paloalto TECHDOCS

Prisma Access Agent User Guide

April 2026

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 28, 2026

Table of Contents

Prisma Access Agent Overview

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent versions: • 25.1.4 (macOS and Windows) • 25.3 (Android and iOS) • 25.7 (Linux) ❑ Supported operating systems: • macOS 14 and later, Windows 10 version 2024 and later desktop devices • Android 10 and later versions or iOS 16 and later mobile devices • Linux Ubuntu 22.04 or 24.04, Arch Linux, Fedora 41 or 42, Debian 13, or Red Hat Enterprise Linux 9.6 or 10.0 devices ❑ Internet access

The Palo Alto Networks Prisma Access Agent is a secure access agent that is purpose-built for a remote-first workforce. It's focused on making the entire user experience better for end users, network admins, and IT help desk personnel without compromising on security.

You can use the Prisma Access Agent to access your organization's network, resources within the network, SaaS applications, or the internet securely from any location so that you can be productive in a hybrid workforce. Prisma Access Agent enables you to easily connect to corporate headquarters, data centers, branch offices, or educational institutions where Prisma Access or Palo Alto Networks Next-Generation Firewalls (NGFW) are deployed. When you're connected to a location (gateway) while working from anywhere, you benefit from the same security policies that protect the sensitive resources in your organization's network.

In addition, the Prisma Access Agent can help secure you and your devices from threats and malware through Advanced Threat Prevention, Advanced URL Filtering, DNS Security, sandboxing, and more.

Prisma Access Agent Features

The following features provide for a simplified agent experience:

- **Automatic Location Selection**

  The Prisma Access Agent is a simplified app that enables you to access your organization's network, resources, SaaS applications, or the internet using your organization's security policies that are extended to your device. If your administrator has configured the agent in **Always On** mode, you are automatically connected to your network using the best available location whenever you log on to your device. If your app is configured in **On Demand** mode, you can connect to the best location with the click of a button.

- **ADEM Integration**

  (macOS and Windows agents only) If your administrator has deployed the Application Experience agent (part of Autonomous Digital Experience Management (ADEM)) along with the Prisma Access Agent to your device, you can remediate network connectivity issues using the ADEM Self-Serve capabilities.

- **Notifications**

  (Not supported on Prisma Access Agent Linux) To minimize disruptions when you re accessing your organization's network, resources within the network, SaaS applications, or the internet, the Prisma Access Agent provides ample notifications so that you're always aware of the status of your connection.

  Prisma Access Agent notifications are fully integrated with your operating system, enabling you to customize how they behave like any other application.

- **Problem Resolution**

  (macOS and Windows agents only) You can save time by using the resources provided by the Prisma Access Agent to help resolve issues without having to contact your IT help desk or administrator. If the Access Experience agent is installed on your device, you can leverage the insights provided by ADEM to fix potential problems.

- **Anti-tamper Protection**

  (macOS and Windows agents only) To safeguard Prisma Access Agent, your administrator can enable the anti-tamper protection feature, which prevents any user from tampering with the Prisma Access Agent, such as unauthorized removal of the agent from your device. The anti-tamper feature can protect the following Prisma Access Agent resources on your device:

  - Prisma Access Agent folders and files—Unauthorized users can't delete or rename any Prisma Access Agent-related files and folders.
  - Prisma Access Agent services and host information profile (HIP) processes—Unauthorized users can't stop any Prisma Access Agent-related services and HIP processes. The HIP processes collect information about the host that the Prisma Access Agent running is running on and submits the host information to Prisma Access for inspection.
  - Prisma Access Agent Registry keys (Windows-only)—Unauthorized users can't delete or update the Windows Registry keys for the Prisma Access Agent.
  - The PACli command-line interface—Unauthorized users can't disable the Prisma Access Agent or the anti-tamper feature using the PACli command-line interface. Administrators

and authorized users who need to perform certain actions for troubleshooting at the command line must provide the anti-tamper unlock password when prompted.

Prisma Access Agent for Desktop Devices

Where Can I Use This?	What Do I Need?

• Prisma Access Agent	☐ Minimum Prisma Access Agent version:
	  • 25.1 (macOS and Windows)
	  • 25.7 (Linux)
	☐ macOS, Windows, or Linux desktop devices
	☐ Check the prerequisites for the supported OS versions
	☐ Internet access

The Prisma Access Agent is an application that's available on macOS, Windows, or Linux devices to enable you to access your organization's applications and services securely from anywhere in the world. Prisma Access Agent uses principles of zero trust network access and the same security policies that protect the sensitive resources in your organization's network.

Use the Prisma Access Agent to access your organization's network, resources in the network, software-as-a-service applications, or the internet, and to secure your device against threats that you might encounter on the internet. When connected, Prisma Access Agent sends traffic from your device to Prisma Access or NGFW, where the data is inspected and secured from threats and malware.

Depending on how your administrator configured the Prisma Access Agent, you will connect using one of the following connection modes:

- **Always On**—In always on mode, you're automatically connected to your network using the best available Prisma Access location whenever you log on to your device.
- **On Demand**—In on-demand mode, you decide when to connect to the best location using the Prisma Access Agent app.
- (macOS and Windows agents only) **Pre-Logon**—In pre-logon mode, Prisma Access Agent will automatically connect your network even before you log on to your operating system. Pre-logon enables IT maintenance tasks to be performed without user intervention, such as pushing agent upgrades to your device.

Learn how to install and use the agent, including how to log in to the Prisma Access Agent, change app settings, connect to a different location, and connect to a different server.

If your company requires you to access your organization's network and resources based on membership in a project, use the Dynamic Privilege Access enabled Prisma Access Agent to access your projects.

Preinstall Tasks for Prisma Access Agents on Linux

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: 25.7 ❑ Linux devices Check the prerequisites for the supported Linux distributions ❑ Internet access

Before you begin to install Prisma Access Agent on Linux, complete the relevant preinstall tasks.

- Set Up the Prisma Access Agent System Tray Icon on Ubuntu 22.04
- Set Up the Prisma Access Agent System Tray Icon on Fedora Linux (Wayland/GNOME)
- Set Up the Prisma Access Agent System Tray Icon on Red Hat Enterprise Linux
- Disable IPv6 on Linux Devices (Optional)
- Prepare Your NixOS System for Prisma Access Agent Installation

Set Up the Prisma Access Agent System Tray Icon on Ubuntu 22.04

If you're using Ubuntu 22.04, before you install the Prisma Access Agent, you need to set up the system tray icon functionality for Prisma Access Agent by installing the required GNOME extensions.

Before you begin:

- You need to be running Ubuntu 22.04 with the GNOME desktop environment
- Ensure that you have administrator (sudo) privileges.
- If you're running on a VM, you might need to disconnect GlobalProtect or Prisma Access Agent from the host system before proceeding.
- Each user on the Linux system needs to complete this configuration individually. These settings apply per user account rather than system-wide.

STEP 1 | Remove any existing AppIndicator extension that might conflict by running the following command in the shell:

```
sudo apt remove gnome-shell-extension-appindicator
```

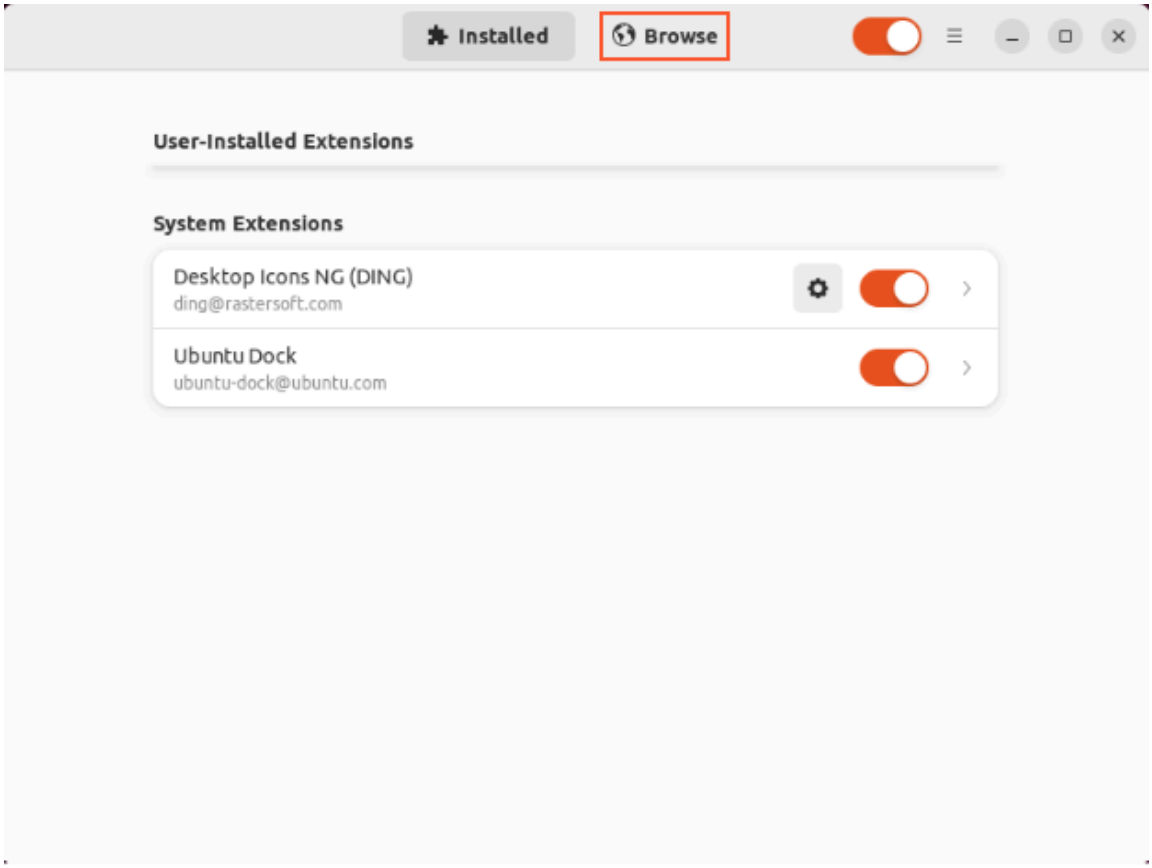
STEP 2 | Install the GNOME Extension Manager to easily manage extensions:

```
sudo apt install gnome-shell-extension-manager
```

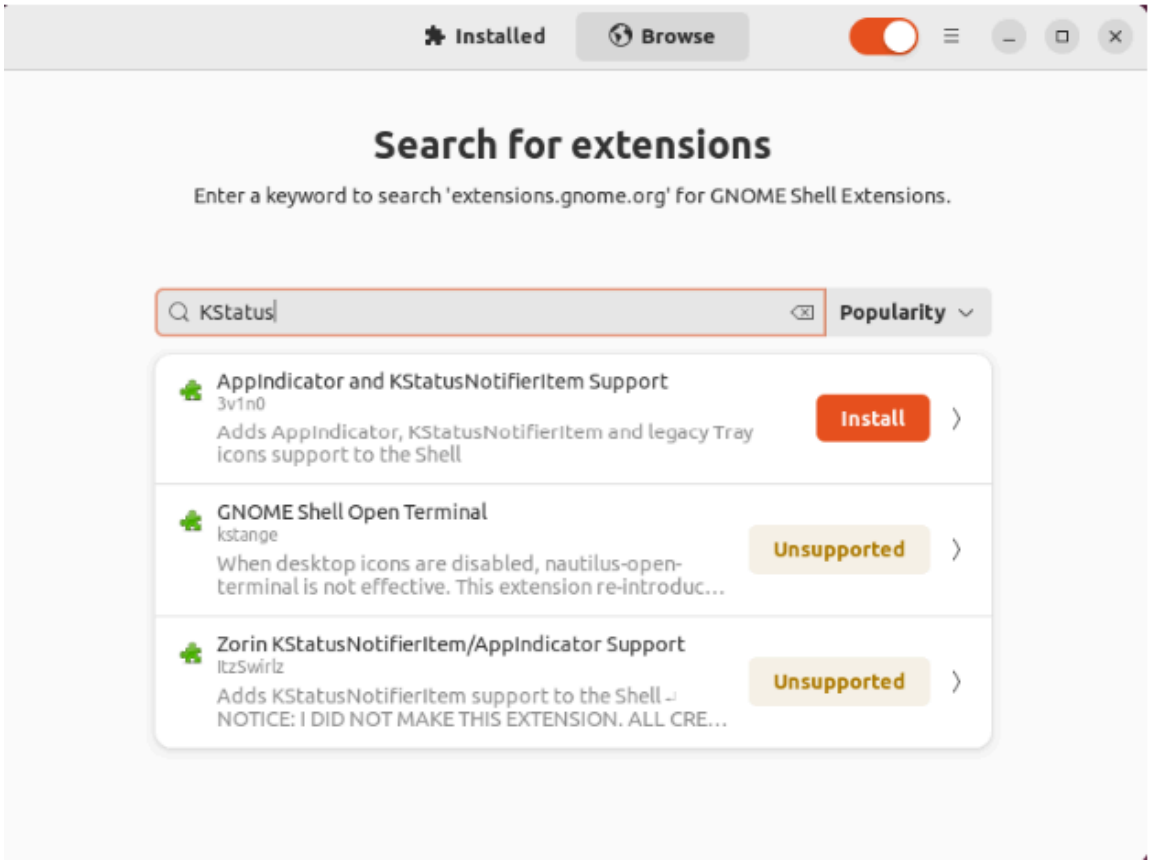

STEP 3 | Apply the changes by logging out of the operating system and logging back in again.

STEP 4 | Install the AppIndicator Support extension.

1. Open the **Extension Manager** application.
2. **Browse** the extensions.

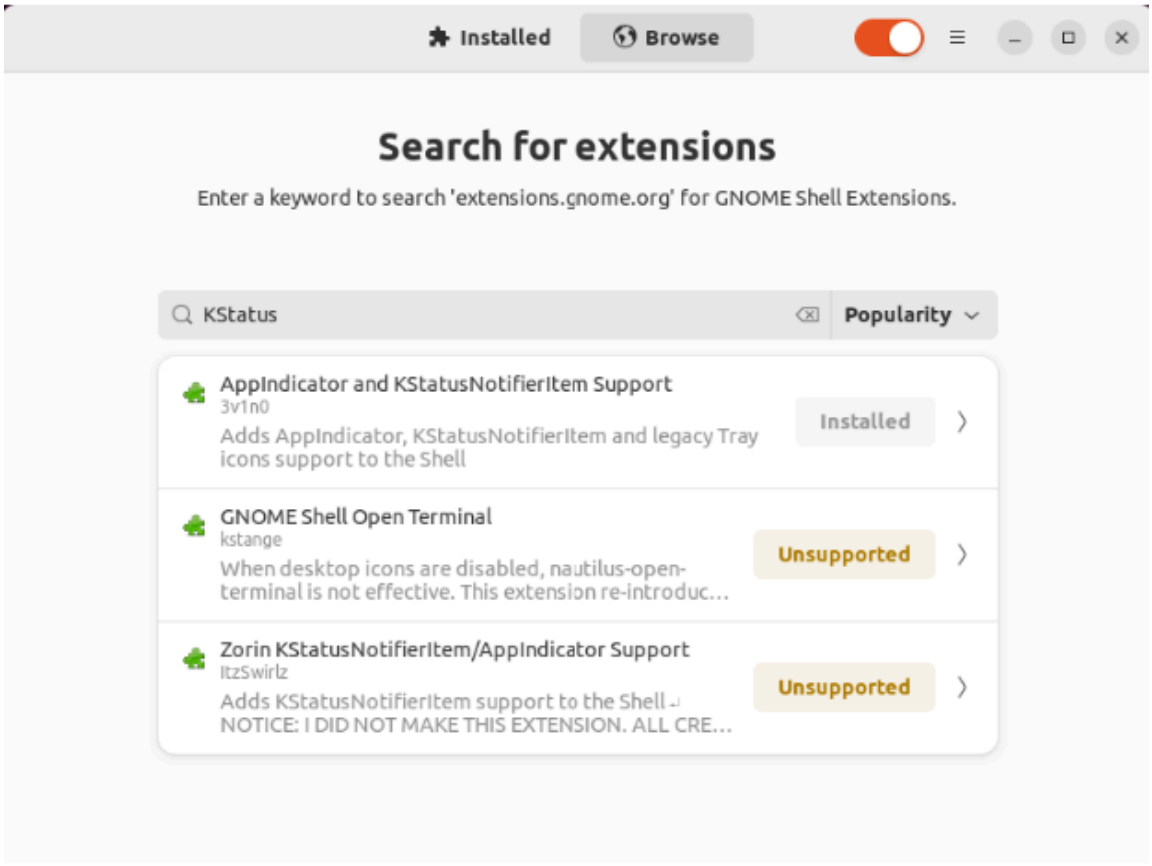


3. Enter **`KStatus`** in the search bar.
4. Locate **AppIndicator and KStatusNotifierItem Support** in the search results and **Install** the extension.



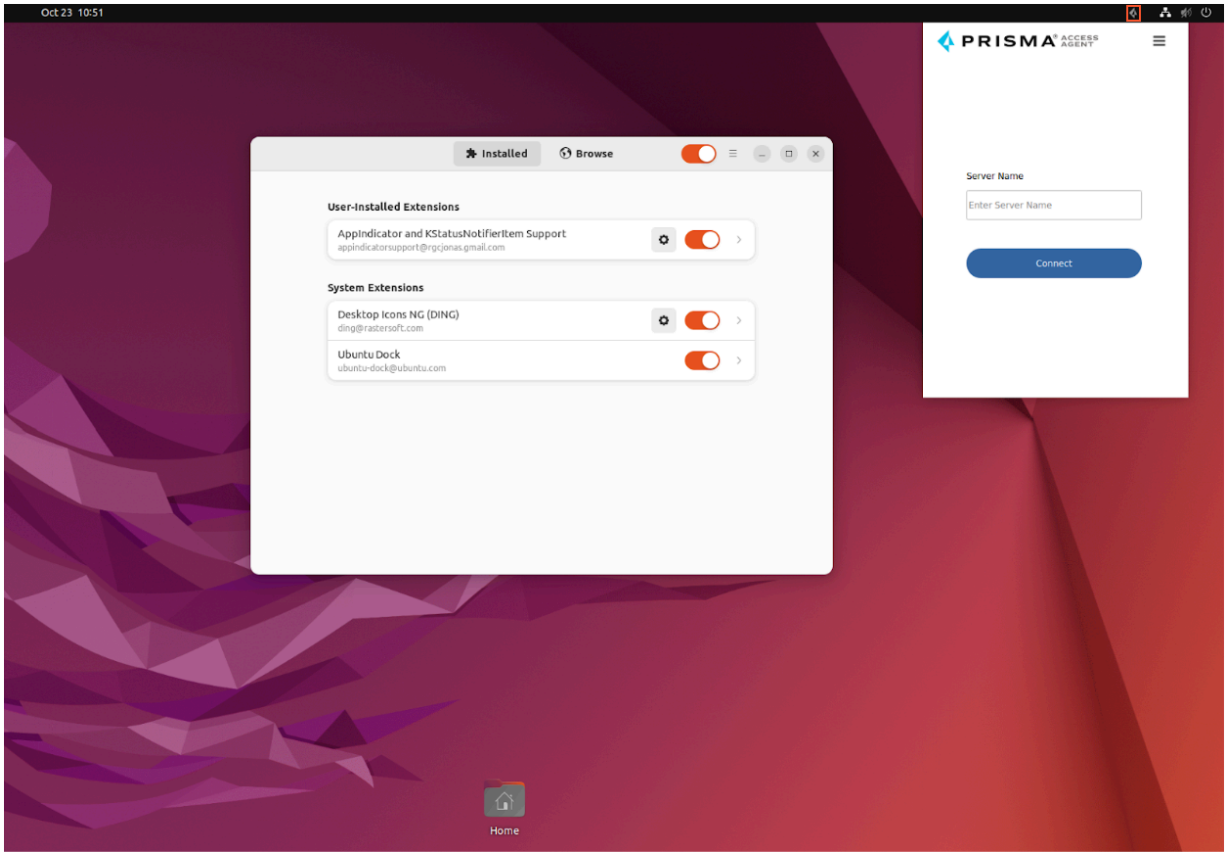
STEP 5 | Verify the installation of the AppIndicator Support extension.

1. Go to the **User-Installed Extensions** section in Extension Manager.
2. Confirm that **AppIndicator and KStatusNotifierItem Support** appears in the list of installed extensions and the extension is enabled (toggle is in the "on" position).



STEP 6 | Proceed with the Prisma Access Agent installation.

Once the extension is successfully installed and verified, you can proceed to install the Prisma Access Agent. The system tray icon should now display properly.



Set Up the Prisma Access Agent System Tray Icon on Fedora Linux (Wayland/GNOME)

Before installing Prisma Access Agent on Fedora Linux systems running the default Wayland display server with the GNOME desktop environment, you need to set up the system tray icon functionality for Prisma Access Agent by installing the required GNOME extensions.

This is a common issue since Wayland doesn't natively support the older system tray protocol that many applications, including Prisma Access Agent, still use. This task applies only to Prisma Access Agents running on Fedora ARM-based endpoints.

Before you begin, ensure that you have:

- Fedora Linux with the GNOME desktop environment
- Wayland display server (default on modern Fedora installations)
- Administrative (sudo) privileges

STEP 1 | Install the translation Layer (AppIndicator extension). This package provides the necessary translation layer to bridge legacy system tray applications with Wayland's security model.

```
sudo dnf install gnome-shell-extension-appindicator
```

STEP 2 | Install management tools (optional but recommended). These tools provide a graphical interface for managing GNOME extensions and browser integration for extension management.

```
sudo dnf install gnome-tweaks gnome-shell-extension-browser-
connector
```

STEP 3 | Enable and validate.

1. Restart your session by logging out and logging back in, or reboot the system to ensure the extension is loaded properly.
2. Enable the extension:
   1. Open the **GNOME Tweaks** application.
   2. Navigate to the **Extensions** section.
   3. Locate **AppIndicator and KStatusNotifierItem Support**.
   4. Toggle the switch to **ON** if not already enabled.
3. Proceed with the Prisma Access Agent installation.
4. Verify the functionality by confirming the Prisma Access Agent system tray icon appears correctly in the GNOME top bar, providing access to the Prisma Access Agent app.

Set Up the Prisma Access Agent System Tray Icon on Red Hat Enterprise Linux

(Prisma Access Agent 26.2) Before you install the Prisma Access Agent on Red Hat Enterprise Linux (RHEL), you need to set up the system tray icon functionality for Prisma Access Agent by installing the required GNOME extensions.

Before you begin, ensure that you have:

- Any supported RHEL distribution running with the GNOME desktop environment
- Administrator (sudo) privileges

STEP 1 | Enable the EPEL repository in the Terminal:

```
sudo dnf install epel-release
```

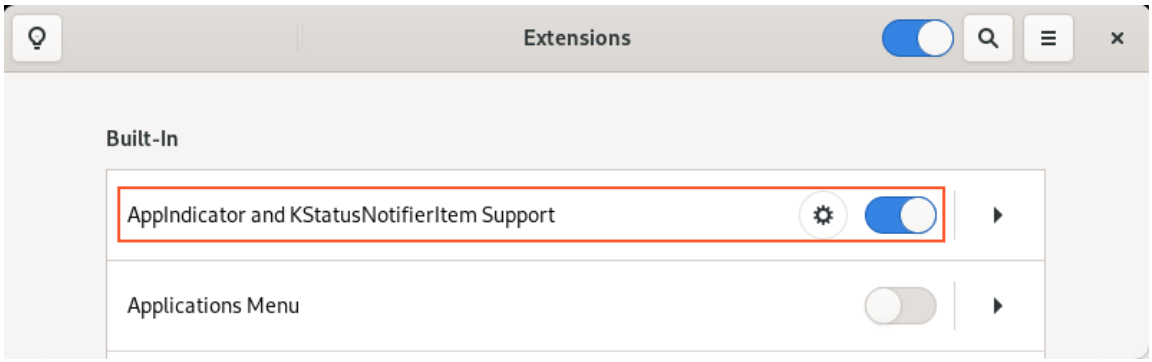
STEP 2 | Install the GNOME Extension Manager to easily manage extensions:

```
sudo dnf install gnome-shell-extension-appindicator
```

STEP 3 | Apply the changes by logging out of the operating system and logging back in again.

STEP 4 | Install the AppIndicator Support extension.

1. Open the **Extensions** application.
2. Search for the **AppIndicator and KStatusNotifierItem Support** extension.
3. Enable the extension by toggling it on.



STEP 5 | Once the extension is successfully installed and verified, you can proceed to install the Prisma Access Agent.

STEP 6 | Verify the functionality by confirming the Prisma Access Agent system tray icon appears correctly in the GNOME top bar, providing access to the Prisma Access Agent app.

Disable IPv6 on Linux Devices (Optional)

Prisma Access Agent for Linux does not support IPv6 sinkholing. If your organization allows IPv6 traffic, you'll need to disable IPv6 on your device before installing the agent to minimize your exposure from IPv6-based threats.

STEP 1 | Disable IPv6 at the system level using any available methods such as GRUB.

1. Edit the GRUB configuration file:

   ```
   sudo nano /etc/default/grub
   ```

2. Add or modify the `GRUB_CMDLINE_LINUX` parameter to include `ipv6.disable=1`:

   ```
   GRUB_CMDLINE_LINUX="quiet splash ipv6.disable=1"
   ```

3. Update the GRUB configuration:
   - For Ubuntu:

     ```
     sudo update-grub
     ```

   - For Arch Linux or Fedora:

     ```
     sudo grub-mkconfig -o /boot/grub/grub.cfg
     ```

4. Reboot the system:

   ```
   sudo reboot
   ```

5. Verify that IPv6 is disabled:

   ```
   cat /proc/sys/net/ipv6/conf/all/disable_ipv6
   ```

   The command should return `1` if IPv6 is successfully disabled.

STEP 2 | The Mozilla Firefox browser also requires disabling IPv6 for DNS queries. To disable DNS over HTTPS (DoH) in Firefox:

1. Open Firefox and enter `about:config` in the address bar.
2. Search for `network.dns.disableIPv6`.
3. Set the value to `true`.

Prepare Your NixOS System for Prisma Access Agent Installation

(Prisma Access Agent 26.2) NixOS support for Prisma Access Agent integrates the agent's security capabilities directly into your declarative NixOS environment. NixOS operates declaratively through your `/etc/nixos/configuration.nix` file, which **nixos-rebuild** processes.

The installation of Prisma Access Agent version 26.2 or later in your NixOS environment requires **nftables** to be enabled and the necessary CA certificates configured in your `configuration.nix` file for the agent's operation.

Complete the following steps so that your system has the necessary services, packages, and certificates before agent installation, aligning with NixOS's immutable system design.

STEP 1 | In NixOS, access your NixOS configuration file:

```
sudo vim /etc/nixos/configuration.nix
```

The default editor for NixOS is Nano. This example uses the Vim editor. You can also use other supported editors of your choice, such as Emacs.

STEP 2 | Enable **nftables** by adding the following statement to your NixOS configuration file:

```
networking.nftables.enable = true;
```

STEP 3 | Add the required system packages to your NixOS configuration:

```
environment.systemPackages = with pkgs; [
  vim
  wget
  nftables
];
```

STEP 4 | (Optional) Enable the SSH service in your `configuration.nix` file.

```
services.openssh.enable = true;
```

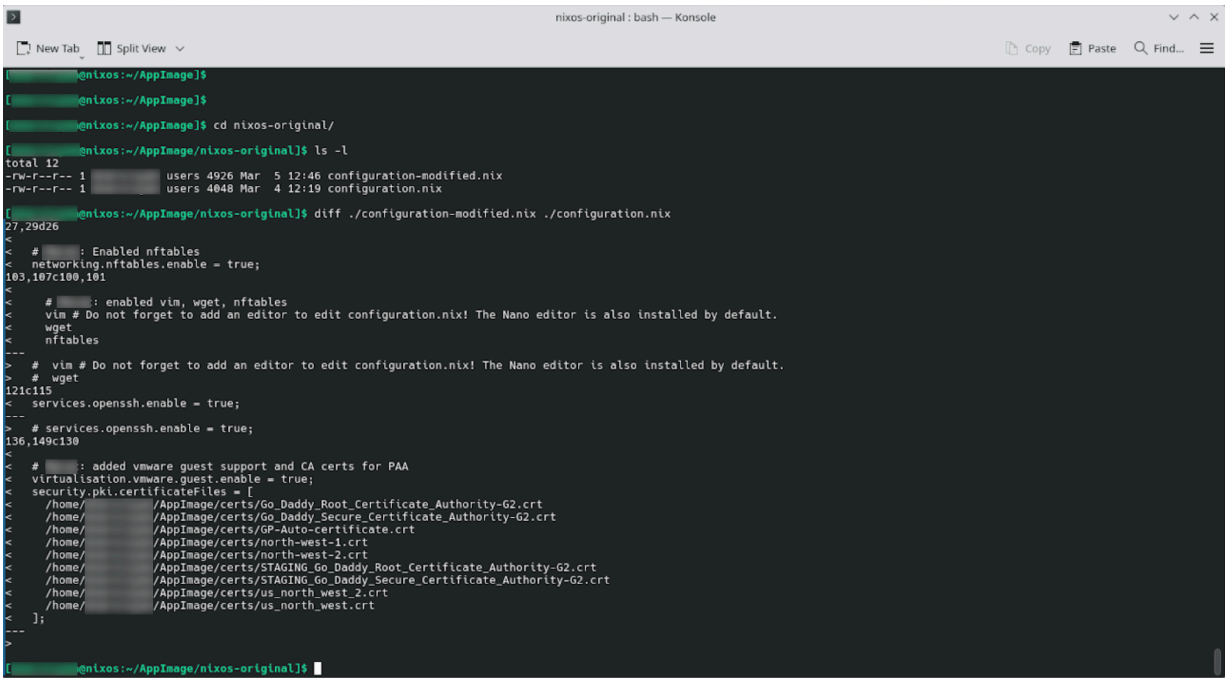
STEP 5 | Configure trusted CA certificates for Prisma Access Agent:

```
security.pki.trusted.pem = [
  "/path/to/your/ca.pem" # Replace with the actual path to your CA
 certificate
```



```
];
```

The following sample image shows the necessary additions to the `/etc/nixos/configuration.nix` file, including enabling **nftables** and adding required packages.



STEP 6 | Rebuild your NixOS system to apply the changes:

```
sudo nixos-rebuild switch
```


Install the Prisma Access Agent

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

If your administrator did not push the Prisma Access Agent to your device using supported mobile device management (MDM) software or an alternative distribution method, you can manually install the Prisma Access Agent on your macOS or Windows devicemacOS, Windows, or Linux device.

(Prisma Access Agent 25.3.1) (macOS and Windows agents only) To enable Endpoint DLP capabilities with Prisma Access Agent, your administrator must deploy the agent to your device using supported MDM software.

The Prisma Access Agent and GlobalProtect app can coexist on the same device, but only one of them can connect to Prisma Access. If you need to use the GlobalProtect app after installing the Prisma Access Agent, you will need to switch to the GlobalProtect app.

