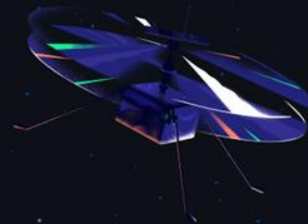# GitHub Copilot Administration & Security

Andrew Scoppa

AGENDA

GitHub Copilot - Overview

Policies and settings

Telemetry

Data privacy

Troubleshooting

Integrations

Q & A

GitHub Copilot Overview

GitHub Copilot

- An intelligent pair programmer
- Draws context from comments & code to suggest individual lines and whole functions
- Powered by OpenAI Codex
    - Copilot uses a transformative model
    - Trained on large datasets to ensure accuracy
- Available as extensions to popular IDEs
- Programming Languages and Technology available in Public code base all are supported

February 2023

sentiment.ts   write_sql.go   parse_expense

```ts
#!/usr/bin/env ts-node

import { fetch } from "fetch-h2";

// Determine whether the sentiment of
// Use a web service
async function isPositive(text: string
  const response = await fetch(`http://
    method: "POST",
    body: `text=${text}`,
    headers: {
      "Content-Type": "application/x-ww
    },
  });
  const json = await response.json();
  return json.label === "pos";
}
```
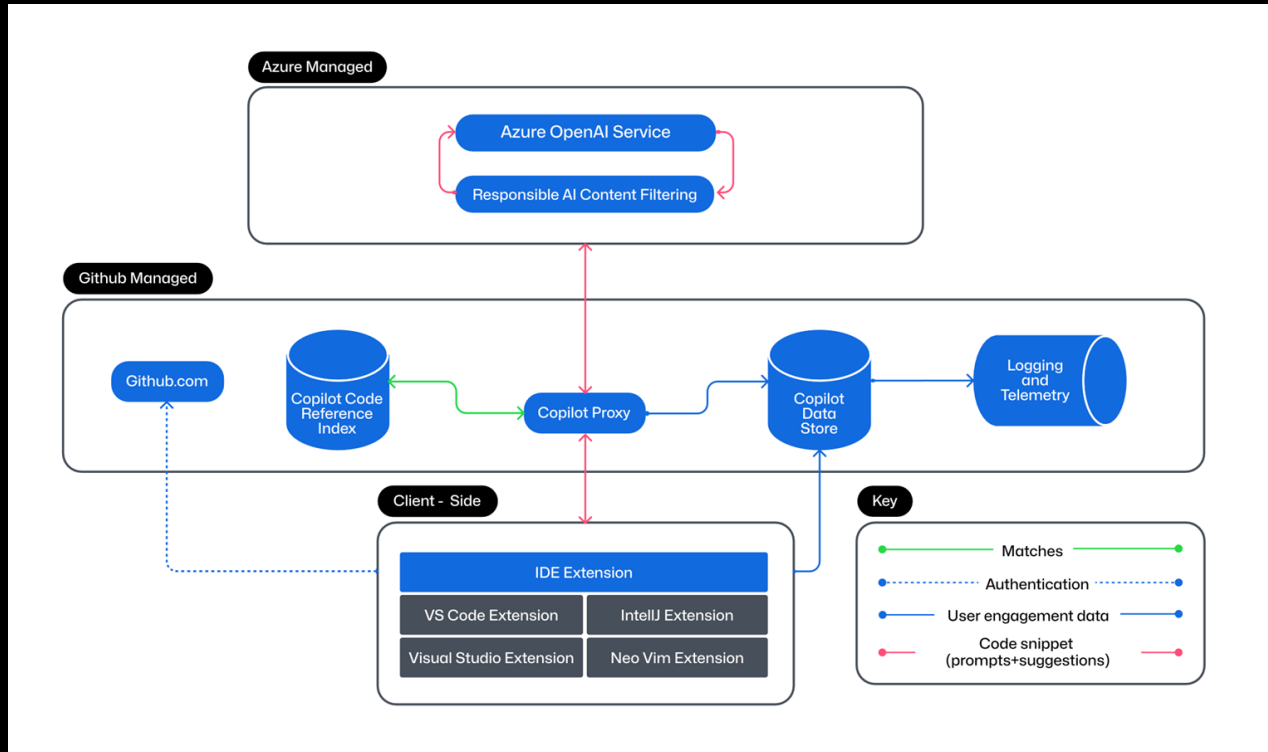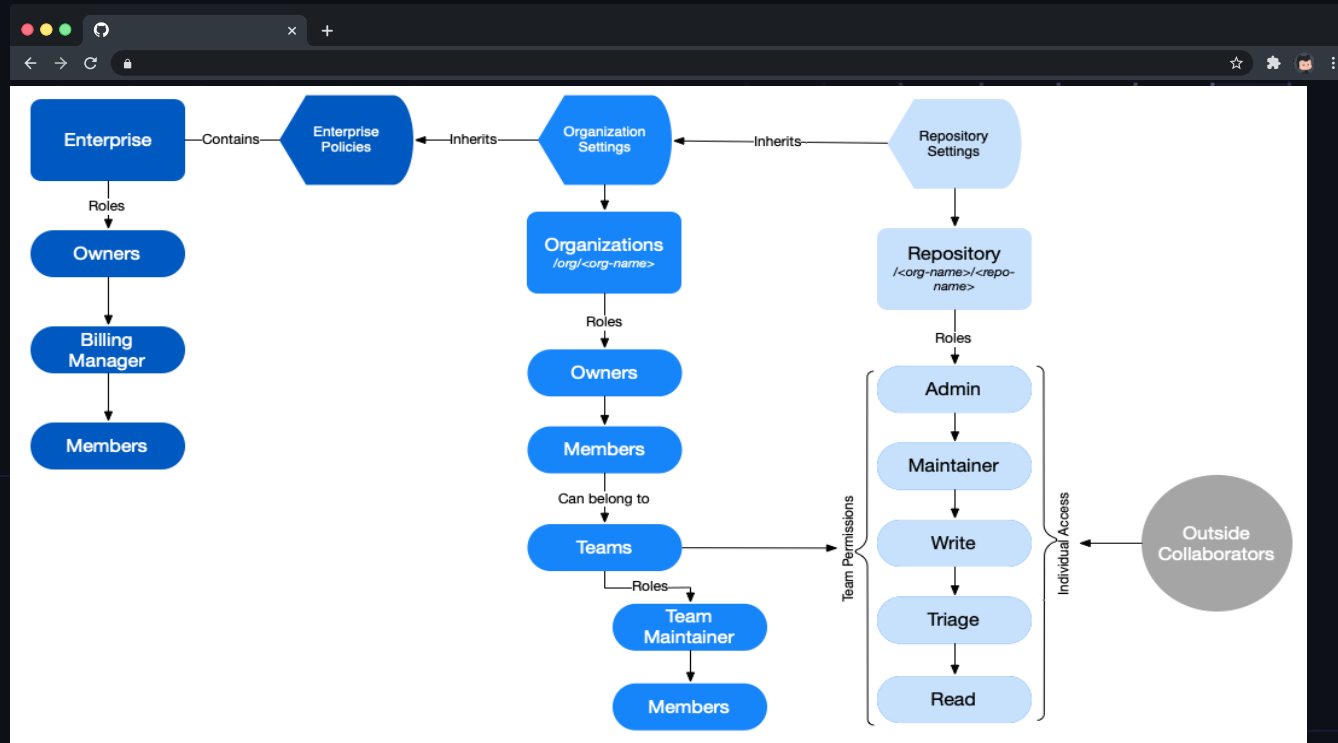
Copilot

Policies and settings

Govern the usage of GitHub Copilot in your Enterprise

Flow of Policies and Permissions

Enterprise Admin Policies

Control whether **suggestions matching public code** is allowed or blocked

- Blocked
- Allow
- No Policy

Manage organization access to GitHub Copilot.

- Disabled
- Allow for all organizations
- Allow for specific organizations

Manage Copilot Chat access.

