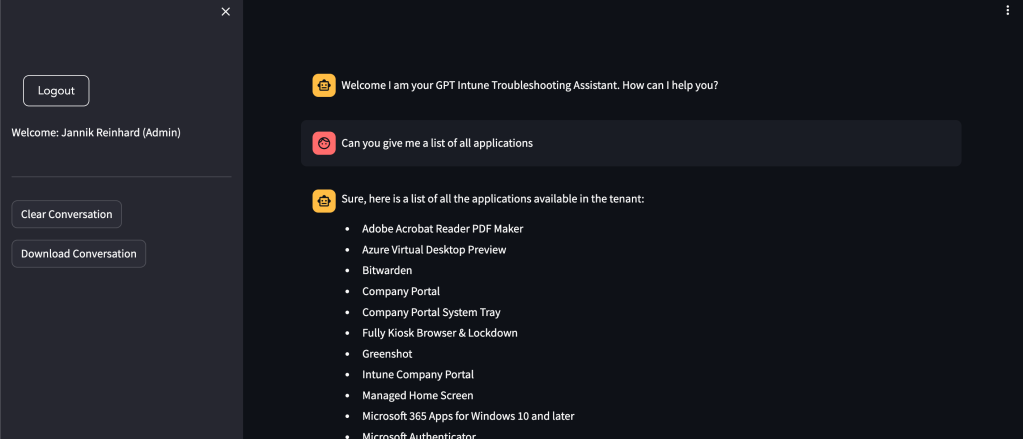
# The Magic of the GPT Intune , Device Troubleshooter

I am more than happy to release my new tool the Infra Shield AI - Cloud Commander. Wouldn’t it be awesome if you have an assistant which you explain what you want to do in Intune an he do the job for you? This dream will now become reality with the Infra Shield AI - Cloud Commander.



## Content

1. [Content](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#content)
2. [What is the Infra Shield AI - Cloud Commander](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#what-is-the-gpt-intune-device-troubleshooter)
3. [What are the prerequisites](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#what-are-the-prerequisites)
4. [How does it work](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-does-it-work)
5. [Get access to Open AI Service](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#get-access-to-open-ai-service)
6. [How it the data privacy when I use the Azure Open AI service](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-it-the-data-privacy-when-i-use-the-azure-open-ai-service)
7. [How to deploy the Infra Shield AI - Cloud Commander](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-to-deploy-the-gpt-intune-device-troubleshooter)
8. [What is the current feature sets and what are example calls](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#what-is-the-current-feature-sets-and-what-are-example-calls)
9. [How to create the app registration](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-to-create-the-app-registration)
10. [Post setup steps](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#post-setup-steps)
11. [How to open the Webpage](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-to-open-the-webpage)
12. [How does the Tool work](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-does-the-tool-work)
13. [How you can contribute?](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-you-can-contribute)
14. [How does the roadmap look like?](https://jannikreinhard.com/2023/09/10/the-magic-of-the-gpt-intune-device-troubleshooter/#how-does-the-roadmap-look-like)

## What is the Infra Shield AI - Cloud Commander

The Infra Shield AI - Cloud Commander is a powerfull tool which helps Intune admins to make here day easier. It answers your free text questions based on your enviroment utilizing graph api. You can ask questions like “Can you check the status of the device XXXX” or “Can you give me a device list with all android devices in csv” and you will get the customised answer to your question.

## What are the prerequisites

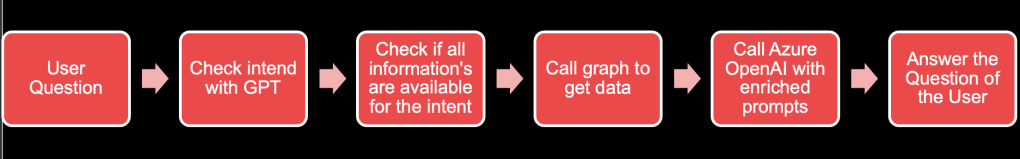
* GPT enabled Subscription
* App registration with deligated permissions for (DeviceManagementConfiguration.Read.All, DeviceManagementManagedDevices.Read.All, DeviceManagementApps.Read.All, User.Read)

