pivot

MS Teams Integration – Full Deployment

Version: 2.0.3

Updated on: January 30, 2026

Introduction

The pivot Microsoft Teams integration combines MTR health data from the Graph API along with device data for single pane visibility into MTR meeting room health.

This guide will walk you through the process of enabling monitoring data to flow from Microsoft to pivot.

If any questions arise, please do not hesitate to reach out to your pivot Integration Specialist or to contact support@pivotnow.io

Purpose

This section provides step -by-step instructions to:

- Create and configure Microsoft Teams Rooms (MTR) accounts
- Register MTR devices in the Teams Rooms Pro Management Portal
- Deploy Azure Arc to MTR devices
- Add device as resource under Data Collection Rules (DCR) for monitoring
- Connect your Azure Arc to pivot

Prerequisites

- Microsoft 365 Admin access
- Teams Admin Center access
- Teams Rooms Pro licenses available
- Azure Global Administrator (GA) credentials
- Physical or remote access to the MTR device
- Admin credentials for the MTR device
- Azure subscription with permissions to:
    - Create Azure Arc resources
    - Assign Resource Groups
    - Create Data Collection Rules
- pivot Client Admin Account

MTR Account Creation and Registration

Step 1: Create MTR Accounts

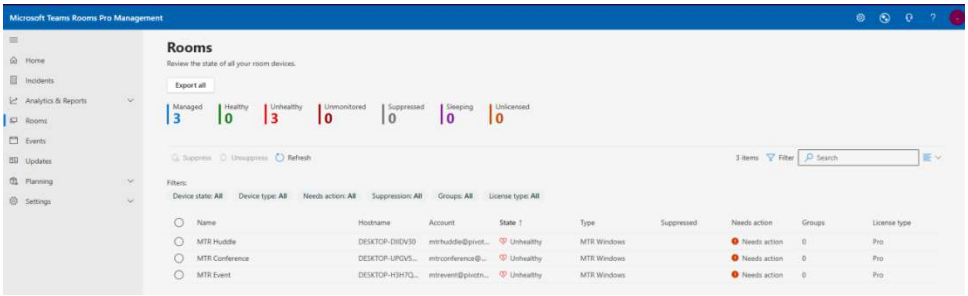
- Log in to the Microsoft 365 Admin Center
- Navigate to Admin Center → Resources → Rooms & Equipment
- Create the required MTR room accounts.

Step 2: Assign Licenses and Group Membership

- Navigate to Active Users
- Locate the automatically created MTR account
- Add each account to the MTR End points group
- Assign a Microsoft Teams Rooms Pro license to each account (if applicable)

Step 3: Register the MTR Device

- Log in to the physical MTR device using the newly created room account.
- Verify Device Registration back on the Teams Admin Center:
  - Go to the Teams Admin Center
  - Teams Devices → Teams Rooms Pro Management Portal
  - Confirm the device appears under Rooms



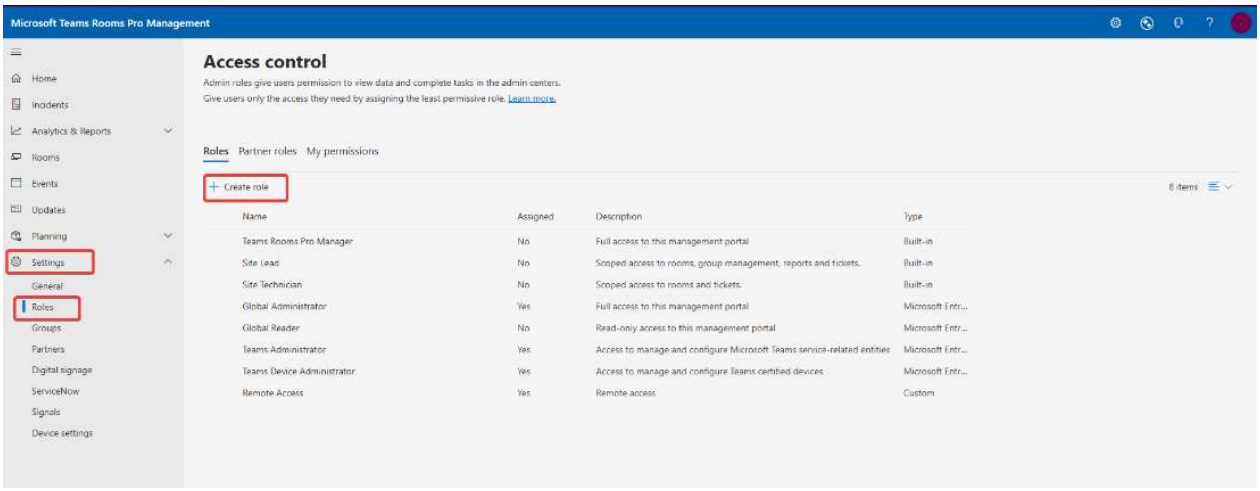
Step 4: Azure Arc Deployment and Data Collection Rule Configuration