- No Policy
- Enabled
- Disabled

Fabrikam EMU
Computer Company in Seattle, Washington

https://fabrikam.com

- Organizations
- People
- Identity provider
- Policies
  - Repositories
  - Codespaces
  - Copilot
  - Actions
  - Projects
  - Teams
  - Code security and analysis
  - Personal access tokens (Beta)
  - Sponsors
- GitHub Connect
- Code Security

GitHub Copilot

Access and policies   Beta features

Suggestions matching public code

GitHub Copilot can allow or block suggestions matching public code. See the GitHub Copilot documentation to learn more.

[No policy ▾]

Manage organization access to GitHub Copilot

Assign which organizations will have access to GitHub Copilot inside your enterprise. Admins of an organization with approved access will receive an email with setup instructions.

○ **Disabled**
Disable GitHub Copilot access for my organizations

◉ **Allow for all organizations**
Allow access to GitHub Copilot for all organizations, including any created in the future

○ **Allow for specific organizations (433 organizations enabled)**
Only specifically-selected organizations may use GitHub Copilot

Your enterprise's use of GitHub Copilot is governed by the GitHub Copilot Product Specific Terms.
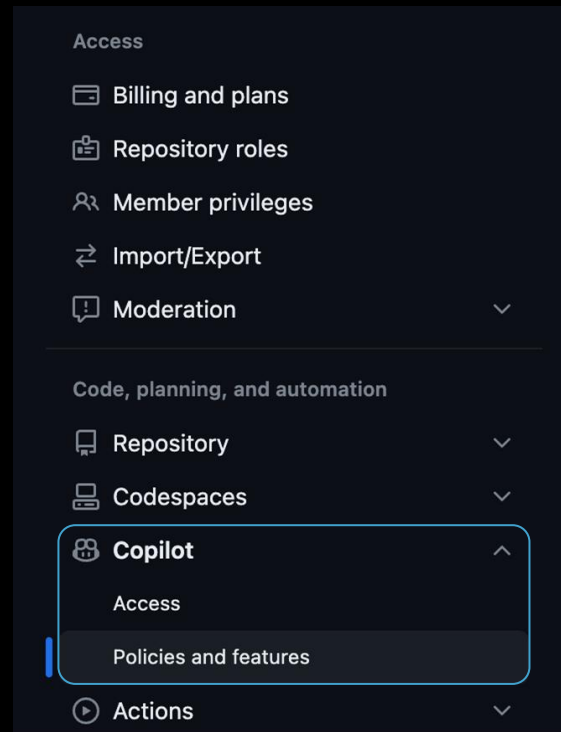
[Save]

8

Organization Settings

Categorization of Copilot Organization settings

Access

Manage, control and audit the users Copilot interaction

Policies and features

Regulate Copilot functionality and feature enablement

Access

- Billing and plans
- Repository roles
- Member privileges
- Import/Export
- Moderation

Code, planning, and automation

- Repository
- Codespaces
- Copilot
  - Access
  - Policies and features
- Actions

Organization Settings

Manage & Control Access

Access Settings

- View Number of Copilot license utilized

- Estimated cost of Copilot Usage within the Org

- Policy to enable Copilot for all members in the org or selective members

- Extract report of Copilot activity per user

GitHub Copilot

Copilot seats

831 seats

Number of purchased seats in this organization.
Learn more on licenses.

Estimated monthly cost

$15,789.00

Each purchased seat is $19 USD/month.
Review billing details.

Copilot in your organization

Control which users or teams will have access to GitHub Copilot inside your organization. Invited users with approved access will receive an email with setup instructions. Organization settings documentation.