- macOS
- Windows
- Linux

Install the Prisma Access Agent (macOS)

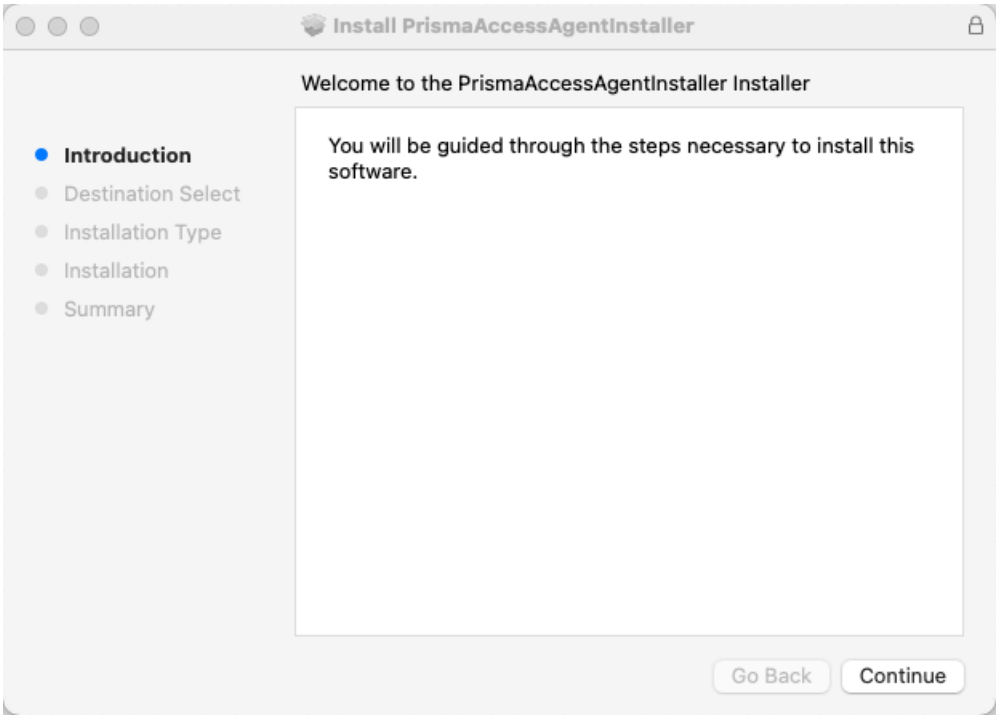
To manually install the Prisma Access Agent on your macOS device:

STEP 1 | Obtain the Prisma Access Agent package that your administrator provided to you. The package name is in the following format:

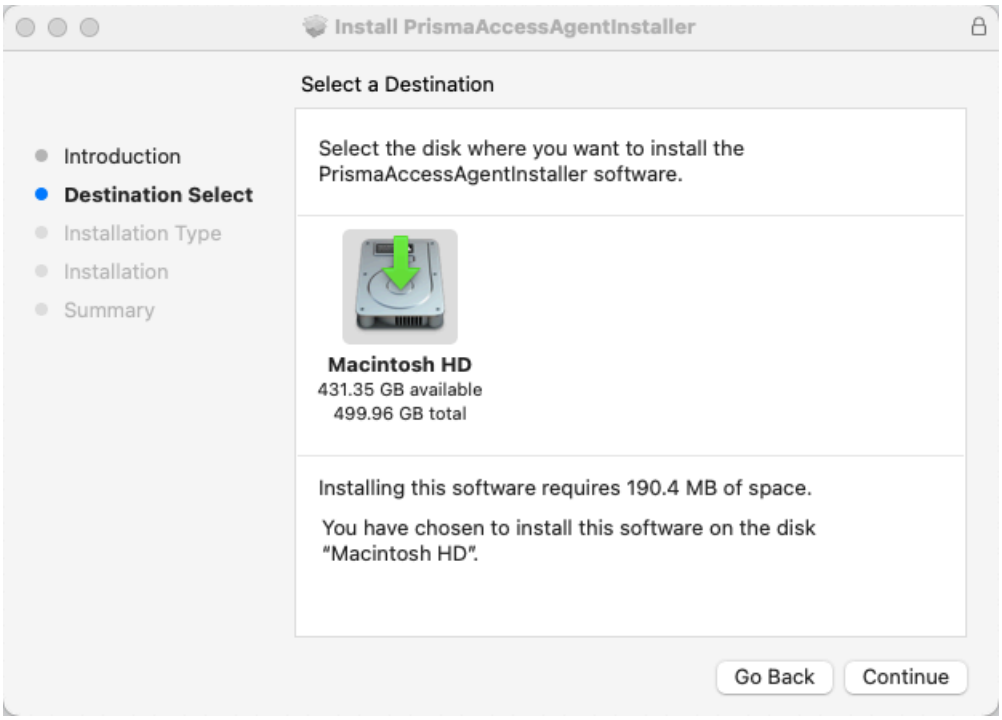
`PrismaAccessAgentInstaller_<version>.pkg`

STEP 2 | In your Downloads folder (or wherever you placed the installation package), open the installation package and follow the prompts to install the Prisma Access Agent.

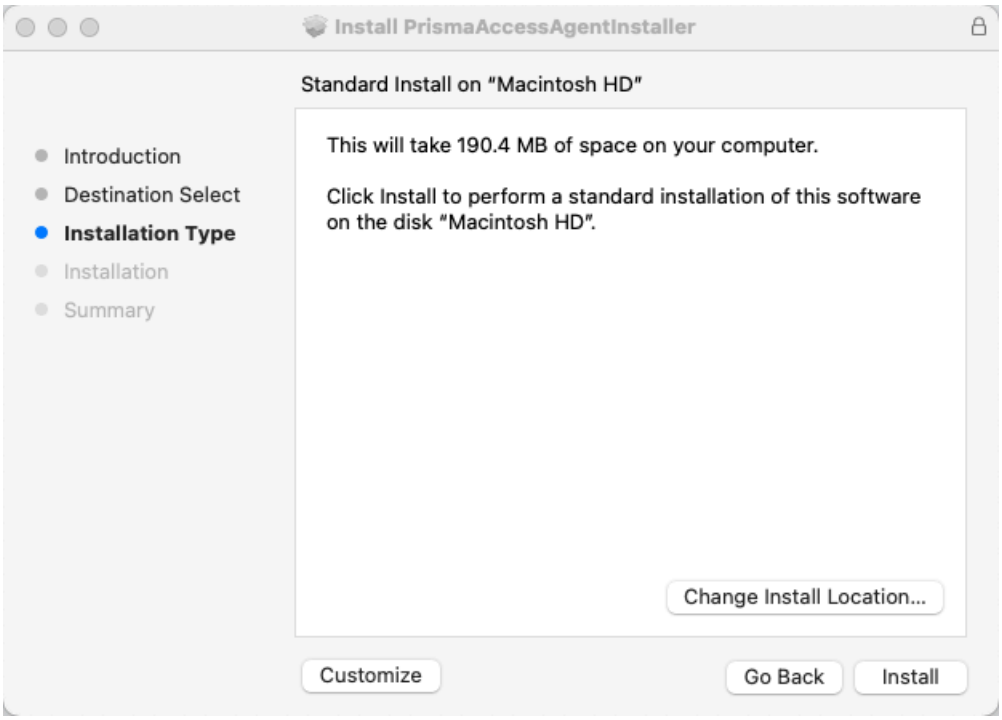
1. From the installer, click **Continue.**



2. Select the folder for the installation of the Prisma Access Agent and click **Continue**.



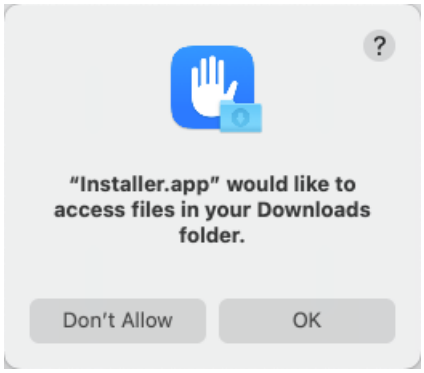
3. Review the information in the Installation Type page and click **Install**.



4. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to begin the installation.

   Alternatively, you can use Touch ID (if it's enabled) to complete this step.

5. When prompted to allow the installer to access files in the folder where you downloaded the installation package, click **OK**.

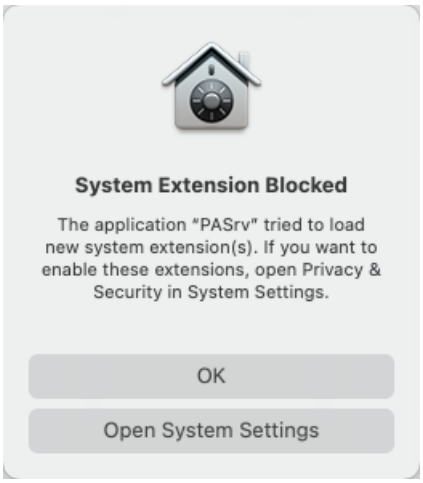


6. By default, macOS blocks the Prisma Access Agent system extensions. The system or network extensions appear if your administrator configured the Prisma Access Agent with traffic forwarding rules to:

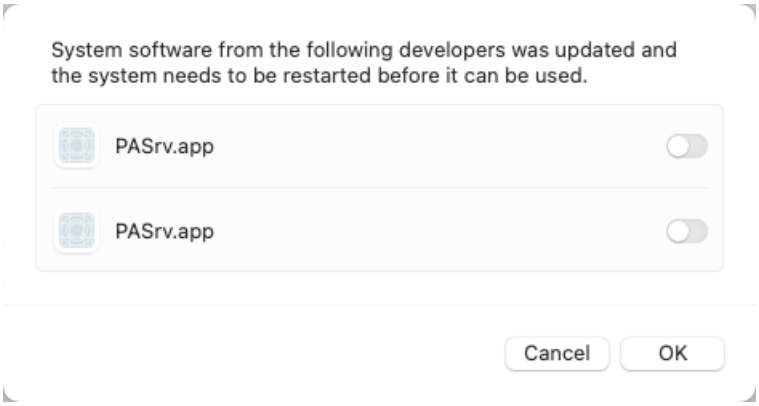
   - Direct network traffic through or outside of the Prisma Access connection.
   - Direct DNS queries for applications and resources through Prisma Access or outside of Prisma Access in addition to network traffic.

   For the Prisma Access Agent to work, you need to enable the system extensions.

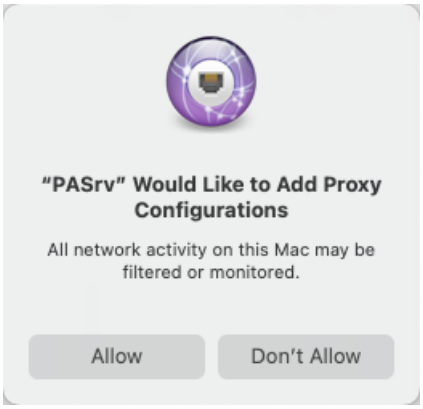
   1. Click **Open System Settings**.



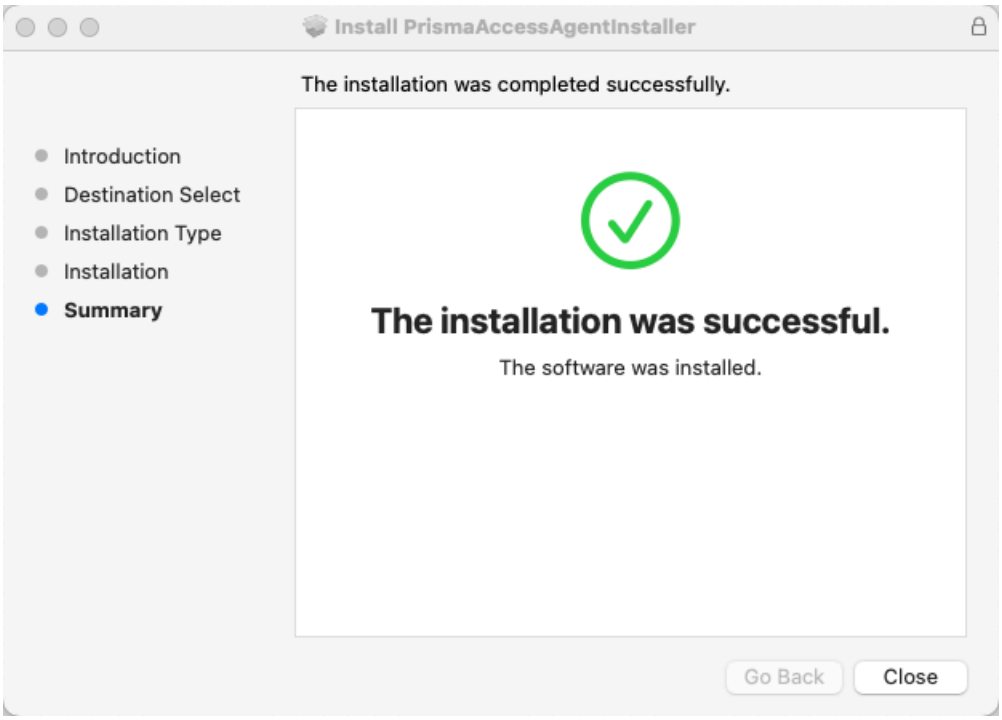
2. In the Privacy & Security window, click **Details** for **Some system software requires your attention before it can be used.**
3. Enable both **PASrv.app** apps and click **OK**.



7. If your administrator enabled the feature to enforce Prisma Access connections for network access, you will be prompted to add a configuration to filter network content. To proceed, click **Allow**.



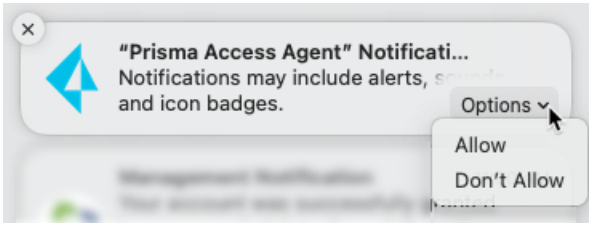
   After you allow this, the Prisma Access Agent will filter and monitor your network connections for security purposes.
8. When the installation is complete, **Close** the installer.



9. If your administrator configured the agent to install the Access Experience app along with the Prisma Access Agent, click **OK** so that you won't be prompted again.
10. Click the Prisma Access Agent notifications pop-up to open the Notifications preferences window.

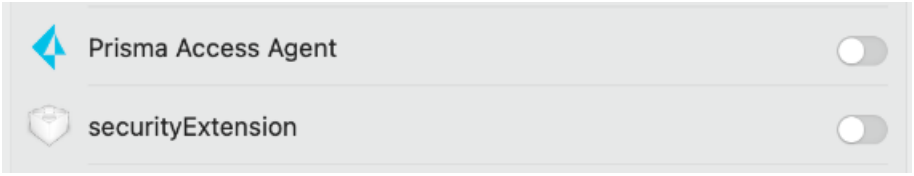
STEP 3 | If prompted, enable Prisma Access Agent notifications.

When the Prisma Access Agent notifications pop-up appears on your desktop, move your cursor over the pop-up and select **Options** > **Allow**.



STEP 4 | For the Prisma Access Agent to access data in the Safari browser, you must grant full disk access to the Security Extension and the Prisma Access Agent.

1. From macOS, select **System Settings** > **Privacy & Security** > **Full Disk Access**. Enable **Prisma Access Agent** and **securityExtension** from the list of apps.



2. When prompted, **Quit & Reopen** the Prisma Access Agent for the changes to take effect.

Uninstall the Prisma Access Agent (macOS)

You can uninstall the Prisma Access Agent manually if you no longer need to use it. Keep in mind that by uninstalling the agent, you will no longer have access to your corporate network, and your endpoint won't be protected by your organization's security policies.

Before you begin, if the administrator enabled anti-tamper protection for the Prisma Access Agent, you must obtain an uninstall one-time password (OTP) from the administrator. If your administrator allowed agent disablement with an OTP, you must obtain the disable agent OTP from them. To uninstall the agent, you must have elevated administrative rights.

Complete the following steps to uninstall the Prisma Access Agent from the command-line interface.

STEP 1 | Disable the Prisma Access Agent by running the following command:

```
/Applications/Prisma\ Access\ Agent.app/Contents/Helpers/pacli
 protect disable
```

1. If prompted for a password, enter the Disable Agent OTP.

STEP 2 | Run the following command to uninstall the agent:

```
/Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
uninstaller
```

STEP 3 | If prompted for the password, enter the Uninstall OTP and press **Enter** to begin the uninstallation of the agent and its extensions.

Install the Prisma Access Agent (Windows)

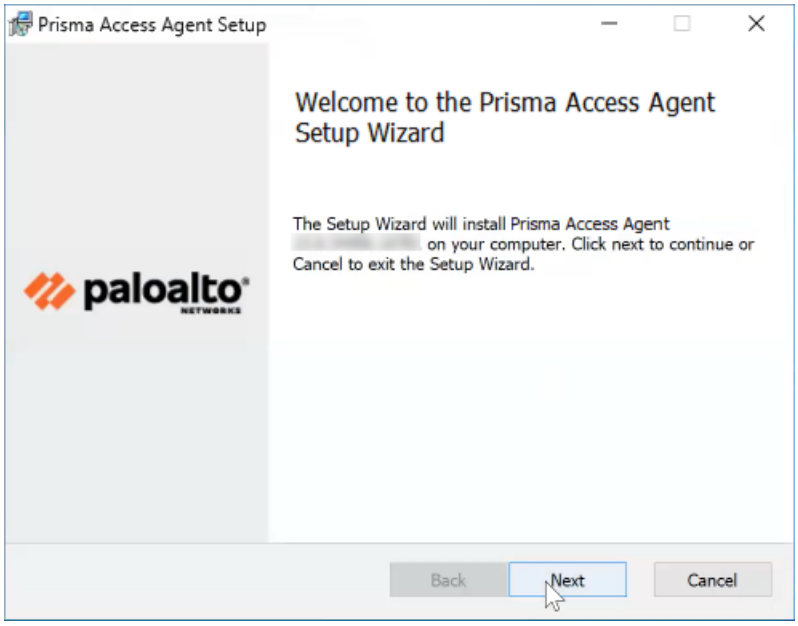
To manually install the Prisma Access Agent on your Windows device.

STEP 1 | Obtain the Prisma Access Agent package that your administrator provided to you. The package name is in the following format:

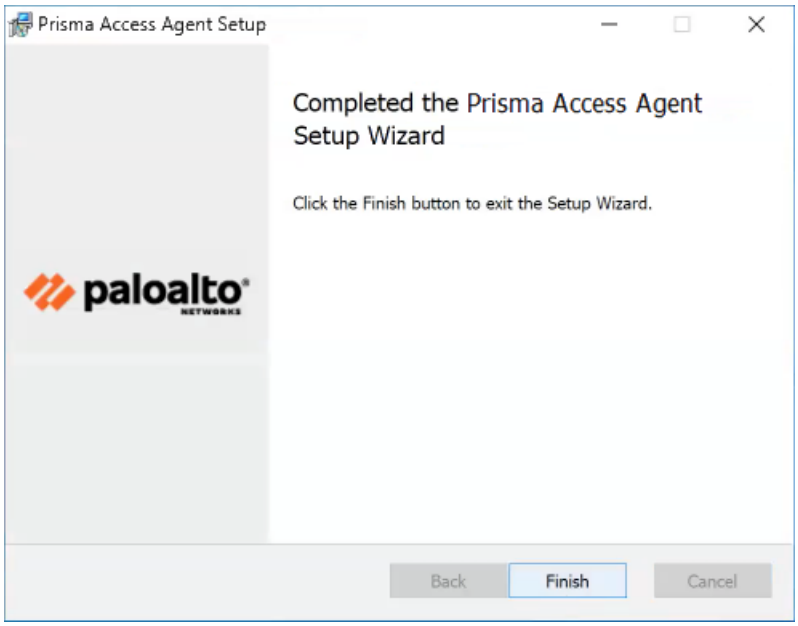
`PrismaAccessAgent_x64_<version>.msi`

STEP 2 | In your Downloads folder (or wherever you placed the installation package), double-click the installation package icon and follow the prompts to install the Prisma Access Agent.

1. When the setup wizard appears, click **Next** to continue.



2. Review the end-user license agreement, select **I accept the terms in the License Agreement**, and click **Next**.
3. Click **Install** to begin the installation.
4. When prompted to **allow this app to make changes to your device**, click **Yes**.
5. When the installation is complete, click **Finish**.



6. If your administrator configured the agent to install the Access Experience app along with the Prisma Access Agent, click **OK** so that you won't be prompted again.

Uninstall the Prisma Access Agent (Windows)

You can uninstall the Prisma Access Agent manually if you no longer need to use it. Keep in mind that by uninstalling the agent, you will no longer have access to your corporate network, and your endpoint won't be protected by your organization's security policies.

Before you begin, if the administrator enabled anti-tamper protection for the Prisma Access Agent, you must obtain an uninstall one-time password (OTP) from the administrator. If your administrator allowed agent disablement with an OTP, you must obtain the disable agent OTP from them. To uninstall the agent, you must have elevated administrative rights.

Complete the following steps to uninstall the Prisma Access Agent:

STEP 1 | Disable the Prisma Access Agent.

1. Run the following command in a Command Prompt window:

```
C:/Program Files/Palo Alto\ Networks/Prisma Access Agent/
PACli.exe" protect disable
```

2. If prompted for a token or OTP, enter the Disable Agent OTP.

STEP 2 | Uninstall the Prisma Access Agent.

- On Windows 11:
  1. Open the **Start** menu.
  2. Select **Settings** > **Apps** > **Installed Apps**.
  3. Scroll to **Prisma Access Agent**.
  4. Select **More Options** > **Uninstall**.
  5. When prompted to continue with the uninstall, click **Yes**.
  6. If prompted for a token or OTP, enter the Uninstall OTP.
- On Windows 10:
  1. Open the **Start** menu.
  2. Select **Settings** > **Apps** > **Apps & Features**.
  3. Scroll to **Prisma Access Agent**.
  4. Select **More** > **Uninstall**.
  5. When prompted to continue with the uninstall, click **Yes**.
  6. If prompted for a token or OTP, enter the Uninstall OTP.

Install, Manage, and Uninstall the Prisma Access Agent (Linux)

If your administrator did not deploy the Prisma Access Agent to your Linux device, you can install it manually. The Prisma Access Agent installation package uses the portable `AppImage` format that eliminates dependency conflicts and works across different Linux configurations without requiring package manager modifications. The Prisma Access Agent Linux AppImage encapsulates all agent components and their dependencies as a read-only `squashfs` file system image that mounts upon execution, ensuring consistent deployment.

This procedure outlines how to install, verify, upgrade, and uninstall the Prisma Access Agent on a supported Linux distribution.

Install the Prisma Access Agent on Linux

Complete the following steps to manually install the Prisma Access Agent on your Linux device.

Before you begin, complete the relevant preinstall tasks for Prisma Access Agents on Linux.

STEP 1 | (All supported Linux distributions except NixOS) Download and install the Prisma Access Agent:

1. Download the Prisma Access Agent package from your designated download location (provided by your administrator). The package name is in the following format:

   `PrismaAccessAgent_<architecture>_<version>.AppImage`

   Where:

   - **<architecture>** identifies the platform architecture (**x86_64** or **arm64**)
   - **<version>** identifies the current version number of the Prisma Access Agent AppImage
2. Set the appropriate execute permissions to the Prisma Access Agent package. For example, for Prisma Access Agent version 25.7.0.10 on x86_64, enter the following command:

   ```
   sudo chmod 755 ./PrismaAccessAgent_x86_64_25.7.0.10.AppImage
   ```
3. When running any AppImage, it mounts itself to a temporary directory under `/tmp/<directory_name>`. Therefore, ensure that:

   - The `/tmp` directory has executable permissions for both user and root accounts
   - Users have read and executable permissions for all files within the `/opt/paloaltonetworks/prismaaccessagent` directory tree
4. Install the Prisma Access Agent from the command line.

   ```
   sudo -E ./PrismaAccessAgent_<architecture>_<version>.AppImage
    -i
   ```

   The following sample image shows the terminal output showing the successful completion of the agent installation on Ubuntu:

(Prisma Access Agent 26.2) During installation, the agent detects your desktop environment and installs only the system tray dependencies your environment requires:

- ***Gnome** — The installer checks for the `gnome-shell-extension-appindicator` extension and installs it if it is not already present.*
- ***KDE** — The agent uses the native `KStatusNotifierItem` protocol to render the system tray icon. No additional packages are installed.*
- ***Other desktop environments** — The installer proceeds without installing any UI dependencies and displays the following warning:*

```
[WARNING] Unsupported Desktop Environment Detected:
 <desktop_environment_name>
The Prisma Access Agent is optimized for Gnome and
 KDE.
On your current environment, the system tray icon
 and UI pop-ups may not render correctly.
The background agent services will still function
 as expected.
Do you wish to proceed with the installation? [y/
N]:
```

STEP 2 | (NixOS) (Prisma Access Agent 26.2) Download and install the Prisma Access Agent package for NixOS. In addition to the Prisma Access Agent AppImage, NixOS requires a separate installer archive (`.tar.gz`), which contains the NixOS-specific configuration and installer script.

Prisma Access Agent integrates with NixOS by defining the AppImage as a custom app package. This process uses the `paa_nixos_configuration.nix` file and `paa_nixos_installer.sh` script for system management. The `paa_nixos_configuration.nix` file declares how NixOS imports the AppImage into

its store, defines the `PASrv` executable as a `Systemd` service, and integrates the `PAGui` UI application.

1. Download the Prisma Access Agent AppImage and NixOS installer archive to the same folder on your computer:
   - `PrismaAccessAgent_<architecture>_<version>.AppImage`
   - `paa_nixos_installer_<version>.tar.gz`
2. Go to the folder containing the installer archive and AppImage and extract the installer archive:

   ```
   tar -zxvf paa_nixos_installer_<version>.tar.gz
   ```

   After extraction, your folder should contain the following files:
   - `PrismaAccessAgent_<architecture>_<version>.AppImage`
   - `paa_nixos_installer.sh`
   - `paa_nixos_configuration.nix`
3. Install the Prisma Access Agent using the dedicated NixOS installer script, which integrates the agent declaratively into your system, treating it as a custom package.
   1. Run the NixOS installer script with the install option as a user.

      ```
      ./paa_nixos_installer.sh --install
      ```

      The script displays installation messages, including steps such as "creating config directories," "copying app image," and "adding PA configuration to the NixOS configuration."

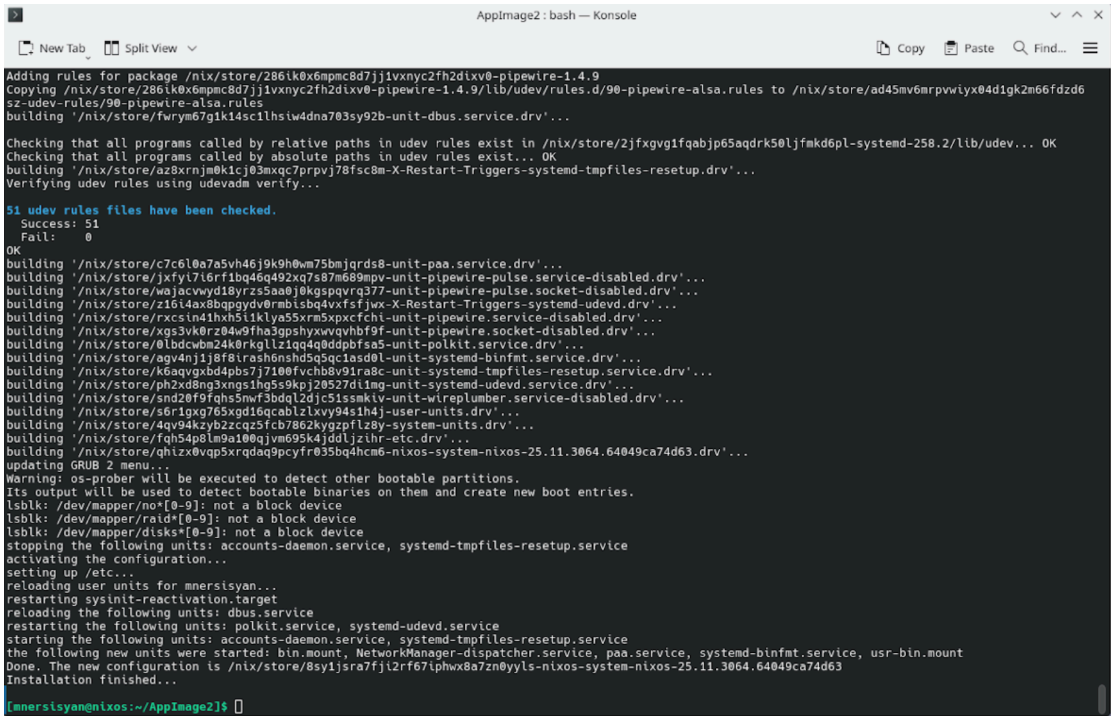
      The installer script will show the following message and prompt the user to enter their `sudo` user password:

      ```
      PrismaAccessAgent for NixOS
      ```



```
[sudo] password for <username>
```

The following sample image shows the terminal output showing the successful completion of the NixOS installer script:



2. Log out and log back into your desktop session. After login, the Prisma Access Agent system tray icon will be visible on your desktop.

STEP 3 | (Ubuntu 22 on ARM64) For Prisma Access Agent to function properly on a VM, complete the following steps:

1. Edit the `50-cloud.init.yaml` file:

   ```
   sudo nano /etc/netplan/50-cloud-init.yaml
   ```

2. In the YAML file, insert the `renderer: NetworkManager` statement in the `network` field and save your changes. For example:

   ```
   network:
        ethernets:
             ens160:
                  dhcp4: true
        version: 2
   ```



```
      renderer: NetworkManager
```

3. To have the YAML changes persist across an instance reboot, create the `/etc/cloud/cloud.cfg.d/99-disable-network-config.cfg` file with the following content:

```
network: {config: disabled}
```

4. Apply the change:

```
sudo netplan apply
```

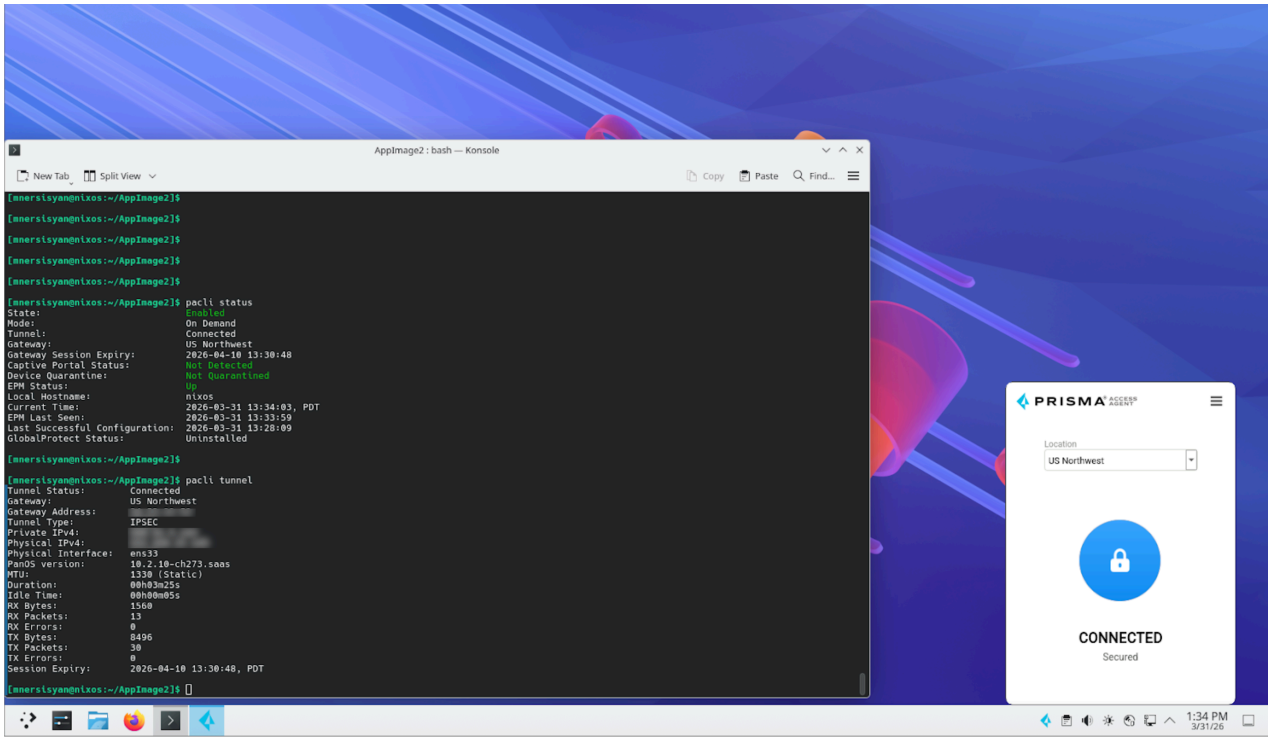
5. Restart the network manager service:

```
sudo systemctl restart NetworkManager.service
```

STEP 4 | (Ubuntu 22.04) Perform a system reboot.

