Use Quick Assist to help users

Article • 09/04/2024 • 4 contributors • Applies to: Windows 11, Windows 10

In this article

Quick Assist is an application that enables a person to share their Windows or macOS device with another person over a remote connection. Your support staff can use it to remotely connect to a user's device and then view its display, make annotations, or take full control. In this way, they can troubleshoot, diagnose technological issues, and provide instructions to users directly on their devices.

> **Important**
>
> Learn how to protect yourself from tech support scams. Tech support scams are an industry-wide issue where scammers use scare tactics to trick you into unnecessary technical support services. Only allow a Helper to connect to your device if you initiated the interaction by contacting Microsoft Support or your IT support staff directly.
>
> If you or someone you know has been affected by a tech support scam, use the technical support scam form to report it.

Before you begin

All you need to use Quick Assist is suitable network and internet connectivity. No roles, permissions, or policies are involved. Neither party needs to be in a domain. The helper must have a Microsoft account. The sharer doesn't have to authenticate.

Authentication

The helper can authenticate when they sign in by using a Microsoft account (MSA) or Microsoft Entra ID. Local Active Directory authentication isn't currently supported.

Network considerations

Quick Assist communicates over port 443 (https) and connects to the Remote Assistance Service at `https://remoteassistance.support.services.microsoft.com` by using the Remote Desktop Protocol (RDP). The traffic is encrypted with TLS 1.2. Both the helper and sharer must be able to reach these endpoints over port 443:

Expand table

Domain/Name	Description
`*.aria.microsoft.com`	Accessible Rich Internet Applications (ARIA) service for providing accessible experiences to users.
`*.cc.skype.com`	Required for Azure Communication Service.
`*.events.data.microsoft.com`	Required diagnostic data for client and services used by Quick Assist.
`*.flightproxy.skype.com`	Required for Azure Communication Service.

`*.live.com`	Required for logging in to the application (MSA).
`*.monitor.azure.com`	Required for telemetry and remote service initialization.
`*.registrar.skype.com`	Required for Azure Communication Service.
`*.support.services.microsoft.com`	Primary endpoint used for Quick Assist application
`*.trouter.skype.com`	Used for Azure Communication Service for chat and connection between parties.
`aadcdn.msauth.net`	Required for logging in to the application (Microsoft Entra ID).
`edge.skype.com`	Used for Azure Communication Service for chat and connection between parties.
`login.microsoftonline.com`	Required for Microsoft sign-in service.
`remoteassistanceprodacs.communication.azure.com`	Used for Azure Communication Service for chat and connection between parties.
`turn.azure.com`	Required for Azure Communication Service.

> **ⓘ Important**
>
> Quick Assist uses Edge WebView2 browser control. For a list of domain URLs that you need to add to the allow list to ensure that the Edge WebView2 browser control can be installed and updated, see Allow list for Microsoft Edge endpoints.

Working with Quick Assist

Either the support staff or a user can start a Quick Assist session.