![](data:application/xhtml+xml;base64,)

## How does it work

![](data:application/xhtml+xml;base64,)

* You can deploy the infrastructure with one click from GitHub to azure
* The code will be pulled to the app service
* The user open the streamlit web page
* The user authenticate via a app registration with delegated permissions for graph
* This token will be used to get data from graph and put them into an prompt
* This prompt with question and enriched informations will be send to the open ai service
* The answer will be presented on the streamlit web page



## Get access to Open AI Service

Fill out the following [request form](https://customervoice.microsoft.com/Pages/ResponsePage.aspx?id=v4j5cvGGr0GRqy180BHbR7en2Ais5pxKtso_Pz4b1_xUOFA5Qk1UWDRBMjg0WFhPMkIzTzhKQ1dWNyQlQCN0PWcu) to enable you subscription to deploy open ai services.

## How it the data privacy when I use the Azure Open AI service

You can finde more information about privacy in this [MS doc](https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy).

## How to deploy the Infra Shield AI - Cloud Commander

You dont have to do so much. The whole magic is behind this button.

[Deploy to Azure](https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fraw.githubusercontent.com%2FJayRHa%2FGPTDeviceTroubleshooter%2Fmain%2Fazuredeploy.json)

But you can also deploy the infratructure and the code manual via my [github repository](https://github.com/JayRHa/GPTDeviceTroubleshooter).

![](data:application/xhtml+xml;base64,)

* Select the subscription and the resource group
* Select the region and the Website sku
* Enter an name for the site and the open ai service account

## What is the current feature sets and what are example calls

Currently the following features are supported:

* Get Device List
* Get Device Status
* Get Single Device
* Intune How To
* Config Profiles
* App List
* Compliance Policies
* Device Group Membership
* Graph Call

Examples are:

* Can you give me a device list with all android devices in csv
* Can you check the status of the device XXXXX
* Can you check the status of the device XXXX and list the object which has conflict or have errors
* Can you give me a list of all applications
* Can you show me a list in csv of all apps which are created later than 01.01.2022
* In which groups is XXXX? Can you give me the display name and the ids

## How to create the app registration

* Open the [Entra portal](https://entra.microsoft.com/#home)
* Select **App registration**

![](data:application/xhtml+xml;base64,)

* Click **+ New registration**
* Enter an name for the App registration
* Select Single-Page application (SPA) as redirect type
* Add https://***WEBPAGENAME***.azurewebsites.net/login/callback as Redirect URI

![](data:application/xhtml+xml;base64,)

* Copy the **App ID**

![](data:application/xhtml+xml;base64,)

* Go to **API permissions** and click **+ Add a permission**

![](data:application/xhtml+xml;base64,)

* Select Graph

![](data:application/xhtml+xml;base64,)

* Select Delegated permissions

![](data:application/xhtml+xml;base64,)

* Add the following permissions (DeviceManagementConfiguration.Read.All, DeviceManagementManagedDevices.Read.All, DeviceManagementApps.Read.All, Group.Read.All, User.Read, Device.Read.All)
* Click Grant admin consent for XXX

![](data:application/xhtml+xml;base64,)

## Post setup steps

Add the App ID and the secret from the OpenAi Service to the Variables in the App Service Configuration

* Open the Open Ai Service

![](data:application/xhtml+xml;base64,)

* Go to Keys and Endpoint

![](data:application/xhtml+xml;base64,)

* Open the App Service

![](data:application/xhtml+xml;base64,)

* Navigate to Configurations
* Fill in the Azure open AI key and the App Id into the variables

![](data:application/xhtml+xml;base64,)