Verify the Prisma Access Agent Installation and Connectivity

After installation, confirm that the agent is running, connected, and enforcing security policies as expected.



STEP 1 | Check the Prisma Access Agent user interface (UI).

1. After logging in to your desktop session, the Prisma Access Agent UI should automatically launch.
2. Log in to Prisma Access using your credentials within the UI.
3. Confirm that the agent displays a **Connected** status.

STEP 2 | Use the command-line interface (`pacli`) to check the agent status.

1. Run the following command to show the status of the agent:

   ```
   pacli status
   ```

2. Run the following command to show the status of the tunnel:

   ```
   pacli tunnel
   ```

3. Run the following command to view traffic logs and policy enforcement.

   ```
   pacli traffic show
   ```

4. Check the Host Information Profile (HIP) status.

   ```
   pacli hip status
   ```

5. View HIP notifications.

   ```
   pacli hip notification
   ```

6. Test network connectivity and policy enforcement.

   1. Run the following command to verify direct access to a common website, such as `google.com`.

      ```
      curl google.com
      ```

   2. Ping a common website such as `google.com` to verify tunnel connectivity.

      ```
      ping google.com
      ```

   3. Attempt to access a known blocked site (for example, `amazon.com`) to confirm policy enforcement.

Upgrade the Prisma Access Agent on Linux

Upgrade the Prisma Access Agent to ensure you have the latest features and security updates.

STEP 1 | (All supported Linux distributions except NixOS) Upgrade the agent as follows:

1. Download the new Prisma Access Agent package from your designated download location. The package name is in the following format:

   `PrismaAccessAgent_<architecture>_<new-version>.AppImage`
2. Set the appropriate execute permissions to the Prisma Access Agent package. For example:

   ```
   sudo chmod 755 ./PrismaAccessAgent_<architecture>_<new-version>.AppImage
   ```
3. Run the following command to upgrade the agent:

   ```
   sudo -E ./PrismaAccessAgent_<architecture>_<new-version>.AppImage -u
   ```

STEP 2 | (NixOS) Upgrade the agent as follows:

1. Download the new Prisma Access Agent AppImage and NixOS installer archive to the same folder on your computer:
   - `PrismaAccessAgent_<architecture>_<new-version>.AppImage`
   - `paa_nixos_installer_<new-version>.tar.gz`
2. Extract the new installer archive to the same directory as the new Prisma Acess Agent AppImage.

   ```
   tar -zxvf paa_nixos_installer_<new-version>.tar.gz
   ```
3. Run the NixOS installer script with the upgrade option as a user.

   ```
   ./paa_nixos_installer.sh --upgrade
   ```

   The script performs a version check, uninstalls the old agent (without removing your user configurations), and then installs the new agent.
4. Log out and log back into your desktop session.

Uninstall the Prisma Access Agent on Linux

You can uninstall the Prisma Access Agent manually if you no longer need to use it. Keep in mind that by uninstalling the agent, you will no longer have access to your corporate network, and your endpoint won't be protected by your organization's security policies.

Complete the following steps to uninstall the agent from the Prisma Access Agent command-line interface (`pacli`).

STEP 1 | (All supported Linux distributions except NixOS) Uninstall Prisma Access Agent by completing the following steps.

1. Run the following command:

   ```
   sudo -E ./PrismaAccessAgent_<architecture>_<version>.AppImage
    -r
   ```

2. Enter your `sudo` password (user account password) when prompted.

STEP 2 | (NixOS) Complete the following steps to remove all Prisma Access Agent components and configurations from your NixOS system, reverting the changes made during installation.

1. Execute the NixOS installer script with the remove option as a user.

   ```
   ./paa_nixos_installer.sh --remove
   ```

   The script stops the Prisma Access Agent UI and service, disables and removes the `Systemd` service configuration, removes soft links, and deletes the AppImage from the installation directory.

2. Log out and log back into your desktop session.

Use Prisma Access Agent Pre-Logon

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.3 (macOS and Windows) ❑ macOS 14 and later or Windows 10 version 2024 and later desktop devices ❑ Internet access

The pre-logon feature for Prisma Access Agent offers a seamless and secure connection experience throughout your device's operation cycle. When your device starts up, the pre-logon mode automatically initializes and establishes a secure connection using your device's machine certificate. This occurs before you reach the operating system login screen, ensuring immediate network connectivity. On Windows machines, you will see a tile at the login screen displaying the pre-logon tunnel status as Internal, Connected, or Disconnected, providing clear visibility of your network status.

As you log in with your credentials, the pre-logon tunnel smoothly transitions to your full user session. The Prisma Access Agent reauthenticates, granting broader access rights based on your user profile. You don't need to manually establish a connection—it's already set up for you. During your session, you have full access to network resources as defined by your organization's policy rules, with the connection remaining active to ensure consistent and secure access.

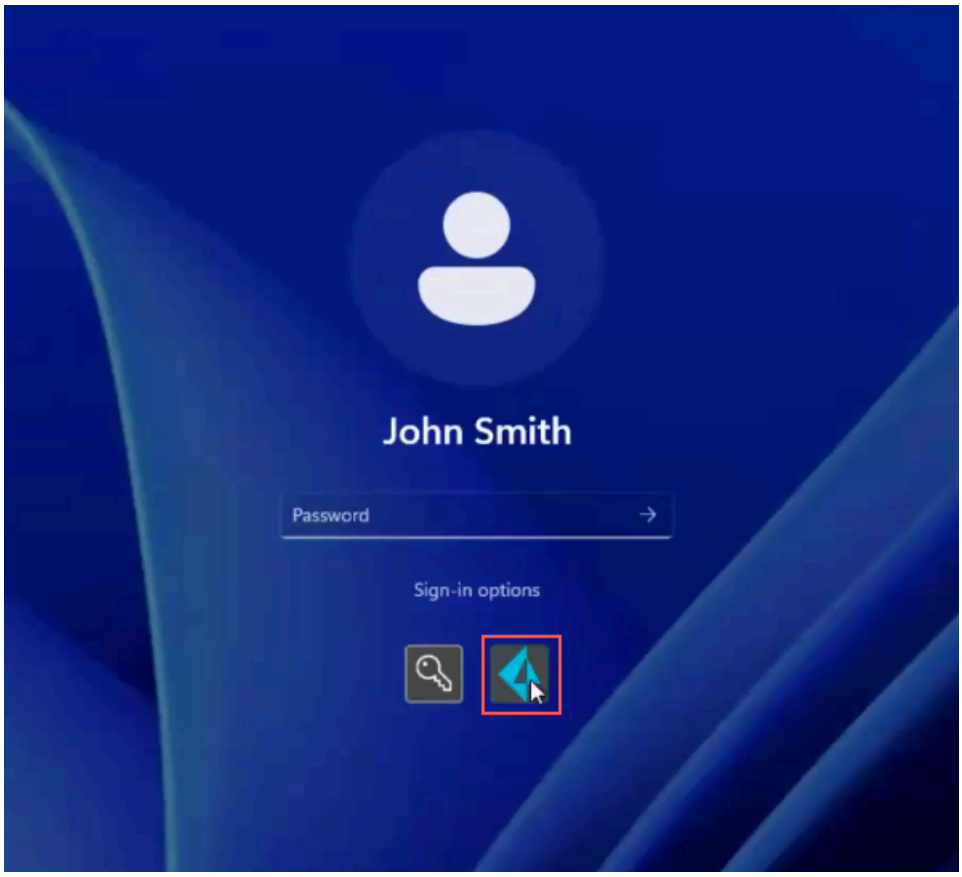
When you log out, your user-specific session ends, but the system automatically re-establishes the pre-logon connection. This ensures your device maintains essential network connectivity for system tasks even when you're not logged in. Each subsequent login follows the same pattern, providing a consistent experience of transitioning from pre-logon to full user access. This pre-logon feature enhances your productivity by ensuring immediate and secure network access, simplifying the login process, and maintaining essential connectivity at all times.

Before you can use pre-logon, your administrator must have configured pre-logon support for the Prisma Access Agent.

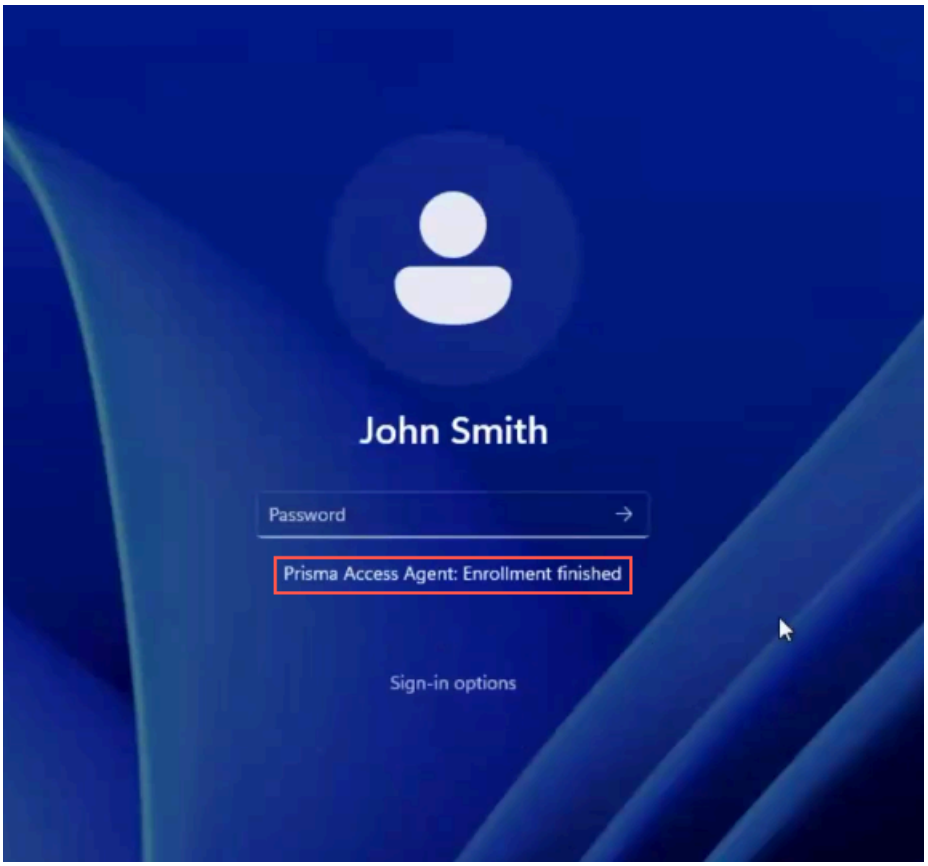
The Windows pre-logon process is different from the pre-logon for macOS. When your device starts up, the pre-logon process on Windows will show you what happens during a pre-logon connection. While on macOS, there are no visual cues related to the pre-logon connection. You just need to sign in when prompted by the operating system.

To use pre-logon on a Windows device:

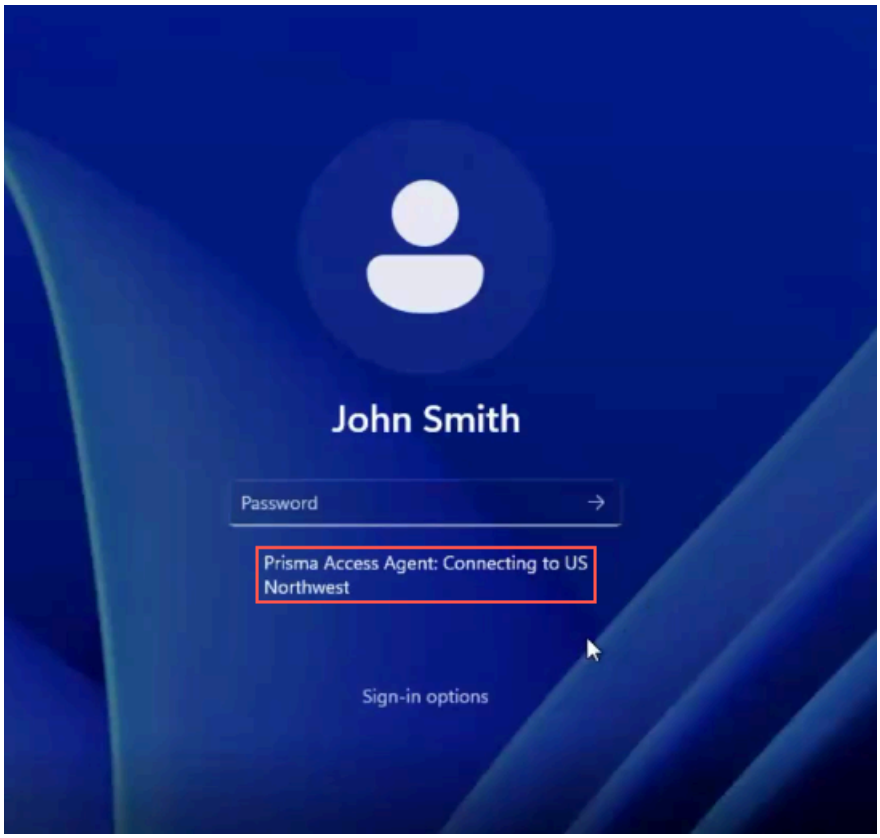
- If your device has never been enrolled, meaning that the Prisma Access Agent has never registered with the server, and never been configured on your device, do the following when your device starts up.
  1. Click the **Sign-in options** in the login screen, and click the Prisma Access Agent icon.



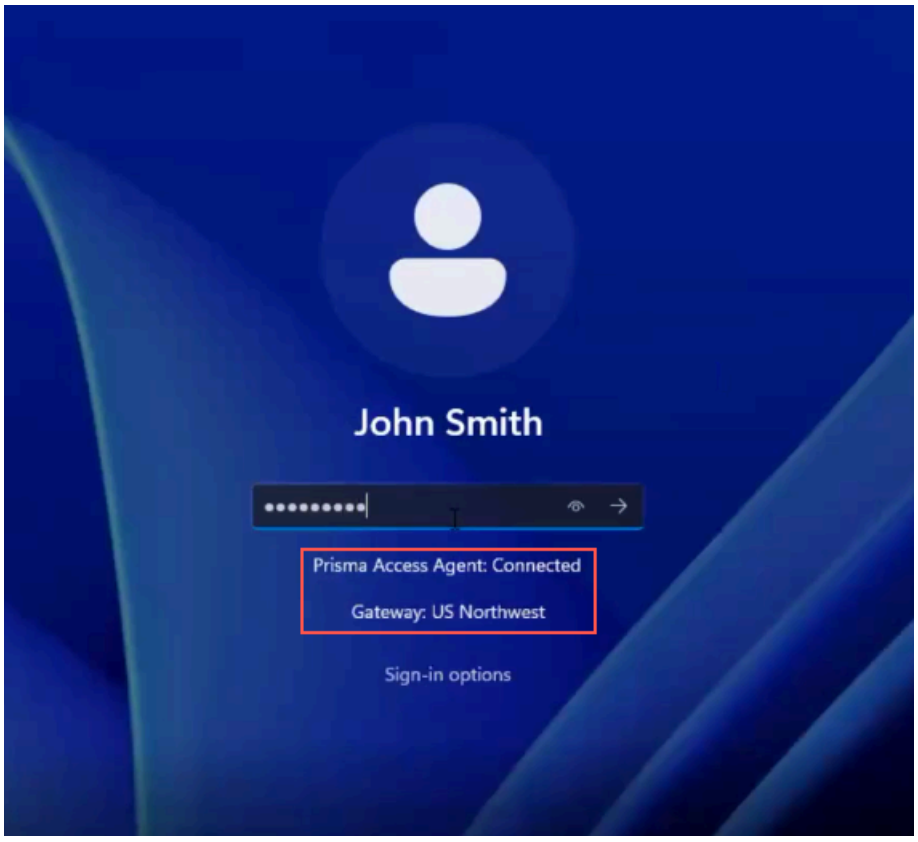
     The agent will use your device's machine certificate to authenticate with the server and establish a secure, pre-logon connection.
  2. Wait for the enrollment process to finish. This will register your device with the server and download the necessary configurations for the Prisma Access Agent to your device.



3. At this point, the Prisma Access Agent will automatically authenticate and connect to the best available gateway.

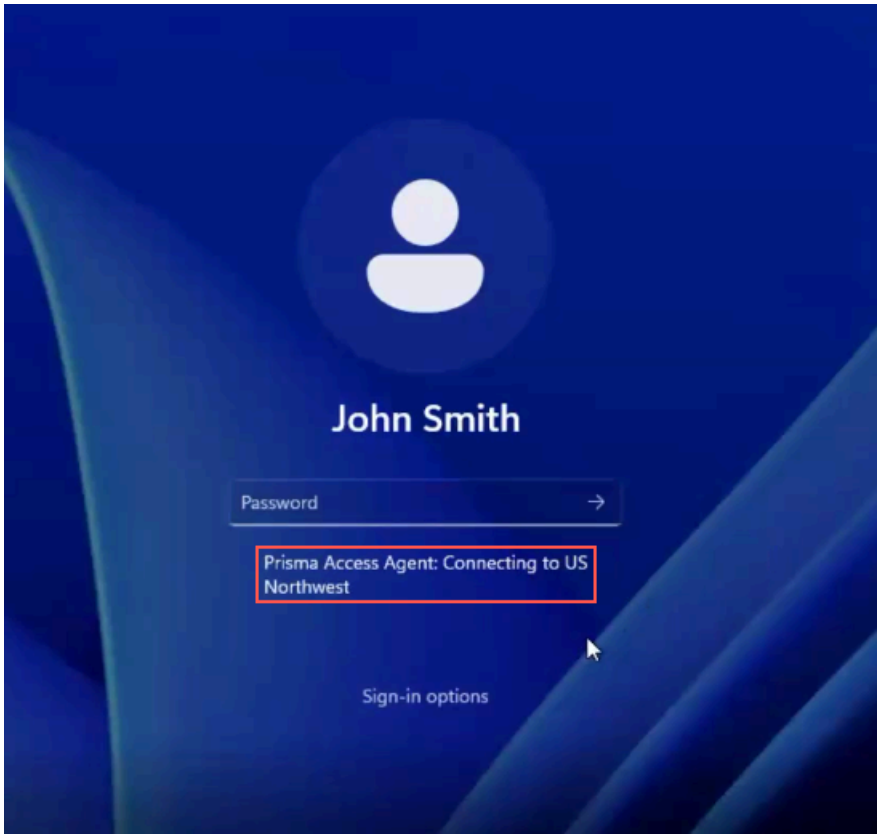


4. When the agent has connected to the gateway, enter your system password and press **Enter**.

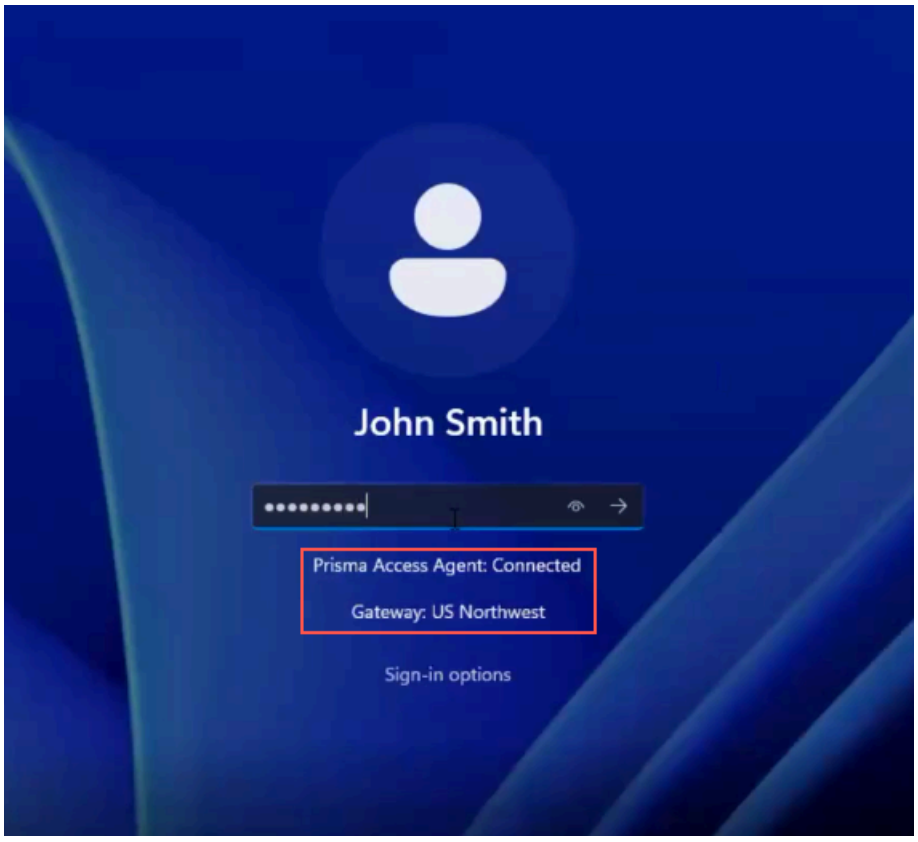


5. After you log in successfully, the pre-logon connection transitions to a full user session with potentially broader access rights, where you can access the resources in your network based on your organization's security policy rules.
6. When you log out of the operating system, your user-specific session ends, but the system automatically re-establishes the pre-logon connection.

- If your device has previously been enrolled and you're just starting it up:
  1. The Prisma Access Agent will automatically authenticate and connect to the best available gateway as shown in the following image:



  2. When the agent has connected to the gateway, enter your system password and press **Enter**.



3. After you log in successfully, the pre-logon connection transitions to a full user session with potentially broader access rights, where you can access the resources in your network based on your organization's security policy rules.
4. When you log out of the operating system, your user-specific session ends, but the system automatically re-establishes the pre-logon connection.

Use Single Sign-On with Prisma Access Agent

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: 26.1 ❑ macOS 14 and later or Windows 10 version 2024 and later desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

When your organization has configured single sign-on (SSO) for Prisma Access Agent, you can connect to the secure network automatically using your existing device credentials without entering separate login information. This seamless authentication leverages your operating system's built-in security features to provide convenient access while maintaining enterprise security policies.

After your administrator configures single sign-on integration on your device, Prisma Access Agent uses your device login credentials to automatically authenticate and connect to your organization's secure network. The agent operates silently once you complete your device login, maintaining your secure connection throughout your work session without requiring additional authentication steps from you.

Prisma Access Agent offers single sign-on capabilities for macOS and Windows devices by leveraging macOS Platform SSO and Windows Hello for Business, respectively.

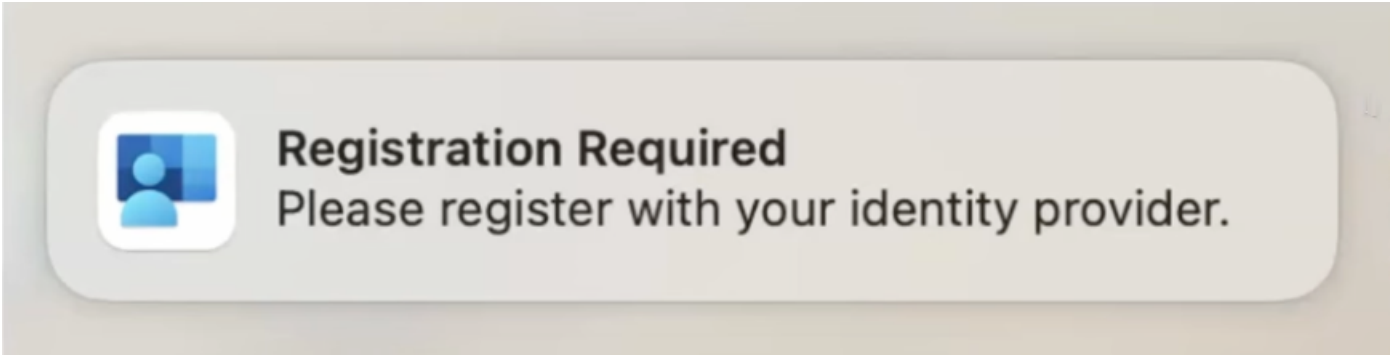
- macOS
- Windows

Use Single Sign-On with macOS Platform SSO

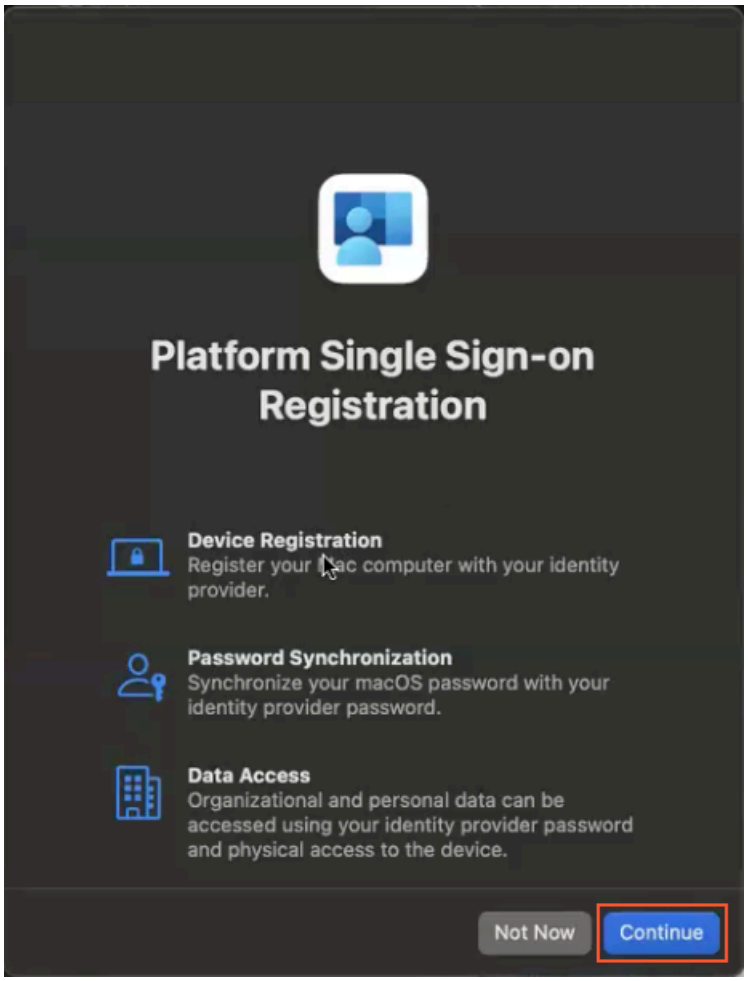
When Platform SSO is configured on your Mac, log into your device using your organization-provided credentials including your password, Touch ID, Face ID, or smart card with PIN. Prisma Access Agent automatically detects your login and begins the authentication process using your existing credentials without displaying browser windows or additional login prompts.

STEP 1 | Log into your Mac using your organization-provided credentials. This may include your password, Touch ID, Face ID, or smart card with PIN, depending on how your IT administrator has configured your device.

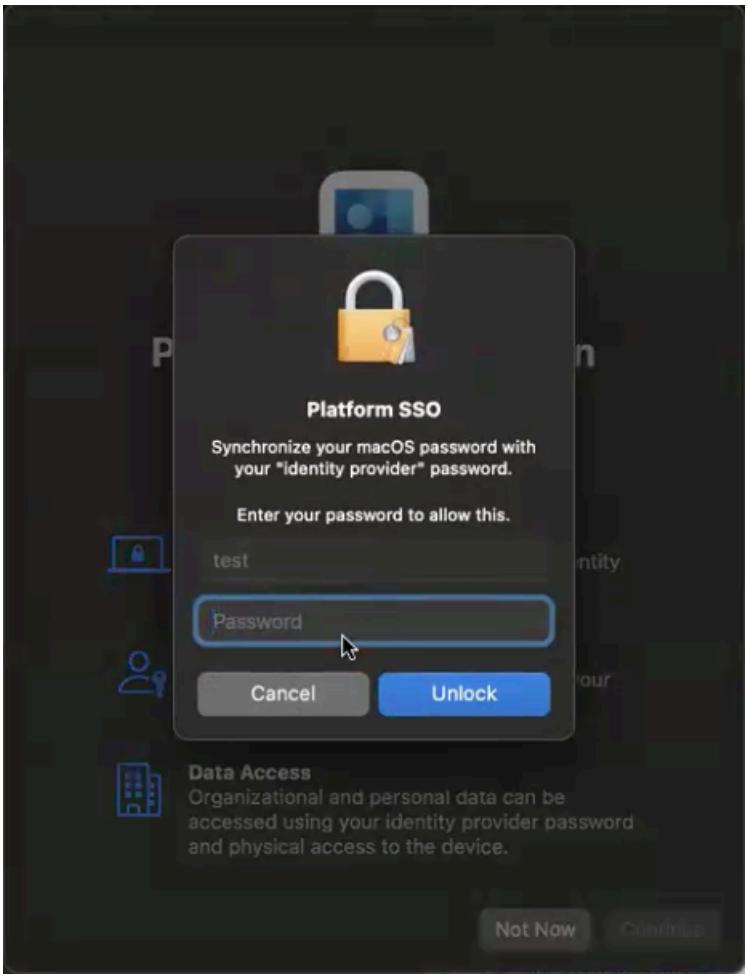
STEP 2 | When your administrator has pushed the Platform SSO profile to you macOS device, you will be notified to register with your identity provide (IdP). Click the notification to proceed.



