



# **MICROSOFT PERFORMANCE DATA IN VANTAGE DX ANALYTICS**

## **REFERENCE GUIDE**

RELEASE 3.20

DOCUMENT DATE: FEBRUARY 20, 2025

## **NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Martello Technologies Corporation. The information is subject to change without notice and should not be construed in any way as a commitment by Martello Technologies or any of its affiliates or subsidiaries. Martello Technologies and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Martello Technologies.

## **Trademarks**

MarWatch™, Savision, Martello Technologies, GSX, and the Martello Technologies logo are trademarks of Martello Technologies Corporation.

Windows and Microsoft are trademarks of Microsoft Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

© Copyright 2025, Martello Technologies Corporation  
All rights reserved

Microsoft Performance Data in Vantage DX Analytics  
Release 3.13 - February 20, 2025

# Contents

## CHAPTER 1

Introduction .....	8
Document Purpose and Intended Audience .....	8
Revision History .....	8

## CHAPTER 2

Integrate Data from your Microsoft Tenant .....	9
Install the Microsoft CQD Integration .....	9
Install the Microsoft 365 Integration .....	15
Configure Meeting Room Data .....	17

## CHAPTER 3

Components .....	20
Microsoft CQD Components .....	20
Components and Health State Calculations .....	20
Configuration Options .....	29
Microsoft 365 Components .....	30
Vantage DX Monitoring Components .....	31

## CHAPTER 4

Alerts and Thresholds .....	35
Microsoft CQD .....	35
Microsoft 365 .....	37
Vantage DX Monitoring Alerts .....	37
Microsoft Entra Connect Thresholds .....	40
ADFS Thresholds .....	40
Exchange DAG Thresholds .....	41
Exchange Advanced Free/Busy Thresholds .....	41
Exchange Edge Thresholds .....	42
Exchange Mailbox Server Thresholds .....	43
Client Access Thresholds .....	43
Database Thresholds .....	43
Lagged Copies Thresholds .....	44
System Thresholds .....	44
Transport Thresholds .....	46
Exchange MAPI Thresholds .....	47

Microsoft Exchange Thresholds .....	47
Exchange OWA Thresholds .....	49
Hybrid Mail Routing Thresholds .....	50
Internal Mail Routing Thresholds .....	51
Microsoft 365 Health Thresholds .....	51
Office 365 Web App Thresholds .....	52
OneDrive Thresholds .....	52
Roundtrip Mail Routing Thresholds .....	53
SharePoint Page Thresholds .....	54
SMTP Gateways Thresholds .....	54
Teams Thresholds .....	55
Teams Advanced Thresholds .....	55
Teams Video Thresholds .....	56
URL Thresholds .....	57

## CHAPTER 5

Searching for Data .....	58
Pre-Defined Teams Searches .....	58
Custom Searches .....	59
Users .....	60
View the Experience of a Specific User .....	60
View the Experience of a Multiple Users .....	60
Identify Users with Low MOS .....	60
View Meetings with Poor Call Quality Attended by Specific Users .....	60
View User Devices by Operating System .....	60
VIP Meeting Organizers .....	60
Meetings with Poor Call Quality for Specified Users .....	61
View Users in a Specific Department .....	61
User Devices with Poor Forward Metrics on Wired connections .....	61
WiFi Users with High Jitter (Forward and Reverse) .....	61
WiFi Users High RTT (Forward and Reverse) .....	61
WiFi Users High Packet Loss (Forward and Reverse) .....	61
Wired Users High Jitter (Forward and Reverse) .....	62
Wired Users High RTT (Forward and Reverse) .....	62
Wired Users High Packet Loss .....	62
Users who Rated a Call with Low Score .....	62
Users or Endpoints that Rated a Call with Low Score .....	62
Connection Type .....	62
Devices .....	63
Devices Experiencing High Latency and Jitter .....	63

---

Audio Devices with Low Average MOS .....	63
Headsets that are Not Certified Brands .....	63
Locations .....	63
Locations with a High Number of Poor Calls .....	63
Cities and Countries with a High Volume of Calls .....	63
Offices with High Call Volume .....	64
Offices By Name .....	64
Geographical Regions .....	64
ISPs .....	65
General Data Related to an ISP .....	65
ISP and Call Volume .....	65
ISPs and Meetings with Poor Call Quality .....	65
ISPs with High RTT .....	65
ISPs with High Jitter .....	65
ISPs with High Packet Loss .....	66
ISP and average MOS .....	66
Meetings .....	66
User Devices Connected to Poor Meetings through a Specified ISP .....	66
Large Meetings where a Specified Number of Users had Poor Calls .....	66
Large Meetings .....	66
Meetings with Poor RTT .....	67
Meetings with Jitter .....	67
Meetings with Packet Loss .....	67
Meetings with a Low Video Frame Rate .....	67
Meetings with Video Frame Loss .....	67
Meetings with Alerts .....	67
Meetings with Alerts, by Country .....	67
All Meetings .....	67
Meeting Organized or Attended by a User .....	67
Meetings that Occurred at a Specific Date or Time .....	68
Meeting Rooms .....	68
Find Meeting Room Devices .....	68
Search Based on Device Properties .....	68
Search for Disconnected Peripherals .....	70
Meeting Rooms and IP Phones with Outdated Software .....	70
Call Quality Metrics and Connection Type .....	71
Number of Dropped Streams by City .....	71
Number of Dropped Streams by ISP .....	71
Number of Dropped Streams by City and Country .....	71
Number of Dropped Streams by ISP and Number of Devices .....	71
ISPs with Round Trip Time as the Top Issue .....	71

ISPs with Jitter as the Top Issue .....	72
ISPs with Packet Loss as the Top Issue .....	72
TCP Calls .....	72
Video Calls .....	72
Video as Poor Call Reason .....	72
Video Errors in a Specified Country .....	72
Video Errors in a Specified City .....	72
Video Errors in Peer-to-Peer Calls .....	73
Video Errors in Conference Calls .....	73
Video Errors and Poor WiFi Signal Strength .....	73
Video Based Screen Sharing (VBSS ) with a Low Video Frame Rate .....	73
Video Error with Frame Loss .....	73
PSTN Calls .....	73
Groups or Users Involved in PSTN Calls Greater than 60 Minutes .....	73
Direct Routing Calls in Specified Countries .....	74
PSTN Trunk with Failed Calls .....	74
PSTN Trunk with Poor Calls .....	74
Find the Poor Call Reasons on all PSTN calls .....	74
Microsoft 365 Services and Workloads .....	74
Service Health—All Services .....	74
Services with Performance Issues .....	74
Services with Correction Action in Progress .....	74
Services Operating Normally .....	74
Availability History of Services .....	75
Workloads Tested by Vantage DX Monitoring .....	75
Microsoft 365 Licenses .....	75
All Microsoft 365 Licenses .....	75
Specific Microsoft 365 Licenses .....	75
Available Licenses .....	76
Service Plans .....	76

## CHAPTER 6

Call Quality Metrics .....	77
----------------------------	----

## APPENDIX A

Microsoft Raw Properties .....	79
Users and Devices .....	80
Call Types .....	87
Locations .....	94
Network Information .....	100

---

Call Conditions .....	106
PSTN-Connected Calls .....	112
Meeting Rooms .....	116
Meeting Room Devices .....	118
Subscriptions .....	118
Licenses .....	118
Services .....	119

## APPENDIX B

Tell Us How We Did .....	120
--------------------------	-----



# Introduction

## Document Purpose and Intended Audience

Welcome to the *Microsoft Performance Data in Vantage DX* Reference Guide.

This document provides information about the Microsoft data available in Vantage DX deployments that include the following integrations:

- Microsoft Call Quality Dashboard (CQD)
- Microsoft 365
- Vantage DX Monitoring

The guide describes the Microsoft performance data that is available in the Vantage DX Analytics interface.

The information available depends on your license package. This guide may contain information about functionality that is not available in your deployment.

This guide is intended for use by system administrators and IT managers.

## Revision History

Document Date	Description
February 20, 2025	Microsoft Performance Data in Vantage DX Analytics Release 3.13

# Integrate Data from your Microsoft Tenant

Use the information in this section to begin monitoring the call quality that your Teams users are experiencing, as well as the health state of your Microsoft services. Complete the setup tasks listed in the following table.

Task	Description
<a href="#">"Install the Microsoft CQD Integration" on page 9</a>	Configure the integration between the Microsoft CQD and VDX Analytics. This integration allows you monitor call quality data about your users in near-real time.
<a href="#">"Install the Microsoft 365 Integration" on page 15</a>	Configure the integration between your Microsoft 365 subscription and VDX Analytics. This integration allows you to monitor the health state of your Microsoft services, including the status of licenses.
<a href="#">"Configure Meeting Room Data" on page 17</a>	Optional. If you have meeting rooms and devices configured in the Microsoft Teams admin portal, we recommend that you create a rule in VDX Analytics that consolidates the meeting room data from Microsoft 365 with the usage data from the Microsoft Teams CQD.

## Install the Microsoft CQD Integration

Use this procedure to integrate the Microsoft Call Quality Dashboard (CQD) with VDX Analytics.

### Before you Begin


Log into the Microsoft Call Quality dashboard through the Office 365 portal and verify that the CQD is activated and accessible.

1. From the main menu, select **Settings**.  
The Integrations tab displays the currently installed integrations.
2. Click the **Add** button at the bottom of the page.
3. Select a monitoring system from the dialog box.
4. Enter the information required for the monitoring system.
5. Click **Save**.

Configure the following properties when you integrate the Microsoft Teams CQD with VDX Analytics to monitor remote users:

Property	Description
<b>Set-up</b>	
Integration Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
<b>Credentials</b>	
Azure Login Name	The Microsoft 365 account that VDX Analytics can use to access the CQD.
Azure Login Password	The password for the Microsoft 365 account.
MFA Shared Secret (Optional)	<p>The optional shared secret is used for multi-factor authentication for Azure Active Directory. To use this option, the account that VDX Analytics uses to connect to your Microsoft CQD must use Azure MFA with a passive authentication flow. In addition, the account must be cloud-native.</p> <p>To generate the password for this field, see the following Knowledge Base article:</p> <p><a href="https://helpcenter.martellotech.com/s/article/000001082">https://helpcenter.martellotech.com/s/article/000001082</a></p>
Leverage Martello VDX Enterprise App	This option is enabled by default. We recommend that you do not change the setting. It allows the integration to use the permissions that you granted to the Martello VDX App when you first registered it.
<b>Data Processing</b>	

Property	Description
Tenant Size	Select the tenant size based on the number of users, or select Custom to provide an alternate value. The selected tenant size sets the defaults for the rest of the data processing values.
Data Retrieval Period	The number of days of data from the CQD to display in VDX Analytics. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Max Data Query Time (minutes)	The maximum time in minutes allowed for a single CQD query. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Data Window Incremental (minutes)	<p>Vantage DX queries the CQD and loads call information into its database at 15-minute intervals, or at the value set in the Operation Interval field. The Data Window Incremental setting determines the length of time, in minutes, that VDX looks back when it queries the CQD. This lookback period is a sliding window, based on the time that VDX last loaded call information into the database.</p> <p>In the CQD, call data is typically available 30 minutes after the end of the call. For conference calls, data about all attendees becomes available after the last attendee disconnects from the call.</p> <p>For example, if VDX queries the CQD and collects call information at 11am, then the next query will use 11am as its starting point and will look back from that time. The default value is 120 minutes, so in this example, VDX would look back to 9am. VDX retrieves any available information about calls that ended within that window.</p> <p>The default value for the Data Window Incremental setting is 120 minutes. If you select a custom tenant size, we recommend that you set 120 minutes as the value in this field.</p>
Use Incremental Sync Start	When enabled, this option retrieves data beginning from the day of the integration, as opposed to VDX Analytics also retrieving historical data. This default value for this option changes, depending on the selected tenant size. If you selected a custom tenant size, you can enable or disable this option.

Property	Description
Split Properties over Multiple Queries	This option is disabled by default and cannot be enabled unless you selected a custom tenant size. Enable this option only if you are advised to do so by a Martello support engineer.
Add Good Calls as Information Events	<p>Select this option if you want each call to display as a separate component in VDX Analytics. This option is disabled by default and cannot be enabled unless you selected a custom tenant size.</p> <div>  <b>Warning:</b> This option significantly increases the amount of data that VDX Analytics retrieves and stores. If you select this option, it may impact the performance of VDX Analytics. </div>
Discovery Interval (minutes)	The interval for collecting components and relationships from the integrated system. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
Operation Interval (minutes)	The interval for collecting alerts, incidents, and component health states. This value changes based on the size of the selected tenant. If you selected a custom tenant size, you must provide a value.
<b>Thresholds</b>	
Poor Call Warning Ratio (%)	The threshold used by VDX Analytics to trigger a warning about the health status of a user device. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the Hours to Look Back for Health Status field. By default, the call warning ratio is 20%.
Poor Call Critical Ratio (%)	The threshold used by VDX Analytics to trigger a critical alert about the health status of a user device. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the Hours to Look Back for Health Status field. By default, the call critical ratio is 30%.

Property	Description
Jitter (ms)	<p>Set the jitter threshold to use.</p> <p>Jitter indicates the size of the buffer that is needed to store packets before they are reconstructed in the correct order. Jitter can cause delays in calls and is an indicator of congestion of the network.</p> <p>Jitter is averaged over 15-second intervals for the duration of the call. Microsoft classifies call quality as poor when the average exceeds 30 ms. By default, VDX Analytics raises an alert when jitter exceeds the 30 ms threshold, but you can use this field to change the threshold that triggers an alert.</p>
Round Trip Time (ms)	<p>Set the round trip time (RTT) threshold to use.</p> <p>RTT is the time in milliseconds that it takes a data packet to travel from point A to B and return. It is determined by the physical distance between the two points, the speed of transmission, and the overhead taken by the routers in between.</p> <p>RTT is averaged over 15-second intervals for the duration of the call. A value over 500 ms can cause poor call quality. By default, VDX Analytics raises an alert when RTT exceeds the 500 ms threshold, but you can use this field to change the threshold that triggers an alert.</p>
Packet Loss (%)	<p>Set the packet loss threshold to use.</p> <p>The number of packets lost in a 15-second interval. Packet loss is calculated as a percentage. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%.</p> <p>By default, VDX Analytics raises an alert when packet loss exceeds the 10% threshold, but you can use this field to change the threshold that triggers an alert.</p>
<b>Localization</b>	
Timezone	<p>Data collected by the Microsoft CQD is stored in UTC. You can use this setting to have VDX Analytics convert from UTC to another time zone.</p>

Property	Description
Localize Call Times	Select this option to show calls in the local timezone of the participant. When you select this option, the local time is shown for each endpoint in the call. VDX Analytics uses the geolocation to determine the local timezone. If geolocation information is not available, the timezone defaults to UTC.
Building Data	<p>Optional. Enable this option if you have uploaded building data to your Microsoft CQD and want to view it in Vantage DX. When you enable this option, Vantage DX displays the building name, country, region and city information retrieved from the building data file. Because the Microsoft CQD correlates VPN and local IP range information from the building data with call data, this information is also integrated with the call quality data displayed in Vantage DX.</p> <p>This option is designed as an alternative to using the Dynamic Office feature in Vantage DX. If you choose to use CQD building data instead of dynamic offices, information that Vantage DX retrieved about dynamic offices prior to the change will continue to display for up to 90 days.</p>
<b>Privacy Protection</b>	
Anonymize Data	Select this check box if you do not want to show identifiable information for your users, such as names, email addresses, and IP addresses. User information displays as number strings.
Disable Caller Resolution	Select this check box if you do not want to show identifiable information about call recipients. When you choose this option, VDX Analytics displays the name of the user who placed a call, but does not show the name of the call recipient
<b>External Users</b>	
Track External Users	Select this check box to include external users in the number of attendees who participated in Teams meetings. Vantage DX Analytics displays objects for external users and devices and provides a link to the meeting in which they participated.
Track External Users in Location Groups	Select this check box if you want to include external users in the groups that Vantage DX Analytics creates for cities and countries.

Property	Description
<b>Options</b>	
Health Status Period (hours)	The number of hours used to calculate the health status of objects. By default, this field is set to 48 hours; however, you can edit this value if you want to calculate the health status over a different period of time.
Disable Dashboard Data Retrieval	Select this check box if you do not want VDX Analytics to retrieve and store data for the dashboarding feature. If you select this option, ensure that you also disable the dashboarding feature using the options on the <b>Settings &gt; General Settings</b> page.

## Install the Microsoft 365 Integration

Use this procedure to integrate your Microsoft 365 subscription with VDX Analytics.

### Before you Begin

The Vantage DX Analytics application must be registered in Azure Active Directory and you must grant consent for the application to retrieve data. If you have configured SSO, the application is already registered and has the necessary permissions. If you have not performed this step, click the following link to automatically register the application, and then follow the prompts on the screen to sign in and grant consent:

[https://login.microsoftonline.com/common/adminconsent?client\\_id=0d75f118-91b7-4a02-8c52-25d8a1590a7c](https://login.microsoftonline.com/common/adminconsent?client_id=0d75f118-91b7-4a02-8c52-25d8a1590a7c)

For a list of permissions that you are granting to the application, see the "Permissions and Access" topic in the Requirements section of the *Vantage DX Deployment Guide*.