Enabled for: All members of the organization ▾

Access management

📄 Get report

🔍 abhi-dutta

831 members with access to Copilot   ⇅ Sort ▾

@abhi-dutta   Last active 2 days ago

10

Organization Settings

Access - Copilot user activity report (sample)

octodemo-seat-usage-1696435416

Login	Status	Team	Last Activity Date	Last Editor Used
Abc	Active	No team	2023-10-04	vscode/1.83.0-insider/copilot-chat/0.8.2023092902
Lakes	Active	No team	2023-09-13	vscode/1.82.0/copilot-chat/0.7.2023090101
Chaos	Active	No team	2023-10-04	vscode/1.82.1/copilot/1.111.404
Akjsda	Active	No team	2023-10-04	vscode/1.82.2/copilot-chat/0.7.1
Sbdkajs	Active	No team	2023-10-04	vscode/1.82.3/copilot-chat/0.7.1
Asa	Active	No team	2023-05-26	vscode/1.78.2/copilot/1.86.82
Baksjdb	Active	No team	2023-10-04	vscode/1.82.3/copilot-chat/0.7.2023090101
Jshbda	Active	No team	2023-10-04	/

Organization Settings

Policies & Features

- Policies and features settings allow an org owner to define policies which will be applicable to all the users that have been onboarded to GitHub Copilot under the org

- Allows org owners to define whether "public code" matching is allowed in suggestions

- Can users use Copilot Chat (beta) feature in the supported IDE's

GitHub Copilot policies and features

Policies

Suggestions matching public code
Copilot can allow or block suggestions matching public code.

Allowed ⌄

Technical preview

Enable or disable limited public beta access for members of your organization with access to GitHub Copilot. Note that users from other organizations may gain access if permitted by their administrators.
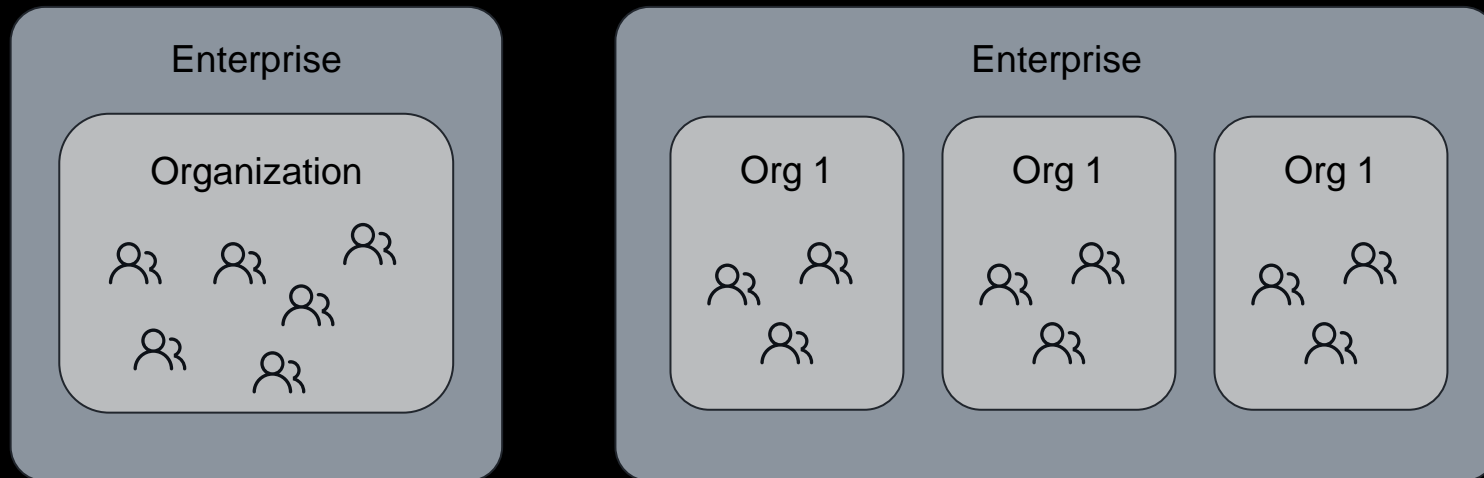
Features

GitHub Copilot Chat Beta
GitHub Copilot to explain a piece of code, propose bug fixes, or generate unit tests in a chat interface from your editor. If enabled, you agree to pre-release terms.

Enabled ⌄

Single Org vs Multi Org

Client Side Settings

Network Settings

Proxy Settings

- GitHub Copilot supports basic HTTP proxy setups. If you need to authenticate to a proxy, GitHub Copilot supports basic authentication or Kerberos. If the proxy URL starts with `https://`, the proxy is not currently supported.