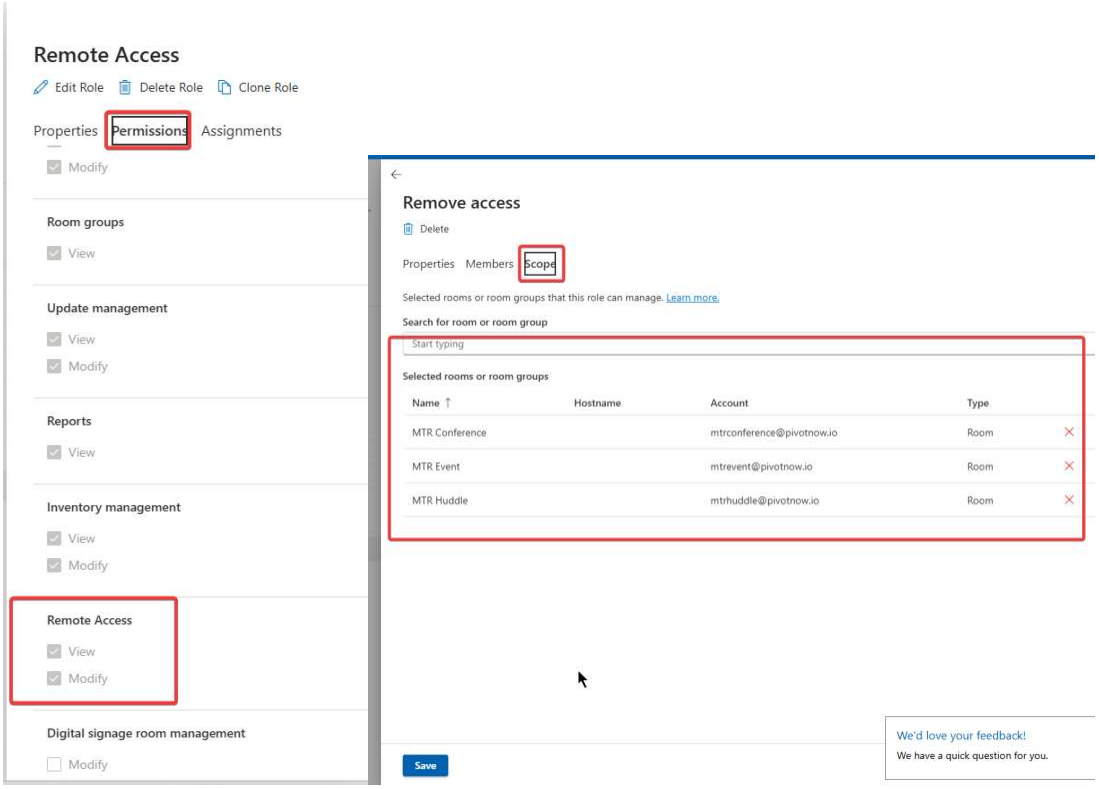
- Enable Remote Access
- Open the Microsoft Teams Rooms Pro Management Portal
- Enable Remote Access for the target MTR devices

Step 5: Create Custom Role for Remote Access (skip if you already have role applicable)

- In the Teams Rooms Pro Management Portal, create a Custom Role
- Ensure the role includes Remote Access permissions

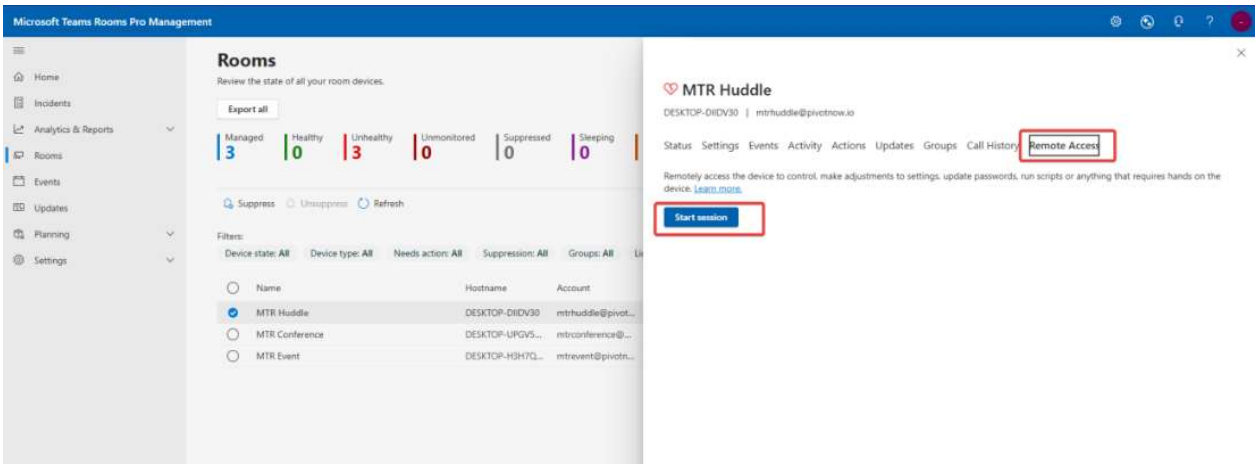
- Under Role Assignment, create assignment, under member add GA account and under scope add the target MTR devices



