



TECHDOCS

Okyo Garde with Prisma Access

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support.html

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

©2021–2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

May 12, 2022

Table of Contents

.....

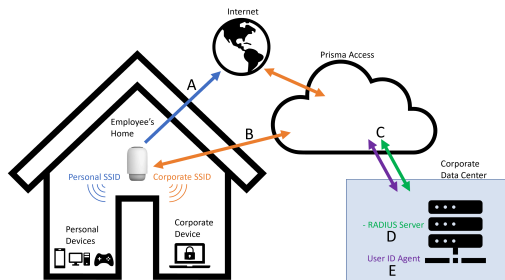
| | |
|--|-----------|
| Prepare to Use Okyo Garde with Prisma Access..... | 5 |
| Under the Hood of Okyo Garde with Prisma Access..... | 6 |
| Getting Started..... | 9 |
| Get Started with Okyo Garde..... | 10 |
| Basics..... | 11 |
| About Okyo Garde..... | 12 |
| Okyo Mobile App..... | 16 |
| Okyo Garde with Prisma Access..... | 16 |
| First Look at Okyo Garde with Prisma Access..... | 17 |
| The Employee Experience..... | 18 |
| Onboarding..... | 18 |
| Things Employees can do with Okyo Garde..... | 22 |
| Contact Okyo Customer Support..... | 24 |
| Network Settings..... | 25 |
| Set up SSO for Okyo Garde Users..... | 26 |
| Obtain your IdP Authentication information..... | 26 |
| Add your IdP Authentication Information to Okyo..... | 31 |
| Provide your Okyo Authentication Information to your IdP..... | 32 |
| Assign Users to your Application..... | 35 |
| Your Network Settings at a Glance..... | 38 |
| Set Up your Corporate Network Access Point..... | 39 |
| Set Up RADIUS Authentication for Okyo Garde..... | 40 |
| Configure Network Address Translation..... | 41 |
| Route Trusted Traffic Directly Through the Internet (Split Tunneling)..... | 42 |
| Company Settings..... | 43 |
| Your Company Settings at a Glance..... | 44 |
| Change your Company's Okyo Garde Info..... | 45 |
| Change your Company's Logo in Okyo Garde..... | 46 |
| Customize Okyo Welcome Email..... | 47 |
| Customize Okyo Mesh Node Assignment Email..... | 48 |
| Customize Okyo Subscription Removal Confirmation..... | 50 |
| Policy Management..... | 51 |
| Manage Security Policy and Profiles for Okyo Garde..... | 52 |

| | |
|--|-----------|
| Cloud Managed Prisma Access Deployments..... | 52 |
| Panorama Managed Prisma Access Deployments..... | 53 |
| Push Policy Updates to Prisma Access..... | 55 |
| Push from Cloud Managed Prisma Access..... | 55 |
| Push from Panorama Managed Prisma Access..... | 55 |
| Manage Employees..... | 57 |
| View Okyo Garde Employee Details..... | 58 |
| Add Employees to Okyo Garde with Prisma Access..... | 61 |
| Bulk Add Employees from a CSV File..... | 61 |
| Add Employees One at a Time..... | 61 |
| Edit Okyo Garde Employee Info..... | 63 |
| Remove Okyo Garde Employees..... | 64 |
| Manage Subscriptions..... | 65 |
| Assign Okyo Garde Subscriptions to Users..... | 66 |
| Add Okyo Garde Mesh Subscriptions to Existing Subscriptions..... | 67 |
| Remove Okyo Garde Subscriptions..... | 68 |
| Monitor Okyo Garde at a Glance..... | 69 |
| Okyo Garde Overview..... | 70 |
| Okyo Garde Dashboard in Insights..... | 72 |

Prepare to Use Okyo Garde with Prisma Access

Okyo needs unencumbered open lines of communication to work with Prisma Access. So, before using Okyo with Prisma Access, you'll need to make sure your RADIUS policy, firewall policy, and user ID mappings allow the traffic Okyo Garde needs to function properly. Let's have a look under the hood of Okyo Garde and make sure we're ready to roll!

Under the Hood of Okyo Garde with Prisma Access



A) Personal network segment

When users set it up, Okyo Garde broadcasts a personal network SSID. Personal devices on this network connect to the internet through the Okyo Garde router.

B) Corporate network segment

Okyo Garde broadcasts a corporate network segment. When NAT ([Network Address Translation](#)) is enabled, corporate devices on this network get a 100.64.x.x IP address from Prisma Access and connect to the internet through Prisma Access. When NAT is not enabled, you'll need to configure a custom client IP pool. In either case, standard security policies are enforced for traffic on this network.

C) Prisma Access side device authentication

Your security policy must allow authentication traffic from managed corporate devices to the RADIUS server to authenticate successfully. Create an explicit [policy](#) rule that allows traffic from IP addresses assigned to Okyo routers by Prisma Access to accomplish this.

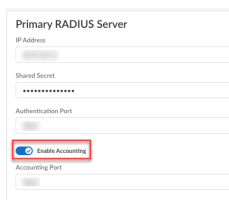
D) RADIUS-side device authentication

Prisma Access uses RADIUS servers (such as Aruba ClearPass or Cisco Identity Services Engine) to authenticate devices and allow them to connect to the corporate network segment. So, it's important to allow communication with the RADIUS server. You can do this by:

1. Establishing a service connection from PA to the data center hosting the RADIUS server so that authentication requests can flow through.
2. Adding the Okyo infrastructure subnet as a trusted RADIUS supplicant for the RADIUS server.

E) Additionally, in cases where user-ID based policies are in use:

- **RADIUS learns the user ID mappings** for the corporate network segment through RADIUS accounting. To achieve this, first **Enable Accounting** for all RADIUS servers in **Okyo Garde RADIUS settings**.



The image shows a configuration form for a 'Primary RADIUS Server'. The form includes fields for 'IP Address', 'Shared Secret', 'Authentication Port', and 'Accounting Port'. The 'Enable Accounting' checkbox is checked and highlighted with a red box.

Then, to teach the user ID agent the proper mappings, follow these steps:

1. Configure your RADIUS server to send RADIUS accounting as syslog messages.
 2. Ensure that there is a predefined Syslog Parse profile for your particular syslog senders. Alternatively, you could create a custom Syslog Parse profile.
 3. Specify which syslog senders the firewall should monitor.
 4. Enable syslog listener services on the interface that the firewall uses to collect user mappings.
- **Prisma Access redistributes UID information.**

Getting Started

Use Okyo Garde with Prisma Access to add employees, to assign Okyo Garde subscriptions to employees, to monitor usage, and to view details about Okyo Garde routers and mesh nodes in your organization. Now that you've got the keys to Okyo Garde, let's take it for a spin!

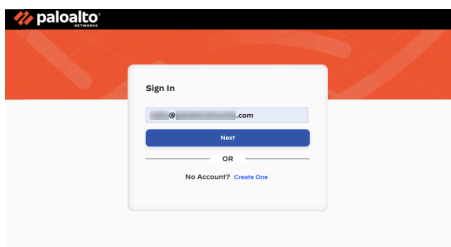
Get Started with Okyo Garde

To use Okyo Garde with Prisma Access for the first time, follow these steps:

STEP 1 | Click the link in the email we sent you.

STEP 2 | If you don't already have a Palo Alto Networks Support account, you will be prompted to set up your account password. Follow the onscreen instructions.

After you set up your password, you will be redirected to the Prisma Access login page.



Take your [First Look at Okyo Garde with Prisma Access](#) for information about how to navigate the subscription manager. If this is your first time using Prisma Access, be sure you follow the prerequisite steps to enable mobile users to access the corporate resources in your organization for either [Cloud Managed](#) or [Panorama Managed](#) Prisma Access.

STEP 3 | Start managing your Okyo Garde subscriptions:

- ❑ [Set up SSO](#) so that employees to whom you assign device subscriptions can log in and use Okyo Garde.
- ❑ Configure your [network settings](#) and [company settings](#), and [customize the welcome email](#) that employees receive when you assign subscriptions to them.
- ❑ [Add employees](#). You need to do this before you assign subscriptions.
- ❑ Assign [Okyo Garde](#) and [Okyo Garde mesh](#) subscriptions to employees.
- ❑ Manage your [Okyo \(and GlobalProtect\) policy](#).
- ❑ View details about [Okyo Garde devices and subscriptions](#) in your organization.

Basics

Learn the basics of Okyo Garde and the Okyo subscription manager.

- > [About Okyo Garde](#)
- > [First Look at Okyo Garde with Prisma Access](#)
- > [The Employee Experience](#)
- > [Contact Okyo Customer Support](#)

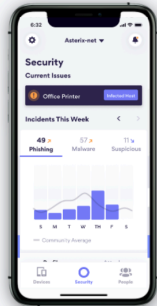
About Okyo Garde

Okyo Garde is a network security solution that's neatly packaged to be deployed in employees' homes to support work-from-home (WFH) use cases. While both Cloud Managed and Panorama Managed Prisma Access deployments support Okyo Garde, Panorama administrators need to go to the Cloud Managed Prisma Access app to manage the Okyo inventory and assign Okyo subscriptions to employees. Okyo Garde is available as a subscription service and includes:

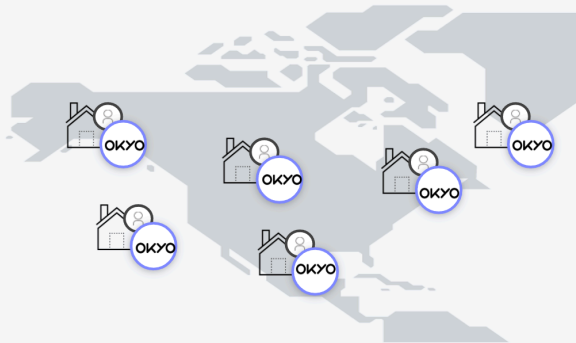
| For Employees | For Administrators |
|---|--|
| <ul style="list-style-type: none">• Okyo Mobile app• Okyo Garde device with security stack that pairs or replaces existing home router | <ul style="list-style-type: none">• Okyo Garde with Prisma Access• Global Standard Customer Success and Support |

Seamlessly secure and manage work-from-home workforce at scale

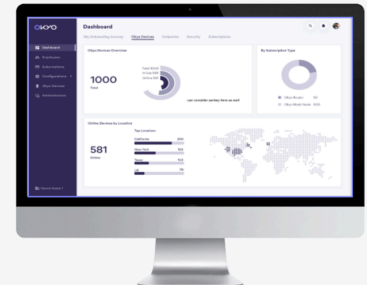
Employee Experience



Simple set-up and intuitive end-user experience via Okyo Gardé mobile app



IT Admin Experience

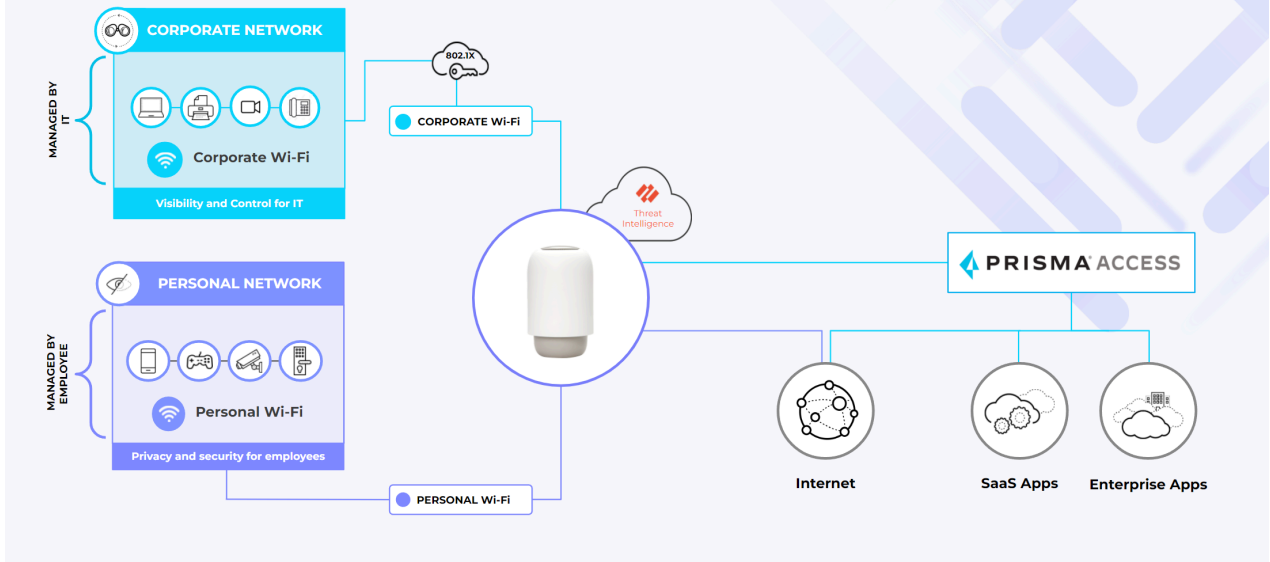


Centralized orchestration and management via Prisma Access cloud-based console

Enterprises can now offer their employees the same Palo Alto Networks security technologies that they trust to secure their campus networks. Employees can set up and manage Okyo Gardé for

security across all connected home devices. A safe home network with smart device segmentation that recognizes and restricts devices based on type and profile association assures a unified and secure work-from-home experience for all employees. Employees first set up the corporate access point and connect their authorized work devices to it. After that, they can create their own personal network (SSID) to connect their personal and IoT devices to. The employee's personal network is private because the employees organization has no visibility into any network activity, and can't enforce security on any network traffic on the employee's personal network.

