|  |
| --- |
|  |
| Quality of Experience Review Guide |
| Practical Guidance for Cloud Voice |

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes

© 2018 Microsoft. All rights reserved.

Microsoft, Azure, Excel, Lync, Office 365, PowerShell, Skype, and Windows are trademarks of the Microsoft group of companies. All other trademarks are property of their respective owners.

Version history

|  |  |  |
| --- | --- | --- |
| Version | Changes | Date |
| 1.0 | Initial release | February 2018 |
| 1.1 | Add link to CQD templates, fix figure numbering | April 2018 |
| 2.0 | Updated for Quality of Experience Review v2.0 | September 2018 |
| 2.1 | Added Diagnostic Alerting | September 2018 |
| 2.2 | Removed references to the CxdCallData script | September 2018 |

Table of Contents

[Quality of Experience Review Guide 1](#_Toc523901507)

[Introduction 1](#_Toc523901508)

[Intended audience 1](#_Toc523901509)

[Prerequisites 2](#_Toc523901510)

[What is quality? 2](#_Toc523901511)

[Service metrics 2](#_Toc523901512)

[Poor Stream Rate 2](#_Toc523901513)

[Setup Failure Rate 3](#_Toc523901514)

[Drop Failure Rate 3](#_Toc523901515)

[Define your target metrics 4](#_Toc523901516)

[User experience 4](#_Toc523901517)

[Rate My Call 5](#_Toc523901518)

[Client and device readiness 5](#_Toc523901519)

[Categories of quality 6](#_Toc523901520)

[Service management tasks 7](#_Toc523901521)

[Network tasks 7](#_Toc523901522)

[Endpoints tasks 7](#_Toc523901523)

[CQD basics 8](#_Toc523901524)

[What is CQD? 8](#_Toc523901525)

[Expectations using CQD 8](#_Toc523901526)

[Report editions 8](#_Toc523901527)

[Report types 9](#_Toc523901528)

[Tenant ID 9](#_Toc523901529)

[Azure portal 9](#_Toc523901530)

[Azure PowerShell 9](#_Toc523901531)

[Skype for Business Online Admin Center 9](#_Toc523901532)

[Skype for Business Online using PowerShell 10](#_Toc523901533)

[Teams vs. Skype for Business 10](#_Toc523901534)

[Summary reports 10](#_Toc523901535)

[Detailed reports 10](#_Toc523901536)

[Managed vs. unmanaged networks 11](#_Toc523901537)

[Dimensions, measures, and filters 11](#_Toc523901538)

[First vs. second 11](#_Toc523901539)

[Stream vs. call 11](#_Toc523901540)

[Good, poor, and unclassified calls 11](#_Toc523901541)

[Common subnets 12](#_Toc523901542)

[CQD Online 12](#_Toc523901543)

[Accessing CQD online 12](#_Toc523901544)

[Getting started 13](#_Toc523901545)

[Editing reports 14](#_Toc523901546)

[Filtering reports 14](#_Toc523901547)

[URL filter 14](#_Toc523901548)

[Query filters 15](#_Toc523901549)

[Report filters 15](#_Toc523901550)

[Import the CQD templates 15](#_Toc523901551)

[Building mapping 16](#_Toc523901552)

[Building data file structure 16](#_Toc523901553)

[Supernetting 17](#_Toc523901554)

[VPN 18](#_Toc523901555)

[Uploading building information 18](#_Toc523901556)

[Updating a building file 19](#_Toc523901557)

[Adding net new subnets 20](#_Toc523901558)

[Updating the current building file 20](#_Toc523901559)

[Missing subnets 20](#_Toc523901560)

[Building mapping tools 21](#_Toc523901561)

[CQD tools 21](#_Toc523901562)

[Network Planner 21](#_Toc523901563)

[Diagnostic alerts 22](#_Toc523901564)

[Message center 22](#_Toc523901565)

[Reliability investigations 22](#_Toc523901566)

[Setup failures 23](#_Toc523901567)

[Setup failure trend analysis 23](#_Toc523901568)

[Setup failure investigations 23](#_Toc523901569)

[Drop failures 25](#_Toc523901570)

[Drop failure trend analysis 25](#_Toc523901571)

[Drop failure investigations 26](#_Toc523901572)

[Quality investigations 29](#_Toc523901573)

[Quality 29](#_Toc523901574)

[Quality trend analysis 29](#_Toc523901575)

[Quality investigations 30](#_Toc523901576)

[TCP 33](#_Toc523901577)

[TCP usage 34](#_Toc523901578)

[TCP vs. UDP 34](#_Toc523901579)

[TCP investigations 35](#_Toc523901580)

[HTTP proxy 36](#_Toc523901581)

[HTTP proxy usage 37](#_Toc523901582)

[HTTP proxy investigations 38](#_Toc523901583)

[Endpoint investigations 39](#_Toc523901584)

[Client versions 39](#_Toc523901585)

[Diagnostic alert 40](#_Toc523901586)

[Remediation 40](#_Toc523901587)

[Devices 41](#_Toc523901588)

[Diagnostic alert 42](#_Toc523901589)

[Remediation 42](#_Toc523901590)

[Appendix 43](#_Toc523901591)

[Office 365 network connectivity principles 43](#_Toc523901592)

[Planning for Wi-Fi 43](#_Toc523901593)

[Lync Networking Guide 43](#_Toc523901594)

[Network performance requirements 43](#_Toc523901595)

[Other resources 44](#_Toc523901596)

[Building data file 44](#_Toc523901597)

[CQD training 44](#_Toc523901598)

[Call Analytics training 44](#_Toc523901599)

[Call Analytics support 44](#_Toc523901600)

[Devices 44](#_Toc523901601)

[Tenant reporting 44](#_Toc523901602)

# Quality of Experience Review Guide

This guide is about the Drive Value phase for Microsoft Teams and Skype for Business Online.

# Introduction

To have the greatest impact on improving the user experience, organizations need to operationalize the key areas that are shown in the following figure. Additional areas include identifying operational tasks, establishing targets for quality metrics, ascertaining the metrics to use to gauge organizational success, and narrowing areas of investigation as needed.

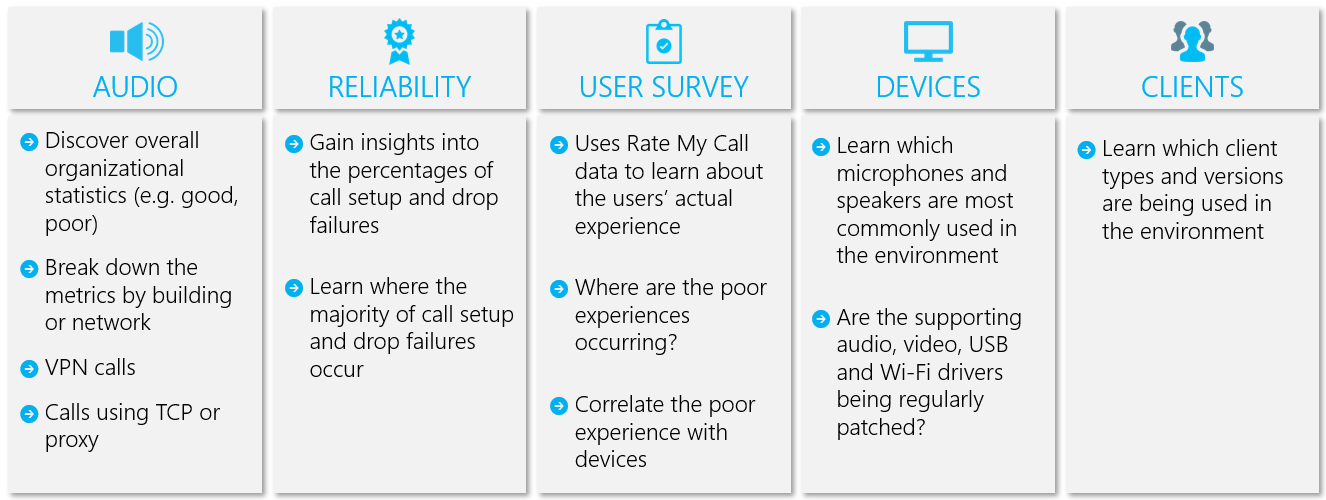


Figure 1 - Key operational areas covered throughout this guide

By continually assessing and remediating the areas described in this guide, you can reduce their potential to negatively affect the quality of your users’ experience. Most user-experience problems encountered in a deployment can be grouped into the following categories:

* Incomplete firewall or proxy configuration
* Poor Wi-Fi coverage
* Insufficient bandwidth
* VPN
* Inconsistent or outdated client versions and drivers
* Unoptimized or built-in audio devices
* Problematic subnets or network devices

Through proper planning and design before deploying Teams or Skype for Business Online, you can reduce the amount of effort that will be required to maintain high-quality experiences.

This guide focuses on using the Call Quality Dashboard (CQD) Online as the primary tool to report and investigate each area, with a special emphasis on audio to maximize adoption and impact. Any improvements made to the network to improve the audio experience will also directly translate to improvements in video and desktop sharing.

To accelerate your assessment, [two curated CQD templates](https://aka.ms/qertemplates) are provided: one is for managing all networks and the other is filtered for managed (internal) networks only. Although the All Networks template reports are configured to display building and network information, they can still be used while you work toward collecting and uploading building information. Uploading building information into CQD enables the service to enhance reporting by adding custom building, network, and location information while differentiating internal from external subnets. For more information, see [Building mapping](#_Building_Mapping_1) later in this guide.

## Intended audience

This guide is intended to be used by partner and customer stakeholders with roles such as Collaboration Lead/Architect, Consultant, Change Management/Adoption Specialist, Support/Help Desk Lead, Network Lead, Desktop Lead, and IT Admin.

This guide is also intended to be used by the designated quality champion(s). For more information, see [the Quality Champion role](https://docs.microsoft.com/MicrosoftTeams/4-envision-plan-my-service-management#the-quality-champion-role).

# Prerequisites

Before using this guide, make sure you have the proper tenant [roles](https://support.office.com/article/About-Office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d) assigned so that you can access CQD.

* **Office 365 Global Administrator role:** Accesses all administrative features in the Office 365 suite of services in your plan, including Skype for Business.
* **Skype for Business Administrator role:** Configures Skype for Business for your organization and is able to view all the [activity reports](https://support.office.com/article/activity-reports-0d6dfb17-8582-4172-a9a9-aed798150263) in the Office 365 admin center. This role is required even if you deploy only Teams.

Alternatively, you can assign the following role to an Office 365 user account to allow access to reporting features only.

* **Reports Reader:** Can view all the [activity reports](https://support.office.com/article/activity-reports-0d6dfb17-8582-4172-a9a9-aed798150263) in the Office 365 admin center, any reports from the [Office 365 Adoption content pack](https://support.office.com/article/Office-365-Adoption-content-pack-77ff780d-ab19-4553-adea-09cb65ad0f1f), and CQD reports.

# What is quality?

When discussing quality in Microsoft Teams and Skype for Business, it’s important to define the term to achieve a common understanding. Quality, as defined here, is a combination of service metrics and user experience.

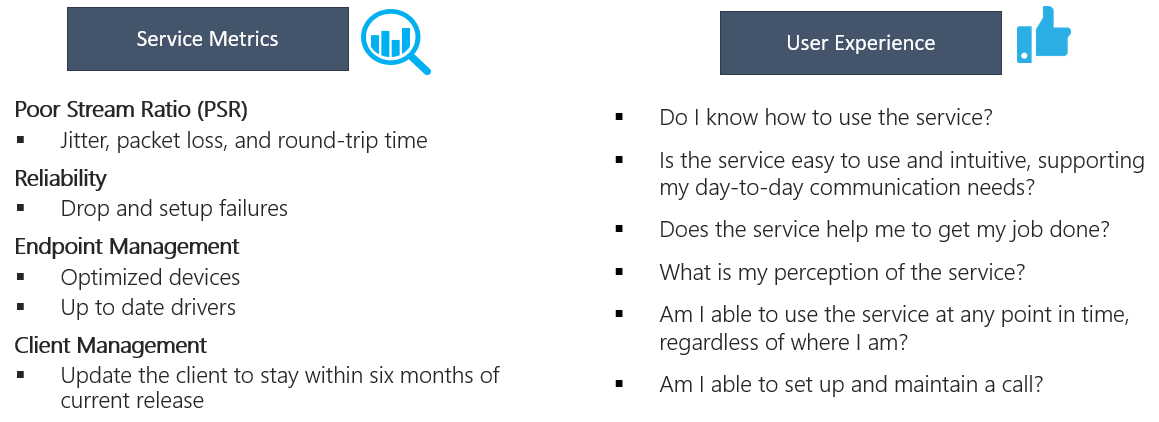


Figure 2 - What is quality?

## Service metrics

Service metrics consist of specific client-based metrics. During each call, the client collects telemetry information about the call and submits a report at the end of each call that can be later accessed through CQD or [Call Analytics](https://techcommunity.microsoft.com/t5/Skype-for-Business-Blog/Introducing-Call-Analytics/ba-p/57309). These metrics include:

* Poor Stream Rate
* Setup Failure Rate
* Drop Failure Rate

### Poor Stream Rate

The poor stream rate (PSR) represents the organization’s overall percentage of streams that have poor quality. This metric is meant to highlight areas where your organization can concentrate effort to have the strongest impact toward reducing this value and improving the user experience, which is why [managed networks](#_Managed_vs._unmanaged) are the primary focus when looking at PSR. External users are important too, but investigation differs on an organizational basis. Consider providing best practices for external users and investigate external calls independently from the overall organization.

The actual measurement in CQD varies by workload, but for the purposes of the Quality Experience Review we focus primarily on the *Audio Poor Percentage* measurement. PSR is made up of the five network metric averages described in the following table. For a stream to be classified as poor, only one metric needs to exceed the defined threshold. For more information about the stream classification process, see [this article](https://docs.microsoft.com/microsoftteams/stream-classification-in-call-quality-dashboard).

|  |  |
| --- | --- |
| Note | CQD provides the “Poor Due To…” measurements to better understand what condition caused the stream to be classified as poor. |

Table 1 - Poor service metrics

|  |  |  |
| --- | --- | --- |
| Metric average | Description | User experience |
| Jitter >30 ms | This is the average change in delay between successive packets over a 20 ms packetization rate. Teams and Skype for Business can adapt to some levels of jitter through buffering. It’s only when the jitter exceeds the buffering that a participant notices the effects of jitter. | The packets arriving at different speeds cause a speaker’s voice to sound robotic. |
| Packet loss rate >10% or 0.1 | This is often defined as a percentage of packets that are lost. Packet loss directly affects audio quality—from small, individual lost packets that have almost no impact to back-to-back burst losses that cause audio to cut out completely. | The packets being dropped and not arriving at their intended destination cause gaps in the media, resulting in missed syllables and words, and choppy video and sharing. |
| Round-trip time >500 ms | This is the time it takes to get an IP packet from point A to point B and back to point A. This network propagation delay is tied to the physical distance between the two points and the speed of light, and includes additional overhead taken by the various devices in the network path. | The packets taking too long to arrive at their destination cause a walkie-talkie effect. |
| NMOS degradation average >1.0 | Average [Network Mean Opinion Score (NMOS)](https://docs.microsoft.com/previous-versions/office/communications-server/bb894481(v=office.12)#network-mos) degradation for stream. Represents how much the network loss and jitter has affected the quality of received audio that caused the NMOS to drop by more than one point. | This is a combination of jitter, packet loss, and—to a lesser degree—increased round-trip time. The user might be experiencing a combination of these symptoms. |
| Average ratio of concealed samples >7% or 0.07 | Average ratio of the number of audio frames with concealed samples generated by packet loss healing to the total number of audio frames. A concealed audio sample is a technique used to smooth out the abrupt transition that would usually be caused by dropped network packets. | High values indicate that significant levels of loss concealment were applied and resulted in distorted or lost audio. |

### Setup Failure Rate

The setup failure rate, otherwise known as the *Total Call Setup Failure Percentage* measurement in CQD, is the number of streams where the media path couldn’t be established between the endpoints at the start of the call.

This represents any media stream that couldn’t be established. Given the severity of the impact on the user experience measured here, the goal is to reduce this value to as close to zero as possible. A high value for this metric is more common in new deployments with incomplete firewall rules than a mature deployment, but it’s still important to watch on a regular basis.

This metric is calculated by taking the total number of streams that failed to set up divided by the total number of streams that submitted a successful call detail record (CDR).