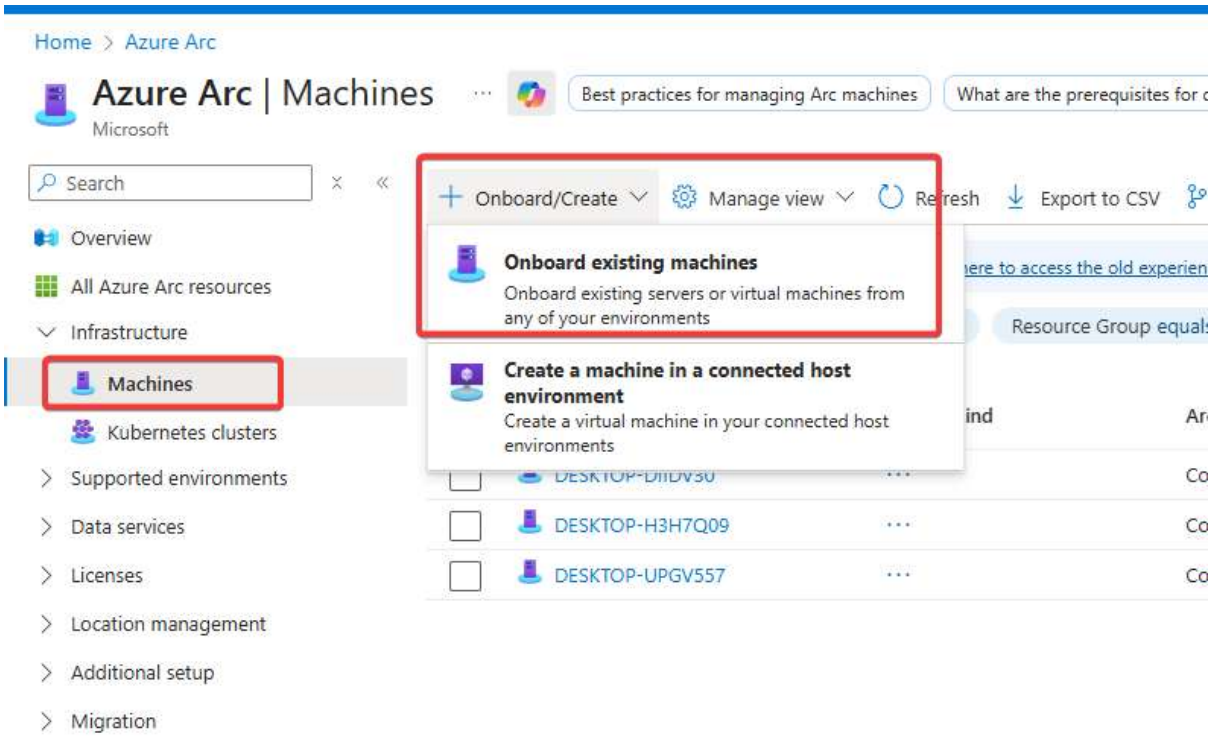


Step 6: Start Remote Session to the MTR Device

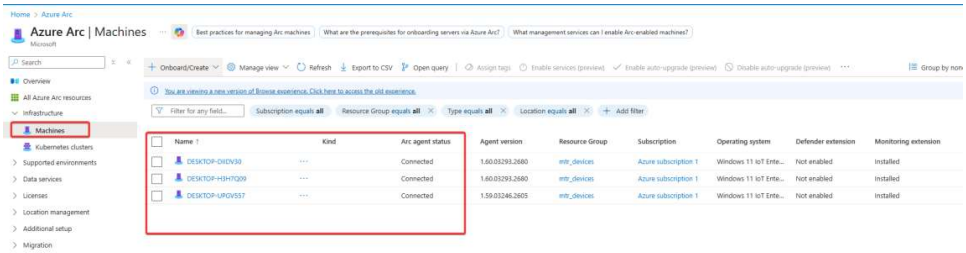
- Navigate to Microsoft Teams Rooms Pro Management → Rooms
- Select the target device
- Click Remote Session → Start Session



- Once connected remotely click Settings
- Enter the device's admin credentials
- Navigate to Windows Security → Sign in with Admin Account
- The device will boot to the Windows desktop
- (Optional – Create and Download scripts prior on Admin's PC, then transfer scripts to each MTR to save time and purge credentials)
- Open Microsoft Edge on the MTR device
- Navigate to the Azure Portal
- Log in using Global Administrator (GA) credentials
- Go to: Azure Arc → Machines → Add → Onboard Existing Machine



- Select the appropriate:
  - Resource Group
  - Azure Region
- Click Download and Run Script
- Open PowerShell as Administrator on the MTR device
- Run the downloaded onboarding script
- Confirm the script completes successfully
- Reboot and Verify:
  - Reboot the MTR device (It takes about 3 minutes to come back online)
  - In the Azure Porta navigate to Azure Arc → Machines
  - Confirm the device is listed and connected.



- Adding MT device as resource to Data Collection Rule (DCR) (Optional : if the device doesn't shows up under DCR -> Resources . This would have taken care by default Azure policy)

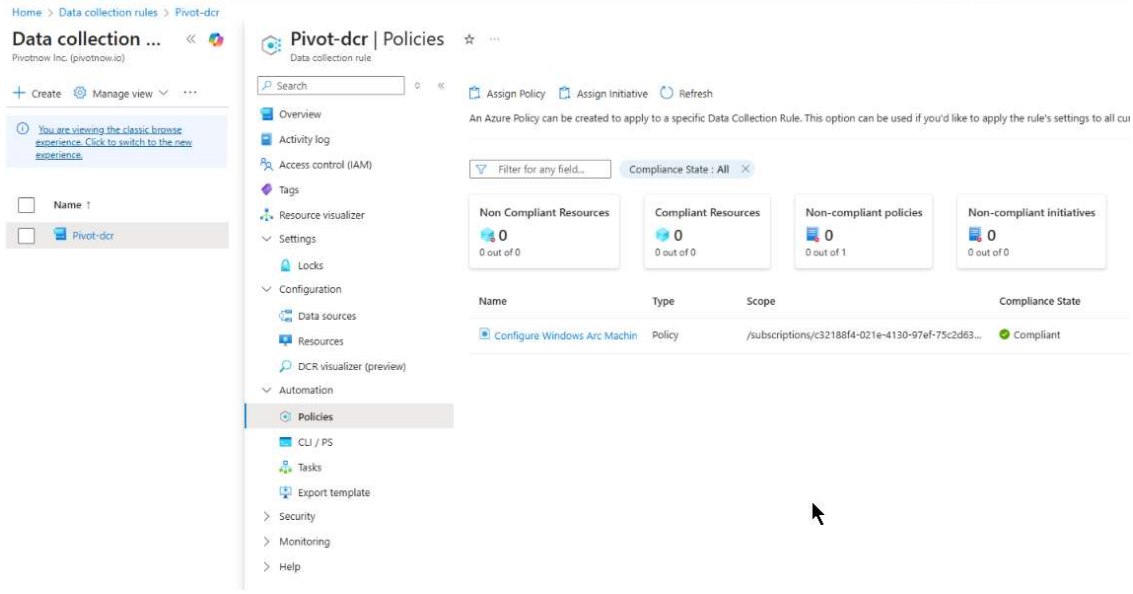
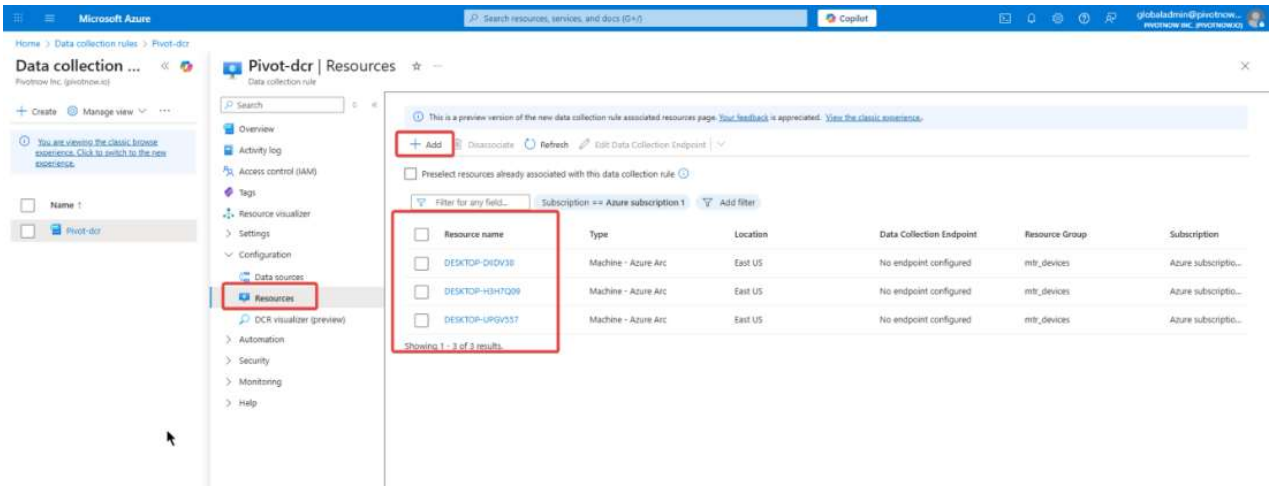


