Okta offers authentication whitelisting and blacklisting based on **zones**. Zones are sets of IP address ranges or geolocations defined by an admin, and are used in **policies**, **Okta sign-on rules**, **VPN Notifications**, and **Integrated Windows Authentication (IWA)**. Zones are created and defined on the **Network** page, and adding or editing a policy rule is where a user's IP can be considered *in zone* or *not in zone*. If a zone definition is updated, any policy rule using it is automatically updated to the new specification.

Setting up Zones

There are two types of zones you can add on the **Network** page: **IP Zone** or **Dynamic Zone**. **IP zones** define IP addresses, and **Dynamic zones** define geographical locations and/or proxy types. To enter zones, do the following:

From the Admin **Dashboard**, navigate to **Security** > **Network**.

- Use the **Add Zone** button and choose between **IP Zones** and **Dynamic Zones**. See below for the details of each option.
- Use the **Edit** or **Delete** buttons next to existing zones to change or remove them.
- You can choose to make the zone **Active** or **Inactive** using the drop-down button.
- If your list contains a **LegacyIpZone**, this is migrated information and cannot be edited or deleted. For details, see **Deleting Zones**, below.

IP Zone

1. Choose **IP Zone** to define a range of IP addresses. The **Add IP Zone** dialog box appears.
2. Populate the fields with a zone name and your addresses.
3. You can set up any number of Gateway IP or Proxy IP addresses. Each zone can contain up to 75 specifications. The following table describes specifications for IP address zones.
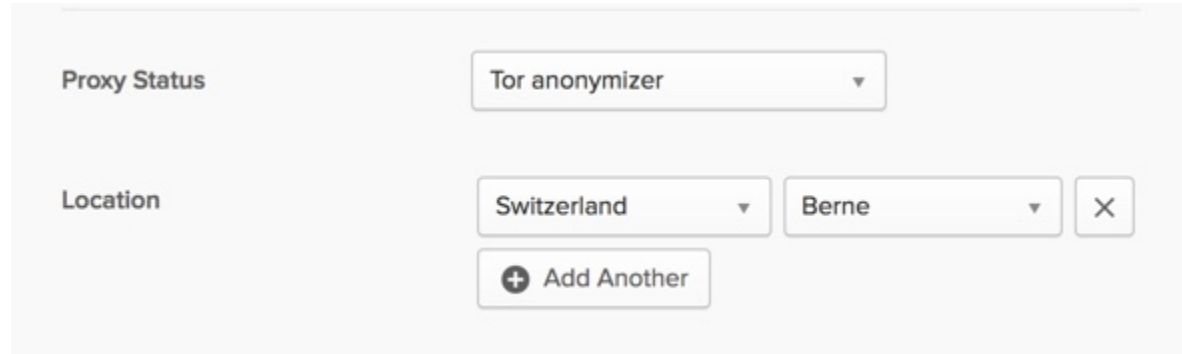
Note: A single IP address will appear as hyphenated, as *1.2.3.4* appears under **Sample** below.

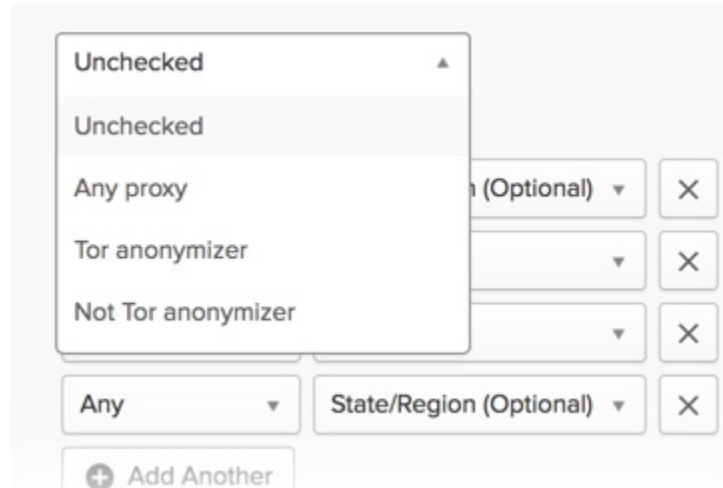| Item	Sample
Gateway IPs addresses – enter one per line or separate by commas. For ranges, either use a hyphen to separate the range, or use CIDR notation.	*1.2.3.6-1.2.3.7, 192.168.0.0/24, 1.2.3.4-1.2.3.4*
Proxy IPs addresses – same format as above	*1.2.3.11–1.2.3.14*

Dynamic Zone

A **Dynamic zone** allows admins to define a proxy status and/or geographical location. If both proxy type and location are specified, only clients coming from that location and using the specified proxy are considered part of that zone. To do so,

1. Choose **Dynamic Zone**. The **Add Dynamic Zone** dialog box appears.
2. Add a zone name, then make choices for proxy and location.

Proxy Status

The **Proxy status** feature determines the "reputation" of a client's IP address and compares it to what is specified in a defined zone. For example, choose **Tor Anonymizer** if you want a particular zone to match all the clients using Tor, then use that zone when creating policy rules. Use the following options to define how the zone is used in a policy.