* **Setup Failure Rate** = Total Call Setup Failed Stream Count / Total CDR Available Stream Count

### Drop Failure Rate

The drop failure rate, otherwise known as the *Total Call Dropped Failure Percentage* measurement in CQD, is the percentage of successfully established streams where the media path didn’t terminate normally.

This represents any media stream that terminated unexpectedly. Although the impact of this isn’t as severe as a stream that failed to set up, it will negatively affect the user experience. Sudden and frequent media drops not only can have a severe impact on the user experience, they result in the need for users to reconnect, resulting in a loss in productivity.

The metric is calculated by taking the total number of dropped streams divided by the total count of streams that set up successfully.

* **Drop Failure Rate** = Total Call Dropped Stream Count / Total Call Setup Succeeded Stream Count

## Define your target metrics

This section discusses some of the core service metrics that we use to assess how services experience health. By continually assessing and driving efforts to keep these metrics below their defined targets, you’ll help ensure that your users experience consistent, reliable call quality. To get you started, the following targets are provided.

Table 2 - Core target health assessment metrics

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Network type | | Quality targets | Reliability targets | |
| Audio Poor Stream Rate | Setup Failure Rate | Drop Failure Rate |
| All | Internal | 2.0% | 0.5% | 2.0% |
| Overall | 3.0% | 1.0% | 3.0% |
| Conferencing | Internal | 2.0% | 0.5% | 2.0% |
| Wired internal | 1.0% | 0.5% | 1.0% |
| Wi-Fi 5 GHz internal | 1.0% | 0.5% | 1.0% |
| Wi-Fi 2.4 GHz internal | 4.0% | 0.5% | 2.0% |
| Overall | 2.0% | 0.5% | 3.0% |
| P2P | Internal | 2.0% | 0.5% | 2.0% |
| Wired/Wi-Fi 5 GHz internal | 1.0% | 0.5% | 1.0% |
| Wired/Wi-Fi 5 GHz overall | 2.0% | 1.0% | 1.0% |
| Overall | 2.0% | 1.0% | 3.0% |

It’s important to discuss and define your organization’s targets to meet your business objectives.

## User experience

Analyzing the user experience is more art than science, because the metrics gathered here don’t always mean that there’s a problem with the network or service but rather, they simply indicate that the user perceives a problem. Microsoft offers a built-in survey mechanism—known as Rate My Call (RMC)—to help gauge overall user experience. RMC will help you answer the following questions from your users’ perspective:

* Do I know how to use the solution?
* Is the solution easy to use and intuitive, and does it support my day-to-day communication needs?
* Does the solution help me get my job done?
* What’s my overall perception of the solution?
* Can I use the solution at any point in time, regardless of where I am?
* Can I set up and maintain a call?

### Rate My Call

Rate My Call (RMC) is built into Teams and Skype for Business and is automatically configured to be displayed to the participant after one in every 10 calls, or 10 percent. This brief survey asks the user to rate the call and provide a little context for why the call quality might have been poor. A one or two rating is considered poor, three to four is good, and five is excellent. Although it’s somewhat of a lagging indicator, this is a useful metric for uncovering issues that service metrics can miss.

|  |  |
| --- | --- |
| Note | Until users are educated to respond to RMC surveys by giving good feedback in addition to bad, responses typically come back as overwhelmingly negative. Most users only respond when call quality is poor. Because of this, your RMC reports might be skewed to the poor side even while service metrics are good. |

You can use CQD to report on RMC user responses, and sample reports are included in the CQD template. However, they aren’t discussed in detail in this guide. For more information about RMC in Skype for Business Online and guidance for educating users to give useful RMC responses, see this [blog post](https://blogs.technet.microsoft.com/jenstr/2015/05/05/rate-my-call-in-skype-for-business-2015/).

### Client and device readiness

You need a solid client and device strategy to help ensure that your users have a consistent and positive user experience. A few key principles drive each readiness strategy.

#### Client readiness

A strong client readiness strategy ensures that your users are running the most recent version of the client while enjoying the best experience possible. Microsoft routinely patches the Skype for Business client; ensuring that you keep it up to date in your environment is vital to your overall success. It’s also important to remember to patch network, video, USB, and audio drivers, because they’re often overlooked and can affect the user’s experience. Consider adding network, Wi-Fi, video, USB, and audio drivers to your current patch management process.

We recommend that you not let your client versions fall behind by more than six months. If you’re using Office Click-to-Run, you’re already being kept up to date by the service. Use the included [client versions](#_Determine_Client_Versions), as described later in this guide, to assist you with this process.

|  |  |
| --- | --- |
| Important | Currently, Microsoft Teams clients are distributed and updated automatically through the Azure Content Delivery Network and will be kept up to date by the service. Due to this, client readiness and investigative activities aren’t applicable to Teams. |

#### Device readiness

No one single strategy can affect the user experience more than your device readiness strategy. Most organizations are happy to remove unnecessary devices (for example, desk phones or other dedicated audio devices) from users, and this is often a core business justification for switching to Teams or Skype for Business. However, those same organizations sometimes hesitate to provide replacement devices, even if those devices are less expensive. Modern-day laptops and PCs, though equipped with built-in microphone and speaker, aren’t optimized for business-class voice over IP (VoIP). This often creates a poor experience for all participants, especially if the speaker is in a noisy environment. Microsoft’s device certification program ensures that when a user participates in a phone call by using any device certified for Teams or Skype for Business, it produces an experience that’s superior to a non-certified device.

We always recommend that Teams and Skype for Business users use a certified headset or speaker when participating in a voice call through the desktop client. For more information about Microsoft certified devices, review these articles about the [certification program](https://docs.microsoft.com/SkypeForBusiness/certification/overview) and view the [partner solutions catalog](https://partnersolutions.skypeforbusiness.com/solutionscatalog/personal-peripherals-pcs). Use the [Devices report](#_Devices_Investigations), described later in this guide, for assistance with managing your devices.

## Categories of quality

The success of operationalizing a high-quality and reliable deployment depends on your building operational rigor. Specifically, pay special attention to the three categories illustrated in the following figure; these are the focus of this guide:

* **Network:** Audio quality focused on the Poor Stream Ratio (PSR) metric, TCP usage, wired and wireless subnets, and identifying the use of HTTP proxies and VPN.
* **Endpoints:** Audio devices and client versions (Skype for Business only).
* **Service Management:** This category comprises two sections:
  + First is Microsoft’s responsibility to manage and maintain the Teams and Skype for Business Online services.
  + Second are tasks your organization must manage to ensure reliable access to the service, such as updating building information and maintaining firewalls for new Office 365 IP addresses as infrastructure is added to the service.

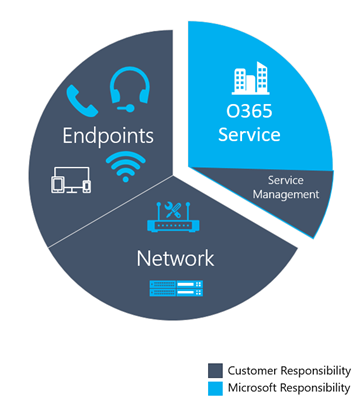


Figure 3 - Critical categories for Teams and Skype for Business Online deployment

The graphic below outlines the tasks you must execute for each category. We recommend that you run these tasks once a week, at a minimum.

The first time you perform these tasks will take more effort than subsequent iterations, because many of these categories require that you validate your deployment configurations. After you’ve achieved the state you want by meeting the targets you’ve defined, performing these tasks will help you maintain that state.

### Service management tasks

In a cloud-first world, you must perform certain service management tasks to maintain high-quality user experiences. These tasks range from ensuring there is sufficient bandwidth to reach the service without saturating internet links, validating that quality of service (QoS) is in place on all managed network areas, and—lastly—staying on top of [Office 365 IP ranges on firewalls](https://aka.ms/o365ips).

### Network tasks

There are two categories of network tasks: reliability and quality. Reliability focuses on measuring the user’s ability to make calls successfully and stay connected. Quality focuses on the aggregated telemetry sent to Teams and Skype for Business Online by the user’s client during the call and after it has ended.

Given the critical impact that reliability has on the user experience, it’s important to begin assessing and investigating those metrics before diving into quality.

### Endpoints tasks

The main task in this category is validating which client versions are running Skype for Business on desktop builds from the last six months, to ensure users are getting the benefit of the continual optimizations made to the Skype for Business desktop client. Additionally, this simplifies overall client management tasks and provides a consistent user experience.

The other important area is monitoring which devices are prevalent in your deployment and driving the use of certified devices to provide the best user experience.

|  |  |
| --- | --- |
| Important | Currently, Teams clients are distributed and updated automatically through the Azure Content Delivery Network and will be kept up to date by the service. Client readiness and investigative activities aren’t applicable to Teams. |

# CQD basics

This section describes the fundamentals of working with CQD. Guidance is given for the following topics:

* What is CQD?
* Expectations using CQD
* Finding your tenant ID
* Reporting on Microsoft Teams versus Skype for Business
* First versus second classifications
* Dimensions, measures, and filters
* Streams versus calls
* Good, poor, and unclassified calls
* Common subnets

For more in-depth training and resources, see the [Appendix](#_Appendix).

## What is CQD?

You use the Call Quality Dashboard (CQD) to gain insight into the quality of calls made by using Teams and Skype for Business services. CQD is designed to help Skype for Business and Teams admins and network engineers optimize the network and keep a close eye on quality, reliability, and the user experience. CQD looks at aggregate telemetry for an entire organization where overall patterns can become apparent, allowing staff to make informed assessments and plan remediation activities to maximize impact. CQD provides reports of metrics that provide insight into overall quality, reliability, and user experience.

|  |  |
| --- | --- |
| Note | CQD doesn’t contain any personally identifiable information (PII). PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. |

This guide will help in understanding the core concepts of CQD to help maximize the impact you can make in improving your users’ experience with Teams or Skype for Business Online. Additional CQD resources can be found in the [Appendix](#_Appendix).

## Expectations using CQD

CQD, although useful for analyzing trends and subnets, doesn’t always provide a specific cause for a given scenario. It’s important to understand this and set the correct expectation when using CQD:

* CQD won’t provide the root cause for every scenario.
* CQD won’t contain Phone System or Audio Conferencing streams.
* CQD will call out areas for further investigation based on trends.
* CQD doesn’t contain any PII.

## Report editions

There are two report editions in CQD Online: Summary and Detailed. Use the drop-down menu located in the blue bar at the top of the screen to open a report edition. The name of the selected report edition is displayed at the top of the screen.

* Summary reports are static and can’t be edited, downloaded, or exported.
* Detailed reports are fully customizable and can be downloaded to a CSV file, exported, or cloned.

For a full description of the difference between the two editions, see [this article](https://docs.microsoft.com/microsoftteams/turning-on-and-using-call-quality-dashboard).

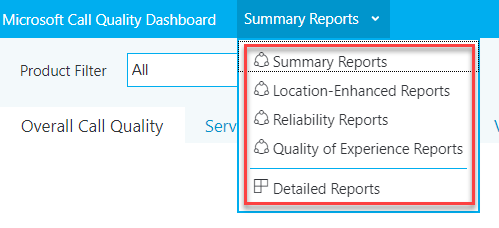


Figure 4 - CQD report categories

The summary reports are divided into four categories:

* **Summary Reports** focus on analyzing quality trends with daily, monthly, and table reports to assist with identifying subnets that have poor quality. This is the default landing page when you first sign in to CQD Online.
* **Location-Enhanced Reports** focus on analyzing quality trends based on location information. To use these reports, you must have uploaded a building file.
* **Reliability Reports** focus on analyzing reliability trends for audio, video, video-based screen sharing (VBSS), and app sharing.
* **Quality of Experience Reports** are a “slimmed-down” version of the detailed QER templates, focusing on key areas for analyzing audio quality and reliability.

## Report types

You can choose from two types of reports in CQD, depending on how you want to view your data. Although this guide doesn’t cover the specifics of creating one type of report over another, the QER CQD templates provide a mix of customizable chart and table reports for you to use:

* **Chart** reports create graphical bar charts to represent data in a visual format. Chart reports are best used to visualize data over a given time period.
* **Table** reports are useful for looking at individual measurements and dimensions where you can export the reports to CSV files for manipulation in Microsoft Excel.

## Tenant ID

Some CQD reports require that you include a filter for your tenant ID. Due to the way CQD aggregates data, federated participant telemetry is included. Although this can prove valuable when analyzing trends, client and device reports require that you filter data to a specific tenant to exclude federated participant telemetry. If you don’t know your tenant ID, you can use one of the following methods to find it.

Note: These methods require the following permissions:

* Global Administrator Role
* Skype for Business Administrator Role

### Azure portal

1. Sign in to the Microsoft Azure portal: [https://portal.azure.com](https://portal.azure.com/)
2. Select **Azure Active Directory**.
3. Under **Manage**, select **Properties**. The tenant ID is shown in the **Directory ID** box.

### Azure PowerShell

1. [Install the Microsoft Azure PowerShell Service Management module](https://docs.microsoft.com/powershell/azure/servicemanagement/install-azure-ps?view=azuresmps-4.0.0).
2. Open an Azure PowerShell command window and run the following script, entering your Office 365 credentials when prompted:  
   **Login-AzureRmAccount**
3. The tenant ID is listed in the output.

### Skype for Business Online Admin Center

1. Go to [https://portal.office.com](https://portal.office.com/).
2. Sign in with your tenant administrator organizational account.
3. Select **Skype for Business** under **Admin Centers**.
4. The tenant ID is listed as **Organization ID** on the Welcome page.

### Skype for Business Online using PowerShell

1. [Set up your computer for Windows PowerShell](https://docs.microsoft.com/SkypeForBusiness/set-up-your-computer-for-windows-powershell/set-up-your-computer-for-windows-powershell).
2. Run the following command:  
   **(Get-cstenant).tenantid**
3. The tenant ID is displayed as a GUID.

## Teams vs. Skype for Business

CQD can report on both Teams and Skype for Business telemetry. However, there might be times when you want to develop a report to look at Teams telemetry separate from Skype for Business.

### Summary reports

To modify the summary reports page to look at only Teams or Skype for Business, select the **Product Filter** drop-down menu from the top of the screen, and then select the product you want.

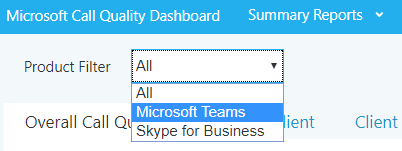


Figure 5 - Select a Product Filter

### Detailed reports

To filter all detailed reports, in the browser bar, append the following to the end of the URL:

/filter/[AllStreams].[Is Teams]|[FALSE]

**Example:**https://cqd.lync.com/cqd/#/1234567/2018-5/filter/[AllStreams].[Is Teams]|[FALSE]

For more information about URL filters, see [Filtering reports](#_Filtering_reports) later in this section.

To filter an individual detailed report, add the filter **Is Teams** to the report and set it to True or False. For more information, see [Editing reports](#_Editing_Reports) later in this section.

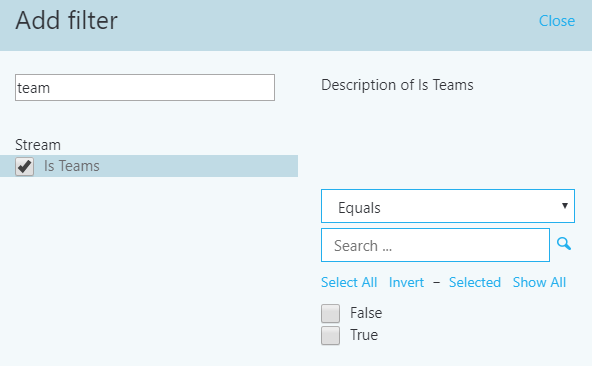


Figure 6 - Adding a Teams filter to a report

## Managed vs. unmanaged networks

By default, all endpoints in CQD are classified as external. As soon as a building file is introduced, we can begin to look at managed endpoint data. As previously discussed, networks in CQD are defined as:

* A *managed* network, often referred to as internal or inside, can be influenced and controlled by the organization. This includes the internal LAN, the remote WAN, and VPN.
* An *unmanaged* network, often referred to as external or outside, can’t be influenced or controlled by the organization. An example of an unmanaged network is a hotel or airport network.

## Dimensions, measures, and filters

A well-formed CQD query contains all three of the following parameters:

* **Dimension:** How I want to pivot on the data.
* **Measure:** What I want to report on.
* **Filter:** How I want to reduce the dataset the query returns.