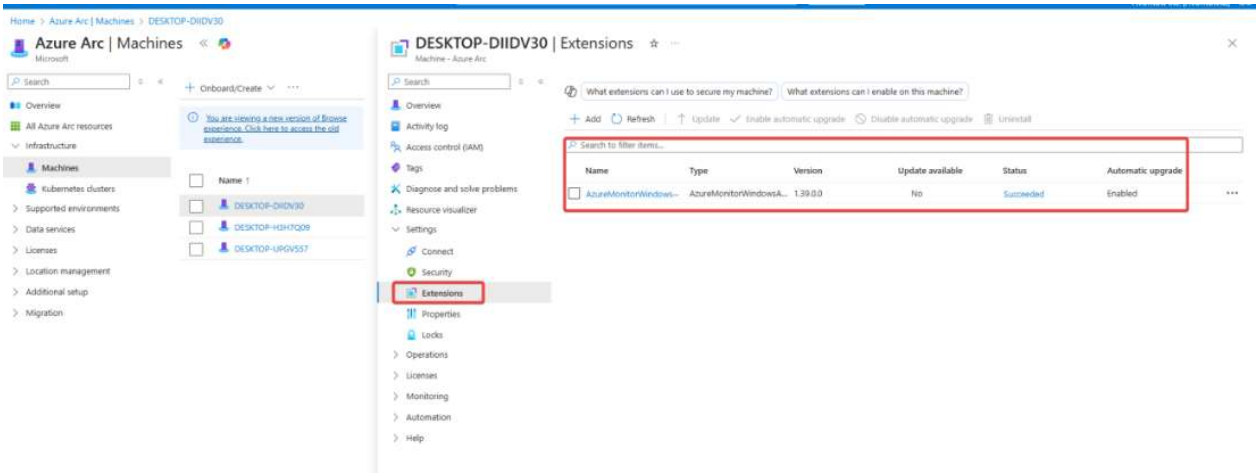
Figure 1 - Screenshot above shows the policy assigned to DCR, it checks for devices under Azure Arc -> Machines and adds them as resource to Pivot-dcr data collection rule

Step 7: Add Device to Data Collection Rule resources manually.

- In the Azure Portal, navigate to Monitor → Data Collection Rules
- Select the appropriate DCR
- Add the Azure Arc–enabled MTR device under Resources .

