enable enhanced logging from the Microsoft Graph API.

EnableMicrosoftMediaPlatformLogging: Set to True to enable enhanced logging from the Microsoft Media Platform.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Video Recording in Microsoft Teams

Video recording of video calls and video desktop sharing sessions in a Teams call are now supported by QMS. To do this you must first have the system licensed for Video recording and have the QMS user assigned a Video Recording license.

A video recording for a particular call will only take place if the audio portion of the call is also being recorded, either by being triggered by a Call Recording Profile or by the recording being demanded by a user. In the case of the audio call recording being triggered by a Call Recording Profile, the video recording will be controlled by assigning the user to a Video Recording Profile which, once the call audio has started to record, can be used to determine if the video should be recorded as well. In the case of the audio recording being demanded, if the user is licensed for video recording, the video recording will also be demanded.

Please be aware that recording video calls will require significantly more Media Processing resources than the normal QMS Screen Recording or Teams video desktop sharing session recordings. For deployments where recording of video calls will be deployed, please refer to the QMS Sizing spreadsheet for suggested server sizes and configurations.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Terms of use

Any software (“Software”) that is made available by Enghouse Interactive Inc. (“Enghouse”), together with any User Documentation (“User Documentation”) is the copyrighted work of Enghouse. Use of the Software is governed by the terms of a Master Purchase Agreement, End User License Agreement, or similar software license agreement ("License Agreement"). End users are not legally authorized to install any Software that is accompanied by or includes a License Agreement unless he or she first agrees to the License Agreement terms.

The Software is made available for installation solely for use by users according to the License Agreement. Any reproduction or redistribution of the Software not in accordance with the License Agreement is expressly prohibited by law and may result in severe civil and criminal penalties. Violators will be prosecuted to the maximum extent possible.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

THE SOFTWARE IS WARRANTED, IF AT ALL, ONLY ACCORDING TO THE TERMS OF THE LICENSE AGREEMENT. ENGHOUSE HEREBY DISCLAIMS ALL OTHER NON-EXPRESS WARRANTIES AND CONDITIONS WITH REGARD TO THE SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT.

Enghouse grants a nonexclusive license to customer for use of the User Documentation. The User Documentation contains copyrighted and other proprietary materials. By accepting the User Documentation, recipients agree that they will not transmit, reproduce, or make available to any external third-party this User Documentation or any information contained herein. Copying, reverse-engineering, or reselling any part of the Software or User Documentation is strictly prohibited.

The information contained in the User Documentation furnished by Enghouse is based on the most accurate information available at the time of printing. No representation or warranty is made by Enghouse as to the accuracy or completeness of such information or any ongoing obligation to update such information. Enghouse reserves the right to change the information contained in this document without notice.

Registered Trademarks

Syntellect®, Voiyager®, Continuum ®, MediaVoice®, Apropos®, Envox®, Envox® Activecall, Envox CT ADE®, Envox CT Connect®, Dynamic Application Discovery®, Interaction Vault® CT Impact®, SmartDialer®, SmartVoice®, SmartCollect®, SmartSupport®, Zeacom®, Enghouse Systems®