Delivers Security and Segmentation to the Whole Home



In case you're wondering, Okyo Garde supports English, French, German, and Japanese on Prisma Access, and 18 languages in the Okyo Mobile app to provide a localized experience for both administrators and employees.

- [Okyo Mobile App](#)
- [Okyo Garde with Prisma Access](#)

Okyo Mobile App

The Okyo Mobile app is designed for simplicity and ease of use for the remote workforce. An interactive wizard for digital onboarding provides a fast and frictionless setup for employees.

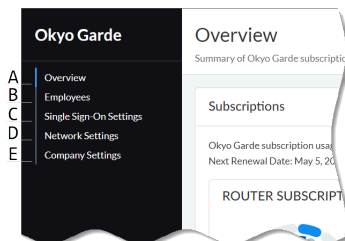
Employees can receive notifications about activity and security incidents on their personal network so that they can take action to block access to suspicious URLs and IP addresses. It can further quarantine a compromised device and isolate it from the network. The Okyo Mobile app also lets parents set time limits, schedule pauses, filter content, and block ads, for a safer digital experience for children. Employees can also get corporate network status updates and info about devices connected to the corporate SSID.

Okyo Garde with Prisma Access

Okyo Garde is a secure web portal for the administrator to centrally manage employees and subscriptions, and to monitor the fleet of Okyo Garde routers and mesh nodes in your organization. See [Getting Started](#).

First Look at Okyo Garde with Prisma Access

When you access Okyo Garde with Prisma Access, the first thing you see is the Overview. You can then use the following tabs to manage employees and subscriptions and manage settings. Use the sidebar navigation to move between screens.



A) Overview

View [Okyo Garde subscriptions](#) for your company.

B) Employees

View and manage [users](#), [Okyo Garde devices](#), and [subscriptions](#). Also, check system and configuration logs.

C) Single Sign-On Settings

Set up [SSO for users](#).

D) Network Settings

View and configure settings for [Corporate Network](#), [RADIUS authentication](#), and [Split Tunneling \(Direct Internet Access\)](#).

E) Company Settings

View and manage your [company-specific configurations](#).

The Employee Experience

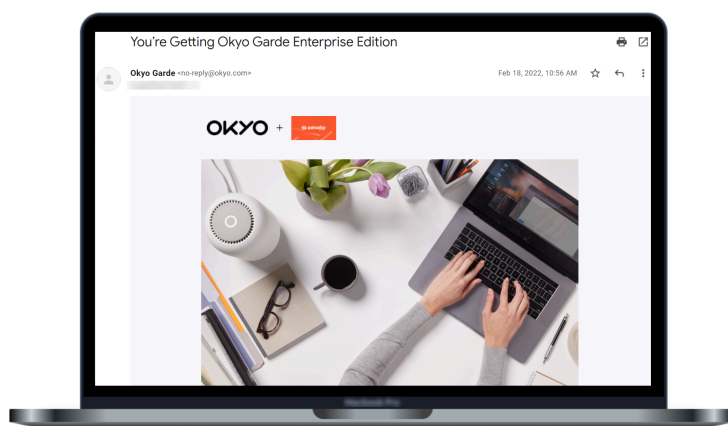
Understanding what employees get out of Okyo Garde will give you some context for your role as an administrator. An employee—let's call her Harrah—starts with the onboarding process, and then secures her home network with Okyo Garde.

Onboarding

Employee onboarding is usually a four-part process. To get started, Harrah needs to complete the following steps.

STEP 1 | Learn about Okyo Garde.

1. Harrah receives a [welcome email](#).

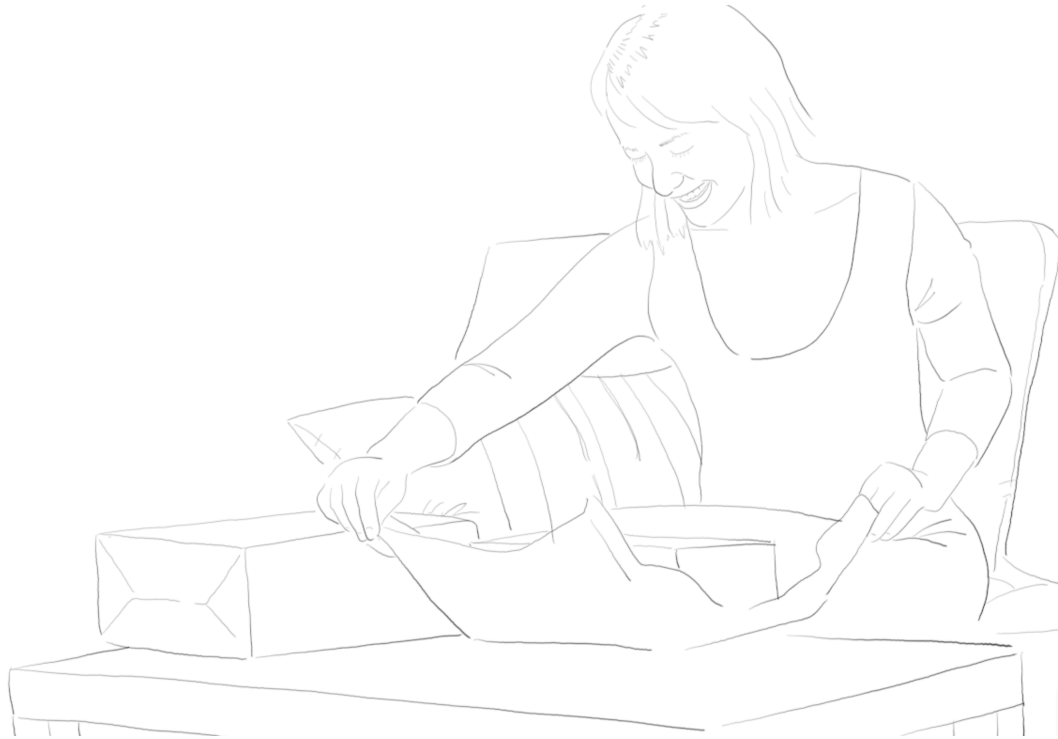


The welcome email is generated automatically when you [assign Harrah an Okyo Garde subscription](#).

2. Harrah follows instructions in the email from Palo Alto Networks to get the Okyo Garde router. She downloads the Okyo Mobile app while she waits for the router to arrive.

STEP 2 | Unbox Okyo Garde

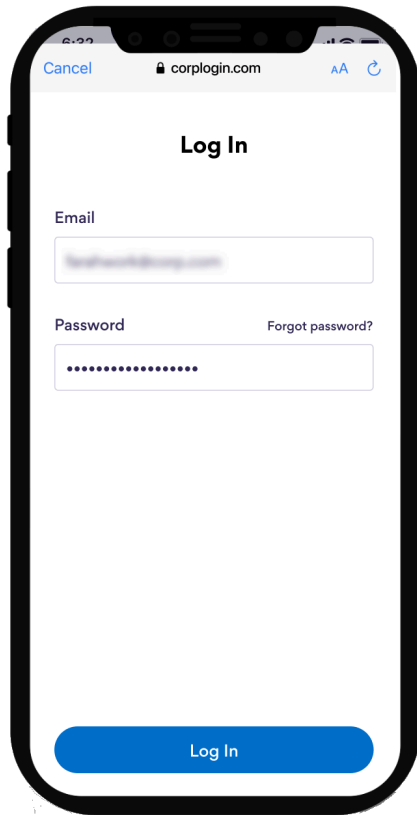
1. Harrah's Okyo Garde router arrives at her home.
2. Harrah unboxes the device and follows the instructions in the app to set up the corporate network.



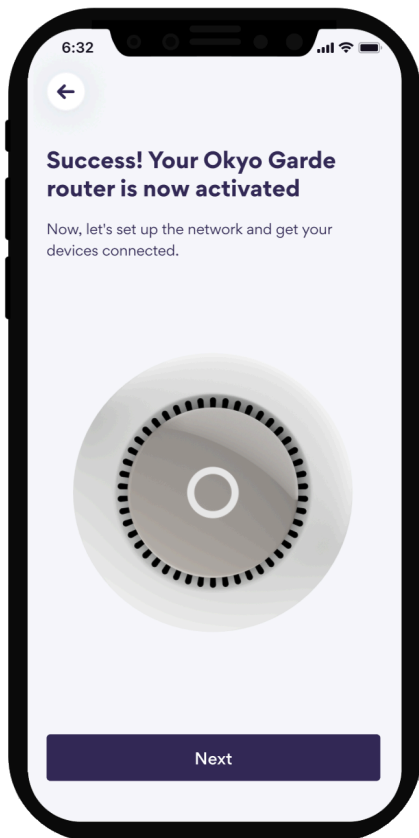
STEP 3 | Set up corporate network

1. Harrah logs in to the Okyo Mobile app.

You've already [set up SSO](#) for her using Okyo Garde with Prisma Access ahead of time.



2. Harrah scans the QR code on her Okyo Garde router, and then plugs it in.
Her Okyo Garde router is activated.



If any updates are available, they're installed, and the corporate network is set up automatically. She repeats this step for any mesh nodes she's been assigned. She'll be able to connect her company computer and work devices and access company resources using this corporate network.

STEP 4 | Set up personal network

1. Although it's optional, Harrah taps **Add Home Protection** in the app and follows the onscreen instructions for setting up a personal network to get more secure Wi-Fi in her home that protects her entire household.

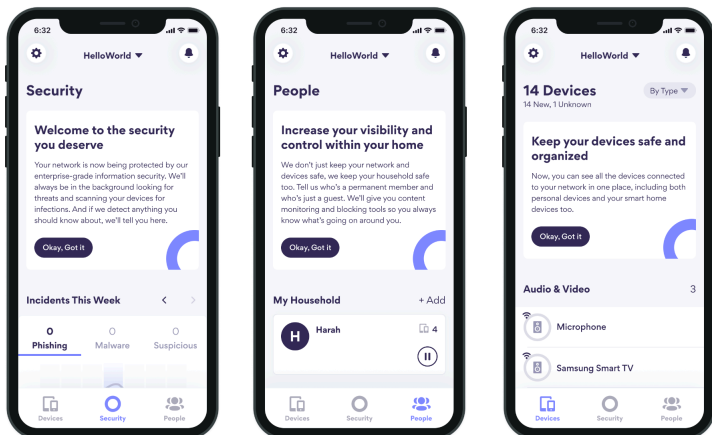
It's private and completely separate from her work network, so she's in control. Harrah can connect her personal and IoT devices to this network and monitor them using the Okyo Mobile app.

Things Employees can do with Okyo Garde

To secure her personal network, Harrah can:

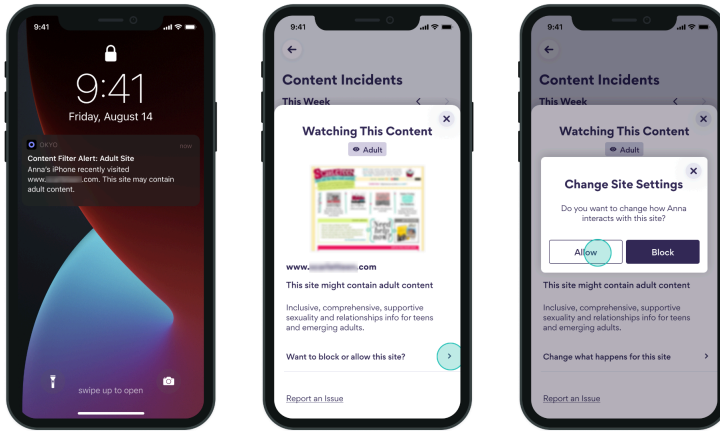
- **Monitor and manage people and devices**

Harrah sees devices on her home network, assigns devices to profiles for people in her household who use those devices, and blocks devices that don't belong on her network. She can even pause the internet for all devices assigned to an individual or for all devices on a specific profile.



- **Manage security settings**

Harrah sets content filters by category, blocks individual websites, and receives notifications when someone attempts to access restricted content. She's even notified when Okyo Garde prevents security incidents she hadn't planned for, such as phishing and malware attacks.