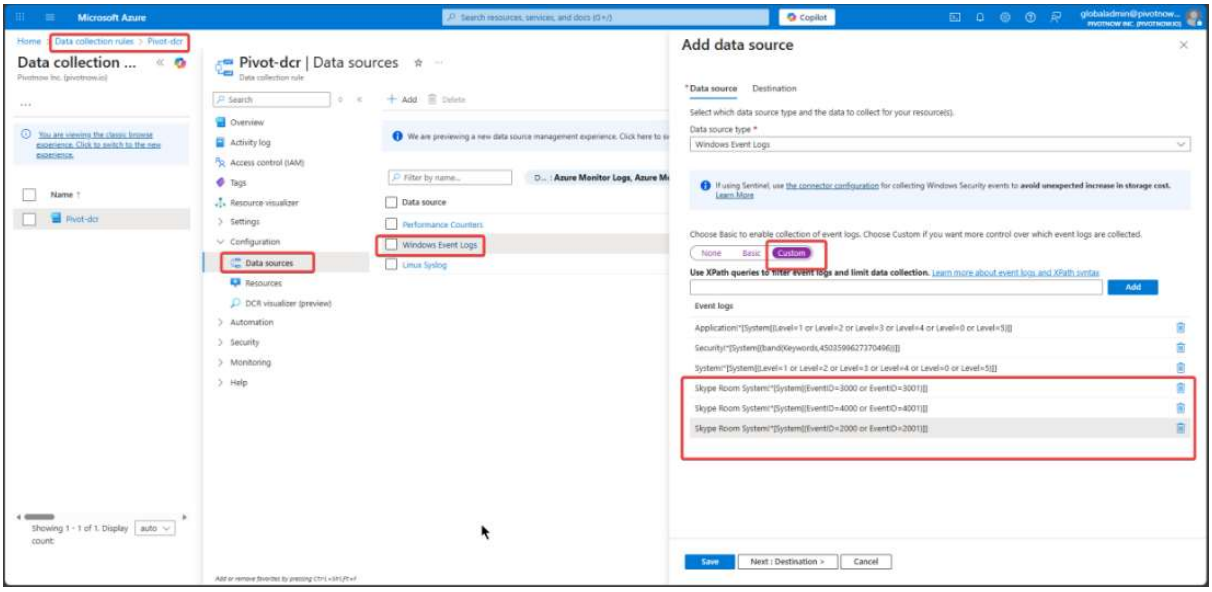


- Once added, the Azure Monitoring Agent (AMA) extension is deployed automatically.
- To confirm:
  - Go to Azure Arc → Machines
  - Select the MTR device
  - Navigate to Extensions
  - Verify the Azure Monitoring Agent is installed

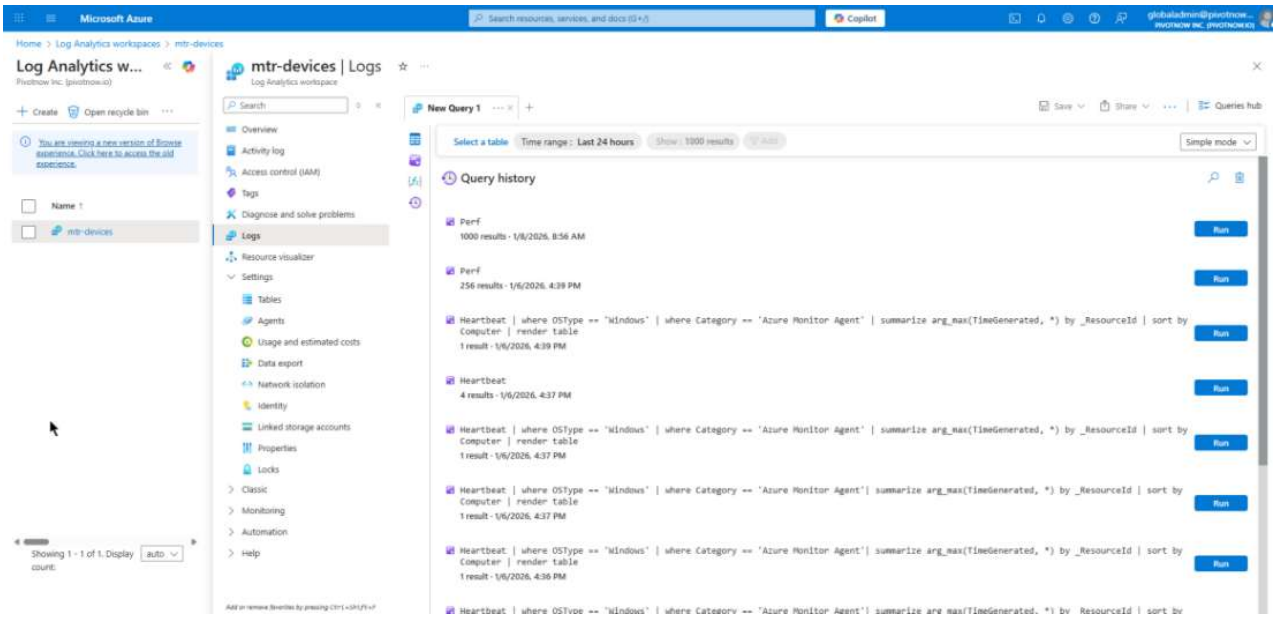


Step 8: Custom Event ID reporting on Data collection Rule

- Go to Data Collection Rule
- Data Sources -> Windows Even logs -> Custom
- Add the following event IDs:
  Skype Room System!*[System[(EventID=3000 or EventID=3001)]]
  Skype Room System!*[System[(EventID=4000 or EventID=4001)]]
  Skype Room System!*[System[(EventID=2000 or EventID=2001)]]



- To confirm data ingest, check the Log Analytics to confirm that data is flowing into the platform.



Connecting Azure Arc to pivot

This next section will be outlining the connection being made between the Azure Arc instance you have created, and pivot.

What permissions are required for this integration

- Place.Read.All – Read all the places (Rooms)
- TeamworkDevice.Read.All – MTR health status

What data is utilized

- Rooms
  - ID
  - Email
- Devices
  - IP
  - MAC
  - Serial
  - Firmware (OS & Application)
  - Health Statuses

Note: Data synced may be periodically updated to enhance monitoring and incident workflows.