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

End User License Agreement

1. **Applicable Law; Definitions**. This End User License Agreement (“Agreement”), the definition of terms used, performance hereunder, and the interpretation of this Agreement shall be governed by and construed in accordance with the laws, other than the conflicts of laws rules, of the state of Arizona. If the Uniform Computer Information Transaction Act (“UCITA”) is enacted as part of the law of the state of Arizona, such statute will not govern any aspect of this Agreement, any license granted hereunder or any of the parties’ rights and obligations arising under this Agreement. "Confidential Information" means any non-public information or documentation provided by Supplier under this Agreement, including but not limited to Software, documentation, and information pertaining thereto. "End- User Customer" means the final licensor of Software who licenses for their use. "Agreement" means this document. "Software" means Supplier’s proprietary Software and any third party proprietary software components licensed to Customer pursuant to this Agreement. "Terms" means, collectively, the terms and conditions set forth below and on the front of this Agreement.
2. **Agreement**. This Agreement constitutes an acceptance of Customer’s offer to license Software contingent and consistent upon the Terms contained herein. Any terms or conditions proposed by Customer inconsistent with or in addition to the Terms shall be void and of no effect, unless specifically agreed to in a signed writing by an authorized Supplier representative. Payment for Software by Customer or furnishing of the Software by Supplier, in whole or in part, shall constitute a binding agreement on the Terms of this Agreement. The failure of Supplier to insist upon performance of this Agreement, to enforce any of the Terms of this Agreement or other purchase orders from Supplier, or to exercise any right or privilege granted to Supplier under this Agreement or under law, shall not be construed as a waiver and the same shall continue in full force and effect.
3. **License Grant**. Subject to Customer's compliance with the terms of this Agreement, Supplier grants to Customer a non-exclusive, non-transferable, perpetual license to install, use and execute the Software in object code form on a per-license basis consistent with the licensing scheme applicable to the type of software purchased on this Agreement at the location specified on the PSOF (“Software License”) as may be changed by Customer from time to time upon prior written notice to Supplier, such Software License limited to the site(s), number of seats, concurrent users, agents, servers, ports, devices, managed applications, and/or copies as applicable to the Software obtained, not to exceed the number of licenses set forth on PSOFs placed pursuant to this Agreement. The Software License shall become effective upon Delivery of the Software and shall remain in force unless terminated pursuant to Section 12 of this Agreement. This right does not include permission to grant sub-licenses or otherwise transfer such rights. The Customer may make one (1) copy of the Software for non-productive archival purposes only, provided that it retains or affixes the equivalent of Supplier's proprietary legend and copyrights to the copy. Additionally, the Customer may make several copies of the system documentation, excluding training manuals and materials, provided that they are for internal use only. Customer may not reverse engineer, disassemble or otherwise translate the Software provided pursuant to this Agreement. Supplier, or any third party that owns the Software License, retains exclusive title to and all rights to the Software. The Customer acknowledges that the Software and documentation are the property of Supplier and that the only right that the Customer obtains to the Software is the right of use in accordance with the terms of this Agreement. To assist Supplier in the performance of its duties under this Agreement and in the protection of its proprietary rights, Customer hereby authorizes a Supplier representative to enter Customer's premises, physically or electronically, and inspect the Software License at reasonable times with prior notice.
4. **Compliance with Laws**. Customer shall comply with all applicable laws, including, without limitation, the export control laws and regulations of the United States of America and those countries involved in transactions concerning the exporting of Software purchased under the terms and conditions or the control or regulation of the exportation of products or technical data supplied to Customer by Supplier. Customer will be responsible to pay all taxes, tariffs and duties. Customer shall comply with the United States Foreign Corrupt Practices Act and shall indemnify Supplier from Customer’s violations of

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

such Act. The United Nations Convention on the International Sale of Goods (CISG) is specifically excluded and shall not apply to any transaction contemplated herein.