Contact Okyo Customer Support

Need to get in touch?

Before you contact Okyo Support, try searching this guide and our online library of [documentation](#) to find helpful information related to your issue.

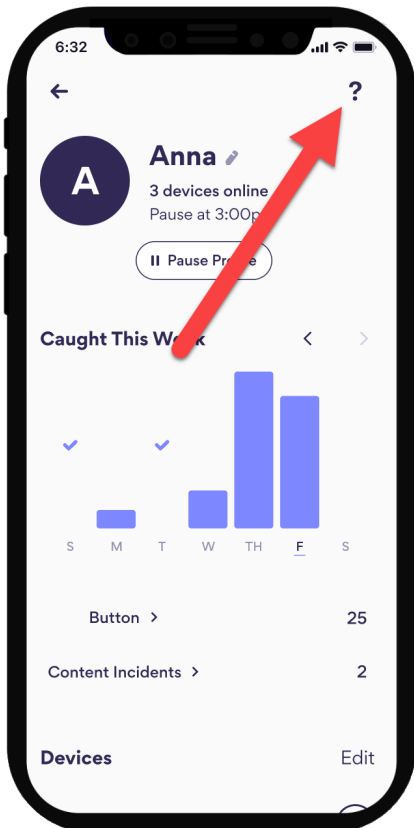
Still can't find the answers you're looking for? We've got you covered.

Are you a Prisma Access administrator who needs help using Okyo Garde with Prisma Access?

Visit the [Customer Support Portal](#) to get assistance around the clock, seven days a week, all year round. You can open a case as well as find links to online [documentation](#), [knowledge base articles](#), and the Palo Alto Networks [LIVEcommunity](#) user community. Telephone assistance is available at 1.866.898.9087 in the US, +1.408.738.7799 outside the US.

Do you need help with your Okyo Garde Device issues or need help setting it up?

Visit [Okyo.com](#) to find Okyo Garde resources and chat with an Okyo Garde expert. You can also email us at support@okyo.com or give us a call at 1.855.916.5961. Employees using the Okyo Mobile app can get help right in the app by tapping the question mark at the top right corner of the screen.



Network Settings

Learn how to configure your Okyo Garde network settings.

- > [Set up SSO for Okyo Garde Users](#)
- > [Your Network Settings at a Glance](#)
- > [Set Up your Corporate Network Access Point](#)
- > [Set Up RADIUS Authentication for Okyo Garde](#)
- > [Configure Network Address Translation](#)
- > [Route Trusted Traffic Directly Through the Internet \(Split Tunneling\)](#)

Set up SSO for Okyo Garde Users

You'll need to configure SSO (single sign-on) so that employees you assign device subscriptions to can log into the mobile app using their corporate credentials. For this setup, we'll be using [Okta as our SAML 2.0 identity provider \(IdP\)](#). The steps on the IdP side will vary.

- [Obtain your IdP Authentication information](#)
- [Add your IdP Authentication Information to Okyo](#)
- [Provide your Okyo Authentication Information to your IdP](#)
- [Assign Users to your Application](#)

Obtain your IdP Authentication information

The information you'll need to provide on this screen comes from your IdP.

Okyo Garde

- Overview
- Employees
- Single Sign-On Settings
- Network Settings
- Company Settings

Single Sign-On Settings

Configure SSO for employees to sign in to the Okyo website and mobile app using SSO.

Identity Provider (IdP) Issuer URI

IdP SSO URL

Certificate Signing Algorithm
SHA-1

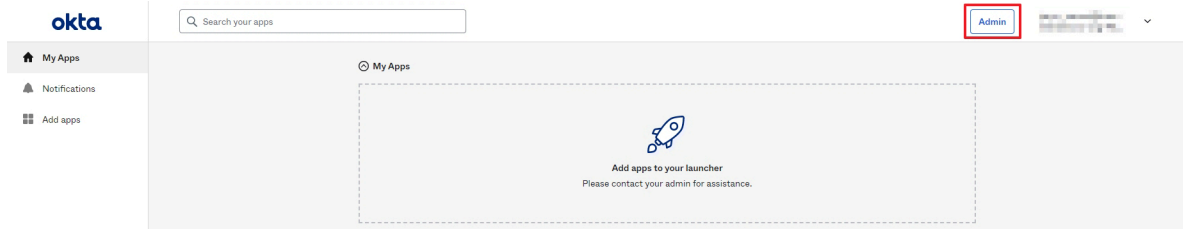
IdP Signature Certificate

Cancel Save

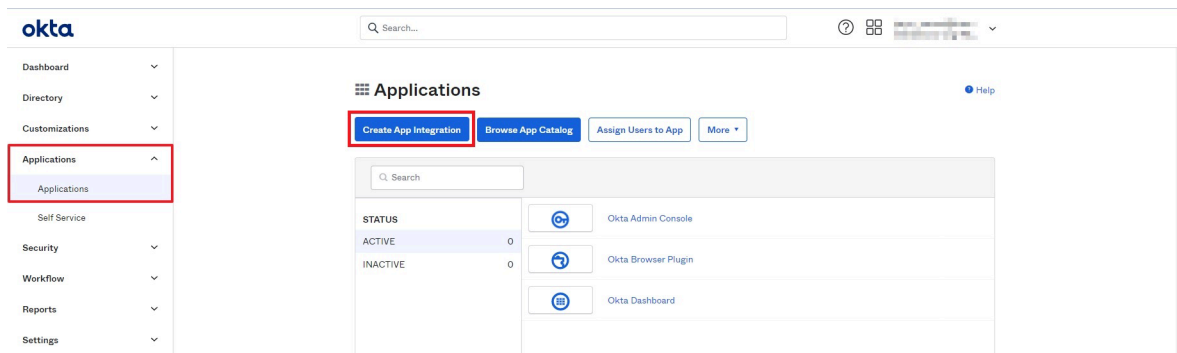
In this setup, we can get this information from an app we'll create in the Okta Developer Console. To create the app, follow these steps.

STEP 1 | Log in to your Okta Developer Console as a user with administrative privileges.

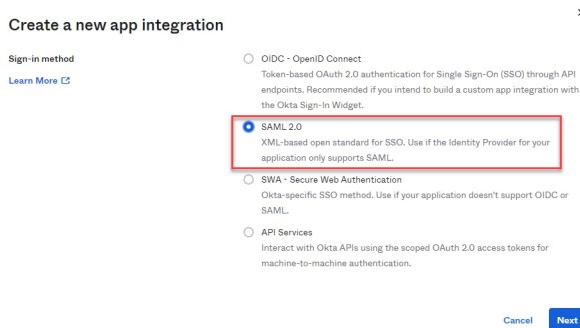
STEP 2 | Click **Admin** in the upper-right corner of your screen.



STEP 3 | Select **Applications > Applications** from the sidebar, and then click **Create App Integration**.

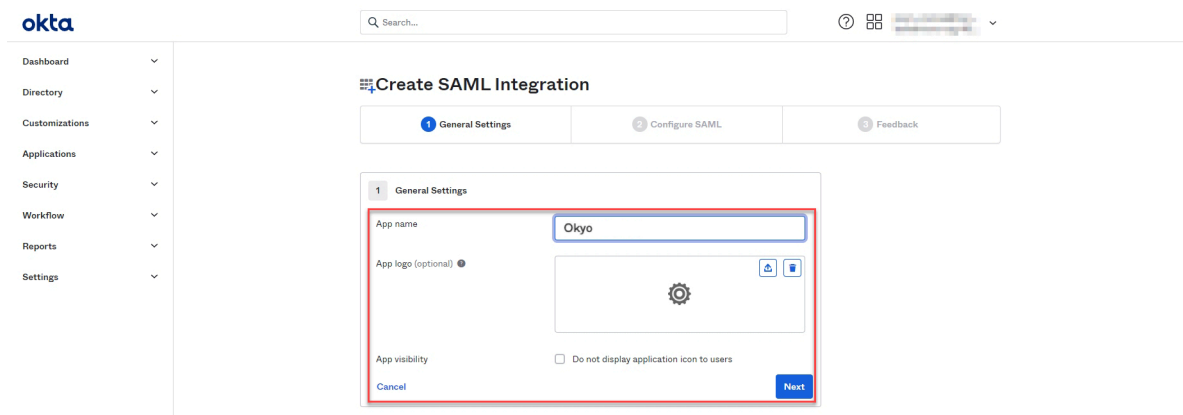


STEP 4 | Select **SAML 2.0** as the sign-in method, and then click **Next**.



The **Create SAML Integration** screen appears.

STEP 5 | On the **General Settings** tab, enter an **App name**. Optionally, upload a logo and choose the visibility settings for your app, then click **Next**.



STEP 6 | Select the **Configure SAML** tab and specify the following:

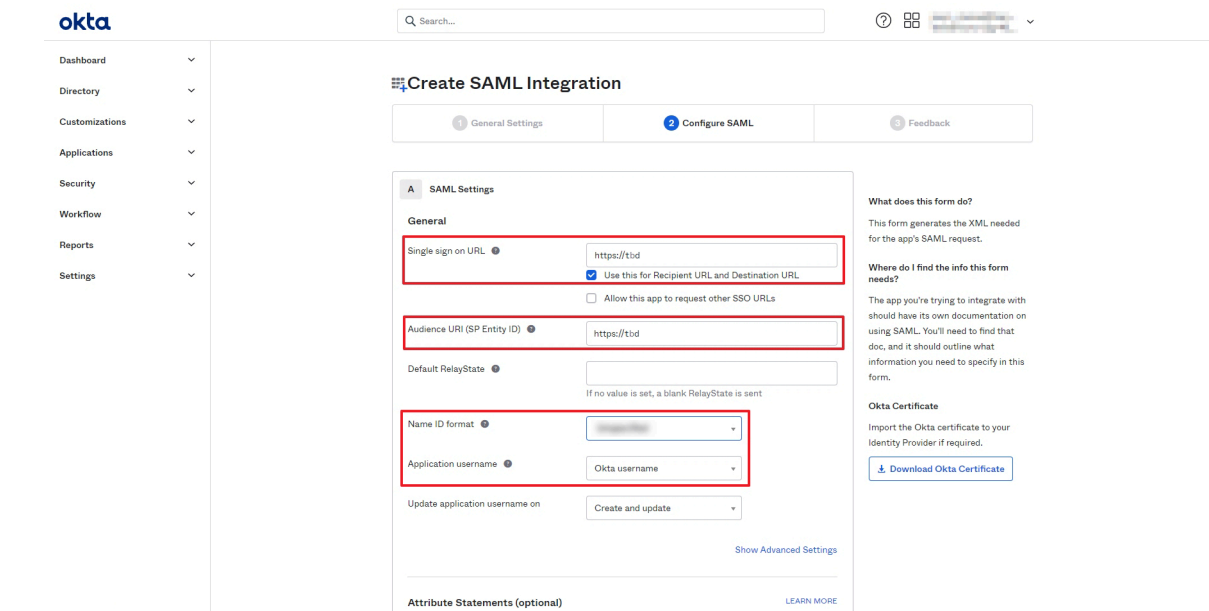
- For now, use a placeholder entry, such as “https://tbd”, in the **Single Sign-on URL** field, and select **Use this for Recipient URL and Destination URL**.

We’ll come back to this field later, in the [Provide your Okyo Authentication Information to your IdP](#) section.

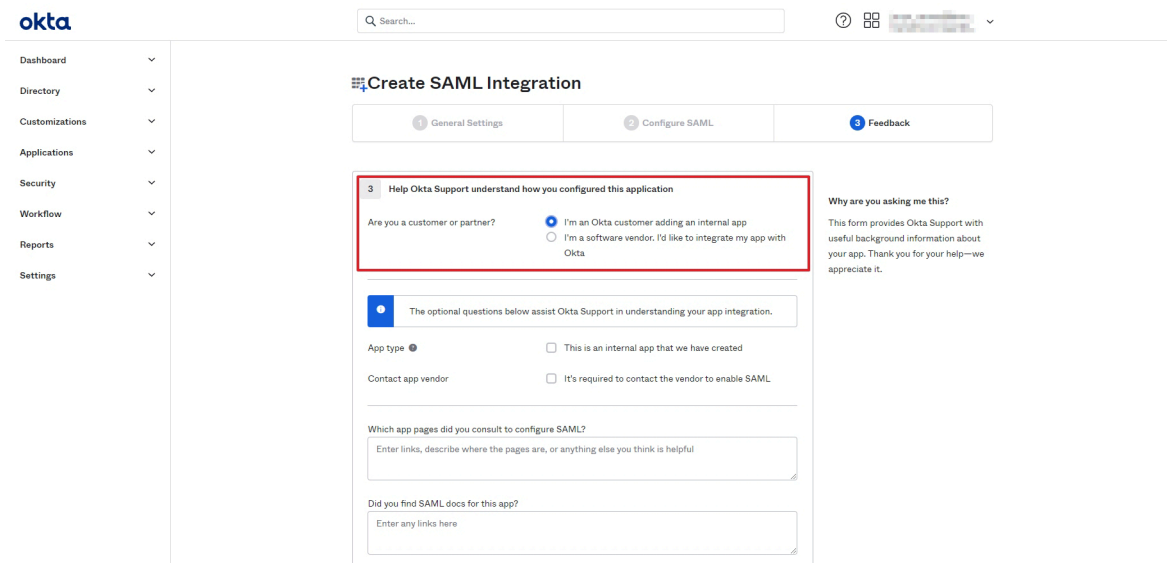
- For now, use a placeholder entry, such as “https://tbd”, in the **Audience URI (SP Entity ID)** field.