- **Unchecked**: The proxy status of the client IP is not checked.
- **Any Proxy:** Any client IP proxy status is matched.
- **Tor anonymizer**: Matches to client IPs using Tor.
- **Not Tor anonymizer**: Matches to client IPs that do not use Tor.

Location

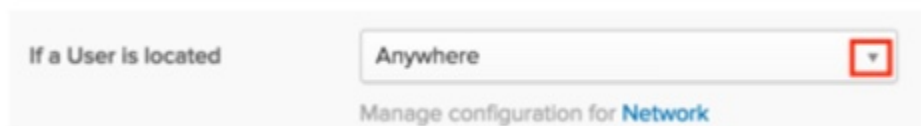**Location** specifications can be made for any number of zones.

- Choose **Any** if you don't want to specify a geolocation, or use the drop-down menu to choose a country and/or region.
- You can set up multiple locations for a single zone by clicking the **Add Another** button.

The following table describes specifications for geographic location zones.

Item	Sample
A country	United States Costa Rica
A state or region – optional	United States, California Canada, Québec

Using Zones

You will assign the zones you've specified from the **Policy** page. To do so,
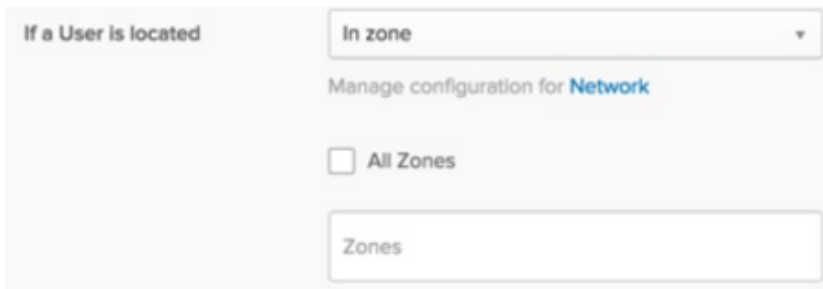
1. From the Admin **Dashboard**, navigate to **Security** > **Policies**.
2. When entering rules for a policy, such as sign-on and MFA policies, specify zone information from the selection shown below.

Choices for the location are *Anywhere*, *In zone*, and *Not in zone*.
After selecting *In zone or Not in zone*, the following zone selection options appear.

- If you check **All Zones**, all of your defined zones are selected, and the box below it is no longer visible, as shown below.

- If you do not check **All Zones**, you can begin typing a zone name in the **Zones** box. A drop-down list appears that contains all existing zones that contain the text you entered anywhere in the zone name. You can choose any number of zones. The following example shows a search for all zones that contain the letter t. In this case, only one zone is found. You still must select it to make it active.
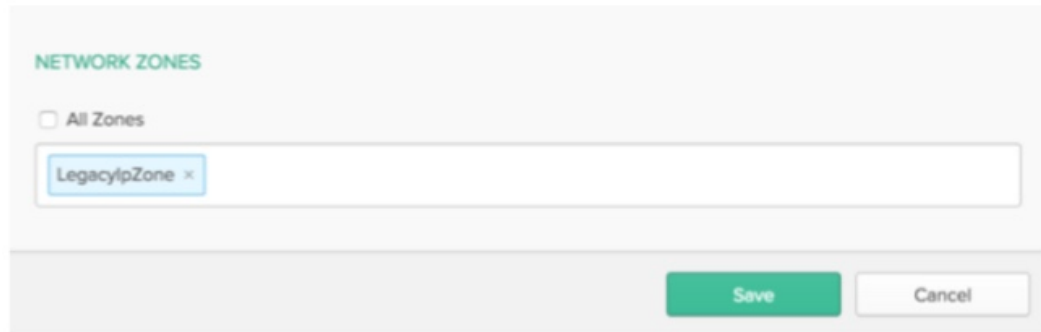

VPN Notifications

When entering rules for VPN notifications, you cannot list specific zones for these notifications; you can specify *Inside Any Zones* or *Outside All Zones*.

Note: You can jump to the Zone setup screens anytime by choosing **Network** link shown above.

IWA

When evaluating IWA logins, Okta checks that the login is from the configured zones. You can edit the configuration and choose any desired zones, or choose *All Zones* as you do in policies. When an IWA agent is configured, the IP address of the client is added to the LegacyIPZone. The LegacyIPZone is the only zone configured by default., as shown below.

Deleting Zones

When an IP is deleted, all rules that use the deleted zone are affected.
- If the zone to delete is the **only zone** in any rule, you cannot delete the zone and receive an error message. Edit the rule to use a different zone then perform the deletion again.
- If the zone to delete is **not the only zone** in any rule you can delete the zone. The zone is removed from all the rules where it is specified.

The Legacy Zone

If you have already defined Public Gateway IP Addresses, the information is migrated to a zone named **LegacyIpZone**. You cannot delete this zone, but you can edit it. For existing rules, **LegacyIpZone** retains the previous settings. This zone is still active and can be used in new assignments.