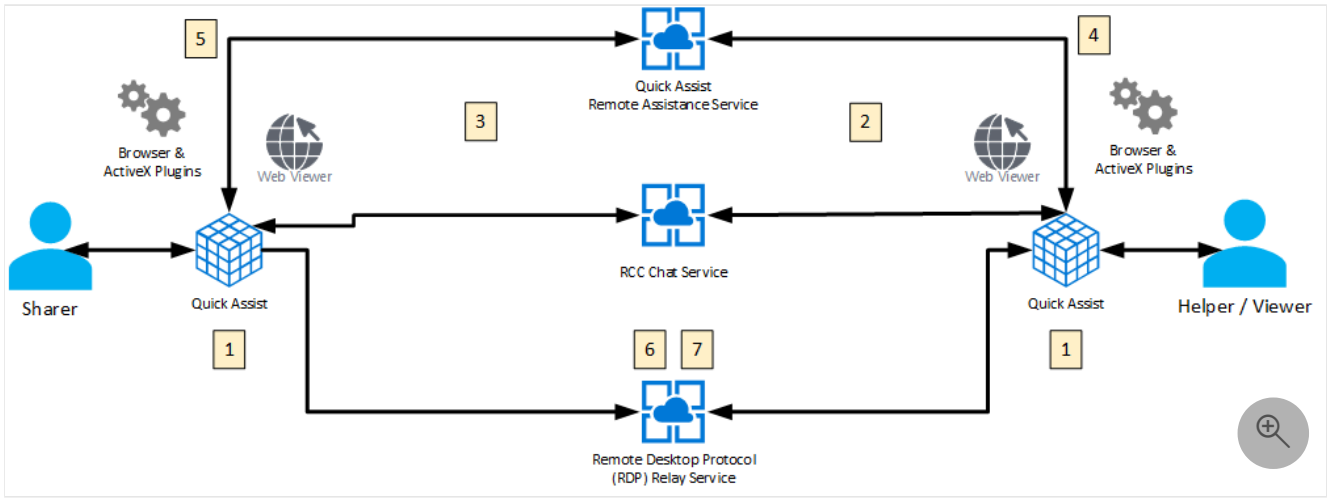
1. Support staff ("helper") and the user ("sharer") can start Quick Assist in any of a few ways:
   - Type *Quick Assist* in the Windows search and press ENTER.
   - Press **CTRL** + **Windows** + **Q**.
   - For **Windows 10** users, from the Start menu, select **Windows Accessories**, and then select **Quick Assist**.
   - For **Windows 11** users, from the Start menu, select **All Apps**, and then select **Quick Assist**.
2. In the **Help someone** section, the helper selects the **Help someone** button. The helper might be asked to choose their account or sign in. Quick Assist generates a time-limited security code.
3. Helper shares the security code with the user over the phone or with a messaging system.
4. The sharer enters the provided code in the **Security code from assistant** box under the **Get help** section, and then selects **Submit**.
5. The sharer receives a dialog asking for permission to allow screen sharing. The sharer gives permission by selecting the **Allow** button and the screen sharing session is established.
6. After the screen sharing session is established, the helper can optionally request control of the sharer's screen by selecting **Request control**. The sharer then receives a dialog asking them if they want to **Allow** or **Deny** the request for control.

> **ⓘ Note**
>
> In case the helper and sharer use different keyboard layouts or mouse settings, the ones from the sharer are used during the session.

How it works

1. Both the helper and the sharer start Quick Assist.
2. The helper selects **Help someone**. Quick Assist on the helper's side contacts the Remote Assistance Service to obtain a session code. An RCC chat session is established, and the helper's Quick Assist instance joins it. The helper then provides the code to the sharer.
3. After the sharer enters the code in their Quick Assist app, Quick Assist uses that code to contact the Remote Assistance Service and join that specific session. The sharer's Quick Assist instance joins the RCC chat session.
4. The sharer is prompted to confirm allowing the helper to share their desktop with the helper.

5. Quick Assist starts RDP control and connects to the RDP Relay service.
6. RDP shares the video to the helper over https (port 443) through the RDP relay service to the helper's RDP control. Input is shared from the helper to the sharer through the RDP relay service.



Data and privacy

Microsoft logs a small amount of session data to monitor the health of the Quick Assist system. This data includes the following information:

- Start and end time of the session
- Errors arising from Quick Assist itself, such as unexpected disconnections
- Features used inside the app such as view only, annotation, and session pause

> **Note**
>
> No logs are created on either the helper's or sharer's device. Microsoft can't access a session or view any actions or keystrokes that occur in the session.
>
> The sharer sees only an abbreviated version of the helper's name (first name, last initial) and no other information about them. Microsoft doesn't store any data about either the sharer or the helper for longer than three days.

In some scenarios, the helper does require the sharer to respond to application permission prompts (User Account Control), but otherwise the helper has the same permissions as the sharer on the device.