We’ll come back to this field later, in the [Provide your Okyo Authentication Information to your IdP](#) section.

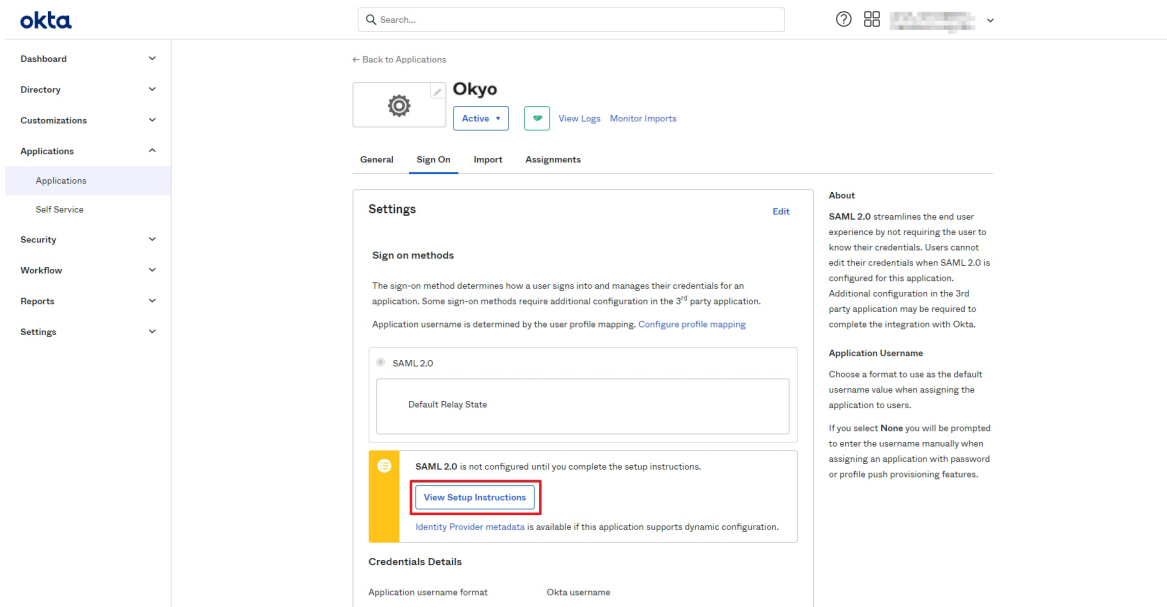
- Select **Okta username** in **Application username**, and then click **Next**.



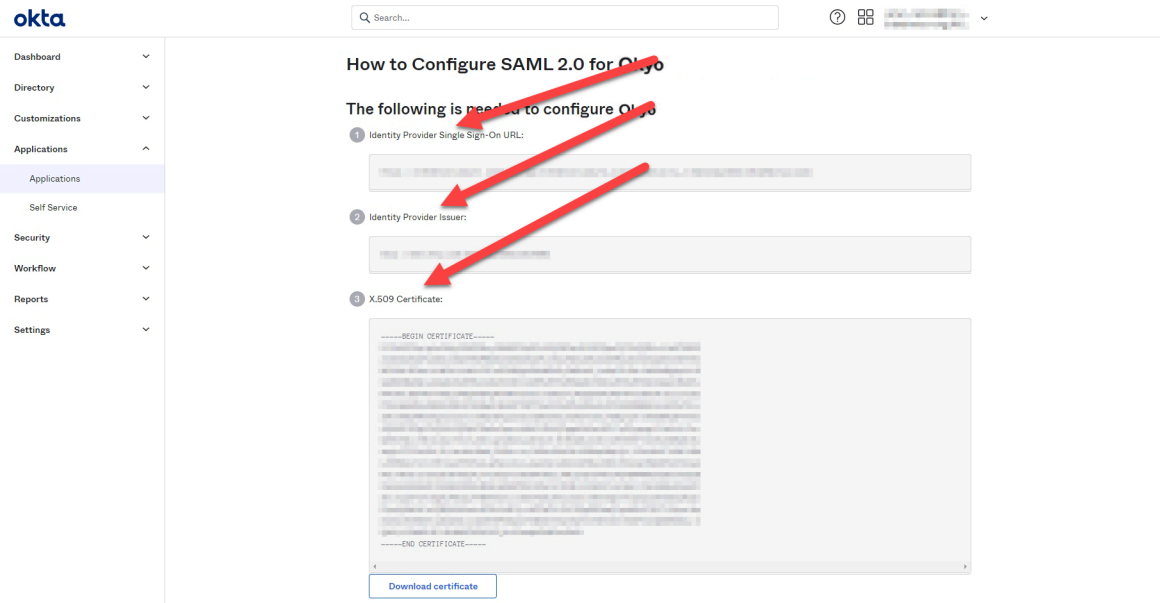
STEP 7 | Select the **Feedback** tab, choose the appropriate options for your organization, and then click **Finish**.



STEP 8 | Click the **View Setup Instructions** button.



STEP 9 | You now have your IdP’s authentication information. Record the content of the **Identity Provider Single Sign-On URL**, **Identity Provider Issuer**, and the **X.509 Certificate** fields. We’ll use this information in the next section.



Add your IdP Authentication Information to Okyo

Now that you have your IdP’s authentication information, add it to your Okyo Garde Single Sign-On Settings.

STEP 1 | Select  **Okyo Garde** > **Single Sign-On Settings** from the sidebar.

STEP 2 | Go to the **Single Sign-on (SSO) Configurations** panel and select  .

STEP 3 | Fill in these SSO fields, and then select **Save**.

| Field | Description |
|---|--|
| Identity Provider (IdP) Issuer URI | The URI that identifies the identity provider issuing a SAML request. This URI is specific to your identity provider. Copy and Paste the Identity Provider Issuer from your IdP here. |
| IdP SSO URL | The URL that Okyo can access to get SSO configuration information from your identity provider. This URL is specific to your identity provider. Copy and Paste the Single Sign-On URL from your IdP here. |
| Certificate Signing Algorithm | The hash algorithm used to sign the SAML certificate. Choose either SHA-1 or SHA-256 . |
| IdP Signature Certificate | The PEM or DER encoded public key certificate of the identity provider used |

| Field | Description |
|-------|---|
| | to verify SAML messages and assertion signatures. Copy and Paste the Certificate from your IdP here. |

STEP 4 | Select **Download** on the **Single Sign-on (SSO) Configurations** panel to download your SAML Metadata, and then provide it to your IdP. Your IdP needs this SAML metadata to be able to complete the SSO handshake with Okyo Garde.

Provide your Okyo Authentication Information to your IdP

Now that you've set up SSO on the Okyo side, you can provide your Okyo authentication information back to your IdP. You'll find this information in the SAML metadata file that you can download from this screen.

STEP 1 | Select **Download** on the **Single Sign-on (SSO) Configurations** panel to download your SAML Metadata. Your IdP needs two pieces of information from this SAML metadata to be able to complete the SSO handshake with Okyo.

Okyo Gardé

- Overview
- Employees
- Single Sign-On Settings
- Network Settings
- Company Settings

Single Sign-On Settings

Configure SSO for employees to sign in to the Okyo website and mobile app using SSO.

Single Sign-On (SSO) Configurations

Identity Provider (IdP) Issuer URI
[Redacted]

IdP SSO URL
[Redacted]

Certificate Signing Algorithm
SHA-1

IdP Signature Certificate
[Redacted]

SAML Metadata
[Download](#)

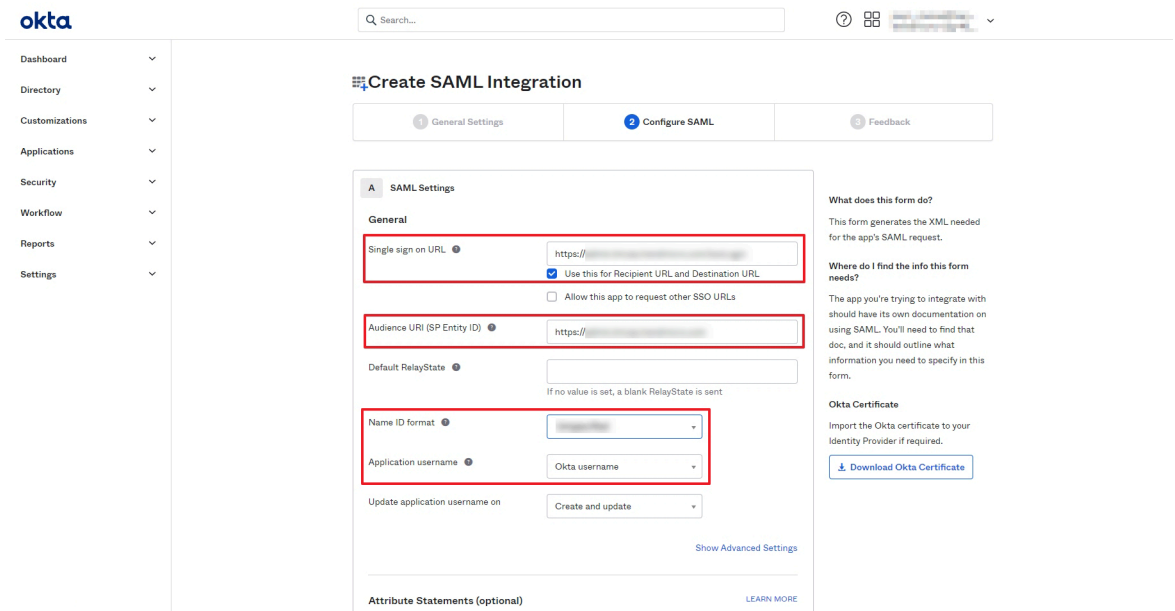
> Last Connection Errors

STEP 2 | Open the SAML Metadata file you just downloaded and find (CTRL + F) both the **entityID=** and the **Location=**. Record the information highlighted in yellow in your file. We'll use it in the next step.