- If you don't configure a proxy directly in your editor, GitHub Copilot checks if a proxy URL is set in any of the following environment variables, from highest to lowest priority.

    - HTTPS_PROXY
    - https_proxy
    - HTTP_PROXY
    - http_proxy

Authentication Modes

- Basic Authentication
- Kerberos Authentication

Configuring network settings

15
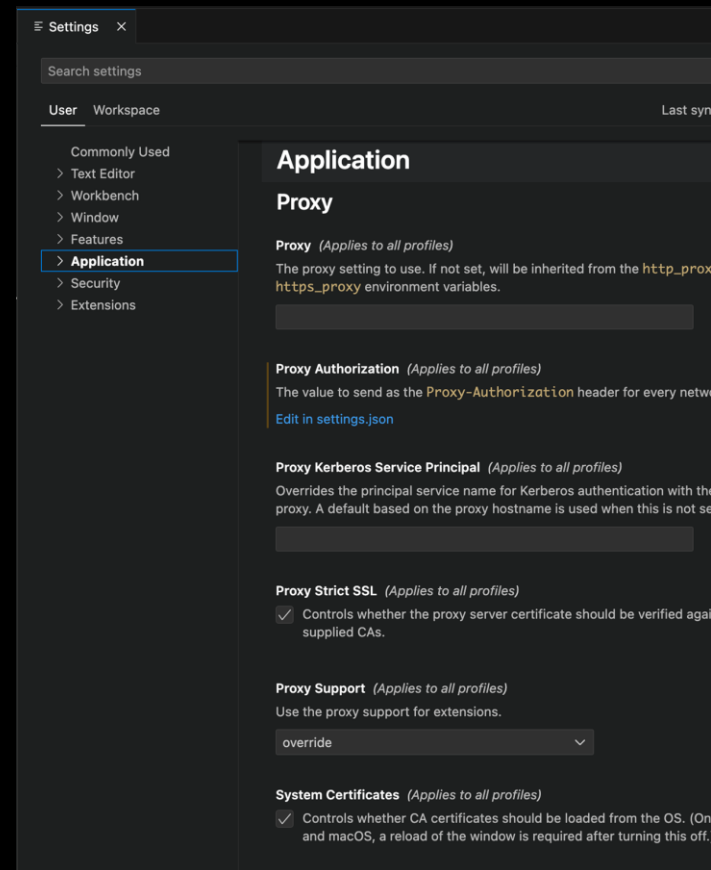
Firewall Settings

If you or your organization employs security measures like a firewall, it may be beneficial to include certain domain URLs in an "allowlist" and open specific ports and protocols.

Domain and/or URL	Purpose
`https://github.com/login/*`	Authentication
`https://api.github.com/user`	User Management
`https://api.github.com/copilot_internal/*`	User Management
`https://copilot-telemetry.githubusercontent.com/telemetry`	Telemetry
`https://default.exp-tas.com/`	Telemetry
`https://copilot-proxy.githubusercontent.com/`	API service for Copilot suggestions
`https://origin-tracker.githubusercontent.com`	API service for Copilot suggestions
`https://*.githubcopilot.com`	API service for Copilot suggestions

troubleshooting firewall settings

IDE Advanced Settings

Supported IDEs

Visual Studio

Visual Studio Code

Jet Brains

Vim/Neovim

Azure Data Studio

Configuring GitHub Copilot in your environment - GitHub Enterprise Cloud Docs

18

Enable non-programming Meta Files

In settings.json, add

```
"github.copilot.enable":
{
    "*": true,
  "yaml": true,
  "plaintext": false,
  "markdown": true
}
```


configuring github copilot

User Onboarding Best Practices

Telemetry

Insights about GitHub Copilot acceptance in your enterprise

21

Telemetry - GitHub REST API

Get Copilot for Business seat information and settings for an organization

Note: You must authenticate using an access token with the ***manage_billing:copilot*** scope