## How to open the Webpage

* Go to the App Service and Select **Browse**

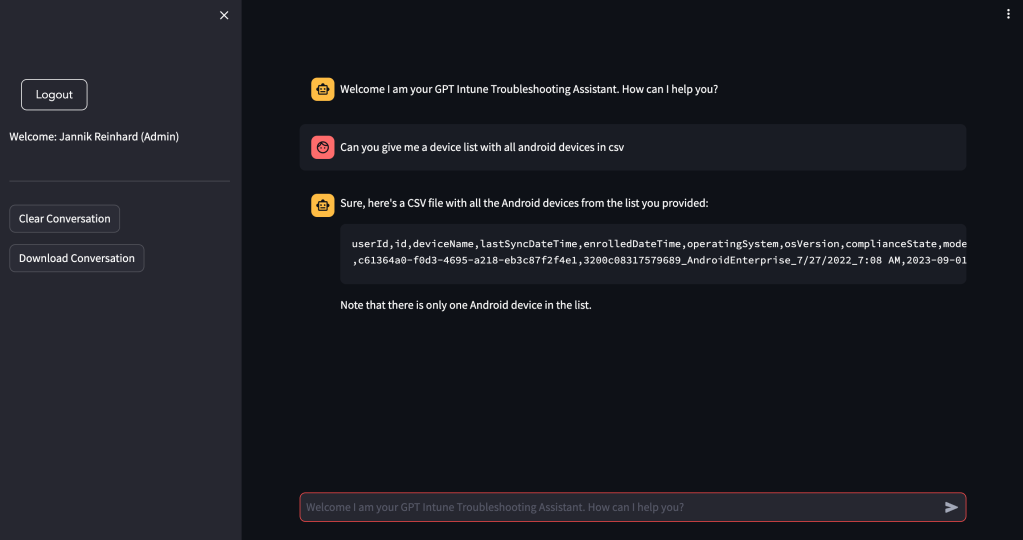
![](data:application/xhtml+xml;base64,)

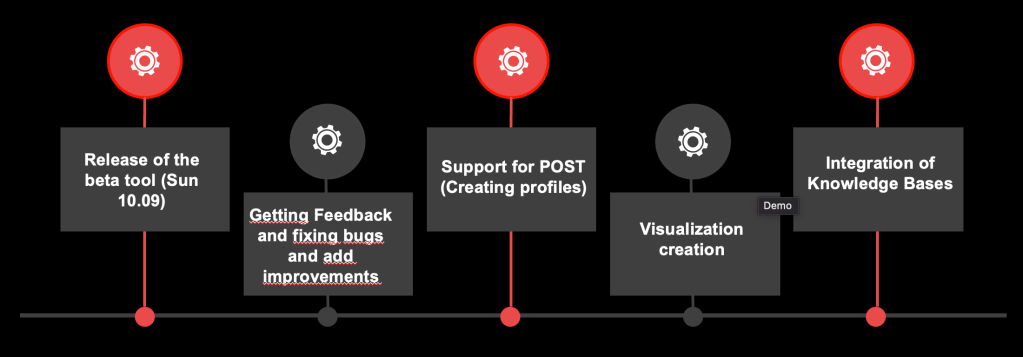
## How does the Tool work

* Click on login to get an Token to authenticate on graph

![](data:application/xhtml+xml;base64,)

* Insert your question in the chat box





Analyze the document and give me bullet points steps , on how to implement the same using PHi3.5 LLM , give me accurate details with each bullet point that you are writing

To implement the Infra Shield AI - Cloud Commander using the PHi3.5 LLM, here are detailed steps:

1. **Get Access to InfraShieldAi Service:**
   * Register for access to the InfraShieldAi Service by filling out the required request form to enable your subscription for OpenAI services.
2. **Create an App Registration in Azure AD (Entra Portal):**
   * In the Azure portal, navigate to the **App Registrations** section.
   * Click **+ New Registration** and enter a name for the application.
   * Choose **Single-Page Application (SPA)** for the redirect type.
   * Set the **Redirect URI** as https://WEBPAGENAME.azurewebsites.net/login/callback (replace with your actual webpage name).
   * After registration, copy the **App ID** for future steps.
3. **Assign Graph API Permissions:**
   * Under **API Permissions** in the app registration, click **+ Add a permission** and select **Microsoft Graph**.
   * Choose **Delegated permissions** and add the following:
     + DeviceManagementConfiguration.Read.All
     + DeviceManagementManagedDevices.Read.All
     + DeviceManagementApps.Read.All
     + Group.Read.All
     + User.Read
     + Device.Read.All
   * Grant **Admin Consent** for these permissions to allow Intune access and device management capabilities.
4. **Deploy Infra Shield AI - Cloud Commander via GitHub to Azure:**
   * Use the **One-Click Deploy** button provided in the GitHub repository to deploy the app to Azure.
   * When prompted:
     + Select the appropriate **Subscription** and **Resource Group**.
     + Choose the **Region** and **Website SKU**.
     + Enter a unique **Site Name** and your **OpenAI Service Account** details.
5. **Configure the App Service in Azure:**
   * Go to the **App Service** settings in Azure and navigate to **Configurations**.
   * In **Application Settings**, add your **InfraShieldAi Key** and the **App ID** from the previous steps as variables.
6. **Post-Deployment Steps for Testing:**
   * Open the App Service in the Azure portal, then select **Browse** to launch the web interface.
   * Log in via the login button on the web interface to obtain a token for Graph API authentication.
7. **Usage and Testing of Key Features:**
   * Enter queries directly into the chat interface, such as:
     + “Get a device list of all Android devices in CSV format.”
     + “Check the status of device [Device ID].”
     + “List all applications created after 01.01.2022.”
   * The system will retrieve data from Intune and provide responses based on the Graph API data.
8. **Security and Data Privacy:**
   * Review Microsoft’s data privacy documentation to ensure compliance with data protection standards, as data handled by the InfraShieldAi Service is processed according to Microsoft’s guidelines.

By following these steps, you can implement the Infra Shield AI - Cloud Commander using PHi3.5 or similar large language models to streamline Intune management tasks and automate device management requests efficiently.

### **Introduction to the InfraShieldAI Cloud Commander:**

**Overview:** The Infra Shield AI - Cloud Commander, powered by self-trained Phi3.5 model, is a solution that enables infra team to handle complex platform management tasks in Microsoft Intune with natural language prompts. The integration of AI and Microsoft’s Graph API allows seamless device tracking, status monitoring, and policy management within our organization network. It simplifies the administrator's job by transforming everyday requests into actionable results, bringing a new level of efficiency to infrastructure management.

**Key Objectives:**

* Simplify platform management in Microsoft Intune.
* Enhance productivity by automating repetitive tasks.
* Improve the accuracy of device diagnostics and reporting.

### **Benefits for an Organization**

1. **Streamlining Device Management Operations**
   * **Quick Access to platform**: Admins can retrieve comprehensive details on device status, compliance, and configurations by simply asking questions in natural language, such as “Show me the status of all Android devices.” This minimizes manual queries and provides instant answers, allowing IT teams to act quickly.
   * **Automated Reporting and Monitoring**: Generate reports on devices, applications, and user groups with commands like “List all applications created after [date].” Automating reporting reduces the time and effort needed to compile data, particularly for compliance audits and inventory management.
2. **Enhanced Troubleshooting and Diagnostics**
   * **Real-Time Device Status Checks**: IT admins can check the status of individual or groups of devices, making it easier to identify non-compliant or offline devices. This rapid diagnostic capability helps prevent issues before they escalate and allows proactive device health monitoring.
   * **Error and Conflict Resolution**: The tool can detect devices with errors or conflicts and display those issues for review. This enables quick corrective actions, improving device reliability and reducing support calls.
3. **Increased Productivity and Reduced Workload for IT Teams**
   * **Minimizing Manual Tasks**: By automating routine tasks like checking device statuses or generating compliance lists, IT teams save significant time. This allows skilled resources to focus on strategic projects rather than repetitive tasks.
   * **Seamless Integration with Microsoft Graph API**: The tool utilizes Microsoft Graph API to access data directly from Intune, making it easier for admins to manage configurations, device groups, and compliance policies in a centralized platform without switching between different interfaces.
4. **Improved Security and Compliance Management**
   * **Up-to-Date Compliance Monitoring**: The Troubleshooter offers real-time insights into device compliance, which is crucial for meeting industry standards and regulatory requirements. The tool can quickly identify non-compliant devices and prompt actions, minimizing risks related to data protection and privacy.
   * **Policy Enforcement**: The Troubleshooter can verify and enforce policies across devices, ensuring that security configurations are correctly applied. This helps in maintaining a secure device fleet, especially in organizations with a mix of operating systems and remote employees.
5. **Data Privacy and Security Assurance**
   * **Data Protection in InfraShieldAi**: The Troubleshooter leverages InfraShieldAi services, which ensures that all queries and responses follow Microsoft’s stringent privacy policies. For organizations, this reduces concerns around data leakage or unauthorized access while using AI in sensitive environments.
   * **Controlled Access**: Role-based access and Azure AD permissions for the Troubleshooter ensure that only authorized users can access device data, adding a layer of security to the tool.
6. **Flexibility and Scalability**
   * **Customizable Queries for Varied Needs**: The natural language processing feature allows admins to create custom queries tailored to their needs. For instance, they can generate lists, create device compliance reports, or check application installations as per specific dates or device types.
   * **Scalability for Large Organizations**: The tool’s integration with Microsoft Intune’s infrastructure and Azure’s robust cloud environment makes it scalable. This is beneficial for large organizations with extensive device fleets and varied user groups, as the tool adapts to increased data volumes and evolving device management needs.