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor entityID="https://www.
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"><SPSSODescriptor AuthnRequestsSigned="
  true" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="encryption"><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/
  xmlns:dsig="ds:X509Data"><ds:X509Certificate>
  japhd6x/nBfJspe/</ds:X509Certificate></ds:X509Data></md:KeyDescriptor><md:NameIDFormat><md:NameIDFormat><md:NameIDFormat><md:NameIDFormat>
  urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat><md:NameIDFormat><md:NameIDFormat><md:NameIDFormat><md:NameIDFormat>
  urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat><md:NameIDFormat><md:NameIDFormat>
  urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat><md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://
  index=0" isDefault="true"/><md:AttributeConsumingService index=0/><md:ServiceName xml:lang="en">Auto3rdParty
  RequestedAttribute FriendlyName="First Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-format:url" isRequired="true"/><md:RequestedAttribute FriendlyName="Last Name"
  Name="lastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-format:url" isRequired="true"/><md:RequestedAttribute FriendlyName="Email" Name="email" NameFormat="
  urn:oasis:names:tc:SAML:2.0:attribute-format:url" isRequired="true"/></md:RequestedAttribute FriendlyName="Mobile Phone" Name="mobilePhone" NameFormat="
```

STEP 3 | Go back to the **Configure SAML** tab in your Okta Developer Console and:

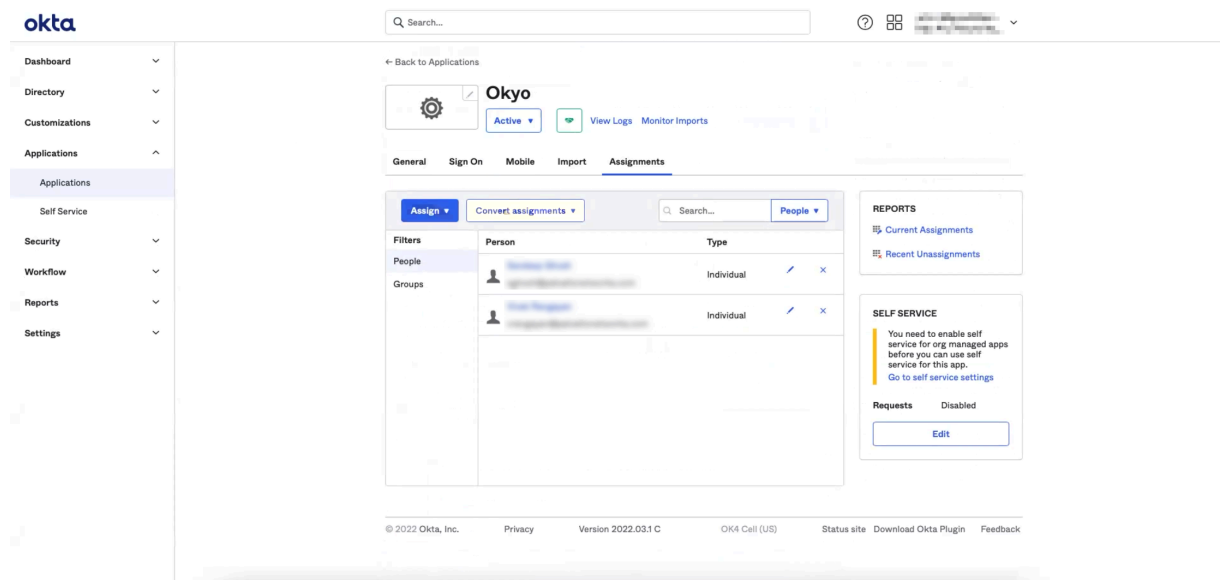
- Replace your placeholder entry with the SSO URL you found in the SAML Metadata file next to "Location=".
- Replace your placeholder entry with the URI you found in the SAML Metadata file next to "entityID=".
- Click **Next**, and then click **Finish**.



Assign Users to your Application

For SSO authentication to work properly for your users, you'll need to associate them with your IdP. Do this by assigning them to your application.

STEP 1 | Go to your Okta app in the Okta Admin Console. Select the **Assignments** tab and **Assign to People or Groups**.



STEP 2 | Select **Assign** next to the user that you want to assign. Note: If this is a new account, the only option available is to choose yourself (the administrator) as the user.

Optionally, for User Name, enter a user name or leave it as the user's email address.

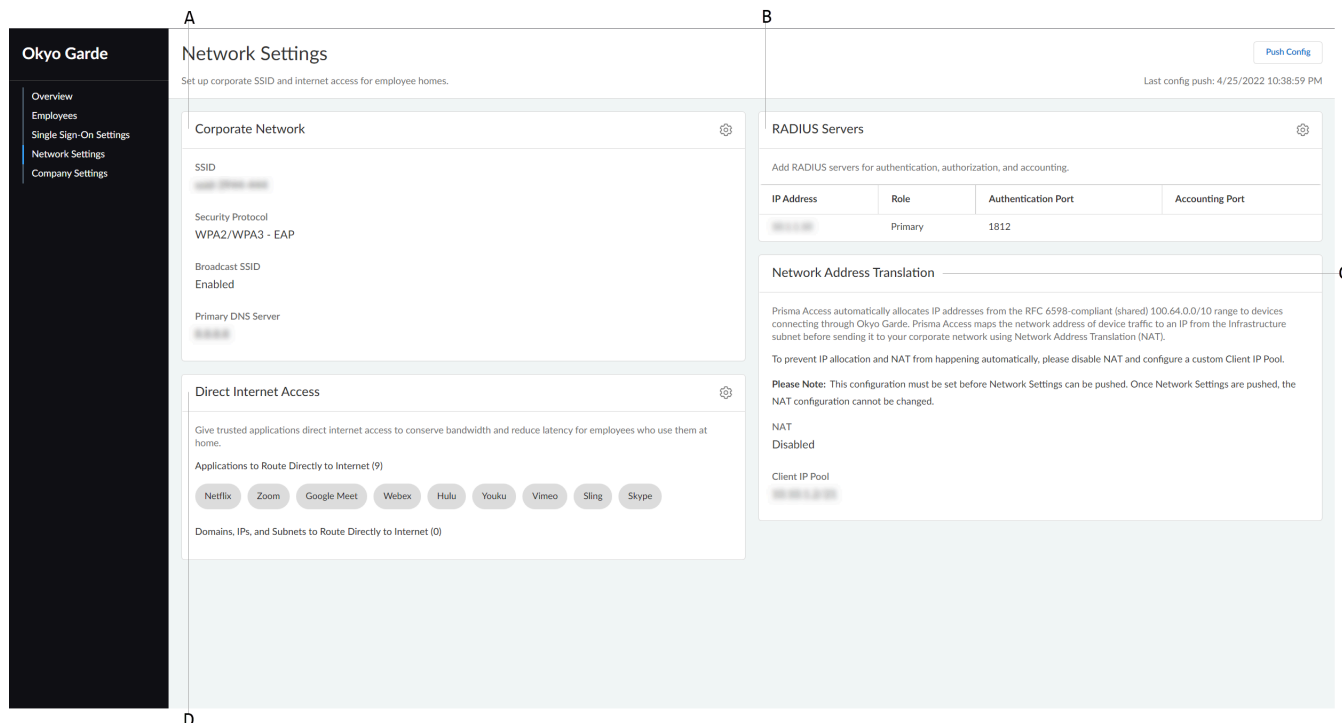
STEP 3 | Select **Save and Go Back** to complete the assignment, and then select, **Done**.

STEP 4 | Repeat the above steps to assign the application to more users as necessary.

Your Network Settings at a Glance

The **Network Settings** screen is the place to view and manage your company's corporate SSID and internet access for employees' homes. You'll need to **Push Config** for changes you make on this screen to take effect. After you **Push Config**, online devices are updated immediately, and offline devices are updated the next time they connect to the Okyo cloud.

To view your network settings, select  **Okyo Garde > Network Settings** from the sidebar.



A) Corporate Network

Set up [your company's internet access point](#).

B) RADIUS Servers

Add [RADIUS](#) servers for authentication, authorization, and accounting.

C) Network Address Translation

Set whether Prisma Access uses [NAT](#) to map the network address of device traffic to an IP from the Infrastructure subnet before sending it to your corporate network.


D) Direct Internet Access

Give trusted applications [direct internet access](#) to conserve bandwidth and reduce latency for employees who use them at home.

Set Up your Corporate Network Access Point

Configure the SSID and broadcast security settings employees use to connect to your corporate network.

Follow these steps to set up your corporate network access point:

STEP 1 | Select  **Okyo Garde > Network Settings** from the sidebar.

STEP 2 | Go to the **Corporate Network** panel and select  .

STEP 3 | Fill in these fields.

| Field | Description |
|---------------------------------------|--|
| Security Protocol | Choose WPA2-EAP , WPA2/WPA3-EAP , WPA3-EAP , or WPA3-EAP 192 . |
| SSID Name (only SSID for IoT devices) | Give your access point a name. |
| Primary DNS (required) | Enter the IP address of your Primary Domain Name System. |
| Secondary DNS (optional) | Enter the IP address of your Secondary Domain Name System. |



STEP 4 | Turn **Broadcast SSID** ON to make your corporate network discoverable to Wi-Fi enabled devices, or leave it OFF to make it harder for others to “see” your corporate network.

STEP 5 | Select **Save**.

Set Up RADIUS Authentication for Okyo Garde

RADIUS (Remote Authentication Dial-In User Service) authenticates the local and remote users on your corporate network using a central database.

Follow these steps to connect to set up RADIUS authentication:


- STEP 1 |** Select  **Okyo Garde > Network Settings** from the sidebar.
- STEP 2 |** Go to the **RADIUS Servers** panel and select  .
- STEP 3 |** Fill in the **IP Address**, **Shared Secret**, and **Authentication Port** fields.
- STEP 4 |** Turn **Enable Accounting** ON to allow RADIUS to collect data to keep an accurate billing of users, and for statistical purposes and network monitoring.
- STEP 5 |** Select **Save**, or add a **Secondary RADIUS Server** and repeat the process.

Configure Network Address Translation

To NAT or not to NAT, that is the question you'll need to answer before you can be done configuring network settings for Okyo. When you enable NAT (Network Address Translation) Prisma Access automatically allocates IP addresses from the RFC 6598-compliant (shared) 100.64.0.0/10 range to devices connecting through Okyo Garde. Prisma Access maps the network address of device traffic to an IP address from the Infrastructure subnet before sending it to your corporate network using a process called Network Address Translation (NAT).

You can, however, prevent automatic IP allocation and NAT by not enabling NAT and configuring a custom client IP pool. You must make your choice to enable NAT or not enable NAT and configure a custom IP pool before you can push your Network Settings to the cloud. Also, **after you push your NAT configuration, you won't be able to change it later. So, be careful!**

Follow these steps to configure network address translation:

STEP 1 | Select  **Okyo Garde > Network Settings** from the sidebar.

STEP 2 | Go to the **Network Address Translation** panel and select  .

STEP 3 | Choose one of these options.

1. **Enable NAT** - Prisma Access automatically maps the network address of device traffic to an IP from the Infrastructure subnet before sending it to your corporate network.
2. **Disable NAT and Configure a Custom Client Pool** - You provide a custom client IP pool network address. You'll enter a valid client IP pool network address, and then choose a subnet mask bit value from 2 to 27. The smaller the mask bit value, the more Okyo Garde devices your IP pool can support. In any case, a single Okyo Garde device can support up to 27 corporate-network-connected clients each.

STEP 4 | **Save** your settings.




When configuring your own custom client pool, proper sizing is a major consideration. Your client should be able to accommodate not only your current devices but also your future devices.

Route Trusted Traffic Directly Through the Internet (Split Tunneling)

Give trusted applications direct internet access to conserve bandwidth and reduce latency for employees who use them at home. This practice is commonly known as “split tunneling”. There is no security enforcement for trusted traffic.

Follow these steps to configure direct internet access for trusted traffic:

STEP 1 | Select  **Okyo Garde > Network Settings** from the sidebar.

STEP 2 | Go to the **Direct Internet Access** panel and select  .

STEP 3 | Turn on direct internet access for applications such as Netflix, YouTube, and Zoom.

STEP 4 | **Add** additional domains, IP addresses, or subnets to give them direct internet access.

To remove domains, IP addresses, or subnets you’ve added, select the checkbox next to the items in the list you want to remove, and then **Delete**.

STEP 5 | **Save** your split tunneling settings.

Company Settings

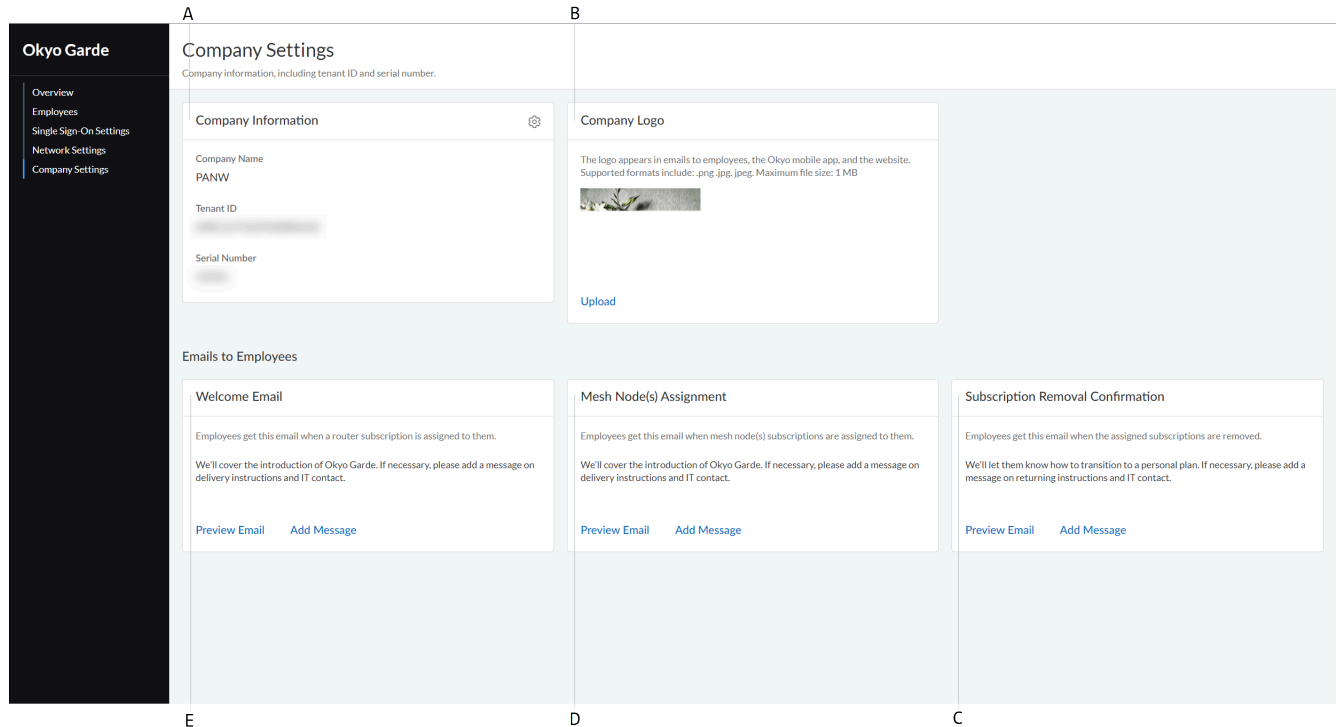
Learn how to configure your Okyo Garde company settings.

- > [Your Company Settings at a Glance](#)
- > [Change your Company's Okyo Garde Info](#)
- > [Change your Company's Logo in Okyo Garde](#)
- > [Customize Okyo Welcome Email](#)
- > [Customize Okyo Mesh Node Assignment Email](#)