Install Quick Assist on Windows

Install Quick Assist from the Microsoft Store

1. Download the new version of Quick Assist by visiting the Microsoft Store.
2. In the Microsoft Store, select **View in store**, then install Quick Assist. When the installation is complete, **Install** changes to **Open**.

For more information, visit Install Quick Assist.

Install Quick Assist with Intune

To deploy Quick Assist with Intune, see Add Microsoft Store apps to Microsoft Intune.

Microsoft Edge WebView2

The Microsoft Edge WebView2 is a development control that uses Microsoft Edge as the rendering engine to display web content in native apps. The new Quick Assist application is developed using this control, making it a necessary component for the app to function.

- For Windows 11 users, this runtime control is built in.
- For Windows 10 users, the Quick Assist Store app detects if WebView2 is present on launch and if necessary, installs it automatically. If an error message or prompt is shown indicating WebView2 isn't present, it needs to be installed separately.

For more information on distributing and installing Microsoft Edge WebView2, visit Distribute your app and the WebView2 Runtime.

Install Quick Assist on macOS

Quick Assist for macOS is available for interactions with Microsoft Support. If Microsoft products on your macOS device aren't working as expected, contact Microsoft Support for assistance. Your Microsoft Support agent will guide you through the process of downloading and installing it on your device.

> **Note**
>
> Quick Assist for macOS is not available outside of Microsoft Support interactions.

Disable Quick Assist within your organization

If your organization utilizes another remote support tool such as Remote Help, disable or remove Quick Assist as a best practice, if it isn't used within your environment. This prevents guests from using Quick Assist to gain access to devices within your organization.

Disable Quick Assist

To disable Quick Assist, block traffic to the `https://remoteassistance.support.services.microsoft.com` endpoint. This is the primary endpoint used by Quick Assist to establish a session, and once blocked, Quick Assist can't be used to get help or help someone.

> **Note**
>
> Blocking the endpoint will disrupt the functionality of Remote Help, as it relies on this endpoint for operation.

Uninstall Quick Assist

Uninstall via PowerShell

Run the following PowerShell command as Administrator:

```
Get-AppxPackage -Name MicrosoftCorporationII.QuickAssist | Remove-AppxPackage -AllUsers
```

Uninstall via Windows Settings

Navigate to **Settings** > **Apps** > **Installed apps** > Quick Assist > select the ellipsis (...), then select **Uninstall**.

Report Abuse

Before joining a session, it's important for you to know who you are connecting to. Anyone that has control over your device can perform actions on your device, and potentially install malicious applications or take other actions that can damage your device.

Follow these best practices for using Quick Assist or any remote desktop software:

- Never allow a connection to your device by someone claiming to be "IT Support" unless you initiated the interaction with them.
- Don't provide access to anyone claiming to have an urgent need to access your device.
- Don't share credentials to any websites or applications.

> **Note**
>
> Microsoft will never contact you through unsolicited emails, phone calls, or other methods to request access to your device. Microsoft will only request access to your device if you have contacted us and directly requested help with solving an issue you are experiencing. If you need customer service support from Microsoft, please visit **Microsoft Support**.

If you suspect that the person connecting to your device is being malicious, disconnect from the session immediately and report the concern to your local authorities and/or any relevant IT members within your

organization.

If you or someone you know has been affected by a tech support scam, use the technical support scam form to report it.

Next steps

If you have any problems, questions, or suggestions for Quick Assist, contact us by using the Feedback Hub app.

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module

Get started with making Remote Assist calls - Training

Learn about Remote Assist.

Certification

Microsoft Certified: Information Security Administrator Associate(beta) - Certifications

As an Information Security Administrator, you plan and implement information security of sensitive data by using Microsoft Purview and related services. You're responsible for mitigating risks by protecting data inside collaboration environments that are managed by Microsoft 365 from internal and external threats and protecting data used by AI...