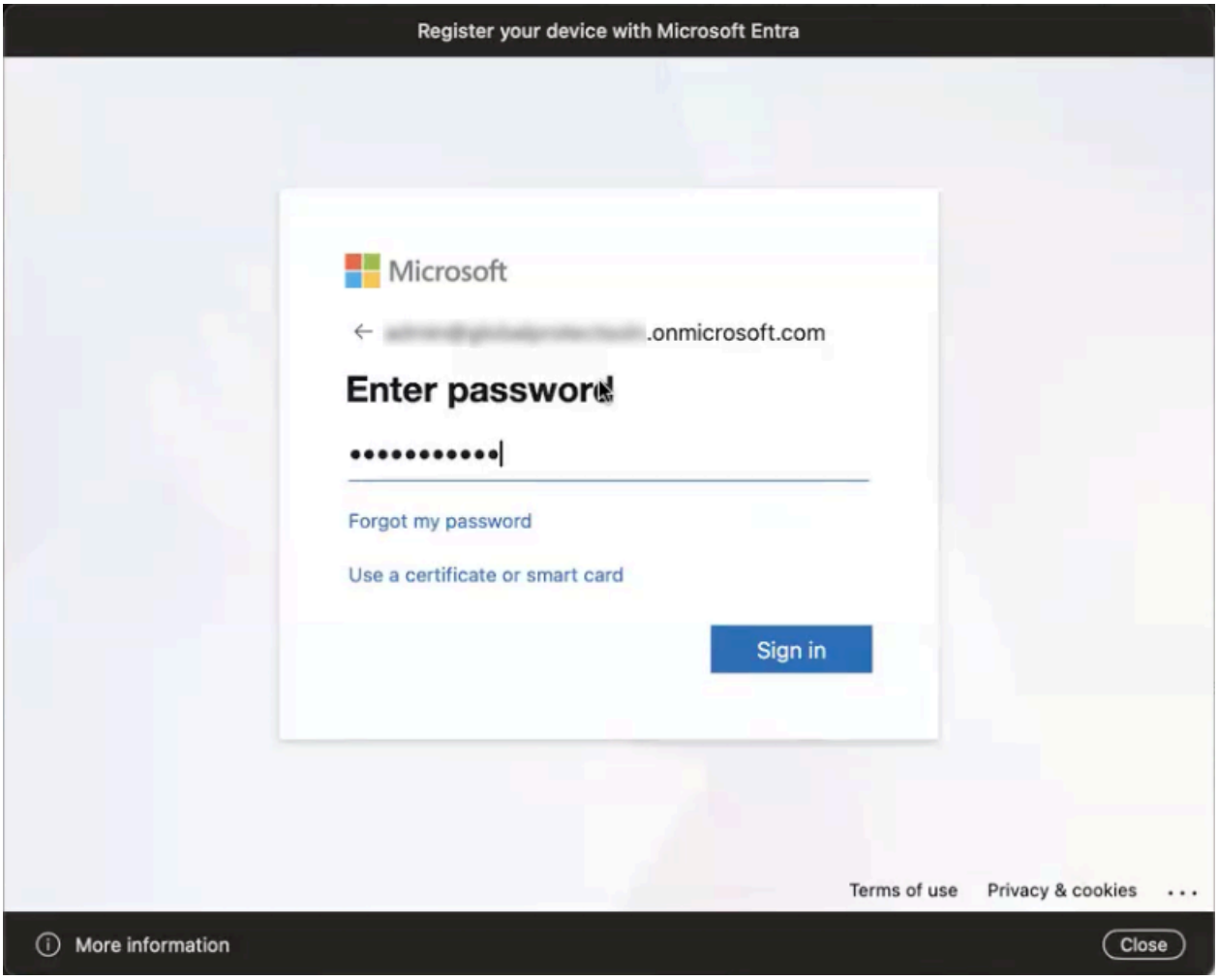
STEP 3 | **Continue** in the Platform Single Sign-on Registration window.



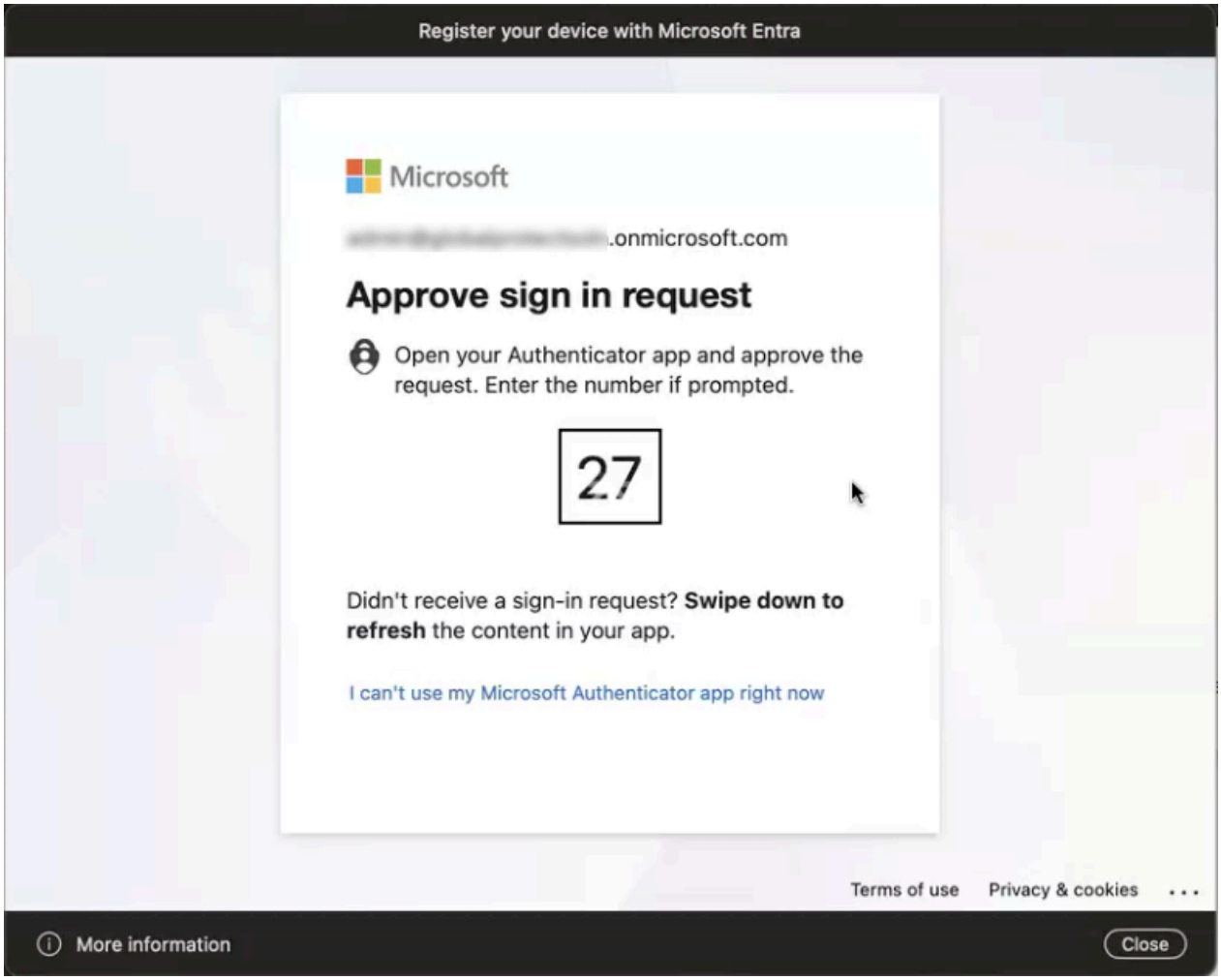
STEP 4 | Enter your credentials to authenticate with your IdP.



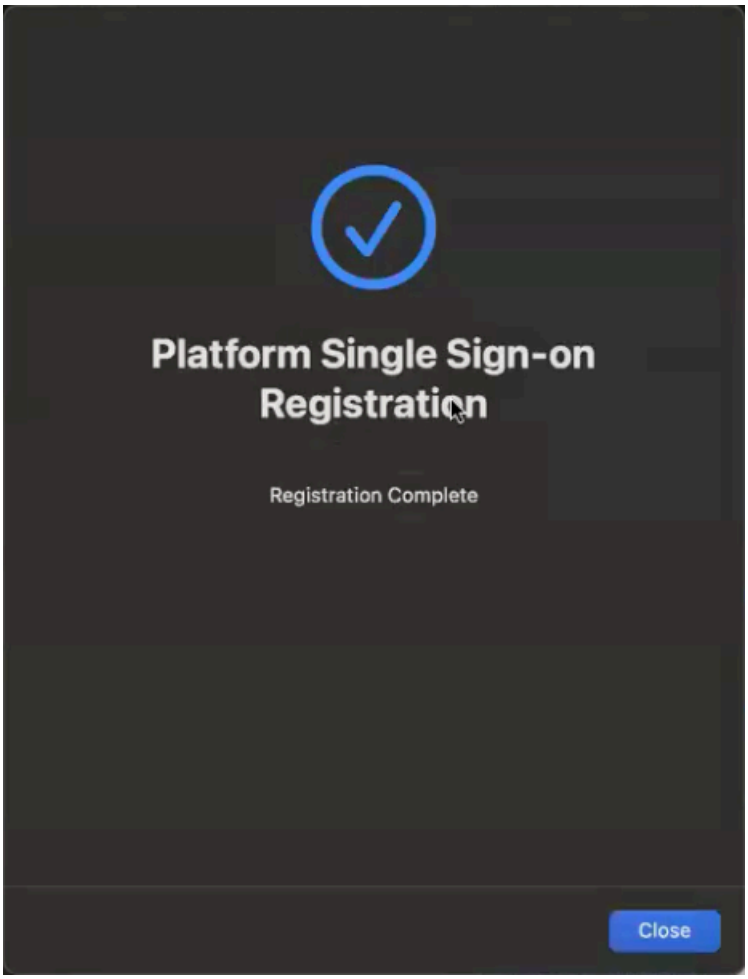
STEP 5 | In the IdP login window, such as Microsoft Entra, enter the same credentials that you entered in the Platform SSO window and **Sign in**.



STEP 6 | If prompted, follow the instructions to approve the sign in request using your Authenticator app.



STEP 7 | When your registration is complete, **Close** the window.

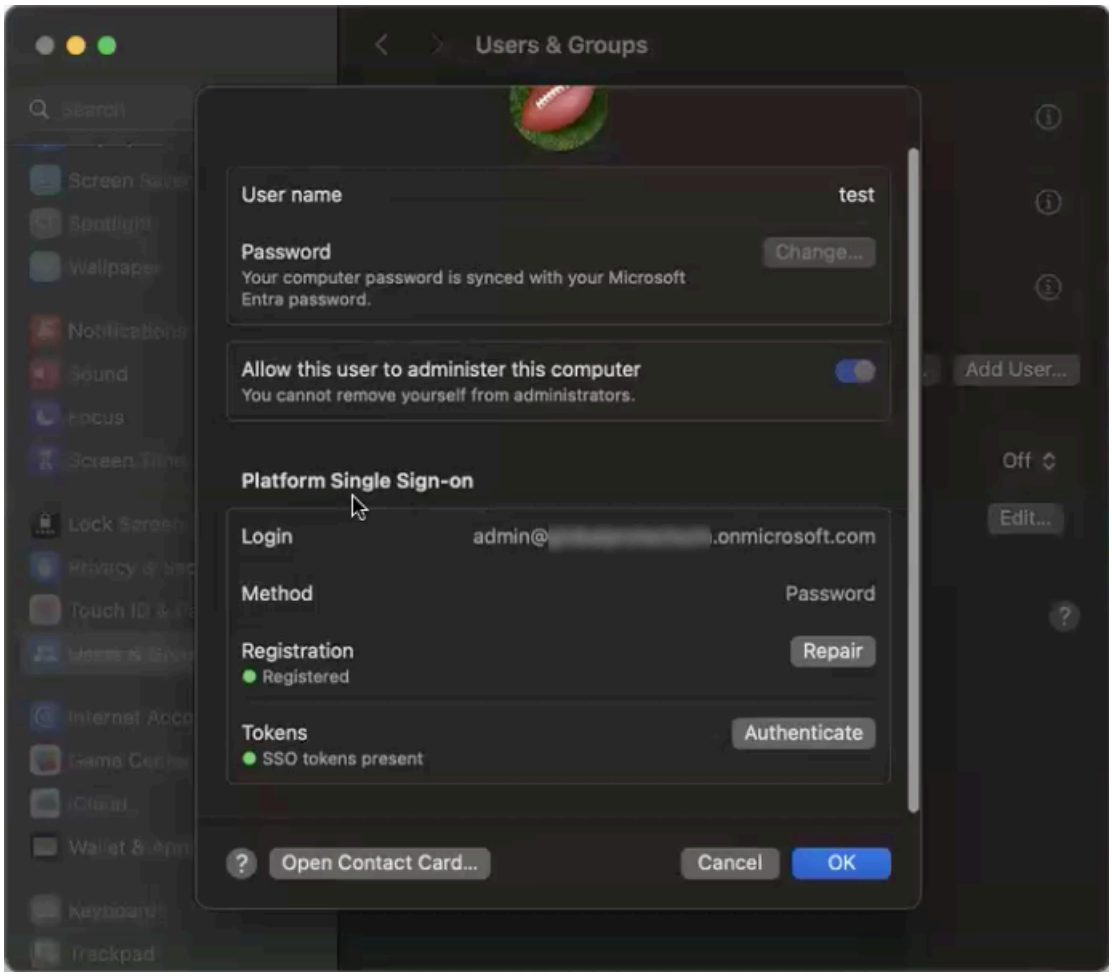


Once authentication completes successfully, you can access your organization's applications and resources through the secure network connection. The agent maintains this connection as long as you remain logged into your device.

If you experience authentication issues, ensure that you have logged into your Mac using your organization-provided credentials and verify your network connection can communicate with your organization's authentication services. If authentication fails, the agent will prompt you to enter credentials manually as a fallback option.

STEP 8 | (Optional) Verify that SSO is enabled on your device.

1. Go to **System Settings** > **Users & Groups**.
2. Select the information icon for you user name and verify that there is a Platform Single Sign-on section showing the same IdP login information, login method, and status of the registration.



STEP 9 | You can now use the Prisma Access Agent.

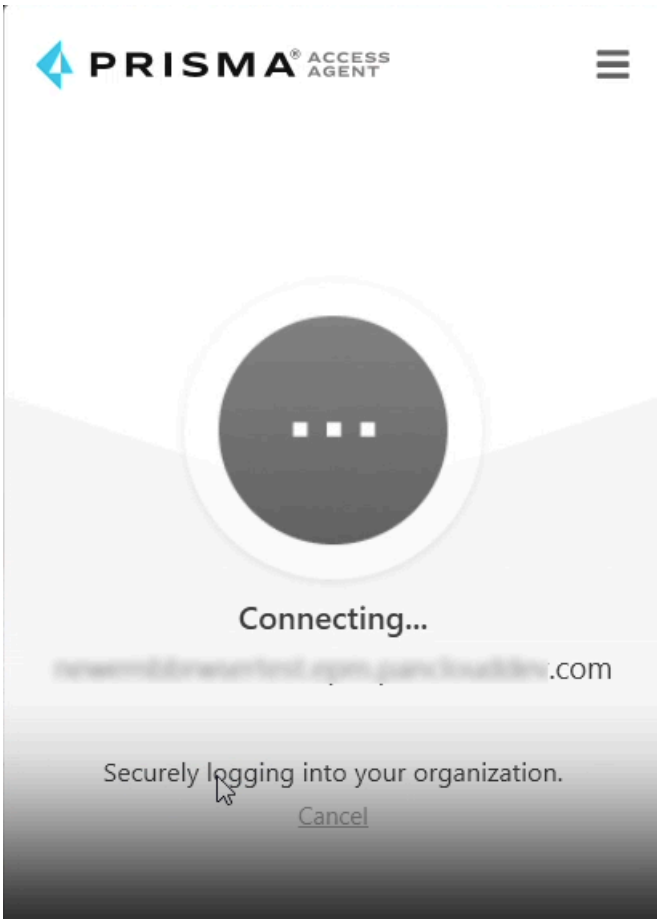
Use Single Sign-On with Windows Hello for Business

When Windows Hello for Business integration is configured on your Windows device, you can log in to your device using your Windows Hello credentials, and Prisma Access Agent will begin the authentication process using your credentials without displaying additional login prompts.

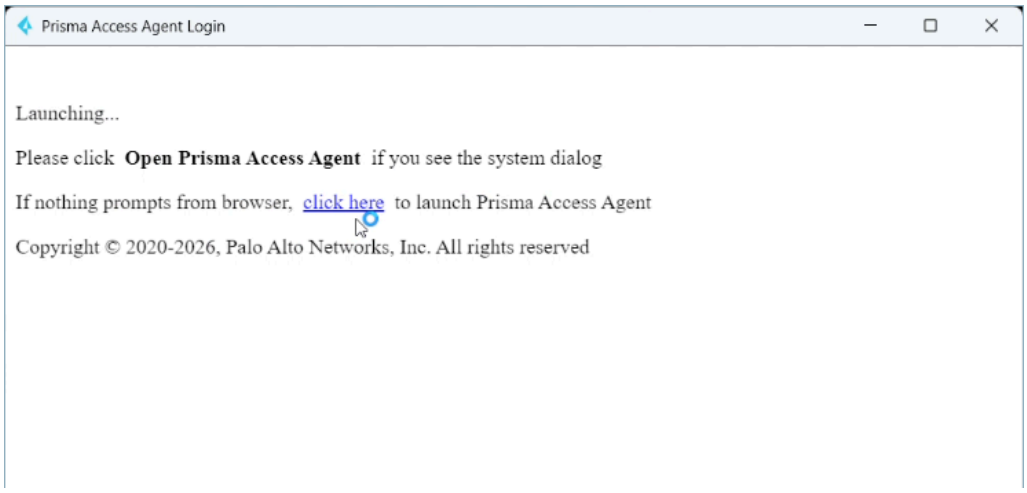
Before you begin, make sure that your Windows PC has joined Microsoft Entra ID.

STEP 1 | Log in to your device using facial recognition, fingerprint scanning, PIN, or smart card credentials.

Prisma Access Agent automatically detects your login and begins the authentication process using your existing Windows Hello session.



- *Depending on your agent configuration, the Prisma Access Agent internal embedded browser or your default system browser will appear. The following image is an example of the embedded browser:*



- *If your administrator configured the agent to use the embedded browser and chose to suppress it, the embedded browser will not appear.*

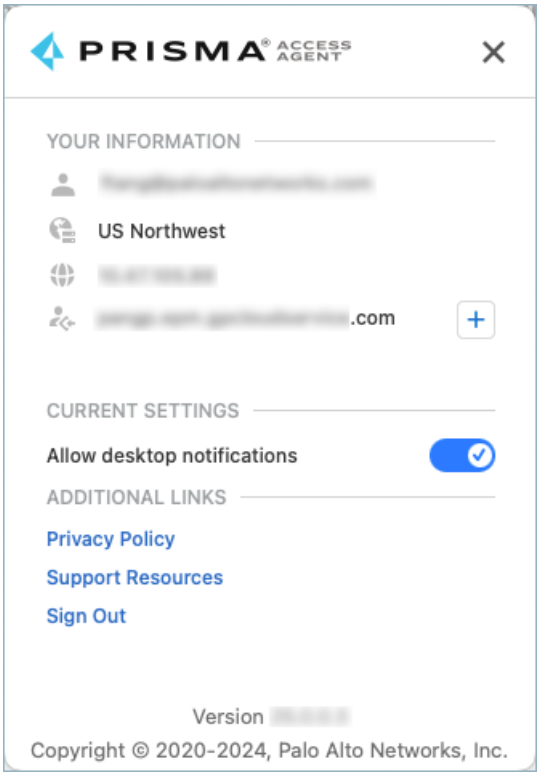
STEP 2 | Once authentication completes successfully, you can access your organization's applications and resources through the secure network connection. The agent maintains this connection as long as you remain logged into your device.

If you experience authentication issues, verify that your Windows Hello for Business setup is functioning properly and that your device can communicate with your organization's authentication services. If authentication fails, the agent will prompt you to enter credentials manually as a fallback option.

STEP 3 | Verify that SSO is working.

You can go to the settings in the Prisma Access Agent app to view the user login information. Confirm that the user name is the same as what you used to log in to your PC.

For example:



Log in to the Prisma Access Agent

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

To access your organization's network, resources, SaaS applications, or the internet, log in to the Prisma Access Agent using your login credentials.

After you log in to the Prisma Access Agent, you're automatically connected to your network using the best location (sometimes called a gateway). The agent automatically selects the best location to provide you with the best performance to provide a better experience, such as viewing websites in your local language. When your device is outside your organization's network, the agent finds the best location to give you the best performance when connecting to the network.

Before you begin, the Prisma Access Agent must be installed on your device. Typically, your administrator will deploy the Prisma Access Agent to the device that you use to access your organization's network, resources, and applications. Your administrator configures the agent according to your organization's policy rules and deploys it to your device. However, if your administrator did not deploy the Prisma Access Agent to your device, you will need to manually install the Prisma Access Agent.

Depending on how Prisma Access is set up in your organization, your administrator should provide you with the name of the server that manages your Prisma Access Agent.

If your administrator configured the macOS or Windows Prisma Access Agent to use single sign-on (SSO), refer to Use Single Sign-On with Prisma Access Agent.

The app icons and app interface can appear in dark mode or light mode depending on your operating system settings.

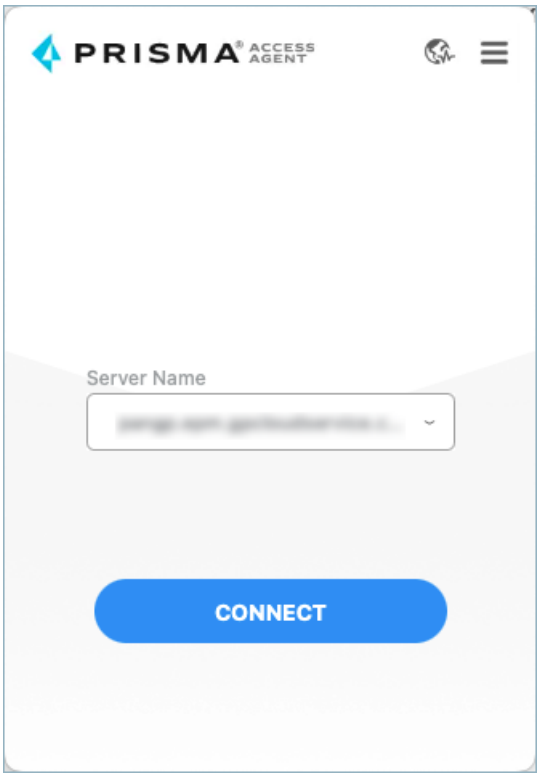
Log in to the Prisma Access Agent by completing the following steps:

STEP 1 | If your administrator configured the Prisma Access Agent in Always On mode, the Prisma Access Agent starts automatically after the installation and whenever you log in to your device.

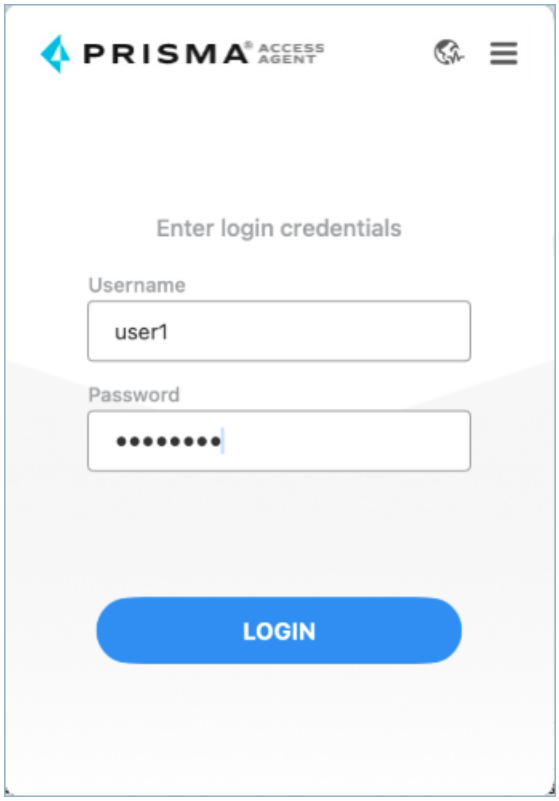
If your administrator configured the Prisma Access Agent in On-Demand mode, you need to start the Prisma Access Agent by clicking the Prisma Access Agent icon from the macOS menu bar, Windows taskbar, or Linux panel.

STEP 2 | Select the **Server Name** of the Prisma Access server that your administrator provided and click **Connect**.

The format of the server name is **`<xxx>.epm.gpcloudservice.com`** (without the **`https://`** protocol). The maximum length of the server name is 256 characters.



STEP 3 | (Not supported on Prisma Access Agent Linux) (Prisma Access Agent 25.3.0.43) If your organization uses LDAP authentication, enter your login credentials for your organization:



1. In the **Login** field, enter the username or email address you use for LDAP authentication.
2. Type the **Password** and press **Enter**.

   On the macOS agent, click **Login** after entering the password to begin the authentication.

   On the Windows agent, after typing in the password and pressing **Enter**, the authentication begins.

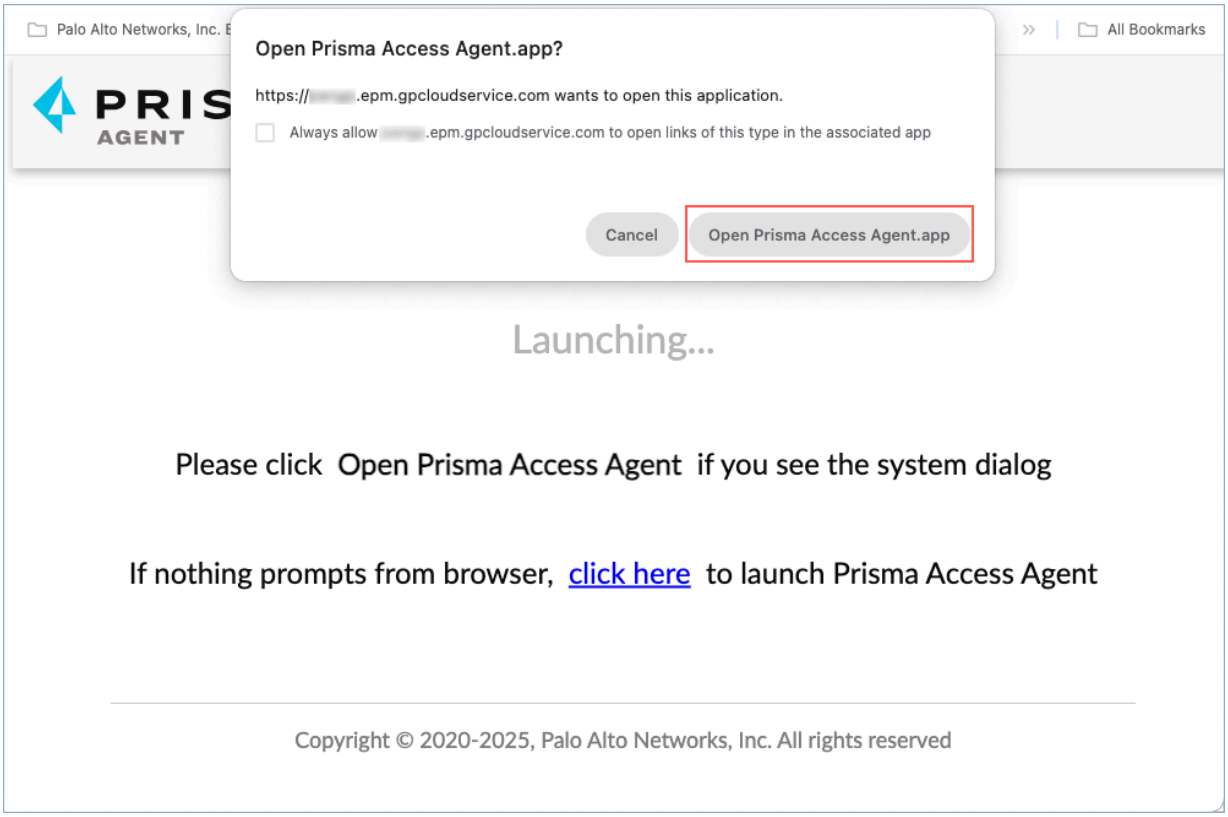
STEP 4 | In the login page that appears in your default web browser, sign in to your organization's single sign-on (SSO) app, such as Okta or Azure Active Directory (AD), by entering your login credentials for your organization.

(Prisma Access Agent 25.3.0.43) Depending on your agent's configuration, the login page can appear in your default system web browser (such as Chrome or Firefox) or in the Prisma Access Agent internal browser. (The internal embedded browser is not supported on Prisma Access Agent Linux.)

If your administrator enabled multi-factor authentication (MFA), you'll need to complete additional verification in the browser when you log in.

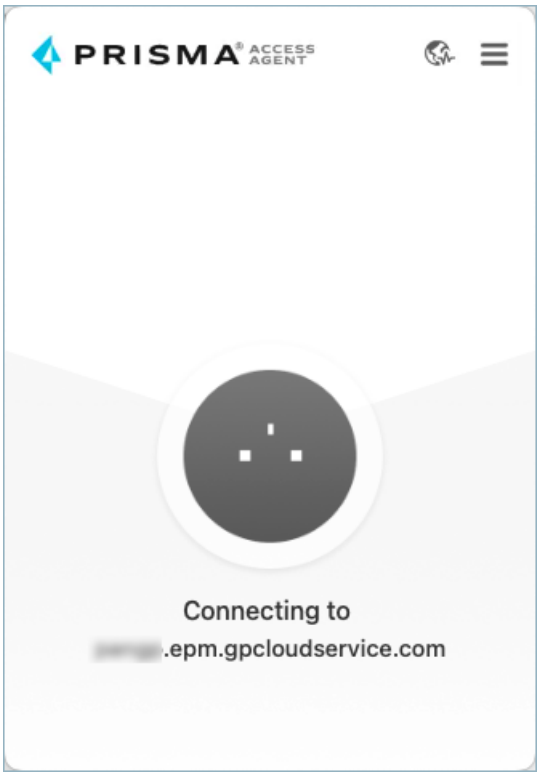
STEP 5 | When the browser prompts you, click **Open Prisma Access Agent**. (Prisma Access Agent 25.3.0.43) If the Prisma Access Agent is using the default system web browser, click **Open Prisma Access Agent** when prompted.

(Optional) If you don't want the browser to prompt you the next time you log in, select **Always allow <site> to open these types of links in the associated app**, then click **Open Prisma Access Agent** (if supported by your default web browser).

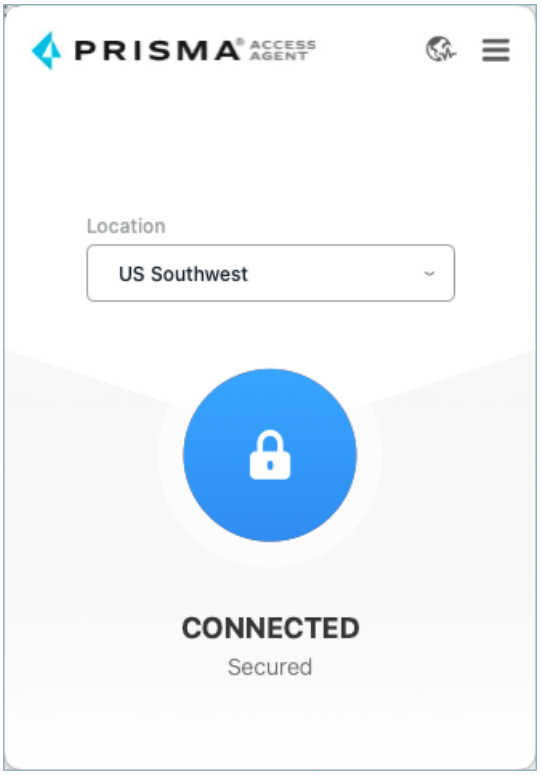


STEP 6 | (Not supported on Prisma Access Agent Linux) (Prisma Access Agent 25.3.0.43) If you're connecting from networks with captive portals, such as hotels, cafes, and airports, the captive portal login page will appear in the browser. Enter your credentials or accept the terms of service as required by the network provider.

STEP 7 | Wait while Prisma Access Agent connects to Prisma Access.



STEP 8 | After successfully logging in, you're connected automatically to the best available location.



You can now access your organization's resources and SaaS apps, along with secure access to the internet.

*If your administrator enabled **Always On** mode for the Prisma Access Agent, you can't disconnect from Prisma Access due to your organization's policy. However, you can still change locations.*

*If your administrator enabled **On Demand** mode for the Prisma Access Agent, you must click the lock icon to connect to Prisma Access.*

If you're using the Prisma Browser to securely access your organization's network and resources and to browse the internet, the Prisma Browser might prompt you to open the Prisma Access Agent again. This can happen if you leave the Prisma Access Agent authentication tab open in the Prisma Browser and then restart the browser and restore all open tabs. This action refreshes the Open Prisma Access Agent browser tab even though your login credentials are still valid and active. Clicking **Open** won't affect the state of the agent and you won't have to authenticate to the agent again.