1. From the main menu, select **Settings**.  
The Integrations tab displays the currently installed integrations.
2. Click the **Add** button at the bottom of the page.
3. Select a monitoring system from the dialog box.
4. Enter the information required for the monitoring system.
5. Click **Save**.

Configure the following properties when you integrate Microsoft 365 with VDX Analytics:

Property	Description
Source	Read-only. The name of the source system.

Property	Description
Agent	Select a server to communicate with the source system. This can be the VDX Analytics web server or a machine that has a VDX Analytics Remote agent installed on it.
Name	Provide a name for the integration; this name displays on the VDX Analytics interface.
Leverage Martello VDX Enterprise App	Select this checkbox if you have used the automated option to register the application in Azure AD. When you select this option, you need to provide your Tenant ID only; you do not need to enter a Client ID or a Client Secret Key.
Tenant ID	Required. For information about how to find your Microsoft tenant GUID, see <a href="https://docs.microsoft.com/en-us/onedrive/find-your-office-365-tenant-id">https://docs.microsoft.com/en-us/onedrive/find-your-office-365-tenant-id</a> .
Client ID	The Application (Client) ID from the above Azure Application registration. This information is required only if you are registering the application and granting consent manually.
Client Secret Key	The Client Secret associated with the Azure Application registration. The Client Secret can have an expiry date configured; if your Client Secret has an expiry date, you will need to regenerate it and update the integration when it expires. This information is required only if you are registering the application and granting consent manually.
Collect Teams Devices	Optional. Select this checkbox to collect information about the following Teams meeting room devices: <ul style="list-style-type: none"><li>• Teams Room devices</li><li>• Surface Hub devices</li><li>• Teams Panel devices</li><li>• Collaboration Bar devices</li><li>• Teams Display devices</li><li>• Touch Console devices</li></ul>

Property	Description
Collect IP Phones	Optional. Select this checkbox to collect information about the following Teams meeting room IP Phone devices: <ul style="list-style-type: none"> <li>• IP Phone devices</li> <li>• Low-Cost Phone devices</li> <li>• SIP devices</li> </ul>
Discovery Interval	How often the objects are loaded from the integrated system. The default is 3600 seconds.
Operation Interval	How often health states, alerts, and/or incidents are collected. The default is 120 seconds.

**Note:**

If you prefer to register the application and grant consent manually, refer to the following Knowledge Base article:

<https://helpcenter.martellotech.com/s/article/Microsoft-365-Integration-VDX-A-Requirements>

If you follow the manual process, ensure that you grant the permissions listed in "[Permissions for the VDX Application](#)" on [page 1](#).

## Configure Meeting Room Data

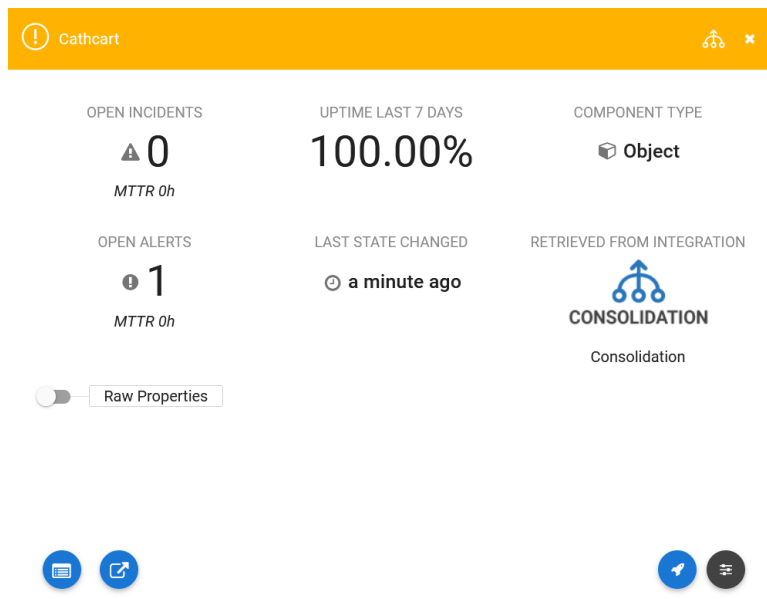
As part of the integration with Microsoft 365, VDX Analytics retrieves data about the meeting room devices that are configured in the Microsoft Teams admin portal, including:

- General information, such as the model number, serial number, and MAC address.
- Health state.
- Peripherals associated with the meeting room device, and their status.

VDX Analytics also retrieves data related to meeting rooms from the integration with the Microsoft Teams Call Quality Dashboard (CQD). If you have meeting rooms and devices configured in the Microsoft Teams admin portal, we recommend that you create a rule in VDX Analytics that consolidates the meeting room data from Microsoft 365 with the meeting room and usage data from the Microsoft Teams CQD. Doing so allows you to view and manage one component that contains all of the data that is available for that meeting room. For example, you can use the consolidated component to see the properties of the meeting room and its devices,

as well as information such as the location, the ISP, number of calls, and information about the call types.

When you create a consolidation rule, VDX Analytics creates a component; the component name is based on the name of the account that is used to log into the meeting room device. The interface lists Consolidation as the source system for the new component because it is created by VDX Analytics rather than retrieved directly from another system. The following image shows an example of a meeting room component that was created using a consolidation rule. In this example, "Cathcart" is the name of the account used to log into the meeting room device, which is also the name of the meeting room.



Use the following procedure to configure a rule that consolidates the meeting room data from Microsoft 365 with the meeting room data from the Microsoft Teams CQD. You must be an administrator to perform these steps.

1. From the VDX Analytics main menu, select **Settings** and click the **Consolidation Rules** tab.
2. Click the expansion icon next to **Object**.  
This setting determines the type of component that VDX Analytics creates.
3. Click **Add Rule**.
4. Enter the following information:
  - **Rule Name**—Enter a name for the rule, such as Teams Meeting Rooms.
  - **Description**—Enter a description of the rule.
5. Choose one of the following options and enter the information shown in the **Field Mapping** section:

**Option 1:** Create a rule that consolidates a meeting room and its devices—as well as non-meeting room devices such as IP phones and SIP devices—into one component. To use this option, ensure that you have selected the "Collect IP Phones" option in the Microsoft 365 integration settings.

Row	Field	Description
1	Integration Type	Microsoft Teams Call Quality
	Field Name	source.Office365CQD.Id
	Match Type	Exact Match
2	Integration Type	Microsoft 365
	Field Name	source.Office365.Id
	Match Type	Exact Match
3	Integration Type	Microsoft 365
	Field Name	source.Office365.currentUser.id
	Match Type	Exact Match

**Option 2:** Create a rule that consolidates data about meeting rooms only, and does not include non-meeting room devices.

Row	Field	Description
1	Integration Type	Microsoft Teams Call Quality
	Field Name	source.Office365CQD.Id
	Match Type	Exact Match
2	Integration Type	Microsoft 365
	Field Name	source.Office365.Id
	Match Type	Exact Match

6. Click **Save**.

7. Click the **Action** button and then click the **Start Consolidation** icon.

8. Click **Ok**.



# Components

In addition to the default dashboards, VDX Analytics creates components that represent data it has retrieved from the source systems it is integrated with. For example, components represent data such as Microsoft licenses, Teams meeting rooms, or Teams calls. There are also components to represent synthetic transaction and network path tests.

These components are a helpful addition to the dashboards because you can pin them to boards or business services to model your data in the way that best suits your needs.

Each source system—also called an integration—uses its own terminology to describe the components it monitors. VDX Analytics standardizes this terminology so that it is easy to correlate data from a variety of source systems. The tables in the following sections list the components that VDX Analytics creates when it retrieves data from your Microsoft tenant and from the Vantage DX modules. The tables also describe how the health state of the component is calculated.

- ["Microsoft CQD Components" on page 20](#)
- ["Microsoft 365 Components" on page 30](#)
- ["Vantage DX Monitoring Components" on page 31](#)

## Microsoft CQD Components

The following sections describe the components that VDX Analytics creates for data it retrieves from the Microsoft Call Quality Dashboard (CQD), and how the integration settings impact the health state calculations.

- ["Components and Health State Calculations" on page 20](#)
- ["Configuration Options" on page 29](#)

## Components and Health State Calculations

The following table lists the component types that VDX Analytics creates for data it retrieves from the Microsoft Call Quality Dashboard (CQD). The table also describes how the health state of each component is calculated.

**Table 1: Microsoft CQD Data**

Component	Description
<b>Objects</b>	
Users	<p>VDX Analytics provides information about the status of the user, such as its health state, the amount of uptime, and the number of incidents and alerts.</p> <p>The overall health state of a user is based on the worst-case health state of the user's devices.</p>
User Devices	<p>This object provides information about a user's experience from a specific location and network connection type. It is based on the geographical location of the device, the network connection type, the operating system, and the IP address. Because this object is based on multiple properties, VDX Analytics may display more than one object for each device. For example, if a user receives a Teams call on a mobile device over broadband while that device is also connected to WIFI in the office or at home, VDX Analytics creates two objects: one for the mobile connection and one for the WIFI connection.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the user device is shown as healthy. This approach prevents a device from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
<b>Groups</b>	

Component	Description
Geographical locations	<p>Cities and countries display as groups. These groups are based on the location of user devices. VDX Analytics provides information about the status of the location, such as its health state, the amount of uptime, and the number of incidents and alerts.</p> <p>The health state is based on the call quality experienced by all the user devices contained in the group.</p> <p>If the average number of calls per user device is lower than the number of devices in the group, the group is shown as healthy. This approach prevents a group from showing a critical health state based on very few calls. For example, if a group contains 5 user devices, but the average number of calls per device is 2, poor quality calls will not trigger a critical health state.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
ISPs	<p>ISPs display as groups. The ISP group is based on the service provider information for user devices. VDX Analytics provides information about the status of the service provider, such as its health state, the amount of uptime, and the number of incidents and alerts.</p> <p>The health state is based on the call quality experienced by all the user devices contained in the group.</p> <p>If the average number of calls per user device is lower than the number of devices in the group, the group is shown as healthy. This approach prevents a group from showing a critical health state based on very few calls. For example, if a group contains 5 user devices, but the average number of calls per device is 2, poor quality calls will not trigger a critical health state.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>

Component	Description
Conference Calls/ Meetings	<p>Teams conference calls display as groups. The groups contain all of the user devices that were part of that meeting. You can view the group properties to see which users experienced poor call quality.</p> <p>The health state is calculated based on the percentage of poor and dropped calls during that meeting.</p> <ul style="list-style-type: none"><li>• <b>Warning state:</b> Occurs if one attendee experiences a poor or dropped call.</li><li>• <b>Critical state:</b> Occurs if multiple attendees experience a poor or dropped call.</li></ul>
Dynamic Offices	<p>A dynamic office is when three or more user devices participate in a call using the same IP address. VDX Analytics creates a group for that IP address.</p> <p>The health state is based on the call quality experienced by all the user devices contained in the group.</p> <p>If the average number of calls per user device is lower than the number of devices in the group, the group is shown as healthy. This approach prevents a group from showing a critical health state based on very few calls. For example, if a group contains 5 user devices, but the average number of calls per device is 2, poor quality calls will not trigger a critical health state.</p> <ul style="list-style-type: none"><li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li><li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li></ul>

Component	Description
TCP Calls	<p>TCP call groups display all the users that make and receive TCP calls.</p> <p>These groups are based on calls. Call quality metrics are aggregated for each group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
Near Time Calls	<p>These groups aggregate metrics for calls that occurred within the last two hours.</p> <p>These groups are based on calls. Call quality metrics are aggregated for each group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>

Component	Description
Network Switching	<p>These groups aggregate information about calls where one of the endpoints experienced a change in the network connection. For example, if a call participant changed from a WIFI connection to a cell connection during the call, that call is included in the Network Switching group. Network switching can also occur if a call participant switches between WIFI base stations, or if a call disconnects and reconnects. Network switching can cause poor call quality by affecting RTT, jitter, or packet loss.</p> <p>Call quality metrics are aggregated for each group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
Low MOS	<p>This groups aggregate data about calls that had low MOS scores.</p> <p>Call quality metrics are aggregated for each group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>

Component	Description
Poor Wifi Strength	<p>These groups aggregate data about calls that had poor WIFI connections.</p> <p>These groups are based on calls. Call quality metrics are aggregated for each group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
Low Client Bandwidth	<p>These groups aggregate data about calls that experienced low bandwidth.</p> <p>Call quality metrics are aggregated for each group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>

Component	Description
Microsoft Data Center	<p>When a Teams call is initiated, the location of the server that hosts the call is typically determined by the first user to join the call. The call is hosted by the Microsoft data center that is in the same region as the first user. VDX Analytics creates a group for each data center and displays the users who participated in calls hosted by that data center.</p> <p>Call quality metrics are aggregated for each group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
PSTN Trunk	<p>These groups display information about user devices that are associated with direct routing calls.</p> <p>Call quality metrics are aggregated for the group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>

Component	Description
PSTN Carrier	<p>These groups display information about user devices that are associated with calling plan calls.</p> <p>Call quality metrics are aggregated for the group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
PSTN Operator Connect	<p>These groups display information about user devices that are associated with operator connect calls.</p> <p>Call quality metrics are aggregated for the group, and the health state is based on the aggregated data.</p> <p>If the total number of calls during the look back period is 2 or less, or if there is not more than 1 call with poor quality, the group is shown as healthy. This approach prevents a group from showing a critical health state based on one poor call.</p> <ul style="list-style-type: none"> <li>• <b>Warning state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Warning Ratio (%)</b> field.</li> <li>• <b>Critical state:</b> Occurs when the percentage of poor or dropped calls for the group is higher than the value set in the <b>Poor Call Critical Ratio (%)</b> field.</li> </ul>
Call rating information	<p>The Call Rating is the score that users provide when they are prompted to rate the quality of a Teams call. The score is on a scale of 1 to 5 and it is optional for users to provide this rating. You can use this group to see which users are rating calls most frequently and how they are rating their experience.</p> <p>When you view the Raw Properties for the group, the Group Type is listed as CallRating.</p>



**Note:**

If the IP address of a device changes during the data collection period, VDX Analytics creates a new device. In this version, you may see multiple instances of the same device if the IP address of a device is changed.

## Configuration Options

When you configure the integration, there are some key settings that affect how health states are calculated:

- There are two settings that determine the time period used to calculate health states:
  - **Health Status Period**—The number of hours used to calculate the health status of objects. By default, this field is set to 48 hours; however, you can edit this value if you want to calculate the health status over a different period of time.
  - **Data Retrieval Period**—The number of days of data from the CQD to display in VDX Analytics. The default setting varies from 4 to 28 days, depending on the tenant size selected for the integration. This field is not directly related to the health state calculations, but it does work in conjunction with the **Health Status Period** field. If the value in the **Health Status Period** is 0, Vantage DX Analytics uses the value in the **Data Retrieval Period** field.
- Use these fields together to specify the data collection window and the health state calculations. For example, you can calculate the health status based on the past 24 hours but continue to display call quality data for the last 7 days.
- **Poor Call Warning Ratio (%)**—The threshold used by VDX Analytics to trigger a warning about the health status of a component. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the **Health Status Period** field. By default, the call warning ratio is 20%. This default value is used if the setting is 0.
- **Poor Call Critical Ratio (%)**—The threshold used by VDX Analytics to trigger a critical alert about the health status of a component. Use this field to specify the percentage of poor calls that must occur during the time period used to calculate health status. The time period is set in the **Health Status Period** field. By default, the call critical ratio is 30%. This default value is used if the setting is 0.

## Microsoft 365 Components

The following table lists the component types that VDX Analytics creates based on data it retrieves about your Microsoft 365 services. The table also describes how the health state of each component is calculated.

**Table 2: Service data from Microsoft 365**

Component	Description
<b>Object</b>	
License	<p>This object component corresponds to applications that are included in a Microsoft 365 Enterprise or Microsoft 365 Frontline license, such as Visio Online or Exchange Online. It provides information about the service plans for the license, as well as the number of purchased and assigned licenses.</p> <p>The health states of Microsoft 365 licenses are calculated as follows:</p> <ul style="list-style-type: none"> <li>• <b>Critical:</b> 0 licenses are available</li> <li>• <b>Warning:</b> Fewer than 2 licenses are available, or if you have more than 20 pre-paid licenses, fewer than 5 are available.</li> </ul>
Teams Meeting Room	<p>VDX Analytics creates an object component for each Teams meeting room configured in your tenant. The component provides license and service plan information, as well as location and number of seats.</p> <p>The health state of a Microsoft Teams meeting room is displayed based on the device health status of the room's devices, as follows:</p> <ul style="list-style-type: none"> <li>• <b>Critical:</b> An issue is causing a significant performance impact on the device, or the device may be unusable.</li> <li>• <b>Warning:</b> An issue may have a limited impact on the device, or the device may be offline.</li> </ul>
Device	<p>This object component corresponds to devices used in meeting rooms, such as a collaboration bar, a phone, or a touch console. Objects may also be low-cost phones, IP phones, and SIP phones.</p> <p>The health state of meeting room devices is determined as follows:</p> <ul style="list-style-type: none"> <li>• <b>Critical:</b> An issue is causing a significant performance impact on the device, or the device may be unusable.</li> <li>• <b>Warning:</b> An issue may have a limited impact on the device, or the device may be offline.</li> </ul>

Component	Description
<b>Group</b>	
Microsoft 365 Subscription	Licensed applications are aggregated into a group component. This component lists all of the licensed applications in your Microsoft 365 subscription and provides information about the number of purchased and available licenses.
	The health states of Microsoft 365 licenses are calculated as follows: <ul style="list-style-type: none"><li>• <b>Critical:</b> 0 licenses are available</li><li>• <b>Warning:</b> Fewer than 2 licenses are available, or if you have more than 20 pre-paid licenses, fewer than 5 are available.</li></ul>
<b>Service</b>	
Service	VDX Analytics creates a service component for each Microsoft 365 service in your subscription, as well a component for the suite of services.
	The components for the individual services provide the status of the service, as well as advisories and the availability history.
	The component that corresponds to the Microsoft 365 suite provides the status of the service, as well as incidents and advisories.
	The health states of services and features are displayed based on the status on the Service Health Dashboard in the Microsoft 365 Admin Center.: <ul style="list-style-type: none"><li>• <b>Critical:</b> Microsoft has reported a service degradation or a service interruption.</li><li>• <b>Warning:</b> Microsoft has reported the service to be in one of the following states: Extended Recovery, False Positive, Investigating, or Restoring Service.</li></ul>

## Vantage DX Monitoring Components

The following table lists the data that VDX Analytics retrieves from Vantage DX Monitoring. The table also describes how the health state of each component is calculated.