- > [Customize Okyo Subscription Removal Confirmation](#)

Your Company Settings at a Glance

The **Company Settings** screen is the place to configure and see how your company name and logo appear in emails to employees.

To view your company settings, select  **Okyo Garde > Company Settings** from the sidebar.



A) Company Information

Change how your company's information appears in Okyo Garde.

B) Company Logo

Change your company logo for Okyo Garde.

C) Okyo Garde Subscription Removal Confirmation

Customize the email that's sent when you remove an Okyo Garde subscription from an employee.

D) Mesh Node Assignment

Customize the email that's sent when you add a mesh subscription to an existing employee subscription.


E) Welcome Email

Customize the welcome email that's sent to employees when you assign them an Okyo Garde subscription.

Change your Company's Okyo Garde Info

You can view and change the information that appears in emails to employees and in the Okyo Mobile app.

Follow these steps to edit your company information:

STEP 1 | Select  **Configurations > Company Settings** from the sidebar.

STEP 2 | Go to the **Company Information** panel and select  .

STEP 3 | Fill in the **Company Name** field.

STEP 4 | Select **Save**.



*You can't change your **Tenant ID** or **Serial Number**.*

Change your Company's Logo in Okyo Garde

Configure and see how your logo appears in emails to employees and in the Okyo Mobile app.

To change your company logo, follow these steps:

STEP 1 | Select  **Okyo Management** > **Company Settings** from the sidebar.

STEP 2 | Go to the **Company Logo** panel and select **Upload**.

STEP 3 | Choose an image from your computer to upload.

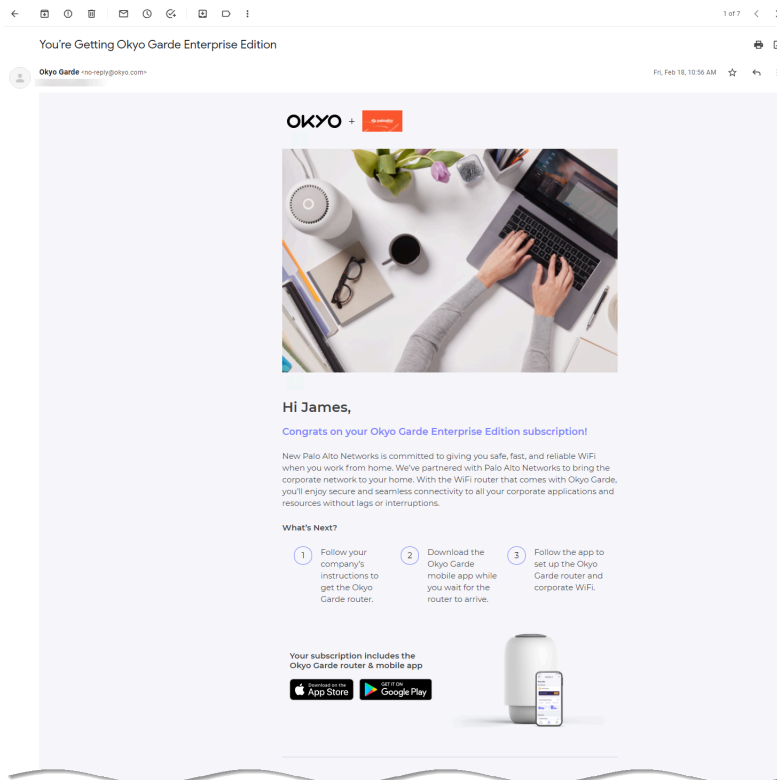
The file you choose is uploaded to the Okyo subscription manager.




- Only .png, .jpg, and .jpeg format images are supported.
- Your image can be up to 1 MB in size.

Customize Okyo Welcome Email

When you assign an Okyo Garde subscription to an employee, we'll send them an email notifying them of their subscription assignment. We'll also show them how to claim and activate their Okyo Garde router. You can customize the welcome email that's sent when you [assign Okyo Garde subscriptions](#) to employees.



Follow these steps to add a custom message to the email employees receive:

STEP 1 | Select  **Okyo Garde > Company Settings** from the sidebar.

STEP 2 | Go to the **Welcome Email** panel and select **Add Message**.

The **Preview of Welcome Email** screen opens.

STEP 3 | Enter your message text.

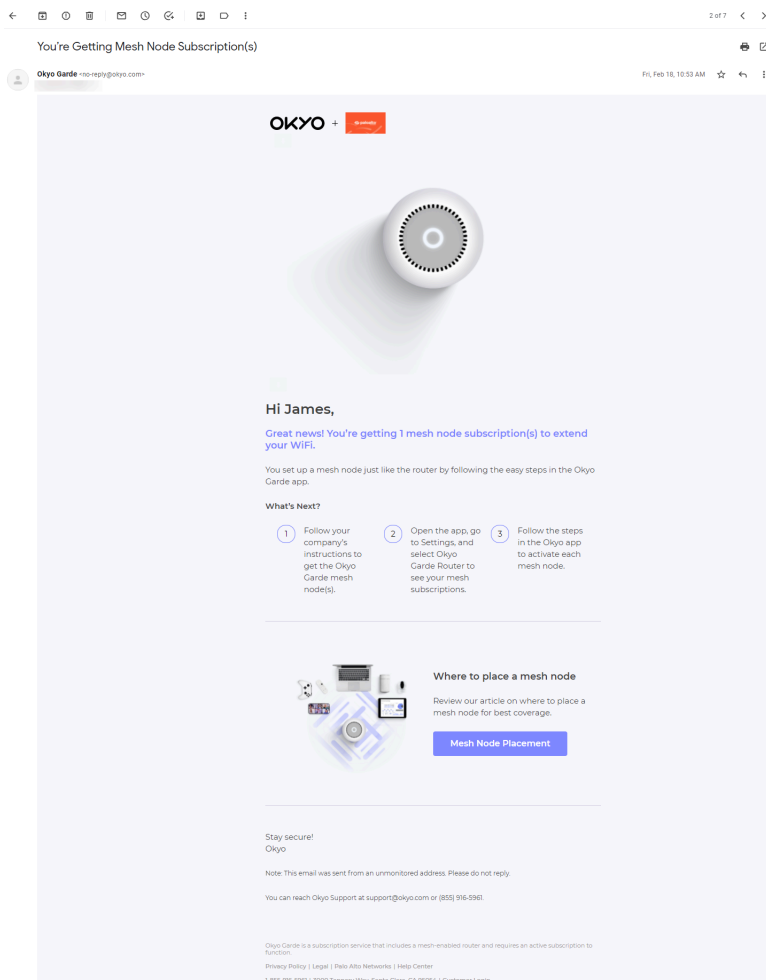
STEP 4 | Select **Save**.

You'll see a preview of your email. Select the **Highlight the added message** checkbox to see your custom message.


STEP 5 | Select **Close** to finish customizing the welcome email.

Customize Okyo Mesh Node Assignment Email

When you assign an Okyo Garde mesh subscription to an employee, we'll send them an email notifying them of their subscription assignment. We'll also show them how to activate their subscription. You can customize the email that's sent when you [add Okyo Garde mesh subscriptions](#) to existing employee subscriptions.



Follow these steps to add a custom message to the email employees receive:

STEP 1 | Select  **Okyo Garde > Company Settings** from the sidebar.

STEP 2 | Go to the **Mesh Node(s) Assignment** panel and select **Add Message**.

The **Preview of Mesh Node(s) Assignment Email** screen opens.

STEP 3 | Enter your message text.

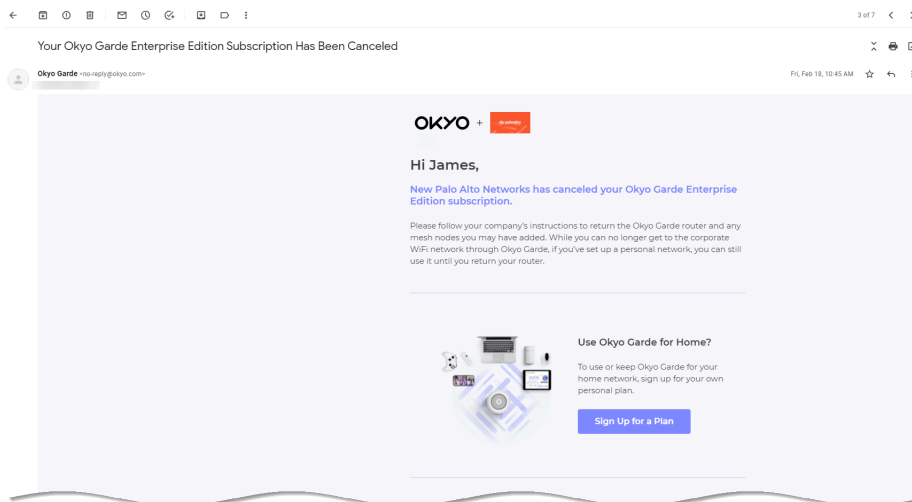
STEP 4 | Select **Save**.

You'll see a preview of your email. Select the **Highlight the added message** checkbox to see your custom message.


STEP 5 | Select **Close** to finish customizing the mesh node(s) assignment email.

Customize Okyo Subscription Removal Confirmation

When you remove an Okyo subscription from an employee, we'll send them an email notifying them of the change. We'll also give them the option to continue using Okyo Garde on their own. You can customize the email that's sent when you [remove subscriptions](#) from employees.



Follow these steps to add a custom message to the email employees receive:

STEP 1 | Select  **Okyo Garde > Company Settings** from the sidebar.

STEP 2 | Go to the **Subscription Removal Confirmation** panel and select **Add Message**.

The **Preview of Subscription Removal Confirmation** screen opens.

STEP 3 | Enter your message text.

STEP 4 | Select **Save**.

You'll see a preview of your email. Select the **Highlight the added message** checkbox to see your custom message.

STEP 5 | Select **Close** to finish customizing the subscription removal confirmation.

Policy Management

Learn how to configure and push your Okyo Garde policy settings.

- > [Manage Security Policy and Profiles for Okyo Garde](#)
- > [Push Policy Updates to Prisma Access](#)

Manage Security Policy and Profiles for Okyo Garde

Okyo Garde Users are a type of Mobile User. So, you can view and manage policies for Okyo Garde in the same space you manage other Mobile User (GlobalProtect) policies.

- [Cloud Managed Prisma Access Deployments](#)
- [Panorama Managed Prisma Access Deployments](#)

Cloud Managed Prisma Access Deployments

Security Policy

To view and manage policy for Mobile Users in Cloud Managed Prisma Access Deployments, select **Manage > Configuration > Security Services** from the sidebar and select the **Remote Workforce** configuration [scope](#).

The screenshot displays the Palo Alto Networks Security Policy configuration interface. The sidebar on the left shows the navigation menu with 'Security Policy' highlighted. The main content area is titled 'Security Policy | Remote Workforce' and includes a 'Best Practice Assessment' section with four gauges: 'Security Rules Failing Checks' (1/13), 'Failed Rule Checks' (3/102), 'Failed Rulebase Checks' (1/9), and 'Failed CSC Checks' (2/9). To the right, a 'FEATURE ADOPTION' section shows progress for App-ID (7.69%), User-ID (0.00%), and Content-ID (15.38%). Below this is a table of 'Security Policy Rules (15)' with columns for Name, BPA Verdict, Cleanup, Zone, Address, User, Device, and Zone. The table lists several rules, including 'Drop Traffic to Known Malicious IP Addresses' and 'Deny Quic', all with a 'Pass' verdict.

| Name | BPA Verdict | Cleanup | Zone | Address | User | Device | Zone |
|--|-------------|---------------|------|---------------|------|--------|------|
| 1 Drop Traffic to Known Malicious IP Addresses | Pass | Zero Hit Rule | any | any | any | any | any |
| 2 Drop Traffic to Potential High Risk IP Addresses | Pass | Zero Hit Rule | any | any | any | any | any |
| 3 Drop Traffic to Bulletproof hosting providers | Pass | Zero Hit Rule | any | any | any | any | any |
| 4 Drop Traffic from Known Malicious IP Addresses | Pass | Zero Hit Rule | any | parnw-kno... | any | any | any |
| 5 Drop Traffic from Potential High Risk IP Addresses | Pass | Zero Hit Rule | any | parnw-high... | any | any | any |
| 6 Drop Traffic from Bulletproof hosting providers | Pass | Zero Hit Rule | any | parnw-bull... | any | any | any |
| 7 Deny Quic | Pass | | any | any | any | any | any |

Security Profiles

Profiles are how you enable [security services](#)—like Threat Prevention, WildFire, and URL Filtering—for your network traffic. You can also manage [security profiles](#) for Okyo Garde together with GlobalProtect. First, [enable](#) security profiles you want to use, then select **Manage > Configuration > Security Services** from the sidebar, and select the profile want to manage.

Manage > Anti-Spyware

Anti-Spyware | Remote Workforce

Best Practice Assessment

PROFILE CHECKS

- 0/0 Profiles Failing Checks
- 0/0 Profiles Not in Use
- 0/0 Failed Checks
- 0/13 Security Rules Not Using Best Practice Profiles

Anti-Spyware Security Profiles (1)

| Name | BPA Verdict | Location | Profile Groups | Security Rules Using This Profile | Overrides |
|---------------|-------------|------------|---|-----------------------------------|-----------|
| best-practice | Pass | predefined | Explicit Proxy - Unknown Users best-practice | 13 / 13 | 0 |

100.0% of your security policy rules are using a Anti-Spyware profile (13 of 13 rules)

Panorama Managed Prisma Access Deployments

Security Policy

To view and manage [security policy](#) for mobile users in Panorama Managed Prisma Access deployments, select **Policies > Security** from the Panorama that manages Prisma Access. The policies that manage Okyo Garde are in the **Mobile_User_Device_Group** device group. Prisma Access uses this device group for both Mobile Users - GlobalProtect and Okyo Garde deployments.