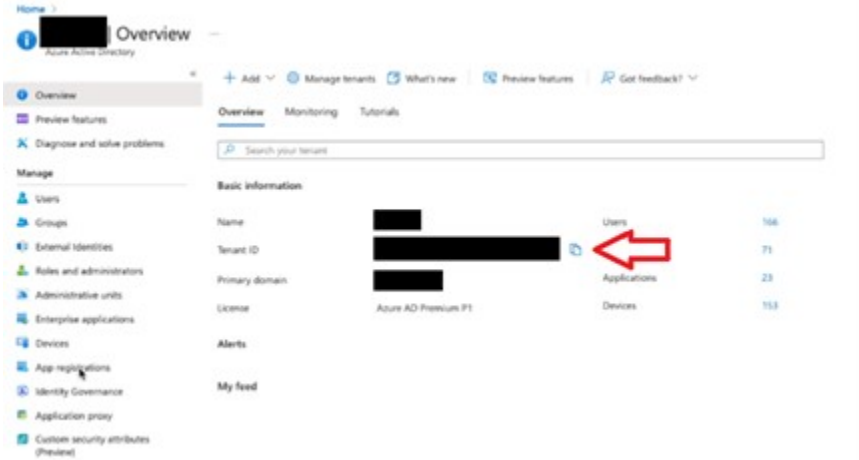
Setup Walkthrough

Step 1: Gather the Tenant ID and authenticate the Microsoft-pivot Integration

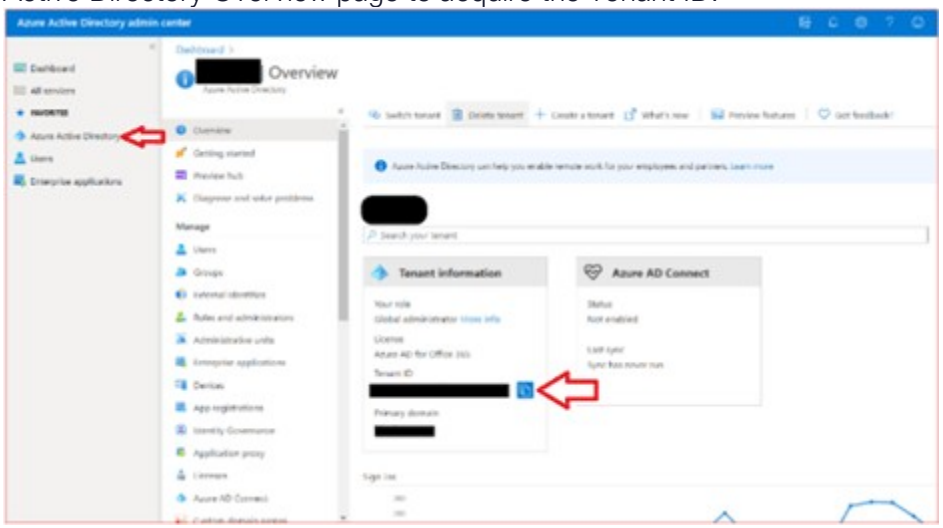
Acquire Tenant ID - MS Teams Admin Permission Requirements

- In order to begin the MS Teams integration, the user will first be required to input the Tenant ID of the Teams organization. The Tenant ID can be found in one of two ways:

- Retrieve from: Microsoft Azure Portal → Azure Active Directory → Overview when logging in as an Administrator.



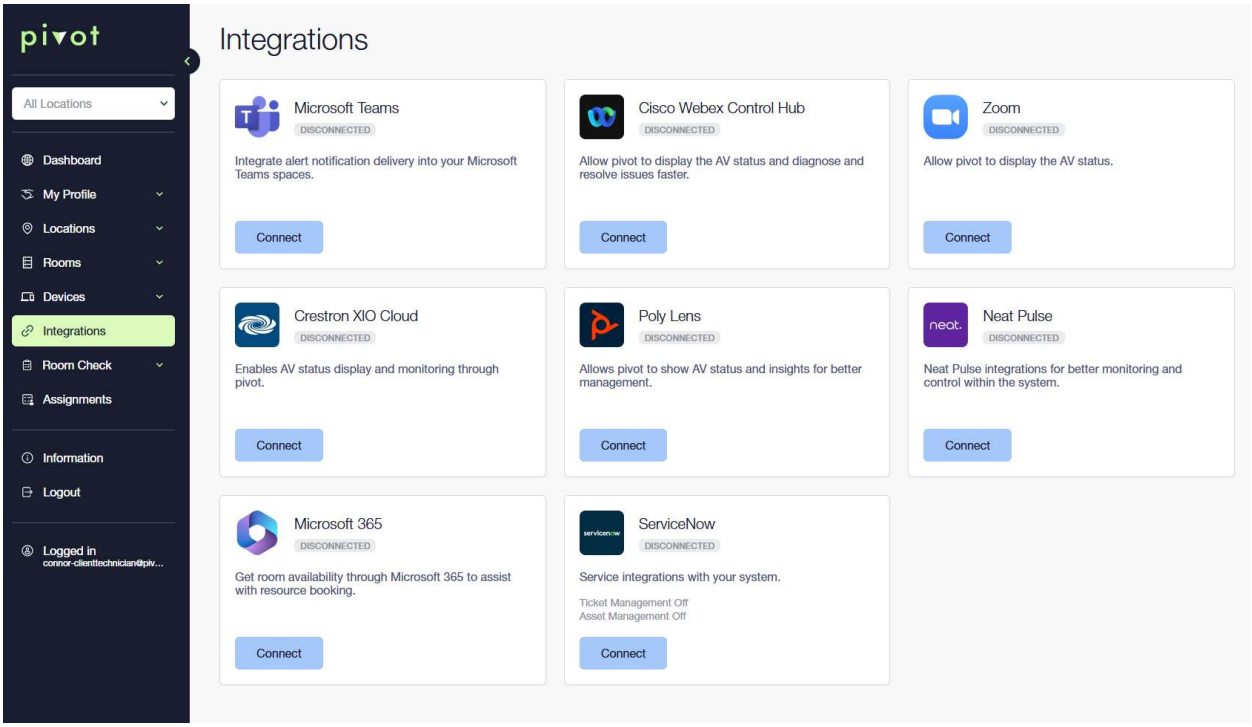
- Alternatively, log into the Microsoft 365 Admin Portal and navigate to the Azure Active Directory Overview page to acquire the Tenant ID.