**Table 3: Synthetic Transactions from Vantage DX Monitoring**

Component	Description
Object	
Workloads	<p>This component represents the applications or workloads that the robots test—such as Microsoft Exchange, SharePoint, or Teams.</p> <p>The robot performs tests and compares the results to performance thresholds. The health state of the workload is based on this comparison. When test results fall below the performance thresholds, the health state of the workload component is either Warning or Critical, and VDX Analytics displays an alert. Health states and alerts are based on the same performance thresholds.</p> <p>The tests and thresholds are different for each workload. For a list of the tests and thresholds used to calculate the health state of the workload components, see <a href="#">"Vantage DX Monitoring Alerts" on page 37</a>.</p>

Component	Description
Robot Manager instances	<p>This component represents the Robot Manager service, which is a Windows service installed at your business sites. VDX Analytics displays one object for every Robot Manager that you configure. This component raises alerts under the following circumstances:</p> <ul style="list-style-type: none"> <li>• If the Robot Manager has not sent a heartbeat, which may indicate that the machine where it is installed is offline.</li> <li>• If any of the workload configurations assigned to this Robot Manager are not working.</li> </ul> <p>You can use this object component in conjunction with the service component, described below. By having two components to represent the Robot Manager instances, you can send notifications to different teams in your organization when there is an alert. For example, you may want to send notifications to a team that is responsible for hardware or infrastructure when the Robot Manager is offline, and send notifications to an applications team if any of the workload configurations assigned to Robot Manager are not working.</p> <p>The health states of the Robot Manager instance is calculated as follows:</p> <ul style="list-style-type: none"> <li>• <b>Critical:</b> To calculate the health state of the Robot Manager service, VDX Analytics monitors its heartbeat. If the Robot Manager service is unavailable, the health state is Critical.</li> <li>• <b>Warning:</b> If a heartbeat has not been received in the last 20 minutes, the health state is Warning.</li> <li>• <b>Critical:</b> If any of the workloads assigned to this Robot Manager are not working.</li> </ul>
Group	
Tags	<p>Tags that are associated with the Robot Manager service display as Groups. These tags indicate the geographical location of the Robot Manager service, and can also be used to categorize the Robot Manager service in other ways. VDX Analytics creates one group for every tag that you configure.</p> <p>Tags do not have health states of their own. Instead, tags reflect the health state of the components that they are associated with. The health state of each tag is based on the worst-case health state of the Robot Manager service and the workloads that they are associated with.</p>
Service	

Component	Description
	<p>This component represents the Robot Manager service, which is a Windows service installed at your business sites. VDX Analytics displays one service for every Robot Manager that you configure.</p> <p>The health states of the Robot Manager service is calculated as follows:</p>
Robot Manager instances	<ul style="list-style-type: none"><li>• <b>Critical:</b> To calculate the health state of the Robot Manager service, VDX Analytics monitors its heartbeat. If the Robot Manager service is unavailable, the health state is Critical.</li><li>• <b>Warning:</b> If a heartbeat has not been received in the last 20 minutes, the health state is Warning.</li><li>• <b>Critical:</b> If the Robot Manager has been unable to perform any synthetic transactions, or if any of the workloads assigned to this Robot Manager are not working.</li></ul>

# Alerts and Thresholds

VDX Analytics displays alerts based on the information it retrieves from the systems it is integrated with.

There are three types of alerts, which are color-coded to indicate severity:

- **Blue:** Information
- **Yellow:** Warning
- **Red:** Error

By default, only alerts with a severity of Error and Warning are displayed on the Alerts tab. Information alerts are not shown unless you choose to show them using the filters on the page.

The following sections describe the alerts and the thresholds that determine their severity:

- ["Microsoft CQD" on page 35](#)
- ["Microsoft 365" on page 37](#)
- ["Vantage DX Monitoring Alerts" on page 37](#)

## Microsoft CQD

VDX Analytics displays alerts for calls where the user experienced poor voice quality. The alerts are based on the settings that you configure for the integration, as well as thresholds that are pre-defined in the Microsoft Call Quality Dashboard (CQD).

VDX Analytics displays alerts for calls made during the data collection period, which you specify when you configure the integration. Alerts are automatically cleared when they are outside of the data collection period.

You can quickly see all alerts related to the Microsoft CQD by using the pre-defined search. You can access the search by clicking the main menu and then selecting **Explore > Teams Alerts**.

The following table lists the metrics and thresholds that trigger alerts.

**Table 4: Metrics and Thresholds for Alerts**

Metric	Description
Packet Loss (Reverse Packet Loss and Forward Packet Loss)	<p>The number of packets lost in a 15-second interval. For example, if 1000 packets are sent in a 15-second interval and 50 are lost, the packet loss rate is 5%.</p> <p>If the packet loss rate is greater than 10%, the call is marked as poor by Microsoft.</p>

Metric	Description
Video Frame Rate Avg	<p>The average number of frames per second received for a video stream, calculated over the duration of the session. Video sessions in Teams include screen sharing and application sharing.</p> <p>An alert is raised if the average is less than 7 FPS (frames per second). A frame rate of 0 indicates that the video failed to stream.</p>
Round Trip (Forward and Reverse)	The average round-trip network propagation time, in milliseconds. If this is greater than 500 ms, call quality is marked as poor.
Jitter (Forward and Reverse)	Jitter indicates the size of the buffer that is needed to store packets before they are reconstructed in the correct order. If jitter is above 30 ms, the call quality is marked as poor.
Video Local Frame Loss Percentage Avg	The average percentage of video frames lost as they are displayed to the user, including frames recovered from network losses. If this value is greater than 50% on any video stream, the call quality is marked as poor.
Degradation	The average Network Mean Opinion Score (NMOS) for an audio stream. It is a measure of how network loss and jitter have degraded audio quality. If the value is greater than 1.0, the call quality is marked poor.
Concealed Ratio	<p>The average ratio of concealed samples generated by audio healing compared to typical samples. The audio output at an endpoint is classified as either "normal" or "concealed."</p> <p>'Concealed samples help improve sound quality by smoothing transitions when packets are lost. High values indicate packet loss or jitter, and result in distorted or lost audio. When the Concealed Ratio is greater than .07, the call is marked as poor.</p>
Client Bandwidth Estimate and End Point Bandwidth Estimate	The average estimated bandwidth available between the first and second endpoint in bits per second (bps). The estimate is based on packet latency.

## Microsoft 365

VDX Analytics displays alerts based on the status of services as reported on the Service Health Dashboard in the Microsoft 365 Admin Center.

The following table lists the status shown in the Microsoft 365 Admin Center and the severity of the corresponding alert in VDX Analytics. The table also provides a brief description of each status; for detailed descriptions, see the Microsoft documentation at the following URL:

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health?view=o365-worldwide#status-definitions>

**Table 5: Alerts for Microsoft 365 Services**

Status in M365 Admin Center	Alert Severity in VDX Analytics	Description
Service Degradation	Error	An issue may affect the performance of a service or feature.
Service Interruption	Error	An issue affects the availability of a service.
Extended Recovery	Warning	Corrective action is in progress.
Restoring Service	Warning	The cause of the issue has been identified and corrective action is in progress.
Service Operational	Information	The service is healthy.
Service Restored	Information	Corrective action has resolved the issue.
False Positive	Information	After investigation, the service is determined to be healthy and operating as designed.
Investigating	Information	Microsoft is investigating a potential issue and is determining the scope of the impact.

## Vantage DX Monitoring Alerts

VDX Analytics displays the following types of alerts related to Vantage DX Monitoring:

- ["Robot Manager Health" on page 38](#)—Alerts about the health state of the Robot Manager, which is a service you install on a dedicated machine in your environment.

- ["Microsoft Teams Outage Detection" on page 38](#)—Alerts when a Teams outage is detected in multiple business locations. This feature consolidates the outage information so that you do not need to manage individual alerts about Teams issues in different locations.
- ["Performance Alerts for Workloads" on page 38](#)—Alerts about the performance of the workloads that you are monitoring.

### Robot Manager Health

A critical alert is raised if the Robot Manager has not sent a heartbeat within the past 15 minutes.

Critical alerts are also raised if any of the robots configured on a Robot Manager machine have failed to perform workload tests at the expected frequency.

### Microsoft Teams Outage Detection

Vantage DX generates an alert named "Microsoft Teams Outage Detection" when at least three Robot Managers from different locations report critical issues when monitoring the Teams Advanced workload. The alert provides the following information:

- **Originally Detected At**—The locations where an outage was initially detected.
- **Presently Affecting**—The locations that are currently affected; the outage at some locations may have been resolved in the interval since the outage was first detected.

This feature is available when you use Vantage DX Monitoring to monitor the Teams Advanced workload at three or more locations. For information about how to configure notifications for these alerts, see "Manage Notifications and Incidents" in the *VDX Analytics User Guide*. The guide is available in the Martello Help Center at:

<https://helpcenter.martellotech.com/s/documentation/vantage-dx-analyticsstandalone>

### Performance Alerts for Workloads

VDX Analytics displays alerts for the workloads that you have configured Vantage DX Monitoring to test. The robot performs tests and compares the results to performance thresholds. The health state of the workload is based on this comparison. The performance thresholds are based on industry standards, but some workloads have configurable thresholds, so that you can change them based on your needs.

The following table lists each workload that Vantage DX Monitoring can test, and indicates which ones have configurable thresholds. Click the links in the table to see information about the thresholds and their default values, as well as the health state and the severity of the alert that is shown if the threshold is breached.

**Table 6: Workloads and Thresholds**

Workload	Thresholds	Configurable?
ADFS	<a href="#">"ADFS Thresholds" on page 40</a>	✓
Exchange DAG	<a href="#">"Exchange DAG Thresholds" on page 41</a>	—
Exchange Edge Server	<a href="#">"Exchange Edge Thresholds" on page 42</a>	✓
Exchange Free/Busy	<a href="#">"Exchange Advanced Free/Busy Thresholds" on page 41</a>	✓
Exchange Mailbox Server	<a href="#">"Exchange Mailbox Server Thresholds" on page 43</a>	✓
Exchange MAPI	<a href="#">"Exchange MAPI Thresholds" on page 47</a>	✓
Exchange Online	<a href="#">"Microsoft Exchange Thresholds" on page 47</a>	✓
Exchange OWA	<a href="#">"Exchange OWA Thresholds" on page 49</a>	✓
Hybrid Mail Routing	<a href="#">"Hybrid Mail Routing Thresholds" on page 50</a>	✓
Internal Mail Routing	<a href="#">"Internal Mail Routing Thresholds" on page 51</a>	✓
Microsoft 365 Health	<a href="#">"Microsoft 365 Health Thresholds" on page 51</a>	—
Microsoft Entra Connect	<a href="#">"Microsoft Entra Connect Thresholds" on page 40</a>	—
Office 365 Web App	<a href="#">"Office 365 Web App Thresholds" on page 52</a>	✓
OneDrive	<a href="#">"OneDrive Thresholds" on page 52</a>	✓
Roundtrip Mail Routing	<a href="#">"Roundtrip Mail Routing Thresholds" on page 53</a>	✓

Workload	Thresholds	Configurable?
SharePoint Page	<a href="#">"SharePoint Page Thresholds" on page 54</a>	✓
SMTP Gateways	<a href="#">"SMTP Gateways Thresholds" on page 54</a>	✓
Teams	<a href="#">"Teams Thresholds" on page 55</a>	✓
Teams Advanced	<a href="#">"Teams Advanced Thresholds" on page 55</a>	✓
Teams Phone	<a href="#">"Teams Phone Thresholds" on page 1</a>	✓
Teams Video	<a href="#">"Teams Video Thresholds" on page 56</a>	✓
URL	<a href="#">"URL Thresholds" on page 57</a>	✓

## Microsoft Entra Connect Thresholds

For the Microsoft Entra Connect workload, formerly Azure Active Directory (AAD) Connect, the robots compare the date that user information in your on-premises Active Directory was synchronized with the Entra Connect tenant of your Microsoft 365 subscription.

The following table lists the performance thresholds for the AAD Connect workload.

**Table 7: Default Thresholds for AAD Connect**

Description	Type of Notification	Threshold
Synchronization date and time	Warning	If last date and time is older than 24 hours
Cannot connect or synchronization error is reported	Critical	—

## ADFS Thresholds

For the Active Directory Federation Services (ADFS) workload, the robots log into an ADFS endpoint and receive authentication tokens.

The following table lists the thresholds that you can configure for the ADFS workload.

**Table 8: Default Thresholds for ADFS**

Threshold Name and Description	Type of Alert	Default Value
ADFS Performance Threshold An alert is raised when the robot does not receive an authentication token within the time specified.	Warning	3000 ms
ADFS Critical Threshold An alert is raised when authentication fails.	Critical	5000 ms

## Exchange DAG Thresholds

The following table lists the performance thresholds for the Exchange DAG workload.

**Table 9: Default Thresholds for Exchange DAG**

Description	Type of Notification
The health check returns an error.	Warning
The health check fails.	Critical

## Exchange Advanced Free/Busy Thresholds

The following table lists the thresholds that you can configure for the Exchange Advanced Free/Busy workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 10: Default Thresholds for Exchange Advanced Free/ Busy**

Threshold Name and Description	Type of Alert	Default Value
Free/Busy Performance Status Threshold for Open Mailbox action An alert is raised based on the time required to open a mailbox.	Warning	6000 ms
Free/Busy Performance Status Threshold An alert is raised based on the time required to query the availability of the user.	Warning	4000 ms
Free/Busy Critical Status Threshold	Critical	6000 ms

Threshold Name and Description	Type of Alert	Default Value
Free/Busy Critical Status Threshold for Open Mailbox action  An alert is raised based on the time required to open a mailbox.	Critical	9000 ms

## Exchange Edge Thresholds

The following table lists the thresholds that you can configure for the Exchange Edge server, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 11: Default Thresholds for Exchange Edge**

Threshold Name and Description	Type of Alert	Default Value
Exchange Edge Unreachable Queue Length Threshold  An alert is raised based on the number of messages that cannot be routed to their destinations.	Warning	100 messages
Exchange Edge RAM Threshold  An alert is raised based on the amount of memory in use compared to the amount of committed memory.	Warning	90%
Exchange Edge Messaged Queued for Delivery Threshold  Vantage DX Monitoring raises a notification based on the number of messages that are in the processing queue for delivery.	Warning	300 messages
Exchange Edge Processor Time Threshold  An alert is raised when the server is executing processes for more then 75% of the time.	Warning	75 %
Exchange Edge Poison Queue Length Threshold  An alert is raised based on the number of messages in the poison queue. The poison queue isolates messages that contain errors and are determined to be harmful to Exchange after a server or service failure.	Warning	5 messages
Exchange Edge Disk Threshold  An alert is raised when less than 10% of the disk is free space.	Warning	10 %

## Exchange Mailbox Server Thresholds

You can configure the following thresholds for the Exchange Mailbox server:

- ["Client Access Thresholds" on page 43](#)
- ["Database Thresholds" on page 43](#)
- ["Lagged Copies Thresholds" on page 44](#)
- ["System Thresholds" on page 44](#)
- ["Transport Thresholds" on page 46](#)

### Client Access Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Client Access workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 12: Default Thresholds for Exchange Mailbox Server Client Access**

Threshold Name and Description	Type of Alert	Default Value
RPC Client Access Requests Threshold Alerts are based on the number of requests processed by the RPC Client Access service.	Warning	40 requests
RPC Client Access Averaged Latency Time Threshold Alerts are based on the average latency for the RPC Client Access service.	Warning	250 ms

### Database Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Database workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 13: Default Thresholds for Exchange Mailbox Server Databases**

Threshold Name and Description	Type of Alert	Default Value
Store RPC Requests Threshold Alerts are based on the number of RPC requests currently executing within the information store.	Warning	70 requests
Database Reads (Attached) Average Latency Time Threshold Alerts are based on the average time of latency to read from the database.	Warning	20 ms