| | NAME | LOCATION | TAGS | TYPE | ZONE | Source | | | Destination | | |
|---|--------------------------|-------------------|------------|-----------|------|-------------------|------------------|--------|-------------|-------------------|--------|
| | | | | | | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE |
| 1 | Block-traffic-from-Hi... | Shared | sase-rules | universal | any | Palo Alto Netw... | any | any | any | any | any |
| 2 | Block-traffic-to-High... | Shared | sase-rules | universal | any | any | any | any | any | Palo Alto Netw... | any |
| 3 | Block-Quick | Shared | none | universal | any | any | any | any | any | any | any |
| 4 | Deny-Corp-Policy-U... | Alvisofin-Comm... | none | universal | any | any | alvisofin/dbell | any | any | any | any |
| 5 | FileShare-Threat-Pre... | Alvisofin-Comm... | none | universal | any | any | alvisofin/jmatt | any | any | 10.10.1.42 | any |
| | | | | | | | alvisofin/msl... | | | 10.10.1.61 | |

Security Profiles

To manage [security profiles](#) in a Panorama Managed Prisma Access deployment, select **Objects > Security Profiles**. Prisma Access provides you with a set of predefined profiles; however, you can add new profiles.

| NAME | LOCATION | PACKET CAPTURE | Decoders | | | |
|--------------|------------|-------------------------------------|----------|----------------------|---------------------------|---------------------------|
| | | | PROTOCOL | SIGNATURE ACTION | WILDFIRE SIGNATURE ACTION | WILDFIRE INLINE ML ACTION |
| default | Predefined | <input type="checkbox"/> | http | default (reset-both) | default (reset-both) | default (reset-both) |
| | | | http2 | default (reset-both) | default (reset-both) | default (reset-both) |
| | | | smtp | default (alert) | default (alert) | default (alert) |
| | | | imap | default (alert) | default (alert) | default (alert) |
| | | | pop3 | default (alert) | default (alert) | default (alert) |
| | | | ftp | default (reset-both) | default (reset-both) | default (reset-both) |
| default-pcap | Shared | <input checked="" type="checkbox"/> | http | default (reset-both) | default (reset-both) | default (reset-both) |
| | | | http2 | default (reset-both) | default (reset-both) | default (reset-both) |
| | | | smtp | default (alert) | default (alert) | default (alert) |
| | | | imap | default (alert) | default (alert) | default (alert) |
| | | | pop3 | default (alert) | default (alert) | default (alert) |
| | | | smb | default (reset-both) | default (reset-both) | default (reset-both) |
| AS-Reset | Shared | <input type="checkbox"/> | http | reset-both | reset-both | reset-both |
| | | | http2 | reset-both | reset-both | reset-both |

By default, Prisma Access uses the **Mobile_User_Device_Group** for mobile user deployments; however, if you created another parent device group when you [set up Prisma Access for mobile users](#), create policies under that device group.

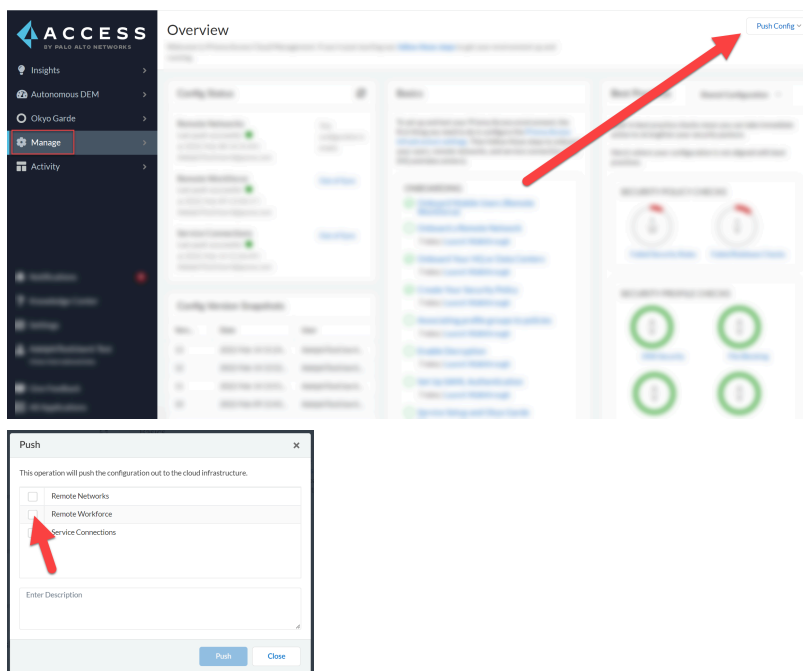
Push Policy Updates to Prisma Access

Policy and network configuration changes you make won't go into effect until you sync them with Prisma Access. To do this, you'll need to "push" your changes to Prisma Access. The process of pushing differs slightly depending on how you manage Prisma Access.

- [Push from Cloud Managed Prisma Access](#)
- [Push from Panorama Managed Prisma Access](#)

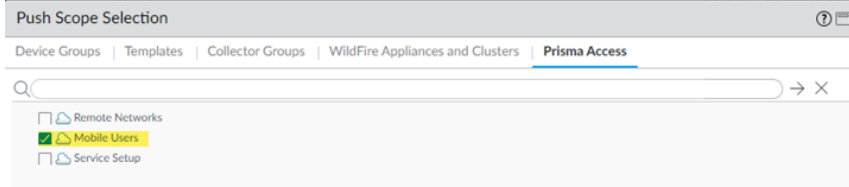
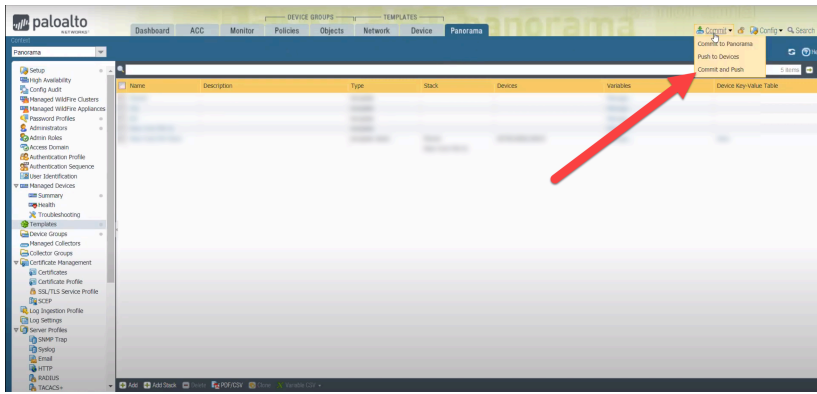
Push from Cloud Managed Prisma Access

To sync your Okyo Garde updates using Cloud Managed Prisma Access, you must [push your configuration](#) to Prisma Access. Select **Push Config** and choose the **Mobile Users** scope. The **Push Config** button is accessible from the top right corner of just about any screen in the **Manage** tab.



Push from Panorama Managed Prisma Access

To sync your Okyo Garde updates using Panorama Managed Prisma Access You must commit and push them to Prisma Access. Select **Commit > Commit and Push** and choose the **Mobile Users** scope. The **Commit** button is accessible from the top right corner of your screen.



Manage Employees

Learn about managing employees.

- > [View Okyo Garde Employee Details](#)
- > [Add Employees to Okyo Garde with Prisma Access](#)
- > [Edit Okyo Garde Employee Info](#)
- > [Remove Okyo Garde Employees](#)

View Okyo Garde Employee Details

The **Employees** screen is the place to view and manage your organization's employees and subscriptions. Sort and filter employee information to see what matters to you most, and even export that information to a file you can download and share.

To view a list of employees, select  **Okyo Garde > Employees** from the sidebar.

Manage Employees

Okyo Garde

Employees

View and manage subscriptions for all employees. Select up to 1,000 employees at a time.

60 total

Download CSV Delete Manage Subscriptions Add

| Name | Email | Subscription Status ↑ | Device(s) | Location |
|------------|------------|-----------------------|------------|-------------------------|
| [Redacted] | [Redacted] | Activated (5) | [Redacted] | Santa Clara, California |
| [Redacted] | [Redacted] | Activated (5) | [Redacted] | -- |
| [Redacted] | [Redacted] | Assigned (5) | -- 1 | -- |
| [Redacted] | [Redacted] | Assigned (5) | -- | -- |
| [Redacted] | [Redacted] | Assigned (5) | -- | -- |
| [Redacted] | [Redacted] | Assigned (5) | -- | -- |
| [Redacted] | [Redacted] | Assigned (5) | -- | -- |
| [Redacted] | [Redacted] | Not Assigned | -- | -- |
| [Redacted] | [Redacted] | Not Assigned | -- | -- |

A) Total number of employees

Shows the total number of employees administrators have added to Okyo Garde with Prisma Access.

B) Filter by columns

Filter the list of employees by employee name, email, subscription status, device, or location. See [Okyo Garde Overview](#) to learn more about the four subscriptions statuses.

To sort the list by these categories, click a column header.

C) Show / Hide columns

Show or hide columns to improve visibility.

D) Download CSV

Export your employee list and save it to your computer.

E) Delete

Remove employees' information from Okyo Garde.

F) Manage Subscriptions

Manage Okyo Garde subscriptions for your company's employees.

G) Reset Filters

Remove your custom filters.

H) Add

[Add employees](#) so you can [assign Okyo Garde subscriptions](#) to them.

I) Employee list

Employees, their subscriptions, and their devices become part of this list as you add them. For a given row, hover your cursor over:

- **Subscription Status** to see details of a particular employee's subscription.
- **Device(s)** to view [logs](#) for a particular device.

Add Employees to Okyo Garde with Prisma Access

Before you can assign Okyo Garde subscriptions to your organization's employees, you'll need to add them. To save time, you can bulk add employees from a CSV file, or one at a time for just a few employees.

- [Bulk Add Employees from a CSV File](#)
- [Add Employees One at a Time](#)

Bulk Add Employees from a CSV File

STEP 1 | Prepare a CSV file that's formatted like this:

| | A | B | C |
|---|-----------|-----------|---------------------|
| 1 | FirstName | LastName | Email |
| 2 | Peter | Smith | psmith@panw.com |
| 3 | Elizabeth | Carpenter | ecarpenter@panw.com |
| 4 | John | Doe | jdoh@panw.com |
| 5 | Beth | Wong | bwong@panw.com |
| 6 | Kathy | Tran | ktran@panw.com |

STEP 2 | Select  **Okyo Garde > Employees** from the sidebar.

STEP 3 | Select **Add > Add Employees with CSV**.

The **Add with CSV** window opens

STEP 4 | Either click on the window to choose a file from your computer to upload, or drag and drop the file you want to upload onto the window.

STEP 5 | Select **Add**.



To avoid errors, be sure your CSV file doesn't have any of these issues:

- *Blank fields*
- *Email address with invalid formats*
- *Duplicate entries*
- *Email address that's already been entered*
- *Email address containing non-ASCII characters*

*To download a sample CSV file, select **View sample**.*

Add Employees One at a Time

STEP 1 | Select  **Okyo Garde > Employees** from the sidebar.

STEP 2 | Select **Add > Add an Employee**.

The **Add Employee** window opens

STEP 3 | Enter the employee's information, and then select **Save**.




To avoid errors, be sure your entry doesn't have any of these issues:

- *Blank fields*
- *Email address with invalid formats*
- *Duplicate entries*
- *Email address that's already been entered*
- *Email address containing non-ASCII characters*

Edit Okyo Garde Employee Info