`GET` `/orgs/{org}/copilot/billing`

cURL

```
curl -L \
  -H "Accept: application/vnd.github+json" \
  -H "Authorization: Bearer <YOUR-TOKEN>" \
  -H "X-GitHub-Api-Version: 2022-11-28" \
  https://api.github.com/orgs/ORG/copilot/billing
```

Example response

Status: 200

```
{
  "seat_breakdown": {
    "total": 12,
    "added_this_cycle": 9,
    "pending_invitation": 0,
    "pending_cancellation": 0,
    "active_this_cycle": 12,
    "inactive_this_cycle": 11
  },
  "seat_management_setting": "assign_selected",
  "public_code_suggestions": "block"
}
```

Note: As of 5th Oct 2023 - The GitHub Copilot for Business API endpoints are in public beta and subject to change. GitHub OPEN API Schemas are available here

22

Telemetry - GitHub Audit Logs

Copilot for Business users will now be able to review updates and changes to their Copilot settings through the **audit log**.

In large organizations or enterprises, tracking setting updates and purchases is crucial.
Our goal is to empower organization and enterprise admins to investigate changes to their Copilot for Business account and settings independently, eliminating the need to rely on support.

Audit Log: Copilot for Business events · Issue #822 · github/roadmap

Audit log

Events   Log streaming   Settings

Filters ▾   🔍 action:copilot

✖ Clear current search query

Events matching search query

dhruvg20 – copilot.cfb_seat_added
Copilot for Business seat was added for dhruv-gupta-live in the ⬛⬛⬛ organization because they were added to the organization
Unknown location | Unknown IP address | 2 weeks ago | ...

jschanfung – copilot.cfb_org_settings_changed
Copilot Chat setting changed from unconfigured to enabled for the ⬛⬛⬛ organization
Australia | 120.158.194.167 | 2 weeks ago | ...

dhruvg20 – copilot.cfb_seat_added
Copilot for Business seat was added for jschanfung in the ⬛⬛⬛ organization because they were added to the organization
Unknown location | Unknown IP address | on Sep 1 | ...

dhruvg20 – copilot.cfb_seat_added
Copilot for Business seat was added for dhruv-gupta-live in the ⬛⬛⬛ organization
India | 101.0.62.219 | on Jun 14 | ...

23

Data privacy

How GitHub protects your data

GitHub Copilot Trust Center

As GitHub's Chief Legal Officer, I understand the nuanced challenges of enabling company-wide AI adoption, especially in an evolving regulatory landscape. GitHub Copilot is enterprise-ready, but organizations need to clearly understand how the tool meets their compliance, security, and accessibility requirements.

Our aim is to bring you that clarity with the **GitHub Copilot Trust Center**.

https://resources.github.com/copilot-trust-center/

25

What Personal Data is Collected & How?

- User Engagement Data
  - Events generated with an IDE
  - Personal Data such as pseudonymous identifiers

- Prompts
  - Collection of code & contextual information to generate suggestions
  - User using a designated keyboard shortcut or pauses typing to request a suggestion

- Suggestions
  - One or more lines of proposed code and other output returned

Personal Data

- Uses the **source code** in IDE only to generate a suggestion.

- Performs several scans to identify and remove certain **information** within a prompt.

- **Prompts** are only transmitted to the AI model to generate suggestions in real-time

- Deleted once the **suggestions** are generated.

- **User engagement data** is used to improve the performance of the Copilot Service; specifically, it's used to

  a. Evaluating GitHub Copilot

  b. Sort algorithms

  c. Detecting potential abuse of GitHub Copilot

○ Copilot for Business does not use your code to train the Azure OpenAI model

Under the hood - Responding to a prompt

- Suggestions are not copied and pasted from any code database.

- Uses probabilistic reasoning to generate suggestions.

- GitHub Copilot sends a prompt to its AI model, which makes a probabilistic determination of what is likely to come next in your coding sequence and provides suggestions.

Aiding Secure Development

GitHub Copilot leverages a variety of security measures

- Remove sensitive information in code

- Block insecure coding patterns *

- Detect vulnerable patterns in incomplete fragments of code.