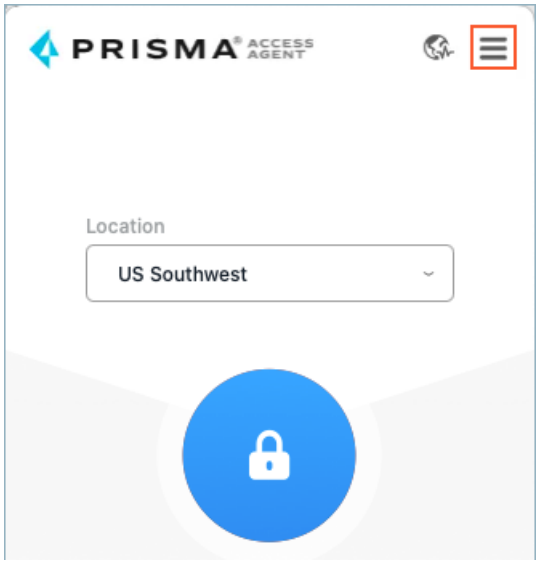
Change Prisma Access Agent App Settings

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

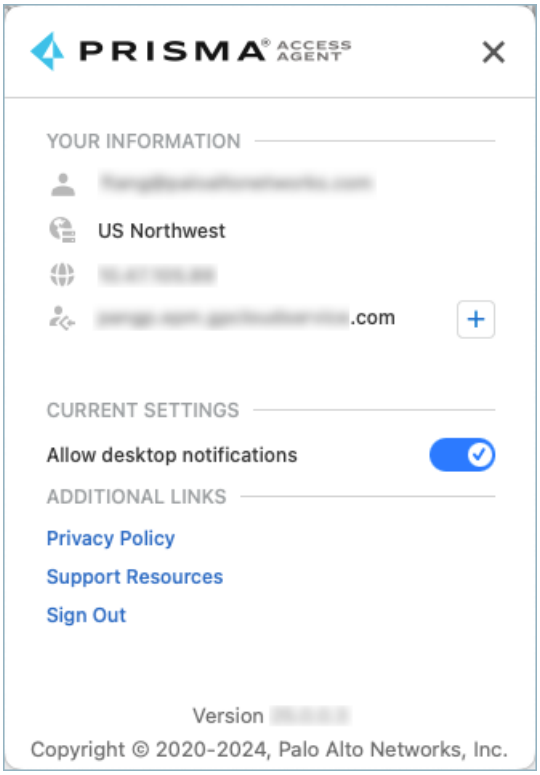
Use the Prisma Access Agent settings window to view information about your device and to change options for your agent, such as enabling desktop notifications.

STEP 1 | Open the Prisma Access Agent by clicking the icon from the macOS menu bar, Windows taskbar, or Linux panel.

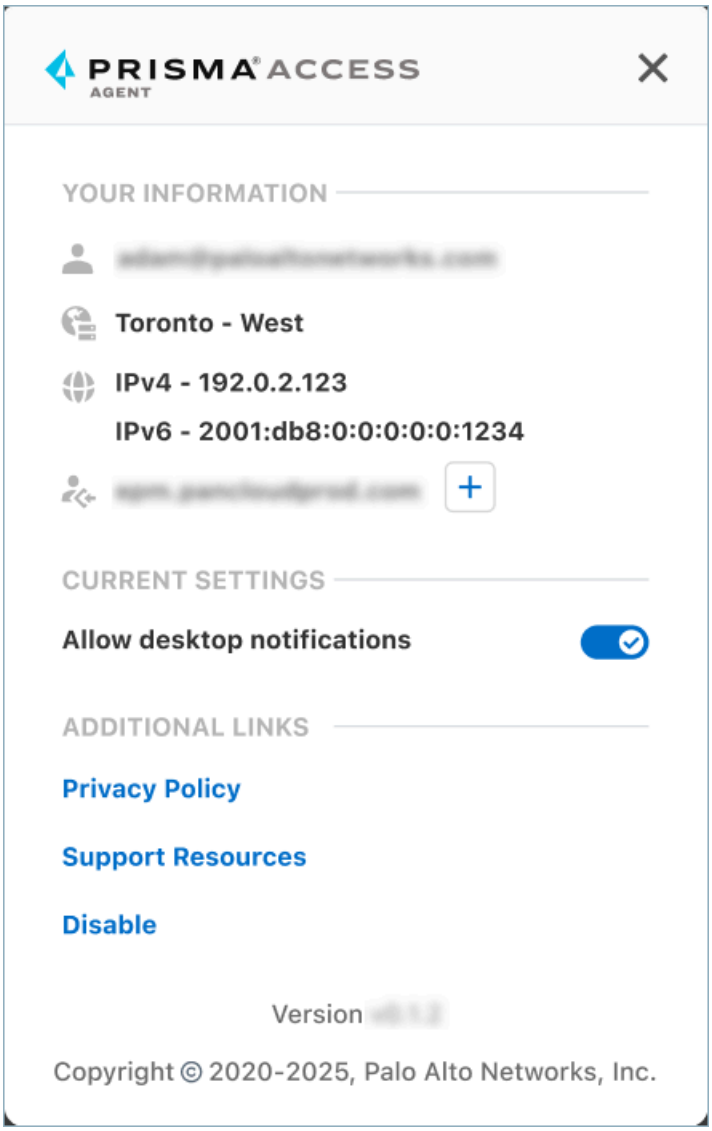
STEP 2 | Click the options icon to open the settings window.



STEP 3 | In the settings window, you can view the following information:



(macOS and Windows agents only) If your administrator has configured IPv6 dual-stack support and if your device is IPv6-enabled, you will see both IPv4 and IPv6 addresses:



Icon	Description
	Your user ID
	The location that your device is connected to
	The IP address assigned to your device *(macOS and Windows agents only) If your administrator has configured IPv6 dual-stack support and if your device is IPv6-enabled, you will see both IPv4 and IPv6 addresses.*
	The hostname or IP address for the server that you're connected to

STEP 4 | (Not supported on Prisma Access Agent Linux) To receive Prisma Access Agent notifications in the menu bar (on macOS) or taskbar (on Windows), **Allow desktop notifications**. This setting is enabled by default.

STEP 5 | To understand what data the Prisma Access Agent collects and how the information is used, view the **Privacy Policy**.

STEP 6 | To get assistance on the Prisma Access Agent, click **Support Resources**.

STEP 7 | If configured, you can **Disable** the Prisma Access Agent.

STEP 8 | If your administrator permits it, **Sign Out** of the Prisma Access Agent.

STEP 9 | View the version of your Prisma Access Agent.

STEP 10 | To close the window, click the **X**.

Connect the Prisma Access Agent to a Different Location

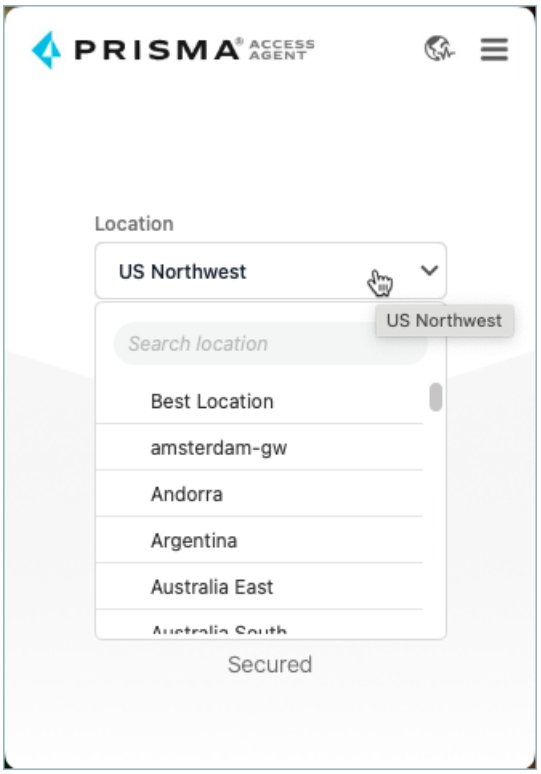
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	☐ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ☐ macOS, Windows, or Linux desktop devices ☐ Check the prerequisites for the supported OS versions ☐ Internet access

After you log in to the Prisma Access Agent, you're automatically connected to the best available Prisma Access location. If you want to change locations, you can do so using the **Location** drop-down. If your device is located inside your organization's network, the agent is connected automatically to an internal location (if your administrator enabled Internal Host Detection). If no internal location is available, the agent will use an external location.

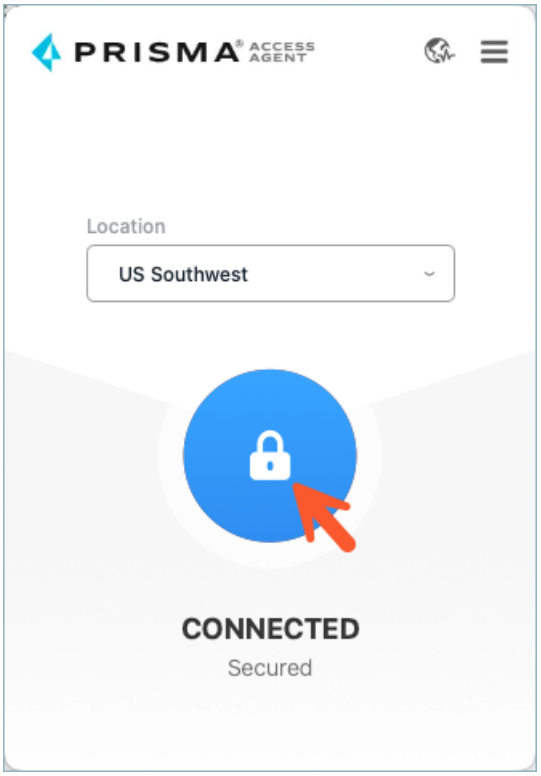
STEP 1 | Launch the Prisma Access Agent by clicking the Prisma Access Agent icon from the macOS menu bar, Windows taskbar, or Linux panel.

STEP 2 | Select a different **Location**. You can **Search** for a location or choose a location from the list.

The list of available locations are sorted according to the best experience based on response time, availability, and other factors. The location that offers the best experience is listed as **Best Location**.



STEP 3 | If your administrator enabled **On Demand** mode for the Prisma Access Agent, click the lock icon to connect to the newly selected location. Otherwise, the Prisma Access Agent proceeds to change locations.



Connect the Prisma Access Agent to a Different Server

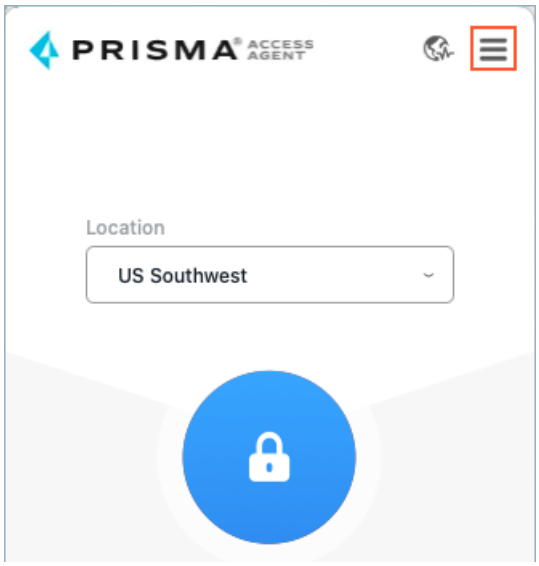
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	☐ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) ☐ macOS 14 and later or Windows 10 version 2024 and later desktop devices ☐ Internet access

An instance of the Prisma Access server is also known as a *tenant*. If your administrators set up multiple Prisma Access servers, you can connect to a different server to access the network or the resources through that server.

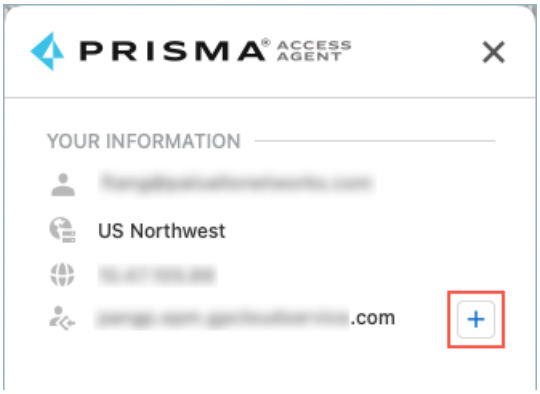
On Prisma Access Agent for Linux, you can connect to a different server only from the login window.

STEP 1 | Open the Prisma Access Agent app by clicking the Prisma Access Agent icon from the macOS menu bar or Windows taskbar.

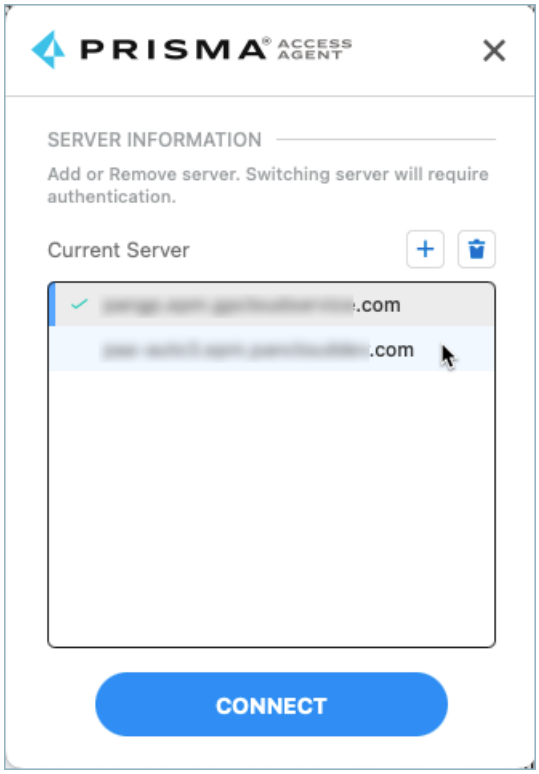
STEP 2 | Click the options icon to open the settings window.



STEP 3 | Click the **+** sign next to the name of the server.



STEP 4 | The server information appears showing the server that you're connected to. If other servers are listed, you can select one and **Connect** to it.



STEP 5 | If you need to add a server, complete the following steps:

1. Click the **+** sign.
2. Enter the new server name (provided by your administrator) and **Add** it.

   The format of the server name is `<xxx>.epm.gpcloudservice.com` without the **`https://`**. The maximum length of the server name is 256 characters. The maximum number of servers allowed on this page is 20.

3. After adding the server, select it and click **Connect**.

STEP 6 | When the Confirmation window appears, click **Yes** to disconnect from the current server and connect to the other server. You will need to provide your sign-on credentials again.

STEP 7 | When prompted, log in to the other server.

View Prisma Access Agent Notifications

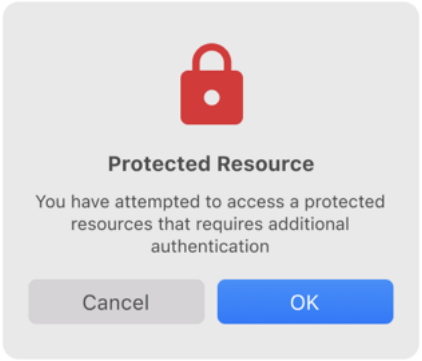
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) ❑ macOS 14 and later or Windows 10 version 2024 and later desktop devices ❑ Internet access

The Prisma Access Agent helps minimize disruptions to your work by notifying you about connection issues or imminent outages. Prisma Access Agent provides notifications on the macOS menu bar or the Windows taskbar (system tray). The agent also displays warnings or errors in pop-up notifications and shows the connection status and any issues in the Prisma Access Agent. (Not supported on Prisma Access Agent Linux)

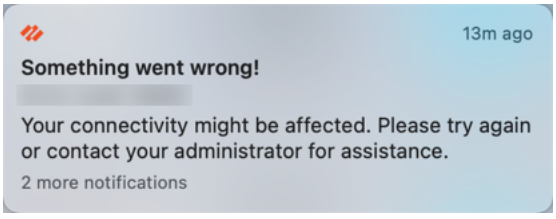
To receive notifications, you must enable desktop notifications.

When an issue occurs, Prisma Access Agent notifies you as follows:

- The Prisma Access Agent icon shows whether the agent is connected or disconnected.
- Prisma Access Agent will prompt you when an application you're accessing requires additional authentication. Click **OK** to authenticate using your organization's authentication method.

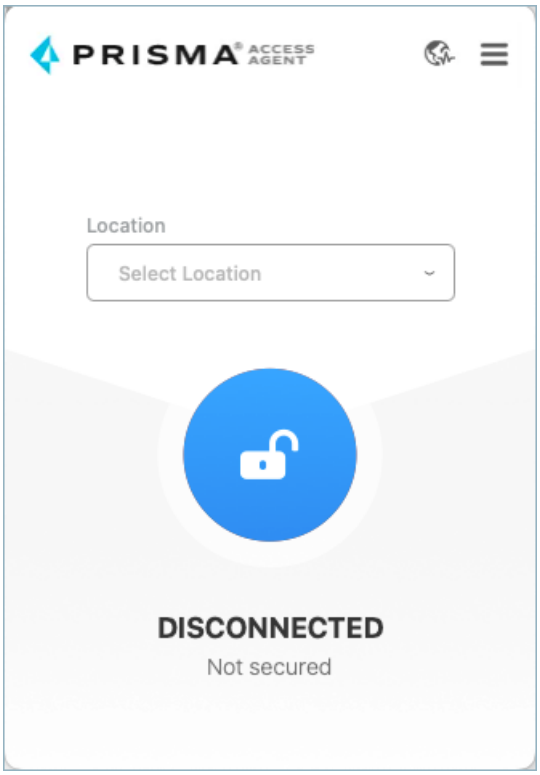


- When a warning or error occurs, a pop-up notification shows the warning or error in minor detail, and may provide a remediation for the issue.



  If Application Experience is running on your device, a pop-up notification from Autonomous DEM appears. You can click the notification to open the Application Experience User Interface to view any suggested remediation for the issue.

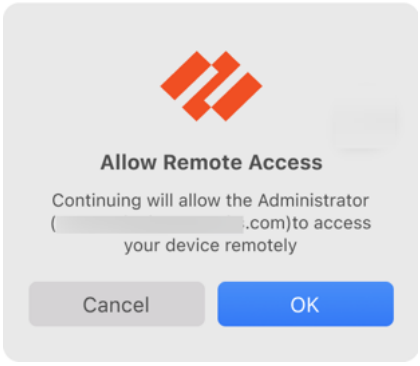
- The main window of the Prisma Access Agent shows whether you are connected or disconnected.



If an error is beyond your control, such as running an unsupported version of the agent, you can click the error pop-up to open the Prisma Access Agent, which will show the error and a brief message to contact your administrator.

When an outage is imminent and you are about to be disconnected from Prisma Access, Prisma Access Agent will issue an alert with an option to refresh the connection or ignore the message.

If you ask your administrator for assistance on a Prisma Access Agent issue, they might need to access your system remotely for troubleshooting. In this case, they will request permission from you to start a remote terminal session on your device that gives them access to advanced commands to troubleshoot and remediate your issues. You can approve or reject this request using the following pop-up that will appear on your device:



Prisma Access Agent Icon States

To keep you informed of your connection status, the Prisma Access Agent provides notifications in the macOS menu bar or Windows taskbar.

The following table shows the possible states of the Prisma Access Agent icons.

Icon	State	Explanation
	Not Connected	The agent isn't connected.
	Connected	The agent is connected to a Prisma Access location. *On supported Linux endpoints, the icon is blue.*

Depending on the settings for your operating system, the Prisma Access Agent icons and notifications can appear in dark mode or light mode.

When a warning or error occurs, a pop-up notification is displayed with a brief message about the issue.

Prisma Access Agent Session Timeouts

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	☐ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) ☐ macOS 14 and later or Windows 10 version 2024 and later desktop devices ☐ Internet access

Prisma Access Agent user sessions are created when you connect to a Prisma Access location and authenticates successfully. Your user session will expire after a certain period of time, or the session will log out automatically after a period of user inactivity. When that happens, you will have to reauthenticate with Prisma Access Agent.

(Not supported on Prisma Access Agent Linux) Your administrator sets the session timeout period as well as when you will be notified of the impending expiration. Once logged in to Prisma Access Agent, you will stay logged in until the session duration is reached, anywhere between 1-30 days. The agent will notify you between 0-120 minutes before the session expires, depending on how your administrator configured the agent.

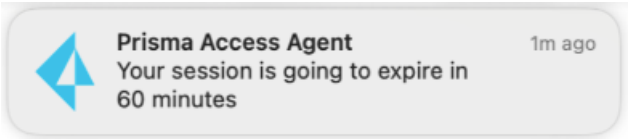
Similarly, once logged in to Prisma Access Agent, you will stay logged in until the agent detects no user activity for a certain amount of time (between 5 seconds to 720 minutes). The agent will notify you between 0-60 minutes before the session logs out automatically due to inactivity, depending on the configuration by your administrator.

Extend the User Session

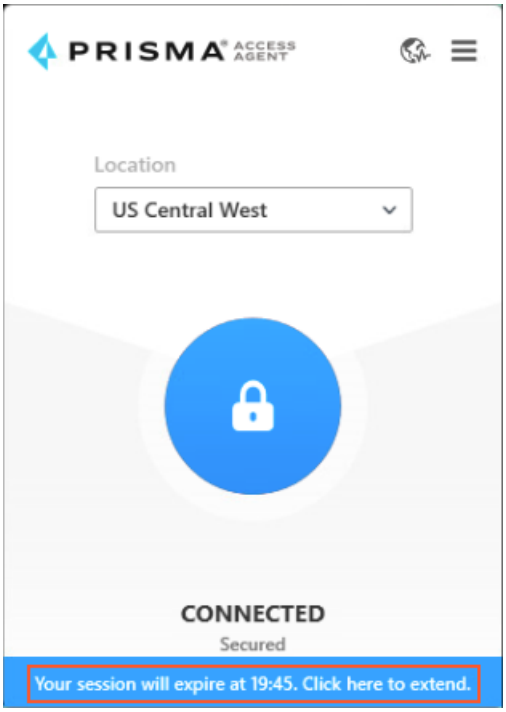
(Not supported on Prisma Access Agent Linux) When you're notified of an impending session timeout, you have the option to extend your Prisma Access Agent user session. If you don't extend the session, it will expire at the time shown on the notification, and you will have to log in to the agent again to continue your session.

The follow is a general workflow for extending a user session:

1. When a Prisma Access Agent user session is about to expire or log out due to inactivity, a system notification will appear. For example:



2. When you click the system notification, the agent will also display a notification in the main window of the Prisma Access Agent app and prompt you to click the banner to extend your session.



3. When you click the banner to extend the session, if your login credentials for your organization are still active, the agent session will continue without further action from you.

   If your credentials have expired, you will need to reenter your login credentials to renew your Prisma Access Agent session.

   After successful authentication, you will be connected to the Prisma Access Agent.

Other Notification Scenarios

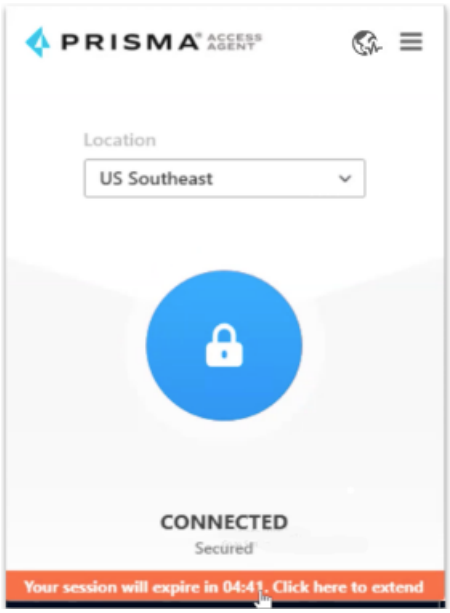
(Not supported on Prisma Access Agent Linux) The following scenarios apply if you don't respond to the initial system notification.

- You missed the system notification or if there is no system notification (for example, if desktop notifications are not enabled on your device).

  The Prisma Access Agent app will open, showing the notification banner at the bottom of the window. You can click on the banner to extend your session.

- You take no action on the system notification or the Prisma Access Agent app.

  Five minutes before session expiration, the notification banner will change to an orange color in the Prisma Access Agent app.

  You can click the banner at any time to extend your session. If you don't click the banner, the session will expire and you will need to reauthenticate in a browser tab to access the agent.
- You click away from the Prisma Access Agent app during the 5-minute countdown to expiration.

  The Prisma Access Agent app will close automatically and a browser tab will appear for you to reauthenticate.
- Your device is in sleep mode.

  The system does not show any expiration notification. You will need to open the Prisma Access Agent and reauthenticate when the browser comes up.

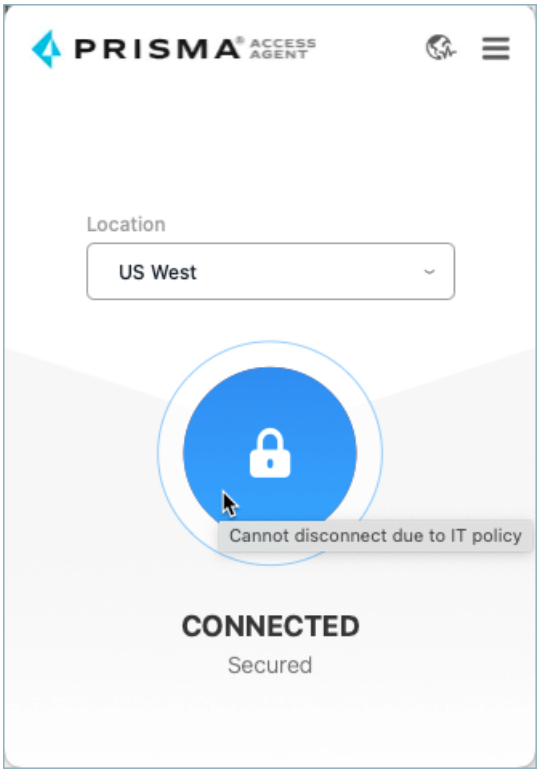
Disconnect the Prisma Access Agent from a Location

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

If your administrator has configured the Prisma Access Agent to run in **On Demand** mode, you can disconnect from a Prisma Access location.

If you disconnect from a location, your device will not be protected by the same security policies that your organization enforces, and you won't be able to access your organization's private and public applications and resources.

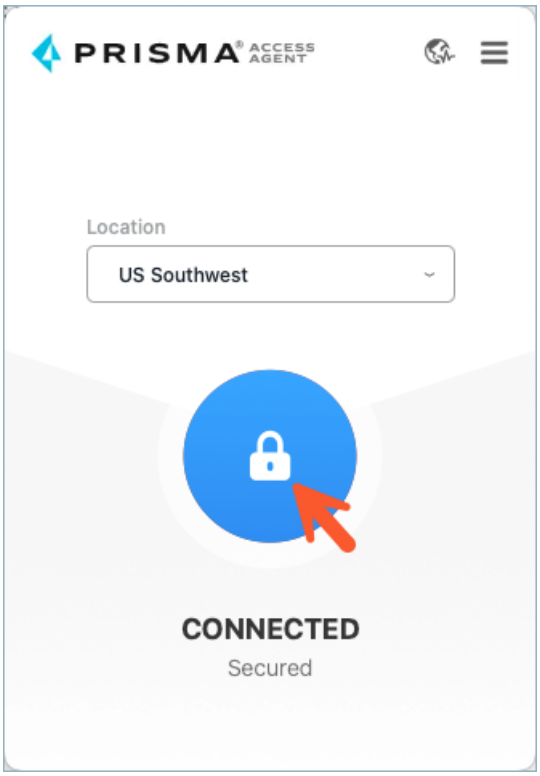
*You cannot disconnect from Prisma Access if your agent is running in **Always On** mode. To see if your agent is in Always On mode, hover your cursor over the lock:*



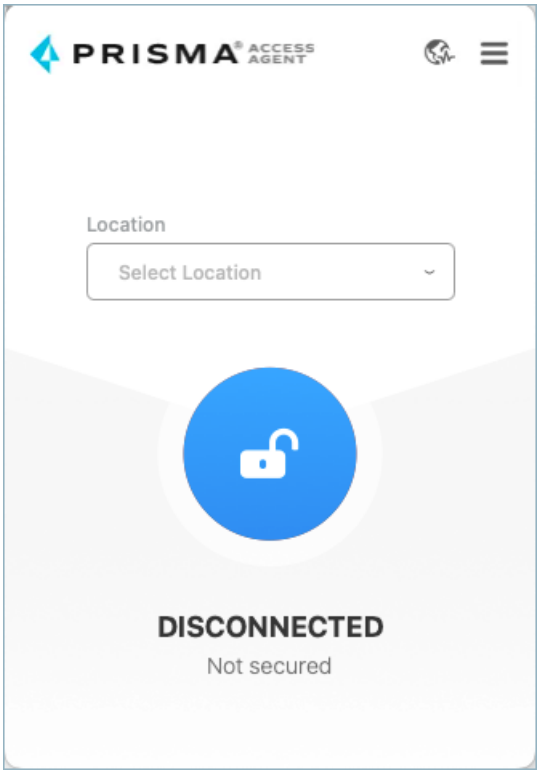
To disconnect from a Prisma Access location:

STEP 1 | Launch the Prisma Access Agent by clicking the Prisma Access Agent icon from the macOS menu bar, Windows taskbar, or Linux panel.

STEP 2 | Click the lock icon to disconnect from the location.



You are disconnected from the location.



Disable the Prisma Access Agent

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

If your administrator enabled it, you can temporarily disable the Prisma Access Agent. This is helpful on devices where other secure access apps, such as the GlobalProtect™ app, coexist with the Prisma Access Agent. In this case, you will have to disable the Prisma Access Agent before you can switch to the other app.

After you disable the Prisma Access Agent, the agent is in the disabled state, where:

- All traffic to Prisma Access locations are disabled, and multi-factor authentication (MFA) is disabled.
- Communication with the server persists so the agent can continue to receive upgrades, remote shell requests from the administrator, and perform HIP checks.
- If configured by the administrator, the anti-tamper feature will continue to function to protect the agent from unauthorized tampering.
- On macOS devices, the system and network extensions for Prisma Access Agent will continue to be active, and the content filter will also continue to be active.
- Connecting to another server reenables the Prisma Access Agent automatically.

To disable the Prisma Access Agent:

- Using the App
- Using PACli

Disable the Prisma Access Agent (Using the App)

To disable the Prisma Access Agent using the Prisma Access Agent app, complete the following steps.

Disabling the agent using a one-time password requires Prisma Access Agent version 25.3.0.43 or later.

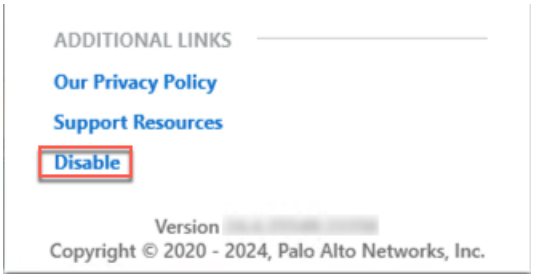
STEP 1 | Open the Prisma Access Agent app by clicking the Prisma Access Agent icon in your taskbar.

If you're disabling the agent for the first time or if you don't see the **Disable** link in the settings page, sign out of the Prisma Access Agent.

1. Select the hamburger menu and select **Sign Out**.
2. Log in to the Prisma Access Agent app again to make the **Disable** link appear in the settings window.

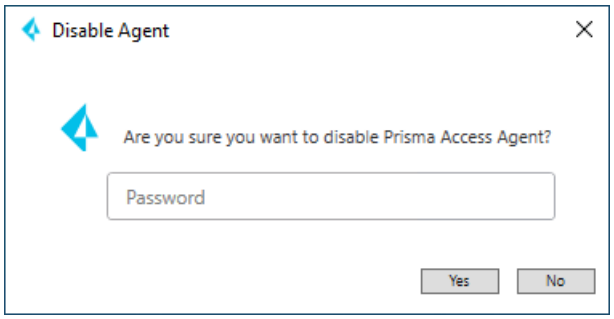
STEP 2 | Click the hamburger menu to open the settings window.