Another way to look at this is that a *dimension* is the grouping function, a *measure* is the data I’m interested in, and a *filter* is how I want to narrow down the results to those that are relevant to my query.

An example of a well-formed query is "Show me Poor Streams [Measure] by Subnet [Dimension] for Building 6 [Filter]." For more information, see [Dimensions and measures available in CQD](https://aka.ms/cqd-dm).

## First vs. second

Many of the dimensions and measures in CQD are classified as either first or second. CQD doesn’t use caller/callee fields—these have been renamed *first* and *second* because there are intervening steps between the caller and callee. The following logic determines which endpoint involved is labeled as first:

* **First** will always be a server endpoint (Conference Server, Mediation Server, and so on) if a server is involved in the stream or call.
* **Second** will always be a client endpoint unless the stream is between two server endpoints.
* If both endpoints are the **same type**, the choice of which is first is based on internal ordering of the user agent category. This ensures the ordering is consistent.

For more information about determining the first or second endpoint when they’re both the same, see [Dimensions and measures available in CQD](https://aka.ms/cqd-dm).

## Stream vs. call

You need to understand the difference between a call and a stream to properly choose which dimensions or measures you’ll be looking at in CQD. Although CQD’s primary focus is on streams, call-based measurements are also available.

* **Stream:** A *stream* exists between only two endpoints. There is only one stream for each direction, and two streams are required for communication. Streams are useful for investigating buildings, networks, or subnets. In some cases, both call and stream are used in the measurement’s name (for example, Call Setup Stream or Call Dropped Stream). These are still classified as streams.
* **Call:** A *call* is a grouping of all streams from all endpoints in a meeting or peer-to-peer call. A call consists of—at minimum—two streams. A single call will have at least two endpoints, each with a minimum of one stream.

For additional guidance on whether the dimension or measure is referring to a call or a stream, see [Dimensions and measures available in CQD](https://aka.ms/cqd-dm).

## Good, poor, and unclassified calls

A call is categorized either as good, poor, or unclassified. Let’s take a moment to talk about each one in more detail.

* **Good or poor:** A good or poor call consists of a call that contains a complete set of service metrics, for which a full QoE report was generated and received by the service. Determining whether a stream is good or poor is described [earlier in this guide](#_Poor_Call_RatioCR).
* **Unclassified:** An unclassified stream doesn’t contain a full set of service metrics. These can be short calls—usually less than 60 seconds—where averages couldn’t be computed and a QoE report wasn’t generated. The most common reason for calls to be unclassified is that there was little to no packet utilization. An example of this would be a participant who joins a meeting on mute and never speaks. The participant is receiving, but not transmitting, media. Without media being transmitted, there won’t be any metrics available for CQD to use to classify the endpoint’s outbound media stream.

For more information about the stream classification process, see [this article](https://docs.microsoft.com/microsoftteams/stream-classification-in-call-quality-dashboard).

## Common subnets

Common subnets are specific private subnets that are used by hotels, home networks, hotspots, and similar areas. These subnets are difficult to triage due to their widespread use. If your organization uses one of these common subnets, we recommend that you move that network to another subnet. This will make reporting easier in CQD. When noted, reports in the All Networks template have been configured to exclude these subnets to eliminate them as a source of poor quality. Common subnets are defined below; their impact will vary by organization.

* 10.0.0.0/24
* 192.168.0.0/24
* 192.168.1.0/24
* 192.168.2.0/24
* 172.20.10.0/24
* 192.168.43.0/24

When investigating a managed network that uses a common subnet, you’ll need to use the Second Reflexive Local IP dimension to group subnets. This dimension contains the endpoint’s public IP address.

# CQD Online

This section describes the fundamentals of accessing CQD. Guidance is given for the following topics:

* Accessing CQD online
* Getting started with CQD
* Editing reports in CQD
* Filtering reports in CQD
* Importing reports in CQD

For more in-depth training and resources, see the [Appendix](#_Appendix).

## Accessing CQD online

You can access CQD one of three ways.

* Go to [https://cqd.lync.com](https://cqd.lync.com/).
* Go to **Microsoft Teams & Skype for Business Admin Center**, and select the link to CQD, as shown in the following illustration.

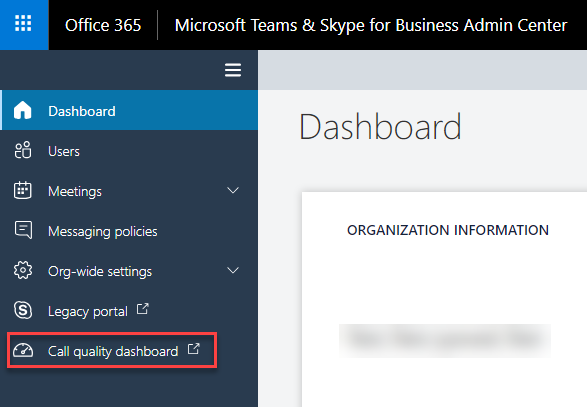


Figure 7 - Accessing CQD through the Microsoft Teams & Skype for Business Admin Center

* Go to the legacy **Skype for Business admin center** > **tools**, and select the link to CQD, as shown below.

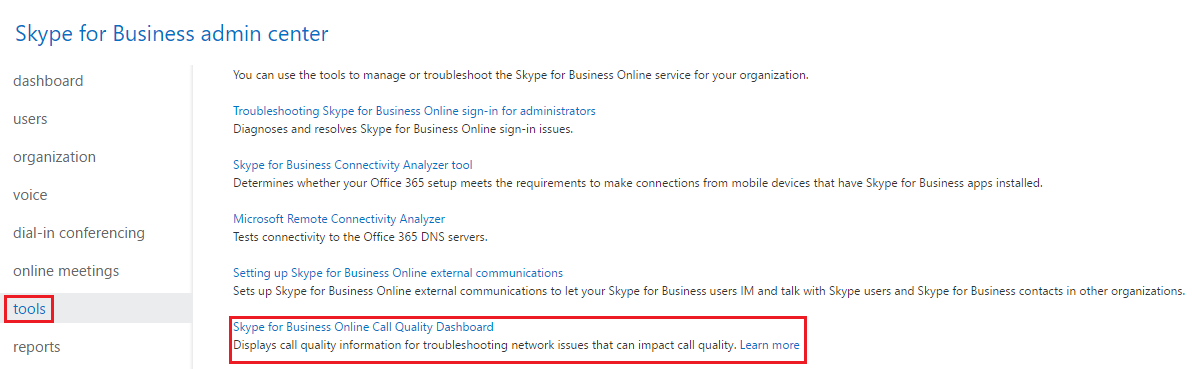


Figure 8 – Accessing CQD through the Skype for Business admin center

## Getting started

When you first browse to CQD, you’ll see the Summary Reports page. The reports described in this guide are custom detailed reports. To get started using the detailed reports, select **Summary Reports** at the top of the page, and then choose **Detailed Reports**.

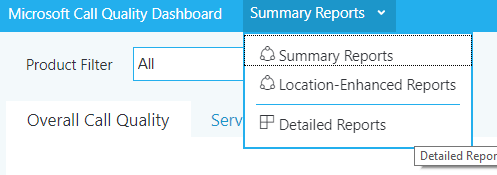


Figure 9 - Navigating to Detailed Reports

The Detailed Reports page in CQD looks like the figure shown below.



Figure 10 - Detailed Reports page

1. The summary pane shows context for the report set that appears to the right.
2. You can select **Edit** in the summary pane to set report-level properties (including y-axis height) and to import new templates.
3. The breadcrumb helps users identify their current location in the report set hierarchy.
4. Reports that have child reports are shown with a blue link. By selecting the link, you can drill down to the child reports.

Point to bar charts and trend lines in the report to display detailed values. The report that has focus will show the action menu: **Edit**, **Clone**, **Delete**, **Download**, and **Export Report Tree**.

## Editing reports

When you select **Edit** on the action menu of a report, you’ll open Query Editor. Each report is backed by a query to CQD. A report is a visualization of the data returned by its query. The Query Editor is a UI for editing these queries in addition to the display options for the report, as illustrated in the following figure.

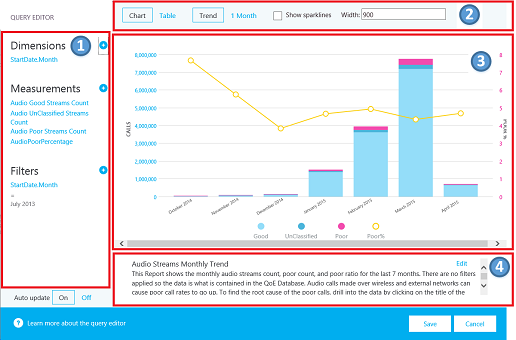


Figure 11 - Query Editor

1. You choose dimensions, measures, and filters from the left pane. Pointing to an existing value displays a close button (**X**) you can select to remove the value.
   * By selecting the dimension or measure, you can change the title by editing the **Title** field. You can also change the order by selecting the blue Up or Down arrows in the top pane.
   * Selecting (**+**) next to a heading opens the dialog box for adding a new dimension, measure, or filter.
   * Enter the first few letters of the dimension, measure, or filter in the **Find a** field to filter the list for easier searching.
2. The top pane shows options for chart customization.
3. The Query Editor shows a preview of the report.
4. Use the **Edit** box at the bottom of the screen to create or edit a detailed description of the report.

## Filtering reports

The templates provided include several built-in queries and report filters. The following sections describe the most common filters used throughout the templates.

### URL filter

You can use a URL filter to filter every report for a specific dimension. The most common URL filters are used to filter reports to exclude federated participant telemetry, or focus on Teams or Skype for Business Online. We recommend that when using filters, you bookmark them for easy reference.

Excluding federated data from CQD reports is useful when you’re remediating managed buildings or networks where federated endpoints might influence your reports.

To implement a URL filter, in the browser address bar, append the following to the end of the URL:

/filter/[AllStreams].[Second Tenant Id]|[YOUR TENANT ID HERE]

**Example:**https://cqd.lync.com/cqd/#/1234567/2018-08/filter/[AllStreams].[Second Tenant Id]|[TENANTID]

To filter the reports for Teams or Skype for Business, append the following to the end of the URL:

/filter/[AllStreams].[Is Teams]|[TRUE | FALSE]

**Example:**https://cqd.lync.com/cqd/#/1234567/2018-08/filter/[AllStreams].[Is Teams]|[TRUE]

|  |  |
| --- | --- |
| Note | The URL examples above are for visual representation only. Please use the default CQD link of [https://cqd.lync.com](https://cqd.lync.com/). |

### Query filters

Query filters are implemented by using the Query Editor in CQD. These filters are used to reduce the number of records returned by CQD, thus minimizing the report’s overall size and query times. This is especially useful for filtering out unmanaged networks. The filters below use regular expressions (RegEx).

Table 3 - Query filters

|  |  |  |
| --- | --- | --- |
| Filter | Description | CQD query filter example |
| No blank values | Some filters don’t have the option to filter for blank values. To filter blank values manually, use the blank expression and set the filter to Equals or Not Equals, depending on your needs. | Second Building Name <> ^\s\*$ |
| Exclude common subnets | Without a valid building file to separate managed from unmanaged networks, home networks will be included in the reports. These home subnets are outside the scope of IT’s control and can be quickly excluded from a report. Common subnets, as defined in this guide, are 10.0.0.0, 192.168.1.0 and 192.168.0.0. | Second Subnet <> 10.0.0.0 | 192.168.0.0 | 192.168.1.0 |
| View inside only | Used to filter a report for managed (inside) or unmanaged (outside). The managed CQD template is already preconfigured with these filters. | Second Inside Corp = Inside |

### Report filters

Report filters are implemented by adding a filter to the rendered report either in the Query Editor or directly to the report. The following report filters are used throughout the template. The report filter doesn’t affect query or load times.

Table 4 - Report filters

|  |  |  |
| --- | --- | --- |
| Filter | Description | CQD report filter example |
| Month | Start with the year first, then month. | 2018-08 |
| Alphabetic | Filters for any alphabetic characters. | [a-z] |
| Numeric | Filters for any numeric characters. | [0-9] |
| Percentage | Filters for a percentage. | ([3-9]\.)|([3-9])|([1-9][0-9]) |

## Import the CQD templates

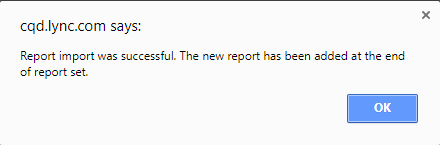
This guide includes [two curated CQD templates](https://aka.ms/qertemplates). These templates accelerate your usage of CQD and provide you an opportunity to quickly leverage CQD’s capabilities to make an impact on your users’ Teams or Skype for Business experience. The All Networks template, though optimized to work with a building data file, can be used while you work toward collecting and uploading building information into CQD, as described in the next section.

**To import the templates (.CQDX) into CQD Online**

1. Go to <https://cqd.lync.com>.
2. Authenticate by using your Office 365 Administrative credentials.

|  |  |
| --- | --- |
| Note | You must have the Office 365 Global Administrator, Skype for Business Administrator, or Report Readers role to access CQD. |

1. Select the **Summary Reports** menu at the top of the page, and then choose **Detailed Reports**.
2. On the summary pane, select **Import**. Go to the CQDX saved location, select the CQDX template, and then select **Open**.
3. After the template is uploaded, a pop-up window will display the message “Report import was successful.” Select **OK.**



1. Repeat steps 4 and 5 for the second CQD template.

|  |  |
| --- | --- |
| Note | The CQD templates are imported per user. If additional users need to use the report, they must sign in and import the templates into their CQD instance. |

# Building mapping

In a Microsoft Teams or Skype for Business Online deployment, all clients are external. That has the implication that by default, all clients are reported as outside in CQD Online, regardless of whether the client was connected on an internal corporate network.

When you work with CQD, you need to know the location of an endpoint and whether it was connected to a network you can manage or a network you can’t manage—the assumption being that you can only improve networks you can manage. By uploading subnet and building information to CQD Online, you enable CQD to determine whether the endpoint was connected to an internal corporate/managed network or to an external/unmanaged network.

## Building data file structure

The format of the data file you upload must meet the following requirements to pass the validation check before uploading.

* The file must be either a TSV file, which means that for each row, each column is separated by a Tab character, or a CSV file in which each column is separated by a comma.
* The file can’t be larger than 50 MB.
* The content of the data file *must not include table headers*. In other words, the first line of the data file must be real data, not column headings such as “Network.”
* For each column, the data type can only be String, Number, or Bool. If the data type is Number, the value must be a numeric value; if it’s Bool, the value must be either 0 or 1.
* For each column, if the data type is String, the data can be empty (but still must be separated by an appropriate delimiter—that is, a Tab character or comma). This just assigns that field an empty string value.
* There must be 14 columns for each row. Each column must have the data type described in the following table, and the columns must be in the order listed in the table.

Table 5 - Building file structure

|  |  |  |  |
| --- | --- | --- | --- |
| Column name | Data type | Example | Guidance |
| Network | String | 192.168.1.0 | Required |
| NetworkName | String | USA/Seattle/SEATTLE-SEA-1 | Required\* |
| NetworkRange | Number | 26 | Required |
| BuildingName | String | SEATTLE-SEA-1 | Required\* |
| OwnershipType | String | Contoso | Optional |
| BuildingType | String | IT Termination | Optional |
| BuildingOfficeType | String | Engineering | Optional |
| City | String | Seattle | Recommended |
| ZipCode | String | 98001 | Recommended |
| Country | String | US | Recommended |
| State | String | WA | Recommended |
| Region | String | MSUS | Recommended |
| InsideCorp | Bool | 1 | Required |
| ExpressRoute | Bool | 0 | Required |

\*While not required by CQD, the templates are configured to display Building and Network name.

### Supernetting

You can use supernetting, commonly called Classless Inter-Domain Routing (CIDR,) in place of defining each subnet. A *supernet* is a combination of several subnets that share a single routing prefix. Instead of adding an entry for each subnet, you can use the supernetted address. Supernetting is supported, but we don’t recommend using it.

For example, Contoso’s marketing building is made up of the subnets below:

* 10.1.0.0/24—first floor
* 10.1.1.0/24—second floor
* 10.1.2.0/24—third floor
* 10.1.3.0/24—fourth floor

Instead of adding an entry for each subnet, you can use the supernetted address—in this example, 10.1.0.0/22.