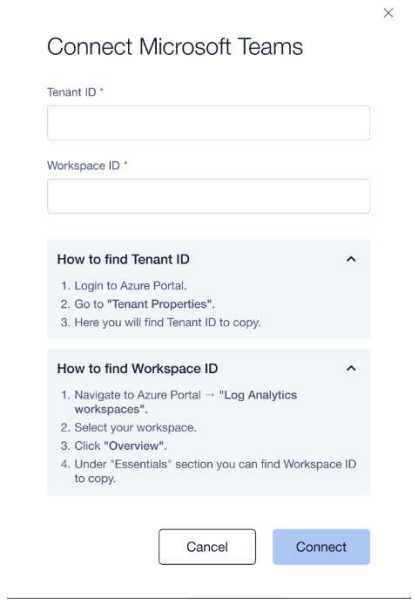
- Using the Tenant ID, pivot can then send a request to the organizations' admin, prompting a consent request later in this process.

Step 2: Integrating MS Teams into pivot

- Once logged into app.pivotnow.io navigate to the integrations tab and select "Connect" under Microsoft Teams.

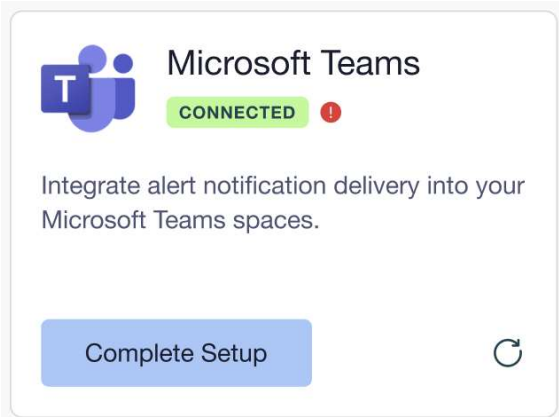


- Input the Tenant ID and Workspace ID

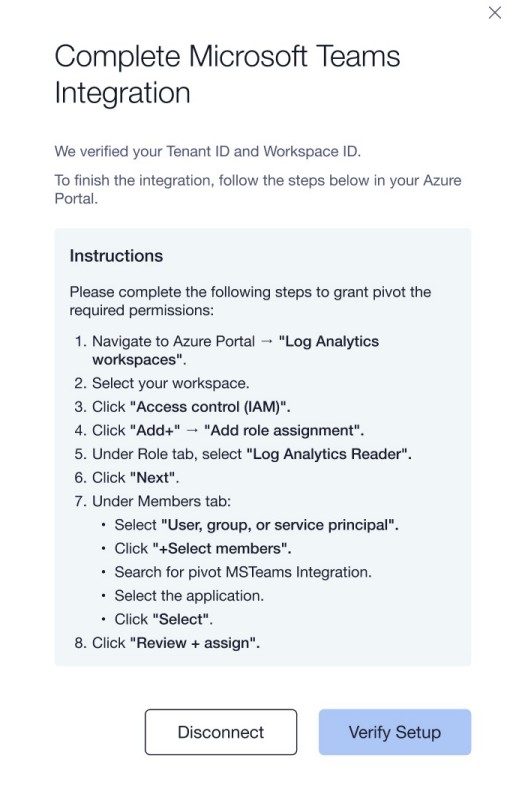


- This will redirect to Microsoft to log in with your organizations' admin account and be prompted to give consent so that call records can be monitored.

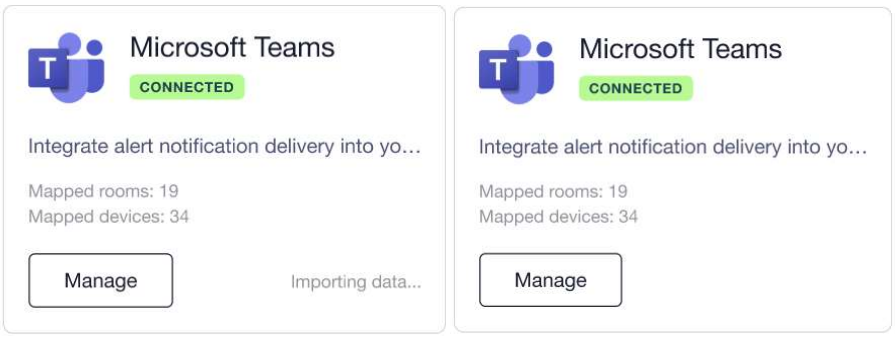
- Selecting “Accept” will redirect the page back to pivotnow.io to continue the integration.
- It will then redirect to the Integrations page, with the Microsoft Teams integration card showing as Connected, and “Connect” button as “Manage”



- Once this is set, you will need to review and assign the member added to your Azure Portal. You will need to add the “Log Analytics Reader“ Role to the pivot Application Added to your tenant.



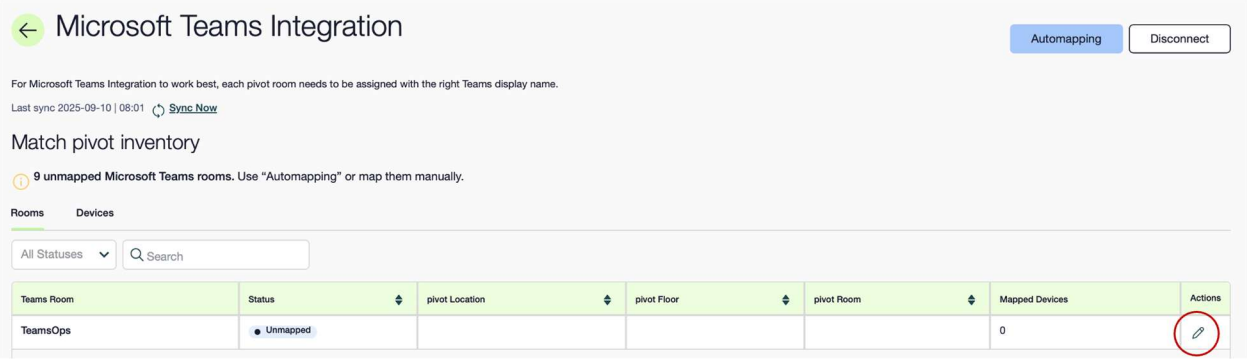
- Once the “Review + assign” is complete, click the “Verify Setup“ button.
- When the connection is established importing of the data process (pulling of the initial list and caching it in the database, automapping of the devices) will start. Importing data... label will indicate it, and once down, will disappear.