STEP 3 | **Disable** the Prisma Access Agent.



STEP 4 | (Prisma Access Agent version 25.3.0.43) (Not supported on Prisma Access Agent Linux) If your administrator requires a one-time password (OTP) to disable the agent, enter the password and click **Yes** on Windows or **OK** on macOS. If you don't have the password, contact your administrator for the password.

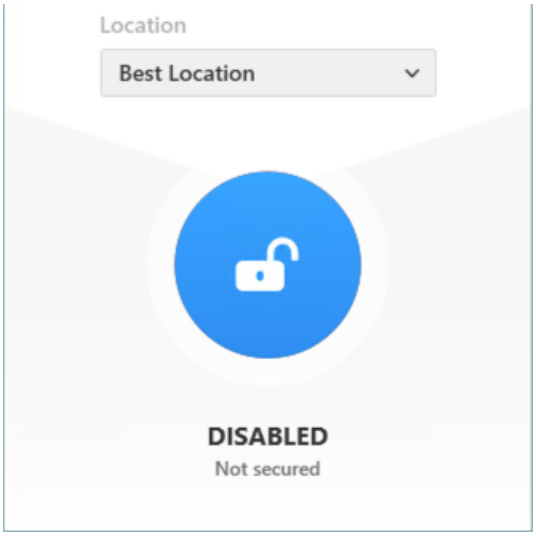
For example, on Windows:



The password is a unique, single-use password. Once you use it to disable the agent, you can't use it again. The next time you disable the agent, you will need to request another one-time password from your administrator. If you forget the password, ask your administrator to share it with you again.

STEP 5 | Close the settings window by clicking the **X**.

The Prisma Access Agent is disabled.



STEP 6 | To reenable the Prisma Access Agent:

1. Open the Prisma Access Agent.
2. Select the hamburger menu and **Enable** the Prisma Access Agent.

The Prisma Access Agent functionality will resume.

Disable the Prisma Access Agent (Using PACli)

You can disable the Prisma Access Agent using the Prisma Access Agent command-line tool (PACli).

STEP 1 | Enter the following command:

- (macOS)

```
/Applications/Prisma\ Access\ Agent.app/Contents/Helpers/pacli
 disable
```

- (Windows)

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent\pacli"
 disable
```

- (Linux)

```
pacli disable
```

STEP 2 | (Prisma Access Agent version 25.3.0.43) (Not supported on Prisma Access Agent Linux) If your administrator requires a one-time password (OTP) to disable the agent, **Enter One Time Password** when prompted. If you don't have the password, contact your administrator for the password.

If successfully disabled, the `Agent is disabled` message is displayed. For example, on Windows:

```
C:\Users\Administrator>pacli disable
Enter One Time Password:
Agent is disabled
```

STEP 3 | To verify that the agent is disabled, run the following command:

```
pacli status
```

In the command output, the **State** should be **Disabled**. For example, on Windows, you should see the following output:

```
C:\Users\Administrator>pacli status
State:                          Disabled
Mode:                           On Demand
Tunnel:                         Not Connected
Captive Portal Status:          Not Detected
Device Quarantine:              Not Quarantined
EPM Status:                     Up
Local Hostname:                 [redacted]
Current Time:                   2025-05-12 16:26:26, Jerusalem Daylight Time
Disabled Until:                 2025-05-12 18:26:17
EPM Last Seen:                  2025-05-12 16:26:18
Last Successful Configuration:  2025-05-12 16:26:18
GlobalProtect Status:           Uninstalled
```

STEP 4 | To reenable the agent, run the following command:

```
pacli enable
```


Use Prisma Access Agent Anti-Tamper Protection

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: 25.4 ❑ macOS 14 and later or Windows 10 version 2024 and later desktop devices ❑ Internet access

When your administrator has enabled anti-tamper protection for Prisma Access Agent, certain operations require additional authentication. This protection prevents unauthorized changes to the agent's critical files, services, and settings, maintaining the security and integrity of your device connection to Prisma Access. (Not supported on Prisma Access Agent Linux)

Anti-tamper protection is transparent during normal operations—you can continue to use your device and applications as usual without interruption. The protection only affects attempts to modify, disable, or uninstall the Prisma Access Agent itself.

When You Will Encounter Anti-Tamper Protection

You might encounter anti-tamper protection when attempting to:

- Disable the Prisma Access Agent temporarily
- Uninstall the Prisma Access Agent from your device
- Modify or restart Prisma Access Agent services
- Change Prisma Access Agent files or registry settings

When you attempt any of these operations, depending on your administrator's configuration, the Prisma Access Agent app might request a password or one-time password (OTP).

Disabling the Agent Temporarily

If you need to temporarily disable the Prisma Access Agent (for example, when troubleshooting network issues), your experience will depend on how your administrator has configured anti-tamper protection:

- If set to **Allow**: You can disable the agent without any password by clicking the **Disable** options in the agent app or using the appropriate command-line instruction.
- If set to **Allow with One Time Password**: You will need to enter a valid one-time password when prompted. Your IT administrator or help desk must provide this password.
- If set to **Disallow**: The **Disable** option won't be visible in the agent app. Contact your IT administrator if you need the agent disabled.

If the agent is temporarily disabled, it will automatically re-enable after a period set by your administrator (typically 30 minutes).

Uninstalling the Agent

When anti-tamper protection is enabled and you attempt to uninstall the Prisma Access Agent:

1. On Windows: Navigate to **Control Panel** > **Programs** > **Uninstall a Program**, select Prisma Access Agent, and click **Uninstall**.
2. On macOS: Run the following command:

```
/Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
uninstaller
```

3. For both Windows and macOS: When prompted, enter the Uninstall OTP provided by your IT administrator.

If you don't have the proper OTP, the uninstallation won't proceed. Contact your IT support team for assistance.

Obtaining a Password or OTP

When you need to perform an operation that requires authentication, you will need to contact your IT support team or help desk. They can generate the appropriate password or OTP for your specific device and the operation you need to perform.

OTPs are typically:

- Unique to your device
- Valid for only one use
- Specific to the operation you need to perform

Your IT team might use different distribution methods to share the OTP with you, such as secure messaging, phone calls, or ticketing systems.

After Using an OTP

After using a Privileged Access OTP to perform an operation, you will have temporary access to perform additional privileged operations without reentering a password. You administrator sets the temporary access period (typically 30 minutes).

During this period:

- You can perform additional privileged operations without reentering a password
- The system will notify you approximately five minutes before this privileged access expires
- After the access period expires, you will need a new OTP for any additional privileged operations

You can check the status of your temporary access period by running the `pacli status` command in a terminal window, which will display the expiration time if privileged access is active.

Troubleshooting

If you encounter issues with anti-tamper protection:

- **Invalid password message**—Ensure you're entering the correct OTP for your specific device and operation. OTPs are case-sensitive and must be entered exactly as provided.

- **Operation still blocked after entering OTP**—The OTP might have expired or already been used. Contact your IT support team for a new OTP.
- **No prompt for password when expected**—Your administrator might have configured anti-tamper protection differently than you expected. Contact your IT support for clarification.
- **Emergency situations**—If you need urgent assistance, especially in cases where network connectivity is limited, inform your IT support team. They have access to emergency authentication methods for critical situations.

All attempts to use OTPs—both successful and unsuccessful—are logged and may be reviewed by your security team.

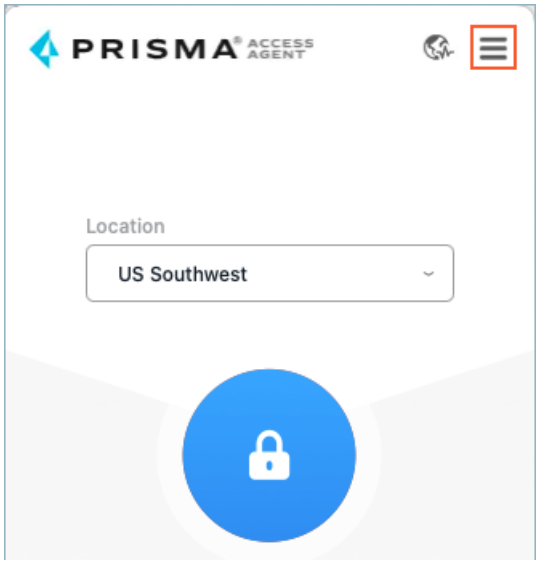
Log out of the Prisma Access Agent

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

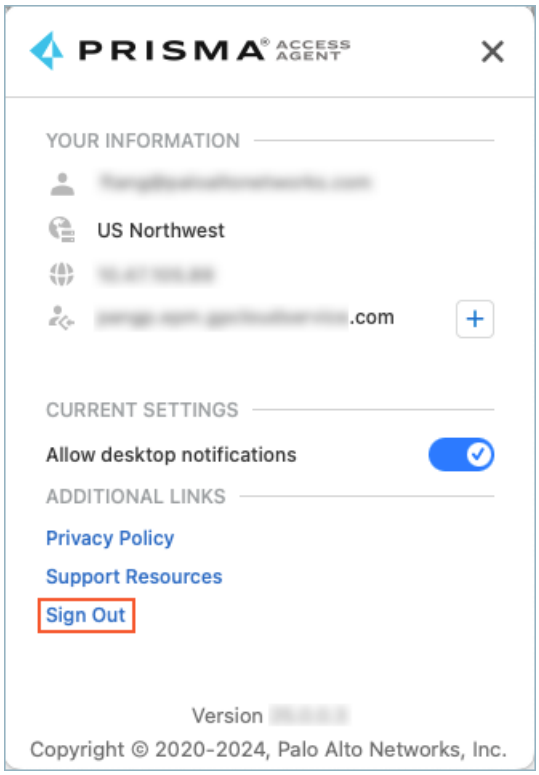
You can log out of the Prisma Access Agent if your administrator configured the Prisma Access Agent to allow user sign-out.

STEP 1 | Open the Prisma Access Agent app by clicking the Prisma Access Agent icon from the macOS menu bar, Windows taskbar, or Linux panel.

STEP 2 | Click the options icon to open the settings window.



STEP 3 | Select **Sign Out** from the settings window.



Get Help for Prisma Access Agent Issues

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

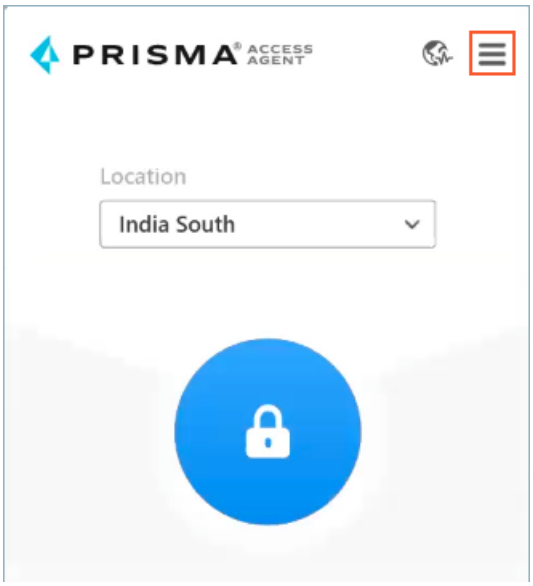
If you need assistance with using the Prisma Access Agent, you can view a website with information about the agent. By default, the support resources link goes to the Prisma Access Agent documentation. Your administrator, however, can configure the help resources link to direct you to another website, such as an internal help website.

If your administrator configured your device with the Access Experience app, you can open the Access Experience app to review any suggested remediation for the issue.

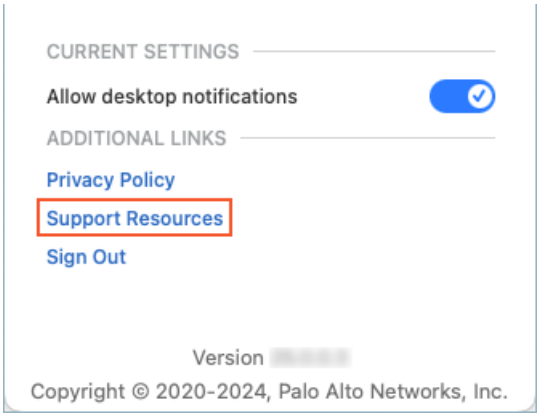
(Not supported on Prisma Access Agent Linux) (Prisma Access Agent version 25.4) The Access Experience icon is integrated directly into the Prisma Access Agent app to give you convenient access to potential solutions to your issues, such as device health and connectivity issues. You will not see a separate Access Experience icon in the Windows taskbar or macOS menu bar.

You can get help for the Prisma Access Agent using one of the following methods:

- From the Prisma Access Agent:
  1. Click the options icon.

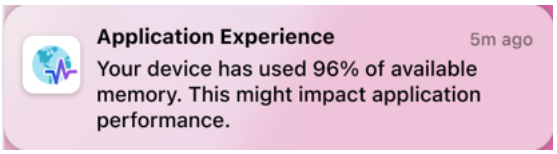


  2. Click **Supported Resources**.

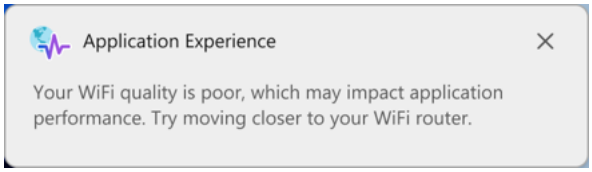


- (Not supported on Prisma Access Agent Linux) From Access Experience:
  - When an OS notification appears due to an issue, click the message to review any suggestions for remediation in the Access Experience agent.

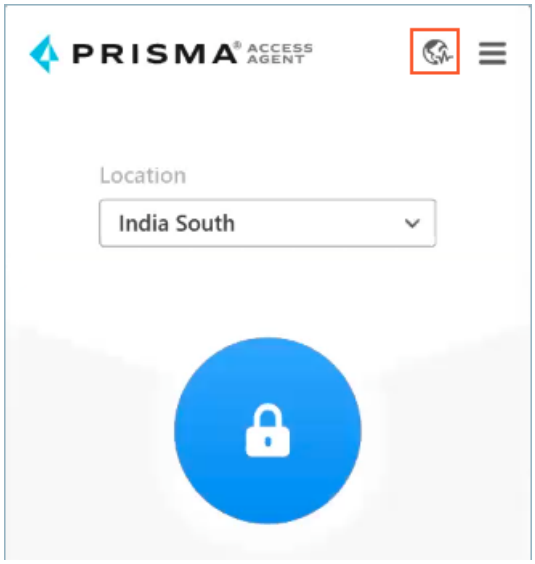
    On macOS:

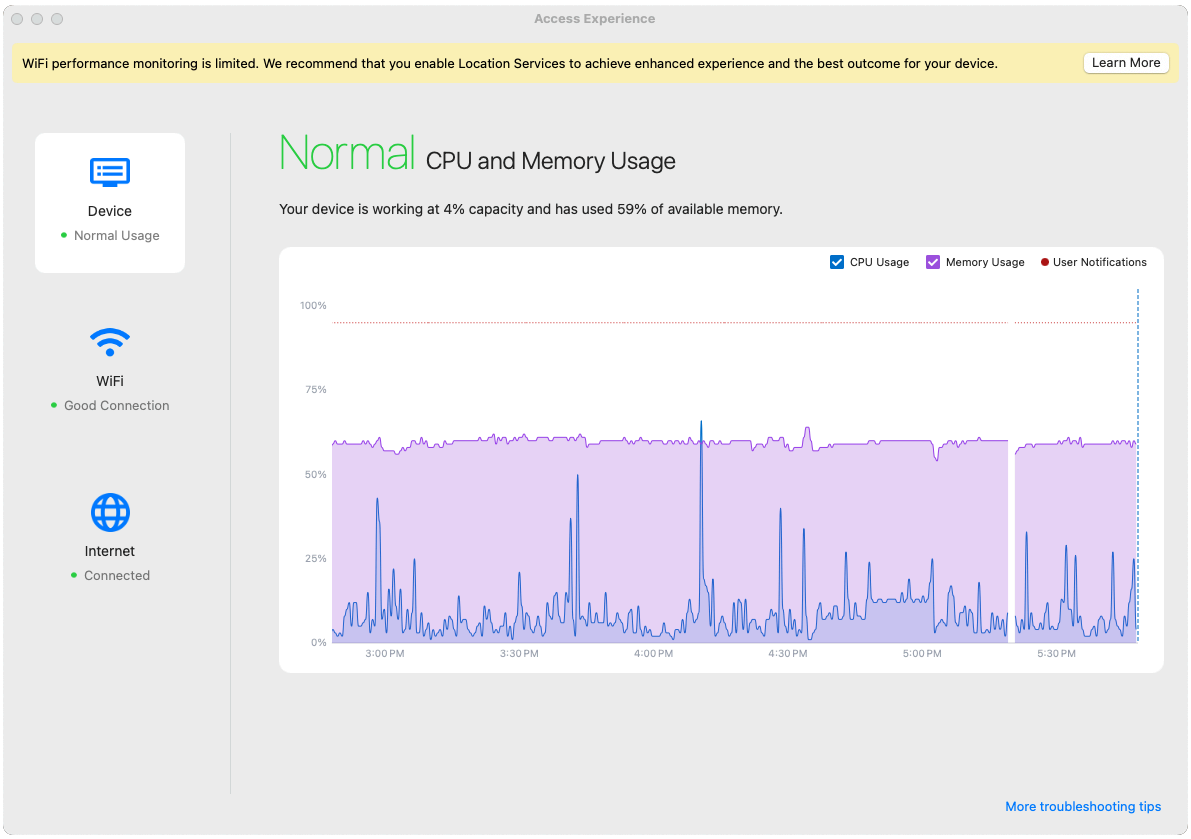
    On Windows:

  - (Prisma Access Agent 25.4) You can also click the Access Experience icon in Prisma Access Agent to open the Access Experience app.

    From the Access Experience app, you can view your device health, connection status, and any suggestions for remediation in the Access Experience agent.



Report Prisma Access Agent Issues for Troubleshooting

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: 25.7 ❑ macOS 14 and later or Windows 10 version 2024 and later desktop devices ❑ Internet access

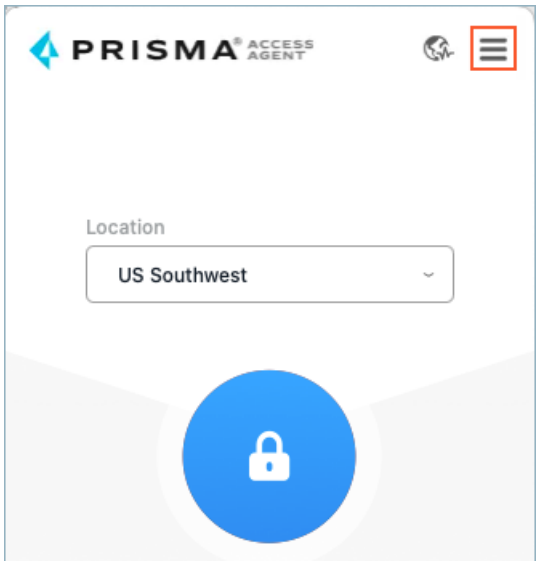
If your administrator enabled the capability to collect diagnostics on your device, when you experience connectivity problems with Prisma Access Agent, you can report issues directly from the Prisma Access Agent app or command line to initiate diagnostic collection. Additionally, your administrator can initiate diagnostic collection and might require your consent before proceeding to collect diagnostic data. Both methods enable immediate troubleshooting and help administrators resolve connectivity issues more efficiently.

Report Issues from the Prisma Access Agent App

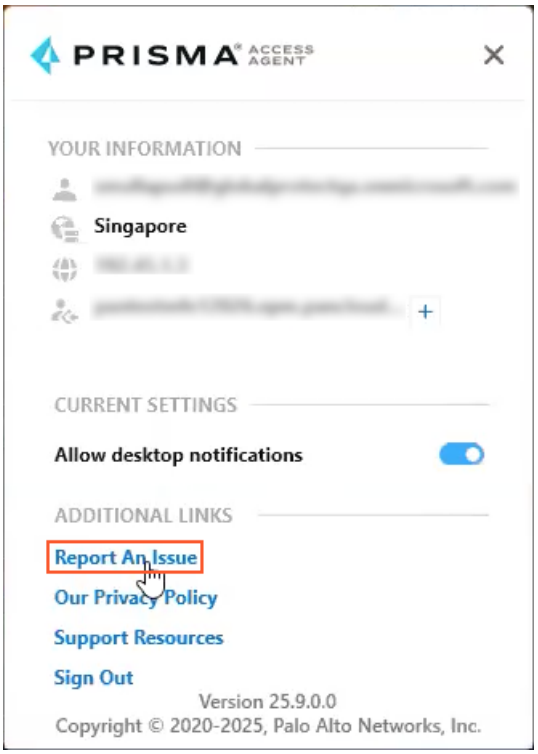
You can report connectivity problems through the Prisma Access Agent app when you experience issues such as connection failures, slow performance, or authentication problems.

To report an issue from the agent app:

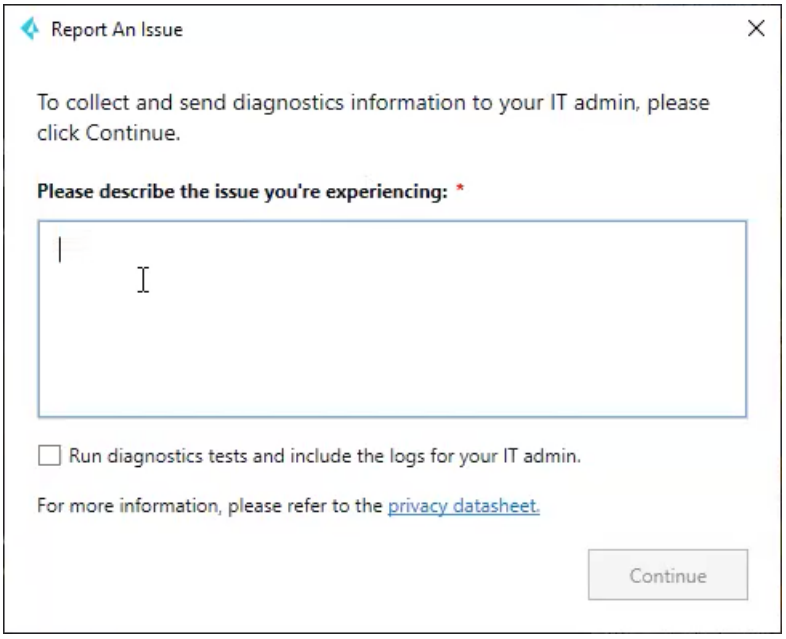
1. Open the Prisma Access Agent from your system tray or applications menu.
2. Click the options icon to open the settings window.



3. Select **Report An Issue**.



4. Report your issue.



   1. **Please describe the issue you're experiencing** in 1000 characters or less.

      Include specific details such as when the issue occurred, what you were trying to do, and any error messages you received. For example:

      ```
      Unable to connect to corporate applications since this morning.
       Getting timeout errors when accessing internal websites.
      ```

   2. Enable **Run diagnostics tests and include logs for your IT admin** to agree to diagnostic data collection.

5. **Continue** to initiate the diagnostic collection process.

   *You cannot click **Continue** unless you enter a description for the issue and enable **Run diagnostics tests and include logs for your IT admin**.*

The system will collect troubleshooting data and upload it to administrators for analysis.

Report Issues from the Command Line

You can also report issues using the Prisma Access Agent command-line interface (PACli), which is useful for scripting or when the Prisma Access Agent app is unavailable.

To report an issue from the command line:

- On macOS, open a Terminal window and issue the following command:

```
/Applications/Prisma\ Access\ Agent.app/Contents/Helpers/pacli eie
 trigger -d "<description>"
```


- On Windows, open a Command Prompt window and issue the following command:

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent\pacli" eie
 trigger -d "<description>"
```

Replace **"<description>"** with a detailed explanation of the issue you are experiencing, enclosed in quotes. The description is limited to 1000 characters.

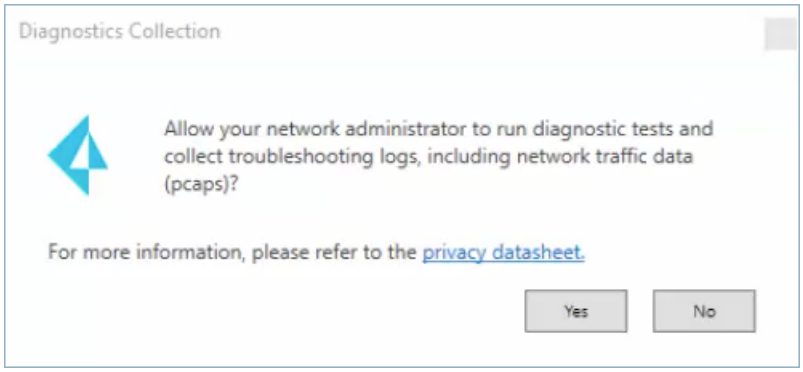
Example:

```
pacli eie trigger -d "Unable to connect to corporate applications
 since this morning. Getting timeout errors when accessing internal
 websites."
```

Administrator-Initiated Diagnostic Collection

Your administrator might also initiate diagnostic data collection from your device to troubleshoot connectivity issues. If they configured user consent requirements from the server and they initiate data collection:

1. You will receive a consent dialog explaining that your administrator has requested diagnostic data collection. For example:



   The dialog contains a link to the Prisma Access Agent privacy datasheet.
2. You can choose to approve or deny the diagnostic collection request.

   If you approve the request, diagnostic data collection will proceed automatically. If you deny the request, no diagnostic data will be collected and your administrator will be notified of the denial.

This consent process ensures your privacy is protected while allowing administrators to gather the information needed for troubleshooting when necessary.

If your administrator did not configure user consent requirements, they will be able to collect diagnostics, but you will not be asked for approval.

Data Collection and Privacy

When you report an issue or approve administrator-initiated collection, the system collects diagnostic data to help administrators troubleshoot connectivity problems. This data includes:

- System logs related to Prisma Access Agent operation

- Configuration information

When requested, you must provide consent before diagnostic data collection begins, whether you or your administrator initiated the process. The collected information is used solely for troubleshooting purposes and is subject to your organization's data retention policies. No personal files or browsing history are collected during this process.

After Reporting an Issue

Once you submit an issue report or approve administrator-initiated collection:

- Diagnostic data collection begins immediately
- Collected data is uploaded to administrators for analysis
- You might be contacted by your IT support team for additional information or to implement recommended solutions

Your issue report or consent to diagnostic collection helps create a record of the problem and provides administrators with the technical data needed to identify and resolve connectivity issues efficiently.

Switch Between the Prisma Access Agent and GlobalProtect App

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ macOS 14 and later or Windows 10 version 2024 and later desktop devices ❑ Internet access

In some organizations, the Prisma Access Agent is installed on user devices that already have the GlobalProtect app installed. After installing the Prisma Access Agent, you can switch between the and the GlobalProtect app as needed.

Before switching to the GlobalProtect app, you must disable the Prisma Access Agent app. The following table shows the Prisma Access Agent behavior after disabling the agent and after switching to GlobalProtect.

Prisma Access Agent Behavior	After Disabling Prisma Access Agent	After Switching to GlobalProtect
Connectivity to the tunnel	No	No
Connectivity to the server (Prisma Access Agent management plane)	Yes	Yes
Prisma Access Agent Notifications	No	No
Prisma Access Agent enforcer	No	No, but GlobalProtect enforcer is enabled
ADEM Access Experience status	Yes (independent of agent status)	Yes (independent of agent status)
Troubleshooting by remote shell	Yes	Yes
Anti-tamper feature	Yes	Yes
PACli commands functional	Yes, but don't use **`pacli connect`**	Yes, but don't use **`pacli connect`**

You can use either the Prisma Access Agent app or the Prisma Access command-line tool (PACli) to switch between the two apps. (Not supported on Prisma Access Agent Linux)

- Prisma Access Agent app

- Prisma Access command line (PACli)

Switch Between the Prisma Access Agent and GlobalProtect App (Using Prisma Access Agent App)

Before switching to the GlobalProtect™ app, you need to disable the Prisma Access Agent. If your administrator configured the feature to allow users to disable the Prisma Access Agent, you can use the app to disable the Prisma Access Agent. After you disable the Prisma Access Agent, you can start the GlobalProtect app.

Your administrator must contact the Palo Alto Networks team to enable this tenant-level feature. It's not available as an agent setting on .

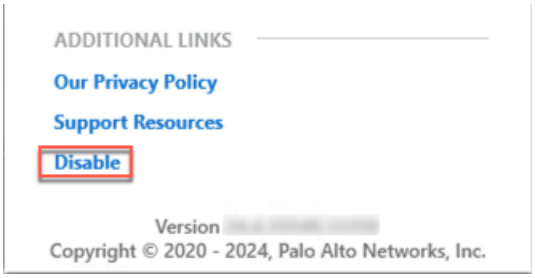
- To switch from the Prisma Access Agent to the GlobalProtect app:
  1. Open the Prisma Access Agent.

     If you're disabling the agent for the first time, open the Prisma Access Agent app and sign out of the Prisma Access Agent.

     1. Select the hamburger menu and select **Sign Out**.
     2. Log in to the Prisma Access Agent app again to make the **Disable** link appear in the preferences window.
  2. Click the hamburger menu to open the preferences window.

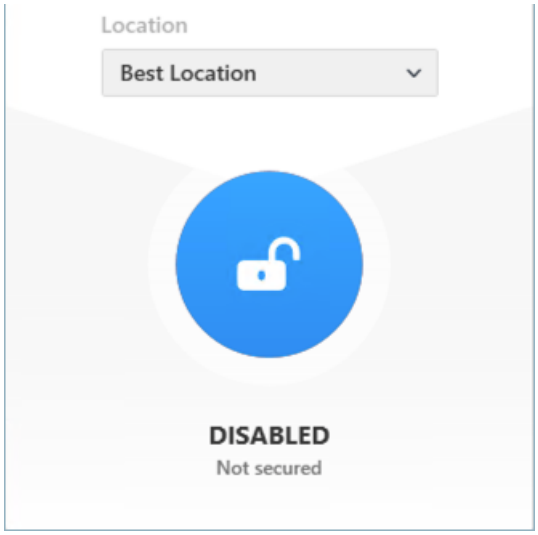
     

  3. **Disable** the Prisma Access Agent.

  4. Close the preferences window by clicking the **X**.

     The Prisma Access Agent is disabled.

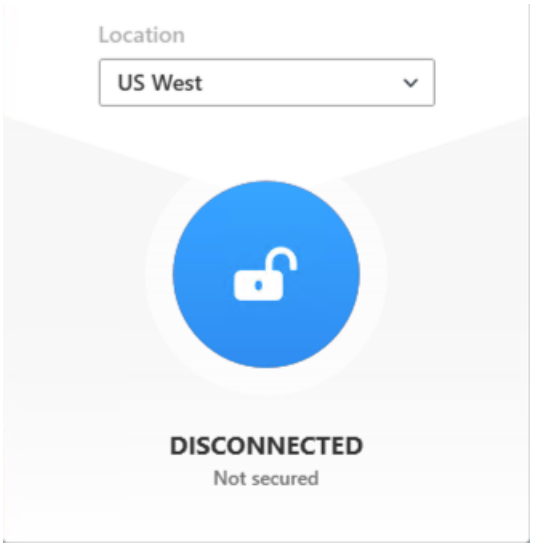
  5. Start the GlobalProtect app and **Connect** to GlobalProtect.

- To switch from the GlobalProtect app back to the Prisma Access Agent:
  1. Open the GlobalProtect app.
  2. Click the options menu and select **Disconnect**.
  3. Launch the Prisma Access Agent app.
  4. Click the hamburger menu to open the preferences window.