* Network = 10.1.0.0
* Network Range = 22

Here are a few things to consider before you implement supernetting:

* Supernetting can only be used in a subnet mapping with 8-bit to 28-bit mask.
* Supernetting takes less time up front, but it comes at the cost of reducing the richness of your data. Let’s say there’s a quality problem involving subnet 200.1.2.0. If you implemented supernetting, you won’t know where in the building the subnet is located or what type of network it is (for example, a lab). If you’d defined all the subnets for a building and uploaded floor location information, you’d be able to see that distinction.
* It’s important to ensure that the supernetted address is correct and isn’t catching unwanted subnets.
* It’s quite common to find 192.168.0.0 in data. For many organizations, this indicates that the user is at home. For others, this is the IP address scheme for a satellite office. If your organization does have offices that use this configuration, don’t include it in your building file because it’s difficult to distinguish between home and internal networks byusing common subnets. See the section [Common subnets](#_Common_Subnets), earlier in this guide.

|  |  |
| --- | --- |
| Important | The network range can be used to represent a supernet. All new building data file uploads will be checked for any overlapping ranges. If you’ve previously uploaded a building file, you should download the current file and upload it again to identify any overlaps and fix the issue. Any overlap in previously uploaded files might result in the wrong mappings of subnets to buildings in the reports. |

### VPN

The quality of experience (QoE) data that clients send to Office 365—which is where CQD data is sourced from—includes a VPN flag. CQD will see this as the First VPN and Second VPN dimensions. However, this flag relies on VPN vendors’ reporting to Windows that the VPN network adapter registered is a Remote Access adapter. Not all VPN vendors properly register Remote Access adapters. Because of this, you might not be able to use the built-in VPN query filters. There are two approaches to accommodating VPN subnets in the building information file:

1. Define a **Network Name** by using the text “VPN” in this field for VPN subnets.

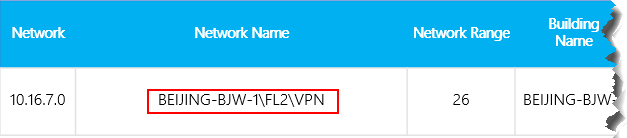


Figure 12 - VPN using network name

1. Define a **Building Name** by using the text “VPN” in this field for VPN subnets.

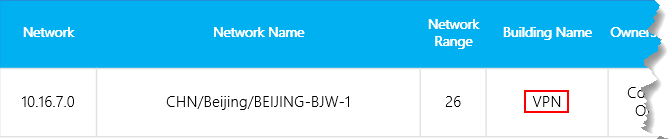


Figure 13 - VPN using building name

|  |  |
| --- | --- |
| Important | Certain VPN implementations don’t accurately report subnet information. If this occurs in your reporting, we recommend that when you add a VPN subnet to the building file, instead of one entry for the subnet, add separate entries for each address in the VPN subnet as a separate 32-bit network. Each row can have the same building metadata. For example, instead of one row for 172.16.18.0/24, you have 253 rows, with one row for each address from 172.16.18.1/32 through 172.16.18.254/32, inclusive. |

|  |  |
| --- | --- |
| Note | VPN connections have been known to misidentify the network connection as wired when the underlying internet connection is wireless. When looking at quality over VPN connections, you can’t assume that the connection type has been accurately identified. |

## Uploading building information

The CQD Summary Reports dashboard includes a **Tenant Data Upload** page, accessed by selecting the **Tenant Data Upload** link tag in the upper-right corner (look for the gear icon). This page is used for admins to upload their own information, such as mapping of IP address and geographical information, mapping each wireless access point and its MAC address, and so on.

1. Go to CQD Online by browsing to [https://cqd.lync.com](https://cqd.lync.com/).
2. Select the gear icon in the upper-right corner, and choose **Tenant Data Upload** from the **Summary Reports** page.

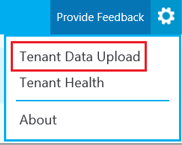


Figure 14 - Tenant Data Upload menu

1. Alternatively, if this is your first time visiting CQD, you’ll be asked to upload building data. You can select **Upload Now** to quickly navigate to the **Tenant Data Upload** page.

Screenshot of a banner in the Call Quality Dashboard that notifies a user to upload building data.

Figure 15 - Building data upload banner

1. On the **Tenant Data Upload** page, select **Browse** to choose a data file.
2. After selecting a data file, specify **Start date** and, optionally, specify an end date.
3. After selecting **Start date**, select **Upload** to upload the file to the CQD.

Before the file is uploaded, it’s validated. If validation fails, an error message is displayed requesting that you correct the file. The following figure shows an error occurring when the number of columns in the data file is incorrect.

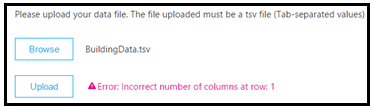


Figure 16 - Building data upload error

1. If no errors occur during validation, the file upload will succeed. You can then see the uploaded data file in the **My uploads** table, which shows the full list of all uploaded files for the current tenant at the bottom of that page.

|  |  |
| --- | --- |
| Note | It can take up to four hours to finish processing the building file. |

|  |  |
| --- | --- |
| Note | If you’ve already uploaded a building file and need to add subnets that might have been missed or excluded, modify the original file by adding the new subnets, remove the current file, and re-upload the newly edited file. There can be only one active building data file in CQD. |

## Updating a building file

While gathering building and subnet information, administrators will often upload the building file in multiple iterations over time, adding new subnets and their building information as it becomes available. When this occurs, you’ll need to re-upload your building file. This process is like the initial upload as described in the previous section, with a few exceptions as noted below.

|  |  |
| --- | --- |
| Important | Only one building file can be active at a time. Multiple building files aren’t cumulative. |

### Adding net new subnets

There are times when you’ll need to add net new subnets to CQD that weren’t originally part of your network topology. To add net new subnets, do the following in the CQD Tenant Data Upload portal:

1. Edit the original building file and provide an end date that occurs at least one day before the net new subnets were acquired.
2. Download the original file, if you don’t already have an up-to-date copy.
3. Append the net new subnets to the original building file.
4. Upload the newly modified building file following the same process as above, and set the start date for one day after the previous building file ends.

### Updating the current building file

If a building file is already uploaded but you need to add missing subnets, do the following in the CQD Tenant Data Upload portal:

1. Download the original file, if you don’t already have an up-to-date copy.
2. Remove the current file in CQD.
3. Append the new subnets to the original file.
4. Upload the building file. Be sure to set the start date to at least eight months prior so that CQD will process historical data.

## Missing subnets

After you upload building information for managed networks, every managed network should have a building association. However, this won’t always be the case; typically, a few subnets are missed. This section covers how to validate those missing networks.

Browse to the **Detailed Reports** page in CQD Online and navigate to the **Missing Subnet Report** included in the CQD templates. This presents all the subnets with 10 or more audio streams that aren’t defined in the building data file and are being marked as outside. Ensure that there are no managed networks in this list. If subnets are missing, update the original building data file and re-upload it to CQD.

|  |  |
| --- | --- |
| Important | You’ll need to add your tenant ID as a query filter for **Second Tenant ID** to this report to filter the report to view only your organization’s tenant data. Otherwise, the report will show federated subnets. |

|  |  |
| --- | --- |
| Note | Be sure to adjust the Month Year report filter to the current month. Select **Edit**, and adjust the **Month Year** report filter to save the new default month. |

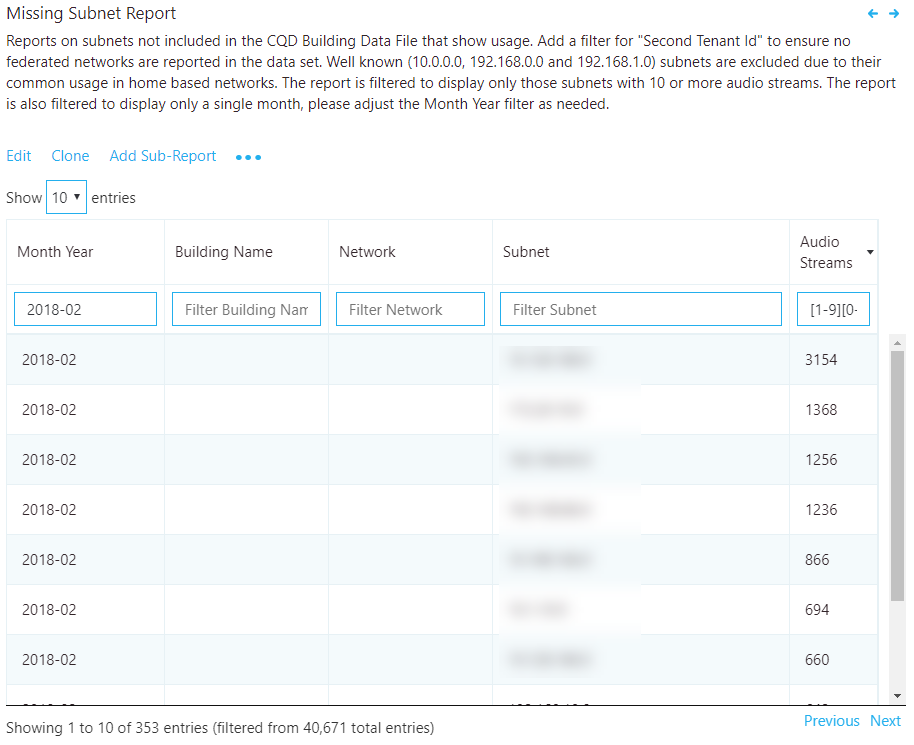


Figure 17 - Missing Building Report

## Building mapping tools

Let’s face it, mapping out subnets in your organization can be difficult. Large global networks are very complex, with different teams managing their respective regions, and there might be no single source of truth for the network topology. There are two tools available to assist with starting the building mapping exercise, described below.

### CQD tools

These tools are based on PowerShell and can leverage Active Directory (AD) Sites and Services and Microsoft DHCP services to help pre-populate your building file. These tools will help with the following tasks:

1. Query AD Sites and Services, and create a building file based on the information contained within.
2. Query a Microsoft DHCP server or servers to pull subnet information and automatically create a building file.
3. Validate an existing building file, checking for duplicates and overlaps.
4. Find unmapped subnets in CQD.

For more information about this tool, see [this blog post](https://aka.ms/cqdtools).

### Network Planner

The Network Planner determines and organizes your network requirements for your Cloud Voice deployment in just a few simple steps. By providing your organization's networking details and Cloud Voice usage, you can get an approximate calculation of the network requirements for your Cloud Voice deployment, manage and export these details for reporting, and view areas for further investigation and next steps.

Although the Network Planner doesn’t automate the building mapping process entirely, after network information is entered into the Network Planner it can then be exported to a building file ready for upload.

We highly recommend that you leverage the Network Planner when deploying media workloads on your network to assess the overall impact.

For more information about the Network Planner, visit [MyAdvisor](https://myadvisor.fasttrack.microsoft.com/CloudVoice/NetworkPlanner).

# Diagnostic alerts

Microsoft proactively monitors CQD telemetry to create diagnostic alerts for known issues that negatively affect the user experience. These alerts are then automatically delivered to the service administrator via the message center. The following table outlines the diagnostic alerts that are shown in the message center, along with links to more information.

Table 6 - Diagnostic alerts

|  |  |
| --- | --- |
| Alert | More information |
| Known poorly performing client versions are in use | [Client versions](#_Determine_Client_Versions) |
| Audio drivers are causing call drops | [Devices](#_Devices_Investigations) |
| Restrictions in the firewall are causing call setup failures | [Setup failure investigations](#_Setup_failure_investigations) |
| Deep packet inspection is causing call setup failures | [Setup failure investigations](#_Setup_failure_investigations) |
| Meeting room devices on Wi-Fi networks are causing poor call quality | [Quality investigations](#_Quality_investigations) |
| UDP traffic is being limited, which causes poor call quality | [TCP](#_TCP) |
| VPN usage is affecting call quality | [Quality investigations](#_Quality_investigations) |

## Message center

The message center alerts you about new updates, features, or issues. The message center is available within the Office 365 admin center to service administrators. Each post provides a high-level overview of how the update, feature, or issue affects your users, and gives links to more detailed information.

To open the message center, in the Office 365 admin center, go to **Health** > **Message center**, or select the message center card on the **Home** dashboard. The dashboard displays the last three messages that were posted and links to the full message center page.

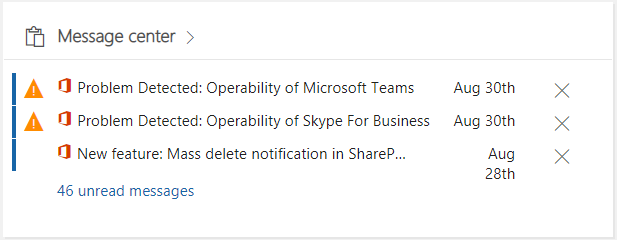


Figure 18 - Message center card

You can also use the [Office 365 Admin app](https://go.microsoft.com/fwlink/p/?linkid=627216) on your mobile device to view the message center, which is a great way to stay current with push notifications. For more information, see [this article](https://support.office.com/article/Message-center-in-Office-365-38FB3333-BFCC-4340-A37B-DEDA509C2093).

# Reliability investigations

The first step to improving quality is to assess the state of reliability across the organization. Because reliability is vital to a positive user experience, we start with the two components that measure reliability:

1. **Setup Failures:** The call couldn’t be established.
2. **Drop Failures:** The call was established and unexpectedly terminated.

Throughout this section, we’ll cover methods to investigate both areas.

|  |  |
| --- | --- |
| Note | Not all reports included in the templates are covered in this guide. However, the methods of investigation explained below still apply. Please refer to the individual report description for more information. |

## Setup failures

Prioritize remediating setup failures in this area first, because these failures have a significant negative impact on the user experience.

Begin your investigation by assessing the percentage of overall setup failures for the organization, and then prioritize areas of investigation based on the highest percentage by building or network.

### Setup failure trend analysis

This report displays the total amount of streams, stream setup failures and the stream setup failure rate. Point to any one of the columns to display its individual values, as shown in the figure below.



Figure 19 - Audio Reliability - Stream Setup Failures

#### Analysis

By using this report, you can answer the following questions and determine your next course of action:

* What is the total stream setup failure rate for the current month?
* Is the total stream setup failure rate below or above the defined target metric?
* Is the failure trend worse or better than the previous month?
* Is the failure trend increasing, steady, or decreasing?

Irrespective of the previous answers, take the time to investigate further by using the companion sub-reports to look for any individual buildings or subnets that might need remediation. Although the overall failure rate might be below the target metric, the failure rates for one or more buildings or networks might be above the target metric and need investigation.