Threshold Name and Description	Type of Alert	Default Value
Database Writes (Attached) Average Latency Time Threshold Alerts are based on the average time of latency to write to the database file.	Warning	50 ms
Database Log Writes Average Latency Time Threshold Alerts are based on the average time of latency for each log write operation.	Warning	10 ms
Database Reads Recovery Average Latency Time Threshold Alerts are based on the average time of latency for each passive database read operation.	Warning	200 ms
Store RPC Average Latency Time Threshold Alerts are based on the average time of latency for RPC requests for each database.	Warning	50 ms
Client Type RPC Average Latency Time Threshold Alerts are based on the average time of latency for the RPC server.	Warning	50 ms

### Lagged Copies Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Lagged Copies workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 14: Default Thresholds for Exchange Mailbox Server Lagged Copies**

Threshold Name and Description	Type of Alert	Default Value
Replay Lag Status Percentage Threshold Alerts are based on the log file replay percentage from an active database into its passive lagged database copy.	Warning	100 %

### System Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server System, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 15: Default Thresholds for Exchange Mailbox Server - System**

Threshold Name and Description	Type of Alert	Default Value
<p>ASPNet Request Wait Time Threshold</p> <p>Alerts are based on the amount of time that the request waited in the queue for processing.</p>	Warning	0 ms
<p>Exchange Mailbox Disk Threshold</p> <p>An alert is raised when less than 10% of the disk is free space.</p>	Warning	10 %
<p>Domain Controllers LDAP Read Time Threshold</p> <p>Alerts are based on the amount of time it takes to send a message to the domain controller and receive a response.</p>	Warning	100 ms
<p>Processor Percentage Time Threshold</p> <p>Alerts are based on the percentage of time that the processor is executing instructions.</p>	Warning	75 %
<p>Processes LDAP Search Time Threshold</p> <p>Alerts are based on the amount of time it takes to send an LDAP search request and receive a response.</p>	Warning	100 ms
<p>Domain Controllers LDAP Search Time Threshold</p> <p>Alerts are based on the time (in ms) to send an LDAP search request to a domain controller and receive a response.</p>	Warning	100 ms
<p>Processor Privileged Percentage Time Threshold</p> <p>Alerts are based on the amount of elapsed time that the service was running in privileged mode.</p>	Warning	75 %
<p>.Net CLR Memory GC Percentage Time Threshold</p> <p>Alerts are based on the amount of time required to perform garbage collection. This process requires CPU and memory and can cause delays and disconnections if it exceeds the threshold.</p>	Warning	10 %
<p>Processes LDAP Read Time Threshold</p> <p>Alerts are based on the amount of time required to send an LDAP request to a domain controller and receive a response.</p>	Warning	100 ms

Threshold Name and Description	Type of Alert	Default Value
<b>ASPNet Application Restarts Threshold</b> Notifications are based on the number of restarts of the ASP.NET application.	Warning	0 restarts
<b>Processor Queue Length Threshold</b> Alerts are based on the number of threads the processor is servicing. A value higher than the threshold can cause high CPU usage and can indicate that processor capacity is not sufficient.	Warning	6 threads
<b>Memory Committed Bytes In Use Percentage Threshold</b> Alerts are based on the amount of committed virtual memory in use, as a percentage of the memory/commit limit.	Warning	80 %
<b>Network Packets Outbound Errors Threshold</b> Alerts are based on the number of outbound packets in error.	Warning	0 packets
<b>ASPNet Requests In Application Queue Threshold</b> Alerts are based on the number of requests waiting for service in the application queue.	Warning	0 requests
<b>Processor User Percentage Time Threshold</b> Alerts are based on the percentage of processor time spent in user mode, which is a processing mode for applications and subsystems.	Warning	75 %
<b>ASPNet Worker Process Restarts Threshold</b> Alerts are based on the number of restarts of the ASP.NET worker process.	Warning	0 restarts

### Transport Thresholds

The following table lists the thresholds that you can configure for the Exchange Mailbox Server Transport workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 16: Default Thresholds for Exchange Mailbox Server—Transport**

Threshold Name and Description	Type of Alert	Default Value
Number Of Messages In Queue Threshold Alerts are based on the number of messages waiting for service in the queue.	Warning	300 messages

## Exchange MAPI Thresholds

The following table lists the thresholds that you can configure for Exchange MAPI, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 17: Default Thresholds for Exchange MAPI**

Threshold Name and Description	Type of Alert	Default Value
MAPI Critical Status Threshold Alerts are based on the amount of time required to create an email message and create a meeting.	Critical	8 s
MAPI Performance Status Threshold Alerts are based on the amount of time required to create an email message and create a meeting.	Warning	5 s
MAPI Critical Status Threshold for Open Mailbox action Alerts are based on the amount of time required to open a mailbox.	Critical	11 s
MAPI Performance Status Threshold for Open Mailbox action Alerts are based on the amount of time required to open a mailbox.	Warning	8 s

## Microsoft Exchange Thresholds

The following table lists the thresholds that you can configure for Exchange, the default values, and the type of type of alert that is raised when the threshold is exceeded. Alerts are based on the amount of time required to perform each task.

These thresholds apply to the Exchange Online workload.

**Table 18: Default Thresholds for Exchange**

Threshold Name and Description	Type of Alert	Default Value
Exchange Critical Status Threshold for Create Folder action	Critical	6000 ms
Exchange Performance Status Threshold for Create Folder action	Warning	4000 ms
Exchange Critical Status Threshold for Delete Folder action	Critical	6000 ms
Exchange Performance Status Threshold for Delete Folder action	Warning	4000 ms
Exchange Critical Status Threshold for Create Message action	Critical	6000 ms
Exchange Performance Status Threshold for Create Message action	Warning	4000 ms
Exchange Critical Status Threshold for Upload Attachment action	Critical	6000 ms
Exchange Performance Status Threshold for Upload Attachment action	Warning	4000 ms
Exchange Critical Status Threshold for Download Attachment action	Critical	6000 ms
Exchange Performance Status Threshold for Download Attachment action	Warning	4000 ms
Exchange Critical Status Threshold for Remove Attachment action	Critical	6000 ms
Exchange Performance Status Threshold for Remove Attachment action	Warning	4000 ms
Exchange Critical Status Threshold for Create Task action	Critical	6000 ms
Exchange Performance Status Threshold for Create Task action	Warning	4000 ms
Exchange Critical Status Threshold for Delete Task action	Critical	6000 ms
Exchange Performance Status Threshold for Delete Task action	Warning	4000 ms

Threshold Name and Description	Type of Alert	Default Value
Exchange Critical Status Threshold for Search Using Filter action	Critical	6000 ms
Exchange Performance Status Threshold for Search Using Filter action	Warning	4000 ms
Exchange Critical Status Threshold for Create Meeting action	Critical	6000 ms
Exchange Performance Status Threshold for Create Meeting action	Warning	4000 ms
Exchange Critical Status Threshold for Query Free/Busy action	Critical	6000 ms
Exchange Performance Status Threshold for Query Free/Busy action	Warning	4000 ms
Exchange Critical Status Threshold for Delete Event action	Critical	6000 ms
Exchange Performance Status Threshold for Delete Event action	Warning	4000 ms
Exchange Critical Status Threshold for Open Mailbox action	Critical	9000 ms
Exchange Performance Status Threshold for Open Mailbox action	Warning	6000 ms

## Exchange OWA Thresholds

The following table lists the thresholds that you can configure for Exchange MAPI, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 19: Default Thresholds for Exchange MAPI**

Threshold Name and Description	Type of Alert	Default Value
OWA Performance Status Threshold for Open Mailbox action.  Alerts are based on the amount of time required to open a mailbox.	Warning	8000 ms

Threshold Name and Description	Type of Alert	Default Value
OWA Critical Status Threshold for Open Mailbox action. Alerts are based on the amount of time required to open a mailbox.	Critical	11000 ms
OWA Critical Status Threshold for Create Email action Alerts are based on the amount of time required to create an email.	Warning	5000 ms
OWA Critical Status Threshold for Create Email action Alerts are based on the amount of time required to create an email.	Critical	8000 ms
OWA Critical Status Threshold for Create Meeting action. Alerts are based on the amount of time required to create a meeting.	Warning	5000 ms
OWA Critical Status Threshold for Create Meeting action. Alerts are based on the amount of time required to create a meeting.	Critical	8000 ms

## Hybrid Mail Routing Thresholds

The following table lists the thresholds that you can configure for Hybrid Mail Routing, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 20: Default Thresholds for Hybrid Mail Routing**

Threshold Name and Description	Type of Alert	Default Value
Hybrid Mail Routing Performance Status Threshold Alerts are based on the amount of time required to connect to Exchange, as well as mail routing times and roundtrip times (RTT).	Warning	30000 ms
Hybrid Mail Routing Critical Threshold Alerts are based on the amount of time required to connect to Exchange, as well as mail routing times and roundtrip times (RTT).	Critical	120000 ms

## Internal Mail Routing Thresholds

The following table lists the thresholds that you can configure for Internal Mail Routing, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 21: Default Thresholds for Internal Mail Routing**

Threshold Name and Description	Type of Alert	Default Value
<p>Internal Mail Routing Performance Status Threshold</p> <p>Alerts are based on the amount of time required to connect to Exchange and route mail to internal addresses.</p>	Warning	15000 ms
<p>Internal Mail Routing Critical Status Threshold</p> <p>Alerts are based on the amount of time required to connect to Exchange and route mail to internal addresses.</p>	Critical	60000 ms

## Microsoft 365 Health Thresholds

When you configure the Office 365 Health workload in Vantage DX Monitoring, the robots test a fixed list of services. The robots monitor whether there are incidents reported by Microsoft, or whether any advisories have been issued.

The services monitored by the robots are:

- Azure Information Protection
- Dynamics 365
- Exchange Online
- Identity Service
- Microsoft Forms
- Flow in Microsoft 365
- Microsoft StaffHub
- Microsoft Teams
- Microsoft Intune
- Office Client Applications
- Office for the Web
- Planner
- PowerApps in Microsoft 365
- Mobile Device Management for Microsoft 365
- Yammer Enterprise
- Office 365 Portal
- OneDrive for Business
- Power BI

- SharePoint Online

If there is a service in the list that you have not deployed in your organization, the health state is shown as red if you do not disable statuses for that service.

The following table lists the performance thresholds for Microsoft 365 services.

**Table 22: Default Thresholds for Microsoft 365 Services**

Description	Type of Notification
Microsoft has issued an advisory to indicate that a problem may affect some users. The service is available and the scope of the impact is limited.	Warning
Microsoft is reporting an incident that is causing major service degradation or a service interruption.	Critical

## Office 365 Web App Thresholds

The following table lists the thresholds that you can configure for the Office 365 Web App, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 23: Default Thresholds for Office 365 Web App**

Threshold Name and Description	Type of Alert	Default Value
Office 365 Web App Performance Status Threshold Alerts are based on the amount of time required for the page to load after logging in.	Warning	5000 ms

## OneDrive Thresholds

The following table lists the thresholds that you can configure for the OneDrive workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 24: Default Thresholds for OneDrive**

Threshold Name and Description	Type of Alert	Default Value
OneDrive Performance Status Threshold for Login action Alerts are based on the time required to log into OneDrive.	Warning	6000 ms

Threshold Name and Description	Type of Alert	Default Value
OneDrive Critical Status Threshold for Login action Alerts are based on the time required to log into OneDrive.	Critical	9000 ms
OneDrive Performance Status Threshold for Download action Alerts are based on the time required to download a file from OneDrive.	Warning	3000 ms
OneDrive Critical Status Threshold for Download action Alerts are based on the time required to download a file from OneDrive.	Critical	5000 ms
OneDrive Performance Status Threshold for Upload action Alerts are based on the time required to upload a file to OneDrive.	Warning	6000 ms
OneDrive Performance Status Threshold for Upload action Alerts are based on the time required to upload a file to OneDrive.	Critical	9000 ms
OneDrive Performance Status Threshold for Create Folder action Alerts are based on the time required to create a OneDrive folder.	Warning	6000 ms
OneDrive Critical Status Threshold for Create Folder action Alerts are based on the time required to create a OneDrive folder.	Critical	9000 ms

## Roundtrip Mail Routing Thresholds

The following table lists the thresholds that you can configure for Roundtrip Mail Routing, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 25: Default Thresholds for Roundtrip Mail Routing**

Threshold Name and Description	Type of Alert	Default Value
Roundtrip Mail Routing Critical Status Threshold Alerts are based on the amount of time required to route mail to external addresses.	Critical	300000 ms
Roundtrip Mail Routing Performance Status Threshold Alerts are based on the amount of time required to route mail to external addresses.	Warning	60000 ms

## SharePoint Page Thresholds

The following table lists the thresholds that you can configure for SharePoint pages, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 26: Default Thresholds for SharePoint Pages**

Threshold Name and Description	Type of Alert	Default Value
SharePoint Page Performance Status Threshold Alerts are based on the amount of time required for the page to load after logging in.	Warning	5000 ms

## SMTP Gateways Thresholds

The following table lists the thresholds that you can configure for SMTP Gateways, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 27: Default Thresholds for SMTP Gateways**

Threshold Name and Description	Type of Alert	Default Value
SMTP Gateways Performance Status Threshold Alerts are based on the amount of time required to connect to Exchange and route SMTP mail.	Warning	60000 ms
SMTP Gateways Critical Status Threshold Alerts are based on the amount of time required to connect to Exchange and route SMTP mail.	Critical	300000 ms

## Teams Thresholds

The following table lists the thresholds that you can configure for the Teams workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 28: Default Thresholds for Teams**

Threshold Name and Description	Type of Alert	Default Value
Teams Performance Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality.	Warning	3.8 MOS
Teams Critical Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality.	Critical	3.5 MOS

## Teams Advanced Thresholds

The following table lists the thresholds that you can configure for the Teams Advanced workload, the default values, and the type of alert that is raised when the threshold is exceeded. Alerts are based on the amount of time required to perform each of the tasks.

**Table 29: Default Thresholds for Teams Advanced**

Threshold Name and Description	Type of Alert	Default Value
Teams Performance Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality.	Warning	3.8 MOS
Teams Critical Status Threshold An alert is raised if the average Mean Opinion Score (MOS) is below this threshold. MOS is a predictor of voice quality.	Critical	3.5 MOS
Teams Performance Status Threshold for Connection Time Action	Warning	6000 ms
Teams Critical Status Threshold for Connection Time Action	Critical	9000 ms
Teams Performance Status Threshold for Create a Channel Time Action	Warning	6000 ms

Threshold Name and Description	Type of Alert	Default Value
Teams Critical Status Threshold for Create a Channel Time Action	Critical	9000 ms
Teams Performance Status Threshold for Post Message to Channel Time Action	Warning	6000 ms
Teams Critical Status Threshold for Post Message to Channel Time Action	Critical	9000 ms
Teams Performance Status Threshold for Upload File to Channel Time Action	Warning	6000 ms
Teams Critical Status Threshold for Upload File to Channel Time Action	Critical	9000 ms
Teams Performance Status Threshold for Download File Time Action	Warning	6000 ms
Teams Critical Status Threshold for Download File Time Action	Critical	9000 ms
Teams Performance Status Threshold for Search User Time Action	Warning	6000 ms
Teams Critical Status Threshold for Search User Time Action	Critical	9000 ms
Teams Performance Status Threshold for Check Presence Time Action	Warning	6000 ms
Teams Critical Status Threshold for Check Presence Time Action	Critical	9000 ms
Teams Performance Status Threshold for Instant Message Time Action	Warning	6000 ms
Teams Critical Status Threshold for Instant Message Time Action	Critical	9000 ms

## Teams Video Thresholds

The following table lists the thresholds that you can configure for Teams Videos, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 30: Default Thresholds for Teams Videos**

Threshold Name and Description	Type of Alert	Default Value
Teams Video Performance Status Threshold Alerts are based on the frames per second (FPS) for outbound video streams.	Warning	7.5 FPS
Teams Video Critical Status Threshold Alerts are based on the frames per second (FPS) for outbound video streams.	Critical	7 FPS



**Note:** If you expect your users to regularly utilize screen sharing on Teams Video, we recommend that you change the default Teams Video Critical Status Threshold from 7 FPS to 1 FPS.

## URL Thresholds

The following table lists the thresholds that you can configure for the URL workload, the default values, and the type of alert that is raised when the threshold is exceeded.

**Table 31: Default Thresholds for URL**

Threshold Name and Description	Type of Alert	Default Value
URL Performance Status Threshold An alert is raised if the HTTP response time is slower than time specified for the threshold.	Warning	3000 ms
URL HTTP Min Status Code Success Threshold The minimum status code for the range of status codes to be excluded from Critical alerts.	Critical	200 status code
URL HTTP Max Status Code Success Threshold The maximum status code for the range of status codes to be excluded from Critical alerts.	Critical	200 status code



# Searching for Data

The following sections provide information about the different types of searches that are available in VDX Analytics.