Throughout the SDLC, including code scanning, secret scanning, and dependency management.

* The Copilot prompt needs to be specific in it's request

FAQ

- How long the collected personal data will be retained?

    - User Engagement Data - 24 Months

    - Prompts - Discarded once a suggestion is returned

    - Suggestions - Not Retained

- Can the users control the sharing & use of their data?

    - User engagement data is required for the use of GitHub Copilot

        - General usage data

        - Pseudonymous identifiers

FAQ

- How does our collected data gets processed by GitHub?

  - Billing & Account Management

  - Produce Aggregated Reports

    - capacity planining, product development, regulatory financial reports

- How's our collected data used?

  - To measure the impact it has on the user

  - Fine Tune ranking & Sorting Algorithms and Prompt Crafting

  - Detect violation of Acceptable Use Policies.

  - Developers and their use of developer tools and services.

FAQ

- Is Telemetry available?

  - No, Telemetry is not available for Copilot for Business

- Organization-wide policy management

  - Yes, Policy settings can be implemented at an Organization level.

- Audit Logs?

  - Yes, Audit Logs are available along with Copilot specific events

- Http Proxy Support

  - Yes, HTTP proxy support via custom certificates available

Troubleshooting

Common issues and where to look

Common Issues

- GitHub's <u>Status Page</u>

- Update GitHub Copilot Extension

- Error: "GitHub Copilot could not connect to server. Extension activation failed"

- Open <u>Discussions on Copilot Community</u> with relevant files

34

Viewing Logs for GitHub Copilot

Supported IDEs

Visual Studio

Visual Studio Code

Vim/Neovim

Jet Brains

Firewall settings

Internal Network   Firewall   Attacker   Internet

GitHub Copilot's requires connectivity to these domain URLs

- Organization employs security measures like a firewall or proxy server

- <u>Allowlist domain URLs,</u> specific ports & protocols

- Interaction with Remote Learning Model

- Trusted domain URLs

Domain and/or URL	Purpose
`https://github.com/login/*`	Authentication
`https://api.github.com/user`	User Management
`https://api.github.com/copilot_internal/*`	User Management
`https://copilot-telemetry.githubusercontent.com/telemetry`	Telemetry
`https://default.exp-tas.com/`	Telemetry
`https://copilot-proxy.githubusercontent.com/`	API service for Copilot suggestions
`https://origin-tracker.githubusercontent.com`	API service for Copilot suggestions
`https://*.githubcopilot.com`	API service for Copilot suggestions

36

Network Proxy setup

- Company Equipment or Corporate Network

- Connecting to Internet via VPN or HTTP Proxy server

- Prevent connecting to GitHub' Servers
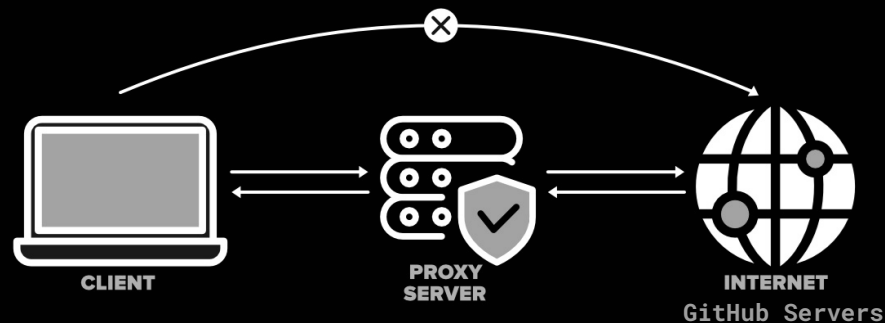
Network Proxy Errors

- Error: GitHub Copilot could not connect to server. Extension activation failed: "read ETIMEDOUT" or "read ECONNRESET"

- Configuring network settings for GitHub Copilot

- Proxy Specific errors:
    - Proxy's URL https:// currently not supported by GitHub Copilot
    - Authenticated supported basic authentication or with Kerberos
    - Custom certificates issues