### Setup failure investigations

This summary report is used to discover and isolate any buildings or subnets that might need remediation.

|  |  |
| --- | --- |
| Note | Be sure to adjust the Month Year report filter to the current month. Select **Edit**,and adjust the **Month Year** report filter to save the new default month. |

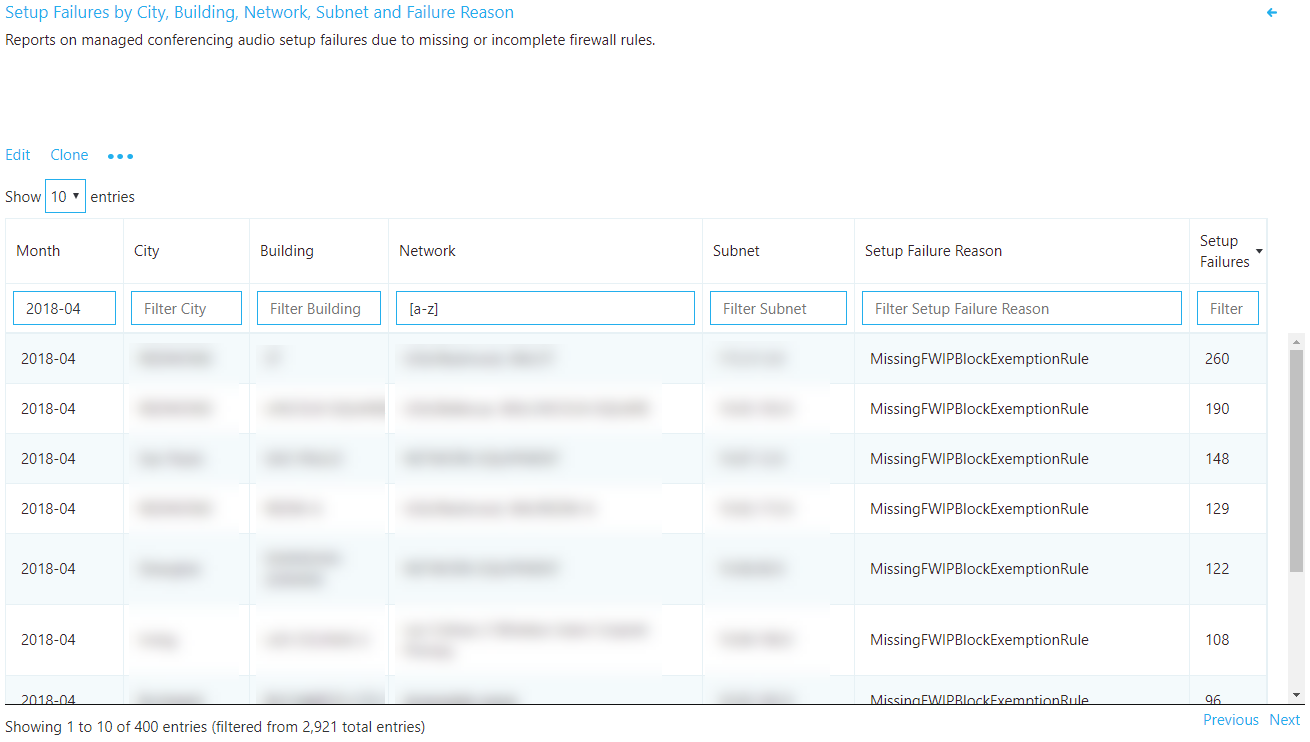


Figure 20 - Audio Setup Failures by Subnet

#### Diagnostic alert

If you received a diagnostic alert “Restrictions in the firewall are causing call setup failures” or “Deep packet inspection is causing call setup failures,” focus your remediation efforts on those identified subnets first. The alert has identified subnets that are negatively affecting call reliability. You can use the Setup Failures reports found in the Reliability section to assist with the remediation.

#### Remediation

Focus your first remediation efforts on buildings or subnets that have the largest volume of failures. This will maximize impact on the user experience and help to quickly reduce the rate of organizational call setup failures. The following table lists the two reasons for setup failures as reported by CQD.

Table 7 – Reasons for Call Setup Failures

|  |  |
| --- | --- |
| Call Setup Failures reason | Typical cause |
| Missing FW Deep Packet Inspection Exemption Rule | Indicates that network equipment along the path prevented the media path from being established due to deep packet inspection rules. This is likely due to firewall rules not being correctly configured. In this scenario, the TCP handshake succeeded but the SSL handshake didn’t. |
| Missing FW IP Block Exception Rule | Indicates that network equipment along the path prevented the media path from being established to the Office 365 network. This might be due to proxy or firewall rules not being correctly configured to allow access to IP addresses and ports used for Teams and Skype for Business traffic. |

Now as you begin your remediation, you can focus your efforts on a particular building or subnet. As the preceding table shows, these issues are due to firewall or proxy configurations. Review the options in the following table for remediation actions.

Table 8 - Next Steps for Call Setup Failure Remediation

|  |  |
| --- | --- |
| Remediation | Guidance |
| Configure firewall(s) | Work with your network team and verify your firewall(s) configuration against [the Office 365 IP address list](https://aka.ms/o365ips).  Verify that the [media subnets](https://support.office.com/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2#bkmk_teams) and ports are included in the firewall rules.  Verify that the necessary ports (listed below) are opened in the firewall. UDP should be given priority because TCP is considered a failback protocol for audio, video, and video-based screen sharing, and its use will affect the quality of the call. Legacy RDP application sharing uses TCP only.   * **TCP:** port 443 * **UDP:** ports 3478–3481 |
| Verify | Use the [Microsoft Network Assessment Tool](https://www.microsoft.com/download/details.aspx?id=53885) to verify connectivity from the affected building or subnet by using the connectivity check function. |

## Drop failures

Unlike setup failure codes, CDQ has no drop failure code to indicate why drop failures occur, which makes it difficult to isolate a specific root cause. To better triage drop failures, use an inferred approach. By remediating any areas of interest for media, patching clients and drivers, and driving usage of certified devices for Teams and Skype for Business, you can expect drop failures to decline.

### Drop failure trend analysis

This report displays the total amount of audio streams, total drop failures, and the drop failure rate. Point to any one of the columns to display its values, as shown in the following figure.

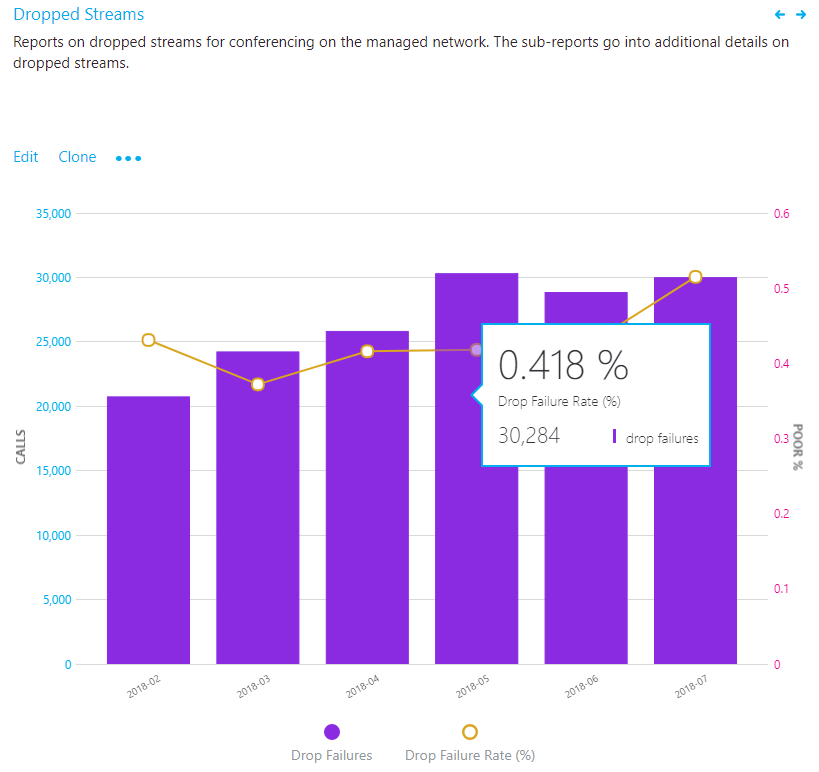


Figure 21 – Dropped stream rate

#### Analysis

By using this type of report, you can answer the following questions:

* What is the current drop failure rate?
* Is the drop failure rate below the defined target metric?
* Is the failure trend worse or better than the previous month?
* Is the failure trend increasing, steady, or decreasing?

Irrespective of the answers to the questions above, take the time to investigate using the sub-reports to look for any buildings or networks that might need remediation. Although the overall drop failure rate might be below the target metric, the drop failure rate for one or more buildings or networks might be above the target metric and need investigation.

### Drop failure investigations

Failures reported here indicate that the call was dropped unexpectedly and resulted in a negative user experience. Unlike the trending reports, these reports provide additional insights into specific subnets that need further investigation.

|  |  |
| --- | --- |
| Note | Be sure to adjust the Month Year filter to the current month. Select **Edit**, and adjust **Month Year** to save the new default month. |

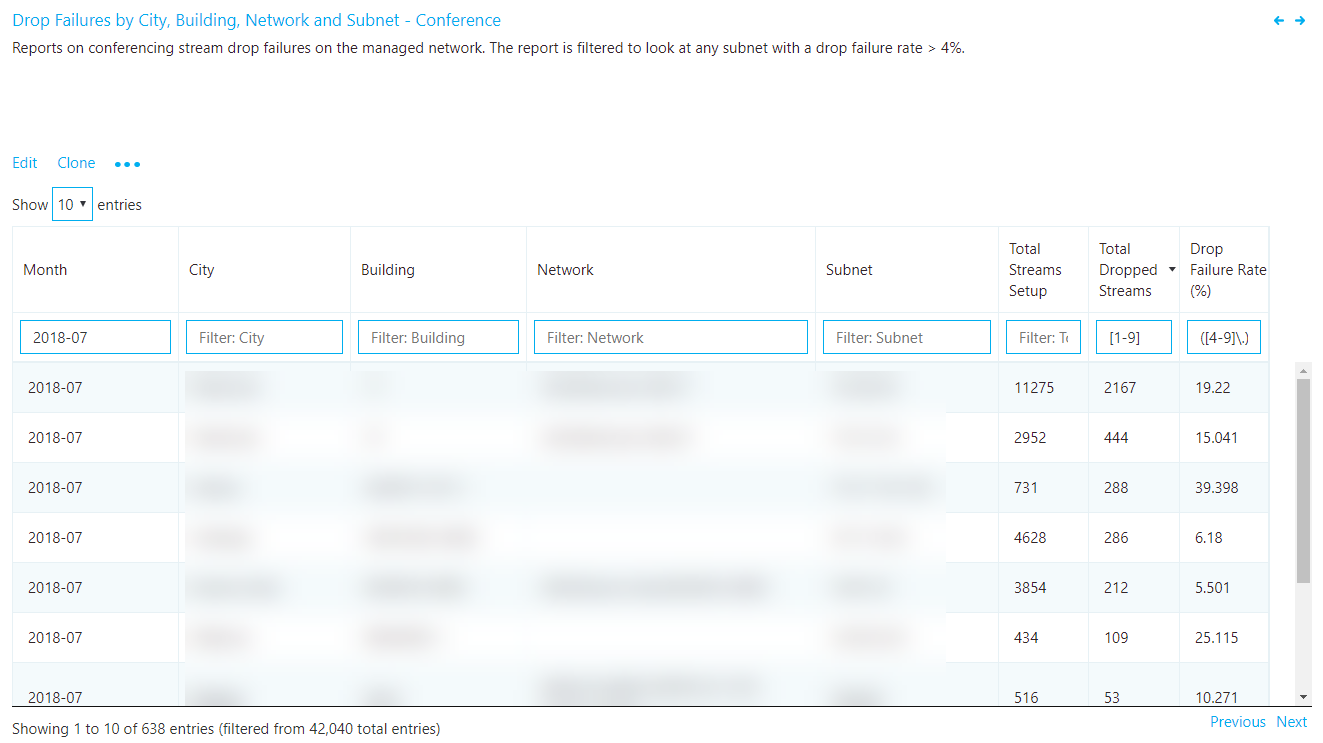


Figure 22 – Drop failures by subnet

#### Remediation

Using the included table reports, you can isolate problem areas in the network where the drop rate is above the target metric you’ve defined. Focus your first remediation efforts on buildings or subnets that have the highest total stream count, to make the biggest impact.

Common causes of call drops:

* Under-provisioned network or internet egress
* No QoS configured on constrained networks
* Older client versions
* User behavior

After you discover your problem areas, you can leverage [Call Analytics](https://techcommunity.microsoft.com/t5/Skype-for-Business-Blog/Introducing-Call-Analytics/ba-p/57309) to further review users in that building for specific issues. Call Analytics contains PII data and can be useful for further isolating potential reasons for the drop failures.

Regardless of your next step, it’s a good practice to notify the helpdesk that an issue has been discovered with specific buildings or subnets. This way, they can quickly respond to incoming calls and triage users more efficiently. Flagged users can then be reported back to the engineering team for further investigation.

The following table lists some common methods to manage and remediate drop failures.

Table 9 - Next steps for call drop remediation

|  |  |
| --- | --- |
| Remediation | Guidance |
| Network/internet | **Congestion**: Work with your network team to monitor bandwidth at specific buildings/subnets to confirm that there are issues with overutilization. If you do confirm that there is network congestion, consider increasing bandwidth to that building or applying QoS. Use the included [Quality Poor Stream summary reports](#_Quality_investigations) to review the problem subnets for issues with jitter, latency, and packet loss, because these will often precede a dropped stream.  You can also leverage the [Network Planner Tool](https://myadvisor.fasttrack.microsoft.com/CloudVoice/NetworkPlanner) to help better understand your organization’s bandwidth needs.  **QoS:** If increasing bandwidth is impractical or cost-prohibitive, consider implementing QoS. This tool is very effective at managing congested traffic and can guarantee that media packets on the managed network are prioritized above non-media traffic. Alternatively, if there’s no clear evidence that bandwidth is the culprit, consider these solutions:   * [Microsoft Teams QoS guidance](https://docs.microsoft.com/MicrosoftTeams/qos-in-teams) * [Skype for Business QoS guidance](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=5_1_0_8)   **Perform a network readiness assessment:** A network assessment provides details about expected bandwidth usage, how to cope with bandwidth and network changes, and recommended networking practices for Microsoft Teams and Skype for Business. Using the preceding table as your source, you have a list of buildings or subnets that are excellent candidates for an assessment.   * [Microsoft Teams Network Readiness Assessment](https://docs.microsoft.com/MicrosoftTeams/3-envision-evaluate-my-environment#test-the-network) * [Skype for Business Network Readiness Assessment](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Offers/?pageState=NetworkReadiness)   **Microsoft Network Assessment Tool:** Use this tool for a simple test of network performance to determine how well the network would perform for a Teams or Skype for Business Online call. The tool helps you assess the performance of a subnet and validate the readiness of the network against Microsoft performance [requirements](https://aka.ms/performancerequirements).   * [Download the Network Assessment Tool](https://www.microsoft.com/download/details.aspx?id=53885) |
| Clients  (Skype for Business Online only) | Some older clients have known, documented issues with media reliability. Review the Call Analytics reports from multiple affected users, or create a custom Client Version table report in CQD filtered to specific buildings or subnets with Total Call Dropped Failure % measure. This information will help you understand whether a relationship exists between call drops in that specific building and a specific version of the client. |
| Devices | We recommend that any users who are experiencing call drops—or poor calls in general—and are using integrated devices should be provisioned a [certified headset or speakerphone](http://partnersolutions.skypeforbusiness.com/solutionscatalog/personal-peripherals-pcs) to eliminate this as a potential source of poor quality and reliability. |
| User Behavior | If you determine that neither network, devices, or clients are the issue, consider engaging [My Advisor](https://aka.ms/myadvisor) for guidance in developing a user adoption strategy to educate users how to best join and exit meetings. A smarter Teams and Skype for Business user will produce a better user experience for all participants in the meeting. A user who puts their laptop to sleep (by closing the lid) without exiting the meeting will be classified as an unexpected call drop. |

# Quality investigations

The next step to assess the state of audio quality across the organization is to investigate Poor Stream Rate (PSR), TCP, and proxy usage. It’s important to remember that CQD data doesn’t provide you a specific root cause, but instead provides you with likely problem areas to begin a collaborative conversation with the appropriate teams for remediation activities.

|  |  |
| --- | --- |
| Note | Not all reports included in the templates are covered in this guide; however, the methods of investigation explained below will still apply for those reports. Refer to the individual report description for more information. |

## Quality

The PSR percentages are used to indicate whether the organization is meeting defined metric targets for a given focus area. It’s important to note that even if the high-level percentages are within the defined target, individual subnets or buildings might not meet the defined targets and, therefore, need further investigation. For example, if the overall audio PSR percentage is 2 percent in April, which meets the sample target, individual buildings and subnets might still be having poor experiences, depending on the overall distribution of that 2 percent.

To assess the percentage of poor streams, use the quality reports. Various quality reports are provided to review metrics for overall, conferencing, two-party, PSTN calling, VPN, and meeting rooms. Monthly, weekly, and daily reports are provided to assist in this process. Weekly and daily reports are limited to the Managed Networks template to increase their effectiveness and reduce noise.