- ["Pre-Defined Teams Searches" on page 58](#)
- ["Custom Searches" on page 59](#)

## Pre-Defined Teams Searches

Under the Explore menu, sub-menus display that provide access to pre-defined searches. These searches allow you to quickly find data that Vantage DX Analytics has retrieved from the Microsoft Teams CQD integration. The following searches are available:

- Users with poor calls within 24 hours\*
- Users with poorly rated calls within 7 days\*
- Users with Wi-Fi signal strength issues within 7 days\*
- User Devices
- Teams Alerts
- Teams Meetings
- Meeting Rooms
- Offices
- Locations with poor calls within 1 month\*
- Offline IP phones

In addition to these CQD searches, an additional pre-defined search is available on the Saved Searches tab, named "Users with SIP Response 408 within 7 days.\*" This search finds users who experienced 20% or more calls that failed due to PSTN issues. In order to use this search successfully, you must edit the search criteria to specify the address of your PSTN trunk. A placeholder address is provided that you can edit when you load the search into the Search bar.



**Tip:**

The \* indicates searches that you can use to configure notifications. Notifications that are based on searches are triggered when the search criteria is met. For information about how to configure these notifications, see "Manage Notifications and Incidents" in the *Vantage DX Deployment Guide*. The guide is available in the Martello Help Center at:

<https://helpcenter.martellotech.com/s/documentation/vantage-dxcloud>



**Note:**

We recommend that you configure a consolidation rule before you use the Meeting Rooms search. For more information, see ["Configure Meeting Room Data" on page 17](#)

## Custom Searches

The following sections provide some suggested searches that you can use to find targeted information in VDX Analytics.

- ["Users" on page 60](#)
- ["Devices" on page 63](#)
- ["Locations" on page 63](#)
- ["ISPs" on page 65](#)
- ["Meetings" on page 66](#)
- ["Meeting Rooms" on page 68](#)
- ["Call Quality Metrics and Connection Type" on page 71](#)
- ["Video Calls" on page 72](#)
- ["PSTN Calls" on page 73](#)
- ["Microsoft 365 Services and Workloads" on page 74](#)
- ["Microsoft 365 Licenses" on page 75](#)

There are three self-guided training modules available to help you learn about searches in VDX Analytics:

- Search Fundamentals
- Custom Searches
- Creating and Using Saved Searches

You can find these modules in the [Managing Data](#) section of our Vantage DX Online Training site.

## Users

This section lists searches that help you find information about users.

### View the Experience of a Specific User

`source.Office365CQD.Name:"<User Name>"`

### View the Experience of a Multiple Users

In the following search, enter the UPNs of specific users, such as VIPs. For example, john.doe@company.com.

`source.Office365CQD.Email:("<UPN1>" OR "<UPN2>" OR "<UPN3>") AND  
source.Office365CQD.CQDComponentType:User`

### Identify Users with Low MOS

`source.Office365CQD.AverageMOS:(>0 AND <4)`

### View Meetings with Poor Call Quality Attended by Specific Users

In the following search, enter the UPNs of specific users, such as VIPs. For example, john.doe@company.com.

`source.Office365CQD.Poor\ Call\ Attendees.UserDeviceId:("<UPN1>" OR "<UPN2>"  
OR "<UPN3>")`

You can also find this information using the display name instead of the UPN:

`source.Office365CQD.Id:("<Display Name 1>" OR "<Display Name 2<" OR "<Display  
Name 3>") AND source.Office365CQD.groupType:Meeting`

### View User Devices by Operating System

The following example searches for Windows devices. You can edit this query to search for other operating systems, such as MacOS, IOS, or Android.

`source.Office365CQD.Email:("<UPN1>" OR "<UPN2>" OR "<UPN3>") AND  
source.Office365CQD.ClientOS:<Windows>`

### VIP Meeting Organizers

The following example searches for meetings organized by specified users.

```
source.Office365CQD.Id("(<Display Name>" OR "<Display Name>" OR "<Display Name>") AND source.Office365CQD.groupType:Meeting
```

### **Meetings with Poor Call Quality for Specified Users**

The following example searches for meetings with poor call quality that involved a specified user.

```
source.Office365CQD.Poor\ Call\ Attendees.UserDisplayName:"<Display Name>"
```

The following example shows how you can modify this search to include multiple users, such as a group of VIPs, by using the AND operator.

```
source.Office365CQD.Poor\ Call\ Attendees.UserDisplayName:"<Display Name>"  
AND "<Display Name>"
```

### **View Users in a Specific Department**

To search on a department, the Department property must be configured in your Azure Active Directory (AAD). The following example searches for a department named Executive Board; edit this property to suit your needs.

```
source.Office365CQD.Department:"<Executive Board>"
```

### **User Devices with Poor Forward Metrics on Wired connections**

```
(source.Office365CQD.ForwardJitter:>30 OR source.Office365CQD.ForwardRTT:>500  
OR source.Office365CQD.ForwardPacketLoss:>0.1) AND  
source.Office365CQD.ConnectionType:Wired
```

### **WiFi Users with High Jitter (Forward and Reverse)**

```
source.Office365CQD.ConnectionType:Wifi AND  
(source.Office365CQD.ForwardJitter:>30 OR source.Office365CQD.ReverseJitter:>30)
```

### **WiFi Users High RTT (Forward and Reverse)**

```
source.Office365CQD.ConnectionType:Wifi AND  
(source.Office365CQD.ForwardRTT:>500 OR source.Office365CQD.ReverseRTT:>500)
```

### **WiFi Users High Packet Loss (Forward and Reverse)**

```
source.Office365CQD.ConnectionType:Wifi AND  
(source.Office365CQD.ForwardPacketLoss:>0.1 OR
```

```
source.Office365CQD.ReversePacketLoss:>0.1)
```

### **Wired Users High Jitter (Forward and Reverse)**

```
source.Office365CQD.ConnectionType:Wired AND  
(source.Office365CQD.ForwardJitter:>30 OR source.Office365CQD.ReverseJitter:>30)
```

### **Wired Users High RTT (Forward and Reverse)**

```
source.Office365CQD.ConnectionType:Wired AND  
(source.Office365CQD.ForwardRTT:>500 OR source.Office365CQD.ReverseRTT:>500)
```

### **Wired Users High Packet Loss**

```
source.Office365CQD.ConnectionType:Wired AND  
(source.Office365CQD.ForwardPacketLoss:>0.1 OR  
source.Office365CQD.ReversePacketLoss:>0.1)
```

### **Users who Rated a Call with Low Score**

```
source.Office365CQD.CQDComponentType:User AND  
source.Office365CQD.PoorCallReasons.Issue:("User Rated Call 1" OR "User Rated Call  
2" OR "EndPoint Rated Call 1" OR "EndPoint Rated Call 2")
```

### **Users or Endpoints that Rated a Call with Low Score**

The following search is helpful if you want to see how a user or an endpoint rated a call. These results display on the Alerts tab.

```
source.Office365CQD.UserCallRating:(1 OR 2) OR  
source.Office365CQD.EndPointCallRating:(1 OR 2)
```

### **Connection Type**

The following searches allow you to identify how your users are connecting to calls.

```
source.Office365CQD.ConnectionType:wifi
```

```
source.Office365CQD.ConnectionType:wired
```

```
source.Office365CQD.ConnectionType:mobileBB
```

## Devices

This section lists searches that help you find information about devices.

### Devices Experiencing High Latency and Jitter

```
source.Office365CQD.ForwardJitter:>30 OR source.Office365CQD.ReverseJitter:>30  
OR source.Office365CQD.ForwardRTT:>500 OR  
source.Office365CQD.ReverseRTT:>500
```

### Audio Devices with Low Average MOS

This search allows you to see if a device that you supply to your users, such as an IP phone or headset, is impacting call quality. You can also use this information to see the audio devices in use, and then compare that to Microsoft's list of devices that are certified for use with Teams. This example searches on devices with "Built-in input," but you can search on specific brands, such as "Jabra," or you can specify "default input device."

The following search finds devices that have a MOS score of less than 3.6:

```
source.Office365CQD.AudioDevices:"Built-In input" AND  
source.Office365CQD.AverageMOS:(>0 AND <=3.6)
```

### Headsets that are Not Certified Brands

```
source.Office365CQD.AudioDevices:(* AND NOT "Logitech" AND NOT "Yealink" AND  
NOT "Jabra" AND NOT "Sennheiser" AND NOT "Microsoft" AND NOT "Poly" AND NOT  
"Bose" AND NOT "EPOS" AND NOT "RealWear" AND NOT "BlueParrot")
```

## Locations

Use the searches in this section to determine the locations where you have a high volume of calls, or where you have a high number of poor calls.

### Locations with a High Number of Poor Calls

```
source.Office365CQD.NumberOfPoorCalls:>50 AND  
source.Office365CQD.groupType:City
```

### Cities and Countries with a High Volume of Calls

This example searches for all countries with more than 100 calls. You can edit this value to suit your needs.

```
source.Office365CQD.groupType:Country AND  
source.Office365CQD.NumberOfCalls:>100
```

This example searches for cities with more than 20 calls. You can edit this value to suit your needs.

```
source.Office365CQD.groupType:City AND source.Office365CQD.NumberOfCalls:>20
```

This example shows how you can search for all cities within a specified country. Edit the Country Name to suit your needs.

```
source.Office365CQD.groupType:City AND source.Office365CQD.Name:Country  
Name
```

### **Offices with High Call Volume**

This example searches for offices with more than 500 calls. You can edit this value to suit your needs.

```
source.Office365CQD.groupType:OfficeGroup AND  
source.Office365CQD.NumberOfCalls:>500
```

### **Offices By Name**

This example searches for offices by name. This office name is set in Azure AD; verify the name that has been assigned to each location in Azure AD and edit the example shown below.

```
source.Office365CQD.Office:"Global Headquarters Chicago"
```

### **Geographical Regions**

The examples below show how to search for Teams users in a specified geographical region:

#### **Europe:**

```
source.Office365CQD.groupType:Country AND (source.Office365CQD.Name:France  
OR source.Office365CQD.Name:Switzerland OR source.Office365CQD.Name:"United  
Kingdom" OR source.Office365CQD.Name:Netherlands OR  
source.Office365CQD.Name:Spain)
```

#### **North America:**

```
source.Office365CQD.groupType:Country AND (source.Office365CQD.Name:"United  
States" OR source.Office365CQD.Name:Canada OR  
source.Office365CQD.Name:Mexico)
```

### **Asia-Pacific:**

source.Office365CQD.groupType:Country AND (source.Office365CQD.Name:India OR source.Office365CQD.Name:Australia OR source.Office365CQD.Name:Singapore)

## **ISPs**

This section lists searches that help you find information about ISPs.

### **General Data Related to an ISP**

This example searches for data from a specific ISP. You can create a saved search for each of your ISPs and compare their performance.

source.Office365CQD.ISPs:"ISP Name"

### **ISP and Call Volume**

This example searches for ISPs with a high call volume. The example searches for all ISPs with more than 1000 calls, but you can edit this value to suit your needs.

source.Office365CQD.groupType:ISP AND  
source.Office365CQD.NumberOfCalls:>1000

### **ISPs and Meetings with Poor Call Quality**

This example finds meetings where a user connected through a specified ISP and experienced poor call quality.

source.Office365CQD.groupType:Meeting AND source.Office365CQD.Poor\ Call\ Attendees.UserDeviceName:"ISP Name"

### **ISPs with High RTT**

This search finds all ISPs where Round Trip Time (RTT) was the top issue on more than 10 calls. You can edit the number of calls in this example to suit your needs.

source.Office365CQD.groupType:ISP AND source.Office365CQD.Top\ Network\ Issue.NumberOfCalls:>10 AND source.Office365CQD.Top\ Network\ Issue.Issue:RoundTrip

### **ISPs with High Jitter**

This search finds ISPs where jitter was the top issue on more than 10 calls. You can edit the number of calls in this example to suit your needs.

source.Office365CQD.groupType:ISP AND source.Office365CQD.Top\ Network\ Issue.NumberOfCalls:>10 AND source.Office365CQD.Top\ Network\ Issue.Issue:Jitter

### ISPs with High Packet Loss

This search finds ISPs where packet loss was the top issue on more than 10 calls. You can edit the number of calls in this example to suit your needs.

```
source.Office365CQD.groupType:ISP AND source.Office365CQD.Top\ Network\
Issue.NumberOfCalls:>10 AND source.Office365CQD.Top\ Network\
Issue.Issue:PacketLoss
```

### ISP and average MOS

This search helps you determine whether poor voice quality is associated with a specific ISP.

```
source.Office365CQD.ISP:"ISP Name" AND
source.Office365CQD.AverageBandwidthEst:(>0 AND <1) AND
source.Office365CQD.AverageMOS:(>0 AND <=3.6)
```

## Meetings

This section lists searches that help you find information about meetings.

### User Devices Connected to Poor Meetings through a Specified ISP

```
source.Office365CQD.groupType:Meeting AND source.Office365CQD.Poor\ Call\
Attendees.UserDeviceName:"<ISP Name>"
```

### Large Meetings where a Specified Number of Users had Poor Calls

This search finds meetings with 50 or more participants, where 3 or more users experienced poor call quality. You can edit these parameters to meet your needs.

```
source.Office365CQD.groupType:Meeting AND source.Office365CQD.Number\ Of\
Attendees:>=50 AND source.Office365CQD.Number\ Of\ Attendees\ With\ Poor\
Calls:>=3
```

### Large Meetings

This search finds meetings with 50 or more participants. You can edit this value to meet your needs.

```
source.Office365CQD.groupType:Meeting AND source.Office365CQD.Number\ Of\
Attendees:>=50
```

### **Meetings with Poor RTT**

source.Office365CQD.Poor\ Call\ Attendees.PoorCallDetails:RoundTrip

### **Meetings with Jitter**

source.Office365CQD.Poor\ Call\ Attendees.PoorCallDetails:Jitter

### **Meetings with Packet Loss**

source.Office365CQD.Poor\ Call\ Attendees.PoorCallDetails:PacketLoss

### **Meetings with a Low Video Frame Rate**

source.Office365CQD.Poor\ Call\ Attendees.PoorCallDetails:VideoFrameRateAvg

### **Meetings with Video Frame Loss**

source.Office365CQD.Poor\ Call\  
Attendees.PoorCallDetails:VideoLocalFrameLossPercentageAvg

### **Meetings with Alerts**

source.Office365CQD.MeetingName:\* AND  
source.Office365CQD.CallClassification:Failure

### **Meetings with Alerts, by Country**

source.Office365CQD.MeetingName:\* AND  
source.Office365CQD.CallClassification:Failure AND  
source.Office365CQD.ClientCountry:Canada

### **All Meetings**

source.Office365CQD.MeetingName:\*  
  
source.Office365CQD.MeetingName:\* AND  
source.Office365CQD.ClientCountry:Canada

### **Meeting Organized or Attended by a User**

source.Office365CQD.groupType:Meeting AND (source.Office365CQD.Name:"<User  
Display Name>" OR source.Office365CQD.Poor\ Call\  
Attendees.UserDisplayName:"<User Display Name>")

### Meetings that Occurred at a Specific Date or Time

Use the examples below to search for meetings that occurred on a specific date, or at a specific time. These searches use sample dates and times to show you the correct format to use. In the second example, which searches for meetings that occurred at 3pm on the specified date, you can see that time is specified in a 24h format as defined in ISO 8601.

```
source.Office365CQD.groupType:Meeting AND source.Office365CQD.Meeting\  
StartTime:2022-07-12
```

```
source.Office365CQD.groupType:Meeting AND source.Office365CQD.Meeting\  
StartTime:2022-07-12T15
```

## Meeting Rooms

This section lists searches that help you find information about meeting room devices.

### Find Meeting Room Devices

This example searches for all meeting room devices.

```
source.Office365.deviceType:*
```

To find specific devices, you can replace the wildcard (\*) with a known device type, such as:

- collaborationBar
- ipPhone
- sip
- teamsDisplay
- teamsPanel
- teamsRoom
- touchConsole

### Search Based on Device Properties

The following queries are examples of the device properties that you can search for. You can edit these examples to suit your needs.

```
source.Office365.hardwareDetail.manufacturer:*
```

source.Office365.hardwareDetail.manufacturer:"<manufacturer name>"

source.Office365.hardwareDetail.manufacturer:"<manufacturer name>"

source.Office365.hardwareDetail.model:\*

source.Office365.hardwareDetail.model:"<model name>"

source.Office365.hardwareDetail.model:"<model name>"

source.Office365.hardwareDetail.macAddresses:ethernet

source.Office365.hardwareDetail.macAddresses:wifi

source.Office365.hardwareDetail.macAddresses:<MAC Address>

source.Office365.Place.displayName:\*

source.Office365.Place.displayName:"<meeting room display name>"

source.Office365.Place.displayName:"<Room Name>"

source.Office365.Place.phone:>0

source.Office365.Place.phone:"<phone number>"

source.Office365.Place.capacity:>0

source.Office365.Place.capacity:>=20

source.Office365.Place.address.city:>0

source.Office365.Place.address.city:"<city name>"

```
source.Office365.Place.address.countryOrRegion:>0
```

```
source.Office365.Place.address.countryOrRegion:ES
```

```
source.Office365.Place.address.countryOrRegion:US
```

### **Search for Disconnected Peripherals**

The following queries are examples of how you can search for meeting rooms and IP phones that have disconnected peripherals.

```
source.Office365.DeviceHealth.peripheralsHealth.roomCameraHealth.connection.connectionStatus:disconnected
```

```
source.Office365.DeviceHealth.peripheralsHealth.speakerHealth.connection.connectionStatus:disconnected
```

```
source.Office365.DeviceHealth.peripheralsHealth.displayHealth.connection.connectionStatus:disconnected
```

```
source.Office365.DeviceHealth.peripheralsHealth.microphoneHealth.connection.connectionStatus:disconnected
```

### **Meeting Rooms and IP Phones with Outdated Software**

```
source.Office365.DeviceHealth.softwareUpdateHealth.adminAgentSoftwareUpdateStatus.softwareFreshness:(* AND NOT latest)
```

```
source.Office365.DeviceHealth.softwareUpdateHealth.companyPortalSoftwareUpdateStatus.softwareFreshness:(* AND NOT latest)
```

```
source.Office365.DeviceHealth.softwareUpdateHealth.teamsClientSoftwareUpdateStatus.softwareFreshness:(* AND NOT latest)
```

```
source.Office365.DeviceHealth.softwareUpdateHealth.firmwareSoftwareUpdateStatus.softwareFreshness:(* AND NOT latest)
```

```
source.Office365.DeviceHealth.softwareUpdateHealth.partnerAgentSoftwareUpdate  
Status.softwareFreshness:(* AND NOT latest)
```

## Call Quality Metrics and Connection Type

This section lists searches that help you find information about call quality metrics and the connection type used for the call.