  5. **Enable** the Prisma Access Agent.

  6. Close the preferences window by clicking the **X**.
  7. If the agent is in Always On mode, the agent is enabled and will connect to the best location.

     If the agent is in On-Demand mode, the Prisma Access Agent is enabled but remains disconnected. Click the lock icon to connect to the Prisma Access location.



Switch Between the Prisma Access Agent and GlobalProtect App (Using PACli)

To switch between the Prisma Access Agent and the GlobalProtect app, run the Prisma Access command-line tool (PACli). When switching to the GlobalProtect app, the PACli tool will prompt

you for the anti-tamper unlock password if the administrator set one up during the onboarding of the Prisma Access Agent. Switching to the desired app disables the app that you're currently using.

STEP 1 | To switch from the Prisma Access Agent to the GlobalProtect app:

1. Run the **`switchto`** command to switch agents:
   - On macOS devices, open a Terminal window and issue the following command:

     ```
     sudo /Applications/Prisma\ Access\ Agent.app/Contents/
     Helpers/pacli switchto GlobalProtect
     ```

   - On Windows devices, open a Command Prompt window and issue the following command:

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" switchto GlobalProtect
     ```

2. (macOS) Enter the admin password when prompted.
3. If prompted, enter **Y** to switch to the GlobalProtect app.
4. If prompted for a supervisor password, enter the anti-tamper unlock password.

   The following text shows an example of switching from the Prisma Access Agent to GlobalProtect on a macOS device:

   ```
   <username@hostname> ~ % cd /Applications/Prisma\ Access\
    Agent.app/Contents/Helpers
   <username@hostname> Helpers % sudo ./pacli switchto
    GlobalProtect
   Enter supervisor password:
   Disabled Prisma Access Agent.
   Starting the GlobalProtect service. This can take up to 60
    seconds...
   Successfuly started GlobalProtect. Switch complete.
   <username@hostname> Helpers %
   ```

   This action stops the Prisma Access Agent service, and starts the GlobalProtect service. An entry is written to the Prisma Access Agent logs indicating that the Prisma Access Agent has been disabled. For example, the following events are logged:

   ```
   <username@hostname> ~ % cd /Applications/Prisma\ Access\
    Agent.app/Contents/Helpers
   <username@hostname> Helpers % ./pacli event
   .
   .
   740      2024-12-11 23:20:57  Tamper Detection   Agent is
    disabled
   741      2024-12-11 23:20:57  Agent Tunnel       Tunnel
    disconnected
   .
   ```



```
.
```

5. (Optional) Show the status of the **switchto** command by running the **pacli switchto status** command.

   The following text shows an example of checking the status of the **switchto** command on macOS:

```
<username@hostname> ~ % cd /Applications/Prisma\ Access\
 Agent.app/Contents/Helpers
<username@hostname> Helpers % sudo ./pacli switchto status
Prisma Access Agent:      Disabled
GlobalProtect:            Enabled
<username@hostname> Helpers %
```

STEP 2 | To switch back to the Prisma Access Agent:

1. Run the **switchto** command to switch agents:

   - On macOS devices, open a Terminal window and issue the following command:

```
sudo /Applications/Prisma\ Access\ Agent.app/Contents/
Helpers/pacli switchto PrismaAccessAgent
```

   - On Windows devices, open a Command Prompt window and issue the following command:

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent
\pacli" switchto PrismaAccessAgent
```

2. (macOS) Enter the admin password when prompted.
3. If prompted, enter **Y** to switch to the Prisma Access Agent.
4. If prompted for a supervisor password, enter the anti-tamper unlock password.

   The following text shows an example of switching from the GlobalProtect app to the Prisma Access Agent on a macOS device:

```
<username@hostname> ~ % cd /Applications/Prisma\ Access\
 Agent.app/Contents/Helpers
<username@hostname> Helpers % sudo ./pacli switchto
 PrismaAccessAgent
Password:
Enter supervisor password:
Stopping the GlobalProtect service. This can take up to 60
 seconds...
Disabled GlobalProtect.
Successfuly started Prisma Access Agent. Switch complete.
```



```
<username@hostname> Helpers %
```

This action stops the GlobalProtect service and starts the Prisma Access Agent service. An entry is written to the Prisma Access Agent logs indicating that the Prisma Access Agent has been enabled. For example, the following events are logged:

```
<username@hostname> ~ % cd /Applications/Prisma\ Access\
 Agent.app/Contents/Helpers
<username@hostname> Helpers % ./pacli event
.
.
742      2024-12-11 23:21:05  Tamper Detection   Agent is
 enabled
743      2024-12-11 23:21:21  Agent Tunnel       Tunnel
 connected
.
.
```

After switching back to the Prisma Access Agent, if the agent is in Always On mode, the agent will be enabled and will connect to the best location. If the agent is in On-Demand mode, the agent will be enabled but disconnected.

5. (Optional) Show the status of the **`switchto`** command by running the **`pacli switchto status`** command.

   The following text shows an example of checking the status of the **`switchto`** command on macOS:

```
<username@hostname> ~ % cd /Applications/Prisma\ Access\
 Agent.app/Contents/Helpers
<username@hostname> Helpers % sudo ./pacli switchto status
Prisma Access Agent:      Enabled
GlobalProtect:            Disabled
<username@hostname> Helpers %
```


Prisma Access Agent Commands

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Minimum Prisma Access Agent version: • 25.1 (macOS and Windows) • 25.7 (Linux) ❑ macOS, Windows, or Linux desktop devices ❑ Check the prerequisites for the supported OS versions ❑ Internet access

The administrator can run Prisma Access Agent commands using the Prisma Access command line (PACli) tool to gain visibility into the Prisma Access Agent deployment. They can run the Prisma Access Agent commands on your behalf in a terminal session on your device or in a remote shell.

Usage

To issue Prisma Access Agent commands on the Prisma Access command-line tool, use the following syntax:

- For macOS agents:

```
/Applications/Prisma\ Access\ Agent.app/Contents/Helpers/pacli /? |
 [command] [/? | help | options]]
```

- For Windows agents:

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent\pacli" /?
 | [command] [/? | help | options]]
```

- For Linux agents:

```
pacli /? | [command] [/? | help | options]]
```

If you enter the **`pacli`** command without arguments or with the **`/?`** option, the list of available Prisma Access Agent commands is displayed.

*If you set up an environment variable for the PACli tool (`pacli`), you can just enter **`pacli <command>`** without the folder path.*

The following tables contain descriptions of the Prisma Access Agent commands and associated options that you can run on the Prisma Access command line. In the command input and output, the terms "EPM" and "epm" refer to the Endpoint Manager or Prisma Access Agent Manager (also known to end users as the server). The Endpoint Manager communicates with the agent, such as

sending commands and configurations to the agent, routing authentication requests to the Cloud Identity Engine, and once authenticated, providing the agent with a token for the gateways.

(macOS and Windows agents only) Some commands also support integration with third-party applications, such as a unified login portal, that need to programmatically control Prisma Access Agent authentication and connectivity without user interaction with the agent. These commands and their expected JSON response fields are listed in order of use in **Commands for Third-Party Integration** below.

Command	Description
`version`	Shows the version of the Prisma Access Agent that's running on the endpoint
`captive-portal`	(Not supported on Prisma Access Agent Linux) Shows the presence of a captive portal with the **`pacli captive-portal status`** command
`connect`	Creates a tunnel connection for Prisma Access Agent traffic by connecting to a gateway. • To connect to a location, enter **`pacli connect <gateway name>`** • To get a list of the Prisma Access locations where your users can connect to, enter **`pacli gateway`** To connect to the best available location, enter **`pacli connect --best`**
`disconnect`	Stops the tunnel connection by disconnecting from the gateway
`status`	Shows the current Prisma Access Agent status. You can view the following status: • **`State`**—Shows the state of the Prisma Access Agent • **`Mode`**—Shows the mode the Prisma Access Agent is running in (**Always On** or **On Demand**) • **`Tunnel`**—Shows the state of the Prisma Access Agent connection • **`HIP Status`**—Shows whether your device is compliant • **`EPM Status`**—Shows the status of the endpoint manager • **`EPM Last Seen`**—Shows the last time your device connected to the to the endpoint manager • **`Local Hostname`**—Shows the hostname of the end-user device
`protect`	(Not supported on Prisma Access Agent Linux) Enables or disables the feature that protects the Prisma Access Agent from being tampered with on the endpoint, such as the unauthorized uninstallation of the agent. You can specify the following options:

Command	Description
	• **status**—Displays the protection status of the Prisma Access Agent files and folders, Prisma Access Agent processes, registry keys (Windows-only), and services and HIP processes. • **enable**—Enables the anti-tamper feature. • **disable**—Disables the anti-tamper feature. Requires the anti-tamper unlock password.
epm	Performs endpoint management actions using the following options: • **status**—Shows the current status of the service that manages . • **address**—Sets the URL for the endpoint manager. You can **add**, **delete**, **list**, or **set** (connect) to a specified server URL. • **signout**—Disconnects the Prisma Access Agent from the endpoint manager and discards the token that the agent management authentication service generated. The token enables the agent to communicate with any endpoint manager component. If you enter **pacli epm signout --keep**, the command will disconnect the agent from the endpoint manager without discarding the token. • **fetch**—Retrieves the Prisma Access Agent configuration immediately. • **set-token**—Resets the token that the agent management authentication service generated. The Prisma Access Agent uses the token to communicate with any agent management component. If you enter **pacli epm** incorrectly or without any arguments, the list of available options is displayed.
config	Manages the local configuration of the Prisma Access Agent. You can use the following options: • **import**—Imports the configuration from a configuration file • **export**—Exports the configuration to a file
loglevel	Manipulates the logging level of Prisma Access Agent logs using the following options: • **status**—Shows the current verbosity level of the logs • **set**—Sets the verbosity level of the logs
event	Shows a list of Prisma Access Agent events
command	Triggers a command that is sent from the server (endpoint manager) to the client (Prisma Access Agent).

Command	Description
gateway	Gets a list of the Prisma Access locations where your users can connect to
enable	Enables the Prisma Access Agent
disable	Disables the Prisma Access Agent. Requires the anti-tamper unlock password.
hip	Runs host information profile actions: • **status**—Shows the current HIP status • **version**—Shows the version of the HIP library • **resend**—Sends a HIP report to the current Prisma Access location and endpoint manager • **update**—Updates the HIP library (if an update is available) • **notification**—Shows the HIP notifications that the agent received
tunnel	Shows the status of the tunnel, including the name and IP address of the Prisma Access location, and the type of tunnel that has been established. Also shows the MTU size and the volume of data that the agent transmitted and received.
getlogs	Creates a zip package of all local Prisma Access Agent logs.
adem	(Not supported on Prisma Access Agent Linux) Shows the current status of the Autonomous DEM agent (if it is installed on the endpoint).
project	(Not supported on Prisma Access Agent Linux) Allows you to connect to a different project for Dynamic Privilege Access enabled agents. You can enter one of the following options: • **logout**—Log out of the current project. • **login <project_name>**—Log in to a project by specifying the project name. The maximum length for the project name is 32 characters. • **list**—Show the list of projects that the user has access to. For example, to log in or to switch to a project, enter **pacli login my_project**.
traffic	Shows the agent's traffic forwarding rules and the traffic routing logs respectively, such as how traffic is routed for each connection and whether it is through the tunnel or directly to the internet. This command will print the active rules in a tabular format on the command line. You can use the following options:

Command	Description
	• **show**—Show the traffic forwarding rules in a forwarding profile • **show <n>**—Show a specific traffic forwarding rule by specifying the row number • **log**—Show the entries in the network connection (traffic routing) log • **log <n>**—Show a specific row in the network connection log by specifying the row number • **export <filename>**—Export the traffic forwarding rules to a file • **import <filename>**—Import the traffic forwarding rules from a file • **user-location**—Shows the user's currently detected locations, including the detection method (reverse DNS or private IP address match) and which forwarding profile rules apply
switchto	Switches between the Prisma Access Agent and the GlobalProtect app, if both apps are installed on an endpoint. You can enter one of the following options: • **GlobalProtect**—Switches to the GlobalProtect app. Requires the anti-tamper unlock password. • **PrismaAccessAgent**—Switches to the Prisma Access Agent. Switching to an app will automatically disable the previously active app.
wpp	(Windows agents) Enables Prisma Access Agent driver logging using the Windows software trace preprocessor (WPP) (Windows-only). You can **start**, **stop**, or **reset** the software trace preprocessor.
dlp status	(Not supported on Prisma Access Agent Linux) Shows the status for the Endpoint Data Loss Prevention feature.
proxy	(Not supported on Prisma Access Agent Linux) Manages the local proxy functionality. You can use the following options with the command: • **status**—Show the local proxy status • **enable**—Enable the local proxy • **disable**—Disable the local proxy
browser	(Not supported on Prisma Access Agent Linux) Manages the Prisma Access Agent embedded browser. You can use the following options with the command: • **status**—Show the current browser setting

Command	Description
	• **internal**—Set the embedded browser for Prisma Access Agent authentication. • **system**—Set the default system browser for Prisma Access Agent authentication.
eie	(Not supported on Prisma Access Agent Linux) Manages Prisma Access Agent endpoint insights. You can use the following options with the command: • **status**—Show the endpoint insights status • **enable**—Enable endpoint insights • **disable**—Disable endpoint insights • **trigger -d "<description>"**—User issue reporting with description to trigger the collection of diagnostics

Prisma Access Agent for iOS

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

The Prisma Access Agent is an application that operates on your endpoint device (such as a desktop computer, laptop, tablet, or smartphone) to safeguard you by enforcing the same security policies that protect the valuable resources within your corporate network.

Your administrators can deploy your corporate account configuration and Prisma Access Agent settings to the compliant endpoints using mobile device management platforms and you can also download Prisma Access agent to your devices as per your corporate guidelines.

Download and Install the Prisma Access Agent for iOS on Unmanaged Devices

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

Before you can connect to the Prisma Access Agent, you must download and install the app from the App Store.

STEP 1 | Open the App Store.

STEP 2 | **Search** for Prisma Access Agent.

STEP 3 | From the search results, select **Prisma Access Agent**.

STEP 4 | **Install** the app.

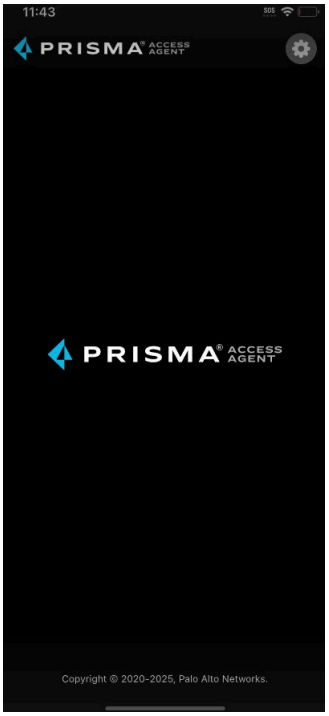
STEP 5 | When prompted, **Sign In** with Apple ID.

Use the Prisma Access Agent App for iOS (Unmanaged Devices)

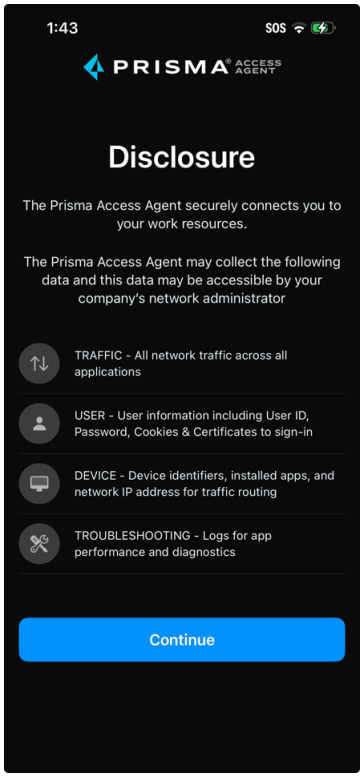
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

To connect the app to the unmanaged devices, you must:

STEP 1 | Open the Prisma Access Agent app by tapping the Prisma Access Agent app icon ( ).

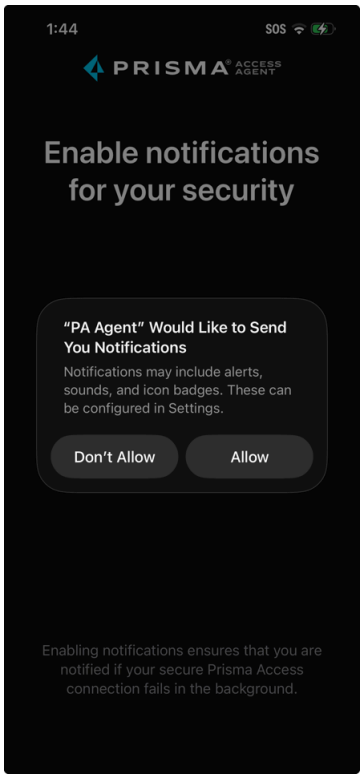


STEP 2 | Read the disclosure about the information Prisma Access Agent may collect or access on your device and click **Continue** to acknowledge and accept the message.

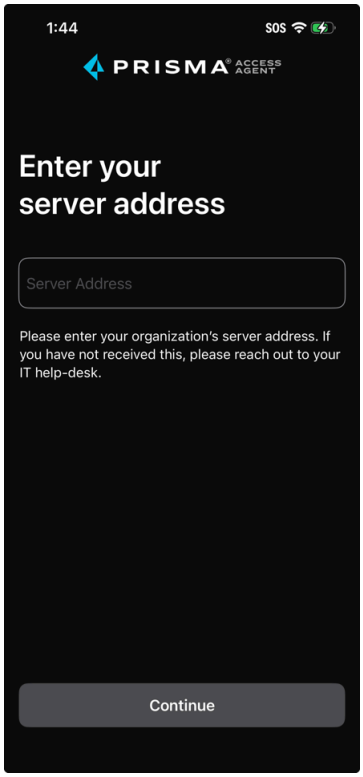


STEP 3 | Enable Prisma Access Agent notifications on your endpoint. A notification permission dialog appears on the app. **Allow** Prisma Access Agent to send you notifications.

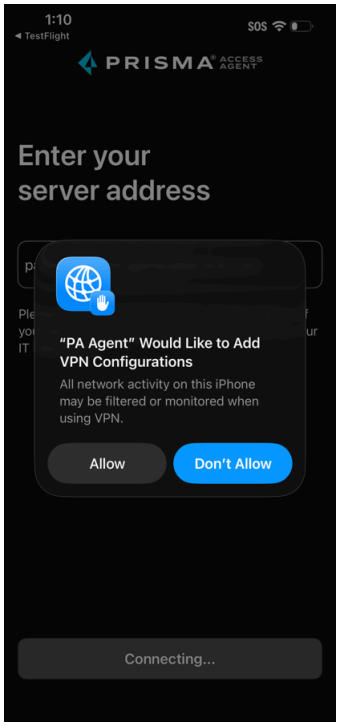
If you **Don't Allow** Prisma Access Agent to send you notifications, you will not receive any alert or notification when you face any issues related to app connectivity.



STEP 4 | Enter the server address that you have obtained from your IT administrator and the connection is initiated automatically.

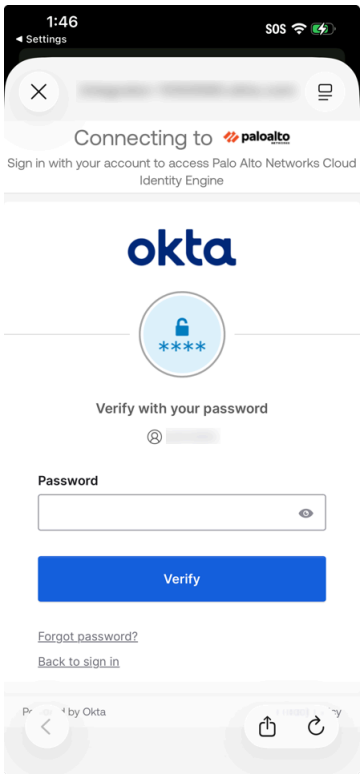


STEP 5 | **Allow** Prisma Access Agent to add the VPN configuration to your endpoint. This setting enables Prisma Access Agent to provide secure access for your device.

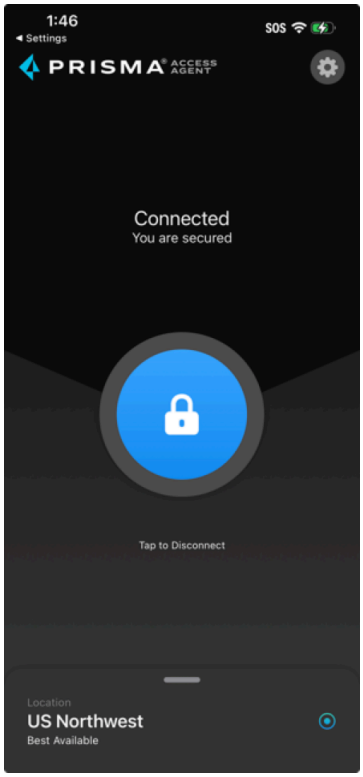


STEP 6 | Enter the credentials that you use to authenticate and access the iOS devices such as password, passcode, biometric credentials and so on. For example, enter the iPhone passcode to authenticate to the device.

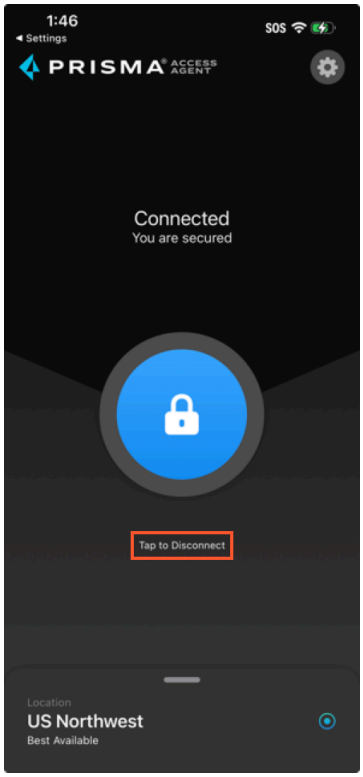
STEP 7 | Enter your organization credentials to authenticate to the app.



After authentication is complete, the connection is established and the app displays the status as **Connected**.



STEP 8 | Tap **Disconnect** on the app when you no longer need to access the resources through Prisma Access Agent.

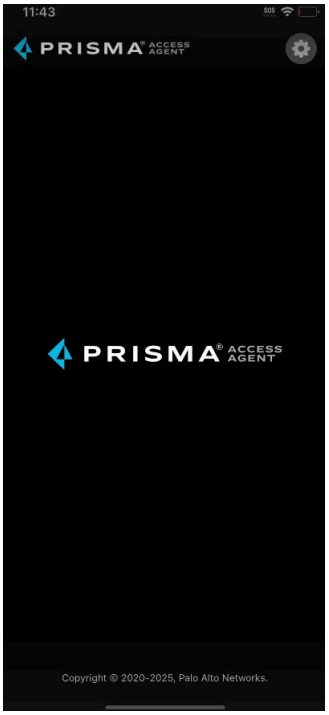


Use the Prisma Access Agent App (Managed Devices) iOS

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

If your iOS endpoint is managed by a mobile device management (MDM) system, your administrator may have automatically pushed the Prisma Access Agent to your endpoint and configured the agent.

STEP 1 | Open the Prisma Access Agent app by tapping the Prisma Access Agent app icon ( ).



STEP 2 | The agent gets connected based on the connect method configured by your Prisma Access Agent administrator. Prisma Access Agent supports the following connect methods:

- **Always-On**

  In an Always-On configuration, Prisma Access Agent automatically connects as soon as you log in.

- **On-Demand**

  In an on-demand configuration, you must manually connect Prisma Access Agent through the application. Traffic is routed through the Prisma Access Agent app only after you initiate and establish the connection.

- **Automatic Configuration**

  - **Per-App**

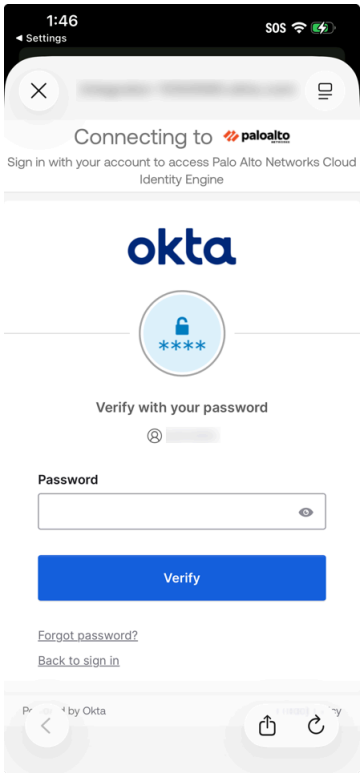
    In a per-app configuration, your administrator can configure the managed apps that will route traffic through Prisma Access Agent. When you access the managed app, Prisma Access Agent will automatically connect and only traffic for the managed apps your administrator has configured under the configuration profile will be routed through Prisma Access Agent.

  - **On-Demand Connect Rules**

    In an on-demand connect rules configuration, while you can manually initiate a connection to the Prisma Access Agent, administrators can also configure Prisma Access Agent to connect automatically when you access a specific domain.

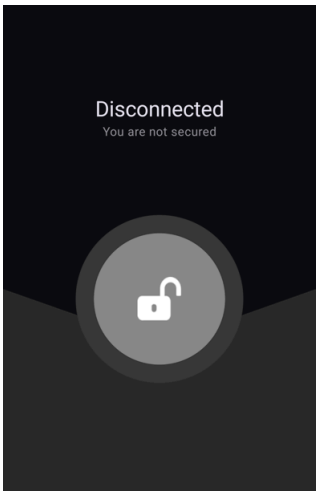
STEP 3 | If your agent is always-on, you'll receive a notification to authenticate with your identity provider.

1. Tap the notification to proceed.
2. Enter your organization credentials to authenticate to the app:

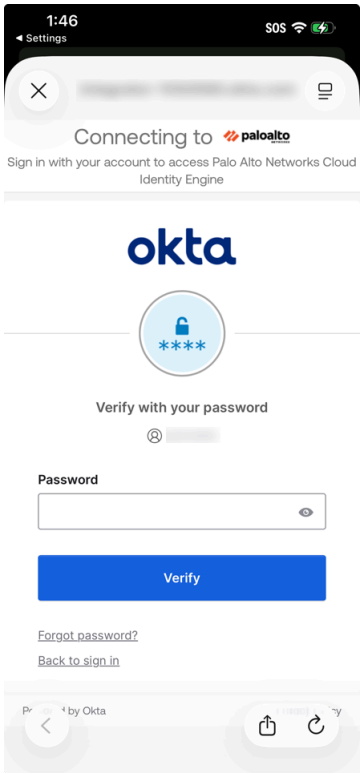


STEP 4 | If your agent is on-demand, manually connect to the agent.

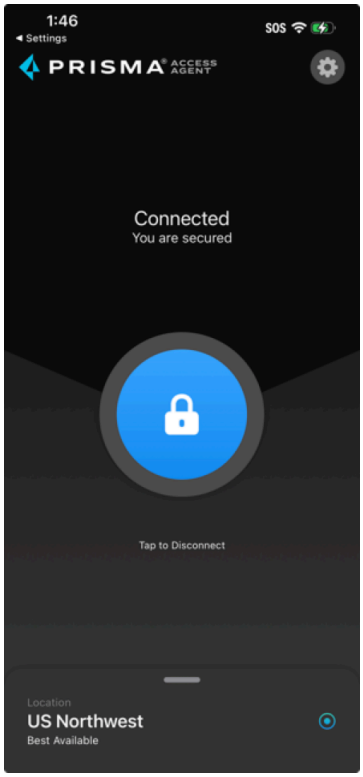
1. Connect by clicking the lock icon.



2. Enter your organization credentials to authenticate to the app:

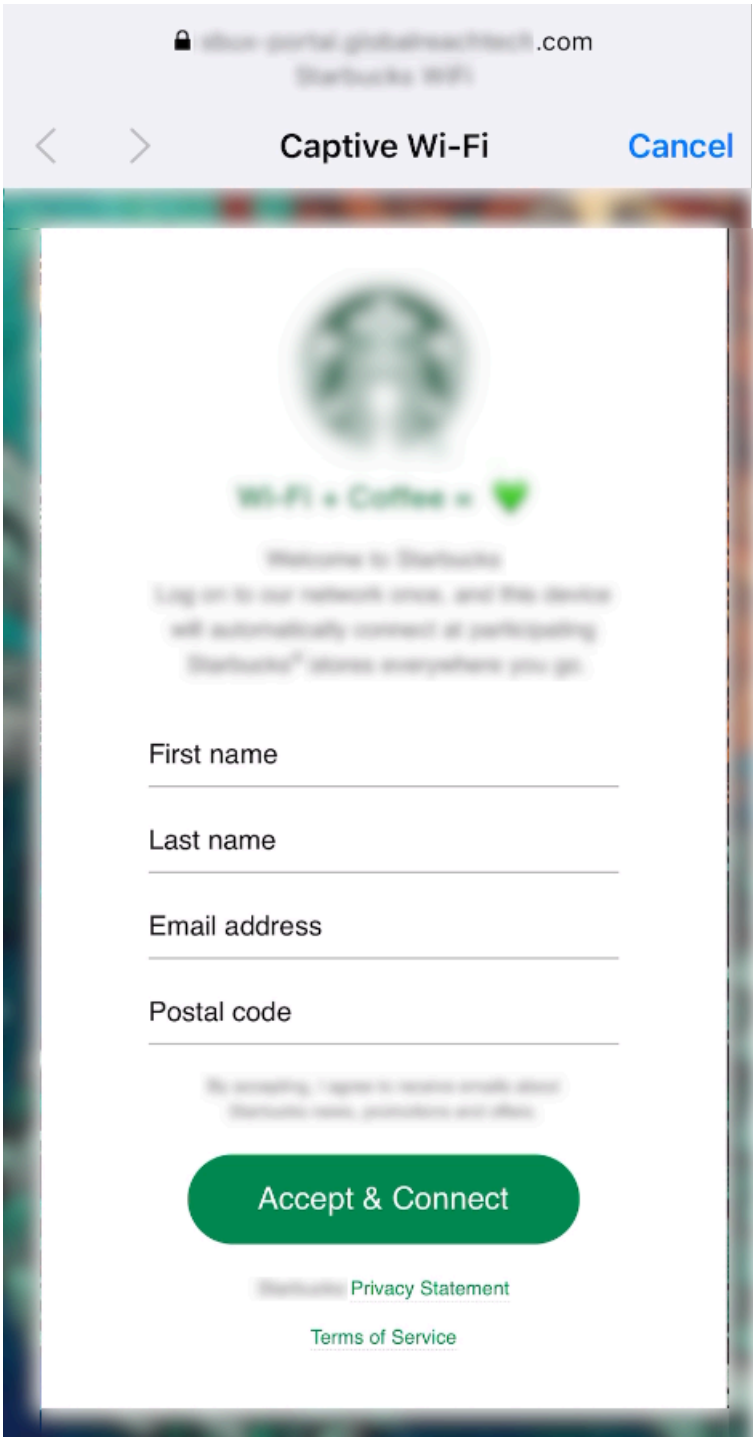


STEP 5 | After authentication is complete, the connection is established and the app displays the status as **Connected**.