### **Implementing the Infra Shield AI - Cloud Commander: Key Steps**

For organizations looking to adopt the Infra Shield AI - Cloud Commander, here are practical steps to get started:

1. **Setting Up Access with ISAI- LLM App Registration**: we need to request access to InfraShieldAi and create an app registration in Azure AD to enable the tool’s permissions to access device management data securely.
2. **Configuring Graph API Permissions**: Assigning delegated permissions in Graph API allows the Troubleshooter to retrieve device information and comply with user-specific data access policies, which is critical for secure and organized data retrieval.
3. **Deploying and Configuring the Tool on Azure**: Deploy the Troubleshooter via the GitHub repository, which provides a one-click deployment option. This quick setup enables a fast rollout across multiple locations if required.
4. **Training IT Staff for Optimal Use**: Familiarizing IT staff with the tool’s features ensures they can fully leverage its capabilities. This includes understanding the scope of queries they can run and troubleshooting methods for common device issues.

### **Use Cases and Real-World Scenarios**

1. **Large Enterprise with Diverse Device Types**:
   * For a company managing thousands of devices across different locations, the tool provides device status snapshots and compliance updates quickly. The Infra Shield AI - Cloud Commander helps keep the device fleet organized, minimizing downtime caused by unresponsive or misconfigured devices.
2. **Remote-First Organization**:
   * In organizations with remote work policies, IT admins can use the tool to verify that all remote devices are compliant with security policies. The ability to remotely monitor device health reduces security risks and ensures that the company’s remote workforce has access to the required resources.
3. **Compliance-Centric Industries**:
   * For sectors like finance or healthcare, where regulatory compliance is critical, the Troubleshooter provides timely compliance reports and policy enforcement insights, supporting data privacy and regulatory adherence.

### **Future of Device Management with AI-Powered Tools**

As AI and machine learning continue to evolve, tools like the Infra Shield AI - Cloud Commander represent the future of efficient, responsive, and intelligent device management. They enable organizations to manage increasingly complex IT environments with minimal human intervention, ensuring that security, compliance, and performance standards are met consistently.

### **Conclusion: Why Organizations Should Adopt the Infra Shield AI - Cloud Commander**

The Infra Shield AI - Cloud Commander addresses critical needs in today’s IT management landscape. It transforms the way organizations handle device management by reducing response times, automating compliance checks, and enhancing productivity. By integrating this AI-powered tool, companies can ensure efficient, scalable, and secure device management, enabling IT teams to focus on strategic tasks that drive business value.

This structure provides a detailed guide on the benefits and implementation of the Infra Shield AI - Cloud Commander for an organization, highlighting how it can transform device management, improve productivity, and secure data, all while adapting to future technological advancements.