### Quality trend analysis

Trending reports display quality information over time and are used to help identify and understand quality trends within each area of interest. As noted above, there are report trees included in the templates for investigating quality; conferencing, two-party, PSTN calling, VPN, and meeting rooms. For the purposes of analyzing quality, the investigative process is the same. However, we recommend that you start with conferencing first, because any improvements in conference quality will also positively affect all other areas.

|  |  |
| --- | --- |
| Note | Investigating two-party, PSTN calling, and meeting rooms are similar to investigating conferencing. The focus is to isloate buildings or subnets that have the worst quality and identify the reason for the poor quality. |

|  |  |
| --- | --- |
| Important | VPN-based reports are filtered by using the *Second VPN* dimension. This dimension requires that the VPN network adapter be properly registered as a Remote Access Adapter. VPN vendors don’t reliably use this flag, and your mileage will vary depending on the VPN vendor deployed at your organization. Follow the guidance outlined [earlier in this guide](#_VPN) for modifying the VPN reports if needed by using the building or network name. |

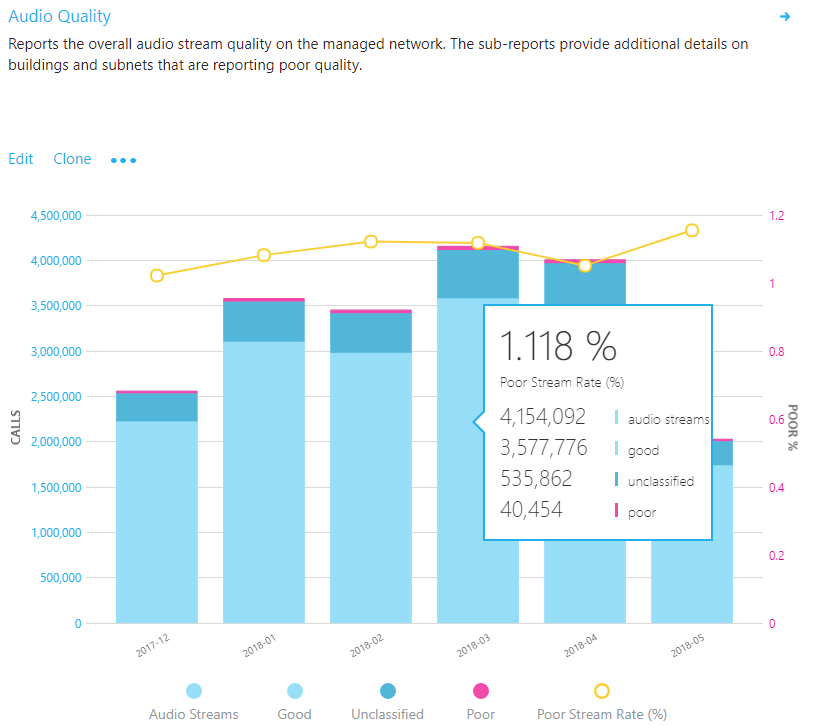


Figure 23 – Audio Quality - Conferencing

#### Investigation

By using these reports, you can answer the following questions:

* What is the total PSR for the current month?
* Is the PSR below the defined target metric?
* Is PSR worse or better than the previous month?
* Is the PSR trend increasing, steady, or decreasing?

Irrespective of the answers to the questions above, take the time to investigate by using the sub-reports to look for any buildings or subnets that might need investigation. Although the overall PSR might be below the target metric, often the PSR for one or more buildings or networks is above the metric and needs remediation.

### Quality investigations

The quality summary reports give you deeper insight into what contributed to the streams’ being classified as poor and helps to isolate problem areas in the managed network.

Although the dimensions used might differ slightly between report, each report will include measures for total streams, total poor streams, PSR, and poor quality due to. Reports have been created for each area of interest: conferencing, two-party, PSTN calling, VPN, and meeting rooms. The Managed Network template includes additional reports to take advantage of the location information uploaded via the building file.

|  |  |
| --- | --- |
| Note | Be sure to adjust the Month Year filter to the current month. Select **Edit**, and adjust **Month Year** to save the new default month. |

|  |  |
| --- | --- |
| Note | Common subnets are difficult to triage due to their widespread use. A separate report that displays the client’s public IP (Second Reflexive Local IP) has been added to the All Networks template to assist with remediating offices that use common networks. |

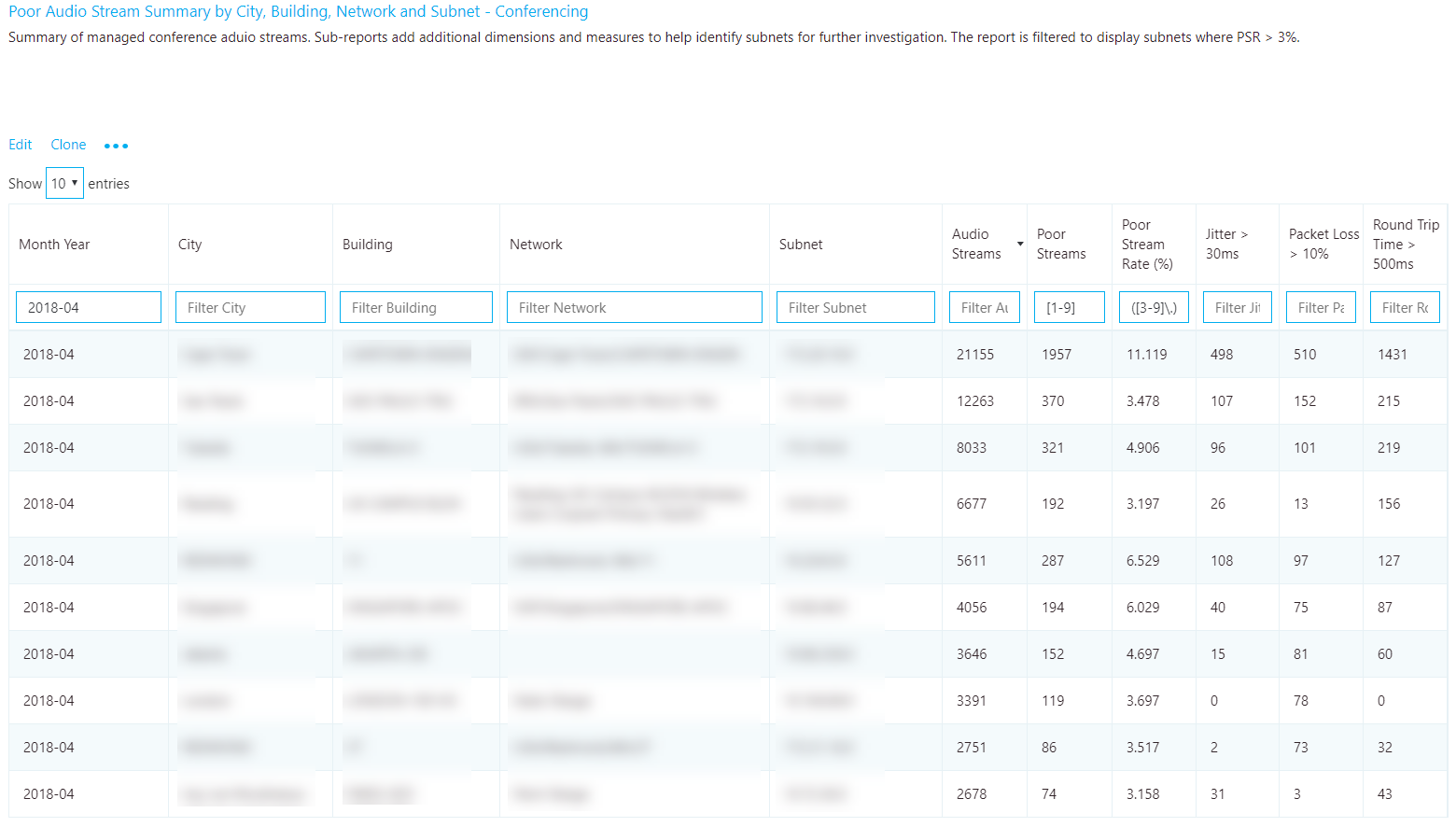


Figure 24 - Poor Audio Stream Summary by Building and Subnet - Conferencing

#### Diagnostic alert

If you received a diagnostic alert “Meeting room devices on Wi-Fi networks are causing poor call quality,” include and prioritize those devices in your remediation efforts. The alert has identified meeting rooms on Wi-Fi that are actively contributing to poor call quality.

If you receive a diagnostic alert “VPN usage is affecting call quality,” investigate a split-tunneling solution to bypass the VPN appliance and allow media to directly connect to the service. The alert has identified that VPN is negatively affecting call quality.

#### Remediation

Focus your remediation efforts on buildings or subnets that have the largest volume of streams, because this will maximize impact and help to improve the user experience quickly. Use the jitter, packet loss, and RTT measurements to understand what’s contributing to the poor quality (it’s possible for there to be more than one problem):

* **Jitter:** Media packets are arriving at different speeds, which causes a speaker to sound robotic.
* **Packet loss:** Media packets are being dropped, which creates the effect of missing words or syllables.
* **RTT:** Media packets are taking a long time to get to their destination, which creates a walkie-talkie effect.

To assist your investigation into quality issues, you can leverage [Call Analytics](https://techcommunity.microsoft.com/t5/Skype-for-Business-Blog/Introducing-Call-Analytics/ba-p/57309). With Call Analytics, you can look at a specific conference or users’ detailed call report. This report will contain PII data and is useful when you’re looking for the cause of a failure. After you know which building is affected, it should be straightforward to track down users in that building.

Don’t forget to let the helpdesk know that these networks are experiencing quality issues, so they can quickly triage and respond to incoming calls.

Table 10 - Common contributors to high PSR

| Remediation | Guidance |
| --- | --- |
| Networks | **Congestion**: An overused or under-provisioned network can cause issues with media quality. Work with the network team to determine whether the network connections from the user to the internet egress point has enough bandwidth to support media. The [Network Planner Tool](https://myadvisor.fasttrack.microsoft.com/CloudVoice/NetworkPlanner) can help you better understand your organization’s bandwidth needs.  **Perform a network readiness assessment:** A network assessment provides details about expected bandwidth usage, how to cope with bandwidth and network changes, and recommended networking practices for Teams and Skype for Business. Using the preceding table as your source, you have a list of buildings or subnets that are excellent candidates for an assessment.   * [Microsoft Teams Network Readiness Assessment](https://docs.microsoft.com/MicrosoftTeams/3-envision-evaluate-my-environment#test-the-network) * [Skype for Business Network Readiness Assessment](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Offers/?pageState=NetworkReadiness)   **Microsoft Network Assessment Tool:** Use this tool for a simple test of network performance to determine how well the network would perform for a Microsoft Teams or Skype for Business Online call. This tool helps you assess the performance of a subnet and validate the readiness of the network against the Microsoft performance [requirements](https://aka.ms/performancerequirements).   * [Download the Network Assessment Tool](https://www.microsoft.com/download/details.aspx?id=53885) |
| Quality of Service (QoS) | QoS is a proven tool to help prioritize packets on a congested network to ensure they arrive at their destination intact and on time. Consider implementing QoS across your organization to maximize the quality of the user experience where bandwidth is constrained. QoS will help solve issues typically associated with high levels of packet loss, and—to a lesser degree—jitter and round-trip times.   * [Microsoft Teams QoS guidance](https://docs.microsoft.com/MicrosoftTeams/qos-in-teams) * [Skype for Business QoS guidance](https://myadvisor.fasttrack.microsoft.com/CloudVoice/NetworkPlanner?SelectedIDs=5_1_0_8) |
| Wi-Fi | Wi-Fi can have a significant impact on call quality. Wi-Fi deployments don’t typically take into consideration the network requirements for VoIP services and are often a source of poor quality. For more information about optimizing your Wi-Fi infrastructure, see [this article about Wi-Fi planning](https://docs.microsoft.com/skypeforbusiness/certification/plan-wifi).  **Wireless driver:** Ensure that wireless drivers are up to date. This will help mitigate any poor user experience related to an outdated driver. Many organizations don’t include wireless drivers in their patch cycles, and these drivers can go unpatched for years. Many wireless issues are solved by ensuring the wireless drivers are up to date.  **WMM:** Wireless Multimedia Extensions (WMM), also known as Wi-Fi Multimedia, provides basic QoS features to wireless networks.Modern wireless networks must support many devices. These devices compete for bandwidth and can lead to quality issues for VoIP services, where speed and latency are vital. Consult your wireless vendor for specifics and consider implementing WMM on your wireless network to prioritize Skype for Business and Teams media.  **Access point density:** Access points might be too far apart or not in an ideal location. To minimize potential interference, place extra access points in conference rooms and in locations that aren’t obstructed by walls or other objects where the Wi-Fi signal is weak.  **2.4 GHz versus 5 GHz:** 5 GHz provides less background interference and higher speeds, and should be prioritized when deploying VoIP over Wi-Fi. However, 5 GHz isn’t as strong as 2.4 GHz and doesn’t penetrate walls as easily. Review your building layout to determine which frequency you can rely on for the best connection. |
| Network device | Larger organizations might have hundreds of devices spread out across the network. Work with your network team to ensure that the network devices from the user to the internet are maintained and up to date. |
| VPN | VPN appliances aren’t traditionally designed to handle real-time media workloads. Some VPN configurations even prohibit the use of UDP (which is the preferred protocol for media). Consider implementing a [VPN split-tunnel solution](https://myadvisor.fasttrack.microsoft.com/CloudVoice/Downloads?SelectedIDs=5_1_0_9) to help reduce VPN as a source of poor quality. |
| Clients  (Skype for Business Online only) | Older clients have been known to cause issues with media. Ensure that clients are being patched within six months of release. Leverage [MyAdvisor](https://aka.ms/myadvisor) for guidance on developing a client readiness strategy and deploy [Click-to-Run](https://docs.microsoft.com/DeployOffice/deployment-guide-for-office-365-proplus). |
| Devices | The use of [optimized devices](https://partnersolutions.skypeforbusiness.com/solutionscatalog/personal-peripherals-pcs) can help to significantly improve the user experience. With all things being equal, optimized devices are designed to maximize the user experience with Teams and Skype for Business, and produce superior quality. Leverage [MyAdvisor](https://aka.ms/myadvisor) for guidance on developing a device readiness strategy. |
| Drivers | Patching network (Ethernet and Wi-Fi), audio, video, and USB drivers should be part of your overall patch management strategy. Many quality issues are solved by updating drivers. |
| Meeting rooms on Wi-Fi | We highly recommend that meeting room devices be connected to the network by using at least a 1-Gbps Ethernet connection. Meeting room devices typically include multiple audio and video streams, along with meeting content such as screen sharing, and have higher network requirements than other Teams or Skype for Business endpoints. Meeting rooms are, by definition, stationary devices where Wi-Fi affords a benefit only during installation.  Meeting rooms need to be treated with extra care and attention to ensure that the experience using these devices is meeting or exceeding expectations. Quality issues with meeting rooms are usually going to be escalated quickly, because they’re often used by senior-level staff.  With all things being equal (apart from convenience), Wi-Fi performance is often less than a wired connection. With the rise of “bring your own device” policies and the proliferation of laptops, Wi-Fi access points are often over-utilized. Real-time media might not be prioritized on Wi-Fi networks, which can lead to quality issues during peak use times. This heavy usage can coincide with a meeting where there might be a dozen people in attendance, each with their own laptop and smartphone, all connected to the same Wi-Fi access point as the meeting room device.  Wi-Fi should only be considered as a temporary solution, for a mobile installation, or when Wi-Fi has been properly provisioned to support business-class, real-time–based media. |

## TCP

TCP is considered a failback transport and not the primary transport you want for real-time media. The reason it’s a failback transport is due to the stateful nature of TCP. For example, if a call is made on a latent network and media packets are delayed, then packets from a few seconds ago—which are no longer useful—compete for bandwidth to get to the receiver, which can make a bad situation worse. This makes the audio healer stitch and stretch audio, resulting in audible artifacts, often in the form of jitter.

The reports in this section don’t make a distinction between good and poor streams. Given that UDP is preferred, the reports look for the use of TCP for audio, video, and video-based screen sharing (VBSS). Poor stream rates are provided to help compare UDP quality versus TCP quality so that you can focus your efforts where the impact is the greatest. TCP usage is primarily caused by incomplete firewall rules. For more information about firewall rules for Teams and Skype for Business Online, see [Office 365 URLs and IP address ranges](https://aka.ms/o365ips).

|  |  |
| --- | --- |
| Important | Having a valid [building file](#_Building_Mapping_1) uploaded is highly recommended so you can quickly distinguish inside from outside streams when looking at TCP usage. |

|  |  |
| --- | --- |
| Note | Audio, video, and VBSS all prefer UDP as their primary transport. The legacy RDP Application Sharing workload only uses TCP. |

### TCP usage

TCP reports indicates the overall TCP usage over the last seven months. All further reports in this section will focus on narrowing down specific buildings and subnets where TCP is most commonly used. Separate reports are available for both conferencing and two-party streams.