Troubleshooting network errors for GitHub Copilot - GitHub Docs

Diagnosing Network Issues

- `curl requests with --verbose`

- `curl --verbose` https://copilot-proxy.githubusercontent.com/_ping

- `curl --verbose -x http://YOUR-PROXY-URL:PORT -i -L` https://copilot-proxy.githubusercontent.com/_ping
  `--insecure` -> Certificate related issues

- diagnostic logs from editors

Diagnosing network issues

Certificate Problems

- Errors: "certificate signature failure", "custom certificate", or "unable to verify the first certificate"

- Github Copilot for Business supports Custom Certificates

- Corporate proxy configurations

- Check GitHub Copilot certificate path

- Ignore Certificate Errors in Proxy settings
  Warning: Ignoring certificate errors can cause security issues and is not recommended

Troubleshooting certificate-related errors

Issues with GitHub Copilot Chat

- Org or Enterprise owners give access to GitHub Copilot Chat beta for users

- Install GitHub Copilot Chat Prerequisites

- Authentication Issues

- Error: "Oops, your response got filtered"

GitHub Copilot Chat - GitHub Enterprise Cloud Docs

Integrations

Use GitHub Copilot Endpoints and data with Enterprise tools

REST API - Copilot for Business

API Endpoints

- Get Copilot for Business seat information and settings for an organization

- List all Copilot for Business seat assignments for an organization

- Add teams to the Copilot for Business subscription for an organization

- Remove teams from the Copilot for Business subscription for an organization

- Add users to the Copilot for Business subscription for an organization

- Remove users from the Copilot for Business subscription for an organization

- Get Copilot for Business seat assignment details for a user

Audit Logs

Review the configuration actions taken by users at an Organisation & Enterprise level.

- Organization's Copilot settings and policies
    - Changes to the Enablement Policy
    - Org Settings changes
    - Enterprise settings changes

- Addition or removal of seats
    - Seat management changed
    - Seat assignment reused
    - Seat assignment refreshed

- Editor chat Settings

- Code Referencing Settings

Reviewing your organization or enterprise audit logs for copilot

44

Audit Log Events

cfb_enterprise_settings_changed	copilot.cfb_seat_cancelled
copilot.cfb_enterprise_org_enablement_changed	copilot.cfb_seat_assignment_reused
clickwrap_save_event	copilot.cfb_seat_assignment_refreshed
cfb_org_settings_changed	copilot.cfb_seat_assignment_created
copilot.cfb_seat_cancelled_by_staff	copilot.cfb_seat_assignment_unassigned
cfb_seat_management_changed	editor_chat_setting
copilot.cfb_seat_added	code_referencing_setting

Audit Logs

To review the actions taken by users at an Enterprise level.

Audit Logs

To review the actions taken by users at an Organisation level.

General
Features

Access

Billing and plans
Organization roles
Repository roles
Member privileges
Import/Export
Moderation

Code, planning, and automation

Repository
Codespaces
Copilot
Actions
Webhooks

Archive

Logs
Sponsorship log
Audit log
Deleted repositories

Events   Settings

Audit log

Filters ⌄   🔍 action:copilot   ⬇ Export Git Events ⌄   ⬇ Export ⌄

✕ Clear current search query

Events matching search query

taylorreis_fabrikam – **copilot.cfb_seat_added**
Copilot Business seat was added for taylorreis-guest_fabrikam in the copilot-for-emus organization because they were added to the organization
United States | 136.36.XX.XX | 3 weeks ago | ...
▶ View SSO details

taylorreis_fabrikam – **copilot.cfb_seat_added**
Copilot Business seat was added for taylorreis-slow_fabrikam in the copilot-for-emus organization
United States | 136.36.XX.XX | 3 weeks ago | ...
▶ View SSO details

taylorreis_fabrikam – copilot.cfb_org_settings_changed
Copilot Business public code suggestions setting changed from unconfigured to allowed for the copilot-for-emus organization
United States | 172.56.173.238 | on May 24 | ...
▶ View SSO details

Q & A

Thank you