### Number of Dropped Streams by City

The following search lists all cities where dropped streams affected call quality.

```
source.Office365CQD.DroppedStreamCount:>=3 and  
source.Office365CQD.NumberOfDroppedStreams:>=30 AND  
source.Office365CQD.groupType:City
```

### Number of Dropped Streams by ISP

The following search lists all ISPs that had more than 40 dropped streams. You can edit this value to suit your needs.

```
source.Office365CQD.NumberOfDroppedStreams:>=40 AND  
source.Office365CQD.groupType:ISP
```

### Number of Dropped Streams by City and Country

To use the example below, edit the country name.

```
source.Office365CQD.NumberOfDroppedStreams:>=3 AND  
source.Office365CQD.groupType:City AND source.Office365CQD.Name:<Country  
name>
```

### Number of Dropped Streams by ISP and Number of Devices

The following example shows how to search for an ISP that had more than 40 dropped streams and more than 300 user devices. The high number of user devices in this example illustrates how you can set this value to exclude home users or small offices from your search. You can edit these values to meet your needs.

```
source.Office365CQD.NumberOfDroppedStreams:>=40 AND  
source.Office365CQD.groupType:ISP AND  
source.Office365CQD.NumberOfDevices:>=300
```

### ISPs with Round Trip Time as the Top Issue

The following example looks for all ISPs where more than 10 poor calls were caused by round trip time. You can adjust the number to meet your needs.

```
source.Office365CQD.groupType:ISP AND source.Office365CQD.Top\ Network\
Issue.NumberOfCalls:>10 AND source.Office365CQD.Top\ Network\
Issue.Issue:RoundTrip
```

### ISPs with Jitter as the Top Issue

The following example looks for all ISPs where more than 10 poor calls were caused by jitter. You can adjust the number to meet your needs.

```
source.Office365CQD.groupType:ISP AND source.Office365CQD.Top\ Network\
Issue.NumberOfCalls:>10 AND source.Office365CQD.Top\ Network\ Issue.Issue:Jitter
```

### ISPs with Packet Loss as the Top Issue

The following example looks for all ISPs where more than 10 poor calls were caused by packet loss. You can adjust the number to meet your needs.

```
source.Office365CQD.groupType:ISP AND source.Office365CQD.Top\ Network\
Issue.NumberOfCalls:>10 AND source.Office365CQD.Top\ Network\
Issue.Issue:PacketLoss
```

### TCP Calls

Use the following search to identify calls that used TCP as the transport protocol.

```
source.Office365CQD.groupType:TCPCalls
```

## Video Calls

This section lists searches that help you find information about video calls.

### Video as Poor Call Reason

```
source.Office365CQD.PoorReason:( VideoFrameRateAvg OR
VideoLocalFrameLossPercentageAvg)
```

### Video Errors in a Specified Country

```
source.Office365CQD.PoorReason:(VideoFrameRateAvg OR
VideoLocalFrameLossPercentageAvg) AND
source.Office365CQD.ClientCountry:"<Country Name>"
```

### Video Errors in a Specified City

```
source.Office365CQD.PoorReason:(VideoFrameRateAvg OR
VideoLocalFrameLossPercentageAvg) AND source.Office365CQD.ClientCity:"<City
```

Name>"

### **Video Errors in Peer-to-Peer Calls**

source.Office365CQD.PoorReason:(VideoFrameRateAvg OR VideoLocalFrameLossPercentageAvg) AND source.Office365CQD.SessionType:P2P

### **Video Errors in Conference Calls**

source.Office365CQD.PoorReason:(VideoFrameRateAvg OR VideoLocalFrameLossPercentageAvg) AND source.Office365CQD.SessionType:Conf

### **Video Errors and Poor WiFi Signal Strength**

This search identifies calls with video errors where the WiFi signal strength was less than 80%. You can edit this value to suit your needs.

source.Office365CQD.PoorReason:(VideoFrameRateAvg OR VideoLocalFrameLossPercentageAvg) AND  
source.Office365CQD.ClientWifiSignalStrength:(>0 AND <80)

### **Video Based Screen Sharing (VBSS ) with a Low Video Frame Rate**

source.Office365CQD.PoorReason:(VideoFrameRateAvg OR VideoLocalFrameLossPercentageAvg) AND  
(source.Office365CQD.ForwardVbssVideoFrameRate:(>0 AND <1) OR  
source.Office365CQD.ReverseVbssVideoFrameRate:(>0 AND <1))

### **Video Error with Frame Loss**

source.Office365CQD.PoorReason:(VideoFrameRateAvg OR VideoLocalFrameLossPercentageAvg) AND  
(source.Office365CQD.ReverseVideoLocalFrameLossPct:(>0 AND <7) OR  
source.Office365CQD.ReverseVideoLocalFrameLossPct:(>0 AND <7))

## **PSTN Calls**

This section lists searches that help you find information about PSTN calls.

### **Groups or Users Involved in PSTN Calls Greater than 60 Minutes**

source.Office365CQD.PSTNCallsTotalMinutes:>60

**Direct Routing Calls in Specified Countries**

source.Office365CQD.Number\ Of\ Direct\ Routing\ Calls:>0  
ANDsource.Office365CQD.groupType:Country

**PSTN Trunk with Failed Calls**

source.Office365CQD.groupType:PSTNTrunk AND source.Office365CQD.Failed\ Call\  
Reasons.NumberOfCalls:>=5

**PSTN Trunk with Poor Calls**

source.Office365CQD.groupType:PSTNTrunk AND source.Office365CQD.Poor\ Call\  
Reasons.NumberOfCalls:>=5

**Find the Poor Call Reasons on all PSTN calls**

source.Office365CQD.PoorReason:\* AND  
source.Office365CQD.PSTNConnectivityType:(DirectRouting OR CallingPlan OR  
OperatorConnect)

## Microsoft 365 Services and Workloads

This section lists searches that help you find information about your Microsoft 365 services.

**Service Health—All Services**

source.Office365.Service:\*

**Services with Performance Issues**

source.Office365.Service:\* AND source.Office365.Status:ServiceDegradation

**Services with Correction Action in Progress**

source.Office365.Service:\* AND source.Office365.Status:ExtendedRecovery

**Services Operating Normally**

source.Office365.Service:\* AND source.Office365.Status:ServiceOperational

### **Availability History of Services**

This example identifies services where the availability history shows more than three issues. You can edit this value to suit your needs.

```
source.Office365.Service:* AND  
source.Office365.AvailabilityHistory.NumberOfIssues:>=3
```

### **Workloads Tested by Vantage DX Monitoring**

The following search finds all workloads that are tested by Vantage DX Monitoring.

```
source.Gizmo.appAlias:*
```

You can also specify the workload, as shown in the examples below.

```
source.Gizmo.appAlias:OneDrive  
source.Gizmo.appAlias:"Teams Advanced"
```

## **Microsoft 365 Licenses**

This section lists searches that help you find information about your Microsoft licenses.

### **All Microsoft 365 Licenses**

```
source.Office365.LicenseName:*
```

### **Specific Microsoft 365 Licenses**

You can search for licenses using the SKU part number, the SKU GUID, or the license name specified by Microsoft.

If you use the license name, be aware that it can vary, depending on how the license was purchased. For example, licenses sold in combinations may have different identifiers. You can find more information about license naming in the Microsoft documentation:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-service-plan-reference>

The following examples show different ways that you can search for licenses:

```
source.Office365.LicenseName:"Exchange Online Plan 1"
```

```
source.Office365.SkuPartNumber:"EXCHANGESTANDARD"
```

```
source.Office365.Sku:4b9405b0-7788-4568-add1-99614e613b69
```

### **Available Licenses**

The following example shows how you can search for applications that have between 0 and 20 remaining licenses. You can edit this value range to suit your needs.

```
source.Office365.LicenseName:* AND source.Office365.AvailableLicenses:(>0 AND <=20)
```

### **Service Plans**

The following example shows how you can search for all licenses that include a specified service plan. This example uses the Exchange Online plan, but you can edit this value to suit your needs.

```
source.Office365.ServicePlans.ServicePlanName:"Exchange Online"
```

## Call Quality Metrics

VDX Analytics retrieves device-level metrics from the Microsoft CQD integration. The metrics are averaged over all the call streams for the device during the data collection window. Video frame rates are averaged separately for video sessions and for screen sharing sessions, and the highest average frame rate is displayed.

The following table lists the metrics that VDX Analytics displays for each device.

**Table 32: Call Quality Metrics**

Metric	Description
Last call time	The time of the last call on this device.
Client forward jitter	The jitter from the client to the destination.
Client forward RTT	The round-trip time from the client to the destination.
Client forward video frame rate	The video frame rate from the client to the destination.
Client reverse jitter	The jitter from the destination to the client.
Client reverse RTT	The round-trip time from the destination to the client.
Client reverse video frame rate	The video frame rate from the destination to the client.
Average MOS	A prediction of end-user audio quality experience. It is based on latency, the packet loss, jitter, and the codec used.
Call times	A list of calls, with their start and end times.
Number of poor calls	The number of calls with poor voice quality that occurred during the data collection period.
Poor call times	The start and end times of calls with poor voice quality.

Metric	Description
Dropped streams call times	The start and end times when call streams were dropped. Calls do not necessarily fail when call streams are dropped. For example, the video stream may drop but the audio stream may continue.
Failed calls times	The start and end times when calls failed.

## Microsoft Raw Properties

The components that VDX Analytics creates contain a wide range of raw properties that are retrieved from the Microsoft Call Quality Dashboard (CQD) and your Microsoft 365 services. You can open a component to view its raw properties, and you can search on any of the raw properties that VDX Analytics retrieves. The search must be based on the field name of the property, which is determined by Microsoft and may differ from the name displayed in the VDX Analytics interface. To verify the field name to use in a search, hover your mouse over the name of the property; a text box displays the field name. For suggested searches, see ["Custom Searches" on page 59](#).

Use the following table to navigate to sections that provide information about the raw properties that are included in each component.

**Table 33: Raw Properties**

Topic	Description	Microsoft CQD	Microsoft 365
<a href="#">"Users and Devices" on page 80</a>	This section lists the raw properties for users and user devices.	✓	—
<a href="#">"Call Types" on page 87</a>	This section lists the raw properties for conferences, TCP calls, and near-time calls.	✓	—
<a href="#">"Locations" on page 94</a>	This section lists the raw properties for countries, cities, dynamic offices, and Microsoft data centers.	✓	—
<a href="#">"Network Information" on page 100</a>	This section lists the raw properties for ISPs and calls where network switching occurred.	✓	—

Topic	Description	Microsoft CQD	Microsoft 365
<a href="#">"Call Conditions" on page 106</a>	This section lists the raw properties for groups that aggregate data about calls that had low MOS, poor WIFI strength, or low client bandwidth. It also provides information about call rating groups.	✓	—
<a href="#">"PSTN-Connected Calls" on page 112</a>	This section lists the raw properties retrieved from devices that participated in direct routing, calling plan, and operator connect calls.	✓	—
<a href="#">"Meeting Rooms" on page 116</a>	Meeting Rooms	✓	✓
<a href="#">"Meeting Room Devices" on page 118</a>	Meeting Room Devices		✓
<a href="#">"Subscriptions" on page 118</a>	Subscriptions		✓
<a href="#">"Licenses" on page 118</a>	Licenses		✓
<a href="#">"Services" on page 119</a>	Services		✓

## Users and Devices

When VDX Analytics retrieves data from your Microsoft CQD, it creates objects for each user and each user device.

- **User**—These objects provide information about the status of the user.
- **User Devices**—These objects provide information about a user's experience from a specific location and network connection type.

The following table lists the raw properties that are retrieved for each of these objects.

**Table 34: Raw Properties for Users and User Devices**

Property	Users	User Devices
Id	✓	✓
Name	✓	✓
Client OS	—	✓
Client OS Detail	—	✓
Client CPU	—	✓
User Agent	—	✓
Email	✓	✓
User Display Name	—	✓
Office *For User Devices, this property is called User Office.	✓	✓
Department	✓	✓
External User (true/false)	✓	✓
IP Address List	—	✓
Connection Type	—	✓
Average Bandwidth Est	—	✓
Locations *for users, one field indicates city, country *for user devices, there are separate fields for city, region, country	✓	✓
ISPs	✓	✓
Average Bandwidth Est	—	✓
Audio Devices	—	✓

Property	Users	User Devices
Audio Codecs	—	✓
Video Devices	—	✓
Video Codecs	—	✓
Devices		
<ul style="list-style-type: none"> <li>Name</li> <li>Last Call Time</li> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> <li>IP Address List</li> </ul>	✓	—
Active Use		
For Users and User Devices:		
<ul style="list-style-type: none"> <li>Call Date</li> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> </ul>	✓	✓
Additional information for User Devices:		
<ul style="list-style-type: none"> <li>Active Users</li> <li>PSTN Outbound Minutes</li> <li>Number Of Direct Routing Calls</li> <li>Outgoing Dial Delay</li> </ul>		
PSTN Carriers	✓	✓
PSTN Operator Connect	—	✓
PSTN Trunks	✓	✓
Last Call Time	—	✓
Number Of Devices	✓	—
Number Of Calls	✓	✓
Internal Calls	✓	—

Property	Users	User Devices
External End Point Calls	✓	—
Number Of Direct Routing Calls	✓	✓
Number Of Operator Connected Calls	✓	✓
Number of PSTN Calls	✓	✓
Number Of P2P Calls	✓	✓
Number Of Conference Calls	✓	✓
Number Of Video Calls	✓	✓
Number Of Cloud Calls	✓	✓
Number Of UDP Calls	—	✓
Number Of TCP Calls	—	✓
Number Of Wired Calls	✓	—
Number Of Wifi Calls	✓	—
Number Of MobileBB Calls	✓	—
Number Of Failed Calls	✓	—
Number Of Failed Direct Routing Calls	✓	✓
Number Of Failed PSTN Calls	—	✓
Number Of Failed Operator Connect Calls	✓	✓
Number Of Failed Cloud Calls	✓	✓
Number Of Failed Conference Calls	✓	✓
Number Of Failed P2P Calls	✓	✓

Property	Users	User Devices
Number Of Failed Video Calls	✓	✓
Number Of Failed TCP Calls	—	✓
Number Of Failed UDP Calls	—	✓
Number Of Poor PSTN Calls	✓	✓
Number Of Poor Direct Routing Calls	✓	✓
Number Of Poor Operator Connect Calls	✓	✓
Number Of Poor P2P Calls	✓	✓
Number Of Poor Conference Calls	✓	✓
Number Of Poor Video Calls	✓	✓
Number Of Poor Cloud Calls	✓	✓
Number Of Poor UDP Calls	—	✓
Number Of Poor TCP Calls	—	✓
Number Of Poor Wired Calls	✓	—
Number Of Poor Wifi Calls	✓	—
Number Of Poor MobileBB Calls	✓	—
Number Of Failed Wired Calls	✓	
Number Of Failed Wifi Calls	✓	
Number Of Failed MobileBB Calls	✓	
Number Of PSTN Inbound Calls	✓	✓
Number Of Direct Routing Inbound Calls	✓	✓

Property	Users	User Devices
Number Of Operator Connect Inbound Calls	✓	✓
Number Of PSTN Outbound Calls	✓	✓
Number Of Direct Routing Outbound Calls	✓	✓
Number Of Operator Connect Outbound Calls	✓	✓
PSTN Calls Total Minutes	✓	✓
Forward Jitter	—	✓
Forward RTT	—	✓
Forward Package Loss	—	✓
Forward Video Frame Rate	—	✓
Forward Video Local Frame Loss Percentage	—	✓
Reverse Jitter	—	✓
Reverse RTT	—	✓
Reverse Package Loss	—	✓
Reverse Video Frame Rate	—	✓
Reverse Video Local Frame Loss Percentage	—	✓
Average MOS	—	✓
NT Jitter	—	✓
NT RTT	—	✓
NT Packet Loss	—	✓
NT Bandwidth	—	✓