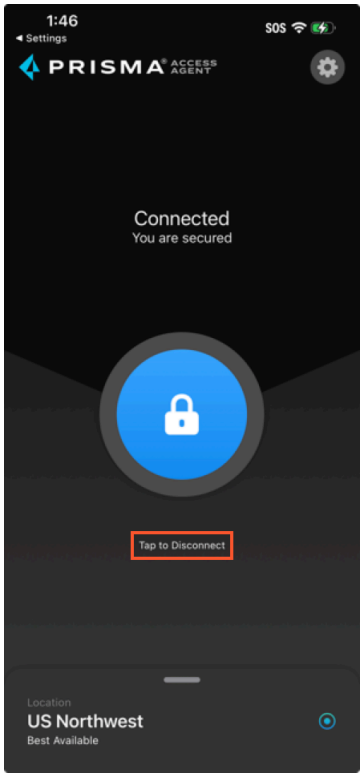
STEP 6 | (Prisma Access Agent 25.7.0) When using Prisma Access Agents configured for per-app deployment, you will receive a notification if you connect to a network that requires captive portal authentication, such as public Wi-Fi at hotels, cafes, or airports.

1. Tap on the notification to proceed.
2. The captive portal login page will appear in the embedded browser. Enter your credentials or accept the terms of service as required by the network provider. For example:

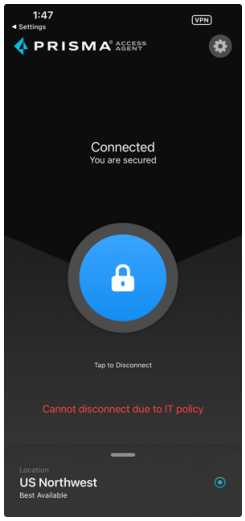


After you connect the app, the app displays the VPN icon on the screen.

STEP 7 | For Prisma Access Agents agents with on-demand or per-app configurations, tap **Disconnect** on the app when you no longer need to access the resources through Prisma Access Agent.



For Prisma Access Agents with always-on configurations, you won't be able to disconnect the agent:



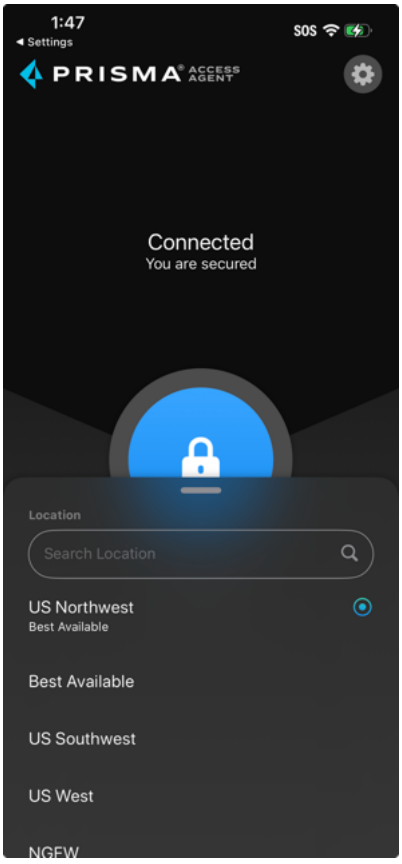
Connect the Prisma Access Agent to a Different Location

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

By default, the endpoint automatically connects to the **Best Available** location based on the configuration that the administrator defines and the response times of the available locations. If your device is located inside your organization's network, the agent is connected automatically to an **Internal** location (if your administrator enabled Internal Host Detection). When your device moves outside of the internal network, the agent will automatically connect to an external location.

To connect to a different location, swipe up the **Location** card at the bottom of the home screen and then use one of the following options:

STEP 1 | Select a location manually from the available list of locations.



STEP 2 | Tap **Best Available** option to force the agent to recalculate and determine the best available location.

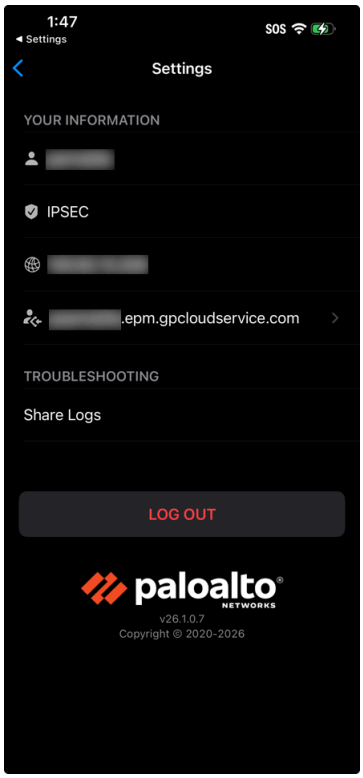
Connect the Prisma Access Agent to a Different Server (Unmanaged Devices)

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

In some cases, you may need to connect to a different server to access a different network. To change the Prisma Access Server

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to **Settings** page by tapping the **Settings** icon to view the connection details.



STEP 3 | Modify the server address.

Server details can only be modified on unmanaged devices. For managed devices, these settings are pre-configured by your administrator and cannot be changed.

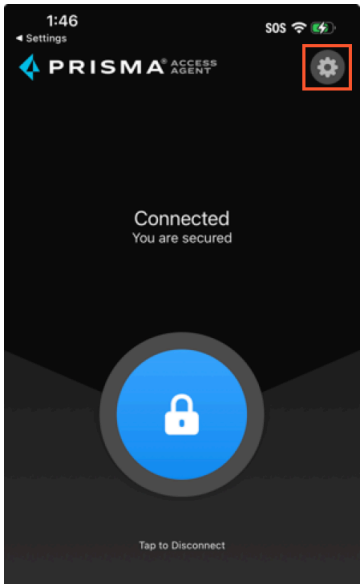
View Prisma Access Agent Settings

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

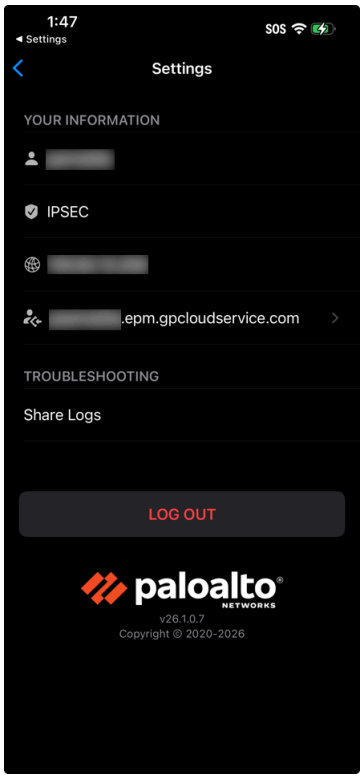
You can view the Prisma Access Agent connection details and troubleshoot any issues on the app settings page.

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to Settings page by tapping the **Settings** icon.



STEP 3 | Review the settings.



STEP 4 | Click the left arrow to dismiss the **Settings**.

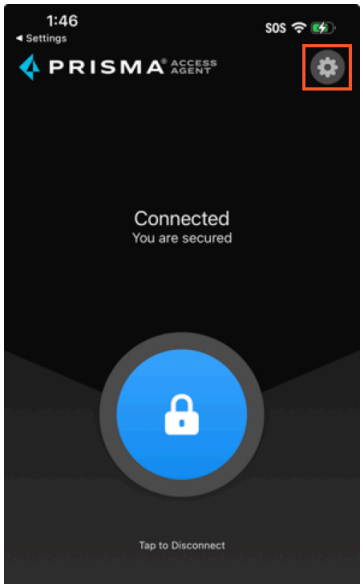
Log Out of the Prisma Access Agent

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

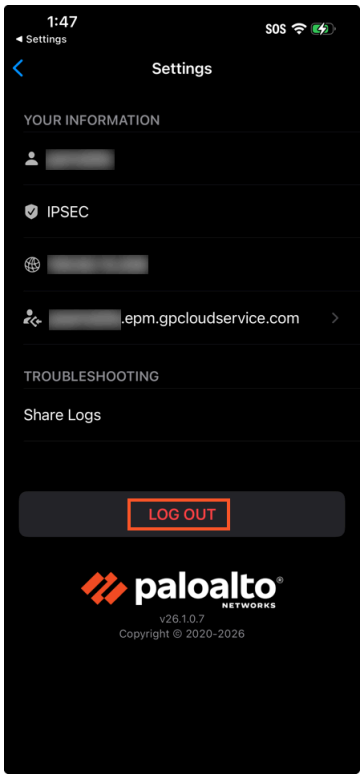
If your administrator has allowed you to sign out, you can do so from the Prisma Access Agent Settings page.

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to Settings page by tapping the **Settings** icon.



STEP 3 | Select **Log Out** from the settings page.



Uninstall the Prisma Access Agent App for iOS

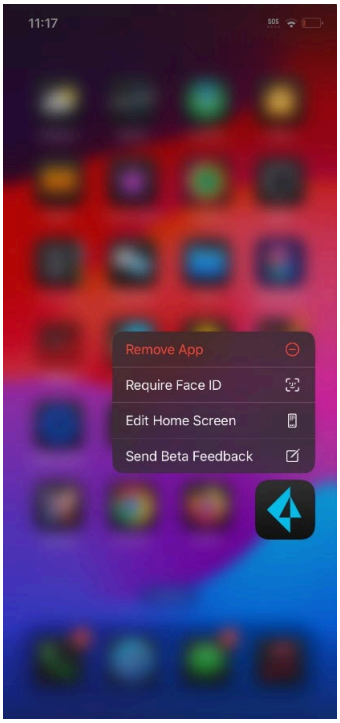
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

To uninstall the Prisma Access Agent from the unmanaged devices:

STEP 1 | Find the **Prisma Access Agent** app icon in your app drawer or on your home screen.

STEP 2 | Tap and hold the **Prisma Access Agent** app icon.

STEP 3 | Select **Remove App** that appears on the screen.



STEP 4 | Confirm the uninstallation.

When you uninstall the app, the VPN profile is also removed.

If your device is managed by an MDM, the ability to uninstall the app might be restricted by your administrator.

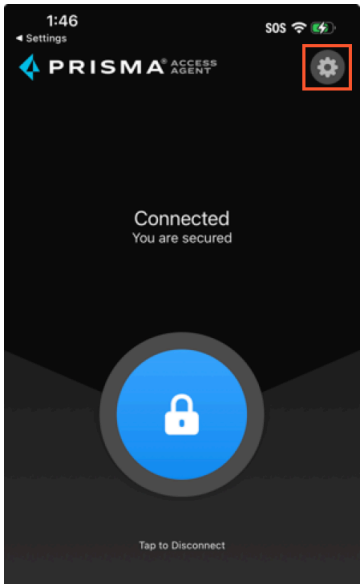
Log Collection and Troubleshooting for iOS

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ iOS 16 and later versions ❑ Internet access

When you experience unusual behavior, you can collect and share logs with your administrator for further troubleshooting

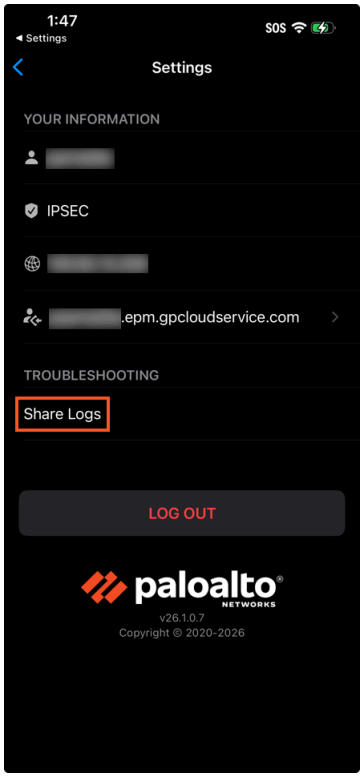
STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to the Settings page by tapping the **Settings** icon.

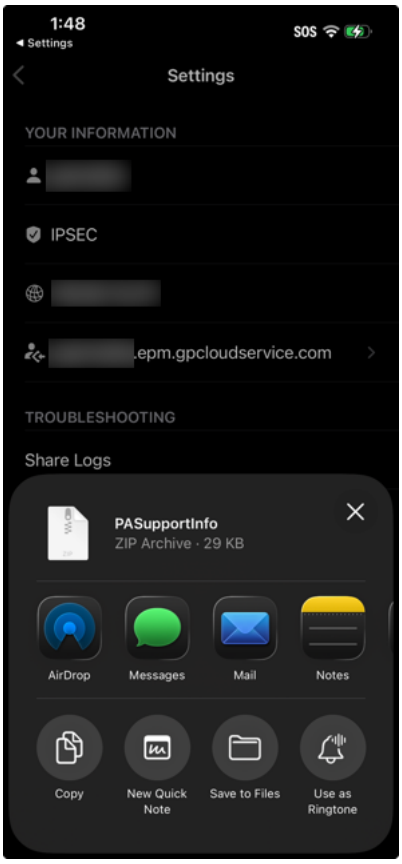


STEP 3 | View connection statistics to see more information to help with troubleshooting.

STEP 4 | Under **Logs**, select **Share Logs** and click **Download** to download the log files locally to your device.



STEP 5 | You can share the logs with your administrators using mail or other preferred apps.



Prisma Access Agent for Android

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

The Prisma Access Agent is an application that operates on your endpoint device (such as a desktop computer, laptop, tablet, or smartphone) to safeguard you by enforcing the same security policies that protect the valuable resources within your corporate network.

Your administrators can deploy your corporate account configuration and Prisma Access Agent settings to compliant endpoints using mobile device management (MDM) platforms. You can also download the Prisma Access Agent to your devices as per your corporate guidelines

Download and Install the Agent (Unmanaged Devices)

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

Before you can connect to the Prisma Access Agent, you must download and install the app from the Google Play Store.

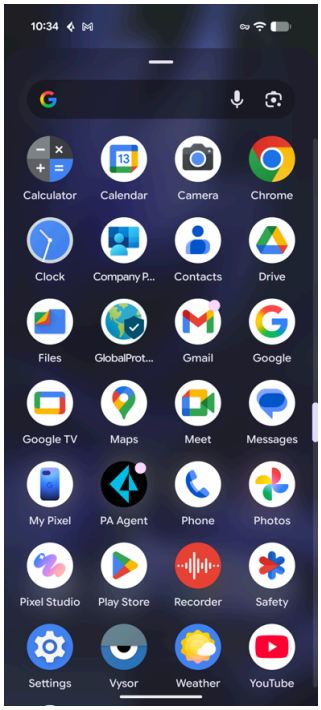
STEP 1 | Open the **Google Play Store** app on your Android device.

STEP 2 | From the search results, select **Prisma Access Agent**.

STEP 3 | **Install** the app.

STEP 4 | When prompted, review and **Accept** the information for which Prisma Access Agent needs access.

Once installed, you can find the app icon on your home screen or in your app drawer.



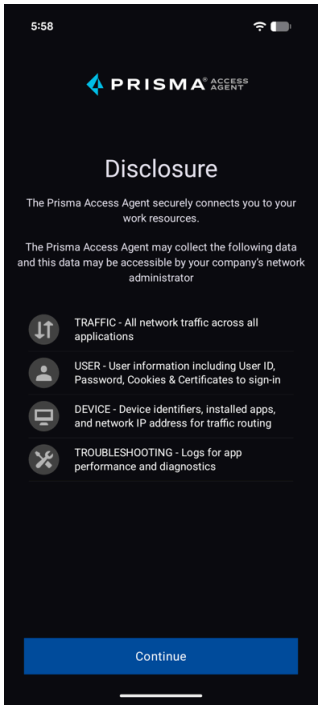
Use the Prisma Access Agent App (Unmanaged Devices)

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

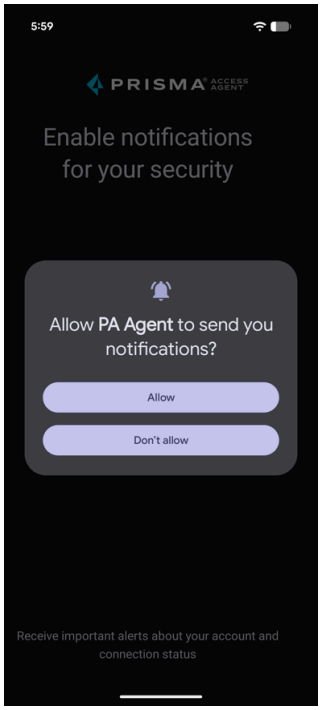
To connect the app on unmanaged devices, you must:

STEP 1 | Open the Prisma Access Agent app by tapping the **PA Agent** icon.

STEP 2 | Read the disclosure about the information the Prisma Access Agent may collect or access on your device. Tap **Continue** to acknowledge and accept the message.

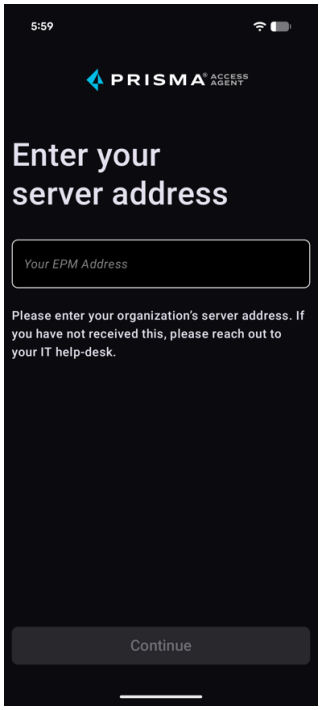


STEP 3 | Enable Prisma Access Agent notifications on your endpoint. A notification permission dialog will appear. Tap **Allow** for the Prisma Access Agent to send you notifications.



If you select **Don't Allow**, you will not receive alerts or notifications regarding app connectivity issues.

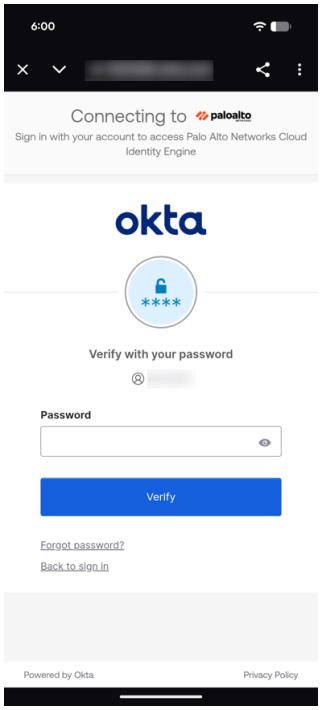
STEP 4 | Enter the **server address** that you have obtained from your IT administrator. The connection is initiated automatically after entering the address.



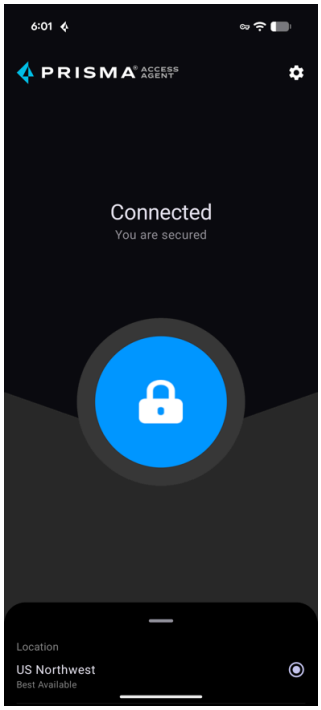
STEP 5 | **Allow** the Prisma Access Agent to add VPN configurations to your endpoint. A system prompt will appear requesting permission to set up a VPN connection. Tap **Allow**. This setting enables the Prisma Access Agent to provide secure access for your device.

STEP 6 | If prompted by the Android device, enter the credentials that you use to authenticate and access your Android device (such as your PIN, pattern, password, or biometric credentials like fingerprint or face unlock).

STEP 7 | Enter your **organization credentials** (username and password, and any multi-factor authentication prompts) to authenticate to the app and to your corporate network.



After authentication is complete, the connection will be established, and the app will display the status as **Connected**.



STEP 8 | After you connect the app, the app typically displays a **VPN icon** in the Android status bar at the top of your screen.

STEP 9 | Tap **Disconnect** on the app when you no longer need to access resources through the Prisma Access Agent.

Use the Prisma Access Agent App (Managed Devices)

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

If your Android endpoint is managed by a mobile device management (MDM) system, your administrator may have automatically pushed the Prisma Access Agent to your endpoint and configured the agent.

STEP 1 | Open the Prisma Access Agent app by tapping the **PA Agent** icon.

STEP 2 | The agent will connect based on the connect method configured by your Prisma Access Agent administrator. The Prisma Access Agent supports the following connect methods:

- **Always-On**

  In an Always-On configuration, Prisma Access Agent automatically connects as soon as end users log in. You can optionally enable Lockdown Mode to enforce all network traffic through the Prisma Access Agent and block traffic that does not go through the Prisma Access Agent.

- **On-Demand**

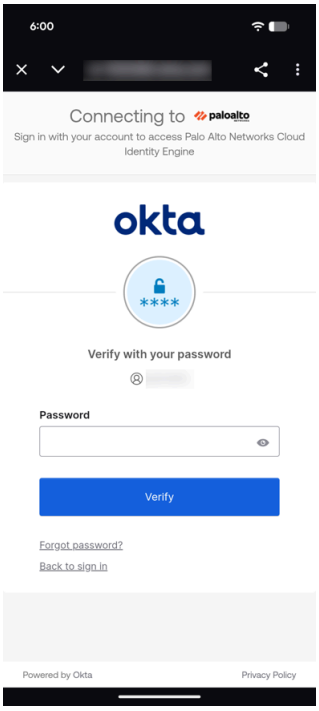
  In an on-demand configuration, end users must manually connect Prisma Access Agent through the application. Traffic is routed through the Prisma Access Agent app only after the end users initiate and establish the connection.

- **Per-App**

  In a per-app configuration, you can specify the managed apps that can route traffic through Prisma Access Agent when connected. If using an allowlist, only the specified apps will be routed through Prisma Access Agent. If using a blocklist, all traffic will be routed through Prisma Access Agent except for the specified apps.

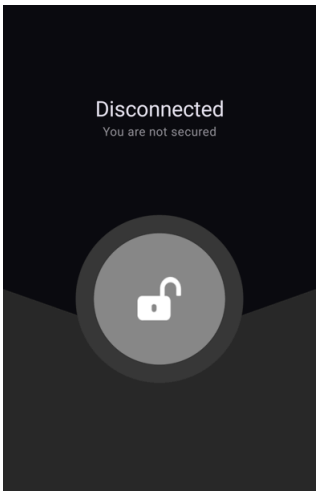
STEP 3 | If your agent is always-on, you'll receive a notification to authenticate with your identity provider.

1. Tap the notification to proceed.
2. Enter your organization credentials to authenticate to the app:

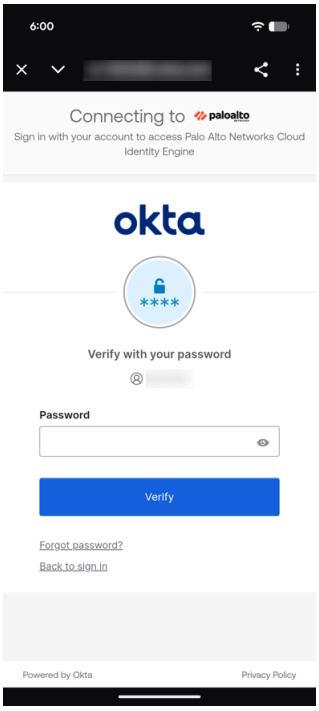


STEP 4 | If your agent is on-demand, manually connect to the agent.

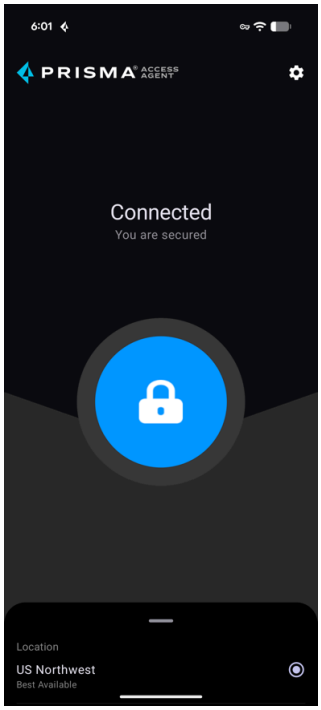
1. Connect by clicking the lock icon.



2. Enter your organization credentials to authenticate to the app:



STEP 5 | After authentication is complete, the connection is established and the app displays the status as **Connected**.



STEP 6 | For Prisma Access Agents agents with on-demand or per-app configurations, tap **Disconnect** on the app when you no longer need to access resources through the Prisma Access Agent.

For Prisma Access Agents with always-on configurations, you won't be able to disconnect the agent due to your organization's IT policy.

STEP 7 | If you connect to a network that requires captive portal authentication, such as public Wi-Fi at hotels, cafes, or airports, you will receive a notification.

1. Tap on the notification to proceed.
2. The captive portal login page will appear in the embedded browser. Enter your credentials or accept the terms of service as required by the network provider.

Connect the Prisma Access Agent to a Different Location

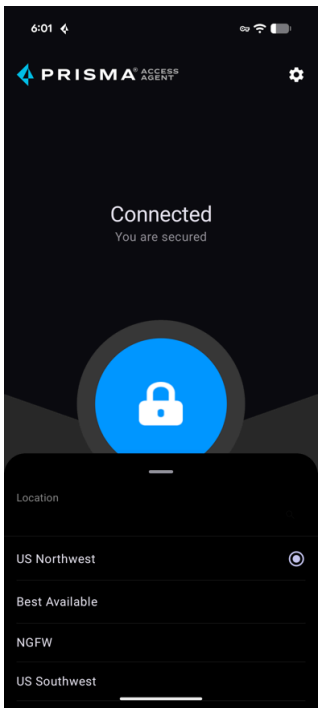
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

By default, the endpoint automatically connects to the **Best Available** location based on the configuration that the administrator defines and the response times of the available locations. To connect to a different location, swipe up the **Location** card at the bottom of the home screen and then use one of the following options:

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Use one of the following options to connect to a different location:

- Select a location manually from the available list of locations.
- Tap a **Best Available** option to force the agent to recalculate and determine the best available location



Connect the Prisma Access Agent to a Different Server for (Unmanaged Devices)

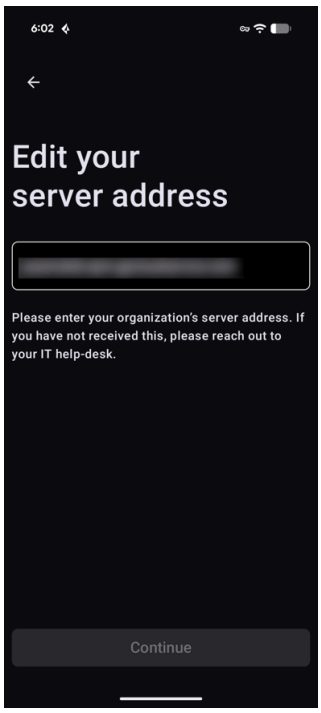
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

In some cases, you may need to connect to a different server to access a different network. To change the Prisma Access Server:

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to the **Settings** page by tapping the Settings icon.

STEP 3 | Modify the server address to the new one provided by your administrator.



Server details can only be modified on unmanaged devices. For managed devices, these settings are pre-configured by your administrator and cannot be changed.

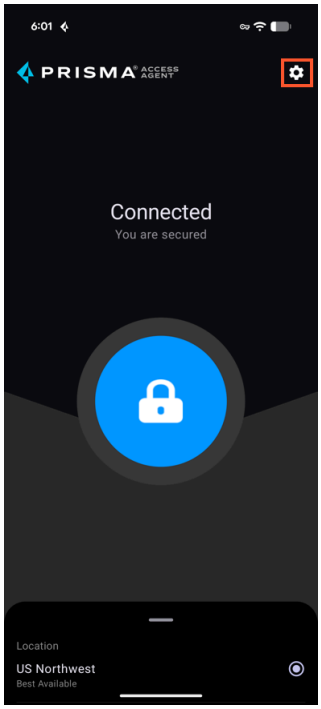
View Prisma Access Agent Settings

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

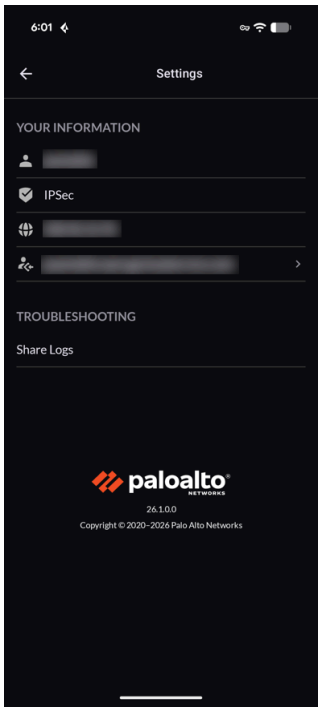
You can view Prisma Access Agent connection details and access troubleshooting options on the app's settings page.

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to the **Settings** page by tapping the Settings icon.



STEP 3 | You can find connection status, gateway information, and other relevant details on the page.



STEP 4 | Click the left arrow to dismiss the **Settings**.

Log Out of the Prisma Access Agent

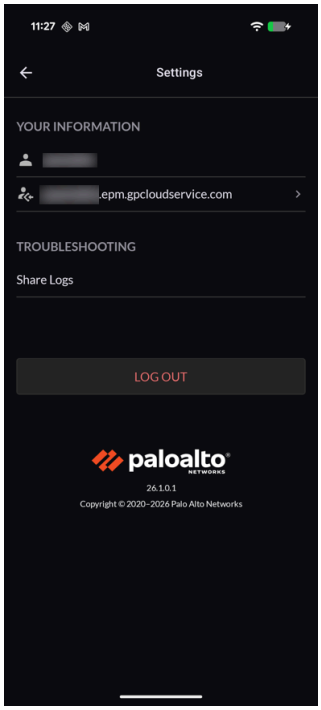
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

If your administrator has allowed you to sign out, you can:

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to the **Settings** page by tapping the Settings icon

STEP 3 | Tap **Log Out**.



Uninstall the Prisma Access Agent App for Android

Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

To uninstall the Prisma Access Agent from the unmanaged devices:

STEP 1 | Find the **Prisma Access Agent** app icon in your app drawer or on your home screen.

STEP 2 | Tap and hold the **Prisma Access Agent** app icon.

STEP 3 | Drag it to an **Uninstall** that appears on the screen, or select Uninstall from the context menu that pops up.

STEP 4 | Confirm the uninstallation.

When you uninstall the app, the VPN profile is also removed.

If your device is managed by an MDM, the ability to uninstall the app might be restricted by your administrator.

Alternatively:

1. Launch the **Settings**app.
2. Navigate to **Apps**.
3. Find and select the **Prisma Access Agent** app from the list.
4. Tap **Uninstall**.
5. Confirm the uninstallation.

Log Collection and Troubleshooting

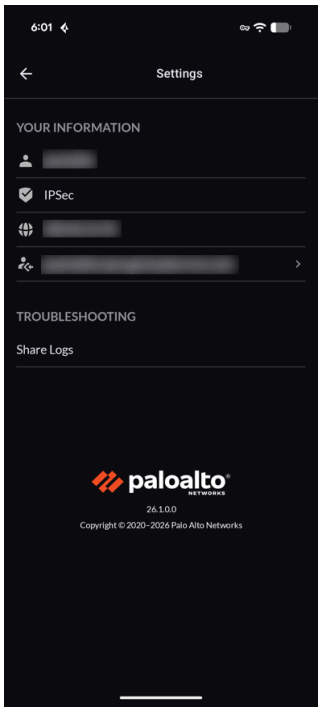
Where Can I Use This?	What Do I Need?
• Prisma Access Agent	❑ Android 10 and later versions ❑ Internet access

When you experience unusual behavior, you can collect and share logs with your administrator for further troubleshooting

STEP 1 | Open the Prisma Access Agent app.

STEP 2 | Go to the Settings page by tapping the Settings icon.

STEP 3 | View connection statistics to see more information to help with troubleshooting.



STEP 4 | Under **Troubleshooting**, select **Share Logs** and click **Download** to download the log files locally to your device. You can share the logs with your administrators using mail or other preferred apps.