Let's face it, when employee life events and company reorgs happen, you might need to make changes to an employee's details. To edit an employee's information, follow these steps:

- STEP 1** | Select  **Okyo Garde > Employees** from the sidebar.
- STEP 2** | Select (click on) the name of the employee you want to edit.
- STEP 3** | Make your changes to the employee's information.
- STEP 4** | Select **Save**.

Remove Okyo Garde Employees

Need to remove employees who no longer need their Okyo Garde routers and mesh nodes? First, [remove their subscriptions](#), and then remove their information from the Okyo Garde with Prisma Access.

To remove employee information, follow these steps:

STEP 1 | Select  **Okyo Garde > Employees** from the sidebar.

STEP 2 | Select the employees you want to remove.

STEP 3 | Select **Delete** and then click **Yes, Remove** to confirm.

If a selected employee is assigned a subscription, you'll need to [remove the subscription](#) first.

Manage Subscriptions

Learn about managing subscriptions.

- > [Assign Okyo Garde Subscriptions to Users](#)
- > [Add Okyo Garde Mesh Subscriptions to Existing Subscriptions](#)
- > [Remove Okyo Garde Subscriptions](#)

Assign Okyo Garde Subscriptions to Users

After you [add employees](#), you'll want to set them up with an Okyo Garde device. If you haven't [set up single sign-on \(SSO\)](#) for employees yet, you'll need to do that first.

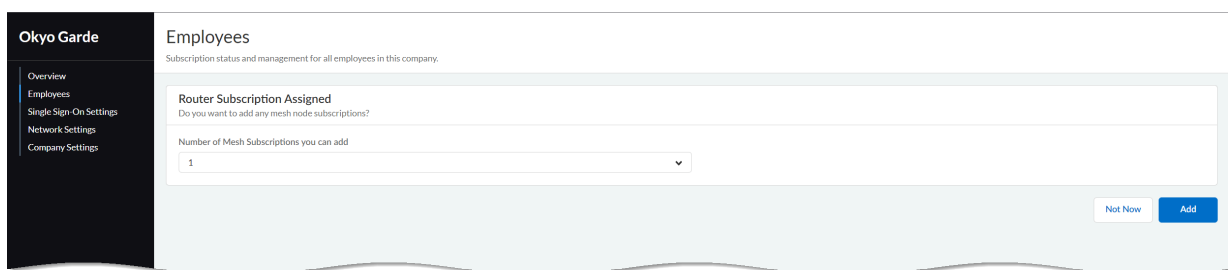
After you've set up SSO, follow these steps to assign or change employee subscriptions:

STEP 1 | Select  **Okyo Garde > Employees** from the sidebar.

STEP 2 | Select the employees you want to assign Okyo Garde router subscriptions to.

STEP 3 | Select **Manage Subscriptions > Assign Subscriptions**.

The **Router Subscription Assigned** window opens. You're given the option to [add one or more mesh subscriptions](#) or select **Not Now**.



A welcome email is sent to the employees you've assigned subscriptions to.



- You can [add a custom message](#) to the email that's sent to employees.
- If a selected employee already has a subscription assigned, select **Yes, Assign** in step 4 to replace the current subscription. Also, if the employee has activated the subscription, assigning a new subscription might change the configurations on the router.

Add Okyo Garde Mesh Subscriptions to Existing Subscriptions

Want to extend network coverage in employees' homes using true mesh technology? Add mesh subscriptions to their existing Okyo Garde subscription.

If you haven't [assigned Okyo Garde subscriptions](#) to your employees yet, you'll need to do that first.

To add mesh subscriptions to an existing employee subscription, follow these steps:

STEP 1 | Select  **Okyo Garde > Employees** from the sidebar.

STEP 2 | Select **Manage Subscriptions > Add Mesh Subscriptions**.

The **Add Mesh Subscriptions** window opens.

STEP 3 | Choose the **Number of Mesh Subscriptions** you want.

STEP 4 | Select **Add Mesh** to confirm.

An email is sent to the employees you've assigned mesh subscriptions to.



- You [add a custom message](#) to the email that's sent to employees.
- You can assign up to 4 Okyo mesh nodes to a single employee at one time.

Remove Okyo Garde Subscriptions

Has an employee left the company? No longer need Okyo Garde subscriptions for certain employees? You'll need to remove their Okyo Garde subscriptions before you [remove those employees](#) from Okyo Garde altogether. When you remove a subscription from an employee, here's what you can expect to happen depending on whether the employee has set up a personal network or not. In either case, employees should reset their Okyo Garde devices to factory settings and return them their organization as soon as possible so that they can be made available to other employees.

| Corporate Network | Personal Network |
|---|--|
| Okyo Garde devices (router and any mesh nodes) assigned to employee are immediately prohibited from accessing the corporate network, and will be reset to factory settings after 30 days. | Okyo Garde devices (router and any mesh nodes) assigned to employee can manage any personal networks set up by the employee for up to 30 days, depending on the policy of their organization. Will be reset to factory settings after 30 days. |

To unassign Okyo Garde subscriptions from employees and deactivate their routers, follow these steps:

STEP 1 | Select  **Okyo Garde** > **Employees** from the sidebar.

STEP 2 | Select the checkboxes next to the employees whose subscriptions you want to remove.

STEP 3 | Select **Manage Subscriptions** > **Remove Subscriptions**.

The **Remove Subscriptions** window opens.

STEP 4 | Choose to **Remove mesh subscriptions only** or **Remove all subscriptions** for the selected employees.

STEP 5 | Select **Remove** to confirm.

An email is sent to the employees you've removed Okyo Garde router subscriptions from. No email is sent when you remove only a mesh node.



- *Even though an employee who's no longer with the company is removed from your company's IdP, their Okyo Garde devices may remain active for a period of time. You can explicitly remove their subscriptions to immediately revoke access to the corporate network.*
- You can [add a custom message](#) to the email that's sent to employees.

Monitor Okyo Garde at a Glance

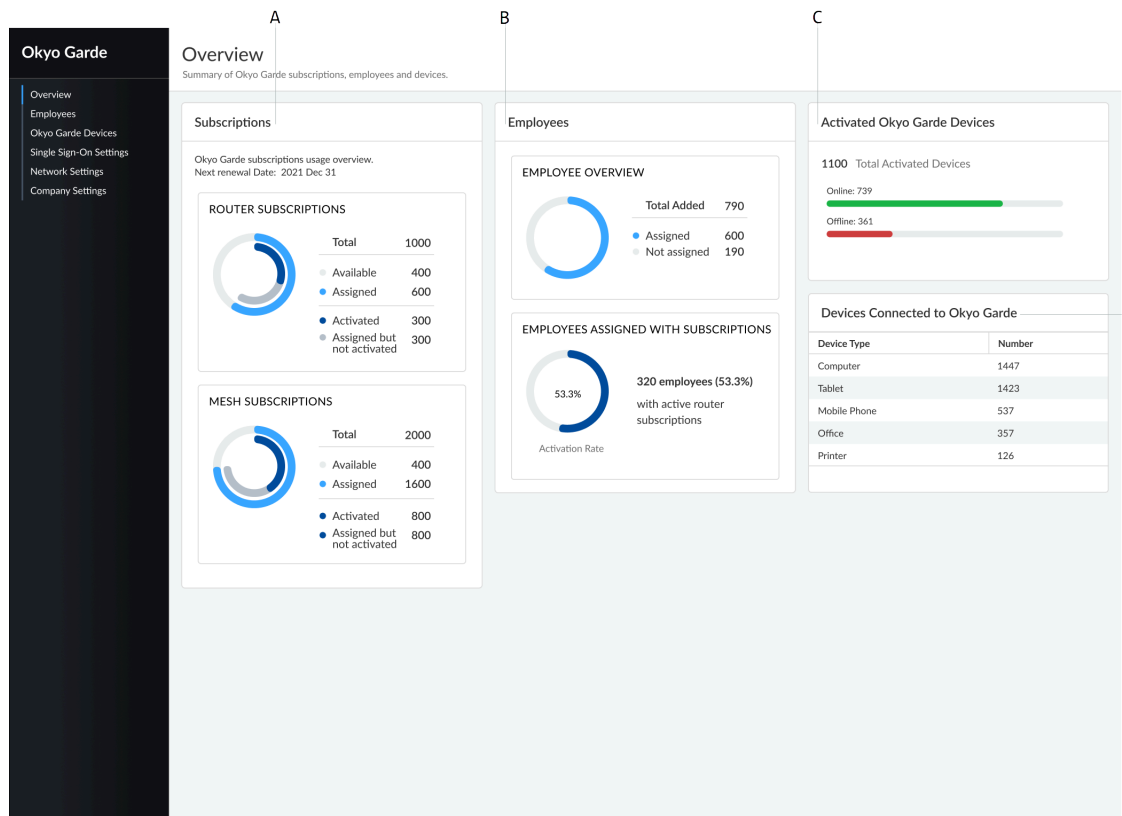
In addition to the Okyo Garde [Employees](#) screen and the [Logs](#), dashboards are a convenient way to monitor the health and usage of Okyo Garde. The Okyo Garde Overview screen and the Insights Okyo Garde dashboard are two places you'll find a wealth of information about what's happening with your Okyo Garde implementation.

- > [Okyo Garde Overview](#)
- > [Okyo Garde Dashboard in Insights](#)

Okyo Garde Overview

The **Overview** screen is the place to view your organization's Okyo Garde subscriptions. Visit this page after you [add employees](#) and [assign subscriptions](#) to them to quickly see the status of your organization's subscriptions.

To view your organization's subscriptions, select  **Okyo Garde > Overview** from the sidebar.



A) Subscriptions

Shows the assigned status of your organization's subscribed devices.

- **Available**

The remaining number of devices you can assign to employees. This number decreases as you assign devices.

- **Assigned**

The number of devices you've assigned to employees regardless of whether employees have activated the devices. This number increases as you assign devices.

- **Activated**

The number of assigned devices that have been activated by employees. This number increases as employees activate their assigned devices. A device is activated when the employee registers it using its QR code and connects it to the Okyo cloud.

- **Assigned but not Activated**

The number of assigned devices that have been not been activated by employees. This number increases as employees activate their assigned devices.

There are two subscription types available:

- **Okyo Garde router** - The gateway to Okyo Garde services from employees' homes.
- **Okyo Garde mesh** - A mesh node to extend the coverage of Okyo Garde in employees' homes.

B) Employees

Shows employees and the status of their subscriptions.

C) Activated Okyo Garde Devices


Shows the online status of activated Okyo Garde routers.

D) Devices Connected to Okyo Garde

Shows the various types of devices that are connected to Okyo Garde.

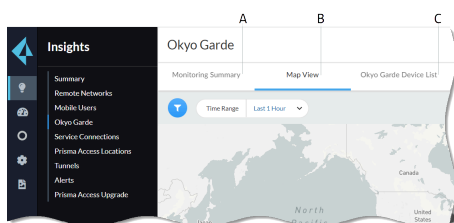
Okyo Garde Dashboard in Insights

The **Insights** Okyo Garde dashboard shows data related to your organization's Okyo Garde devices and the users who connect through those devices.

To view the Okyo Garde Dashboard in Insights, select  **Insights** > **Okyo Garde** from the sidebar. This dashboard has the following tabs:

- Monitoring Summary Tab
- Map View Tab
- Okyo Garde Device List Tab

For detailed information about the Okyo Garde Dashboard widgets introduced below, see [Prisma Access Insights](#).



A) Monitoring Summary

Shows an overview of the health of your Okyo Garde connection. The Monitoring Summary tab has the following widgets:

- Top 5 Alerts by Severity
- Device Status
- Tunnel Status
- Unique Okyo Garde Device Connections to Prisma Access Locations (Real Time)

B) Map View

Shows how many Okyo Garde devices are connected through a given geographic location during a specified time period.

C) Okyo Garde Device List

Provides an overview of the devices that are connected at a specific time, based on the Time Range selected. This tab includes the following widgets:

- Unique Okyo Garde Devices Connected Over Time
- Total Okyo Garde Devices