Property	Users	User Devices
NT Wifi Strength	—	✓
Call Times		
<ul style="list-style-type: none"> <li>Start Time</li> <li>End Time</li> <li>End Point User</li> <li>Meeting</li> <li>Call Type</li> <li>Phone Number</li> <li>Post Dial Delay</li> <li>Detail</li> </ul>	—	✓
Poor Calls		
*For User Devices, this property is called Number of Poor Calls.	✓	✓
Poor Call Reasons		
<ul style="list-style-type: none"> <li>Issue</li> <li>Number Of Calls</li> </ul>	✓	✓
Top Network Issue		
<ul style="list-style-type: none"> <li>Issue</li> <li>Number Of Calls</li> </ul>	✓	✓
Poor Call Times		
<ul style="list-style-type: none"> <li>Start Time</li> <li>End Time</li> <li>Caller Display Name</li> <li>End Point User</li> <li>Call Type</li> <li>Phone Number</li> <li>Post Dial Delay</li> <li>Detail</li> <li>Meeting</li> </ul>	—	✓

Property	Users	User Devices
Dropped Streams Call Times <ul style="list-style-type: none"> <li>Start Time</li> <li>End Time</li> <li>Caller Display Name</li> <li>End Point User</li> <li>Call Type</li> <li>Phone Number</li> <li>Post Dial Delay</li> <li>Detail</li> <li>Meeting</li> </ul>	—	✓
Number Of Failed Calls	—	✓
Failed Calls Times <ul style="list-style-type: none"> <li>Start Time</li> <li>End Time</li> <li>Caller Display Name</li> <li>End Point User</li> <li>Call Type</li> <li>Phone Number</li> <li>Post Dial Delay</li> <li>Detail</li> <li>Meeting</li> </ul>	—	✓
Microsoft Datacenters <ul style="list-style-type: none"> <li>Name</li> <li>Number Of Calls</li> </ul>	—	✓
Active Alert (true/false)	—	✓
External End Points <ul style="list-style-type: none"> <li>Name</li> <li>Number Of Calls</li> </ul>	✓	✓
CQD Component Type	✓	✓

## Call Types

When VDX Analytics retrieves data from your Microsoft CQD, it creates groups for the following types of calls:

- **Conference Calls/Meetings**—Teams conference calls display as groups. The groups contain all of the user devices that were part of that meeting. You can view the group properties to see which users experienced poor call quality.
- **TCP Calls**—TCP call groups display all the users that make and receive TCP calls.
- **Near-Time Calls**—These groups aggregate metrics for calls that occurred within the last two hours.

The following table lists the raw properties that are retrieved for each of these groups.

**Table 35: Raw Properties by Call Type**

Property	Conference / Meeting	TCP	Near-Time
Id	✓	✓	✓
Name	✓	✓	✓
IP Address	✓	✓	✓
Top 25 Locations	✓	✓	✓
Top 25 Users	✓	✓	✓
Top 25 ISPs	✓	✓	✓
Number Of Devices	✓	✓	✓
Number Of PSTN Devices	✓	✓	✓
Number Of Calls	✓	✓	✓
Number Of Direct Routing Calls	✓	✓	✓
Number Of PSTN Calls	✓	✓	✓
Number Of P2P Calls	✓	✓	✓
Number Of Conference Calls	✓	✓	✓
Number Of Video Calls	✓	✓	✓
Number Of Cloud Calls	✓	✓	✓

Property	Conference / Meeting	TCP	Near-Time
Number Of Wired Calls	✓	✓	✓
Number Of Wifi Calls	✓	✓	✓
Number Of MobileBB Calls	✓	✓	✓
Number Of UDP Calls	✓	✓	✓
Number Of TCP Calls	✓	✓	✓
Number Of TCP Calls	✓	✓	✓
Number Of Failed Direct Routing Calls	✓	✓	✓
Number Of Failed PSTN Calls	✓	✓	✓
Number Of Failed Cloud Calls	✓	✓	✓
Number Of Failed Conference Calls	✓	✓	✓
Number Of Failed P2P Calls	✓	✓	✓
Number Of Failed Video Calls	✓	✓	✓
Number Of Failed Wired Calls	✓	✓	✓
Number Of Failed Wifi Calls	✓	✓	✓
Number Of Failed MobileBB Calls	✓	✓	✓
Number Of Failed UDP Calls	✓	✓	✓
Number Of Failed TCP Calls	✓	✓	✓
Number Of Poor PSTN Calls	✓	✓	✓
Number Of Poor Direct Routing Calls	✓	✓	✓

Property	Conference / Meeting	TCP	Near-Time
Number Of Poor P2P Calls	✓	✓	✓
Number Of Poor Conference Calls	✓	✓	✓
Number Of Poor Video Calls	✓	✓	✓
Number Of Poor Cloud Calls	✓	✓	✓
Number Of Poor Wired Calls	✓	✓	✓
Number Of Poor Wifi Calls	✓	✓	✓
Number Of Poor MobileBB Calls	✓	✓	✓
Number Of Poor UDP Calls	✓	✓	✓
Number Of Poor TCP Calls	✓	✓	✓
Number Of PSTN Inbound Calls	✓	✓	✓
Number Of Direct Routing Inbound Calls	✓	✓	✓
Number Of PSTN Outbound Calls	✓	✓	✓
Number Of Direct Routing Outbound Calls	✓	✓	✓
PSTN Calls Total Minutes	✓	✓	✓
External End Point Calls	✓	✓	✓
Number Of Poor Calls	✓	✓	✓
Windows Calls			
• Number Of Calls			
• Number Of Poor Calls	✓	✓	✓
• Number Of Failed Calls			
• Top Issue			

Property	Conference / Meeting	TCP	Near-Time
Android Calls			
• Number Of Calls			
• Number Of Poor Calls	✓	✓	✓
• Number Of Failed Calls			
• Top Issue			
IOS Calls			
• Number Of Calls			
• Number Of Poor Calls	✓	✓	✓
• Number Of Failed Calls			
• Top Issue			
MacOS Calls			
• Number Of Calls			
• Number Of Poor Calls	✓	✓	✓
• Number Of Failed Calls			
• Top Issue			

Property	Conference / Meeting	TCP	Near-Time
Daily Active Users			
• Call Date			
• Active Users			
• Number Of Calls			
• Number Of Poor Calls			
• Number Of Failed Calls			
• Number Of PSTN Calls			
• PSTN Inbound Minutes			
• PSTN Outbound Minutes			
• Number Of Direct Routing Calls			
• Direct Routing Inbound Minutes	✓	✓	✓
• Direct Routing Outbound Minutes			
• Number Of Operator Connect Calls			
• Operator Connect Inbound Minutes			
• Operator Connect Outbound Minutes			
• Outgoing Dial Delay			
• Incoming Dial Delay			
• Number Of Failed PSTN Calls			
Top 5 User Issues:			
• User Display Name	✓	✓	✓
• Number Of Poor Calls	✓	✓	✓
• Number Of Failed Calls			
• Top Issue			
Poor Call Reasons:			
• Issue: Jitter	✓	✓	✓
• Number Of Calls			
Top Network Issue			
• Issue	✓	✓	✓
• Number Of Calls			

Property	Conference / Meeting	TCP	Near-Time
Last 30 Poor Calls:			
• Start Time			
• End Time			
• Caller Display Name			
• End Point User	✓	✓	✓
• Call Type			
• Phone Number			
• Post Dial Delay			
• Detail			
• Meeting			
Number Of Dropped Streams	✓	✓	✓
Last 30 Dropped Calls			
• Start Time			
• End Time			
• Caller Display Name			
• End Point User	✓	✓	✓
• Call Type			
• Phone Number			
• Post Dial Delay			
• Detail			
• Meeting			
Last 30 Failed Calls			
• Start Time			
• End Time	✓	✓	✓
• Caller Display Name			
• End Point User			
Microsoft Datacenters			
• Name	✓	✓	✓
• Number Of Calls			
External End Points:			
• Name	✓	✓	✓
• Number Of Calls			

Property	Conference / Meeting	TCP	Near-Time
Group Type	✓	✓	✓
Active Alert (true/false)	✓	✓	✓

## Locations

When VDX Analytics retrieves data from your Microsoft CQD, it creates groups for the following types of locations:

- **Country**—These groups are based on the location of user devices.
- **City**—These groups are based on the location of user devices.
- **Dynamic Offices**—A dynamic office is when three or more user devices participate in a call using the same IP address. VDX Analytics creates a group for that IP address. Devices that connect to a call from the same IP address are typically located in the same office.
- **Microsoft Datacenter**—When a Teams call is initiated, the location of the server that hosts the call is typically determined by the first user to join the call. The call is hosted by the Microsoft data center that is in the same region as the first user. VDX Analytics creates a group for each data center and displays the users who participated in calls hosted by that data center.

The following table lists the raw properties that are retrieved for each of these groups.

**Table 36: Raw Properties for Locations**

Property	Country	City	Dynamic Offices	Microsoft Datacenter
Id	✓	✓	✓	✓
Name	✓	✓	✓	✓
IP Address	✓	✓	✓	✓
Top 25 Locations	✓	✓	✓	✓
Top 25 Users	✓	✓	✓	✓
Top 25 ISPs	✓	✓	✓	✓
Number Of Devices	✓	✓	✓	✓
Number Of PSTN Devices	✓	✓	✓	✓

Property	Country	City	Dynamic Offices	Microsoft Datacenter
Number Of Calls	✓	✓	✓	✓
Number Of Direct Routing Calls	✓	✓	✓	✓
Number Of PSTN Calls	✓	✓	✓	✓
Number Of P2P Calls	✓	✓	✓	✓
Number Of Conference Calls	✓	✓	✓	✓
Number Of Video Calls	✓	✓	✓	✓
Number Of Cloud Calls	✓	✓	✓	✓
Number Of Wired Calls	✓	✓	✓	✓
Number Of Wifi Calls	✓	✓	✓	✓
Number Of MobileBB Calls	✓	✓	✓	✓
Number Of UDP Calls	✓	✓	✓	✓
Number Of TCP Calls	✓	✓	✓	✓
Number Of TCP Calls	✓	✓	✓	✓
Number Of Failed Direct Routing Calls	✓	✓	✓	✓
Number Of Failed PSTN Calls	✓	✓	✓	✓
Number Of Failed Cloud Calls	✓	✓	✓	✓
Number Of Failed Conference Calls	✓	✓	✓	✓
Number Of Failed P2P Calls	✓	✓	✓	✓
Number Of Failed Video Calls	✓	✓	✓	✓

Property	Country	City	Dynamic Offices	Microsoft Datacenter
Number Of Failed Wired Calls	✓	✓	✓	✓
Number Of Failed Wifi Calls	✓	✓	✓	✓
Number Of Failed MobileBB Calls	✓	✓	✓	✓
Number Of Failed UDP Calls	✓	✓	✓	✓
Number Of Failed TCP Calls	✓	✓	✓	✓
Number Of Poor PSTN Calls	✓	✓	✓	✓
Number Of Poor Direct Routing Calls	✓	✓	✓	✓
Number Of Poor P2P Calls	✓	✓	✓	✓
Number Of Poor Conference Calls	✓	✓	✓	✓
Number Of Poor Video Calls	✓	✓	✓	✓
Number Of Poor Cloud Calls	✓	✓	✓	✓
Number Of Poor Wired Calls	✓	✓	✓	✓
Number Of Poor Wifi Calls	✓	✓	✓	✓
Number Of Poor MobileBB Calls	✓	✓	✓	✓
Number Of Poor UDP Calls	✓	✓	✓	✓
Number Of Poor TCP Calls	✓	✓	✓	✓
Number Of PSTN Inbound Calls	✓	✓	✓	✓
Number Of Direct Routing Inbound Calls	✓	✓	✓	✓

Property	Country	City	Dynamic Offices	Microsoft Datacenter
Number Of PSTN Outbound Calls	✓	✓	✓	✓
Number Of Direct Routing Outbound Calls	✓	✓	✓	✓
PSTN Calls Total Minutes	✓	✓	✓	✓
External End Point Calls	✓	✓	✓	✓
Number Of Poor Calls	✓	✓	✓	✓
Windows Calls				
<ul style="list-style-type: none"> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> <li>Number Of Failed Calls</li> <li>Top Issue</li> </ul>	✓	✓	✓	✓
Android Calls				
<ul style="list-style-type: none"> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> <li>Number Of Failed Calls</li> <li>Top Issue</li> </ul>	✓	✓	✓	✓
iOS Calls				
<ul style="list-style-type: none"> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> <li>Number Of Failed Calls</li> <li>Top Issue</li> </ul>	✓	✓	✓	✓
MacOS Calls				
<ul style="list-style-type: none"> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> <li>Number Of Failed Calls</li> <li>Top Issue</li> </ul>	✓	✓	✓	✓

Property	Country	City	Dynamic Offices	Microsoft Datacenter
Daily Active Users				
• Call Date				
• Active Users				
• Number Of Calls				
• Number Of Poor Calls				
• Number Of Failed Calls				
• Number Of PSTN Calls				
• PSTN Inbound Minutes				
• PSTN Outbound Minutes				
• Number Of Direct Routing Calls				
• Direct Routing Inbound Minutes	✓	✓	✓	✓
• Direct Routing Outbound Minutes				
• Number Of Operator Connect Calls				
• Operator Connect Inbound Minutes				
• Operator Connect Outbound Minutes				
• Outgoing Dial Delay				
• Incoming Dial Delay				
• Number Of Failed PSTN Calls				
Top 5 User Issues:				
• User Display Name				
• Number Of Poor Calls	✓	✓	✓	✓
• Number Of Failed Calls				
• Top Issue				
Poor Call Reasons:				
• Issue: Jitter	✓	✓	✓	✓
• Number Of Calls				

Property	Country	City	Dynamic Offices	Microsoft Datacenter
Top Network Issue				
• Issue	✓	✓	✓	✓
• Number Of Calls				
Last 30 Poor Calls:				
• Start Time				
• End Time				
• Caller Display Name				
• End Point User	✓	✓	✓	✓
• Call Type				
• Phone Number				
• Post Dial Delay				
• Detail				
• Meeting				
Number Of Dropped Streams	✓	✓	✓	✓
Last 30 Dropped Calls				
• Start Time				
• End Time				
• Caller Display Name				
• End Point User	✓	✓	✓	✓
• Call Type				
• Phone Number				
• Post Dial Delay				
• Detail				
• Meeting				
Last 30 Failed Calls				
• Start Time				
• End Time	✓	✓	✓	✓
• Caller Display Name				
• End Point User				
Microsoft Datacenters				
• Name	✓	✓	✓	✓
• Number Of Calls				

Property	Country	City	Dynamic Offices	Microsoft Datacenter
External End Points:				
• Name	✓	✓	✓	✓
• Number Of Calls				
Group Type	✓	✓	✓	✓
Active Alert (true/false)	✓	✓	✓	✓

## Network Information

When VDX Analytics retrieves data from your Microsoft CQD, it creates groups for the following network information:

- **ISP**—The ISP group is based on the service provider information for user devices.
- **Network Switching**—These groups aggregate information about calls where one of the endpoints experienced a change in the network connection. For example, if a call participant changed from a WIFI connection to a cell connection during the call, that call is included in the Network Switching group. Network switching can also occur if a call participant switches between WIFI base stations, or if a call disconnects and reconnects.

The following table lists the raw properties that are retrieved for each of these groups.