5. **Limited Warranty**. Supplier warrants to Customer that Software will perform in every material respect according to the published specifications for a period of thirty (30) days from Delivery. However, neither Supplier nor its third-party supplier's warrant Software will meet Customer's requirements or that the Software operation will be uninterrupted or error-free. Remedies for Software defects reported during the warranty period consist of (and are limited to), at Supplier's option, repairing, replacing or refunding the purchase price of the Software. This warranty is contingent upon the proper use and application of the Software in accordance with Supplier's instructions. The warranty does not (i) cover the Software if modified by anyone other than Supplier; (ii) apply if Software warranty support is requested as a result of accident, neglect, or operating conditions exceeding specifications; (iii) cover malfunctions caused by defects in or incompatibility to Customer's computer system or equipment; (iv) cover malfunctions caused by defects in or arising from the installation, repair, or programming of the Software other than by Supplier; and (v) apply if Customer has rejected or not used any Software corrections, updates, or modifications supplied or made available by Supplier. THE WARRANTIES HEREIN DO NOT APPLY TO THIRD-PARTY SOFTWARE FURNISHED BY SUPPLIER UNDER THIS AGREEMENT, AND SUCH PRODUCTS ARE PROVIDED ON AN "AS IS" BASIS. AS APPLICABLE, SUPPLIER AGREES TO ASSIGN ANY WARRANTY IT MAY HAVE WITH RESPECT TO THIRD-PARTY SOFTWARE TO CUSTOMER, AND CUSTOMER AGREES TO PROCEED DIRECTLY AND EXCLUSIVELY AGAINST THE THIRD-PARTY SUPPLIER AS TO ANY CLAIMS OF WARRANTY. THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.
6. **Limitation of Liability**. SUPPLIER'S LIABILITY FOR DAMAGES FOR ANY CAUSE WHATSOEVER, AND REGARDLESS OF THE FORM OF ACTION, SHALL BE LIMITED TO, AT SUPPLIER'S OPTION, REPAIR OR REPLACEMENT OF THE DEFECTIVE SOFTWARE. IN NO EVENT WILL SUPPLIER BE LIABLE FOR DAMAGES IN EXCESS OF the fees paid PURSUANT TO AN ORDER THAT FORMS THE BASIS OF THE CLAIM. IN NO EVENT SHALL SUPPLIER BE LIABLE OR RESPONSIBLE FOR ANY REPROCUREMENT COSTS, LOSS OF PROFITS, LOSS OF USE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES OF ANY KIND, WHETHER IN AN ACTION OF CONTRACT OR TORT, EVEN IF ADVISED OF THE POSSIBILITY THEREOF. THIS LIMITATION OF LIABILITY AND EXCLUSION OF CERTAIN DAMAGES SHALL APPLY REGARDLESS OF THE SUCCESS OR EFFECTIVENESS OF OTHER REMEDIES. NO ACTION ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR ANY TRANSACTION HEREUNDER MAY BE BROUGHT AGAINST SUPPLIER MORE THAN TWELVE (12) MONTHS AFTER THE CAUSE OF ACTION HAS ARISEN.
7. **Relationship of the Parties**. Each party acknowledges that they are independent contractors, and that the relationship between Supplier and Customer is that of manufacturer/Customer. Neither party shall in any way represent or obligate the other party to any contract, term, or condition, nor may it represent the other party as agent, employee, franchisee, or in any other capacity. Customer is expressly prohibited from making representations to other third parties regarding Supplier or the Software and Services in excess of or contrary to representations contained in Supplier's or its third-party supplier's product specifications, brochures, newsletters, and other publications provided to Customer by Supplier. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute products which are functionally similar to the other party's products, so long as Confidential Information of the other party is not used in such development or distribution.
8. **Assignment**. Neither this Agreement nor any rights under it may be assigned by Customer without Supplier's prior written consent. Any unauthorized assignment by Customer shall be void. Supplier may assign the Agreement, in whole or in part, upon thirty (30) days' notice to the Customer.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

9. Severability. If a court of competent jurisdiction holds any provision in this Agreement to be invalid, void, or unenforceable, the remaining provisions will yet continue in full force without being impaired or invalidated in any way

10. **Notices**. Any notices given to Supplier may be made either by facsimile, overnight courier, hand delivery, or by registered or certified mail, postage prepaid with return receipt requested. Mailed notices shall be addressed to Supplier at the address appearing below, but Supplier may change such address by written notice in accordance with this paragraph. Notices mailed, or delivered personally or by electronic means will be deemed communicated as of actual receipt or the date of transmission, as applicable.

    Enghouse Interactive

    216 Route 17 North, Suite 301

    Rochelle Park, NJ 07662, United States

11. **Confidentiality**. The parties agree to accept in confidence all Confidential Information provided to them. The parties further agree not to use or disclose any Confidential Information supplied by the other except as required to perform their obligations in accordance with this Agreement. Any disclosure of Confidential Information to agents or employees shall be made only in the normal course of business, on a need-to-know basis, within the scope and purpose of this Agreement, and under written agreements requiring such agents or employees to treat all such information as strictly confidential. The parties agree not to use, publish, reproduce, disseminate, or otherwise disclose the other's proprietary or Confidential Information, including, but not limited to customer lists, without the prior written consent of the other.

    Customer shall not develop, manufacture, maintain, or, except as contemplated under this Agreement, market products or services incorporating Supplier's Confidential Information or Software. Customer agrees to include Supplier's proprietary notice on all copies of Supplier's Confidential Information made by Customer and to maintain records of the location of these copies.

    Customer agrees that the Software, and any proprietary and/or trade secret information and data furnished to Customer by Supplier or any of its third-party suppliers will be considered Confidential Information and subject to the provisions of this Section. Supplier reserves for itself all proprietary rights in all designs, engineering details, and other data pertaining to the Software and other proprietary data arising out of work done in connection with designing, manufacturing, servicing, and testing the Software, including the sole right to manufacture and, except as provided herein, market all such items. Customer shall not reverse, translate, disassemble, or decompile the Software or any component of the Software.

12. **Entire Agreement**. This Agreement is the entire agreement of the parties regarding the subject matter hereof, and supersedes and terminates any prior agreements, understandings or representations, written or oral, except with respect to any trade indebtedness owing between the parties.

Publish Date: Tuesday, January 23, 2024
UID: E20190902550988

Enghouse Interactive