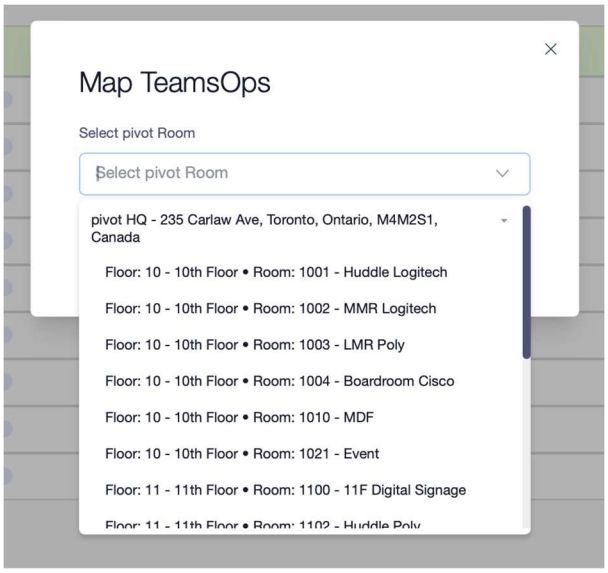
- Once down importing, you will likely have 0 mapped rooms and devices, as this will be a fresh integration, so let's move onto Step 3: Mapping your Rooms/Devices

Step 3: Mapping your Rooms/Devices

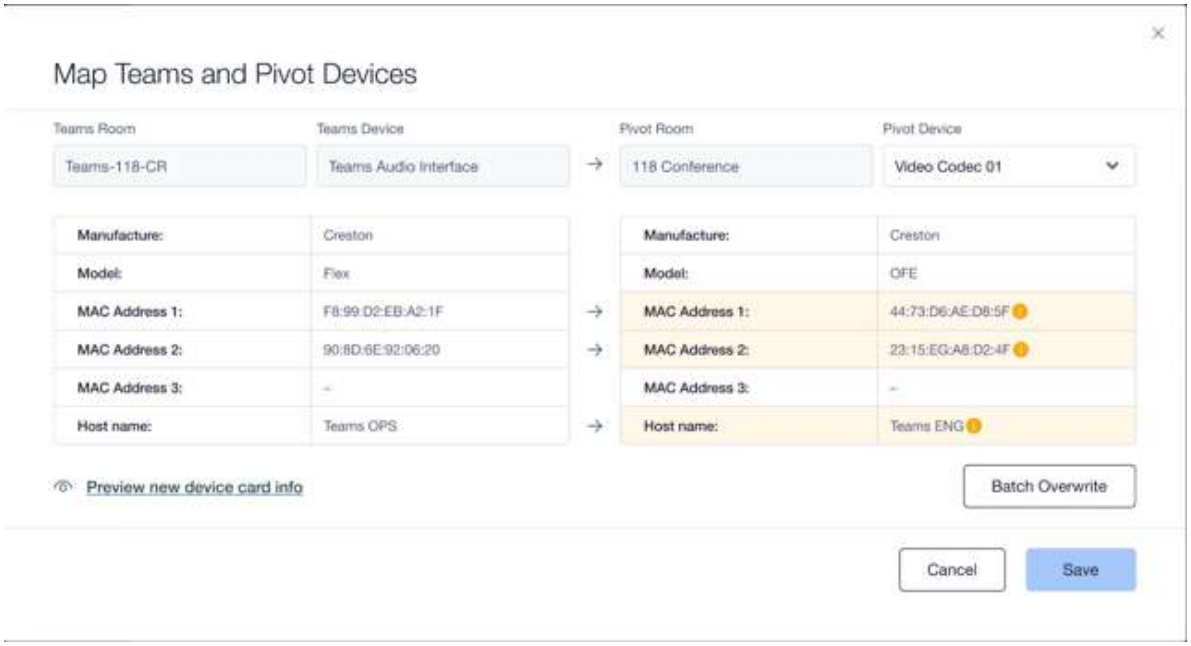
- On the Integration Page, Select the "Manage" Button on the Integration Card. On the "Match pivot Inventory" page select the edit button on the row of the MTR room to map.



- From the dropdown, Select the room to map



- Select the  icon to map devices in the room
- Map the MTR reporting device to the Device Type in the room.



- Integration setup is now complete. To verify data is flowing, go to the meeting room, click on the device card to view the live monitoring data.

Understand Pricing

Enabling Azure Monitor is a chargeable service billed by Microsoft on top of any pivot licensing. The following table provides an estimate of the Azure cost base on 100 reporting MTRs using the pivot recommended DCR. This calculation is provided as an estimate and should be confirmed and monitored by each client.

Plan	Estimated Data/MTR/Day	Estimated Billing per 100 MTR/Month
Pay-As-You-Go $2.76/GB https://azure.microsoft.com/en-us/pricing/details/monitor/	X MB	$X.XX

Performance counters are collected every minute from the resource — see [Collect performance counters with Azure Monitor Agent - Azure Monitor | Microsoft Learn]

Estimated volume:

Based on our earlier calculation, one server collecting 10 performance counters at a 1-minute interval generates approximately **60 MB per month**.

Azure Monitor ingestion rate:

For Arc-enabled servers, the "Azure Monitor Analytics Logs" ingestion rate is **US$ 2.76 per GB** (Analytics Logs plan). See [Pricing – Azure Arc | Microsoft Azure]

These services are billed on a per GB ingested basis.

Management and Security Service for Azure Arc-enabled servers	Rate
Azure Monitor Analytics Logs	$2.76/GB
Azure Monitor SCOM Managed Instance	$6/month
Microsoft Sentinel	$5.22/GB-ingested