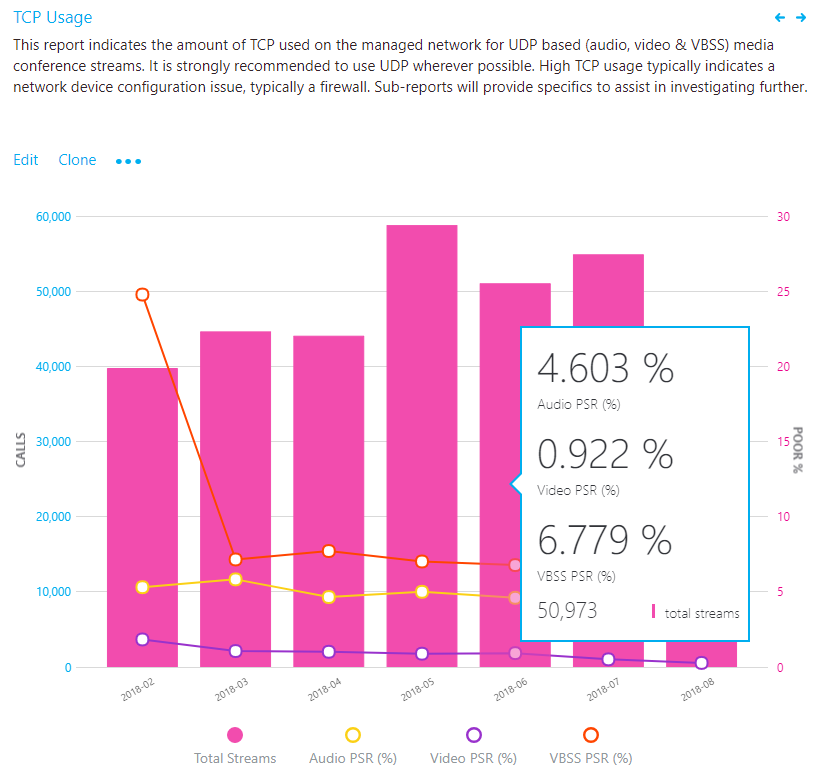


Figure 25 – Audio Streams with TCP Usage

#### Investigation

By using this report, you can answer the following questions:

* What is the total volume of TCP streams for the current month?
* Is it worse or better than the previous month?
* Is the TCP usage trend increasing, steady, or decreasing?
* Is the TCP PSR the same as my overall PSR?

If you notice that the TCP usage trend is increasing or above normal monthly usage, take the time to investigate by using the sub-reports to look for any buildings or networks that might need remediation. Ideally, you want as few TCP-based audio sessions as possible on the managed network.

### TCP vs. UDP

This report identifies the volume of TCP versus UDP usage reporting on the latest month for audio, video, and video-based screen sharing (VBSS).

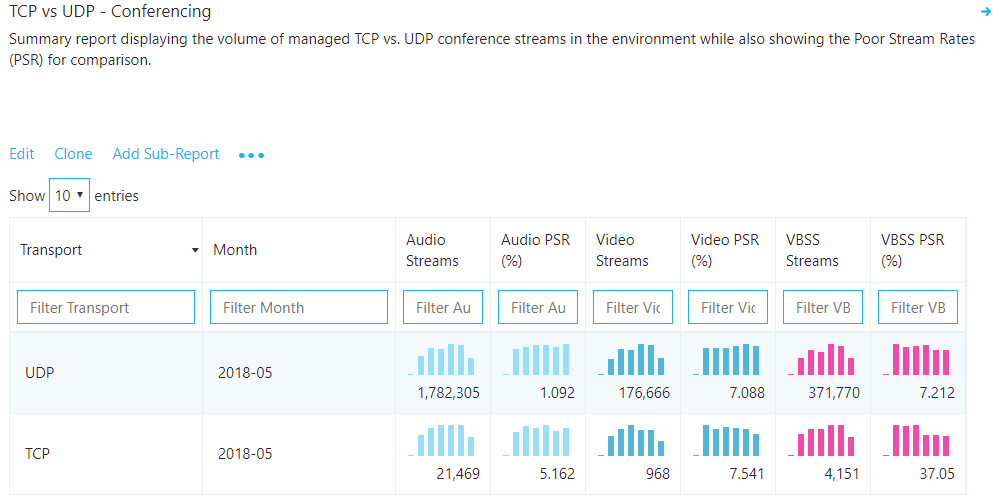


Figure 26 – TCP vs. UDP - Conferencing

#### Analysis

Although you want TCP usage to be as low as possible, you might see a bit of TCP usage in an otherwise healthy deployment. TCP by itself won’t contribute to a poor call, so stream rates are provided to help identify whether TCP usage is a contributor to poor quality.

### TCP investigations

In the provided CQD templates, navigate to theTCP Streams by Building and Subnetreports by using either the Managed Networks or All Networks template. For the purpose of investigating TCP usage, the process is the same, so we’ll focus the discussion here on conferencing.

|  |  |
| --- | --- |
| Important | Having a valid [building file](#_Building_Mapping_1) uploaded is recommended so you can quickly distinguish inside from outside streams when looking at TCP usage. |

|  |  |
| --- | --- |
| Note | Be sure to adjust the Month Year filter to the current month. Select **Edit**, and adjust **Month Year** to save the new default month. |

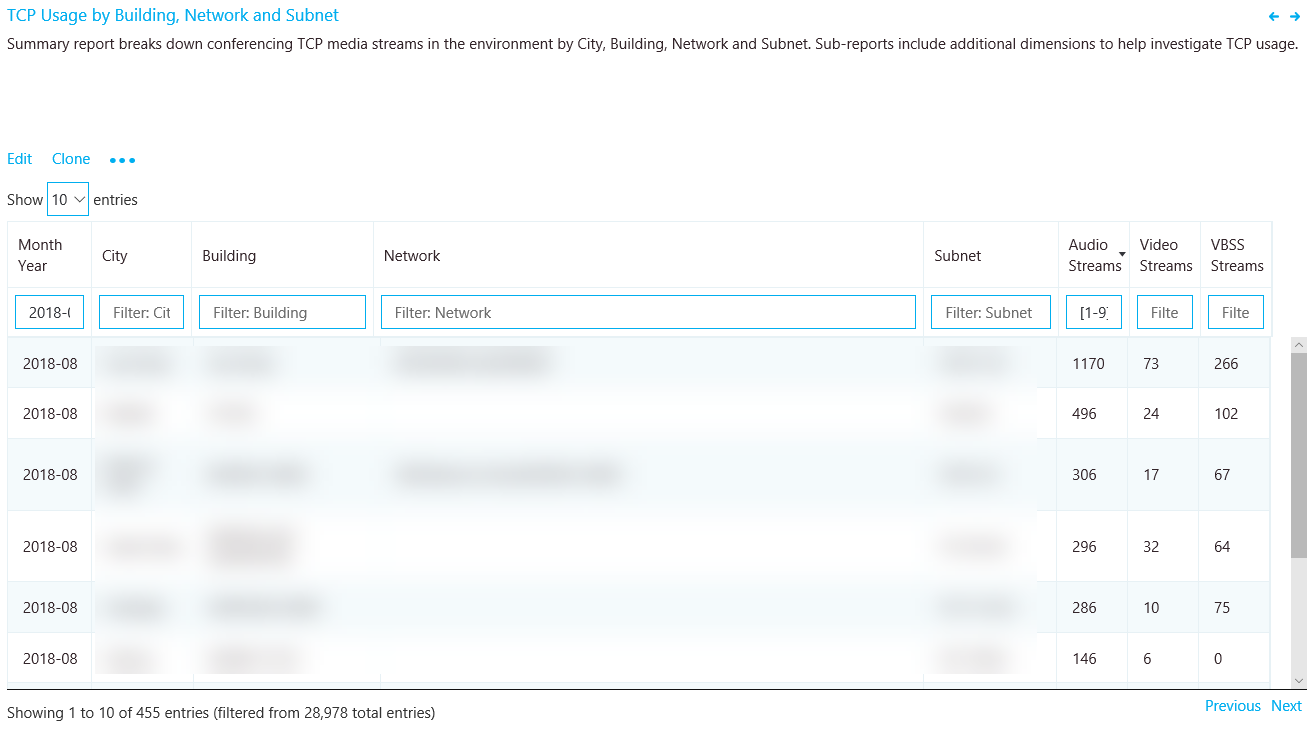


Figure 27 – TCP Streams by Building and Subnet - Conferencing

#### Diagnostic alert

If you received a diagnostic alert “UDP traffic is being limited, which causes poor call quality,” focus your TCP remediation efforts on those subnets first. The alert has identified subnets where the use of TCP is negatively affecting call quality.

#### Remediation

This report identifies specific buildings and subnets that are contributing to the volume of TCP usage. An additional report is also included to identify the Microsoft Relay IP that was used in the call to help isolate missing firewall rules. Focus your remediation efforts on those buildings that have the highest volume of TCP streams to maximize impact.

The most common cause of TCP usage is missing exception rules in firewalls or proxies. We’ll be talking about proxies in the next section, so for now focus your efforts on the firewalls. By using the building or subnet provided, you can determine which firewall needs to be updated.

*Table 11 - Remediation* guidance for TCP streams by building and subnet

|  |  |
| --- | --- |
| Remediation | Guidance |
| Configure firewall | Verify that [Office 365 IP ports and addresses](https://aka.ms/o365ips) are excluded from your firewall. For media-related TCP issues, focus your initial efforts on the following:   * Verify that the client [media subnets](https://aka.ms/o365ips#bkmk_teams) 13.107.64.0/18 and 52.112.0.0/14 are in your firewall rules. * [UDP ports 3478–3481](https://cqd.lync.com) are the required media ports and must be opened, otherwise the client will fail back to TCP port 443. |
| Verify | Use the [Microsoft Network Assessment Tool](https://www.microsoft.com/download/details.aspx?id=53885) to check for issues with connectivity to specific Office 365 IP addresses and ports from the affected building or subnet. |

## HTTP proxy

HTTP proxies aren’t the preferred path for establishing media sessions, for a multitude of reasons. Many contain deep packet inspection features that can prevent connections to the service from being completed and introduce disruptions. Additionally, almost all proxies force TCP as opposed to allowing UDP, which is recommended for optimal audio quality.

We always recommend that you configure the client to directly connect to Teams and Skype for Business services. This is especially important for media-based traffic.

|  |  |
| --- | --- |
| Important | Having a valid [building file](#_Building_Mapping_1) uploaded makes it easy to properly distinguish inside from outside audio streams when analyzing proxy usage. |

### HTTP proxy usage

The HTTP proxy stream report in this section of the template is much like the TCP reports. It doesn’t look at whether calls are poor or good, but whether the call is connected over HTTP.

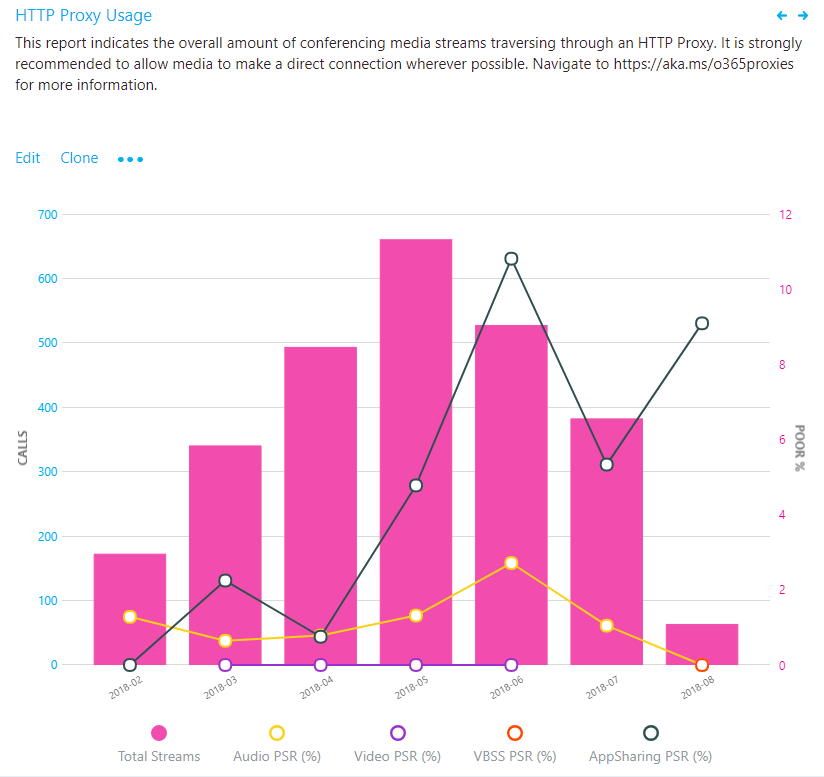


Figure 28 – Audio Streams with HTTP Proxy Usage

#### Analysis

You want to see as little HTTP media streams as possible. If you have streams traversing your proxy, consult your networking team to ensure that the proper exclusions are in place so that clients are directly routing to Teams or Skype for Business Online media subnets.

If you have only one internet proxy in your organization, verify the proper [Office 365 URLs and IP address range exclusions](https://aka.ms/o365ips). If more than one internet proxy is configured in your organization, use the HTTP sub-report to isolate which building or subnet is affected.

For organizations that can’t bypass the proxy, ensure that the Skype for Business client is configured to sign in properly when it’s located behind a proxy, as outlined in the article [Skype for Business should use proxy server to sign in instead of trying direct connection](https://support.microsoft.com/help/3207112/skype-for-business-should-use-proxy-server-to-sign-in-instead-of-tryin).

### HTTP proxy investigations

This report identifies specific buildings and subnets that are contributing to HTTP usage.

|  |  |
| --- | --- |
| Important | Having a valid [building file](#_Building_Mapping_1) uploaded makes it easy to properly distinguish inside from outside audio streams when analyzing proxy usage. |

|  |  |
| --- | --- |
| Note | Be sure to adjust the Month Year filter to the current month. Select **Edit**, and adjust **Month Year** to save the new default month. |

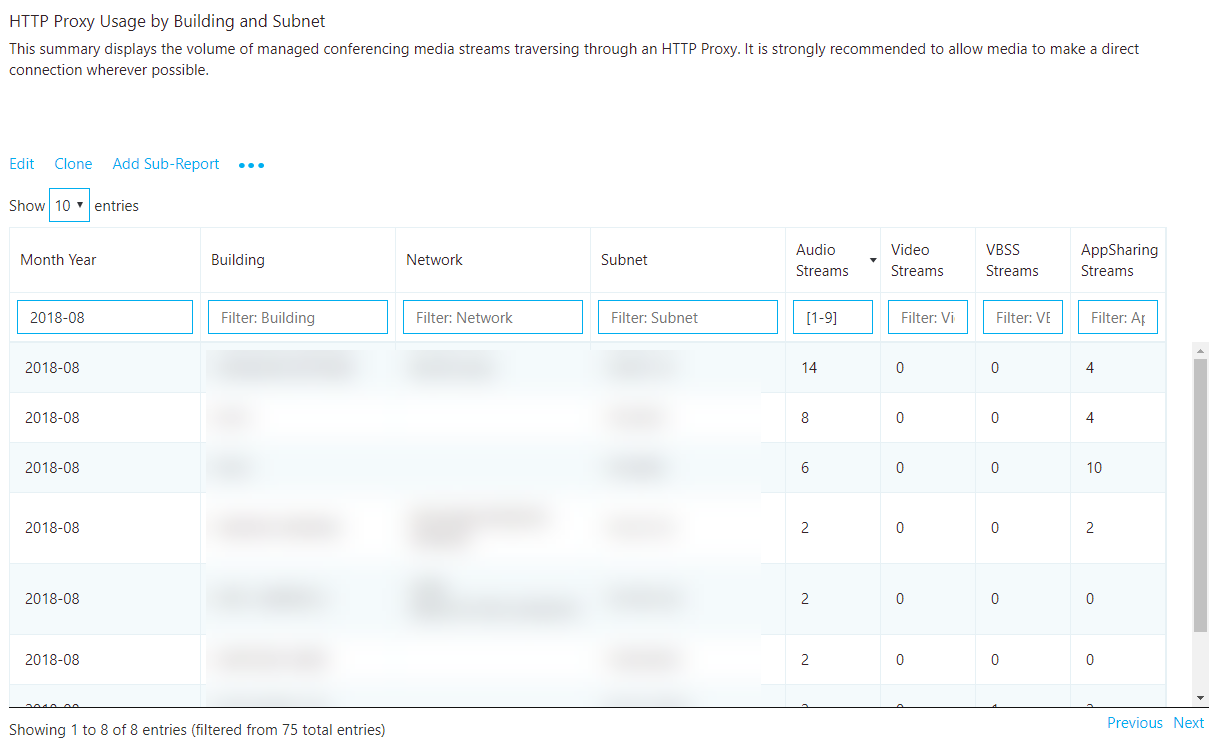


Figure 29 – HTTP Proxy Usage by Building and Subnet

#### Remediation

We [recommend](https://docs.microsoft.com/skypeforbusiness/optimizing-your-network/proxy-servers-for-skype-for-business-online) that you always bypass proxies for Skype for Business and Teams, especially media traffic. Proxies don't make Skype for Business more secure, because its traffic is already encrypted. Performance-related problems can be introduced to the environment through latency and packet loss. Issues such as these will result in a negative experience with audio, video and screen sharing, where real-time streams are essential.