**Table 37: Raw Properties for Network Information**

Property	ISP	Network Switching
Id	✓	✓
Name	✓	✓
IP Address	✓	✓
Top 25 Locations	✓	✓
Top 25 Users	✓	✓
Top 25 ISPs	✓	✓
Number Of Devices	✓	✓
Number Of PSTN Devices	✓	✓

Property	ISP	Network Switching
Number Of Calls	✓	✓
Number Of Direct Routing Calls	✓	✓
Number Of PSTN Calls	✓	✓
Number Of P2P Calls	✓	✓
Number Of Conference Calls	✓	✓
Number Of Video Calls	✓	✓
Number Of Cloud Calls	✓	✓
Number Of Wired Calls	✓	✓
Number Of Wifi Calls	✓	✓
Number Of MobileBB Calls	✓	✓
Number Of UDP Calls	✓	✓
Number Of TCP Calls	✓	✓
Number Of TCP Calls	✓	✓
Number Of Failed Direct Routing Calls	✓	✓
Number Of Failed PSTN Calls	✓	✓
Number Of Failed Cloud Calls	✓	✓
Number Of Failed Conference Calls	✓	✓
Number Of Failed P2P Calls	✓	✓
Number Of Failed Video Calls	✓	✓
Number Of Failed Wired Calls	✓	✓
Number Of Failed Wifi Calls	✓	✓

Property	ISP	Network Switching
Number Of Failed MobileBB Calls	✓	✓
Number Of Failed UDP Calls	✓	✓
Number Of Failed TCP Calls	✓	✓
Number Of Poor PSTN Calls	✓	✓
Number Of Poor Direct Routing Calls	✓	✓
Number Of Poor P2P Calls	✓	✓
Number Of Poor Conference Calls	✓	✓
Number Of Poor Video Calls	✓	✓
Number Of Poor Cloud Calls	✓	✓
Number Of Poor Wired Calls	✓	✓
Number Of Poor Wifi Calls	✓	✓
Number Of Poor MobileBB Calls	✓	✓
Number Of Poor UDP Calls	✓	✓
Number Of Poor TCP Calls	✓	✓
Number Of PSTN Inbound Calls	✓	✓
Number Of Direct Routing Inbound Calls	✓	✓
Number Of PSTN Outbound Calls	✓	✓
Number Of Direct Routing Outbound Calls	✓	✓
PSTN Calls Total Minutes	✓	✓
External End Point Calls	✓	✓

Property	ISP	Network Switching
Number Of Poor Calls	✓	✓
Windows Calls		
<ul style="list-style-type: none"> <li>• Number Of Calls</li> <li>• Number Of Poor Calls</li> <li>• Number Of Failed Calls</li> <li>• Top Issue</li> </ul>	✓	✓
Android Calls		
<ul style="list-style-type: none"> <li>• Number Of Calls</li> <li>• Number Of Poor Calls</li> <li>• Number Of Failed Calls</li> <li>• Top Issue</li> </ul>	✓	✓
IOS Calls		
<ul style="list-style-type: none"> <li>• Number Of Calls</li> <li>• Number Of Poor Calls</li> <li>• Number Of Failed Calls</li> <li>• Top Issue</li> </ul>	✓	✓
MacOS Calls		
<ul style="list-style-type: none"> <li>• Number Of Calls</li> <li>• Number Of Poor Calls</li> <li>• Number Of Failed Calls</li> <li>• Top Issue</li> </ul>	✓	✓

Property	ISP	Network Switching
Daily Active Users		
• Call Date		
• Active Users		
• Number Of Calls		
• Number Of Poor Calls		
• Number Of Failed Calls		
• Number Of PSTN Calls		
• PSTN Inbound Minutes		
• PSTN Outbound Minutes		
• Number Of Direct Routing Calls		
• Direct Routing Inbound Minutes	✓	✓
• Direct Routing Outbound Minutes		
• Number Of Operator Connect Calls		
• Operator Connect Inbound Minutes		
• Operator Connect Outbound Minutes		
• Outgoing Dial Delay		
• Incoming Dial Delay		
• Number Of Failed PSTN Calls		
Top 5 User Issues:		
• User Display Name		
• Number Of Poor Calls	✓	✓
• Number Of Failed Calls		
• Top Issue		
Poor Call Reasons:		
• Issue: Jitter	✓	✓
• Number Of Calls		
Top Network Issue		
• Issue	✓	✓
• Number Of Calls		

Property	ISP	Network Switching
Last 30 Poor Calls:		
• Start Time		
• End Time		
• Caller Display Name		
• End Point User	✓	✓
• Call Type		
• Phone Number		
• Post Dial Delay		
• Detail		
• Meeting		
Number Of Dropped Streams	✓	✓
Last 30 Dropped Calls		
• Start Time		
• End Time		
• Caller Display Name		
• End Point User	✓	✓
• Call Type		
• Phone Number		
• Post Dial Delay		
• Detail		
• Meeting		
Last 30 Failed Calls		
• Start Time		
• End Time	✓	✓
• Caller Display Name		
• End Point User		
Microsoft Datacenters		
• Name	✓	✓
• Number Of Calls		
External End Points:		
• Name	✓	✓
• Number Of Calls		
Group Type	✓	✓
Active Alert (true/false)	✓	✓

## Call Conditions

When VDX Analytics retrieves data from your Microsoft CQD, it creates groups for the following call conditions:

- **Low MOS**—These groups aggregate data about calls that had low MOS scores.
- **Poor WIFI Strength**—These groups aggregate data about calls that had poor WIFI connections.
- **Low Client Bandwidth**—These groups aggregate data about calls that experienced low bandwidth.
- **Call Rating**—The Call Rating is the score that users provide when they are prompted to rate the quality of a Teams call.

The following table lists the raw properties that are retrieved for each of these groups.

**Table 38: Raw Properties by Call Conditions**

Property	Low MOS	Poor WIFI Strength	Low Client Bandwidth	Call Rating
Id	✓	✓	✓	✓
Name	✓	✓	✓	✓
IP Address	✓	✓	✓	✓
Top 25 Locations	✓	✓	✓	✓
Top 25 Users	✓	✓	✓	✓
Top 25 ISPs	✓	✓	✓	✓
Number Of Devices	✓	✓	✓	✓
Number Of PSTN Devices	✓	✓	✓	✓
Number Of Calls	✓	✓	✓	✓
Number Of Direct Routing Calls	✓	✓	✓	✓
Number Of PSTN Calls	✓	✓	✓	✓
Number Of P2P Calls	✓	✓	✓	✓
Number Of Conference Calls	✓	✓	✓	✓

Property	Low MOS	Poor WIFI Strength	Low Client Bandwidth	Call Rating
Number Of Video Calls	✓	✓	✓	✓
Number Of Cloud Calls	✓	✓	✓	✓
Number Of Wired Calls	✓	✓	✓	✓
Number Of Wifi Calls	✓	✓	✓	✓
Number Of MobileBB Calls	✓	✓	✓	✓
Number Of UDP Calls	✓	✓	✓	✓
Number Of TCP Calls	✓	✓	✓	✓
Number Of TCP Calls	✓	✓	✓	✓
Number Of Failed Direct Routing Calls	✓	✓	✓	✓
Number Of Failed PSTN Calls	✓	✓	✓	✓
Number Of Failed Cloud Calls	✓	✓	✓	✓
Number Of Failed Conference Calls	✓	✓	✓	✓
Number Of Failed P2P Calls	✓	✓	✓	✓
Number Of Failed Video Calls	✓	✓	✓	✓
Number Of Failed Wired Calls	✓	✓	✓	✓
Number Of Failed Wifi Calls	✓	✓	✓	✓
Number Of Failed MobileBB Calls	✓	✓	✓	✓
Number Of Failed UDP Calls	✓	✓	✓	✓

Property	Low MOS	Poor WIFI Strength	Low Client Bandwidth	Call Rating
Number Of Failed TCP Calls	✓	✓	✓	✓
Number Of Poor PSTN Calls	✓	✓	✓	✓
Number Of Poor Direct Routing Calls	✓	✓	✓	✓
Number Of Poor P2P Calls	✓	✓	✓	✓
Number Of Poor Conference Calls	✓	✓	✓	✓
Number Of Poor Video Calls	✓	✓	✓	✓
Number Of Poor Cloud Calls	✓	✓	✓	✓
Number Of Poor Wired Calls	✓	✓	✓	✓
Number Of Poor Wifi Calls	✓	✓	✓	✓
Number Of Poor MobileBB Calls	✓	✓	✓	✓
Number Of Poor UDP Calls	✓	✓	✓	✓
Number Of Poor TCP Calls	✓	✓	✓	✓
Number Of PSTN Inbound Calls	✓	✓	✓	✓
Number Of Direct Routing Inbound Calls	✓	✓	✓	✓
Number Of PSTN Outbound Calls	✓	✓	✓	✓
Number Of Direct Routing Outbound Calls	✓	✓	✓	✓
PSTN Calls Total Minutes	✓	✓	✓	✓

Property	Low MOS	Poor WIFI Strength	Low Client Bandwidth	Call Rating
External End Point Calls	✓	✓	✓	✓
Number Of Poor Calls	✓	✓	✓	✓
Windows Calls				
• Number Of Calls				
• Number Of Poor Calls	✓	✓	✓	✓
• Number Of Failed Calls				
• Top Issue				
Android Calls				
• Number Of Calls				
• Number Of Poor Calls	✓	✓	✓	✓
• Number Of Failed Calls				
• Top Issue				
IOS Calls				
• Number Of Calls				
• Number Of Poor Calls	✓	✓	✓	✓
• Number Of Failed Calls				
• Top Issue				
MacOS Calls				
• Number Of Calls				
• Number Of Poor Calls	✓	✓	✓	✓
• Number Of Failed Calls				
• Top Issue				

Property	Low MOS	Poor WIFI Strength	Low Client Bandwidth	Call Rating
Daily Active Users				
• Call Date				
• Active Users				
• Number Of Calls				
• Number Of Poor Calls				
• Number Of Failed Calls				
• Number Of PSTN Calls				
• PSTN Inbound Minutes				
• PSTN Outbound Minutes				
• Number Of Direct Routing Calls	✓	✓	✓	✓
• Direct Routing Inbound Minutes				
• Direct Routing Outbound Minutes				
• Number Of Operator Connect Calls				
• Operator Connect Inbound Minutes				
• Operator Connect Outbound Minutes				
• Outgoing Dial Delay				
• Incoming Dial Delay				
• Number Of Failed PSTN Calls				
Top 5 User Issues:				
• User Display Name				
• Number Of Poor Calls	✓	✓	✓	✓
• Number Of Failed Calls				
• Top Issue				

Property	Low MOS	Poor WIFI Strength	Low Client Bandwidth	Call Rating
Poor Call Reasons:				
• Issue: Jitter	✓	✓	✓	✓
• Number Of Calls				
Top Network Issue				
• Issue	✓	✓	✓	✓
• Number Of Calls				
Last 30 Poor Calls:				
• Start Time				
• End Time				
• Caller Display Name				
• End Point User	✓	✓	✓	✓
• Call Type				
• Phone Number				
• Post Dial Delay				
• Detail				
• Meeting				
Number Of Dropped Streams	✓	✓	✓	✓
Last 30 Dropped Calls				
• Start Time				
• End Time				
• Caller Display Name				
• End Point User	✓	✓	✓	✓
• Call Type				
• Phone Number				
• Post Dial Delay				
• Detail				
• Meeting				
Last 30 Failed Calls				
• Start Time				
• End Time	✓	✓	✓	✓
• Caller Display Name				
• End Point User				

Property	Low MOS	Poor WIFI Strength	Low Client Bandwidth	Call Rating
Microsoft Datacenters				
• Name	✓	✓	✓	✓
• Number Of Calls				
External End Points:				
• Name	✓	✓	✓	✓
• Number Of Calls				
Group Type	✓	✓	✓	✓
Active Alert (true/false)	✓	✓	✓	✓

## PSTN-Connected Calls

When VDX Analytics retrieves data from your Microsoft CQD, it creates groups for the following types of PSTN calls:

- **PSTN Carrier**—These groups display information about user devices that are associated with calling plan calls.
- **PSTN Trunk**—These groups display information about user devices that are associated with direct routing calls.
- **PSTN Operator Connect**—These groups display information about user devices that are associated with operator connect calls.

The following table lists the raw properties that are retrieved for each of these groups.

**Table 39: Raw Properties for Teams PSTN Calls**

Property	PSTN Carrier	PSTN Trunk	PSTN Operator Connect
Id	✓	✓	✓
Name	✓	✓	✓
PSTN MP Locations	✓	✓	✓
Top 25 Users	✓	✓	✓
Number Of Users	✓	✓	✓

Property	PSTN Carrier	PSTN Trunk	PSTN Operator Connect
Daily Active Users			
• Call Date			
• Active Users			
• Number Of PSTN Calls			
• PSTN Inbound Minutes			
• PSTN Outbound Minutes			
• Number Of Direct Routing Calls			
• Direct Routing Inbound Minutes			
• Direct Routing Outbound Minutes	✓	✓	✓
• Number Of Operator Connect Calls			
• Operator Connect Inbound Minutes			
• Operator Connect Outbound Minutes			
• Outgoing Dial Delay			
• Incoming Dial Delay			
• Number Of Failed PSTN Calls			
Top 25 Locations	✓	✓	✓
Number Of PSTN Devices	✓	✓	✓
Number Of PSTN Calls	✓	✓	✓
Number Of Failed PSTN Calls	✓	✓	✓
Number Of Poor Direct Routing Calls	✓	✓	✓
Number Of Poor PSTN Calls	✓	✓	✓
Number Of Poor Operator Connect Calls	✓	✓	✓
Number Of PSTN Inbound Calls	✓	✓	✓

Property	PSTN Carrier	PSTN Trunk	PSTN Operator Connect
Number Of PSTN Outbound Calls	✓	✓	✓
Number Of Operator Connect Inbound Calls	✓	✓	✓
Number Of Operator Connect Outbound Calls	✓	✓	✓
Number Of Direct Routing Calls	✓	✓	✓
Number Of Operator Connect Calls	✓	✓	✓
Number Of Failed Direct Routing Calls	✓	✓	✓
Number Of Failed Operator Connect Calls	✓	✓	✓
Number Of Direct Routing Outbound Calls	✓	✓	✓
Number Of Direct Routing Inbound Calls	✓	✓	✓
Number Of Wired Calls	✓	✓	✓
Number Of Wifi Calls	✓	✓	✓
Number Of MobileBB Calls	✓	✓	✓
Number Of Poor Wired Calls	✓	✓	✓
Number Of Poor Wifi Calls	✓	✓	✓
Number Of Poor MobileBB Calls	✓	✓	✓
Number Of Failed Wired Calls	✓	✓	✓
Number Of Failed Wifi Calls	✓	✓	✓
Number Of Failed MobileBB Calls	✓	✓	✓

Property	PSTN Carrier	PSTN Trunk	PSTN Operator Connect
PSTN Calls Total Minutes	✓	✓	✓
Top 5 User Poor Call Issues:			
• User Display Name	✓	✓	✓
• Number Of Failed Calls			
• Top Issue			
Top 5 User Failed Call Issues:			
• User Display Name	✓	✓	✓
• Number Of Failed Calls: 3			
• Top Issue			
Last 30 Poor Calls			
• Start Time			
• End Time			
• Caller Display Name	✓	✓	✓
• Phone Number			
• Post Dial Delay			
• Detail			
Last 30 Failed Calls			
• Start Time			
• End Time	✓	✓	✓
• Caller Display Name			
• Detail			
Poor Call Reasons			
• Issue	✓	✓	✓
• Number Of Calls			
Failed Call Reasons			
• Issue	✓	✓	✓
• Number Of Calls			
Microsoft Datacenters	✓	✓	✓
Group Type	✓	✓	✓

## Meeting Rooms

The following table lists the raw properties that are retrieved from each integration. We recommend that you configure a consolidation rule for meeting rooms, so that all of these properties are available to you in one component. For information about how to configure a consolidation rule, see ["Configure Meeting Room Data" on page 17](#).

**Table 40: Raw Properties for Users and User Devices**

Property	CQD	M365
Id	✓	✓
Name	✓	—
Email	✓	—
Office	✓	—
Location	✓	—
ISPs	✓	—
Devices		
<ul style="list-style-type: none"> <li>Name</li> <li>Last Call Time</li> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> <li>IP Address List</li> </ul>	✓	—
Active Use		
<ul style="list-style-type: none"> <li>Call Date</li> <li>Number Of Calls</li> <li>Number Of Poor Calls</li> </ul>	✓	—
Number Of Devices	✓	—
Number Of Calls	✓	—
Number of Conferences	✓	—
Number of Video Calls	✓	—
Number of Cloud Calls	✓	—

Property	CQD	M365
Number of Wired Calls	✓	—
Number of Poor Conference Calls	✓	—
Number of Poor Video Calls	✓	—
Number of Poor Cloud Calls	✓	—
Poor Call Reasons	✓	—
Display name	—	✓
Teams Room License	—	✓
Email Address	—	✓
Usage Location	—	✓
User Principal Name	—	✓
Proxy Addresses	—	✓
Place		
<ul style="list-style-type: none"> <li>• Id</li> <li>• Email Address</li> <li>• Display Name</li> <li>• Nickname</li> <li>• Address</li> </ul>	—	✓
Meeting Room Devices		
<ul style="list-style-type: none"> <li>• Id</li> <li>• Display Name</li> <li>• Device Type</li> <li>• Hardware Details</li> <li>• Health Status</li> <li>• Activity State</li> <li>• Software Details</li> </ul>	—	✓

## Meeting Room Devices

The following raw properties for meeting room devices are retrieved from the Microsoft 365 integration.

- Id
- Device Type
- Health Status
- Activity State
- Created Date Time
- Last Modified Date Time
- Hardware Detail
  - Serial Number
  - Unique Id
  - MAC Addresses
  - Manufacturer
  - Model
  - Current User
  - Device Health

## Subscriptions

The Subscription component contains the following raw properties, which are retrieved from the Microsoft 365 integration:

- Id
- Group Type
- Organization Name
- Organization Domain Name
- Number of Subscriptions
- Licenses
- Assigned and Inactive for each license type (Eg Exchange Assigned, Exchange Inactive)

## Licenses

The License component contains the following raw properties, which are retrieved from the Microsoft 365 integration:

- Id
- SKU
- SKU Part Number
- License Name
- Applies To
- Purchased Licenses

- Assigned Licenses
- Available Licenses
- Service Plans

## Services

The Services component contains the following raw properties, which are retrieved from the Microsoft 365 integration:

- Service
- Status
- Id
- Advisories
- Availability History



## Tell Us How We Did

How did we do? Did you find the content you needed? Your feedback will help us improve our documentation.

Click [here](#) to provide feedback.



© Copyright 2025, Martello Technologies Corporation. All Rights Reserved.

MarWatch™, Savision, CSX, Martello Technologies, and the Martello Technologies logo are trademarks of Martello Technologies Corporation.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.