The most common cause of HTTP usage is missing exception rules in proxies. By using the building or subnet provided, you can quickly determine which proxy needs to be configured for media bypass.

Verify that the required [Office 365 FQDNs and IPs](https://aka.ms/o365ips) are whitelisted in your proxy.

For more information about using proxies with Skype for Business Online and Teams, see [this article](https://docs.microsoft.com/skypeforbusiness/optimizing-your-network/proxy-servers-for-skype-for-business-online).

# Endpoint investigations

This section is focused on the tasks for reporting on client versions and the use of certified devices. Reports are available to outline usage for client versions, client type, capture devices and drivers (microphone), video capture devices, and Wi-Fi vendor and driver versions.

|  |  |
| --- | --- |
| Note | Not all reports included in the templates are covered in this guide; however, the methods of investigation explained below still apply. Refer to the individual report description for more information. |

## Client versions

The reports in this space focus on identifying Skype for Business client versions in use and their relative volume in the environment.

|  |  |
| --- | --- |
| Important | Currently, Teams clients are distributed and updated automatically through the Azure Content Delivery Network and will be kept up to date by the service. Client readiness and investigative activities aren’t applicable to Teams. |
| Important | Unless you exclude federated participant data, these reports will include client telemetry from federated endpoints. To exclude federated endpoints, you must add a [query filter](#_Query_filters) for **Second Tenant ID** set to your organization’s [tenant ID](#_Tenant_ID_1). Alternatively, you can use a [URL filter](#_URL_filter) to exclude federated participant telemetry. |
| Note | Be sure to adjust the Month Year filter to the current month. Select **Edit**, and adjust **Month Year** to save the new default month. |

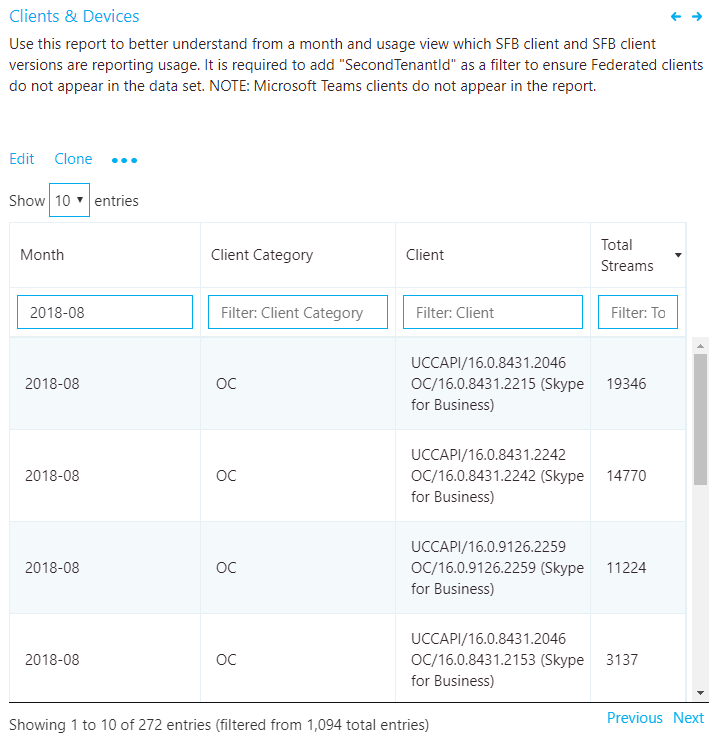


Figure 30 - Client version report

### Diagnostic alert

If you received a diagnostic alert ”Known poorly performing client versions are in use,” focus on updating those clients first. The alert has identified that these clients are negatively affecting your call quality. You can use the Client & Devices report (shown above) to help ensure that the clients that have known issues are no longer being updated.

### Remediation

A critical part of driving high-quality user experiences is ensuring that managed clients are running up-to-date versions of Skype for Business, in addition to ensuring the supporting audio, video, network, and USB drivers are up to date. This provides several benefits, among them:

* It’s easier to manage a few versions versus many versions.
* It provides a level of consistency of experience.
* It makes it easier to troubleshoot problems with call quality and usability.
* Microsoft continually makes general improvements and optimizations across the product. Ensuring that users receive these updates reduces their risk of running into a problem that has already been solved.

Limiting your deployment to client versions that are less than six months old will improve the overall user experience and improve manageability by reducing the number of versions that need to be supported.

If you’re using only Office Click-to-Run, you’ll automatically be within the six-month window. No further action is required.

If you have a mix of Click-to-Run and installer packages (MSI), you can use the report to verify that the MSI clients are being updated regularly. If you notice clients are falling behind, work with the team responsible for managing Office updates and ensure that they’re approving and deploying client patches regularly.

It’s also important to consider and ensure that the network, video, USB, and audio drivers are being patched as well. It can be easy to overlook these drivers and not include them in your patch management strategy.

Version numbers for Skype for Business can be found via the links below:

* [Release information for updates to Office ProPlus](https://docs.microsoft.com/officeupdates/release-notes-office365-proplus)
* [Update history for Office 365 ProPlus](https://docs.microsoft.com/officeupdates/update-history-office365-proplus-by-date)
* [Skype for Business downloads and updates](https://docs.microsoft.com/SkypeForBusiness/software-updates)

## Devices

To make use of the microphone device report, we need to understand the concept of the mean opinion score (MOS). MOS is the gold-standard measurement to gauge the perceived audio quality. It’s represented as an integer rating from 0 to 5.

The basis of all measures of voice quality is how a person perceives the quality of speech. Because it’s affected by human perception, it’s inherently subjective. There are several different methodologies for subjective testing. Most voice quality measures are based on an absolute categorization rating (ACR) scale.

In an ACR subjective test, a statistically significant number of people rate their quality of experience on a scale of 1 (bad) to 5 (excellent). The average of the scores is the MOS. The resulting MOS depends on the range of experiences that were exposed to the group and to the type of experience being rated.

Because it’s impractical to conduct subjective tests of voice quality for a live communication system, Microsoft Teams and Skype for Business generate MOS values by using advanced algorithms to objectively predict the results of a subjective test.

The available set of MOS and associated metrics provide a view into the quality of the experience being delivered to the users by an audio device.

By supplying users with devices certified for Teams and Skype for Business, you reduce the likelihood of encountering negative experiences due to the device itself (which is more likely, for example, with built-in laptop speakers and microphones). For more information, see these articles on the [certification program](https://docs.microsoft.com/SkypeForBusiness/certification/overview) and the [partner solutions catalog](https://partnersolutions.skypeforbusiness.com/solutionscatalog/personal-peripherals-pcs).

The device reports are used to assess device usage by volume and MOS score (audio only), and can be found in the accompanying templates under Clients & Devices*.*

|  |  |
| --- | --- |
| Important | Unless you exclude federated participant data, these reports will include client telemetry from federated endpoints. To exclude federated endpoints, you must add a query filter for **Second Tenant ID** set to your organization’s [tenant ID](#_Tenant_ID_1). Alternatively, you can use a [URL filter](#_URL_filter) to exclude federated participant telemetry. |

|  |  |
| --- | --- |
| Note | Be sure to adjust the Month Year filter to the current month. Select **Edit**, and adjust **Month Year** to save the new default month. |
|  |  |
| Note | You might notice when viewing this report that you see the same device reported multiple times. This is due to the way the device is being reported to CQD. Differences in hardware and OS locale cause differences in how device data is reported. |

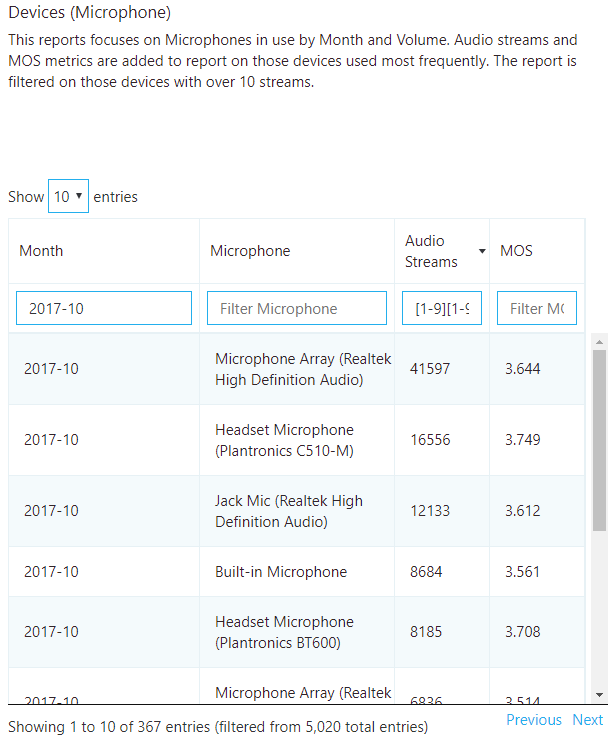


Figure 31 - Devices (Microphone) report

### Diagnostic alert

If you received a diagnostic alert “Audio drivers are causing call drops,” focus on remediating those drivers first. The alert has identified that known bad drivers are causing calls to drop and are negatively affecting call reliability. You can use the Microphone-Drivers report (shown above), which is found in the Client & Devices section, to help with the process.

### Remediation

Typically, you’ll need to discover and phase out non-certified devices and replace them with certified devices. Some considerations when reviewing the device reports include:

* + - Are the devices in use certified for Teams and Skype for Business?
    - You can identify users of a specific device through [Call Analytics](https://techcommunity.microsoft.com/t5/Skype-for-Business-Blog/Introducing-Call-Analytics/ba-p/57309). Check to make sure they have the latest device drivers and that their device isn’t connected through a USB hub or docking station.
    - How many different versions of various drivers are in use? Are they being patched regularly? Ensuring that audio, video, and Wi-Fi drivers are being patched regularly will help eliminate these as a source of quality issues and make the user experience more predictable and consistent.

#### Audio

The next task is to determine the overall usage of [certified audio devices](https://partnersolutions.skypeforbusiness.com/solutionscatalog/personal-peripherals-pcs). We recommend that at least 80 percent of all audio streams use a certified audio device. This is best accomplished by exporting the microphone devices report to Excel to calculate the usage of certified or approved devices. Organizations typically keep a list of all approved devices, so filtering and sorting the data should be straightforward.

#### Video

Video drivers are important to keep updated as well. Ensuring that video cards are being regularly patched will help exclude video drivers as a source of poor quality for video streams. Using [certified video devices](https://partnersolutions.skypeforbusiness.com/solutionscatalog/personal-peripherals-pcs) will help ensure a smooth and high-quality user experience. Video devices that support H.264 native encoding are preferred, to reduce CPU usage during video conferencing.

#### Wi-Fi

Wi-Fi drivers also need to be patched on a regular cadence as well and should be included in your patch management strategy. Many quality issues can be corrected by maintaining up-to-date Wi-Fi drivers. For more information about optimizing your Wi-Fi infrastructure, see [this article about Wi-Fi planning](https://docs.microsoft.com/skypeforbusiness/certification/networking-wifi).

# Appendix

## Office 365 network connectivity principles

Before you begin planning your network for Office 365 network connectivity, it’s important to understand the connectivity principles for securely managing Office 365 traffic and getting the best possible performance. The following article will help you understand the most recent guidance for securely optimizing Office 365 network connectivity:

[Office 365 Network Connectivity Principles](https://aka.ms/pnc)

## Planning for Wi-Fi

Microsoft’s approach to drive quality and agility into wireless networks comes in three parts: end-to-end planning, best practices in deployment, and proactive maintenance and operations. The following solution brief walks you through this process to ensure an enterprise-class wireless Skype for Business experience:

[Ensuring an Enterprise Class Wireless Skype for Business Experience](https://www.microsoft.com/download/details.aspx?id=47257)

## Lync Networking Guide

For more background on the Microsoft Teams and Skype for Business networking concepts and rationale behind their importance to quality, the [Lync Server 2013 Networking Guide](https://blogs.technet.microsoft.com/nexthop/2013/06/03/lync-server-2013-networking-guide-network-planning-monitoring-and-troubleshooting-with-microsoft-lync-server/) is still applicable.

## Network performance requirements

The quality of real-time media (audio, video, and application sharing) over IP is greatly affected by the quality of end-to-end network connectivity. For optimal Teams or Skype for Business media quality, your network must meet the following network performance metrics.

Table 12 - Network performance requirements

|  |  |  |
| --- | --- | --- |
| Metric | Client to Microsoft edge | Customer edge to Microsoft edge |
| Latency (one way) | <50 ms | <30 ms |
| Latency (RTT, or round-trip time) | <100 ms | <60 ms |
| Burst packet loss | <10% during any 200-ms interval | <1% during any 200-ms interval |
| Packet loss | <1% during any 15-sec interval | <0.1% during any 15-sec interval |
| Packet inter-arrival Jitter | <30 ms during any 15-sec interval | <15 ms during any 15-sec interval |
| Packet reorder | <0.05% out-of-order packets | < 0.01% out-of-order packets |

For more information, see [this article about media quality and network performance](https://aka.ms/performancerequirements) for Teams and Skype for Business Online.

## Other resources

### Building data file

* [Turning on and using Call Quality Dashboard for Microsoft Teams and Skype for Business Online](https://docs.microsoft.com/SkypeForBusiness/using-call-quality-in-your-organization/turning-on-and-using-call-quality-dashboard)

### CQD training

* <https://aka.ms/sof-cqd>
* [Getting started with CQD](https://www.skypeoperationsframework.com/Academy?SOFTrainings=Configuring%20Call%20Quality%20Dashboard%20to%20monitor%20your%20Skype%20for%20Business%20Online%20Environment) guide and workshop.
* [Dimensions and measures available in Call Quality Dashboard](https://aka.ms/cqd-dm)

### Call Analytics training

* [Introducing Call Analytics](https://techcommunity.microsoft.com/t5/Skype-for-Business-Blog/Introducing-Call-Analytics/ba-p/57309)
* [Set up Call Analytics](https://docs.microsoft.com/microsoftteams/set-up-call-analytics)
* [What's the difference between Call Analytics and Call Quality Dashboard?](https://docs.microsoft.com/microsoftteams/difference-between-call-analytics-and-call-quality-dashboard)
* [Use Call Analytics to troubleshoot poor call quality](https://docs.microsoft.com/microsoftteams/use-call-analytics-to-troubleshoot-poor-call-quality)

### Call Analytics support

* Community: [Skype for Business Preview Program](https://techcommunity.microsoft.com/t5/Skype-for-Business-Preview/bd-p/SkypeforBusinessPreviewProgram)
* To get support, sign in to our preview portal [www.skypepreview.com](http://www.skypepreview.com), select **Report an issue**, and use the **Create New Bug** option to report an issue. Please note that support engineers are available to provide support from Monday through Friday, between the hours of 6 AM and 9 PM Eastern Time (United States). Requests outside of those hours will be triaged the following day.

### Devices

* [Skype for Business Solutions Catalog Personal Peripherals & PCs](http://partnersolutions.skypeforbusiness.com/solutionscatalog/personal-peripherals-pcs)

### Tenant reporting

* [Office 365 Adoption Content Pack](https://www.microsoft.com/microsoft-365/blog/2017/05/22/announcing-the-public-preview-of-the-office-365-adoption-content-pack-in-powerbi/)
* [Microsoft 365 usage analytics](https://support.office.com/article/Microsoft-365-usage-analytics-77ff780d-ab19-4553-adea-09cb65ad0f1f)
* [Skype for Business Online reporting](https://docs.microsoft.com/SkypeForBusiness/skype-for-business-online-reporting/skype-for-business-online-reporting)
* [Microsoft Teams reporting](https://techcommunity.microsoft.com/t5/Microsoft-Teams-Blog/New-usage-reports-for-Microsoft-Teams/ba-p/132614)